

# **Anti-DDoS Pro**

# **Anti-DDoS Basic**

# **Product Documentation**



## Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

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

## Trademark Notice



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

## Service Statement

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

# Contents

## Anti-DDoS Basic

### Product Introduction

- Overview

- Strengths

- Use Cases

- Relevant Concepts

### Purchase Guide

### Operation Guide

- Operations Overview

- Use Limits

- Viewing Protection Configuration

- Viewing Statistical Reports

- Setting Security Event Notification

### Troubleshooting

- A public IP suffered DDoS attacks

# Anti-DDoS Basic

## Product Introduction

### Overview

Last updated : 2021-08-23 16:31:52

## Overview

With Tencent Cloud Anti-DDoS Basic, you can enjoy free 2 Gbps basic DDoS protection capability for resources such as Cloud Virtual Machine (CVM) and Cloud Load Balancer (CLB) to meet your daily security protection needs. Tencent Cloud will dynamically adjust the blocking threshold based on your security reputation score that is subject to historical attacks and cloud resource details. If your score is too low, you may not use the free protection capability until your security reputation is restored. Anti-DDoS Basic is enabled by default to monitor network traffic in real time and cleanse attack traffic as soon as it is detected, with protection for Tencent Cloud public IPs started within seconds.

Note :

If you need higher DDoS protection capability for your daily operations, select a desired [Anti-DDoS Pro service](#).

## Key Features

### Multidimensional protection

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

### Report management

---

This supports collecting attack events and attack traffic, allowing users to view attack reports within a custom period.

# Strengths

Last updated : 2021-08-23 16:31:52

Anti-DDoS Basic provides basic DDoS protection capability for Tencent Cloud users to meet their daily security protection needs. Anti-DDoS Basic has the following advantages.

## Auto start without manual configuration

Anti-DDoS Basic is automatically started to offer basic DDoS protection capability for Tencent Cloud users by default, without requiring costly cleaning equipment.

## High-quality protection resource

Anti-DDoS Basic guarantees the business availability and security with [BGP](#) network and high-quality bandwidth. Tencent Cloud's BGP network links 30 ISPs, which can effectively reduce cross-network latency and improve access speed.

## Real-time detection and precise protection

Anti-DDoS Basic checks traffic in real time based on proprietary protection clusters and algorithms to discover attack traffic immediately and start protection within seconds. It accurately identifies and cleanses attack traffic using extraordinary feature recognition algorithms so as to effectively defend your business against common DDoS attacks such as SYN flood and ICMP flood.

# Use Cases

Last updated : 2021-08-23 16:31:52

Anti-DDoS Basic provides Tencent Cloud users with free basic protection capability that can meet daily security protection needs. It mainly protects the businesses of Tencent Cloud users that are unlikely to be attacked and where attack traffic does not exceed the free basic protection capability.

If you need higher protection capability for your business needs, select a desired [Anti-DDoS Pro service](#) to defend attacks.

# Relevant Concepts

Last updated : 2021-08-23 16:31:52

## DDoS Attack

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

### Network layer DDoS attack

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

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

### CC attack

A CC attack is a malicious attempt to make a targeted server unavailable by occupying its application layer resources and exhausting its processing capacity.

Common attacks include HTTP/HTTPS-based GET/POST Flood, layer-4 CC, and connection flood attacks, etc.

## Cleansing

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

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

## Blocking

### Blocking threshold

The default blocking threshold of Anti-DDoS Basic:



Region	General User	VIP User
Chinese mainland	2 Gbps	10 Gbps
Outside the Chinese mainland	2 Gbps	2 Gbps

## Blocking duration

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

The blocking duration is subject to the following factors:

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

Note :

For IPs that are blocked extra frequently, Tencent Cloud reserves the right to extend the duration and lower the threshold.

## Why is blocking necessary

Tencent Cloud reduces costs of using clouds by sharing the infrastructure, with one public IP shared among all users. When a large traffic attack occurs, the entire Tencent Cloud network may be affected, not only the target servers. To protect other users and ensure network stability, we have to block the target server IP.

## Why isn't anti-DDoS service always free

DDoS attacks not only threaten the targets but also the entire cloud network, affecting non-attacked Tencent Cloud users as well. Also, DDoS protection incurs high costs, including cleansing costs and bandwidth costs, in which bandwidth costs the most. Bandwidth costs are calculated based on the total amount of traffic; there is no difference between costs incurred by normal traffic and attack traffic.

