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

©2013-2022 Tencent Cloud. All rights reserved.

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
- AI 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

©2013-2022 Tencent Cloud. All rights reserved.

- Connecting a Blocked Server
- Unblocking an IP

©2013-2022 Tencent Cloud. All rights reserved.

Protection Overview

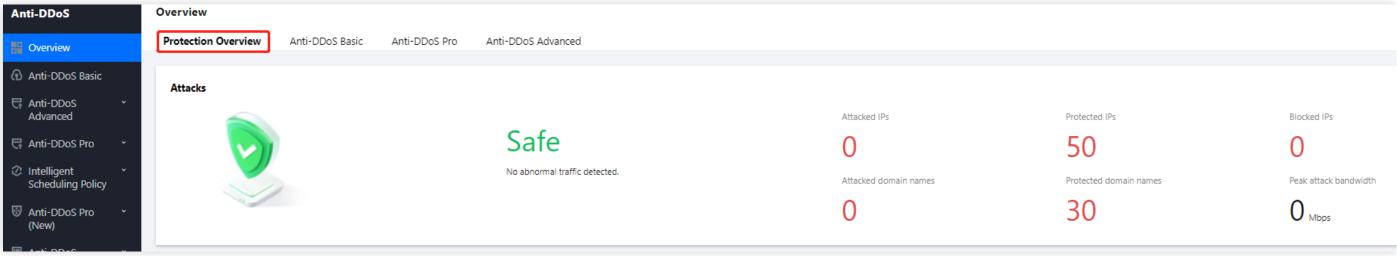
Last updated：2022-02-22 16:40:03

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.



Attacks

Safe

No abnormal traffic detected.

Attacked IPs 0

Protected IPs 50

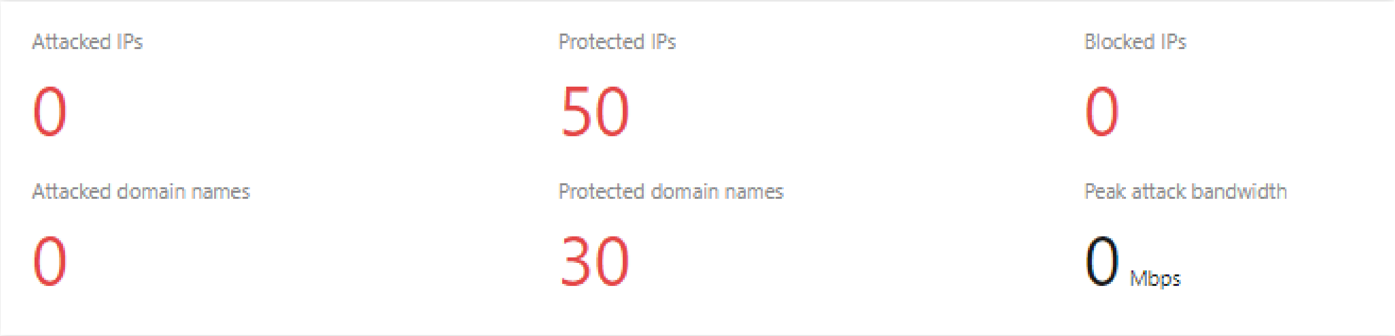
Blocked IPs 0

Attacked domain names 0

Protected domain names 30

Peak attack bandwidth 0 Mbps

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	0 Mbps

Field description:

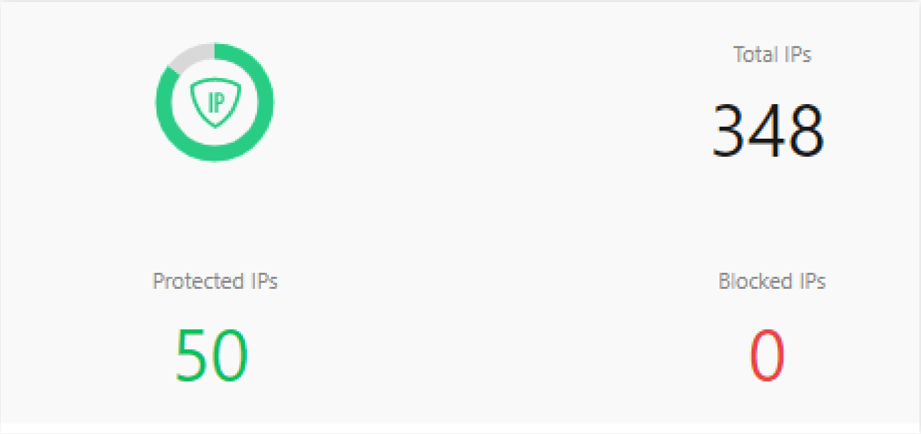
- Attacked IPs: the total number of attacked application IPs of basic protection, Anti-DDoS Pro and Anti-DDoS Advanced.
- Protected IPs: the total number of protected application IPs of Anti-DDoS Pro and Anti-DDoS Advanced.

©2013-2022 Tencent Cloud. All rights reserved.

- 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.

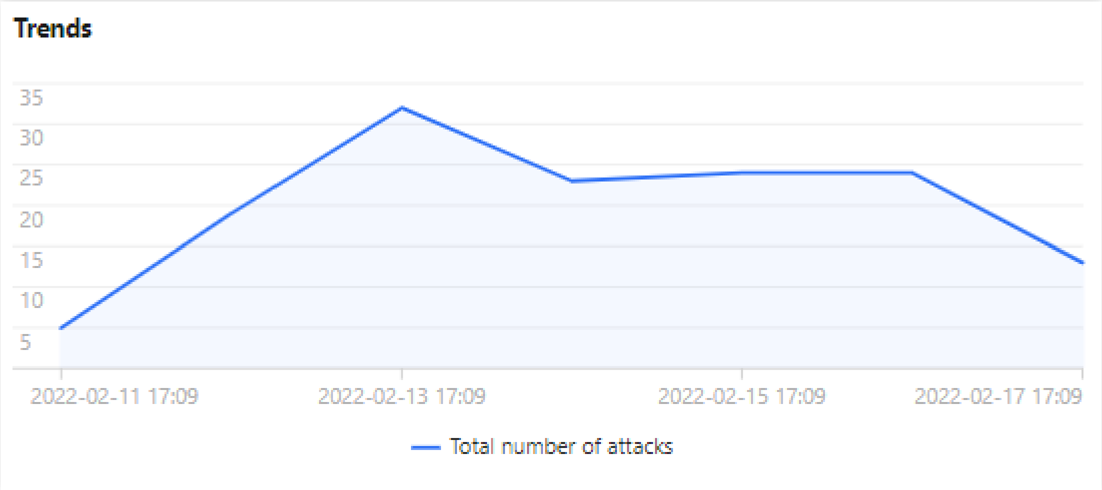


Field description:

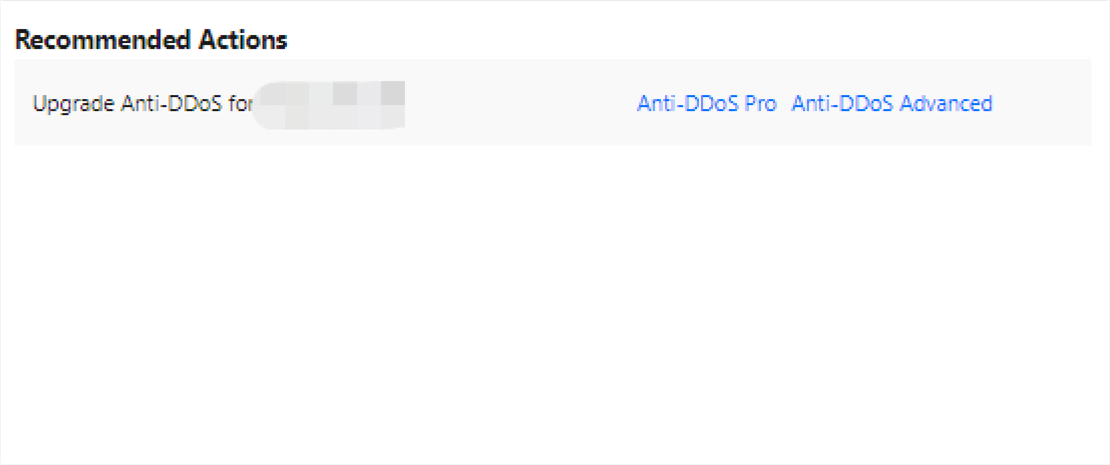
- Total IPs: the total number of application IPs, including IPs of basic protection, Anti-DDoS Pro and Anti-DDoS Advanced.
- Protected IPs: the total number of protected application IPs of Anti-DDoS Pro and Anti-DDoS Advanced.
- Blocked IPs: the total number of blocked IPs of basic protection, Anti-DDoS 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.

©2013-2022 Tencent Cloud. All rights reserved.



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

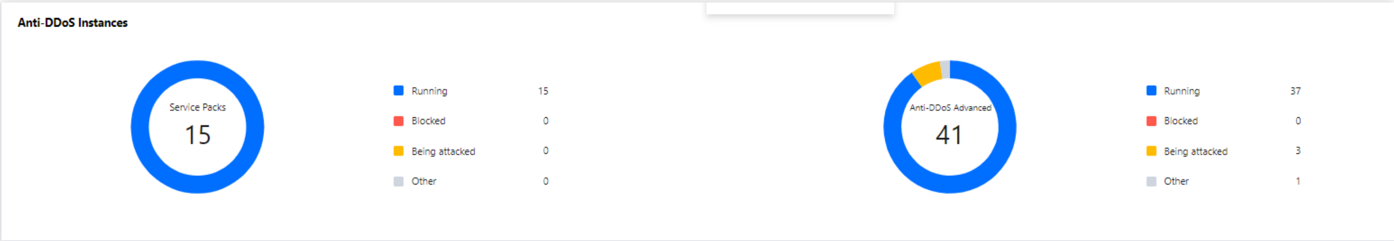


Recommended Actions

Upgrade Anti-DDoS for [redacted]

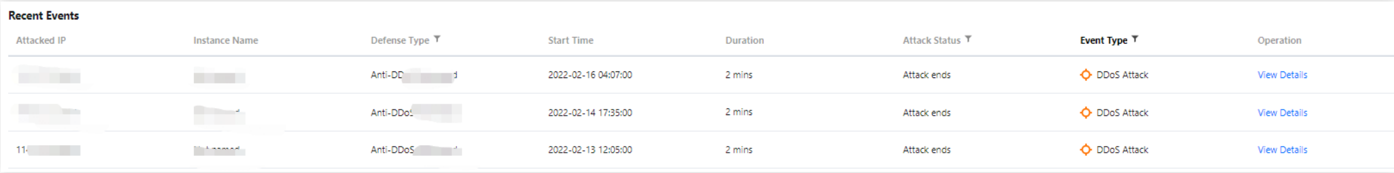
Viewing instance statistics

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.



Viewing recent events

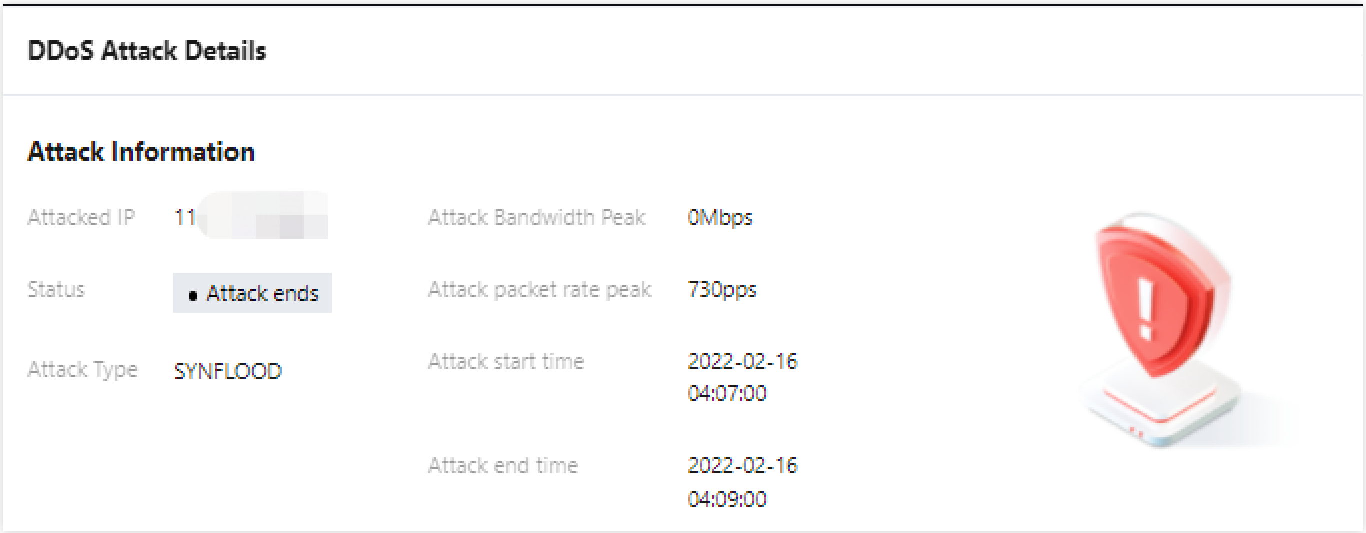
1. Log in to the new Anti-DDoS console, and select **Overview** on the left sidebar to enter the **Protection Overview** page.
2. The "Recent Events" module shows you all the recent attack events. For attack analysis and source tracing, click **View Details** to enter the event details page.



Recent Events

Attacked IP	Instance Name	Defense Type	Start Time	Duration	Attack Status	Event Type	Operation
[redacted]	[redacted]	Anti-DD[redacted]d	2022-02-16 04:07:00	2 mins	Attack ends	DDoS Attack	View Details
[redacted]	[redacted]	Anti-DDo[redacted]	2022-02-14 17:35:00	2 mins	Attack ends	DDoS Attack	View Details
11[redacted]	[redacted]	Anti-DDoS[redacted]	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 Information

Attacked IP: 11[redacted]

Status: ● Attack ends

Attack Type: SYNFLOOD

Attack Bandwidth Peak: 0Mbps

Attack packet rate peak: 730pps

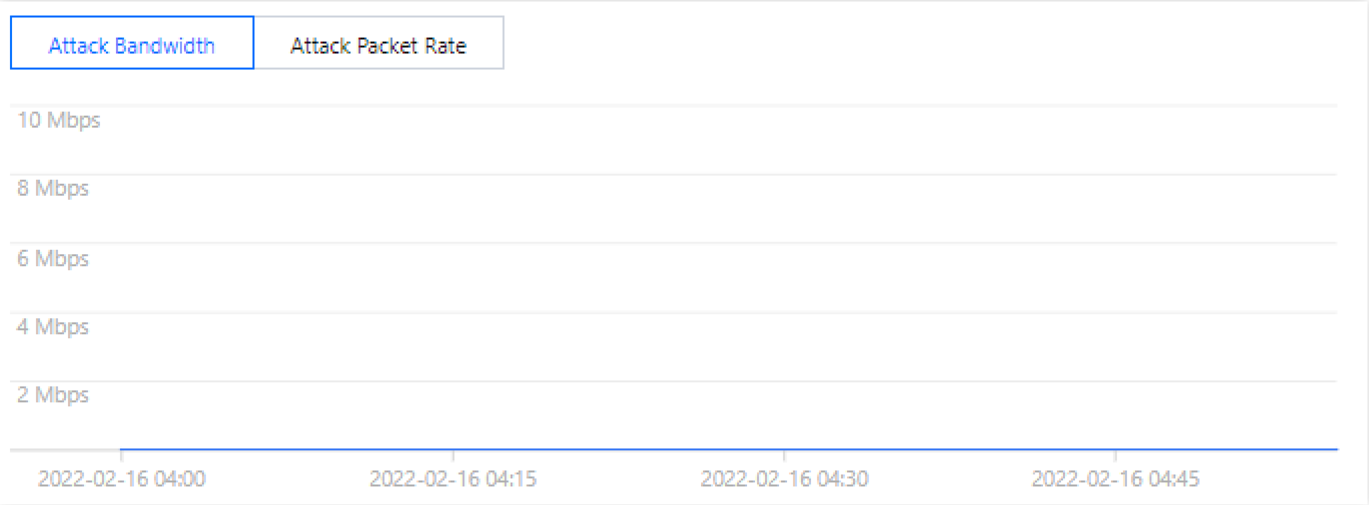
Attack start time: 2022-02-16 04:07:00

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.

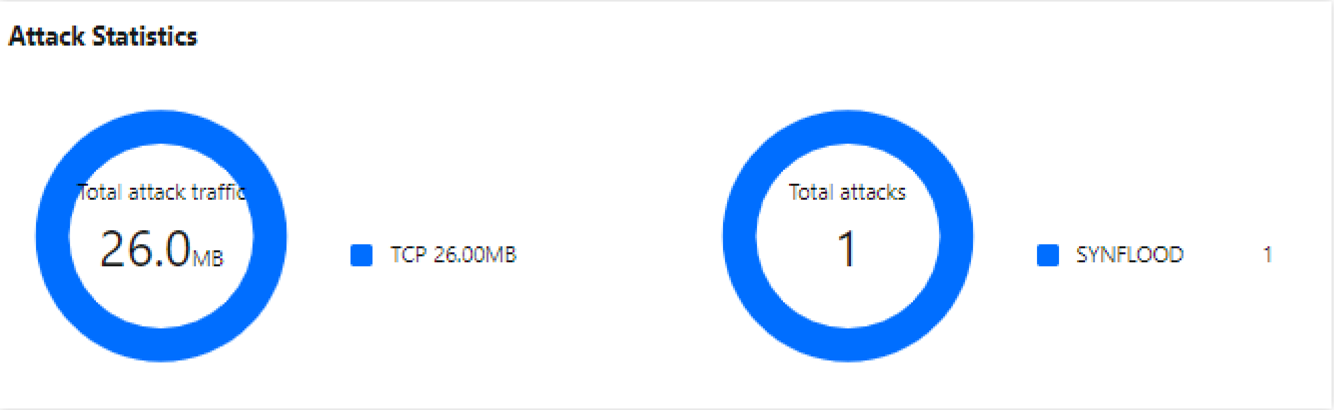
> Note：
> This module provides complete, real-time data in the attack period.

©2013-2022 Tencent Cloud. All rights reserved.



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.



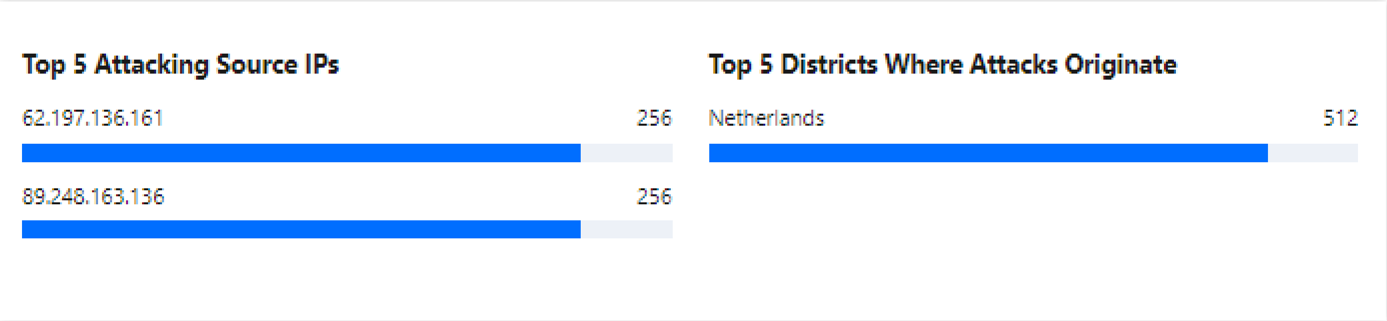
Field description:

- Attack traffic protocol distribution: 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.

©2013-2022 Tencent Cloud. All rights reserved.

> Note：
> This module provides sampled data in the attack period.



Top 5 Attacking Source IPs

62.197.136.161 256

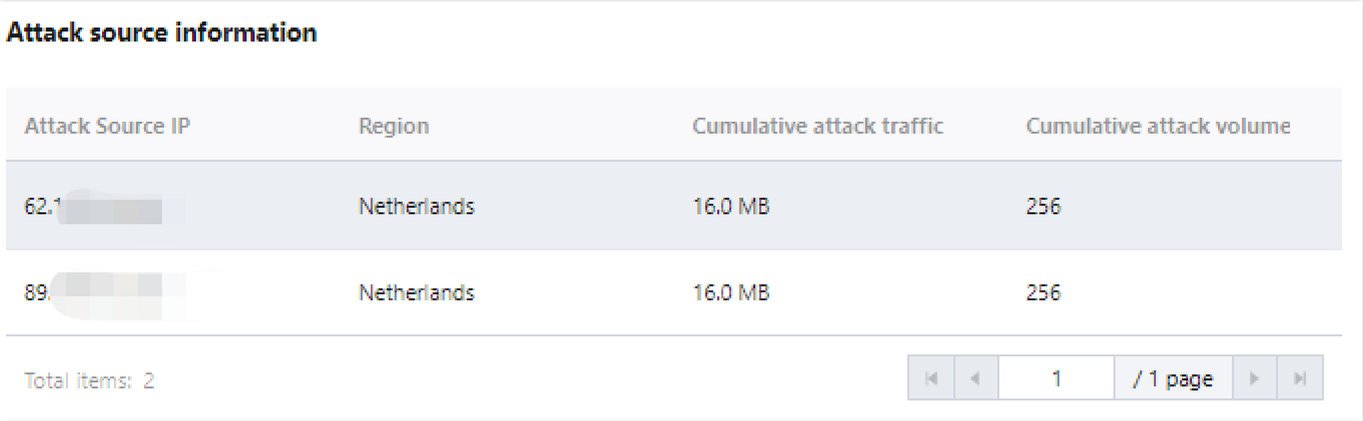
89.248.163.136 256

Top 5 Districts Where Attacks Originate

Netherlands 512

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[redacted]	Netherlands	16.0 MB	256
89.[redacted]	Netherlands	16.0 MB	256

Total items: 2

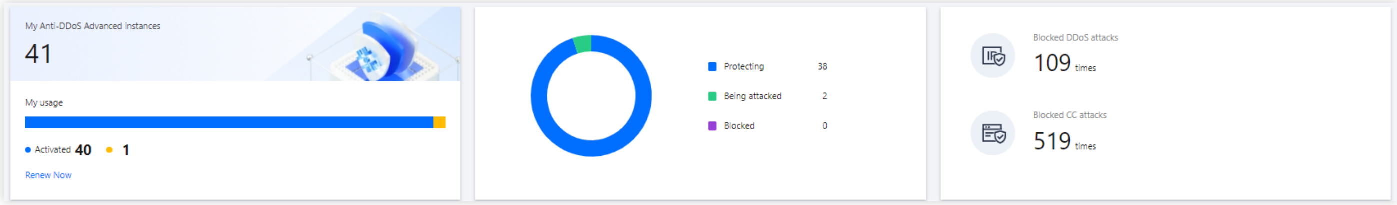
Anti-DDoS Pro Overview

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.

©2013-2022 Tencent Cloud. All rights reserved.

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.

