Aegis Anti-DDoS

Product Introduction

Product Documentation

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

Product Introduction

Overview

Last updated : 2020-07-30 11:31:43

Leveraging Tencent's over a decade of experience in security accumulated from various lines of business, Tencent Cloud Aegis Anti-DDoS is a multi-layer, all-around, cost-effective protection solution against DDoS attacks for your business. It is capable of precise purge of various types of network attack traffic and directing of normal traffic to business servers, preventing business fluctuations, service interruptions and user experience downgrading caused by potential DDoS attacks. In addition, it features protective resources at the Tbps level and customizable advanced security policies for targeted protection against specific attack behaviors.

Product Categories

Aegis Anti-DDoS offers the following options: DDoS protective IP and DDoS protection pack which are paid services; advanced anti-DDoS policy, advanced HTTP anti-CC defense policy and watermark protection which can be configured free of charge.

Pricing

Aegis Anti-DDoS uses a mixed billing model including prepaid and pay-per-use on a daily basis. Base protection bandwidth is prepaid on a monthly basis, while elastic protection bandwidth and forwarded business traffic are pay-per-use on a daily basis. For detailed pricing of Aegis Anti-DDoS, see:

- **Single-IP Pricing for DDoS Protective IP**
- **Package Pricing for DDoS Protective IP**
- **Single-IP Pricing for DDoS Protection Pack**
- **Multi-IP Pricing for DDoS Protection Pack**

How to Use

Tencent Cloud Aegis Anti-DDoS has web-based UIs (i.e. console). If you have already signed up for a Tencent Cloud account, you can log in to the Aegis Anti-DDoS Console to purchase and perform various operations.

Related Concepts

The following concepts are usually involved in Aegis Anti-DDoS:

- **DDoS**
  This is short for distributed denial-of-service, a network attack technique that uses network resources to initiate service requests to specific target servers and makes end user's normal service requests impossible to be completed by exhausting the bandwidth or other resources of the target servers.
- **IP blocking**
  If the DDoS attack traffic exceeds the protection bandwidth set by the user, Aegis Anti-DDoS will block all service requests to the attacked target servers for a period of time.
- **BGP network**
  This is the type of network directly connected to the Internet AS using the Border Gateway Protocol (BGP). Tencent Cloud's BGP links are connected to 28 ISPs, eliminating cross-network latency and enabling an excellent network access experience.
- **China Telecom, China Unicom and China Mobile networks**
  This refers to the non-BGP networks of China Mobile, China Unicom and China Telecom. They provide static IP resources, and non-local users need cross-network access when using these resources.
- **Forwarding rule**
  This is to configure the rule according to which the business request first accesses the protective IP's service port and then is forwarded to the real server port of the real server IP address. Port forwarding rules can be configured and real server polling by weight or by minimum number of connections is supported.
- **Traffic-forwarding egress IP address**
  This is the exit IP address used when forwarding the business request from the protective IP to the real server. If relevant security policies are configured for the real server, the exit IP address should be added to the allowlist to avoid mistaking normal requests for attacks.
- **Protection bandwidth**
  This is divided into base protection bandwidth and elastic protection bandwidth. If optional elastic protection is chosen, the protection bandwidth is the highest bandwidth that can protect against the actual attacks. If the attack traffic exceeds the protection bandwidth, the system will temporarily block the attacked IPs.
- **Region**
  This refers to the region where a protective IP or protection pack is available. It is recommended to choose the region closest to the real server. Protection pack can only be bound to the Tencent Cloud public IP addresses in the same region where it is available.

Related Services

- **DDoS protective IP**
  This is a large-traffic DDoS protection service for Tencent Cloud customers (including off-cloud servers). The protective IP is used as the access point for the business traffic. The backend protection system checks the traffic and performs traffic purges if any DDoS attacks are detected, and then forwards the normal business request to the real server of the business.
- **Protected domain name**
  Protected domain name is provided free of charge when the user creates a business in the console. The user can configure the CNAME of their primary domain name to resolve to the protected domain name for easy access. Resolution to the protective IP can be enabled for the protected domain name for smart resolution based on request source.
- **DDoS protection pack**
  This is an enhanced DDoS protection service for Tencent Cloud customers' in-cloud servers. It works in single-IP or multi-IP mode. Single-IP protection pack can be bound to one Tencent Cloud public IP, while multi-IP protection pack can be bound to multiple Tencent Cloud public IPs.
- **Elastic traffic pack**
  DDoS protection pack is billed based on the elastic protection traffic, and when the attacks exceed the base protection and trigger elastic protection, the incurred elastic traffic will be deducted from a purchased elastic traffic pack in the same region. Compared with billing by the elastic bandwidth, it can effectively cope with peak-type high-bandwidth attacks with lower protection costs.

