

# **Anti-DDoS Advanced**

## **Anti-DDoS Advanced (Global Enterprise Edition)**

### **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

## Anti-DDoS Advanced (Global Enterprise Edition)

### Product Introduction

Overview

Strengths

Use Cases

Relevant Concepts

### Purchase Guide

Billing Overview

Purchase Instructions

### Getting Started

### Operation Guide

Operation Overview

Viewing Protection Overview

Protection Configuration

DDoS protection

DDoS Protection Level

Protocol Blocking

Feature Filtering

AI Protection

Connection Attack Protection

IP Blocklist/Allowlist

IP and Port Rate Limiting

Regional Blocking

Port Filtering

Watermark Protection

CC protection

CC Protection and Cleansing Threshold

Regional Blocking

IP Blocklist/Allowlist

Precise Protection

CC Frequency Limit

Application Connection

Instance Management

Viewing Instance Information

Setting Instance Alias and Tag

Setting Security Event Notification

Viewing Operation Logs

# Anti-DDoS Advanced (Global Enterprise Edition)

## Product Introduction

### Overview

Last updated : 2021-12-02 16:31:55

## Overview

Anti-DDoS Advanced (Global Enterprise Edition) is a paid product that enhances DDoS protection capabilities for businesses deployed on Tencent Cloud.

- Anti-DDoS Advanced (Global Enterprise Edition) owns ten Tencent Cloud entries around the world for handling bandwidth needs with all-out protection, making access to each node as smooth as possible.
- Anycast provides near-source cleansing and near-source reinjection, with up to TB-level protection capability. It ensures smooth traffic and low latency by cleansing attack traffic and then forwarding normal traffic back to the real server close to the region of your Anti-DDoS Advanced (Global Enterprise Edition) instance deployed. The instance will directly protect the target IP on Tencent Cloud.

## Features

### Multidimensional protection

Protection Type	Description
Malformed packet filtering	Filters out frag flood, smurf, stream flood, and land flood attacks as well as malformed IP, TCP, and UDP packets.
DDoS protection at the network layer	Filters out UDP floods, SYN floods, TCP floods, ICMP floods, ACK floods, FIN floods, RST floods and DNS/NTP/SSDP reflection attacks and null sessions.
DDoS protection at the application layer	Filters out CC attacks and slow HTTP attacks and supports HTTP custom filtering such as host filtering, user-agent filtering, and referer filtering.

### Flexible defense options

Anti-DDoS Advanced (Global Enterprise Edition) supports switching IPs of the protected object to meet your protection needs for public IPs of Tencent Cloud resources outside the Chinese mainland. The objects that support switching include CVM and CLB.

Note :

This service is supported in Moscow, Silicon Valley, Frankfurt, Seoul, Hong Kong (China), Tokyo, Singapore, Bangkok and Mumbai.

## Security protection policy

Anti-DDoS Advanced (Global Enterprise Edition) provides basic security policies by default on the basis of protection algorithms such as IP profiling, behavior pattern analysis, and AI-based smart recognition, effectively coping with common DDoS attacks. It also offers diverse and flexible protection policies, which can be tailored to your special needs to deal with ever-changing attack tricks.

## Self-Service IP unblocking

If a protected business IP is blocked when the attack traffic bursts or the protection bandwidth of your Anti-DDoS Advanced (Global Enterprise Edition) instance is too low, you can unblock the IP in a self-service manner in the console.

## Protection statistical reports

Anti-DDoS Advanced (Global Enterprise Edition) provides multi-dimensional traffic reports and attack protection details to help you stay on top of the protection effects of Anycast Anti-DDoS Advanced (Global Enterprise Edition) instances in a timely and accurate manner.

Note :

Only DDoS attack protection reports can be displayed currently. CC attack protection and business reports will be available in the future.

# Strengths

Last updated : 2021-07-19 21:48:14

Anti-DDoS Advanced (Global Enterprise Edition) is a paid security service that can enhance DDoS protection capabilities of Tencent Cloud services such as CVM and CLB. It has the following strengths:

## Cloud Native Solution for Quick Deployment

Anti-DDoS Advanced (Global Enterprise Edition) provides a product solution more toward cloud native architecture to facilitate quick deployment. With such an instance, you only need to bind it to the target object without adjustment required.

## Massive Protection Resources

Anti-DDoS Advanced (Global Enterprise Edition), combined with ten cleansing nodes outside the Chinese mainland, supports TB-level protection capability globally that provides security and stability for essential businesses such as promotional campaigns and launch events.

## Leading Cleansing Capability

Leveraging the powerful protective clusters developed by Tencent and multi-dimensional algorithms, such as IP profiling, behavior pattern analysis, and cookie challenges, Anti-DDoS Advanced (Global Enterprise Edition) can accurately and promptly detect attack traffic. With the aid of a smart AI engine that continuously optimizes the algorithms, it is also flexible in coping with attack tricks.

## Stable Access Experience

Tencent Cloud's BGP linkage covers multiple ISPs, which can easily address access latency and ensure network quality. It also supports smart routing and automatic network scheduling, delivering a stable and smooth access experience for various user groups.

## Detailed Protection Reports

Anti-DDoS Advanced (Global Enterprise Edition) provides multi-dimensional statistical reports to display clear and accurate protection traffic and attack details, helping you stay on top of attacks in real time.

## Lower Security Protection Costs

1. The simplified billing mode enables you to flexibly choose the "number of protected IPs + protected times" according to your business size and protection needs. The following solutions are available to cope with high-volume traffic attacks.
  - Anti-DDoS Advanced (Global Enterprise Edition) has multiple global nodes that can work together to defense against DDoS attack traffic for all-out protection.
  - By scheduling and blocking, Anti-DDoS Advanced (Global Enterprise Edition) maximizes your business availability particularly under attacks.
2. The flexible billing mode for bandwidth "pay-as-you-go + quarterly paid" helps reduce your security cost.

# Use Cases

Last updated : 2021-07-19 21:50:04

## Gaming

DDoS attacks are particularly common in the overseas gaming industry. Anti-DDoS Advanced (Global Enterprise Edition) guarantees the availability and continuity of games to deliver a smooth player experience. Meanwhile, it helps ensure that normal gaming continues throughout events, new game releases, and peak hours such as holidays.

## Ecommerce

The overseas ecommerce industry has been worldwide with increasing global visits and orders during festivals and promotional campaigns. Anti-DDoS Advanced (Global Enterprise Edition) safeguards continuity and security for global businesses, especially during major ecommerce promotions.

## Website

Anti-DDoS Advanced (Global Enterprise Edition) guarantees smooth access to websites and uninterrupted global businesses, maintaining a stable and safe performance for daily visits and burst visits during special festivals or events.

# Relevant Concepts

Last updated : 2021-07-14 15:19:26

## DDoS Attack

A Distributed Denial of Service (DDoS) attack is a malicious attempt to make a targeted server unavailable by blocking its network bandwidth or overwhelming its system with a flood of internet traffic.

### Network layer DDoS attack

A network layer DDoS attack attempts to make a targeted server unavailable to its intended users by blocking its network bandwidth and exhausting its system layer resources with a flood of internet traffic.

Common attacks include SYN Flood, ACK Flood, UDP Flood, ICMP Flood, and DNS/NTP/SSDP/Memcached reflection attacks.

### CC attack

A CC attack is a malicious attempt to make a targeted server unavailable by occupying its application layer resources and exhausting its processing capacity. Common attacks include HTTP/HTTPS-based GET/POST Flood, layer-4 CC, and Connection Flood attacks.

## Protection Capability

Protection capability refers to the capability to defend against DDoS attacks. Anti-DDoS Advanced (Global Enterprise Edition) intelligently schedules global node resources for max protection.

## Anycast

The protection address (Anycast EIP) is broadcast to ISPs in various regions through BGP Anycast. After this IP is bound with backend resources, user traffic (including normal traffic and attack traffic) in the access regions will be directed to the nearest Tencent Cloud node (Anycast access point) for near-source cleansing. Smart routing and automatic network scheduling are used together to stably deliver users' network access requests to the instances in Tencent Cloud.

## Cleansing

If the public network traffic of the target IP exceeds the preset protection threshold, Tencent Cloud Anti-DDoS service will automatically cleanse the inbound public network traffic of the target IP. With the Anti-DDoS routing protocol, the traffic will be redirected to the DDoS cleansing devices which will analyze the traffic, discard the attack traffic, and forward the clean traffic back to the target IP.

In general, cleansing does not affect access except on special occasions or when the cleansing policy is configured improperly. If no exception is found (which is dynamically determined based on the attack) in the traffic for a period of time, the cleansing system will determine that the attack has stopped and then stop cleansing.

## Blocking

Once the attack traffic exceeds the blocking threshold of the target IP, Tencent Cloud will block the IP from all public network access through ISP service to protect other Tencent Cloud users. In short, once the traffic attacking your IP goes over the maximum protection capacity of Tencent Cloud in the current region, Tencent Cloud will block the IP from all public network access. If your protected IP address is blocked, you can log in to the console to unblock it.

### Blocking duration

An attacked IP is blocked for 2 hours by default. The actual duration can be up to 24 hours depending on how many times the IP is blocked and how high the peak attack bandwidth is.

The blocking duration is subject to the following factors:

- Continuity of the attack. The blocking period will extend if an attack continues. Once the period extends, a new blocking cycle will start.
- Frequency of the attack. Users that are frequently attacked are more likely to be attacked continuously. In such a case, the blocking period extends automatically.
- Traffic volume of the attack. The blocking period extends automatically in case of ultra-large volume of attack traffic.

### Blocking level

- Single-ISP: one single ISP is blocked. In this case, the application cannot be accessed in one or more regions through this ISP.
- Single-Region nodes: nodes in one single region are blocked. In this case, the application cannot be accessed in this region.
- All regions: Tencent Cloud directly blocks access to the application. In this case, the application cannot be accessed globally.

Note :

- According to the extent of the impact surface of attacks, different levels of blocking will be triggered.

- For example, after a customer suffers DDoS attacks, when the attack traffic reaches the blocking threshold of the ISP, the ISP will be blocked; when the attack traffic reaches the node blocking threshold of a region, nodes in the region will be blocked, and the customer's application will be inaccessible in the region; when the total attack traffic suffered by the customer on all nodes reaches the all-region blocking threshold, the customer's application will be blocked in all regions, and it will be inaccessible globally.

## Scheduling

When the traffic reaches the threshold of the current ISP, cross-ISP scheduling will be performed to ensure the application availability.

Note :

To ensure the application availability, several rounds of scheduling may occur.

# Purchase Guide

## Billing Overview

Last updated : 2022-09-30 10:52:20

### Background

Anti-DDoS Advanced (Global Enterprise Edition) is committed to helping your business outside the Chinese mainland with DDoS attacks by providing unlimited all-out protection.

Usually malicious attacks will not end before causing losses to the target business, which is also a cost to attackers. Leveraging Tencent Cloud's Anti-DDoS cleansing capability outside the Chinese mainland, Anti-DDoS Advanced (Global Enterprise Edition) safeguards your business with unlimited all-out protection.

Note :

- Tencent Cloud reserves the right to restrict the traffic if the DDoS attacks on your business affect the infrastructure in the Tencent Cloud Anti-DDoS cleansing center outside the Chinese mainland. If the traffic of your Anti-DDoS Advanced (Global Enterprise Edition) instance is restricted, your business may suffer the problems such as limited or blocked business access traffic.
- Anti-DDoS Advanced (Global Enterprise Edition) is a pay-as-you-go service that is billed monthly. The minimum subscription term is 12 months. Upon expiry, your subscription will be auto-renewed unless canceled by [contacting us](#). Your instances cannot be terminated during a subscription term.
- Make sure that you have three-month credit to be frozen when activating this service.
- Payments for this service are not refundable.

### Anti-DDoS Advanced (Global Enterprise Edition) billing

Number of IPs	Service Fee (USD/month)	Payment Mode
1	7500	Prepaid
5	33000	Prepaid
30	180000	Prepaid
100	600000	Prepaid

### Application bandwidth billing

Application bandwidth is billed in a pay-as-you-go approach. Specifically, you will be charged by monthly 95th percentile of either the outbound or inbound bandwidth (whichever is higher) at a unit price of 18.86 USD/Mbps/month.

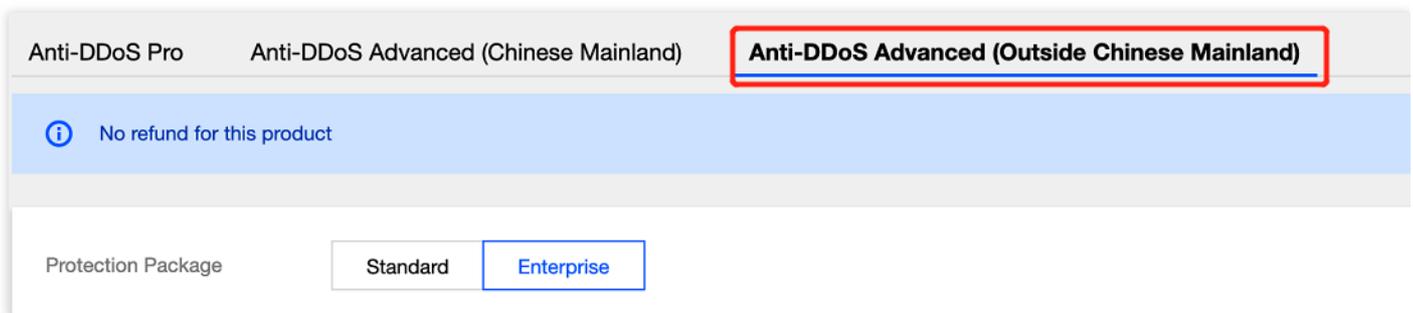
# Purchase Instructions

Last updated : 2022-09-30 10:52:21

Note :

- Anti-DDoS Advanced (Global Enterprise Edition) is a pay-as-you-go service that is billed monthly. The minimum subscription term is 12 months. Upon expiry, your subscription will be auto-renewed unless canceled by [contacting us](#). Your instances cannot be terminated during a subscription term.
- Make sure that you have three-month credit to be frozen when activating this service.
- Payments for this service are not refundable.

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) purchase page.
2. Click **Anti-DDoS Advanced (Outside Chinese Mainland)** to proceed to the product page.



3. On the page, select **Enterprise** for your protection package and configure parameters such as "Application Bandwidth", "IP Quantity", "Validity Period" and "Auto-Renewal".

Note :

- Your package will be automatically renewed for 1 month.
- Application bandwidth is billed using pay-as-you-go. **Total Amount** does not include the cost of application bandwidth.

