Web Application Firewall

Product Introduction

Product Documentation

Contents

Product Introduction

Overview

Last updated：2023-12-29 10:58:11

WAF Overview

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 WAF resolves a domain name to the CNAME address provided by the WAF cluster through DNS and configures the real server IP through WAF. In this way, malicious traffic is cleansed and filtered, and normal traffic is forwarded to the real server, protecting the website security.

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.

Key Features

Feature	Description
AI + WAF	Web attack recognition is based on AI + rules. It is anti-bypass and low in both false negative and false positive rates. Web attack recognition defends effectively against common web attacks, including the OWASP top 10 web security threats (SQL injection, unauthorized access, cross-site scripting, cross-site request forgery, web shell trojan upload, etc).
Virtual zero-day vulnerability patching	The 24*7 monitoring service from Tencent security team identifies and responds to vulnerabilities proactively. Within 24 hours, it issues virtual patches to zero-day and high-risk web vulnerabilities. Protected users can get zero-day and emergency vulnerability protection instantly and automatically, shortening vulnerability response time dramatically.

Web tampering protection	You can cache core web contents to the cloud and publish cached web pages. This acts like a substitute and can prevent negative consequences of web page tampering.
Data leakage protection	Backend data is well protected by pre-event server and application concealing, mid-event attack prevention, and post-event sensitive data replacement and concealing.
CC attack protection	Smart CC protection intelligently generates defense policies based on the real server's abnormal responses (such as timeout and response delay) and website behavior big data analysis. It supports multidimensional custom accurate access control, intelligently and effectively filters malicious access requests, and defends against CC attacks with measures such as CAPTCHA and frequency control.
Crawler and bot traffic management	The AI + rules-based webpage crawler and bot management feature help you avoid business risks caused by malicious bot behaviors, including website user data leakage, content infringement, competing price comparison, inventory search, malicious SEO, and business strategy leakage.
30 BGP lines for access protection	With its 30 dedicated BGP lines for protective nodes, WAF supports smart node scheduling to effectively solve the issues with access delay to ensure high access speed in metropolises and small towns. It implements cloud-based security protection without compromising the website access speed.

Why WAF

WAF can effectively protect website systems and businesses of enterprises in the following use cases.

Data leakage (leakage of core information assets)

A website is the entry to enterprise information assets and may be hacked for asset theft, causing incalculable losses to enterprises.

Malicious access and data crawling (unavailability and data utilized by competitors)

Hackers control botnets to launch CC attacks on a website, which will consume all its resources and makes it unavailable. Malicious users scrape core content of websites (blog, recruitment, forum, and ecommerce websites) by using web crawlers. For example, ecommerce offering details are crawled by competitors for analysis, and low-price offering information is crawled or promotion intelligence is obtained before sales campaigns by bargain hunters for their benefits.

Network trojans and tampering (affecting credibility and image)

After obtaining website or server permissions, attackers can inject malicious code to make users execute malicious programs, drive traffic, steal accounts, and show off. They may also implant links to pornographic, gambling, and illegal information or tamper with the images and texts on the website, adversely affecting website operations, undermining the credibility, and damaging the image.

Framework vulnerability (attacks during patching)

Many web systems are based on common open-source frameworks such as Structs 2, Spring, and WordPress, which are prone to security vulnerabilities. A lot of attacks will emerge just one day after the vulnerabilities are discovered, making patching extremely hard.

Business interruption due to high-traffic DDoS attacks

DDoS attacks have become a cost-effective and easy way to interrupt the business of competitors or make their key portals inaccessible. These attacks have severe impact on business continuity and brand image. More often than not, companies are very passive when attacked.

