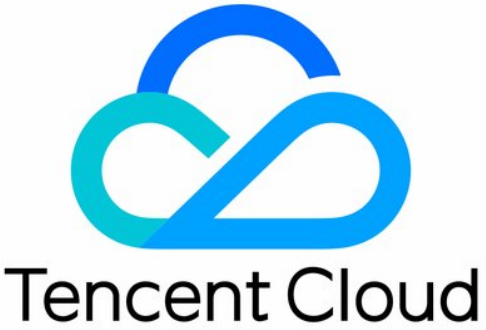
# Web Application Firewall
# Product Introduction



## Copyright Notice



## Trademark Notice



## Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

## Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

# Contents

# Product Introduction
# Overview

Last updated: 2024-10-24 20:55:19

## What is a Web Application Firewall

Web Application Firewall (WAF) is a one-stop AI-based risk prevention solution for web business operations. It can identify malicious traffic with the aid of AI and rule engines to protect websites and further improve the website security and reliability. By leveraging bot behavior analysis, it can defend against malicious access requests and safeguard core website businesses and data.
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.

- SaaS-based WAF resolves the domain to the CNAME address provided by the WAF cluster via DNS resolution. By configuring the origin server IP through WAF, malicious traffic targeting the domain is cleansed and filtered, and normal traffic is pulled to the origin server to protect the security of the website.
- CLB WAF works with the Tencent Cloud CLB cluster to mirror the HTTP/HTTPS traffic of CLB instances to the WAF cluster. Then, WAF performs bypass threat detection and cleansing and syncs the trusted status of user requests to the CLB cluster, which will block or allow the requests accordingly to protect the website security.

WAF can effectively prevent SQL injection, cross-site scripting (XSS), trojan upload, unauthorized access, and other OWASP attacks. In addition, it can also provide all-around protection for website systems and businesses by effectively filtering CC attacks, providing zero-day vulnerability patches, and preventing webpage tampering.

## Main Feature

| Features | Introduction |
| --- | --- |
| AI + Web Application Firewall | AI + Rules Web is characterized by its ability to accurately identify attacks, prevent bypass attempts, minimize missed reports and false positives, and provide effective defense against a wide range of common Web attacks, such as SQL injection, unauthorized access, XSS cross-site scripting, CSRF cross-site request forgery, Webshell Trojan upload and other top ten Web security threat attacks defined by OWASP |
| 0day Vulnerability | Tencent Security Team provides 24/7 monitoring, proactively discovers and responds, issues high-risk Web vulnerabilities within |

| | |
|---|---|
| Virtual Patching | 24 hours, 0day vulnerability protection with virtual patches, no action required from protected users to obtain emergency security patches, 0day attack prevention capabilities, significantly reducing the vulnerability response cycle |
| Webpage anti-tampering | Users can set up cloud caching of core web page content and publish cached web page content to achieve web page replacement effect, preventing web page tampering from bringing negative impact to the organization |
| Data Leakage Prevention | Prevent backend database from being stolen by hackers through server application hiding beforehand, intrusion protection during the process, and sensitive data replacement hiding policy afterward |
| CC Attack Prevention | Intelligent CC Protection, based on comprehensive analysis of origin server abnormal responses (timeouts, response delays) and big data analysis of website behavior, generates defense strategies through intelligent decision-making. It employs multi-dimensional Customized Precise Access Control, combining CAPTCHA and Frequency Control to effectively filter junk access and mitigate CC attack issues |
| Crawler and BOT behavior management | With AI-based rule engine and rule library, this feature manages web crawlers and BOTs to help prevent user data leakage, content infringement, competition-based pricing, inventory query, black hat SEO, business strategy disclosure, and other business risks caused by malicious BOT behavior |
| API Security | Refers to measures to protect Application Programming Interfaces (APIs) from malicious attacks or abuse, automatically discovering APIs in business access through proactive learning. It helps users quickly identify and classify known and unknown API assets, creating an API profile list. Additionally, based on threat detection and data identification engines, it provides attack protection, impersonation protection, abuse protection, and data protection capabilities |
| 30 BGP lines for access protection | WAF supports protection with 30 dedicated BGP IP link access nodes. Intelligent scheduling of nodes effectively solves access latency issues, ensuring the site access speed for users in different cities. It enables a seamless security protection deployment with Cloud WAF, making the impact on website access speed unnoticeable |

## Why do you need a Web Application Firewall

In the following scenarios, WAF can effectively defend and prevent, ensuring the system and business security of the enterprise website.

- **Data leakage (leakage of core information assets)**
  Web sites are the entrance to corporate information assets. Hackers can steal corporate information assets through Web intrusions, causing immeasurable losses to the companies.
- **Malicious access and data scraping (Unable to serve normally, data exploited by business competitors)**
  Hackers control botnets to launch CC attacks on Web sites, exhausting resources and hindering normal service. Malicious users use web crawlers to scrape the core content of websites (literature blogs, recruitment websites, forum websites, comments within e-commerce) E-commerce websites are deliberately crawled by competitors to study product details. Bargain hunters attempt to search for low-priced product information or gain intelligence before major marketing promotions to find arbitrage opportunities.
- **Websites defaced and tampered with (Affecting website operation and image)**
  After obtaining Web site or server permissions, attackers insert malicious code to cause users to execute malicious programs, earn traffic, steal accounts, show off skills, etc.; implant "pornography, gambling, illegal" links; tamper with webpage images and text; greatly affect the operation of the website, damaging the website operator's image.
- **Framework vulnerability (attacks during patching)**
  Many web systems are based on common open-source frameworks such as Structs2, Spring, and WordPress, which often have security vulnerabilities. The patching period is a difficult and dangerous time as many attacks will emerge just one day after the vulnerabilities are disclosed.
- **CC attack (business interruption and consuming server resources)**
  In an attempt to disrupt business operations or make key portal websites inaccessible, CC attacks have become a low-cost and low-barrier method. Attackers often flood business servers with large amounts of data packets, causing resource occupation to soar and a sudden increase in request quantity, thereby blocking normal website access or even causing downtime. This greatly affects business continuity and brand reputation, leaving operators in a passive position when under attack.