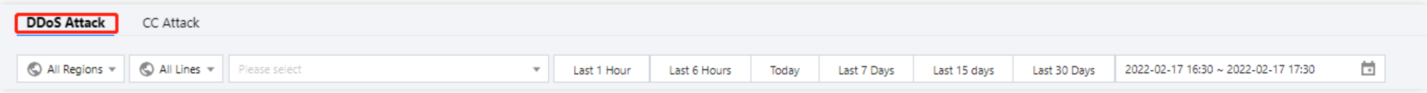

My Anti-DDoS Advanced Instances
41
My usage
● Activated 40 ● 1
Renew Now

🟦 Protecting	38
🟩 Being attacked	2
🟪 Blocked	0

Blocked DDoS attacks
109 times
Blocked CC attacks
519 times

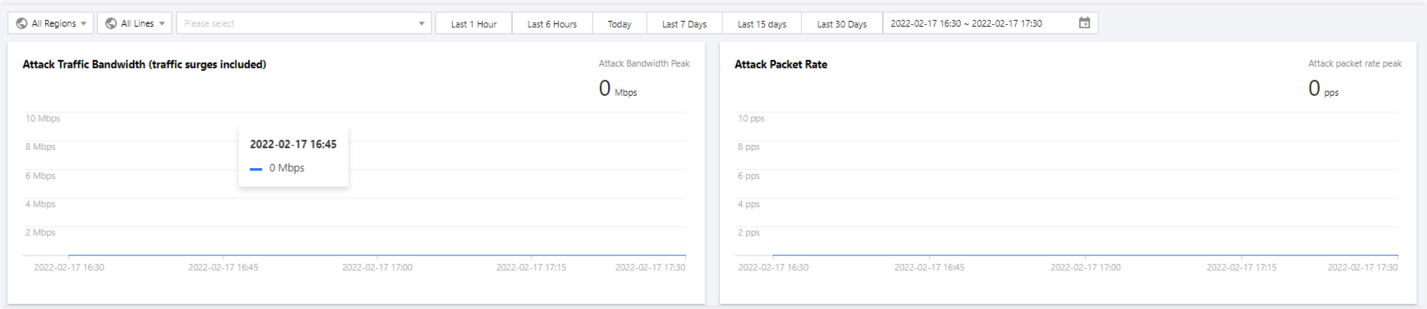
2. On the **DDoS Attack** tab, select a query period, target region, and an instance to check whether the instance has been attacked. The complete attack data is displayed by default.

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



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

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.



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

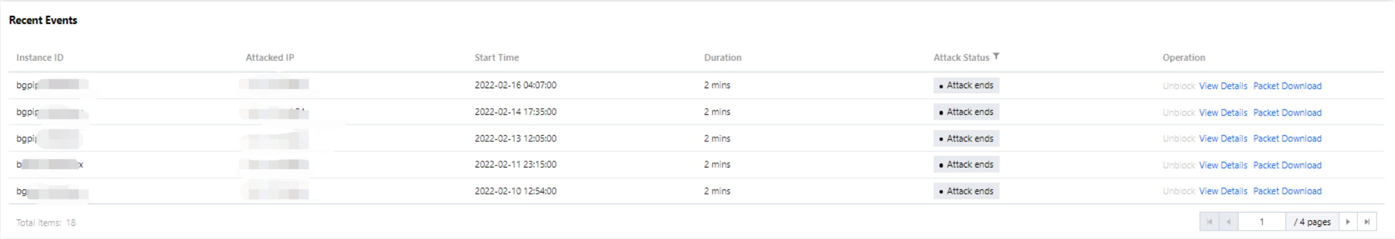
Attack Traffic Bandwidth (traffic surges included)
Attack Bandwidth Peak
0 Mbps
2022-02-17 16:45
0 Mbps

Attack Packet Rate
Attack packet rate peak
0 pps

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.

©2013-2022 Tencent Cloud. All rights reserved.

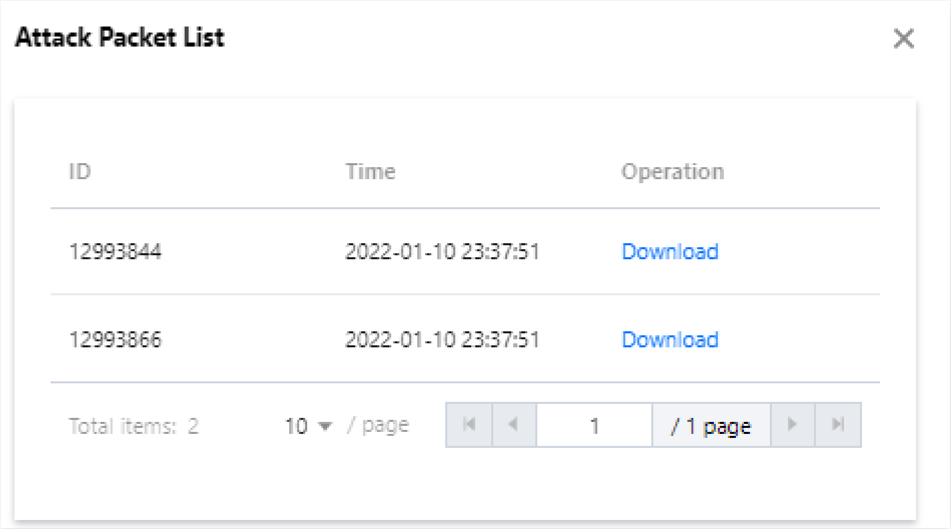


Recent Events

Instance ID	Attacked IP	Start Time	Duration	Attack Status	Operation
bgpip[redacted]	[redacted]	2022-02-16 04:07:00	2 mins	● Attack ends	Unblock View Details Packet Download
bgpip[redacted]	[redacted]	2022-02-14 17:35:00	2 mins	● Attack ends	Unblock View Details Packet Download
bgpi[redacted]	[redacted]	2022-02-13 12:05:00	2 mins	● Attack ends	Unblock View Details Packet Download
b[redacted]x	[redacted]	2022-02-11 23:15:00	2 mins	● Attack ends	Unblock View Details Packet Download
bg[redacted]	[redacted]	2022-02-10 12:54:00	2 mins	● Attack ends	Unblock View Details Packet Download

Total items: 18

- 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.

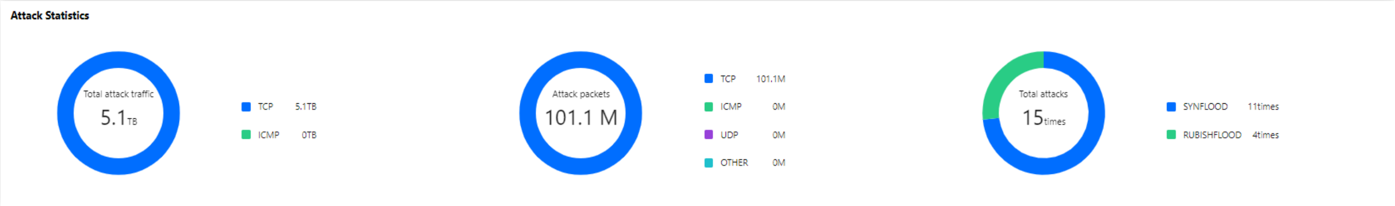


Attack Packet List

ID	Time	Operation
12993844	2022-01-10 23:37:51	Download
12993866	2022-01-10 23:37:51	Download

Total items: 2

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

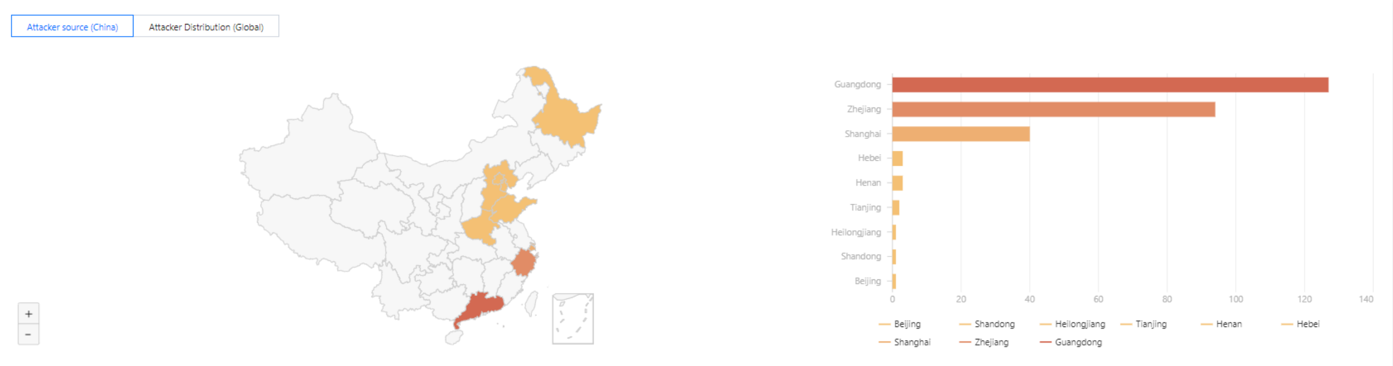


Field description:

- 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.

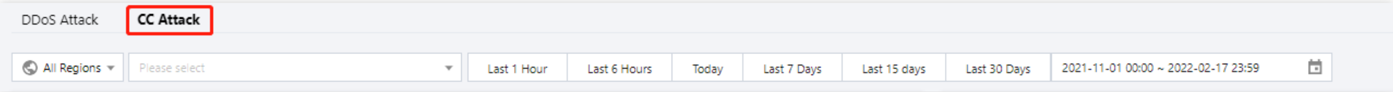
- Attack type distribution: displays how attacks on the selected Anti-DDoS Pro instance distribute over different attack types within the queried period.

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.

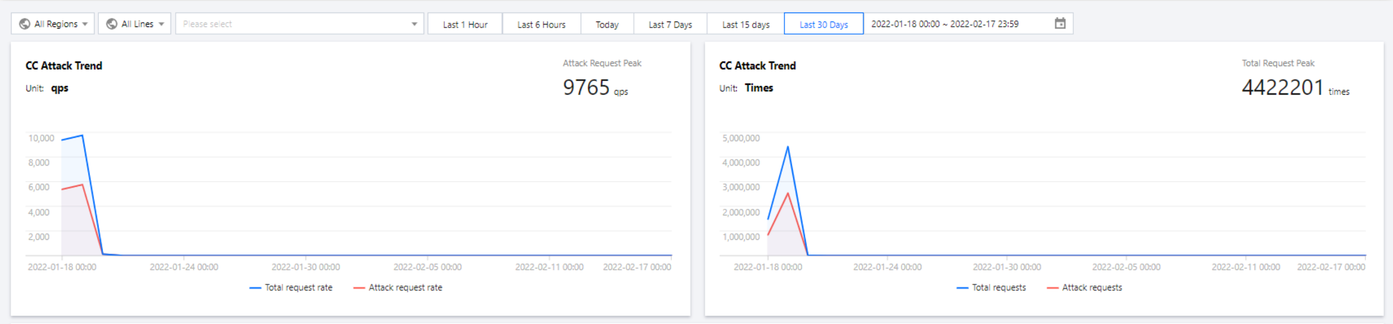


Viewing CC protection details

1. On the **CC Protection** tab, select a query period, target region, and an instance to check whether the instance has been attacked.



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

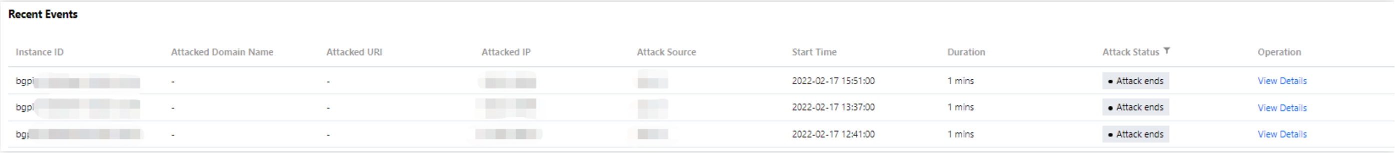


Field description:

- 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.

©2013-2022 Tencent Cloud. All rights reserved.

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	Operation
bgpi[redacted]	-	-	[redacted]	[redacted]	2022-02-17 15:51:00	1 mins	● Attack ends	View Details
bgpi[redacted]	-	-	[redacted]	[redacted]	2022-02-17 13:37:00	1 mins	● Attack ends	View Details
bg[redacted]	-	-	[redacted]	[redacted]	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.

©2013-2022 Tencent Cloud. All rights reserved.

Instance Management

Viewing Instance Information

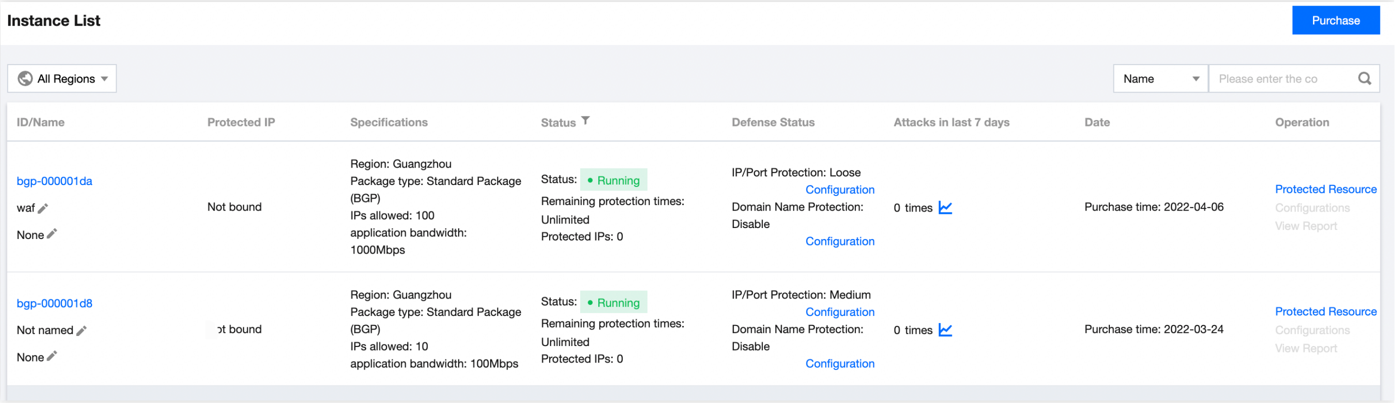
Last updated：2022-04-22 11:29:54

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

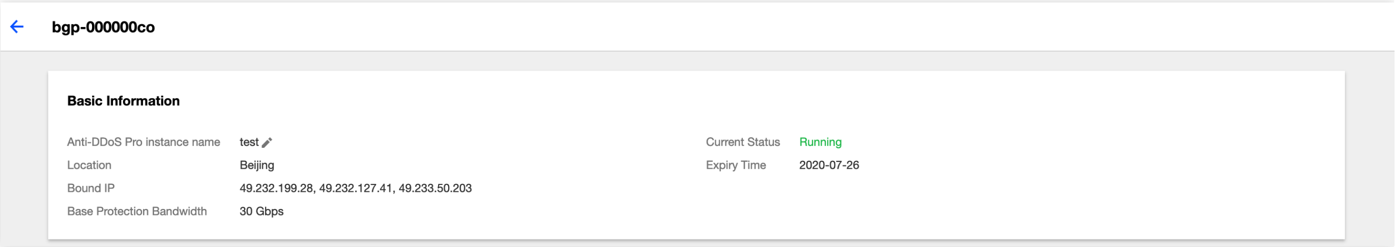
This example shows you how to view the information of the single IP instance `bgp-0000008o` in the Guangzhou region.

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-0000008o` 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.



ID/Name	Protected IP	Specifications	Status	Defense Status	Attacks in last 7 days	Date	Operation
bgp-000001da waf None	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: 2022-04-06	Protected Resource Configurations View Report
bgp-000001d8 Not named None	›t 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: 2022-03-24	Protected Resource Configurations View Report

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



bgp-000000co

Basic Information

Anti-DDoS Pro instance name	test	Current Status	Running
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.

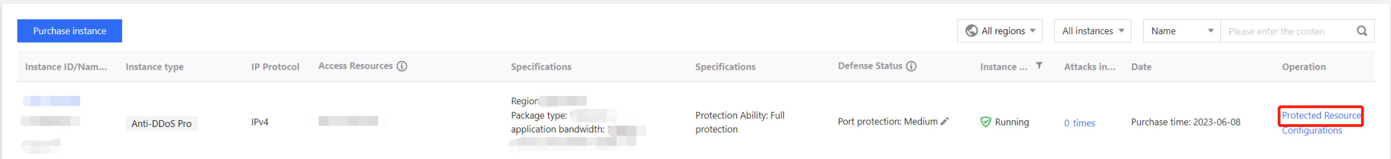
Prerequisite

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.



Instance ID/Nam...	Instance type	IP Protocol	Access Resources	Specifications	Specifications	Defense Status	Instance ...	Attacks in...	Date	Operation
[redacted]	Anti-DDoS Pro	IPv4	[redacted]	Region [redacted] Package type: [redacted] application bandwidth: [redacted]	Protection Ability: Full protection	Port protection: Medium	Running	0 times	Purchase time: 2023-06-08	Protected Resource Configurations

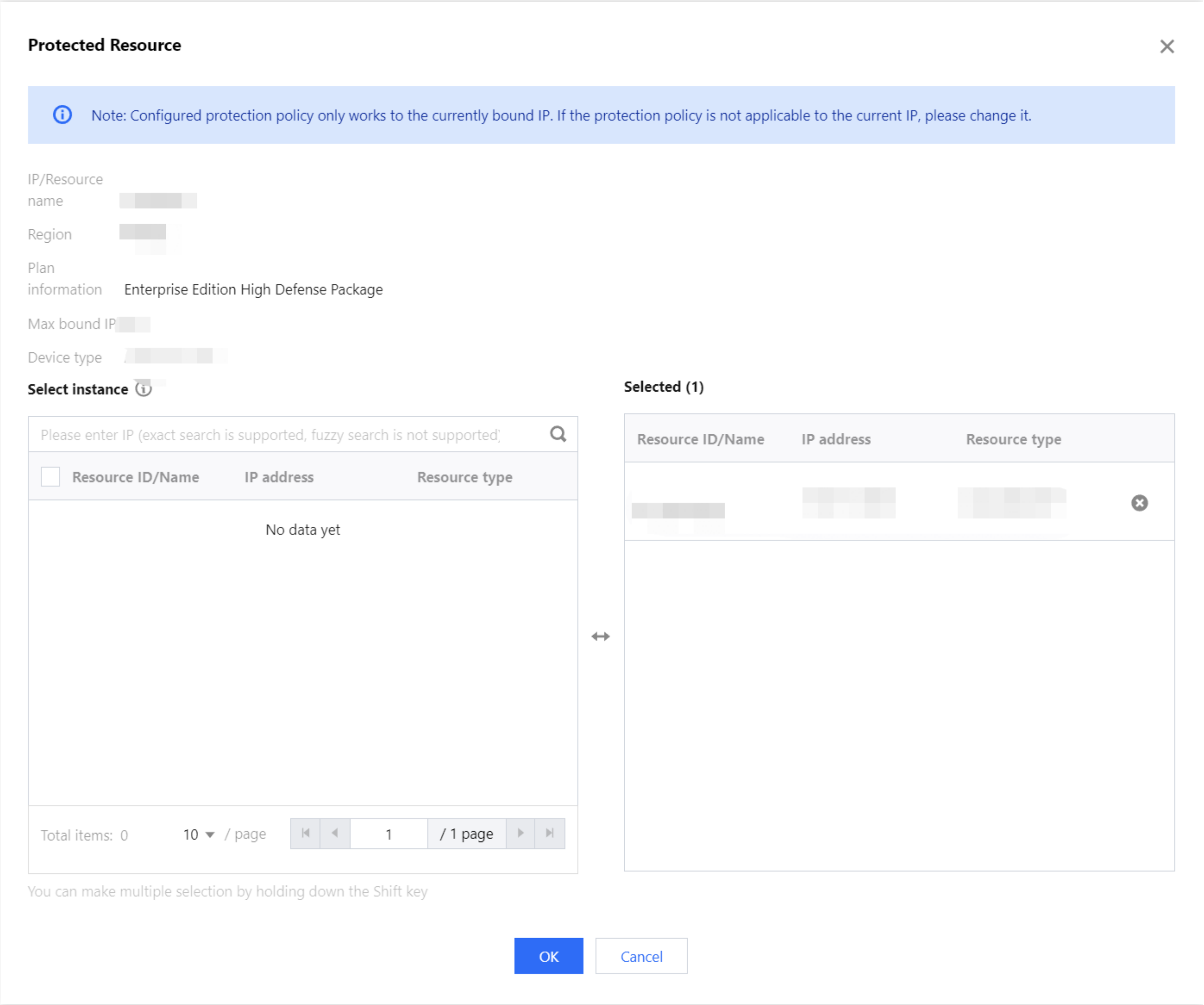
3. On the **Protected Resource** page, select a resource type and a resource instance as needed.

- 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.

©2013-2022 Tencent Cloud. All rights reserved.

- 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 the protection policy is not applicable 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

Please enter IP (exact search is supported, fuzzy search is not supported)

□ Resource ID/Name	IP address	Resource type
No data yet		

Total items: 0 10 / page 1 / 1 page

Selected (1)

Resource ID/Name	IP address	Resource type

You can make multiple selection by holding down the Shift key

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

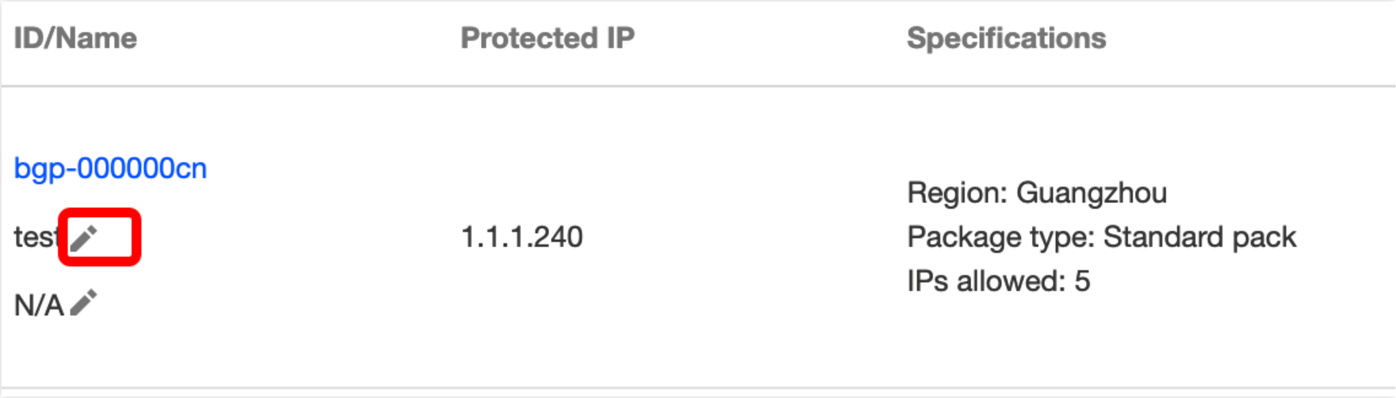
You need to purchase an Anti-DDoS Pro instance and set the protected object's IP first.

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.