Therefore, Tencent Cloud provides Anti-DDoS Basic service free of charge for all users. But once the attack traffic exceeds the free quota, we will have to block the attacked IP from all public network access.

# Purchase Guide

Last updated : 2021-08-23 16:31:52

- Anti-DDoS Basic is free of charge.
- If you have any questions, please [contact us](#) for assistance.

# Operation Guide

## Operations Overview

Last updated : 2021-08-26 14:53:45

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

## Anti-DDoS Basic

[Viewing Protection Configuration](#)

## Statistic Report

[Viewing Statistic Report](#)

## Security Event Notification

[Setting Security Event Notifications](#)

# Use Limits

Last updated : 2021-08-26 14:53:45

## Applicable services

Tencent Cloud provides free basic DDoS protection for Tencent Cloud services such as CVM, CLB and NAT Gateway.

# Viewing Protection Configuration

Last updated : 2021-08-26 14:53:45

## Scenarios

You can view the Anti-DDoS Basic protection details and modify the protection configuration in the [Anti-DDoS Console](#).

## Directions

1. Log in to the [Anti-DDoS Console](#) and click **Anti-DDoS Basic**.
2. Select a server type and a region, and then click the server name.

Blackholing Threshold	300 Gbps (services deployed on this CVM will be interrupted for 2 hours once the black hole is triggered) <a href="#">Purchase Anti-DDoS Advanced/Pro</a>	
DDoS Protection	<input checked="" type="checkbox"/>	Disabling DDoS protection will expose your server to attacks.
CC Attack Protection	<input checked="" type="checkbox"/>	
HTTP Request Threshold	<input type="text" value="100 QPS"/>	When the number of HTTP requests exceeds the set value, CC defense is triggered.

### Note :



DDoS protection is enabled by default. When an attack occurs, DDoS traffic cleansing will be triggered and the DDoS system will detect and filter out malicious traffic.

You should carefully consider disabling DDoS protection as it may cause server crashes and service interruptions.

- Threshold for triggering black hole

It displays the current protection threshold of the resource. When the attack traffic exceeds the threshold, blocking will be triggered, causing abnormal business access for a period of time. If you need higher DDoS protection capability, you can purchase appropriate Anti-DDoS products for your business needs.

- CC protection

It is disabled by default and displayed as . To enable it, you can click  while setting the HTTP request threshold. If the number of HTTP requests exceeds the threshold you set, CC protection will be triggered and the Anti-DDoS system will detect and filter out malicious traffic.

# Viewing Statistical Reports

Last updated : 2021-08-26 14:53:45

## Scenarios

When you receive a DDoS attack alarm message or notice any issue with your business, you need to view the attack details including the attack traffic and current protection effect. Enough information is critical for you to take measures to keep your business running smoothly.

The Anti-DDoS Basic console allows you to stay on top of attack details with statistical reports.

## Directions

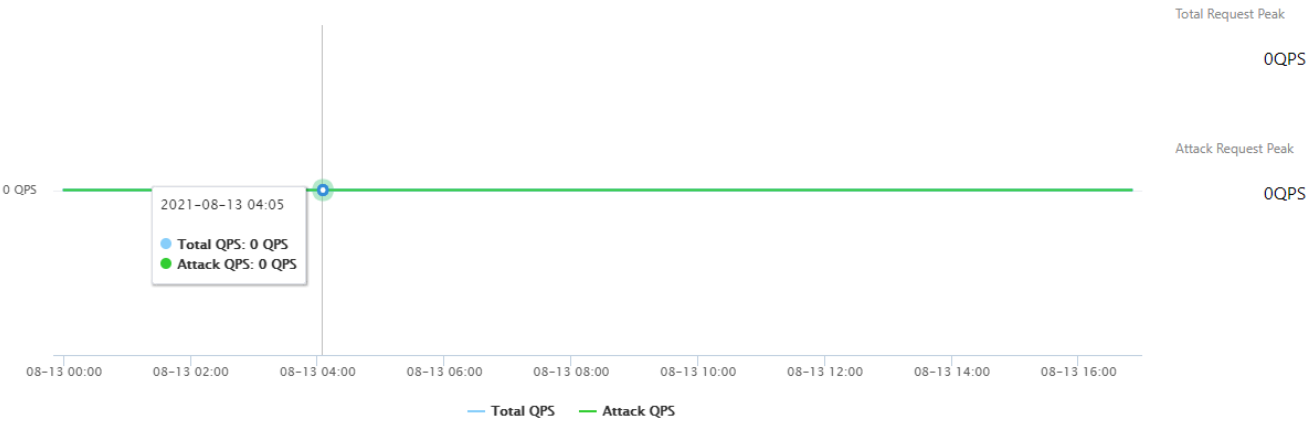
1. Log in to [Anti-DDoS Console](#).
2. On the *\*Anti-DDoS Basic \** page, select a server type and a region, and then click the server name.
3. On the **DDoS Attacks** tab, set a query period.
  - In the **Attack Traffic Statistics** section, you can view the DDoS attack trend within the set period.
  - In the **DDoS Attack Records** section, you can view the DDoS attack records including the start and end time of the attack, whether blocking is triggered and the cleansed traffic volume.



