Web Application Firewall

Product Documentation

Contents

Web Application Firewall 3
- Product Introduction 3
  - Product Overview 3
  - Product Strengths 6
  - Product Category 8
  - Use Cases 12
- Quick Start 13
  - FAQs for Beginners 13
  - Quick Start 14
- Operation Guide 20
  - List of Features of the Tenant Side 20
  - CLB WAF Domain Name Access 22
  - Rule Engine 26
  - CC Protection Settings 31
  - Custom Policy 38
  - Webpage Anti-Tampering 42
  - Information Leakage Prevention 45
  - Regional Blocking 47
  - Allowlist and Blocklist Management 49
    - Feature Description 49
    - IP Allowlist 50
    - Precise Allowlist Management 55
    - Rule Allowlist 58
    - IP Blocklist 60
  - Attack Log 64
  - IP Address Management 70
  - Common Operations 74
    - Scenario 1: Creating an Instance 74
    - Scenario 2: Adding a CLB WAF Protected Domain Name 76
    - Scenario 3: Adding a SaaS WAF Protected Domain Name 78
    - Scenario 4: Deleting a Protected Domain Name 80
    - Scenario 5: Deleting an Instance 81
    - Scenario 6: Adding a Custom Rule 84
    - Scenario 7: Adding a CC Protection Rule 86
    - Scenario 8: Checking Whether a Domain Name Is in Protected Status 88
    - Scenario 9: Emergency Plan 91
- Best Practice 94
  - Building a CLB WAF Test Environment 94
  - Building a SaaS WAF Origin Server 98
- FAQs 103
  - FAQs 103

Product Introduction
Product Overview

What Is WAF?

Web Application Firewall (WAF) is an AI-based one-stop risk protection solution for web workload operations. It identifies malicious traffic through the AI and rule engines to protect website security and improve the security and reliability of websites.

WAF provides two types of cloud WAF, SaaS WAF and CLB WAF. The security protection capabilities provided by the two WAFs are basically the same, but the access methods are different.

- SaaS WAF resolves a domain name to the CNAME address provided by the WAF cluster through DNS and configures the origin server IP address through WAF. In this way, malicious traffic is cleansed and filtered, and normal traffic is forwarded to the origin server, protecting website security.
- CLB WAF integrates with the CLB cluster to copy the HTTP/HTTPS traffic of the CLB to the WAF cluster. WAF performs bypass threat detection and filtering, and synchronizes the trusted status of user requests to the CLB cluster for threat interception or allowance to protect website security. WAF can effectively defend against OWASP attacks such as SQL injection, XSS cross-site scripting, trojan upload, and unauthorized access. In addition, it can effectively filter CC attacks, detect DNS linkage hijacking, provide zero-day vulnerability patches, and prevent webpage tampering to protect the website system and workload security in all aspects through various means.

Main Features

Feature	Introduction
AI + WAF	AI and rule-based web attack identification prevents bypass attempts, ensures low false alarms and false positives, and provides effective defense against common web attacks such as SQL injection, unauthorized access, XSS, cross-site request forgery (CSRF), and WebShell Trojan upload, and other top 10 web security threats defined by OWASP.
Zero-day vulnerability virtual patching	The security team provides 24/7 monitoring, proactive discovery and response, and issues virtual patches for high-risk web vulnerabilities and zero-day vulnerabilities. Protected users can obtain protection capabilities against emergency vulnerability and zero-day vulnerability attacks without any operation, which greatly shortens the vulnerability response cycle.

Feature	Introduction
Webpage anti-tampering	Users can configure core webpage content to be cached in the cloud and publish the cached webpage content externally. This ensures that even if the original page is tampered with, the cached content acts as a substitute, preventing negative impacts on the organization caused by webpage tampering.
Data leakage prevention	Prevent the background database from being stolen by hackers through server application hiding before events, intrusion protection during events, and sensitive data replacement and hiding after events.
CC attack protection	Intelligent CC protection integrates exception responses (timeout or response delay) of the origin server and big data analysis of website behaviors to generate defense policies with intelligent decision-making. Multi-dimensional and customizable precise access control, combined with countermeasures such as human-machine recognition and frequency control, effectively filters junk access and mitigates CC attacks.

Why Do You Need WAF?

In the following scenarios, using WAF can effectively defend and prevent threats, ensuring the system and workload security of enterprise websites.

- Data leakage (core information asset leakage)
  Websites serve as portals to many enterprise information assets. Hackers can steal enterprise information assets through web intrusions, causing immeasurable losses to enterprises.
- Malicious access and data crawling (unable to provide normal services, data being used by opponents)
  Hackers control the botnet to launch CC attacks on websites, exhausting resources and making it impossible to provide normal services. Malicious users use web crawlers to capture the core content of websites (comments in literary blogs, recruitment websites, forum websites, and e-commerce websites). Product details on e-commerce websites are deliberately crawled by competitors for research. Deal hunters try to search for information on low-priced products or obtain intelligence in advance of marketing promotions to find arbitrage possibilities.
- Website WebShell attacks or tampering (impacting credibility and image)
  After obtaining permissions of websites or servers, attackers insert malicious code to make users execute malicious programs, earn traffic, steal accounts, or show off. They implant links related to pornographic, gambling, and illegal content, and tamper with webpage images and text, causing a significant impact on website operation and damaging the image of website operators. The public credibility and image of the website suffer losses.
- Framework vulnerability (attacked during patch fixing period)

Many web systems are based on common open-source frameworks such as Structs2, Spring, and WordPress. These frameworks often have security vulnerabilities, but the maintenance period of waiting for patches to be installed is a difficult and dangerous process. Many attacks will spread within one day after the vulnerability is announced.

Product Strengths

Multiple Access Protection Methods

- Once WAF is enabled, the access protection can be implemented without requiring any workload changes. By binding with Converge Cloud CLB with one click, the bypass detection and threat cleaning for websites can be achieved. Additionally, a one-click bypass feature is provided to ensure the separation of workload forwarding and security protection, resulting in a stable and reliable solution.
- WAF is accessed through CNAME to hide the user's actual origin server and perform the origin-pull operation on trusted traffic, covering both Converge Cloud and non-Converge 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 and Rule-based Dual Engine Protection

- Based on the OWASP Top 10 defense (such as SQL injection, unauthorized access, XSS, CSRF, and command line injection) performed by the security rule engine, AI defense capabilities are introduced to accurately and effectively capture various conventional web attacks, zero-day attacks, and other new unknown attacks through cross-validation and continuous learning.
- Personalized protection policies based on the workload are generated through continuous learning of the features of massive workload data to avoid false alarms. Users can manage false alarms and missed alarms through a self-service feature provided by the AI engine, enhancing operation efficiency.

Timely Patch Fix Assurance

- It provides critical vulnerability patch updates within 12 hours and general vulnerability patch updates within 24 hours.
- It provides automatic cloud updates and second-level synchronous policy distribution, helping enterprises safeguard against web vulnerabilities.

Intelligent CC Protection

- The session can be customized, and CC protection can be performed through the session dimension

to more accurately protect against CC attacks and reduce false alarms.
- The IP addresses in the CC blocking status can be viewed in real time for quick adjustment of protection policies as needed.
- With one-click anti-DDoS linkage, sensitive and large-volume DDoS attacks can be easily handled without the worry of unexpected risks.

Stable and Highly Available Workload Assurance

- It offers users seamless access with no hardware or software installation or maintenance required. The service delivers a stable, low-latency, high-performance VIP direct connect. While hiding and protecting the origin server IP address, premium acceleration routes ensure millisecond-level workload latency and configuration response speed.

IPv6 Security Protection

- Cloud NAT64 instances can be used to enable IPv6 access protection for websites, providing support for IPv6 access and protection without the need to modify IPv4 sites.
- By linking with CLB, IPv4 and IPv6 access traffic can be seamlessly handled with the same level of security protection, ensuring a simple and quick process.

Product Category

Type Overview

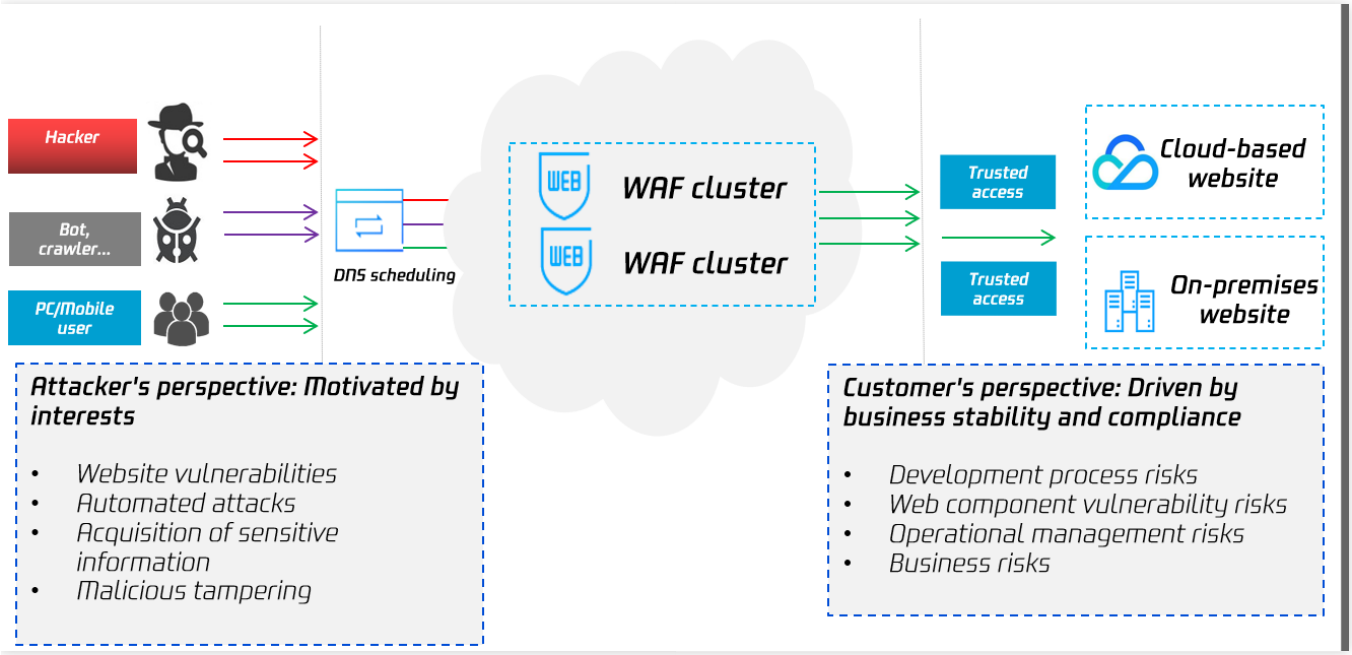
Converge Cloud provides two types of cloud WAF, SaaS WAF and CLB WAF. The security protection capabilities provided by the two WAFs are basically the same, but the access methods and applicable scenarios are different. You can choose the appropriate type of WAF according to your actual deployment needs.

Category	SaaS Type	CLB Type
Applicable scenario	Applicable to all users (cloud users or local IDC users). Domain name access is achieved through DNS resolution scheduling.	Applicable to users who have used or plan to use layer-7 CLB on Converge Cloud.
Core strengths	·It has a broad scope of application, covering users both on Converge Cloud and not on Converge Cloud. ·It supports hiding the origin server to reduce the exposure surface of risks.	·It features seamless access and millisecond-level latency. The existing network architecture does not need to be adjusted for WAF access. ·It features separate website workload forwarding and security protection, with one-click bypass to ensure the security, stability, and reliability of the website workload. ·It supports multi-region access.
How to choose	For users who have websites that need protection both on Converge Cloud and locally, or do not use layer-7 CLB on Converge Cloud, it is recommended to use SaaS WAF.	For users who have used or plan to use layer-7 CLB on Converge Cloud and have the needs of web security protection, compliance protection, and website security operations, it is recommended to use CLB WAF.

> Note:
>
> CLB WAF is currently available in grayscale. If you need to use it, submit an application, and we will verify and activate it for you as soon as possible.

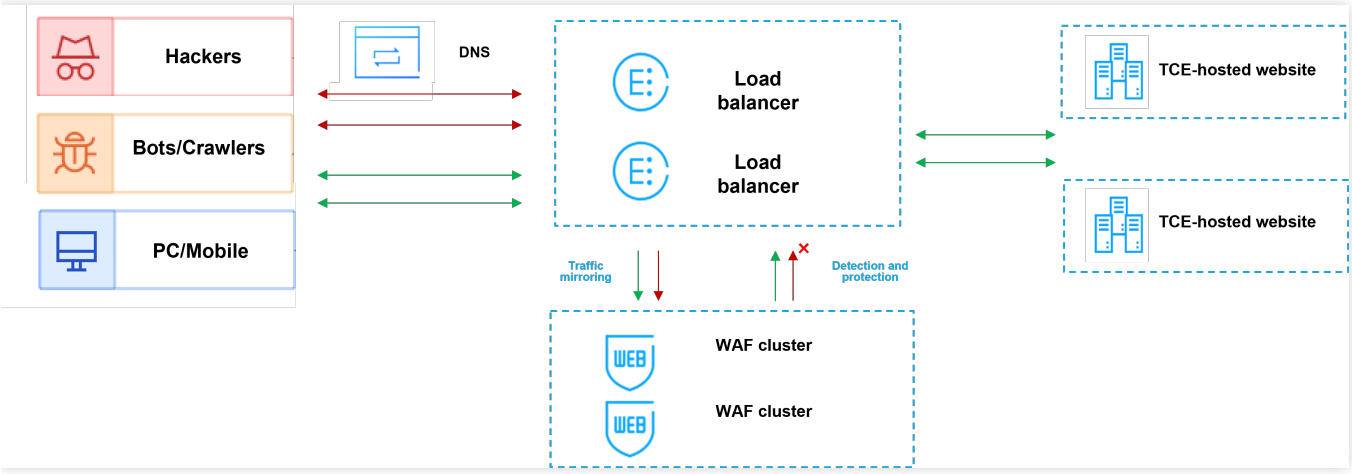
SaaS WAF

WAF is delivered in a SaaS model. By modifying the DNS traffic diversion settings, web protection capabilities can be obtained in minutes on the user side without the need to deploy any hardware equipment. After the WAF cluster performs malicious traffic detection and protection on the protected domain names, it performs the origin-pull operation on normal traffic to the origin server to protect website security.



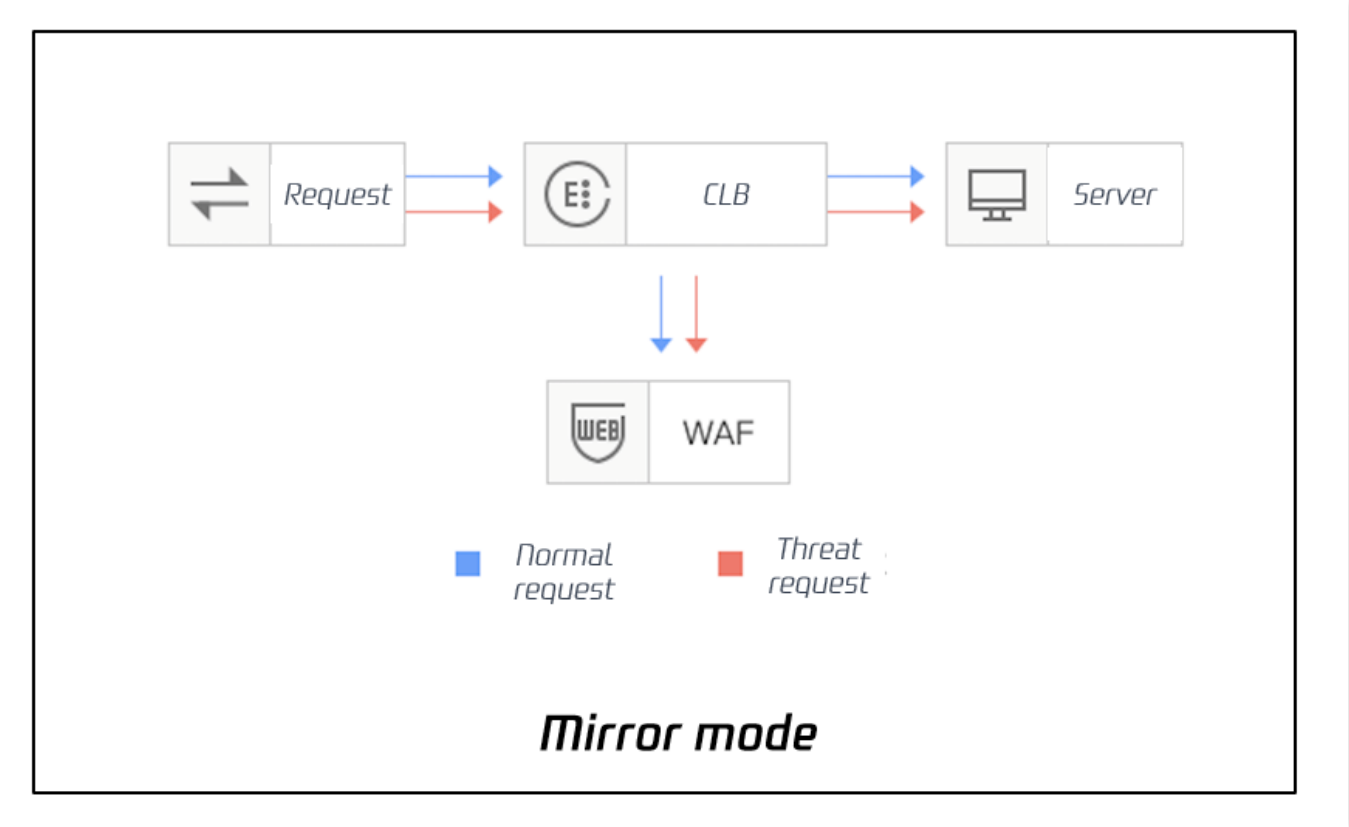
CLB WAF

WAF integrates with the layer-7 CLB (listener) cluster in various network environments of Converge Cloud through domain name configuration to perform bypass threat detection and filtering on HTTP/HTTPS traffic transiting through the CLB, realize the separation of workload forwarding and security protection, minimize the impact of security protection on the network workload, and protect stable website operation.

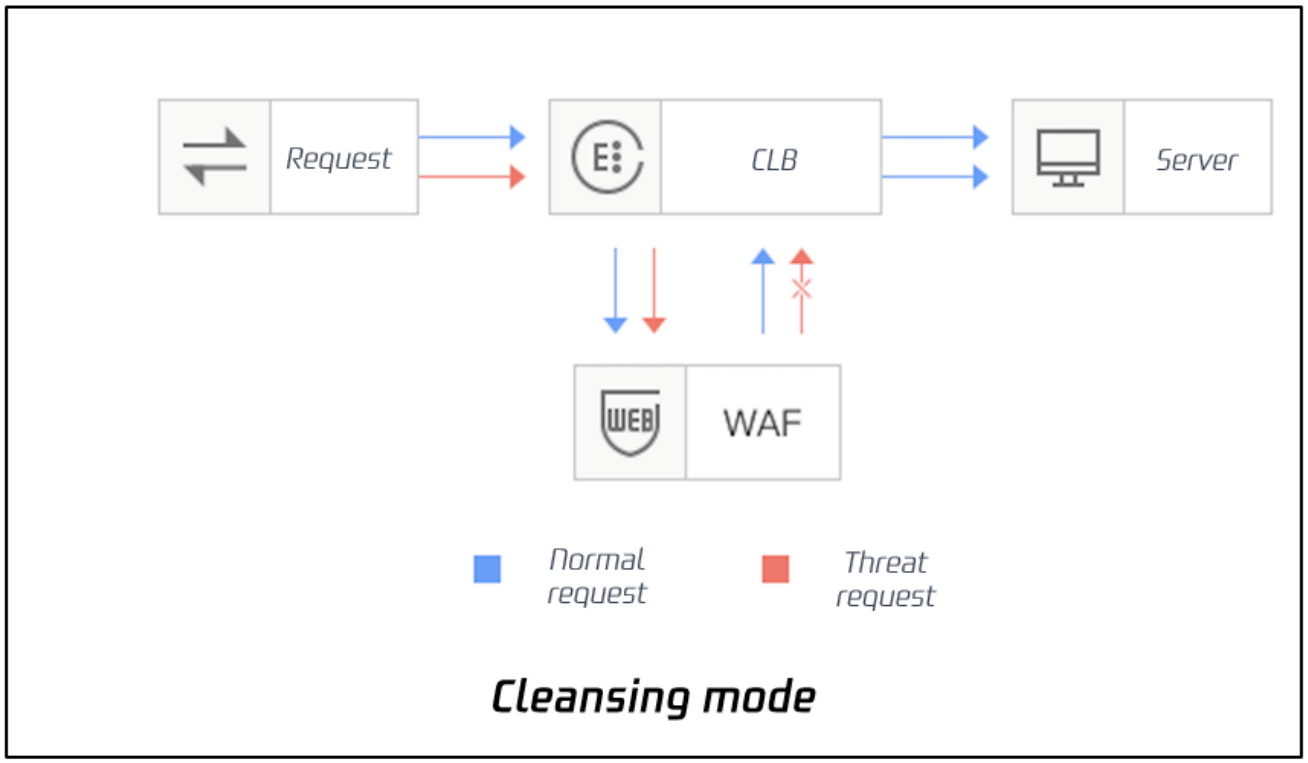


CLB WAF provides two traffic processing modes:

- 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.


Request
CLB
Server
WAF
Normal request
Threat request
Cleansing mode

Use Cases

Financial Website Protection

- It provides one-click access protection, can be organically combined with large-traffic DDoS defense, and possesses web security protection.
- It effectively monitors DNS linkage hijacking to prevent website traffic from being maliciously directed.
- It can effectively detect abnormal accesses such as credential stuffing to protect user information from leakage.
- The strengths of cloud resources and automatic scaling make it easy to handle workload emergencies and large-traffic CC attacks.

Government Website Protection

- It provides one-click access protection, and hides and protects the origin server with easy configuration to protect the website content from hacker intrusion and tampering. It ensures the accuracy of website information, the availability of government services, and the satisfaction and smoothness of public access.

E-Commerce Website Protection

- It continuously optimizes protection rules, accurately intercepts web attacks, and comprehensively defends against OWASP Top 10 web application risks.
- In a high-concurrency panic buying scenario, it can intelligently filter malicious attacks and junk access to ensure the smoothness of normal access.

Data Leakage Prevention

- It avoids the leakage of core website data due to injection attacks by hackers.
- Anti-CC attack: It prevents malicious CC (HTTP GET flood) and ensures website availability by blocking massive malicious requests at layer-4 and layer-7.

Quick Start
FAQs for Beginners

What Are the WAF Access Methods?

WAF is divided into two types: SaaS WAF and CLB WAF. The domain name access methods of the two types of WAF are different. Complete the access according to the actual situation.

Does WAF Support HTTPS Protection?

WAF fully supports HTTPS workload. The user only needs to upload the SSL certificates and private key according to the prompts to enable WAF to protect HTTPS workload traffic.

How Many Origin-Pull IP Addresses Can Be Set for a Protected Domain Name of WAF?

Up to 50 origin-pull IP addresses can be set for a protected domain name of WAF.

Does WAF Support Health Checks?

WAF enables health checks by default. It detects the connection status of all origin server IP addresses. If an origin server IP has no response, WAF will no longer forward requests to this IP until the access status returns to normal.

How Long Does It Approximately Take for the Configuration Change to Take Effect in the WAF Console?

Generally, the changed configuration takes effect within 10 seconds.

Do SaaS WAF and CLB WAF Support SM Certificate Authentication?

SaaS WAF does not support SM certificate authentication, while CLB WAF supports SM certificate authentication.

Quick Start

WAF is divided into two types: SaaS WAF and CLB WAF. The domain name access methods of the two types of WAF are different. Complete the access according to the actual situation.

SaaS WAF Access Configuration

SaaS WAF allocates a CNAME to the protected domain name, modifies the DNS resolution record of the website, and forwards the web requests received by the website to WAF, thereby providing security protection for the website. When it is used in conjunction with security groups, it can prevent attackers from bypassing the WAF and directly attacking the origin server of the website. To achieve the above features, you need to complete the following steps:

Step 1: Domain Name Addition

To enable WAF to recognize the domain names that require protection, you should first add the domain names to WAF. The following uses the protection of waf.qcloudwaf.com as an example to describe the configuration steps.

1. Log in to the WAF console. In the left sidebar, select Asset Center > Access Management to enter the Domain Name Access page.
2. On the Domain Name Access page, click Add Domain Name, enter the Add Domain Name page, and select SaaS Type.
3. Configure relevant basic parameters on the Add Domain Name page.

- Domain name configuration

1. Add the domain name waf.qcloudwaf.com to be protected in the domain name input box.
2. The protocol and port can be selected according to the actual situation. For example, check HTTP and select port 80; check HTTPS and select port 443.
3. Optional HTTPS origin-pull method: HTTP or HTTPS.
4. Optional certificate source: Hosted certificate or self-owned certificate.
5. Enter the real IP address of the origin server of the website to be protected, that is, the public IP address of the origin server, in the origin server IP input box.

- Other configurations

1. Check whether network traffic transits through other intermediate proxy devices before reaching the WAF. If so, select Yes, and WAF supports configuring the obtaining method of the custom source IP. If not, select No.
2. Click Save. After completing the configuration, you can see the domain name you just added and the CNAME address allocated for the site in the domain name list.

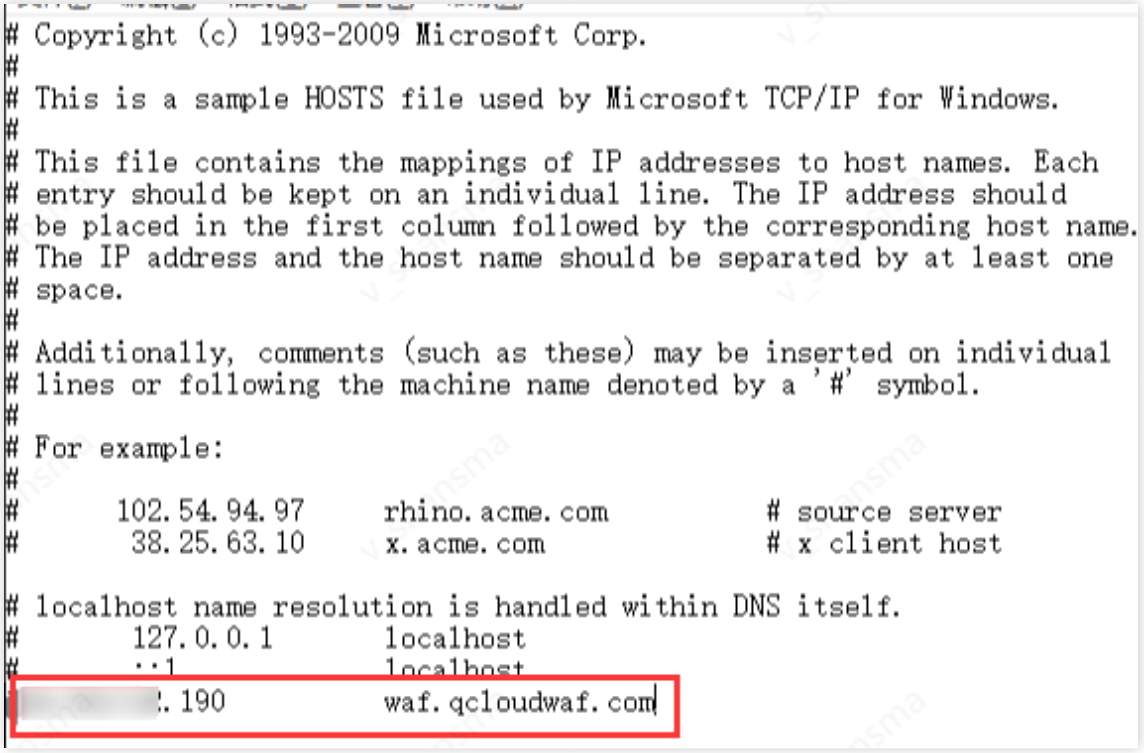
WAF will allocate a unique CNAME to each domain name added to WAF (regardless of whether it is a first-level or second-level domain name).

Step 2: Local Test

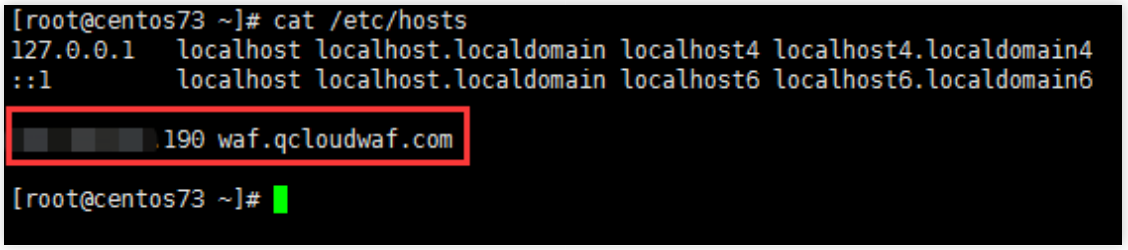
To access the website, DNS resolution should be performed on the local machine. Before that, the IP address corresponding to the target domain name will be obtained from the local hosts file. Therefore, you can modify the hosts file to route local access traffic to WAF. This allows you to test the line connectivity of accessing the website via WAF without directly modifying the DNS resolution record, which could affect public network users' access to the website.

1. Log in to the WAF console. In the left sidebar, select WAF > Protection Settings to view the VIP address of waf.qcloudwaf.com in the domain name list.
2. Modify the hosts file.

- Modify C:\Windows\System32\drivers\etc\hosts on Windows and add entries.
  Format: VIP address + domain name accessing the WAF.



- Modify /etc/hosts on Linux and add entries.
  Format: VIP address + domain name connected to WAF.



3. Perform an access test.
   (1) Access the website on the local computer. If the website can be opened normally, it means that the line connectivity for WAF to access the web origin server is normal.
   (2) Enter the following URL in the browser and access it.

   http://waf.qcloudwaf.com/?test=alert(123)

(3) If the browser redirects to the blocking page, it indicates that the WAF protection feature is normal.

Step 3: DNS Resolution Modification

To use WAF to protect the traffic of websites accessed by public network users, you need to modify the DNS resolution record. The necessary modification to the DNS CNAME record can be performed through the standard DNS modification procedure.

Step 4: Security Group Setting

A security group is a firewall at the instance level provided by the cloud platform that can control the inbound or outbound traffic of any CVM. By setting the security group to permit only traffic from WAF to access the website, attackers can be prevented from bypassing WAF and directly attacking the origin server of the website.
The following example describes the configuration process by allowing the origin-pull IP address 111.230.27.90 of WAF in the security group.

1. Log in to the CVM console. In the left directory, click Security Group.

2. Enter the Security Group page, click Create, fill in the information according to the requirements, select Custom for the template, enter the name of the security group (for example, my-security-group), fill in the relevant notes, and click OK after filling in.

3. In the security group list, find the created security group and click its ID to enter the details page.

4. On the Inbound Rules page, click Add Rule.

5. Fill in the relevant information in the pop-up box, select HTTP (80) as the type, fill in the origin-pull IP that requires allowance, input the port and policy as required, and click Finish after filling in.

6. Click Associated Instance in the tab, and click Add Association on the CVM page.

7. Select the CVM to be bound in the pop-up box and click OK.
   You can also enter the CVM List page to view or modify the security group bound to a CVM. Select the CVM ID that requires security group adjustment on the list page, choose More > Security Group > Configure Security Group in the Operation column on the right side, and select the security group for binding.

CLB WAF

CLB WAF integrates with the layer-7 CLB (listener) cluster through domain name configuration to perform

bypass threat detection and filtering on HTTP or HTTPS traffic transiting through the CLB and realize the separation of workload forwarding and security protection. To implement integrated protection, you need to complete the following steps:

Step 1: Confirming CLB Configuration

CLB WAF detects and intercepts HTTP or HTTPS traffic transiting through the CLB listener by adding a domain name and binding it to the CLB listener. Before accessing the CLB WAF, ensure that your website workload is already on the cloud platform and that the CLB (original application-type CLB with a public network type) is being used. If your website workload is not on the cloud platform, it is recommended that you use SaaS WAF for protection.

To enable CLB WAF to identify the protected domain name, you need to configure the CLB and configure the corresponding domain name in the listener to achieve normal workload forwarding.

This document takes the protection of wow.qcloudwaf.com as an example to view the CLB listener configuration information.

1. Log in to the cloud console, click Cloud Product > Cloud Computing and Network > CLB to enter the CLB console.
2. In the LB Instance List, find the created CLB instance, and click Instance ID to enter the CLB details page.
3. On the CLB Details page, click Listener Management to view the listener domain name configuration information. The listener name is waftest, the protocol is HTTP, and the port is 80.
4. When you create a forwarding rule, set the domain name listened by the listener forwarding rule to wow.qcloudwaf.com , fill in "/" for the URL path, select whether to perform monitoring check and session maintenance, and click Submit to complete the domain name addition. At this point, the domain name protection status is Not Enabled.

Step 2: Adding a Domain Name and Binding It to CLB

Operation Steps

1. Log in to the WAF console. In the left sidebar, select Asset Center > Access Management to enter the Domain Name Access page.
2. On the Domain Name Access page, click Add Domain Name, enter the Add Domain Name page, and select CLB Type.
3. On the Add Domain Name page, fill in the domain name to be protected, select the listener information according to the location of the domain name, configure the proxy situation, and confirm to complete the access.

> Note:
>
> The domain name filled in should be consistent with the added domain name in the CLB listener.

Step 3: Verification Test

1. Ensure that the local computer can access websites normally.
2. Enter the URL http://wow.qcloudwaf.com/?test=alert(123) and access it in the browser.

   > Note:
   >
   > wow.qcloudwaf.com is the domain name in this case. Replace the domain name with the actual added domain name.

3. Log in to the WAF console. In the left sidebar, select Log Service > Attack Logs to enter the Attack Log Query page and perform a log query.
4. Select the domain name added for protection, and click Query. If you see the attack type is "XSS attack", it means the WAF configuration has taken effect.

   > Note:
   >
   > If DNS is not configured for the domain name, see Step 2: Local Test in SaaS WAF Quick Start to verify the access validity.

Operation Guide
List of Features of the Tenant Side

Contents	Page	Feature Item
Security visualization	Overview	Security overview display.
		Attack overview display.
		Basic security analysis display.
		Workload operation analysis display.
		Display the TOP 5 (times) of web attacks on domain names.
		Display the TOP 5 (times) of CC attacks on domain names.
		Display the TOP 5 (times) of attack source IP addresses.
		Display the attack type proportion.
		Display the attack source region distribution (times).
Log service	Attack log	Log service (original data display).
		Search logs.
		Download logs.
Asset center	Access management	Add domain names.
		Delete domain names.
		Edit domain names.
		Display the domain name list.
		WAF switch.
	Instance management	Create instances.
		Delete instances.
		Manage domain names.
Configuration center	Basic security	Customization of the returned interception page.
		Protection mode selection.

		Protection level selection.
		Malicious file detection.
		IP blocking settings, including the number of web attacks, detection duration, and blocking duration.
		TIGA rule list.
		TIGA rule search.
		Single TIGA rule switch.
		Add a TIGA rule to the allowlist.
		Regional blocking.
		Access control rule management.
		CC protection.
		Webpage anti-tampering.
		Information leakage prevention.
	Blocklist/Allowlist	IP blocklist.
		IP allowlist.
		Precise allowlist.
		Rule allowlist.
Service management	Web rule base	Protection rule list.
	Audit log	Call WAF API log list in the console.

