Web Application Firewall

FAQ

Product Documentation

Copyright Notice

Trademark Notice

Tencent Cloud

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.

FAQ

Last updated : 2020-02-25 14:49:06

Can non-Tencent Cloud servers use Web application firewall?

WAF can be connected with servers in data centers outside Tencent Cloud. WAF protects servers in any public networks, including but not limited to Tencent Cloud, cloud from other vendors, and IDC. Domain names connected in Mainland China must be ICP licensed as required by MIIT.

Does the Web application firewall support HTTPS protection?

WAF completely supports HTTPS service. You just need to upload the SSL certificate and private key as instructed, or select the Tencent Cloud hosting certificate to make WAF protect HTTPS traffic.

Is the QPS limit specification of the Web application firewall for the entire instance or the configured QPS limit for a single domain name?

The QPS limit in WAF is for the entire instance. For example, if three domain names are under protection of the WAF, the total QPS of the three domains names cannot exceed the upper limit. If the QPS limit of the purchased instance is exceeded, speed limit is triggered, which will result in packet loss.

Can real server IP of Web application firewall Enter Tencent Cloud CVM Private IP?

When adding a domain name to the Web application firewall, Enter's real server address must be a public network IP or a domain name. Egress IP, of public network IP, including CVM public network IP, CLB public network IP or other local IDC, does not support Private IP of Enter CVM.

Can the Web application firewall use Anti-DDoS Pro directly?

Yes, you can directly select the IP of the Web application firewall instance on the Anti-DDoS Pro console configuration page to enable WAF to have high defense capability. For more information, please see Anti-DDoS Pro access practice .

How does Web application firewall connect with CDN or Anti-DDoS Pro?

- The Web application firewall can directly overlay Anti-DDoS Pro. Real server of CDN can point to the IP of the Web application firewall instance. The best deployment architecture: client > CDN > Web application firewall + high defense package > Cloud Load Balancer > real server.
  If you need CDN and high defense capability, set the CNAME provided after the connection to WAF to the CDN origin server, and associate the Dayu high defense package with the WAF instance. The user traffic, after going through CDN, is forwarded to WAF, which has the capability of

cleaning high-traffic DDOS attacks, and then be forwarded to the origin server to achieve a full protection.

Web application firewall how many Origin-pull IP? can be set for a protected domain name

A maximum of 20 intermediate IP can be set for a protected domain name of Web application firewall.

How to load the Web application firewall when configuring multiple real server?

If multiple Origin-pull IP,Web application firewalls are configured, Cloud Load Balancer will be used for Access requests by polling.

Does the Web application firewall support Health check?

Health check is enabled by default in Web application firewall. The Web application firewall will check the access status of all real server IP. If a real server IP does not respond, the Web application firewall will no longer request repost to the real server IP until the access status Resume is normal.

Does the Web application firewall support Session maintenance?

The firewall of Web application can be maintained by Session. It is enabled by default.

In the console of the Web application firewall, how long will it take to take effect after changing the configuration?

In general, the changed configuration will take effect within 10 seconds.

Will the Web application firewall automatically add intermediate IP segment to the security group?

The high defense intermediate IP segment is not automatically added to the security group. Please see Quick Start Add the corresponding intermediate IP to the security group.

If the uploaded files are blocked, will they still be blocked when using HTTPS or SFTP?

If you do not use Web application firewall will not be Block, if you use Web application firewall and turn on Block mode, using HTTP or HTTPS to upload malicious files will be Block. However, uploading files using SFTP will not be protected by Block. SFTP is not HTTP or HTTPS Protocol. Web application firewall does not support protection.