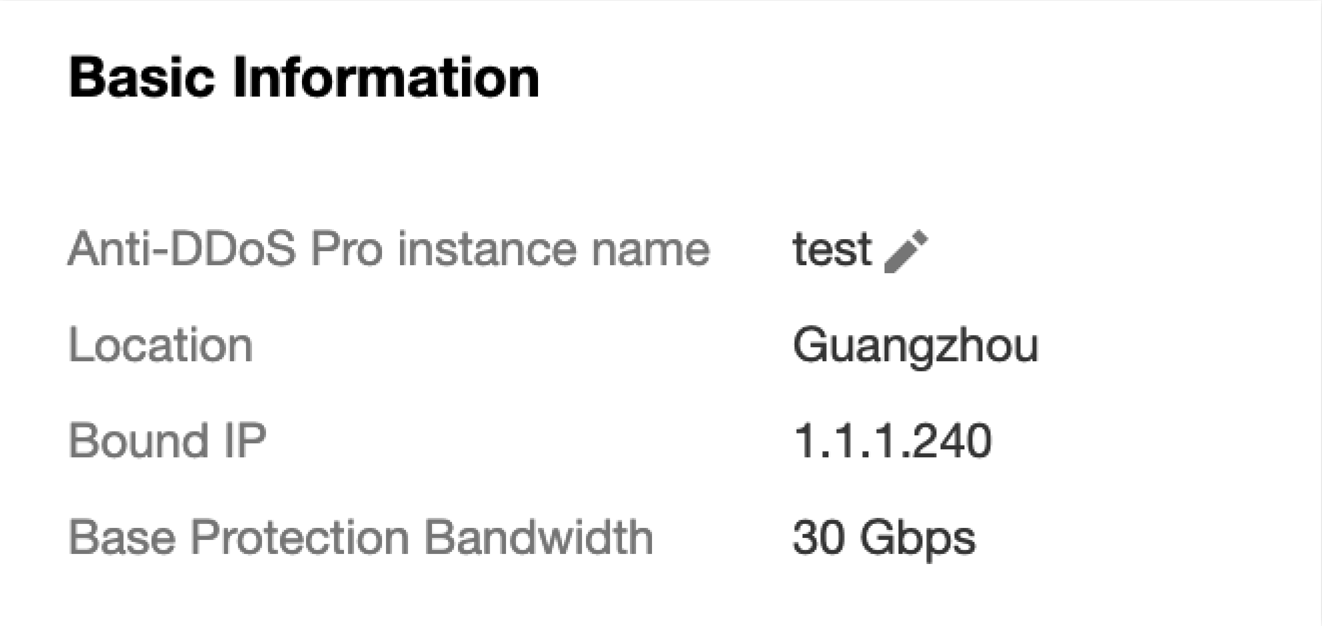
ID/Name	Protected IP	Specifications
bgp-000000cn test ✎ N/A ✎	1.1.1.240	Region: Guangzhou Package type: Standard pack IPs allowed: 5

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.

©2013-2022 Tencent Cloud. All rights reserved.

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.



Basic Information

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:

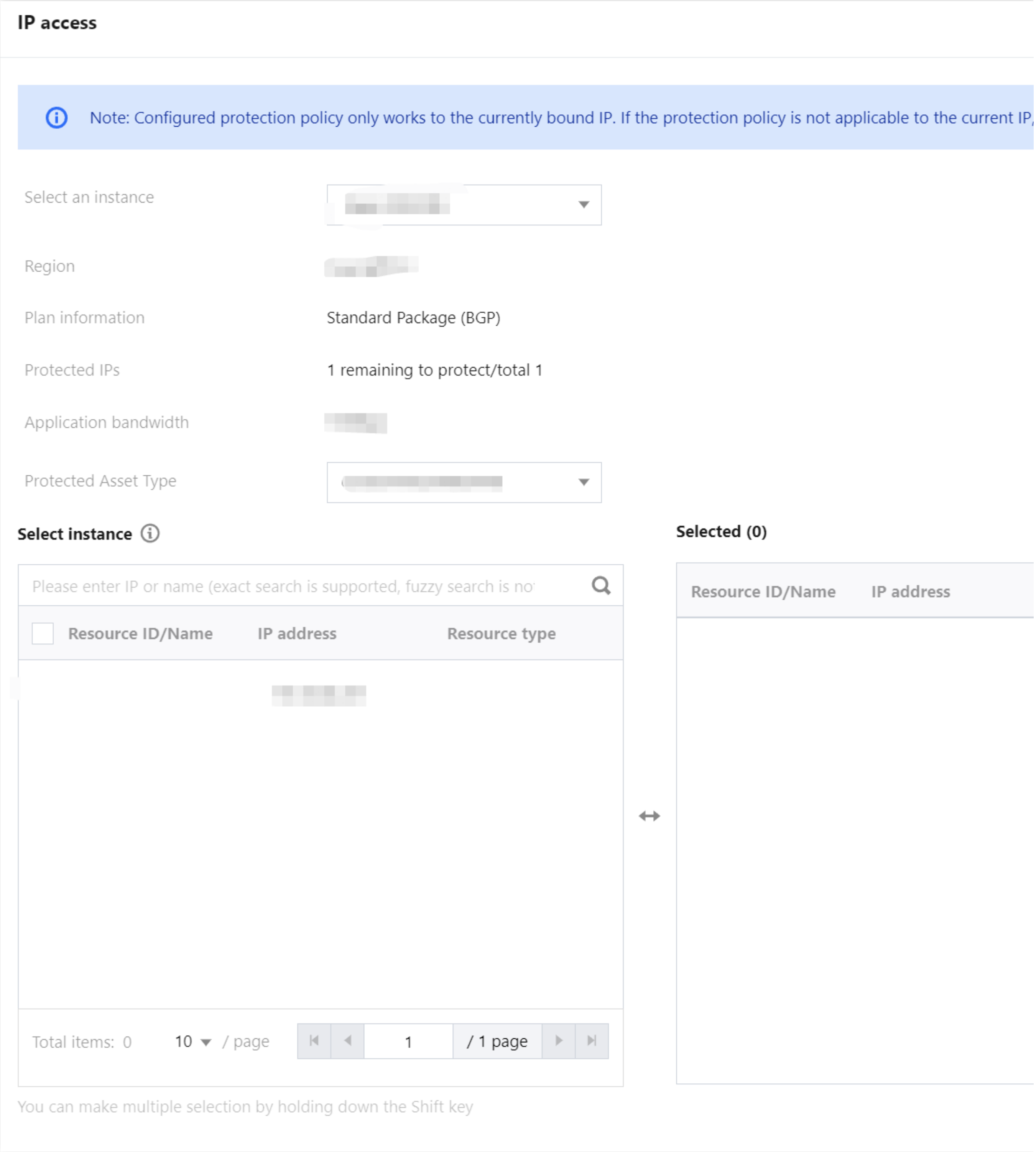
Quick IP access allows you to quickly bind an Anti-DDoS Pro instance to a cloud asset. Note that for an Anti-DDoS Pro (Enterprise) instance, you need to first unbind the cloud asset from the original public IP and bind it to an EIP in the CVM console. If you want to hide the IP of the real server, please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



IP access

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

Select an instance	
Region	
Plan information	Standard Package (BGP)
Protected IPs	1 remaining to protect/total 1
Application bandwidth	
Protected Asset Type	

Select instance

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

□ Resource ID/Name	IP address	Resource type

Total items: 0 10 / page 1 / 1 page

Selected (0)

Resource ID/Name	IP address

You can make multiple selection by holding down the Shift key

Note

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

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

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

4. Click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.

Domain Name Connection

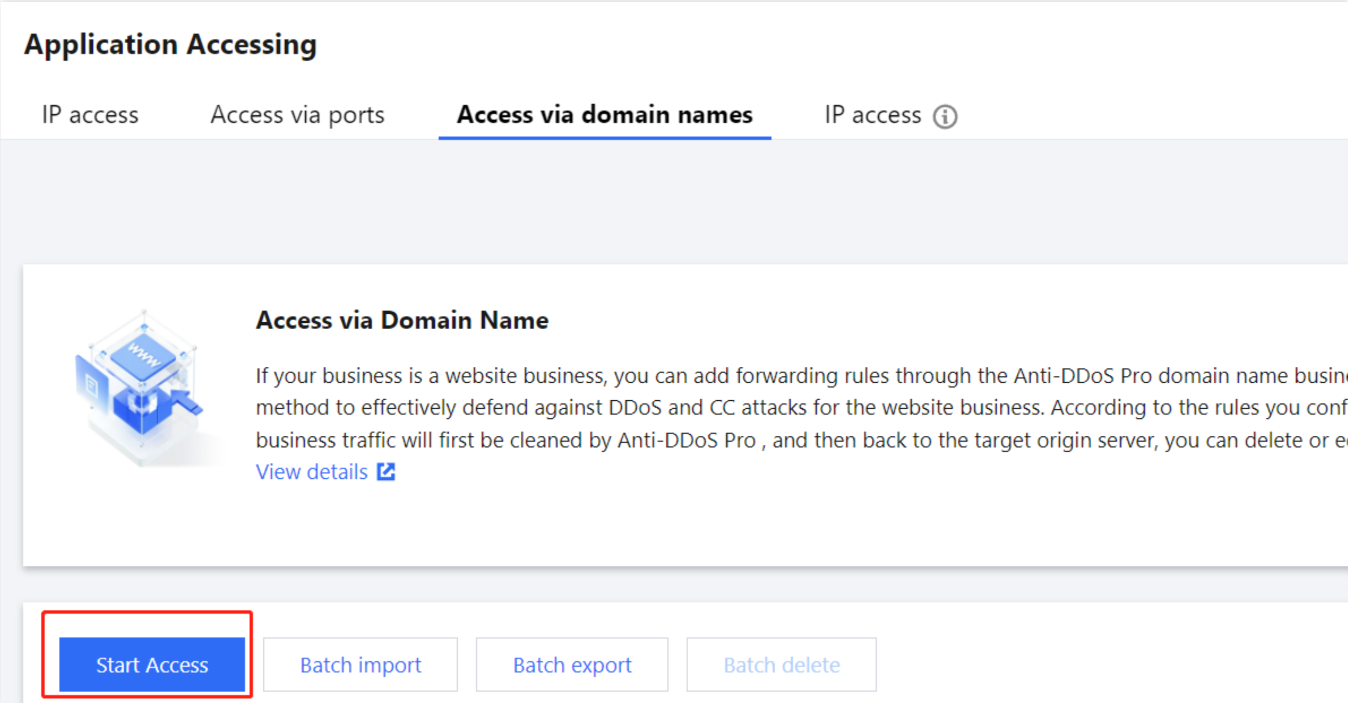
Last updated：2024-01-24 15:14:11

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 Domain Name

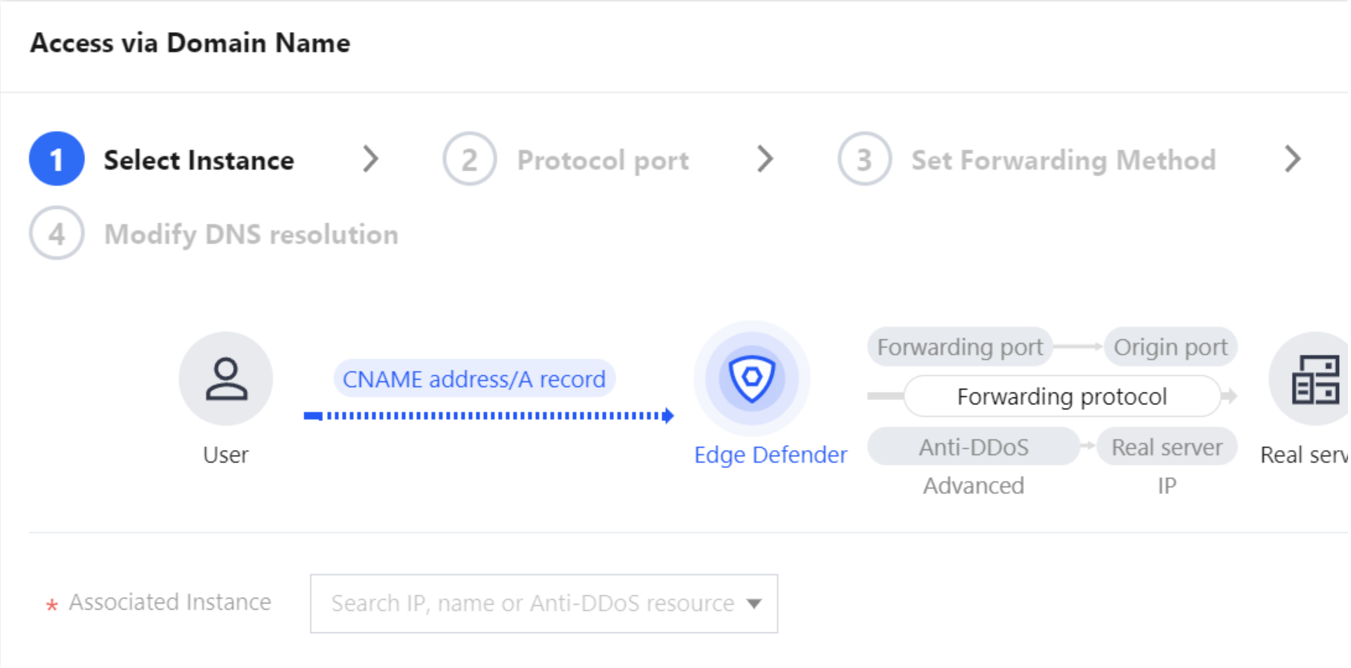
If your business is a website business, you can add forwarding rules through the Anti-DDoS Pro domain name busin
method to effectively defend against DDoS and CC attacks for the website business. According to the rules you conf
business traffic will first be cleaned by Anti-DDoS Pro , and then back to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

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

Note:

You can select multiple instances.

©2013-2022 Tencent Cloud. All rights reserved.

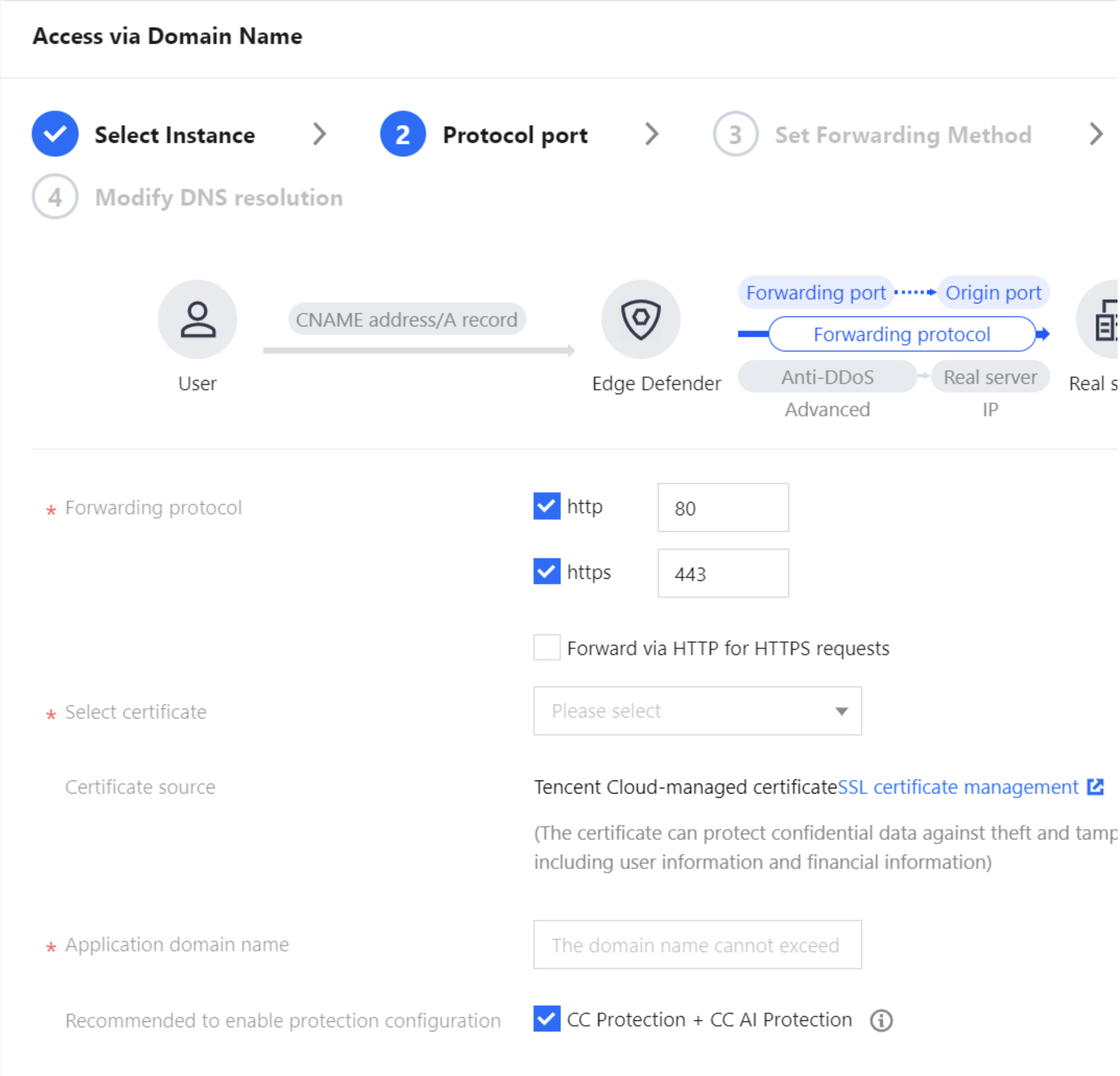


Access via Domain Name

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

* Associated Instance: Search IP, name or Anti-DDoS resource ▾

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



Access via Domain Name

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

* Forwarding protocol: ☑ http 80; ☑ https 443

□ Forward via HTTP for HTTPS requests

* Select certificate: Please select

Certificate source: Tencent Cloud-managed certificateSSL certificate management

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

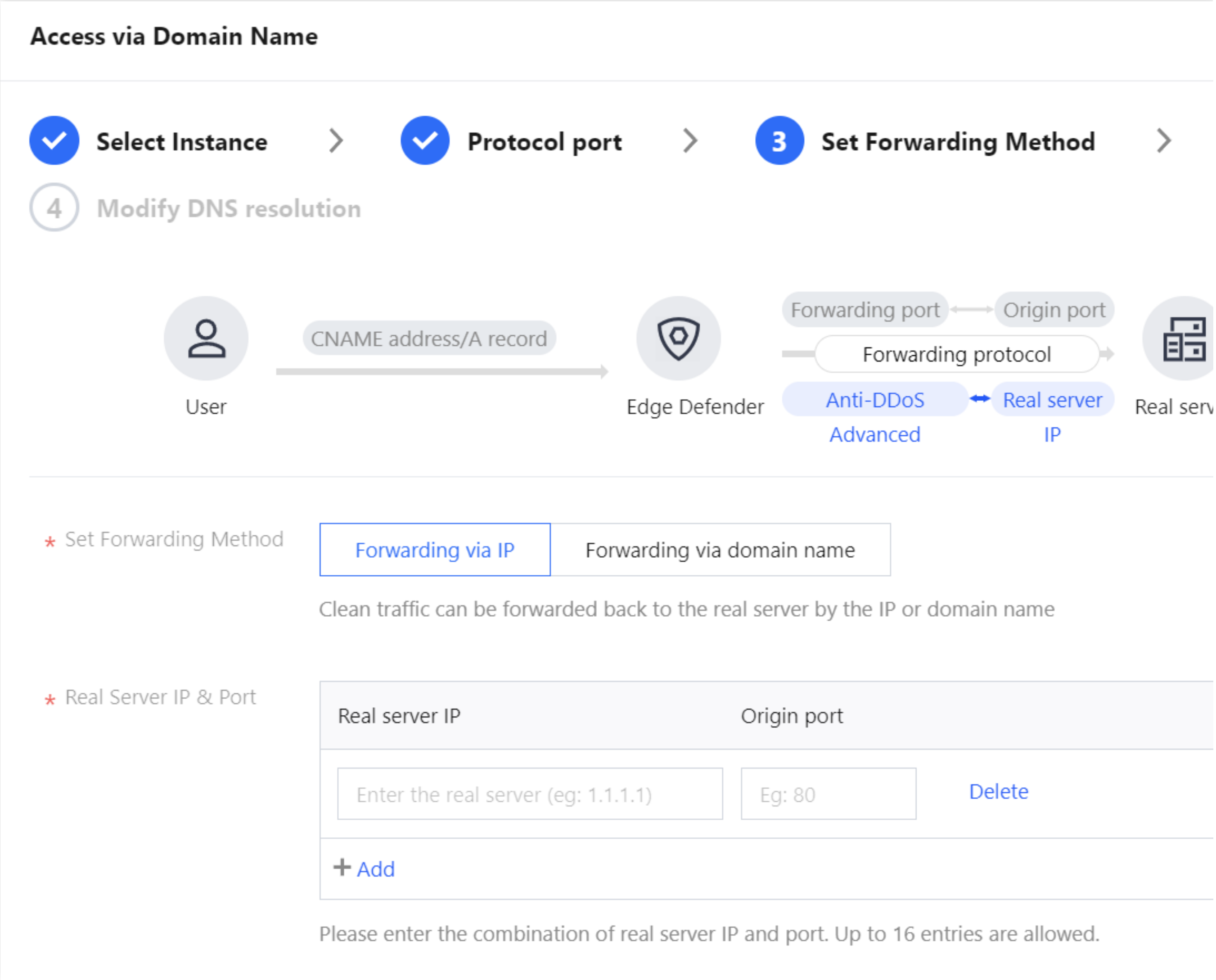
* Application domain name: The domain name cannot exceed

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 Name

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

* Set Forwarding Method: Forwarding via IP | Forwarding via domain name

Clean traffic can be forwarded back to the real server by the IP or domain name

* Real Server IP & Port

Real server IP	Origin port	
Enter the real server (eg: 1.1.1.1)	Eg: 80	Delete

+ Add

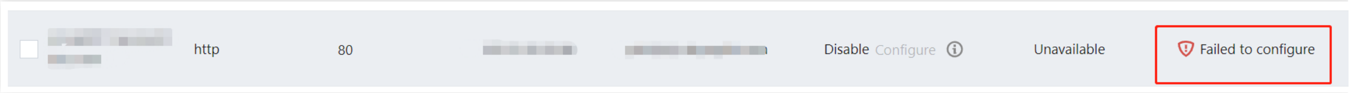
Please enter the combination of real server IP and port. Up to 16 entries are allowed.

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

Note:

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

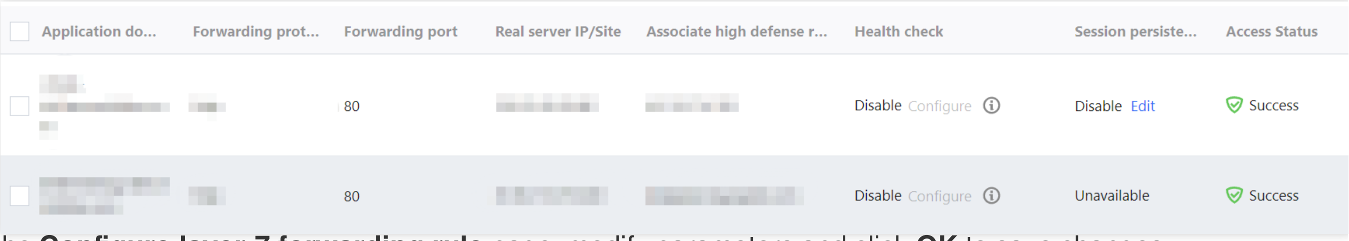
To avoid seconds of interruptions, update the certificate for connected domain names during off-peak periods.



