# Web Application Firewall

# Getting Started

# Product Documentation

# Contents

# Getting Started

# Getting Started

Last updated：2023-12-29 11:38:05

This document describes how to quickly deploy and use a WAF instance. Specifically, purchase a WAF instance, organize the website domain name information, perform domain name connection and protection configuration, and get an overview of the business and security through the reports and stay on top of security status. You can view traffic processing details in attack logs and then adjust the protection configuration accordingly to meet special business needs. You can also use CM to configure different types of custom alarms and notification channels for more efficient Ops.

## Step 1. Purchase an instance

You can purchase multiple WAF instances. Multi-instance management better suits your business division and management requirements and allows you to achieve nearby access and protection of multi-region active-active instances in a unified manner.
For more information on instance purchase, see Purchase Guide.
For more information on instance management and renewal, see Instance Management.

## Step 2. Connect your website

There are SaaS WAF and CLB WAF instances.

### Domain name connection guide for SaaS WAF

To protect your website, SaaS WAF assigns a CNAME to your domain name under protection, modifies the DNS resolution record of your website, and forwards the web requests received by your website to WAF. Used with security groups, SaaS WAF can prevent direct attacks toward the real server of your website. To achieve the above, you need to follow the steps below:
Step 1. Add a domain name
Step 2. Perform local testing
Step 3. Modify DNS resolution
Step 4. Set a security group
Step 5. Verify the configuration

### Domain name connection guide for CLB WAF

CLB WAF associates with Tencent Cloud Layer-7 CLB (listener) cluster by your domain name, and detects and purges HTTP or HTTPS traffic that goes through the CLB instance for side-channel threats. In this way, it can provide protection without interrupting your traffic forwarding. To achieve the above, you need to follow the steps below:

Step 1. Confirm CLB configuration

Step 2. Bind a domain name to the CLB instance

Step 3. Verify the configuration

## Step 3. Configure the protection

WAF will protect the traffic to the connected website. It has multiple detection and protection modules to help your website tackle different types of security threats. The rule engine is enabled by default and used to defend against common web application attacks such as SQL injection, XSS, and web shell upload. Other modules can be enabled and configured with protection rules manually as needed.

## Step 4. Analyze logs

By default, WAF logs attacks only. After purchasing and activating the log service, you can have all access requests logged by domain name.

### Attack log

An attack log records the time, source IP, type, and details of an attack to facilitate real-time threat check and analysis as well as protection policy adjustment, fully meeting the needs of routine security Ops and business.
Currently, attacks are displayed in an aggregated manner; that is, logs of the same type from the same request source IP within a specific period are displayed as one log to reduce your Ops workload and improve the efficiency.
Additionally, you can query attack logs with full-text search, fuzzy search, and search by filter. For more information, see Attack Logs.

### Access log

Access logging is used to record access logs of domain names protected by WAF. It allows you to query and download access logs generated in the last 30 days and retain them for at least 180 days. For more information, see Access Log.

## Step 5. Generate a security report

After your website is connected to WAF for protection, you can go to the WAF overview page to query the current total number of domain names, connected website conditions, instance conditions, website business and attack traffic

analysis data in the last 30 days, and rule updates. In this way, you can have a better picture of the overall security of your website business. For more information, see Access Log.

## Step 6. Configure alarms in CM

After your website is connected to WAF protection, you can configure alarms in CM. Then, WAF will send you alarm notifications when exceptions are detected in the website request traffic and business traffic, so you can stay informed of your business security changes. In this way, you can quickly respond to exceptions and adjust WAF policies to ensure business stability and security.
You can configure the same domain name into instances of the same type in different regions to separate the connection configurations of forwarding and protecting resources while using the same protection policy.

# FAQs for Beginners

Last updated：2023-04-06 14:34:32

## Connection

### Is WAF available to servers outside Tencent Cloud?

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.

**Note:**

Domain names connected in the Chinese mainland must be ICP filed as required by the Ministry of Industry and Information Technology of China.

### 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-hosted certificate to use WAF for HTTPS traffic protection.

### How many intermediate IPs can be set for one protected domain name in WAF?

Up to 20 intermediate IPs can be set for one protected domain name in WAF.

### Does WAF support health check?

Health check is enabled for WAF by default. WAF checks the connection status of all real server IPs. For the real server IP that does not respond, WAF will not forward requests to this IP until its connection status becomes normal.

### Does WAF support session persistence?

WAF supports session persistence. You can submit a ticket to activate this feature.

### How long does it take for configuration changes to take effect in the WAF console?

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

### Is the SSL mutual authentication supported by both the SaaS WAF and CLB WAF?

It is supported by CLB WAF but not by SaaS WAF.

## Domain Name

### 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.

### Will the intermediate IP change?

The intermediate IP address may change due to WAF maintenance and upgrades. You will be notified via SMS, email, or Message Center if it changes. You can view your intermediate IP address in the Domain Name List.

### Will the SaaS WAF-connected VIP address change?

The VIP address may change when WAF is maintaining and upgrading its in/cross-region disaster recovery capabilities. To ensure the service availability, WAF only supports configuring VIP addresses by adding the CNAME.

### Can I modify the SaaS WAF-connected VIP address?

A SaaS WAF-connected VIP address cannot be modified. If the associated domain name fails due to DDoS attacks, you can submit a ticket for assistance.

### 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 logging 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**.