

# Anti-DDoS Pro Operation Guide Product Documentation





#### Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

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

Trademark Notice

#### 🔗 Tencent Cloud

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

#### Service Statement

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

### Contents

**Operation Guide** 

Overview

Protection Overview

Use Limits

Instance Management

Viewing Instance Information

Managing Protected Object

Setting Instance Alias and Tag

**Business Connection** 

**Quick IP Connection** 

**Domain Name Connection** 

**IP** Connection

Port Connection

**Protection Configuration** 

**AI** Protection

Port Filtering

DDoS Protection Levels

IP Blocklist/Allowlist

IP and Port Rate Limiting

Protocol Blocking

Feature Filtering

**Connection Attack Protection** 

**Regional Blocking** 

Viewing Operation Log

**Blocking Operations** 

Configuring Security Event Notification

Connecting a Blocked Server

Unblocking an IP

## Operation Guide Overview

Last updated : 2023-04-20 16:43:51

This document lists the references for common operations while using Anti-DDoS Pro.

## **Instance Management**

- Viewing Instance Information
- Managing Protected Object
- Setting Instance Alias and Tag
- Unblocking Protected IP

## **Protection Configuration**

#### **IP and port protection**

- Protection Level and Cleansing Threshold
- Protocol Blocking
- Attribute Filtering
- Al Protection
- IP Blocklist/Allowlist
- Exceptional Connection Protection
- Connection Protection
- Regional Blocking

## Statistic Report

- Viewing Protection Overview
- Viewing Operation Log

## **Blocking Operation**

Configuring Security Event Notification

🔗 Tencent Cloud

- Connecting a Blocked Server
- Unblocking an IP

## **Protection Overview**

Last updated : 2022-02-22 16:40:03

## Protection Overview

The protection overview page of the Anti-DDoS console shows you complete, real-time indicators for basic protection, Anti-DDoS Pro, and Anti-DDoS Advanced applications, including the protection status and DDoS attack events, which can be used for analysis and source tracing.

### Viewing attack statistics

1. Log in to the new Anti-DDoS console, and select **Overview** on the left sidebar to enter the **Protection Overview** page.

Anti-DDoS	Overview				
🔡 Overview	Protection Overview Anti-DDoS Basic	Anti-DDoS Pro Anti-DDoS Advanced			
Anti-DDoS Basic	Attacks				
Anti-DDoS *     Advanced			Attacked IPs	Protected IPs	Blocked IPs
다 Anti-DDoS Pro *		Safe	0	50	0
<ul> <li>Intelligent ~</li> <li>Scheduling Policy</li> </ul>		No abnormal traffic detected.	Attacked domain names	Protected domain names	Peak attack bandwidth
S Anti-DDoS Pro (New)			0	30	O Modes

- 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.

Attacked IPs	Protected IPs	Blocked IPs
0	50	0
Attacked domain names	Protected domain names	Peak attack bandwidth
0	30	O Mbps

### 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 new Anti-DDoS console, and select **Overview** on the left sidebar to enter the **Protection Overview** page.
- 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	Anti-DDoS Pro Anti-DDoS Advanced					

#### **Viewing instance statistics**

- 1. Log in to the new Anti-DDoS console, and select **Overview** on the left sidebar to enter the **Protection Overview** page.
- 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.

Anti-DDoS Instances					
	Running	15		Running	37
Service Packs	Blocked	0	Anti-DDos Advanced	Blocked	0
	Being attacked	0	41	Being attacked	3
	Other	0		Other	1

### Viewing recent events

- 1. Log in to the new Anti-DDoS console, and select **Overview** on the left sidebar to enter the **Protection Overview** page.
- 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.

Recent Events							
Attacked IP	Instance Name	Defense Type 🔻	Start Time	Duration	Attack Status 🔻	Event Type T	Operation
	All second se	Anti-DD 1	2022-02-16 04:07:00	2 mins	Attack ends	DDoS Attack	View Details
		Anti-DDo1	2022-02-14 17:35:00	2 mins	Attack ends	DDoS Attack	View Details
11.	10 A second	Anti-DDoS	2022-02-13 12:05:00	2 mins	Attack ends	DDoS Attack	View Details

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 Info	Attack Information								
Attacked IP	11	Attack Bandwidth Peak	OMbps						
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.



Attack Bandwidth	Attack Packet Rate
10 Mbps	
8 Mbps	
6 Mbps	
4 Mbps	
2 Mbps	
2022-02-16 04:00	2022-02-16 04:1

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.





#### Field description:

- Attack traffic protocol distribution: displays how attacks on the selected Anti-DDoS Pro instance distribute over different attack traffic protocols within the queried period.
- Attack type distribution: displays how attacks on the selected Anti-DDoS Pro 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	
62.197.136.161	256	Netherlands	512
89.248.163.136	256		

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
62.1	Netherlands	16.0 MB	256
89.	Netherlands	16.0 MB	256
Total items: 2		H H	1 / 1 page 🕨 🕨

### Anti-DDoS Pro Overview

After an IP address is bound to an Anti-DDoS Pro 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. S All Regions • S All Lines • Please select

### Viewing DDoS protection details

1. Log in to the new Anti-DDoS console, select Overview on the left sidebar and then open the Anti-DDoS Pro tab.



2. On the **DDoS Attack** tab, select a query period, target region, and an instance to check whether the instance has been attacked. 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 Pro instance within the queried period, such as the trends of attack traffic bandwidth/attack packet rate.

Last 6 Hours

Today

Last 7 Days

Last 15 days

Last 30 Days

2022-02-17 16:30 ~ 2022-02-17 17:30

Ċ.

Last 1 Hour

S All Regions * S All Lines * Please select	* Last 1 Hour Last 6 Hours	Today Last 7 Days	Last 15 days Last 30 Days 2022-02-17 16:30 ~ 2022-02-17 17:30	
Attack Traffic Bandwidth (traffic surges inc	:luded)	Attack Bandwidth Peak	Attack Packet Rate	Attack packet rate peak
10 Mbps			10 pps	
8 Mbps	2022-02-17 16:45		8 pps	
6 Mbps	— 0 Mbps		брря	
4 Mbps			4 pps	
2 Mbps			2 pps	
2022-02-17 16:30 2022-02-11	7 1645 2022-02 <sup>-</sup> 17 17:00 2022-02 <sup>-</sup> 17 17:15	2022-02-17 17:30	2022-02-17 1630 2022-02-17 1645 2022-02-17 17:00 2022-02-17 17:15	2022-02-17 17:30

- 3. You can view the recent DDoS attacks in the **Recent Events** section.
- Select an event and click **View Details**. You will see the attacker IP, source region, generated attack traffic, and attack packet size on the right, which can be used for attack and source analyses.