Protection Package:  Standard  Enterprise

Specifications: Access mode: agency  
 Resource overview: 1 dedicated Anycast IP  
 Protection quota: unlimited  
 All-out protection: [Defend against attacks with the highest capability of Tencent Cloud Anti-DDoS cleansing centers outside the Chinese mainland. >>](#)

---

Application Bandwidth:  Limited  Unlimited

Slider: 500Mbps 1000Mbps 1500Mbps 2000Mbps [ - 1 + ] Mbps

The total application bandwidth used in all regions is charged in the manner of pay-as-you-go for the public network fee settlement. Please set a bandwidth cap that is equal to or higher than your actual application bandwidth. There may be a high bandwidth cost if the bandwidth is not limited. [Pricing](#)

IP Quantity:

Tag (optional) ⓘ:   ×

[+ Add](#)

4. Click **Pay Now** to complete your purchase.

**Current Configuration**

---

Purchase Type: **Advanced DoS**

Bandwidth Cap: **1Mbps**

Number of IPs: **1**

Protected Times: **Unlimited**

---

**Total Amount** ⓘ

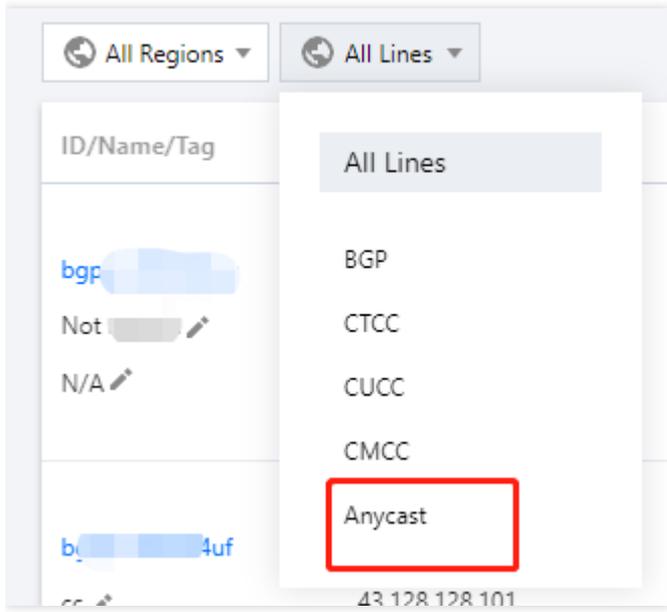
**7,500.00 USD/month**

[Pay Now](#)

5. Log in to the [Anti-DDoS console \(Global Enterprise Edition\)](#) and select **Anti-DDoS Advanced -> Instance List** to enter the instance list page.

6. On the page, select **All Lines -> Anycast** to view your Anti-DDoS Advanced (Global Enterprise Edition) instance

details.



# Getting Started

Last updated : 2022-06-10 14:12:06

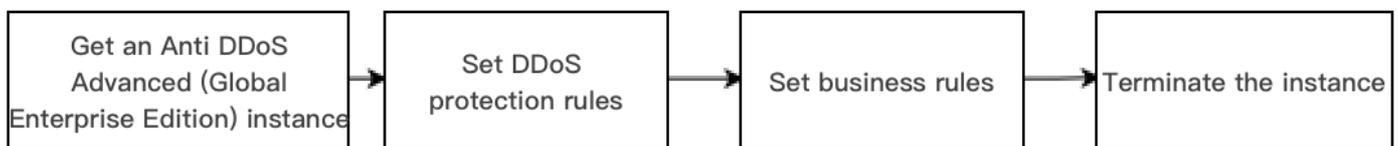
Anti-DDoS Advanced (Global Enterprise Edition) is a paid service aimed at global users with businesses deployed in Tencent Cloud to improve their global DDoS protection capabilities.

- It allows you to purchase and hold public IP address resources independently.
- After it is bound to cloud resources, the cloud resources can communicate with the public network through it.

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

## Background

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



1. [Purchasing Anti-DDoS Advanced \(Global Enterprise Edition\) instance](#): purchase Anti-DDoS Advanced (Global Enterprise Edition) resources according to your actual needs.
2. [Configuring protection rules](#) for the Anti-DDoS Advanced (Global Enterprise Edition) instance: configure protection policies that fit your application.
3. Configuring application rules for the Anti-DDoS Advanced (Global Enterprise Edition) instance: associate the instance with the cloud resources to be protected.
4. Terminating Anti-DDoS Advanced (Global Enterprise Edition) instance: after unassociating the instance from cloud resources, you can associate the instance with other cloud resources. The unassociating operation may cause the network of the corresponding cloud resource to be disconnected, and instances that are not bound to cloud resources will incur IP resource fees.

## Directions

## Purchasing Anti-DDoS Advanced (Global Enterprise Edition) instance

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) console.
2. Refer to the [Purchase Guide](#) to purchase an instance.
3. Click **Anti-DDoS Advanced (New) > Service Packages** on the left sidebar to view the purchased Anti-DDoS Advanced (Global Enterprise Edition) instance, which is not bound.

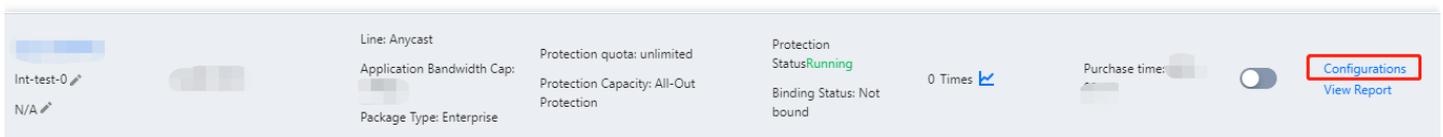
### Note :

We recommend binding cloud resources to the Anti-DDoS Advanced (Global Enterprise Edition) instance promptly so as to save IP resource fees. IP resource fees are charged by hour accurate to the second level, and if the duration is less than one hour, fees will be charged according to the proportion of idle time. Therefore, please bind cloud resources in time. For more information, please see [Billing Overview](#).



## Configuring protection rule

Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) console, click **Anti-DDoS Advanced (New) > Service Packages** on the left sidebar, select the corresponding instance, and click **Protection Configuration**. For more information on configuration methods, see [Protection Configuration](#).



## Associating cloud resource

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) console. Select **Anti-DDoS Advanced > Application Accessing > IP Access**.

2. Click **Start Access**.

**Application Accessing**

**Without Anti-DDoS Advanced**

Real servers are exposed directly to the internet. When a DDoS attack starts, they can easily be overwhelmed.



**With Anti-DDoS Advanced**

You need to add a CNAME record for the application domain name at your DNS ISP. When network traffic flows through Anti-DDoS Advanced, it automatically filters out malicious traffic to protect the security of the real server.



**Troubleshooting** [View All](#)

- [Connecting applications to Anti-DDoS Advanced](#)
- [IP blocking and unblocking](#)
- [Modifying DNS resolution](#)
- [Solutions for an exposed origin server IP address](#)

No applications connected yet, please select a connection method



Access via Port

Applicable to non-website applications such as PC games, mobile games and apps

Configure Now



Access via Domain Name

Applicable to website applications such as ecommerce websites and corporate websites

Configure Now



IP Access

Applicable to applications of Tencent Cloud enterprise users outside the Chinese mainland

Configure Now

3. Select an Anti-DDoS Advanced (Global Enterprise Edition) instance and a cloud resource, and then click **OK**.

Note :

Cloud resources that has been bound to a public IP or Anycast IP cannot be bound again.

### Bound Resource ✕

Associate Anycast IP

Cloud Virtual Machine  Load balance

Instance ID/Name	Availability Zone	Private IP	Bound public IP
<input type="radio"/> ir-██████████	Hong Kong (China)	██████████	
<input checked="" type="radio"/> ██████████	Hong Kong (China)	██████████	██████████

Total items: 2      10 / page      1 / 1 page

### Unassociating cloud resource

1. On the IP accessing page, select an instance to delete and click **Delete** on the right.
2. In the pop-up window, click **OK**.

Note :

Note that the unbinding may disconnect your cloud resource from the network. You can bind it with other resources later.

# Operation Guide

## Operation Overview

Last updated : 2022-05-18 14:15:23

This document lists the references for common operations in Anti-DDoS Advanced (Global Enterprise Edition).

### Protection overview

[Viewing Protection Overview](#)

### Protection configuration

[DDoS Protection Level](#)

[Protocol Blocking](#)

[Feature Filtering](#)

[AI Protection](#)

[Connection Protection](#)

[IP Blocklist/Allowlist](#)

[IP and Port Speed Limit](#)

[Location Blocking](#)

[Port Filtering](#)

[Watermark Protection](#)

### Application Connection

[IP Connection](#)

### Instance Management

[Viewing Instance Information](#)

[Setting Instance Alias and Tag](#)

### Security event notification

[Setting Security Event Notification](#)

### Operation log

[Viewing Operation Log](#)

# Viewing Protection Overview

Last updated : 2022-12-09 15:07:49

## Protection Overview

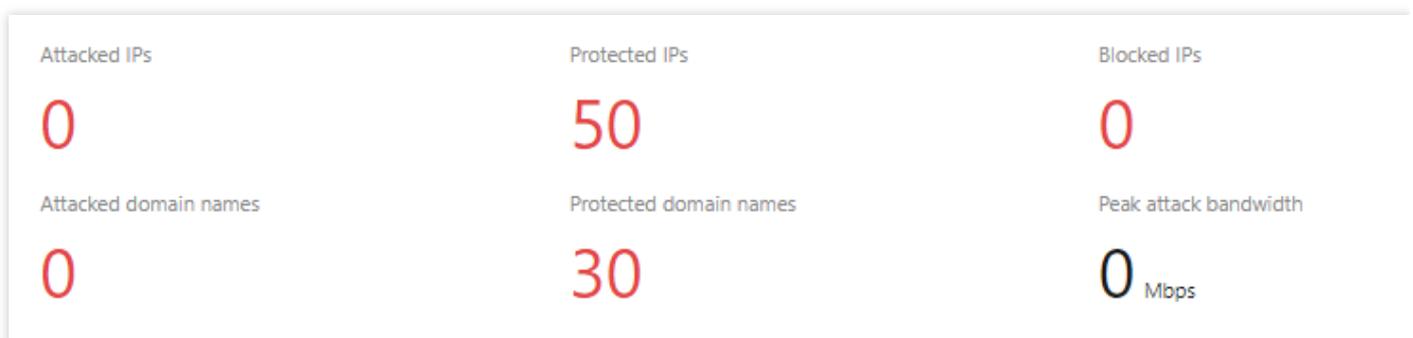
After connecting your application to and routing its traffic to the Anti-DDoS Advanced (Global Enterprise Edition) service, you can check the application traffic status and Anti-DDoS protection status in the console. Attack packet data can be downloaded for source tracing and analysis.

### Viewing attack statistics

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) console and select **Overview > Protection Overview**.



2. In the "Attacks" module, you can view the application security status, the latest attack and the attack type. To obtain higher protection, you can click **Upgrade Protection**.
3. This module also displays the details of the following data.



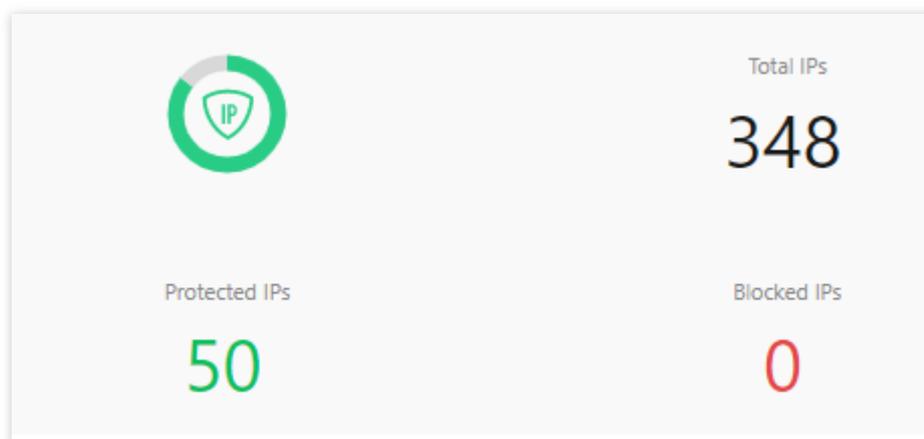
#### Field description:

- Attacked IPs: The total number of attacked application IPs of basic protection, Anti-DDoS Pro and Anti-DDoS Advanced.

- Protected IPs: The total number of protected application IPs of Anti-DDoS Pro and Anti-DDoS Advanced.
- Blocked IPs: The total number of blocked IPs of basic protection, Anti-DDoS Pro and Anti-DDoS Advanced.
- Attacked domain names: The total number of domain names of attacked Anti-DDoS Advanced instances and ports.
- Protected domain names: The number of domain names connected to Anti-DDoS Advanced instances.
- Peak attack bandwidth: The maximum attack bandwidth of the current attack events.

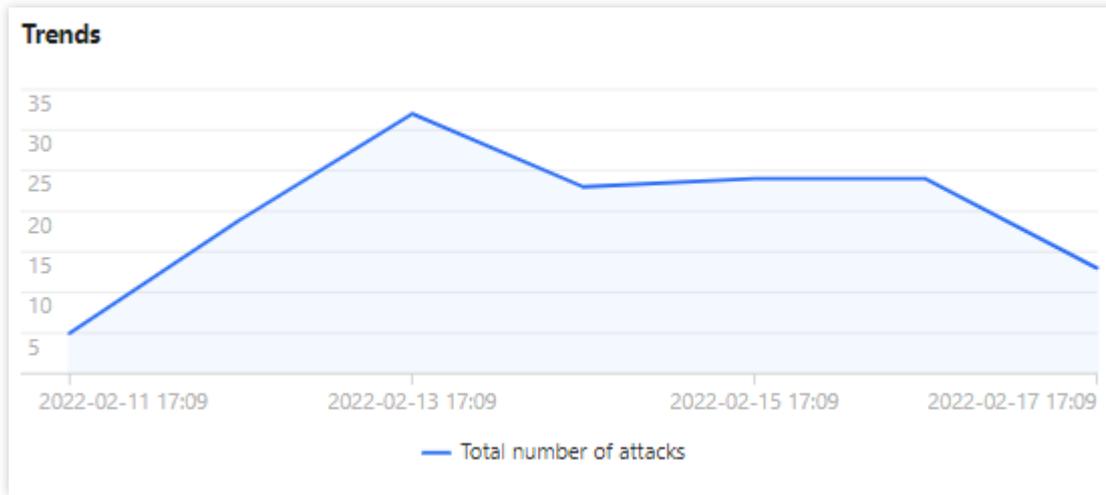
## Viewing defense statistics

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) console and select **Overview > Protection Overview**.
2. In the "Defense" module, you can easily see the application IP security status.



### Field description:

- Total IPs: The total number of application IPs, including IPs of basic protection, Anti-DDoS Pro and Anti-DDoS Advanced.
  - Protected IPs: The total number of protected application IPs of Anti-DDoS Pro and Anti-DDoS Advanced.
  - Blocked IPs: The total number of blocked IPs of basic protection, Anti-DDoS Pro and Anti-DDoS Advanced.
3. This module also displays the total number of attacks on your applications, giving you a picture of the distribution of attacks.



