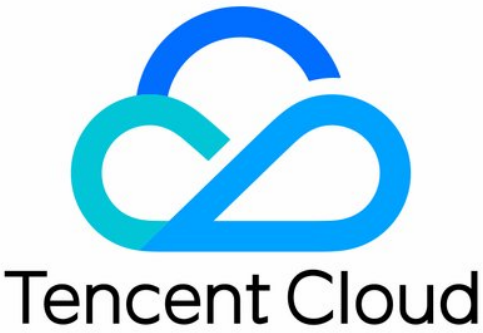
Web Application Firewall

Operation Guide

Product Documentation



©2013-2022 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Operation Guide
- Overview
- SaaS WAF Connection
  - Step 1. Add a Domain Name
  - Step 2. Perform Local Testing
  - Step 3. Modify DNS Resolution
  - Step 4. Configure a Security Group
  - Step 5. Verify the Configuration
- CLB WAF Connection
  - Step 1. Confirm CLB Configuration
  - Step 2. Bind Domain Name to CLB Instance
  - Step 3: Verify the configuration
- Asset Center
  - Instance Management
  - Domain Name List
  - Advanced Connection Feature
  - API Asset Management
- Basic Security Configurations
  - Rule Engine
  - IP Blocking Penalty
  - Access Control
  - Region Blocking
  - CC Protection Rule Settings
  - Web Tamper Protection
  - Data Leakage Protection
  - API Security
- Bot and Application Security
  - Bot Settings
    - Bot Management
      - Overview
      - Rule Overview
      - Advanced
      - Client Risk Identification
      - Bot Analytics
        - AI Policies

©2013-2022 Tencent Cloud. All rights reserved.

Threat Intelligence Module
Bot Flow Statistics Module
Action Settings
Bot Traffic Analysis
Bot Traffic Details
Blocklist/Allowlist Protection Settings
Features
IP Blocklist
IP Allowlist
Precise Allowlist Management
Rule Allowlist
Traffic Inspection
Statistics and Logs
Attack Logs
Access Logs
Log Shipping
IP Query

©2013-2022 Tencent Cloud. All rights reserved.

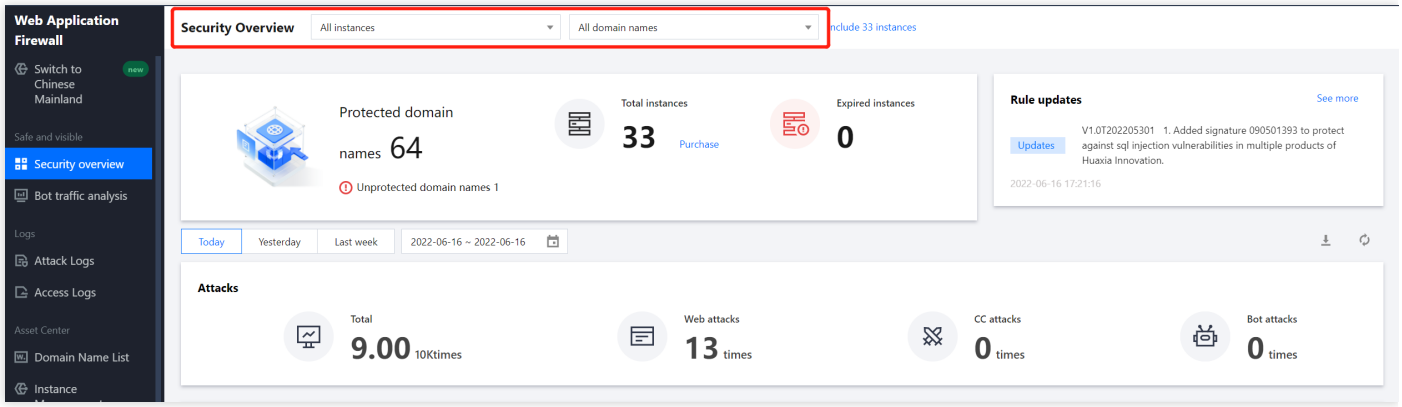
Operation Guide
Overview

Last updated：2022-06-24 10:42:43

The Overview page allows you to get an overall picture of the security status of your domain name.

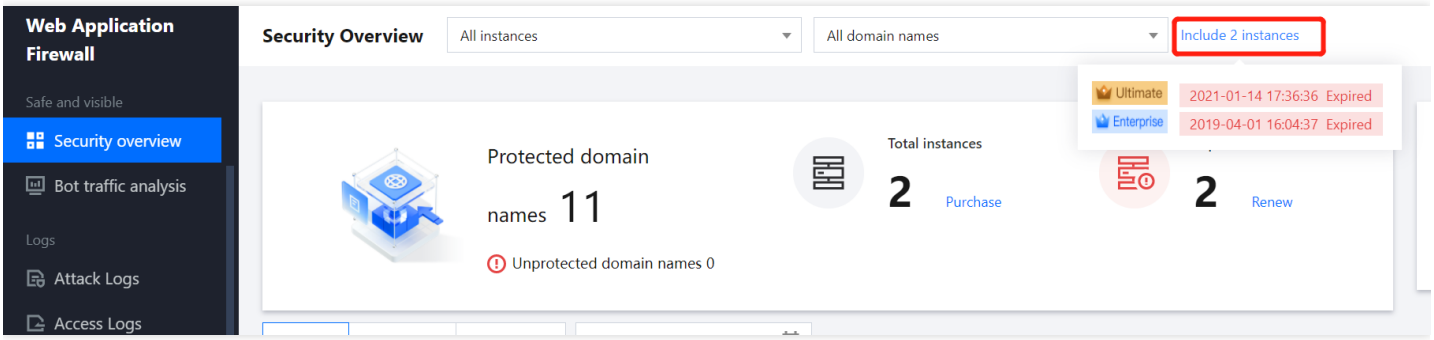
Security Overview

1. Log in to the WAF console and select **Overview** on the left sidebar. Then open the **Security Overview** tab.
2. Select a domain name to view data that measures the security status of the domain name.



Instance Overview

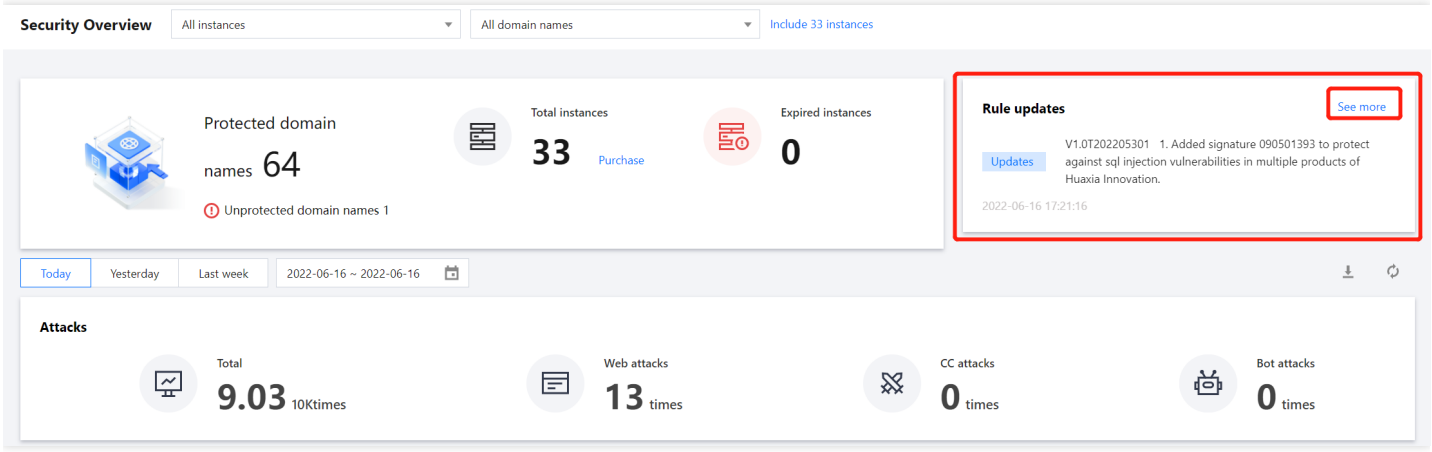
To view expired instances under your account, select a domain name and click **Include x instances**.



©2013-2022 Tencent Cloud. All rights reserved.

Rule Updates

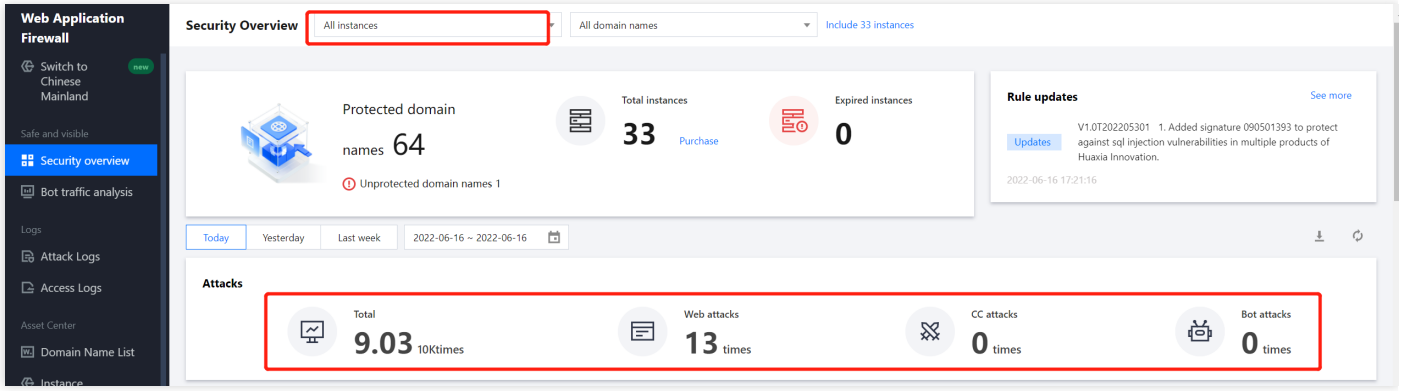
By clicking **See more** in the rule updates section, you can view WAF supported rules in detail.



Attacks Overview

All domain names

1. When "All domain names" is selected, all attack data are displayed. You can also set a time range to display data you want to see.



2. At the lower part of the page, you can view the following information including top 5 domain names by web attacks, top 5 attacker IPs, and top 5 domain names by CC attacks.

©2013-2022 Tencent Cloud. All rights reserved.

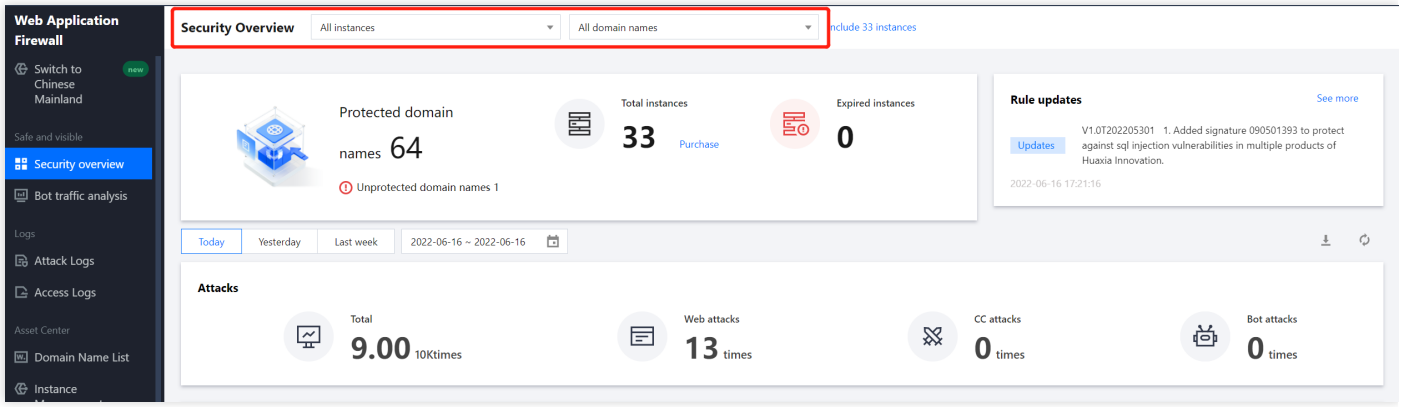
Field description:

- Top 5 domain names by web attacks: It displays five domain names that suffer web attacks most frequently.
- Top 5 attacker IPs: It displays five IPs that initiate attacks most frequently.
- Top 5 domain names by CC attacks: It displays five domain names that suffer CC attacks most frequently.
- Top 5 requester IPs: It displays five IPs that send access requests most frequently.
- Distribution of attacker IPs: It displays how the attacker IPs distribute across regions.
- Types of attacks (%): It displays the distribution of the attack types.
- Types of browsers (%): It displays the distribution of the browser types.

Single domain name

1. When a specific domain name is selected, the corresponding attack data is displayed. You can also set a time range to display data you want to see.

©2013-2022 Tencent Cloud. All rights reserved.



2. At the lower part of the page, you can view the following information including top 5 attacker IPs, top 5 requester IPs and distribution of attacker IPs.

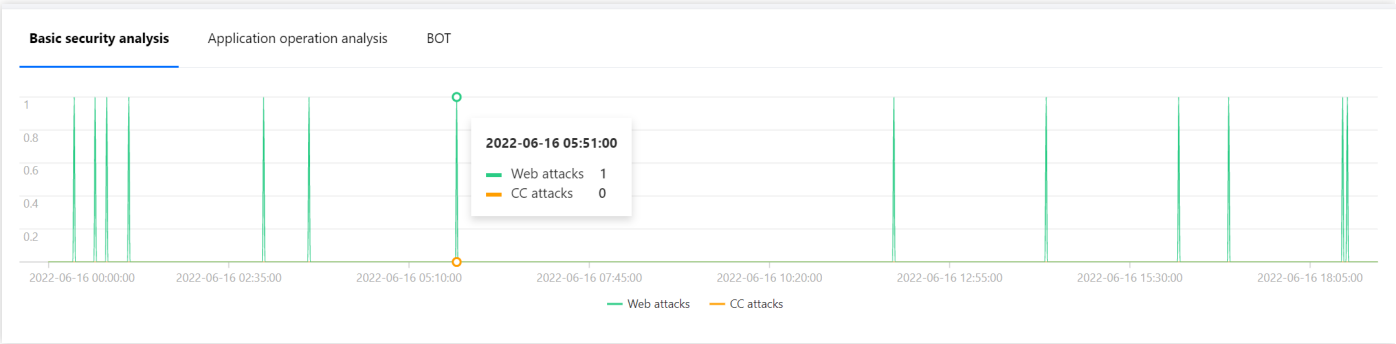
Field description:

- Top 5 attacker IPs: It displays five IPs that initiate attacks most frequently.
- Top 5 requester IPs: It displays five IPs that send access requests most frequently.
- Distribution of attacker IPs: It displays how the attacker IPs distribute across regions.
- Types of attacks (%): It displays the distribution of the attack types.
- Types of browsers (%): It displays the distribution of the browser types.

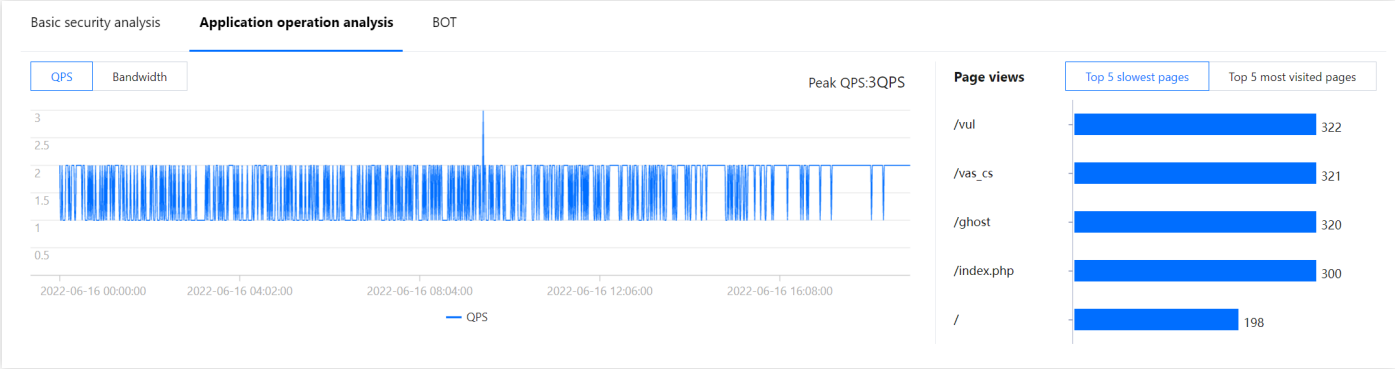
Overview of Security Analysis

©2013-2022 Tencent Cloud. All rights reserved.

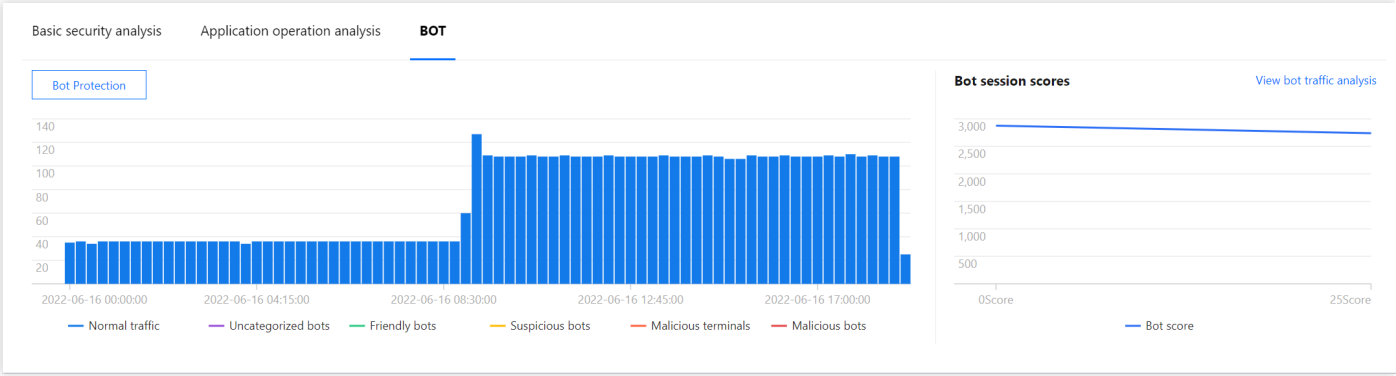
- Basic security analysis: It displays the number of web attacks on the selected domain name during the specified period.



- Application operation analysis: It displays the QPS and bandwidth of the selected domain name on the left, and top 5 slowest pages and top 5 most visited pages on the right.



- Application security analysis: It displays the bot information of the selected domain name during the specified period. To view more details, you can click View bot traffic analysis.



©2013-2022 Tencent Cloud. All rights reserved.

SaaS WAF Connection
Step 1. Add a Domain Name

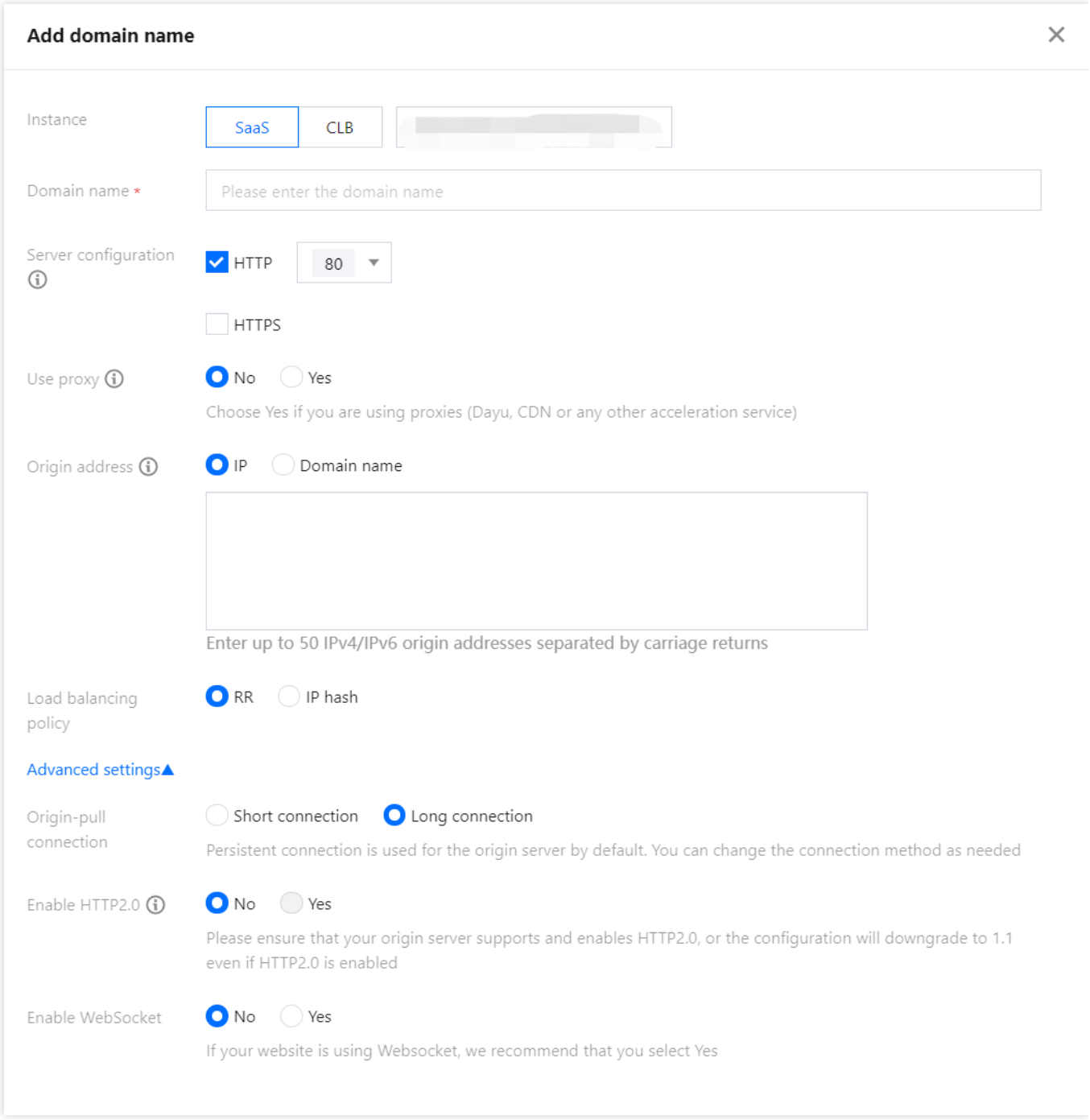
Last updated：2023-12-29 14:22:37

This document describes how to connect a domain name to SaaS WAF. Before using WAF to protect your web business, you need to connect the website to WAF; otherwise, WAF protection cannot take effect.

Directions

1. Log in to the WAF console and select **Asset Center** > **Domain Name List** on the left sidebar.
2. Click **Add domain name**.
3. On the page that appears, configure the basic parameters.

©2013-2022 Tencent Cloud. All rights reserved.



Field description

Instance: Select **SaaS** and the target instance on the right.

Domain name: Enter the domain name to be protected, such as `saas.technicalsupport.cn` .

Server configuration: Select a protocol and port as needed. For more port options, see Port Access.

Select the **HTTP** protocol and enter a port.

Select the **HTTPS** protocol and enter a port. Then, you need to configure the associated certificate, forced HTTPS redirection, and HTTPS forwarding method.

Associate certificate: Click **Associate certificate** and select a Tencent Cloud-managed or external certificate as needed.

©2013-2022 Tencent Cloud. All rights reserved.

Force HTTP redirect: To enable forced HTTPS redirect, you need to select both HTTP and HTTPS access protocols.
HTTPS origin-pull method: Select an origin-pull method as needed: HTTP or HTTPS.

Note

For HTTP as an origin-pull method, you can specify a port for origin-pull. For HTTPS, the open port is also used for origin-pull.

Proxy: Select whether proxy services including Anti-DDoS and CDN are used based on the actual conditions.

Note

If you select **Yes**, WAF will get real client IPs, which may be forged, from the XFF field as the source IPs.

Origin address: Enter the IP or domain name as needed.

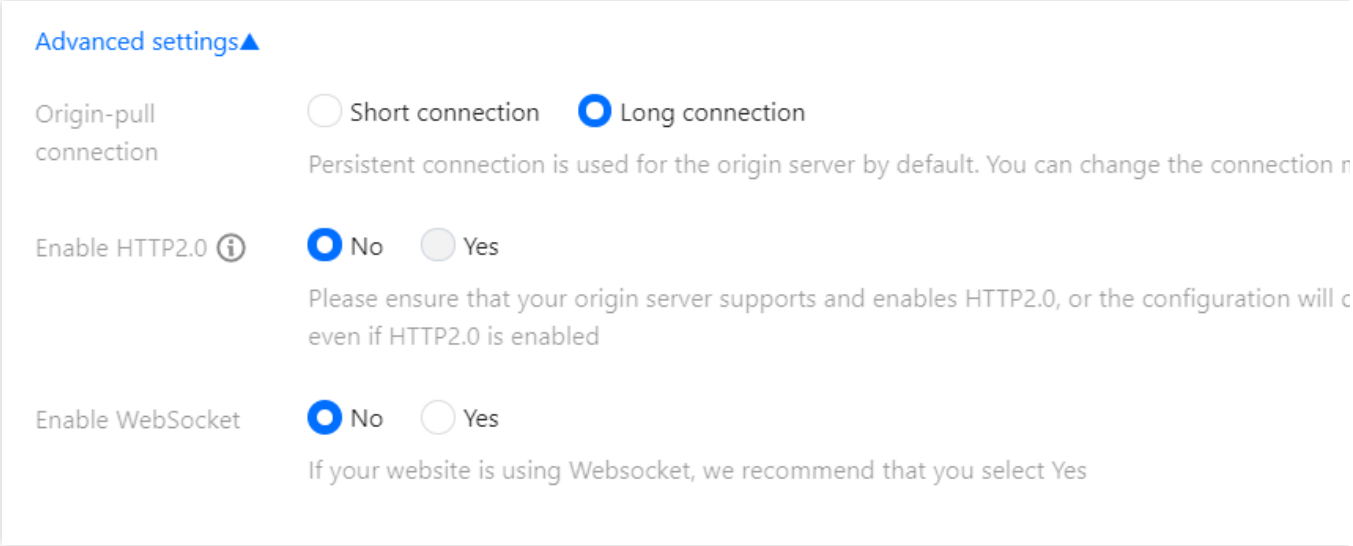
IP: Enter up to 20 IPv4 or IPv6 addresses and separate them with line breaks.

Domain name: Enter the origin domain name. Note that it must be different from the protected domain name.

Weighted round robin: Use this method when you set multiple origin server IPs for forwarding.

Load balancing policy: Select RR (default option) or IP hash as needed

4. After configuring the basic parameters, you can configure advanced parameters as needed. Click **OK** to save the settings.



Field description

Connection method: Persistent connection is used for forwarding by default. Make sure that the origin server supports persistent connection; otherwise, even if persistent connection is selected, non-persistent connection will still be used.

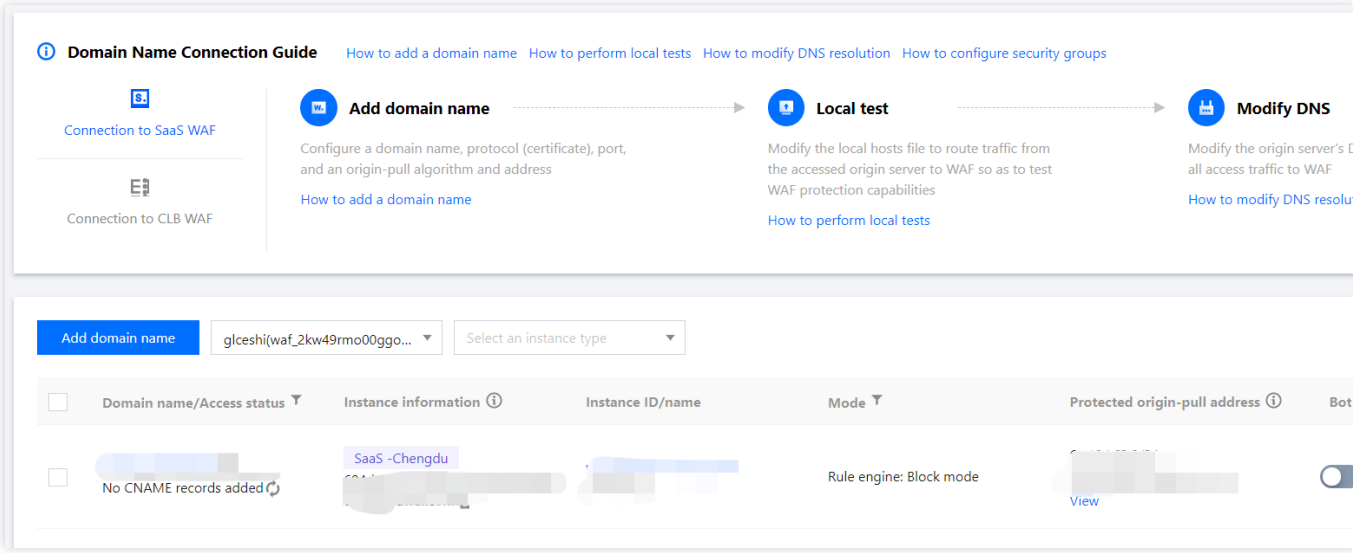
Enable HTTP 2.0: Make sure that your origin server supports HTTP 2.0 and enable it; otherwise, even if HTTP 2.0 is enabled, it will be downgraded to 1.1.

Enable WebSocket: If your website uses WebSocket, we recommend you select **Yes**.

Enable Health check: The enterprise version and the above versions support the opening of the four-layer health check mechanism based on the return IP.

©2013-2022 Tencent Cloud. All rights reserved.

5. After the configuration, you can see the newly added domain name in the domain name list. The current page prompts that you haven't configured a CNAME record. You need to perform local testing and then modify DNS resolution.



Note

WAF assigns a unique CNAME to each domain name added to WAF regardless of whether it is top-level or second-level.

Subsequent Operations

After adding a domain name, you can proceed to the following steps:

Step 2. Perform Local Testing

Step 3. Modify DNS Resolution

Step 4. Set a Security Group

©2013-2022 Tencent Cloud. All rights reserved.

Step 2. Perform Local Testing

Last updated：2023-12-29 14:23:09

This document describes how to perform local testing before modifying DNS records to ensure the service availability.

Directions

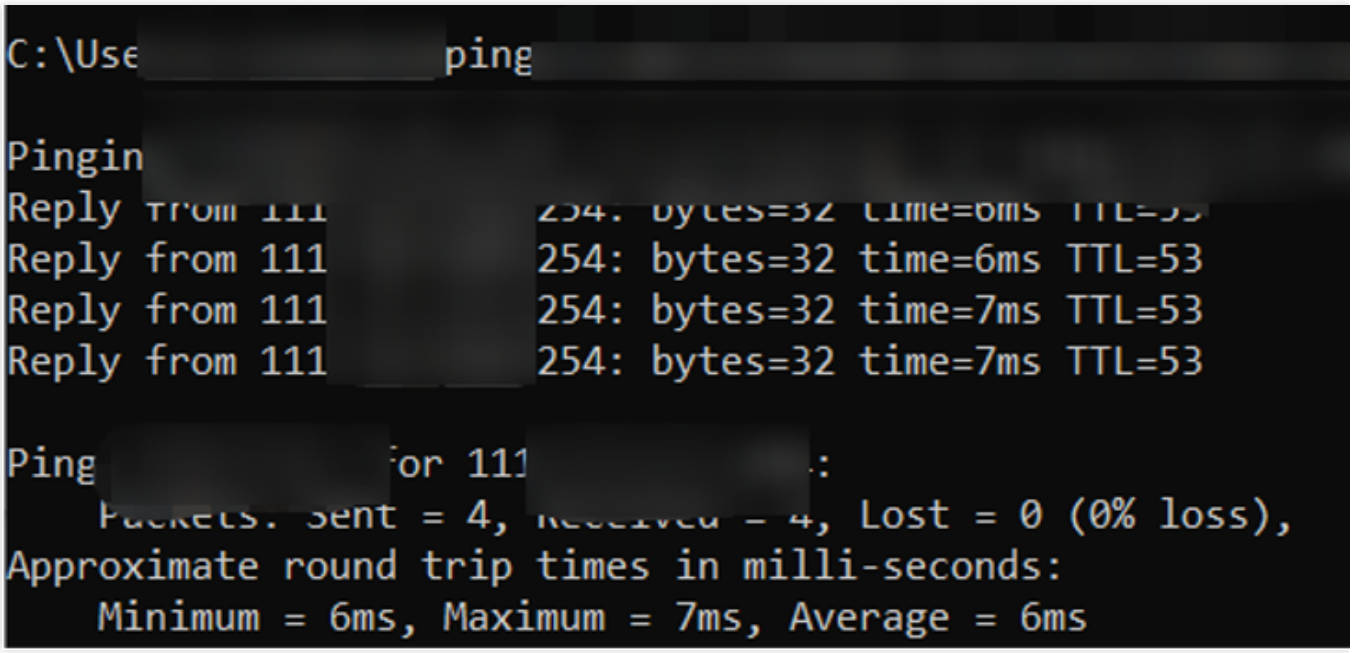
DNS resolution is required when a local server accesses a website. Before DNS resolution, the IP address of the destination domain name will be obtained from the local `hosts` file. Therefore, you can modify the `hosts` file to direct local access traffic to WAF to test the connectivity between the website and WAF. This avoids direct modification of DNS records that may affect Internet users' access to the website.

1. Log in to the WAF console, select **Asset Center** > **Domain Name List** on the left sidebar. You can check the CNAME address of `saas.technicalsupport.cn` .

If you need to get the VIP address of the corresponding domain name, you can get it by pinging the CNAME address.

i. In Windows, open Command Prompt.

ii. Run the command: `ping <WAF CNAME address>` .



iii. The ping command output will record the WAF IP address of the domain name, which is required for subsequent

©2013-2022 Tencent Cloud. All rights reserved.

operations.

