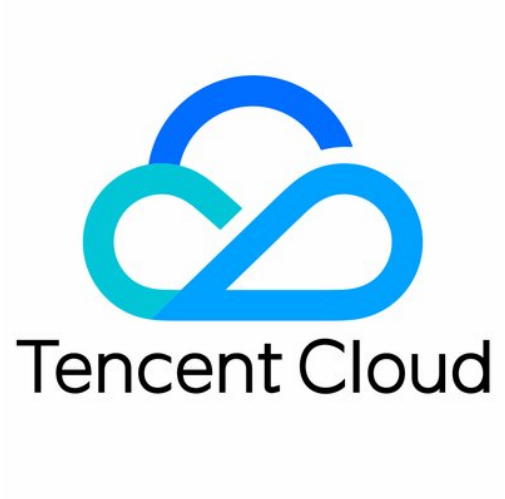
Anti-DDoS

Glossary

Product Documentation



Glossary

Last updated：2024-07-01 11:43:46

A Record

A record that maps a host name or domain name to an IP address.

BGP Network

A high-speed and interconnected network type based on Border Gateway Protocol (BGP) and Internet autonomous systems (AS). Tencent cloud has a BGP network encompassing 30 ISPs, which can ensure the speed and reliability of Internet connections and thus improve the user experience.

CNAME

An alias record that maps one domain name to another. You can use CNAME to point multiple host names to one alias so that you can quickly change IP addresses.

CC Attack

A Challenge Collapsar attack (CC attack) is a malicious attempt to make a targeted server unavailable by occupying its application-level resources and exhausting its processing power. Common CC attacks include HTTP/HTTPS-based GET/POST Flood, Layer-4 CC, Connect Flood, etc.

DDoS Attack

A Distributed Denial of Service (DDoS) attack is a malicious attempt to make a targeted server unavailable by overloading its system resources with a flood of Internet traffic.

Blocking

Once the attack on a targeted server goes over the basic protection bandwidth or the maximum protection bandwidth that has been purchased, Tencent Cloud will temporarily block the server from all public network access through ISP service.

Protection Bandwidth

Maximum protection capability of an Anti-DDoS instance, which includes base protection bandwidth and elastic protection bandwidth.
Base protection bandwidth refers to the basic protection capability of an Anti-DDoS Pro instance. The fees for the base protection bandwidth will be frozen once you purchase it. The bill of the current month will need to be settled in the following month.
Elastic protection bandwidth refers to the maximum protection capability of an Anti-DDoS Pro instance. The elastic protection is pay-as-you go and billed daily; you only need to pay for what you use.

If elastic protection is enabled and configured for an Anti-DDoS Pro instance, the elastic protection bandwidth will be its maximum protection bandwidth. Once the attack traffic exceeds the maximum protection bandwidth, the attacked IP will be blocked.

Traffic Cleansing

If the public network traffic of the target server exceeds the pre-set protection threshold, Tencent Cloud Anti-DDoS service will automatically cleanse the inbound public network traffic. With the BGP 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 server. In general, cleansing does not affect access except on special occasions or when the cleansing policy is configured improperly.

Forwarding Rule

A load balancing scheduling algorithm that distributes traffic to multiple servers at the backend. It supports weighted polling and source IP hashing. With certain rule configurations, the service traffic can be directed to the Anti-DDoS IP first before being sent back to the origin server.