# Product Classification

Last updated: 2024-10-24 20:56:01

## Type Overview

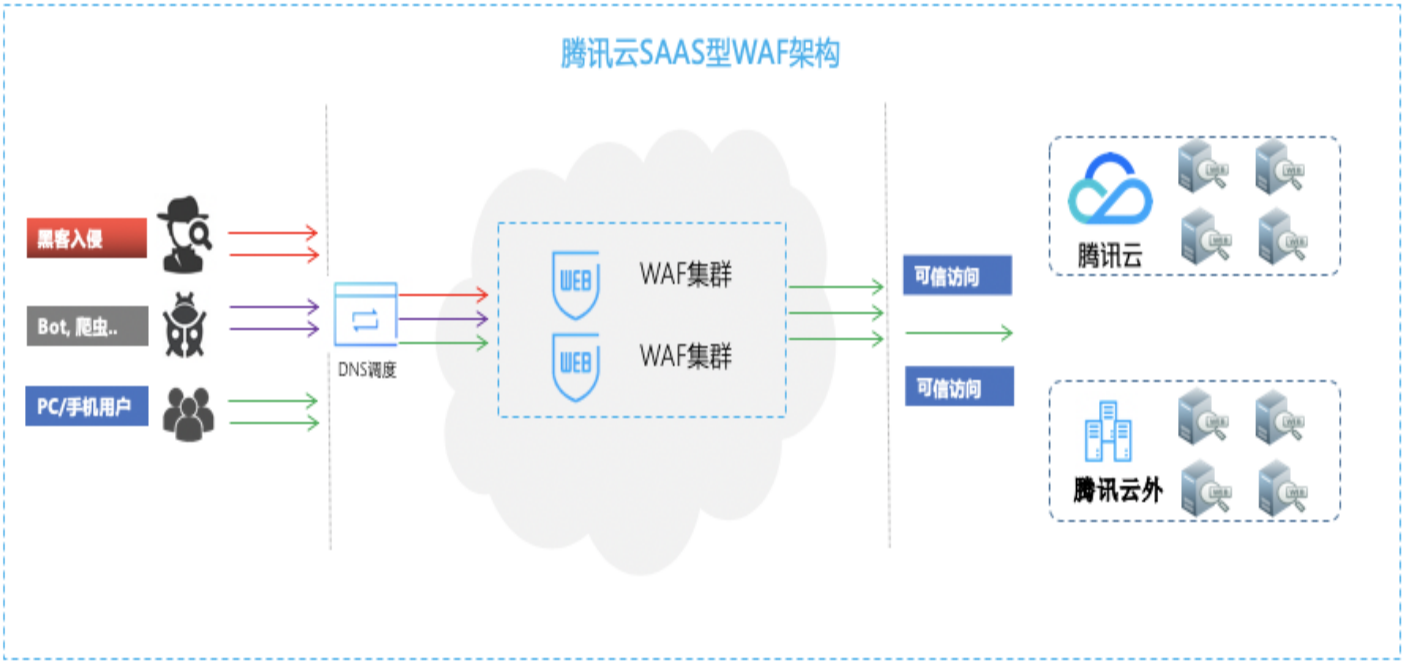
Tencent Cloud offers two types of cloud-based WAFs: SaaS-type WAF and CLB-type WAF. Both WAFs have similar security protection capabilities but differ in connection methods and use cases. You can choose the type of WAF based on your actual deployment requirements.

| Category | SaaS-type | CLB-Based |
| --- | --- | --- |
| Applicable Scenario | Suitable for all users (Tencent Cloud users or local IDC users), domain access is achieved through DNS resolution scheduling. | Users on Tencent Cloud who are using or planning to use Layer 7 CLB. |
| Core Strength | The wide application scope covers both Tencent Cloud users and non-Tencent Cloud users. | • Seamless access with millisecond latency; domain access to WAF requires no changes to the existing network architecture.<br>• Website traffic forwarding and security protection are separated; one-click bypass ensures website business security, stable and reliable.<br>• Supports multi-region access. |
| How to Choose | • If the user has websites on both Tencent Cloud and locally that need protection, or if layer-7 CLB is not used on Tencent Cloud, we recommend using SaaS-type WAF.<br>• If you need to use the web page tamper proofing and data leakage prevention features, only the SaaS-type WAF can support them. | For users on Tencent Cloud who are using or planning to use layer-7 CLB, and have web security protection, BOT traffic management, Cybersecurity Classified Protection Compliance Service protection, or website security operation needs, we recommend using CLB type WAF. |

| | | |
|---|---|---|
| Selecting Region | When purchasing the SaaS-type WAF, you need to select the corresponding region. | Purchasing a CLB-based WAF does not require selecting a region; after purchase, you can associate it with the supported region of the CLB when configuring in the console. |