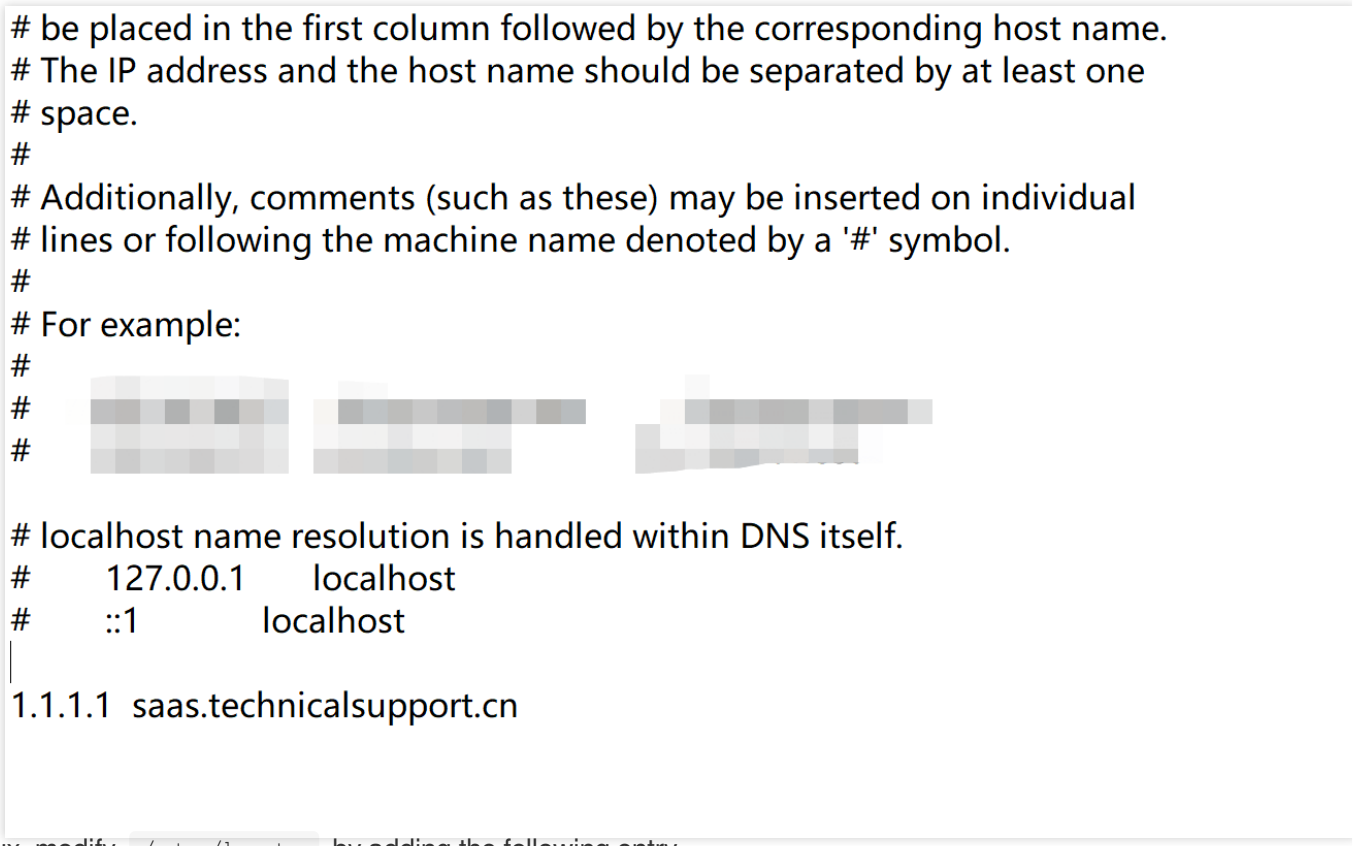
2. Modify `hosts` file.

In Windows, modify `C:\\Windows\\System32\\drivers\\etc\\hosts` by adding the following entry.

Format: VIP address + Domain name added to WAF

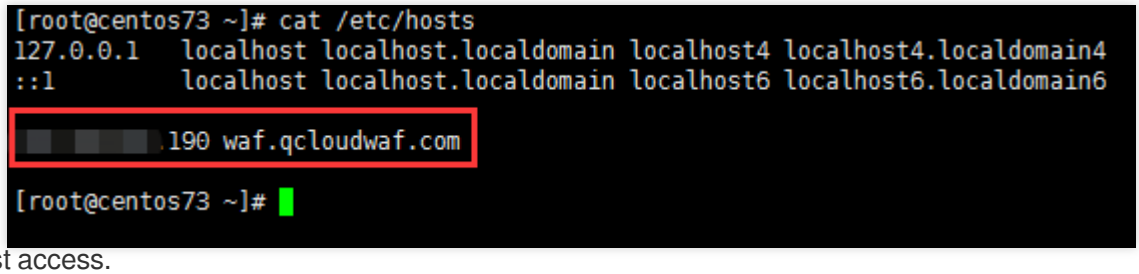
Note:

Here, `1.1.1.1` is a test address, and it should be the VIP address in actual use.



In Linux, modify `/etc/hosts` by adding the following entry.

Format: VIP address + Domain name added to WAF

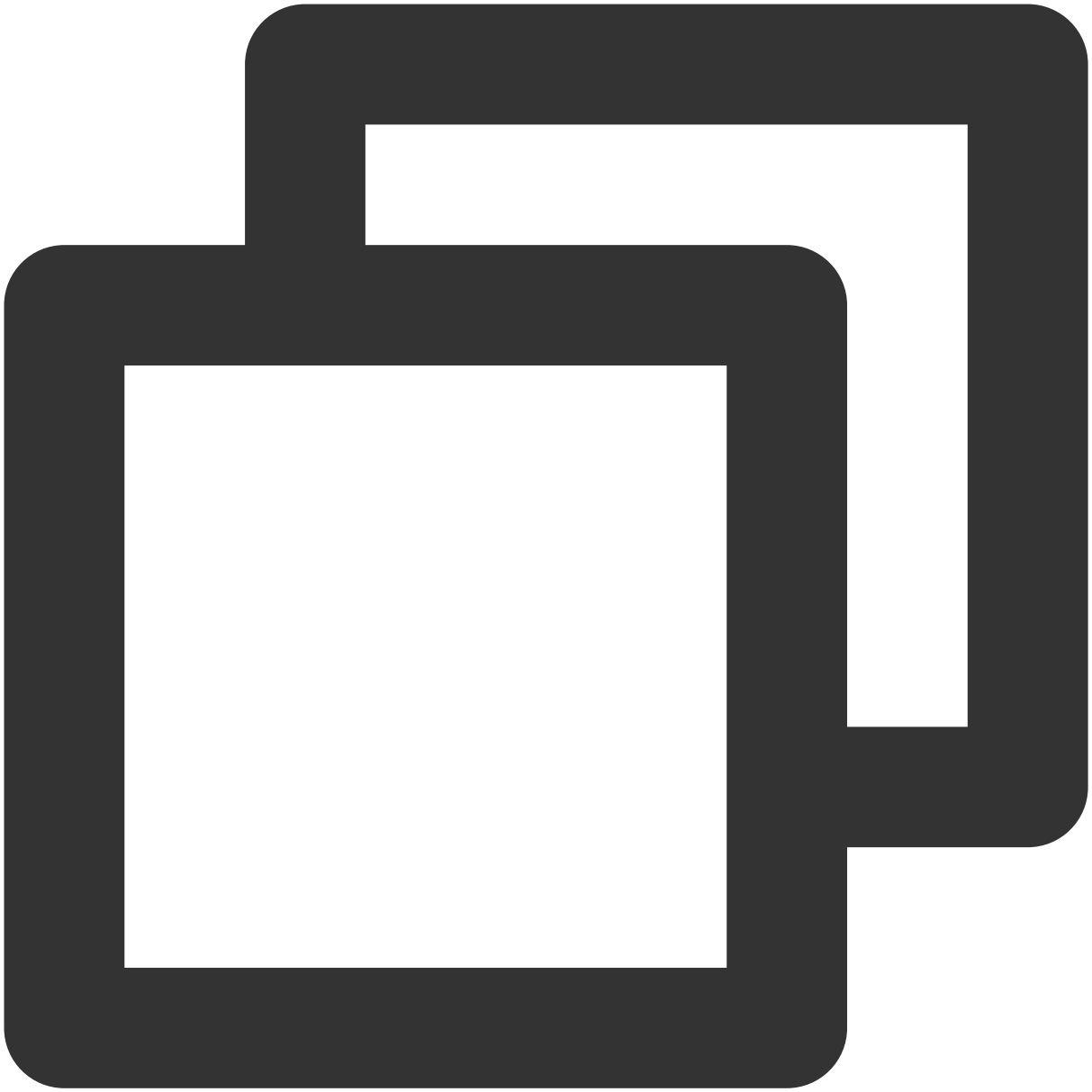


3. Test access.

Access the website from your local computer. If the website can be opened properly, the connectivity between the origin server and WAF is normal.

i. Enter the following URL in your browser to access:

©2013-2022 Tencent Cloud. All rights reserved.



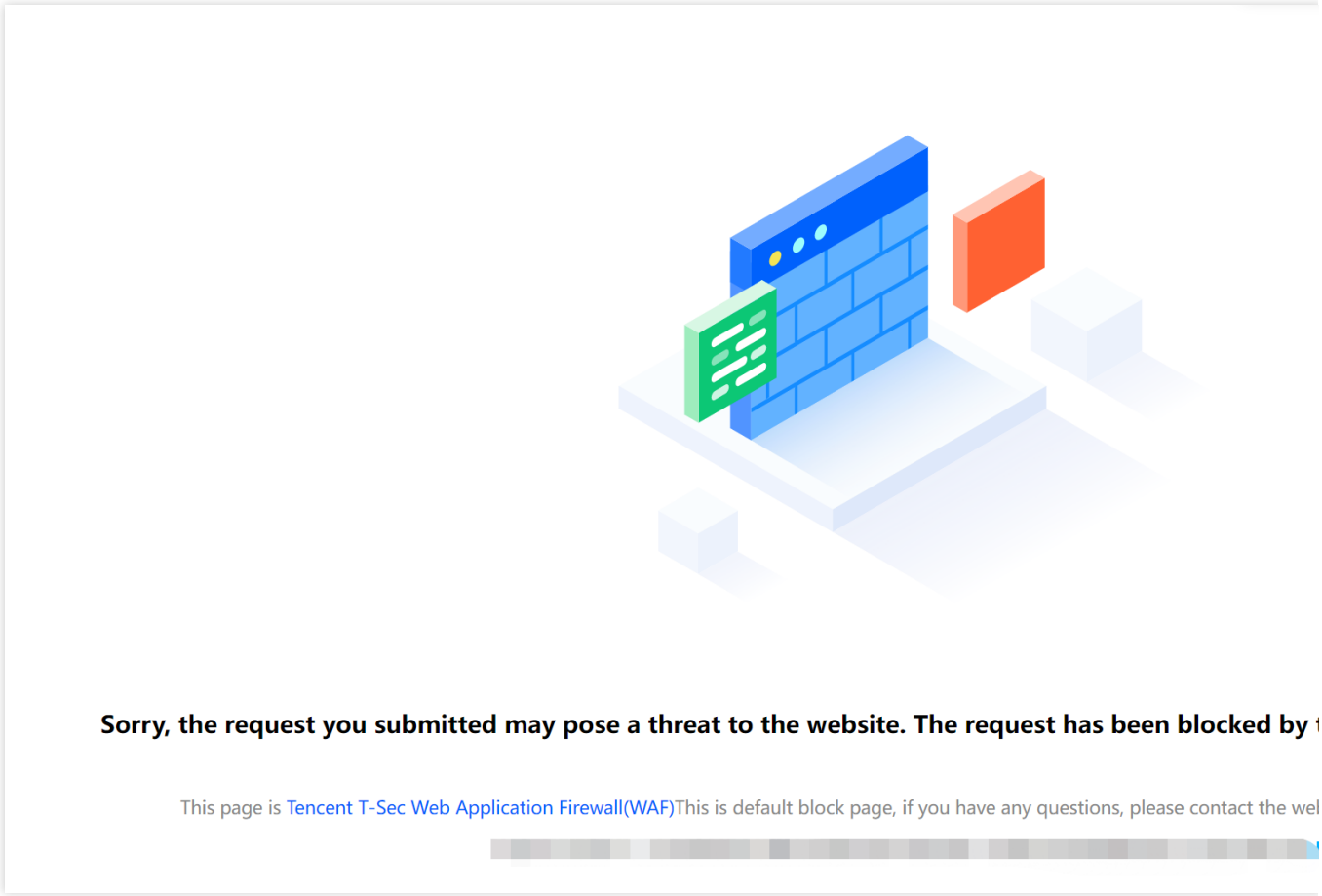
```
http:// saas.technicalsupport.cn/?test=alert(123)
```

ii. If the browser returns a block page, the WAF is working properly.

Note:

To view the block page, you can access the default WAF prompt.

©2013-2022 Tencent Cloud. All rights reserved.



Subsequent Operations

After performing the local test, you can proceed as follows:

Step 3. Modify DNS Resolution

Step 4. Set a Security Group

©2013-2022 Tencent Cloud. All rights reserved.

Step 3. Modify DNS Resolution

Last updated：2023-12-29 14:23:24

This document will guide you how to modify the DNS resolution record, so that WAF can protect the traffic generated when public network users access your website.

Directions

To protect the public network traffic to websites with WAF, you need to modify the DNS resolution record. The following uses `waf.qcloudwaf.com` as an example to describe how to modify its DNS resolution record on Tencent Cloud DNSPod.

1. Log in to the DNSPod console, click **My Domain** on the left sidebar, and then click **Resolve** on the right of the domain name `.technicalsupport.cn` to be accessed to WAF.
2. Click **Add Record**.
3. Enter the information required on the configuration page.
Enter the host record of the website in the "Host Record". In this example, `saas.technicalsupport.cn` is added to WAF, so the host record is `saas` .
Select "CNAME" as the record type.
Enter the CNAME domain name assigned by WAF for the record value. In this example, the CNAME domain name format is `xxxx.qcloudcjgj.com` .
Click **Save** after filling in all the information.
4. When the modification is complete, DNS records will take effect and WAF will protect traffic accessing the website. Meanwhile, WAF will display **Normal Protection** on the console after detecting that the resolution of the protected domain name is normal.

Note:

DNS records will take effect in about 10 minutes.

Subsequent Operations

After modifying your DNS resolution records, you can proceed to Step 4. Configure a Security Group.

©2013-2022 Tencent Cloud. All rights reserved.

Step 4. Configure a Security Group

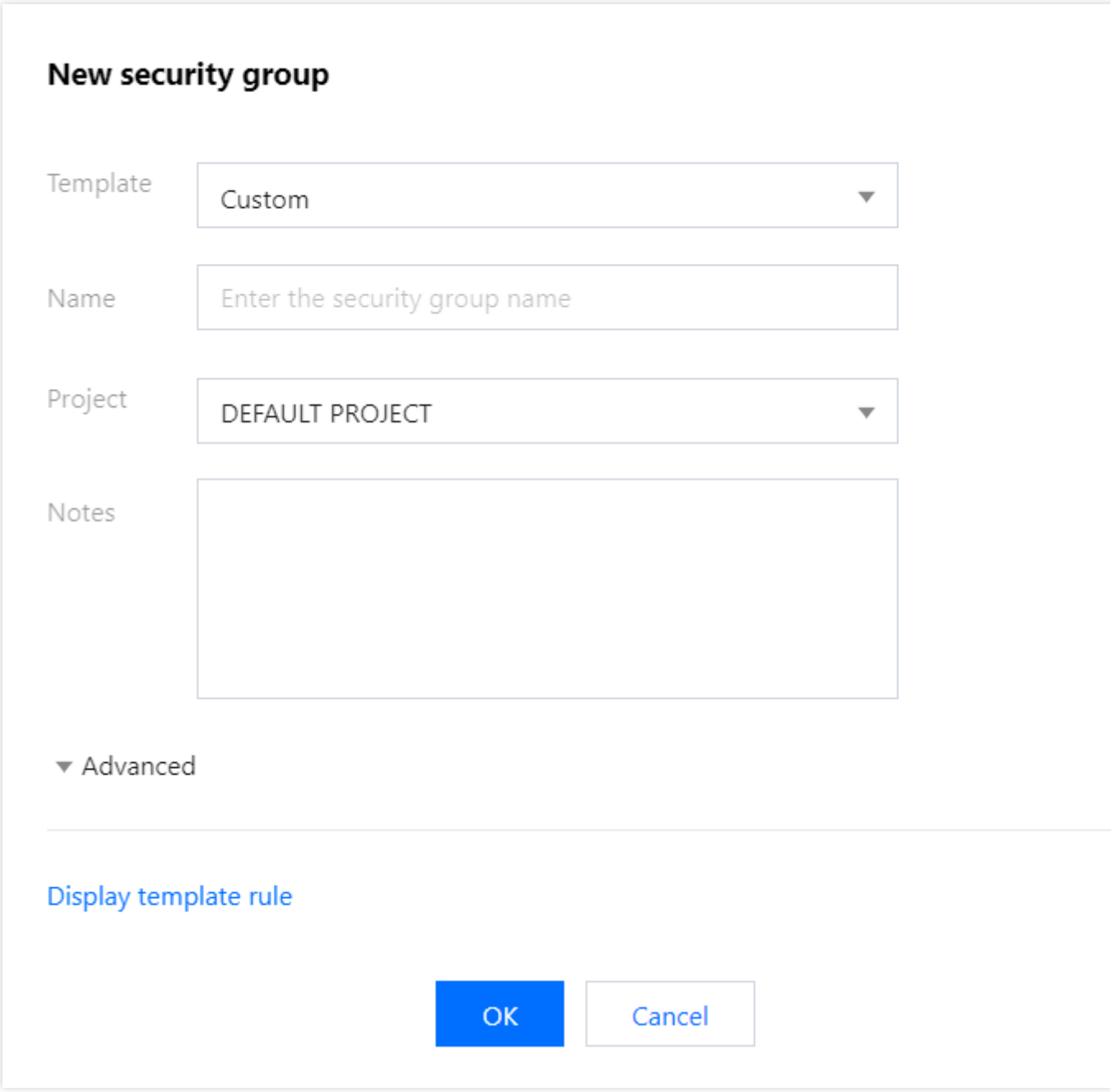
Last updated：2023-12-29 14:23:51

This document will guide you to set a security group and allow only traffic from WAF to access websites.

Directions

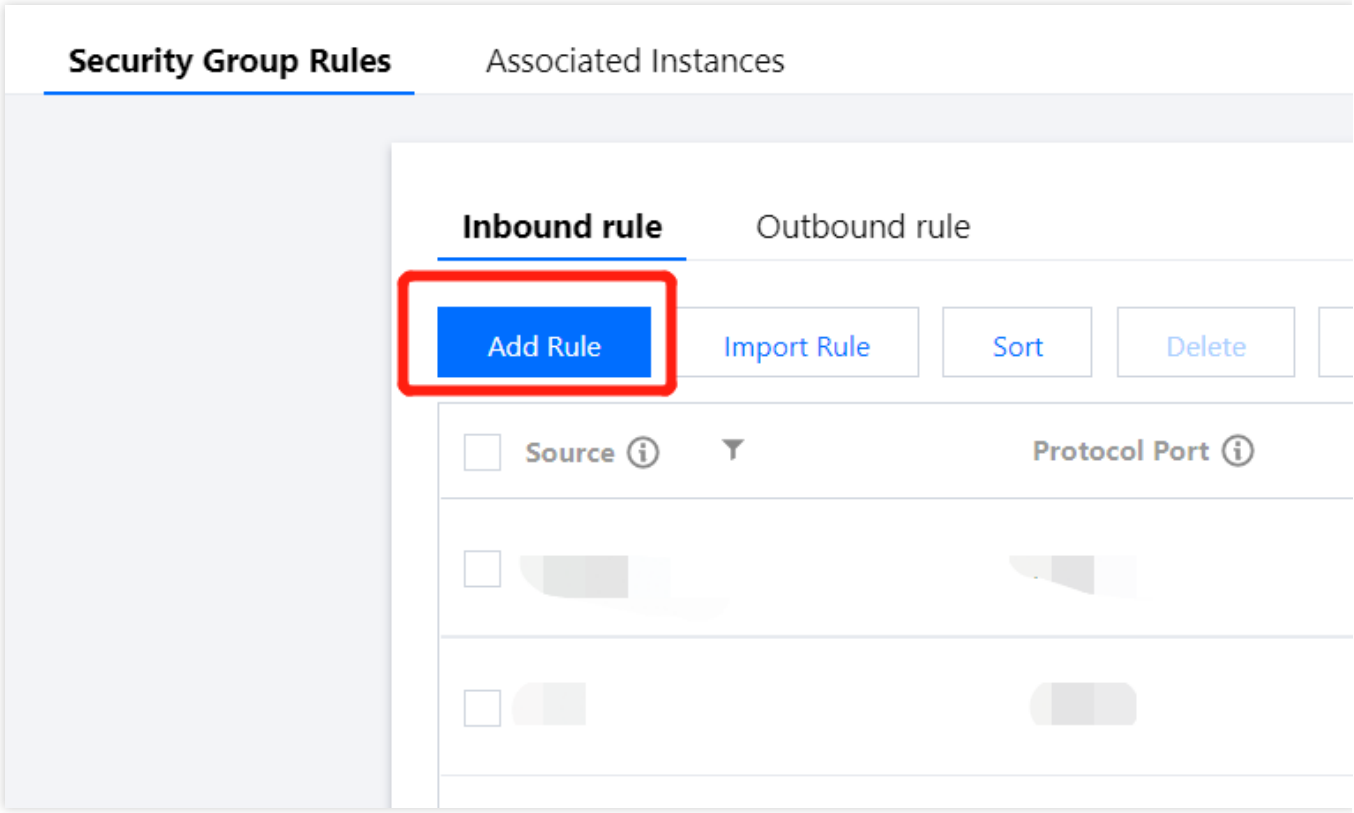
Security group is an instance-level firewall service provided by Tencent Cloud to control inbound and outbound traffic of CVM instances. You can configure a security group to allow only traffic from WAF to access your website, preventing attackers from bypassing WAF and directly attacking your origin server.
The following uses allowing the WAF intermediate IP `111.230.27.90` in the security group as an example to describe how to configure the security group.
Note:
The intermediate IP can be viewed at Domain Name List in the WAF console.
1. Log in to the CVM console and click **Security Group** on the left sidebar.
2. Click **Create**. On the pop-page, select **Custom** for the template, enter the security group name (such as `my-security-group`) and remarks, and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.

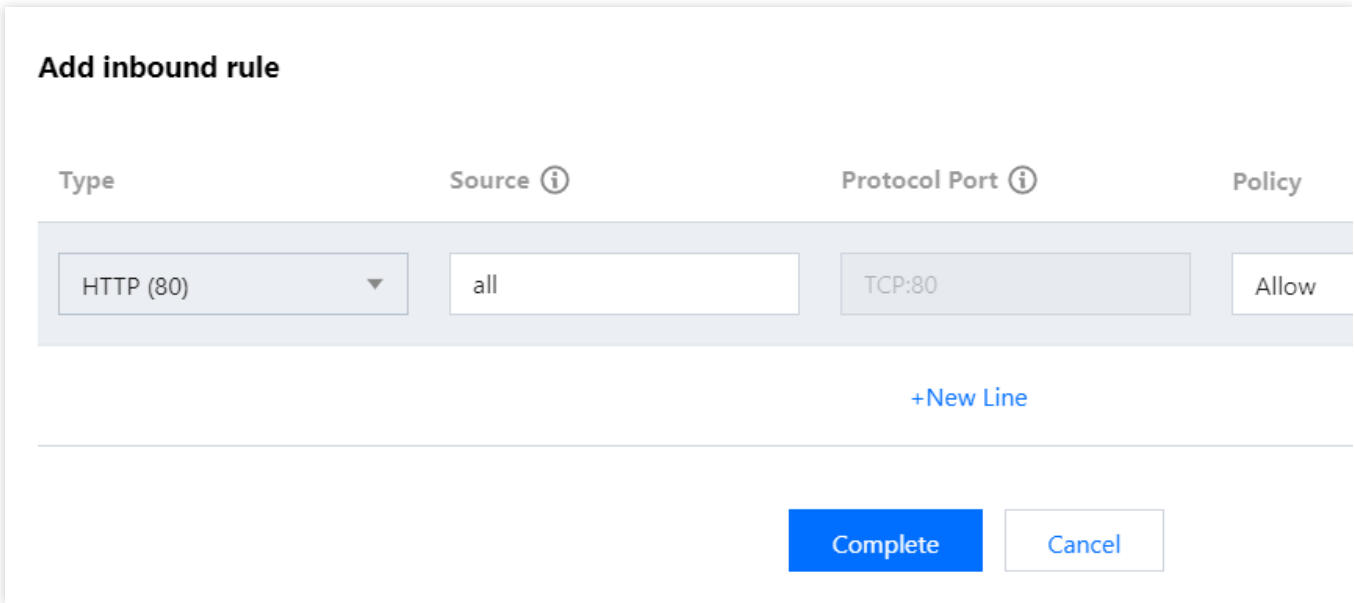


3. In the security group list, find the newly created security group, and click its ID to enter its details page.
4. On the inbound rule page, click **Add rule**.

©2013-2022 Tencent Cloud. All rights reserved.

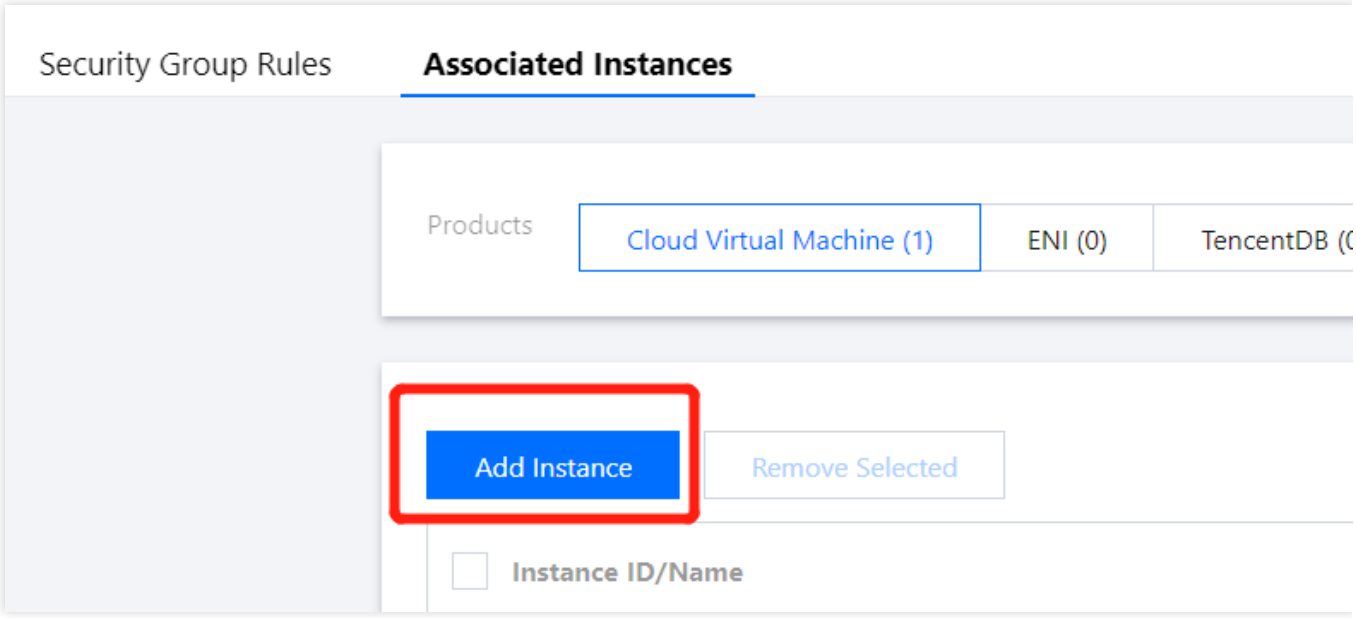


5. In the pop-up window, select "HTTP (80)" as the type, enter the intermediate IP that needs to be allowed for the source, and enter the port and policy as required. After completing the settings, click **OK**.



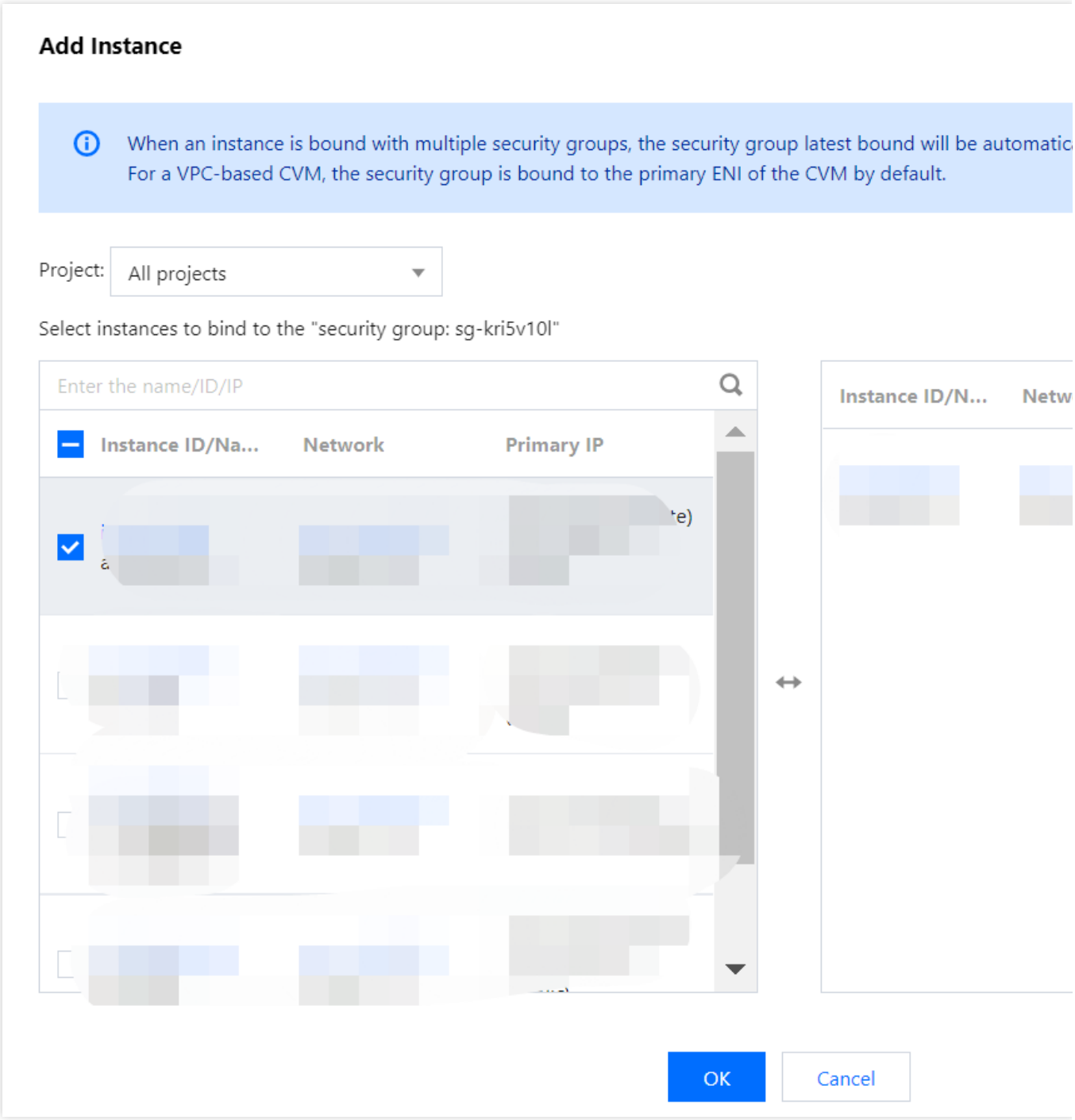
6. Click the **Associate Instance** tab and click **Add Instance** on the CVM page.

©2013-2022 Tencent Cloud. All rights reserved.



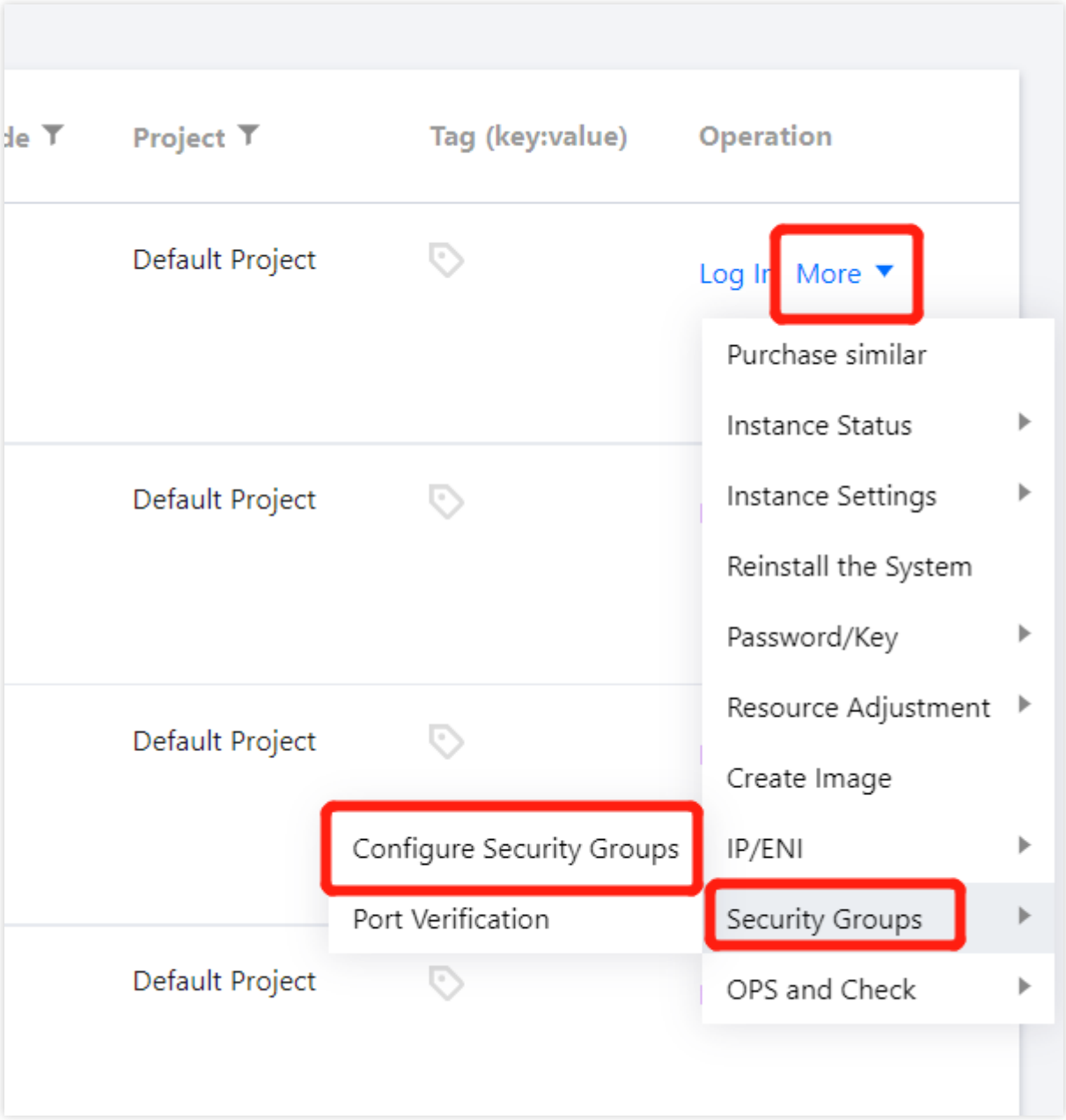
7. In the pop-up window, select the CVM instance to be bound to and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Alternatively, you can go to the CVM instance list page to view or modify the security group bound to a CVM instance. On the list page, select the ID of the CVM instance whose security group you want to adjust and click **More** > **Security Groups** > **Configure Security Groups** in the **Operation** column on the right for configuration.

©2013-2022 Tencent Cloud. All rights reserved.



©2013-2022 Tencent Cloud. All rights reserved.