4. On the **CC Attacks** tab, set a query period so that you can view the CC attack requests and trend within the period.

DDoS Attacks **CC Attacks**

Real time 6 hours **Today** Last 7 days Last 15 days Last 30 days 2021-08-13



# Setting Security Event Notification

Last updated : 2021-08-26 14:53:45

## Scenarios

Tencent Cloud will send you alarm messages for your public IP via the channels you configured including Message Center, SMS, email and phone call 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.

## Directions

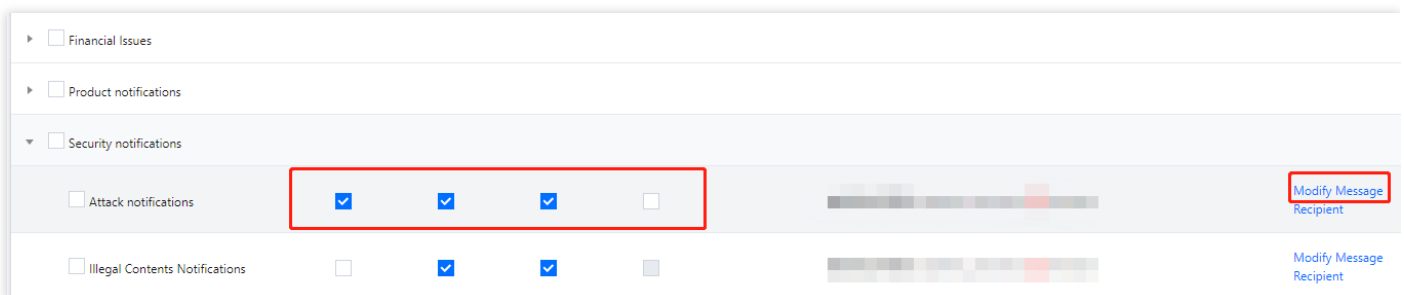
1. Log in to your Tencent Cloud account and go to [Message Center](#).

Note :



You can also log in to the [console](#), click  on the top bar, and click **Message Center** on the pop-up page.

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





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

Modify Message Recipient

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 Recipient

Modify User Information

Search for user name

<input checked="" type="checkbox"/> User Name	Mobile Number	Email

4 selected

OK

Cancel

# Troubleshooting

## A public IP suffered DDoS attacks

Last updated : 2021-08-26 14:53:45

### Problem

DDoS attacks overwhelm your business with massive amounts of traffic, exhausting the server performance and network bandwidth and thus crashing down the server.

### Common Cause

Tencent Cloud's free basic protection capability (2 Gbps) is not enough to defeat the DDoS attacks.

### Solutions

- **Replace a public IP (expedient)**

When attackers start DDoS attacks against your specific business IP, you can avoid the blocking trouble temporarily by replacing the attacked IP with a new one. However, the new IP is still exposed to DDoS attacks, causing potential business interruptions.

- **Get an Anti-DDoS product (recommended)**

By getting an Anti-DDoS instance, you can improve IP protection capability to defend against large traffic attacks. If the Anti-DDoS Pro instance of the region is unable to defeat massive attack traffic, you can use an Anti-DDoS Advanced instance with greater protection capability as needed.

### Directions

#### Replace a public IP (expedient)

The use limits are as follows:

- Each account can change public IP addresses in the same region a maximum of 3 times per day.
- Each instance can only change its public IP once.
- The old public IP will be released after it is replaced.

For details, see [Changing Public IP Addresses](#).

### **Get and set an Anti-DDoS product (recommended)**

- To learn more about purchasing and configuring an Anti-DDoS Pro instance, see [Purchase Directions](#) and [Getting Started](#).
- To learn more about purchasing and configuring an Anti-DDoS Advanced instance, see [Purchase Directions](#) and [Getting Started](#).

For details on differences between Anti-DDoS Pro and Anti-DDoS Advanced instances, see [Comparison of Anti-DDoS Protection Schemes](#).