Product Category

Last updated：2023-12-29 10:59:11

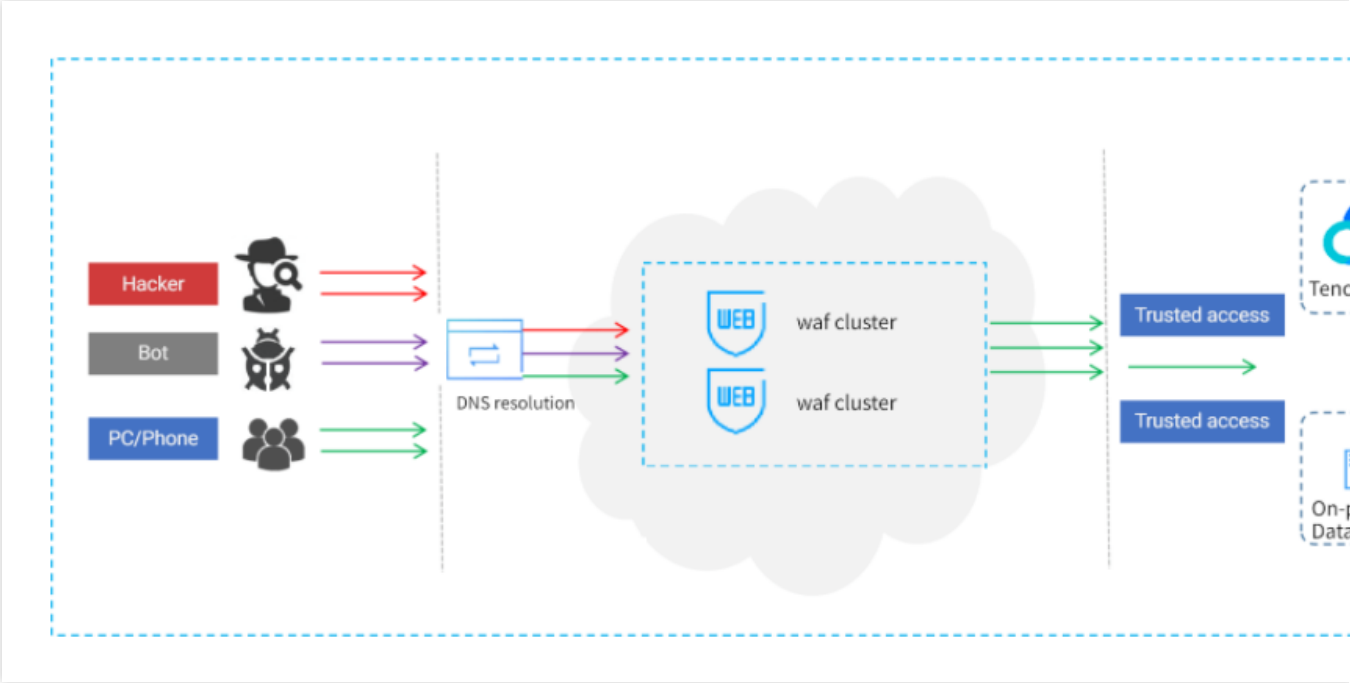
Type Overview

Tencent Cloud provides two types of 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.
Strength	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. 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. 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 traffic management, CCPC protection, or website security operation, you are recommended to use CLB WAF.
Region	You need to select a region when purchasing SaaS WAF	You need to select a region in the console after purchasing CLB WAF.