Recent Events					
Instance ID	Attacked IP	Start Time	Duration	Attack Status T	Operation
bgpir		2022-02-16 04:07:00	2 mins	Attack ends	Unblock View Details Packet Download
bgpir		2022-02-14 17:35:00	2 mins	Attack ends	Unblock View Details Packet Download
bgpli		2022-02-13 12:05:00	2 mins	Attack ends	Unblock View Details Packet Download
b x		2022-02-11 23:15:00	2 mins	Attack ends	Unblock View Details Packet Download
bg		2022-02-10 12:54:00	2 mins	Attack ends	Unblock View Details Packet Download
Total items: 18					I         1         /4 pages         ▶         Ħ

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

Attack Packet List		>
ID	Time	Operation
12993844	2022-01-10 23:37:51	Download
12993866	2022-01-10 23:37:51	Download
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.



#### Field description:

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

### ठ Tencent Cloud

- Attack type distribution: displays how attacks on the selected Anti-DDoS Pro 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, select a query period, target region, and an instance to check whether the instance has been attacked.

DDoS Attack	CC Attack									
S All Regions 🔻	Please select	•	Last 1 Hour	Last 6 Hours	Today	Last 7 Days	Last 15 days	Last 30 Days	2021-11-01 00:00 ~ 2022-02-17 23:59	Ħ

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

S All Regions * All Lines * Pesse select * Last 1 Hour Last	6 Hours Today Last 7 Days	Last 15 days Last 30 Days 2022-01-18 00:00 ~ 2022-02-17 23:59	
CC Attack Trend Unit: qps	Attack Request Peak 9765 qps	CC Attack Trend Unit Times	Total Request Peak 4422201 times
10,000 8,000 4,000 2,000		5,000,000 4,000,000 3,000,000 1,000,000	
2022-01-18 00:00 2022-01-24 00:00 2022-01-30 00:00 2022-01-30 00:00 2022 — Total request rate — Attack request rate	-02-11 00:00 2022-02-17 00:00	2022-01-18 00:00 2022-01-34 00:00 2022-01-30 00:00 2022-02-05 00:00 2 — Total requests — Attack requests	022-02-11 00:00 2022-02-17 00:00

#### 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, 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 T	Operation
bgpi					2022-02-17 15:51:00	1 mins	Attack ends	View Details
bgpi					2022-02-17 13:37:00	1 mins	Attack ends	View Details
bgi		-		100 C	2022-02-17 12:41:00	1 mins	Attack ends	View Details

## **Use Limits**

Last updated : 2020-07-30 12:08:28

## Limit on Applicable Services

Anti-DDoS Pro is only applicable to Tencent Cloud services, such as CVM, CLB, and NAT gateway.

### Limit on Access

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

## Limit on Blocklist/Allowlist

- For DDoS protection, up to 100 IP addresses can be added to the IP blocklist and allowlist in total.
- IP blocklist/allowlist and URL allowlist currently cannot be configured for CC protection.

## Limit on Available Regions

An Anti-DDoS Pro instances can only be bound to Tencent Cloud devices in the same region. Currently available regions include Beijing, Shanghai, and Guangzhou.

## Instance Management Viewing Instance Information

Last updated : 2022-04-22 11:29:54

You can view the basic information (such as the base protection bandwidth and running status) and configure elastic protection of all purchased Anti-DDoS Pro instances in the Anti-DDoS Console.

## Directions

This example shows you how to view the information of the single IP instance bgp-00000080 in the Guangzhou region.

1. Log in to the new Anti-DDoS Pro Console and click Anti-DDoS Pro Instance on the left sidebar. Find the instance whose ID is bgp-00000080 and click the ID to view the instance details. If there are many instances, you can use the search box in the top-right corner for filtering.

Instance List							Pur	rchase
S All Regions 🔻						Name	▼ Please enter the co	Q
ID/Name	Protected IP	Specifications	Status T	Defense Status	Attacks in last 7 days	Date	Operation	1
bgp-000001da waf a* None a*	Not bound	Region: Guangzhou Package type: Standard Package (BGP) IPs allowed: 100 application bandwidth: 1000Mbps	Status: • Running Remaining protection times: Unlimited Protected IPs: 0	IP/Port Protection: Loose Configuration Domain Name Protection: Disable Configuration	0 times 🗠	Purchase time: 202	Protected I 2-04-06 Configurati View Repo	Resource ions ort
bgp-000001d8 Not named #* None #*	ot bound	Region: Guangzhou Package type: Standard Package (BGP) IPs allowed: 10 application bandwidth: 100Mbps	Status: • Running Remaining protection times: Unlimited Protected IPs: 0	IP/Port Protection: Medium Configuration Domain Name Protection: Disable Configuration	0 times 🗠	Purchase time: 202	Protected I 2-03-24 Configurati View Repo	Resource ions ort

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

÷ I	bgp-000000co			
	Paris Information			
	Anti DDoS Pro instance name	toot é	Current Statue	Dunning
	Location	Beijing	Expiry Time	2020-07-26
	Bound IP	49.232.199.28, 49.232.127.41, 49.233.50.203		
	Base Protection Bandwidth	30 Gbps		

Parameter description:

#### Name

This is the name of the Anti-DDoS Pro instance for easier instance identification and management. You can set a custom instance name containing 1–20 character of any type as desired.

#### Region

This is the **region** selected when the Anti-DDoS Pro instance is purchased.

Bound IP

This is the actual IP of the business protected by the Anti-DDoS Pro instance.

Base protection bandwidth

This is the base protection bandwidth of the Anti-DDoS Pro instance, i.e., the **base protection bandwidth** selected when the instance is **purchased**. If elastic protection is not enabled, this will be the maximum protection bandwidth of the instance.