□	[redacted]	http	80	[redacted]	[redacted]	Disable Configure ⓘ	Unavailable	Failed to configure

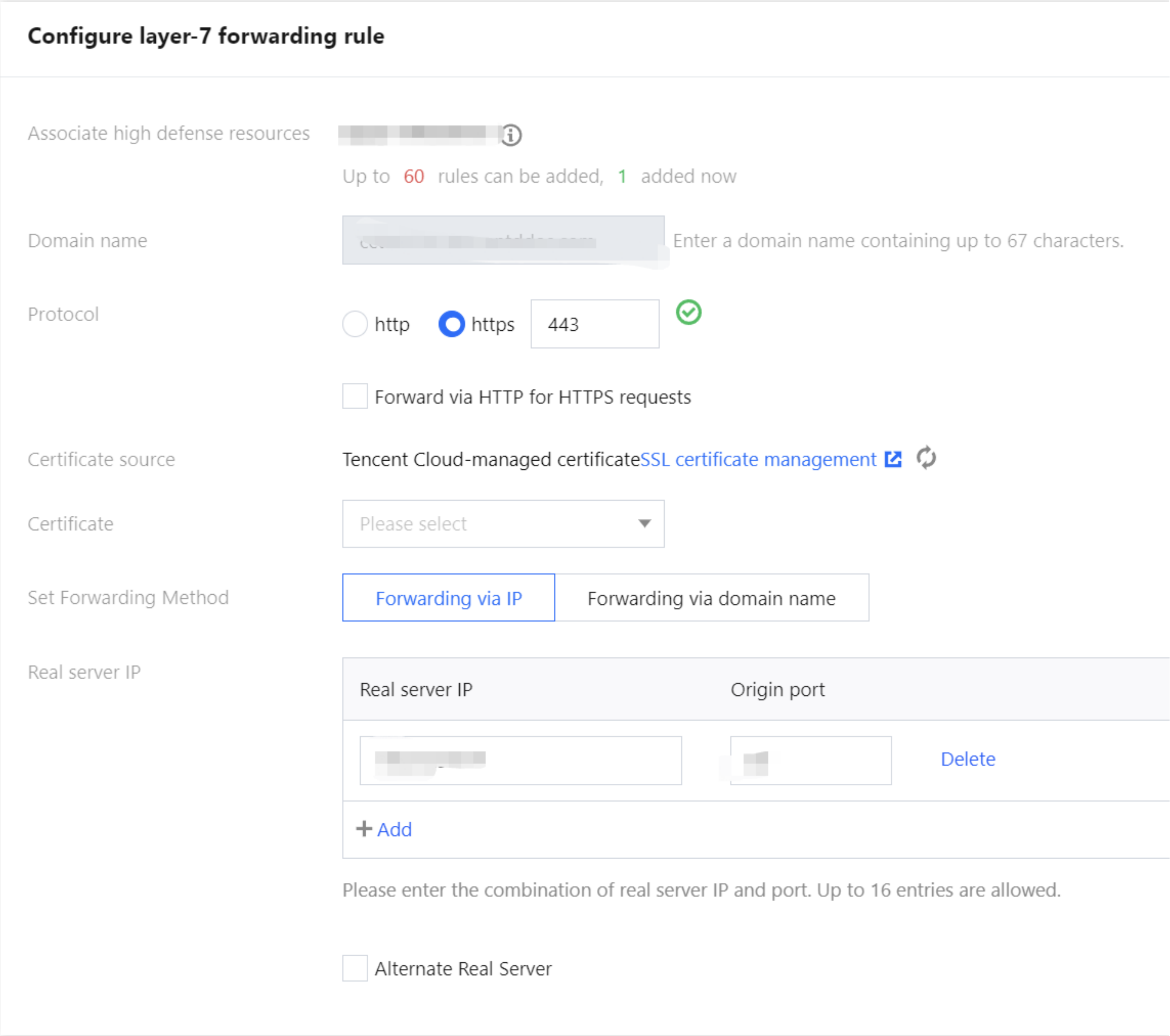
Editing a rule

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



☐	Application do...	Forwarding prot...	Forwarding port	Real server IP/Site	Associate high defense r...	Health check	Session persiste...	Access Status
☐	[redacted]	[redacted]	80	[redacted]	[redacted]	Disable Configure ⓘ	Disable Edit	✓ Success
☐	[redacted]	[redacted]	80	[redacted]	[redacted]	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 [redacted] ⓘ

Up to 60 rules can be added, 1 added now

Domain name [redacted] Enter a domain name containing up to 67 characters.

Protocol ○ http ● https 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	
[redacted]	[redacted]	Delete

+ Add

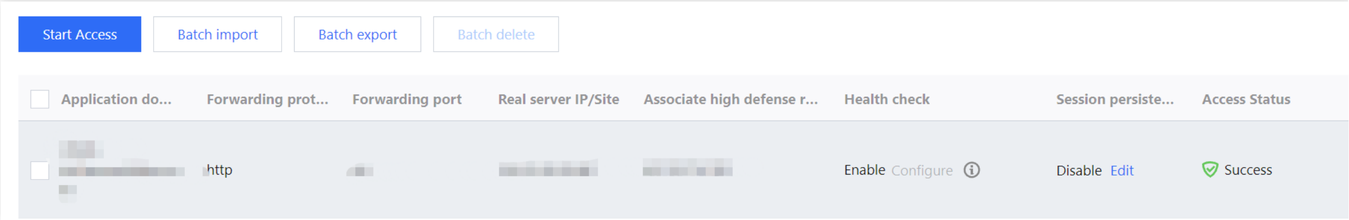
Please enter the combination of real server IP and port. Up to 16 entries are allowed.

☐ Alternate Real Server

Deleting a rule

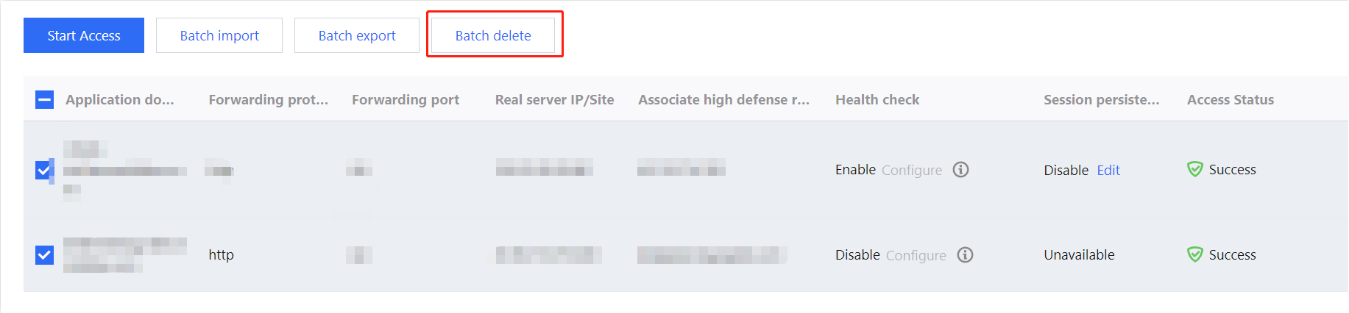
1. On the Access via domain name page, you can delete one or more rules.

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



□	Application do...	Forwarding prot...	Forwarding port	Real server IP/Site	Associate high defense r...	Health check	Session persiste...	Access Status
□	[redacted]	http	[redacted]	[redacted]	[redacted]	Enable Configure ⓘ	Disable Edit	✓ Success

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



☐	Application do...	Forwarding prot...	Forwarding port	Real server IP/Site	Associate high defense r...	Health check	Session persiste...	Access Status
☑	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Enable Configure ⓘ	Disable Edit	✓ Success
☑	[redacted]	http	[redacted]	[redacted]	[redacted]	Disable Configure ⓘ	Unavailable	✓ Success

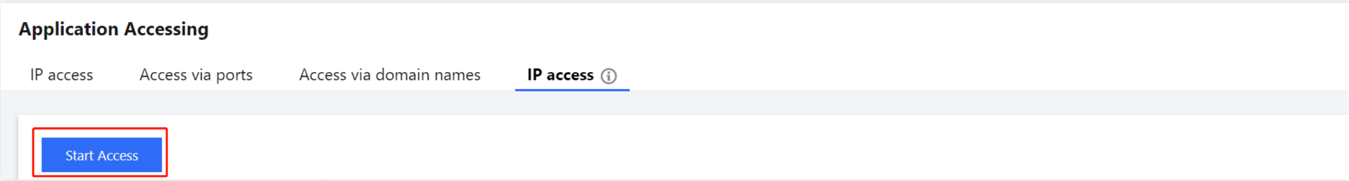
2. In the pop-up window, click **Delete**.

IP Connection

Last updated：2024-01-24 15:18:45

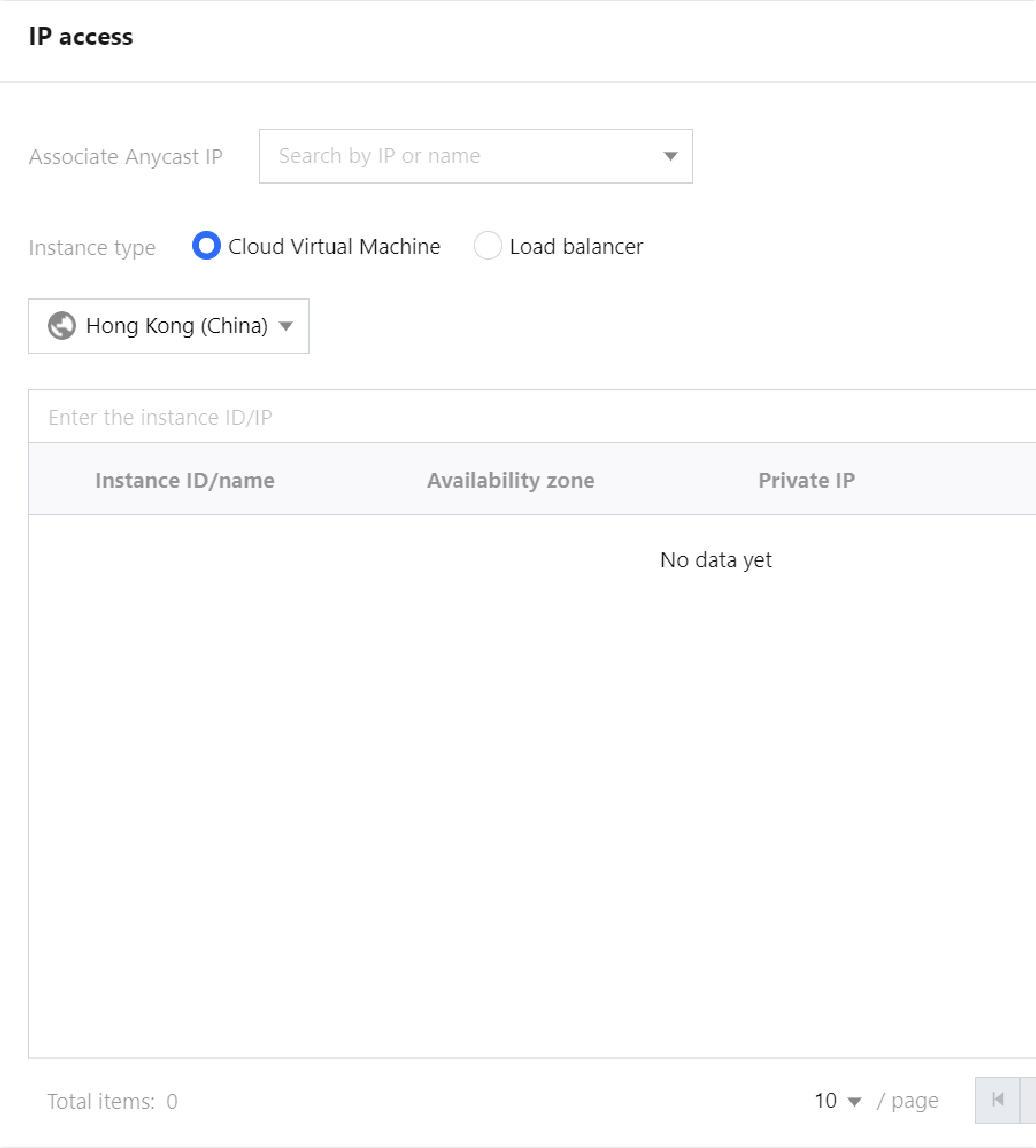
Connecting a rule

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



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

©2013-2022 Tencent Cloud. All rights reserved.



IP access

Associate Anycast IP: Search by IP or name

Instance type: ● Cloud Virtual Machine ○ Load balancer

Hong Kong (China)

Enter the instance ID/IP

Instance ID/name	Availability zone	Private IP
No data yet		

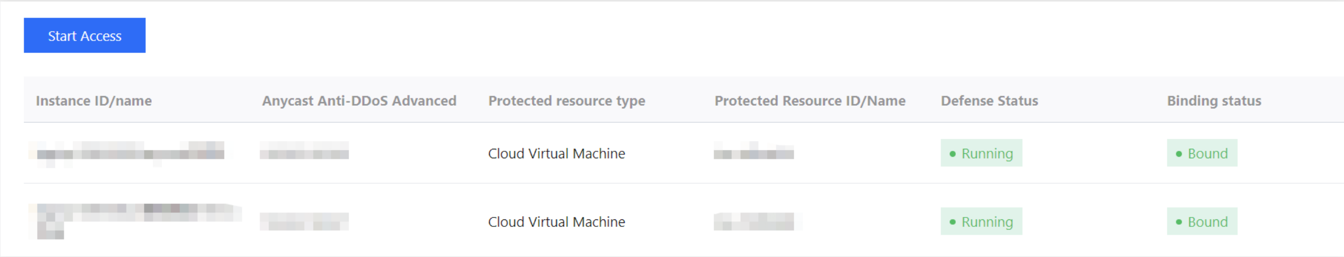
Total items: 0

10 / page

Deleting a rule

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

©2013-2022 Tencent Cloud. All rights reserved.



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

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

Port Connection

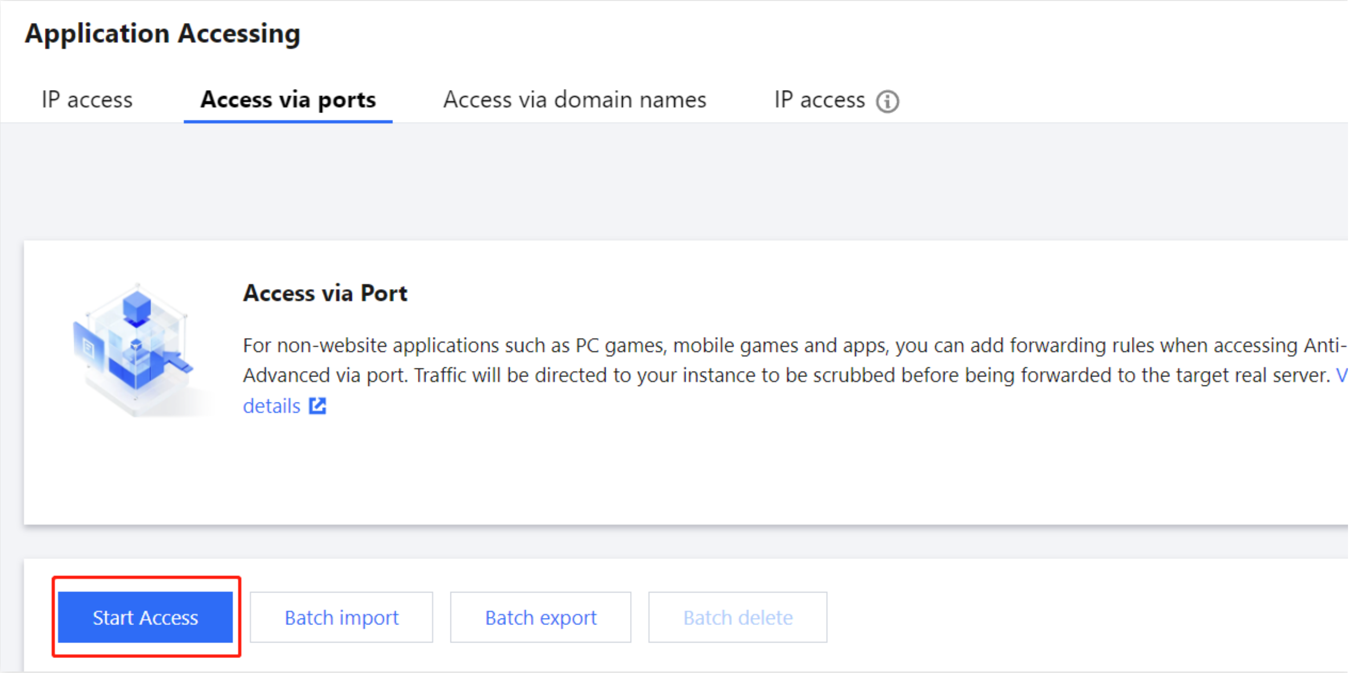
Last updated：2024-01-24 15:19:43

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

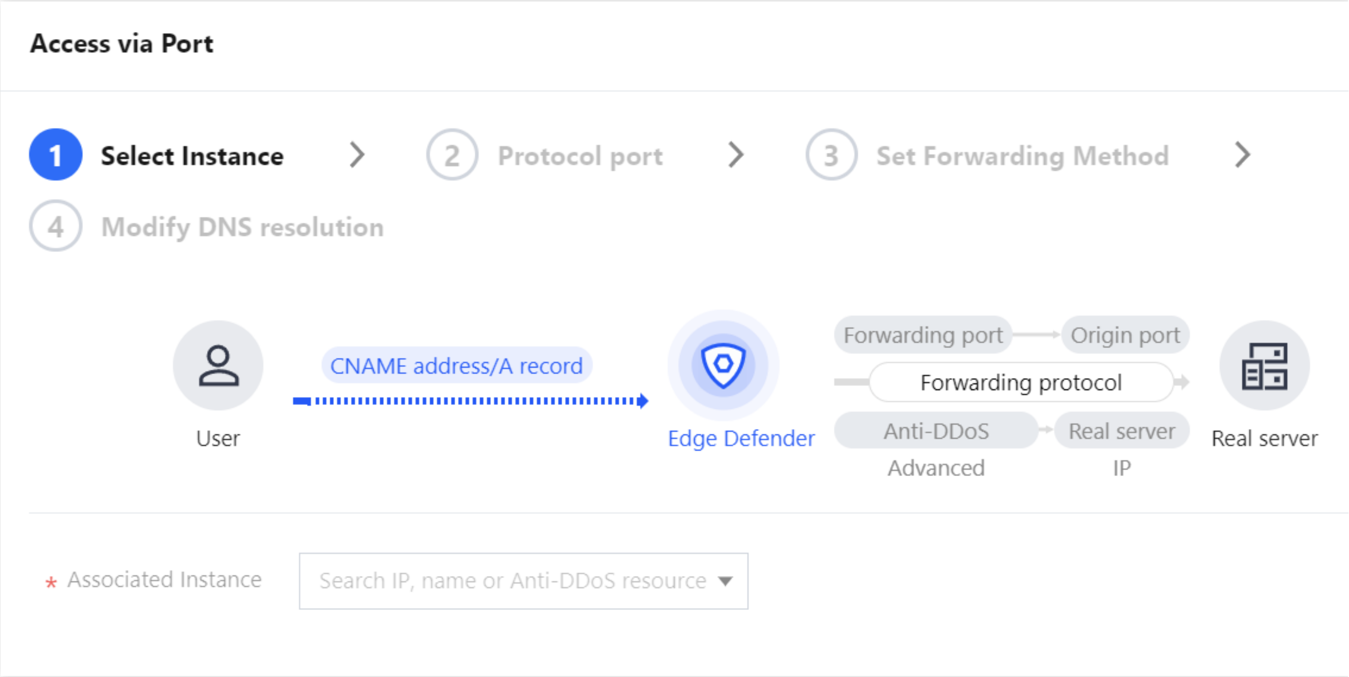
Access via Port

For non-website applications such as PC games, mobile games and apps, you can add forwarding rules when accessing Anti-Advanced via port. Traffic will be directed to your instance to be scrubbed before being forwarded to the target real server. V details

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

Note:

You can select multiple instances.