Step 5. Verify the Configuration

Last updated：2023-12-29 14:25:24

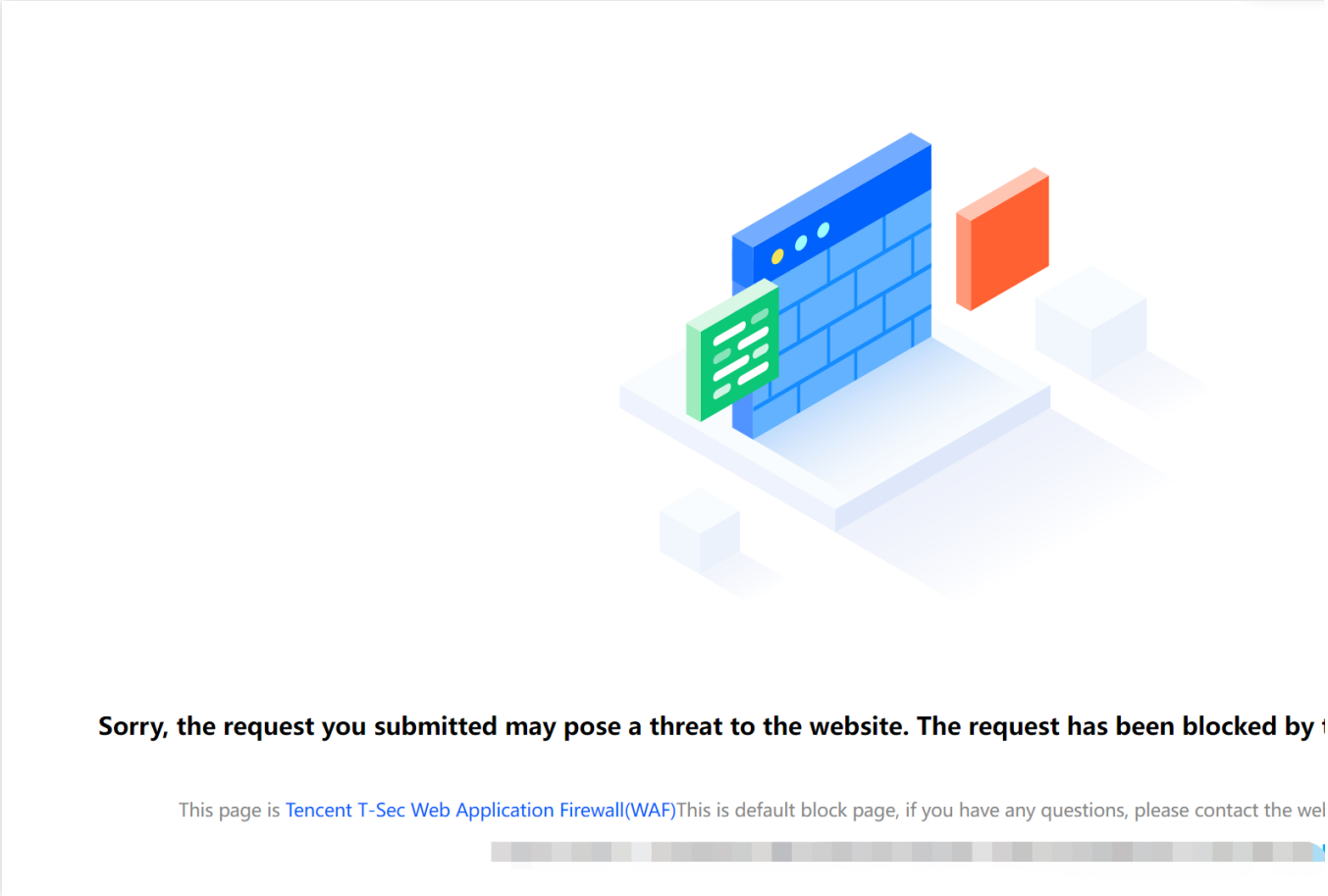
This document describes how to check whether the SaaS WAF is running.

Directions

1. Bind a WAF instance via a domain name and origin server to protect traffic. To verify whether the SaaS WAF is effective, make sure that your local computer can normally access to the domain names on your SaaS WAF instances.
2. Open `http:// saas.technicalsupport.cn/?test=alert(123)` in a browser. If a block page is displayed, WAF protection works properly.

Note:

Please replace `saas.technicalsupport.cn` with your actual domain name.



©2013-2022 Tencent Cloud. All rights reserved.

CLB WAF Connection
Step 1. Confirm CLB Configuration

Last updated：2023-12-29 14:25:46

This document describes how to confirm your CLB configuration prior to accessing CLB WAF.

Directions

By associating domain names with a CLB listener, CLB WAF checks and blocks HTTP or HTTPS traffic passing through the listener. Before accessing CLB WAF, make sure that your website business has been deployed on Tencent Cloud and used Tencent Cloud CLB (previously Application Load Balancer) over the public network.

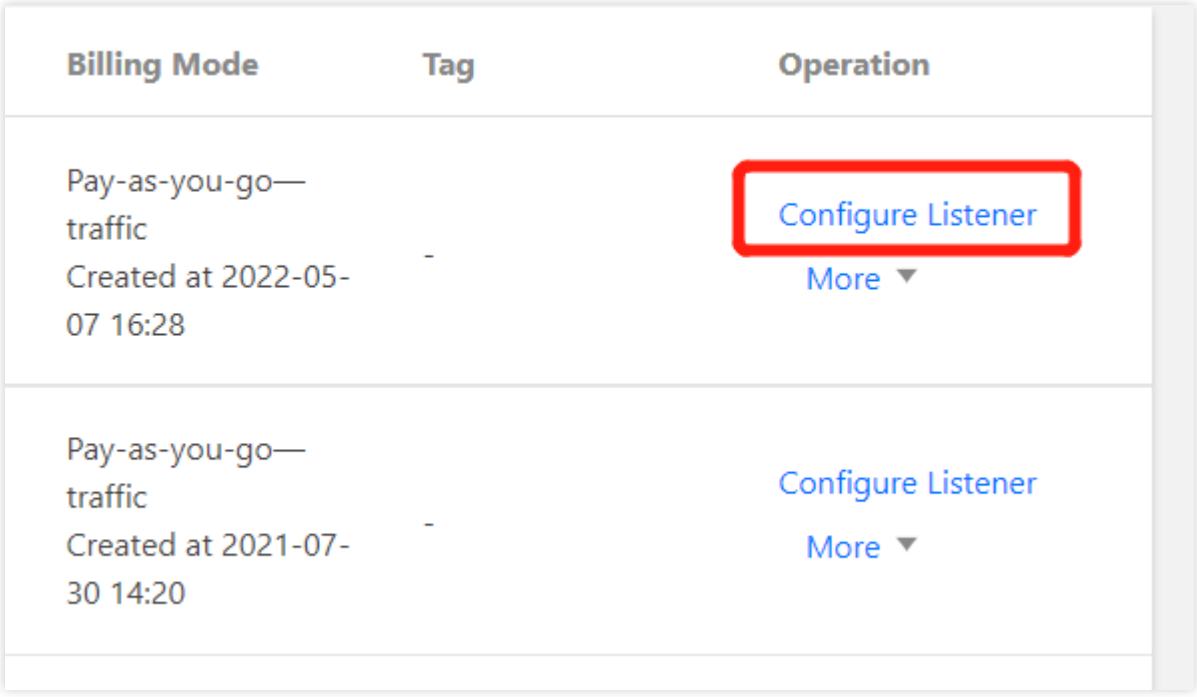
Note:

We recommend using SaaS WAF for website business not deployed on Tencent Cloud.

To ensure traffic forwarding, it is necessary to configure your CLB instance and associating your domain name with a listener. For more details, see Configuring an HTTP Listener and Configuring an HTTPS Listener.

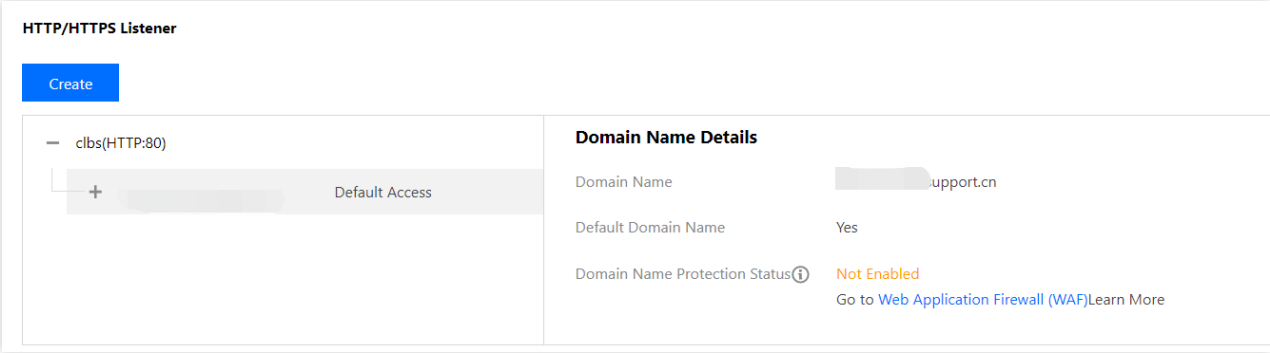
Perform the following steps to view the CLB listener configuration. `clb.technicalsupport.cn` is used as an example.

1. Log in to the CLB console, and click **Instance Management** on the left sidebar.
2. Select a region and CLB instance. Click **Configure listener** on the right.



©2013-2022 Tencent Cloud. All rights reserved.

3. On the page displayed, click **Listener Management** to view the listener configuration details. In this example, the listener name is `waftest`, and the domain name is `clb.technicalsupport.cn` and is in "Not Enabled" status.



Subsequent Operations

After confirming your CLB configuration, you can proceed to the following steps:

Step 2. Bind Domain Name to CLB Instance

Step 3. Verify the Configuration

©2013-2022 Tencent Cloud. All rights reserved.

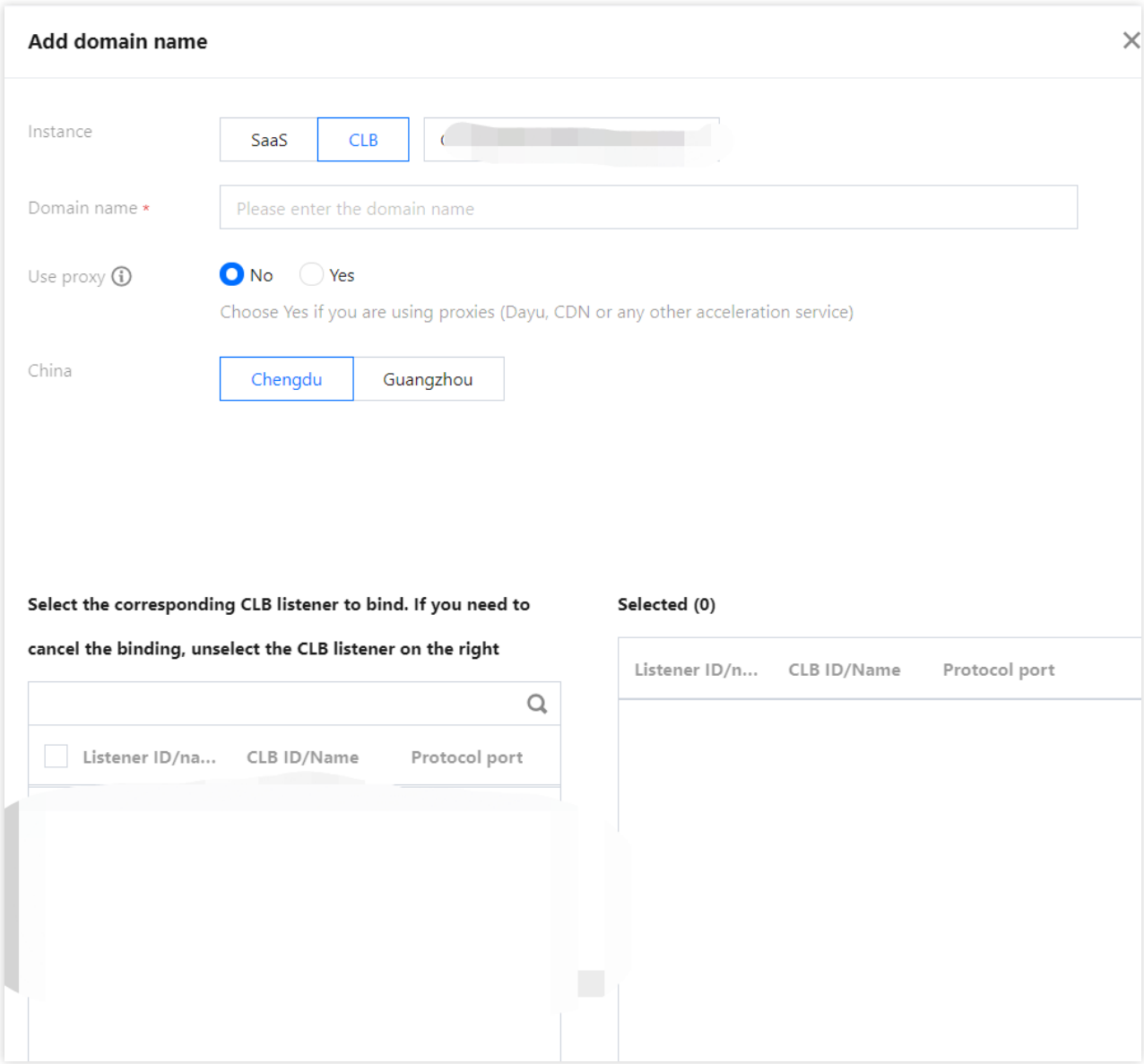
Step 2. Bind Domain Name to CLB Instance

Last updated：2023-12-29 14:26:03

This document describes how to bind a domain name to a CLB instance in the WAF console.

Directions

1. Log in to the WAF console and select **Asset Center** > **Domain Name List** on the left sidebar.
2. On the domain name list page, click **Add domain name**, configure relevant parameters, and click **OK**.



Field description

©2013-2022 Tencent Cloud. All rights reserved.

Instance: Select the CLB type and an instance name.

Domain name: Enter the domain name to be protected, such as `clb.technicalsupport.cn` .

Proxy: Select whether proxy services including Anti-DDoS and CDN are used based on the actual conditions.

Note:

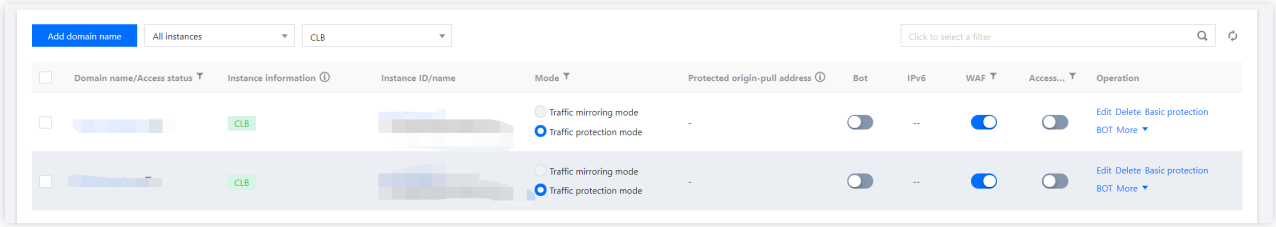
If you select **Yes**, WAF will get real client IPs, which may be forged, from the XFF field as the source IPs.

Chinese Mainland regions: Select as needed.

Global regions: Select as needed.

CLB listener: Select as needed.

3. Click **OK** to return to the domain name list, where you can view the protected domain name `clb.technicalsupport.cn` and the ID, name, VIP, and listener information of the CLB instance.



Subsequent Operations

After the domain name is bound to a CLB instance, you can proceed to Step 3. Verify the Configuration.

©2013-2022 Tencent Cloud. All rights reserved.

Step 3: Verify the configuration

Last updated：2023-12-29 14:26:17

This document describes how to check whether the CLB WAF is running.

Directions

1. By binding domain names to a CLB listener, WAF can protect traffic to the domain names passing through the CLB listener. To check whether the CLB WAF is running, ensure that your local computer can access the domain names added to different CLB instances.

Note:

To check whether the access to domain names added in CLB is normal for IPv4 domain name requests, see Getting Started with CLB. For IPv6 domain name requests, see Getting Started with IPv6 CLB.

2. Open `http://wow.qcloudwaf.com/?test=alert(123)` in a browser.

Note:

`wow.qcloudwaf.com` is a sample domain name. Please replace it with the actual domain name that has been added.

©2013-2022 Tencent Cloud. All rights reserved.

Sorry, the request you submitted may pose a threat to the website. The request has been blocked by t

This page is Tencent T-Sec Web Application Firewall(WAF)This is default block page, if you have any questions, please contact the wel

©2013-2022 Tencent Cloud. All rights reserved.

Asset Center
Instance Management

Last updated：2023-12-29 14:26:32

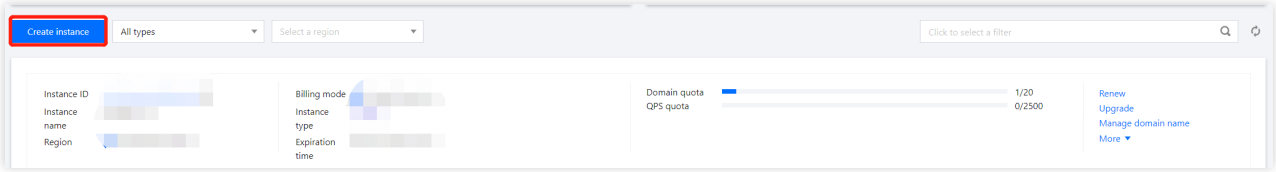
Scenarios

This document describes how to view instances, and purchase and renew instances and extra packs in the WAF console.

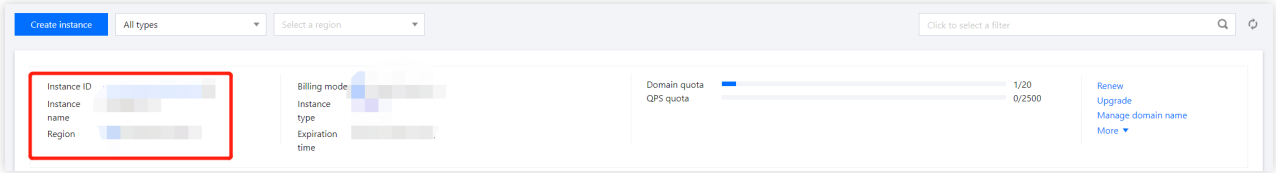
Directions

Creating and viewing instances

1. Log in to the WAF console and select **Asset Center** > **Instance Management** on the left sidebar.
2. On the page displayed, click **Create instance** to switch to the purchase page where you can purchase instances as needed. For more details, see Purchase Guide.



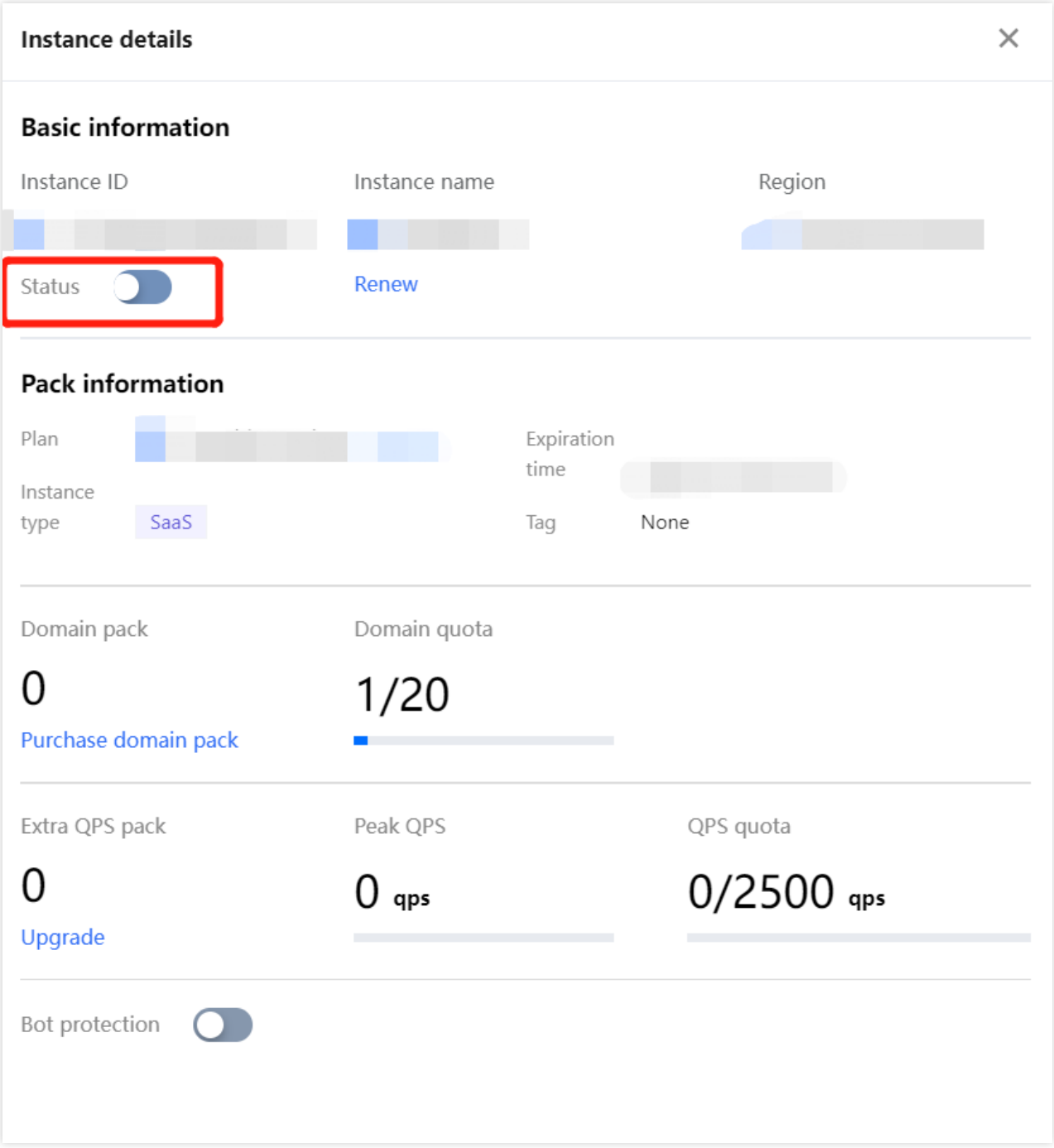
3. On the instant management page, select an instance you want to view and click its instance ID.



4. The details about the instance and the plan you purchase will be displayed. If you do not want to renew the plan, toggle off the switch

©2013-2022 Tencent Cloud. All rights reserved.

.



Searching existing instances

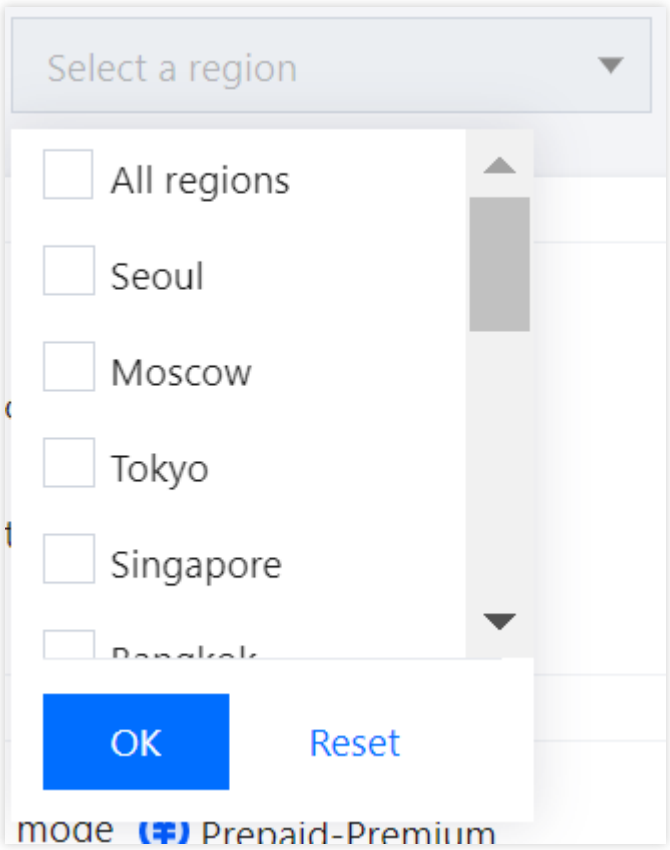
Searching WAF instances by region and instance type or keywords is supported.

1. Log in to the WAF console and select **Asset Center** > **Instance Management** on the left sidebar.

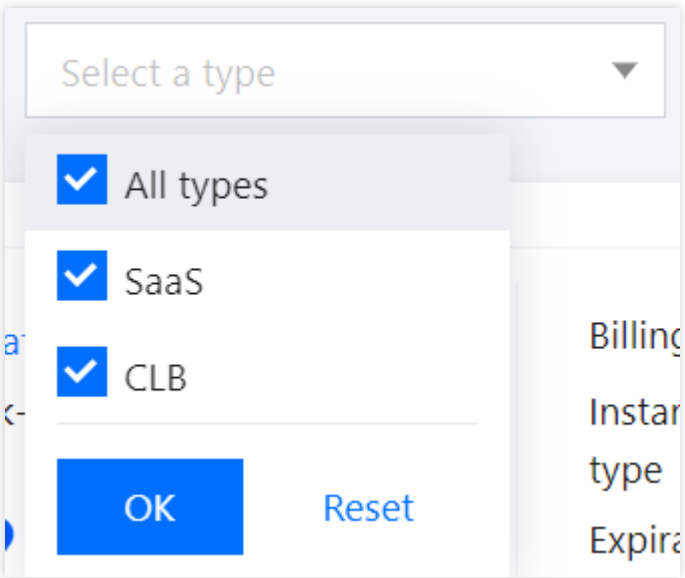
2. On the page displayed, you can search your WAF instances by region and instance type or keywords.

To filter WAF instances by instance type, you can click the drop-down list in the top left corner and select an instance type.

©2013-2022 Tencent Cloud. All rights reserved.

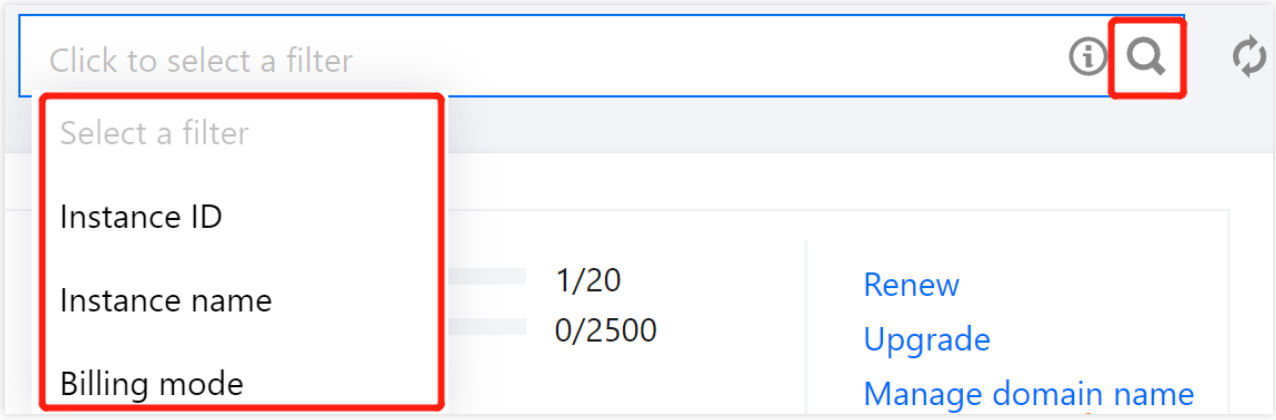


To filter WAF instances by region, you can click the drop-down list in the top left corner and select a region.



To search WAF instances by keywords, you can enter keywords in an instance ID, instance name or billing method.

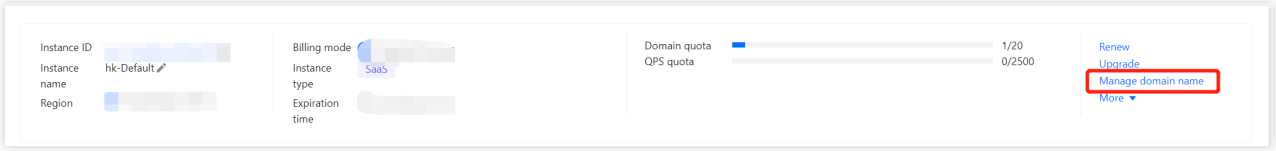
©2013-2022 Tencent Cloud. All rights reserved.



Managing domain names

After you find the instance you want to view, you need to configure domain names for the instance.

1. On the Instance management page, click **Manage domain name** to switch to the domain name list page.

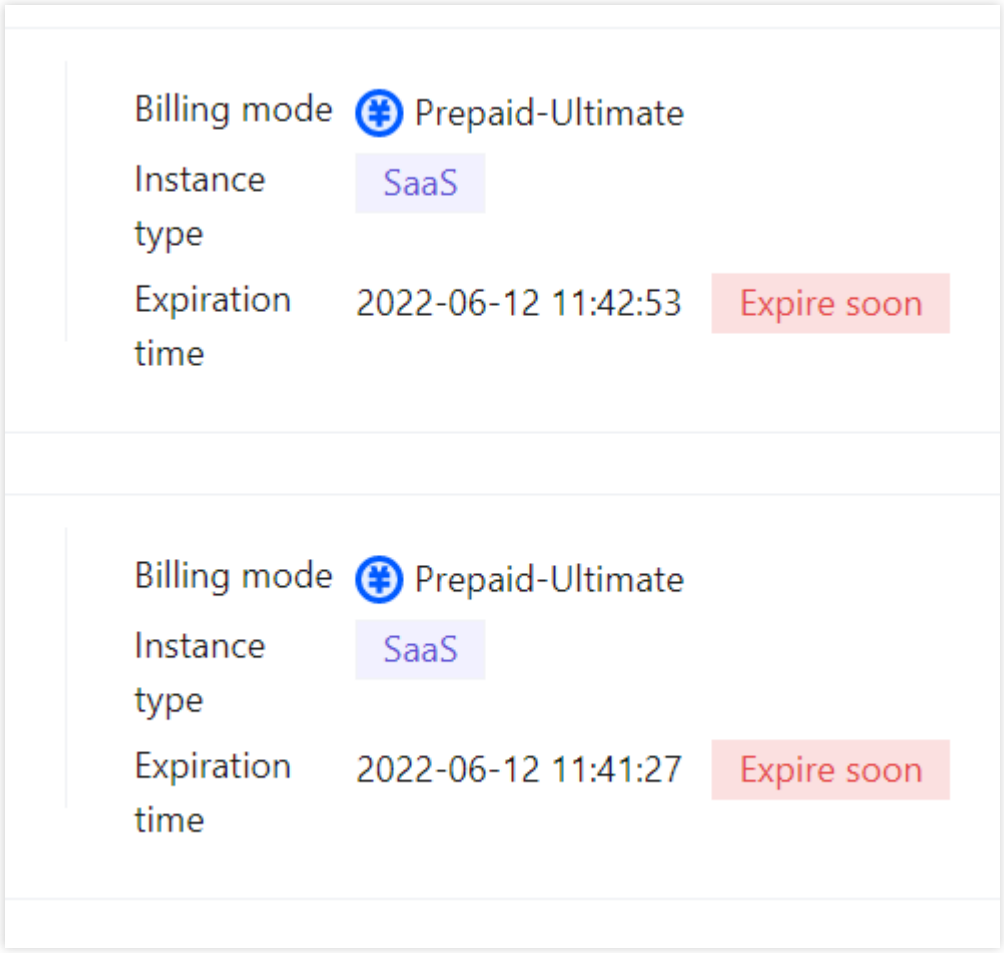


2. On the domain name list page, you can create, edit and delete a domain name. For more details, see Domain Name List.

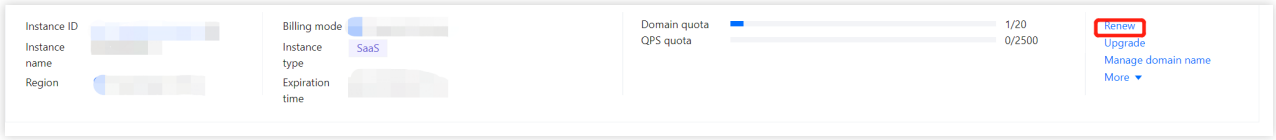
Renewing instances and purchasing extra packs

After you find the instance you want to view, you can check its plan expiration date and extra pack usage on the domain name list page.

©2013-2022 Tencent Cloud. All rights reserved.



1. If the plan is about to expire, you can click **Renew** to renew it as needed. On the pop-up renewal page, select a validity period before clicking **Renew now**.



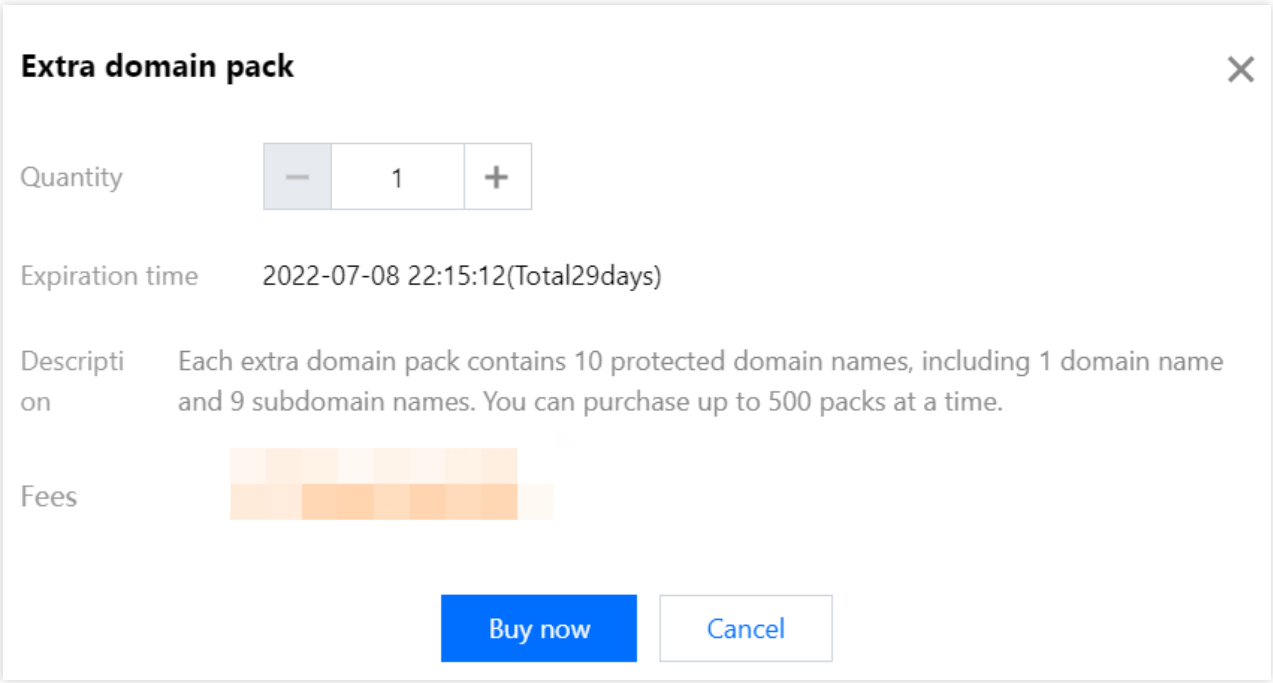
2. If your domain packs or QPS quota is about to run out, you can click **More** to display all billable items, and purchase a domain pack, an extra QPS pack, or the bot and application security service as needed.