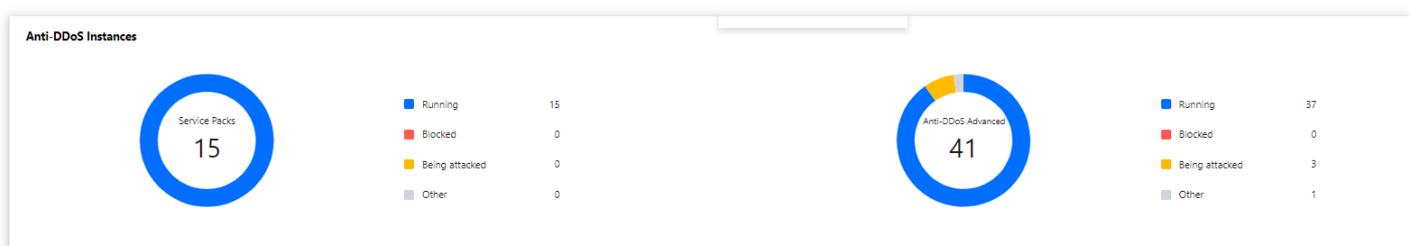
4. Meanwhile, this module provides recommended actions for the attacked IPs connected to basic protection, allowing you to quickly upgrade your Anti-DDoS service.

**Recommended Actions**

Upgrade Anti-DDoS for [IPs] [Anti-DDoS Pro](#) [Anti-DDoS Advanced](#)

### Viewing Anti-DDoS Advanced instance statistics

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) console and select **Overview > Protection Overview**.
2. The "Anti-DDoS Instances" module visualizes the Anti-DDoS instance status data, providing an easy and complete way to know the distribution of insecure applications.



## Viewing recent events

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) console and select **Overview > Protection Overview**.
2. The "Recent Events" module shows you all the recent attack events. For attack analysis and source tracing, click **View Details** to enter the event details page.

Attacked IP	Instance Name	Defense Type	Start Time	Duration	Attack Status	Event Type	Operation
[Redacted]	[Redacted]	Anti-DDoS [Redacted]	2022-02-16 04:07:00	2 mins	Attack ends	DDoS Attack	<a href="#">View Details</a>
[Redacted]	[Redacted]	Anti-DDoS [Redacted]	2022-02-14 17:35:00	2 mins	Attack ends	DDoS Attack	<a href="#">View Details</a>
11[Redacted]	[Redacted]	Anti-DDoS [Redacted]	2022-02-13 12:05:00	2 mins	Attack ends	DDoS Attack	<a href="#">View Details</a>

3. In the "Attack Information" module 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.

### DDoS Attack Details

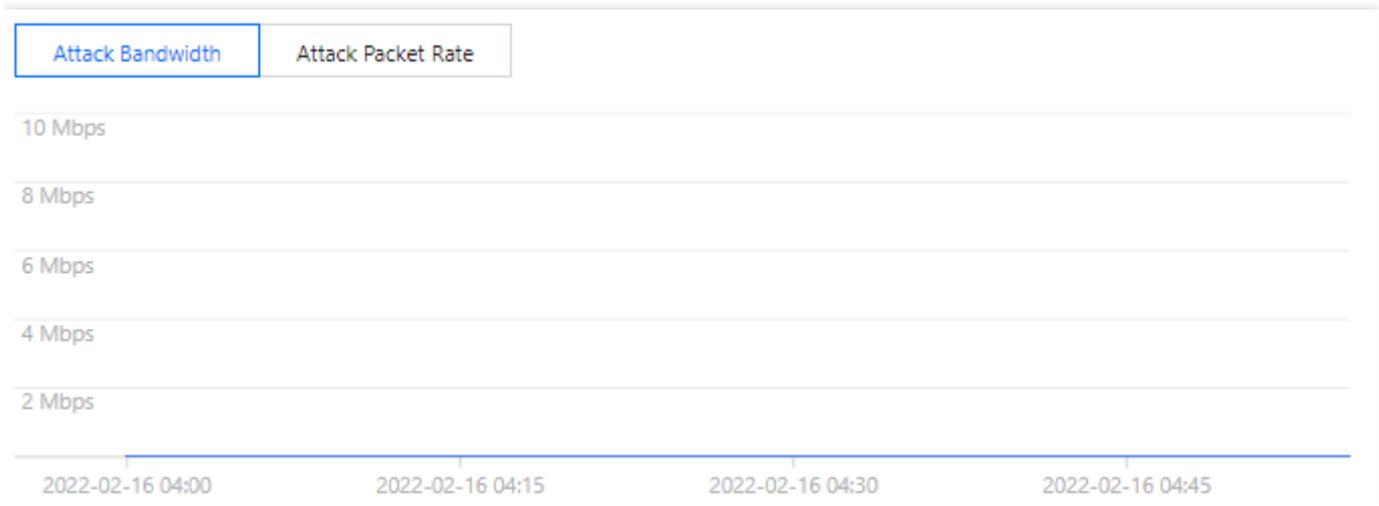
#### Attack Information

Attacked IP	11 [Redacted]	Attack Bandwidth Peak	0Mbps	
Status	● Attack ends	Attack packet rate peak	730pps	
Attack Type	SYNFLOOD	Attack start time	2022-02-16 04:07:00	
		Attack end time	2022-02-16 04:09:00	

4. In the "Attack Trend" module of the event details page, you can view the trend of attack bandwidth and attack packet rate and easily find the peak spikes.

Note :

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



5. In the "Attack Statistics" module of the event details page, you can view how attacks distribute over different attack traffic protocols and attack types.

Note :

This module provides sampled data in the attack period.



#### Field description:

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

6. The "Top 5" modules 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 module provides sampled data in the attack period.

#### Top 5 Attacking Source IPs



#### Top 5 Districts Where Attacks Originate



7. In the "Attacker Information" module 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 module provides sampled data in the attack period.

#### Attack source information

Attack Source IP	Region	Cumulative attack traffic	Cumulative attack volume
62.197.136.161	Netherlands	16.0 MB	256
89.248.163.136	Netherlands	16.0 MB	256

Total items: 2

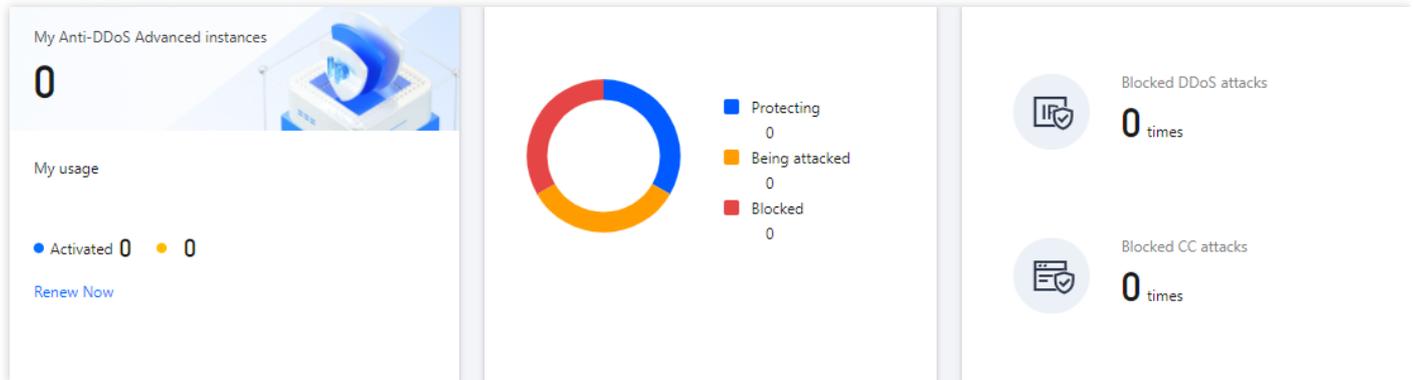
« ‹ 1 / 1 page › »

## Anti-DDoS Advanced Overview

After an IP address is bound to an Anti-DDoS Advanced instance, when you receive a DDoS attack alarm message or notice any issue with your business, you need to view the attack details in the console, including the attack traffic and current protection effect. Enough information is critical for you to take measures to keep your business running smoothly.

## Viewing DDoS protection details

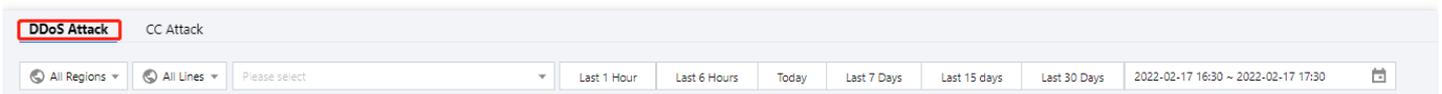
1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) console and select **Overview > Protection Overview**.



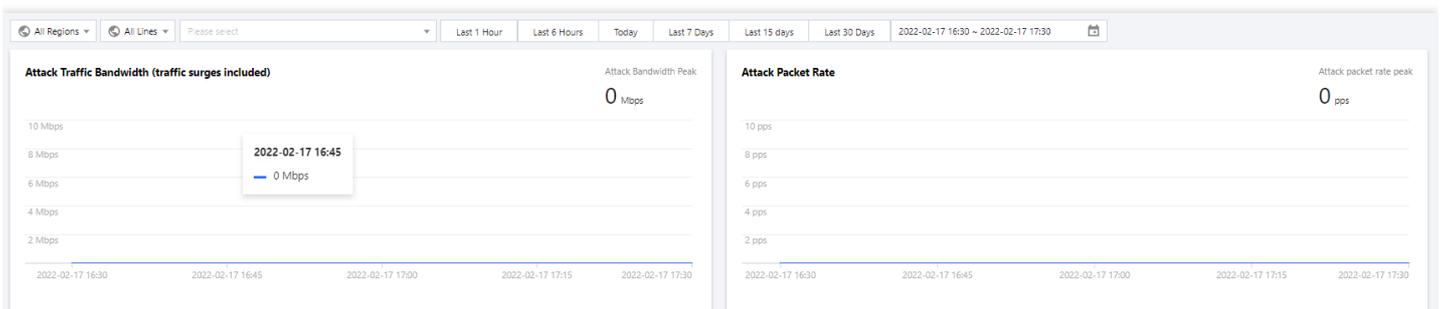
2. On the **DDoS Protection** tab, set a query period, and select **All Lines > Anycast** to check whether there are attacks. The complete attack data is displayed by default.

Note :

You can query attack traffic and DDoS attack events in the past 180 days.



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



3. You can view the recent DDoS attacks in the **Recent Events** section. To view event details, you can click **View Details**.

Recent Events							
Attacked IP	Instance Name	Defense Type	Start Time	Duration	Attack Status	Event Type	Operation
[Redacted]	[Redacted]	Anti-DDoS	2022-02-16 04:07:00	2 mins	Attack ends	DDoS Attack	<a href="#">View Details</a>
[Redacted]	[Redacted]	Anti-DDoS	2022-02-14 17:35:00	2 mins	Attack ends	DDoS Attack	<a href="#">View Details</a>
11[Redacted]	[Redacted]	Anti-DDoS	2022-02-13 12:05:00	2 mins	Attack ends	DDoS Attack	<a href="#">View Details</a>

- Information including attacker IP, attack source region, generated attack traffic, and attack packet size will be displayed for source analysis and tracing.

### DDoS Attack Details

#### Attack Information

Attacked IP	11[Redacted]	Attack Bandwidth Peak	0Mbps	
Status	Attack ends	Attack packet rate peak	730pps	
Attack Type	SYNFLOOD	Attack start time	2022-02-16 04:07:00	
		Attack end time	2022-02-16 04:09:00	

- To view sampled attack data within a specified period, click **Packet Download**.

Recent Events						
Instance ID	Attacked IP	Start Time	Duration	Attack Status	Operation	
bgp[Redacted]	[Redacted]	2022-02-16 04:07:00	2 mins	Attack ends	Unblock	<a href="#">View Details</a> <a href="#">Packet Download</a>
bgp[Redacted]	[Redacted]	2022-02-14 17:35:00	2 mins	Attack ends	Unblock	<a href="#">View Details</a> <a href="#">Packet Download</a>
bgp[Redacted]	[Redacted]	2022-02-13 12:05:00	2 mins	Attack ends	Unblock	<a href="#">View Details</a> <a href="#">Packet Download</a>
bg[Redacted]	[Redacted]	2022-02-11 23:15:00	2 mins	Attack ends	Unblock	<a href="#">View Details</a> <a href="#">Packet Download</a>
bg[Redacted]	[Redacted]	2022-02-10 12:54:00	2 mins	Attack ends	Unblock	<a href="#">View Details</a> <a href="#">Packet Download</a>

Total Items: 18 1 / 4 pages

- The sampled attack packet data can be downloaded to help customize a protection plan.

## Attack Packet List

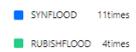
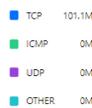


ID	Time	Operation
12993844	2022-01-10 23:37:51	<a href="#">Download</a>
12993866	2022-01-10 23:37:51	<a href="#">Download</a>

Total items: 2    10 / page    << < 1 / 1 page > >>

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

## Attack Statistics

**Field description:**

- Attack traffic protocol distribution: It displays how attacks on the selected Anti-DDoS Advanced instance distribute over different attack traffic protocols within the queried period.
- Attack packet protocol distribution: It displays how the attacks suffered by the selected Anti-DDoS Advanced instance distribute across different attack packet protocols within the queried period.
- Attack type distribution: It displays how attacks on the selected Anti-DDoS Advanced instance distribute over different attack types within the queried period.

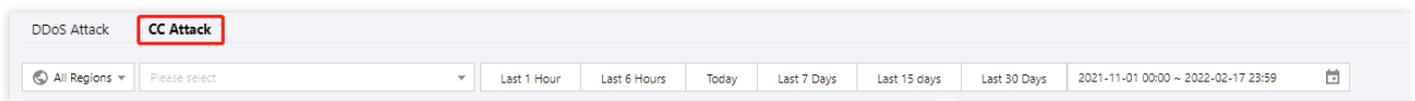
5. In the attack source section, you can view the distribution of DDoS attack sources in and outside the Chinese

mainland within the queried period, so that you can take further protective measures.