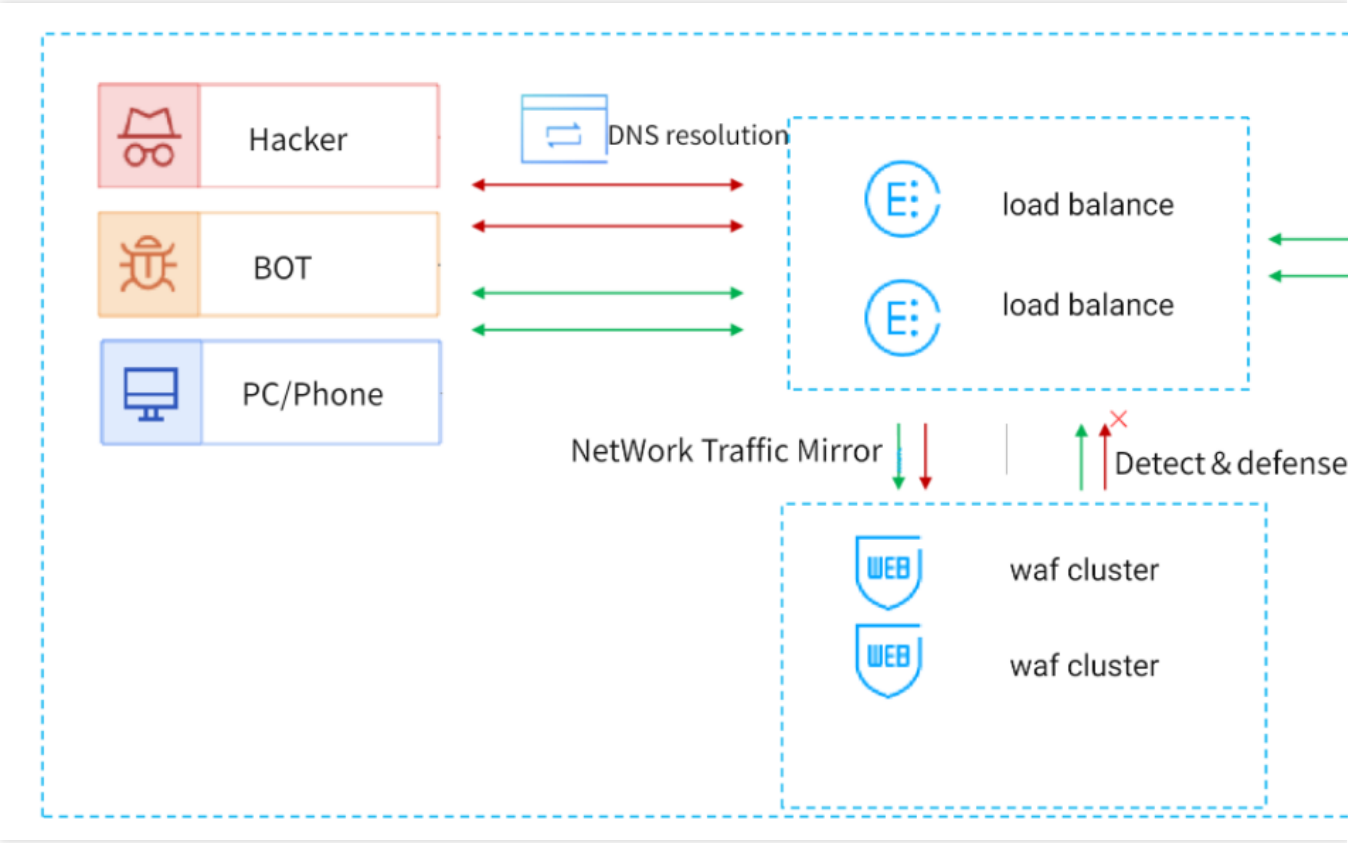
SaaS WAF

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.