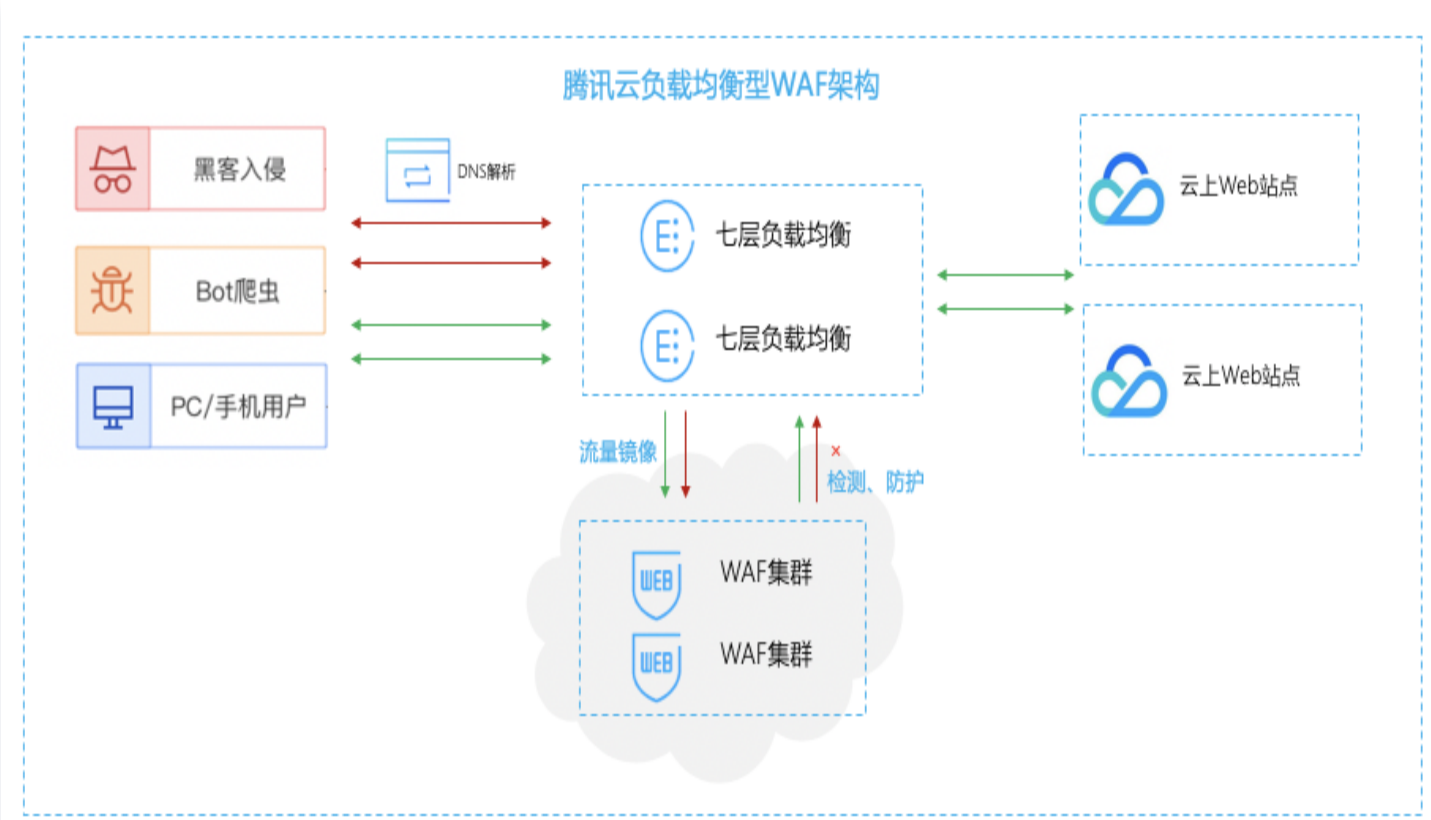
## SaaS-based WAF

After a user adds a protected domain and sets the origin information on WAF, WAF allocates a unique CNAME address for the protected domain. The user can modify DNS resolution, changing the original A Record to a CNAME Record, and direct the protected domain traffic to the WAF Cluster. The WAF Cluster carries out malicious traffic detection and protection for the protected domain and routes the normal traffic back to the origin server, ensuring website security.