CLB WAF Domain Name Access

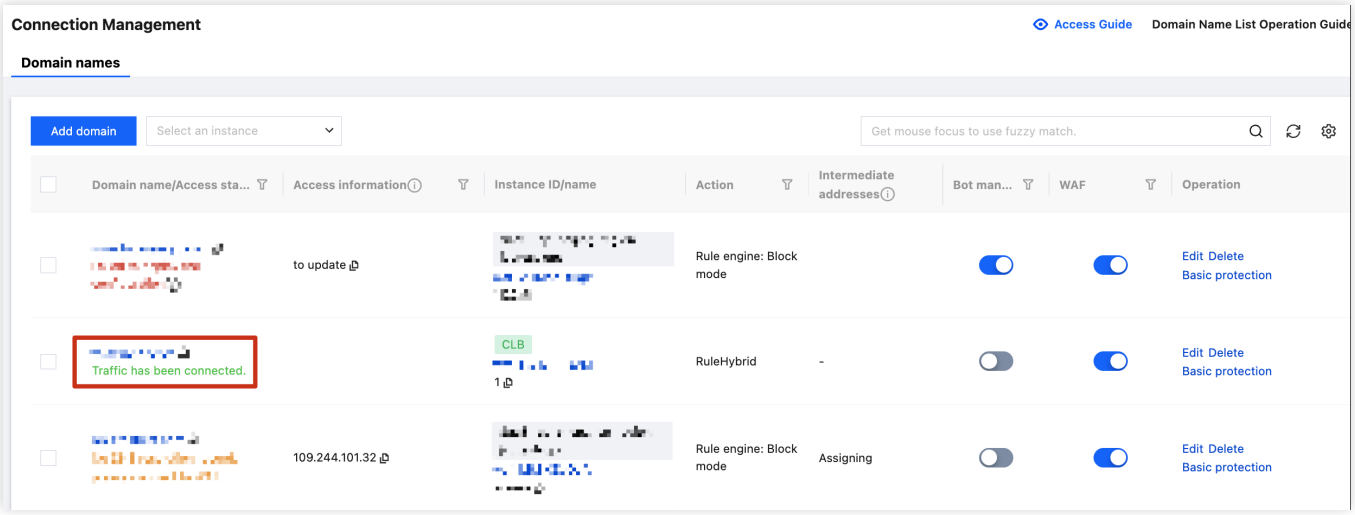
CLB WAF integrates with the layer-7 CLB (listener) cluster through domain name configuration to perform bypass threat detection and filtering on HTTP or HTTPS traffic transiting through the CLB and realize the separation of workload forwarding and security protection. To implement integrated protection, you need to complete the following steps:

Step 1: Confirming CLB Configuration

CLB WAF detects and intercepts HTTP or HTTPS traffic transiting through the CLB listener by adding a domain name and binding it to the CLB listener. Before accessing the CLB WAF, ensure that your website workload is already in the tenant's VPC and that the CLB (original application-type CLB with a public network type) is being used.
If your website workload is not using CLB, it is recommended that you use SaaS WAF for protection.

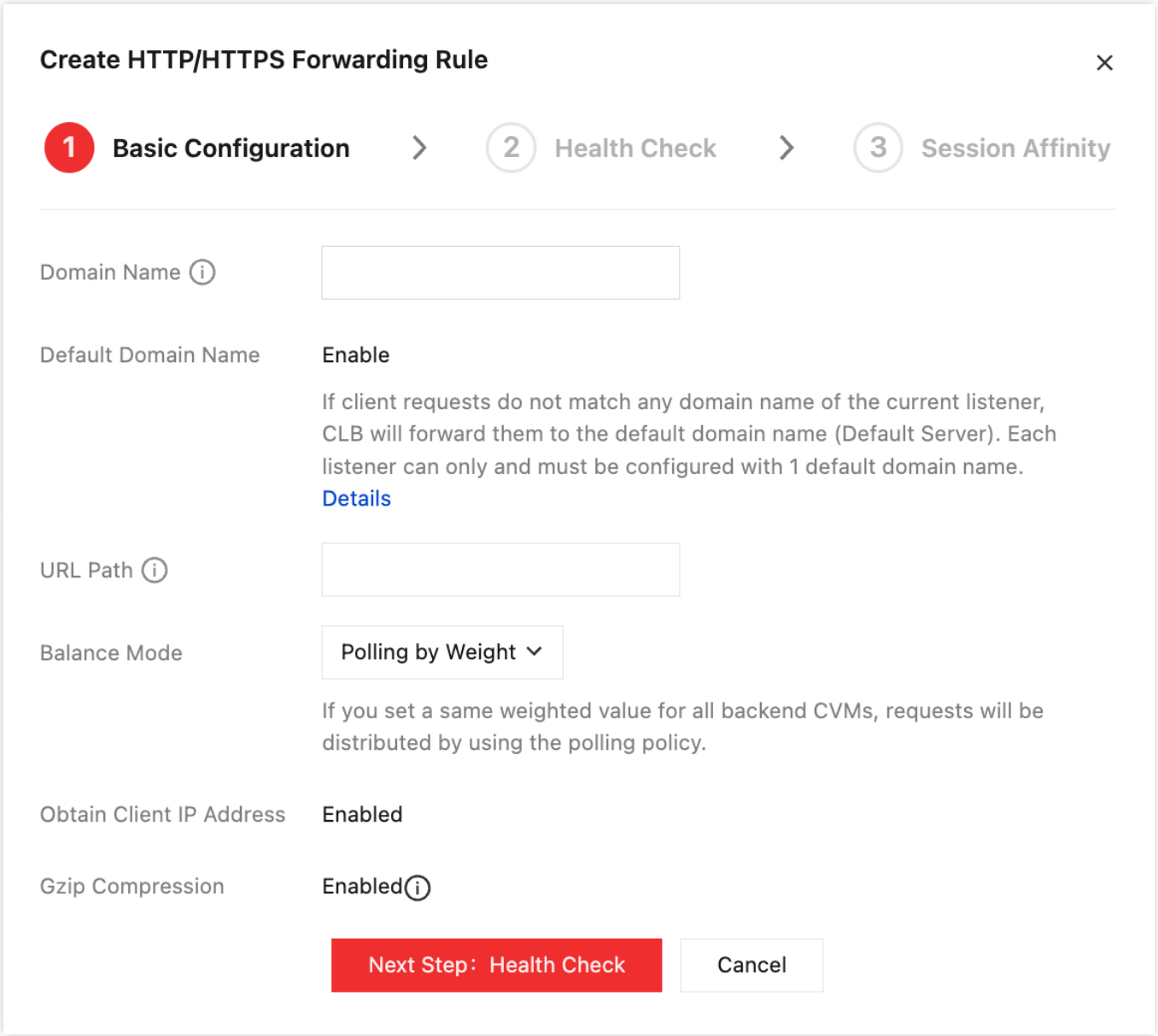
To enable CLB WAF to identify the protected domain name, you need to configure the CLB and configure the corresponding domain name in the listener to achieve normal workload forwarding.
This document takes the protection of wow.qcloudwaf.com as an example to view the CLB listener configuration information.

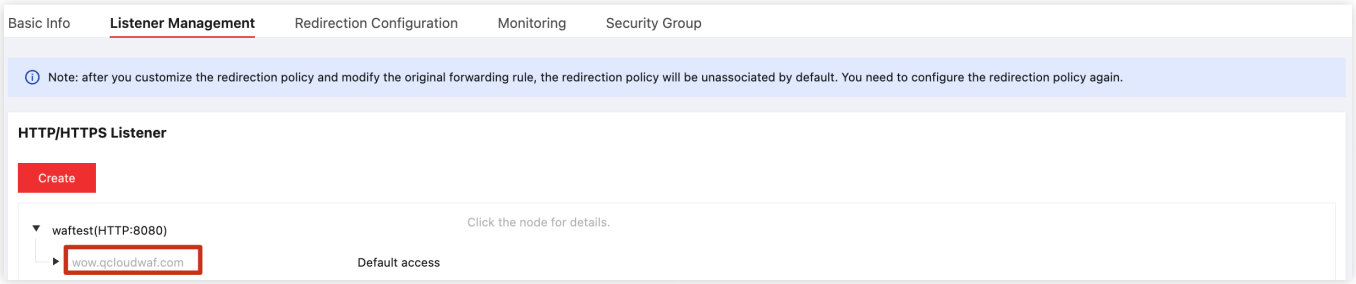
1. Log in to the tenant side console on the cloud platform, choose Cloud Product > Cloud Computing and Network > CLB to enter the CLB console.
2. In the LB Instance List, find the created CLB instance clb-test, and click Instance ID to enter the CLB details page.
3. On the CLB Details page, click Listener Management to view the listener domain name configuration information. The listener name is waftest, the protocol is HTTP, and the port is 80.



4. When you create a forwarding rule, set the domain name listened by the listener forwarding rule to wow.qcloudwaf.com , fill in "/" for the URL path, select whether to perform monitoring check and session

maintenance, and click Submit to complete the domain name addition. At this point, the domain name protection status is Not Enabled.





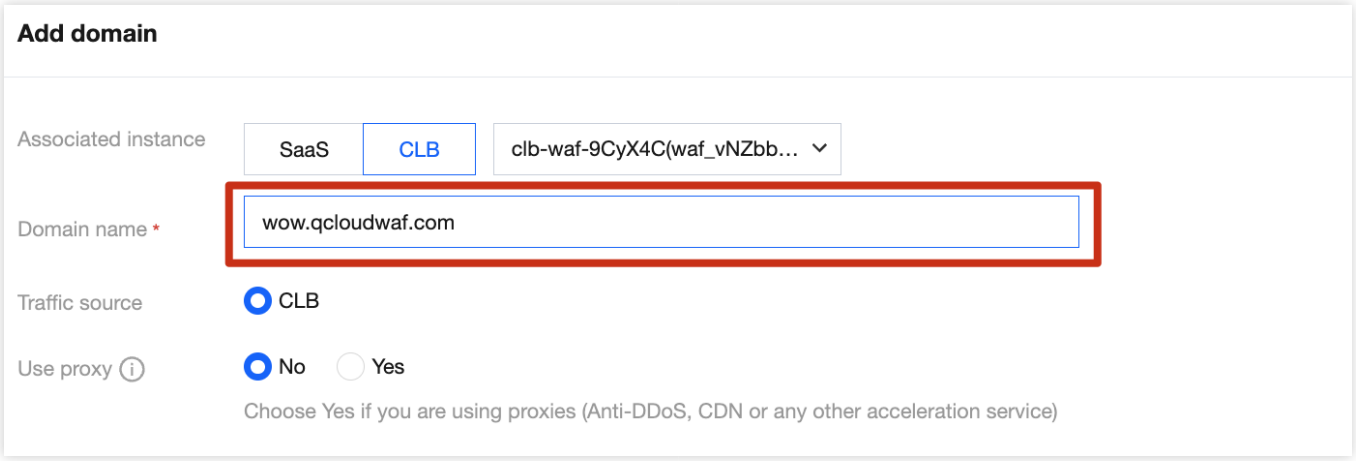
Step 2: Adding a Domain Name and Binding It to

CLB

1. Log in to the WAF console. In the left sidebar, select Asset Center > Access Management to enter the Domain Name Access page.

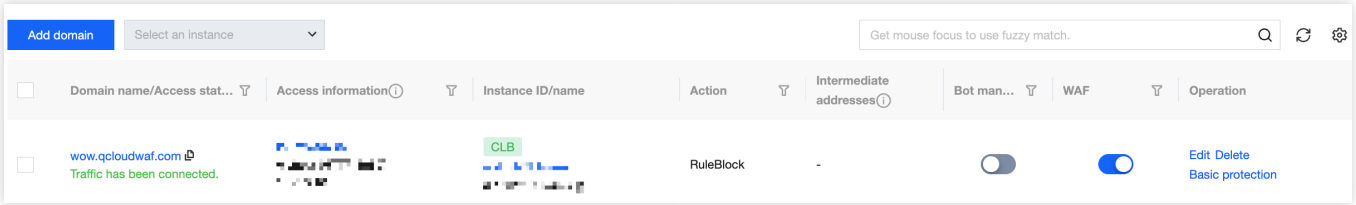
2. On the Domain Name Access page, click Add Domain Name, enter the Add Domain Name page, and select CLB Type.

3. On the Add Domain Name page, fill in the domain name to be protected, select the listener information according to the location of the domain name, configure the proxy situation, and confirm to complete the access.



> Note:
>
> The domain name filled in should be consistent with the added domain name in the CLB listener.

4. After binding, click Complete at the bottom of the page to return to the domain name list. In the domain name list, you can view the protected domain name wow.qcloudwaf.com and the CLB ID, name, VIP, and listener information of the CLB.



Step 3: Verification Test

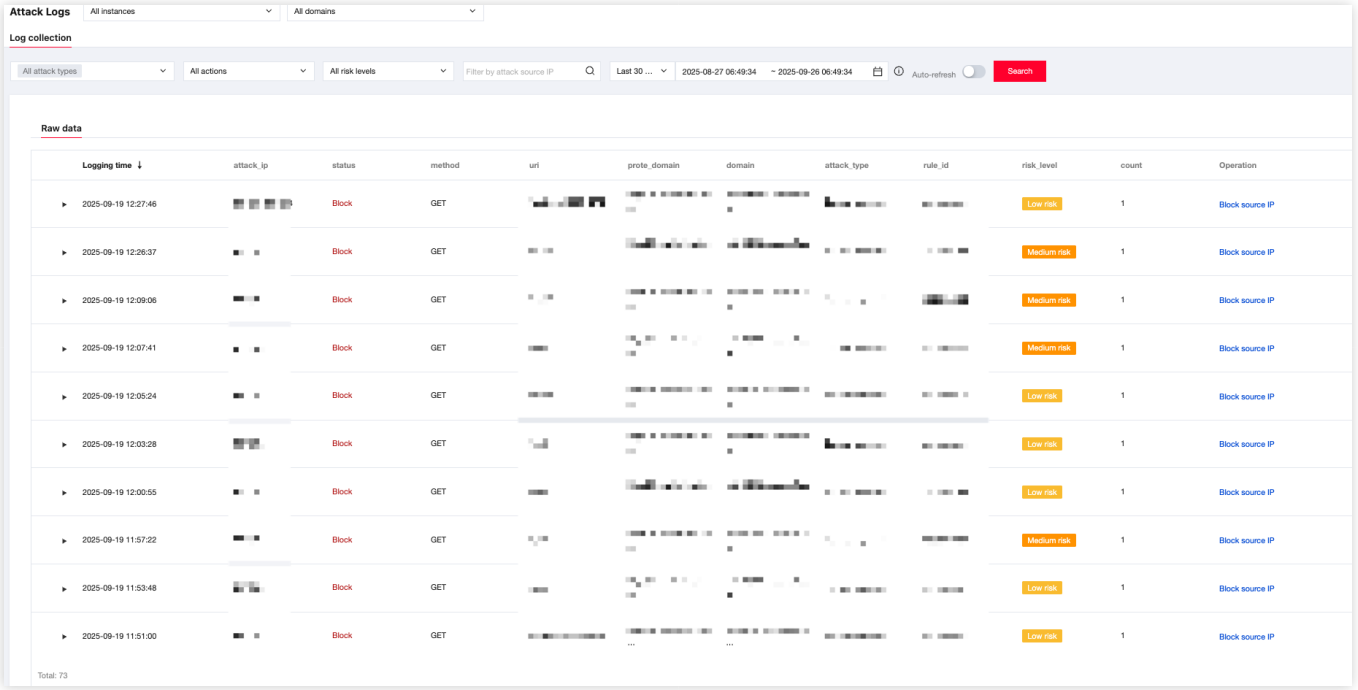
1. Ensure that the local computer can access websites normally.

2. Enter the URL http://wow.qcloudwaf.com/?test=alert(123) and access it in the browser.

> Note:
>
> wow.qcloudwaf.com is the domain name in this case. Replace the domain name with the actual added domain name.

3. Log in to the WAF console. In the left sidebar, choose Log Service > Attack Logs to enter the Attack Log Query page and perform a log query.

4. Select the domain name added for protection, and click Query. If you see the attack type is "XSS attack", it means the WAF configuration has taken effect.



> Note:
>
> If DNS is not configured for the domain name, see Step 2: Local Test in SaaS WAF Quick Start to verify the access validity.

Rule Engine

This document describes how to perform rule protection settings through WAF to protect against web attacks.

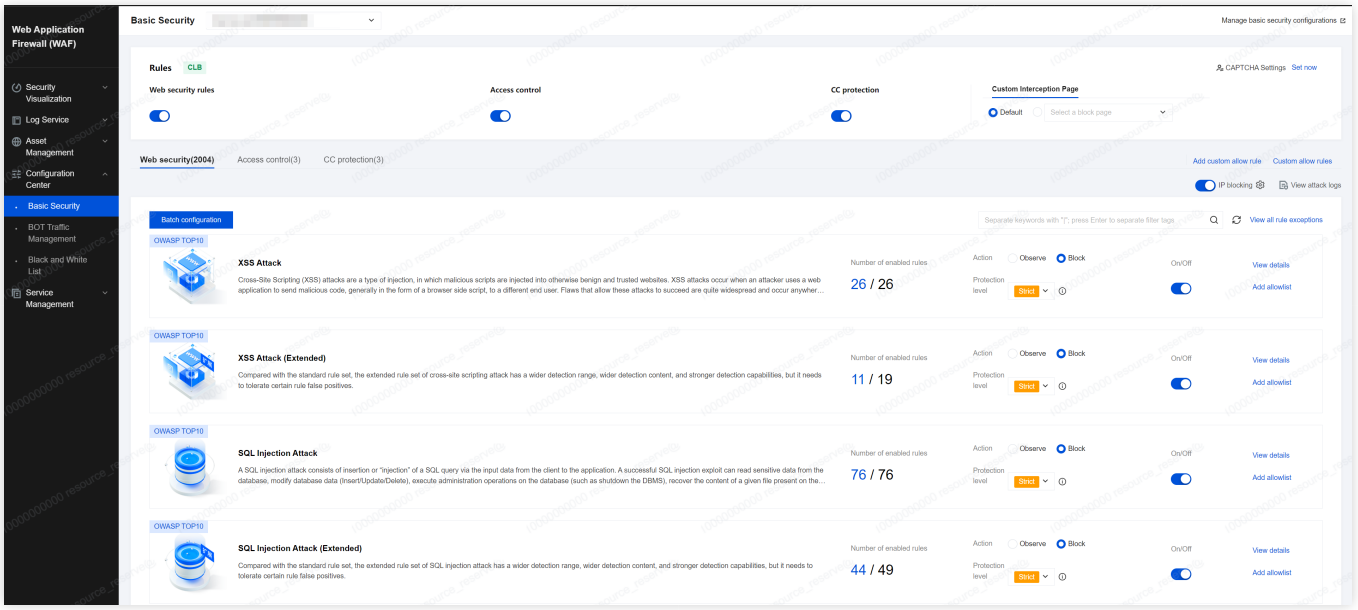
Background Information

WAF uses a rule protection engine based on regular expressions and an AI protection engine based on machine learning to protect against web vulnerabilities and unknown threats.
The WAF rule protection engine provides expert rule sets based on our accumulated web threat intelligence to prevent OWASP top 10 attacks. Currently, it can defend against 12 categories of common web attacks, such as SQL injections, XSS attacks, malicious scans, command injection attacks, web application vulnerabilities, WebShell uploads, non-compliant protocols, Trojans, and backdoors.
The WAF rule protection engine supports rule level configuration. You can configure the rule protection level according to your actual business needs, and enable or disable rule sets, individual rules, and preset rules. You can also use the allowlist of specified URLs and rule IDs to process false positives.

Operation Steps

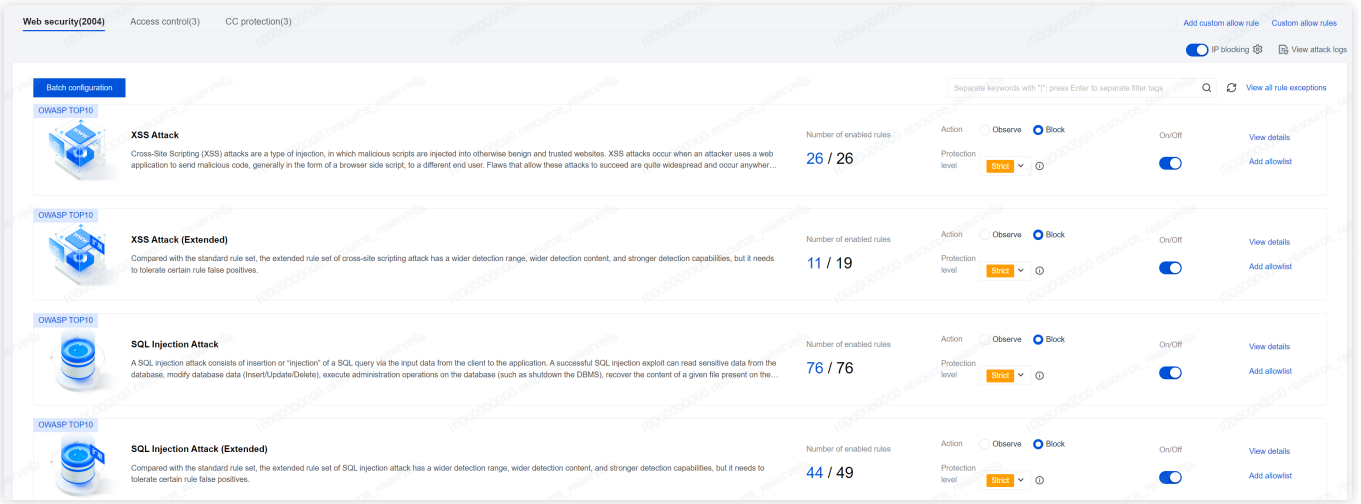
Settings of Domain Name Rule Protection Engine

1. Log in to the WAF console. In the left sidebar, select Configuration Center > Basic Security > WEB Security.
2. On the protection settings page, configure the protection mode, protection level, and malicious file detection method for basic web protection. On this page, you can also enable the scan protection feature and set IP address blocking rules.



Field description:

- Rule Engine Switch: The switch is turned on by default. When it is turned off, requests for domain names passing through WAF will not undergo threat processing by the rule engine.
- Protection Mode: Rule engine operation mode, which is set to Interception by default.
- Observation: Does not block attack requests, but triggers alarms and generates observation logs.
- Interception: Directly blocks web attack requests and generates interception logs.
- Protection level: Rule engine protection level, which is normal by default.
    - Normal: detects common web application attacks. If you notice excessive false interceptions at the default level, or if your workload involves significant uncontrolled user input (such as websites with rich text editors), it is recommended that you select this mode.
    - Strict: strictly detects web application attacks such as SQL injections, XSS attacks, and command execution. It is the default mode.
- Rule management: Through rule management, users can view rule engine information and set the rule engine, including viewing attack classifications, viewing rule content included in rule levels and rule set update dynamics, enabling or disabling single rules, and adding rules to the allowlist based on domain name URLs and rule IDs.
- Supported decoding types: The rule engine currently supports the following decoding types by default and does not support manual configuration.
- URL decoding (multiple decoding), JavaScript Unicode decoding, comment processing, whitespace compression, UTF-7 decoding, HTML entity decoding, Multipart parsing, JSON parsing, XML parsing, and Form parsing.
- Batch configuration: Supports unified default settings for multiple threat types.

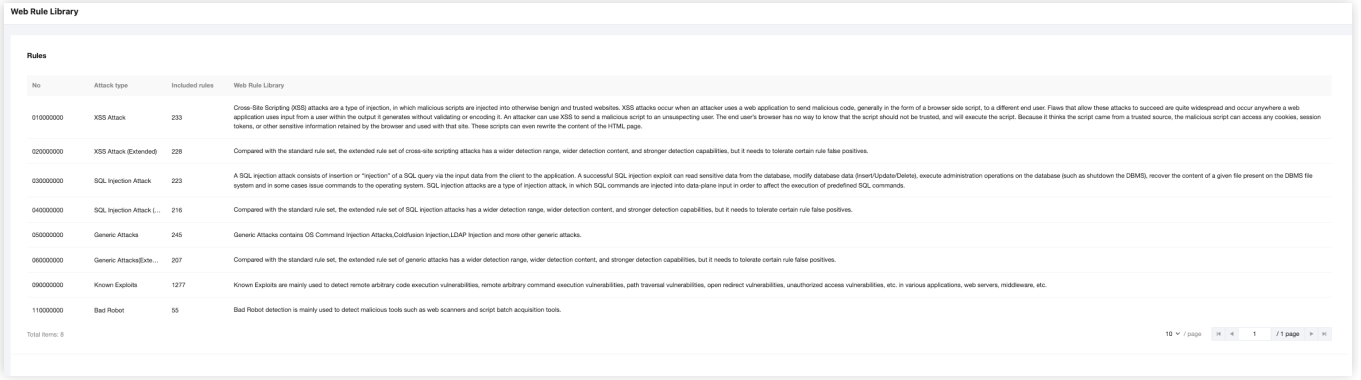


Viewing rule classifications

1. Enter the Rule Engine Settings page.

- Method 1: Log in to the WAF console. In the left sidebar, choose Asset Center > Access Management to go the domain name list management page. Select any domain name and click Protection Configuration in the Operation column to go to the web security protection configuration page of the domain name and view rule details.
- Method 2:
- a. Log in to the WAF console. In the left sidebar, choose Configuration Center > Basic Security.
- b. In the domain name list, click the domain name to be protected to go to the web security settings page, and then go to the rule engine page.

2. Enter the Rule Base Management page.
   Log in to the WAF console. In the left sidebar, choose Service Management > Web Rule Base to view descriptions of attack categories currently protected by WAF and updates on rules.



The attack classifications supported by the current WAF for protection are as follows:

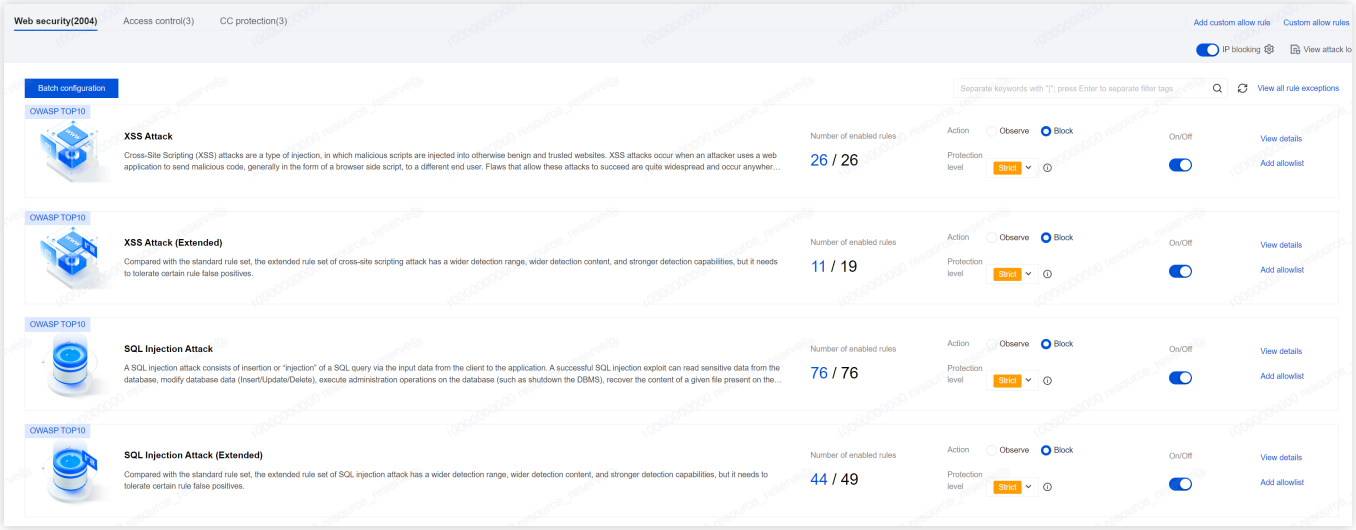
Attack	Attack Description

Classification	
XSS attack	XSS attacks are a type of injection where malicious scripts are injected into other trusted websites. An XSS attack occurs when an attacker uses a web application to send malicious code (typically in the form of a browser-side script) to a different end user. Flaws that allow these attacks to succeed are widespread and occur wherever a web application uses input from a user within its generated output without validating or encoding it. Attackers can use XSS to send malicious scripts to unsuspecting users. The end user's browser has no way of knowing that the script should not be trusted and will execute it. Since it believes the script comes from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of HTML pages.
XSS attack (extended)	The extended rule set of XSS attacks has a broader detection range, wider detection content, and stronger detection capability compared with the standard rule set, but it needs to tolerate certain rule false positives.
SQL injection attack	SQL injection attacks include inserting or "injecting" SQL queries through input data from the client to the application. A successful SQL injection vulnerability can read sensitive data from the database, modify (insert/update/delete) database data, perform management operations on the database (such as shutting down the DBMS), recover the content of a given file existing in the DBMS file, and issue a command to the operating system in some cases. The SQL injection attack is a type of injection attack where SQL commands are injected into data plane inputs to impact the execution of predefined SQL commands.
SQL injection attack (extended)	The extended rule set for SQL injection attacks has a broader detection range, wider detection content, and stronger detection capabilities compared to the standard rule set, but requires tolerance for a certain degree of rule false positives.
General attack	General attacks include operating system command injection attacks, Coldfusion injections, LDAP Injections, and other general attacks.
General attack (extended)	The extended rule set of general attacks has a broader detection range, wider detection content, and stronger detection capability compared with the standard rule set, but it needs to tolerate certain rule false positives.
Known weakness	Known weaknesses are primarily used to detect various remote code execution vulnerabilities, remote command execution vulnerabilities, path traversal vulnerabilities, open redirect vulnerabilities, and unauthorized access vulnerabilities occurring in applications, web servers, and middleware.
Bad bot	Bad bot detection is primarily used to detect malicious tools such as web scanners and batch script obtaining tools.

Rule management

1. Log in to the WAF console. In the left sidebar, choose Configuration Center > Basic Security, select the domain name to be managed, and then go to the web security page.
2. On the web security management page, enable or disable rules, set Protection Mode to Observation, and add rules to the allowlist.

Remarks: The interception mode is enabled for all rules by default.



3. Users can search for rule sets according to Rule Level, Attack Classification, and CVEID, or by entering Rule ID, and view specific rules and perform operations.

> Note:
>
> The strict rule level includes normal and strict rules.

CC Protection Settings

Feature Introduction

CC protection provides access protection for specific URLs on a website.

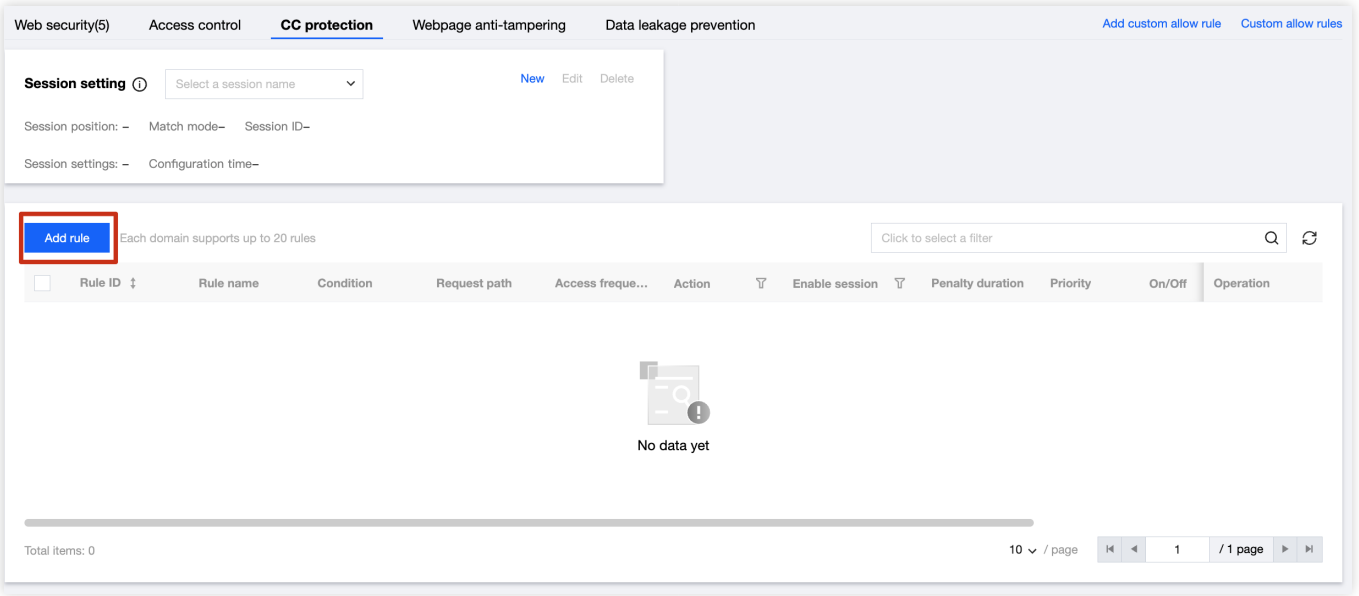
- To use the CC protection policy based on SESSION, you need to perform SESSION settings before setting the policy.

Configuration Steps

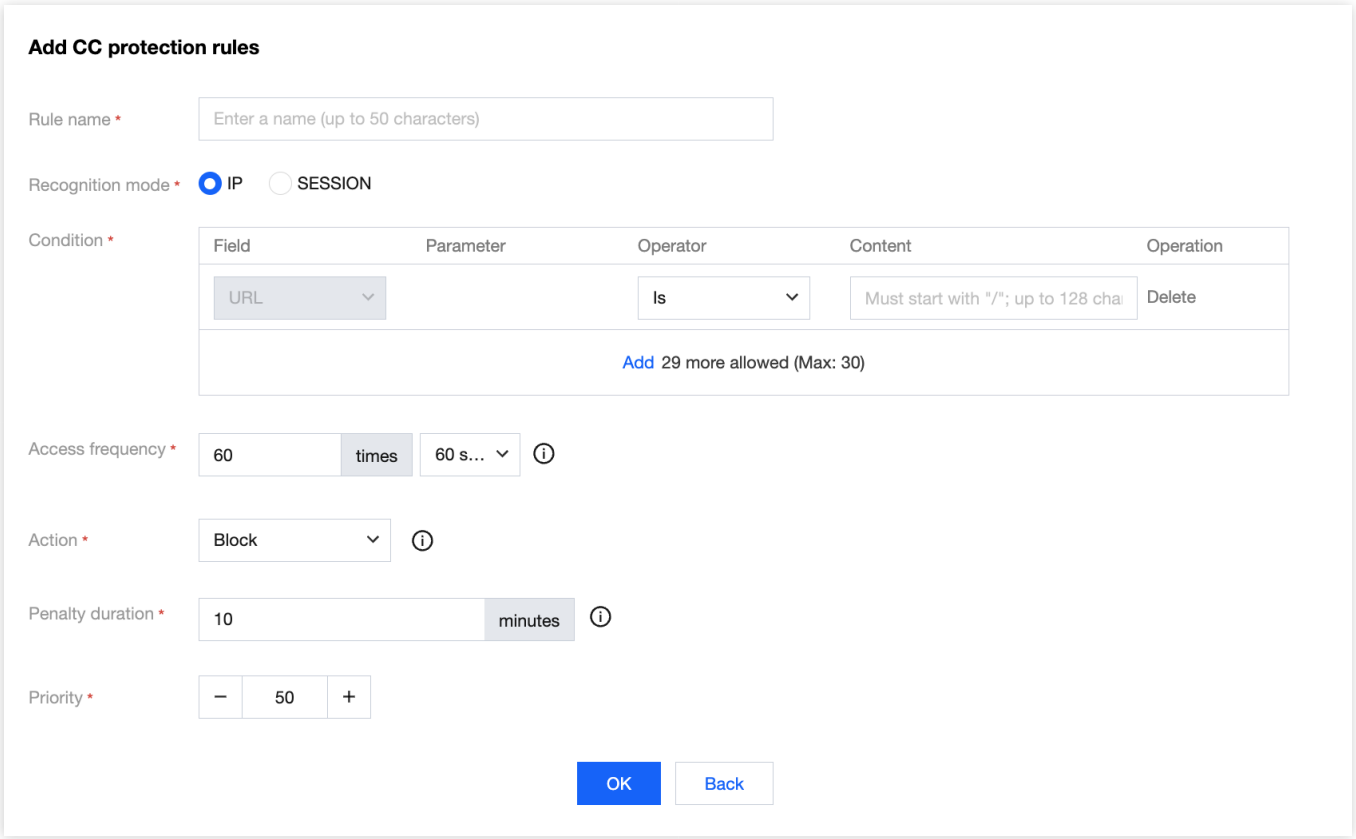
Example 1: CC Protection Settings Based on the Source IP

For IP-based CC protection policies, you can directly configure them without the need to set the SESSION dimension.