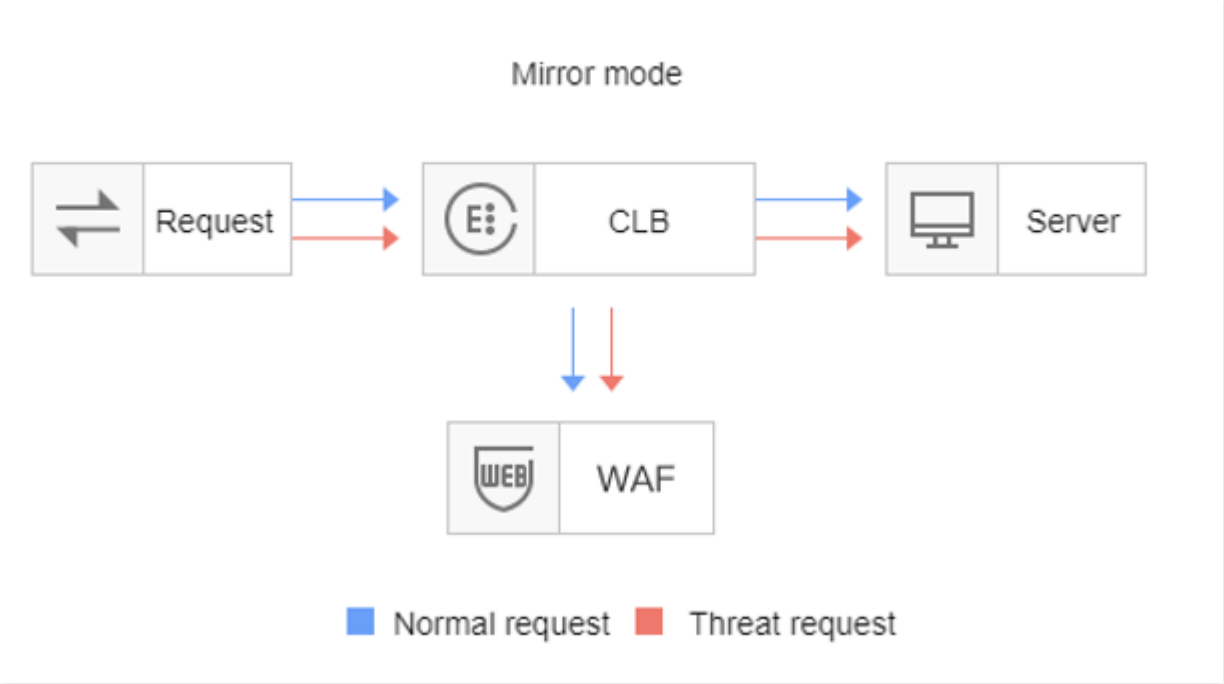
CLB WAF

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.

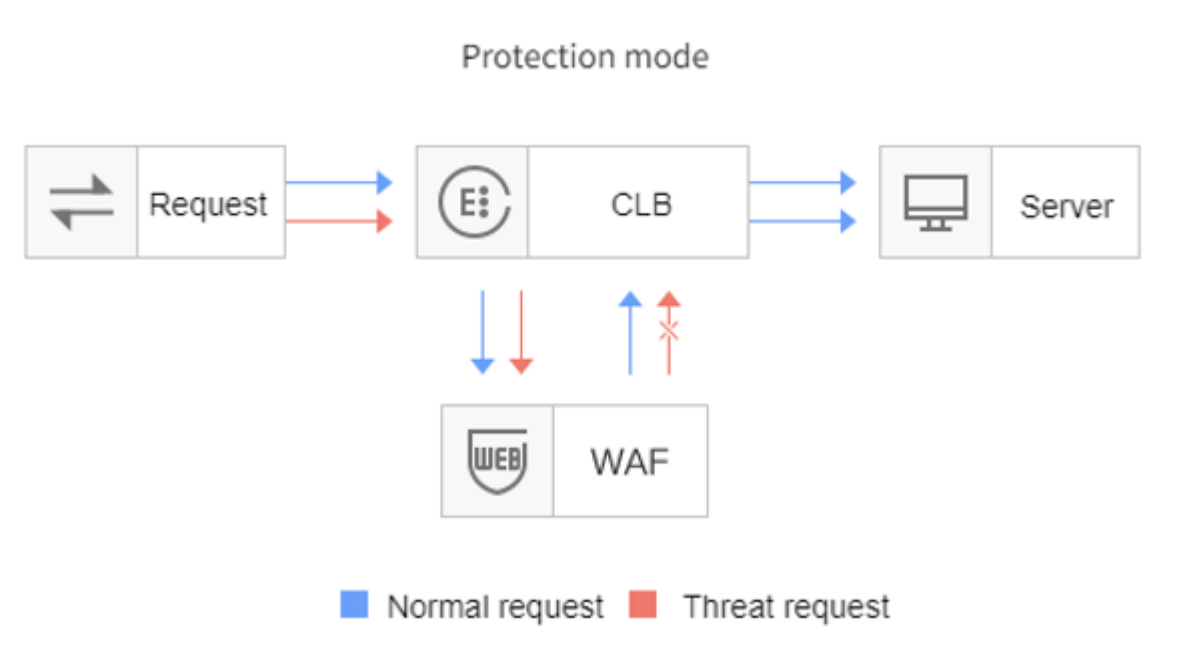


CLB WAF provides two traffic processing modes:

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.