Note:

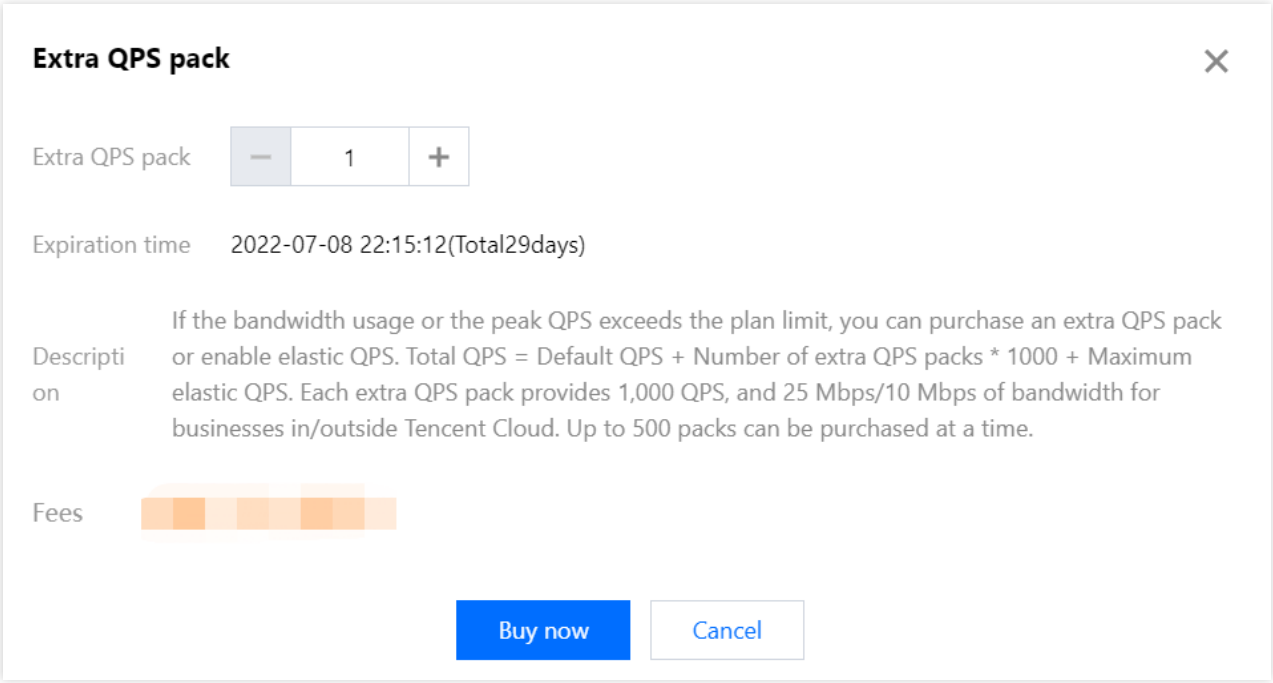
If the instance or domain pack already expires, please renew it first before you purchase another one.

Purchase domain pack: Up to 500 packs can be purchased. After you specify the number of domain packs to purchase, click **Buy now**.

©2013-2022 Tencent Cloud. All rights reserved.

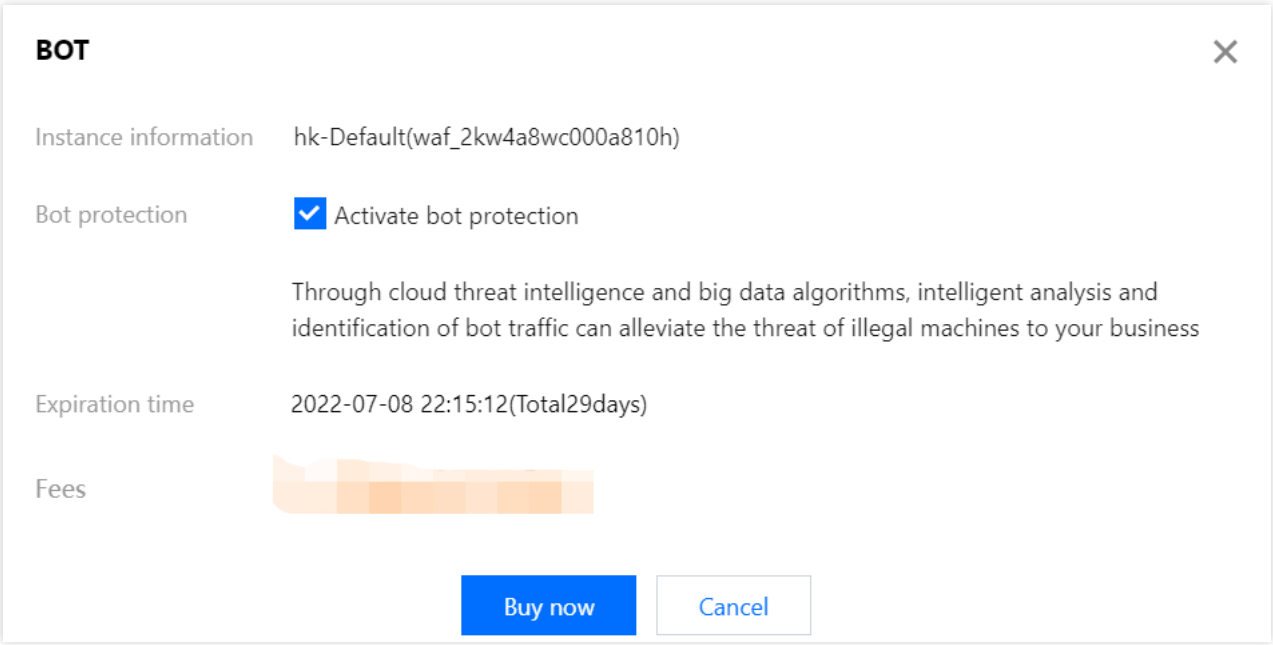


Purchase extra QPS pack: Up to 500 packs can be purchased. After you specify the number of extra QPS packs to purchase, click **Buy now**.



Bot and application security: Select the protection services as needed, and then click **Buy now**.

©2013-2022 Tencent Cloud. All rights reserved.



©2013-2022 Tencent Cloud. All rights reserved.

Domain Name List

Last updated：2023-12-29 14:26:48

Scenarios

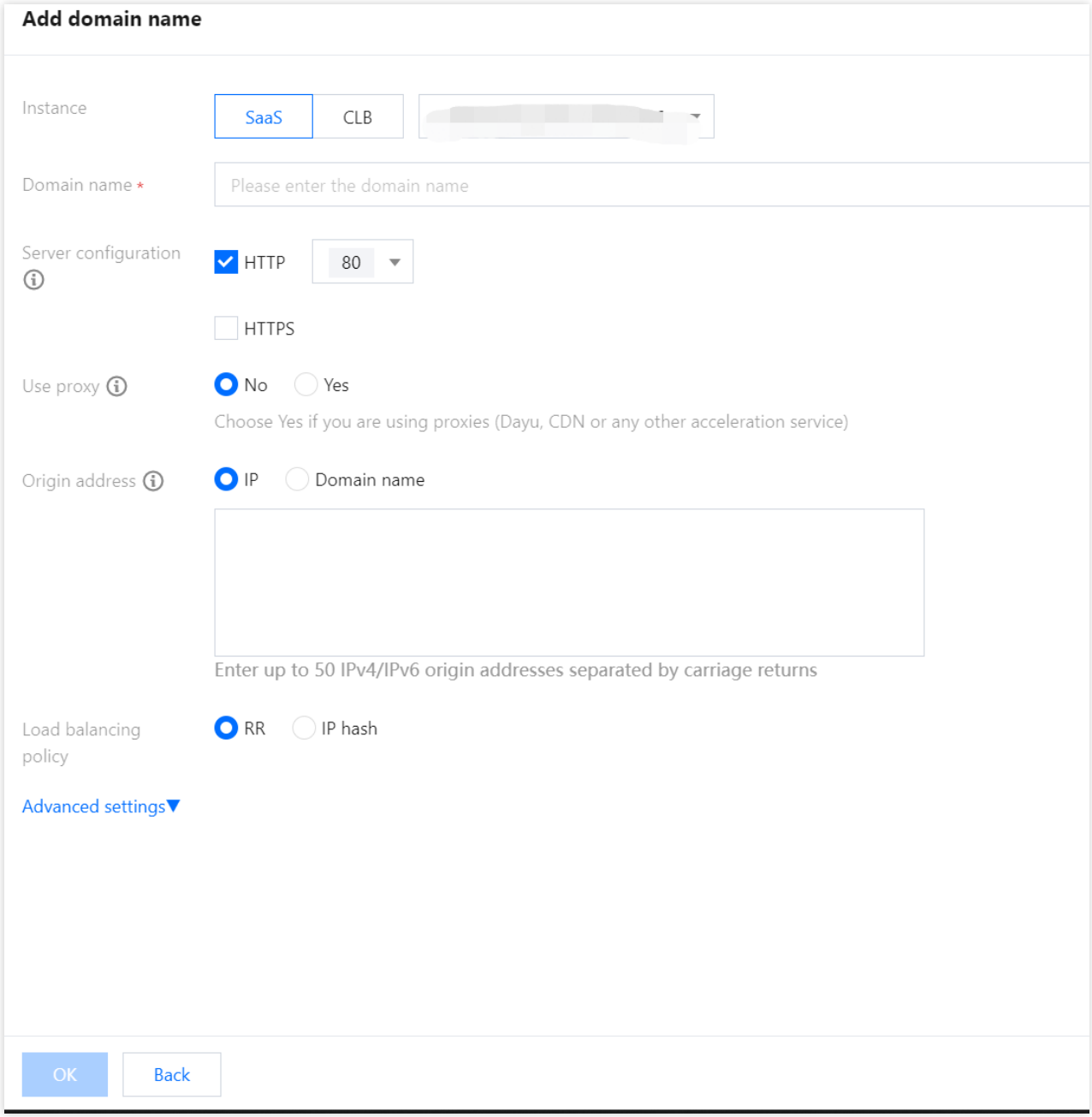
This document instructs you to manage your domain names in the WAF console.

Directions

Adding and viewing a domain name

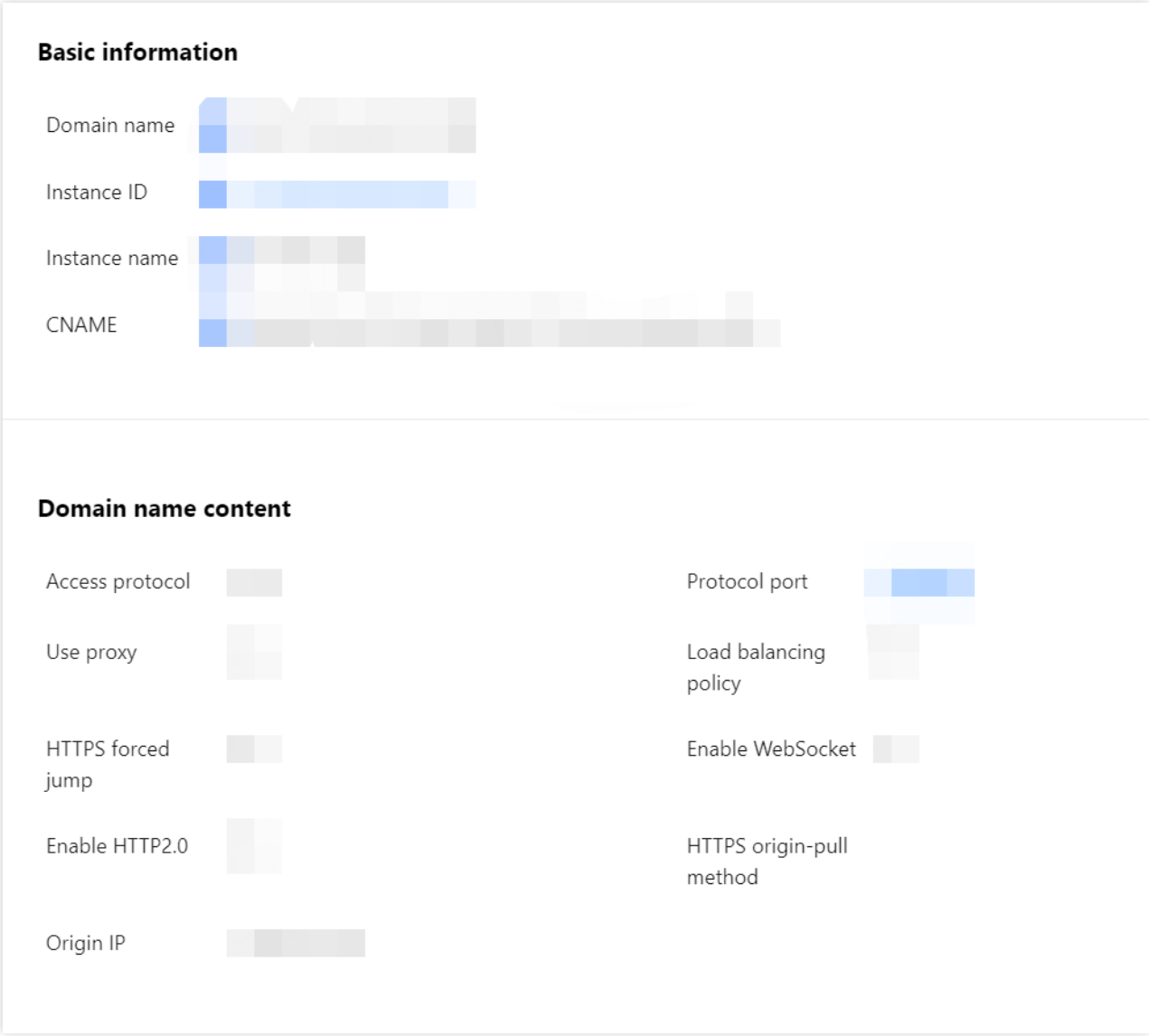
1. Log in to the WAF console and select **Asset Center** > **Domain Name List** on the left sidebar.
2. On the page displayed, click **Add domain name**.
3. On the pop-up page, configure the required parameters and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



4. On the domain name list page, click a domain name you want to view. The basic details of the domain name will be displayed.

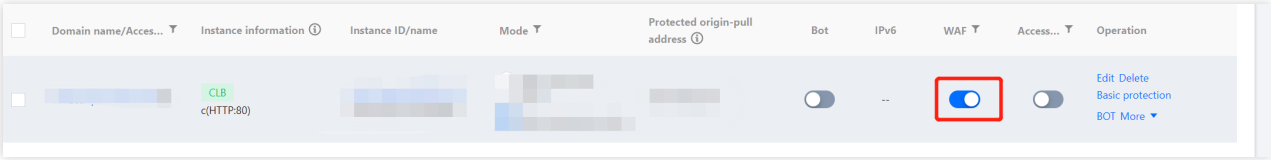
©2013-2022 Tencent Cloud. All rights reserved.



Toggling on protection switch

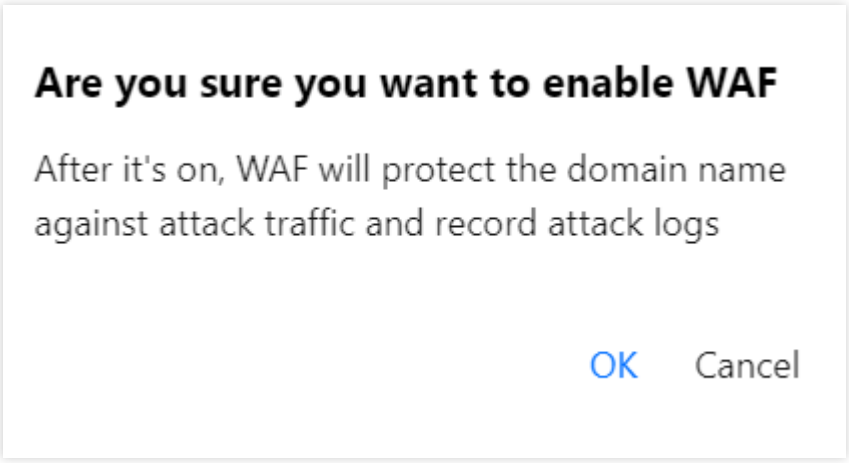
1. On the domain name list page, click the WAF switch

. A window will pop up to ask you to confirm your operation.



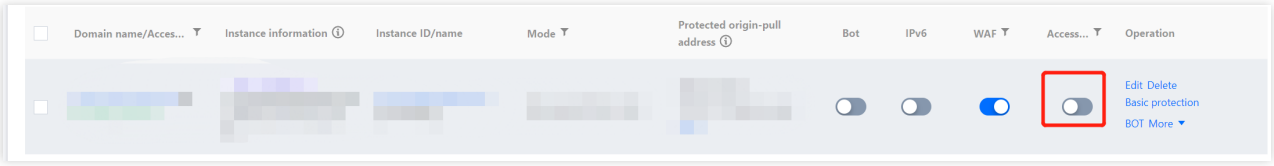
©2013-2022 Tencent Cloud. All rights reserved.

2. In the pop-up window, click **OK**. After the switch is on, WAF protection will take effect based on your custom policies and defense settings.



3. On the domain name list page, click the access logging switch

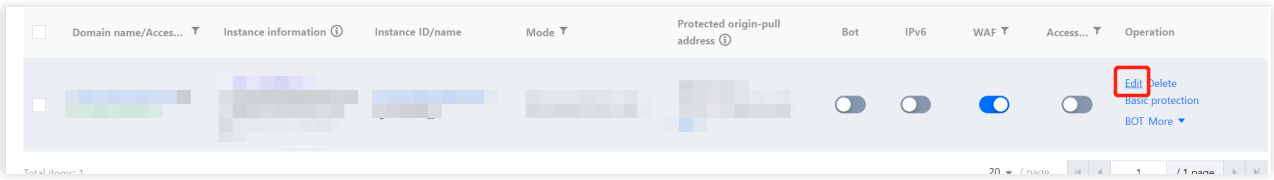
. A window will pop up to ask you to confirm your operation.



4. In the pop-up window, click **OK**. When the switch is on, access traffic of the domain name will be recorded.

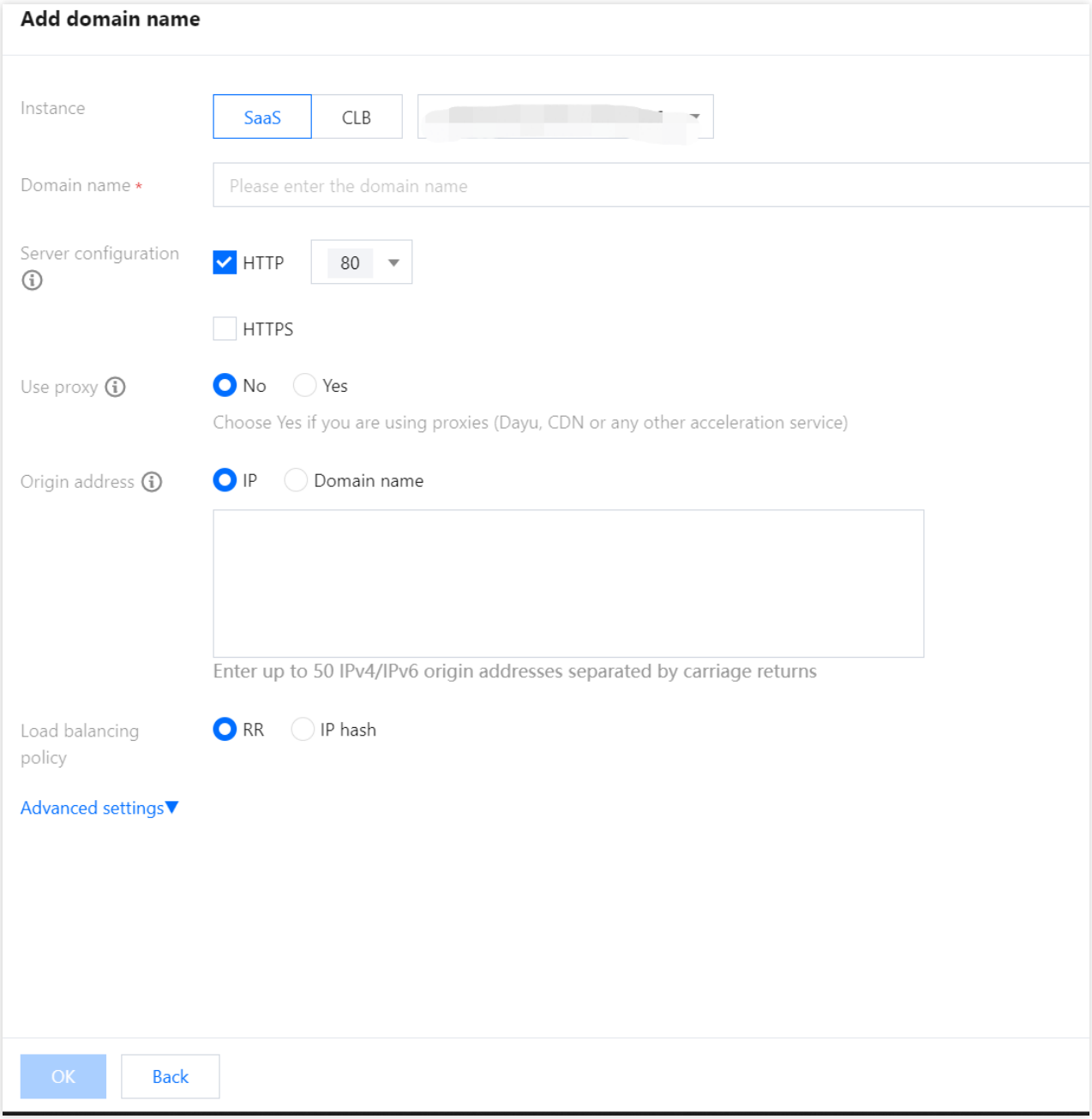
Editing a domain name

1. On the domain name list page, select the target domain name and click **Edit**.



©2013-2022 Tencent Cloud. All rights reserved.

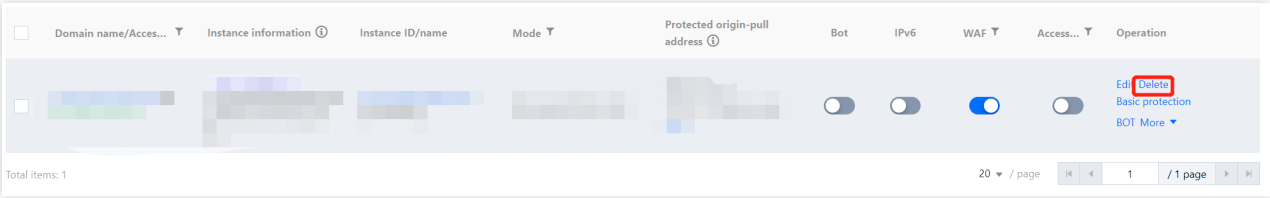
2. On the page displayed, modify the server configuration, proxy, and origin address, and click **OK** to save your changes.



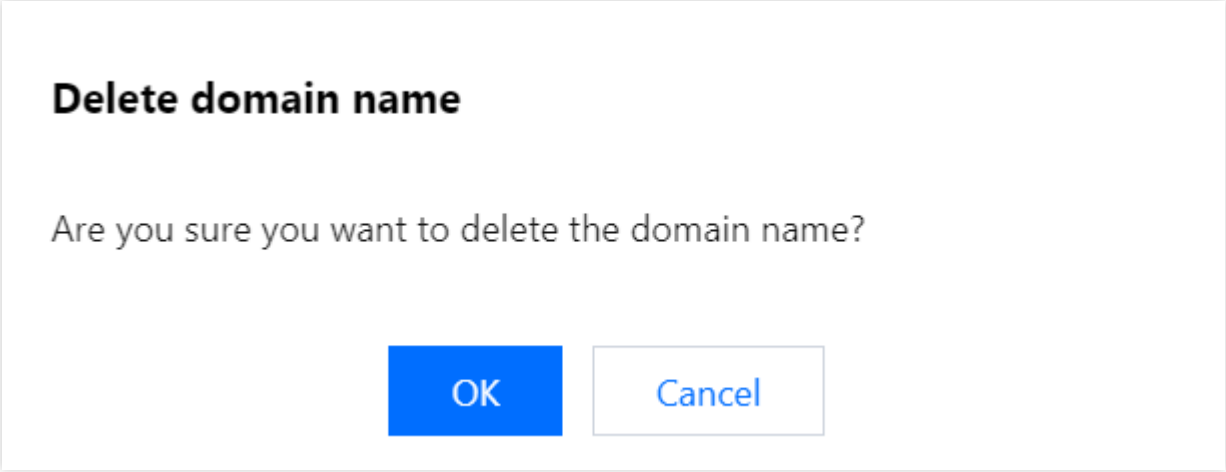
Deleting a domain name

1. On the domain name list page, select a domain name to delete and click **Delete** on the right.

©2013-2022 Tencent Cloud. All rights reserved.



2. In the pop-up window, click **OK** to delete the domain name.



©2013-2022 Tencent Cloud. All rights reserved.

Advanced Connection Feature

Last updated：2023-12-29 14:27:04

This document instructs you to configure advanced features for domain names, such as traffic tagging, remote client address transfer and access logging, to meet your compliance requirements.

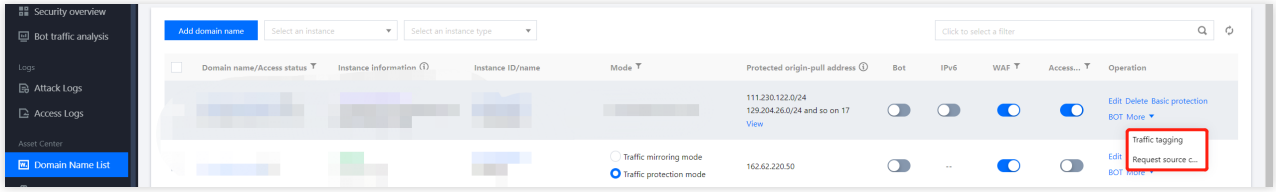
Note:

Only WAF Enterprise, Ultimate, and Exclusive editions support advanced features.

Enabling Traffic Tagging

Traffic tagging is used to tag a client request forwarded to the origin server by adding a custom field in the request header.

1. Log in to the WAF console and select **Asset Center** > **Domain Name List** on the left sidebar.
2. On the page that appears, select a domain name and click **More** > **Traffic tagging**.



3. In the pop-up window, click the checkbox

to enable traffic tagging, enter the required parameters, and then click **Save**.

Field description:

Traffic tag name: Name of the traffic tag.

Traffic tag value: Value of the traffic tag.

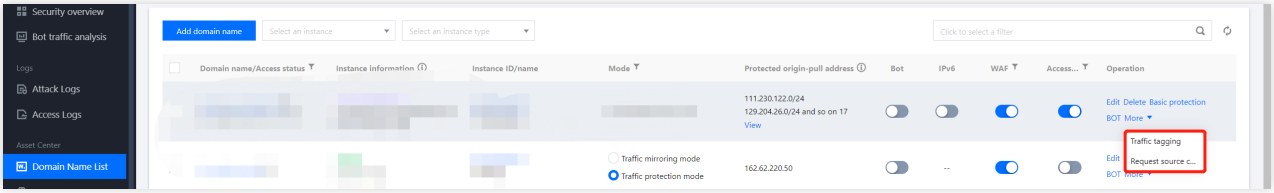
4. After the configuration is complete, click **Back** to return to the Domain Name List page.

Enabling Remote Client Address Transfer

Remote client address transfer is used to pass the IP address and source port of the previous hop to the backend when WAF forwards client requests to the origin server.

©2013-2022 Tencent Cloud. All rights reserved.

1. On the Domain Name List page, select a domain name. Click **More** > **Request configuration** on the right.



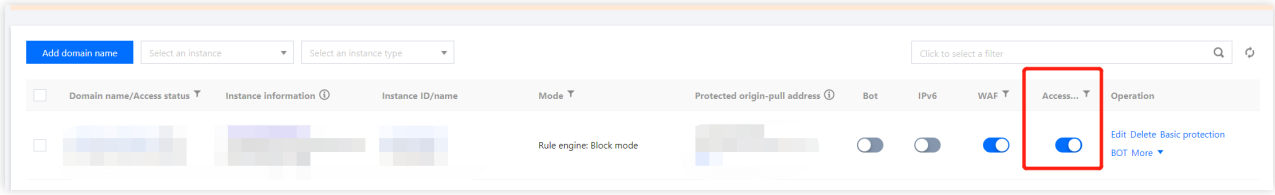
2. In the pop-up window, click the checkbox

to enable remote client address transfer. The real client IP and related information will then be recorded.

Enabling Log Service

On the Domain Name List page, select a domain name and toggle on the access logging switch

. Access logs will then be recorded automatically, and used for quick retrieval and source-tracking analysis.



©2013-2022 Tencent Cloud. All rights reserved.

API Asset Management

Last updated：2023-12-29 14:27:23

API Asset Management

API analytics helps find and manage open APIs and gather data for analysis and reporting on security events and traffic. Users are provided with risk mitigation recommendations and API lifecycle data to secure APIs.

Prerequisite

You have activated a monthly subscribed WAF instance for the Chinese mainland and the API security service.

Note

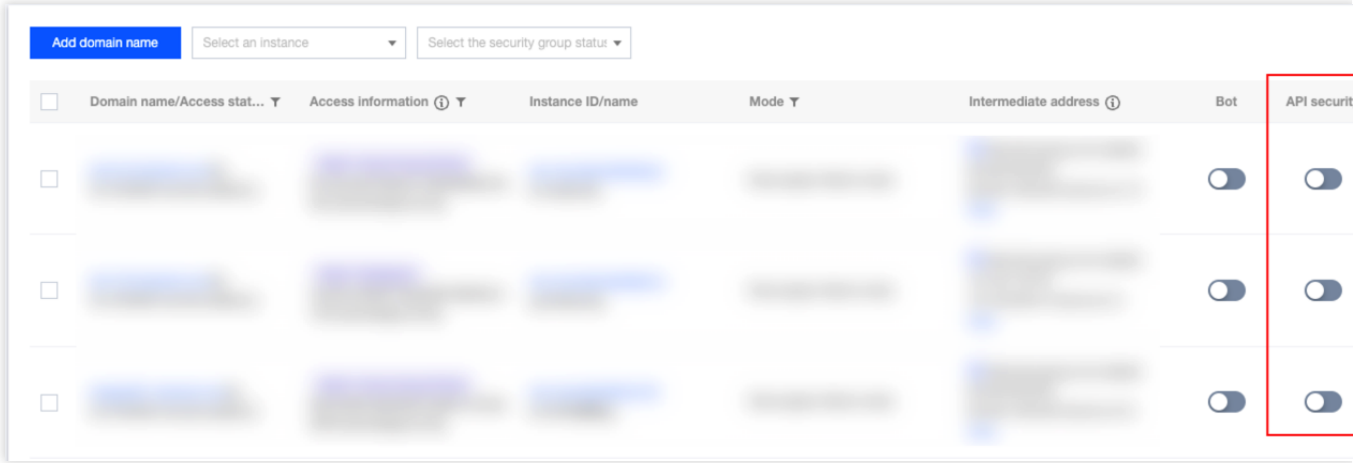
API analytics only supports 3 domain names in beta.

Enabling API Analytics

1. Log in to the WAF console and enable API analytics in the following ways.

On the domain name list page, view domain names that have API analytics activated and toggle on the API analytics switch

. After a second confirmation is made, the switch will be turned on.

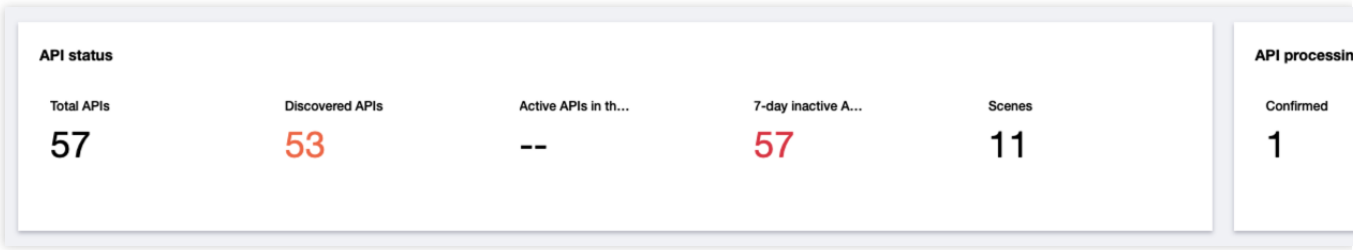


©2013-2022 Tencent Cloud. All rights reserved.

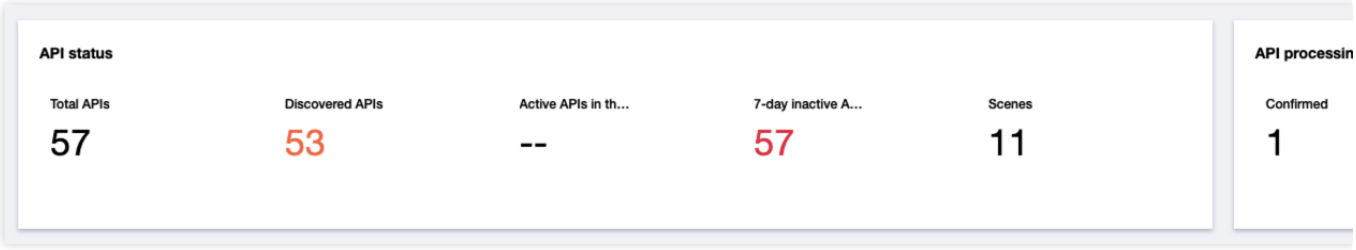
On the API assets page, select a domain name and click the switch in the API protection overview.
2. After the API analytics switch is toggled on for the domain name, you can analyze the API traffic.

Viewing API Assets

When API analytics is on, API security will discover and capture traffic data, analyze and sort out business items, and display them on the API assets page.
The **API overview** section displays total APIs, active/inactive APIs in the past 7 days and sensitive APIs under the current domain name, as well as WoW changes, so that you can keep track of your APIs.



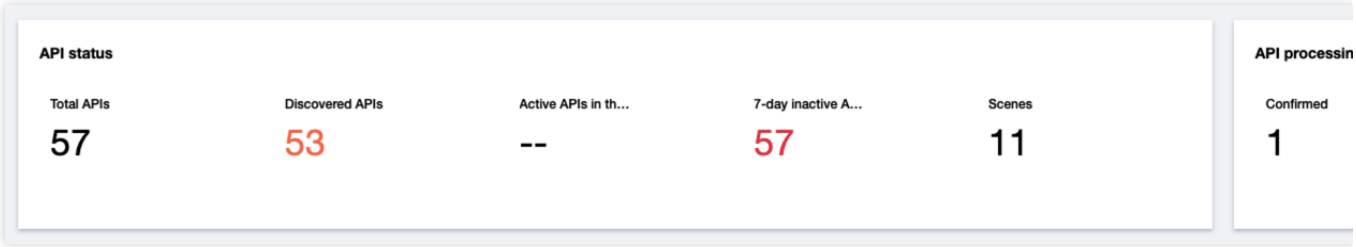
Field description
Total APIs: The total number of API assets identified.
7-day active APIs: : The number of APIs with active traffic in the past 7 days.
7-day inactive APIs: The number of APIs with no active traffic in the past 7 days, which may potentially become zombie APIs.
Sensitive APIs: The number of APIs that contain sensitive fields.
WoW: Compares the API count 7-day period to the previous 7-day period.
The **API security** section displays the number of use cases covered by the domain name, recommended actions and the API analysis content.



Field description
Use cases: The number of use cases covered by the current API.
Recommended actions: The actions recommended for API protection.

©2013-2022 Tencent Cloud. All rights reserved.

In the API list, you can view information related to the API, including the request method, domain name, use case, sensitive fields, status in the last 7 days, recommended action, and the time when the API was discovered, and the time when the API parameters were last updated. To learn more details about the API, click **View details**.



Field description

API: The API content identified after normalization.

Request method: HTTP request method.

Domain name: The domain name of the current API.

Use case: The usage scenario identified by API control, such as verification codes and callbacks. If the result is inaccurate, corrections can be made in API details.

Sensitive fields: The sensitive content detected by API control during parameter transmission, such as bank card number and ID. If the result is inaccurate, corrections can be made in API details.

Active in the past 7 days: Whether the traffic was active in the past 7 days.

Latest update: The time that the fields of the API were last updated.

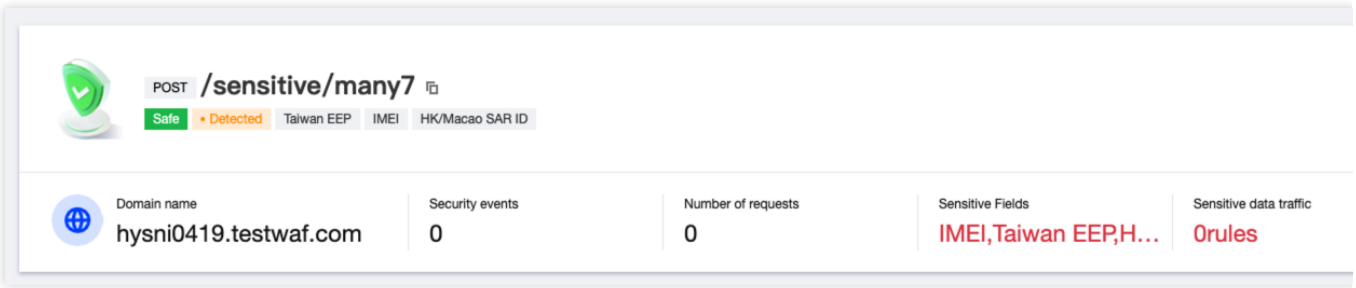
Detection time: The time when the API was first discovered by the API analytics module.