DDoS Protective IP

Last updated : 2020-02-27 19:41:49

What is DDoS High Defense IP

DDoS high defense IP is the main product of Internet business defense against DDoS attacks, which can effectively deal with Traffic's DDoS attacks. High defense IP can provide you with rich defense resources by region and line dimension. You can choose the resources that suit you according to the region and network where your business is located. At present, Mainland China BGP and triple-net high-defense IP, are available, including Hong Kong, China, the western United States, Japan, South Korea, Singapore and other regions. Tencent Cloud high defense IP can deal with T-level attack Traffic.

Use cases

DDoS High Defense IP serves all Cloud Virtual Machine except Tencent Cloud and Tencent Cloud.

Protection principle

DDoS High Defense IP protects real server server through Proxy repost mode. Business Traffic directly Access High Defense IP, then Origin-pull to real server server. If a DDoS attack occurs, the defense system will filter and clean the high defense IP when attacking Traffic, and send the cleaning business Traffic, repost and Origin-pull to the business server to ensure the availability of the business in the DDoS attack scenario.

Why choose DDoS High Defense IP

Hidden IP of origin server
DDoS high defense IP through Proxy repost mode, the business Traffic repost to real server IP, to hide the source IP, attack Traffic was cleaned to protect real server business.

- Ultra-large bandwidth protection
  DDoS High Defense IP provides T-level protection against cloud and internal servers, easily resisting Traffic DDoS attacks and CC attacks.

Notes:
To configure higher bandwidth protection, please contact Agent for advice.

- Support single IP and package purchase
  DDoS High Defense IP supports flexible purchase of one or more different lines at one time, which is suitable for various business scenarios. If the business demand is mainly a certain ISP line, you can directly purchase single IP protection. The package provides multi-line protection to prevent users from crossing the network Access.
  Flexible Billing
  Prepaid's protection on a monthly basis + Postpaid's elastic protection on a daily basis will be charged according to the actual attack volume, which will save you the cost. For more information, please see Billing Description .

What do you need to pay attention to when using it?

DDoS High Defense IP uses High Defense IP as a business IP to hide real server IP, to publish to achieve protection. If user real server has been attacked and the origin server IP has been Open, it is recommended to replace real server IP, after purchasing DDoS High Defense IP service to ensure the secrecy of real server IP, so that attackers cannot directly attack real server. If it is Tencent Cloud server IP, please see How to change the IP address of Tencent Cloud server .

How to configure DDoS High Defense IP

Login [Aegis Security console], on the left, Directory, click [DDos High Defense IP], and select "purchase High Defense IP". For details of the operation, see DDoS High Defense IP .

DDoS Protection Pack

Last updated : 2020-03-04 11:13:58

What is DDoS High Defense package

DDoS high defense package is the main product against DDoS attacks, which is deployed on Tencent Cloud for Internet business. The DDoS high defense package is easy to use, and can be configured quickly and easily in situations where it is not convenient to change the IP address or there are a large number of IP to protect. At present, DDoS high defense package has single IP mode and multi-IP mode.

Use cases

DDoS High Defense package is only applicable to Tencent Cloud products, including Cloud Virtual Machine, Cloud Load Balancer, CPM, BM, Cloud Load Balancer, NAT IP, EIP, GAAP IP and so on.

Why choose DDoS High Defense package

- No configuration required, effective immediately
  After purchasing the DDoS high defense package, you can bind Tencent Cloud services products directly through the high defense package, without the need for additional replacement of the source IP, quick protection.
- Ultra-large bandwidth protection
  DDoS high defense package provides 200Gbps protection and 400Gbps elastic protection for servers in the cloud.

> If you need to configure high bandwidth protection, please contact Agent for advice.

- Support single IP mode and multi-IP mode
  DDoS High Defense package supports one-time purchase order IP or multi-IP, flexible purchase, which is suitable for various business scenarios. Multi-IP supports binding multiple different business IP, at the same time and configuring high defense policy at the same time.
  Flexible Billing

Monthly Prepaid's bottom protection + daily Postpaid's elastic protection / elastic Traffic bag for payment after dosage. When the bandwidth of the business attack exceeds that of base protection bandwidth and does not exceed elastic protection bandwidth, the DDoS high defense package continues to protect, and the portion exceeding the guaranteed peak value will be paid according to the usage, thus saving costs for users. For more information, please see Billing Description . When the bandwidth of business attack exceeds that of base protection bandwidth, you will press **Peak elastic bandwidth / elastic Traffic package** Billing. Elastic Traffic packet Bill-by-traffic, compared with Bill-by-bandwidth, the peak of elastic bandwidth, when the bandwidth of business attack is very high but the actual Traffic is not many, elastic Traffic packet can effectively deal with peak high bandwidth attacks with lower protection cost.

How to configure DDoS High Defense package

Login [Aegis security console], click "DDos High Defense package" on the left side of Directory, and select "purchase High Defense package". For details of the operation, see DDoS High Defense package .