Strengths

Last updated：2023-12-29 11:01:16

Multiple Access Methods

Supports quick access to WAF services without any application adjustment, and provides quick binding to Tencent Cloud CLB to perform bypass detection and traffic cleansing with the quick bypass feature, which can separate business request forwarding from security protection.
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.
Supports cross-region deployment of cluster protection resources, dynamic scaling, and on-demand usage to avoid redundancy and single points of failure.

Protection from AI Engine and Rule Engine

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.
WAF continuously learns the characteristics of massive business data to generate business-oriented personalized protection policies and avoid false positives. You can use the AI engine to handle false positives and false negatives to improve operation 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 sessions to define protection policies for various 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 Protection Against CC Attacks

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.
Supports custom sessions to defend against CC attacks at the session level, realizing more accurate protection against CC attacks and less false positives.
Allows you to view IP addresses that are blocked due to CC protection in real time to quickly adjust protection policies as needed.
Supports quick access to 100 Gbps of Anti-DDoS capability to defend against traffic-intensive DDoS attacks, helping you easily cope with sudden attacks.

Scenarios

Last updated：2023-12-29 11:01:34

Government Website Protection

WAF allows you to quickly connect to the protection service. Then, you can simply configure parameters to hide your real server and protect your website content from tampering, thereby ensuring the availability of government services and smooth user access.

Ecommerce 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.

Finance 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 detect abnormal 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 Protection

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.

Plans and Editions

Last updated：2023-12-29 11:01:55

Chinese Mainland Editions

SaaS WAF

Feature	Item	Premium	Enterprise	Ultimate	Exclusive
Basic support	Use case	Applicable to standardized protection for small and medium websites	Applicable to protection for small and medium website applications and customized protection for medium and large websites	Applicable to protection for large and super large website applications and customized protection for complex website applications	Applicable to protection for large and super large web and API services, with dedicated resources and customizable protection capabilities
	Peak QPS	2,500 QPS	5,000 QPS	10,000 QPS	50,000 QPS
	Bandwidth (in/outside Tencent Cloud)	50 Mbps/15 Mbps	100 Mbps/30 Mbps	200 Mbps/50 Mbps	1,000 Mbps/250 Mbps
	Dedicated IP	-	√	√	√
	Primary domain names	2	3	4	1,000 (customizable)
	Domain names (primary domain names+subdomain names)	20	30	40	20,000 (customizable)
	Wildcard domain name protection	-	√	√	√
	IPv6 protection	-	√	√	√
	Certificate	-	-	-	√

	customization				
	HTTP2/WebSocket	√	√	√	√
Basic security protection	Rule protection engine	√	√	√	√
	Virtual zero-day vulnerability patching	√	√	√	√
	IP blocklist/allowlist	1,000 pcs/domain name	5,000 pcs/domain name	20,000 pcs/domain name	20,000 pcs/domain name (customizable)
	Regional blocking	√	√	√	√
	Access control	10 pcs/domain name	20 pcs/domain name	50 pcs/domain name	200 pcs/domain name
	Emergency CC protection	√	√	√	√
	IP/Session-based CC protection	5 pcs/domain name	20 pcs/domain name	50 pcs/domain name	50 pcs/domain name
	Data leakage prevention	5 pcs/domain name	10 pcs/domain name	20 pcs/domain name	50 pcs/domain name
	Tamper protection	10 pcs/domain name	20 pcs/domain name	50 pcs/domain name	50 pcs/domain name
	AI engine	-	-	√	√
	Advanced vulnerability protection (AI engine)	-	-	√	√
Log processing	Attack log query and download	√	√	√	√
	Access log query	√	√	√	√

	and download (with log package required)				
Professional services	Non-standard port support	-	√	√	√
	One-to-one presales support	-	√	√	√
	24/7 remote + Weixin group support	-	√	√	√
	Remote expert service	-	-	√	√
	One-to-one on-site expert support	-	-	-	5 times
	Presales and aftersales support through ticket	√	√	√	√