View details: The details of the corresponding API.

API Details

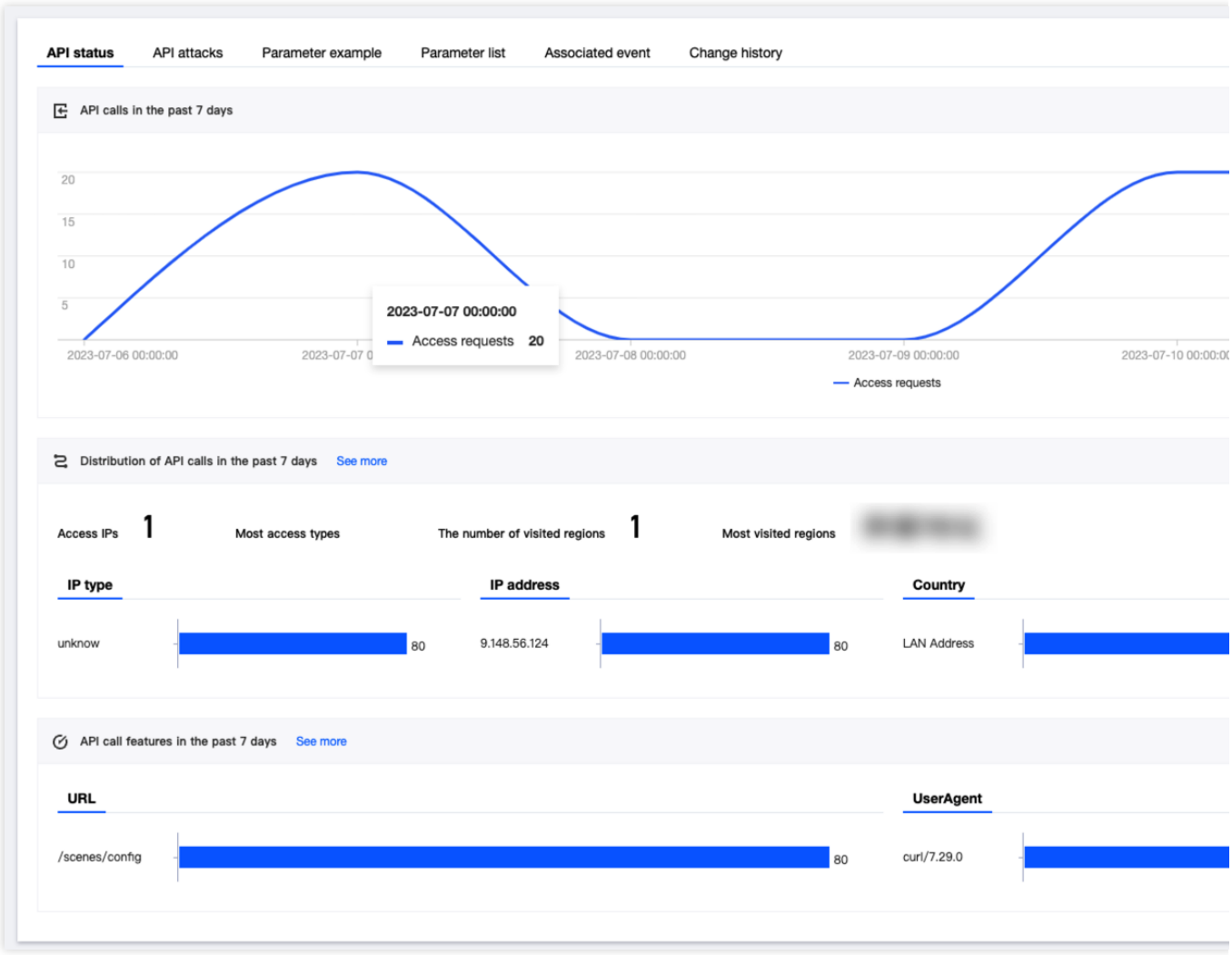
To view details of the API, click **View details** in the **Operation column**. On the page that appears, you can view the following information:

API information: Displays the domain name, request method, tag, sensitive fields, whether the API is active, and the API content after normalization.



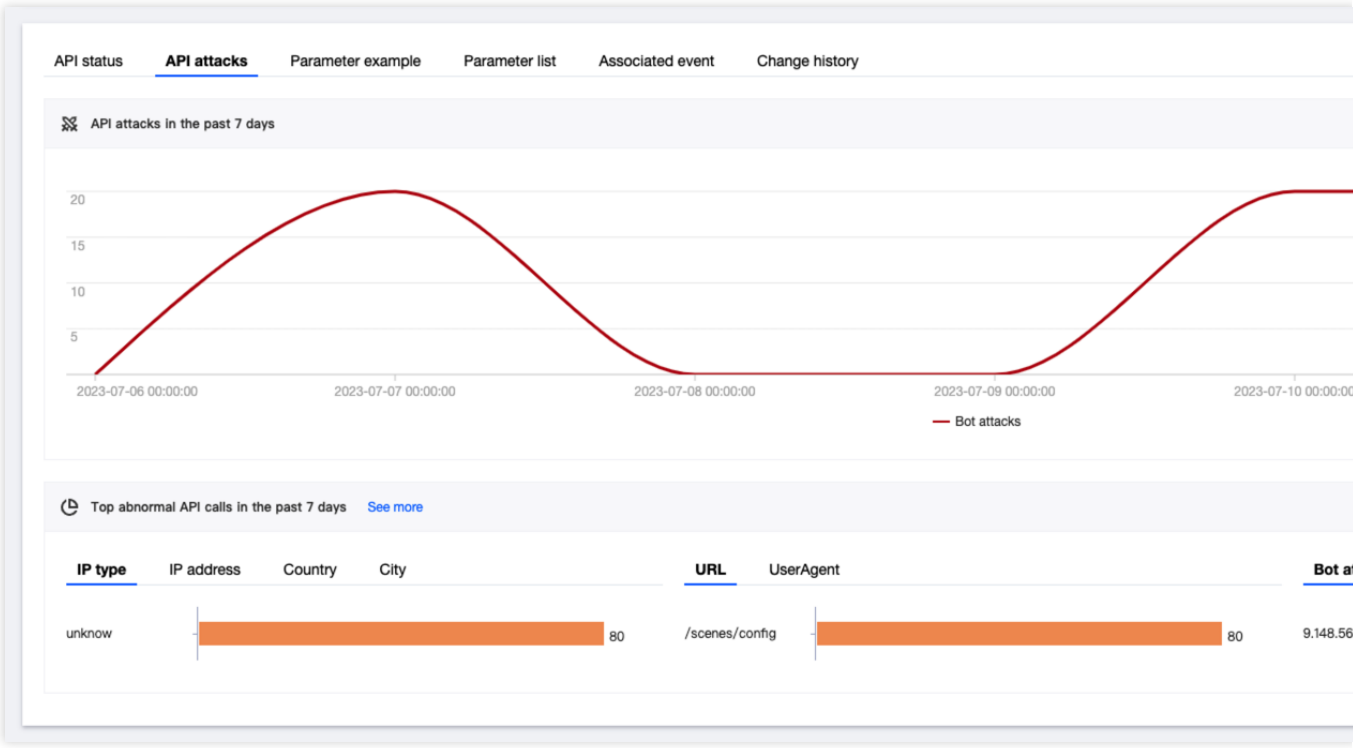
©2013-2022 Tencent Cloud. All rights reserved.

API overview: Displays the total requests and request trend of the corresponding API, distribution of access sources, and the most visited URLs and UA types in the last 7 days.

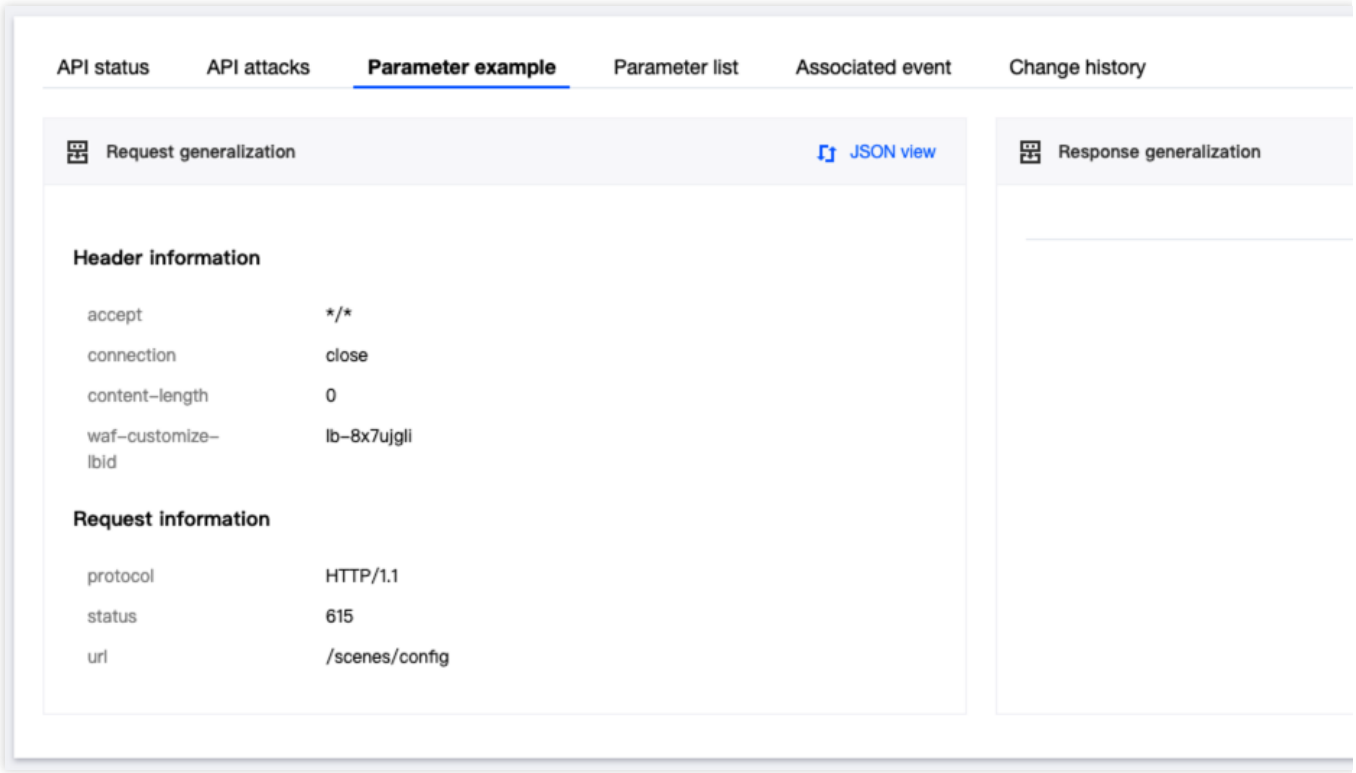


API attacks: Displays the attack trend and attack distribution of the API in the last 7 days, including the IP type and source, URL, UA, and attack type.

©2013-2022 Tencent Cloud. All rights reserved.

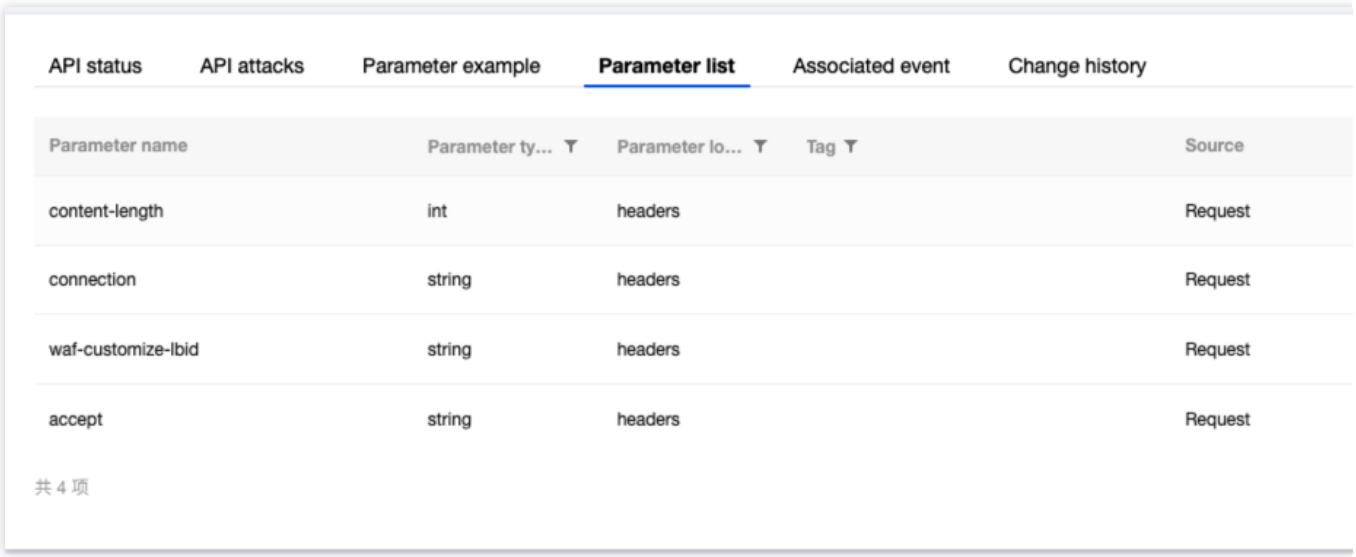


Request parameter sample: Displays the abstracted data of the API.



Parameter list: Displays the content and location of each parameter transmitted by the API. You can add marks to the information manually.

©2013-2022 Tencent Cloud. All rights reserved.



©2013-2022 Tencent Cloud. All rights reserved.

Basic Security Configurations
Rule Engine

Last updated：2023-12-29 14:27:43

This document describes how to configure protection rules in Web Application Firewall (WAF) to defend against web attacks.

Overview

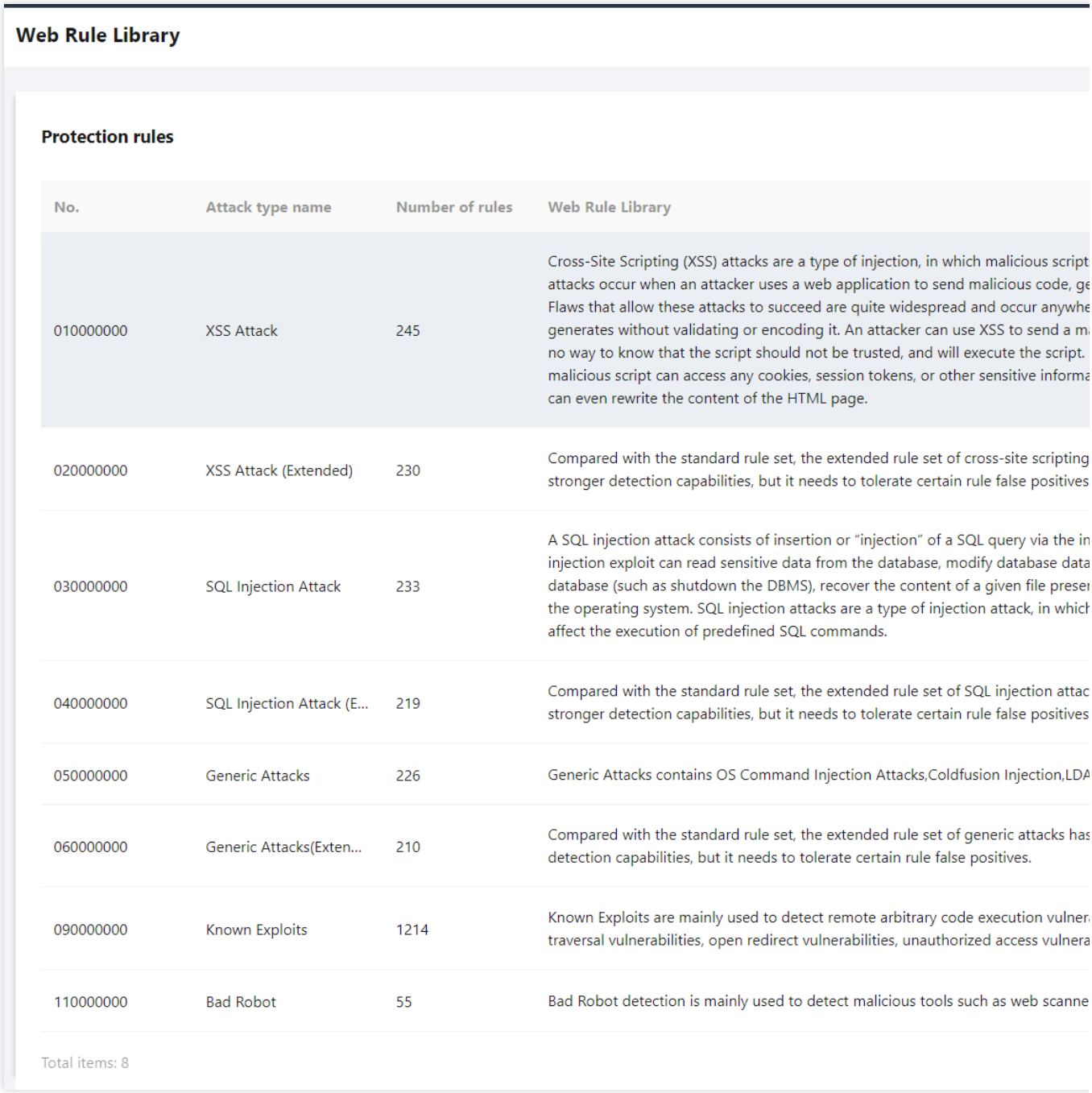
WAF uses a regex-based rule protection engine and a machine learning-based AI protection engine to defend against web vulnerabilities and unknown threats.
WAF's rule protection engine provides expert rule sets based on Tencent Security's accumulated web threat intelligence to automatically prevent OWASP top 10 attacks. Currently, it can defend against 17 categories of common web attacks, such as SQL injections, XSS attacks, malicious scanning, command injection attacks, web application vulnerabilities, WebShell uploads, non-compliant protocols, and trojans.
WAF's rule protection engine supports rule level configuration. You can set 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.

Directions

Viewing the rule category

1. Log in to the WAF console and select **Service Management** > **Web Rule Library** on the left sidebar.
2. On the **Protection rules** tab, you can view the descriptions and rule updates of the attack categories that WAF currently can defend against.

©2013-2022 Tencent Cloud. All rights reserved.



Web Rule Library

Protection rules

No.	Attack type name	Number of rules	Web Rule Library
010000000	XSS Attack	245	Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious script attacks occur when an attacker uses a web application to send malicious code, ge Flaws that allow these attacks to succeed are quite widespread and occur anywhe generates without validating or encoding it. An attacker can use XSS to send a m no way to know that the script should not be trusted, and will execute the script. malicious script can access any cookies, session tokens, or other sensitive informa can even rewrite the content of the HTML page.
020000000	XSS Attack (Extended)	230	Compared with the standard rule set, the extended rule set of cross-site scripting stronger detection capabilities, but it needs to tolerate certain rule false positives
030000000	SQL Injection Attack	233	A SQL injection attack consists of insertion or "injection" of a SQL query via the in injection exploit can read sensitive data from the database, modify database data database (such as shutdown the DBMS), recover the content of a given file preser the operating system. SQL injection attacks are a type of injection attack, in which affect the execution of predefined SQL commands.
040000000	SQL Injection Attack (E...	219	Compared with the standard rule set, the extended rule set of SQL injection attac stronger detection capabilities, but it needs to tolerate certain rule false positives
050000000	Generic Attacks	226	Generic Attacks contains OS Command Injection Attacks,Coldfusion Injection,LDA
060000000	Generic Attacks(Exten...	210	Compared with the standard rule set, the extended rule set of generic attacks has detection capabilities, but it needs to tolerate certain rule false positives.
090000000	Known Exploits	1214	Known Exploits are mainly used to detect remote arbitrary code execution vulner traversal vulnerabilities, open redirect vulnerabilities, unauthorized access vulnera
110000000	Bad Robot	55	Bad Robot detection is mainly used to detect malicious tools such as web scanne

Total items: 8

Attack categories that WAF currently can defend against include:

Attack Category	Attack Description
SQL injection attack	In the implementation of websites, the input parameters are not strictly filtered, resulting in the unauthorized acquisition of SQL database content.
XSS attack	XSS vulnerabilities occur when the application's new webpage contains untrusted data or data that is not properly validated or escaped, or when an existing webpage is updated using a browser API that can create HTML or JavaScript. XSS enables attackers to execute scripts in victims' browsers, hijack user sessions, destroy websites, or redirect users to malicious sites.

©2013-2022 Tencent Cloud. All rights reserved.

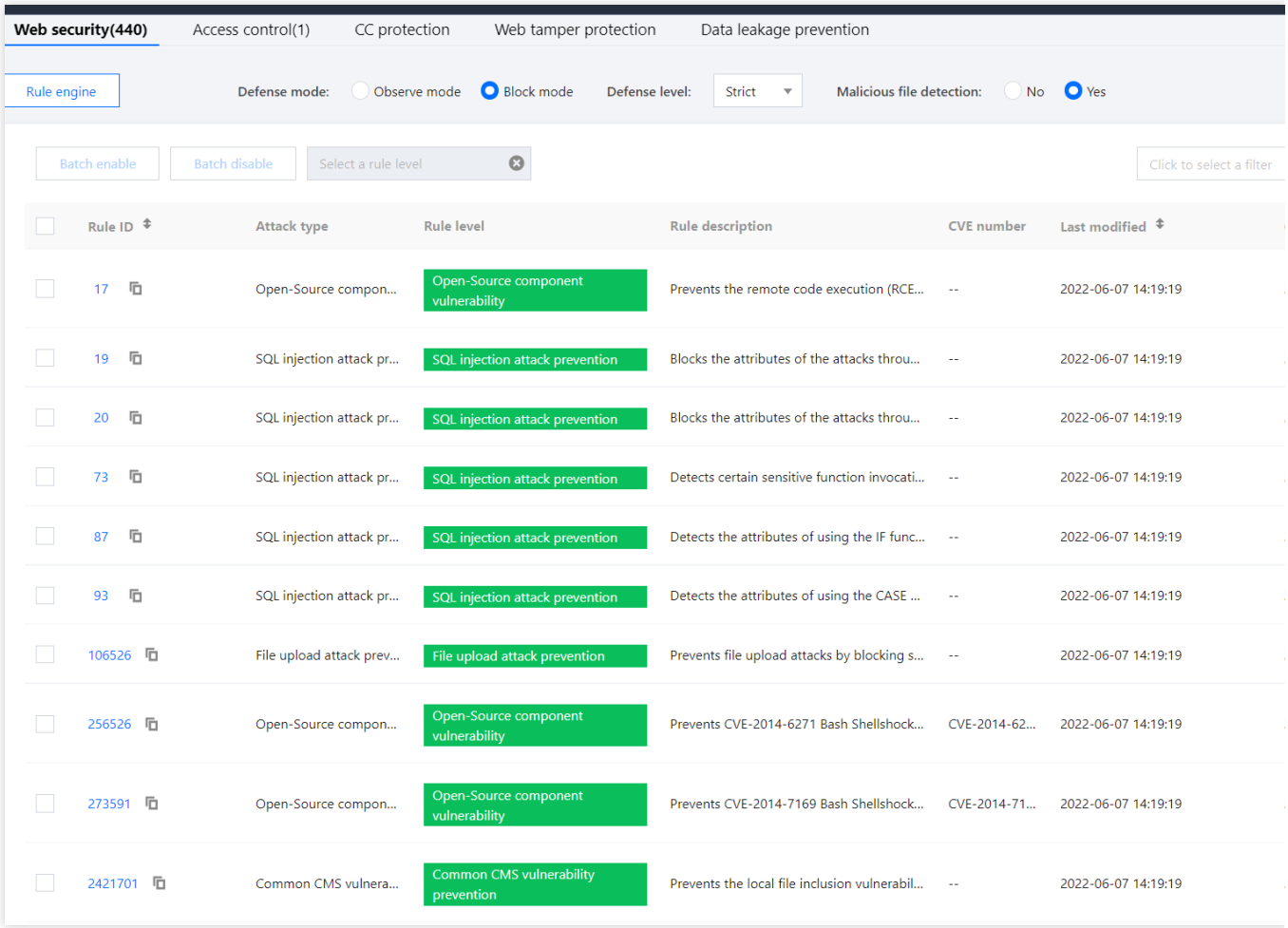
Malicious scanning	WAF can detect whether the website has been maliciously scanned.
Unauthorized access to core files	WAF can detect whether certain configuration files, database files, and parameter data are downloadable at will.
Open-source component vulnerability exploiting	Attacks caused by vulnerabilities in common open-source web components.
Command injection attack	This is a type of injection attacks, such as shell command injections, PHP code injections, and Java code injections, which can cause websites to execute the injected code if successfully exploited by attackers.
Web application vulnerability exploiting	Web application security (security of Java, ActiveX, PHP, and ASP code running on the web server).
XXE attack	If the XML processor has external entity references in the XML file, attackers can use external entities to steal internal files and shared files that use the URI file processor, monitor internal scanning ports, execute remote code, and implement denial of service attacks.
Trojan horse attack	WAF can detect the communication with the control terminal during or after trojan upload.
File upload attack	After a malicious script disguised as a file with a normal extension is uploaded, attackers can execute it through the local file inclusion vulnerability.
Other vulnerability exploiting	Attacks caused by the security configuration or vulnerabilities of the web server itself and other software.
Non-compliant protocol	Exceptions with HTTP protocol and header parameters.

3. You can view the rule updates on the right of the **Protection rules** tab. For more security notifications, please see Security Advisory.

Rule management

1. Log in to the WAF console and select **Configuration Center** > **Basic Security** on the left sidebar.
2. On the page that appears, click **Web security**. On the **Rule engine** tab, you can enable individual rules based on domain names. All rules are enabled by default.

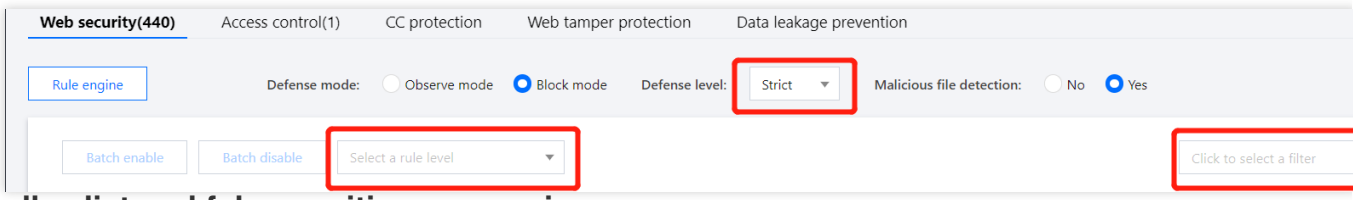
©2013-2022 Tencent Cloud. All rights reserved.



3. You can search in the rule set by specifying the rule level, defense level, rule ID, attack category, or CVE number to view specific rules and perform operations.

Note:

The level "Strict" covers rules of the level "Normal" and "Loose", and "Normal" covers "Loose".



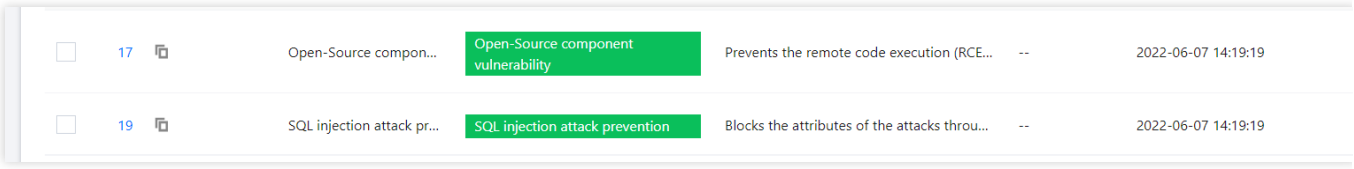
Rule allowlist and false positive processing

1. Log in to the WAF console and select **Configuration Center** > **Basic Security** on the left sidebar.

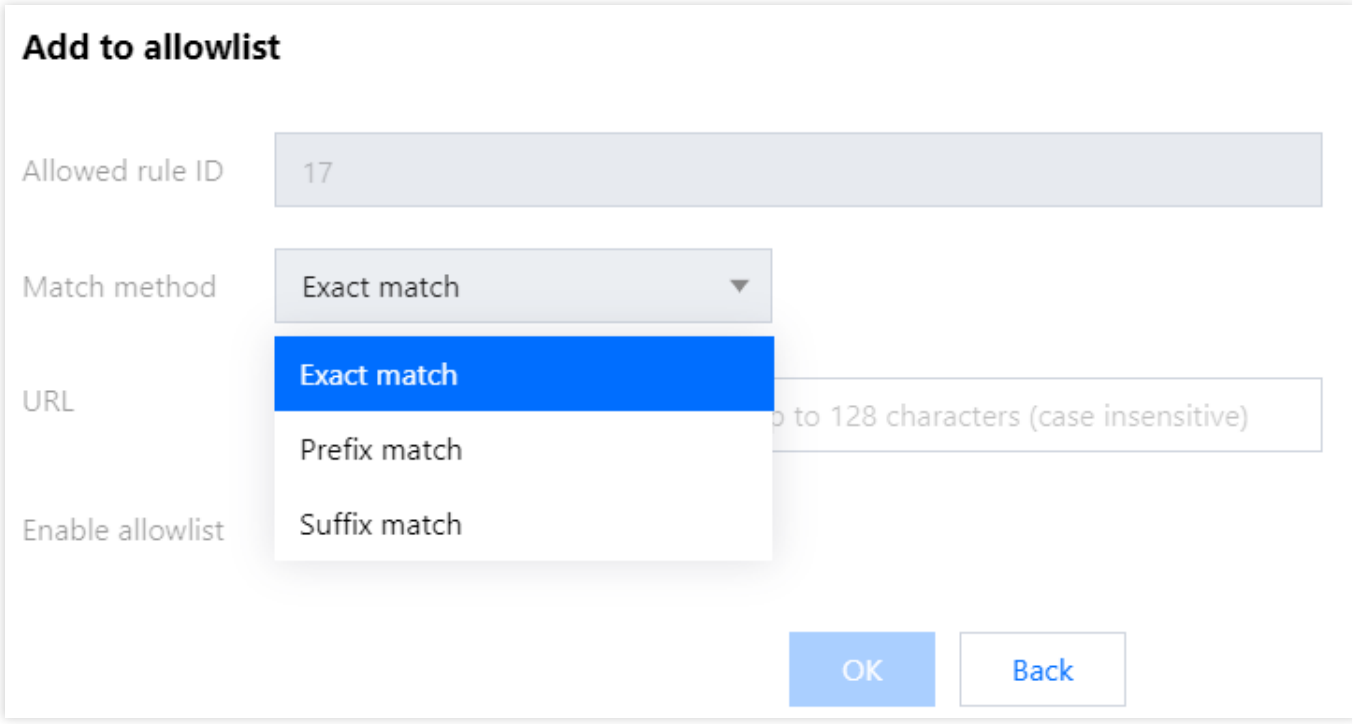
2. On the basic security page, click **Web security**. On the "Rule engine" tab, you can add domain name URLs and rule IDs to the allowlist and process false positives.

3. On the **Rule engine** tab, select the target rule, click **Add to allowlist**, and the custom rule adding window will pop up.

©2013-2022 Tencent Cloud. All rights reserved.



4. In the pop-up window, configure relevant parameters and click **OK**.



Field description

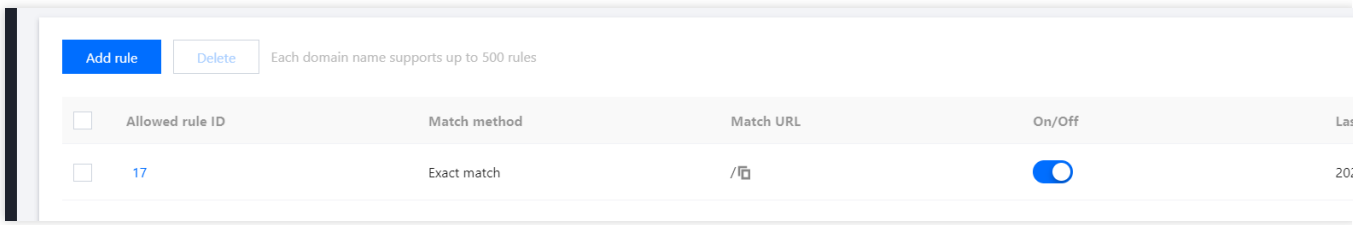
Rule ID: ID of the rule that needs to be allowed. You can add one rule ID for each policy.

Match method: Match method of the URL to be allowed. You can select "Exact match" (default value), "Prefix match", or "Suffix match".

URL: URL path to be allowed. The URL must be unique under one domain name.

Enable allowlist: It controls whether to enable allowlist, which is disabled by default.

5. After the allowlist is configured, click **View allowlist** to view the allowed rules and perform relevant operations.



Field description:

Rule ID: ID of the rule added to the allowlist, which can be obtained through attack logs or rule management.

©2013-2022 Tencent Cloud. All rights reserved.

Match method: Match method of the URL to be allowed. You can select "Exact match" (default value), "Prefix match", or "Suffix match".

URL: URL path to be allowed. The URL must be unique under one domain name.

Enable allowlist: It controls whether to enable allowlist.

Last modified: The last time the rule was added or modified.

Operation: It allows you to edit or delete a rule.

Click **Edit**, modify relevant parameters, and click **OK**.

Click **Delete** and confirm the deletion.

©2013-2022 Tencent Cloud. All rights reserved.

IP Blocking Penalty

Last updated：2023-12-29 14:30:37

This document describes Web Application Firewall (WAF) attacker IP penalty, which can quickly block malicious attacker IPs and defeat attacks and threats from malicious scanners, proxies and webs to improve defense efficiency.

Overview

Attacker IP penalty can automatically block repeated web attacks the client IP suffered in a short period of time. You can view attack logs for attack details.

Prerequisites

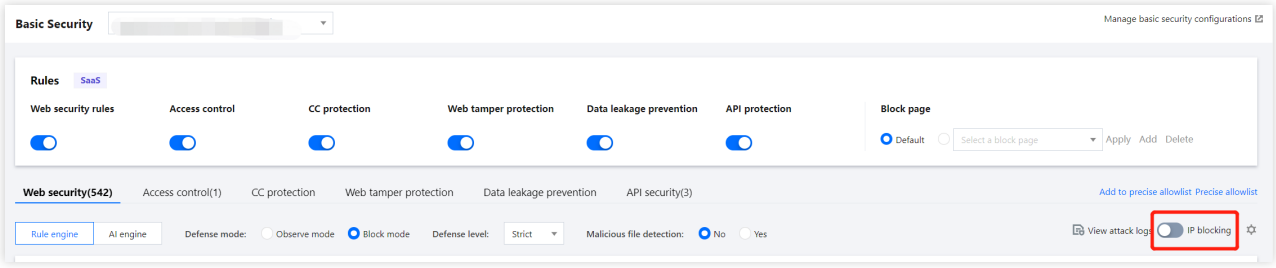
You have purchased a WAF plan.
You have added a protected domain name, and ensured the domain name is in normal protection. For detailed directions, see Getting Started.
Currently, IPs can be blocked by domain name. Domain names can have different blocking durations, which are calculated separately.