1. Log in to the WAF console. In the left sidebar, choose WAF > Configuration Center > Basic Security. Select a protected domain name and click to select CC Protection to enter the configuration page.



2. Click Add Rule. Users can customize the CC Protection Rule page and fill in the corresponding information.



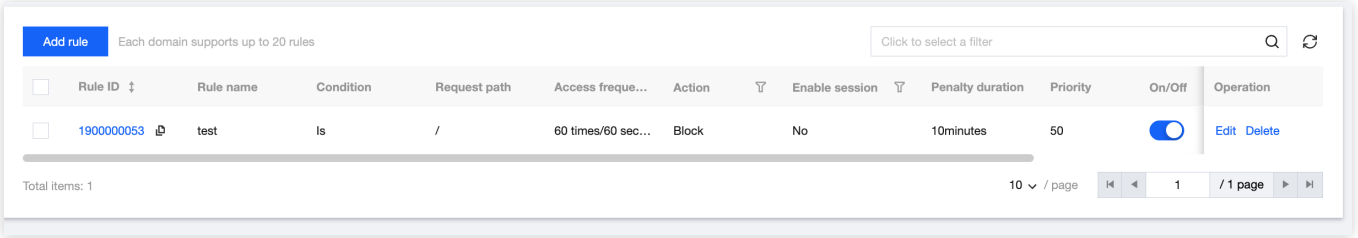
Configuration item description:

- Identification mode: IP and SESSION.
- Matching condition: Including equal, prefix matching, and contained.

Advanced configuration:

- Matching method: Set according to all matching fields in the custom rule.
- Access frequency: Set access frequency according to workload conditions. The recommended input is 3 to 10 times the normal access speed. For example, if the website is accessed 20 times per minute on average, it can be configured as 60 to 200 times per minute, adjustable according to the severity level of the attack.
- Execution action: Observing, human-machine recognition, and blocking.
- Penalty duration: No shorter than one minute and no longer than one week.
- Priority: Enter an integer from 1 to 100. The smaller the number, the higher the execution priority of this rule. Under the same priority, the later the creation time, the higher the priority.

1. Perform rule operations. You can select the created rule and disable, modify, and delete the rule.

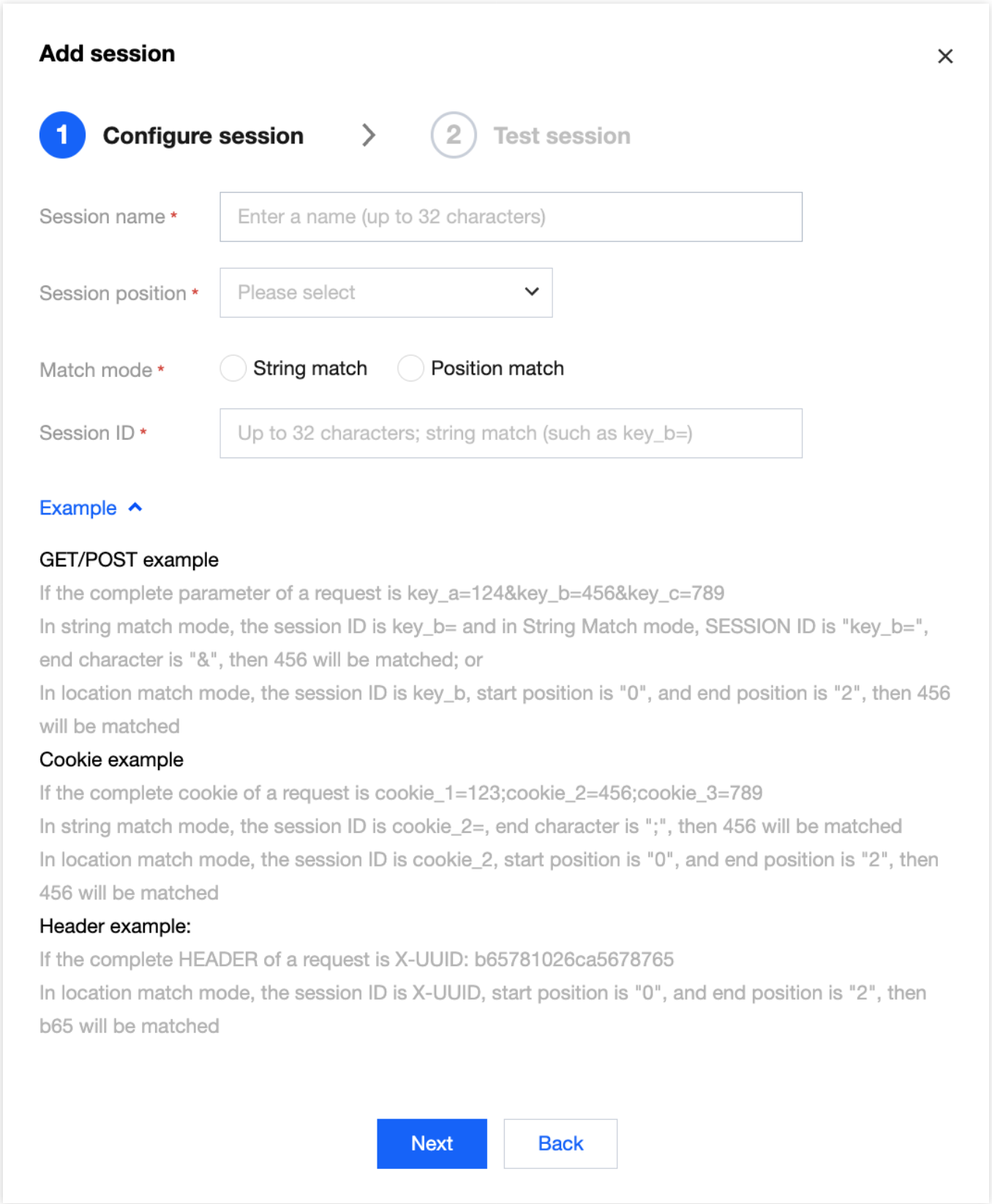


2. According to the rule settings, you can see the interception page returned by WAF after the CC attack protection rule is triggered.
3. View real-time IP blocking information. In the left sidebar, select IP Management > IP Blocking Status to view real-time blocked IP information and add the IP to the allowlist or blocklist.

Example 2: CC Protection Settings Based on SESSION

CC protection based on the SESSION access rate can effectively solve the issue of misinterception caused by users using the same egress IP address in office networks, supermarkets, and public WIFI scenarios.

1. Enter the WAF console. In the left sidebar, choose WAF > Configuration Center > Basic Security. Select a protected domain name and click to select CC Protection to enter the configuration page.
2. Click Add in CC Protection Settings, and you can customize the SESSION field settings.



3. Enter the SESSION Settings page. In this example, COOKIE is selected as the test content. The identifier is security, the start position is 0, and the end position is 9. After completing the configuration, click Set.

Configuration item description:

- SESSION location: You can select COOKIE, GET, or POST. Among them, GET or POST refers to HTTP request content parameters rather than HTTP header information.
- Matching description: Match by location or string.
- SESSION identifier: Value identifier.
- Start position: The start position of a string or location match.
- End position: The end position of a string or location match.

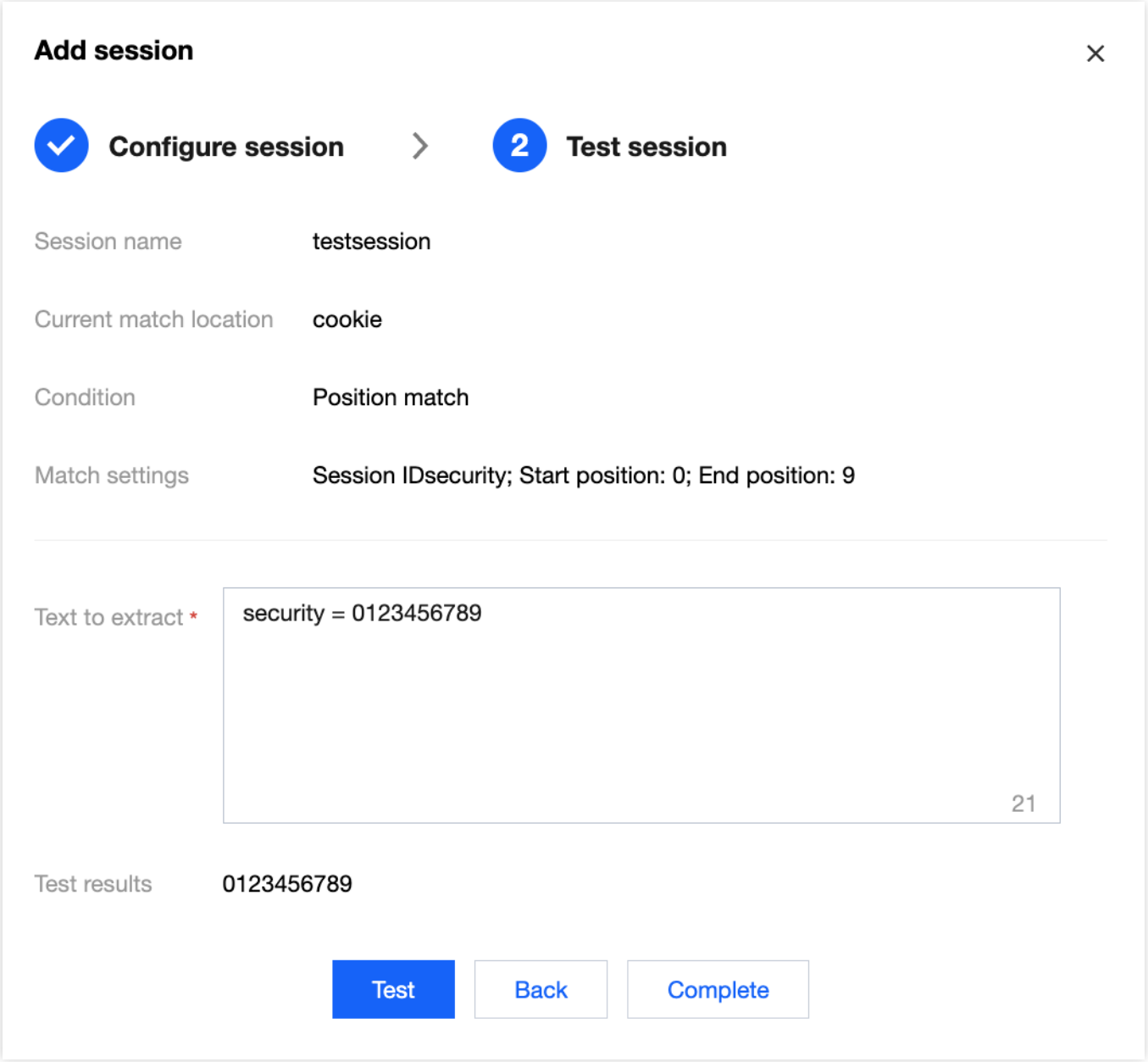
GET/POST example:
If the complete parameter content of a request is: key_a = 124&key_b = 456&key_c = 789:

- Under the string matching mode, if the SESSION identifier is key_b = and the end character is &, the matching content is 456.
- Under the position matching mode, if the SESSION identifier is key_b, the start position is 0, and the end position is 2, the matching content is 456.

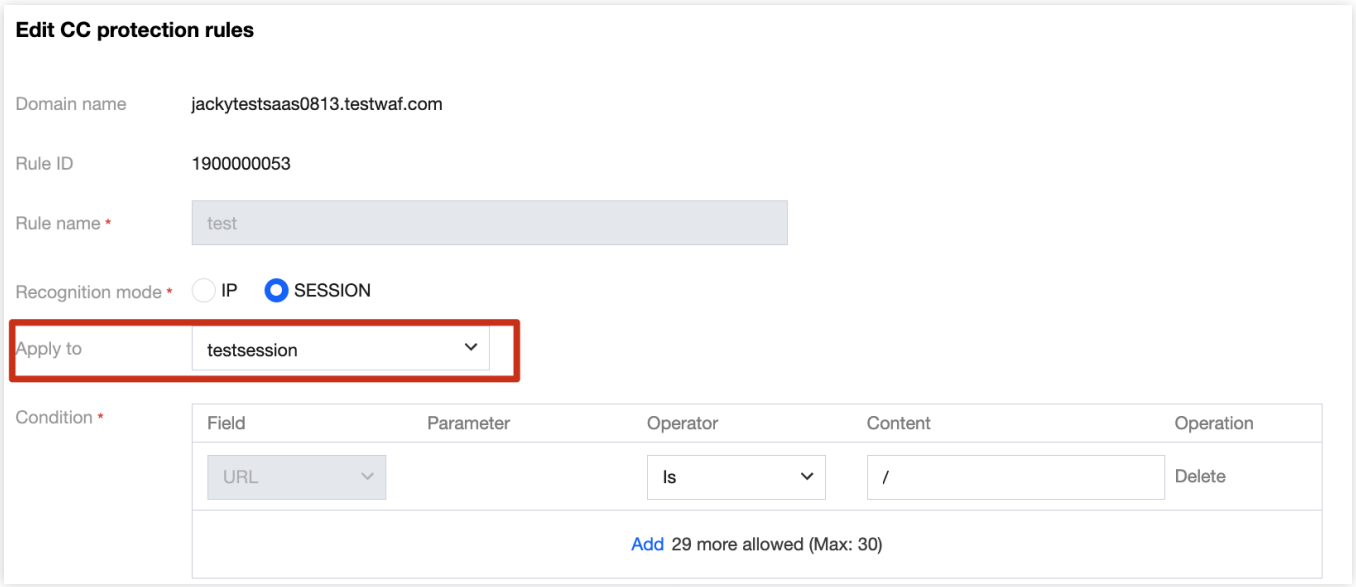
COOKIE example:
If the complete COOKIE content of a request is: cookie_1 = 123;cookie_2 = 456;cookie_3 = 789:

- Under the string matching mode, if the SESSION identifier is cookie_2 = and the end character is ";", the matching content is 456.
- Under the position matching mode, if the SESSION identifier is cookie_2, the start position is 0, and the end position is 2, the matching content is 456.

1. Perform a SESSION dimension information test. After addition, click Test to test the filled content.



2. Set the CC protection policy based on SESSION. The configuration process is consistent with Example 1. Select SESSION as the identification mode.



3. The configuration is completed, and the CC protection policy based on SESSION takes effect.
   If you use the CC protection mechanism based on SESSION, you cannot view blocking information in the IP blocking status.

Custom Policy

Feature Introduction

Custom policies support combining multiple characteristics of HTTP messages such as the request path, GET parameters, POST parameters, Referer, and User-Agent, and controlling the access of public network users through characteristic matching. Facing various attack behaviors from the Internet, users can use custom policies to respond flexibly and combine targeted rules to block these attack behaviors.

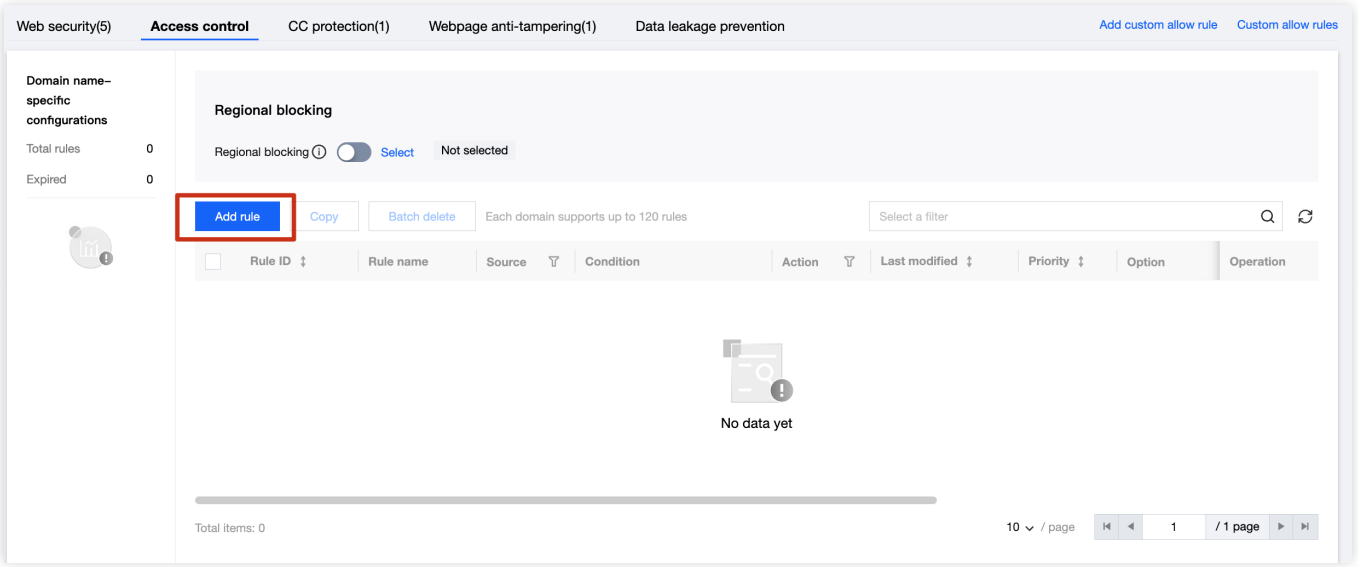
- Each custom policy can be set up to 5 conditions for characteristic control.
- The relationship between multiple conditions in each custom policy is "and", that is, all conditions should be matched for the policy to take effect.
- Two processing actions can be configured after each custom policy is matched: blocking and allowing.
- Effective mode: Four different configuration options are supported: immediate, custom, weekly, and monthly.
- Priority: The smaller the priority value, the higher the priority. That is, 1 represents the highest priority and 100 represents the lowest priority.

Configuration Cases

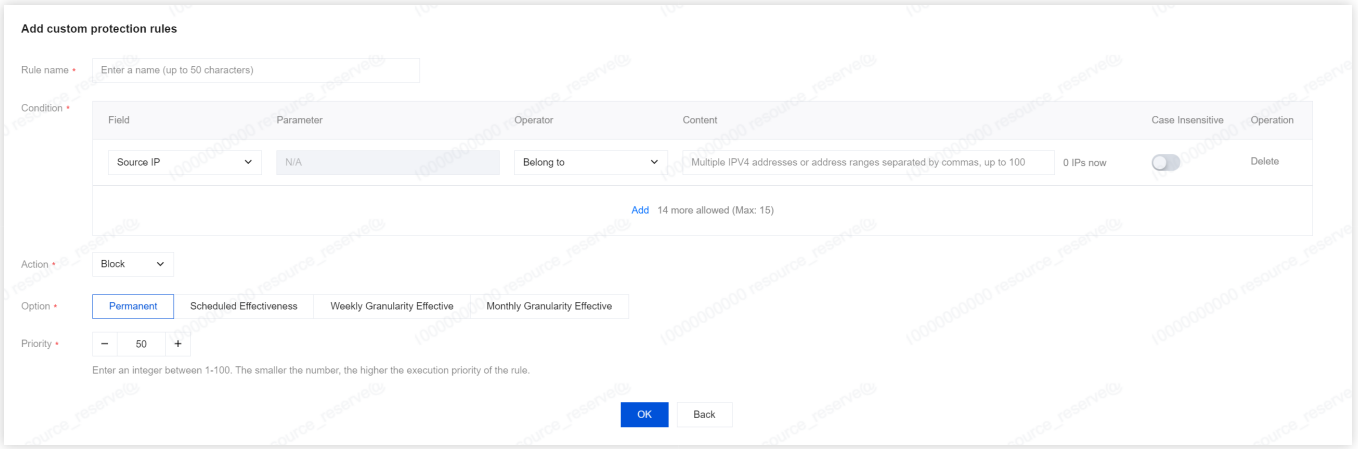
Case 1: Prohibiting a Specific IP Address from Accessing a Specific Site

When website administrators need to prohibit a specific IP address from accessing a specified site, they can perform the following configurations:

1. Log in to the WAF console. In the left sidebar, select WAF > Configuration Center > Basic Security. Select a protected domain name (such as www.qcloudwaf.com) and click to select Access Control to enter the configuration page.

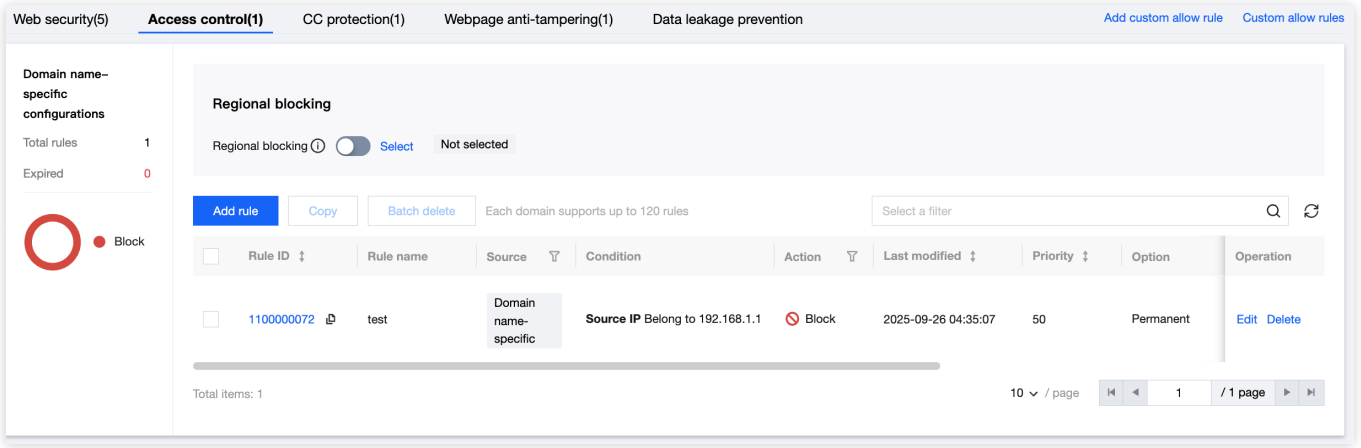


2. On the Add Rule page, enter a rule name (such as 001). Select a field (such as Source IP) in the matching field and select Match for the logical symbol. Fill in the source IP to be blocked in the matching content (such as 192.168.1.1) and select an execution action (such as Block). After completing, click Add to save the rule.



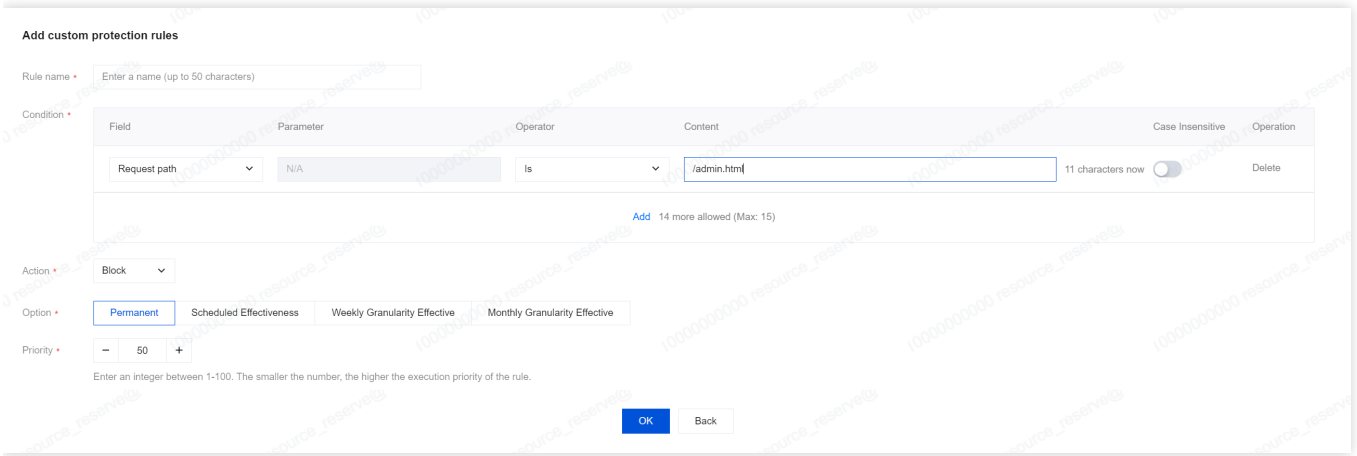
The custom policy of WAF supports using masks to control access requests from source IP addresses in a specific IP range. We can enter a specific IP range in the matching content (such as 10.10.10.0/24).

3. The rule will take effect. HTTP access requests from the specific source IP will be blocked.



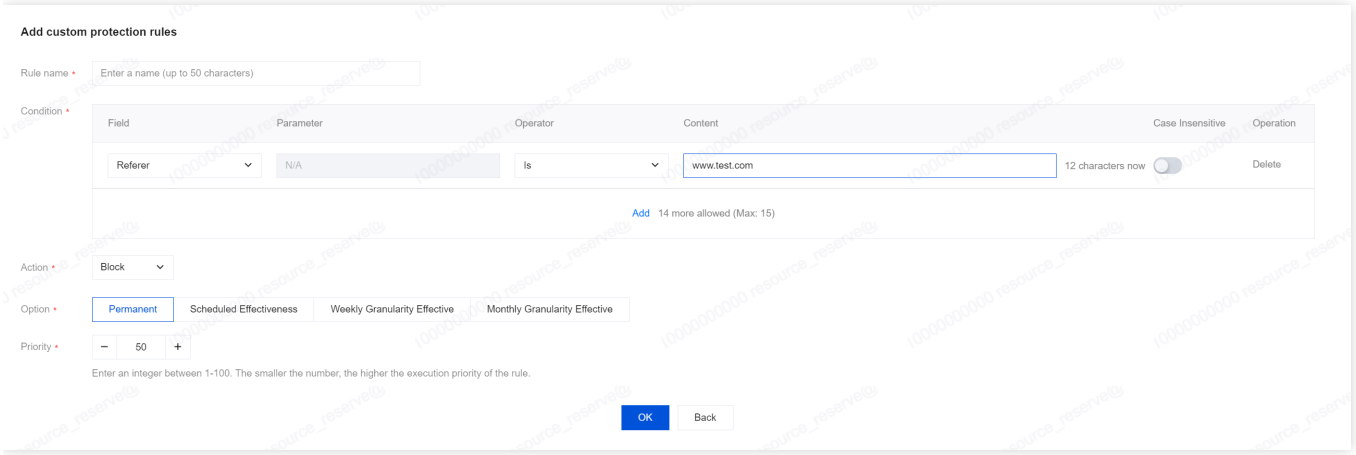
Case 2: Prohibiting Public Network Users from Accessing Specific Web Resources

When website administrators do not want public network users to access certain specific web resources (such as the management backend /admin.html), they can perform the following configurations: Set the matching field to Request Path, set the logical symbol to Equal, fill in /admin.html as the matching content, and set the the execution action to Block. After the configuration is completed, click Add.



Case 3: Prohibiting an External Site from Obtaining Resources Through Hotlink

When website administrators need to block hotlink activities from an external site (such as www.test.com), they can use custom policies to capture and block the Referer characteristics of hotlink requests. The configurations are as follows: Set the matching field to Referer, set the logical symbol to Contain, fill in www.test.com as the matching content, and set the execution action to Block. After the configuration is completed, click Add.


Add custom protection rules
Rule name *
Enter a name (up to 50 characters)
Condition *
Field
Parameter
Operator
Content
Case Insensitive
Operation
Referer
N/A
Is
www.test.com
12 characters now
Delete
Add 14 more allowed (Max: 15)
Action *
Block
Option *
Permanent
Scheduled Effectiveness
Weekly Granularity Effective
Monthly Granularity Effective
Priority *
50
Enter an integer between 1-100. The smaller the number, the higher the execution priority of the rule.
OK
Back

Webpage Anti-Tampering

Feature Introduction

The anti-tampering feature can be used to prevent the specified page from being tampered with and displaying abnormally.
The specified page is limited to .html , .shtml , .txt , .js , .css , .jpg , .png , and other static resources.

> Note:
>
> CLB WAF instances currently do not support this feature.

Prerequisites

A cloud platform SaaS WAF instance has been created, and the domain name has been connected to the SaaS WAF instance.

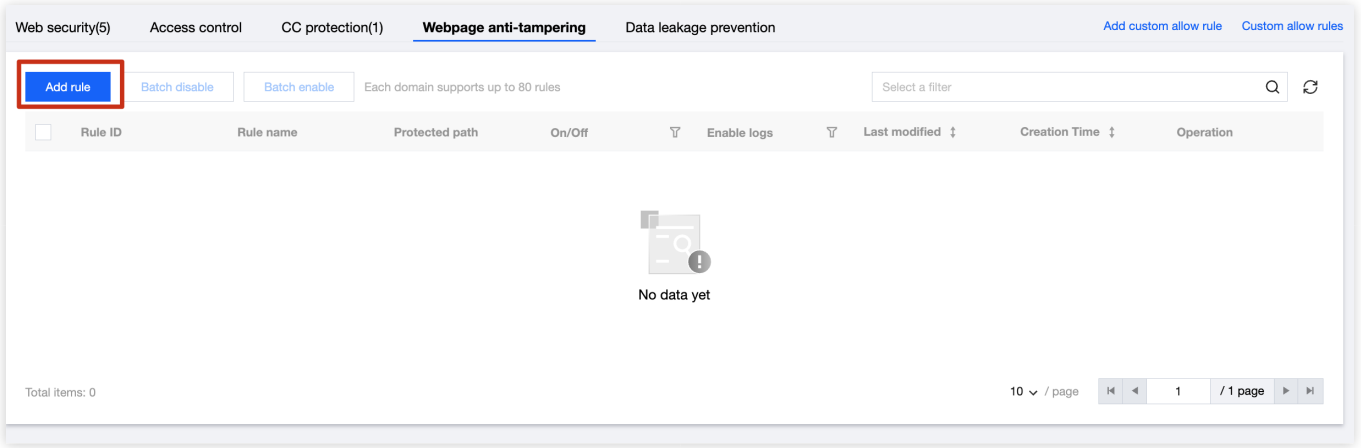
Configuration Example

Protecting Website Homepage from Tampering

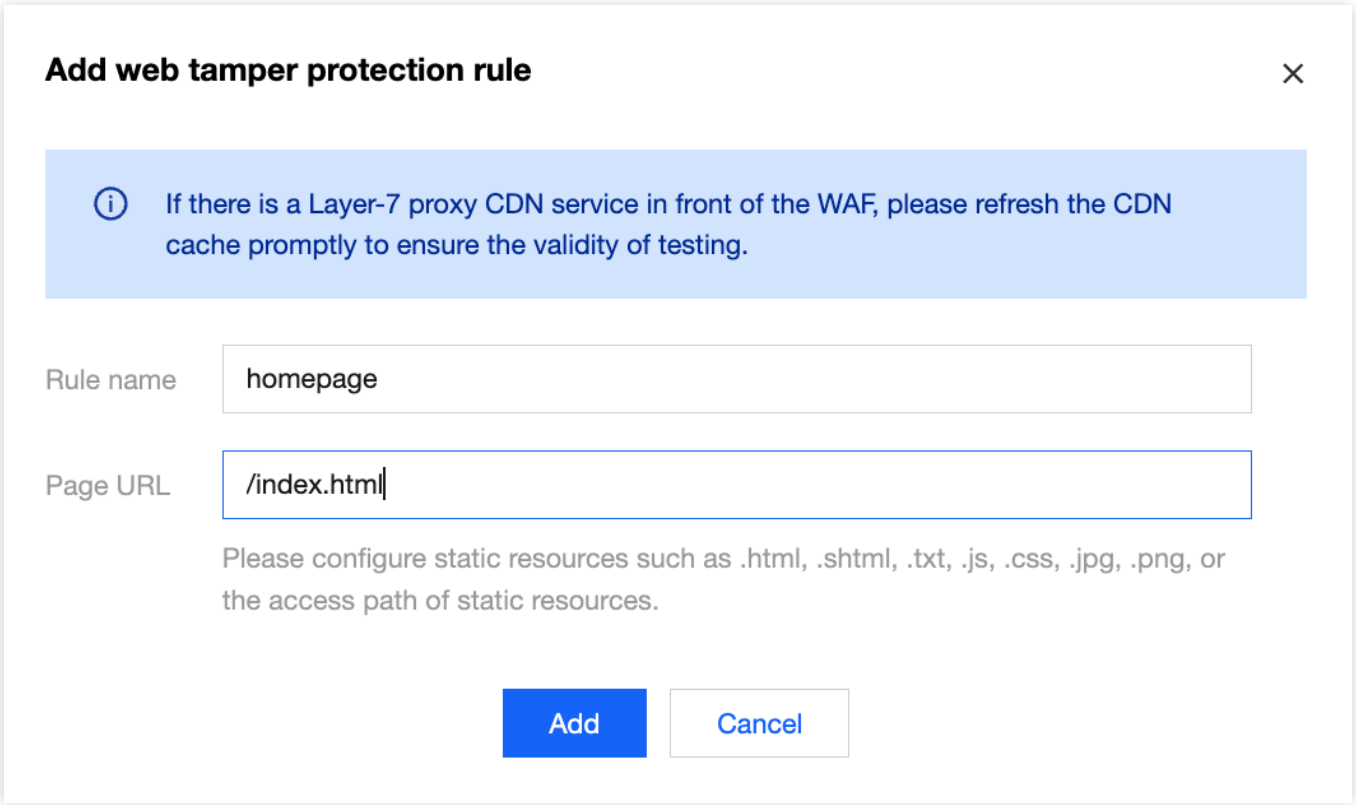
1. Log in to the WAF console. In the left sidebar, choose WAF > Configuration Center > Basic Security, select the domain name to be protected (such as www.qcloudwaf.com), and click Anti-tampering to go to the configuration page.



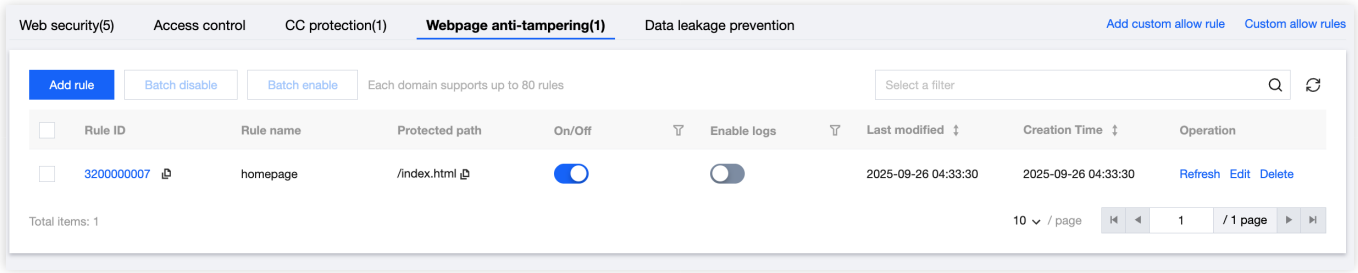
2. Enter the Protection Settings page. If required, replace the domain name of the site to be protected at the top. Click Anti-tampering to enter the Anti-tampering Configuration interface. Click Add Rule.



3. In the Add Anti-tampering Rule pop-up window, enter the rule name (such as homepage) and the complete URL path (such as http://www.qcloudwaf.com/index.html) of the rule (such as homepage), and click Add after entering to save the rule.



