Aegis Anti-DDoS

Glossary

Product Documentation

Glossary

Last updated：2019-01-17 15:57:45

DDoS

DDoS (Distributed Denial-of-Service) is an attempt to make an online service unavailable to its intended users and prevent legitimate requests from being fulfilled by overwhelming the target servers with traffic from multiple sources and depleting the bandwidth or resources of target servers.

CC Attack

CC (Challenge Collapsar) attack is a type of DDoS attack. It is an attempt to make an online service unavailable to its intended users and prevent legitimate requests from being fulfilled by flooding the target servers with data packets from a large number of terminals (which mimic legitimate users) and depleting the resources of target servers.

IP Blocking

IP blocking is a security protection that blocks all access requests to the IP of target server for a period of time when the traffic of DDoS attack on the target server exceeds the protection peak set by user.

BGP Network

BGP (Border Gateway Protocol) network is a network that connects directly with the autonomous systems (AS) in the Internet by using border gateway protocol. Tencent Cloud's BGP linkage has gained access to 28 ISPs to eliminate cross-network delay and provide excellent network access experience.

Non-BGP Network

This refers to China Telecom, China Unicom and China Mobile's non-BGP networks, which provide static IP resources. If a user in a non-BGP network wants to access the resources from another non-BGP

network with which he/she is not registered with, cross-network access is required.

3 Non-BGP IPs

One protective IP is configured for each of the three non-BGP networks (China Telecom, China Unicom and China Mobile). A total of three protective IPs are configured.

2 Non-BGP IPs

One protective IP is configured for each of two of the three non-BGP networks (China Telecom, China Unicom and China Mobile). A total of two protective IPs are configured.

1 BGP + 3 Non-BPG IPs

A total of four protective IPs are configured, out of which one for BGP network, and three for China Telecom, China Unicom and China Mobile non-BGP networks (one for each of them).

1 BGP + 2 Non-BPG IPs

A total of three protective IPs are configured, with one for BGP network, and two for two of the three non-BGP networks (China Telecom, China Unicom and China Mobile).

Base Protection Bandwidth

This refers to the maximum value of base protection bandwidth. This service is billed on a monthly or yearly basis.

Elastic Protection Bandwidth

This refers to the maximum value of protection bandwidth against attack. It is set to defend against the attack traffic that exceeds the base protection bandwidth.

Protective Domain Name

This refers to a protective domain name ending with "gsadds.com" that is generated when an application is created. Protective domain names enable the use of protective IPs' s smart parsing function.

Forwarding Rule

This refers to the rule by which the traffic from the server port at protective IP is directed to the real server ports at real server IPs. Polling real servers by weight or by minimum number of connections is supported.

Forwarding Egress IP

This refers to the egress IP address used by a protective IP to forward traffic to the IP of real server, that is, the traffic source IP from the perspective of real server.

Region

This refers to the region where protective IPs or protection packs provide services. It is recommended to select a region closest to the real server.

Session Persistence

Session persistence is a means of directing a series of associated access requests to the same server. When there are multiple real server IPs under the same forwarding rule, if the requests from the same customer need to be processed by a single server, session persistence is required.

Polling Policies

When there are multiple real server IPs under the same forwarding rule, polling by weight or by minimum number of connections can be selected to determine the proportion of application requests processed by each backend real server. Polling policies include polling by weight and polling by minimum number of connections.

- Polling by weight: With forwarding rule in place, the traffic forwarded to real servers is distributed among the servers based on their weights.
- Polling by minimum number of connections: With forwarding rule in place, the connection requests are distributed evenly among the real servers.

Forwarding Port

This refers to the port that provides service at a protective IP. Any business request from a client or user directly accesses this port at protective IP.

Real Server Port

This refers to the port from which real server provides service. It is paired with the forwarding port. A protective IP forwards a user's business request on the forwarding port to the real server port at the real server's IP address.

Real Server Public IP and Weight

Real server public IP refers to the IP address of a backend real server that provides service. If there are multiple real server public IPs, the protective IP allocates the business requests to the real servers through polling. The bigger the weight set for a real server, the more business requests received by the real server.