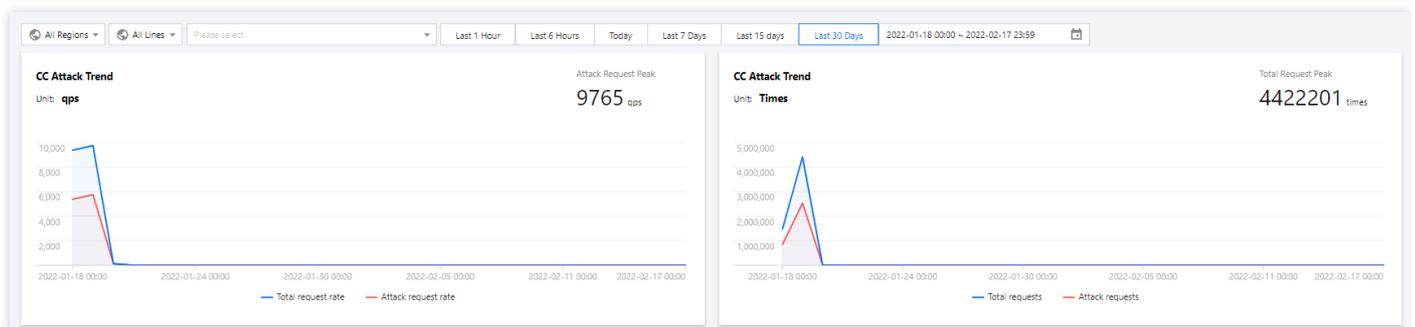


### Viewing CC protection details

1. On the **CC Protection** tab, set a query period, and select **All Lines** > **Anycast** to check whether there are attacks.



2. You can select **Today** to view the following data to identify the impact of attacks on your business.



#### Field description:

- Total request rate: The rate of total traffic (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, attacked URI, total request peak, attack request

peak, and attacker IP. You can also check the attack information, attack trends, and detailed CC records.

**Recent Events**

Instance ID	Attacked Domain Name	Attacked URI	Attacked IP	Attack Source	Start Time	Duration	Attack Status <span>▼</span>	Operation
bgp[REDACTED]	-	-	[REDACTED]	[REDACTED]	2022-02-17 15:51:00	1 mins	Attack ends	<a href="#">View Details</a>
bgp[REDACTED]	-	-	[REDACTED]	[REDACTED]	2022-02-17 13:37:00	1 mins	Attack ends	<a href="#">View Details</a>
bgp[REDACTED]	-	-	[REDACTED]	[REDACTED]	2022-02-17 12:41:00	1 mins	Attack ends	<a href="#">View Details</a>

# Protection Configuration

## DDoS protection

### DDoS Protection Level

Last updated : 2022-04-28 10:10:18

This document introduces the use cases of different protection levels and the actions Anti-DDoS Advanced (Global Enterprise Edition) takes to defend against DDoS attacks. You can follow this guide to set the DDoS protection levels in the console.

## Use Cases

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

- Loose
- Medium
- Strict

Protection Level	Protection Action	Description
Loose	<ul style="list-style-type: none"><li>• Filters SYN and ACK data packets with explicit attack attributes.</li><li>• Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specifications.</li><li>• Filters UDP data packets with explicit attack attributes.</li></ul>	<ul style="list-style-type: none"><li>• This cleansing policy is loose and only defends against explicit attack packets.</li><li>• We recommend choosing this protection level when normal requests are blocked. Complex attack packets may pass through the security system.</li></ul>

Note :

- If you need to use UDP in your business, please contact [Tencent Cloud Technical Support](#) to customize an ideal policy for not letting the level Strict affect normal business process.
- The level Medium is chosen by default for your Anti-DDoS Advanced (Global Enterprise Edition) instance. You can set the DDoS protection level for your business needs and also the cleansing threshold. Attack

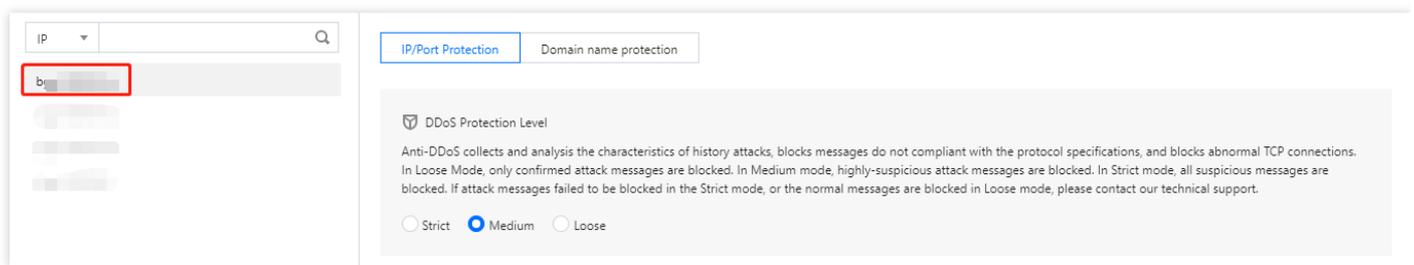
traffic will be cleansed when it is detected higher than the threshold you set.

## Prerequisites

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) instance and set the object to protect.

## Directions

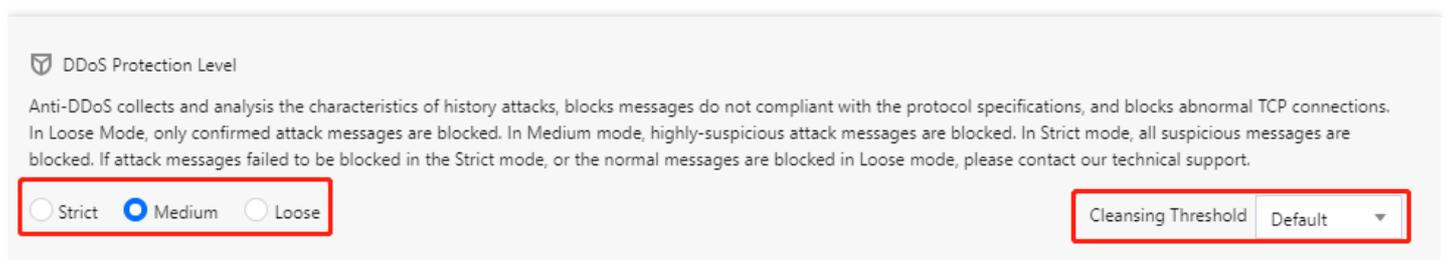
1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) Console](#) and click **Anti-DDoS Advanced (New)** -> **Configurations**->**DDoS Protection** on the left sidebar.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "xxx.xx.xx.xx bgpip-000003n2".



3. Set the protection level and cleansing threshold in the **DDoS Protection** section on the right.

### Note :

If you have a clear concept about the threshold, set it as required. Otherwise leave it to the default value.  
Anti-DDoS will automatically learn through AI algorithms and calculate the default threshold for you.



### Parameter Description:

- **Level**

If the protection is enabled, the level Medium is chosen by default for your Anti-DDoS Advanced (Global Enterprise Edition) instance. You can adjust the DDoS protection level for your business needs.

- **Cleansing Threshold**

- This indicates a value to trigger cleansing. Cleansing will not be triggered by the traffic below the threshold you set even though it is found malicious.
- If the protection is enabled, your Anti-DDoS Advanced instance will use the default cleansing threshold after your business is connected, and the system will generate a baseline based on historical patterns of your business traffic. You can also set the cleansing threshold for your business needs.

# Protocol Blocking

Last updated : 2022-04-28 10:55:43

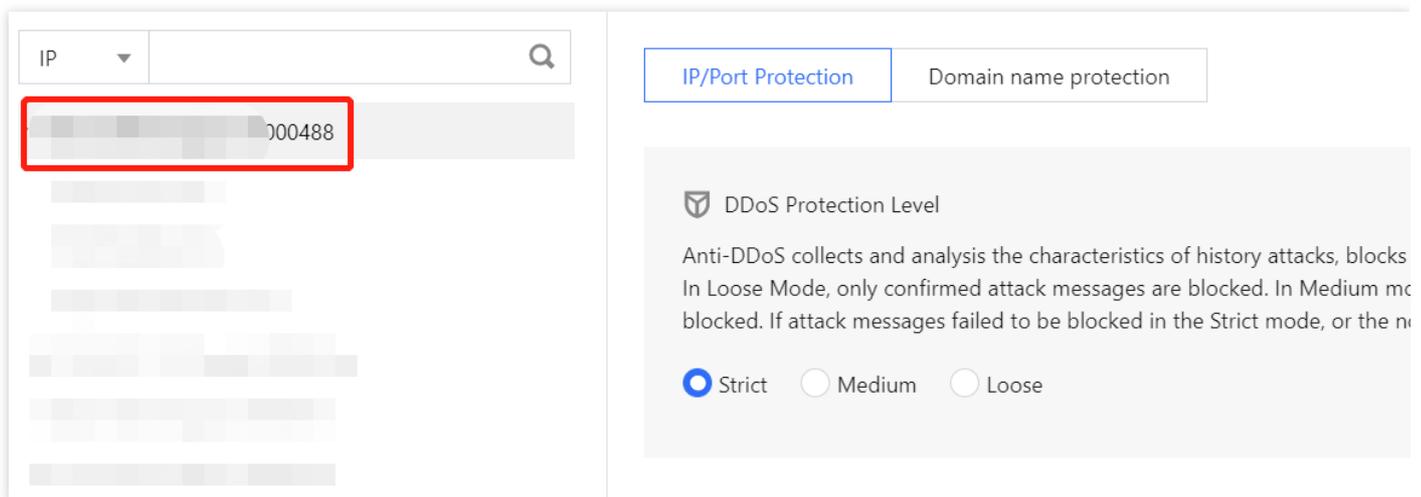
Anti-DDoS Advanced (Global Enterprise Edition) supports blocking the source traffic accessing Anti-DDoS instances based on specified protocols, such as ICMP, TCP, UDP, and other protocols. After the configuration is completed, all matched access requests will be directly blocked. Due to the connectionless feature of UDP protocol (unlike TCP, which requires a three-way handshake process), it has natural security vulnerabilities. If you do not have UDP businesses, we recommend blocking the UDP protocol.

## Prerequisite

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) instance and set the object to protect.

## Directions

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced > Configurations > DDoS Protection**.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "xxx.xx.xx.xx bgpip-000003n2".



3. Click **Set** in the **Block by protocol** section.

4. Click **Create**. On the pop-up page, enter the instance ID, configure the settings you need, and then click **OK**.

### Create Protocol Blocking Policy ✕

Associate Anti-DDoS Advance

Block ICMP Protocol

Block TCP Protocol

Block UDP Protocol

Block other protocols

OK
Cancel

5. After the rule is created, it is added to the list. You can turn the settings on or off as needed.

← **Block by protocol**

Create

Q

Associated Resource	Block ICMP Protocol	Block TCP Protocol	Block UDP Protocol	Block other protocols	Operation
bgpip-000002hl/119.28.217.238	Close	Enable	Enable	Enable	<a href="#" style="color: #007bff;">Configuration</a>

Total items: 1
10 / page

⏪ ⏩ 1 / 1 page

# Feature Filtering

Last updated : 2022-04-28 10:55:43

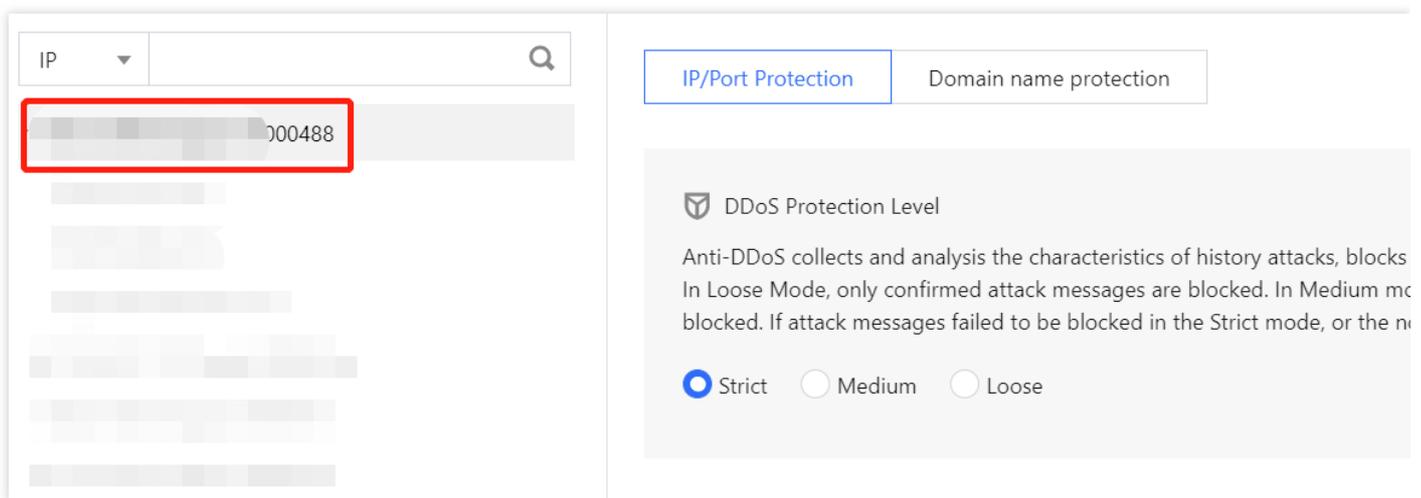
Anti-DDoS Advanced (Global Enterprise Edition) supports configuring custom blocking policies against specific IP, TCP, UDP message header or payload. After enabling feature filtering, you can combine the matching conditions of the source port, destination port, message length, IP message header or payload, and set the protection action to continue protection, allow/block/discard matched requests, block the IP for 15 minutes, or discard the request and then block the IP for 15 minutes, etc. With feature filtering, you can configure accurate protection policies against business message features or attack message features.

## Prerequisite

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) instance and set the object to protect.

## Directions

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced > Configurations > DDoS Protection**.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "xxx.xx.xx.xx bgpip-000003n2".