4. The rule will take effect. If the rules are updated, click Refresh Cache in the right operation column to update the cache content.


Web security(5)
Access control
CC protection(1)
Webpage anti-tampering(1)
Data leakage prevention
Add custom allow rule
Custom allow rules
Add rule
Batch disable
Batch enable
Each domain supports up to 80 rules
Select a filter
Rule ID
Rule name
Protected path
On/Off
Enable logs
Last modified
Creation Time
Operation
3200000007
homepage
/index.html
2025-09-26 04:33:30
2025-09-26 04:33:30
Refresh
Edit
Delete
Total items: 1
10 / page
1
/ 1 page

Information Leakage Prevention

Feature Introduction

The information leakage prevention feature supports replacing sensitive information returned on your webpage, such as phone numbers and ID numbers.

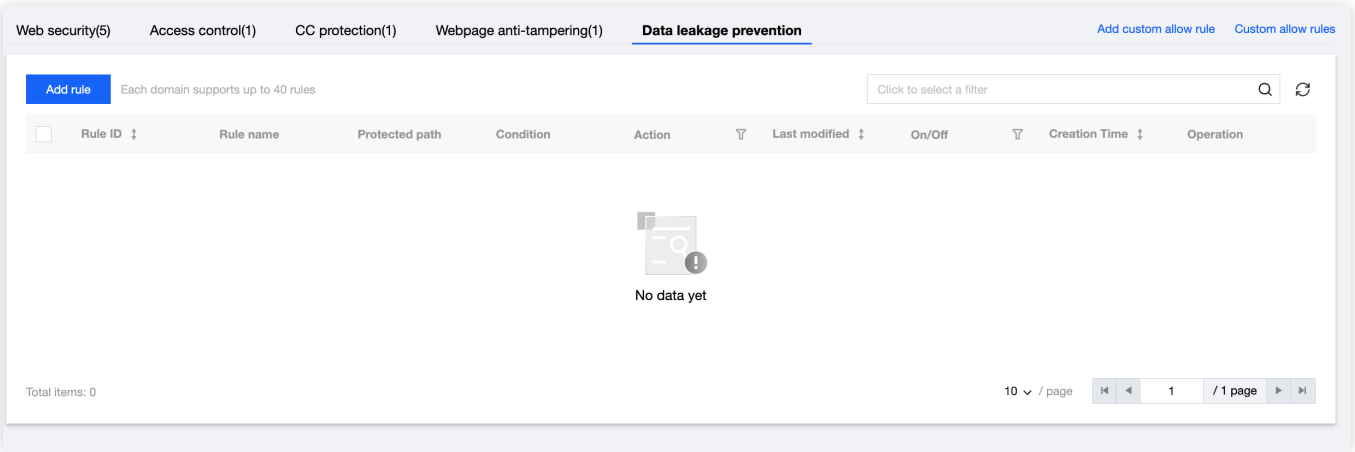
> Note:
>
> CLB WAF instances currently do not support this feature.

Prerequisites

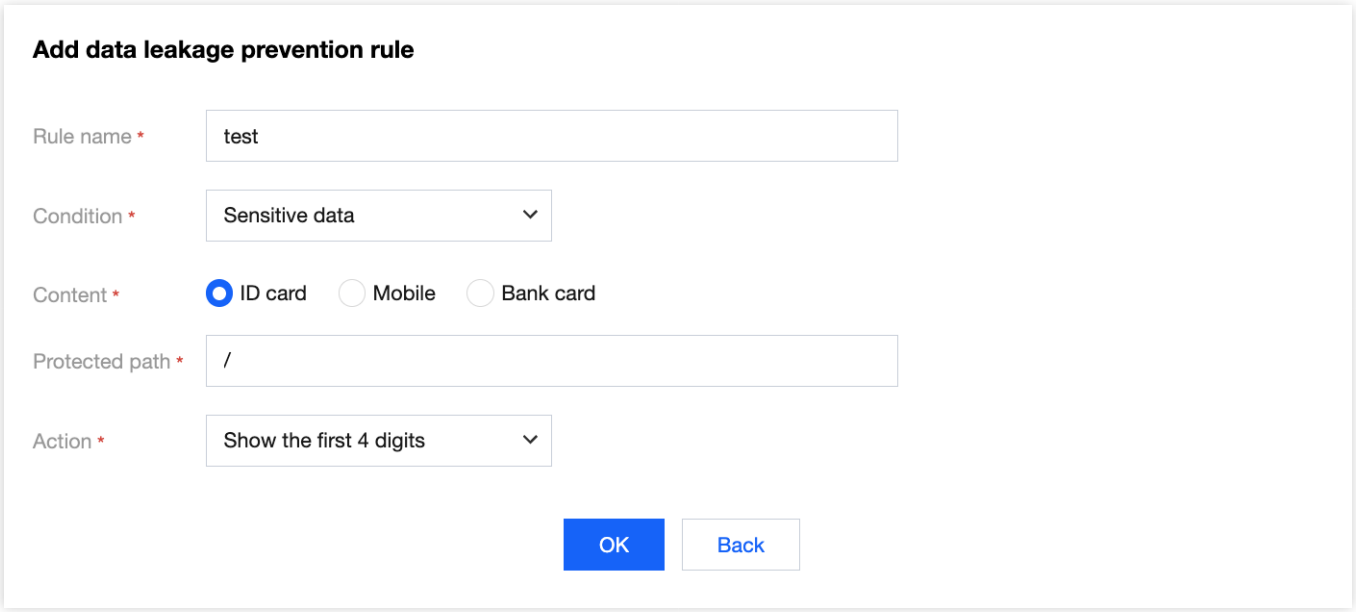
A cloud platform SaaS WAF instance has been created, and the domain name has been connected to the SaaS WAF instance.

Configuration Example

1. Log in to the WAF console. In the left sidebar, select WAF > Configuration Center > Basic Security. Select a protected domain name (such as www.qcloudwaf.com) and click to select Information Leakage Prevention to enter the configuration page. Select Information Leakage Prevention > Add Rule.

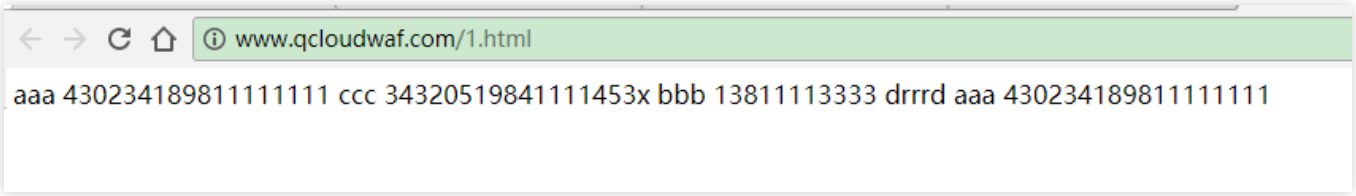


   On the Add Rule page, enter the rule name, select the matching condition (the matching field is Sensitive Information, the matching condition is Contain, and the matching content is ID Card or Mobile Number) and execution action (Replace or Observe), and click OK to save.



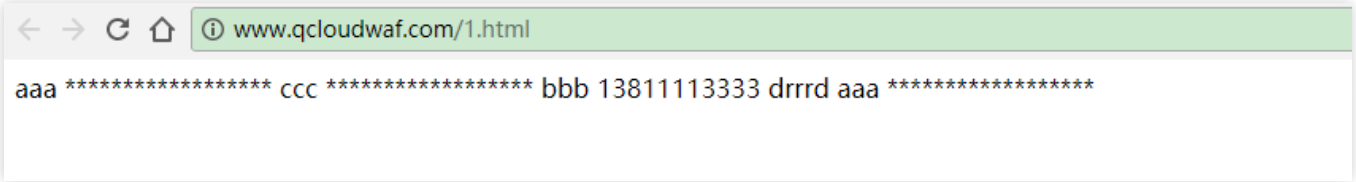
2. When the rule takes effect, it will protect the sensitive information returned from your webpage. The protection effect is as follows (the sensitive content is fictitious):

- Before the protection is enabled:



Before the protection is enabled

- After the protection is enabled:

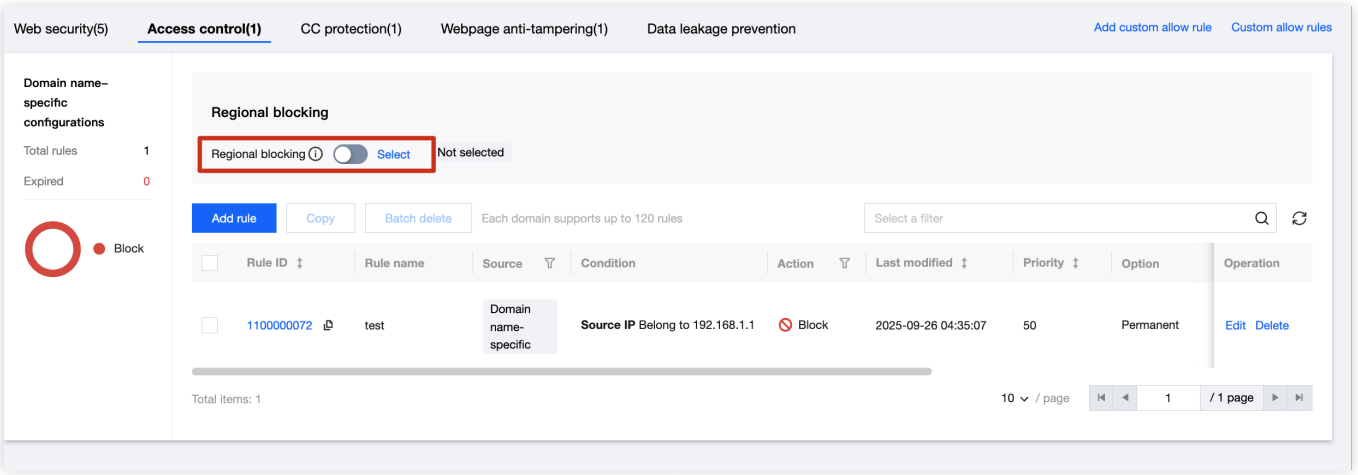


After the protection is enabled

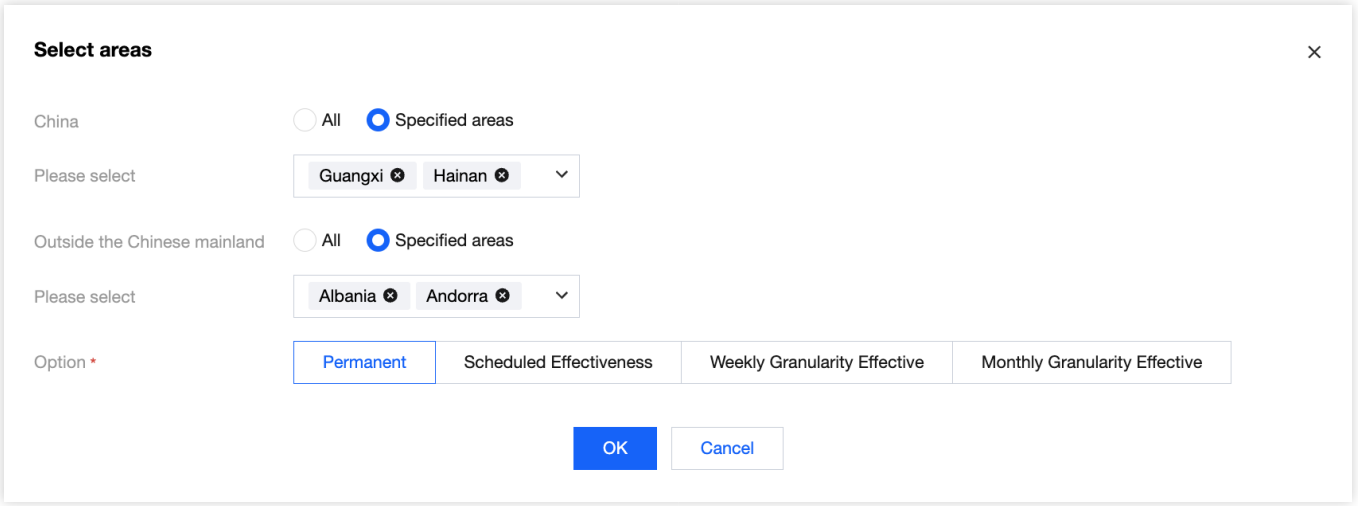
Regional Blocking

Configuration Instructions

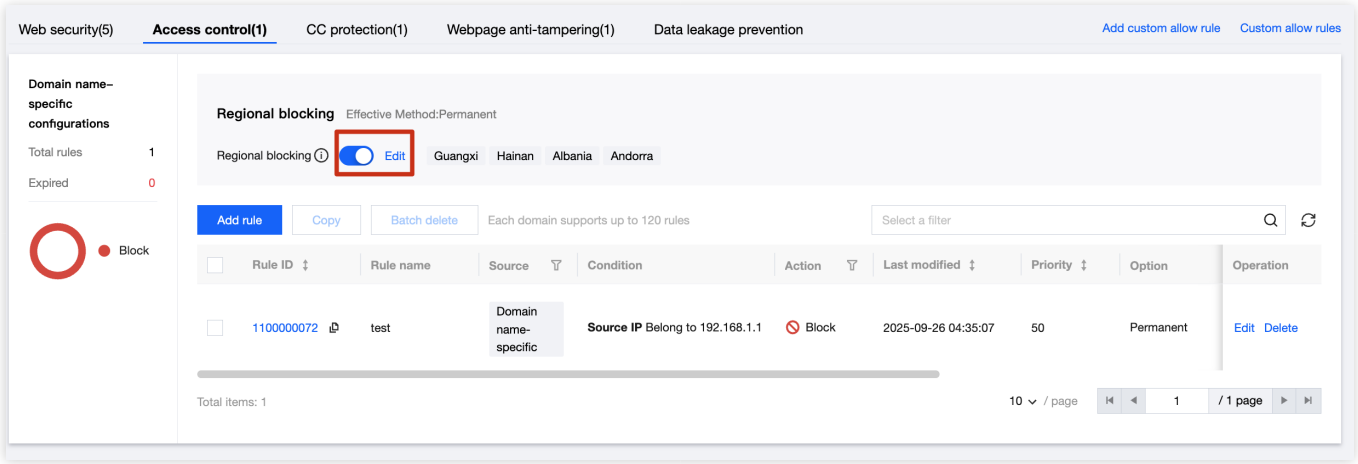
1. Log in to the WAF console. In the left sidebar, choose Web Application Firewall (WAF) > Configuration Center > Basic Security. Select a protected domain name (such as www.qcloudwaf.com) and click Access Control to enter the Configuration page and perform the regional blocking configuration.



2. On the Access Control Settings page, click Select to enter the regional blocking configuration page.



3. On the Blocked Region Settings page, check the Chinese mainland regions that need to be blocked. For regions outside the Chinese mainland, you can search or click the dropdown list to select. After selecting the regions, click OK.



4. After editing, enable the regional blocking status.
5. Access from the regions you have selected to block will be prevented from reaching your website. After all regions outside the Chinese mainland are listed as blocked regions, WAF will display an interception notification when a user accesses the protected website using an IP address outside the Chinese mainland.

Allowlist and Blocklist Management Feature Description

The blocklist/allowlist feature of the WAF refers to setting the blocklist/allowlist for source IP addresses transiting through WAF-protected domain names, as well as performing precise allowlist settings for multiple HTTP characteristics. The main features include: IP blocklist/allowlist settings, precise allowlist settings, and rule allowlist settings.

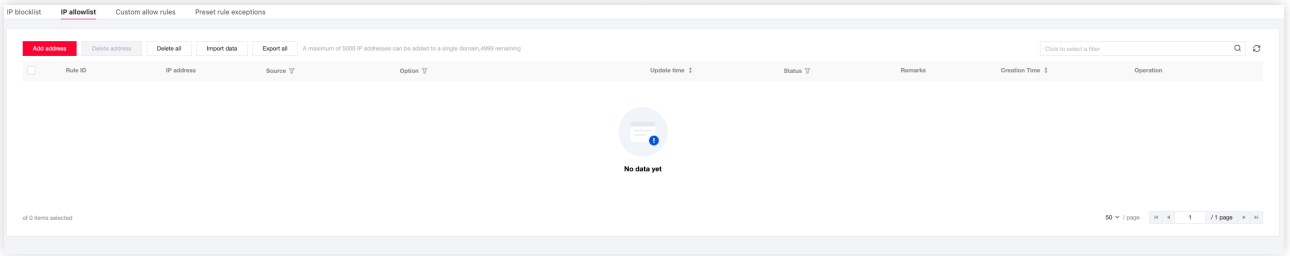
- IP blocklist/allowlist settings support setting domain-based or global IP blocklist/allowlist rules, and support IP range settings.
- Precise allowlist settings support combining multiple characteristics of HTTP messages such as the request path, GET parameters, POST parameters, Referer, and User-Agent, and adding the specific public network user access to the allowlist through characteristic matching.
- Rule allowlist settings support combining rule type, rule ID, and multiple characteristics of HTTP messages such as the request path, GET parameters, POST parameters, Referer, and User-Agent, and allow traffic according to the combination characteristics, rule ID, or rule type.
  Meanwhile, you can add domain-based or global blocklists/allowlists. The effectiveness priority description is as follows:
- The priority of the blocklist/allowlist is only lower than the precise allowlist policy of WAF and higher than other detection logics.
- Priority from high to low of the blocklist/allowlist: Global allowlist, domain name allowlist, rule allowlist, precise allowlist policy, domain name blocklist, and other protection modules.

IP Allowlist

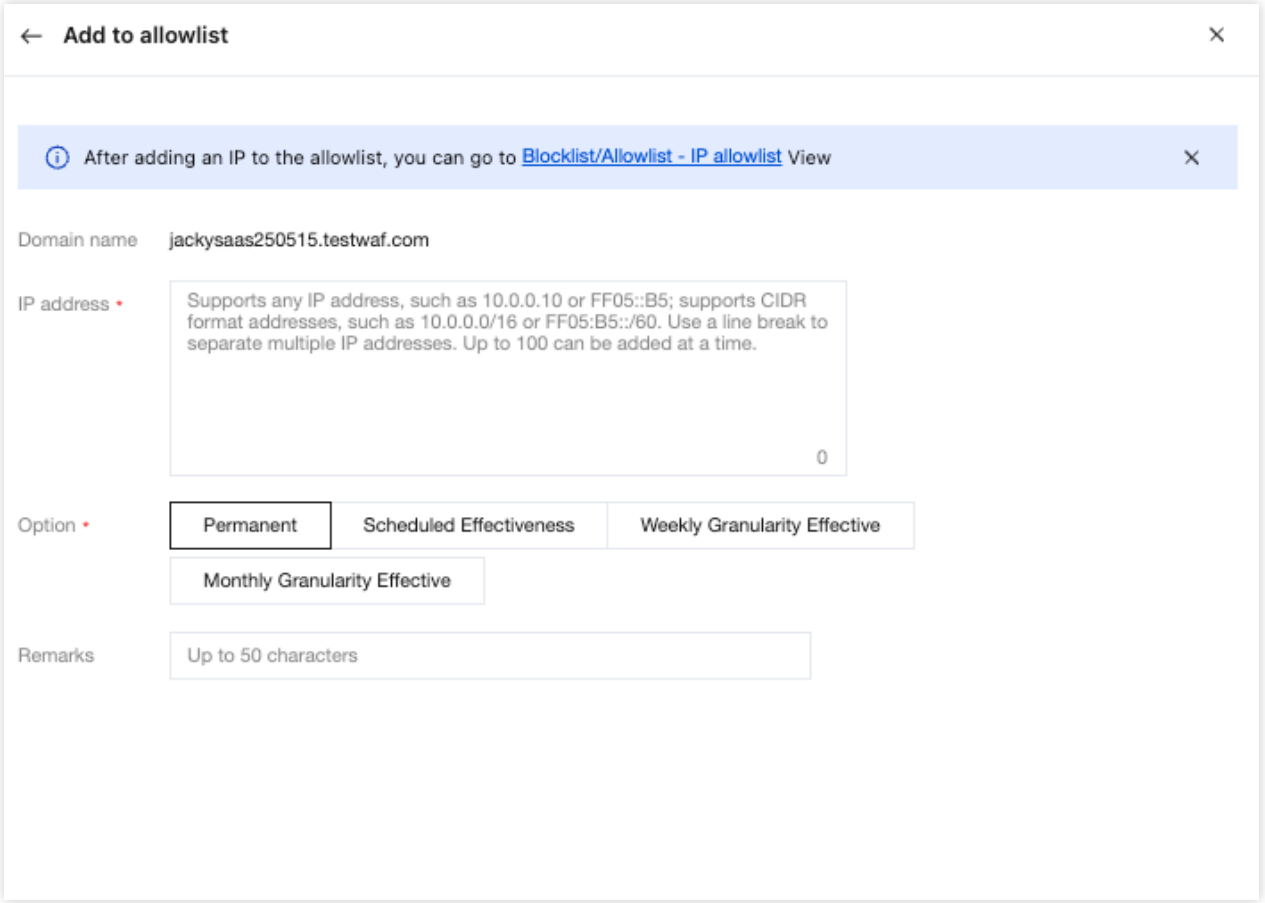
Adding an IP Address to the Allowlist

Manual Addition

1. Log in to the WAF console. In the left sidebar, click Configuration Center > Blocklist/Allowlist to enter the Blocklist/Allowlist page.
2. On the Blocklist/Allowlist page, select the domain name to be protected in the upper left corner and click IP Allowlist to enter the IP Allowlist page.



3. On the IP Allowlist page, click Add Address to enter the Add to Allowlist page.
4. On the Add to Allowlist page, configure related parameters and click OK.



Parameter description

- IP address: Support any IP address, such as 10.0.0.10 or FF05::B5; support CIDR format address, such as 10.0.0.0/16 or FF05:B5::/60. Use a line break to separate the addresses, and up to 20 addresses can be added at a time.

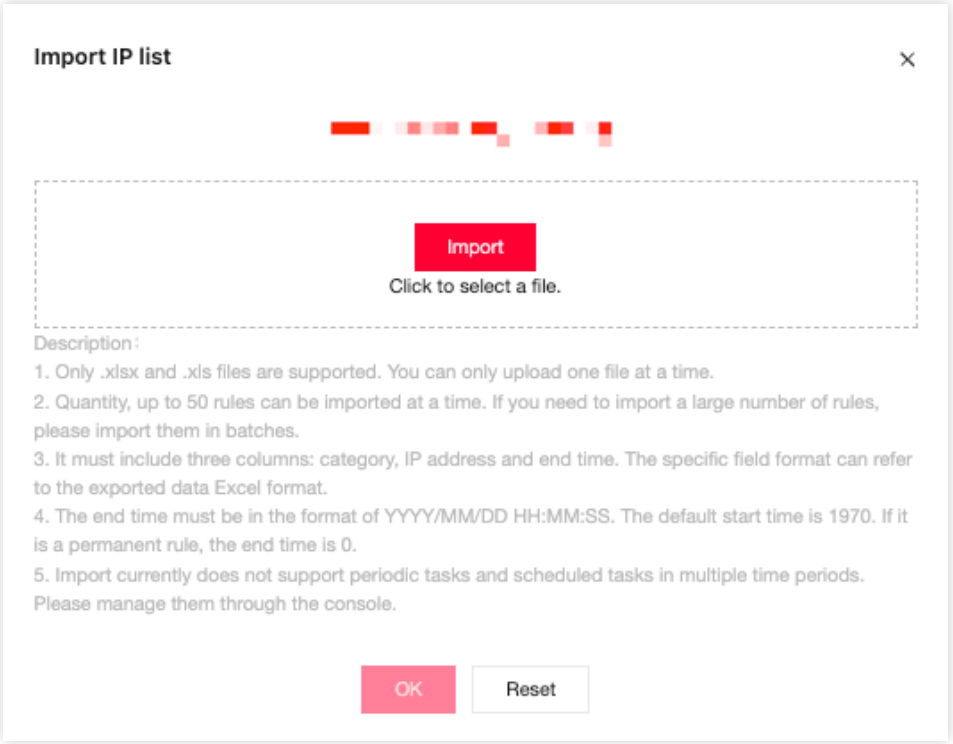
  > Description
  >
  > - When the selected domain name is Global, the IP address or IP range will be added to the global allowlist.

- Effective method: Permanently effective, regularly effective, effective on a monthly granularity period, and effective on a weekly granularity period.

- Remarks: Customized within 50 characters.

Importing Data

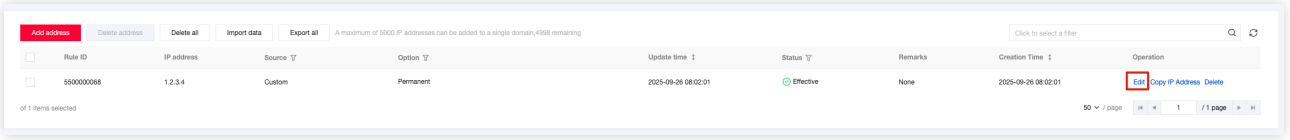
1. On the Blocklist/Allowlist page, select the domain name to be protected in the upper left corner and click IP Allowlist to enter the IP Allowlist page.
2. On the IP Allowlist page, click Import Data > Import. After the data is parsed successfully, click Confirm Import.



">

Editing the IP Allowlist

1. On the Blocklist/Allowlist page, select the domain name to be protected in the upper left corner and click IP Allowlist to enter the IP Allowlist page.
2. On the IP Allowlist page, select the required IP address, click Edit in the operation column, modify the expiration time and remarks, and click OK to save.



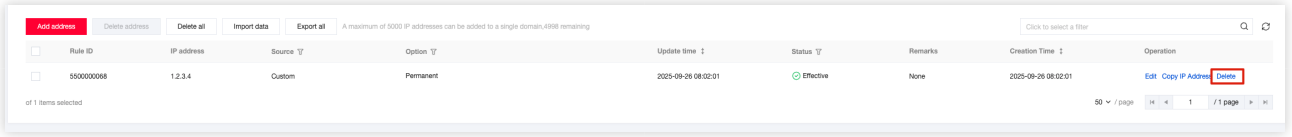
Deleting an IP Address from the Allowlist

1. On the Blocklist/Allowlist page, select the domain name to be protected in the upper left corner and click IP Allowlist to enter the IP Allowlist page.

2. On the IP Allowlist page, you can delete a single address, partial addresses, or all addresses. Specific operations are as follows:

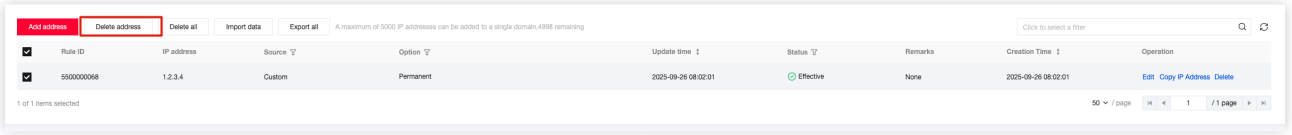
    - Single: Select a single IP address, click Delete address or Delete in the operation column, and a Confirm Deletion pop-up window will appear.

> Description
>
> The deleted IP address cannot be recovered. It should be re-added to take effect.



- Partial: Select multiple IP addresses, click Delete Address, and a Confirm Deletion pop-up window will appear.

> Description
>
> The deleted IP address cannot be recovered. It should be re-added to take effect.



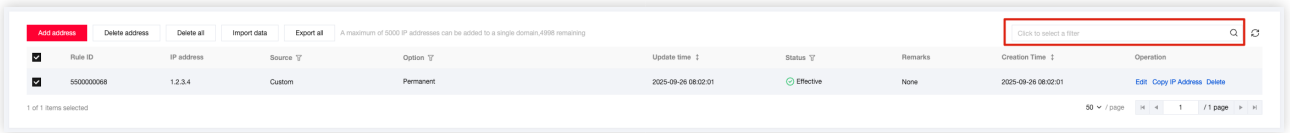
- All: Click Delete All, and a Confirm Deletion pop-up window will appear.

> Note
>
> This operation will clear all IP blocklist/allowlist information under the current domain name. Proceed with caution. The deleted IP address cannot be recovered. It should be re-added to take effect.

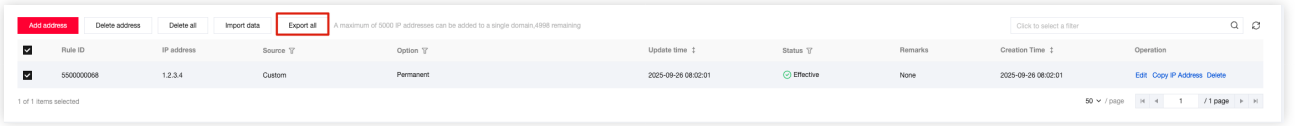
3. In the Confirm Deletion pop-up window, click OK to delete the address.

Exporting All Filtered Results

1. On the Blocklist/Allowlist page, select the domain name to be protected in the upper left corner and click IP Allowlist to enter the IP Allowlist page.
2. On the IP Allowlist page, click the search box to filter IP addresses by IP Address, or click Source to filter IP addresses by source type.



3. After the required IP addresses are filtered, click Export All Filtered Results to export the required IP filtering results.


Add address
Delete address
Delete all
Import data
Export all
A maximum of 5000 IP addresses can be added to a single domain,4998 remaining
Click to select a filter
Rule ID
IP address
Source
Option
Update time
Status
Remarks
Creation Time
Operation
5500000068
1.2.3.4
Custom
Permanent
2025-09-26 08:02:01
Effective
None
2025-09-26 08:02:01
Edit
Copy IP Address
Delete
1 of 1 items selected
50 / page
1
/ 1 page

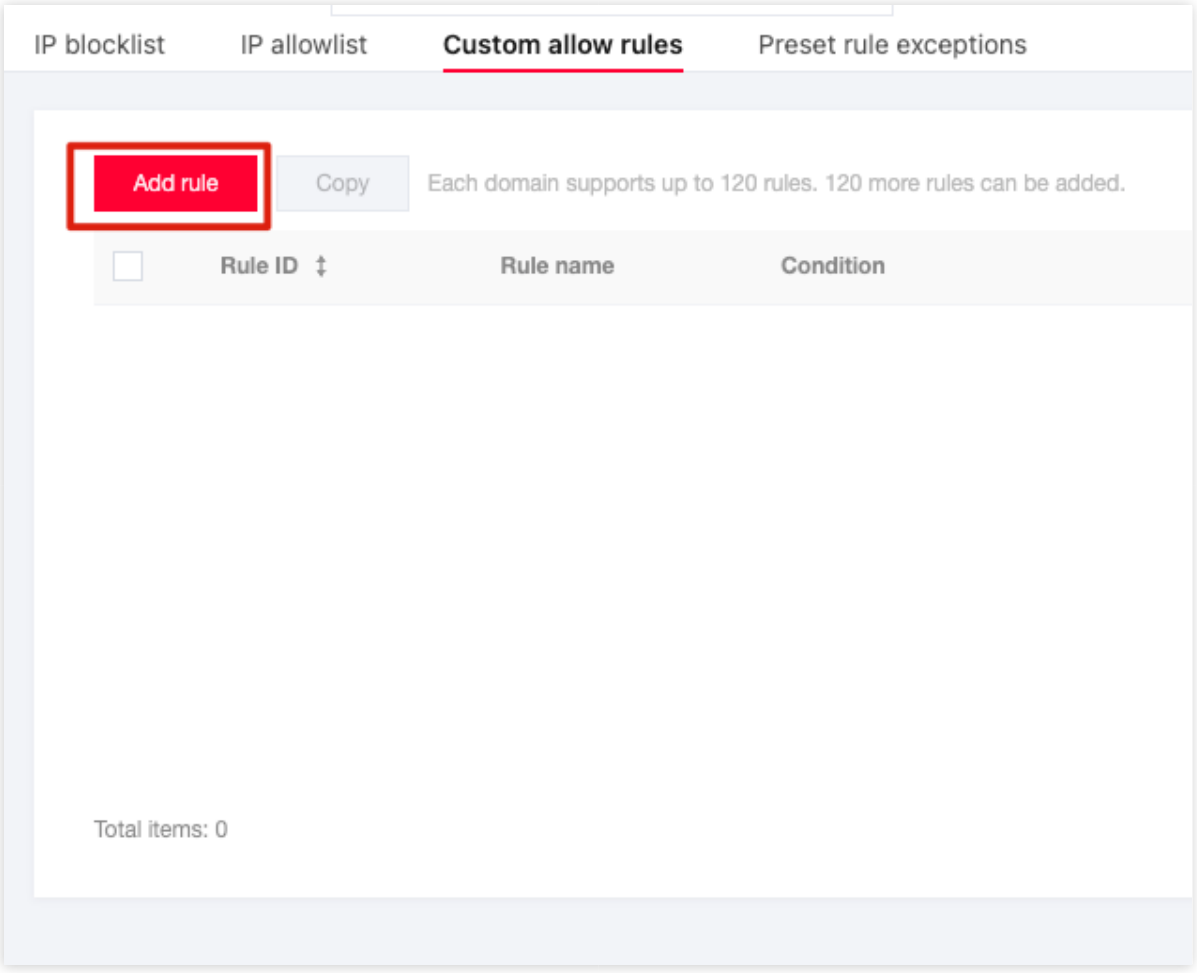
Precise Allowlist Management

When website administrators need to allow public network users to access a specific site based on users' access request characteristics, they can configure it by adding rules to the precise allowlist.

Adding a Rule to the Precise Allowlist

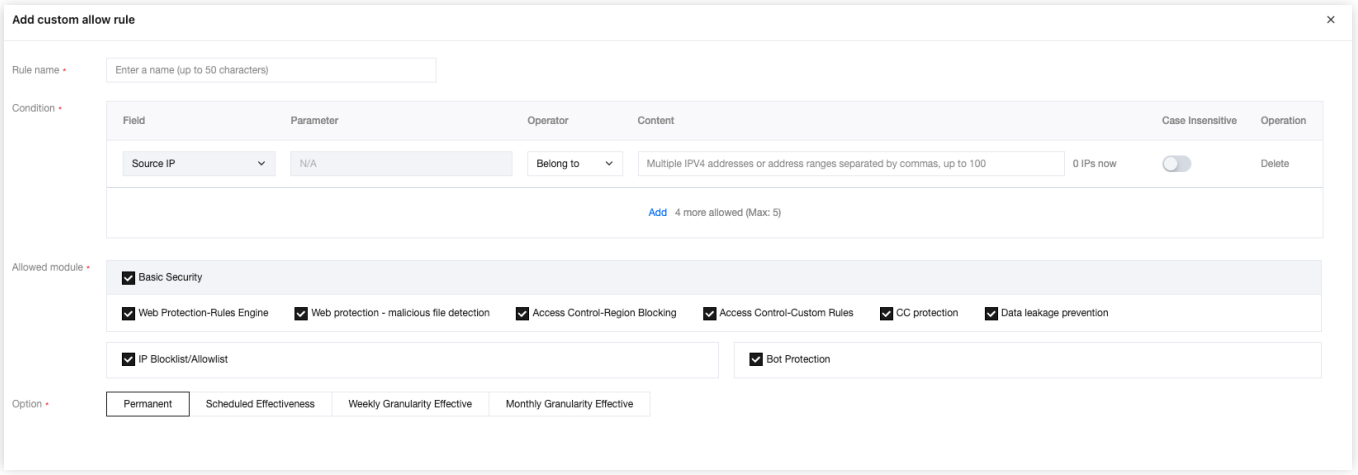
1. Log in to the WAF console. In the left sidebar, click Configuration Center > Blocklist/Allowlist to enter the Blocklist/Allowlist page.

2. On the Blocklist/Allowlist page, select the domain name to be protected in the upper left corner and click Precise Allowlist to enter the Precise Allowlist page.