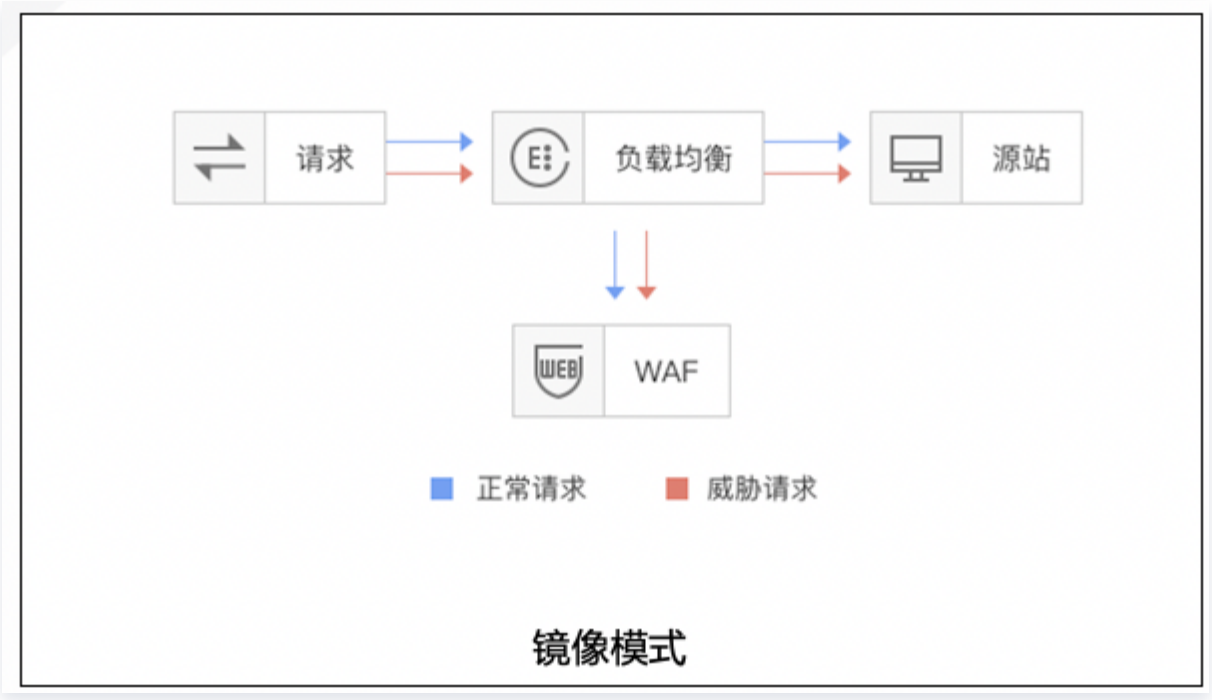

## Cloud Load Balancer (CLB) WAF

WAF integrates with the domain and Tencent Cloud Layer-7 CLB (Listener) Cluster to perform bypass threat detection and cleansing on HTTP/HTTPS traffic processed by the CLB, achieving business forwarding and security separation. This minimizes the impact of security protection on website operations, ensuring stable website performance.



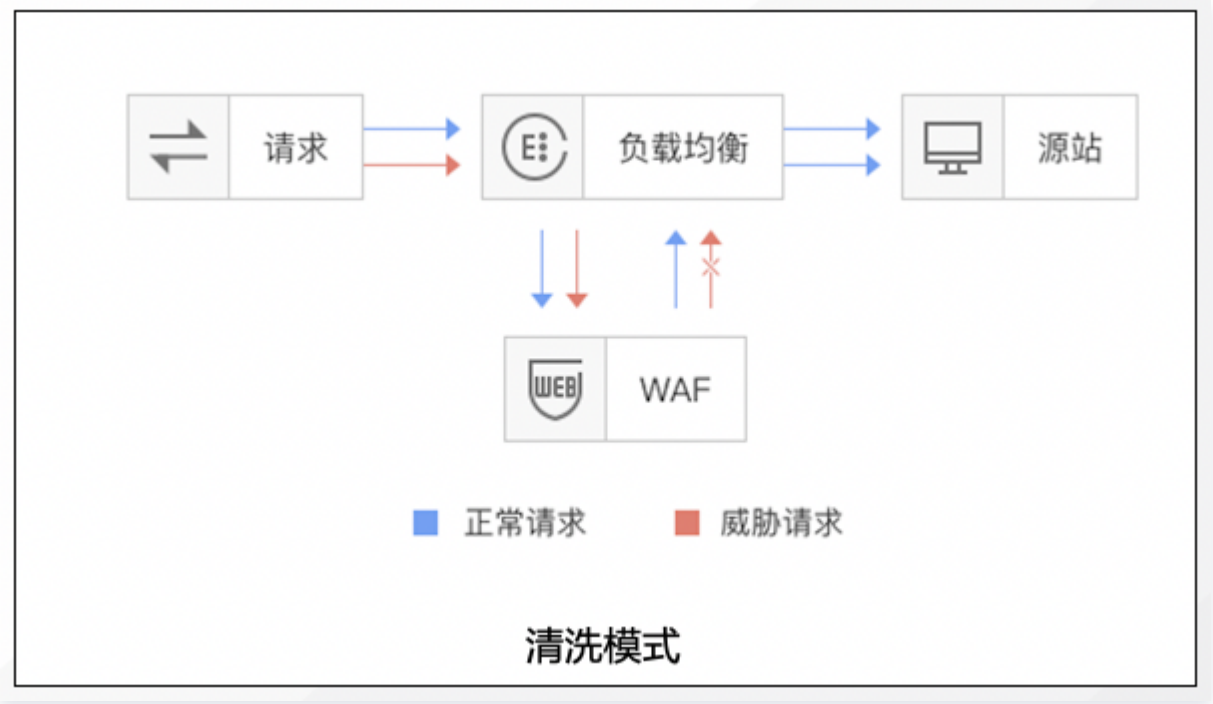

The CLB-based WAF provides two traffic processing modes:

- **Mirror mode**: Associated via domain, CLB mirrors traffic to the WAF Cluster, which performs bypass detection and alarm but does not return the trusted request status.




- **Cleaning mode**: Associated via domain, CLB mirrors traffic to the WAF Cluster, which performs bypass detection and alarm while synchronizing the trusted request status. The

CLB Cluster intercepts or bypasses requests based on this status.