3. Click **Set** in the **Feature Filtering** section.

4. Click **Create**. On the pop-up page, enter the required fields based on the action you select, and click **OK**.

### Create Feature Filter ✕

Associate Anti-DDoS Advance

Filter feature

Field	Logic	Value	
Source Port	equals to	5000	<a href="#">Delete</a>
Destination port	equals to	808	<a href="#">Delete</a>
Message length	equals to	1350	<a href="#">Delete</a>
IP header	Find matching it	ddos	Byte offset <input type="text" value="Start"/> <input type="text" value="End"/> <a href="#">Delete</a>
Payload	Find matching it	ae86	Byte offset <input type="text" value="Start"/> <input type="text" value="End"/> <a href="#">Delete</a>
Add			

Action

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

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

Feature Filtering

Enter IP

ID	Associated Resource	Feature List	Action	Operation
00gipjkv	bgpip-000002hl/119.28.217.238	Source port equals to 5000 Destination port equals to 808 Message length equals to 1350 IP headerFind matching items via regexddos,Offset byte starts at 5, ends at 60 and PayloadFind matching items via regexae86,Offset byte starts at 5, ends at 60	Allow	<a href="#">Configuration</a> <a href="#">Delete</a>

Total items: 1 10 / page   1 / 1 page

# AI Protection

Last updated : 2022-04-28 11:14:26

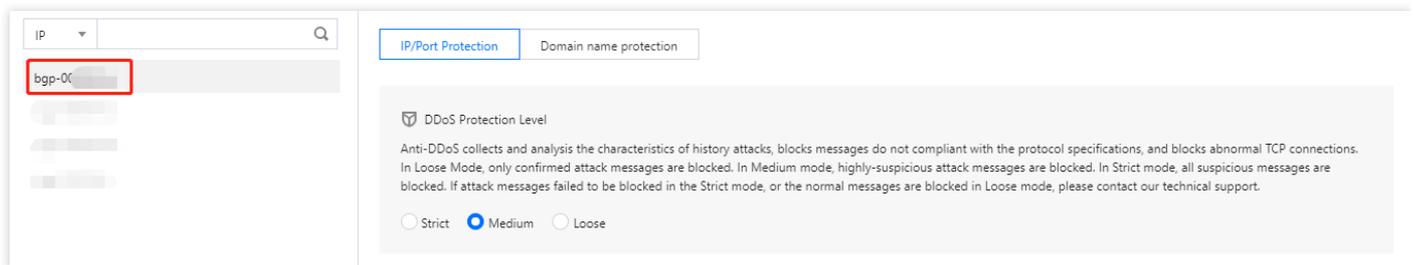
Anti-DDoS Advanced (Global Enterprise Edition) allows you to enable AI protection for powerful defense effect. With AI protection enabled, Anti-DDoS will learn connection baselines and traffic features using algorithms, auto-tune its cleansing policies, and detect and block 4-layer CC attacks.

## Prerequisite

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) instance and set the object to protect.

## Directions

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced > Configurations > DDoS Protection**.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "xxx.xx.xx.xx bgpip-000003n2".





3. Click  in the **AI Protection** section to enable the setting.

<p><b>Connection Attack Protection</b></p> <p>Set refined protection policies targeting connection attacks</p>  <p>• Configured 1 rules <a href="#">Set</a></p>	<p><b>AI Protection</b></p> <p>The AI engine learns the connection number baseline and traffic characteristics, discovers and blocks layer-4 connection CC attacks, and can effectively defend against layer-4 connection attacks.</p>  <p>Defense status <input checked="" type="checkbox"/></p>
<p><b>Block by location</b></p> <p>Block requests to access Anti-DDoS Advanced instances from IP addresses in specified regions.</p>  <p>• Configured 1 rules <a href="#">Set</a></p>	<p><b>IP/Port Speed Limit</b></p> <p>Controls access to the business IP by configuring speed limits on IPs and ports.</p>  <p>• Configured 1 rules <a href="#">Set</a></p>

# Connection Attack Protection

Last updated : 2022-04-28 11:17:32

Anti-DDoS Advanced (Global Enterprise Edition) can automatically trigger blocking policies facing abnormal connections. With **Maximum Source IP Exceptional Connections** enabled, a source IP that frequently sends a large number of messages about abnormal connection status will be detected and added to the blocklist. The source IP will be accessible after being blocked for 15 minutes. You can set the following configurations as needed:

Note :

- **Source New Connection Rate Limit:** limits the rate of new connections from source ports.
- **Source Concurrent Connection Limit:** limits the number of active TCP connections from source addresses at any one time.
- **Destination New Connection Rate Limit:** limits the rate of new connections from destination IP addresses and destination ports.
- **Destination Concurrent Connection Limit:** limits the number of active TCP connections from destination IP addresses at any one time.
- **Maximum Source IP Exceptional Connections:** limits the maximum number of abnormal connections from source IP addresses.

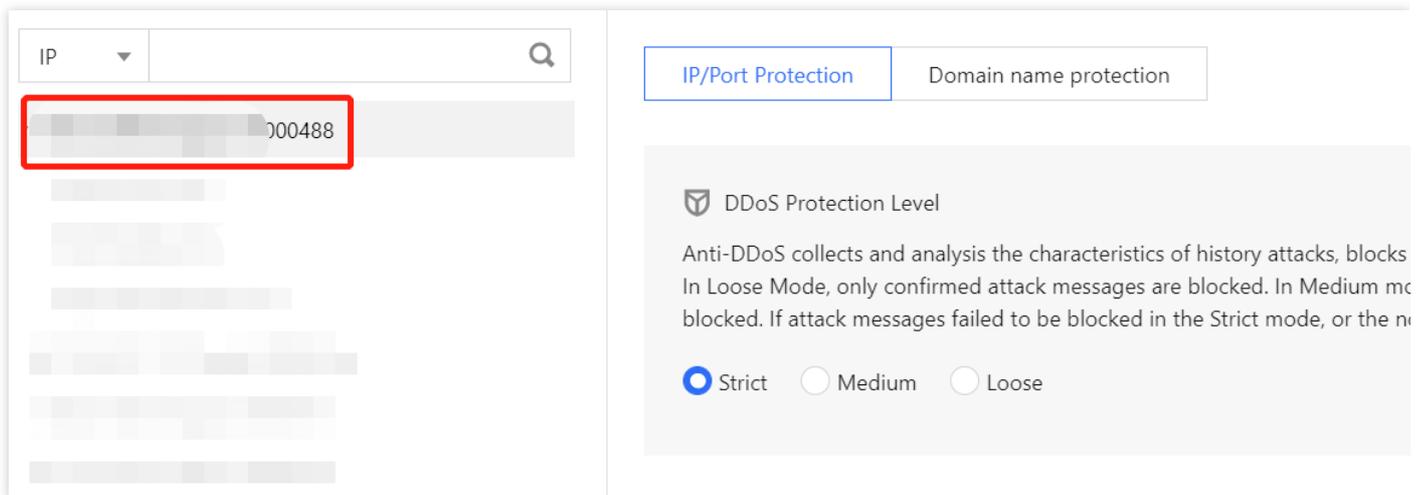
## Prerequisite

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) instance and set the object to protect.

## Directions

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced > Configurations > DDoS Protection**.

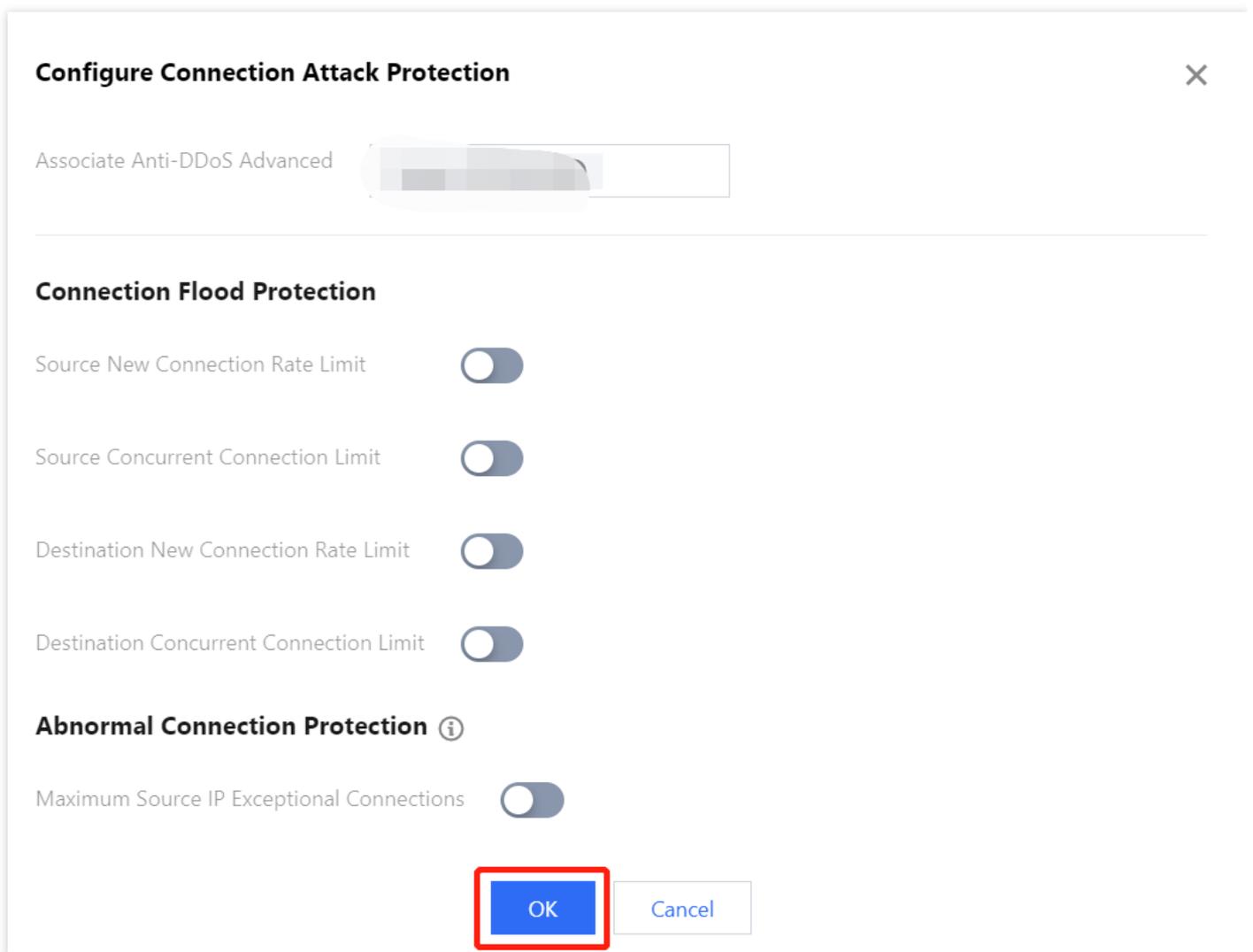
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "xxx.xx.xx.xx bgpip-000003n2".



The screenshot shows the Tencent Cloud console interface. On the left, there is a list of Anti-DDoS Advanced instances. One instance ID, "xxx.xx.xx.xx bgpip-000003n2", is highlighted with a red box. On the right, the "IP/Port Protection" tab is selected. Below the tabs, the "DDoS Protection Level" section is visible, with three radio buttons: "Strict" (selected), "Medium", and "Loose".

3. Click **Set** in the **Connection Attack Protection** section.

4. Click **Create**. On the pop-up page, configure the protection settings and click **OK**.



The screenshot shows the "Configure Connection Attack Protection" dialog box. At the top, there is a section for "Associate Anti-DDoS Advanced" with a dropdown menu. Below this, the "Connection Flood Protection" section contains four toggle switches, all of which are currently turned off: "Source New Connection Rate Limit", "Source Concurrent Connection Limit", "Destination New Connection Rate Limit", and "Destination Concurrent Connection Limit". The "Abnormal Connection Protection" section has an information icon and one toggle switch, "Maximum Source IP Exceptional Connections", which is also turned off. At the bottom, there are two buttons: "OK" (highlighted with a red box) and "Cancel".

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

Associated Resource	Source New Connection Rat...	Source Concurrent Connecti...	Destination New Connection...	Destination Concurrent Con...	Maximum Source IP Excepti...	Operation
[REDACTED]	Close	Close	Close	Close	Close	<a href="#">Configuration</a>

# IP Blocklist/Allowlist

Last updated : 2022-04-28 11:20:31

Anti-DDoS Advanced (Global Enterprise Edition) supports configuring IP blocklist and allowlist to block or allow source IPs accessing the Anti-DDoS services, restricting the users accessing your business resources. If the accessing traffic exceeds the cleansing threshold, the allowed IPs will be allowed to access resources without being filtered by any protection policy; while the access requests from the blocked IPs will be directly denied.

## Prerequisite

- You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) instance and set the object to protect.

Note :

The IP blocklist and allowlist filtering take effect only when your business is under DDoS attacks.

- The allowed IPs will be allowed to access resources without being filtered by any protection policy.
- The access requests from the blocked IPs will be directly denied.

## Directions

- Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced > Configurations > DDoS Protection**.
- Select an Anti-DDoS Advanced instance ID in the list on the left, such as "xxx.xx.xx.xx bgpip-000003n2".

The screenshot displays the 'Protection Policy' configuration interface. It contains four main sections, each with a title, a brief description, and a 'Set' button:

- 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. Status: 4 blocklists, 1 allowlists. A red box highlights the 'Set' button.
- Port Filtering:** Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range. Status: 1 rules.
- Block by protocol:** 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. Status: 1 rules.
- Watermark Protection:** The application end and Anti-DDoS share the same watermark algorithm and key. In this case, every message sent out from the client is embedded with the watermark, so as to defense layer-4 CC attacks, such as. Status: 1 rules.

3. Click **Set** in the **IP Blocklist/Allowlist** section.

4. Click **Create**. On the pop-up page, select a protocol type, enter an IP, and then click **Save**.

The screenshot shows the 'IP Blocklist/Allowlist' 'Create' dialog. It includes a search bar 'Enter an IP' and a table with the following columns: Associated Resource, Associated IP, Protocol Type, Domain Name, Blocked/Allowed IPs, Type, Modification Time, and Operation. A row is shown with 'http' as the protocol type and a 'Save' button highlighted in red.

Associated Resource	Associated IP	Protocol Type	Domain Name	Blocked/Allowed IPs	Type	Modification Time	Operation
bgp-0		http			Blocklist		Save Cancel
bgp-f		http		1	Blocklist	2021-12-27 22:10:23	Set Delete

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

The screenshot shows the 'IP Blocklist/Allowlist' main interface. The table now contains one rule. The 'Delete' button in the 'Operation' column of this rule is highlighted in red.