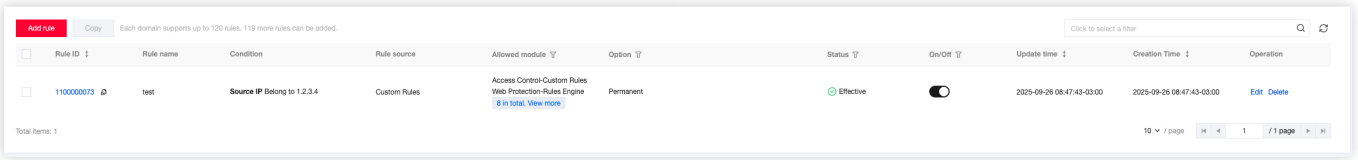
3. On the Precise Allowlist page, click Add Rule, and an Add to Precise Allowlist pop-up window will appear.

4. In the Add to Precise Allowlist pop-up window, configure related parameters and click OK.



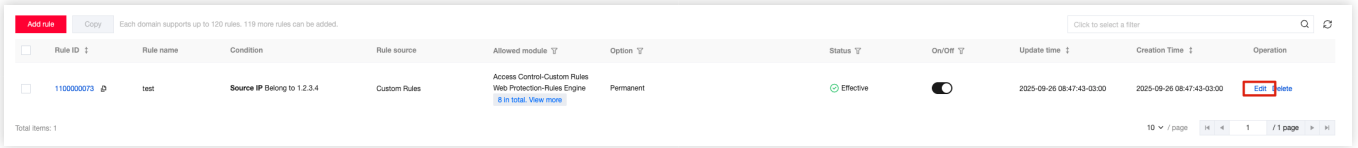
> Note:
>
> The precise allowlist of WAF supports using masks to allow access requests from source IP addresses in a specific IP range. We can enter a specific IP range in the matching content (such as 10.10.10.0/24).

5. The rule will take effect. HTTP access requests from the specific source IP will be allowed.



Editing the Precise Allowlist

1. On the Blocklist/Allowlist page, select the domain name to be protected in the upper left corner and click Precise Allowlist to enter the Precise Allowlist page.
2. On the Precise Allowlist page, select the required rule and click Edit, and an Edit Precise Allowlist pop-up window will appear.



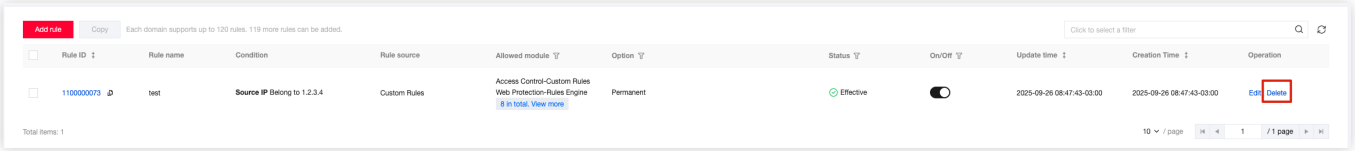
3. In the Edit Precise Allowlist pop-up window, modify the relevant parameters and click OK to save.

Deleting a Rule from the Precise Allowlist

1. On the Blocklist/Allowlist page, select the domain name to be protected in the upper left corner and click

Precise Allowlist to enter the Precise Allowlist page.

2. On the Precise Allowlist page, select the required rule and click Delete, and a Confirm Deletion pop-up window will appear.



3. In the Confirm Deletion pop-up window, click OK to delete the rule.

> Note:
>
> The deleted IP address cannot be recovered. It should be re-added to take effect.

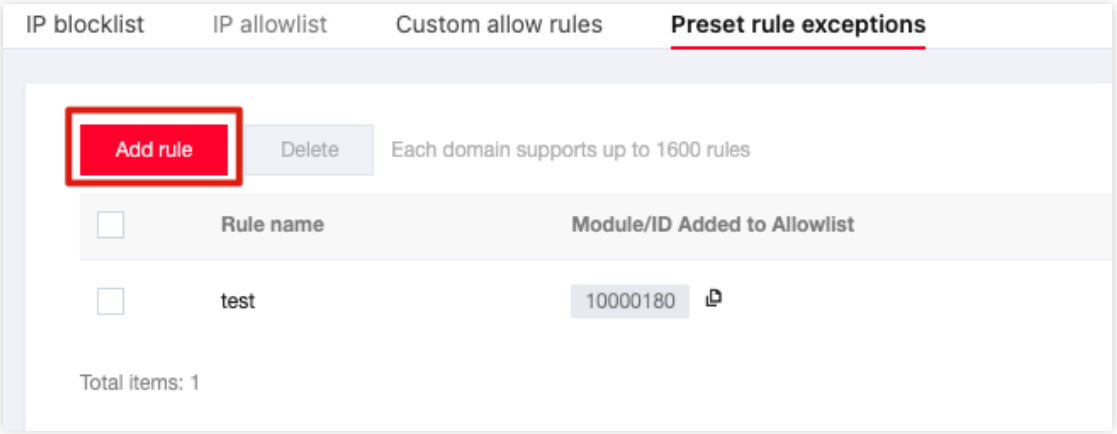
Rule Allowlist

Scenarios

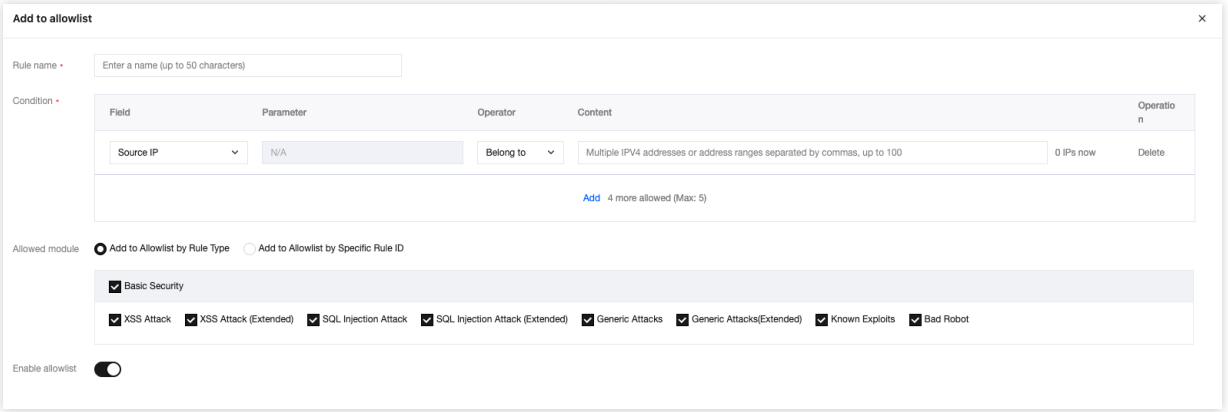
If normal access traffic is intercepted by the WAF rule engine in a production environment, you can add the corresponding rule to the allowlist through the Rule Allowlist in the blocklist/allowlist. After the rule is added to the allowlist, it will not be intercepted.

Operation Steps

1. Log in to the WAF console. In the left sidebar, click Configuration Center > Blocklist/Allowlist.
2. On the Blocklist/Allowlist page, select the domain name to be protected in the upper left corner and click Rule Allowlist.
3. On the Rule Allowlist page, click Add Rule, and an Add to Allowlist pop-up window will appear.



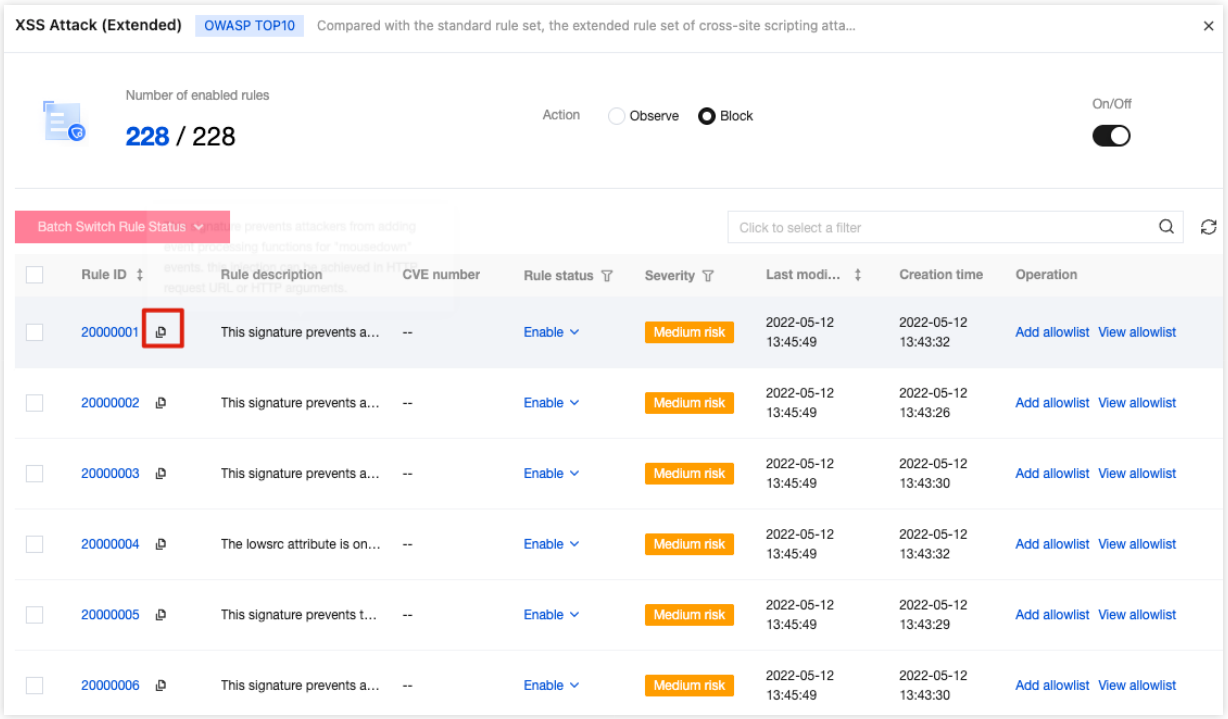
4. In the Add Rule pop-up window, configure related parameters and click OK.



Field description:

- Rule ID to be allowlisted: Fill in the rule ID that needs to be allowlisted. A policy can add up to 10 rule IDs. The obtaining method is as follows:

- On the Basic Security page, select the required rule ID and click to copy.



- On the Log Service page, select the required data and copy the rule_id of the data.

- Matching method: The matching method for the allowlisted URL path, supporting exact matching (default), prefix matching, and suffix matching.

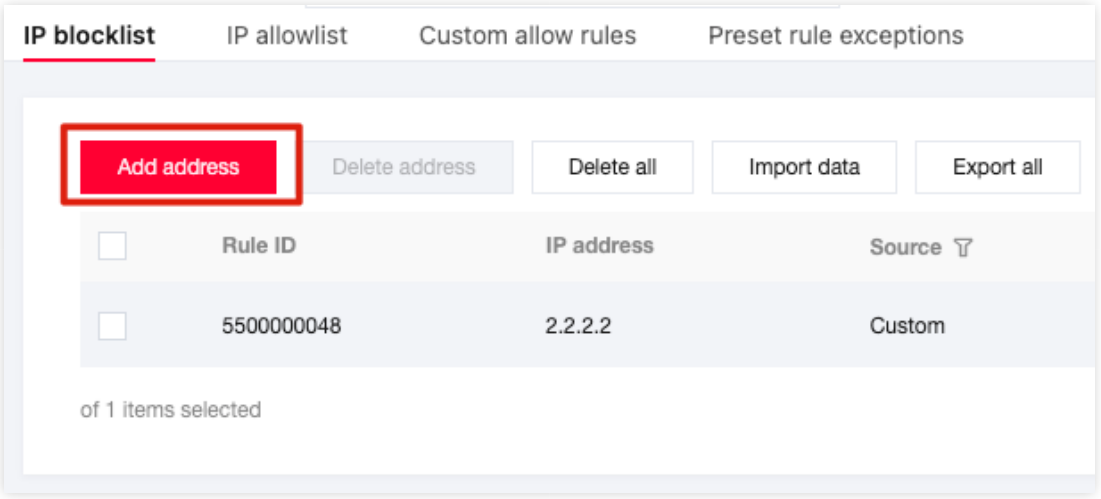
- URL path: The URL path that needs to be allowlisted. URLs under the same domain name cannot be added repeatedly.

IP Blocklist

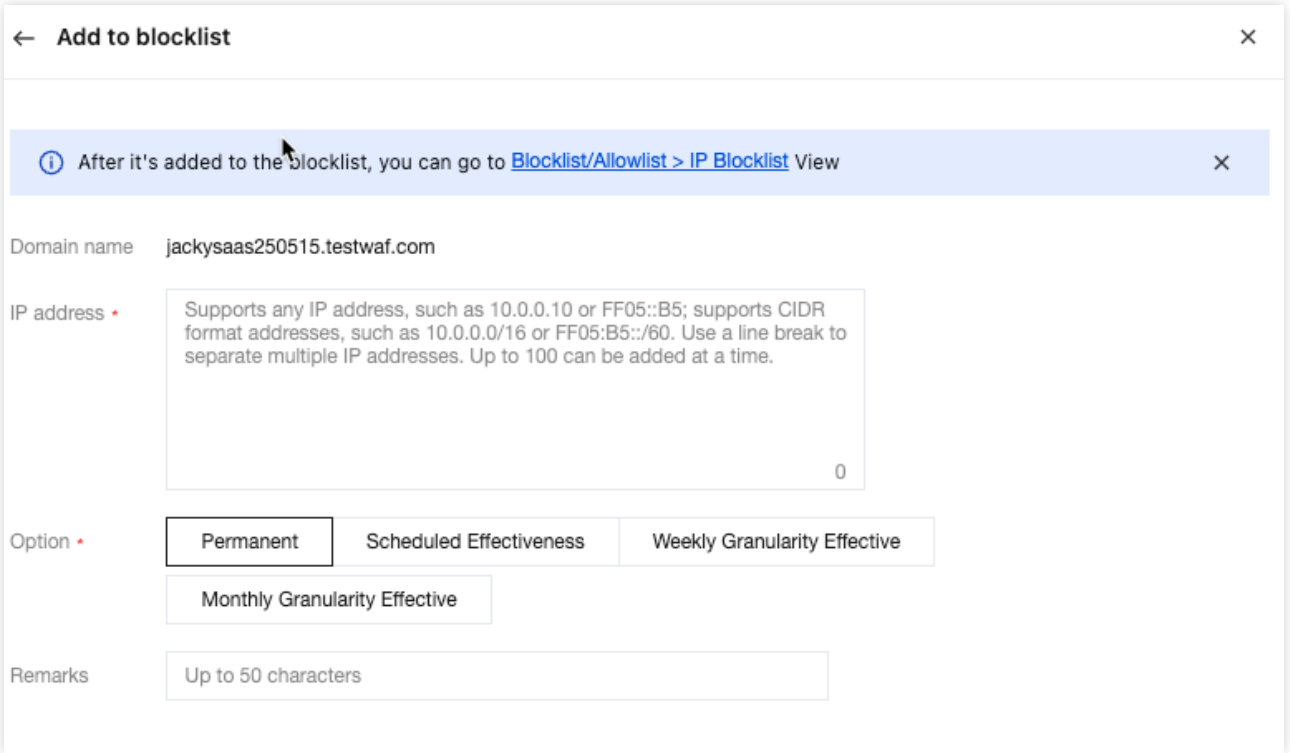
Adding an IP Address to the Blocklist

Manual Addition

1. Log in to the WAF console. In the left sidebar, select Configuration Center > Blocklist/Allowlist.
2. On the Blocklist/Allowlist page, select the domain name to be protected in the upper left corner and click IP Blocklist.



3. On the IP Blocklist page, click Add Address to enter the Add to Blocklist page.
4. On the Add to Blocklist page, configure related parameters and click OK.



Field description:

- IP address: Support any IP address or IP address range, such as 10.0.0.10 or FF05::B5; support CIDR format address, such as 10.0.0.0/16 or FF05:B5::/60. Use a line break to separate the addresses, and up to 20 addresses can be added at a time.

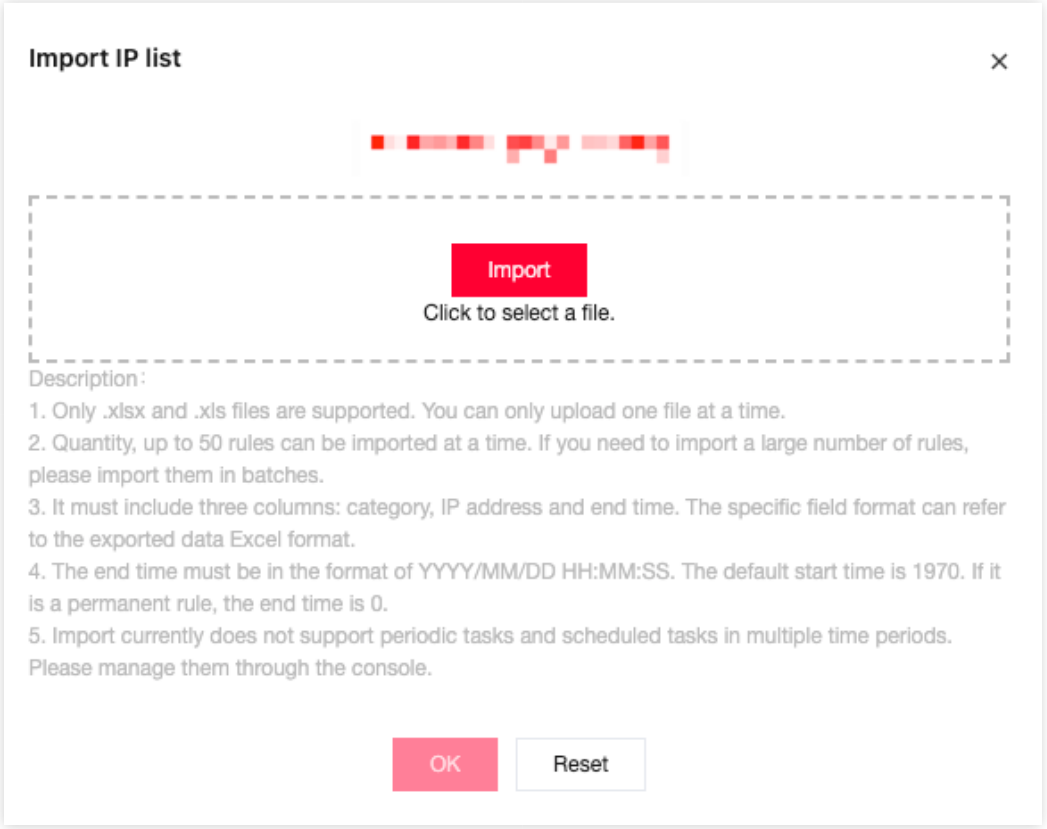
  > Note:
  >
  > - When the selected domain name is Global, the IP address or IP range will be added to the global blocklist/allowlist.

- Effective method: Permanently effective, regularly effective, effective on a monthly granularity period, and effective on a weekly granularity period.

- Remarks: Customized within 50 characters.

Importing Data

1. On the Blocklist/Allowlist page, select the domain name to be protected in the upper left corner and click IP Blocklist.
2. On the IP Blocklist page, click Import Data > Import. After the data is parsed successfully, click Confirm Import.

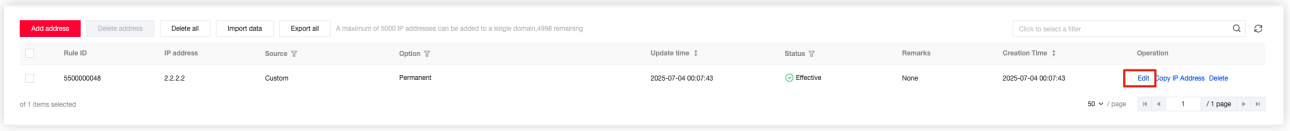


Editing the IP Blocklist

1. On the Blocklist/Allowlist page, select the domain name to be protected in the upper left corner and click IP

Blocklist.

2. On the IP Blocklist page, select the required IP address, click Edit in the operation column, modify the expiration time and remarks, and click OK to save.



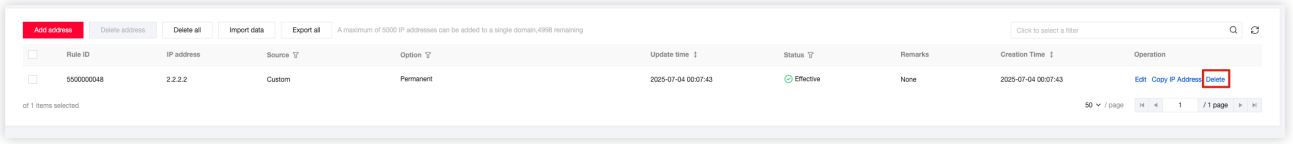
Deleting an IP Address from the Blocklist

1. On the Blocklist/Allowlist page, select the domain name to be protected in the upper left corner and click IP Blocklist.

2. On the IP Blocklist page, you can delete a single address, partial addresses, or all addresses. Specific operations are as follows:

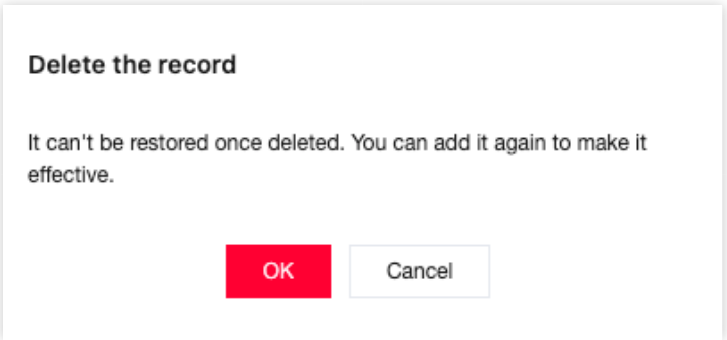
   - Single: Select a single IP address, click Delete address or Delete in the operation column, and a Confirm Deletion pop-up window will appear.

     > Description
     >
     > The deleted IP address cannot be recovered. It should be re-added to take effect.



   - Partial: Select multiple IP addresses, click <1>Delete Address

     > Description
     >
     > The deleted IP address cannot be recovered. It should be re-added to take effect.



- All: Click Delete All, and a Confirm Deletion pop-up window will appear.

  > Note
  >
  > This operation will clear all IP blocklist/allowlist information under the current domain name. Proceed with caution. The deleted IP address cannot be recovered. It should be re-added to take effect.

3. In the Confirm Deletion pop-up window, click OK to delete the address.

Exporting All Filtered Results

1. On the Blocklist/Allowlist page, select the domain name to be protected in the upper left corner and click IP Blocklist.
2. On the IP Blocklist page, click the search box to filter IP addresses by IP Address, or click Source to filter IP addresses by source type.
3. After the required IP addresses are filtered, click Export All Filtered Results to export the required IP filtering results.

Attack Log

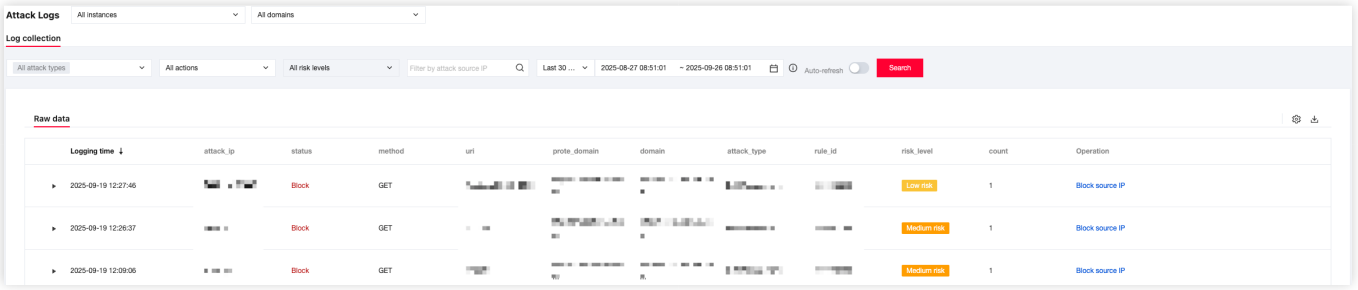
Feature Introduction

By default, WAF records web attack log information, including the attack occurrence time, attack source IP address, attack type, and attack details. You can query logs according to the filter conditions and download the query results as needed.

Usage Instructions

Querying Attack Logs

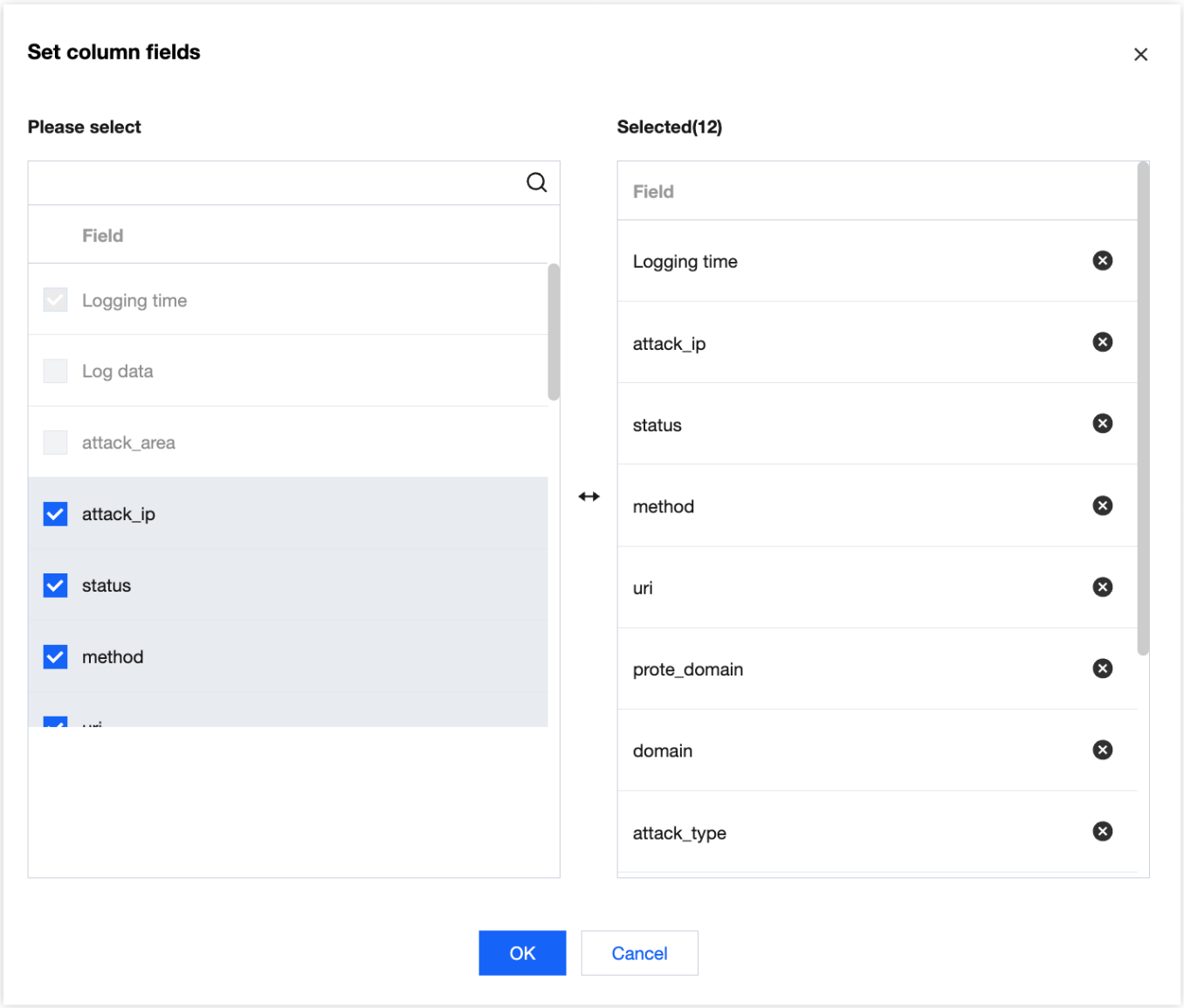
1. Log in to the WAF console. In the left sidebar, choose Log Service > Attack Logs to enter the Attack Log Query page. Click Log Query, select a domain name from the dropdown search list above, set query conditions as needed, and click Query to view the corresponding attack log information.



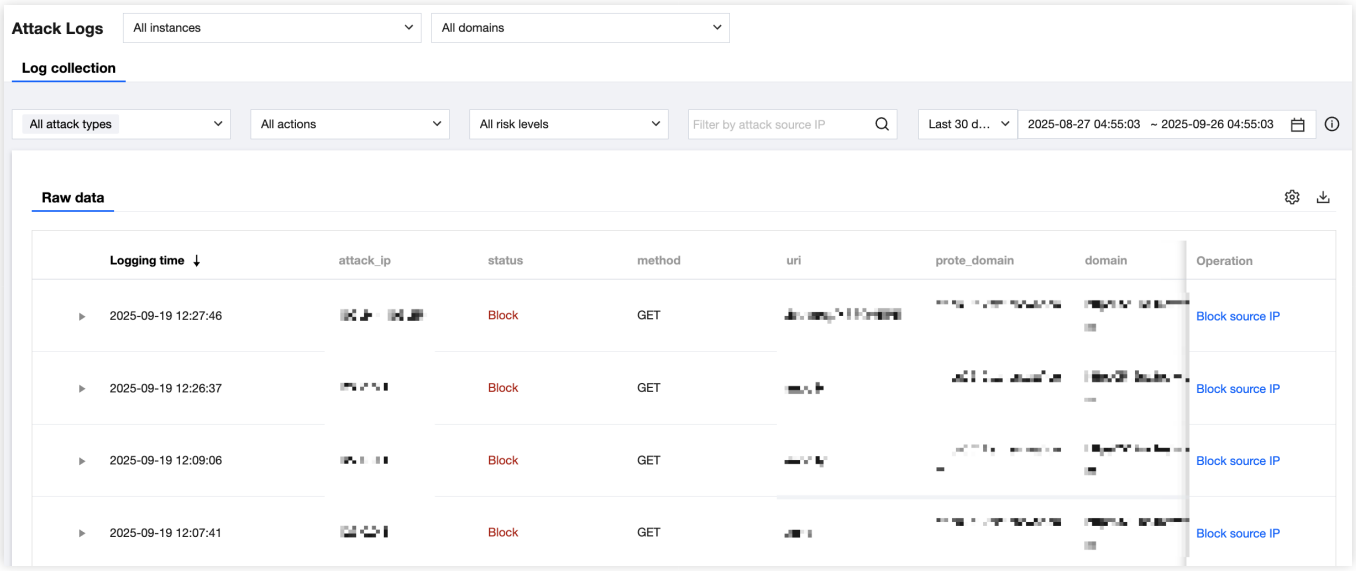
Query condition description:

- Domain name: Select the domain name to be queried in the domain name dropdown search list.
- Time condition: 1 hour, by default. You can query the attack log information from the last 30 days at most.
- Risk level: All, by default. You can select high risk, medium risk, or low risk.
- Execution action: All, by default. You can select observing or intercepting.
- Policy ID: Enter the policy ID you need to query. (The policy ID can be viewed in the log entry.)
- Attack source IP: Enter the attack source IP to conduct a query.

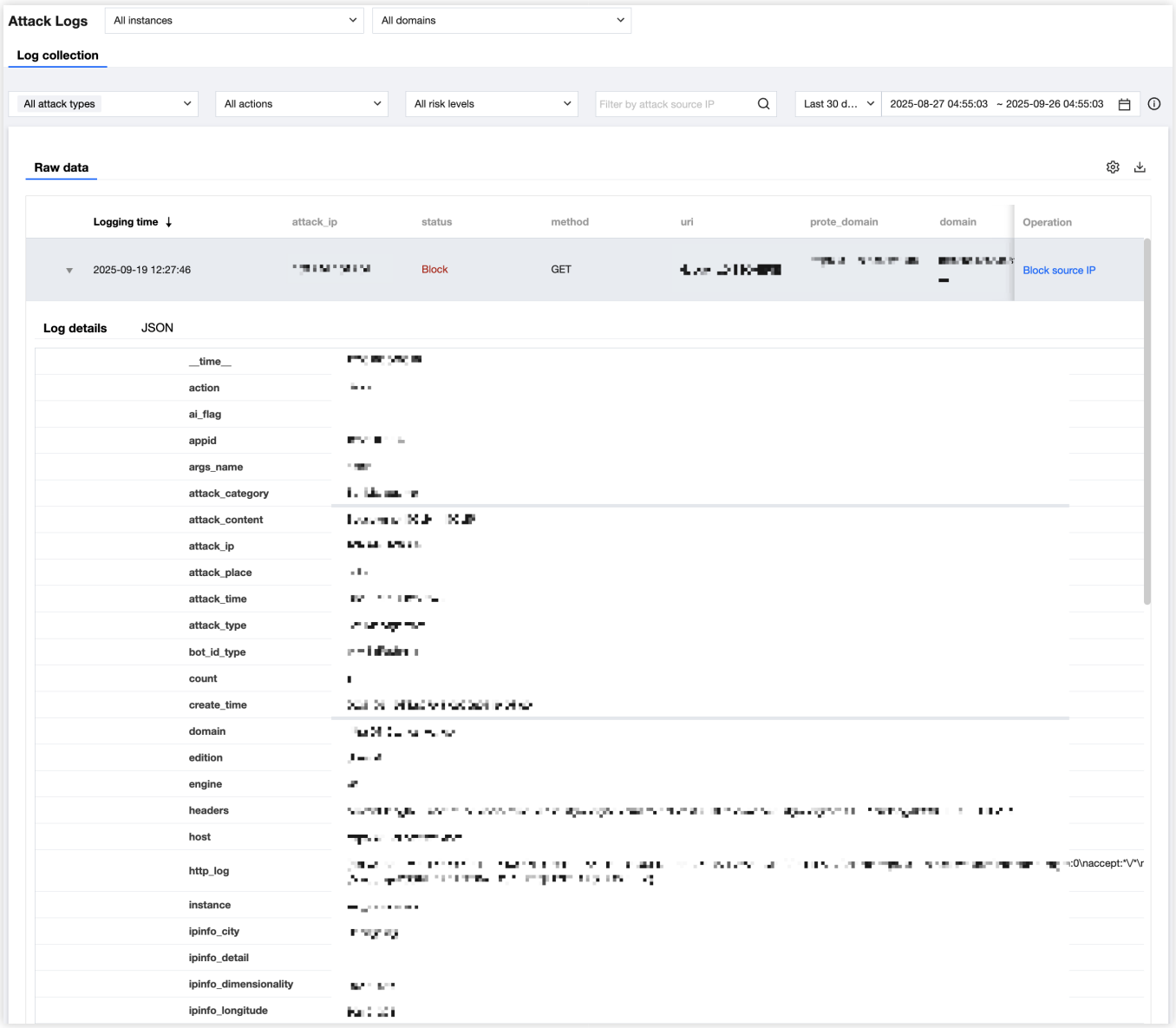
2. Click the Set button in the upper right corner of the attack log. In the Custom List Fields pop-up window, select the list details to display, as shown in the figure below:



3. View attack details. Select the log entry you need to view and click Details in the right operation column to view attack details.