Directions

1. Log in to the WAF console and select **Configuration Center** > **Basic Security** > **Web Security** on the left sidebar.
2. On the web security page, select the target domain name in the top-left corner and click

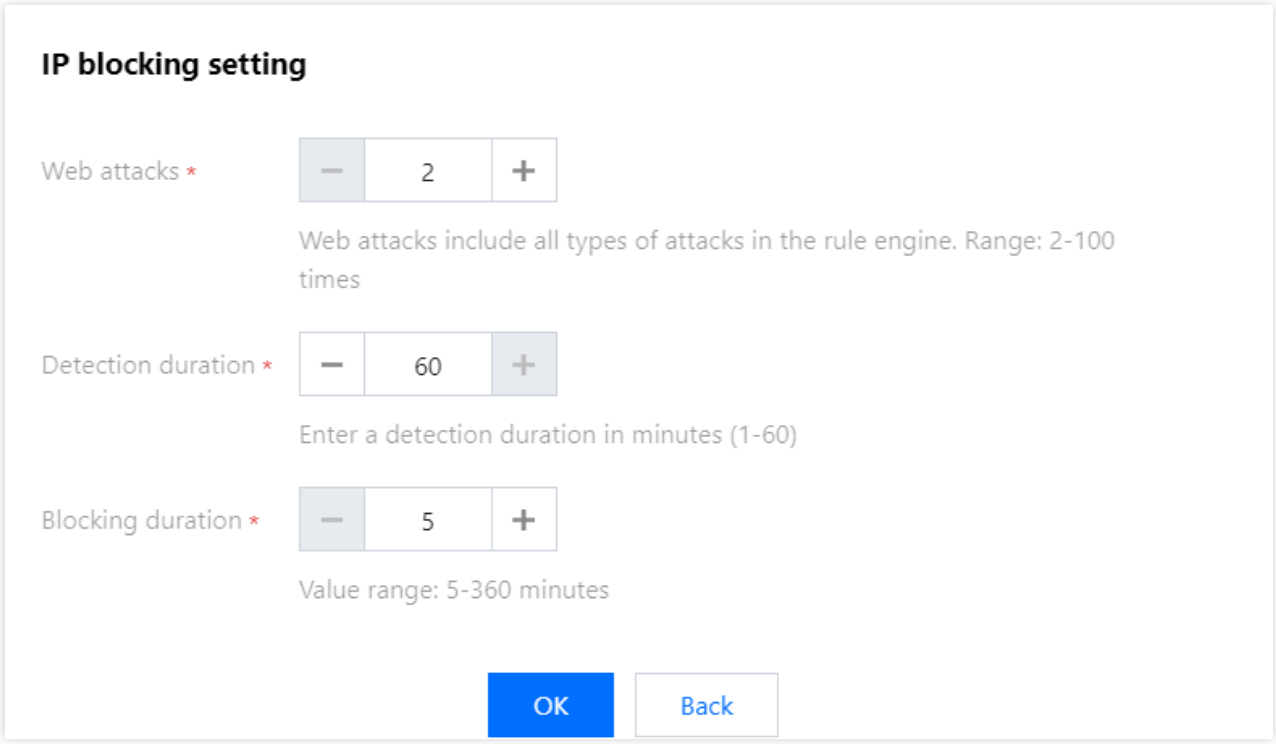
next to **IP blocking** to enable IP blocking.

©2013-2022 Tencent Cloud. All rights reserved.



3. On the web security page, click

next to **IP blocking** to modify default parameters and click **OK**.



Field description:

Web attacks: It records the number of web attacks from a malicious IP in a specified period. The attacks will trigger the rule engines against web attacks excluding AI engine, custom policies and CC protection.

Detection duration: It specifies the duration to detect the attacker IP.

Blocking duration: It specifies the duration to block the attacker IP.

©2013-2022 Tencent Cloud. All rights reserved.

Access Control

Last updated：2023-12-29 14:35:38

Overview

Access control rules allow you to control access from public network users by matching HTTP message sections such as request path, GET parameters, POST parameters, Referer, and User-Agent. This feature enables Tencent Cloud users to respond flexibly with a combination of rules to easily block various cyber attacks.

Note:

Each rule can contain up to 5 conditions.

Conditions in each rule are evaluated using a logical AND, that is, the rule does not take effect unless all the conditions are matched.

Each rule supports four actions: Block, CAPTCHA, Observe, and Redirect.

Block: Enables WAF to block access requests that hit the specified rule.

CAPTCHA: Enables WAF to verify access requests that hit the specified rule.

Observe: Enables WAF to observe access requests that hit the specified rule.

Redirect: Enables WAF to redirect access requests that hit the specified rule.

Priority: The value range is 1-100. A smaller number represents higher priority.

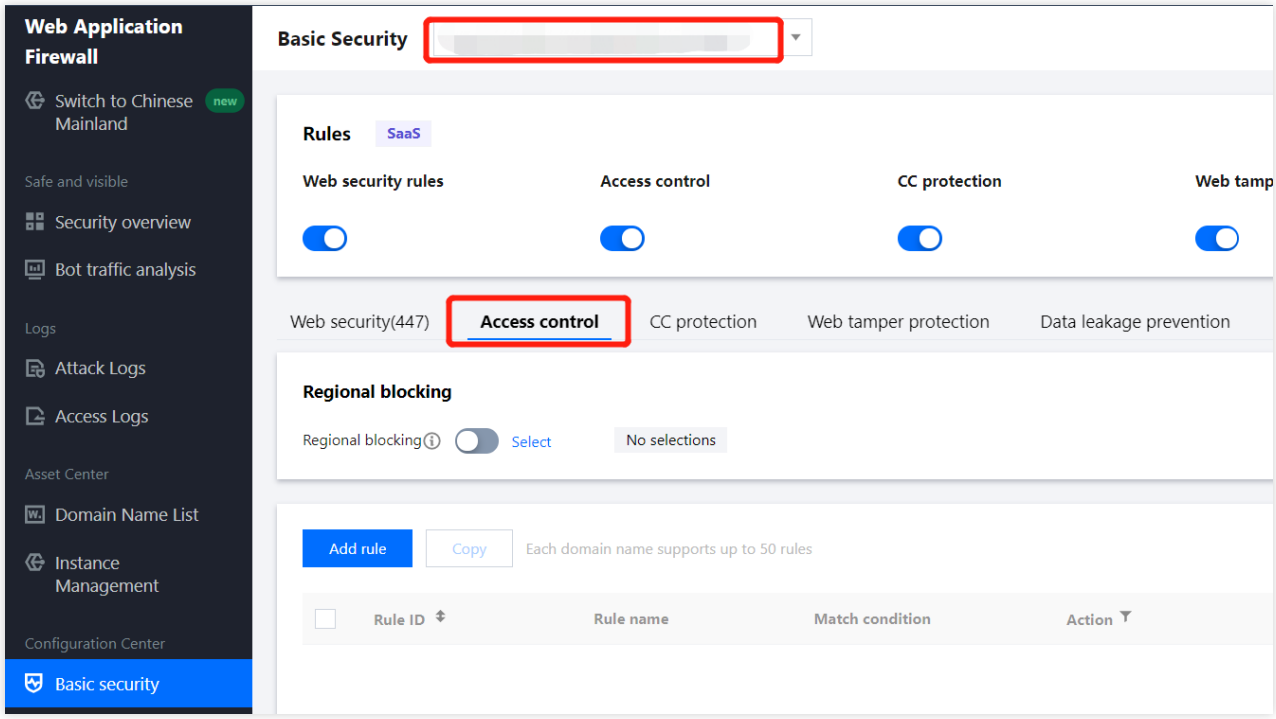
Example

Example 1: Banning specific IP addresses from access to a designated site

To ban specific IP addresses from access to a designated site, the webmaster can perform configuration with the following steps:

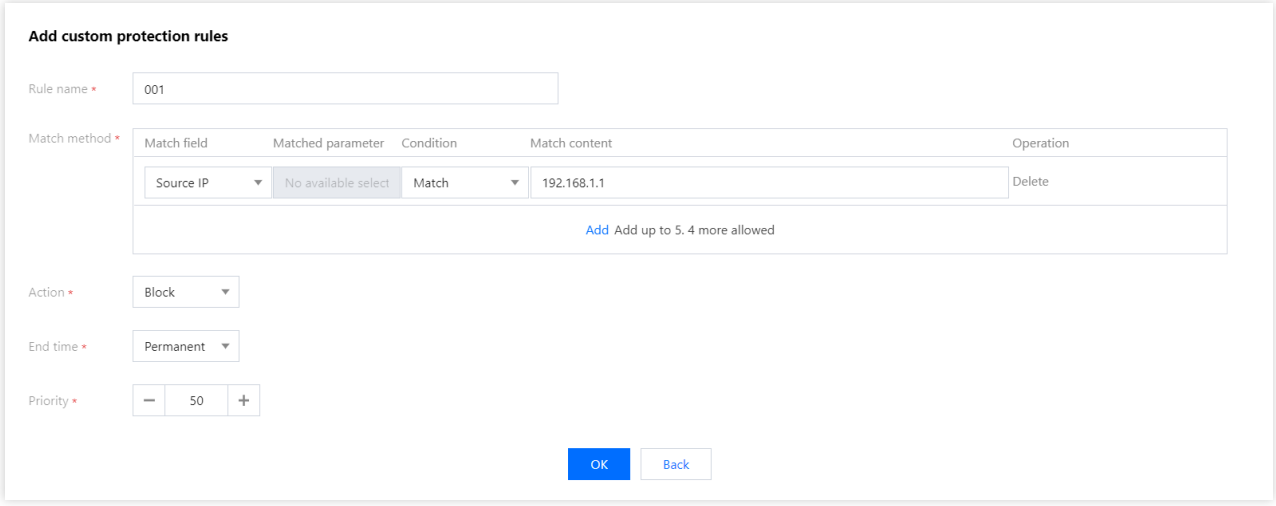
1. Log in to the WAF console and click **Configuration Center** > **Basic Security** on the left sidebar.
2. On the basic security page, select the target domain name in the top-left corner and click **Access control**.

©2013-2022 Tencent Cloud. All rights reserved.



3. On the access control page, click **Add rule**, and the rule adding window will pop up.

4. Enter the name of the rule (e.g. "001"), select an option (such as "source IP") for **Field**, select “Match” for **Logical operator**, and enter the source IP (e.g. `192.168.1.1`) banned from access for **Content**. Then select an action (e.g. "Block"), and click **OK** to save the rule.

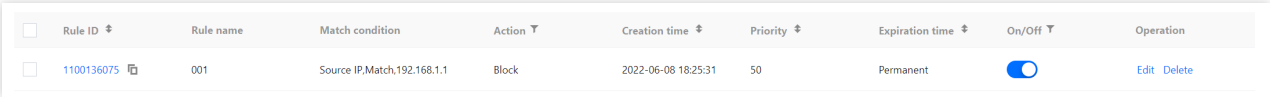


Note:

WAF access control rules allow you to use masks to control access requests from source IPs within a range. We can enter a specific IP address range (e.g. `10.10.10.10/24`) in **Content**.

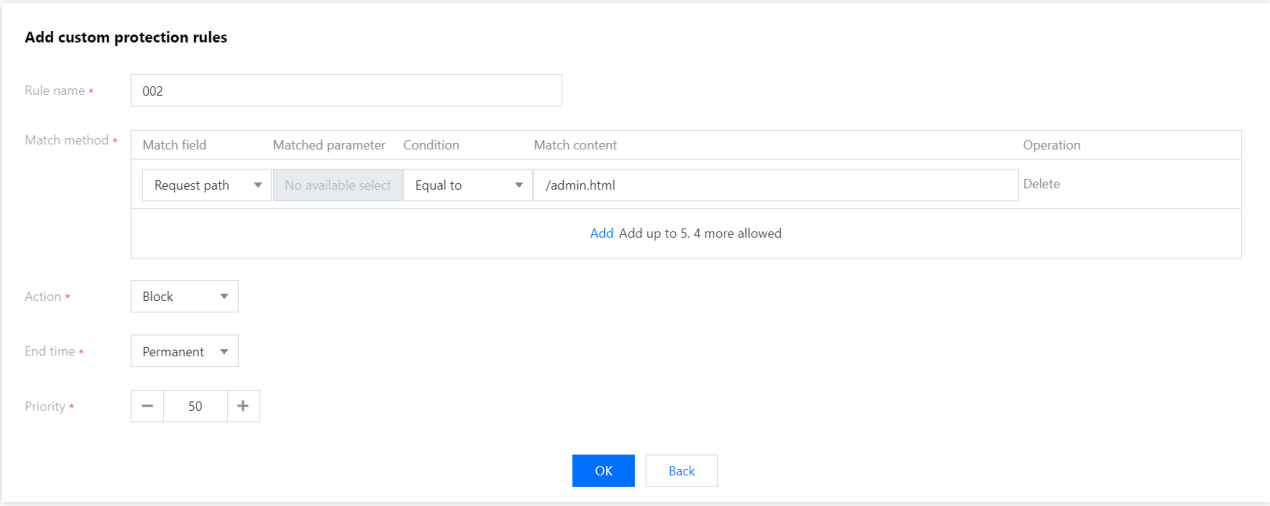
5. Now, the rule will take effect immediately, and block all HTTP access requests from specific source IPs.

©2013-2022 Tencent Cloud. All rights reserved.



Example 2: Banning public network users from access to specified Web resources

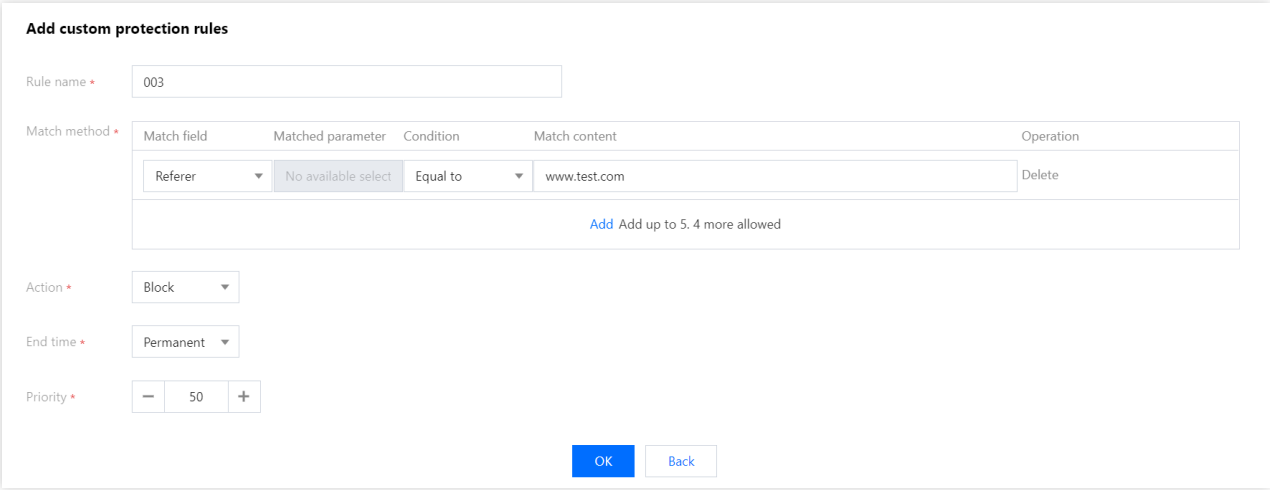
If the webmaster does not want a public network user to access specified web resources, such as administration backend `/admin.html`, he or she can configure as follows: select "Request Path" for **Field**, select "Equal to" for **Condition**, enter `/admin.html` in **Content**, select "Block" for **Action**, and click **OK**.



Example 3: Banning an external site from hot-linking certain resources

To block hotlink attacks by external sites, such as `www.test.com`, the webmaster can use access control rules to capture and block the Referer in a hotlink request. The configuration is as follows: select "Referer" for **Field**, select "Include" for **Condition**, enter `www.test.com` in **Content**, select "Block" for **Action**, and click **OK**.

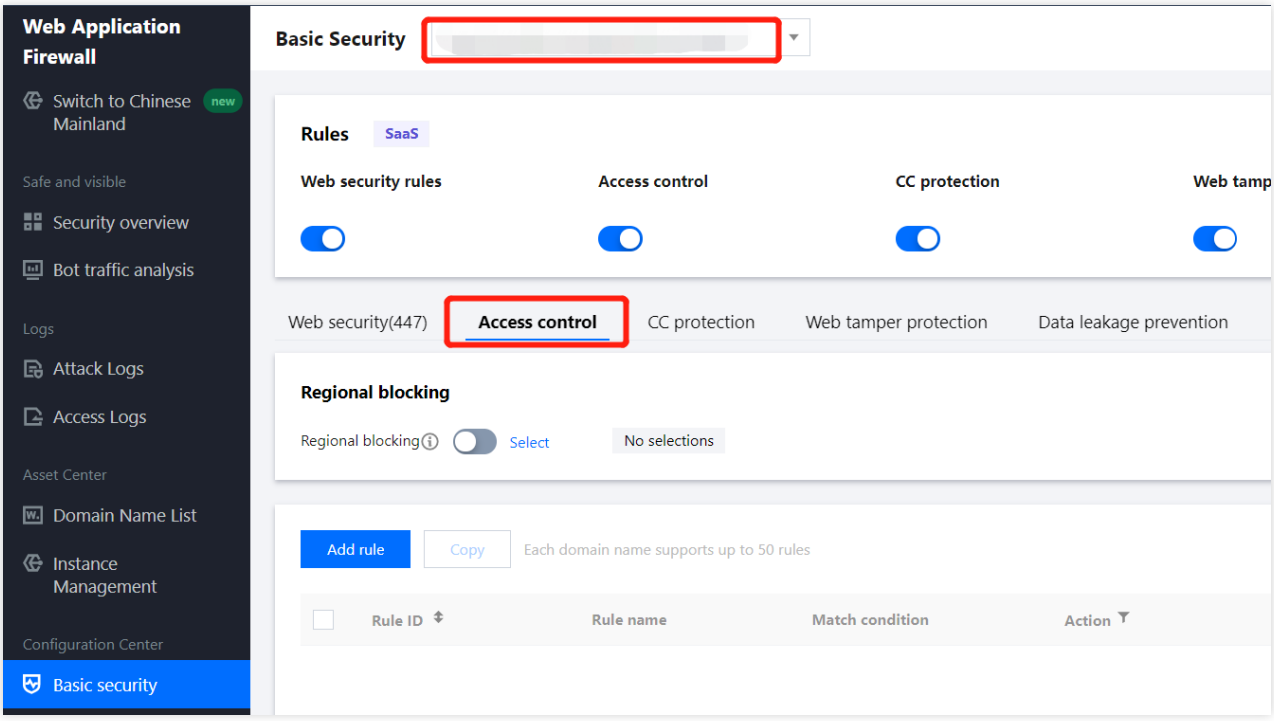
©2013-2022 Tencent Cloud. All rights reserved.



Example 4: Copying rules to target domain names

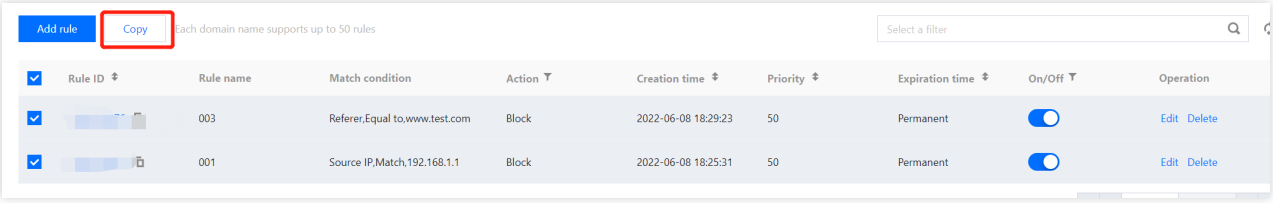
You can copy the rule you configured to other domain names by using the copy operation.

1. Log in to the WAF console and click **Configuration Center** > **Basic Security** on the left sidebar.
2. On the basic security page, select the target domain name in the top-left corner and click **Access control**.

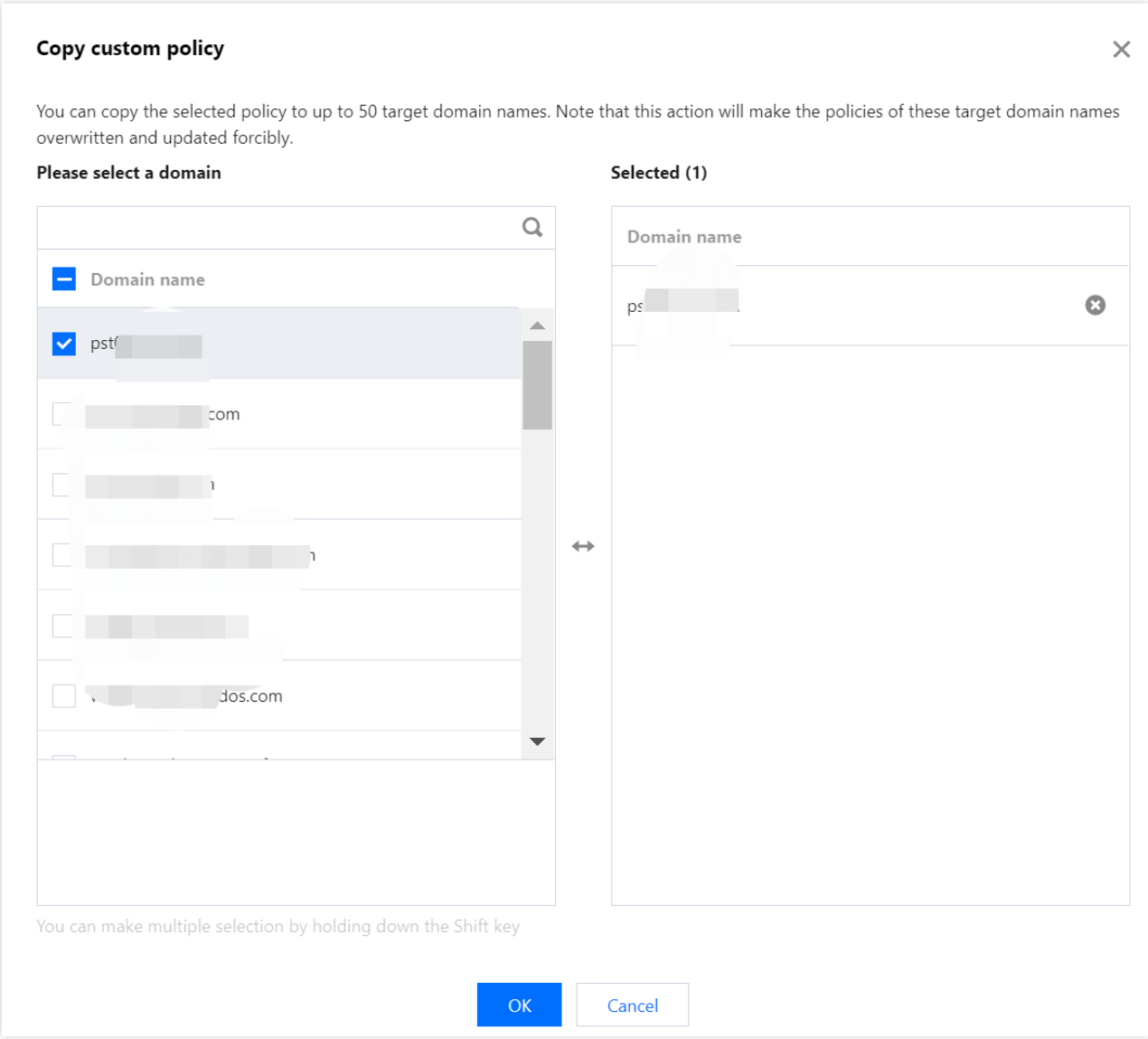


3. On the access control page, select the required policy, click **Copy**, and the custom policy copy window will pop up.

©2013-2022 Tencent Cloud. All rights reserved.



4. In the pop-up window, select a domain name and click **OK** to copy the rules to the target domain name.



©2013-2022 Tencent Cloud. All rights reserved.

Region Blocking

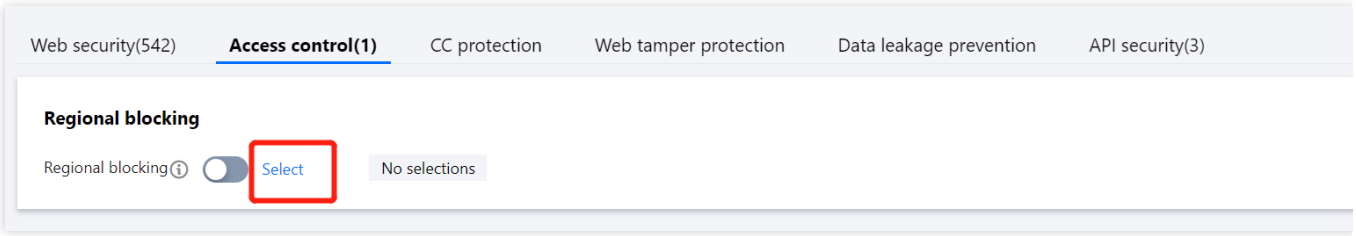
Last updated：2023-12-29 14:36:57

Overview

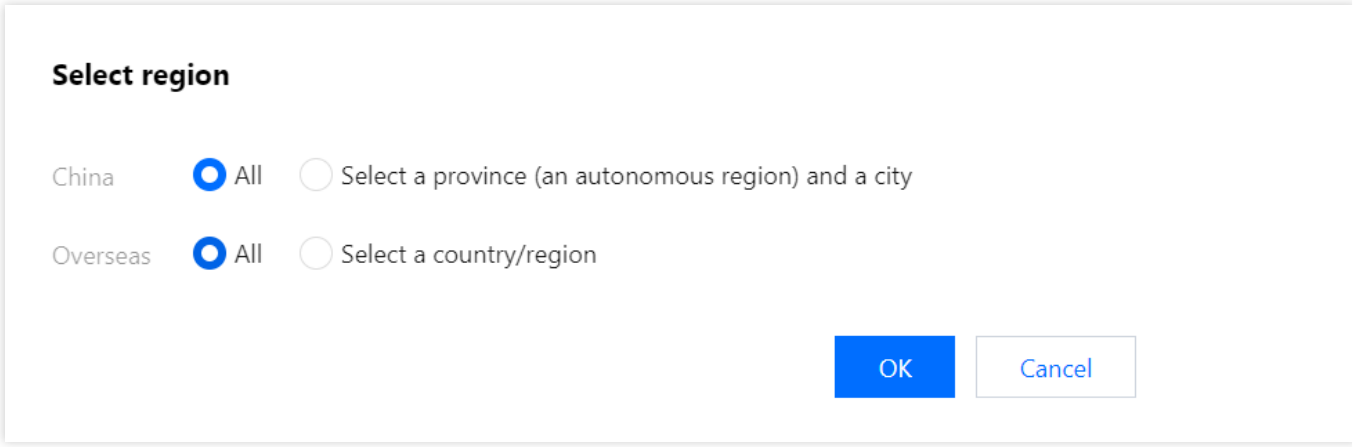
You can add regions to the blocklist to block all access sources from the specific regions.

Directions

1. Log in to the WAF console and select **Configuration Center** > **Basic Security** on the left sidebar.
2. On the basic security page, select the target domain name in the top-left corner and click **Access control**.
3. On the access control page, click **Edit** next to the region being blocked.



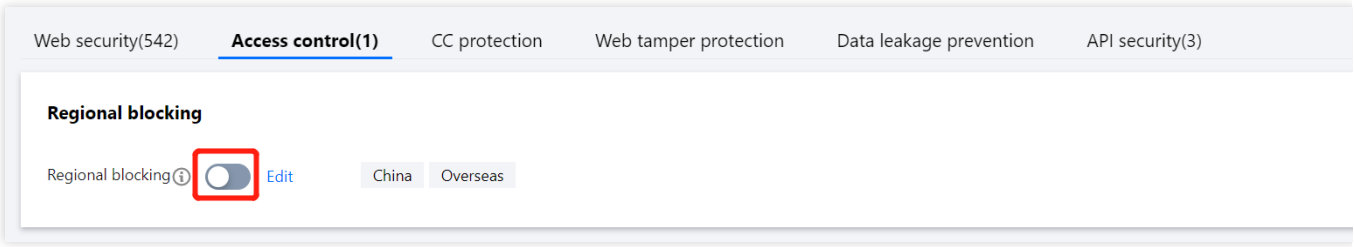
4. In the pop-up window, select the target region and click **OK**.



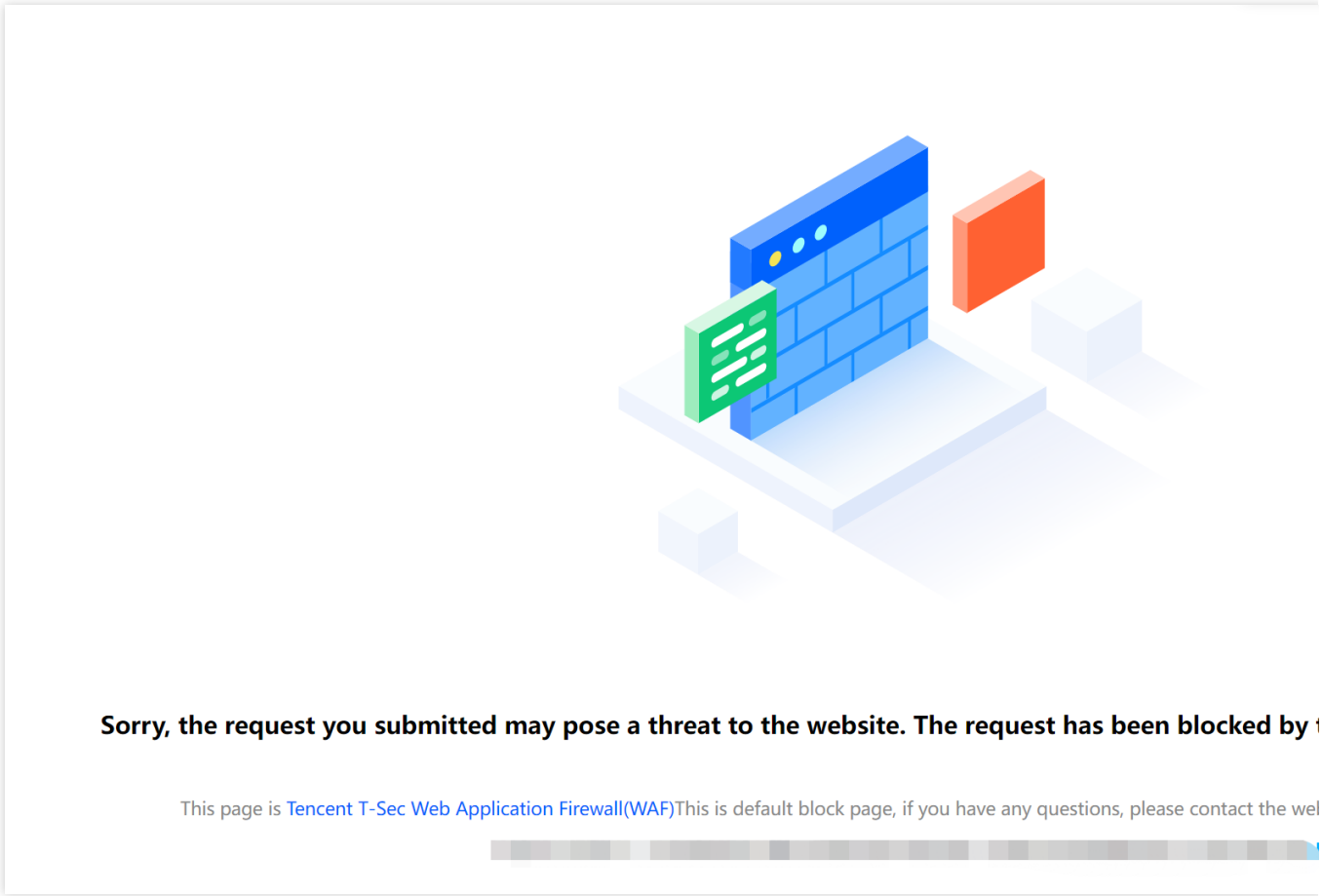
5. After saving the change, click

in **Region blocked** to enable region blocking.

©2013-2022 Tencent Cloud. All rights reserved.



6. Now you will be unable to visit your website from any of the blocked regions. For example, if you block all foreign regions, and visit a WAF-protected website with an overseas IP address, WAF will notify you that you have been blocked with an error page as shown below:



Supported Regions

The following regions are supported:

China

Region	Province/City/Autonomous Region

©2013-2022 Tencent Cloud. All rights reserved.

East China	Shandong, Jiangsu, Anhui, Zhejiang, Fujian, Jiangxi, Shanghai
South China	Guangdong, Guangxi, Hainan
Central China	Hubei, Hunan and Henan
North China	Beijing, Tianjin, Hebei, Shanxi, Inner Mongolia
Northwest China	Ningxia, Xinjiang, Qinghai, Shaanxi, Gansu
Southwest China	Sichuan, Yunnan, Guizhou, Tibet, Chongqing
Northeast China	Liaoning, Jilin, Heilongjiang
Hong Kong, Macao and Taiwan	Hong Kong, Macao and Taiwan

Other countries and regions

Continent	Country/Region
Asia	Azerbaijan, Armenia, Afghanistan, Bangladesh, Bahrain, Brunei, Bhutan, Cyprus, Cambodia, Timor-Leste, Georgia, Guernsey, India, Indonesia, Iran, Israel, Iraq, Japan, Jordan, Kazakhstan, Kuwait, Kyrgyzstan, Lebanon, Laos, Morocco, Mongolia, Myanmar, Maldives, Oman, Nepal, Palestine, Pakistan, Philippines, South Korea, Qatar, Sri Lanka, Syria, Saudi Arabia, Singapore, Thailand, Türkiye, Tajikistan, Turkmenistan, United Arab Emirates, Uzbekistan, Vietnam, Yemen, North Korea
Europe	Austria, Albania, Andorra, Belgium, Bulgaria, Belarus, Bosnia and Herzegovina, Czech Republic, Croatia, Denmark, Estonia, France, Finland, Faroe Islands, Germany, Greece, Gibraltar, Hungary, Italy, Ireland, Iceland, Isle of Man, Jersey, Lithuania, Latvia, Luxembourg, Liechtenstein, Moldova, Macedonia, the Republic of Malta, Montenegro, Monaco, Netherlands, Norway, Portugal, Poland, Switzerland, Sweden, Spain, Romania, Russia, Serbia, Slovenia, Slovakia, San Marino, United Kingdom, Ukraine, Vatican City
Africa	Algeria, Angola, Burkina Faso, Benin, Botswana, Burundi, Côte d'Ivoire, Cameroon, Democratic Republic of the Congo, Republic of the Congo, Cape Verde, Chad, Central Africa, Comoros, Djibouti, Egypt, Ecuador, Ethiopia, Equatorial Guinea, Ghana, Gabon, Gambia, Guinea, Guinea-Bissau, Kenya, Libya, Lesotho, Liberia, Morocco, Mauritius, Malawi, Mozambique, Madagascar, Mali, Mauritania, Niger, Namibia, Nigeria, South Africa, Rwanda, Reunion, Sudan, Seychelles, Somalia, Swaziland, Sierra Leone, Senegal, Sao Tome and Principe, South Sudan, Tunisia, Tanzania, Togo, Uganda, Zambia, Zimbabwe
Oceania	Australia, American Samoa, Cook Islands, Fiji Islands, French Polynesia, Guam, Federated States of Micronesia, New Zealand, Nauru, Mariana Islands, New Caledonia, Papua New Guinea, Palau, Saint Lucia, Samoa, Solomon Islands, Tonga, Tuvalu, Vanuatu
North America	Antigua and Barbuda, Anguilla, Barbados, Belize, Bahamas, Bermuda, Canada, Costa Rica,

©2013-2022 Tencent Cloud. All rights reserved.