Current status

This is the current status of the Anti-DDoS Pro instance, such as Running, Cleansing, and Blocked.

• Tag

This is the tag name of the Anti-DDoS Pro instance, which can be edited and deleted.

## Managing Protected Object

Last updated : 2023-06-25 14:42:22

Anti-DDoS Pro provides stronger anti-DDoS protection for Tencent Cloud public IPs. It supports Tencent Cloud services including CVM, CLB, NAT, and WAF.

You can add or delete IPs protected by Anti-DDoS Pro instances as needed.

### Prerequisite

You have purchased an Anti-DDoS Pro instance.

Note :

Anti-DDoS Pro (Enterprise) takes effect only after binding with an Anti DDoS EIP. You need to **change the cloud IP to Anti DDoS EIP**. Anti-DDoS Pro (Enterprise) must be located in the same region with the bound cloud resource. For details, see Creating Anti DDoS EIP.

### Directions

- 1. Log in to the Anti-DDoS Pro Console and click **Protection Instance** in the left sidebar.
- 2. Click the **Protected Resource** on the right of the target Anti-DDoS Pro instance.

6	Purchase instance							🔇 All regions 🔻	All instances 🔹	Name    Please e	nter the conten	Q
	Instance ID/Nam	Instance type	IP Protocol	Access Resources (j)	Specifications	Specifications	Defense Status 🧊	Instance T	Attacks in	Date	Operation	
		Anti-DDoS Pro	IPv4		Region Package type: " application bandwidth: "	Protection Ability: Full protection	Port protection: Medium 🎤	⊘ Running	0 times	Purchase time: 2023-06-08	Protected Resou Configurations	urce

- 3. On the **Protected Resource** page, select a resource type and a resource instance as needed.
- Resource type: Supports cloud resources with public IPs such as CVM, CLB, and WAF.

Note :

Anti-DDoS Pro (Enterprise) takes effect only after binding it with an Anti DDoS EIP.

- Select resource: To add one or more resource instances for protection, tick the checkbox for the resource ID. The number of selected resource instances cannot exceed the max number of protected IPs.
- Selected: To delete the selected resource instance, click Delete on the right of it.

Protected Resource					>
() Note: Configured protection policy only works to the currently bound IP. If t	he pro	tection policy is not applic	able to the current IP,	please change it.	
IP/Resource name Region					
Plan information Enterprise Edition High Defense Package					
Max bound IP					
Device type					
Select instance 🕕		Selected (1)			
Please enter IP (exact search is supported, fuzzy search is not supported) Q		Resource ID/Name	IP address	Resource type	
Resource ID/Name IP address Resource type					8
No data yet					¥
	$\leftrightarrow$				
Total items: 0     10 ▼ / page     I     I     I page     I					
You can make multiple selection by holding down the Shift key					
	_				
ОК		Cancel			

Note:

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

4. Click OK.

## Setting Instance Alias and Tag

Last updated : 2020-07-07 16:04:05

When multiple Anti-DDoS Pro instances are used, you can set "instance names" to identify and manage instances quickly.

## Prerequisites

You need to purchase an Anti-DDoS Pro instance and set the protected object's IP first.

### Directions

### Method 1

- 1. Log in to the new Anti-DDoS Pro Console and select Anti-DDoS Pro Instance on the left sidebar.
- 2. Click the "Edit" icon on the second row in the "ID/Name" column of the target instance and enter a name.

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

ID/Name	Protected IP	Specifications
bgp-00000cn test	1.1.1.240	Region: Guangzhou Package type: Standard pack IPs allowed: 5

### Method 2

- 1. Log in to the new Anti-DDoS Pro Console and click Anti-DDoS Pro Instance on the left sidebar.
- 2. In the instance list below, click the ID of the target instance in the "ID/Name" column to enter its basic information page.

3. On the basic information page of the instance, click the "Edit" pencil icon on the right of the instance name and enter a name.

<b>Basic Information</b>	
Anti-DDoS Pro instance name	test 🎤
Location	Guangzhou
Bound IP	1.1.1.240
Base Protection Bandwidth	30 Gbps

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

## Business Connection Quick IP Connection

Last updated : 2024-01-24 15:12:22

#### Note:

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

### Prerequisite

You have purchased an Anti-DDoS Pro instance.

### Directions

1. Log in to the new Anti-DDoS console, click **Business Access** on the left sidebar, and then click the **Quick IP access** tab.

2. On the Quick IP access tab, click Start Access.

3. In the pop-up page, select an Anti-DDoS instance and resource instances as needed.

elect an instance			•		
egion					
an information	Standard	l Package (BGP)			
rotected IPs	1 remain	ing to protect/total	1		
pplication bandwidth					
rotected Asset Type			•		
lect instance (i)				Selected (0)	
Please enter IP or name (exact	search is supported	d, fuzzy search is no	Q	Resource ID/Name	IP address
Resource ID/Name	IP address	Resource ty	pe		
			*	*	
			*	•	
			4	*	

#### Note

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

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

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

4. Click OK.

## **Domain Name Connection**

Last updated : 2024-01-24 15:14:11

### Note:

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

## Connecting a rule

1. Log in to the new Anti-DDoS console, click **Business Access** on the left sidebar, and then click the **Access via domain name** tab.

2. On the Access via domain name page, click Start Access.

Application	Accessing		
IP access	Access via ports	Access via domain names	IP access 🚯
	Access via Don If your business is method to effectiv	<b>nain Name</b> a website business, you can add fo rely defend against DDoS and CC a	orwarding rules through the Anti-DDoS Pro domain name busing ttacks for the website business. According to the rules you conf
	business traffic wil View details 🗹	II first be cleaned by Anti-DDoS Pro	) , and then back to the target origin server, you can delete or e
Start Acce	Batch import	Batch export Bat	ch delete

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

### Note:

You can select multiple instances.