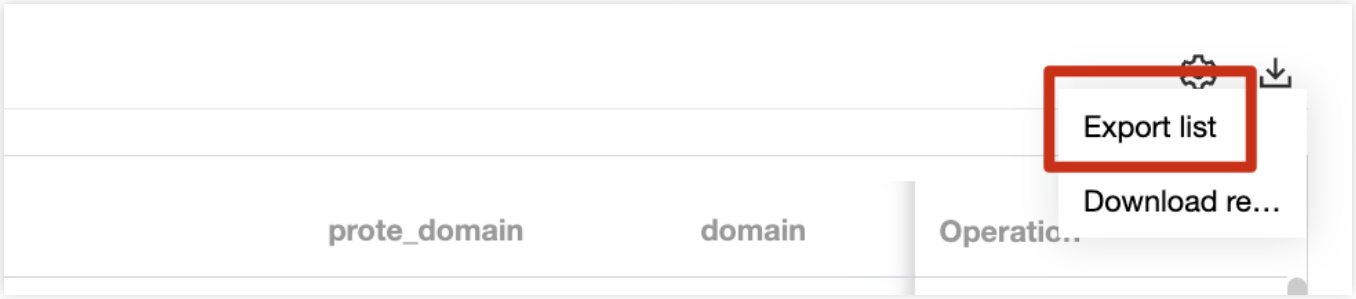


4. Enter the Log Details page and view corresponding fields.



Exporting Attack Logs

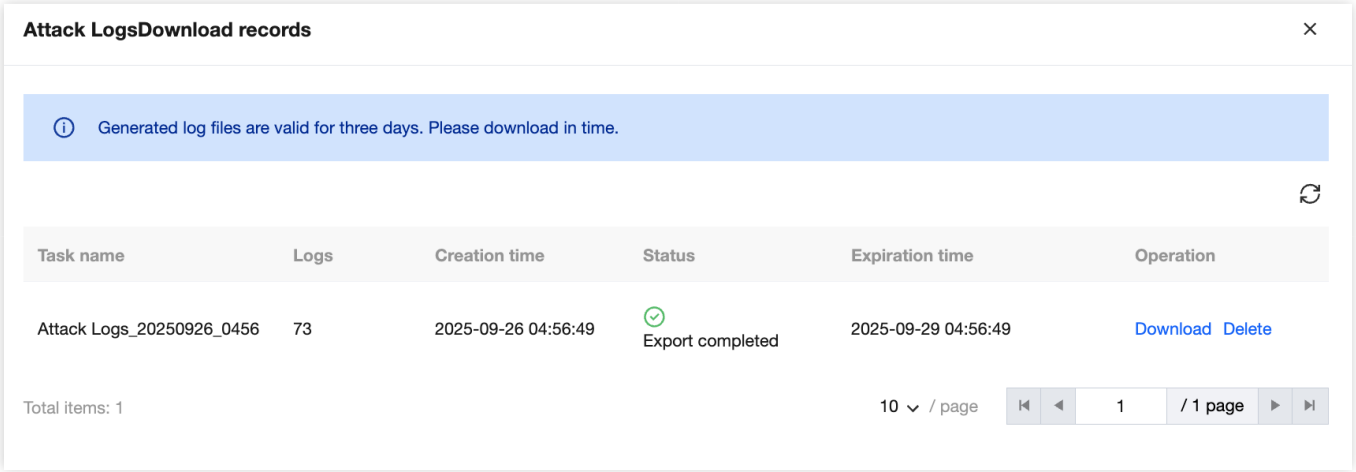
1. Log in to the WAF console. In the left sidebar, select Log Service > Attack Logs to enter the Attack Log Query page. Click Log Query, select a domain name from the dropdown search list above, set query conditions as needed, and click Query to view the corresponding attack log information. Click Export Logs to export the corresponding attack log information.



Export condition description:

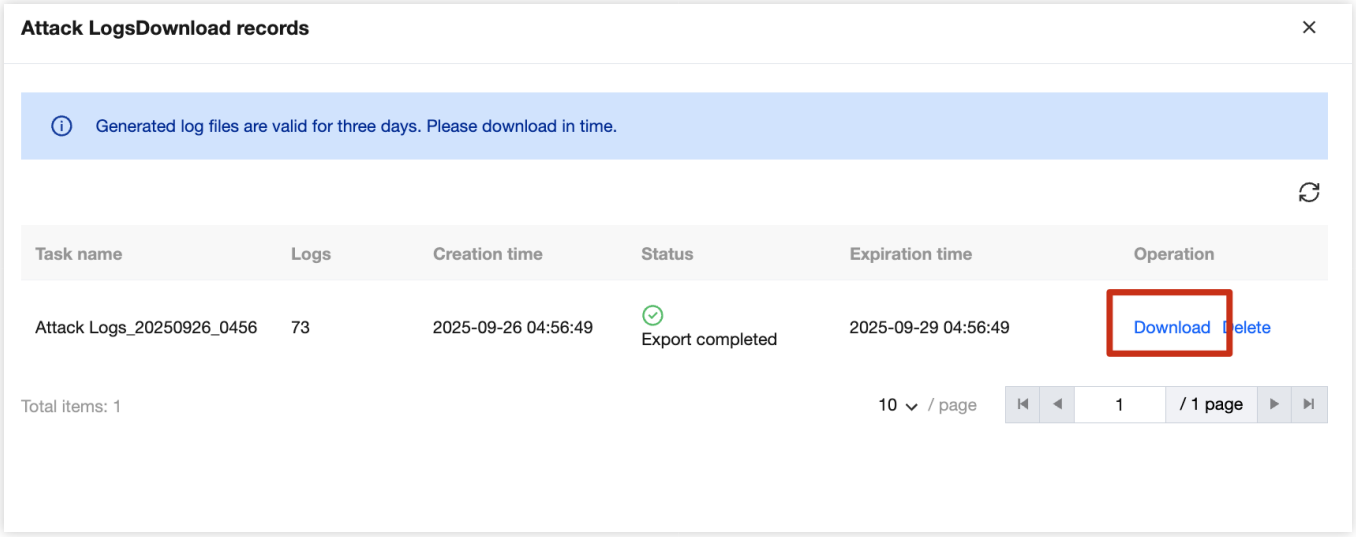
- Domain name: Select the domain name to be queried in the domain name dropdown search list.
- Time condition: 1 hour, by default. You can query the attack log information from the last 30 days at most.
- Risk level: All, by default. You can select high risk, medium risk, or low risk.
- Execution action: All, by default. You can select observing or intercepting.
- Policy ID: Enter the policy ID you need to query. (The policy ID can be viewed in the log entry.)
- Attack source IP: Enter the attack source IP to conduct a query.
- Log table content cannot be empty.

2. Choose Log Service > Attack Logs > Download Task to enter the download task query page, as shown in the figure below:



3. Click Download, and a prompt "The address of the log file has been successfully copied. Open it in a new browser window" will appear. Copy the link to the browser and open it to successfully download the

compressed log file.



Log details field description:

- Basic information

Field Name	Field Description
Domain Name	Client access domain name.
Attack Type	Information on the attack types currently supported by WAF. The default value is All.
Number of Aggregate Attacks	Total number of attacks generated every 10 seconds with the same attack source IP address and attack type.
Attack Source IP Address	Source IP address of the client attack.
Hit Rule ID	The rule ID that triggers the protection policy. For attacks detected by the AI engine, the rule ID is 0.
Hit Rule Name	The policy name that triggers the protection policy. The policy name of the rule engine and AI engine is empty.
Request Method	Client attack request method.
Risk Level	The risk level triggered by the client attack.
Attack Time	The time when the client attack is triggered.
Matching Source	Client attack matching source information, such as the source IP address.
Execution Action	Actions triggered by the client attack.
Request URI	Request URI content.

Field Name	Field Description
Attack Content	The content of the triggered client attack.

- Attack IP details

Field Name	Field Description
Region	English abbreviation of the country where the source IP address is used
IP Owner	Owner information of the used source IP address
Country	Country name of the attack source IP address
Province	Province information of the attack source IP address
City	City information of the attack source IP address
ISP	ISP information of the attack source IP address
Longitude	Longitude information of the attack source IP address
Latitude	Latitude information of the attack source IP address

- Detailed information

Field Name	Field Description
Protocol Version	HTTP protocol version information of the attack source IP address
User-Agent	Browser type and operating system identifier provided by the attack source IP address to the server

IP Address Management

Feature Introduction

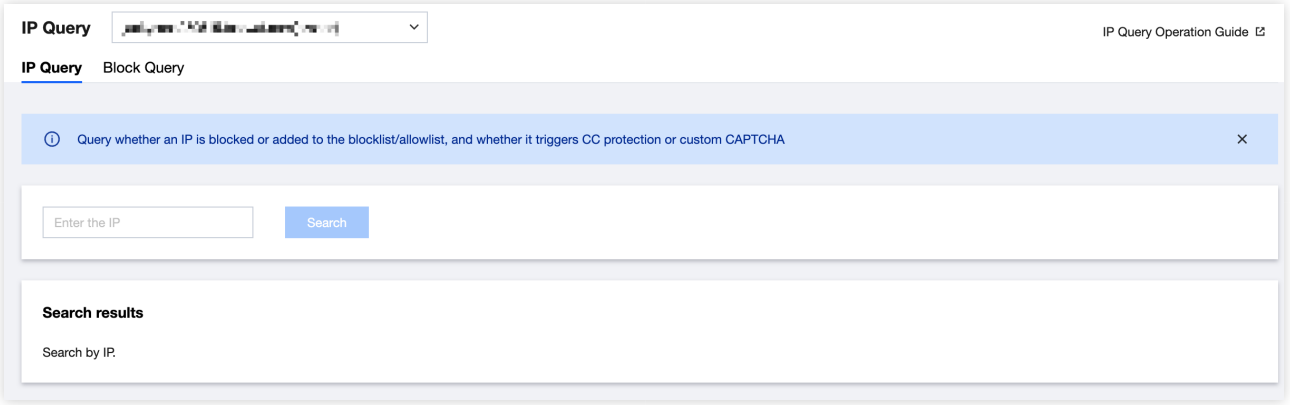
The IP management feature of WAF performs status queries and blocklist/allowlist settings on the source IP addresses transiting through WAF-protected domain names. The main features include: IP query, IP blocklist/allowlist settings, and IP blocking status query.

- IP query supports querying the protected domain name status information of the input IP, including whether in the blocklist/allowlist, and whether in the blocked status.
- IP blocklist/allowlist settings support setting domain-based or global IP blocklist/allowlist rules.
- IP blocking status supports real-time viewing of source IP blocking status information, such as CC attacks and human-machine recognition of custom policies.

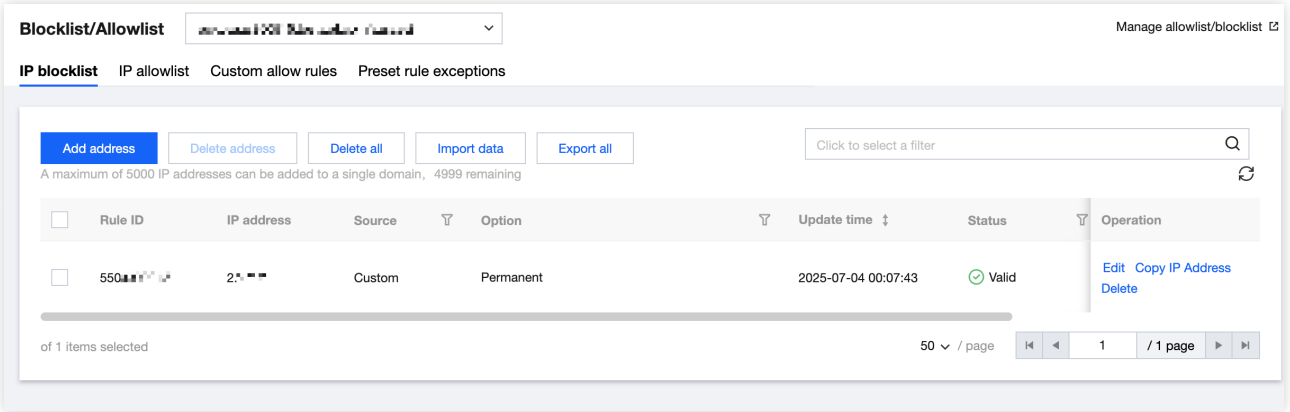
Configuration Steps

Example 1: Querying IP Addresses

1. Enter the WAF console, select IP Management > IP Query, enter the IP address to be queried, and view IP status.

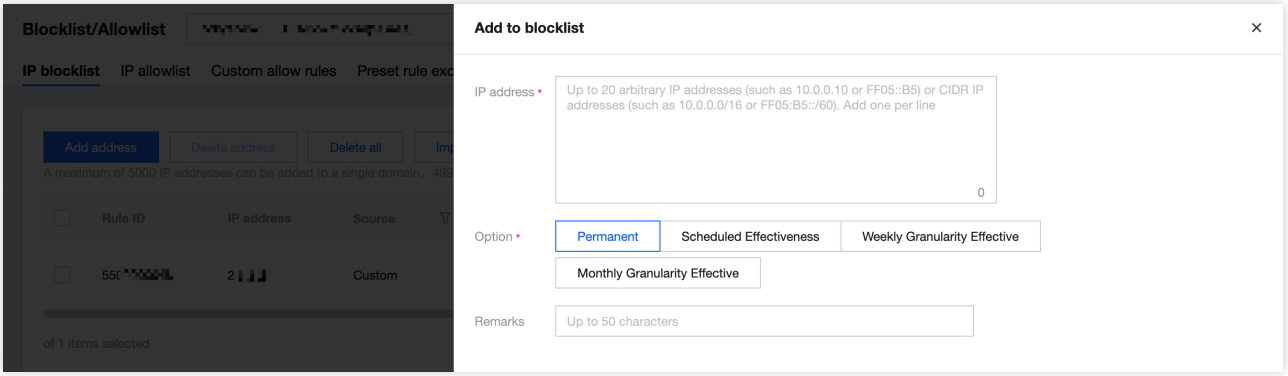


2. The queried IP address can be manually added to the blocklist/allowlist.



Example 2: Adding an IP Address to the Blocklist

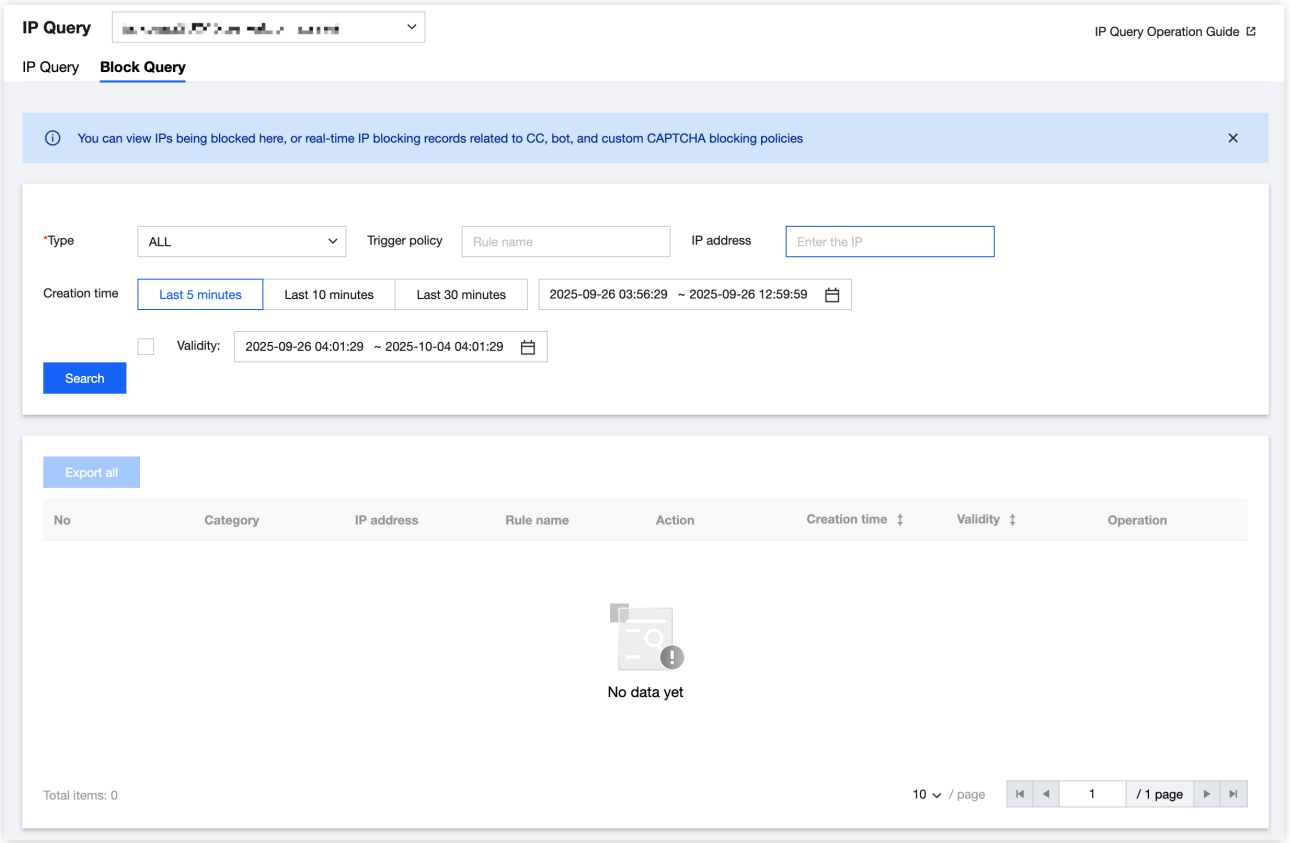
1. Enter the WAF console, select IP Management > IP Blocklist/Allowlist to enter the configuration page.
   The IP address blocklist/allowlist module can add domain-based blocklists/allowlists or global blocklists/allowlists. The effective priority is as follows:
   - The priority of the blocklist/allowlist is only lower than the custom allowing policy of WAF and higher than other detection logics.
   - Priority from high to low of the IP blocklist/allowlist: Global allowlist, domain name allowlist, domain name blocklist, and global blocklist.



   Configuration item description:
   - Category: Blocklist and allowlist.
   - Source: CC protection and custom rule.
   - Advanced filtering: Filter IP information by creation time and expiration time.
2. Add to the blocklist/allowlist. Select the domain name to be protected in the upper left corner, click Add to Blocklist/Allowlist, select Blocklist, and add the IP address to be blocked.



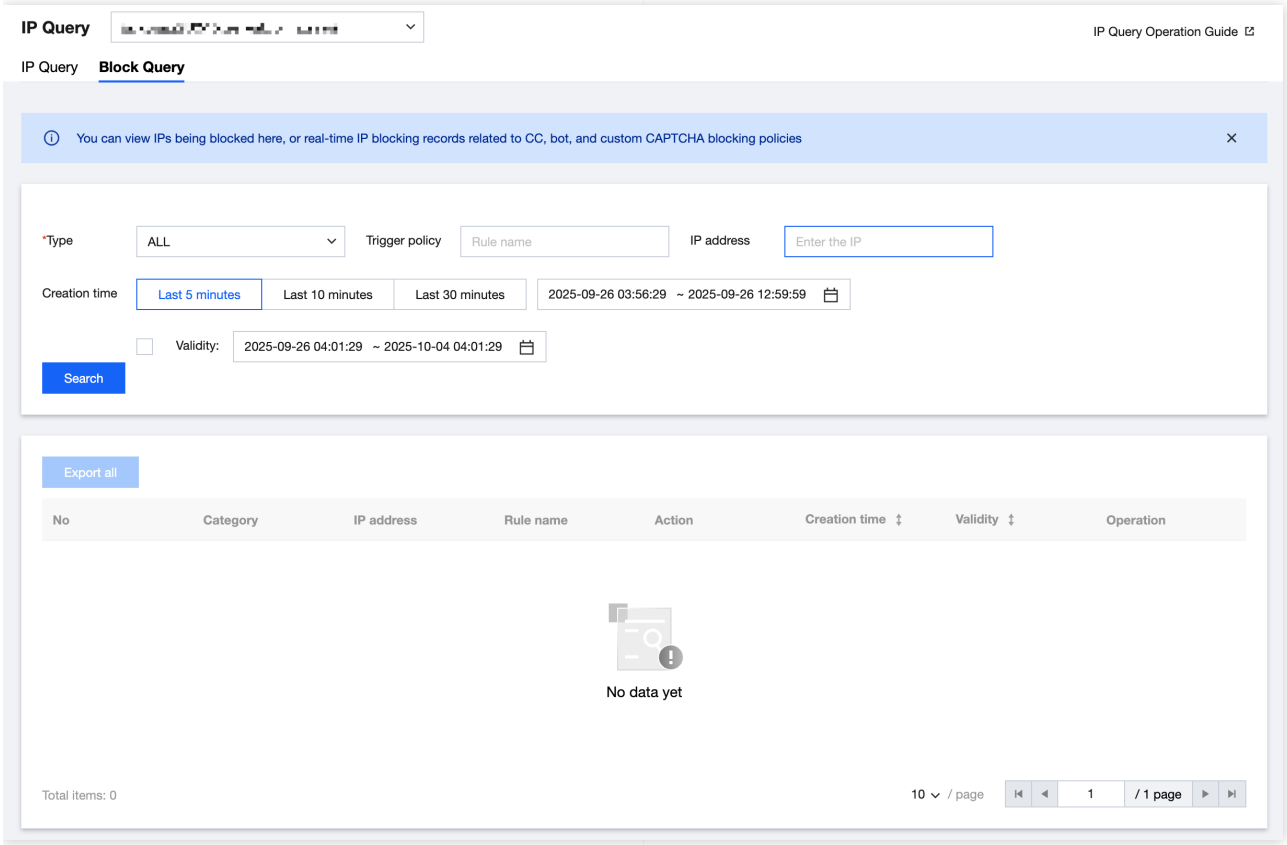
   When the domain name is set to ALL, the added IP blocklist/allowlist is the global blocklist/allowlist.
3. The blocklist/allowlist supports import and filtered result export. See the export format when the IP information is imported.



4. After adding, you can enter the added source IP in IP Query to query status information.

Example 3: IP Blocking Status Query

Enter the WAF console, select IP Management > IP Blocking Status to enter the query page. You can query the IP information intercepted by custom rules and the CC protection module. You can also export query results and add a single IP address to the blocklist/allowlist.

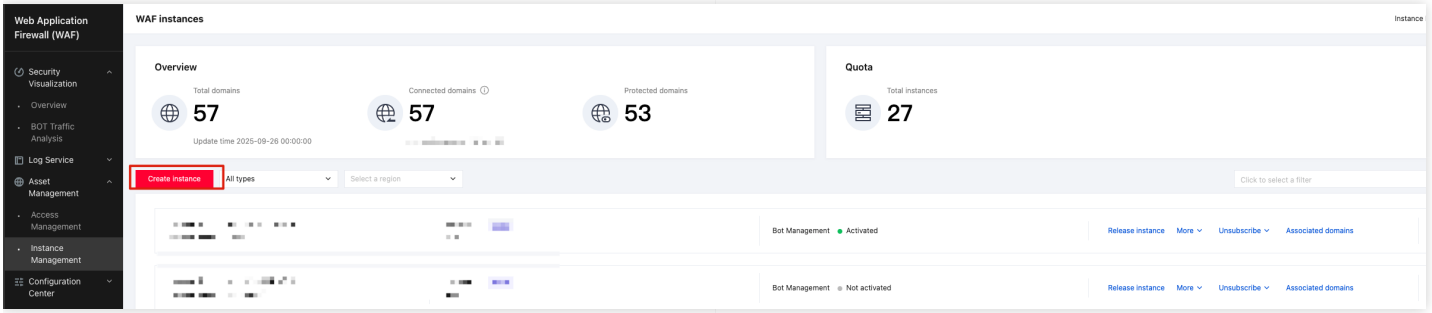

IP Query
IP Query Operation Guide
IP Query
Block Query
You can view IPs being blocked here, or real-time IP blocking records related to CC, bot, and custom CAPTCHA blocking policies
*Type
ALL
Trigger policy
Rule name
IP address
Enter the IP
Creation time
Last 5 minutes
Last 10 minutes
Last 30 minutes
2025-09-26 03:56:29 ~ 2025-09-26 12:59:59
Validity:
2025-09-26 04:01:29 ~ 2025-10-04 04:01:29
Search
Export all
No
Category
IP address
Rule name
Action
Creation time
Validity
Operation
No data yet
Total items: 0
10 / page
1
/ 1 page

Common Operations
Scenario 1: Creating an Instance

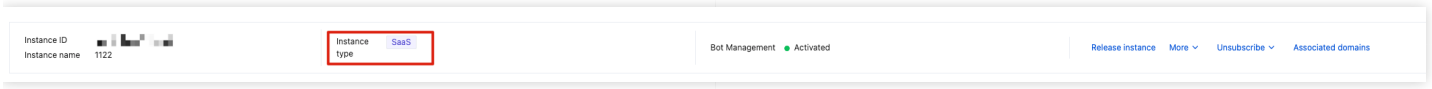
An instance is the minimum metering unit of WAF. Multiple instances can be created, and one instance can manage 20 domain names.
The following operations take the cloud as an example to create an instance.

Creating a SaaS Instance

1.Log in to the Tenant Side WAF > Asset Center > Instance Management page, and click Create Instance.

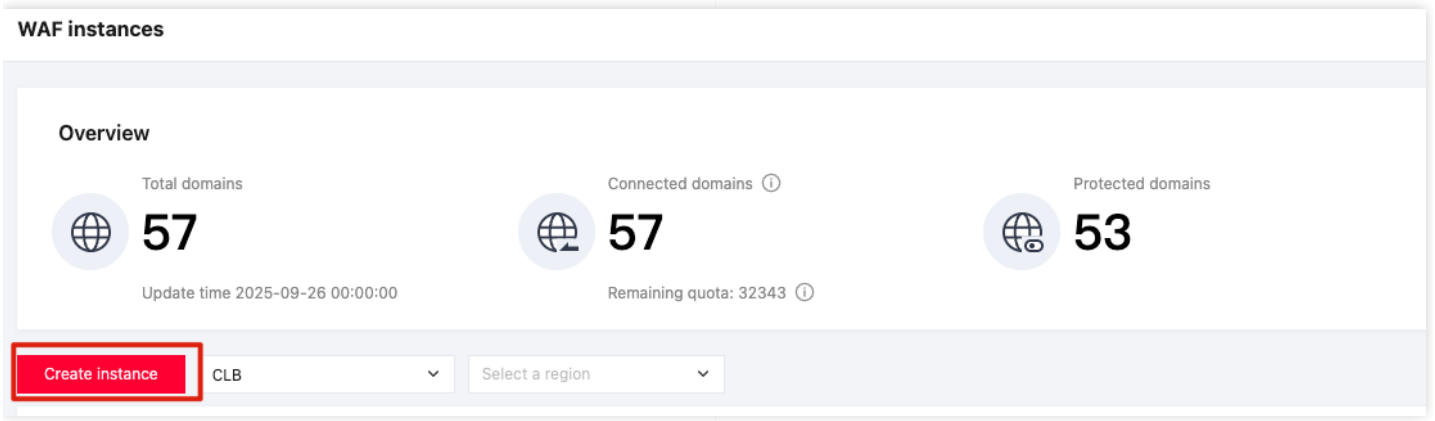


2.On the purchase page, select SaaS Type for the instance type, fill in "cloud" for the instance name, and click Buy Now.

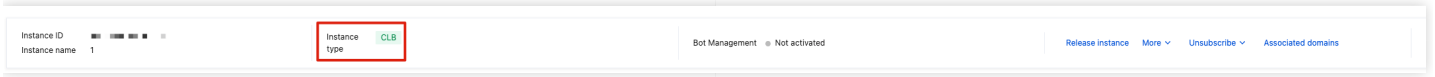


Creating a CLB Instance

1.Log in to the Tenant Side WAF > Asset Center > Instance Management page, and click Create Instance.



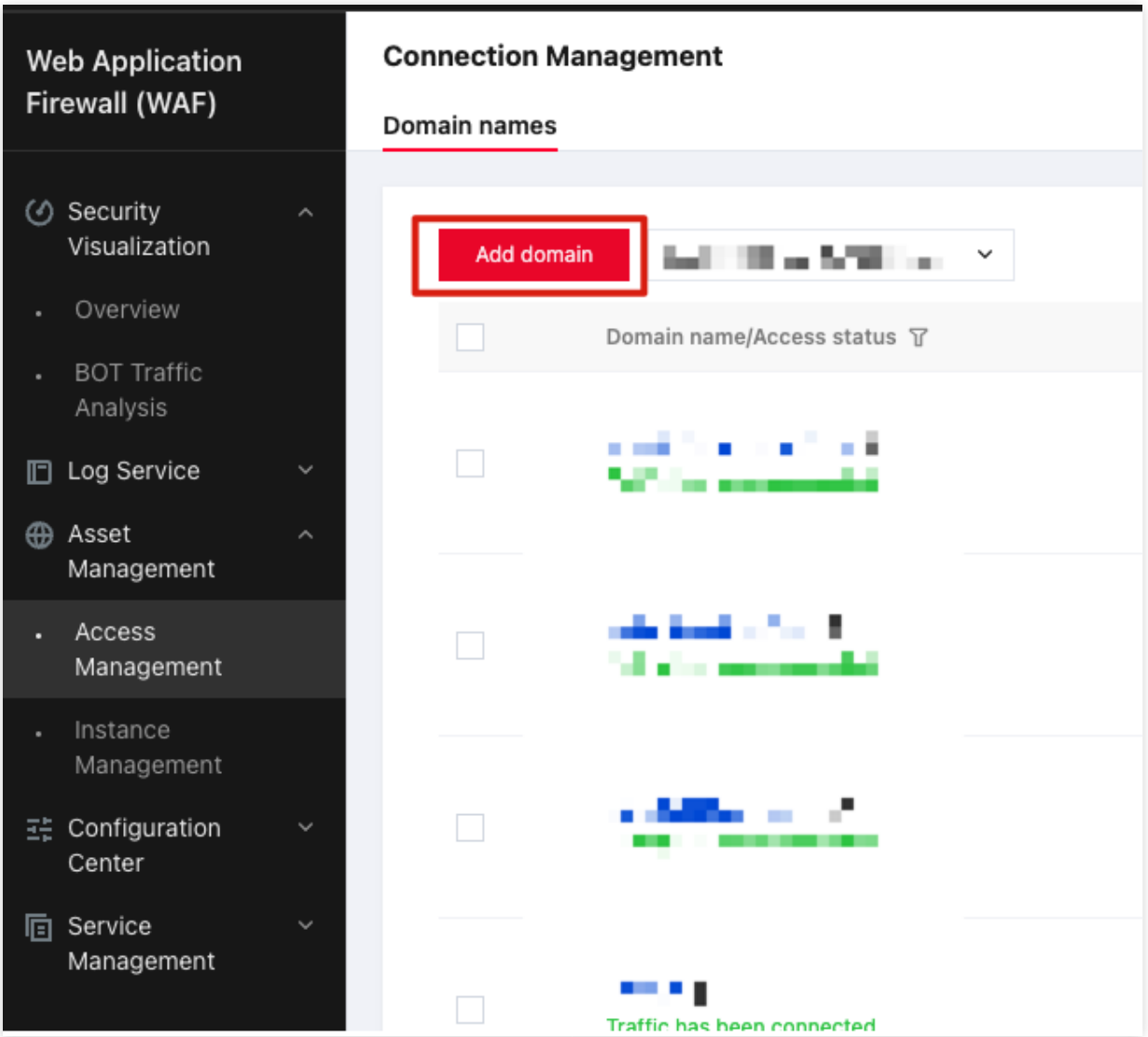
2.On the purchase page, select CLB Instance for the instance type, fill in "cloud" for the instance name, and click Buy Now.



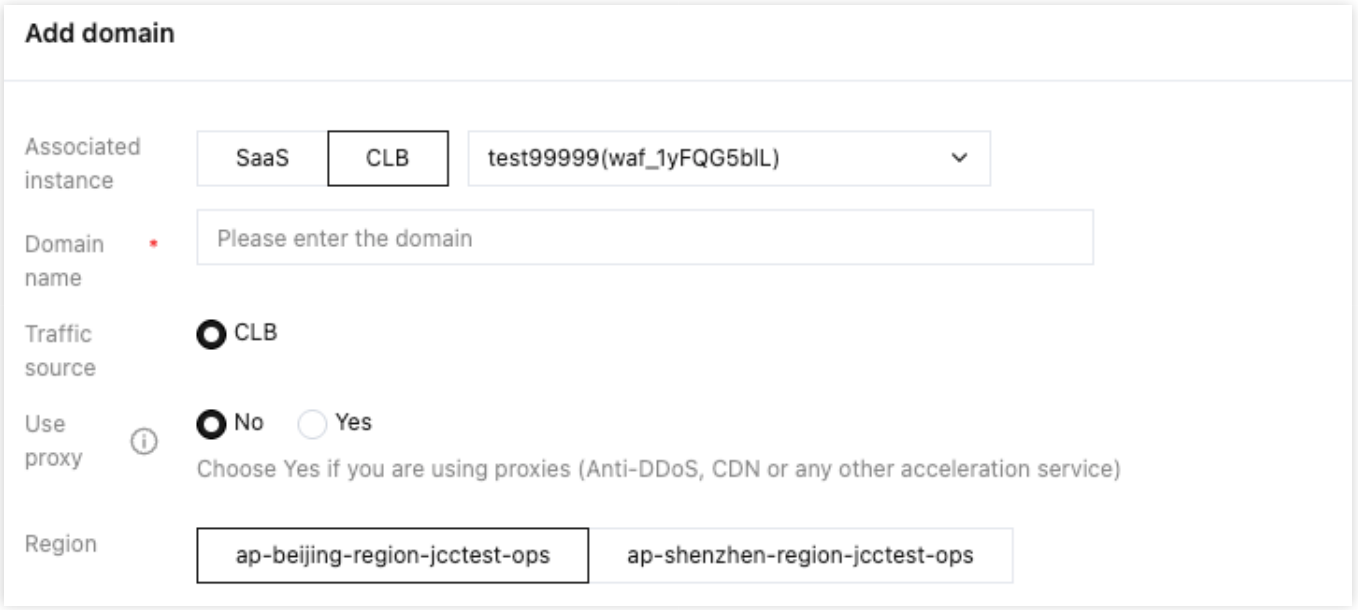
Scenario 2: Adding a CLB WAF Protected Domain Name

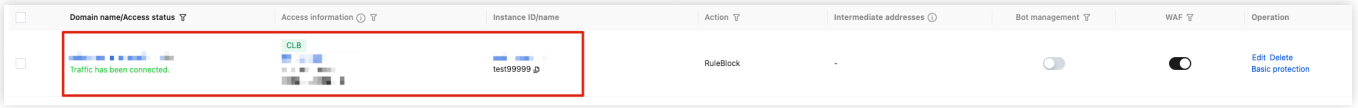
The following operations take "www.sz.com" as an example. The "www.sz.com" domain name is bound to the CLB of this tenant.

1. Log in to the Tenant Side WAF > Asset Center > Access Management page, select an instance, and click Add Domain Name.



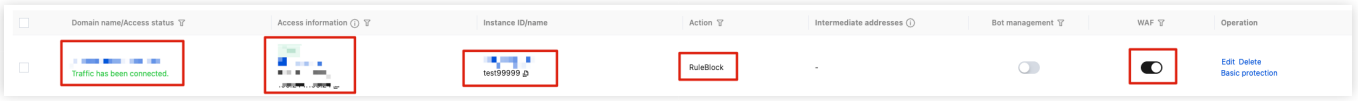
2. On the Add Domain page, enter a domain name, select its corresponding load balancer listener, and then click Confirm.





3. Enter the Access Management interface and check the domain name protection status.

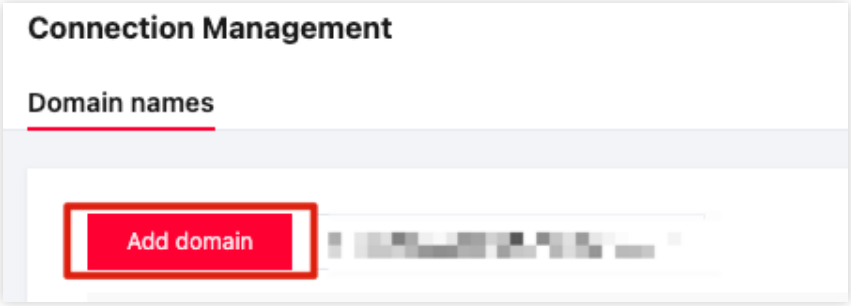
- Check the domain name/access status and confirm that the added domain name is the expected one.
- Check that the IP in the access information is the VIP in the CLB instance.
- Check that the ID/name of the associated instance is the expected instance ID.
- Check that the filtering mode is in use: The filtering mode can detect traffic and intercept malicious traffic; the image mode cannot intercept traffic but can detect traffic.
- Check that the WAF switch is in the blue enabled status.