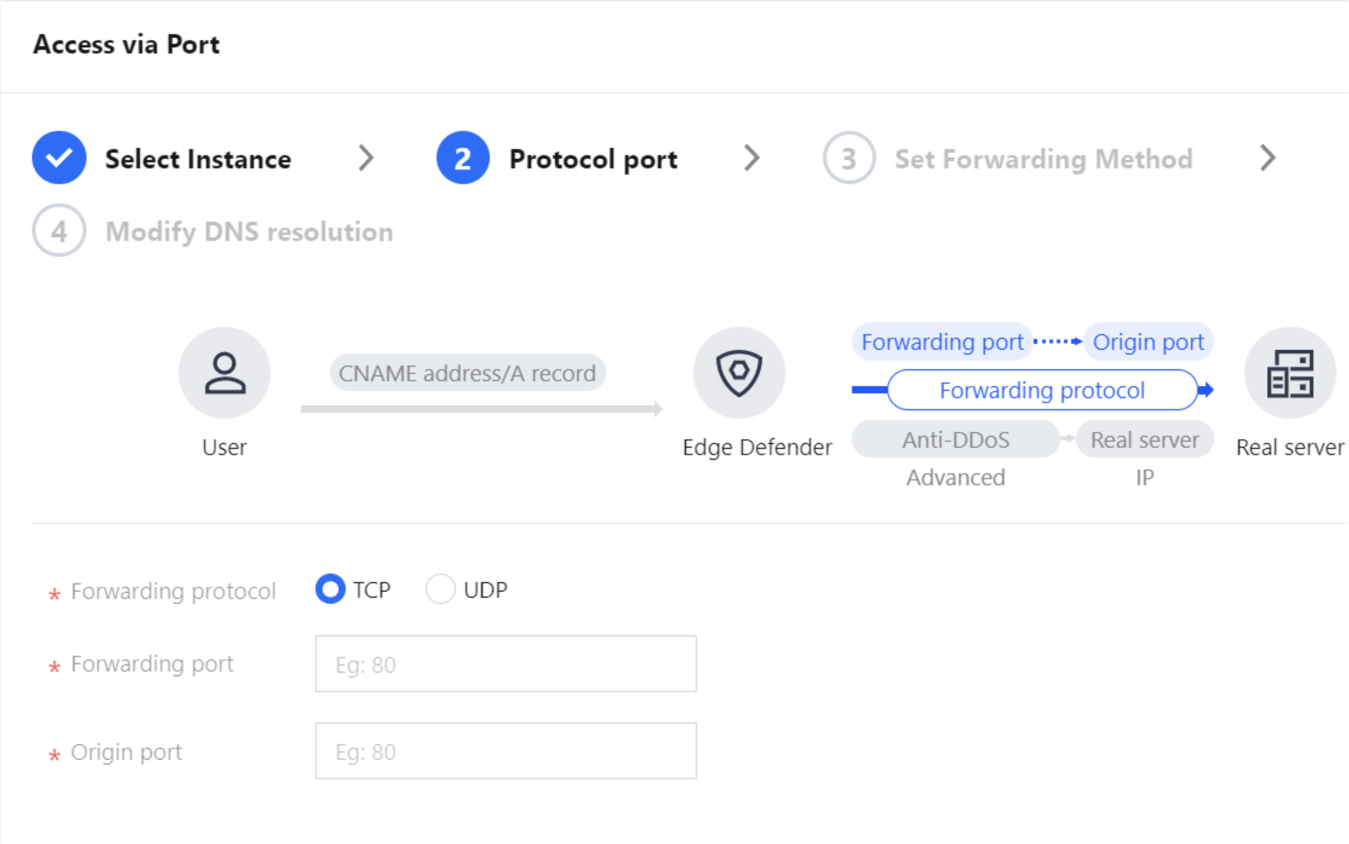


Access via Port

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

* Associated Instance: Search IP, name or Anti-DDoS resource ▾

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



Access via Port

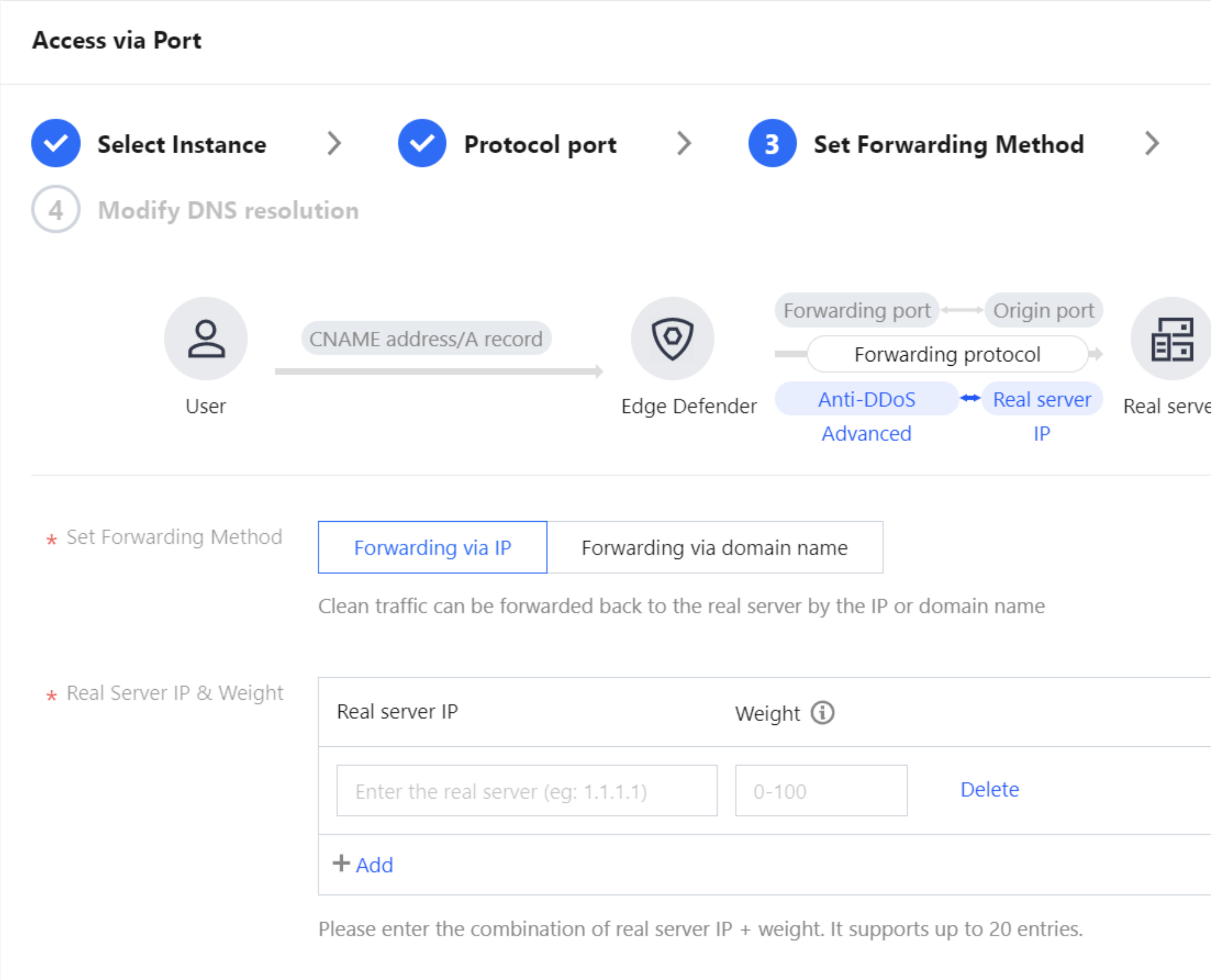
✓ Select Instance > 2 Protocol port > 3 Set Forwarding Method > 4 Modify DNS resolution

* Forwarding protocol: ● TCP ○ UDP

* 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**.



Access via Port

Select Instance > Protocol port > 3 Set Forwarding Method >

4 Modify DNS resolution

* Set Forwarding Method: Forwarding via IP | Forwarding via domain name

Clean traffic can be forwarded back to the real server by the IP or domain name

* Real Server IP & Weight

Real server IP	Weight	
Enter the real server (eg: 1.1.1.1)	0-100	Delete

+ Add

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

Note:

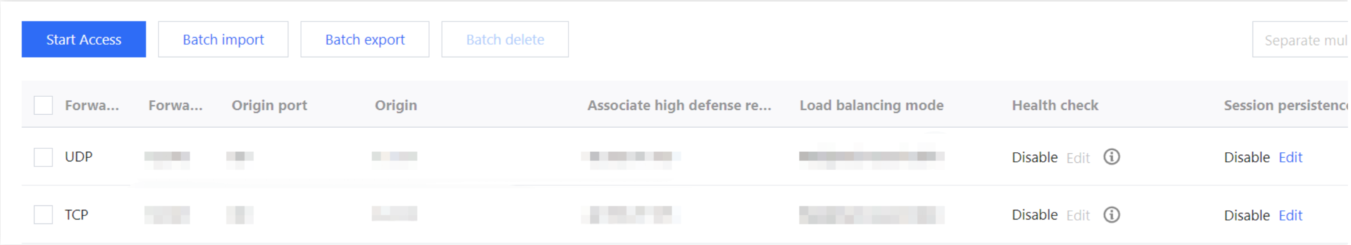
An alternate real server is used when the forwarding to the real server fails.

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

6. Click **Complete**.

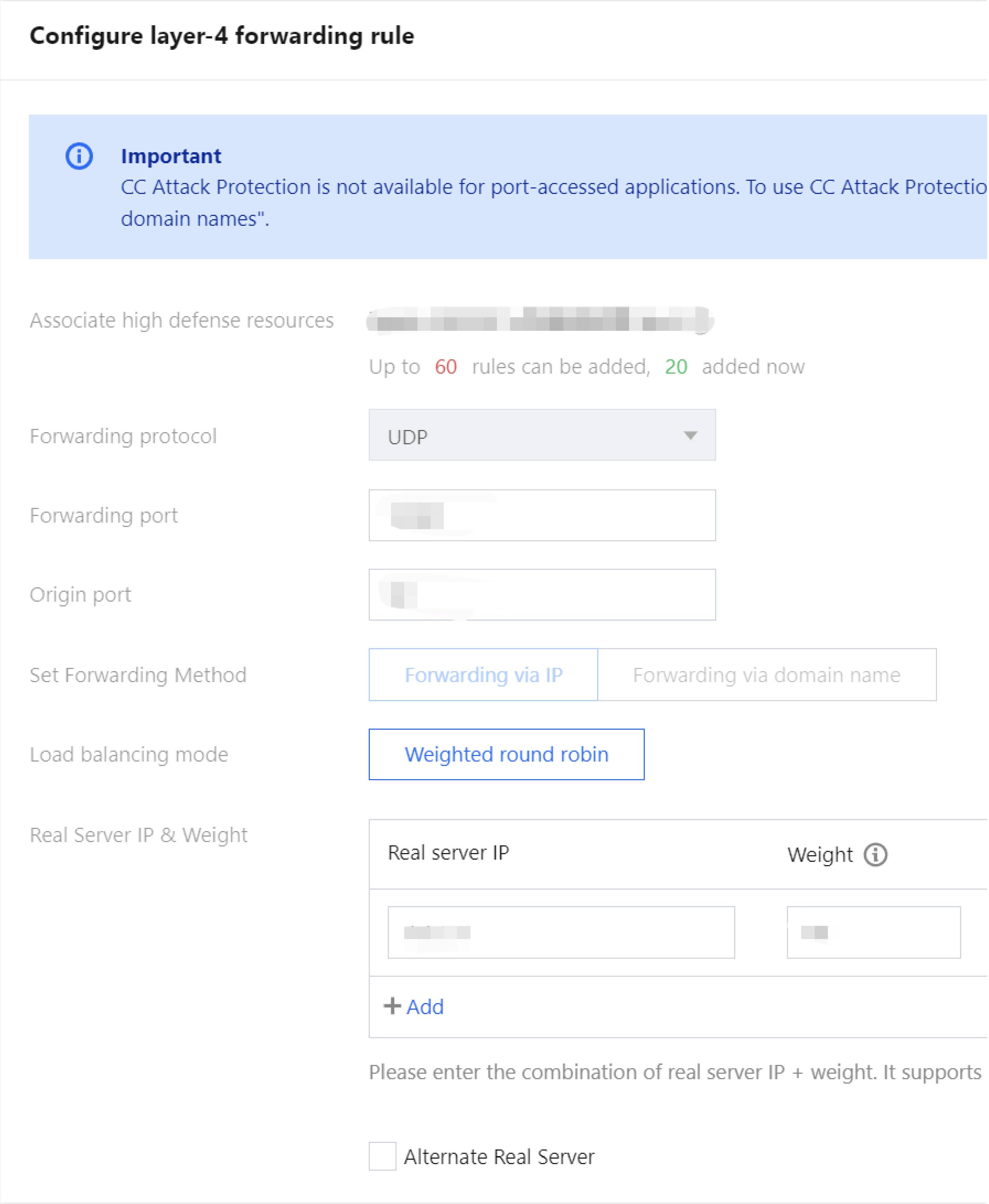
Editing a rule

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



□	Forwa...	Forwa...	Origin port	Origin	Associate high defense re...	Load balancing mode	Health check	Session persistenc
□	UDP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Disable Edit ⓘ	Disable Edit
□	TCP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Disable Edit ⓘ	Disable Edit

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



Configure layer-4 forwarding rule

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

Associate high defense resources

Up to 60 rules can be added, 20 added now

Forwarding protocol: UDP

Forwarding port

Origin port

Set Forwarding Method: Forwarding via IP | Forwarding via domain name

Load balancing mode: Weighted round robin

Real Server IP & Weight

Real server IP	Weight

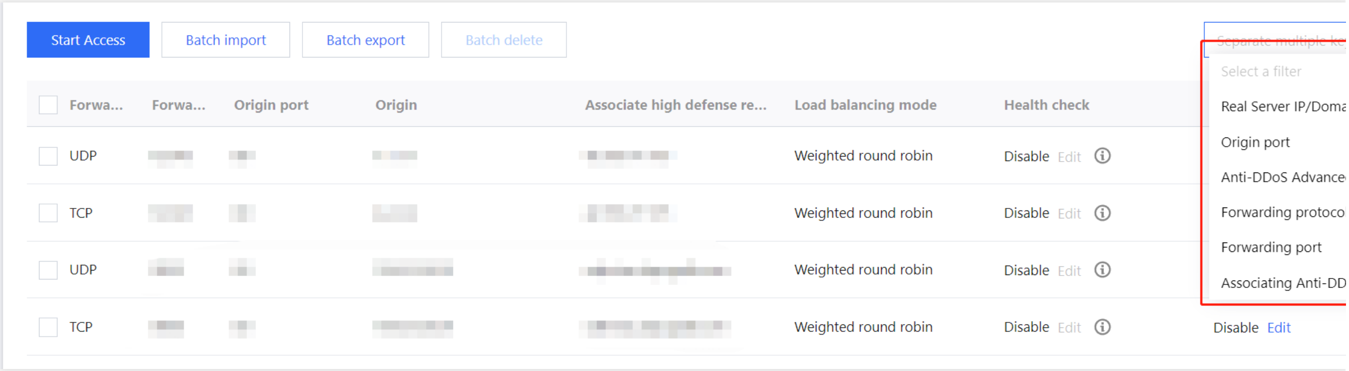
+ Add

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

□ Alternate Real Server

Querying a rule

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

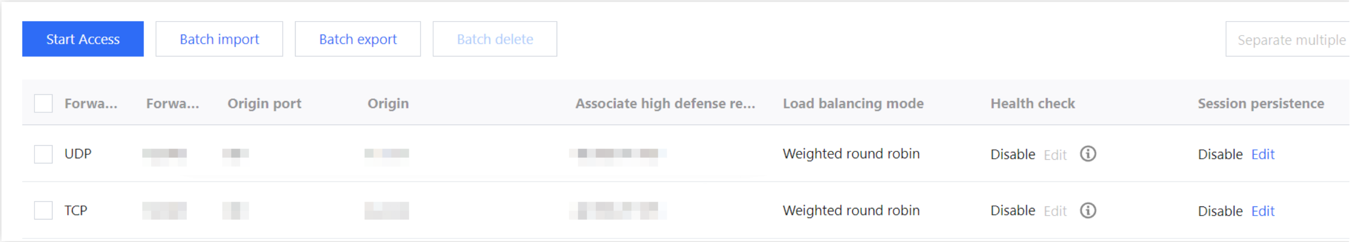


□	Forwa...	Forwa...	Origin port	Origin	Associate high defense re...	Load balancing mode	Health check	
□	UDP	[redacted]	[redacted]	[redacted]	[redacted]	Weighted round robin	Disable Edit ⓘ	
□	TCP	[redacted]	[redacted]	[redacted]	[redacted]	Weighted round robin	Disable Edit ⓘ	
□	UDP	[redacted]	[redacted]	[redacted]	[redacted]	Weighted round robin	Disable Edit ⓘ	
□	TCP	[redacted]	[redacted]	[redacted]	[redacted]	Weighted round robin	Disable Edit ⓘ	Disable Edit

Deleting a rule

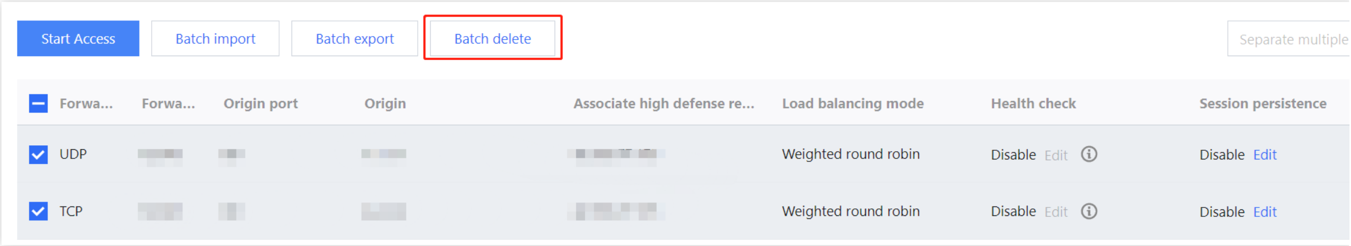
1. On the Access via port page, you can delete one or more rules.

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



□	Forwa...	Forwa...	Origin port	Origin	Associate high defense re...	Load balancing mode	Health check	Session persistence
□	UDP	[redacted]	[redacted]	[redacted]	[redacted]	Weighted round robin	Disable Edit ⓘ	Disable Edit
□	TCP	[redacted]	[redacted]	[redacted]	[redacted]	Weighted round robin	Disable Edit ⓘ	Disable Edit

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



☑	Forwa...	Forwa...	Origin port	Origin	Associate high defense re...	Load balancing mode	Health check	Session persistence
☑	UDP	[redacted]	[redacted]	[redacted]	[redacted]	Weighted round robin	Disable Edit ⓘ	Disable Edit
☑	TCP	[redacted]	[redacted]	[redacted]	[redacted]	Weighted round robin	Disable Edit ⓘ	Disable Edit

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

©2013-2022 Tencent Cloud. All rights reserved.

Protection Configuration

AI Protection

Last updated：2022-02-22 16:40:03

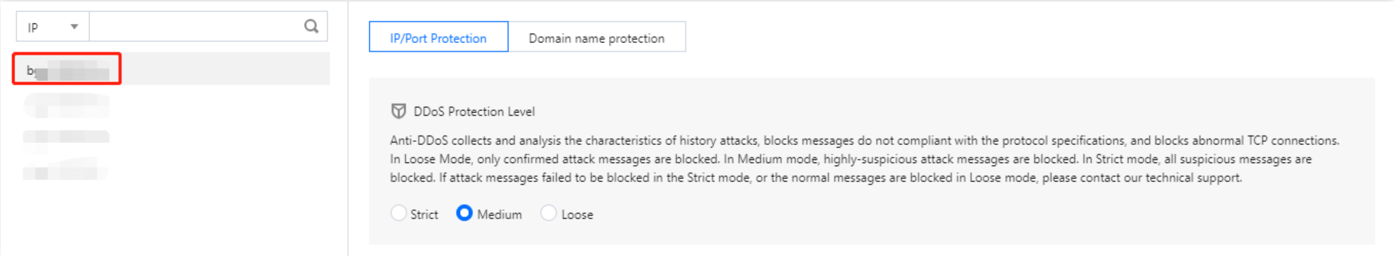
Anti-DDoS Pro supports AI protection. After AI protection is enabled, with its algorithms, Anti-DDoS Pro can self-learn the connection quantity baseline and traffic characteristics, adaptively adjust cleansing policies, discover and block layer-4 connection CC attacks to deliver an optimal protection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

Prerequisites

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

Operation Directions

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".

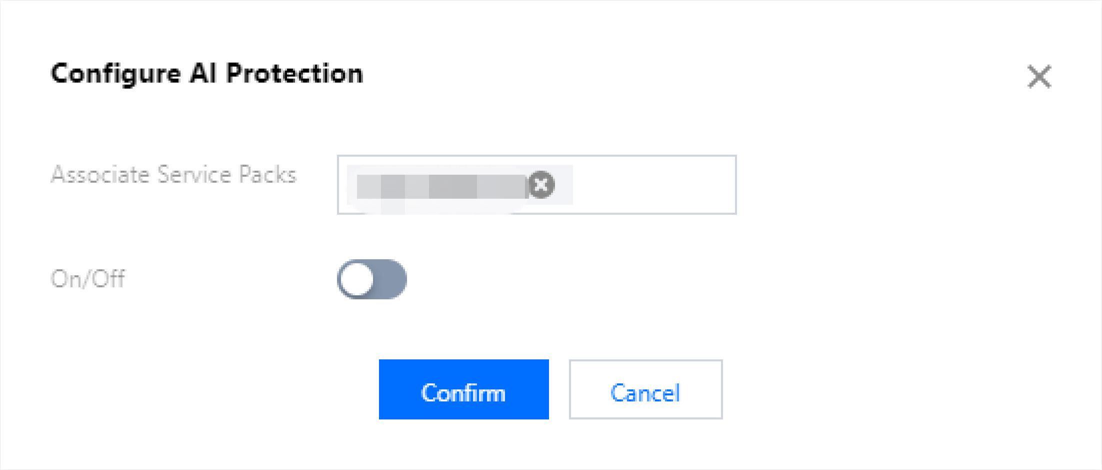


DDoS Protection Level

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 ● Medium ○ Loose

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



Configure AI Protection

Associate Service Packs: [redacted]

On/Off

Port Filtering

Last updated：2022-07-06 14:43:29

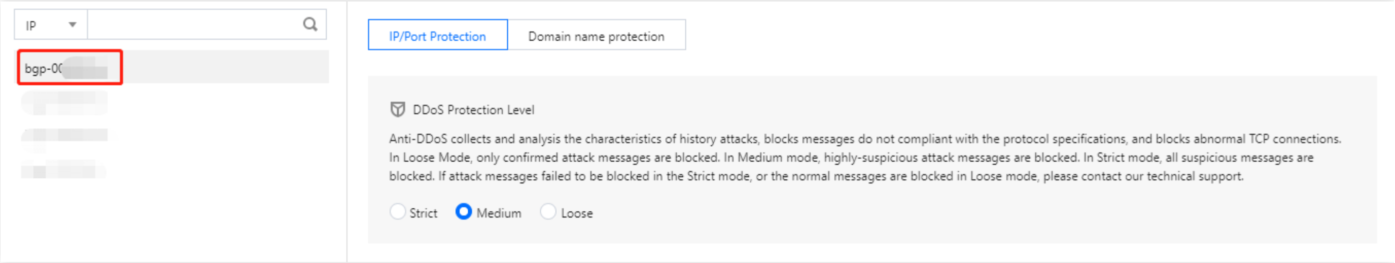
Port filtering is a fine-grained way to restrict inbound traffic based on port. When it is enabled, you can create a rule by setting the protocol type, source port range, destination port range and action (Discard/Allow/Continue protection).

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".