Access via Domain Name						
1       Select Instance         4       Modify DNS reserved	> 2 Protocol por	t >	3 Set Forwarding Method	>		
<b>O</b> User	CNAME address/A record	Edge Defende	Forwarding port Origin port Forwarding protocol Anti-DDoS Real server Advanced IP	Real serv		
* Associated Instance	Search IP, name or Anti-DDoS res	ource 🔻				

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

Access via Domain Name	
<ul> <li>Select Instance</li> <li>Modify DNS resolution</li> </ul>	ol port > 3 Set Forwarding Method >
CNAME address/A record	Edge Defender Anti-DDoS Real server Advanced IP
★ Forwarding protocol	<ul> <li>http</li> <li>80</li> <li>https</li> <li>443</li> <li>Forward via HTTP for HTTPS requests</li> </ul>
★ Select certificate	Please select
	(The certificate can protect confidential data against theft and tamp including user information and financial information)
* Application domain name	The domain name cannot exceed
Recommended to enable protection configuration	✓ CC Protection + CC AI Protection (

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

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

Access via Domain Nam	e				
Select Instance           4         Modify DNS resol	> <b>Protoco</b> ution	ol port >	3 Set Forv	varding Method	>
<b>O</b> User	CNAME address/A record	Edge Defend	Forwarding p Forwarding p Forwarding forward	ort $\leftrightarrow$ Origin port arding protocol S $\leftrightarrow$ Real server d IP	Real
★ Set Forwarding Method	Forwarding via IP Clean traffic can be forwa	Forwarding via do	omain name I server by the IP o	r domain name	
★ Real Server IP & Port	Real server IP		Origin port		
★ Real Server IP & Port	Real server IP	eg: 1.1.1.1)	Origin port Eg: 80	Delete	

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

#### Note:

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

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

-	http	80		Disable Configure (j)	Unavailable	Failed to configure

## Editing a rule

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



Application do	Forwarding prot	Forwarding port	Real server IP/Site	Associate high defense r	Health check	Session persiste	Access Status
-	-	80			Disable Configure	Disable Edit	Ø Success
-	-	80	10000	The second second	Disable Configure	Unavailable	Success

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

Configure layer-7 forwarding rule					
Associate high defense resources	Up to 60 rules can be added, 1 added now				
Domain name	Enter a domain name containing up to 67 characters.				
Protocol	http Ohttps 443				
	Forward via HTTP for HTTPS requests				
Certificate source	Tencent Cloud-managed certificateSSL certificate management 🗹 🧔				
Certificate	Please select				
Set Forwarding Method	Forwarding via IP Forwarding via domain name				
Real server IP	Real server IP Origin port				
	Delete				
	+ Add				
	Please enter the combination of real server IP and port. Up to 16 entries are allowed.				
	Alternate Real Server				

### Deleting a rule

1. On the Access via domain name page, you can delete one or more rules.

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

Start Access Ba	Itch import Ba	tch export Bate					
Application do	Forwarding prot	Forwarding port	Real server IP/Site	Associate high defense r	Health check	Session persiste	Access Status
-	http	-40			Enable Configure (i)	Disable Edit	Success

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

Start Access Ba	tch import Bat	ch export Bate	h delete				
Application do	Forwarding prot	Forwarding port	Real server IP/Site	Associate high defense r	Health check	Session persiste	Access Status
	-				Enable Configure 🛈	Disable Edit	Success
	http		10000	100000000000000000000000000000000000000	Disable Configure	Unavailable	𝔝 Success

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

## **IP** Connection

Last updated : 2024-01-24 15:18:45

## Connecting a rule

Log in to the new Anti-DDoS console, click Business Access on the left sidebar, and then click the IP access tab.
 On the IP access page, click Start Access.

	Application	Accessing		
	IP access	Access via ports	Access via domain names	IP access
	Start Acc	ess		
the	Associ	ate Anycast	IP field, select an A	Anycast IP.



IP access		
Associate Anycast IP	Search by IP or name	•
Instance type O Clo	oud Virtual Machine 🔷 Load balancer	
S Hong Kong (Chin	a) 🔻	
Enter the instance ID/	ΊΡ	
Instance ID/nam	ne Availability zone	Private IP
		No data yet
Total items: 0		10 🔻 / page

## Deleting a rule

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

Start Access					
Instance ID/name	Anycast Anti-DDoS Advanced	Protected resource type	Protected Resource ID/Name	Defense Status	Binding status
-		Cloud Virtual Machine		• Running	• Bound
100 million (100 million (100 million))	1000	Cloud Virtual Machine	0.000	• Running	• Bound

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

## **Port Connection**

Last updated : 2024-01-24 15:19:43

#### Note:

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

## Connecting a rule

1. Log in to the new Anti-DDoS console, click **Business Access** on the left sidebar, and then click the **Access via port** tab.

2. On the Access via port page, click Start Access.

Application Accessing							
IP access	Access via ports	Access via domain names	IP access (j)				
	Access via Port						
	For non-website ap Advanced via port.	oplications such as PC games, mobile of Traffic will be directed to your instanc	games and apps, you can add forwarding rules when accessing Anti- e to be scrubbed before being forwarded to the target real server. V				
	details 🔽						
Start Acce	ss Batch import	Batch export Batch of	lelete				

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

#### Note:

You can select multiple instances.

Access via Port				
1     Select Instance       4     Modify DNS res	> 2 Protocol por olution	rt <b>&gt;</b> (3	3 Set Forwarding Metho	d >
<b>Q</b> User	CNAME address/A record	Edge Defender	Forwarding port Origin p Forwarding protocol Anti-DDoS Real serv Advanced IP	ver Real server
* Associated Instance	Search IP, name or Anti-DDoS res	source 🔻		

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

Access via Port					
Select Instance (4) Modify DNS res	> 2 Protocol prosolution	ort > 🤇	3 Set Forwardir	ng Method	>
<b>Q</b> User	CNAME address/A record	Edge Defender	Forwarding port ···· Forwarding Anti-DDoS Advanced	<ul> <li>Origin port</li> <li>protocol</li> <li>Real server</li> <li>IP</li> </ul>	Real server
★ Forwarding protocol					
★ Forwarding port	Eg: 80				
★ Origin port	Eg: 80				

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

Select Instance	> 📀 Protoco	l port > 3 Set Forwarding Metho	d
4 Modify DNS resolu	ition		
<b>O</b> User	CNAME address/A record	Forwarding port       Origin p         Forwarding port       Origin p         Forwarding protocol       Anti-DDoS         Advanced       IP	ver Re
Set Forwarding Method	Forwarding via IP	Forwarding via domain name	
	Clean traffic can be forwa	rded back to the real server by the IP or domain name	
Real Server IP & Weight	Real server IP	Weight (j)	
Real Server IP & Weight	Real server IP	Weight ①           eg: 1.1.1.1)         0-100         Delete	