CLB WAF

Feature	Item	Premium	Enterprise	Ultimate	Exclusive
Basic support	Use case	Applicable to standardized protection for small and medium websites	Applicable to protection for small and medium website applications and customized protection for medium and large websites	Applicable to protection for large and super large website applications and customized protection for complex website applications	Applicable to protection for large and super large web and API services, with dedicated resources and customizable protection capabilities
	Peak QPS	2,500 QPS	5,000 QPS	10,000 QPS	50,000 QPS
	Bandwidth	100 Mbps	200 Mbps	400 Mbps	400 Mbps

	Multi-region linkage	-	-	10 regions	√
	CLB listeners	200	300	500	1,000 (customizable)
	Primary domain names	2	3	4	1,000 (customizable)
	Domain names (primary domain names+subdomain names)	20	30	40	20,000 (customizable)
	Wildcard domain name	-	√	√	√
	IPv6 protection	√	√	√	√
Basic security protection	Rule protection engine	√	√	√	√
	Virtual zero-day vulnerability patching	√	√	√	√
	IP blocklist/allowlist	1,000 pcs/domain name	5,000 pcs/domain name	20,000 pcs/domain name	20,000 pcs/domain name (customizable)
	Regional blocking	√	√	√	√
	Access control	10 pcs/domain name	20 pcs/domain name	50 pcs/domain name	200 pcs/domain name
	IP/Session-based custom CC protection	5 pcs/domain name	20 pcs/domain name	50 pcs/domain name	50 pcs/domain name
	AI engine	-	-	√	√
	Advanced vulnerability protection (AI engine)	-	-	√	√

Log processing	Attack log query and download	√	√	√	√
	Access log query and download (with log package required)	√	√	√	√
Professional services	Two-way certificate authentication	√	√	√	√
	One-to-one presales support service	-	√	√	√
	24/7 remote + Weixin group support	-	√	√	√
	Remote expert service	-	-	√	√
	One-to-one on-site expert support	-	-	-	5 times
	Presales and aftersales support through ticket	√	√	√	√

Non-Chinese Mainland Editions

Notes

The editions are being upgraded. To purchase the desired edition, submit a ticket.

SaaS WAF

Feature	Item	Premium	Enterprise	Ultimate	Exclusive
Basic support	Use case	Applicable to standardized protection for	Applicable to protection for small and	Applicable to protection for large and	Applicable to protection for large and super

		small and medium websites	medium website applications and customized protection for medium and large websites	super large website applications and customized protection for complex website applications	large web and API services, with dedicated resources and customizable protection capabilities
	Peak QPS	2,500 QPS	5,000 QPS	10,000 QPS	50,000 QPS
	Bandwidth (in/outside Tencent Cloud)	50 Mbps/15 Mbps	80 Mbps/30 Mbps	100 Mbps/50 Mbps	1,000 Mbps/250 Mbps
	Dedicated IP	-	√	√	√
	Primary domain names	2	3	4	1,000 (customizable)
	Domain names (primary domain names+subdomain names)	20	30	40	20000 (customizable)
	Wildcard domain name protection	-	√	√	√
	Certificate customization	-	-	-	√
	HTTP2/WebSocket	√	√	√	√
Basic security protection	Rule protection engine	√	√	√	√
	Virtual zero-day vulnerability patching	√	√	√	√
	IP blocklist/allowlist	1,000 pcs/domain name	5,000 pcs/domain name	20,000 pcs/domain name	20,000 pcs/domain name (customizable)
	Regional blocking	√	√	√	√

	Access control	10 pcs/domain name	20 pcs/domain name	50 pcs/domain name	200 pcs/domain name
	Emergency CC protection	√	√	√	√
	IP/Session-based CC protection	5 pcs/domain name	20 pcs/domain name	50 pcs/domain name	50 pcs/domain name
	Data leakage prevention	5 pcs/domain name	10 pcs/domain name	20 pcs/domain name	50 pcs/domain name
	Tamper protection	10 pcs/domain name	20 pcs/domain name	50 pcs/domain name	50 pcs/domain name
	AI engine	-	-	√	√
Log processing	Attack log query and download	√	√	√	√
	Access log query and download (with log package required)	√	√	√	√
Professional services	Non-standard port support	-	√	√	√
	One-to-one presales support	-	√	√	√
	24/7 remote + Weixin group support	-	√	√	√
	Remote expert service	-	-	√	√
	One-to-one on-site expert support	-	-	-	5 times
	Presales and aftersales support through ticket	√	√	√	√