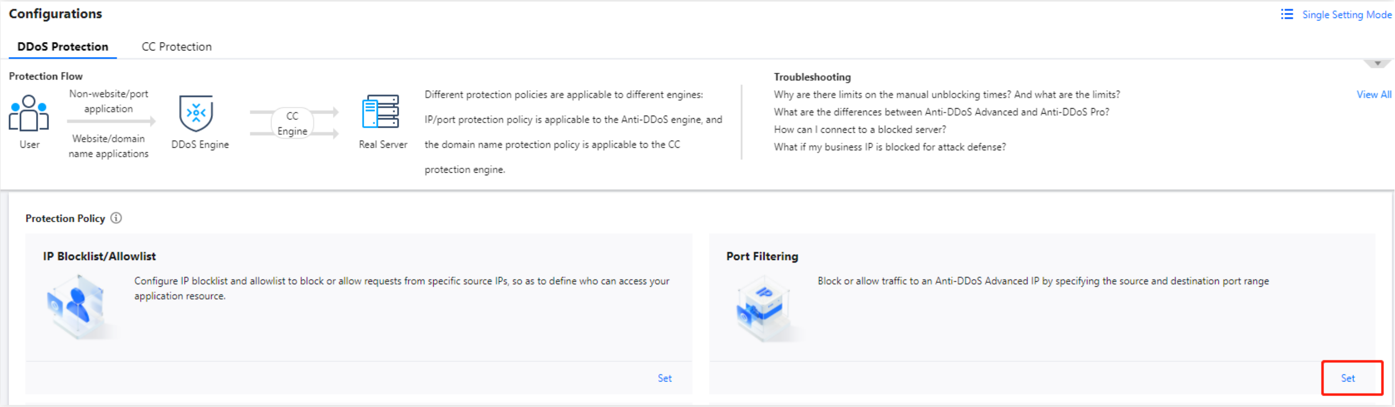


DDoS Protection Level

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 ● Medium ○ Loose

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



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

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

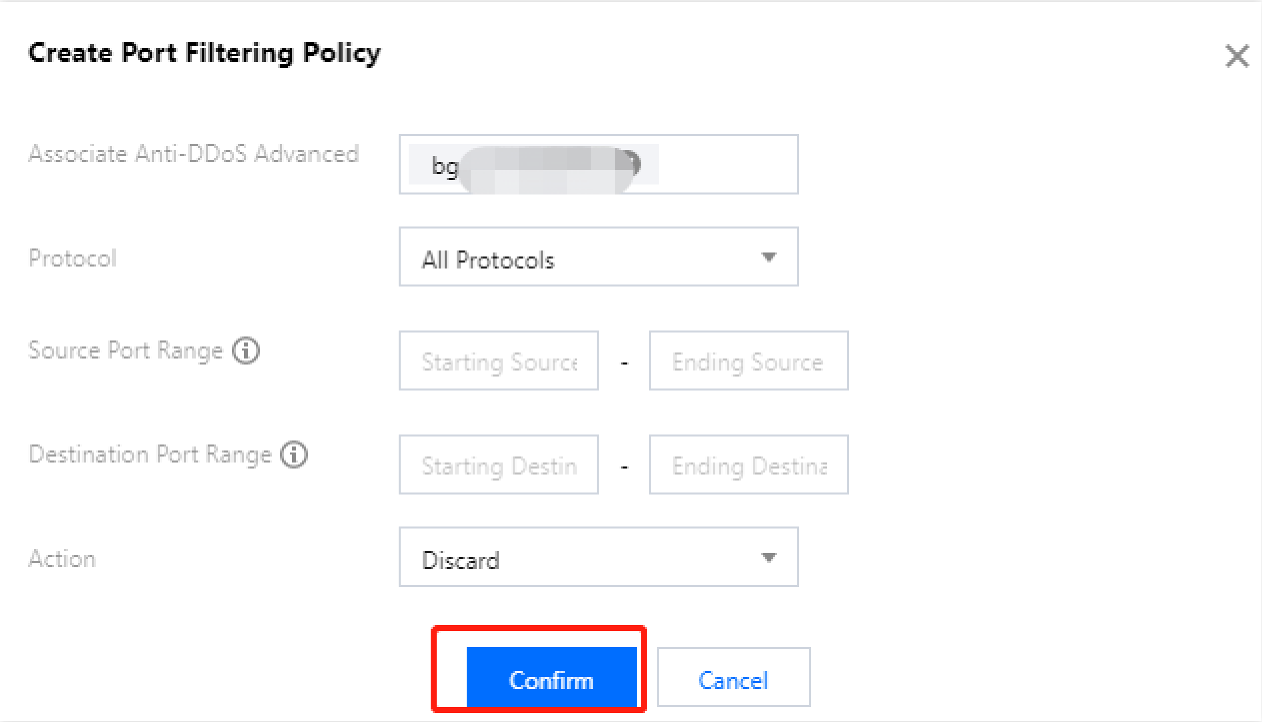
IP Blocklist/Allowlist: Configure IP blocklist and allowlist to block or allow requests from specific source IPs, so as to define who can access your application resource.

Port Filtering: Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range

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

©2013-2022 Tencent Cloud. All rights reserved.

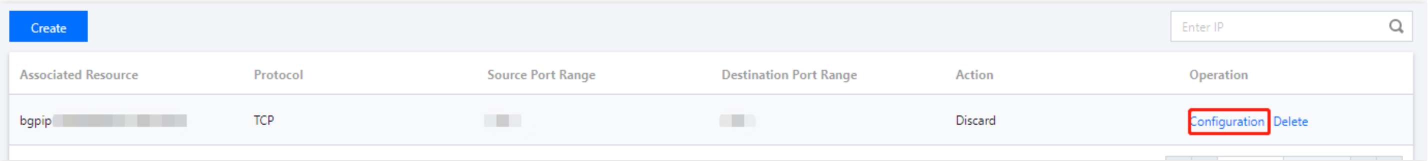
> Note：
> Multiple instances can be created at a time. For instances without protected resources, you cannot create rules.



Create Port Filtering Policy

Associate Anti-DDoS Advanced	bg[redacted]
Protocol	All Protocols
Source Port Range	Starting Source - Ending Source
Destination Port Range	Starting Destin - Ending Destina
Action	Discard

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.



Associated Resource	Protocol	Source Port Range	Destination Port Range	Action	Operation
bgpip[redacted]	TCP	[redacted]	[redacted]	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	• Filters SYN and ACK data packets with explicit attack attributes. • Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specifications. • Filters UDP data packets with explicit attack attributes.	• This cleansing policy is loose and only defends against explicit attack packets. • We recommend choosing this protection level when normal requests are blocked. Complex attack packets may pass through the security system.

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.

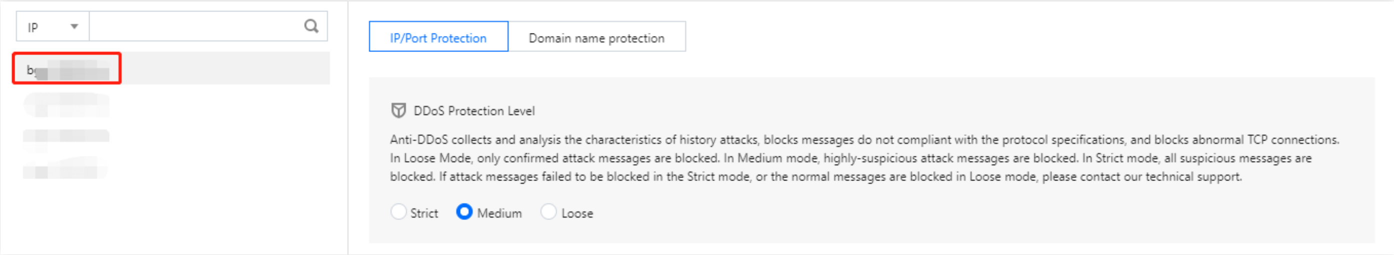
©2013-2022 Tencent Cloud. All rights reserved.

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".

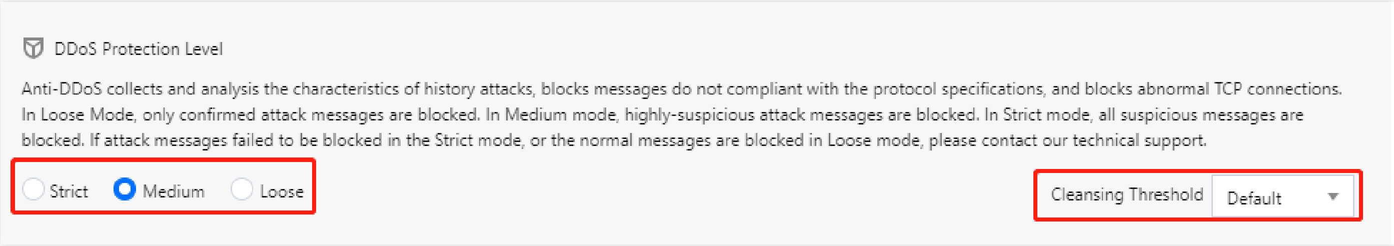


DDoS Protection Level

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 ● Medium ○ Loose

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, 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 ● 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.

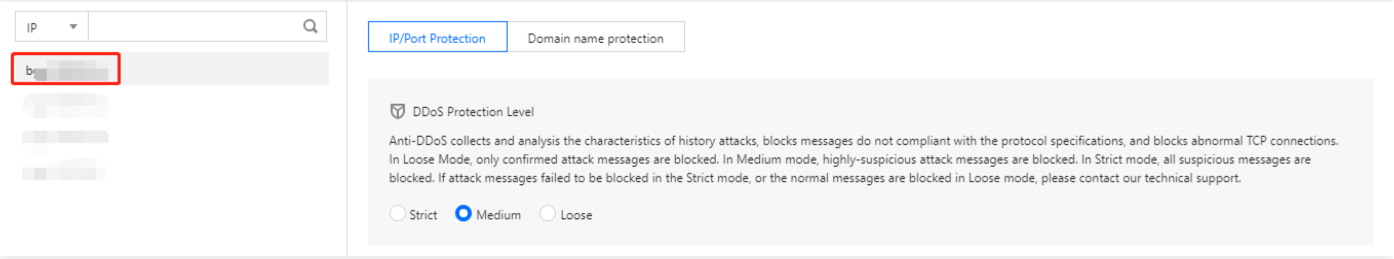
Prerequisites

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

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".

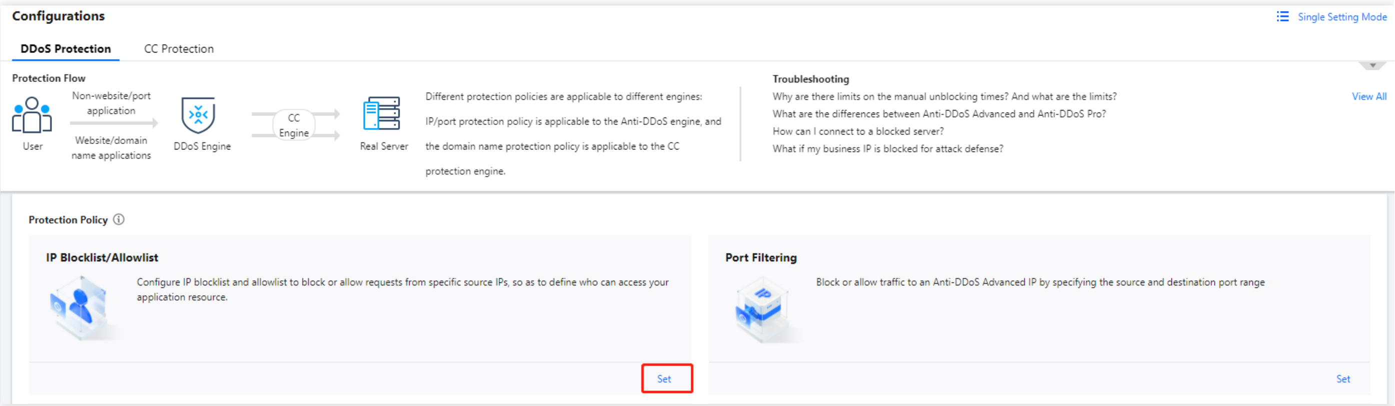


DDoS Protection Level

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 ● Medium ○ Loose

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



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.

Troubleshooting

Why are there limits on the manual unblocking times? And what are the limits?

What are the differences between Anti-DDoS Advanced and Anti-DDoS Pro?

How can I connect to a blocked server?

What if my business IP is blocked for attack defense?

Protection Policy ⓘ

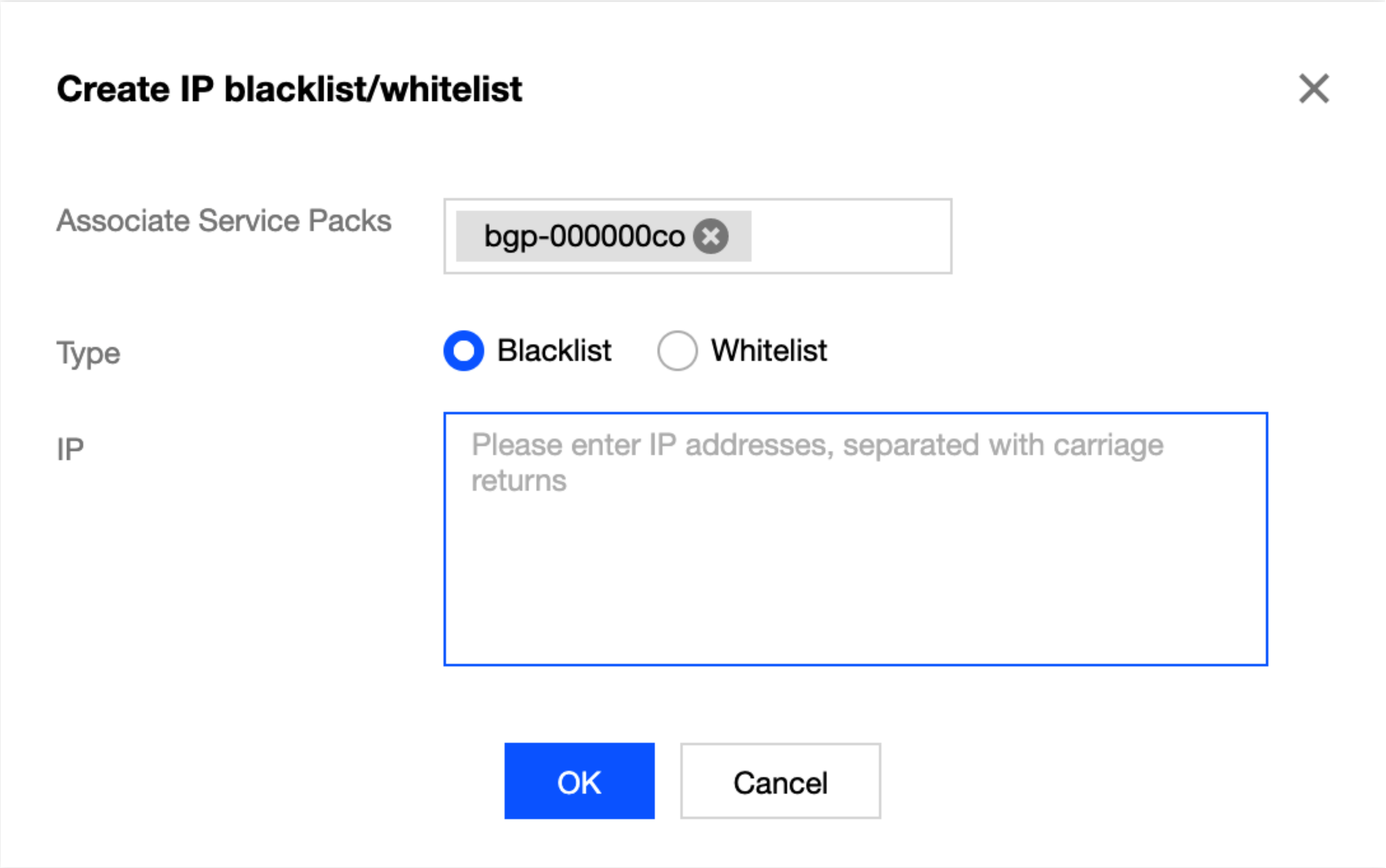
IP Blocklist/Allowlist

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

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



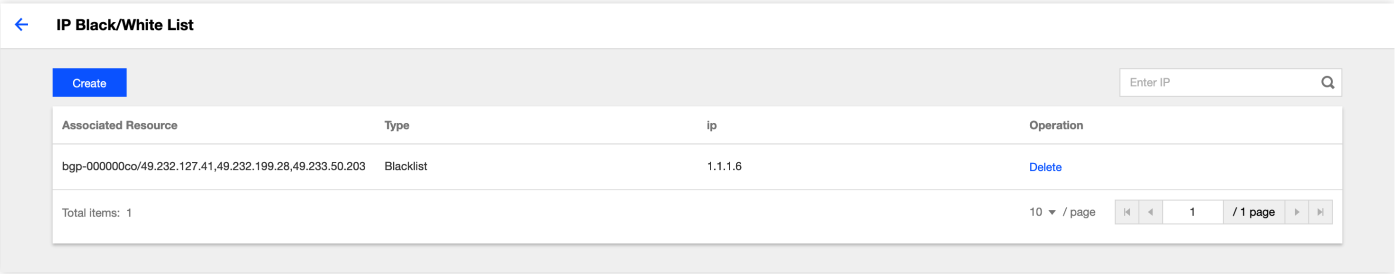
Create IP blacklist/whitelist

Associate Service Packs: bgp-000000co ⊗

Type: ● Blacklist ○ Whitelist

IP: Please enter IP addresses, separated with carriage returns

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.



Associated Resource	Type	ip	Operation
bgp-000000co/49.232.127.41,49.232.199.28,49.233.50.203	Blacklist	1.1.1.6	Delete

IP and Port Rate Limiting

Last updated：2022-02-22 16:40:03

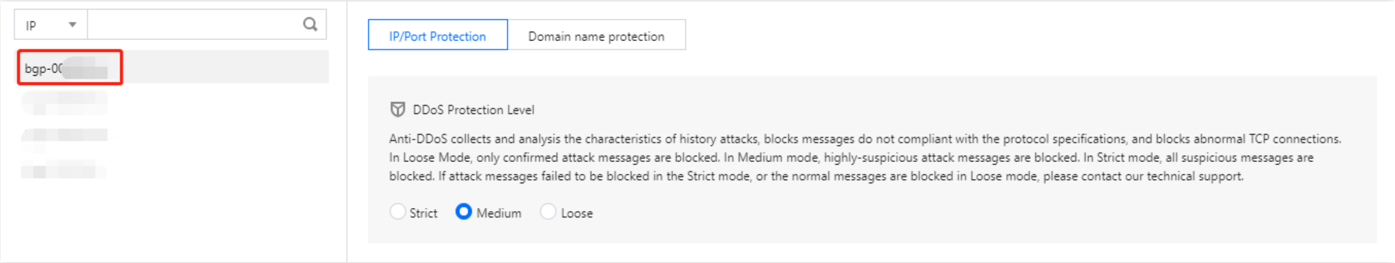
Anti-DDoS Pro allows you to limit traffic rate for business IPs and ports.

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".

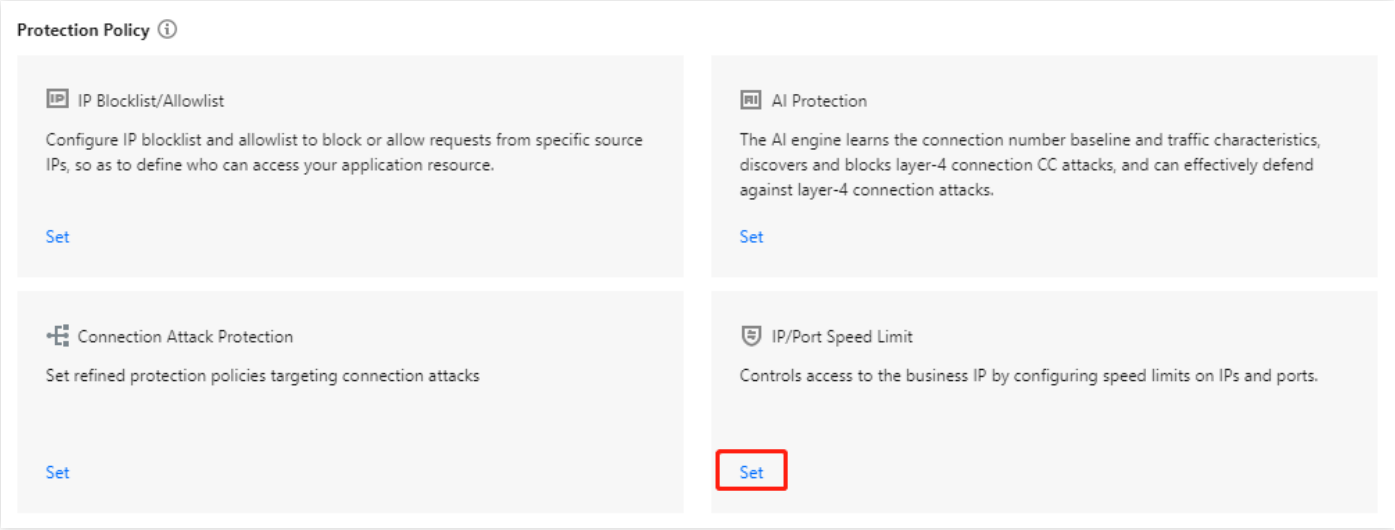


DDoS Protection Level

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 ● Medium ○ Loose

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



Protection Policy

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.

Set

AI Protection

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.

Set

Connection Attack Protection

Set refined protection policies targeting connection attacks

Set

IP/Port Speed Limit

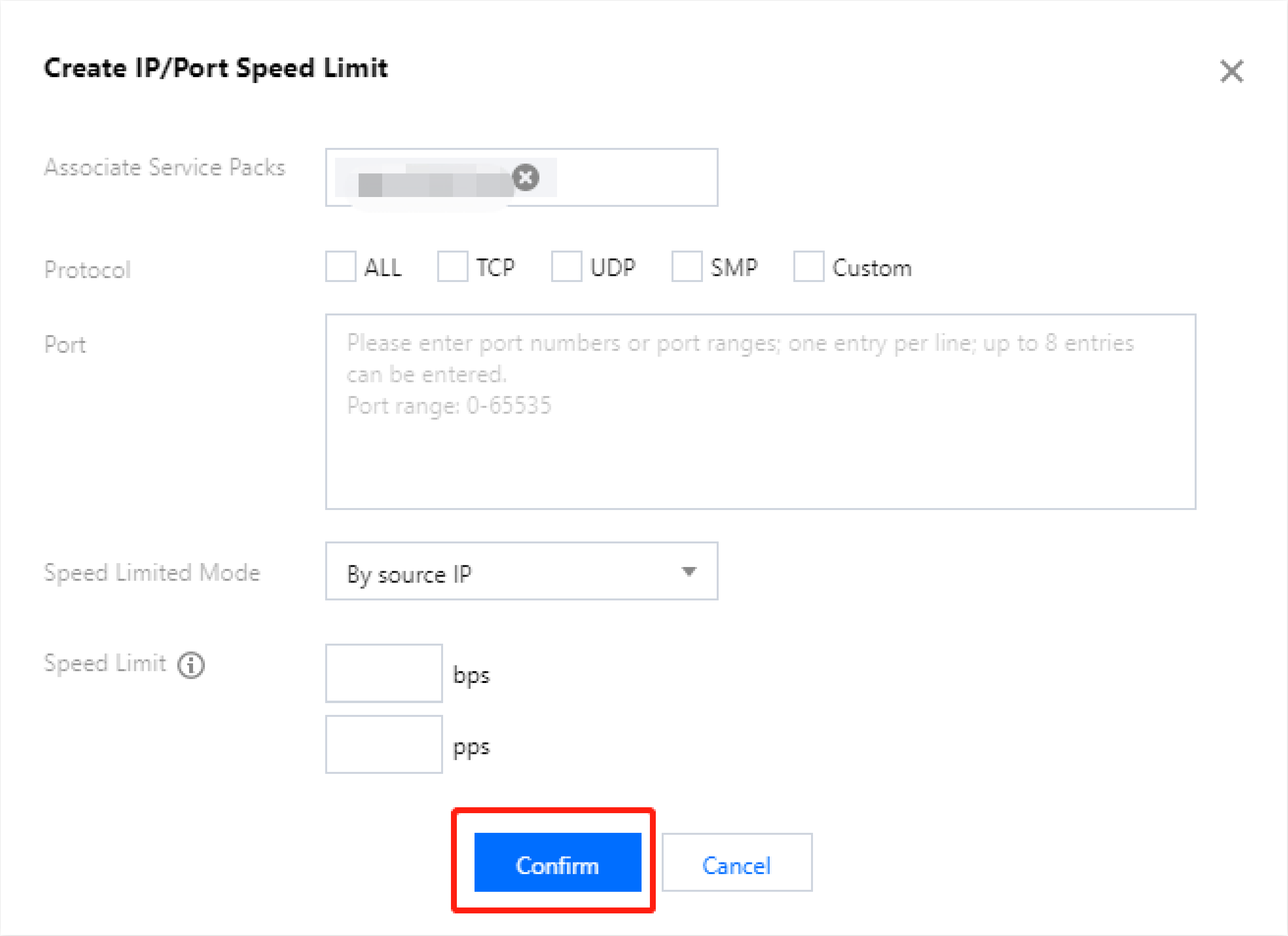
Controls access to the business IP by configuring speed limits on IPs and ports.