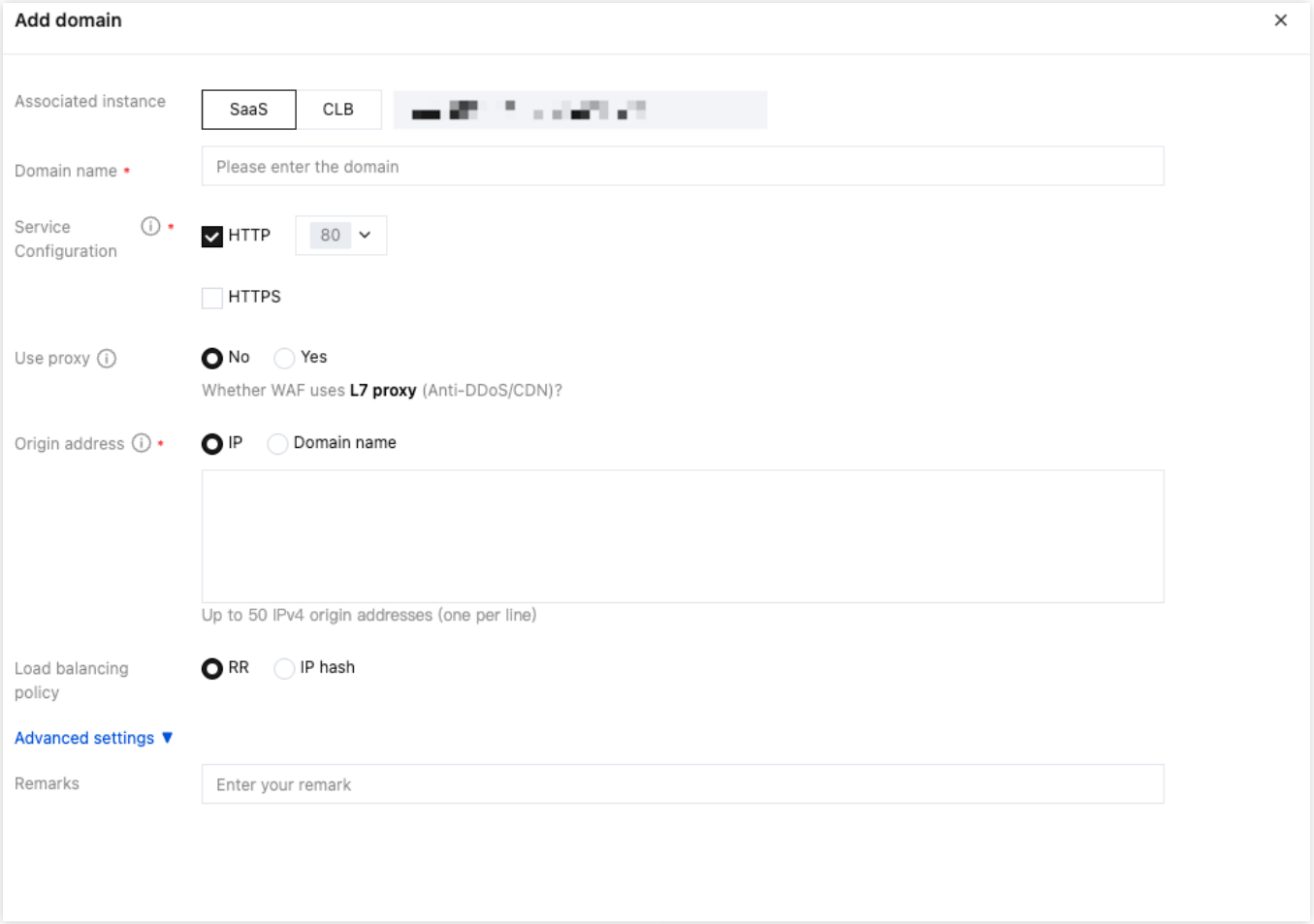
Scenario 3: Adding a SaaS WAF Protected Domain Name

The following operations take "www.cloud.com" as an example.

1. On the Tenant Side WAF > Asset Center > Access Management page, select a "cloud" instance, and click the Add Domain Name button.



2. In the Add Domain Name interface, select the SaaS type, and confirm that the instance is the expected one. Fill in the instance domain name, select the actual site port, write the actual origin server address, and click the OK button.



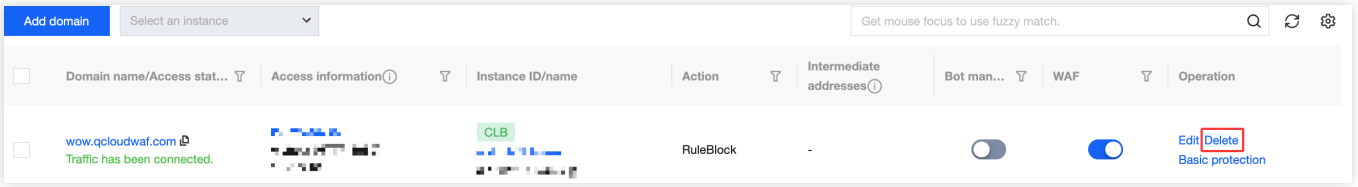
3. After the domain name is successfully accessed, go to the Tenant Side WAF > Asset Center > Access Management page and check that the domain name access status is normal and the WAF switch is enabled properly.



Scenario 4: Deleting a Protected Domain Name

The following operations take "www.sz.com" as an example.

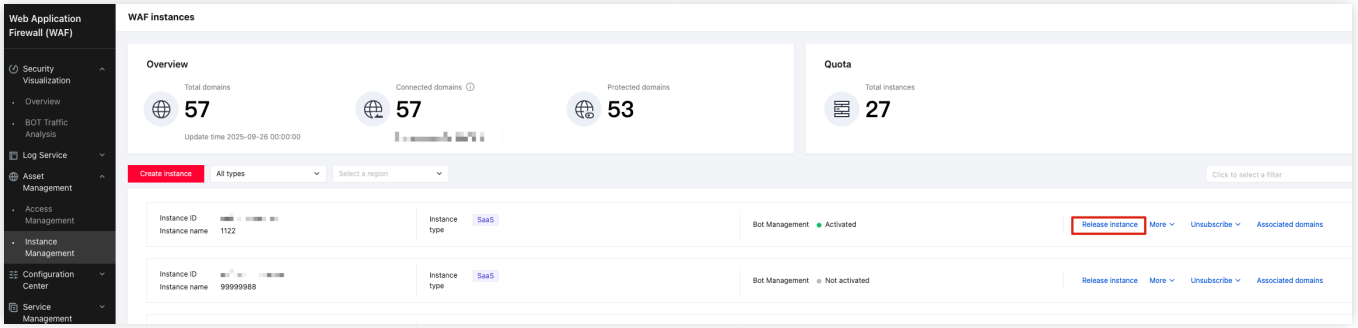
1. Log in to the Tenant Side WAF > Asset Center > Access Management, find the corresponding domain name, and delete it.

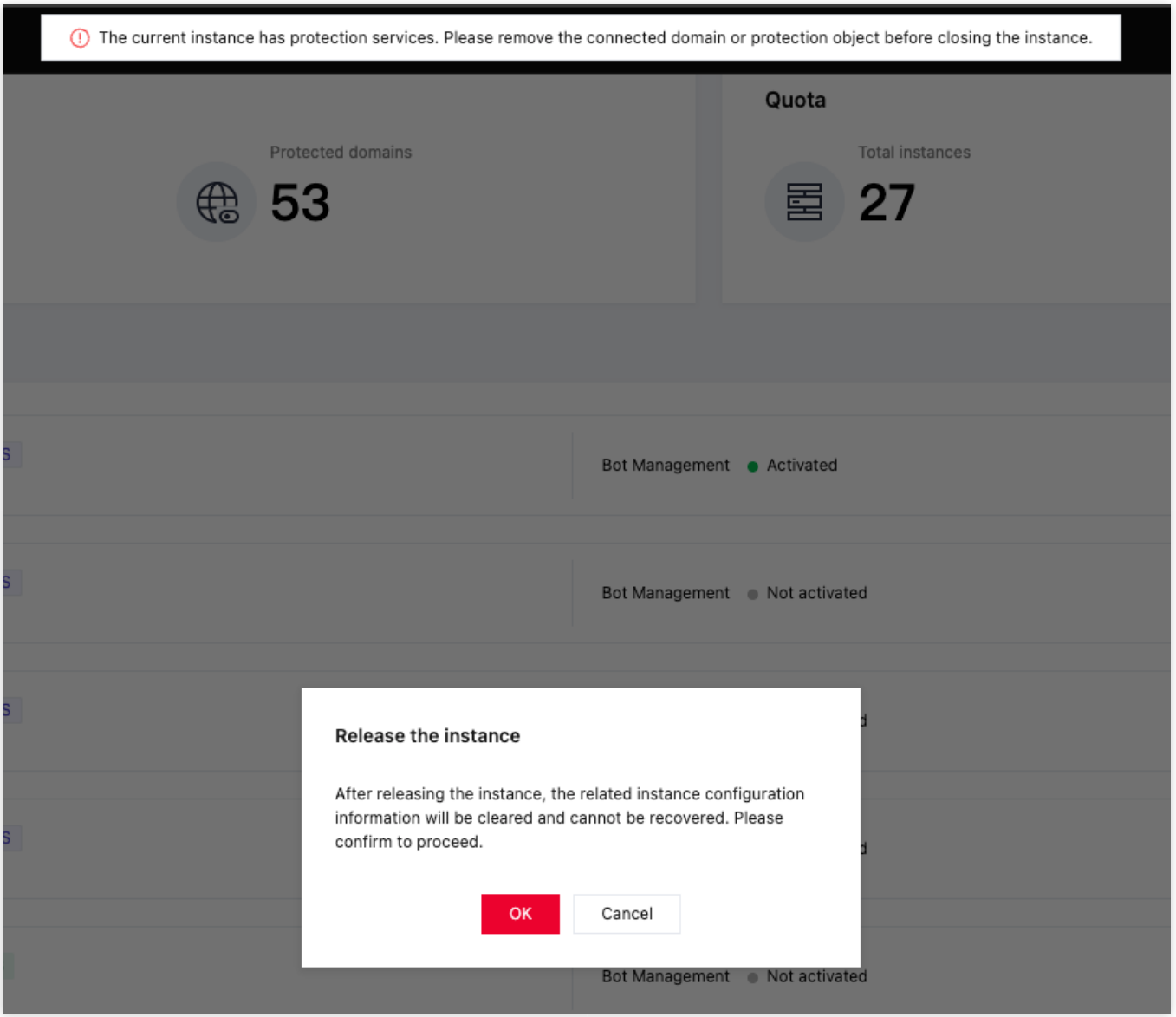


Scenario 5: Deleting an Instance

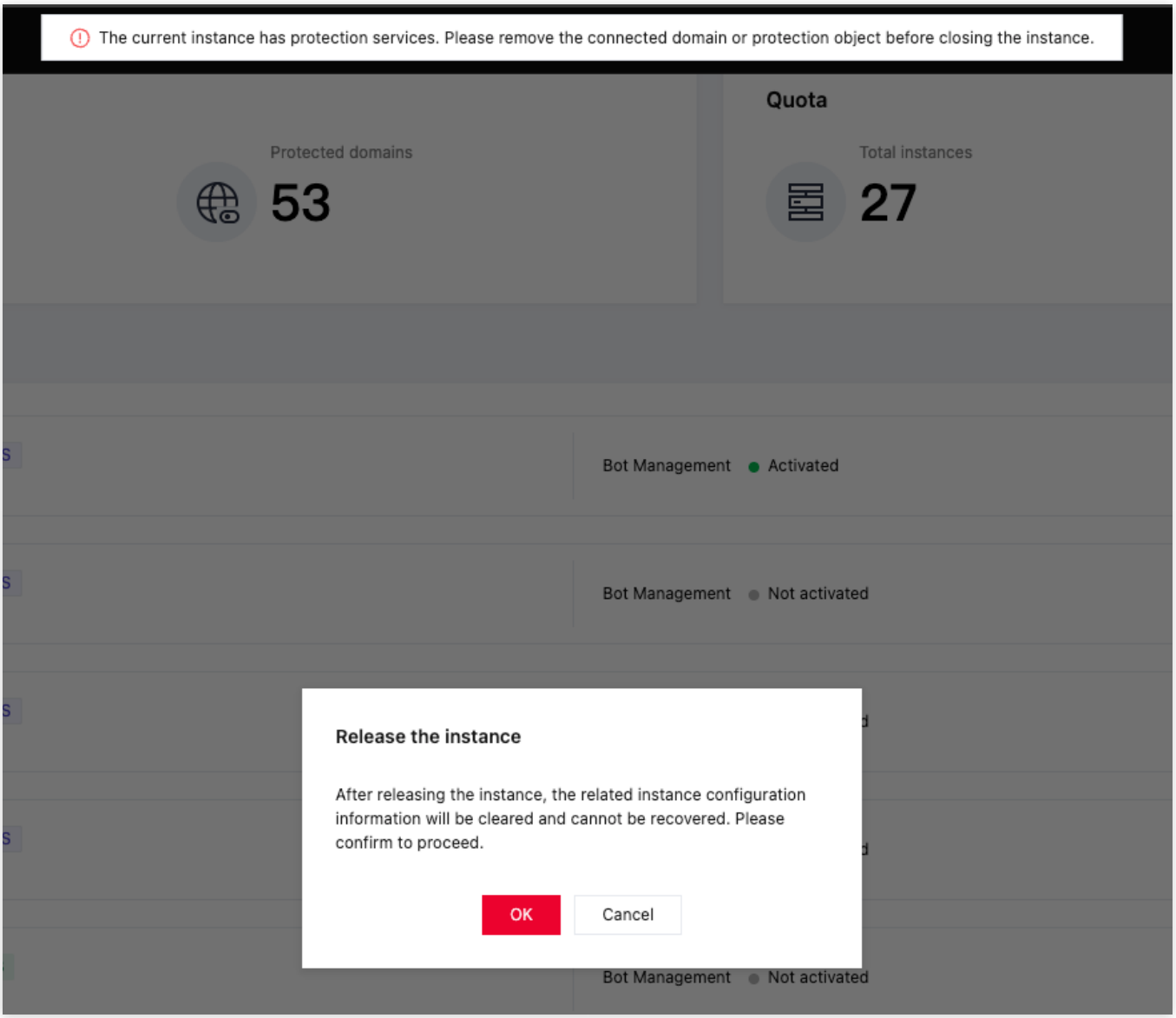
The following operations take CLB WAF as an example, with the prerequisite that there is no domain name in the instance:

1. Log in to the Tenant Side WAF > Asset Center > Instance Management, find the corresponding instance, click the Release Instance button, and click OK.



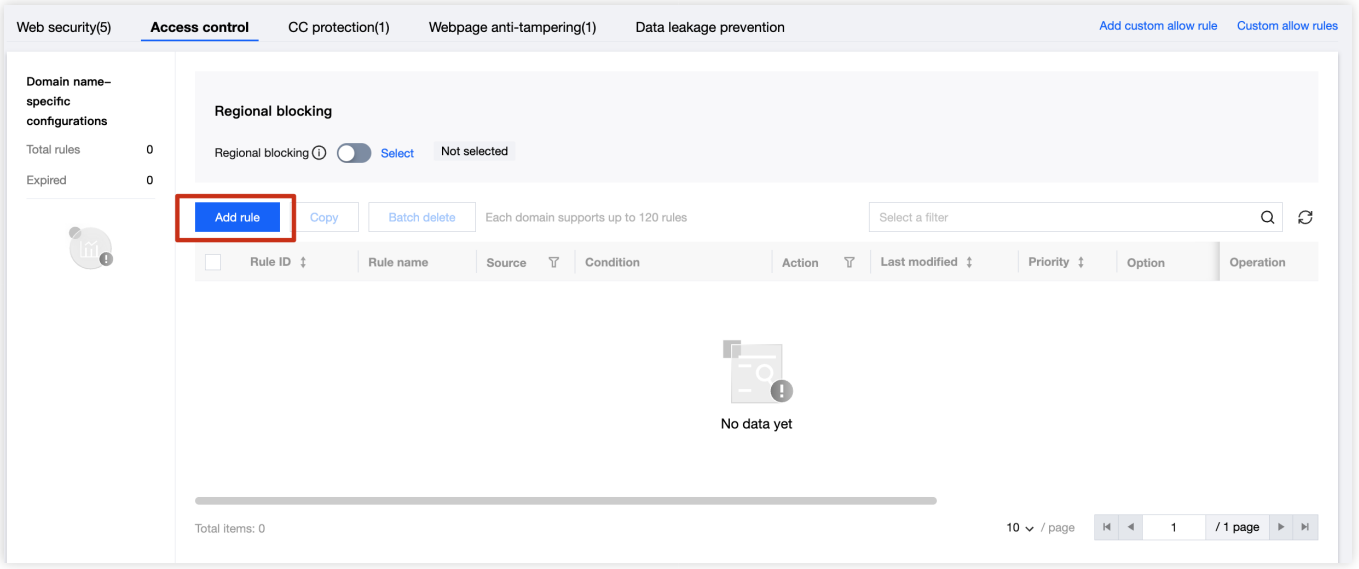


2. If there is a domain name in the instance, the instance release will fail.

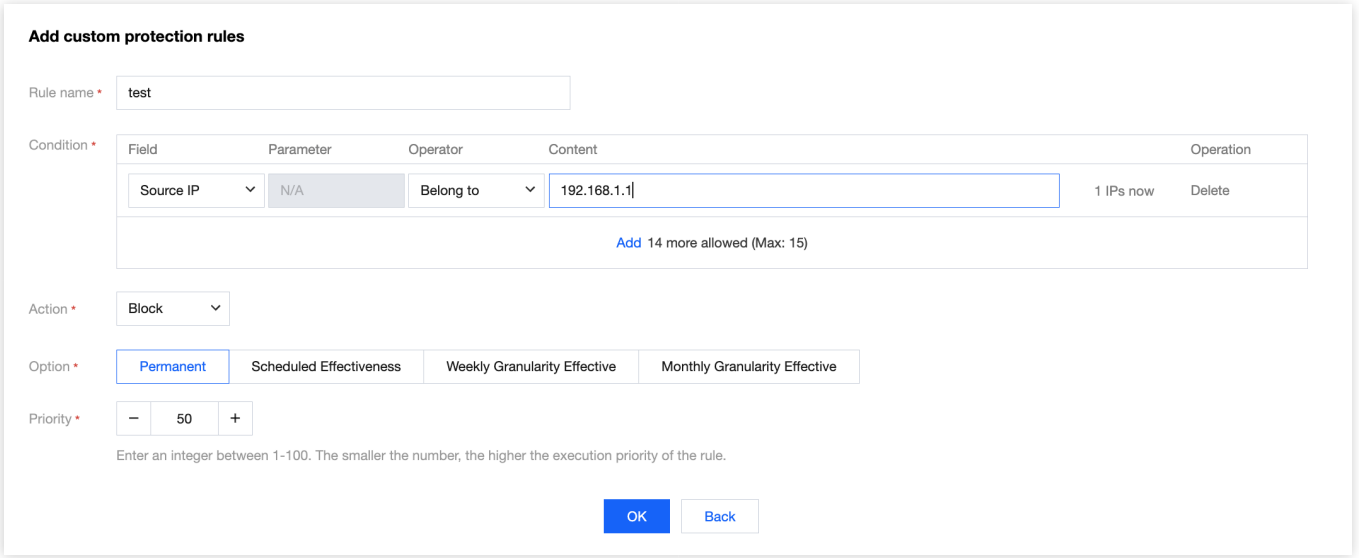

The current instance has protection services. Please remove the connected domain or protection object before closing the instance.
Quota
Protected domains
53
Total instances
27
Bot Management Activated
Bot Management Not activated
Release the instance
After releasing the instance, the related instance configuration information will be cleared and cannot be recovered. Please confirm to proceed.
OK
Cancel
Bot Management Not activated

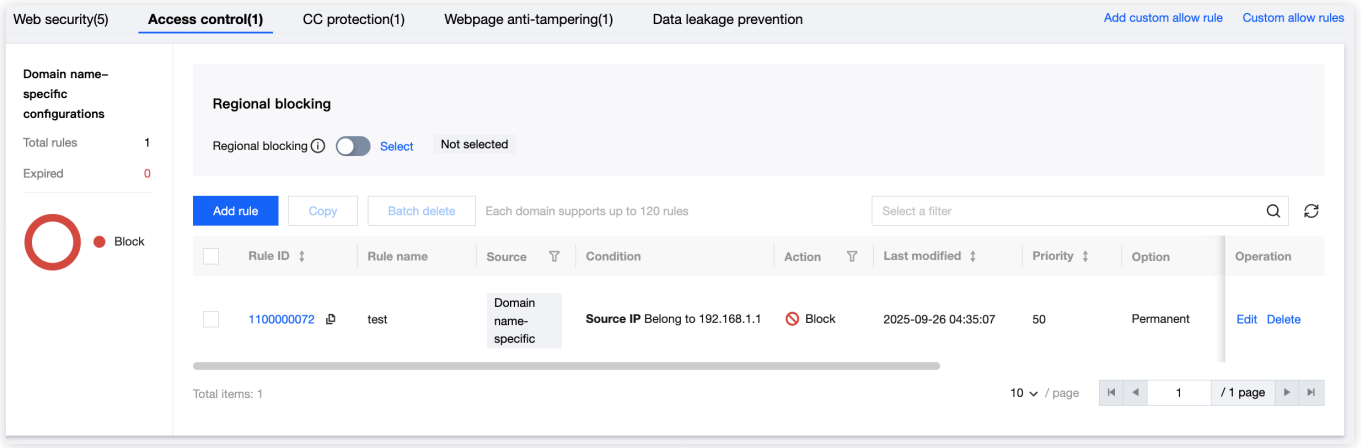
Scenario 6: Adding a Custom Rule

1. Log in to the tenant-side WAF console and navigate to the basic security page. Select the required domain name and click Access Control.



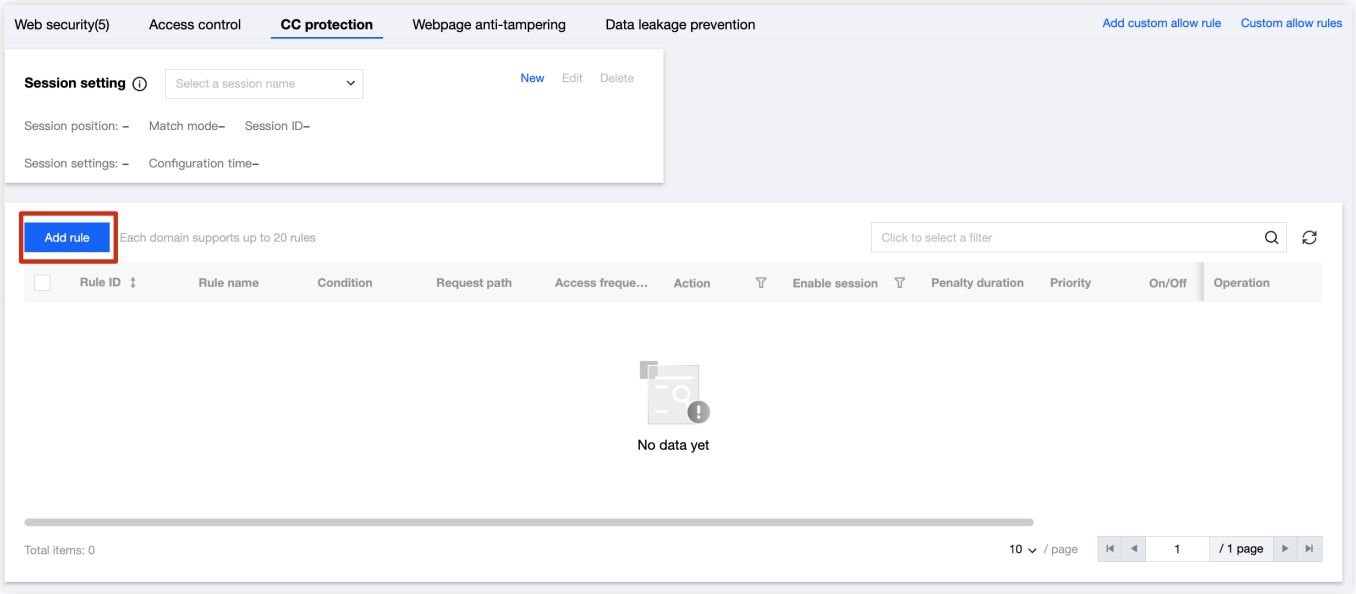
2. Click Add Rule to add a custom policy. Set the matching field to 'Request Path', select 'Contains' as the logical operator, set the matching content to '/admin', and configure the action to Block. Finally, click OK.



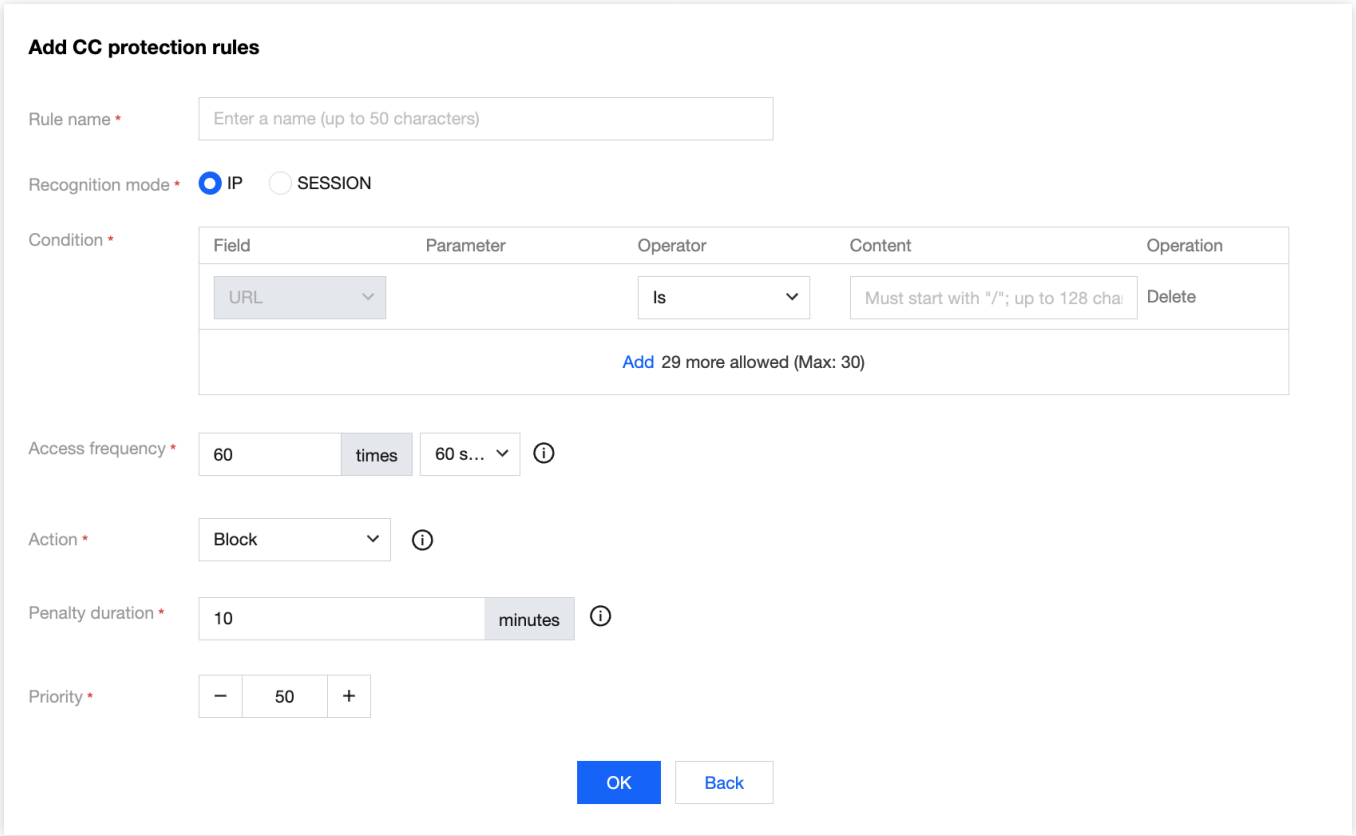

Web security(5)
Access control(1)
CC protection(1)
Webpage anti-tampering(1)
Data leakage prevention
Add custom allow rule
Custom allow rules
Domain name–specific configurations
Total rules 1
Expired 0
Block
Regional blocking
Regional blocking
Select
Not selected
Add rule
Copy
Batch delete
Each domain supports up to 120 rules
Select a filter
Rule ID
Rule name
Source
Condition
Action
Last modified
Priority
Option
Operation
1100000072
test
Domain name-specific
Source IP Belong to 192.168.1.1
Block
2025-09-26 04:35:07
50
Permanent
Edit
Delete
Total items: 1
10 / page
1
/ 1 page

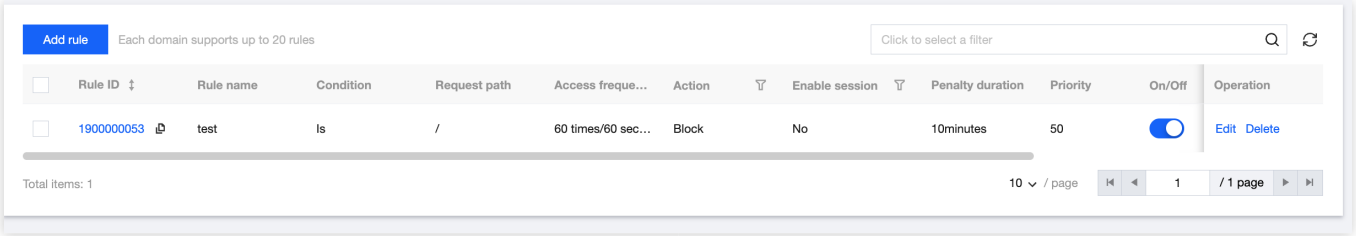
Scenario 7: Adding a CC Protection Rule

1. Log in to the tenant-side WAF console and navigate to the basic security page. Select the required domain name and click CC Protection.



2. Click Add Rule to add a CC protection rule. Enter the rule name, specify the URL as '/test.html', set the access frequency to 3 times/10 seconds, select the Intercept action, set the penalty duration to 2 minutes, and finally click OK.




Add rule
Each domain supports up to 20 rules
Click to select a filter
Rule ID
Rule name
Condition
Request path
Access freque...
Action
Enable session
Penalty duration
Priority
On/Off
Operation
1900000053
test
Is
/
60 times/60 sec...
Block
No
10minutes
50
Edit
Delete
Total items: 1
10 / page
1
/ 1 page

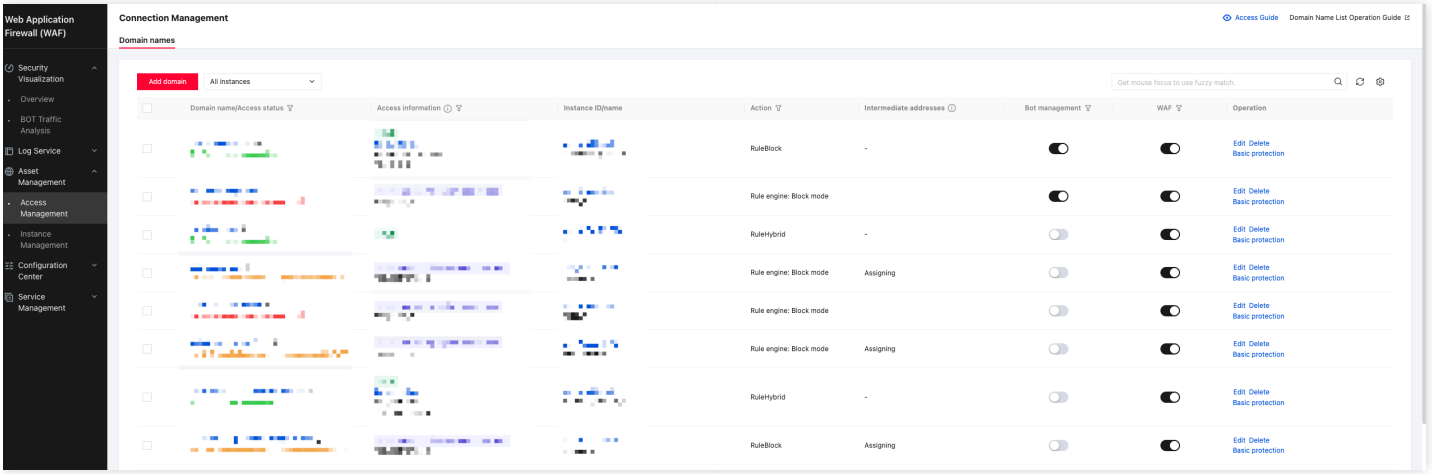
Scenario 8: Checking Whether a Domain Name Is in Protected Status

Inspection Scheme for Whether the Domain Name on the Tenant Side Has Enabled Protection

Operator: Tenant side Ops personnel.

Step 1: Viewing the Number of Protected Domain Names and Specific Domain Names in WAF

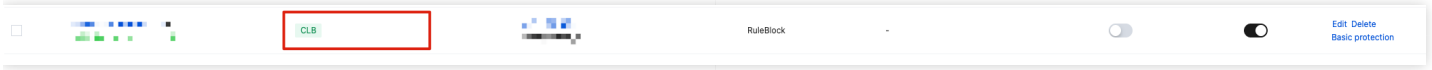
Log in to the Tenant Side WAF > Asset Center > Access Management interface, and view the number of WAF-protected domain names and specific domain names.

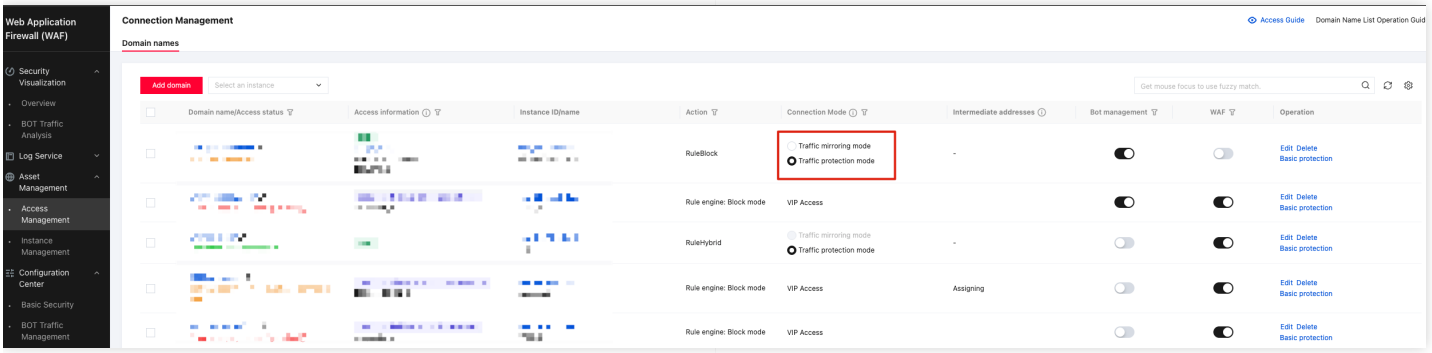


Step 2: Viewing the Domain Name Protection Status (The domain name protection status is disabled in the following four scenarios.)

The Listener Being Blank or "Default"

Log in to the Tenant Side WAF > Asset Center > Access Management interface to view the domain name access information. If the access information is blank or default, the domain name protection is abnormal.