#### Note:

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

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

6. Click Complete.

## Editing a rule

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



Start Access	Batch	n import	Batch export	Batch delete				
Forwa	Forwa	Origin port	Origin		Associate high defense re	Load balancing mode	Health check	Session persistence
UDP							Disable Edit 🛈	Disable Edit
ТСР					2002	100 C 100 C	Disable Edit 🛈	Disable Edit

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

Configure layer-4 forwardi	ng rule	
(i) Important CC Attack Protection is domain names".	not available for port-accesse	d applications. To use CC Attack Prote
Associate high defense resources	-	
	Up to <b>60</b> rules can be ac	lded, 20 added now
Forwarding protocol	UDP	~
Forwarding port		
Origin port		
Set Forwarding Method	Forwarding via IP	Forwarding via domain name
oad balancing mode	Weighted round robin	1
Real Server IP & Weight	Real server IP	Weight 🛈
	+ Add	
	Please enter the combinat	ion of real server IP + weight. It supp
	Alternate Real Server	

## Querying a rule

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

Start Access	Batch	i import Batcl	n export Batch delete				Separate multiple ke Select a filter
Forwa	Forwa	Origin port	Origin	Associate high defense re	Load balancing mode	Health check	Real Server IP/Dom
UDP					Weighted round robin	Disable Edit	Origin port Anti-DDoS Advance
TCP				200.00	Weighted round robin	Disable Edit	Forwarding protoco
UDP		-			Weighted round robin	Disable Edit	Forwarding port Associating Anti-DD
ТСР		-			Weighted round robin	Disable Edit	Disable Edit

### Deleting a rule

1. On the Access via port page, you can delete one or more rules.

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

Start Access	Batc	h import Ba	tch export	Batch delete				
Forwa	Forwa	Origin port	Origin		Associate high defense re	Load balancing mode	Health check	Session persistence
UDP						Weighted round robin	Disable Edit 🛈	Disable Edit
ТСР					10000	Weighted round robin	Disable Edit 🚯	Disable Edit

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

Start Access	Batch	n import	Batch export	Batch delete				
Forwa	Forwa	Origin port	Origin		Associate high defense re	Load balancing mode	Health check	Session persistence
VDP	100					Weighted round robin	Disable Edit 🛈	Disable Edit
🔽 ТСР					210.010	Weighted round robin	Disable Edit 🚯	Disable Edit

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

## Protection Configuration AI Protection

Last updated : 2022-02-22 16:40:03

Anti-DDoS Pro supports AI protection. After AI protection is enabled, with its algorithms, Anti-DDoS Pro can self-learn the connection quantity baseline and traffic characteristics, adaptively adjust cleansing policies, discover and block layer-4 connection CC attacks to deliver an optimal protection effect.

### Prerequisites

You have successfully purchased an Anti-DDoS Pro instance and set the protected target.

## **Operation Directions**

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

lb 🖌 Q	IP/Port Protection Domain name protection
	<ul> <li>DDoS Protection Level</li> <li>Anti-DDoS collects and analysis the characteristics of history attacks, blocks messages do not compliant with the protocol specifications, and blocks abnormal TCP connections. In Loose Mode, only confirmed attack messages are blocked. In Medium mode, highly-suspicious attack messages are blocked. In Strict mode, all suspicious messages are blocked. If attack messages failed to be blocked in the Strict mode, or the normal messages are blocked in Loose mode, please contact our technical support.</li> <li>Strict O Medium Loose</li> </ul>



3. Click

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

Configure Al Protect	tion	×
Associate Service Packs	۲	
On/Off		
	Confirm Cancel	

## Port Filtering

Last updated : 2022-07-06 14:43:29

Port filtering is a fine-grained way to restrict inbound traffic based on port. When it is enabled, you can create a rule by setting the protocol type, source port range, destination port range and action (Discard/Allow/Continue protection).

## Prerequisites

You have successfully purchased an Anti-DDoS Pro instance and set the protected target.

## Directions

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

IP V Q	IP/Port Protection Domain name protection
	DDoS Protection Level Anti-DDoS collects and analysis the characteristics of history attacks, blocks messages do not compliant with the protocol specifications, and blocks abnormal TCP connections. In Loose Mode, only confirmed attack messages are blocked. In Medium mode, highly-suspicious attack messages are blocked. In Strict mode, all suspicious messages are blocked. If attack messages failed to be blocked in the Strict mode, or the normal messages are blocked in Loose mode, please contact our technical support. Strict O Medium Loose

3. Click **Set** in the **Port Filtering** section to enter the port filtering page.

Configurations	:≣ Single	: Setting Mor
DDoS Protection CC Protection		
Protection Flow Non-website/port application CC C Different protection policy is applicable to different engi IP/port protection policy is applicable to the Anti-DDoS eng IP/port protection policy is applicable to the Anti-DDoS eng	Troubleshooting           nes:         Why are there limits on the manual unblocking times? And what are the limits?           What are the differences between Anti-DDoS Advanced and Anti-DDoS Pro?           Juncation and the biologic down and biologic down and anti-DDoS Pro?	View A
User Website/domain DDoS Engine Real Server the domain name protection policy is applicable to the CC protection engine.	How can i connect to a blocked server : What if my business IP is blocked for attack defense?	
Protection Policy ①		
IP Blocklist/Allowlist Configure IP blockist and allowlist to block or allow requests from specific source IPk, so as to define who can access your application resource.	Port Filtering Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range	
Set		Set

4. Click Create, enter the required fields based on the action you select, and then click Save.



#### Note :

Multiple instances can be created at a time. For instances without protected resources, you cannot create rules.

Create Port Filtering Policy			2	×
Associate Anti-DDoS Advanced	bg			
Protocol	All Protocols	~		
Source Port Range 🛈	Starting Source -	Ending Source		
Destination Port Range 🛈	Starting Destin -	Ending Destina		
Action	Discard	•		
	Confirm	Cancel		

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.

