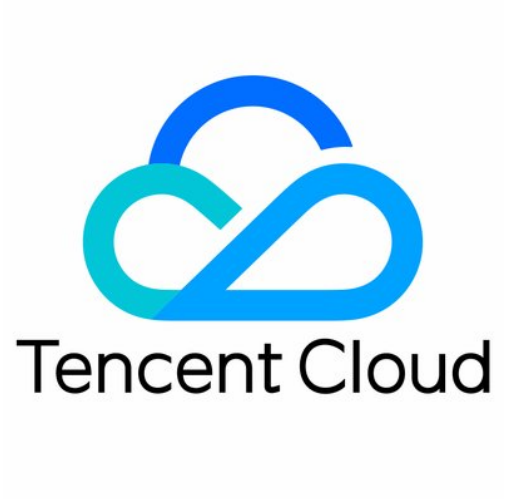
# Web Application Firewall

# Product Introduction

# Product Documentation



# Contents

# Product Introduction
# Overview

Last updated : 2020-09-27 17:08:04

## What is Web Application Firewall?

Tencent Cloud Web Application Firewall (WAF) is an AI-based, one-stop web service protection solution. It uses the AI+ rules dual engine to identify malicious traffic and improve website security and reliability. In addition, it performs BOT behavior analysis to protect against malicious access behaviors and ensure the security of core services and data of websites.
WAF provides SaaS-based WAF and load-balanced WAF. These 2 types provide basically the same security protection capabilities but different access methods.

- SaaS-based WAF resolves a domain name to the CNAME address provided by the WAF cluster through DNS resolution. The IP address of the real server is configured through the WAF service. SaaS-based WAF cleanses and filters out malicious domain name traffic and returns legitimate traffic to the real server to ensure website security.
- Load-balanced WAF works with the Tencent Cloud Load Balancer cluster to mirror load-balanced HTTP/HTTPS traffic to the WAF cluster. WAF performs bypass threat detection and cleansing and then synchronizes the trusted status of user requests to the Tencent Cloud Load Balancer cluster to block threats and pass legitimate requests, helping ensure the security of websites.

The WAF service can effectively prevent SQL injection, cross-site scripting (XSS), trojan upload, unauthorized access, and other OWASP attacks. In addition, it can provide all-round protection for website systems and services by effectively filtering out CC attacks, providing zero-day vulnerability patches, and preventing web page tampering.

## Key features

| Feature | Description |
| --- | --- |
| AI+ web application firewall | With the web attack identification based on AI+ rules, anti-bypass, low false negative, and low false positive, this service can precisely and effectively defend against common web attacks, such as SQL injection, unauthorized access, XSS, cross-site request forgery (CSRF), Webshell |

| | |
|---|---|
| | trojan upload, and other OWASP top 10 web security threats and attacks. |
| Virtual patching for zero-day vulnerabilities | The Tencent security team provides 24/7 monitoring to uncover and respond to vulnerabilities. It distributes virtual patches for high-risk web vulnerabilities and zero-day vulnerabilities within 24 hours upon detection. Protected users can obtain the defense capability against emergency vulnerability and zero-day vulnerability attacks without performing any operation. The response cycle is significantly shortened. |
| Anti-tampering of web pages | Users can cache core web page content to the cloud and publish cached web pages for substitution. This helps to protect organizations against the negative consequences caused by web page tampering. |
| Data leakage prevention | WAF provides ex-ante server application hiding, real-time intrusion prevention, and ex-post sensitive data replacement and hiding policies to prevent backend databases from being hacked. |
| Defense against CC attacks | WAF provides intelligent defense against CC attacks, and performs intelligent decision-making to generate defense policies based on the exceptional responses (timeout and response delay) of the real server and big data analysis of website behaviors. In addition, it provides multi-dimensional, custom, and precise access control, human-machine identification, frequency control, and other countermeasures to efficiently filter out unwanted access and mitigate CC attacks. |
| Crawler BOT behavior management | Based on the AI+ rules repository, WAF provides web page crawler and BOT robot management to help enterprises mitigate business risks caused by malicious BOT behaviors. Business risks include website user data leakage, content infringement, competitive pricing, inventory query, black hat SEO, and business strategy disclosure. |
| 30-line BGP IP access protection | WAF supports dedicated 30-line BGP IP link access for defense nodes. The nodes are scheduled intelligently, which effectively solves the access delay problem and ensures the site access speed of users in all tiers of cities. This helps to deploy imperceptible cloud WAF security protection without affecting the website access speed. |

# Why do we need WAF?

In the following scenarios, the WAF service can provide effective defense and prevention against risks, and ensure system and business security of enterprise websites.