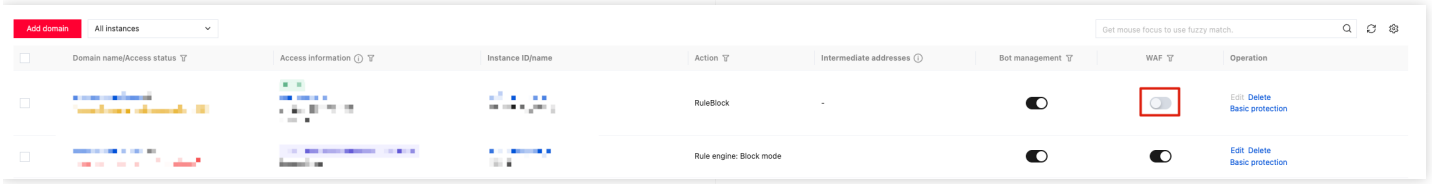




The Domain Name Protection Switch Being "Disabled"

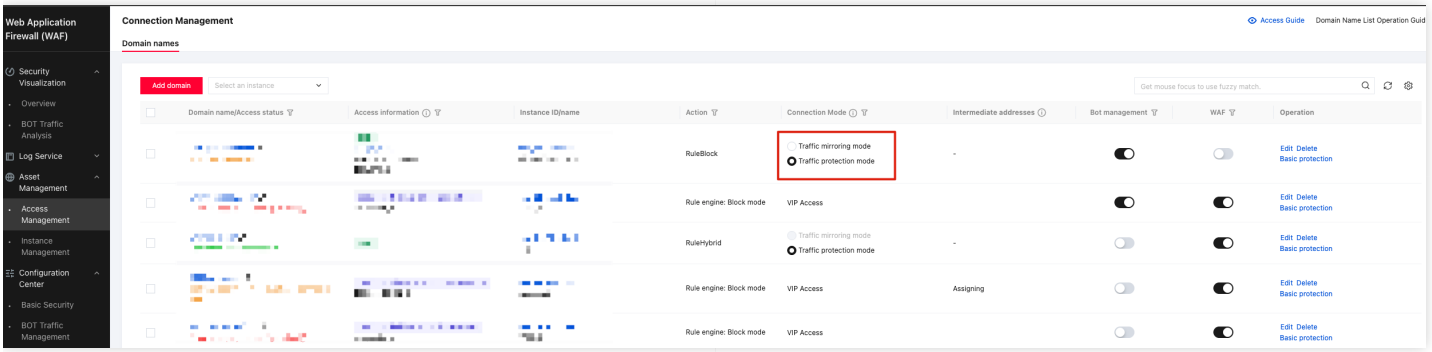
Log in to the Tenant Side WAF > Asset Center > Access Management interface to check the WAF switch. If the WAF switch is "gray", traffic will not be transferred to WAF, and the domain name protection does not take effect.

Remarks: The WAF switch is "blue" when enabled and "gray" when disabled.



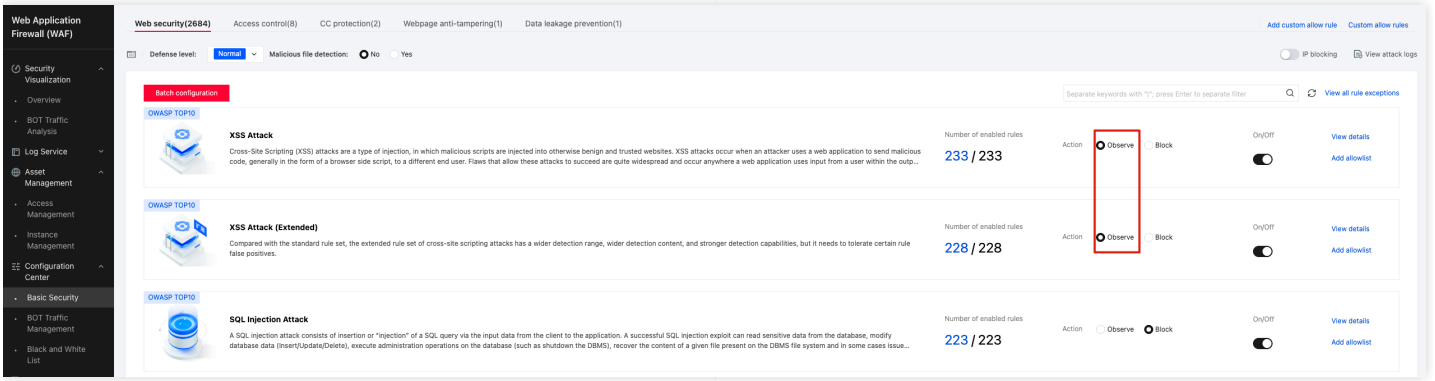
The Domain Name Traffic Mode Is "Image Mode"

Log in to the Tenant Side WAF > Asset Center > Access Management interface to view the domain name usage mode. If it is image mode, it only records attack logs without interception, and the domain name protection and interception do not take effect.



The Domain Name Rule Mode Being "Observation Mode"

Log in to the Tenant Side WAF > Configuration Center > Basic Security interface, select a domain name, and view the domain name protection mode. If it is observation mode, the domain name rule interception feature does not take effect.



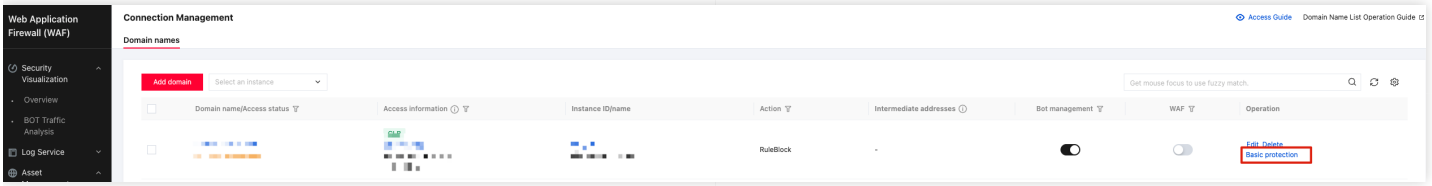
Scenario 9: Emergency Plan

Emergency Plan for the False Interception of Customer Workload by the Protected Domain Name

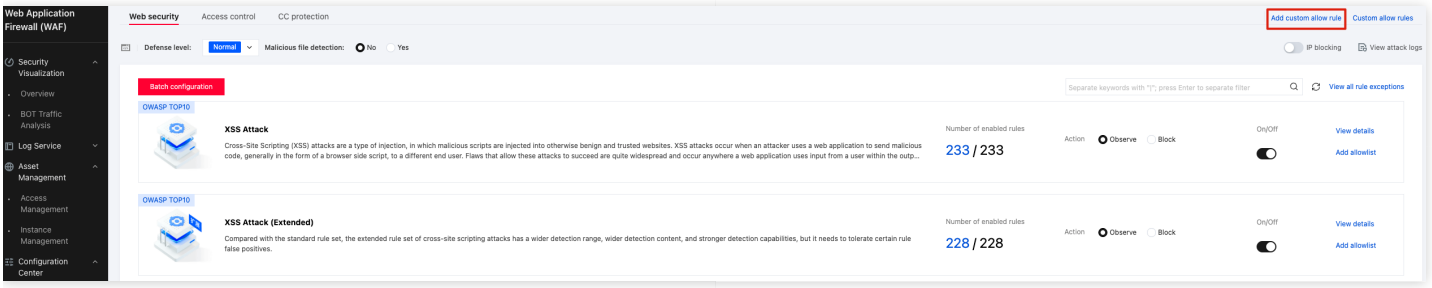
After a protected domain name is connected to WAF, normal access to some URLs is intercepted. Based on an assessment of the business impact scope, it is recommended to sequentially use Method 3, Method 2, and Method 1.

Emergency Method 1: Adding to Allowlist (Allow Specific Allowlist and Intercept Other Access that Hits Rules)

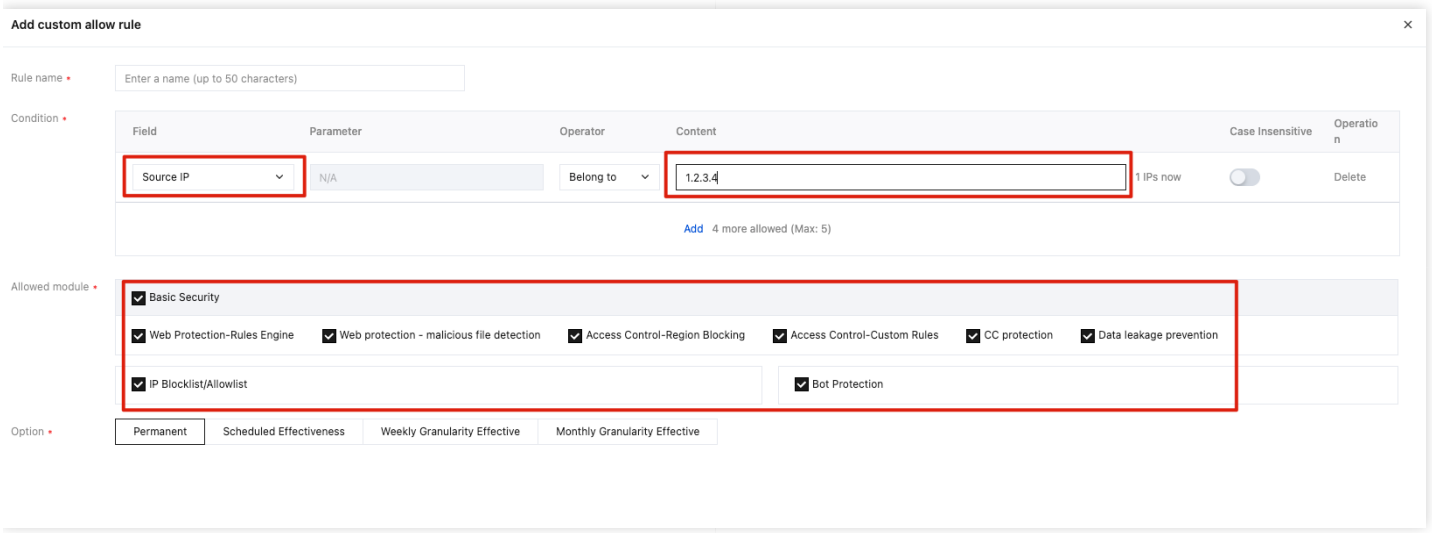
Add allowing rules on the console page.



Select the Precise Allowlist.



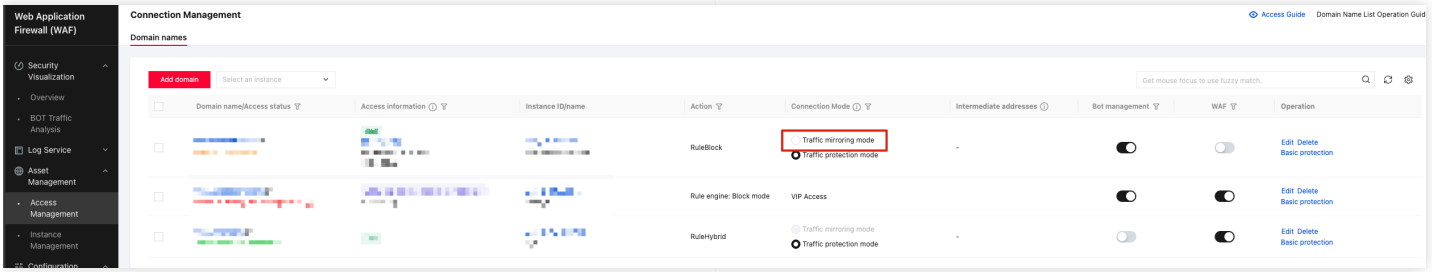
Configure rules according to the path of the alarm.



If the above configuration does not meet expectations, execute Method 2.

Emergency Method 2: Changing the Traffic Mode to Image Mode (Alarm Only Without Interception)

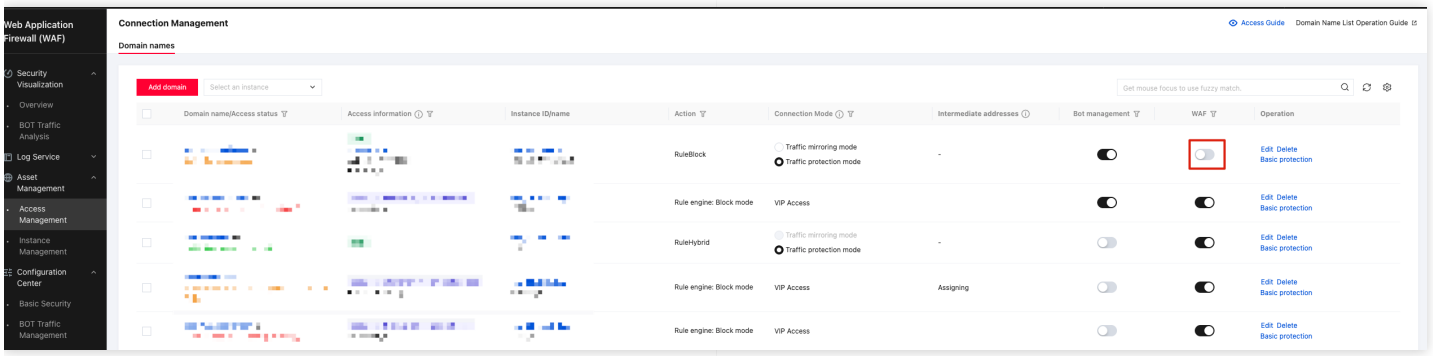
Change the WAF working mode to image mode on the console page.
Click Access Management and configure the Image Mode.



If the configuration still does not meet expectations, execute Method 3.

Emergency Method 3: Disabling the Protection Capability of the Domain Name (No Alarms or Interception)

Turn off the WAF switch on the console page. At this point, the entire domain name does not intercept any attacks.


Web Application Firewall (WAF)
Security Visualization
Overview
BOT Traffic Analysis
Log Service
Asset Management
Access Management
Instance Management
Configuration Center
Basic Security
BOT Traffic Management
Connection Management
Access Guide
Domain Name List Operation Guide
Domain names
Add domain
Select an instance
Get mouse focus to use fuzzy match.
Domain name/Access status
Access information
Instance ID/name
Action
Connection Mode
Intermediate addresses
Bot management
WAF
Operation
RuleBlock
Traffic mirroring mode
Traffic protection mode
Edit Delete
Basic protection
Rule engine: Block mode
VIP Access
RuleHybrid
Assigning

Best Practice
Building a CLB WAF Test Environment

Building a CLB WAF Test Environment

Creating a CVM

1. Log in to the tenant side, enter the CVM page, select the corresponding region, and click Create.
2. Select the network consistent with the CLB network, select other options according to the actual situation, and click Next: Select Image.
3. After selecting the image according to the actual situation, click Next: Select Storage and Bandwidth.
4. After selecting the storage and bandwidth according to the actual situation, click Next: Set Security Group and Host.
5. After selecting the security group and host according to the actual situation, enter the host password and click Next: Confirm Configuration Information.
6. Check the information you just selected. After confirming that everything is correct, click Enable.

Applying for an EIP and Binding It to the CVM

1. Under the CVM menu, click Elastic IP, select the same region as the CVM region, and click Apply. Then select options according to the actual situation.
2. Click Confirm to return to the Elastic IP List page, and you can see that the created elastic IP address is displayed as Unbound.
3. Click the Operation column on the Elastic IP page, click More, and select Bind.
4. Select the CVM you want to bind and click Confirm.
5. Check the information that needs to be confirmed. After confirming that everything is correct, click Confirm.
6. Go to the Elastic IP List page. You can see that the created EIP address is displayed as Bound.

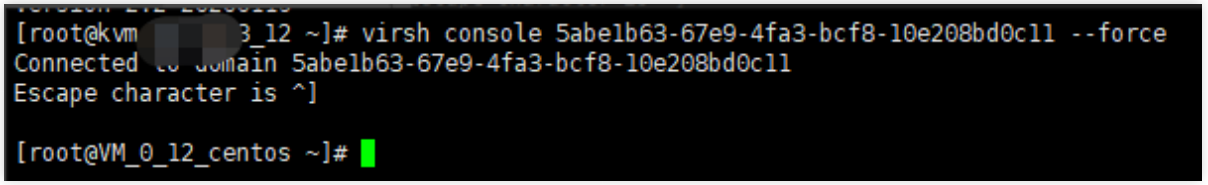
Installing Nginx and Enabling Port 80

1. Click the CVM ID. On the CVM parameter page, copy the server ID of the CVM.

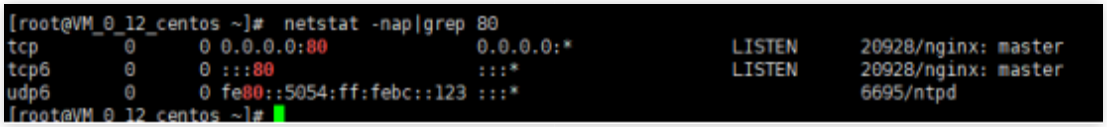
2. Enter CVM on the operation side, choose VM Management > Tenant-Side Resources, select UUID in the search box, and then paste the server ID you just copied to find the private IP address of the host.

3. Log in to the private IP address of the host and enter the command: ssh host private IP address. The password is the one entered when you activated CVM.

4. Enter the virsh console UUID --force command. For example, enter the virsh console 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11 --force command to enter CVM.



5. After entering CVM, enter the following command to perform an installation:
   Install: <1>yum install -y nginx
   Start the Nginx service: service nginx start .
   Check whether port 80 is enabled: netstat -nap|grep 80 .



Since some customers prohibit external access to ports 80 and 443 on their public IP addresses, you need to forward port 80 of the CVM to another port (for example, port 788) through a NAT gateway and associate this gateway in the route table. You can ignore this step if it is not involved.

1. Under the VPC menu, select NAT Gateway. After selecting the corresponding region, click Create to create a NAT gateway.
2. Enter information according to the actual situation and click Create to return to the NAT Gateway List page.
3. In the created NAT gateway, click the gateway ID.
4. Click Port Forwarding.
5. Click Create.

6. Add a port to be forwarded.
7. Under VPC, select Route Table. Under the corresponding region, click Create to create a route table.
8. Enter information and click Create. Select the policy as the added NAT gateway.
9. A prompt indicates that you need to associate a subnet. After selecting the associated subnet, click OK to return to the Route Table List page.

http://public ip address:788/ to verify whether the website is normal">Visiting http://Public IP Address:788/ to Verify Whether the Website Is Normal

Adding a CLB Instance and Listener

1. Click CLB. On the LB Instance List page, click Create.

2. Enter information according to the actual situation. The CLB should be consistent with that of the CVM network. Then click Confirm Activation.

3. On the Purchase Confirmation page, click Confirm.

4. Click Finish.

5. On the LB Instance List page, view the instance you just created and click the instance ID.

6. Click Listener Management.

7. Click Create or Start Creation to create a listener.

8. Enter the name, protocol, and port number. Enter the port number forwarded through the NAT gateway, such as 788. Then click OK.

9. Click Start Creation under the listener and enter the domain name to be configured. For subsequent steps, see "Binding HTTP Listeners in CLB Instance" in the "Functional Test Case (CLB) Tenant Side" documentation.

Adding Engine Nodes for CLB WAF:

1. Log in to the operation side. In Virtual Machine Management > Operation-side Resource in the CVM, allocate engine node IP addresses after submitting a request to the environment administrator.
2. Log in to the WAF operation side and click Add in Cluster Management.
3. Enter the engine IP addresses, use ";" to separate them, and click Confirm.
4. The IP addresses are added successfully.

Building a SaaS WAF Origin Server

Building a SaaS WAF Origin Server

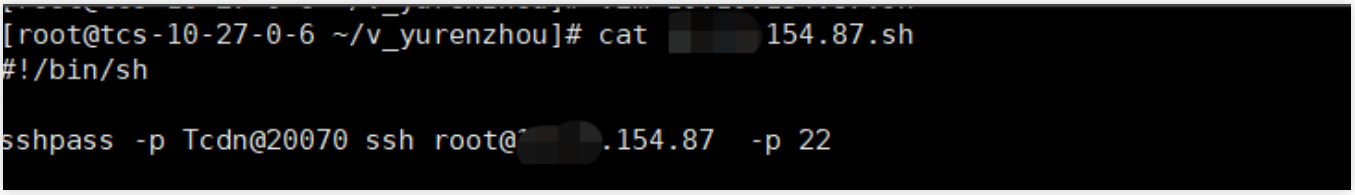
When you create a SaaS WAF domain name, you need to enter the origin server address. The origin server address only needs to be connected to the SaaS WAF engine. The origin server IP address can be either a private IP address or a public IP address. Next, an origin server of the private IP address type and an origin server of the public IP address type will be created, respectively.

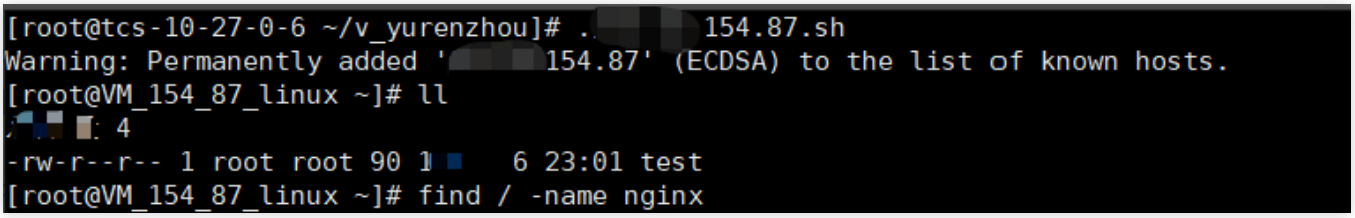
1. Origin Server with a Private IP Address

1. Log in to the operation side, select CVM to create a CVM. Click Operation-side Resource and click Create.

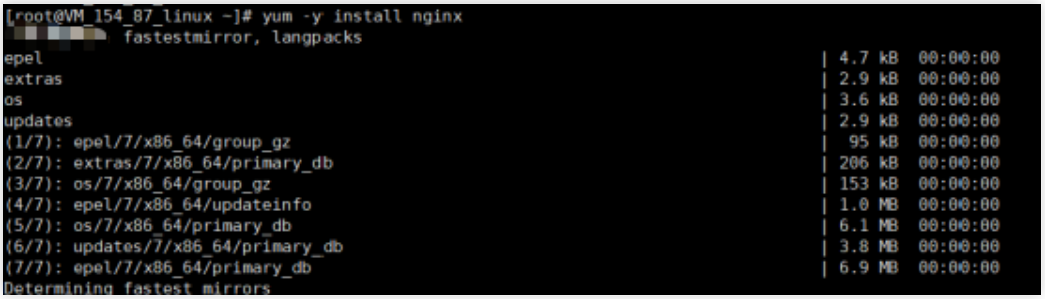
2. After configuring all information on the Create CVM page, view the newly added CVM.

3. Enter the newly-added CVM.





4. Install Nginx in the CVM and enter the <1>yum install -y nginx



Start the Nginx service: service nginx start .

Check whether port 80 is enabled: netstat -nap|grep nginx .

```
[root@VM_154_87_linux ~]# service nginx start
Redirecting to /bin/systemctl start nginx.service
[root@VM_154_87_linux ~]# netstat -nap |grep nginx
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      27979/nginx: master
tcp6       0      0 :::80                   :::*                    LISTEN      27979/nginx: master
unix  3      [ ]         STREAM     CONNECTED     103293   27979/nginx: master
unix  3      [ ]         STREAM     CONNECTED     103296   27979/nginx: master
unix  3      [ ]         STREAM     CONNECTED     103295   27979/nginx: master
unix  3      [ ]         STREAM     CONNECTED     103294   27979/nginx: master
```

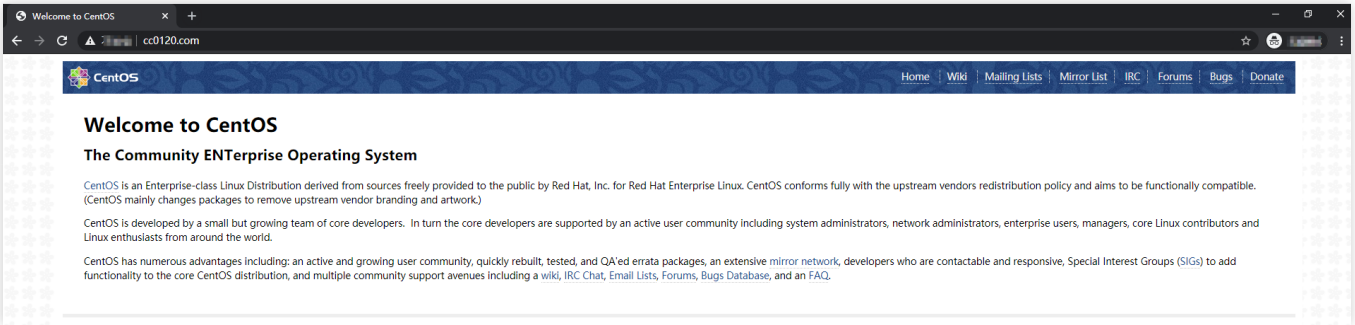
5. In the SaaS engine, use the ping or telnet command to test whether the IP address and port of the CVM are connected.

```
[root@VM_12_7_centos ~]# ping [redacted].154.87
PING 10.10.154.87 (10.10.154.87) 56(84) bytes of data.
64 bytes from [redacted].154.87: icmp_seq=1 ttl=53 time=0.823 ms
64 bytes from [redacted].154.87: icmp_seq=2 ttl=53 time=0.832 ms
^C
--- [redacted].154.87 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.823/0.827/0.832/0.029 ms
```

```
[root@VM_12_7_centos ~]# telnet [redacted].154.87 80
Trying [redacted].154.87...
Connected to [redacted].154.87.
Escape character is '^]'.
^]
telnet>
```

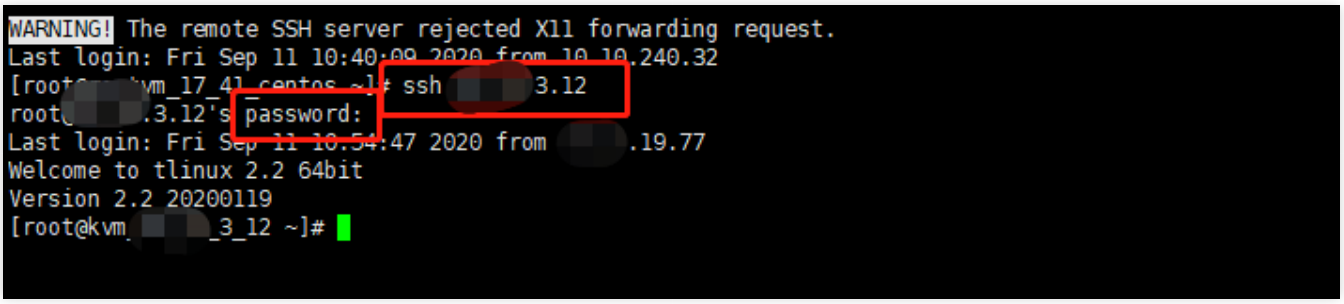
6. Add a domain name in SaaS WAF. For the origin server IP address, enter the CVM IP address you applied for.

7. Configure a host and access the newly added domain name. You can access the origin server of the private IP address type.

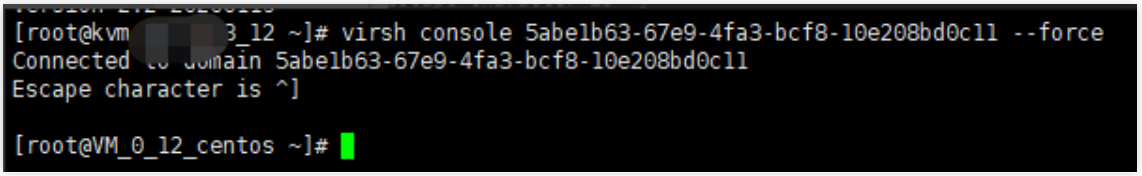


2. Origin Server with a Public IP Address

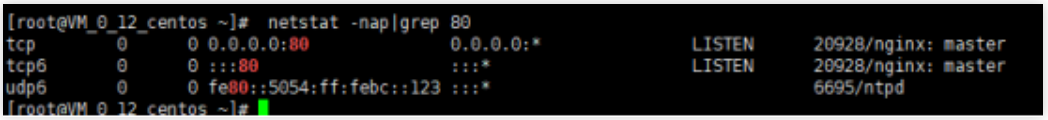
1. Log in to the tenant side, go to the CVM page, select the corresponding region, and click Create.
2. Select the network consistent with the CLB network, select other options according to the actual situation, and click Next: Select Image.
3. After selecting the image according to the actual situation, click Next: Select Storage and Bandwidth.
4. After selecting the storage and bandwidth according to the actual situation, click Next: Set Security Group and Host.
5. After selecting the security group and host according to the actual situation, enter the host password and click Next: Confirm Configuration Information.
6. Check the information you just selected. After confirming that everything is correct, click Enable.
7. Apply for an elastic IP address and bind it to the CVM. Under the CVM menu, click Elastic IP, select the same region as the CVM region, and click Apply. Then select options according to the actual situation.
8. Click Confirm to return to the Elastic IP List page, and you can see that the created elastic IP address is displayed as Unbound.
9. Click the Operation column on the Elastic IP page, click More, and select Bind.
10. Select the CVM you want to bind and click Confirm.
11. Check the information that needs to be confirmed. After confirming that everything is correct, click Confirm.
12. Go to the Elastic IP List page. You can see that the created EIP address is displayed as Bound.
13. Install Nginx, enable port 80, and then click the CVM ID. On the CVM parameter page that appears, copy the server ID of the CVM.
14. Enter CVM on the operation side, choose VM Management > Tenant-Side Resources, select UUID in the search box, and then paste the server ID you just copied to find the private IP address of the host.
15. Log in to the private IP address of the host and enter the command: ssh host private IP address. The password is the one entered when you activated CVM.



16. Enter the virsh console UUID --force command. For example, enter the virsh console 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11 --force command to enter CVM.



17. After entering CVM, enter the following command to perform an installation:
    Install: <1>yum install -y nginx
    Start the Nginx service: service nginx start .
    Check whether port 80 is enabled: netstat -nap|grep 80 .



18. Since some customers prohibit external access to ports 80 and 443 on their public IP addresses, you need to forward port 80 of the CVM to another port (for example, port 788) through a NATGW, and associate this gateway in the route table (ignore steps 2.18 to 2.26 if it is not involved). Under the VPC menu, select NAT Gateway. After selecting the corresponding region, click Create to create a NAT gateway.

19. Enter information according to the actual situation and click Create to return to the NAT Gateway List page.

20. In the created NAT gateway, click the gateway ID.

21. Click Port Forwarding.

22. Click Create.

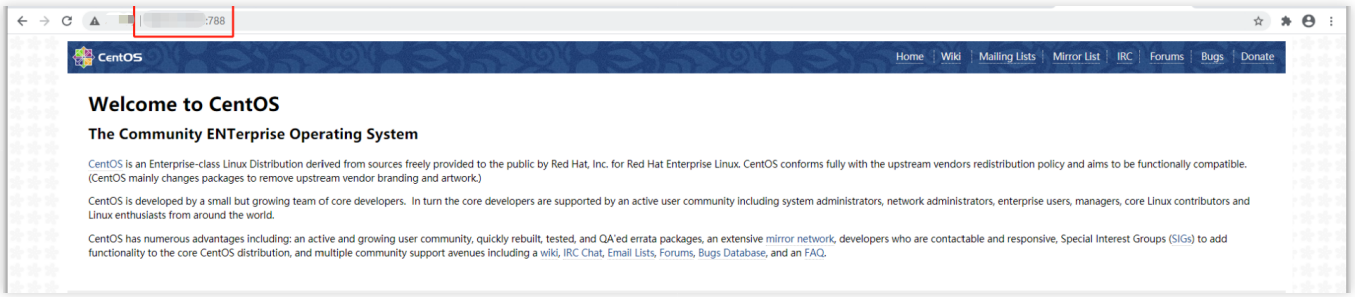
23. Add a port to be forwarded.

24. Under VPC, select Route Table. Under the corresponding region, click Create to create a route table.

25. Enter information and click Create. Select the policy as the added NAT gateway.

26. A prompt indicates that you need to associate a subnet. After selecting the associated subnet, click OK to return to the Route Table List page.

27. Visiting http://Public IP Address:788/ to Verify Whether the Website Is Normal



28. Add a domain name in SaaS WAF. For the origin server IP address, enter the elastic IP address.

FAQs

FAQs

Can a Non-Cloud Server Use WAF?

WAF supports off-cloud IDC user access and can protect any public network server, including but not limited to cloud platforms, including other vendors' cloud platforms and IDCs.

> Note:
>
> Domain names accessed in certain regions should comply with local policy requirements.

Does WAF Support HTTPS Protection?

WAF fully supports HTTPS workload. The user only needs to upload the SSL certificates and private key according to the prompts to enable WAF to protect HTTPS workload traffic.

Can the Origin Server IP of WAF Be a Private IP?

When a domain name is added to WAF, the origin server address should be a public IP address or a domain name. If a private IP address is entered, it should be confirmed by the administrator.

How Many Origin-Pull IP Addresses Can Be Set for a Protected Domain Name of WAF?

Up to 20 origin-pull IP addresses can be set for a protected domain name of WAF.

How to Achieve Load Balancing When Configuring Multiple Origin Servers for WAF?

If multiple origin-pull IP addresses are configured, WAF uses a round-robin scheduling approach to balance the load of access requests.

Does WAF Support Health Checks?

WAF enables health checks by default. It detects the connection status of all origin server IP addresses. If an origin server IP has no response, WAF will no longer forward requests to this IP until the access status returns to normal.

Does WAF Support Session Persistence?

WAF supports session persistence, which is enabled by default.

How Long Does It Approximately Take for the Configuration Change to Take Effect in the WAF Console?

Generally, the changed configuration takes effect within 10 seconds.

Will the WAF Automatically Add the Origin-Pull IP Range to the Security Group?

The origin-pull IP range will not be automatically added to the security group. See Quick Start to add the corresponding origin-pull IP address to the security group.

If the Uploaded File Is Intercepted, Will the File Using HTTPS or SFTP to Upload Still Be Intercepted?

If WAF is not used, it will not be blocked. If WAF is used and the interception mode is enabled, malicious files uploaded using HTTP or HTTPS will be intercepted. However, files uploaded using SFTP will not be intercepted. SFTP is a non-HTTP or HTTPS protocol, and WAF protection does not cover files uploaded using SFTP.

Which Non-Standard Ports Does WAF Support?

Protocol Name	Port
HTTP protocol	80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 97, 800, 805, 808, 1000, 1090, 2020, 3333, 3501, 3601, 5000, 5222, 6001, 6666, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7007, 7008, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7040, 7070, 7081, 7082, 7083, 7088 7097, 7510, 7621, 7777, 7800, 8000, 8002, 8003, 8004, 8005, 8006, 8007, 8008, 8009, 8010, 8011, 8012, 8020, 8021 8022, 8060, 8025, 8026, 8060, 8077, 8078, 8080, 8081, 8082, 8083, 8086, 8087, 8088, 8089, 8090, 8106, 8181, 8182, 8184, 8210, 8215, 8334, 8336, 8445, 8686, 8800, 8888, 8889, 8999, 9000, 9001, 9002, 9003, 9021, 9023, 9027, 9037, 9080, 9081, 9082, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211 9212, 9213, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9999, 10000, 10001, 10080, 10083, 12601, 20080, 20083, 25060, 28080, 28080, 33702, 48800, and 52301.
HTTPS protocol	443, 4443, 5100, 5200, 5443, 6443, 7443, 8084, 8085, 8091, 8442, 8443, 8553, 8663, 9443, 9550, 9553, 9663, 10803, and 18980.