Create					Enter IP	Q
Associated Resource	Protocol	Source Port Range	Destination Port Range	Action	Operation	
bgpip	ТСР			Discard	Configuration Delete	

## **DDoS Protection Levels**

Last updated : 2022-07-06 14:28:30

This guide describes protection levels the Anti-DDoS Pro provides in different scenarios and how to set them in the console.

## Use Cases

Anti-DDoS Pro 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> <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> <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 in each Anti-DDoS Pro instance.
- The real server may suffer seconds of attacks in the following situations:
  - It happens when you are changing the protection level.
  - It happens when you are connecting to Anti-DDoS Pro.

## Prerequisites

You have successfully purchased an Anti-DDoS Pro instance and set the protected target.

## Directions

- Log in to the new Anti-DDoS console and select Anti-DDoS Pro (New) > Configurations on the left sidebar.
   Open the DDoS Protection tab.
- 2. Select an Anti-DDoS Pro instance ID in the list on the left, such as "bgp-00xxxxx".



3. Choose a protection level in the **DDoS Protection Level** section.

DDoS Protection Level	
Anti-DDoS collects and analysis the characteristics of history attacks, blocks messages do not compliant with the protocol specifications. In Loose Mode, only confirmed attack messages are blocked. In Medium mode, highly-suspicious attack messages are blocked. In Strict blocked. If attack messages failed to be blocked in the Strict mode, or the normal messages are blocked in Loose mode, please contact	s, and blocks abnormal TCP connections. t mode, all suspicious messages are our technical support.
Strict O Medium Loose	Cleansing Threshold Default 🔹

## IP Blocklist/Allowlist

Last updated : 2022-02-22 16:40:03

Anti-DDoS Pro supports IP blocklist and allowlist configurations to block or allow source IPs to access the Anti-DDoS service, restricting the users from accessing your business 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.

## Prerequisites

You have successfully purchased an Anti-DDoS Pro instance and set the protected target.

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.

## **Operation Directions**

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



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

Configurations	i⊟ Single Setting M
DDoS Protection         CC Protection           Protection Flow         Different protection policies are applicable to different engin application         Different protection policy is applicable to the Anti-DDoS engine           User         Website/domain name applications         DoS Engine         Engine         Different protection policy is applicable to the CC protection engine.	es: Why are there limits on the manual unblocking times? And what are the limits? View ne, and What are the differences between Anti-DDoS Advanced and Anti-DDoS Pro? How can I connect to a blocked server? What if my business IP is blocked for attack defense?
Protection Policy ① 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.	Port Filtering Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range
Set	Set

4. In the pop-up window, tick **Blocklist** or **Allowlist** as the type, enter the target IP, and click **OK**.

Create IP blacklist/wh	itelist
Associate Service Packs	bgp-00000co 😢
Туре	O Blacklist O Whitelist
IP	Please enter IP addresses, separated with carriage returns
	OK Cancel



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.

÷	IP Black/White List					
	Create				Enter IP C	Q
	Associated Resource	Туре	ip	Operation		
	bgp-000000co/49.232.127.41,49.232.199.28,49.233.50.203	Blacklist	1.1.1.6	Delete		
	Total items: 1			10 🔻 / page	I         /1 page         ▶         ▶	

## IP and Port Rate Limiting

Last updated : 2022-02-22 16:40:03

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

## Prerequisites

You have successfully purchased an Anti-DDoS Pro instance and set the protected target.

### Directions

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



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





- 4. Click Create to create an IP/port speed limit rule.
- 5. In the pop-up window, select a protocol, port and speed limit mode, enter a speed limit threshold, and click **OK**.

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	

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	Port	Speed Limited Mode	Packet rate limit	Operation
bg¢	SMP;UDP	-	By source IP		Configuration Delete

## **Protocol Blocking**

Last updated : 2022-07-06 14:48:31

Anti-DDoS supports blocking inbound traffic based on its protocol type. You can enable "Block ICMP protocol/Block TCP protocol/Block UDP protocol/Block other protocols" to block their access requests directly. Note that UDP is a connectionless protocol that dose not provide a three-way handshake process like TCP and thus has security vulnerabilities. We recommend blocking UDP if it is not used for your business.

### Prerequisites

You have successfully purchased an Anti-DDoS Pro instance and set the protected target.

### Directions

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

IP v Q	IP/Port Protection Domain name protection
	<ul> <li>DDoS Protection Level</li> <li>Anti-DDoS collects and analysis the characteristics of history attacks, blocks messages do not compliant with the protocol specifications, and blocks abnormal TCP connections. In Loose Mode, only confirmed attack messages are blocked. In Medium mode, highly-suspicious attack messages are blocked. In Strict mode, all suspicious messages are blocked. If attack messages failed to be blocked in the Strict mode, or the normal messages are blocked in Loose mode, please contact our technical support.</li> <li>Strict O Medium Loose</li> </ul>

3. Click Set in the Block by Location section.

Protection Policy ①	
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.	Port Filtering Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range
Set	Set
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.	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
Set	This is a value-added feature. Please contact your after-sales rep if necessary.

4. Click **Create** to create a protocol blocking rule.

Create		
Associated Resource	Block ICMP Protocol	Block TCP Protocol

5. In the pop-up window, click the button on the right of a protocol, and click **Confirm**.

Create Protocol Bloc	king Policy	×
Associate Service Packs	Search by IP or name	
Block ICMP Protocol		
Block TCP Protocol		
Block UDP Protocol		
Block other protocols		
	Confirm	



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	Block ICMP Protocol	Block TCP Protocol	Block UDP Protocol	Block other protocols	Operation
bg,	Disable	Disable	Disable	Disable	Configuration

## Feature Filtering

Last updated : 2022-02-22 16:40:04

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

### Prerequisites

You have successfully purchased an Anti-DDoS Pro instance and set the protected target.

### Directions

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



3. Click **Set** in the **Port Filtering** section to enter the port filtering page.

Block by locat	tion Block requests to access Anti-DDoS Advanced instances from IP addresses in specified regions.		IP/Port Speed Limit Controls access to the business IP by configuring speed limits on IPs and ports.	
		Set		Set
Feature Filteri	ng Configure custom blocking policy against specific IP, TCP, UDP message header or payload.			
		Set	]	

4. Click **Create** to create a feature filtering rule.



5. In the pop-up window, fill in the configuration fields, and click **OK**.

Associate Service Packs	Search by IP or name			
ilter feature	Field	Logic	Value	
		Logic	Value	
	Add			
Action	Allow OBlock	Discard Reject red	uests and block IP for 15 mins	
(cton				

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.