- **Data leakage (leakage of core information assets)**
  For many enterprises, websites are typically used as the entries to information assets. Hackers can steal enterprise information assets by means of web intrusion, resulting in incalculable losses to enterprises.

- **Malicious access and data crawling (data manipulation by opponents causes service unavailable)**
  Hackers use zombie computers to launch CC attacks on the web server. As a result, the resources available are exhausted and the server fails to respond normally. Malicious users capture the core content of websites (literature blogs, recruitment sites, forum sites, and e-commerce site comments) through web crawling. Product details on e-commerce websites are scraped deliberately by competitors for research. Speculators seek for arbitrage by searching for low-price product information or obtaining marketing intelligence in advance.

- **Website malicious code and tampering (affecting the credibility and image)**
  After obtaining permissions of websites or servers, attackers inject malicious code to make users execute malicious programs, to earn traffic, to steal accounts, or to show off. They insert links of illicit content, and tamper with web page images and texts. These behaviors severely influence the operation of websites and impair the image and credibility of website operators.

- **Framework vulnerabilities (frameworks attacked during the patch fixing period)**
  Many web systems are based on common open-source frameworks, such as Structs2, Spring, and WordPress, which often carry security vulnerabilities. It is a tough and dangerous period before patches are ready to use, because many attacks spring up soon after the vulnerabilities are uncovered.

- **Service interruption caused by large traffic DDoS attacks**
  As a cheap and easy-to-use attack means, DDoS attacks are often used to disrupt the business operation of competitors or to make key portals inaccessible, leading to significant impact on business continuity and branding. Operators are often very passive when their websites are attacked.

# Product Category

Last updated : 2020-11-25 19:23:36

## Type Overview

Tencent Cloud provides two types of on-cloud WAF, namely, SaaS WAF and CLB WAF. They have basically the same security protection capabilities but different connection methods and use cases. You can select an appropriate WAF type based on your actual deployment.

| Type | SaaS WAF | CLB WAF |
| --- | --- | --- |
| Use case | It is suitable for all users (Tencent Cloud users and local IDC users) and can be connected through domain names by means of DNS resolution and scheduling. | It is suitable for Tencent Cloud users who are using or plan to use layer-7 CLB. |
| Strengths | It is widely applicable to users in and outside Tencent Cloud. | • Imperceptible connection to WAF with millisecond-level latency is implemented, which does not require adjustment of your existing network architecture.<br>• Website business forwarding and security protection are isolated from each other, and quick bypass is supported, ensuring that your website business is secure, stable, and reliable.<br>• Multi-region connection is supported. |
| How to choose | If you need to protect both Tencent Cloud-hosted and local websites or layer-7 CLB is not used for your Tencent Cloud resources, you are recommended to use SaaS WAF. | If you are using or plan to use layer-7 CLB and have requirements for web security protection, bot behavior management, CCPCS-based protection, or website security operation, you are recommended to use CLB WAF. |

# SaaS WAF

After you add a protected domain name and set the origin-pull information on WAF, it will assign a unique CNAME address to the protected domain name. You can modify the DNS resolution to change the original A record to the CNAME record and schedule traffic to the protected domain name to the WAF cluster, which will detect and block malicious traffic and forward normal traffic to the real server in order to protect your website security.

# CLB WAF

By configuring a domain name, WAF can be connected to a layer-7 CLB (listener) cluster to detect threats in HTTP/HTTPS traffic passing through CLB and cleanse malicious traffic so as to separate business request forwarding from security protection, which minimizes the affect of security protection on your website business and thus ensures stable website operation.
CLB WAF provides two traffic processing modes:

- **Mirror mode**: associated with WAF through a domain name, CLB mirrors traffic to the WAF cluster, which performs bypass detection and alarming but does not return the request credibility status.
- **Cleansing mode**: associated with WAF through a domain name, CLB mirrors traffic to the WAF cluster, which performs bypass detection and alarming and synchronizes the request credibility status. Then, the CLB cluster will block or allow the requests based on their status.