Associated Resource	Associated IP	Protocol Type	Domain Name	Blocked/Allowed IPs	Type	Modification Time	Operation
bgp-f		http	a		Blocklist	2021-12-27 22:10:23	Set Delete

# IP and Port Rate Limiting

Last updated : 2022-04-28 11:20:07

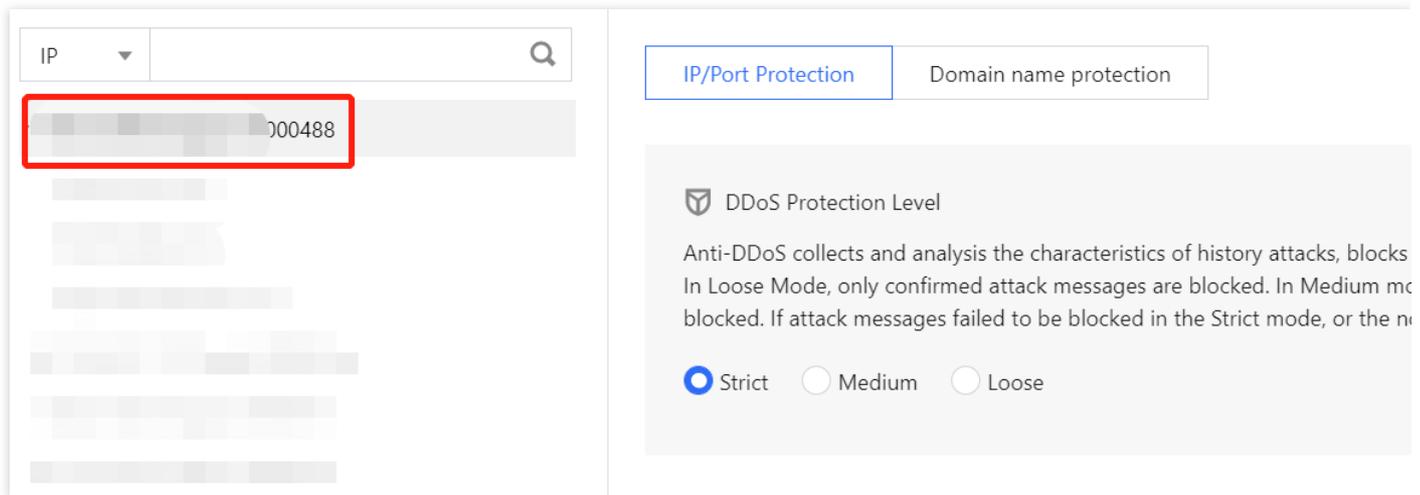
Anti-DDoS Advanced (Global Enterprise Edition) allows you to limit traffic rate for application IPs and ports.

## Prerequisite

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) instance and set the object to protect.

## Directions

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced > Configurations > DDoS Protection**.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "xxx.xx.xx.xx bgpip-000003n2".



3. Click **Set** in the **IP/Port Speed Limit** section.

4. Click **Create**. On the pop-up page, select a protocol, port and limit mode, enter a limit threshold, and then click **OK**.

### Create IP/Port Speed Limit ✕

Associate Service Packs ✕

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 ▼  
By source IP

Speed Limit ⓘ  bps  
 pps

Confirm
Cancel

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

Associated Resource	Protocol	Port	Speed Limited Mode	Packet rate limit	Operation
bgr: <span style="background-color: #ccc; border: 1px solid #ccc; display: inline-block; width: 50px; height: 12px;"></span>	SMP,UDP	<span style="background-color: #ccc; border: 1px solid #ccc; display: inline-block; width: 20px; height: 12px;"></span>	By source IP	<span style="background-color: #ccc; border: 1px solid #ccc; display: inline-block; width: 50px; height: 12px;"></span>	<span style="border: 2px solid red; padding: 2px 5px; font-size: small;">Configuration</span> <span style="margin-left: 5px; font-size: small; color: #007bff;">Delete</span>

# Regional Blocking

Last updated : 2022-04-28 11:22:29

Anti-DDoS Advanced (Global Enterprise Edition) 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.

Note :

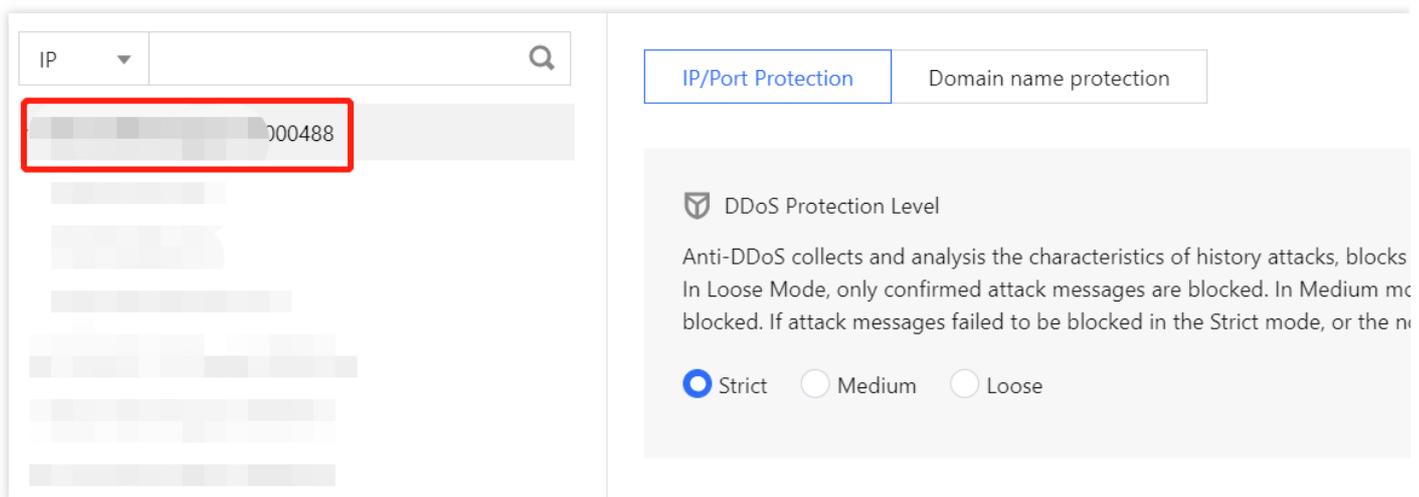
After you configure the regional blocking setting, attack traffic targeting the region will still be recorded but will not be allowed to your real server.

## Prerequisite

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) instance and set the object to protect.

## Directions

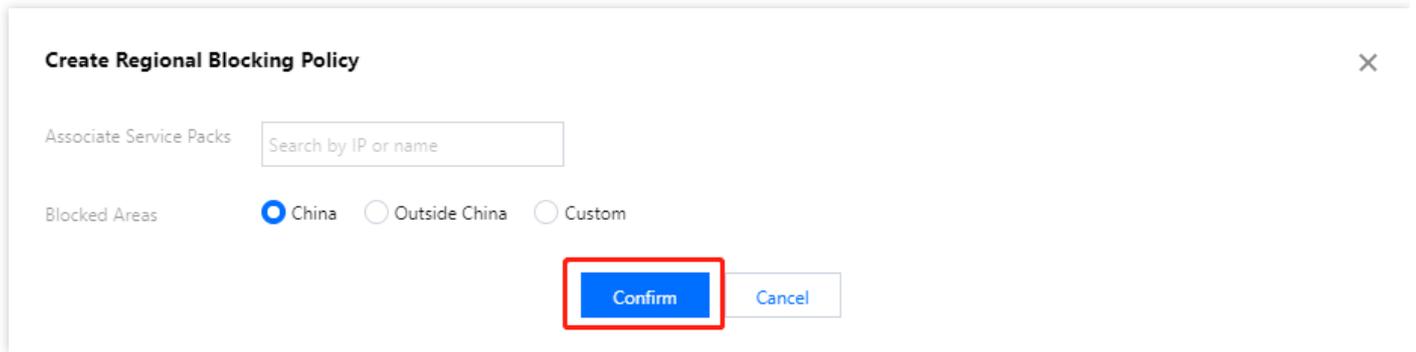
1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced > Configurations > DDoS Protection**.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "xxx.xx.xx.xx bgpip-000003n2".



The screenshot displays the configuration interface for DDoS Protection. On the left, a list of instances is shown, with the instance ID "xxx.xx.xx.xx bgpip-000003n2" highlighted by a red rectangular box. On the right, the configuration details for the selected instance are visible. The "IP/Port Protection" tab is active, and the "Domain name protection" tab is also present. Below the tabs, the "DDoS Protection Level" is set to "Strict", with "Medium" and "Loose" options also visible but unselected. The "Strict" option is indicated by a blue radio button.

3. Click **Set** in the **Block by location** section.

4. Click **Create**. On the pop-up page, select a region and click **OK**.



**Create Regional Blocking Policy** ×

Associate Service Packs

Blocked Areas  China  Outside China  Custom

[Confirm](#) [Cancel](#)

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

Associated Resource	Blocked Areas	Operation
bg 		<a href="#">Configuration</a> <a href="#">Delete</a>

# Port Filtering

Last updated : 2022-04-28 10:55:43

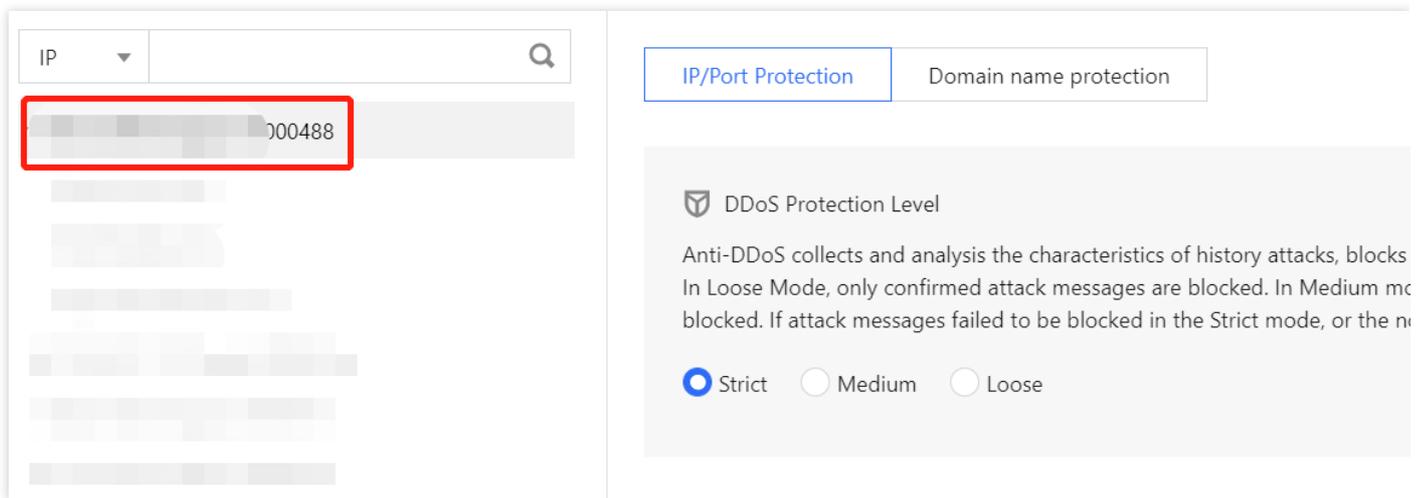
Anti-DDoS Advanced (Global Enterprise Edition) enables you to block or allow inbound traffic by ports. With port filtering enabled, you can customize port settings against inbound traffic, including the protocol type, source port and destination port ranges and set the protection action (allow/block/discard) for the matched rule.

## Prerequisite

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\) instance](#) and set the object to protect.

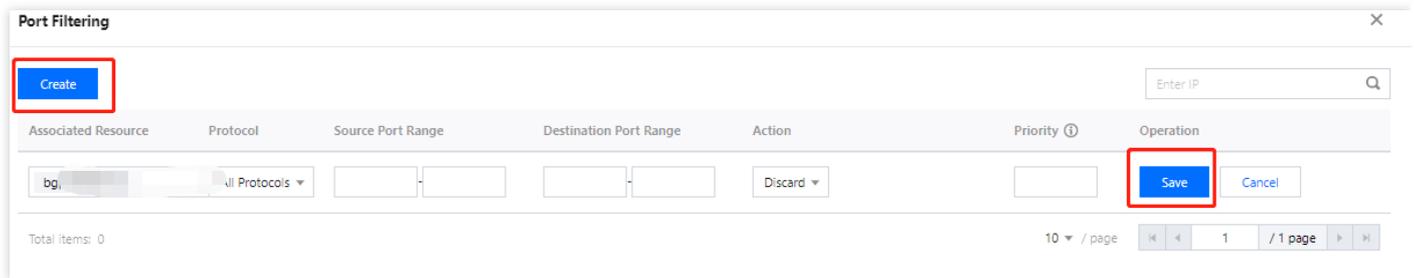
## Directions

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced > Configurations > DDoS Protection**.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "xxx.xx.xx.xx bgpip-000003n2".



3. Click **Set** in the **Port Filtering** section.

4. Click **Create**. On the pop-up page, select an action and enter the required fields.



Port Filtering

Create

Enter IP

Associated Resource	Protocol	Source Port Range	Destination Port Range	Action	Priority	Operation
bgp	All Protocols			Discard		Save Cancel

Total items: 0

10 / page

5. Click **Save**.

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

Associated Resource	Protocol	Port	Speed Limited Mode	Packet rate limit	Operation
bgp	SMP;UDP		By source IP		Configuration Delete

# Watermark Protection

Last updated : 2022-04-28 10:55:43

Anti-DDoS Advanced (Global Enterprise Edition) supports watermark protection for the messages sent by the application end. Within the range of the UDP and TCP message ports configured, the application end and Anti-DDoS share the same watermark algorithm and key. After the configuration is completed, every message sent from the client will be embedded 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.

## Prerequisite

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\) instance](#) and set the object to protect.

Note :

This feature is a paid service. Please [contact us](#) for activation.

## Directions

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced > Configurations > DDoS Protection**.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "xxx.xx.xx.xx bgpip-000003n2".

The screenshot displays the console interface for DDoS Protection. On the left, a list of instances is shown with a search bar and a dropdown menu set to 'IP'. One instance ID, 'xxx.xx.xx.xx bgpip-000003n2', is highlighted with a red box. On the right, the 'IP/Port Protection' tab is selected, and the 'DDoS Protection Level' is configured. The 'Strict' mode is selected with a radio button, while 'Medium' and 'Loose' are unselected. Below the mode selection, a brief description of the protection levels is provided: 'Anti-DDoS collects and analysis the characteristics of history attacks, blocks In Loose Mode, only confirmed attack messages are blocked. In Medium mode, all attack messages are blocked. If attack messages failed to be blocked in the Strict mode, or the n...

- Click **Set** in the **Watermark Protection** section.
- Click **Create**. On the pop-up page, enter the required fields and click **OK**.

### Create a Watermark Protection Policy

Associate Anti-DDoS Advanced

Watermark Check Mode  Normal  Compact

Port

Protocol	Port
<a href="#">Add</a>	

Watermark offset

- After the rule is created, it is added to the list. You can click **Key Configuration** to view and configure a key.

### Watermark Protection

Associated Reso...	Protocol Port	Offset	Check Mode	Status	Operation
	T	1	Normal	<input checked="" type="checkbox"/>	<a href="#">Delete</a> <a href="#">Key Configuration</a>

Total items: 1      10 / page        1 / 1 page

6. In the pop-up window, you can view or copy the key.

The screenshot shows the 'Watermark Protection' interface. At the top left is a 'Create' button. At the top right is a search box labeled 'Enter IP'. Below is a table with the following data:

Associated Resource	Protocol port	Status	Operation
bgpip-000002hl/119.28.217.238	TCP-80	Run Now	<a href="#">Delete</a> <a href="#">Key Configuration</a>

At the bottom left, it says 'Total items: 1'. At the bottom right, there is a pagination control showing '10 / page' and '1 / 1 page'.

7. You can also add or delete a key. A key can be deleted if you have another key. Up to two watermark keys can be created.