	Cuba, Cayman Islands, Caribbean Netherlands, Dominica, El Salvador, Guatemala, Greenland, Guadero Puerto Rico, Grenada, Honduras, Haiti, Jamaica, Mexico, Martinique, Nicaragua, Puerto Rico, Panama, Saint Martin, Saint Vincent and the Grenadines, Saint Martin, Saint Kitts and Nevis, Trini Da and Tobago, Tajikistan, English Virgin Islands, Dominica, Turks and Caicos Islands, United States, United States Virgin Islands
South America	Argentina, Aruba, Brazil, Bolivia, Colombia, Chile, Curacao, French Guiana, Guyana, Paraguay, Peru, Suriname, Uruguay, Venezuela

©2013-2022 Tencent Cloud. All rights reserved.

CC Protection Rule Settings

Last updated：2023-12-29 14:41:22

Overview

CC protection can safeguard the access to specified URLs. CC protection settings 2.0 is upgraded with emergency CC protection and custom CC rules. Emergency CC protection can perform big data analysis on websites' access history and their real servers' exceptional response such as timeout and response delay, to generate protection policies for emergencies, blocking frequent access requests in real time. Custom CC rules support customizing protection rules based on user access source IPs or SESSION frequency to handle access by blocking, setting alarms, or verifying identity with CAPTCHA.

Note:

Emergency CC protection and custom CC rules cannot be enabled at the same time.

SESSION must be set before using the session-based CC protection policy.

Slow Attack Protection: When forwarding traffic, web application firewalls aggregate and clean slow requests, providing a certain level of slow attack protection capabilities.

Slow Attack Protection

Slowloris, RUDY, and other slow attacks are techniques that slow down server response times, typically by sending a large number of slow or incomplete requests to consume server resources, preventing normal users from accessing web applications.

When forwarding traffic, web application firewalls aggregate and clean slow requests by default, providing slow attack protection capabilities and the ability to clean slow attacks similar to Slowloris.

When a web application firewall cleans slow requests, HTTP protocol type requests will return a status code of 400, while TCP protocol type requests will return a TCP RST.

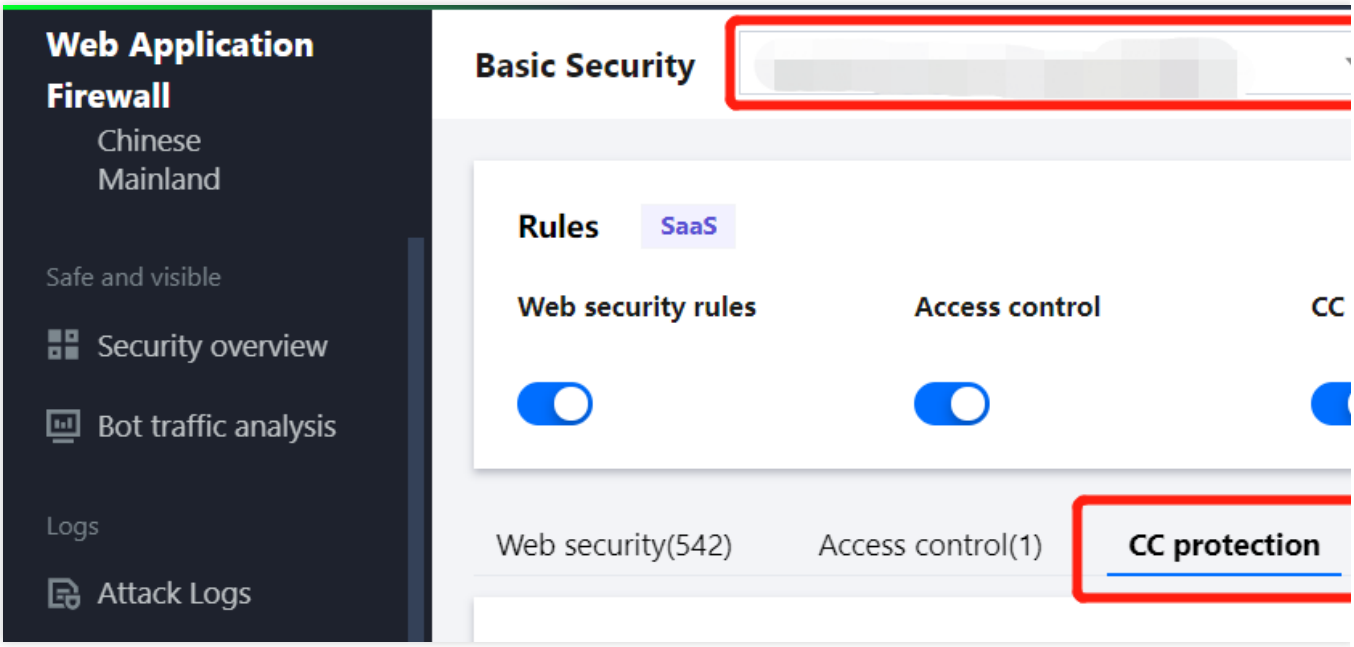
Directions

Example 1: Emergency CC protection settings

Emergency CC protection is disabled by default. Before enabling it, please make sure that the custom CC rule feature is disabled.

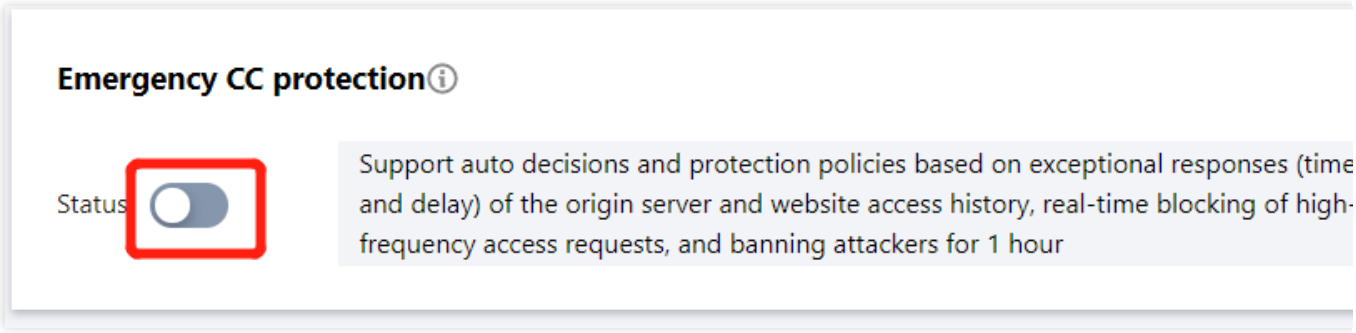
1. Log in to the WAF console and select **Configuration Center** > **Basic Security** on the left sidebar.
2. On the basic security page, select the target domain name in the top-left corner and click **CC Protection**.

©2013-2022 Tencent Cloud. All rights reserved.



3. Click

in the emergency CC protection module and confirm the operation to configure emergency CC protection.



Configuration item description:Status switch: After emergency CC protection is enabled, if a website is under massive CC attacks (with a website QPS of 1000 or above), the protection will be automatically triggered. If there are no specific protection paths, we recommend enabling emergency CC protection. As there may be some false alarms, you can click IP Query on the left sidebar to view the information of blocked IPs and handle them in time.

Note:

If there are specific protection paths, we recommend using custom CC rules.

CLB WAF does not support emergency protection. We recommend using custom CC protection.

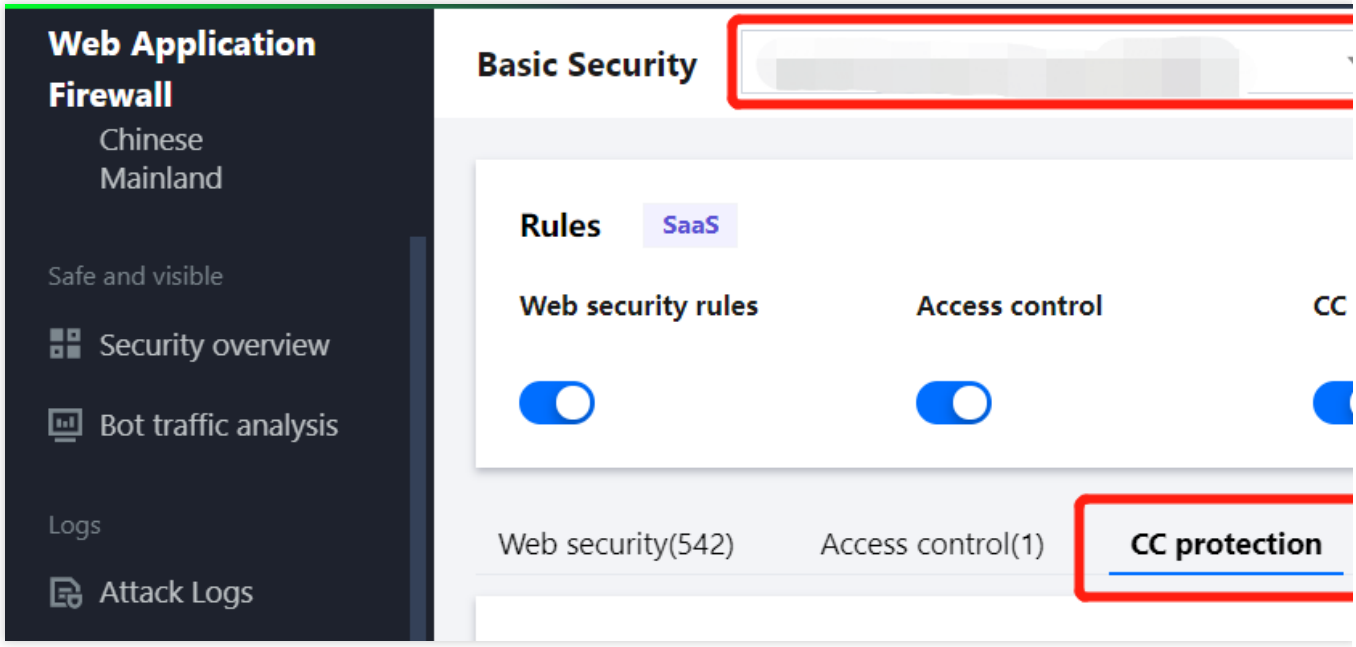
Example 2: Access source IP-based CC protection settings

An IP-based CC protection policy can be directly configured without setting SESSION.

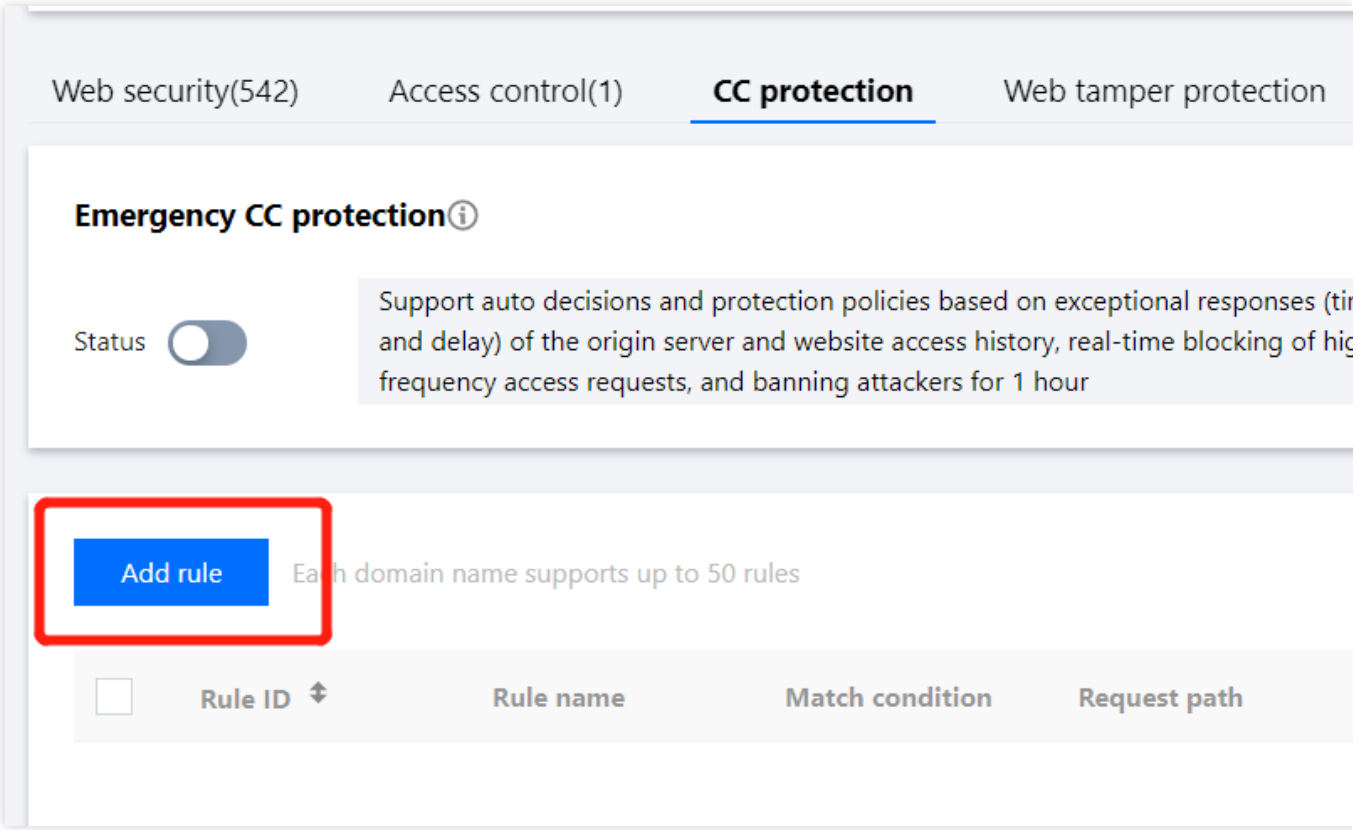
1. Log in to the WAF console and select **Configuration Center** > **Basic Security** on the left sidebar.

©2013-2022 Tencent Cloud. All rights reserved.

2. On the basic security page, select the target domain name in the top-left corner and click **CC Protection**.

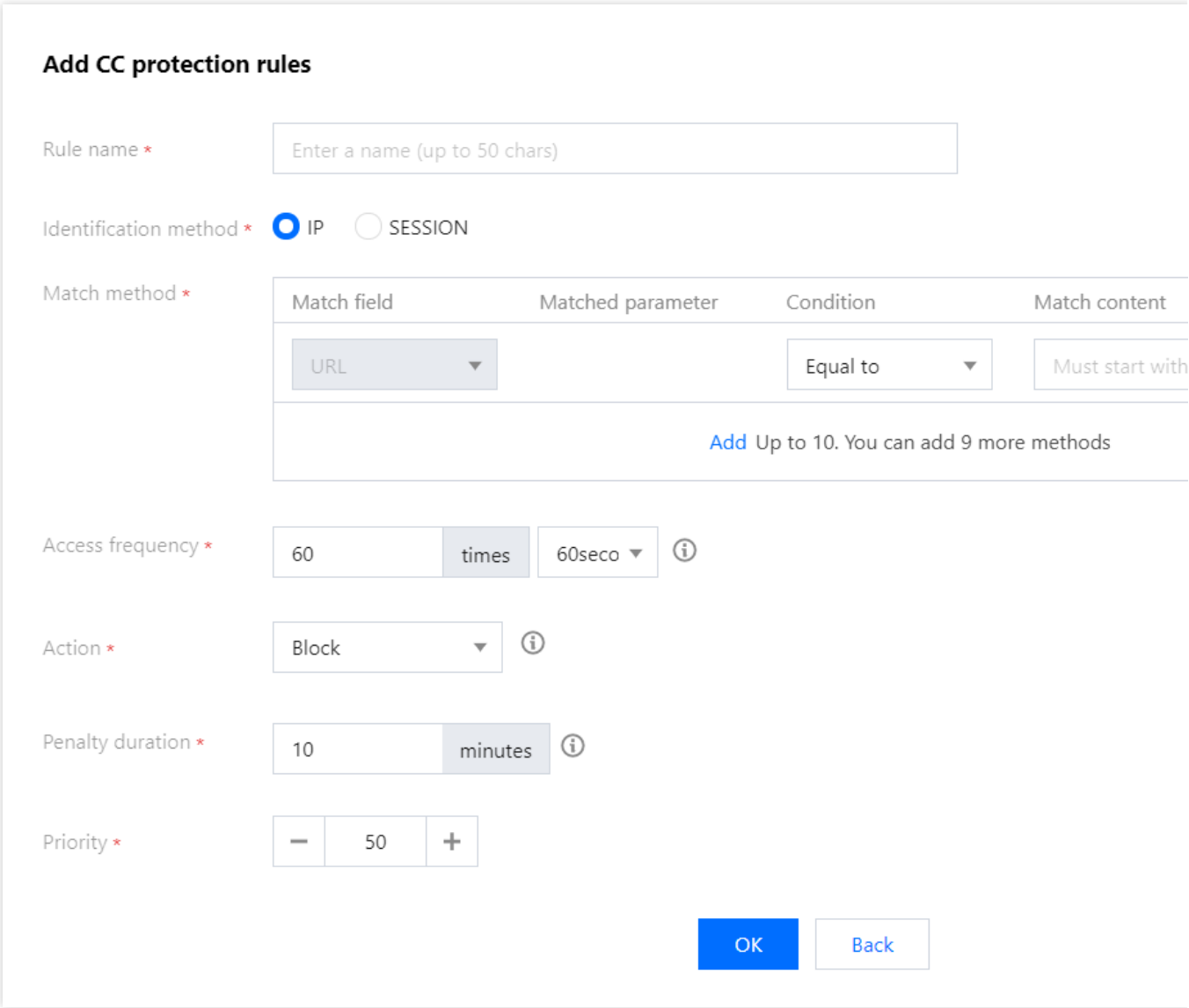


3. On the CC protection page, click **Add rule**, and the rule adding window will pop up.



4. In the pop-up window, configure relevant parameters and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Field description:

Rule name: Name of the CC protection rule. It can contain up to 50 characters.

Recognition mode: It supports two modes: IP recognition (default) and SESSION recognition. To use SESSION recognition, you need to set the SESSION position first.

Match method: It specifies the match parameter, logical operator and match content to control access frequency. The match parameter defaults to URL. For the same rule, you can set up to 10 conditions with the logical AND operator, which should contain at least one URL condition. The fields are described as follows:

Match Field	Match Parameter	Logical Operators	Match Content Description
URL	N/A	Equal to Include Prefix match	Required. The URL prefixed with "/" can contain up to 128 characters, which can

©2013-2022 Tencent Cloud. All rights reserved.

			be a directory or specific path.
Method	N/A	Equal to Include Not equal to	Values: `HEAD`, `GET`, `POST`, `PUT`, `OPTIONS`, `TRACE`, `DELETE`, `PATCH` and `CONNECT`. You can specify a method as needed.
Query	Key value in the `Query` parameter	Equal to	Required. The key value can contain up to 512 characters, which can be set multiple times.
Referer	N/A	Equal to Include Prefix match	The value can contain up to 512 characters.
Cookie	Key value in the `Cookie` parameter	Equal to Include Not equal to	Required. The key value can contain up to 512 characters.
User-Agent	N/A	Equal to Include Not equal to	The value can contain up to 512 characters.
Custom request header	Request header key value, such as Accept, Accept-Language, Accept-Encoding, and Connection.	Equal to Include Not equal to Blank Not exist	The key value can contain up to 512 characters, which can be set multiple times. If the matching content is blank or does not exist, you can directly enter the matching parameter.

Access frequency: sets the access frequency based on actual business requirements. We recommend setting a value 3 to 10 times the normal access frequency. For example, if your website is accessed 20 times per minute per visitor, you can set the access frequency to 60 to 200 times per minute, which can be further adjusted based on the attack severity.

Action: Defaults to "Block". You can set this field as needed. The detailed field description is as follows:

Action Type	Description
Observe	Session requests that meet the specified conditions will be monitored and logged. You

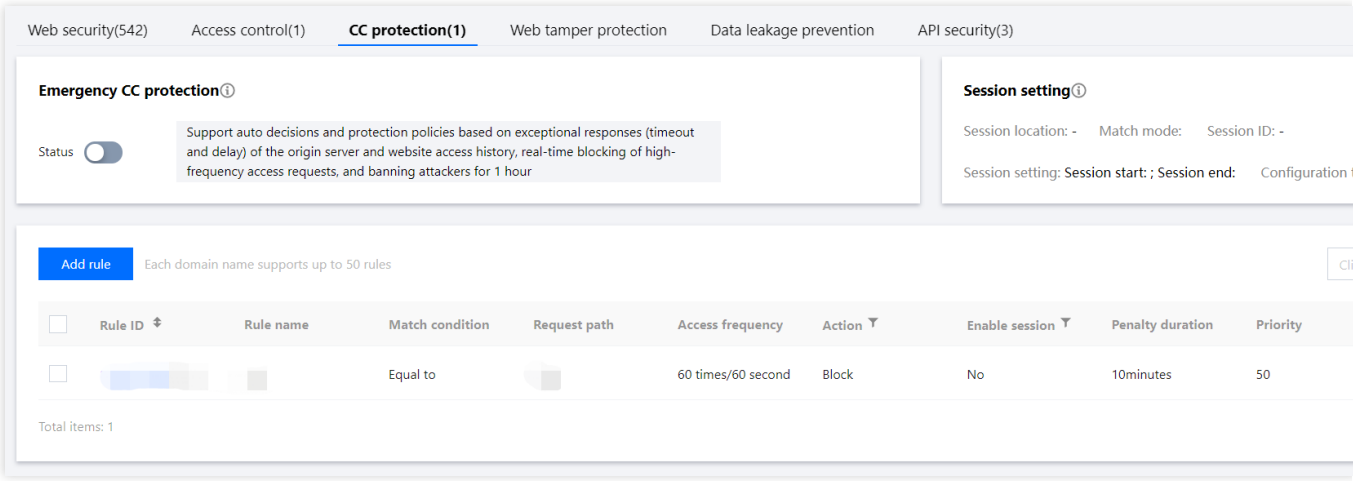
©2013-2022 Tencent Cloud. All rights reserved.

	can check the records in Attack Logs.
CAPTCHA	This is applicable only to the access through browsers. Session requests that match the specified conditions will be verified through CAPTCHA. If they fail, they will be blocked. Otherwise, they can normally access within the penalty period. CAPTCHA logs will be observed.
Precise block	Access requests that match the specified frequency control rules will be blocked precisely, indicating that the specific IP, instead of the domain name, will be blocked from accessing the protected URL within the penalty period ranging from 5 minutes to 10,080 minutes (7 days). You can view the blocking results in Attack Logs.
Block	Access requests that match the set frequency control rules will be blocked, indicating that the specific IP will be blocked from accessing all URLs within the penalty period ranging from 5 minutes to 10,080 minutes (7 days). You can view the blocking results in Attack Logs and check the blocked IPs in real time in IP Query.

Penalty duration: It ranges from 1 minute to 1 week. Default: 10 minutes.

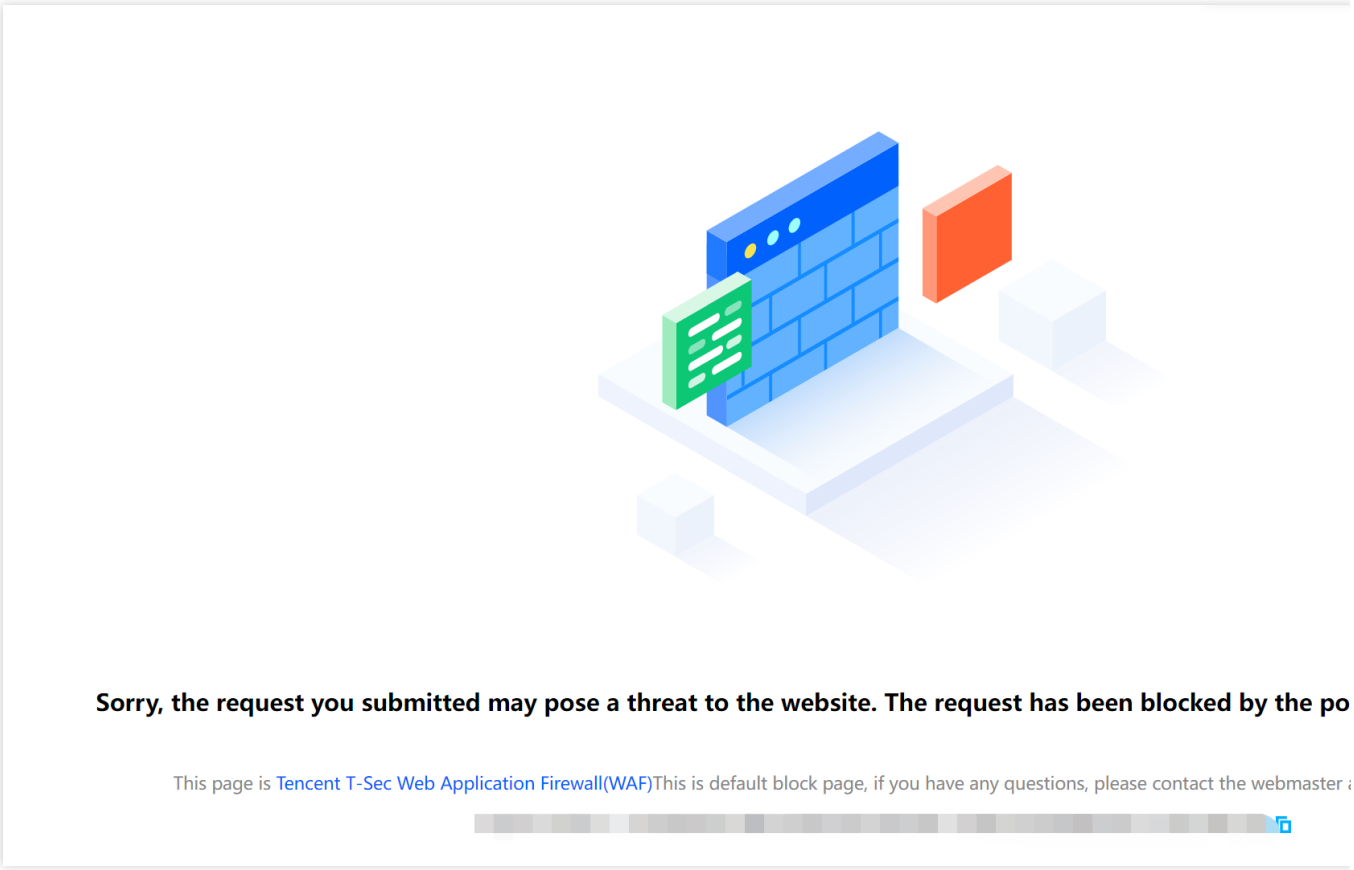
Priority: Enter an integer from 1 to 100 (default: 50). The smaller the value, the higher the priority of this rule. For rules with the same priority, the last created one will be used.

5. You can select a created rule to disable, modify, or delete it.



6. Conduct test CC attacks based on the rule settings.

©2013-2022 Tencent Cloud. All rights reserved.



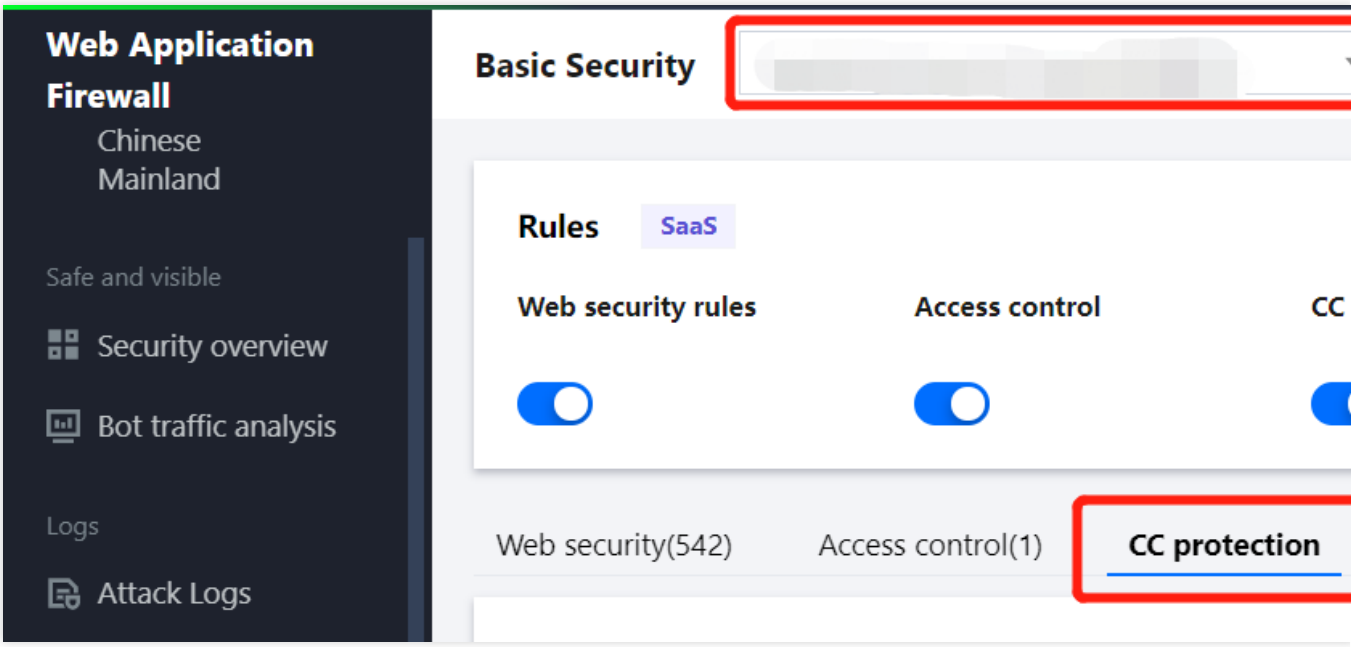
7. You can add IPs to the blocklist/allowlist on the blocklist/allowlist page and view the blocking information on the IP query page.

Example 3: Session-based CC protection settings

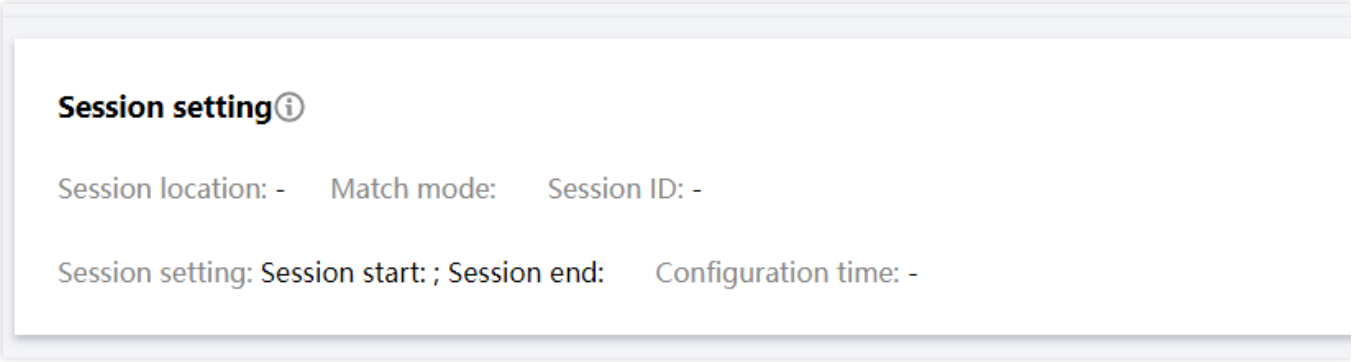
CC protection based on session access frequency effectively resolves false positive problems that may occur when the same IP egress is used by multiple users in office buildings, stores, supermarkets, and other public Wi-Fi networks.

1. Log in to the WAF console and select **Configuration Center** > **Basic Security** on the left sidebar.
2. On the basic security page, select the target domain name in the top-left corner and click **CC protection**.

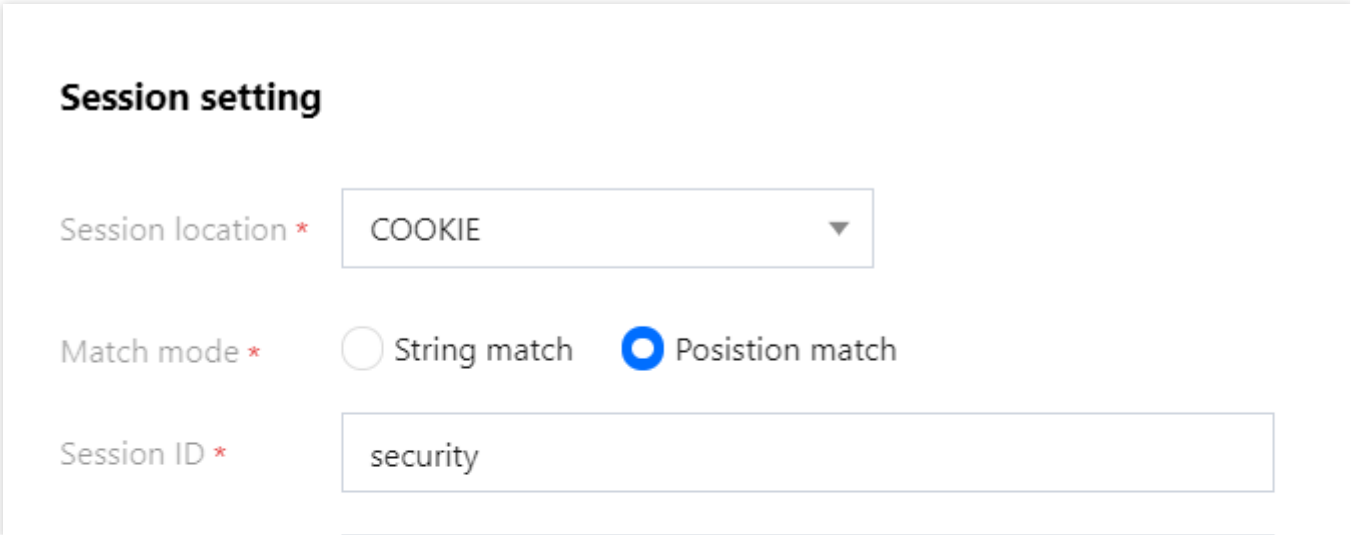
©2013-2022 Tencent Cloud. All rights reserved.