# Advantages

Last updated : 2020-04-22 14:43:30

## Multiple access protection methods

- With no need to modify service configurations, WAF can be directly connected to your service after it is activated. WAF supports quick binding to Tencent Cloud Load Balancer for website bypass detection and threat cleansing. It also provides a quick bypass feature to separate service forwarding from security protection.
- Connecting to WAF by using a CNAME can hide the real server of the user and return trusted traffic to the real server for Tencent Cloud users and non-Tencent Cloud users.
- Protection cluster resources are deployed in multiple regions and can be dynamically scaled based on user demands. This helps to avoid redundancy and single points of failure.

## Protection from the AI+ rules dual engine

- The security rule engine protects your service against the OWASP top 10 attacks, including SQL injection, unauthorized access, cross-site scripting (XSS), cross-site request forgery (CSRF), and command line injection. In addition, WAF introduces AI defense capabilities to enable continuous learning through cross-validation and accurately and effectively capture common web attacks, zero-day attacks, and other new unknown attacks.
- WAF continuously learns the characteristics of massive service data to generate personalized protection strategies based on services and avoid false positives. Users can use the AI engine to handle false positives and false negatives to improve operation efficiency.
- Tencent United Security Laboratory continuously provides security protection capabilities for Tencent Cloud security services, and the protection systems of WAF are continuously upgraded by the dedicated protection team on a 24/7 basis. This ensures your website protection systems remain at the cutting edge of the industry.

## BOT behavior management

- Uses the AI-based behavior analysis engine to track real-time sessions and match behavior models and labels by using traffic portraits to efficiently detect malicious BOT behaviors.
- Provides more than 1,000 disclosed BOT types to quickly establish protection strategies.
- Provides crawler and IP intelligence features to quickly identify BOT behaviors.

- Provides protocol features and more than 50 session features to define protection strategies for multiple business scenarios.
- Provides detailed reports and statistics of known, unknown, and custom types of BOT behaviors to quickly identify and prevent malicious BOT behaviors and secure website services.

## Intelligent protection against CC attacks

- Performs intelligent decision-making based on the exceptional real server responses (timeout and response delay) and historical website access data to generate defense policies and block attack sources and high-frequency access requests in real time.
- Supports custom sessions to defend against CC attacks at the session level. This feature helps to achieve more accurate protection against CC attacks and reduce false positives.
- Views CC-blocked IP addresses in real time to quickly adjust protection policies as needed.
- Provides 100-GB anti-DDoS capabilities and supports seamless quick connection to your service to defend against large traffic DDoS attacks and avoid sudden risks.

## IPv6 security protection

- Uses NAT64 instances on the cloud to provide protected IPv6 access to websites without reconstructing IPv4 sites.
- Works with Tencent Cloud Load Balancer to seamlessly process IPv4 and IPv6 access traffic with the same security protection capabilities.

# Scenarios

Last updated : 2020-05-12 17:07:32

### Government website protection

WAF can be accessed with one click, and configured with ease. It can hide and protect origin servers, and prevent the website content from being stolen and tampered by hackers, ensuring correct website information, availability of government services, and satisfied and smooth public access.

### E-commerce website protection

- WAF provides continuous optimization of protection rules, precise blocking of Web attacks, and all-round protection against OWASP Top 10 Web application risks.
- In case of highly concurrent purchases, it can intelligently filter malicious attacks and junk access to ensure smooth access to businesses.

### Financial website protection

- WAF can be accessed with one click, and integrates with the large-traffic DDoS defense, and also provides web security protection.
- WAF can effectively monitor DNS linkage hijacking to avoid malicious directing of website traffic.
- WAF can effectively detect exceptional access like account credential enumeration attack to avoid user information leakage.
- With cloud resources and automatic scaling capability, WAF can easily deal with sudden business growth and large-traffic CC attacks.

### Data leakage prevention

- WAF can avoid website core data leakage caused by hacker injection and intrusion attacks.
- CC attack protection: protection against malicious CC (HTTPFlood) attacks. WAF can ensure website availability by blocking massive malicious requests on layer 4 and layer 7.

