Web Application Firewall

FAQS

Product Documentation

Contents

FAQS
Connection

Last updated : 2020-09-14 10:47:01

Can non-Tencent Cloud servers use Web Application Firewall (WAF)?

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, and clouds and IDCs from other vendors.

> Domain names connected in Mainland China must be ICP licensed as required by MIIT.

Does WAF support HTTPS protection?

WAF fully supports HTTPS services. 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.

Does the WAF QPS limit apply to the entire instance, or to 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 the real server IP added to WAF be a private IP in Tencent Cloud CVM?

When adding a domain name to WAF, you must enter a public IP or domain name as real server address, including CVM public IP, CLB public IP, or Egress IP from other local IDCs, and cannot enter a CVM private IP.

Can WAF use Anti-DDoS Pro directly?

Yes, you can empower WAF with high DDoS protection capability simply by selecting IPs specified in a WAF instance in the Anti-DDoS Pro console configuration page. For more information, please see Anti-DDoS Pro access practice.

How does WAF connect with CDN or Anti-DDoS Pro?

- WAF can be associated directly with Anti-DDoS Pro as long as the CDN origin server points to the IP specified in the WAF instance. The best deployment architecture is: client > CDN > WAF + Anti-

DDoS Pro > CLB > real server.

- If you need the CDN and Anti-DDoS capabilities, simply set the CNAME provided after the connection to WAF to CDN origin server, and associate Anti-DDoS Pro 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 finally reaches the real server for full protection.

How many intermediate IPs can I set for a WAF-protected domain name?

You can set up to 20 ones for a WAF-protected domain name.

How does WAF handle load when configuring multiple real servers?

In case of multiple intermediate IPs, WAF will load balance access requests with Round Robin algorithm.

Does WAF support health check?

In WAF, health check is enabled by default. WAF will detect if any real server IP is inaccessible. If a real server IP does not respond, WAF will stop forwarding requests to this IP until it goes back to normal.

Does WAF support session persistence?

Session persistence is enabled in WAF by default.

How long does it roughly take for a configuration change to take effect in the WAF console?

In general, a configuration change takes effect within 10 seconds.

Will WAF automatically add an intermediate IP range to a security group?

No, WAF won’t automatically add an intermediate IP range to a security group. To add intermediate IPs to a security group, see Getting Started with WAF.

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

They won’t be blocked if WAF is disabled. However, if you enable block mode in WAF, it blocks malicious files uploaded with HTTP or HTTPS, but does not block any files uploaded with SFTP, a non-HTTP or -HTTPS protocol beyond protection of WAF.

Do SaaS WAF and CLB WAF support SSL mutual authentication?

CLB WAF supports SSL mutual authentication, while SaaS WAF does not.

Which cipher suites are supported by SaaS WAF and CLB WAF?

- SaaS WAF does not support SSL cipher suite settings.
- CLB WAF supports the following cipher suite.
  ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-CHACHA20-POLY1305:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128:AES256:AES:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK

Domain Name

Last updated : 2020-10-20 14:20:55

How do I connect a domain name?

You can connect a domain name using the WAF Console. For more information, see Add a Domain Name.

Does WAF support connecting wildcard domain names?

Yes.

Note :

- If you have configured a wildcard domain name in WAF, contact us quickly to help process it by submitting a ticket. The wildcard domain name configuration will then be available for you in WAF, which automatically matches the corresponding sub-domain names.
- If a wildcard domain name, such as `*.test.com`, is already connected to Tencent Cloud, then any of its sub-domain names cannot be connected to another account.
- If the wildcard domain name `*.test.com` is already connected to your account, then wildcard domain names in formats such as `*.a.test.com` cannot be connected to this account.
- If you add both a wildcard and a precise domain name (e.g. `*.test.com` and `a.test.com`), WAF first uses the protection policies configured for the precise domain name.

How long does it take to update the DNS resolution (protection) status of my domain name?

Verify that CNAME configuration for your website domain name is correct. Once you add a CNAME record in DNS, please wait 10-20 minutes for the protection status to be updated. If you have waited over 30 minutes, and the protection status has not been updated yet, you can contact us for help by submitting a ticket.

Will WAF notify me when the intermediate IP address of my domain name is changed?

In principle, the intermediate IP address of your domain name is not changed. If it happens, we will notify you by SMS, email or Message Center. You can view your intermediate IP address in the [Domain Name List] (https://console.cloud.tencent.com/guanjia/waf/config) of the console.

What are the requirements for connecting a domain name to WAF?

The business content on your real server must be legal, and you can modify the DNS resolution properly. Otherwise, you will not be able to connect your domain name to WAF.

