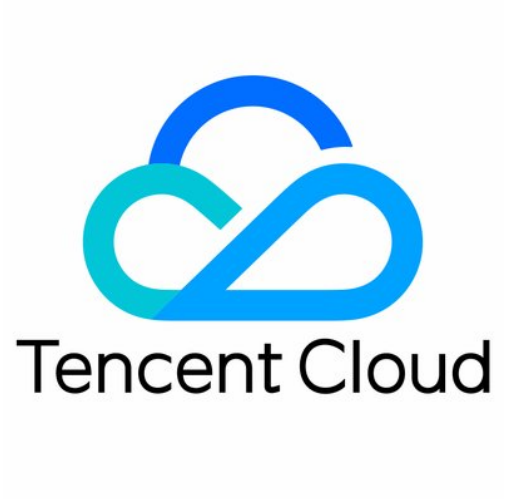
Anti-DDoS Advanced

Glossary

Product Documentation



Copyright Notice

Trademark Notice

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.

Glossary

Last updated：2019-05-07 10:27:18

A Record

A record is used to specify the corresponding IP address of a hostname (or domain name).

BGP Network

Border Gateway Protocol (BGP) network is a network type where BGP is used as the routing protocol and high-speed interconnection of Internet AS (autonomous systems) is provided. Tencent cloud BGP line connects to 30 ISPs, which can fix slow/unstable Internet connections and thus improve the user experience.

CNAME

A CNAME (Canonical Name) is a alias record that can map one domain name (an alias) to another. CNAME can map more than one hostname to the same alias so as to realize the quick change of IP addresses.

CC Attack

In a CC (Challenge Collapsar) attack, the attacker uses a proxy server to send a large number of deceptive requests to the target server to occupy the application-level resources and consume server's processing power, resulting in server failures. Common CC attacks include HTTP/HTTPS-based GET/POST Flood, layer 4 CC, and Connect Flood.

DDoS Attack

A DDoS (Distributed Denial of Service) attack is a malicious attempt to render services unavailable by overwhelming the targeted system with a flood of Internet traffic.

Block

When the target server receives attack traffic exceeding the protection bandwidth limit of the purchased anti-DDoS service package, Tencent Cloud will temporarily stop all public network accesses to the server via the ISPs.

Protection Bandwidth

Protection bandwidth refers to the maximum protection capability of your purchased Anti-DDoS service, which includes base protection and elastic protection.

- Base protection: Monthly subscription Anti-DDoS service plan that provides base protection of an Anti-DDoS Advanced instance. Fees for the first month will be frozen upon purchase and billed the next month.
- Elastic protection bandwidth: Pay-as-you-go daily Anti-DDoS service plan that provides maximum elastic protection capability of an Anti-DDoS Advanced instance.

With elastic protection enabled, your Anti-DDoS Advanced instance will have a protection bandwidth limit equivalent to the peak value of your purchased elastic protection bandwidth. The attacked IP will be automatically blocked as soon as the attack traffic exceeds the elastic protection bandwidth limit.

Traffic Cleansing

When the incoming public network traffic exceeds the protection threshold of the target server, Tencent Cloud Anti-DDoS Advanced IP will automatically start the traffic cleansing process. The traffic will then be redirected via BGP to an Anti-DDoS Advance IP, which will clean and remove the attack traffic, then forward the cleansed traffic back to the target server. Generally, traffic cleansing does not affect normal access, unless the cleansing policy is wrongly configured.

Forwarding Rule

A forwarding rule is a load balancing scheduling algorithm that distributes traffic to multiple servers at the back end. It supports weighted polling and source IP hashing, and its configuration enables the redirection of business request traffic to the Anti-DDoS Advanced IP before sending the traffic back to the real server.