ID	Associated Resource	Feature List	Action	Operation
00		Source port equals to 100 Destination port equals to 13 Message length equals to 198	Continue Protection	Configuration Delete

## **Connection Attack Protection**

Last updated : 2022-02-22 16:40:04

Anti-DDoS Pro 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.

Note :

The following fields are supported:

- 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.

## Prerequisites

You have successfully purchased an Anti-DDoS Pro instance and set the protected target.

### Directions

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

lp v Q	IP/Port Protection Domain name protection
	<ul> <li>DDoS Protection Level</li> <li>Anti-DDoS collects and analysis the characteristics of history attacks, blocks messages do not compliant with the protocol specifications, and blocks abnormal TCP connections. In Loose Mode, only confirmed attack messages are blocked. In Medium mode, highly-suspicious attack messages are blocked. In Strict mode, all suspicious messages are blocked. If attack messages failed to be blocked in the Strict mode, or the normal messages are blocked in Loose mode, please contact our technical support.</li> <li>Strict O Medium Loose</li> </ul>

3. Click Set in the Connection Attack Protection to enter the configuration page.

Configurations	I≣ Single Setting Mo
DDoS Protection       CC Protection         Yotection Flow       Different protection policies are applicable to different engine         User       Non-website/port application       DoS Engine       CC       Fingine       Different protection policy is applicable to the Anti-DDoS engine         User       User       DoS Engine       CC       Fingine       Real Server       the domain name protection policy is applicable to the CC protection engine.	Troubleshooting       es:     Why are there limits on the manual unblocking times? And what are the limits?     View       what are the differences between Anti-DDoS Advanced and Anti-DDoS Pro?     How can I connect to a blocked server?       What if my business IP is blocked for attack defense?     What if my business IP is blocked for attack defense?
Protection Policy ① IP Blocklist/Allowlist Onfigure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource. Set	Port Filtering           Society           Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range
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.	Watermark Protection           Image: State of 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
Set Connection Attack Protection Set refined protection policies targeting connection attacks	This is a value-added feature. Please contact your after-sales rep if necessary.      Al Protection     The Al engine learns the connection number baseline and traffic characteristics, discovers and blocks layer-4 connection     C attacks, and can effectively defend against layer-4 connection attacks.
Set	Set

- 4. Click **Create** to create a connection attack protection rule.
- 5. In the pop-up window, enable **Connection Flood Protection** and **Abnormal Connection Protection**, and click **OK**.

Configure Connection Attack Prote	ection	×
Associate Service Packs	8	
Connection Flood Protection		
Source New Connection Rate Limit		
Source Concurrent Connection Limit		
Destination New Connection Rate Limit		
Destination Concurrent Connection Limit		
Abnormal Connection Protection (	j	
Maximum Source IP Exceptional Connection	ns	
[	Confirm	

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	Source New Connection Rat	Source Concurrent Connecti	Destination New Connection	Destination Concurrent Con	Maximum Source IP Excepti	Operation
	Disable	Disable	Disable	Disable	Disable	Configuration

## **Regional Blocking**

Last updated : 2022-02-22 16:40:04

Anti-DDoS Pro 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.

## Prerequisites

You have successfully purchased an Anti-DDoS Pro instance and set the protected target.

## Directions

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

DDoS Protection CC Protection		
Protection Flow Non-website/port application User Webste/domain name application DOS Engine Re	Different protection policies are applicable to different engines:     Propert protection policy is applicable to the Anti-DoSe engine, and     Server     the domain name protection policy is applicable to the CC     protection engine.     Troubleshooting     Troubleshooting     Why are there limits on the manual unblocking times? And what are the limits?     How can I connect to a blocked server?     Attack-related FAQ	View All
	For details about configuring domain name protection, contact your sales rep  C Protection and Ceansing Threshold () CC Protection and Ceansing Threshold () CC protection detects mail cloue behaviors according to access modes and connection status. In Loose Mode, only confirmed attack requests are blocked. In Medium mode, highly-suplicious requests are blocked. In Strict mode, all suspicious request are blocked. In Medium mode, highly-suplicious requests are blocked. In Strict mode, all suspicious request are blocked. In Medium mode, highly-suplicious requests are blocked. In Strict mode, all suspicious request are blocked. In Medium mode, highly-suplicious requests are blocked. In Strict mode, all suspicious request are blocked. In Medium mode, highly-suplicious requests are blocked. In Strict mode, all suspicious request are blocked. In Medium mode, highly-suplicious requests are blocked. In Strict mode, all suspicious request are blocked. In Medium mode, highly-suplicious requests are blocked. In Strict mode, all suspicious request are blocked. In Medium mode, highly-suplicious requests are blocked. In Strict mode, all suspicious request are blocked. In Medium mode, highly-suplicious requests are blocked. In Strict mode, all suspicious request are blocked. In Strict mode, all suspicious request are blocked. In Strict mode, all suspicious request are blocked. In Medium mode, highly-suplicious requests are blocked. In Strict mode, all suspicious request are blocked. In Medium mode, highly-suplicious requests are blocked. In Strict mode, all suspicious request are blocked. In Strict mode, all suspicious	sts



3. Click Set in the Block by Location section to get to configuration.

Block by location Block requests to access Anti-DDoS Advanced instances from IP addresses in specified regions.	IP Blocklist/Allowlist Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.
Configured 1 rules     Set	Configured 5 rules (max: 50 rules)     Set
Precise Protection A protection policy with a combination of conditions of common HTTP fields	CC Frequency Limit Set a limit to control to access frequency from the source IP.
Configured 1 rules Set	Defense Status 🚺 Defense Level 🛈 Urgent 💌

- 4. Click **Create** to create a regional blocking rule.
- 5. In the pop-up window, select a region to block and click **OK**.

Create Regional Bloc	cking Policy	×
Associate Service Packs	Search by IP or name	
Blocked Areas	O China ○ Outside China ○ Custom	
	Confirm	

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.