The screenshot shows a 'Key information' pop-up window. At the top right is a close button (X). Below is a blue information bar with an info icon and the text: 'Each application can have up to 2 keys. To add a new key, please delete the old key first. When there is only on valid key, it cannot be deleted.'

Below the bar is a table with the following data:

Key	Status	Generation Time	Operation
b26a8365c2c203ec-5bba-b26a8365c2c203ece093f421bc36e78c12b37e60	Enabled	2020-07-01 22:11:13	<a href="#">Copy</a> <a href="#">Delete</a>
b26a8365c2c203ec-5bba-b26a8365c2c203ec9acbab02bc36e78ce329a1db	Enabled	2020-07-01 22:11:16	<a href="#">Copy</a> <a href="#">Delete</a>

At the bottom of the window are two buttons: 'Add Key' and 'Close'.

# CC protection

## CC Protection and Cleansing Threshold

Last updated : 2022-04-28 10:55:43

### Protection Description

"CC Protection" identifies and blocks CC attacks based on access attributes and connection status. It provides scenario-specific configurations to create protection rules, helping secure your business. It also supports the cleaning threshold setting.

### Prerequisite

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\) instance](#) and set the object to protect.

### Directions

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced > Configurations > CC Protection**.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgp-00xxxxxx".

The screenshot displays the 'Configurations' page for Anti-DDoS Advanced. The 'CC Protection' tab is active. The 'Protection Flow' diagram illustrates the process: User (Non-website/port application and Website/domain name applications) connects to the DDOS Engine, which then connects to the Real Server. A note states: '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.' The 'Troubleshooting' section provides links for manual unblocking limits, differences between editions, and blocked server connections. The main configuration area shows a list of instances on the left, with 'bgp-00xxxxxx' selected. The right side shows the 'CC Protection and Cleansing Threshold' settings, including a toggle for 'CC Protection' and a 'Cleansing Threshold' set to '1~20000 QPS'.

3. Click **Set** in the **CC Protection Level and Cleansing Threshold** section.
4. Click **Create**. Enter the required fields and set a cleansing threshold.
5. Click **Save**.

Note :

Refined rules take precedence over instance-level rules.



6. After the rule is created, it is added to the rule list. When the defense level is "Custom", click  and  to enable CC protection and set a cleansing threshold.

# Regional Blocking

Last updated : 2022-04-28 10:55:43

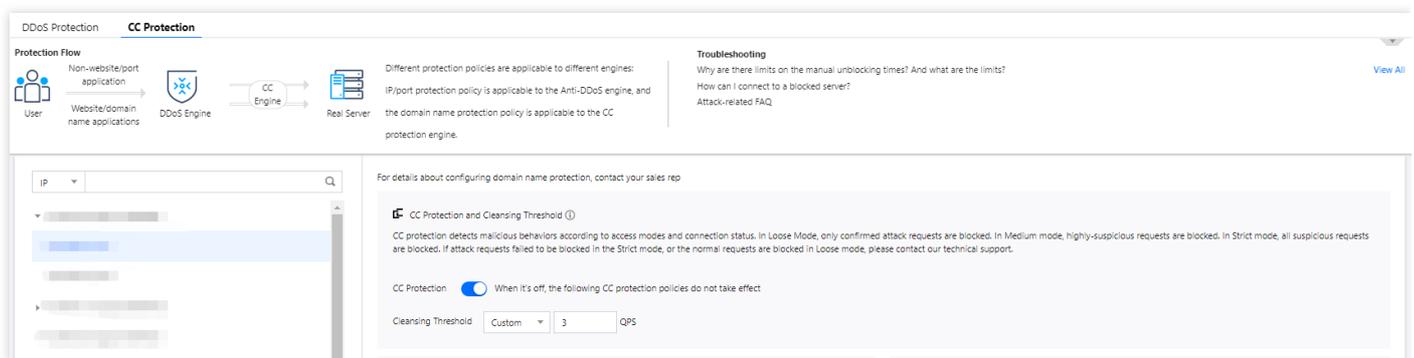
Anti-DDoS Advanced (Global Enterprise Edition) allows you to block website access requests from source IP addresses in specific geographic locations, with just one click. You can block all website access requests from whatever regions or countries you need.

## Prerequisite

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\) instance](#) and set the object to protect.

## Directions

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced > Configurations > CC Protection**.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgp-00xxxxxx".



3. Click **Set** in the **Block by location** section.

4. Click **Create**. On the pop-up page, select an IP, a domain name and region, and click **OK**.

### Create Regional Blocking Policy

Associate Service Packs **bgp-000001cg**

IP

Protocol  HTTP

Domain

Blocked Areas  China  Outside China  Custom

5. Click **Save**.

Note :  
Refined rules take precedence over rules at the instance level.

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

Associated Resource	Protocol	Domain	Blocked Areas	Operation
bgp-0000-218			China	<input type="button" value="Configuration"/> <input type="button" value="Delete"/>

# IP Blocklist/Allowlist

Last updated : 2022-04-28 10:55:44

Anti-DDoS Advanced (Global Enterprise Edition) supports IP blocklist and allowlist configurations to block and allow IPs connected to Anti-DDoS, restricting the users from accessing your resources. For the allowed IPs, they are allowed to access without being filtered by any protection policy; while the access requests from the blocked IPs are directly denied.

Note :

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

- The allowed IPs will be allowed to access resources without being filtered by any protection policy.
- The access requests from the blocked IPs will be directly denied.

## Prerequisite

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\) instance](#) and set the object to protect.

## Directions

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) Console](#) and select **Anti-DDoS Advanced > Configurations > CC Protection**.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgp-00xxxxxx".

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

**CC Protection and Cleansing Threshold** ⓘ

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

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

Cleansing Threshold ⓘ  QPS Set

**Block by location**

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

 Configured 1 rules Set

**IP Blocklist/Allowlist**

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

 Configured 1 rules (max: 50 rules) Set

- Click **Set** in the **IP Blocklist/Allowlist** section.
- Click **Create**. On the pop-up page, enter the required fields.

The screenshot shows the 'IP Blocklist/Allowlist' configuration interface. At the top left is a 'Create' button. To the right is a search box labeled 'Enter an IP'. Below is a table with the following columns: Associated Resource, Associated IP, Protocol Type, Domain Name, Blocked/Allowed IPs, Type, Modification Time, and Operation. The first row shows a form for creating a new rule: 'bgp-0...' for Associated Resource, an IP input field for Associated IP, 'http' for Protocol Type, an empty input for Domain Name, an empty input for Blocked/Allowed IPs, 'Blocklist' for Type, and 'Set' and 'Delete' for Operation. The 'Save' button in the 'Operation' column is highlighted with a red box. Below the table, it says 'Total items: 1' and '10 / page' with pagination controls.

#### Parameter description:

- For **Protocol Type**, select "http" or "https" as needed.
- For **Domain Name**, enter the domain name under the instance.
- For **Blocked/Allowed IPs**, enter the IP or IP range.
- For **Type**, select "Blocklist" or "Allowlist" as needed.

- Click **Save**.
- (Optional) After the rule is created, it is added to the list. You can click **Delete** on the right of the rule to delete it.

The screenshot shows the 'IP Blocklist/Allowlist' configuration interface after a rule has been created. The 'Create' button is still present. The table now contains one rule: 'bgp-...' for Associated Resource, an IP for Associated IP, 'http' for Protocol Type, 'a...' for Domain Name, an IP for Blocked/Allowed IPs, 'Blocklist' for Type, '2021-12-27 22:10:23' for Modification Time, and 'Set' and 'Delete' for Operation. The 'Delete' button in the 'Operation' column is highlighted with a red box. Below the table, it says 'Total items: 1' and '10 / page' with pagination controls.

# Precise Protection

Last updated : 2022-04-28 10:55:44

Anti-DDoS Advanced (Global Enterprise Edition) supports precise protection for connected web businesses. With the precise protection, 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 the requests matched 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.

## Prerequisite

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\) instance](#) and set the object to protect.

## Directions

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced > Configurations > CC Protection**.
2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgp-00xxxxxx".

The screenshot shows the 'CC Protection' configuration page in the Anti-DDoS Advanced console. At the top, there is a 'Protection Flow' diagram illustrating the process from User to Real Server, involving Non-webster/port application, DDoS Engine, and CC Engine. Below this, there is a 'Troubleshooting' section with links for manual unblocking times, blocked servers, and FAQs. The main configuration area includes a search bar for IP addresses, a list of instances, and a detailed configuration for 'CC Protection and Cleansing Threshold'. The 'CC Protection' toggle is turned on, and the 'Cleansing Threshold' is set to 'Custom' with a value of '3' QPS.

3. Click **Set** in the **Precise Protection** section.

4. Click **Create**. On the pop-up page, enter the required fields and click **OK**.

### Create Precise Protection Policy ✕

Associate Anti-DDoS Advance

IP

Protocol  HTTP  HTTPS

Domain name

Condition

Field	Logic	Value	
uri	equa	/	Delete
ua	equa	chrome	Delete
cook	equa	4d5a	Delete
refer	equa		Delete
<a href="#">Add</a>			

Match Operation

**Parameter description:**

- For "Domain Name", select a domain name.
- For "Match Condition", set a match condition to identify requests that use HTTP fields. The following HTTP fields are supported:

Match Field	Field Description	Logic
-------------	-------------------	-------

Match Field	Field Description	Logic
URI	The URI of an access request.	Equals to, includes, or does not include.
UA	The identifier and other information of the client browser that initiates an access request.	Equals to, includes, or does not include.
Cookie	The cookie information in an access request.	Equals to, includes, or does not include.
Referer	The source website of an access request, from which the access request is redirected.	Equals to, includes, or does not include.
Accept	The data type to be received by the client that initiates the access request.	Equals to, includes, or does not include.

- For "Match Action", set to "CAPTCHA", "Block" or "Allow".
  - If "CAPTCHA" is selected, requests that matched the specified conditions will be verified via CAPTCHA.
  - If "Block" is selected, requests that matched the specified conditions will be blocked.
  - If "Allow" is selected, requests that matched the specified conditions will be allowed.

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

The screenshot shows the 'Precise Protection' interface with a 'Create' button and a table of rules. The table has columns for ID, Associated Resource, Protocol, Domain name, Condition, Match Operation, Creation Time, and Operation. Two rules are listed:

ID	Associated Resource	Protocol	Domain name	Condition	Match Operation	Creation Time	Operation
ccPrecs-00000ouy	bgpip-000002j1/153.3.137.126	http	test.probe.tencentdayu.com	uri equals to / cookie equals to 4d5a ua equals to chrome	Discard	2020-07-06 14:59:38	<a href="#">Configuration</a> <a href="#">Delete</a>
ccPrecs-00000out	bgpip-000002j1/153.3.137.126	http	test.probe.tencentdayu.com	uri equals to /	CAPTCH	2020-06-30 20:32:07	<a href="#">Configuration</a> <a href="#">Delete</a>

At the bottom of the table, it shows 'Total items: 2' and a pagination control for '10 / page' with a page number '1 / 1 page'.

# CC Frequency Limit

Last updated : 2022-04-28 10:57:41

Anti-DDoS Advanced (Global Enterprise Edition) supports CC frequency limiting for connected web applications to restrict the access frequency of source IPs. It provides multiple defense 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 based on the real-time traffic using the following levels:

- Loose
- Medium
- Strict
- Urgent
- Custom

At this level, there may be a risk that a small number of abnormal requests can bypass the policy. You can change the defense level when attacks come or configure the CC frequency limit for protection.

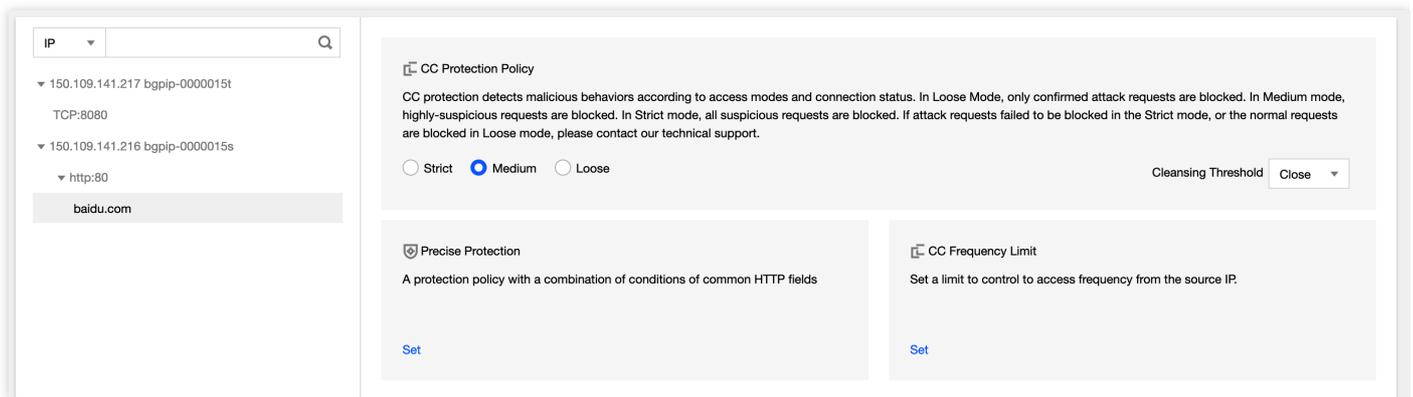
## Prerequisite

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\) instance](#) and set the object to protect.

## Directions

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced > Configurations > CC Protection**.

2. Select an Anti-DDoS Advanced instance ID in the list on the left, such as "bgp-00xxxxx".



3. Click **Set** in the **CC Frequency Limit** section.

4. Click **Create**. Select or add a domain name, turn on the "Defense" switch, and then select an appropriate defense level.

5. To configure custom rules, click **Add Rule**. On the pop-up page, enter the required fields and click **OK**.

### Create CC Frequency Limit ✕

Associate Anti-DDoS Advance

IP

Protocol  HTTP  HTTPS

Domain name

Field	Mode	Value	
Uri	equa	/	Delete
Add			

Frequency Limit Policy

Condition When  Access  Times

Punishment Time  seconds

#### Parameter description:

- For "Domain name", select a domain name.
- For "Action", set to "Discard" or "CAPTCH".
  - If "Discard" is selected, requests that matched the specified conditions will be discarded.
  - If "CAPTCH" is selected, requests that matched the specified conditions will be verified via CAPTCH.
- For "Condition", set the number of requests that are allowed to access a source IP within a specified period.
- For "Punishment time", set a time period.

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

← CC Frequency Limit

Create

ID	Bound Resource	Protocol	Domain name	Detection Perio...	Detection Times	Match Type	Match value	Action	Creation Time	Operation
ccRule-000000cg	bgpip-000002o9/212.64.62.249	http	prob1.probe.tencentdayu.com	10	1	Uri	/	CAPTCH	2020-06-02 11:24:24	<a href="#">Configuration</a> <a href="#">Delete</a>

Total items: 1

10 / page

1 / 1 page

# Application Connection

Last updated : 2022-05-09 10:15:28

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced > Application Accessing > IP Access**.