What options does WAF offer for domain name origin-pull?

WAF performs origin-pull based on domain name or IP. You can choose which option to configure as you need. For more information, see Add a Domain Name.

How do I bind a CNAME to my domain name connected to WAF?

See CNAME Configuration for how to bind CNAME with your DNS service provider.

Will the logging feature still be available once WAF is disabled for the domain name list?

Once WAF is disabled, all its protection features are unavailable, and only the traffic forwarding mode starts to run instead, with no logs recorded.

Will the CNAME change if my domain name is deleted and added again?

No, it won't. You can go to the WAF Console, click your domain name in the Domain Name List, and view the CNAME in **Basic Settings**.

Can I change the VIP address of my domain name?

No, you can't change it, in principle. However, if an exception occurs to your WAF service, you may contact us quickly by submitting a ticket so that we can switch it to another working VIP address for you.

What should I do if the VIP address of my WAF-protected domain name is blocked due to DDoS?

WAF provides anti-DDoS Basic capabilities (2 G) for VIP addresses by default. In case of an urgent need to resume your business for a VIP address blocked by anti-DDoS Basic, you can:

- Log in to the DDoS Protection Console, and unblock the VIP address manually. You are allowed to do so three times each month.
- Or buy a Anti-DDoS Pro instance, and bind it to your WAF-protected VIP address.

You are allowed to remove blocking manually only three times per month. The system resets the count of blocking removals at zero o'clock on the 1st day of every month, and the remaining number of allowed removals from last month is not carried over to this month.

How do I connect a CDN domain name to WAF?

To connect a CDN domain name, simply use the CNAME address that WAF assigned for your domain name as CDN origin server. The content is pulled from the origin as traffic flows through the architecture “user > CDN > WAF > CLB > real server”. Meanwhile, you can log in to the WAF Console, and select **Yes** for *Proxy** in the Add domains page. Then, WAF obtains the real IP of your client for protection based on the XFF field in HTTP headers.

How do I add a real server domain name to WAF?

To add a real server domain name to WAF, enter the CNAME or other domain name different from the protection domain names. You may leave the protocol (HTTP or HTTPs) empty.

Differences Between WAF and CFW

Last updated : 2020-12-15 16:16:22

What are the differences between Web Application Firewall (WAF) and Tencent Cloud Firewall (CFW)?

Their differences are as follows:

Product / Item	WAF		CFW
	SaaS WAF	CLB WAF	
Protection Object	Web and API service	Web and API service	Businesses entirely opened to the Internet
Use Cases	Cybersecurity classified protection, intensifying protection, web and API security protection, application layer protection, and anti-cheating protection.	Cybersecurity classified protection, intensifying protection, web and API security protection, application layer protection, anti-cheating protection, and layer-7 CLB instance application.	Cybersecurity classified protection, intensifying protection, CVM host and web security protection.

Product / Item	WAF		CFW
	SaaS WAF	CLB WAF	
Core Protection Capability	• Web vulnerability defense, unknown threat defense, and self-service false-negative and false-positive attack processing. • CC attack defense. • Bot action management and crawler defense. • API security and business security protection. • Anti-leak and anti-tampering.	• Web vulnerability defense, unknown threat defense, and self-service false-negative and false-positive attack processing. • CC attack defense. • Bot action management. • API security and business security protection. • IPv6 web protection.	• IPS virtual patching, which eliminates the needs for realistic CVM patches and restarting. The basic vulnerability defense for OWASP top 10 attacks is covered. • Automatic detection for compromised hosts and automatically blocking CVM malicious external connections. • Domain name-based active external connection control.

Product / Item	WAF		CFW
	SaaS WAF	CLB WAF	
Core Strength	The wide scenarios ranging the application needs of users both within and outside Tencent Cloud.	It is a Tencent Cloud native service, which can be connected across regions, eliminating the need to adjust the existing network architecture. Web business forwarding and security protection are separated, therefore WAF service can be easily disconnected during service breakdown to achieve stable and reliable web security protection. It can only be used for businesses within Tencent Cloud.	The Tencent Cloud native firewall can be quickly enabled not affecting the existing businesses. It integrates security capabilities such as IIPS, threat intelligence, and vulnerability scanning, etc., which is ideal for cybersecurity classified protection and intensifying protection. It can only be used for businesses within Tencent Cloud.
Service Selection	For businesses requiring web and API security protection for both Tencent Cloud and local IDCs, we recommend using SaaS WAF.	For businesses using or planning to use layer-7 CLB instances, we recommend using CLB WAF.	For businesses requiring CVM protection, especially the ones with other public network services opened except the web service, we recommend using CFW.