# Supported Regions

Last updated : 2020-12-15 15:20:26

You can select a WAF type and region according to the deployment method and region of your business. WAF currently supports service in the following regions:

| WAF Type | Supported Regions |
| --- | --- |
| SaaS WAF | • South China: Guangzhou<br>• East China: Shanghai<br>• North China: Beijing<br>• Southwest China: Chengdu<br>• Hong Kong (China) |
| CLB WAF | • South China: Guangzhou<br>• East China: Shanghai, Nanjing, Shanghai Finance<br>• North China: Beijing<br>• Southwest China: Chengdu, Chongqing<br>• Hong Kong (China)<br>• Southeast Asia: Singapore, Bangkok<br>• South Asia: Mumbai<br>• Northeast Asia: Seoul, Tokyo<br>• Europe: Frankfurt, Moscow<br>• North America: Silicon Valley |

**Note :**

- More supported regions are coming soon. For region updates, please see WAF console.
- CLB WAF supports binding IPv6 CLB instances to protect IPv6 websites. If you want to use IPv6 web protection, please make sure that the selected region supports IPv6 CLB instances and IPv6 web deployment has been completed.
- IPv6 CLB instances currently support main regions. The supported regions are subject to the ones on the CLB purchase page.

# Basic Concepts

Last updated : 2020-12-17 17:34:33

## SSL Certificate

Secure Sockets Layer (SSL) is a security protocol designed to ensure the security and data integrity of internet communication. Based on the SSL protocol, an SSL certificate can be installed on a server to achieve encrypted data transmission.

## Domain Name Resolution

Servers on the internet communicate with each other through IP addresses. However, most people are used to remembering a domain name that can be mapped to multiple IP addresses. The conversion between a domain name and an IP address is called domain name resolution.
The following are common domain name resolution types:

- A record resolution: it specifies the IPv4 address of the domain name.
- Select "A" as the record type.
- Enter the server IP address provided by Tencent Cloud as the record value.
- MX priority does not need to be configured.
- Set TTL to 600 by default.
- CNAME record resolution: it is used to point a domain name to another one which will be used to provide the IP address.
- Select "CNAME" as the record type.
- Enter the CNAME record generated after the protected domain name is added to WAF as the record value.
- MX priority does not need to be configured.
- Set TTL to 600 by default.

## Security Group

A security group is a virtual firewall that features stateful data packet filtering. It is used to configure the network access control of CVM instances. You can add CVM instances with the same network security isolation requirements in the same region to the same security group to filter their inbound and outbound traffic through the network policies of the security group.

## QPS

Queries per second (QPS) is a metric measuring how much traffic is processed by a particular query server within the specified time period. On the internet, the performance of DNS servers is often measured with QPS, which corresponds to fetches/sec (responded requests per second, i.e., the maximum throughput).

## Intermediate IP Address

After you add a domain name, WAF will automatically allocate multiple intermediate IP addresses to it accordingly, which can be used as the egress IPs of WAF to forward filtered normal traffic to your real server.

## CC Attack Protection

Challenge Collapsar (CC) attack protection refers to a protection service against CC attacks where attackers use certain tools to simulate multiple users in order to continuously send connection requests to your website and make your business unavailable. You can add CC protection rules to defend against CC attacks for webpage requests.

## Anti-Tampering

Anti-Tampering refers to a mechanism where core webpages can be cached to the cloud and those in the cache can be published instead to realize the effect of webpage substitution. When the core webpages receive requests, content stored in cloud will be returned.

## Anti-Leakage

Anti-Leakage refers to a mechanism where the responding webpages are checked for sensitive information such as ID and phone numbers and any sensitive information detected will be observed or replaced with asterisks (*) according to the preset match behaviors, which helps avoid leakage of sensitive information.

## Region Blocking

Region blocking refers to a mechanism that determines the region of an attacking IP and blocks access requests from all IPs in the specific region in order to quickly block attacks.

## AI engine

Artificial Intelligence (AI) engine refers to a technology used in WAF to detect web attacks based on machine learning. With its self-learning, self-evolvement, and adaptation capabilities, it can maximize the detection rate and capture rate for known and unknown threats, minimize false positives, and flexibly adapt to ever-changing web applications.