Note :

Anti-DDoS Advanced (Global Enterprise Edition) only supports IP access.

**Application Accessing**

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

**Without Anti-DDoS Advanced**

Real servers are exposed directly to the internet. When a DDoS attack starts, they can easily be overwhelmed.

**With Anti-DDoS Advanced**

You need to add a CNAME record for the application domain name at your DNS ISP. When network traffic flows through Anti-DDoS Advanced, it automatically filters out malicious traffic to protect the security of the real server.

**Troubleshooting** [View All](#)

- [Connecting applications to Anti-DDoS Advanced](#)
- [IP blocking and unblocking](#)
- [Modifying DNS resolution](#)
- [Solutions for an exposed origin server IP address](#)

[Start Access](#)

2. Click **Add Rule** on the IP accessing page.

[Start Access](#)

Instance ID/Name	Anycast Anti-DDoS Adva...	Protected Resource Type	Protected Resource ID/...	Defense Status	Binding Status	Modification Time	Operation
bgpip-000004tz/Int-test-0	■ ■ ■ ■ ■ ■ ■ ■ ■ ■	■ ■ ■ ■ ■ ■ ■ ■ ■ ■	■ ■ ■ ■ ■ ■ ■ ■ ■ ■	Running	Bound	2021-09-02 14:56:57	Delete

3. In the pop-up **Bound Resource** window, select an Anycast IP, a region and an Anti-DDoS Advanced instance, and then click **OK** to bind the resource.

Note :

- The supported regions include Hong Kong of China, Singapore, Seoul, Mumbai, Bangkok, Tokyo, Silicon Valley, Virginia, Frankfurt and Moscow.
- Only the following resource types can be bound: CVM and CLB.

### IP Access



Associate Anycast IP

Search by IP or name

Cloud Virtual Machine  Cloud Load Balancer

Hong Kong (China) ▾

		Private IP		Bound public IP	
Hong Kong, Macau and Taiwan (China)	West US				
Hong Kong (China)	Silicon Valley	■ ■		■ ■ ■ ■	
Asia Pacific	East US				
Singapore	Virginia	■ ■ ■ ■			
Seoul		■ ■ ■ ■ ■ ■		■ ■ ■ ■ ■ ■	
Mumbai	Europe				
Bangkok	Frankfurt	■ ■ ■ ■ ■ ■		■ ■ ■ ■ ■ ■	
Tokyo	Moscow				

Total items: 4

10 / page

1 / 1 page

# Instance Management

## Viewing Instance Information

Last updated : 2022-04-28 10:55:44

You can view the basic information (such as the expiration time and running status) and configuration of your purchased Anti-DDoS Advanced (Global Enterprise Edition) instances in the Anti-DDoS (Global Enterprise Edition) Console.

## Directions

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) console](#) and select **Anti-DDoS Advanced** > **Service Packages** on the left sidebar.
2. Set **All Lines** to "Anycast". Click **Instance ID** of the instance you select, and you can view details.

Note :

If there are many instances, you can find your instance using the filters in the top right corner.

ID/Name/Tag	Anti-DDoS Adv...	Specifications	Specifications	Status	Attacks in last 7 days	Date	Auto Ext...	Operation
bgpip-000004r1	Unnamed	Line: Anycast	Protection quota: unlimited	Protection StatusRunning	0 Times	Purchase time: 2021-07-02	Off	Configurations View Report

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

**Basic Information**

Anti-DDoS Advanced Name: bgpip-000004r1      Current Status: Running

IP: N/A

Line: Anycast

**Parameter description:**

- **Anti-DDoS Advanced Name**

This is the name of the Anti-DDoS Advanced (Global Enterprise Edition) instance for easier instance identification and management. You can set a custom instance name containing 1–20 characters of any type as desired.

- **IP**

This is the Anycast IP address provided by the Anti-DDoS Advanced (Global Enterprise Edition) instance.

- **Current Status**

This is the current status of the Anti-DDoS Advanced (Global Enterprise Edition) instance, such as **Running**, **Cleansing**, and **Blocked**.

- **Expiry Time**

This is calculated based on the purchase duration selected when the instance is [purchased](#) and the time when the order is paid, which is accurate to second. Tencent Cloud will send expiration and renewal reminders to the account creator and all collaborators through Message Center, SMS, and email within 7 days before the instance expires.

- **Tag**

This is the tag name of the Anti-DDoS Advanced (Global Enterprise Edition) instance, which can be edited and deleted.

# Setting Instance Alias and Tag

Last updated : 2022-03-18 10:16:08

When multiple Anti-DDoS Advanced instances are used, you can set resource names to quickly identify and manage them.

## Prerequisites

You have purchased an [Anti-DDoS Advanced \(Global Enterprise Edition\) instance](#) and set your target to protect.

## Directions

### Method 1

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) Console](#) and select **Anti-DDoS Advanced** -> **Service Packages** on the left sidebar.



2. Find the instance that you need to edit in the instance list, click the icon in the second row in the "ID/Name/Tag" column of the target instance, and enter a name.

Note :

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

### Method 2

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\) Console](#) and select **Anti-DDoS Advanced** -> **Service Packages** on the left sidebar.
2. Find the instance that you need to edit in the instance list, and click the "ID/Name/Tag" column of the target instance.



3. On the basic information page, click the icon right to **Anti-DDoS Advanced Name**, and enter a name.

# Setting Security Event Notification

Last updated : 2021-08-26 12:15:14

Tencent Cloud will send you alarm messages via the channels (including Message Center, SMS, and email) you configured in **[Message Center -> Message Subscription]**

(<https://console.tencentcloud.com/message/subscription>) when:

- An attack starts.
- An attack ended 15 minutes ago.
- An IP is blocked.
- An IP is unblocked.

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

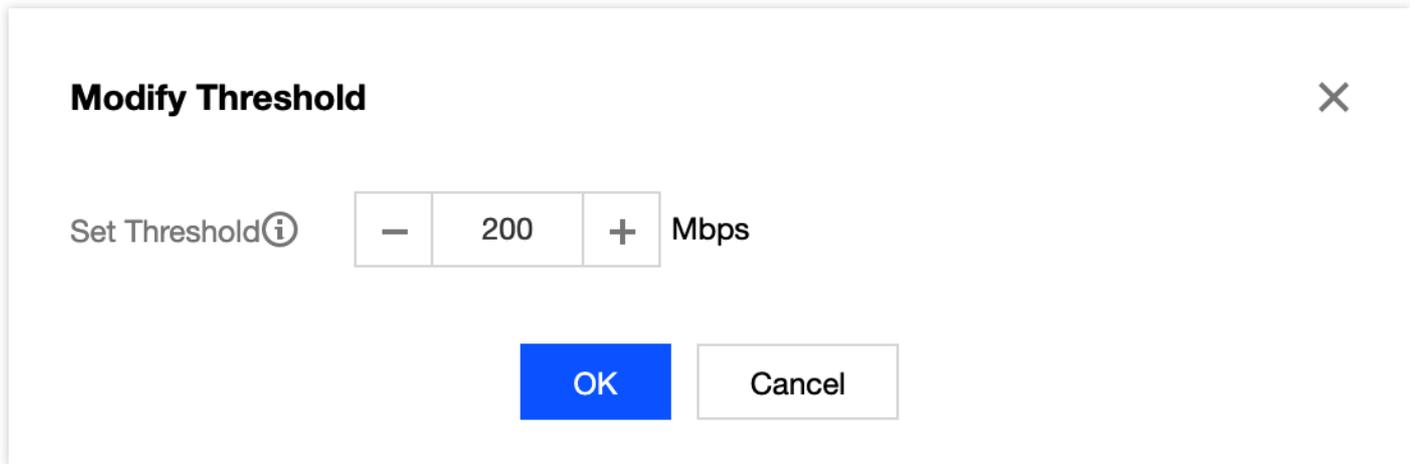
## Configuring the alarm threshold:

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) console and select **Anti-DDoS Advanced -> Alarm Thresholds** on the left sidebar.
2. You can now set the **Inbound Traffic Threshold Per IP**, **DDoS Cleansing Threshold** and **CC Traffic Cleansing Alarm**.

### Alarm Thresholds Purchase

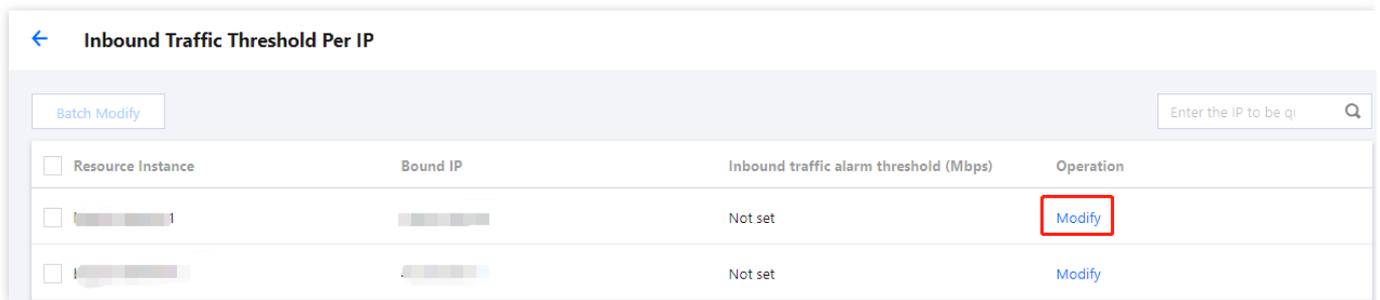
<h4>Inbound Traffic Threshold Per IP</h4> <p>When the inbound traffic to an IP exceeds the threshold, you will get notification in the message center.</p> <p><a href="#">Advanced Settings</a>    Default threshold: Not set </p>	<h4>DDoS Cleansing Traffic Alarm</h4> <p>When an IP is being attack, and the inbound traffic exceeds the threshold, cleansing is triggered, and you will get notifications in message center.</p> <p><a href="#">Advanced Settings</a>    Default threshold: Not set </p>	<h4>CC Traffic Cleansing Alarm</h4> <p>When an IP is being attack, and the inbound traffic exceeds the threshold, cleansing is triggered, and you will get notifications in message center.</p> <p><a href="#">Advanced Settings</a>    Default threshold: Not set </p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3. Click the pencil icon next to thresholds to modify them, and click **OK**.

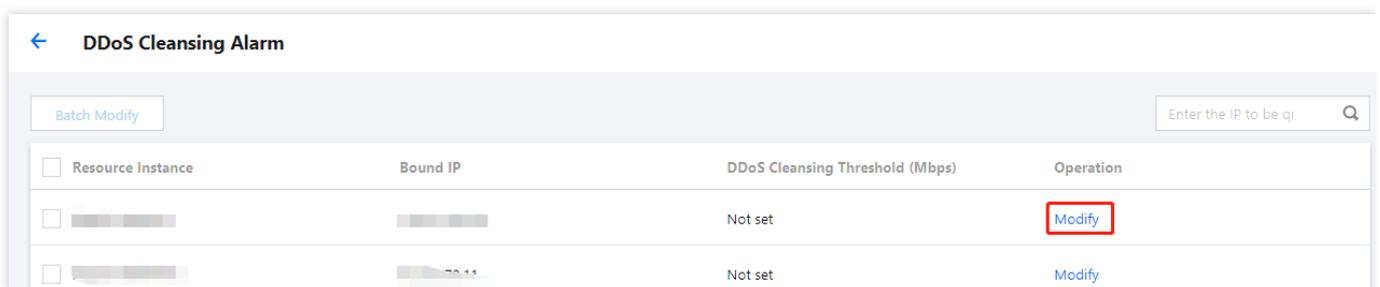


4. Click **Advanced Settings** of each section to enter its alarm setting list, and then click **Modify** to set different thresholds for each instance.

- Setting the inbound traffic threshold for an IP



- Setting the DDoS cleansing threshold



- Setting the CC traffic cleansing alarm

<input type="checkbox"/>	Resource Instance	Bound IP	Cleansing Threshold (in QPS)	Operation
<input type="checkbox"/>	[blurred]	[blurred]	Not set	<a href="#">Modify</a>
<input type="checkbox"/>	[blurred]	[blurred]	Not set	<a href="#">Modify</a>
<input type="checkbox"/>	[blurred]	[blurred]	Not set	<a href="#">Modify</a>

5. Instances can be edited in batch. After selecting multiple instances, click **Batch Modify** to modify them.

<input checked="" type="checkbox"/>	Resource Instance	Bound IP	Cleansing Threshold (in QPS)	Operation
<input checked="" type="checkbox"/>	bgpip-000004tz	162.62.163.31	Not set	<a href="#">Modify</a>
<input type="checkbox"/>	bgpip-000004tw	43.128.241.102	Not set	<a href="#">Modify</a>
<input type="checkbox"/>	bgpip-000004tv	162.62.160.48	Not set	<a href="#">Modify</a>

## How to Set Message Channel

1. Log in to your Tencent Cloud account and go to [Message Center](#).

Note :



You can also log in to the [console](#), click  on the top bar, and click **More** to enter the Message Center.

2. Click **Message Subscription** in the left sidebar.
3. Tick message channels in **Security Notification** and click **Modify Message Receiver**.

<input type="checkbox"/>	Security notifications						
<input type="checkbox"/>	Attack notifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">8163196@qq.com</a>	<a href="#">Modify Message Receiver</a>
<input type="checkbox"/>	Illegal Contents Notifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<a href="#">8163196@qq.com</a>	<a href="#">Modify Message Receiver</a>

4. Tick recipients on the setting page and click **OK**.

### Modify Message Receiver ✕

**ⓘ** Please make sure that the user's email and mobile are verified by Tencent Cloud, and the responding method is enabled.

Message Type **Attack notifications**

Recipients   [Add Message Receiver](#) [Modify User Information](#) **1 selected**

<input type="checkbox"/> User Name	Mobile Number	Email
<input checked="" type="checkbox"/> 8163196@qq.com	<input checked="" type="checkbox"/> 158****0375	<input type="checkbox"/> 81*****@qq.com
<input type="checkbox"/> v_szgwu	<input checked="" type="checkbox"/> 188****5245	<input checked="" type="checkbox"/> v_*****@tencent.com

# Viewing Operation Logs

Last updated : 2021-07-12 18:24:37

## Introduction

You can view Anti-DDoS Advanced (Global Enterprise Edition) operation logs over the last 180 days, including:

- 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

## Operation Directions

1. Log in to the [Anti-DDoS Advanced \(Global Enterprise Edition\)](#) console, click **Anti-DDoS Advanced (New)** -> **Operation Logs**.
2. Select a time period and then click **Unfold** to view log details.