## **Viewing Operation Log**

Last updated : 2023-04-20 16:37:37

## Use Cases

Anti-DDoS Pro allows you to view logs of important operations in the last 90 days on the operation log page in the Anti-DDoS Pro Console. The following types of logs are available:

- · Logs of protected object's IP replacement
- Logs of DDoS protection policy change
- · Logs of cleansing threshold adjustment
- Logs of protection level change
- Logs of resource name change

## Directions

- 1. Open the Operation Log page in the new Anti-DDoS Pro Console.
- 2. Set the time range to query relevant operation records.

Oper	ation Logs									Purchase
	Today Yesterday Operation Time 2020-07-06 16:15:53		Last 7 days Last 30 days 2020-07-06 00:00 ~ 2020-07-			20-07-06 23:59				
			Dependent ID Object ID		Product Type	Product Type Action Result		Operator Account	Operation	
					Service Packs CreateInstanceNam		Buccess	100001500880	Unfold	
	Total items: 1							10 🔻 / page	I I /1 page	▶ ▶

## Blocking Operations Configuring Security Event Notification

Last updated : 2022-05-09 17:03:00

## Use Cases

Tencent Cloud will send you alarm messages for your IPs protected by Anti-DDoS Pro via the channels (including Message Center, SMS, and email) you configured in Message Center -> 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.

### How to Set Alarm Threshold

- 1. Log in to the Anti-DDoS Pro Console and select 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**.



3. Click **Advanced Settings** of each section to enter its alarm setting list and set different thresholds for each instance.

· Setting the inbound traffic threshold for an IP

÷	Inbound Traffic Threshold Per IP					
	Batch Modify				Enter the IP to be q	Q
	Resource Instance	Bound IP	Inbound traffic alarm threshold (Mbps)	Operation		
	bgp-000000co	49.232.199.28;49.233.50.203;49.232.127.41	101	Modify		
	bgp-000000cn	1.1.1.240	101	Modify		
	bgp-000000cm	2402:4e00:1400:e57b:0:8f9c:903:5e6e;118.89.113.189	200	Modify		
	Total items: 3			10 🔻 / page 🔣 🖣	1 /1 page ▶	M

• Setting the DDoS cleansing threshold

÷	DDoS Cleansing Alarm					
	Batch Modify	Enter the IP to be q	Q			
	Resource Instance	Bound IP	DDoS Cleansing Threshold (Mbps)	Operation		
	bgp-000000co	49.232.199.28;49.233.50.203;49.232.127.41	Not set	Modify		
	bgp-000000cn	1.1.1.240	Not set	Modify		
	bgp-000000cm	2402:4e00:1400:e57b:0:8f9c:903:5e6e;118.89.113.189	Not set	Modify		
	Total items: 3			10 🔻 / page 🛛 🛤 🖪	1 / 1 page >	M

• Setting the CC traffic cleansing alarm

← CC Traffic Cle	eansing Alarm			
	Batch Modify			Enter the IP to be queen Q
	Resource Instance	Bound IP	Cleansing Threshold (in QPS)	Operation
	bgp-000001bt	162.62.190.169	20	Modify
	bgp-000001bs	119.91.77.141	20	Modify
	bgp-0000016m	119.91.82.253	Not set	Modify
	bgp-000000ij	111.230.63.220	1	Modify
	Total items: 4			10 ▼ / page H 4 1 / 1 page ► H

## How to Set Message Channel

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

Note :



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

Gecurity notifications							
Attack notifications		<b>~</b>	<b>~</b>		8163196@qq.com	Modify Message Receiver	
Illegal Contents Notifications			<b>~</b>		8163196@qq.com	Modify Message Receiver	

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

Iodify Messa	age Receiver				
i Please	make sure that the user's email and m	obile are verified by Tencent Cloud, a	nd the responding method is enabled.		
essage Type	Attack notifications				
cipients	User User Group	Add Messa	ge Receiver 🛂 Modify User Information 🖸	1 selected	
	Search for user name		Q	8163196@qq.com	×
	User Name	Mobile Number	Email		
	✓ 8163196@qq.com	⊘ 158****0375	81*****@qq.com		
	v_szgwu	⊘ 188****5245	✓ v_*****@tencent.com		
				↔	

## Connecting a Blocked Server

Last updated : 2021-08-26 11:51:18

This document describes how to connect a blocked server.

## Directions

- 1. Log in to the CVM Console and click Instances on the left sidebar to enter the instance details page.
- 2. Click the drop-down list in the top left corner and modify the region.
- 3. Click the search box to use filters such as "Instance Name", "Instance ID" and "Instance Status" to locate the blocked server.
- 4. Click Log In for the blocked server to display the Log in to Linux Instance pop-up window.
- 5. In the pop-up window, select Login over VNC and click Log In Now to connect the server via browser VNC.

## Unblocking an IP

Last updated : 2022-11-15 15:23:17

## **Unblocking Procedure**

### Auto unblocking

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

- 1. Log in to the Anti-DDoS Console, select **Self-Service Unblocking** > **Unblock Blocked IP** on the left sidebar to get to unblocking operation.
- 2. Check the predicted unblocking time of an IP in Estimated Unblocking Time on the unblocking page.

### Manual unblocking

You can perform unblocking earlier as follows:

Note :

- Only **three** chances of self-service unblocking are provided for Anti-DDoS Pro or Advanced users every day. The system resets the chance counter daily at midnight. Unused chances cannot be accumulated for the next day.
- If the attack persists, you cannot perform unblocking. You need to wait for the attack to end before manual unblocking or auto unblocking.
- 1. Log in to the Anti-DDoS Console, select **Self-Service Unblocking** > **Unblock Blocked IP** on the left sidebar to get to unblocking operation.
- 2. Find the protected IP in Pending Auto Unblocking and click Unblock in the Operation column on the right.
- Click OK in the Unblock Blocked IP dialog box. If you receive a notification indicating successful unblocking, the IP has been successfully unblocked. You can refresh the page to check whether the protected IP is in running status.

### Unblocking Operation Record



Log in to the Anti-DDoS Console, select **Self-Service Unblocking** > **Unblocking History** on the left sidebar. You can check all unblocking records in the specified period, including records of automatic unblocking and manual unblocking.