# Advantages

Last updated: 2024-10-24 20:56:22

## Multiple Methods of Connecting to Protection

- Layer 7 CLB can access WAF without any business changes, providing one-click binding to Tencent Cloud CLB to enable exact domain web traffic bypass detection and threat cleansing; also offering the one-click Bypass feature and timeout automatic Bypass feature to achieve business forwarding and security separation, with high stability and high reliability.
- Layer 7 CLB can access WAF, supporting one-click activation of CLB instance object protection. Based on exact domain access protection, it offers default traffic policy management, providing a high-security, reliable, and comprehensive Web protection solution.
- Supports access to WAF services through CNAME, hiding your real server and forwarding trusted traffic to the real server for Tencent Cloud and non-Tencent Cloud users.
- Protection cluster resources are deployed in multiple locations, dynamically expanded, and used on demand to avoid redundancy and single points of failure.

## AI + Rule Dual-engine Protection

- The security rule engine protects your business against the OWASP top 10 attacks, including SQL injection, unauthorized access, cross-site scripting (XSS), cross-site request forgery (CSRF), and command line injection. WAF is also powered with 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.
- Personalized protection policies are generated through continuous learning of the features of massive business data to avoid false alarms. Users have the ability to manage false alarms and missed alarms through a self-service feature powered by AI, which enhances operational efficiency.
- Tencent United Security Laboratory provides outstanding security protection capabilities for Tencent Cloud. WAF's protection systems are continuously upgraded by the dedicated protection team 24/7, building up cutting-edge protection systems for your website.

## Bot Traffic Management

- With the AI-based behavior analysis engine, this feature realizes real-time session tracking, and efficient detection of malicious bots based on the matching of behavior models and behavior labels by using traffic profile.

- Provides more than 1,000 known bot types to quickly set up protection policies.
- Provides crawler and IP intelligence features to quickly identify bot behaviors.
- Provides features of protocols and over 50 session characteristics to define protection policies for various business scenarios.
- Provides detailed reports and statistics of known, unknown and custom bot types to quickly locate malicious bots and defend your website against them.

## Intelligent CC Protection

- Intelligently generates and applies protection policies to defeat attacks and blocks high-frequency access requests in real time to block attacker IPs based on the real server's abnormal response such as timeout and response latency, and historical data of website access.
- You can customize the session and perform CC protection through the session dimension to more accurately protect against CC attacks and reduce false positives.
- You can monitor the real-time status of IP addresses being blocked by the CC feature and make necessary adjustments to the protection policy promptly.

## IPv6 Security Protection

By integrating with Tencent Cloud CLB, seamlessly handle IPv4 and IPv6 access traffic, providing equal security protection capabilities simply and efficiently.

# Use Cases

Last updated: 2024-10-24 20:56:48

## Government Website Protection

One-click access defense, easy to configure, hide and protect the origin server, ensuring the website content is not tampered with by hacker intrusions. Guarantee the accuracy of website information, normal availability of government services, and satisfactory smoothness of public access.

## E-commerce Website Protection

- Continuously optimize protection rules, accurately intercept Web attacks, and comprehensively defend against OWASP Top 10 Web application risks.
- In high-concurrency rush-buying scenarios, malicious attacks and junk access can be intelligently filtered to ensure smooth and uninterrupted access to normal services.

## Financial Website Protection

- Connect to protection with one click can be organically combined with large-volume DDoS defense to provide Web security protection.
- Exception access, such as database collisions, can be effectively detected to safeguard user information from potential leaks.
- The strengths of cloud resources and automatic scaling make it easy to handle business emergencies and large-scale CC attacks.

## Data Leakage Prevention

- Core website data leakage from injection intrusion attacks by hackers will be avoided.
- 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.

# Plans and Editions

Last updated: 2024-10-24 20:57:10

WAF (Web Application Firewall, abbreviated as WAF) supports two payment models: annual and monthly prepaid, as well as annual and monthly prepaid plus elastic postpaid. Instance types are divided into SaaS model and CLB model. This article introduces the features supported by different instances and package versions of WAF.

## SaaS WAF instance (Chinese mainland region)

| Classify | Category | Advanced Edition | Enterprise Edition | Flagship Edition |
|---|---|---|---|---|
| Package Basic Information | Applicable Scenario | Standard protection for small and medium non-business websites. | Customized protection services for small to medium general business sites and large official websites. | Customized protection services for large and extra-large business websites and complex business sites. |
| | QPS Peak<br>Note: If you need customized specifications, please contact your business manager or architect. | • Default package QPS: 2,500 QPS<br>• Supports business expansion package to extend QPS: 20,000 QPS<br>• Supports elastic postpaid to extend QPS: 100,000 QPS | • Default package QPS: 5,000 QPS<br>• Supports business expansion package to extend QPS: 30,000 QPS<br>• Supports elastic postpaid to extend QPS: 150,000 QPS | • Default package QPS: 10,000 QPS<br>• Supports Business Extension Package to Extend QPS: 40,000 QPS<br>• Supports Elastic Postpaid Extension QPS: 200,000 QPS |
| | Bandwidth cap<br>Note: If you need customized | • Package Default Bandwidth: 50 Mbps<br>• Supports Business | • Package Default Bandwidth: 100 Mbps<br>• Supports Business | • Package Default Bandwidth: 200 Mbps<br>• Supports Business |

| | | | | |
|---|---|---|---|---|
| | specifications, please contact your account manager or architect. | Extension Package to Extend Bandwidth: 500 Mbps | Extension Package to Extend Bandwidth: 750 Mbps | Extension Package to Extend Bandwidth: 1,000 Mbps |
| | Dedicated IP | Supported | Supported | Supported |
| | Number of Supported Primary Domains | 2 | 3 | 4 |
| | Number of Total Supported Domains (including primary domains and their subdomains) | 20 | 30 | 40 |
| | Wildcard Domain Protection | Not supported. | Supported | Supported |
| | IPv6 Protection | Not supported. | Supported | Supported |
| Access Manage | Supported Access Ports | Supports standard ports 80, 8080, 443, 8443 | In addition to standard ports, protection is provided for services on specific non-standard ports, up to 5 per domain/protocol type | In addition to standard ports, protection is provided for services on specific non-standard ports, up to 10 per domain/protocol type |