Set

©2013-2022 Tencent Cloud. All rights reserved.

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**.



Create IP/Port Speed Limit

Associate Service Packs [redacted]

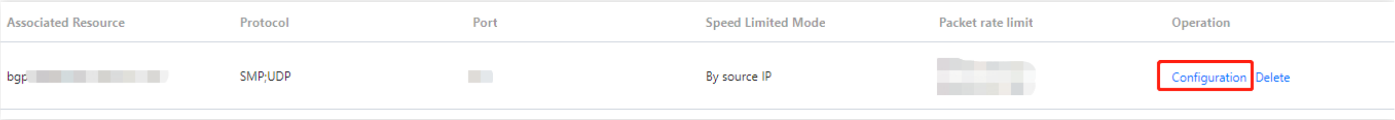
Protocol □ ALL □ TCP □ UDP □ SMP □ Custom

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

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
bgp[redacted]	SMP;UDP	[redacted]	By source IP	[redacted]	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.

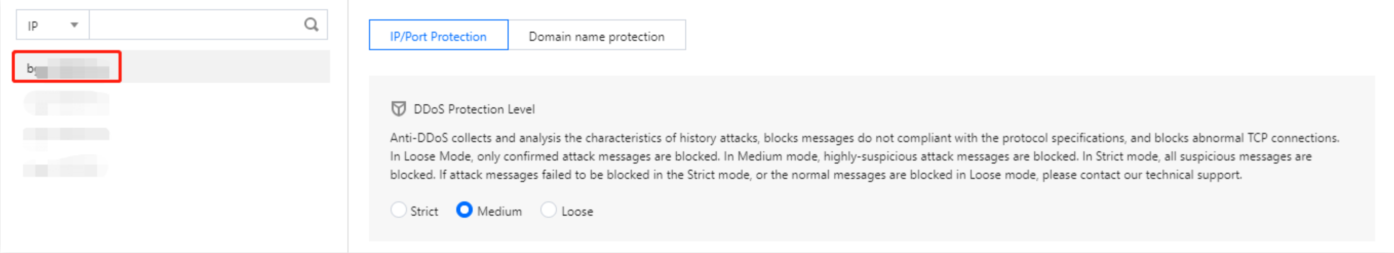
Prerequisites

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

Directions

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".



b[redacted]

[redacted]

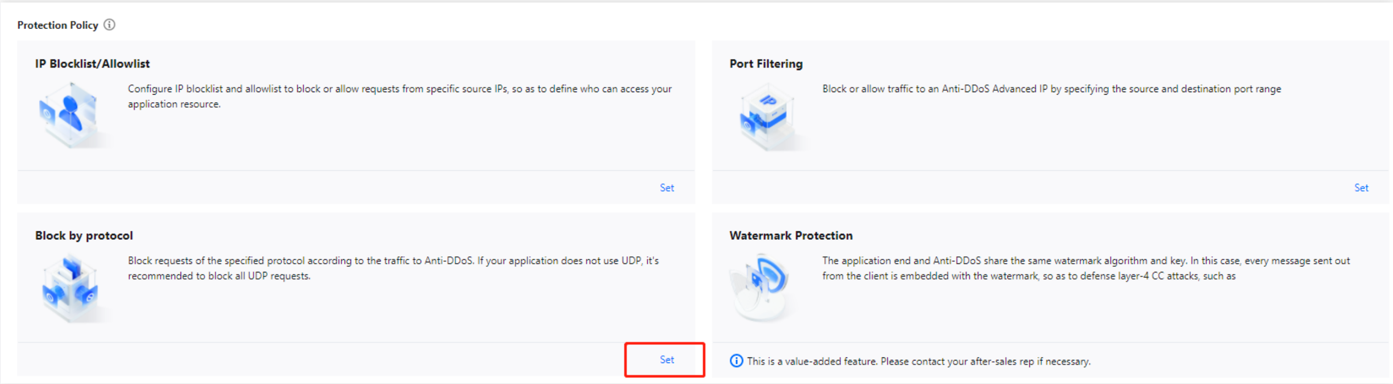
DDoS Protection Level

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 ● Medium ○ Loose

©2013-2022 Tencent Cloud. All rights reserved.

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



Protection Policy

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

Block by protocol

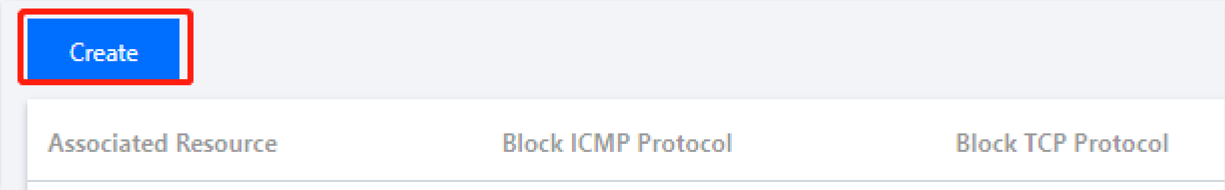
Block requests of the specified protocol according to the traffic to Anti-DDoS. If your application does not use UDP, it's recommended to block all UDP requests.

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

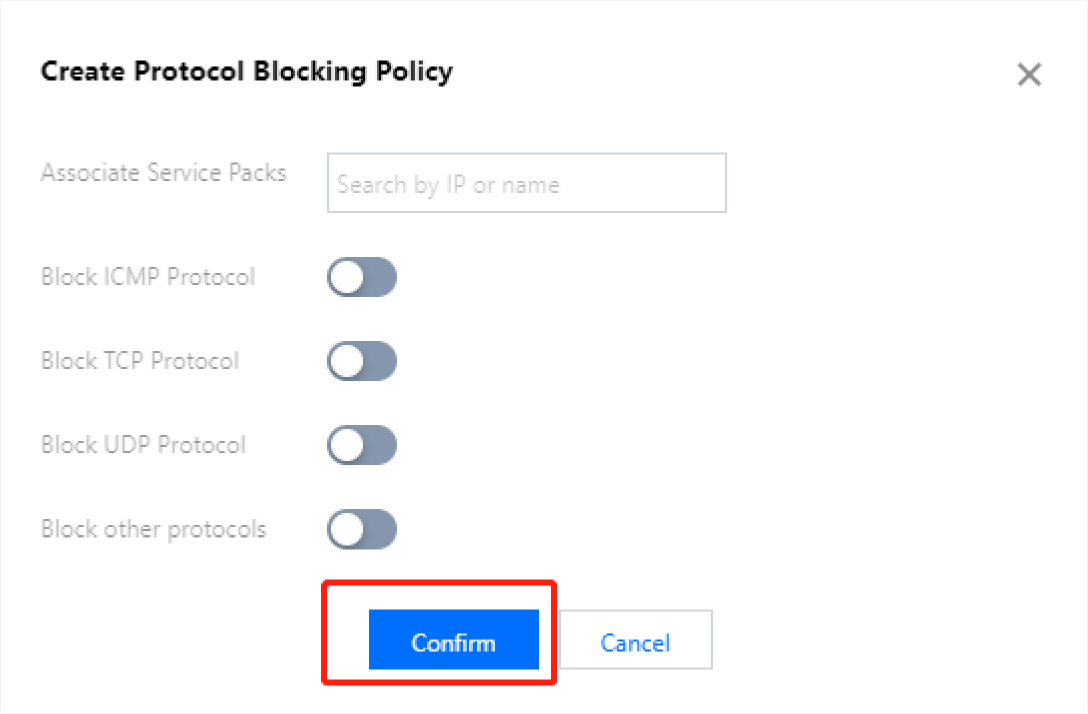
This is a value-added feature. Please contact your after-sales rep if necessary.

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



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 Blocking Policy

Associate Service Packs: Search by IP or name

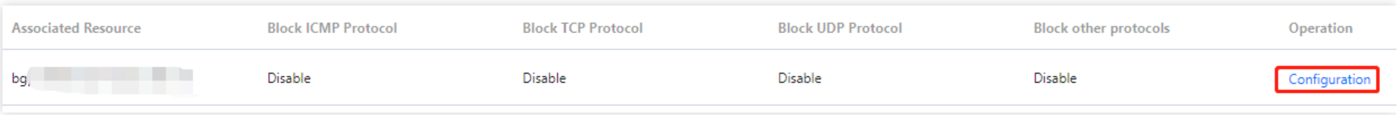
Block ICMP Protocol

Block TCP Protocol

Block UDP Protocol

Block other protocols

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[redacted]	Disable	Disable	Disable	Disable	Configuration

Feature Filtering

Last updated：2022-02-22 16:40:04

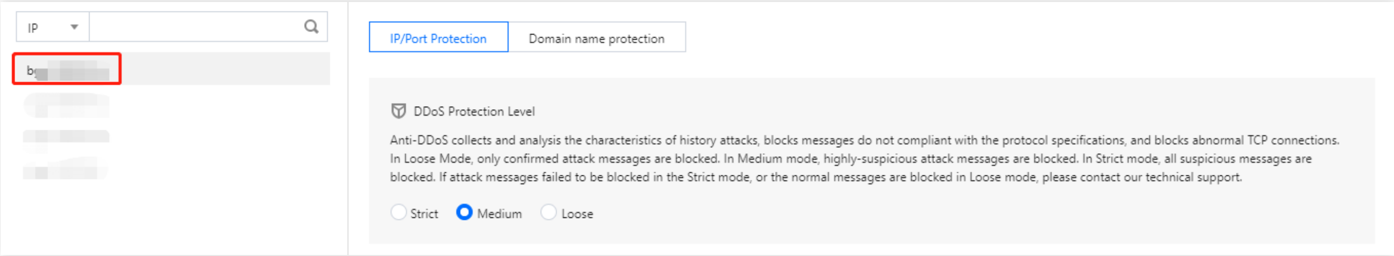
Anti-DDoS Pro supports configuring custom blocking policies against specific IP, TCP, UDP message header or load. After enabling feature filtering, you can combine the matching conditions of the source port, destination port, message length, IP message header or load, and set the protection action to 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

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".

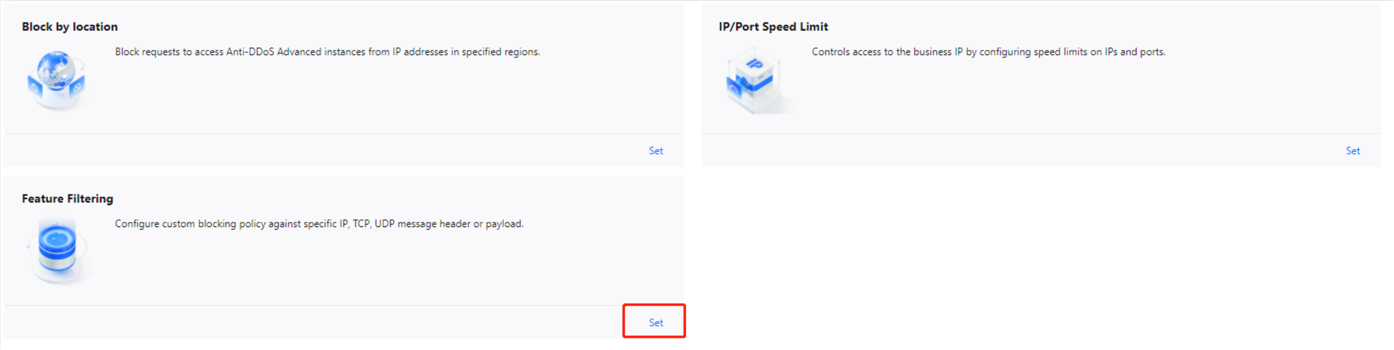


DDoS Protection Level

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 ● Medium ○ Loose

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



Block by location

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

Set

IP/Port Speed Limit

Controls access to the business IP by configuring speed limits on IPs and ports.

Set

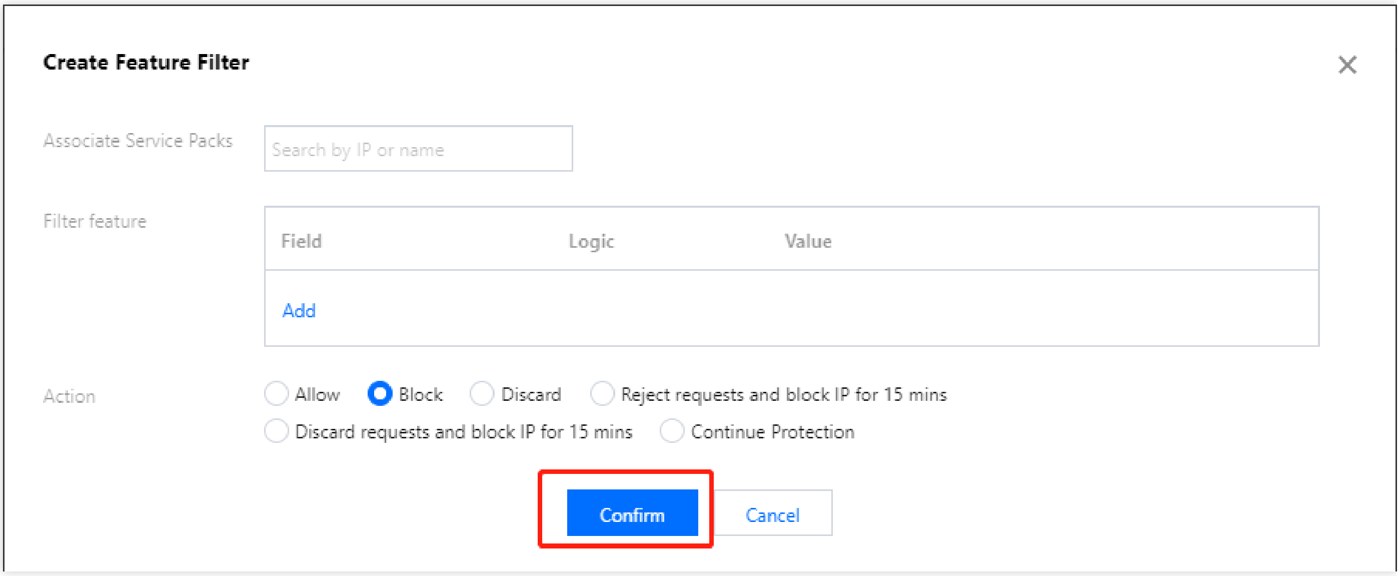
Feature Filtering

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**.



Create Feature Filter

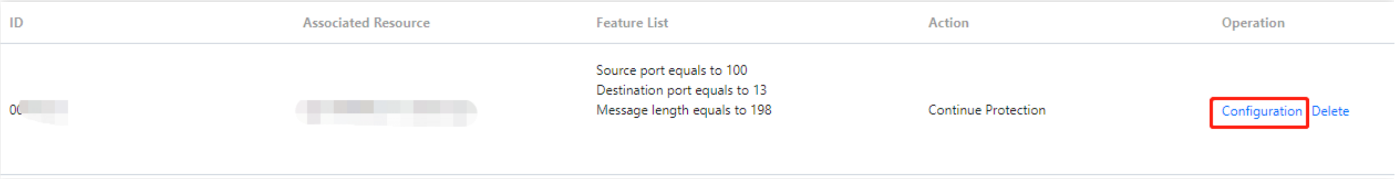
Associate Service Packs: Search by IP or name

Filter feature:

Field	Logic	Value
Add		

Action: ○ Allow ● Block ○ Discard ○ Reject requests and block IP for 15 mins ○ Discard requests and block IP for 15 mins ○ Continue Protection

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



ID	Associated Resource	Feature List	Action	Operation
0[redacted]	[redacted]	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.

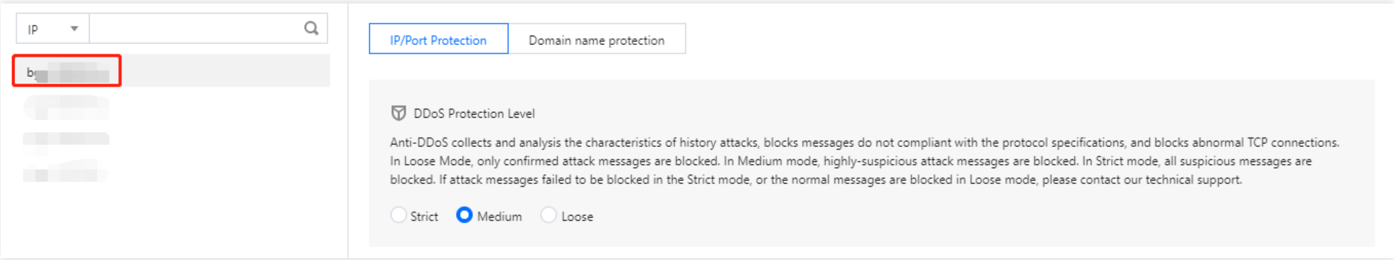
Prerequisites

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".



IP

b[redacted]

[redacted]

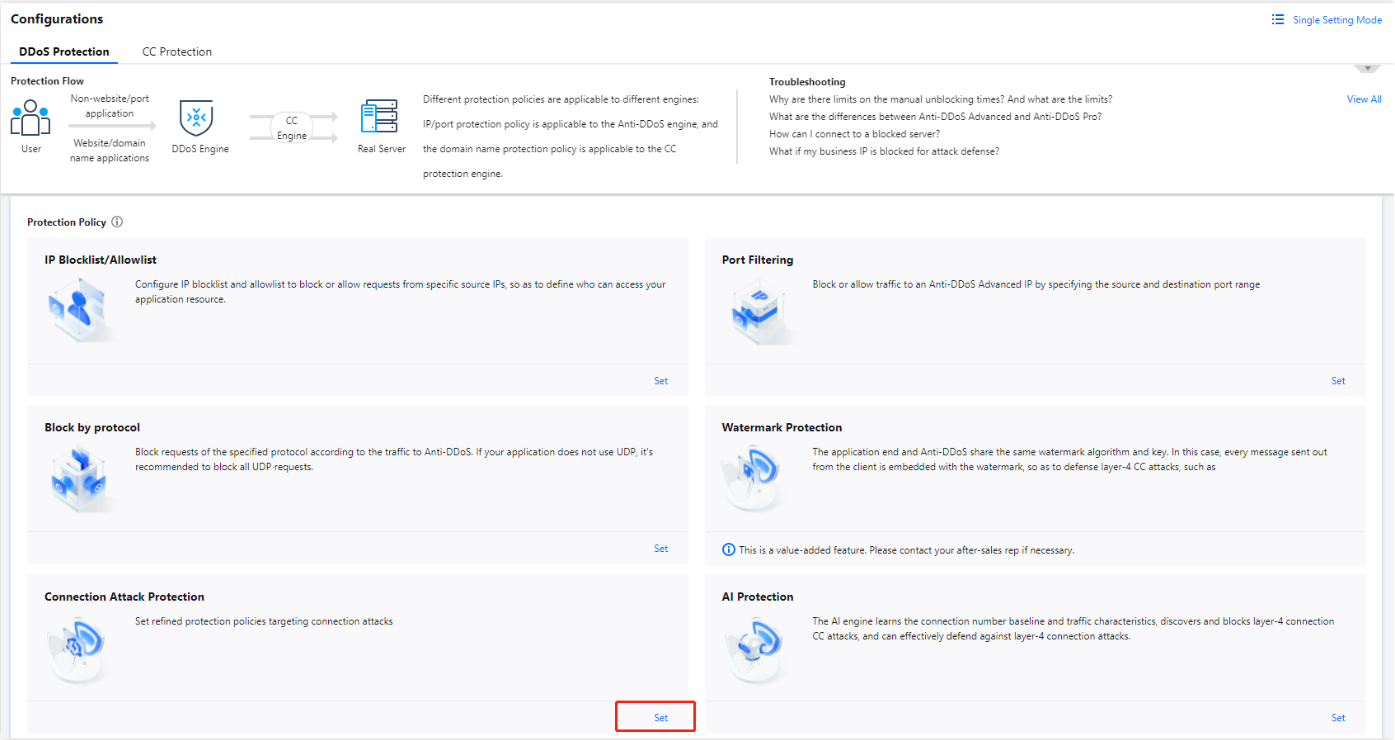
IP/Port Protection | Domain name protection

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 ● Medium ○ Loose

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



Configurations

Single Setting Mode

DDoS Protection | CC Protection

Protection Flow

User
Non-website/port application
Website/domain name applications
DDoS Engine
CC Engine
Real Server

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.

Troubleshooting

View All

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

Protection Policy ⓘ

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.

Set

Port Filtering

Block or allow traffic to an Anti-DDoS Advanced IP by specifying the source and destination port range

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.

Set

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

ⓘ This is a value-added feature. Please contact your after-sales rep if necessary.

Connection Attack Protection

Set refined protection policies targeting connection attacks

Set

AI Protection

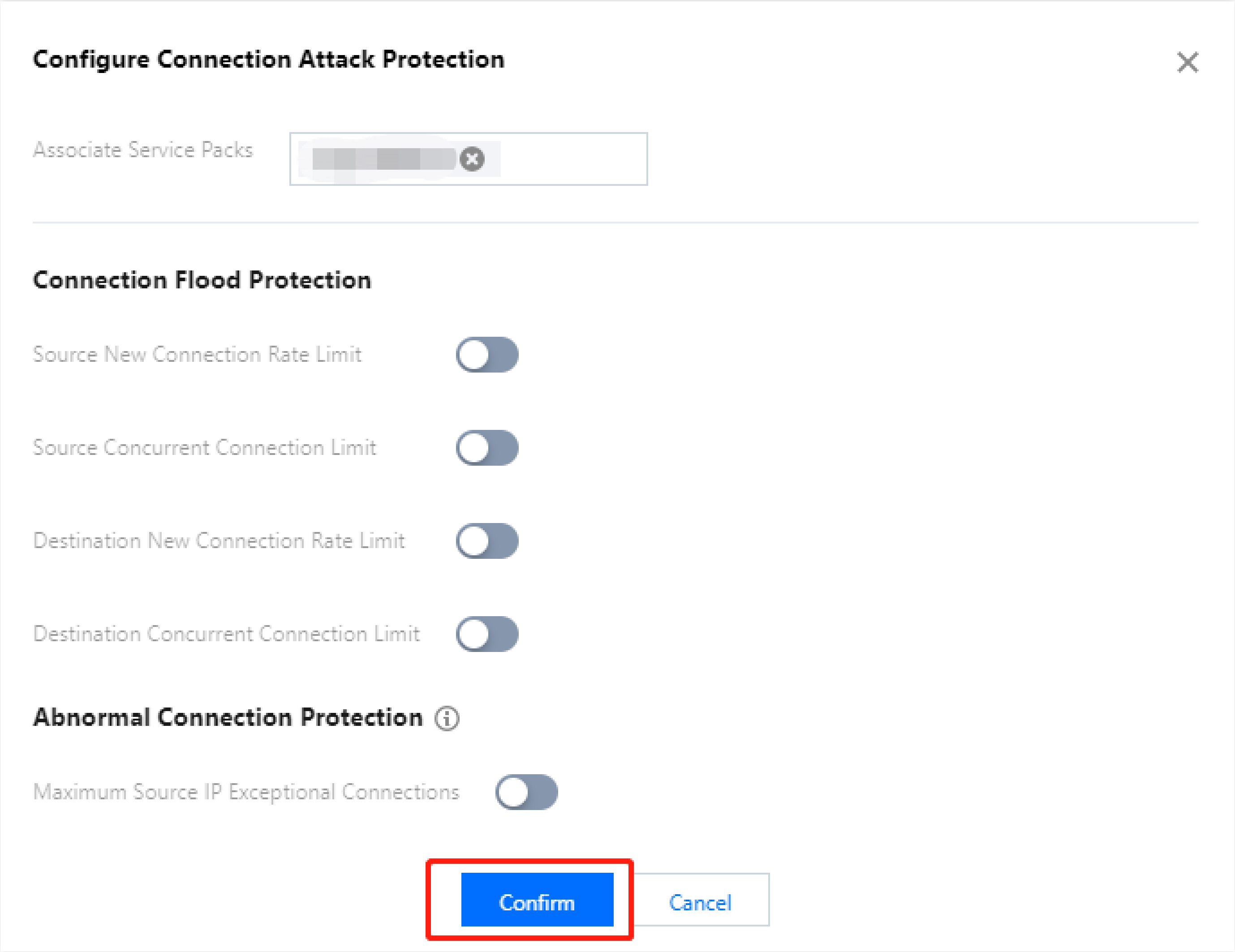
The AI engine learns the connection number baseline and traffic characteristics, discovers and blocks layer-4 connection CC attacks, and can effectively defend against layer-4 connection attacks.

