

# **Anti-DDoS Pro**

## **Getting Started**

### **Product Documentation**



## Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

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

## Trademark Notice



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

## Service Statement

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

# Getting Started

Last updated : 2022-12-21 17:29:48

Anti-DDoS Pro provides Tencent Cloud public IPs with higher anti-DDoS capability. It supports Tencent Cloud services such as CVM, CLB, NAT, and WAF. It is easy to access and requires no IP changes.

## Prerequisites

You have purchased an [Anti-DDoS Pro](#) before you can bind it to the IP addresses you want to protect.

## Directions

1. Log in to the [Anti-DDoS Pro \(New\) Console](#) and click **Service Packs** on the left sidebar.
2. Select a region of the target Anti-DDoS Pro instance and click **Protected Resource** on the right of the instance.

The screenshot shows the 'Service Packs' page in the Anti-DDoS Pro console. At the top right is a 'Purchase' button. Below it is a search bar with a dropdown for 'Guangzhou' and a search input. The main table has the following data:

| ID/Name                                     | Protected IP | Specifications                                                     | Status                                                                                                  | Attacks in last 7 days | Date                                                 | Auto Ex... | Operation                                                                                                                                                        |
|---------------------------------------------|--------------|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|------------------------|------------------------------------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">bpg-000000cn</a><br>test<br>N/A | 1.1.1.240    | Region: Guangzhou<br>Package type: Standard pack<br>IPs allowed: 5 | Status: <span style="color: green;">Running</span><br>Remaining protection times: 9<br>Protected IPs: 1 | 0 Times                | Purchase time: 2020-04-26<br>Expiry time: 2020-07-26 |            | <a href="#">Protected Resource</a><br><a href="#">Configurations</a><br><a href="#">View Report</a><br><a href="#">Upgrade</a><br><a href="#">Extend Service</a> |

At the bottom, it shows 'Total items: 1' and pagination controls for 10 items per page, currently on page 1 of 1.

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

### Note :

Anti-DDoS Pro supports Tencent Cloud managed IPs, which is currently available for beta users. If you want to use this feature, please call 4009100100 ext. 1 (Monday–Sunday, 9:00–18:00), or [submit a ticket] ([https://console.cloud.tencent.com/workorder/category?level1\\_id=141&level2\\_id=630&source=0&data\\_title=DDOS%E9%98%B2%E6%8A%A4\(%E5%A4%A7%E7%A6%B9\)&level3\\_id=861&radio\\_title=%E5%8A%9F%E8%83%BD%E5%92%A8%E8%AF%A2&queue=15&scene\\_code=20597&step=2](https://console.cloud.tencent.com/workorder/category?level1_id=141&level2_id=630&source=0&data_title=DDOS%E9%98%B2%E6%8A%A4(%E5%A4%A7%E7%A6%B9)&level3_id=861&radio_title=%E5%8A%9F%E8%83%BD%E5%92%A8%E8%AF%A2&queue=15&scene_code=20597&step=2)).

- Resource type: supports public cloud resources with public IPs such as CVM, CLB, and WAF.

- Select resource: supports one or more resources. The maximum resources selected cannot exceed the number of bound IPs.

**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 Unnamed

Region

Max Bound

IPs

Resource Type Cloud Virtual Machine ▼

**Select resource**

| <input type="checkbox"/>                     | Resource ID/Name                | IP Address    | Resource Type         |
|----------------------------------------------|---------------------------------|---------------|-----------------------|
| <input type="checkbox"/>                     | ins-n9f01kte<br>hrt-ceshi       | 123.207.62.30 | Cloud Virtual Machine |
| <input type="checkbox"/>                     | ins-rgcrtofc<br>ulricwang-test2 | 129.204.214.5 | Cloud Virtual Machine |
| <input type="checkbox"/>                     | ins-r397nyvi<br>ulricwang-test1 | 134.175.10.59 | Cloud Virtual Machine |
| <input type="checkbox"/>                     | ins-qysaot36                    | 162.14.18.58  | Cloud Virtual Machine |
| Total items: 9    100 ▼ / page    1 / 1 page |                                 |               |                       |

Press Shift key to select more

**Selected (1)**

| Resource ID/Name | IP Address | Resource Type |
|------------------|------------|---------------|
| 1.1.1.240        | 1.1.1.240  |               |

OK

Cancel

**4. Click OK.**

Note :

After you have accessed the service, you can customize your protection settings on the [Configurations](#) page.  
For more details, see [Protection Configuration](#).