| | | | | |
|---|---|---|---|---|
| ment | Dedicated IP | Supported | Supported | Supported |
| | Traffic Tagging | Not supported. | Supported | Supported |
| | Client Information Transmission | Not supported. | Supported | Supported |
| | HTTP2/WebSocket | Supported | Supported | Supported |
| Basic Security Protection | Rule Protection Engine | Supported | Supported | Supported |
| | 0Day Vulnerability Virtual Patching | Supported | Supported | Supported |
| | Precise allowlist | 20 entries/domain | 40 entries/domain | 100 entries/domain |
| | Rule Allowlist | 200 entries/domain | 400 entries/domain | 500 entries/domain |
| | IP Blocklist and Allowlist | 1000 entries/domain | 5000 entries/domain | 20000 entries/domain |
| | Origin return concurrent long connections | No limit | No limit | No limit |
| | Regional block | Supported | Supported | Supported |
| | Access Control | 10 entries/domain | 20 entries/domain | 50 entries/domain |

| | | | | |
|---|---|---|---|---|
| | (self-defined policy) | | | |
| | Emergency mode CC Protection | Supported | Supported | Supported |
| | Self-defined CC Protection based on IP/Session | 5 entries/domain | 20 entries/domain | 50 entries/domain |
| | Data Leakage Prevention | 5 entries/domain | 10 entries/domain | 20 entries/domain |
| | Webpage anti-tampering | 10 entries/domain | 20 entries/domain | 50 entries/domain |
| | Batch Protection | Not supported. | Supported | Supported |
| | Advanced Vulnerability Protection feature (AI Engine) | Not supported. | Not supported. | Supported |
| Advanced Security Val | BOT Traffic Management | Paid Support | Paid Support | Paid Support |

| | | | | |
|---|---|---|---|---|
| ue-added Protection | API Security | Paid Support | Paid Support | Paid Support |
| | Business Security | Paid Support | Paid Support | Paid Support |
| LogManagement | Attack Log Query and Download | Supported | Supported | Supported |
| | Attack Log Delivery | Not supported. | Supported | Supported |
| | Storage of Attack Logs for All Attack Types | Supported | Supported | Supported |
| | Access Log Delivery | Paid Support | Paid Support | Paid Support |
| | Access Log Query and Download (Log package purchase required) | Supported | Supported | Supported |
| Professio | One-on-One Pre-sales | Not supported. | Supported | Supported |

| | | | | |
|---|---|---|---|---|
| nal Service | Support Service | | | |
| | WeChat or WeCom Support | 5*8 hours | 7*12 hours | 7*12 hours |
| | 7*24 hours Ticket-based Pre-sales and After-sales Support | Supported | Supported | Supported |

## SaaS WAF Instance (Non-Chinese mainland Regions)

| Classify | Category | Advanced Edition | Enterprise Edition | Flagship Edition |
|---|---|---|---|---|
| Package Basic Information | Applicable Scenario | Standard protection for small and medium non-business websites. | Custom Protection Service for Small and Medium-sized Ordinary Business Sites and Medium and Large-sized Official Websites | Custom Protection Service for Large and Extra-large Business Websites and Complex Business Sites |
| | QPS Peak Note: For custom specifications, please contact the business manager or architect. | • Default package QPS: 2,500 QPS<br>• Supports business expansion package to extend QPS: 5,000 QPS | • Default package QPS: 5,000 QPS<br>• Supports business expansion package to extend QPS: 10,000 QPS | • Default package QPS: 10,000 QPS<br>• Supports business expansion package to extend QPS: 20,000 QPS |
| | Bandwidth cap Note: For custom | • Package Default Bandwidth: 50 Mbps | • Package Default Bandwidth: 100 Mbps | • Package Default Bandwidth: 200 Mbps |

| | | | | |
|---|---|---|---|---|
| | specifications, please contact the business manager or architect. | • Supports business expansion package to extend bandwidth: 125 Mbps | • Supports business expansion package to extend bandwidth: 250 Mbps | • Supports Business Extension Package to Extend Bandwidth: 500 Mbps |
| | Dedicated IP | Supported | Supported | Supported |
| | Number of Supported Primary Domains | 2 | 3 | 4 |
| | Number of Total Supported Domains (including primary domains and their subdomains) | 20 | 30 | 40 |
| | Wildcard Domain Protection | Not supported. | Supported | Supported |
| | IPv6 Protection | Not supported. | Supported | Supported |
| Access Management | Supported Access Ports | Supports standard ports 80, 8080, 443, 8443 | In addition to standard ports, protection is provided for services on specific non-standard ports, up to 5 per domain/protocol type | In addition to standard ports, protection is provided for services on specific non-standard ports, up to 10 per domain/protocol type |
| | Dedicated | Supported | Supported | Supported |