CLB WAF

Feature	Item	Premium	Enterprise	Ultimate	Exclusive
Basic support	Use case	Applicable to standardized protection for small and medium websites	Applicable to protection for small and medium website applications and customized protection for medium and large websites	Applicable to protection for large and super large website applications and customized protection for complex website applications	Applicable to protection for large and super large web and API services, with dedicated resources and customizable protection capabilities
	Peak QPS	2,500 QPS	5,000 QPS	10,000 QPS	50,000 QPS
	Bandwidth	100 Mbps	200 Mbps	400 Mbps	400 Mbps
	Multi-region linkage	-	-	10 regions	√
	CLB listeners	200	300	500	1,000 (customizable)
	Primary domain names	2	3	4	1,000 (customizable)
	Domain names (primary domain names+subdomain names)	20	30	40	20,000 (customizable)
	Wildcard domain name	-	√	√	√
Basic security protection	Rule protection engine	√	√	√	√
	Virtual zero-day vulnerability patching	√	√	√	√

	IP blocklist/allowlist	1,000 pcs/domain name	5,000 pcs/domain name	20,000 pcs/domain name	20,000 pcs/domain name (customizable)
	Regional blocking	√	√	√	√
	Access control	10 pcs/domain name	20 pcs/domain name	50 pcs/domain name	200 pcs/domain name
	IP/Session-based CC protection	5 pcs/domain name	20 pcs/domain name	50 pcs/domain name	50 pcs/domain name
	AI engine	-	-	√	√
Log processing	Attack log query and download	√	√	√	√
	Access log query and download (with log package required)	√	√	√	√
Professional services	Two-way certificate authentication	√	√	√	√
	One-to-one presales support	-	√	√	√
	24/7 remote + Weixin group support	-	√	√	√
	Remote expert service	-	-	√	√
	One-to-one on-site expert support	-	-	-	5 times
	Presales and aftersales support through ticket	√	√	√	√

Supported Regions

Last updated：2023-12-29 11:08:13

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:

Product Type	Supported Region	Details
SaaS WAF	Chinese mainland	South China: Guangzhou
		East China: Shanghai
		North China: Beijing
		Southwest China: Chengdu
	Outside Chinese mainland	Hong Kong/Macao/Taiwan (China): Hong Kong (China)
		Southeast Asia: Singapore, Bangkok, and Jakarta
		Northeast Asia: Seoul and Tokyo
		South Asia: Mumbai
		West US: Silicon Valley
		North America: Toronto
		Europe: Moscow and Frankfurt
		East US: Virginia
		South America: Sao Paulo
CLB WAF	Chinese mainland	South China: Guangzhou and Shenzhen Finance
		East China: Shanghai, Nanjing, and Shanghai Finance
		North China: Beijing and Beijing Finance
		Southwest China: Chengdu and Chongqing
	Outside Chinese mainland	Hong Kong/Macao/Taiwan (China): Hong Kong (China)
		Southeast Asia: Singapore, Bangkok, and Jakarta
		South Asia: Mumbai

		Northeast Asia: Seoul and Tokyo
		West US: Silicon Valley
		East US: Virginia
		North America: Toronto
		Europe: Moscow and Frankfurt

Note:

We recommend you place your SaaS WAF instance and web real server in the same region to reduce business latency.

CLB WAF supports binding IPv6 CLB instances to protect IPv6 websites. If you want to use IPv6 web protection, 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. For more information on IPv6 CLB, see Getting Started with IPv6 CLB.

If you have never added a protected domain name in WAF, you can contact us to change the region. Otherwise, you cannot change the region.

Basic Concepts

Last updated：2023-12-29 11:08:37

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.

Tamper Protection

Tamper protection 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.

Leakage Protection

Leakage protection 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.

Quick Bypass

Quick bypass refers to a feature that can quickly switch to pure forwarding. On the domain name management page, you can select the target domain name and click

to enable this feature and quickly allow all blocked traffic for a swift business recovery.