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**.

©2013-2022 Tencent Cloud. All rights reserved.



Configure Connection Attack Protection

Associate Service Packs [redacted]

Connection Flood Protection

Source New Connection Rate Limit

Source Concurrent Connection Limit

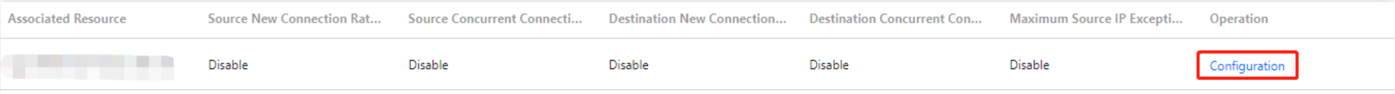
Destination New Connection Rate Limit

Destination Concurrent Connection Limit

Abnormal Connection Protection

Maximum Source IP Exceptional Connections

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
[redacted]	Disable	Disable	Disable	Disable	Disable	Configuration

©2013-2022 Tencent Cloud. All rights reserved.

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.

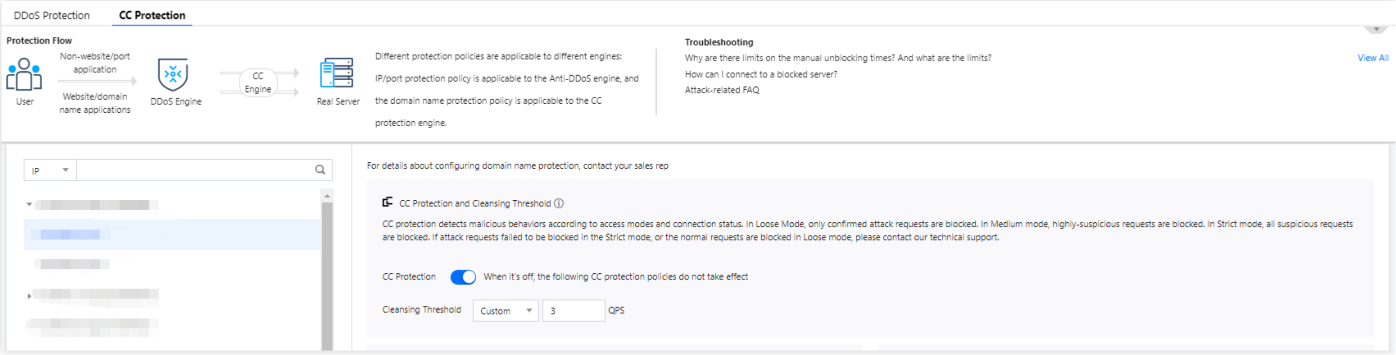
> Note：
> After you configure the regional blocking setting, attack traffic targeting the region will still be recorded but will not be allowed to your real server.

Prerequisites

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

Directions

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".



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

Why are there limits on the manual unblocking times? And what are the limits?

How can I connect to a blocked server?

Attack-related FAQ

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

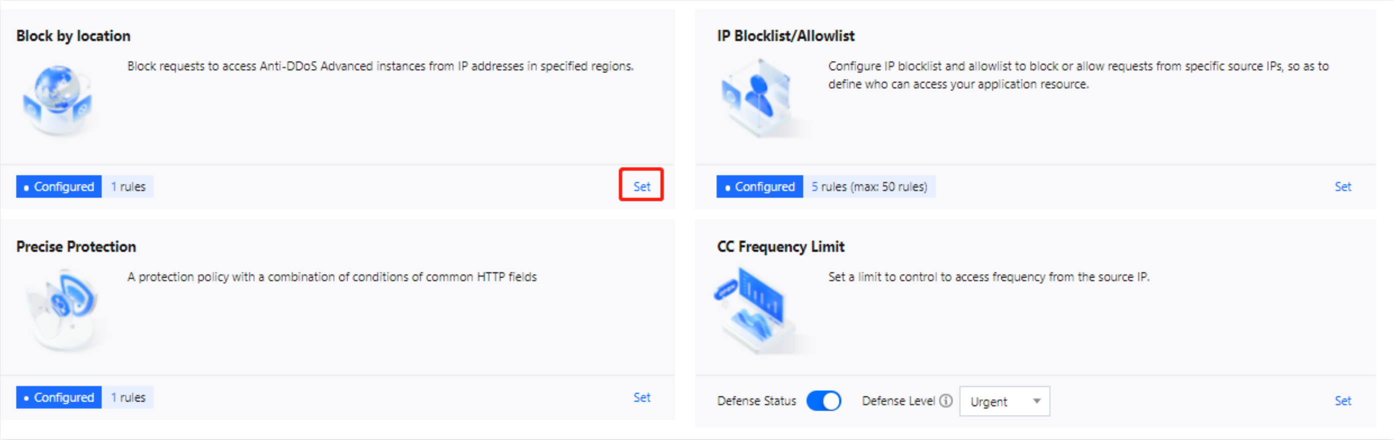
CC Protection and Cleansing Threshold

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 Custom 3 QPS

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.

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 5 rules (max: 50 rules) Set

Precise Protection

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

Configured 1 rules Set

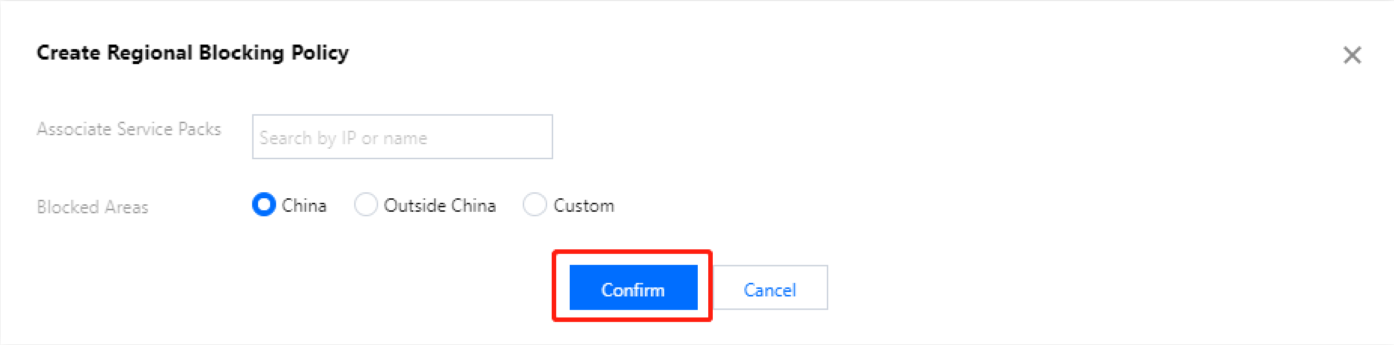
CC Frequency Limit

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

Defense Status Defense Level Urgent Set

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

5. In the pop-up window, select a region to block and click **OK**.



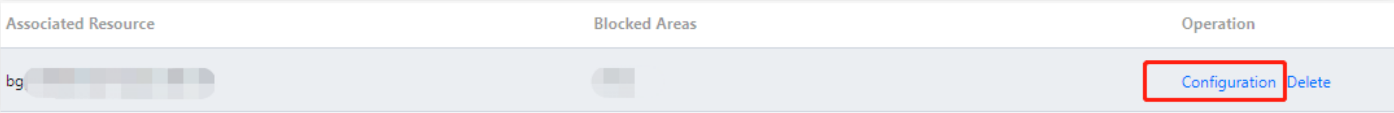
Create Regional Blocking Policy

Associate Service Packs: Search by IP or name

Blocked Areas: ● China ○ Outside China ○ Custom

Confirm Cancel

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	Blocked Areas	Operation
bg[redacted]	[redacted]	Configuration Delete

Viewing Operation Log

Last updated：2023-04-20 16:37:37

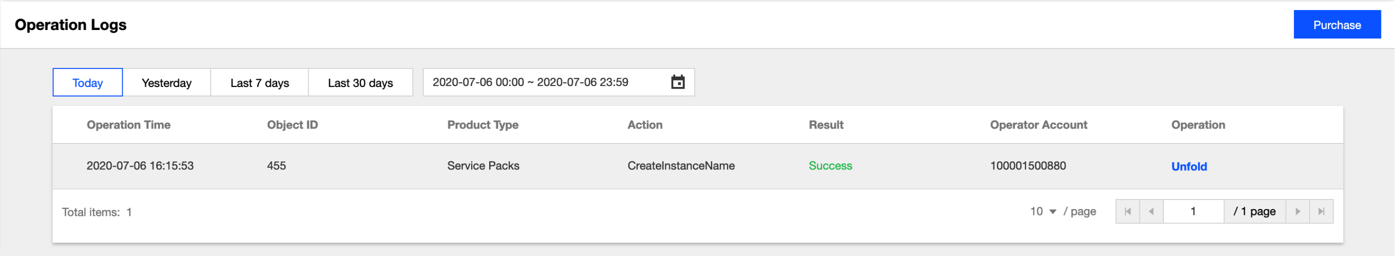
Use Cases

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.



Operation Logs

2020-07-06 00:00 ~ 2020-07-06 23:59

Operation Time	Object ID	Product Type	Action	Result	Operator Account	Operation
2020-07-06 16:15:53	455	Service Packs	CreateInstanceName	Success	100001500880	Unfold

Total items: 1

10 / page 1 / 1 page

Blocking Operations

Configuring Security Event Notification

Last updated：2022-05-09 17:03:00

Use Cases

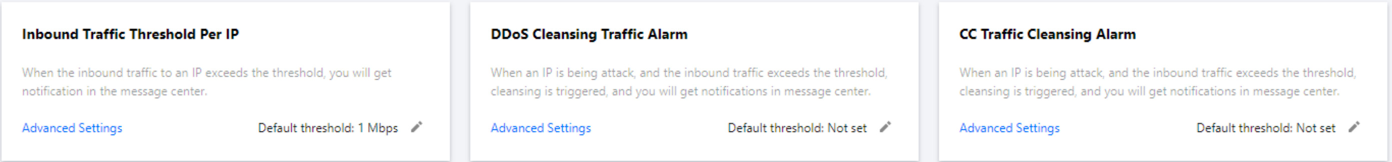
Tencent Cloud will send you alarm messages for your IPs protected by Anti-DDoS Pro via the channels (including Message Center, SMS, and email) you configured in **Message Center -> Message Subscription** when:

- 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**.



Inbound Traffic Threshold Per IP

When the inbound traffic to an IP exceeds the threshold, you will get notification in the message center.

Advanced Settings   Default threshold: 1 Mbps

DDoS Cleansing Traffic Alarm

When an IP is being attack, and the inbound traffic exceeds the threshold, cleansing is triggered, and you will get notifications in message center.

Advanced Settings   Default threshold: Not set

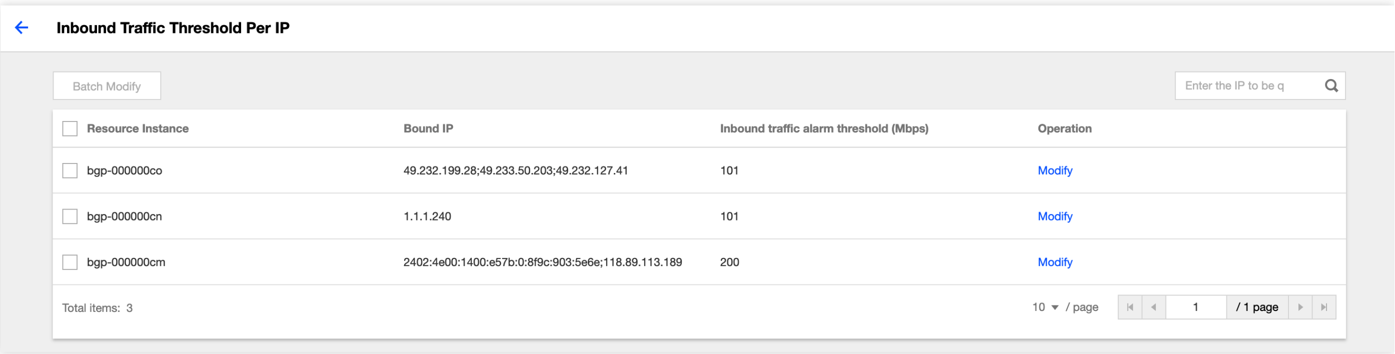
CC Traffic Cleansing Alarm

When an IP is being attack, and the inbound traffic exceeds the threshold, cleansing is triggered, and you will get notifications in message center.

Advanced Settings   Default threshold: Not set

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

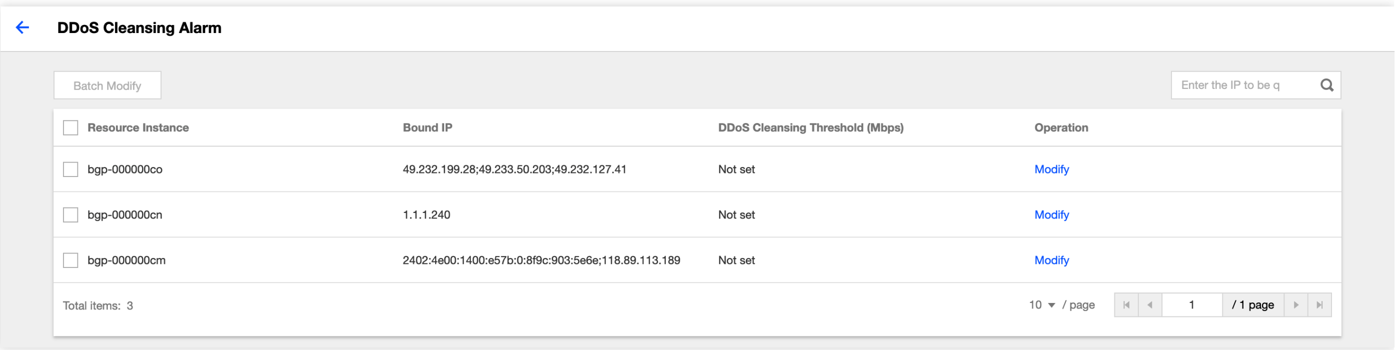
Enter the IP to be q

□ 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

- Setting the DDoS cleansing threshold



DDoS Cleansing Alarm

Batch Modify

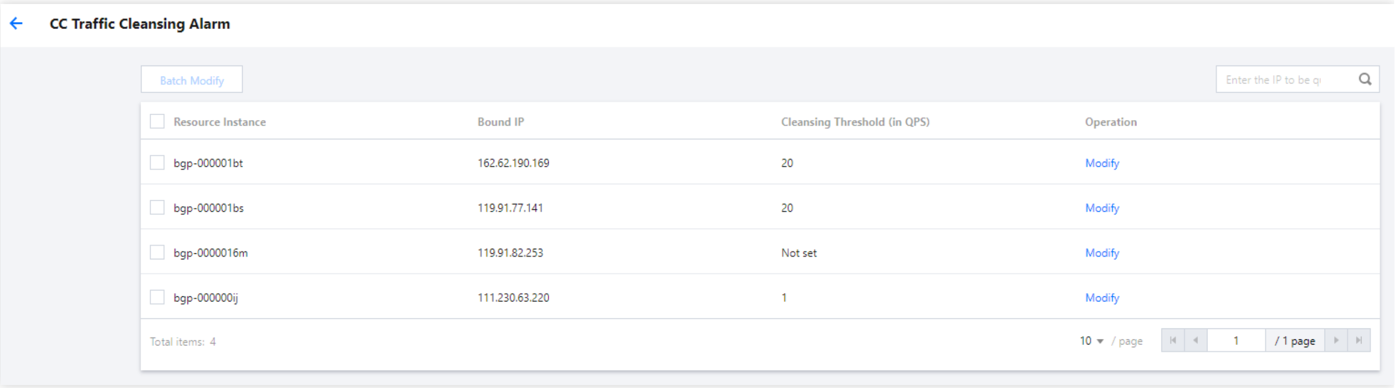
Enter the IP to be q

□ 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

- Setting the CC traffic cleansing alarm



CC Traffic Cleansing Alarm

Batch Modify

Enter the IP to be 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 1 / 1 page

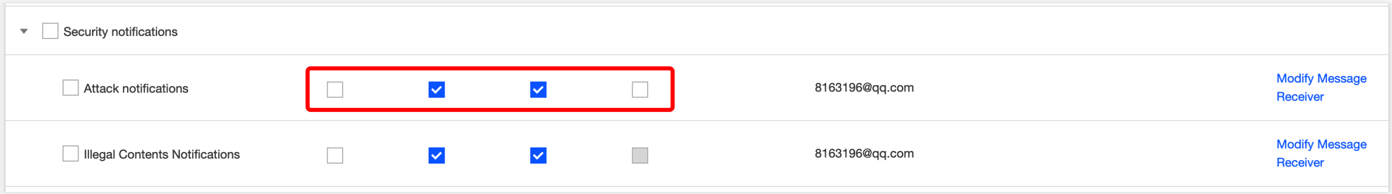
How to Set Message Channel

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

> Note：

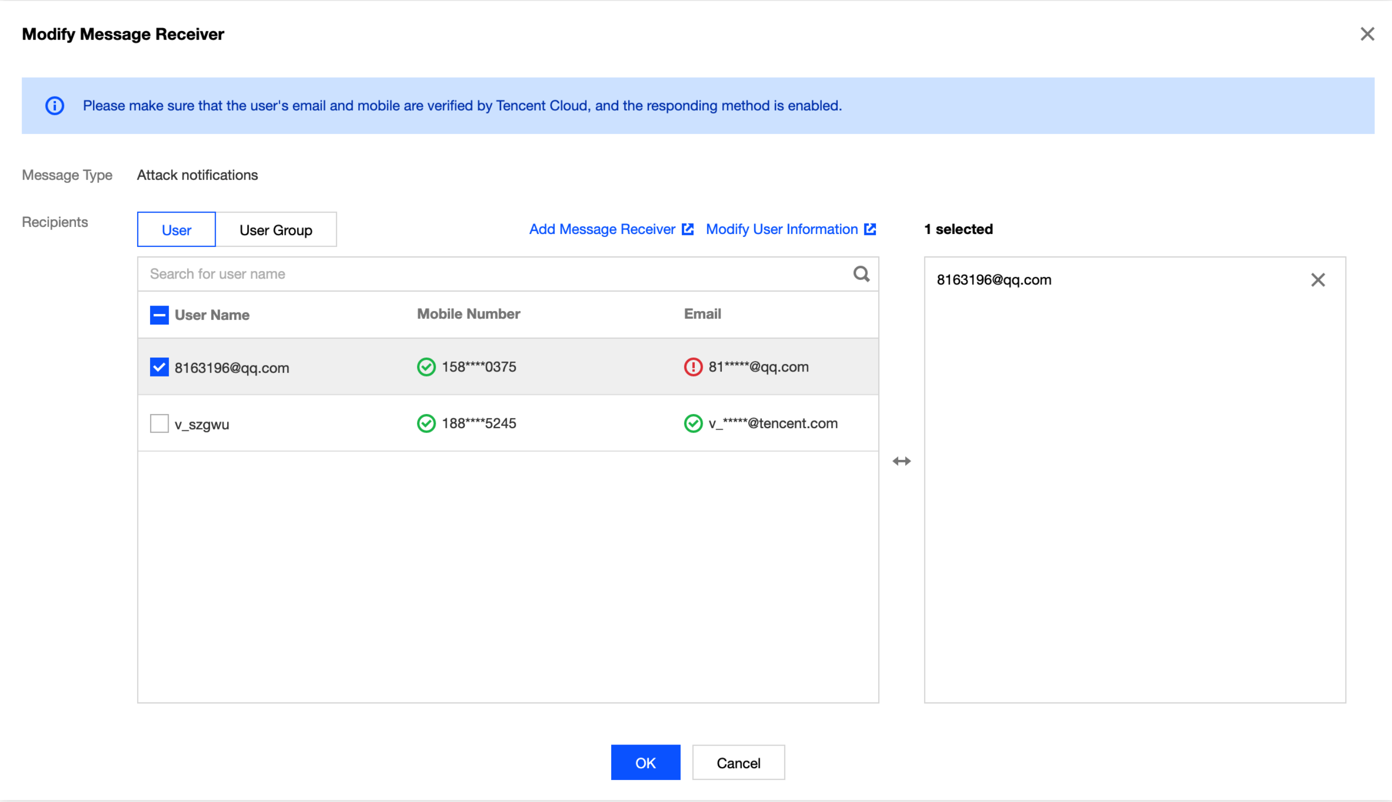
> You can also log in to the console, click ✉ on the top bar, and click **More** to enter the Message Center.

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



▾ □ Security notifications						
□ Attack notifications	□	☑	☑	□	8163196@qq.com	Modify Message Receiver
□ Illegal Contents Notifications	□	☑	☑	▨	8163196@qq.com	Modify Message Receiver

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: User | User Group — Add Message Receiver, Modify User Information

Search for user name

User Name	Mobile Number	Email
☑ 8163196@qq.com	✓ 158****0375	! 81*****@qq.com
□ v_szgwu	✓ 188****5245	✓ v_*****@tencent.com

1 selected

8163196@qq.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.

©2013-2022 Tencent Cloud. All rights reserved.

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.

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

Unblocking Operation Record

©2013-2022 Tencent Cloud. All rights reserved.

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.

©2013-2022 Tencent Cloud. All rights reserved.