| | | | | |
|---|---|---|---|---|
| ent | IP | | | |
| | Traffic Tagging | Not supported. | Supported | Supported |
| | Client Information Transmission | Not supported. | Supported | Supported |
| | HTTP2/WebSocket | Supported | Supported | Supported |
| Basic Security Protection | Rule Protection Engine | Supported | Supported | Supported |
| | 0Day Vulnerability Virtual Patching | Supported | Supported | Supported |
| | Precise allowlist | 20 entries/domain | 40 entries/domain | 100 entries/domain |
| | Rule Allowlist | 200 entries/domain | 400 entries/domain | 500 entries/domain |
| | IP Blocklist and Allowlist | 1000 entries/domain | 5000 entries/domain | 20000 entries/domain |
| | Regional block | Supported | Supported | Supported |
| | Access Control (self-defined policy) | 10 entries/domain | 20 entries/domain | 50 entries/domain |
| | Emergency mode CC Protection | Supported | Supported | Supported |
| | Self-defined CC Protection | 5 entries/domain | 20 entries/domain | 50 entries/domain |

| | | | | |
|---|---|---|---|---|
| | based on IP/Session | | | |
| | Data Leakage Prevention | 5 entries/domain | 10 entries/domain | 20 entries/domain |
| | Webpage anti-tampering | 10 entries/domain | 20 entries/domain | 50 entries/domain |
| | Batch Protection | Not supported. | Supported | Supported |
| | Advanced Vulnerability Protection feature (AI Engine) | Not supported. | Not supported. | Not supported. |
| Advanced Security Value-added Pr | BOT Traffic Management | Paid Support | Paid Support | Paid Support |
| | API Security | Paid Support | Paid Support | Paid Support |
| | Business Security | Paid Support | Paid Support | Paid Support |

| | | | | |
|---|---|---|---|---|
| otection | | | | |
| Log Management | Attack Log Query and Download | Supported | Supported | Supported |
| | Attack Log Delivery | Not supported. | Supported | Supported |
| | Storage of Attack Logs for All Attack Types | Supported | Supported | Supported |
| | Access Log Delivery | Paid Support | Paid Support | Paid Support |
| | Access Log Query and Download (Log package purchase required) | Supported | Supported | Supported |
| Professional Service | One-on-One Pre-sales Support Service | Not supported. | Supported | Supported |
| | WeChat or WeCom Support | 5*8 hours | 7*12 hours | 7*12 hours |
| | 7*24 hours Ticket-based Pre-sales and After-sales Support | Supported | Supported | Supported |

## CLB-based WAF Instance (Chinese mainland region)

| Classify | Category | Advanced Edition | Enterprise Edition | Flagship Edition |
|---|---|---|---|---|
| Package Basic Information | Applicable Scenario | Standard protection for small and medium-sized non-business websites | Customized protection services for small and medium-sized regular business sites and medium to large official websites. | Customized protection services for large and extra-large business websites and complex business sites. |
| | QPS Peak Value<br>Note: If you need customized specifications, please contact your account manager or architect. | • Default package QPS: 2,500 QPS<br>• Business expansion package supports QPS expansion up to 40,000 QPS<br>• Elastic postpaid expansion supports QPS up to 200,000 QPS | • Default package QPS: 5,000 QPS<br>• Business expansion package supports QPS expansion up to 60,000 QPS<br>• Elastic postpaid expansion supports QPS up to 300,000 QPS | • Default QPS in package: 10,000 QPS<br>• Business expansion package supports QPS expansion up to 80,000 QPS<br>• Elastic postpaid expansion supports QPS up to 400,000 QPS |
| | **Cross-Regional Joint Support** | **Not supported** | **Not supported** | **Supports 10 regions** |
| | Number of bound CLB Listeners | 200 | 300 | 500 |
| | Number of Supported Primary Domains | 2 | 3 | 4 |
| | Total number of | 20 | 30 | 40 |

| | | | | |
|---|---|---|---|---|
| | supported domains (including protected primary domains and their subdomains) | | | |
| | Wildcard domain name support | Not supported. | Supported | Supported |
| | IPv6 Protection | Supported | Supported | Supported |
| Access Management | Object Connection | Not supported. | Supported | Supported |
| Basic Security Protection | Rule Protection Engine | Supported | Supported | Supported |
| | 0Day Vulnerability Virtual Patching | Supported | Supported | Supported |
| | Precise allowlist | 20 entries/domain | 40 entries/domain | 100 entries/domain |
| | Rule | 200 entries/domain | 400 entries/domain | 500 entries/domain |

| | | | | |
|---|---|---|---|---|
| ction | Allowlist | | | |
| | IP Blocklist and Allowlist | 1000 entries/domain | 5000 entries/domain | 20000 entries/domain |
| | Regional block | Supported | Supported | Supported |
| | Access Control (self-defined policy) | 10 entries/domain | 20 entries/domain | 50 entries/domain |
| | Self-defined CC Protection based on IP/Session | 5 entries/domain | 20 entries/domain | 50 entries/domain |
| | Batch Protection | Not supported. | Supported | Supported |
| | Advanced Vulnerability Protection feature (AI Engine) | Not supported. | Not supported. | Supported |
| Advanced Security Val | BOT Traffic Management | Paid Support | Paid Support | Paid Support |

| | | | | |
|---|---|---|---|---|
| ue-added Protection | | | | |
| | API Security | Paid Support | Paid Support | Paid Support |
| Log Management | Attack Log Query and Download | Supported | Supported | Supported |
| | Attack Log Delivery | Not supported. | Supported | Supported |
| | Storage of Attack Logs for All Attack Types | Supported | Supported | Supported |
| | Access Log Delivery | Paid Support | Paid Support | Paid Support |
| | Access Log Query and Download (Log package purchase required) | Supported | Supported | Supported |
| Professional S | Two-way Certificate Authentication | Supported | Supported | Supported |
| | One-on-One Pre-sales | Not supported. | Supported | Supported |

| | | | | |
|---|---|---|---|---|
| ervice | Support Service | | | |
| | WeChat or WeCom Support | 5*8 hours | 7*12 hours | 7*12 hours |
| | 7*24 hours Ticket-based Pre-sales and After-sales Support | Supported | Supported | Supported |

## CLB Type WAF Instance (Non-Chinese Mainland Regions)

| Classify | Category | Advanced Edition | Enterprise Edition | Flagship Edition |
|---|---|---|---|---|
| Package Basic Information | Applicable Scenario | Standard protection for small and medium-sized non-business websites | Customized protection services for small and medium-sized regular business sites and medium to large official websites. | Customized protection services for large and extra-large business websites and complex business sites. |
| | QPS Peak Value Note: For custom specifications, please contact the business manager or architect. | • Default package QPS: 2,500 QPS<br>• Supports business expansion package to extend QPS: 10,000 QPS | • Default package QPS: 5,000 QPS<br>• Supports business expansion package to extend QPS: 20,000 QPS | • Default QPS in package: 10,000 QPS<br>• Business expansion package supports QPS expansion up to 40,000 QPS |
| | **Cross-Regional Joint Support** | **Not supported** | **Not supported** | **Supports 10 regions** |

| | | | | |
|---|---|---|---|---|
| | Number of bound CLB Listeners | 200 | 300 | 500 |
| | Number of Supported Primary Domains | 2 | 3 | 4 |
| | Total number of supported domains (including protected primary domains and their subdomains) | 20 | 30 | 40 |
| | Wildcard domain name support | Not supported. | Supported | Supported |
| | IPv6 Protection | Supported | Supported | Supported |
| AccessManagement | Object Connection | Not supported. | Supported | Supported |
| Ba | Rule Protection | Supported | Supported | Supported |

| | | | | |
|---|---|---|---|---|
| sic Security Protection | Engine | | | |
| | 0Day Vulnerability Virtual Patching | Supported | Supported | Supported |
| | Precise allowlist | 20 entries/domain | 40 entries/domain | 100 entries/domain |
| | Rule Allowlist | 200 entries/domain | 400 entries/domain | 500 entries/domain |
| | IP Blocklist and Allowlist | 1000 entries/domain | 5000 entries/domain | 20000 entries/domain |
| | Regional block | Supported | Supported | Supported |
| | Access Control (self-defined policy) | 10 entries/domain | 20 entries/domain | 50 entries/domain |
| | Self-defined CC Protection based on IP/Session | 5 entries/domain | 20 entries/domain | 50 entries/domain |
| | Batch Protection | Not supported. | Supported | Supported |
| | Advanced Vulnerability Protection feature (AI Engine) | Not supported. | Not supported. | Not supported. |
| Advan | BOT Traffic Management | Paid Support | Paid Support | Paid Support |

| | | | | |
|---|---|---|---|---|
| cedSecurityValue–addedProtection | | | | |
| | API Security | Paid Support | Paid Support | Paid Support |
| Log Management | Attack Log Query and Download | Supported | Supported | Supported |
| | Attack Log Delivery | Not supported. | Supported | Supported |
| | Storage of Attack Logs for All Attack Types | Supported | Supported | Supported |
| | Access Log Delivery | Paid Support | Paid Support | Paid Support |
| | Access Log Query and Download (Log package | Supported | Supported | Supported |

| | | | | |
|---|---|---|---|---|
| | purchase required) | | | |
| Professional Service | Two-way Certificate Authentication | Supported | Supported | Supported |
| | One-on-One Pre-sales Support Service | Not supported. | Supported | Supported |
| | WeChat or WeCom Support | 5*8 hours | 7*12 hours | 7*12 hours |
| | 7*24 hours Ticket-based Pre-sales and After-sales Support | Supported | Supported | Supported |

# Concepts

Last updated: 2024-11-26 10:09:08

## AI Engine

AI Engine (Artificial Intelligence Engine) refers to Tencent Cloud WAF's pioneering application of machine learning-based web attack detection technology. Through the self-learning, self-evolving, and self-adapting capabilities of the AI Engine, the detection and capture rates of both known and unknown web threats are maximized, while minimizing false positives, and flexibly adapting to ever-changing web applications.

## 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.

## CC Attack Protection

Challenge Collapsar (CC) Attack Protection refers to protection against CC attacks where attackers use tools to simulate multiple users continuously sending connection requests to your website, making your business unavailable. Adding CC protection rules can help users defend against CC attacks targeting page requests.

## Region Blocking

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

## Tamper protection

Tamper protection (Tamper Proofing) 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 the cloud will be returned.

## Leakage protection

Leakage protection (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.

## IP Ban

IP Ban (IP Block) detects and analyzes malicious attacks or scanning traffic in requests, helping websites automatically block them. For example, if the source IP makes multiple different types of web attacks in a short period or if the source IP comes from common scanning tools or a malicious attack IP database.

## Forwarding IP Address

A forwarding IP address (Return Source IP Address) is automatically assigned by WAF based on the domains added by the customer. It acts as the WAF's egress IP to direct filtered normal traffic to the customer's origin server.

## Queries per second

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).

## 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.

## One-click Bypass

The one-click Bypass feature allows you to switch to pure forwarding with a single click. On the domain management page, select the desired domain name and click . After enabling this feature, you can quickly allow all blocked traffic, ensuring rapid business recovery.


## 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.