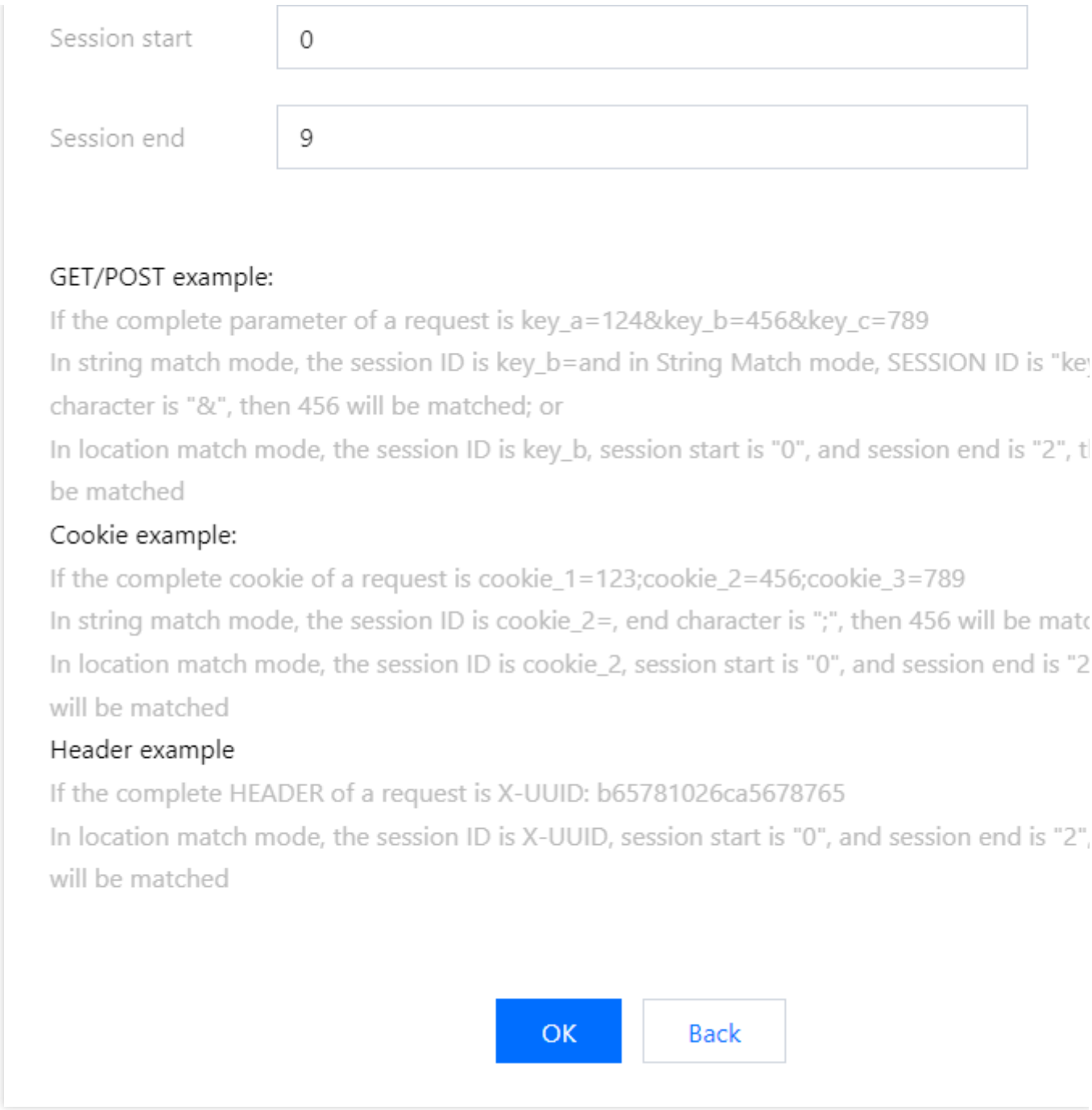
3. Click **Settings** in SESSION settings and the SESSION settings window will pop up.



4. In the pop-up window, enter the required information. In this example, a cookie is used as the test object, whose ID is `security`, start position is `0`, and end position is `9`. After completing the settings, click **OK**.



©2013-2022 Tencent Cloud. All rights reserved.



Field description:

Session position: "COOKIE", "GET", or "POST". GET and POST are HTTP request content parameters rather than HTTP header information.

Match mode: It supports two modes: position match and string match.

Session ID: ID of the session.

Start position: Position where string or position match starts.

End position: Position where string or position match ends.

GET/POST example:

Assume that the complete parameter content in a request is `key_a = 124&key_b = 456&key_c = 789` , then:

©2013-2022 Tencent Cloud. All rights reserved.

In string match mode, if the session ID is `key_b =` , and the end character is `&` , then the matched content will be `456` .
In position match mode, if the session ID is `key_b` , the start position is `0` , and the end position is `2` , then the matched content will be `456` .

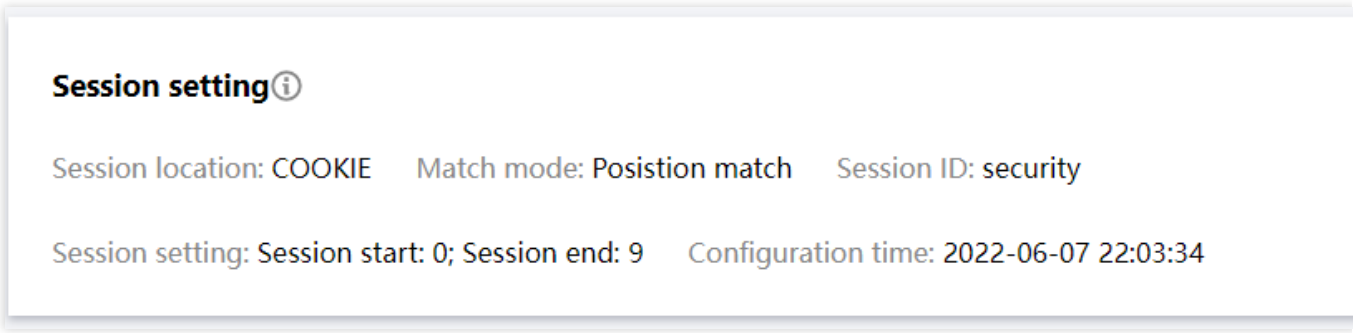
COOKIE example:

Assume that the complete cookie content in a request is `cookie_1 = 123;cookie_2 = 456;cookie_3 = 789` , then:
In string match mode, if the session ID is `cookie_2 =` , and the end character is `;` , then the matched content will be `456` .
In position match mode, if the session ID is `cookie_2` , the start position is `0` , and the end position is `2` , then the matched content will be `456` .

HEADER example:

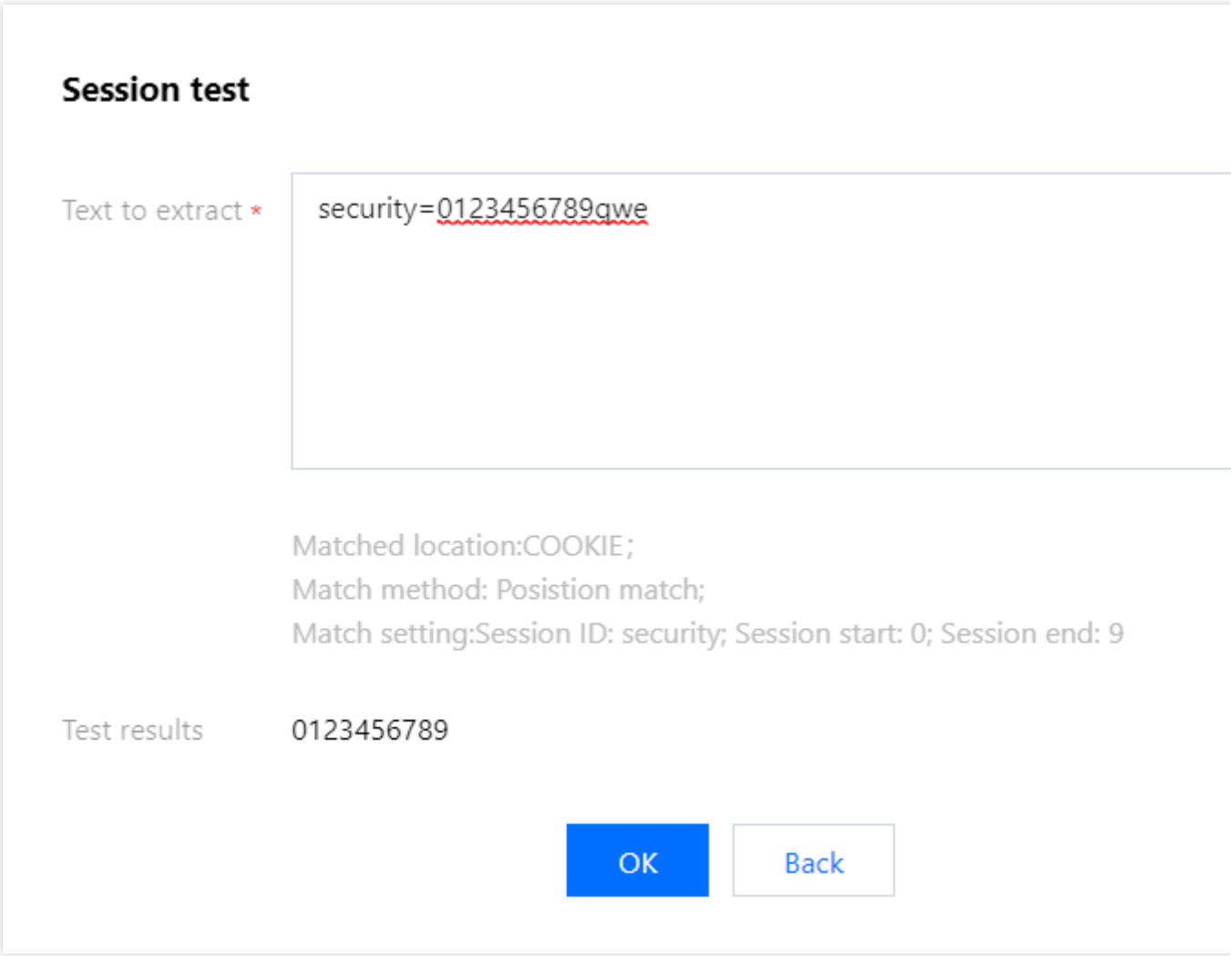
Assume that the complete header content in a request is `X-UUID: b65781026ca5678765` , then:
In position match mode, if the session ID is `X-UUID` , the start position is `0` , and the end position is `2` , then the matched content will be `b65` .

5. Click **Test**, enter relevant content, and click **OK** to test the session information.



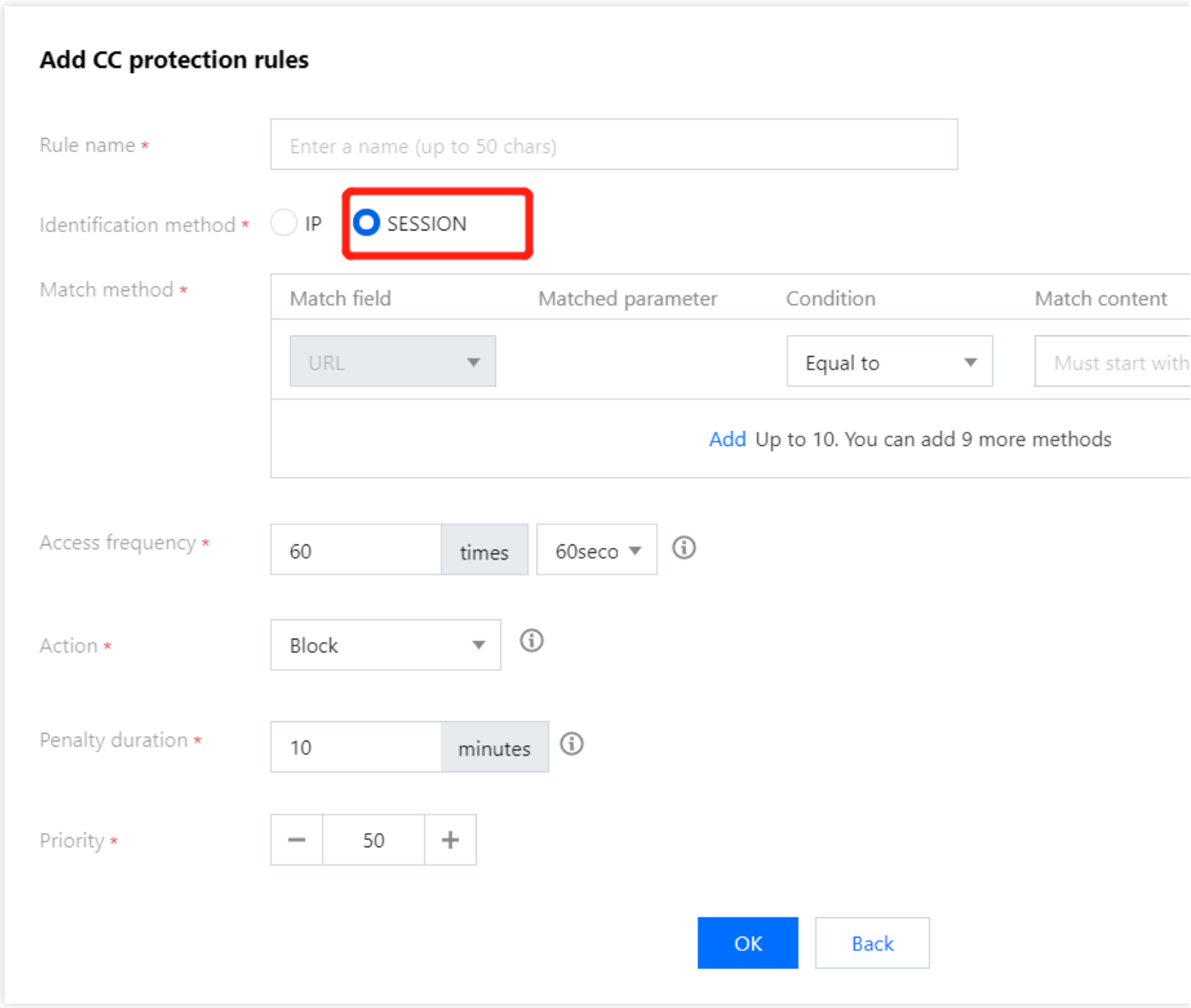
6. Go to the SESSION settings page and set the content to `security = 0123456789` . Then, WAF will use the 10 characters following `security` as the session ID. You can also delete or reconfigure the session information.

©2013-2022 Tencent Cloud. All rights reserved.



7. Set a session-based CC protection policy as instructed in Example 1, but select "SESSION" as the recognition mode.

©2013-2022 Tencent Cloud. All rights reserved.



8. After the configuration is completed, the session-based CC protection policy will take effect.

Note:

If you use session-based CC protection, you cannot view IP blocking information in the IP blocking status section.

©2013-2022 Tencent Cloud. All rights reserved.

Web Tamper Protection

Last updated：2023-12-29 14:41:42

This document describes the tamper protection feature of WAF. It is used to protect core static webpages. By caching pages and locking access requests, it protects your website from being affected by malicious tampering with your real server pages. In addition, you can also configure tamper protection rules as needed.

Overview

With the tamper protection feature, you can add protection rules to protect core webpages from being tampered with as needed. You can refresh the protected pages, during which WAF will update them to ensure that they are the same as those on the real server. Moreover, you can also choose whether to retain rule hit logs to analyze hit conditions.
Note:
CLB WAF doesn't support the tamper protection feature. For more information on detailed specifications, see Billing Overview.

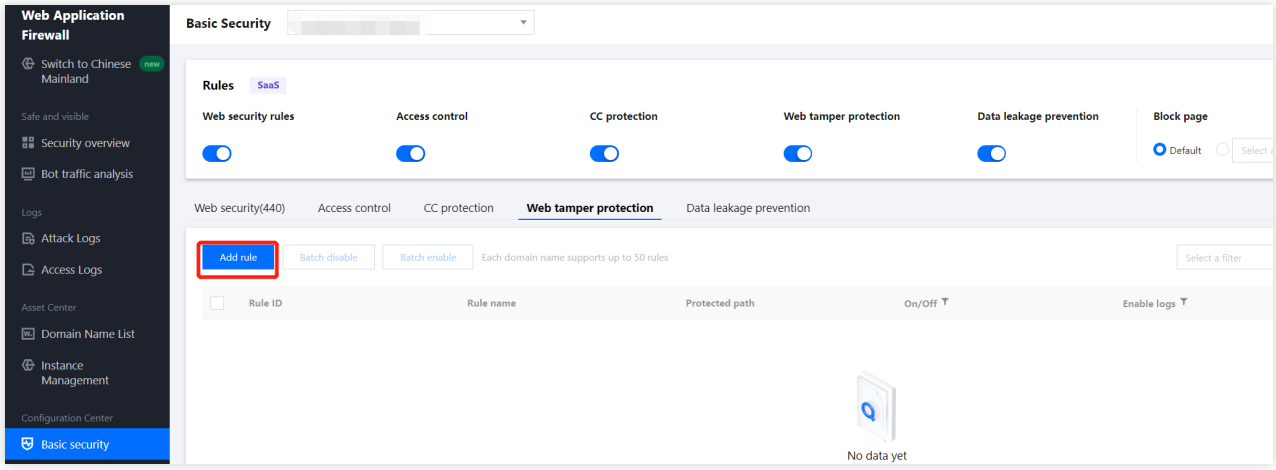
Prerequisites

You have added a protected domain name to SaaS WAF, and ensured the domain name is in normal protection.

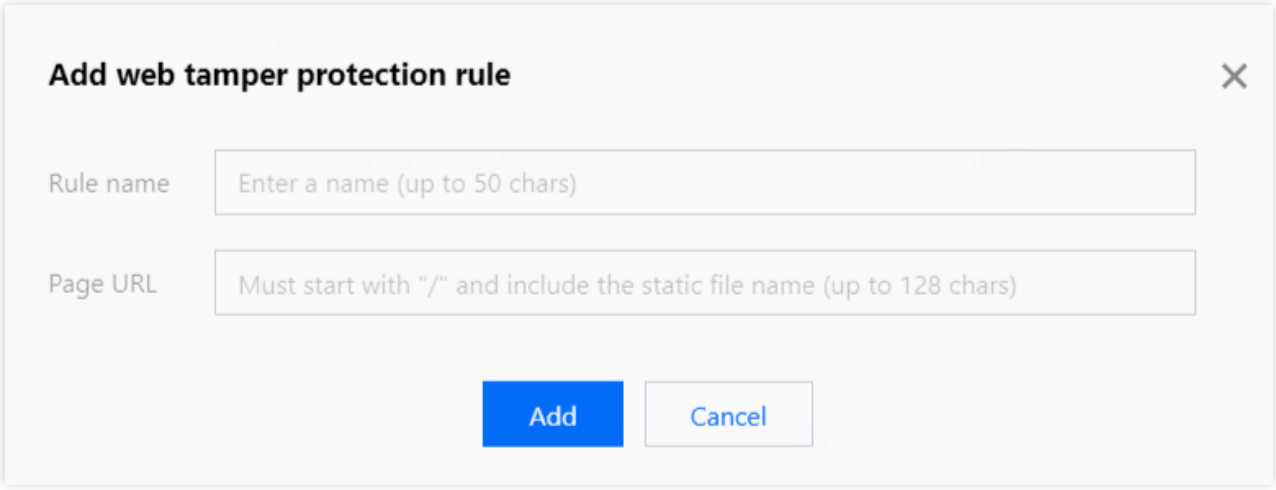
Adding Rules

1. Log in to the WAF console and select **Configuration Center** > **Basic Security** on the left sidebar.
2. On the basic security page, select the target domain name in the top-left corner and click **Web tamper protection**.
3. On the tamper protection page, click **Add rule**, and the rule adding window will pop up.

©2013-2022 Tencent Cloud. All rights reserved.



4. In the pop-up window, configure relevant fields and click **OK**.



Field description:

Rule name: Tamper protection rule name of up to 50 characters. You can search for rules by name in attack logs.

Page path: Path of the page to be protected from tampering. You need to enter a specific URL rather than a path.

Note:

The specified page is limited to static resources such as .html, .shtml, .txt, .js, .css, .jpg, and .png.

After the rule is added, when a user accesses this page for the first time, WAF will cache the page, and subsequent access requests will be directed to the WAF-cached page.

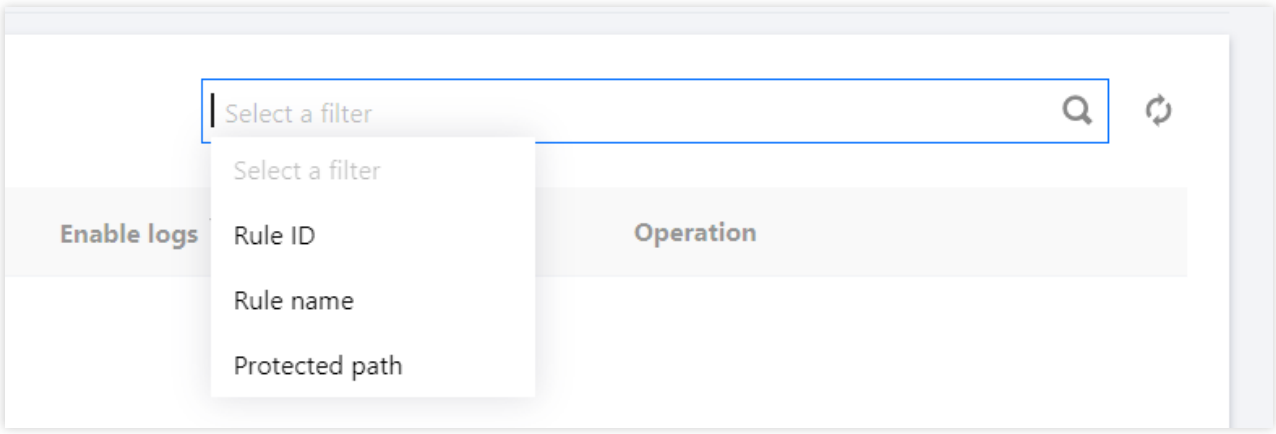
5. After the tamper protection rule is added, it will be enabled by default.

Searching Rules

1. On the basic security page, select the target domain name in the top-left corner and click **Tamper Protection**.

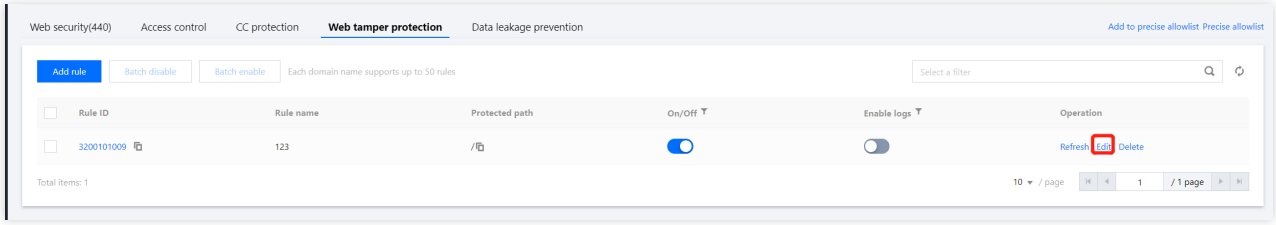
©2013-2022 Tencent Cloud. All rights reserved.

2. On the tamper protection page, click the search box to filter rules by keywords such as rule ID, rule name, and protection path.



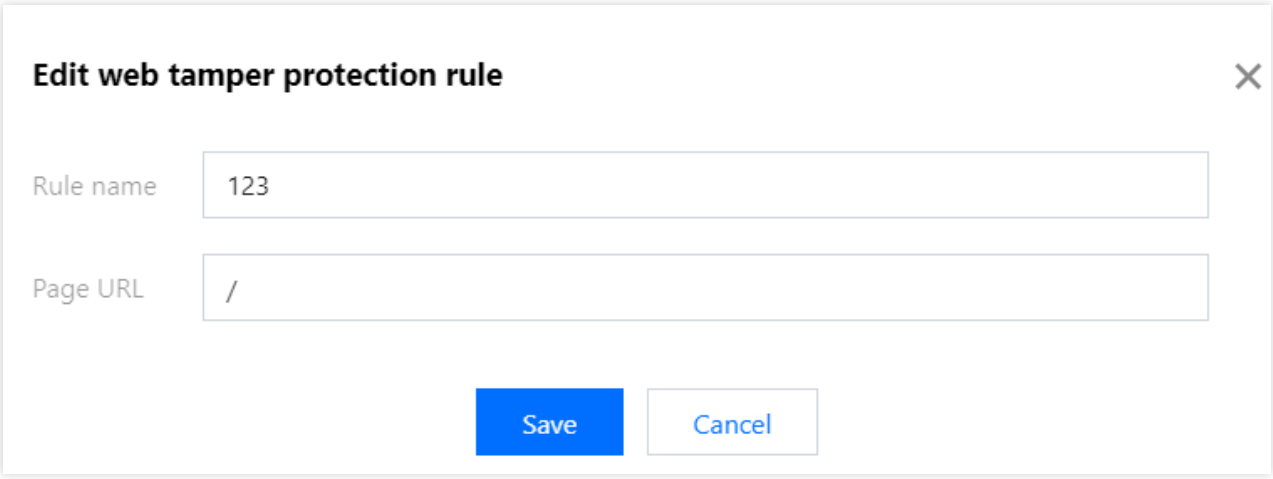
Editing Rules

1. On the basic security page, select the target domain name in the top-left corner and click **Web tamper protection**.
2. On the tamper protection page, select the target rule, click **Edit** in the **Operation** column, and the rule editing window will pop up.



3. In the pop-up window, modify relevant parameters and click **Save**.

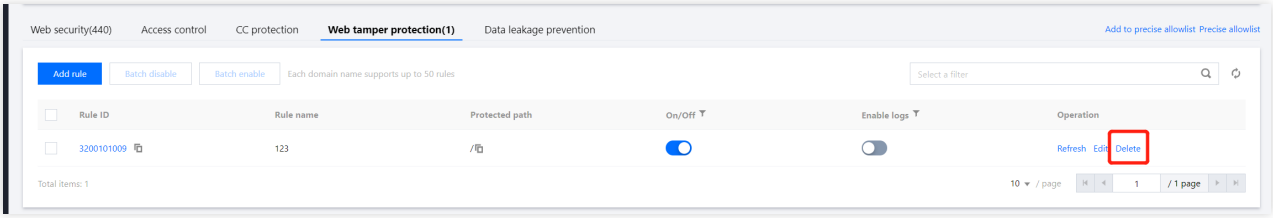
©2013-2022 Tencent Cloud. All rights reserved.



4. After the protected page is updated, click **Refresh** to cache the updated page to WAF.

Deleting Rules

1. On the basic security page, select the target domain name in the top-left corner and click **Web tamper protection**.
2. On the tamper protection page, select the target rule, click **Delete** in the **Operation** column, and the deletion confirmation window will pop up.



3. In the pop-up window, click **Delete**.

Note:

Once deleted, it cannot be restored and takes effect only after being added again.

©2013-2022 Tencent Cloud. All rights reserved.

Data Leakage Protection

Last updated：2023-12-29 14:41:57

This document describes the information leakage protection feature of WAF. It can filter and then replace, mask, and block sensitive information (e.g., identity card/mobile/bank card numbers), keywords, and response codes returned by websites. This helps meet the requirements of data security protection and cybersecurity classified protection by setting leakage protection rules as needed.

Overview

With the leakage protection feature, you can add protection rules to filter the content returned by websites as needed, such as identity card/mobile/bank card numbers. You can also customize keywords (regex is supported) to filter order numbers and addresses and completely or partially replace them. Moreover, you can block or trigger alarms for status codes other than 200 returned by websites to meet compliance requirements.

Note:

CLB WAF doesn't support the data leakage protection feature. For more information on detailed specifications, see Billing Overview.

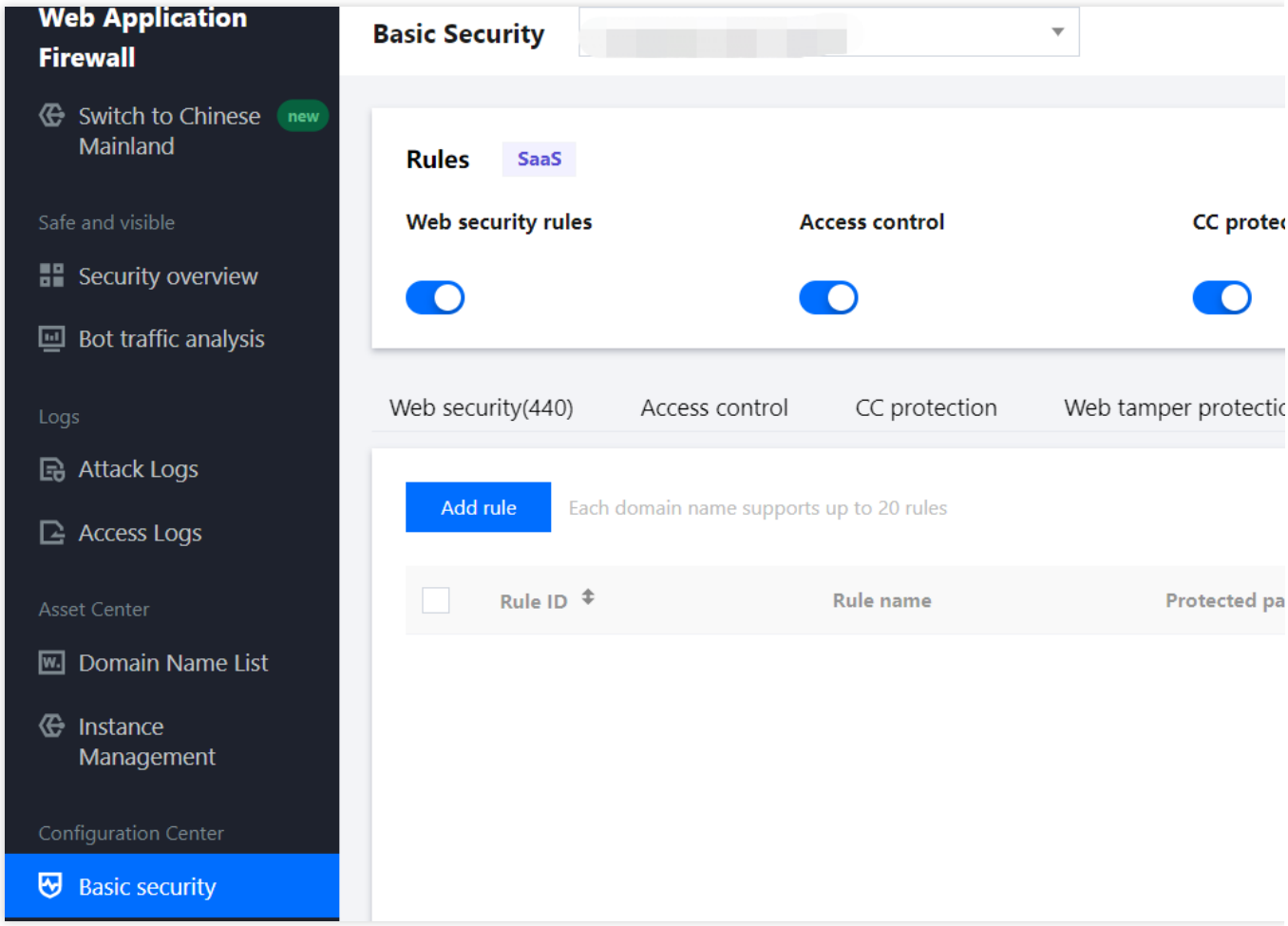
Prerequisites

You have added a protected domain name to SaaS WAF, and ensured the domain name is in normal protection.

Adding a Rule

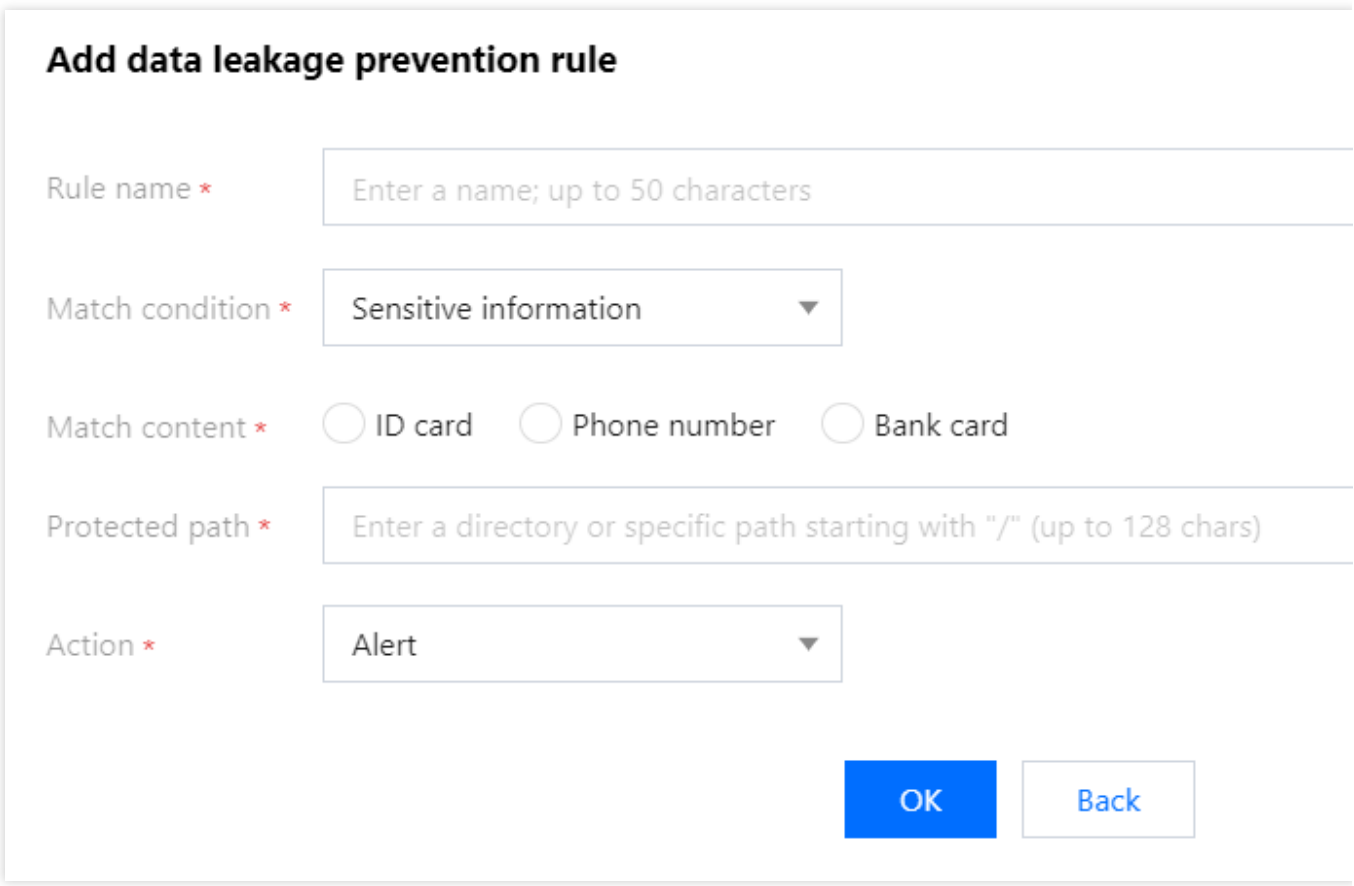
1. Log in to the WAF console and select **Configuration Center** > **Basic Security** on the left sidebar.
2. On the basic security page, select the target domain name in the top-left corner and click **Data leakage prevention**.
3. On the page displayed, click **Add rule**, and the rule adding window will pop up.

©2013-2022 Tencent Cloud. All rights reserved.



4. In the pop-up window, configure relevant fields and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Field description:

Rule name: Leakage protection rule name of up to 50 characters. You can search for rules by name in attack logs.

Condition: Match condition for leakage protection. You can select sensitive information, keyword, or response code, and the match content and action type vary by the condition as follows:

Condition	Content	Action
Sensitive information	Identity card/mobile/bank card numbers	Alert, Replace all, Show the last 4 digits, Show the first 4 digits, and Block
Keyword	Keyword and regex	Alert, Replace all, and Blcok
Response code	400, 403, 404, other 4XX codes, 500, 501, 502, 504, and other 5XX codes	Alert and Block

Content: The match content varies by match condition.

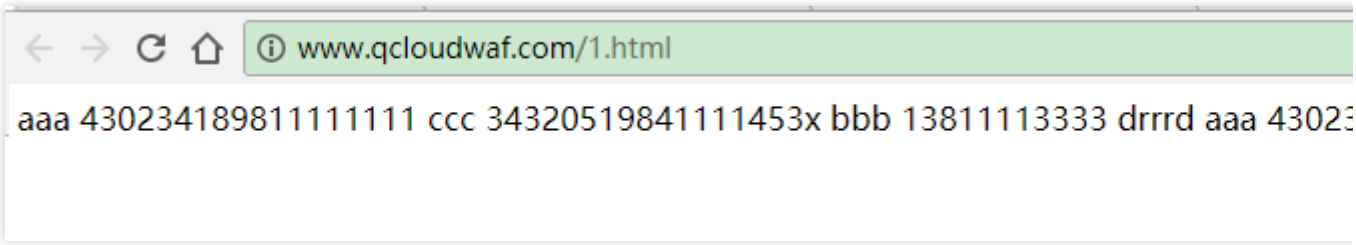
Protected path: Specific path where the information needs to be protected from leakage. You can enter a directory or specific path as needed.

Action: Action to be executed after the match condition is hit. You can view the relevant hit information in attack logs.

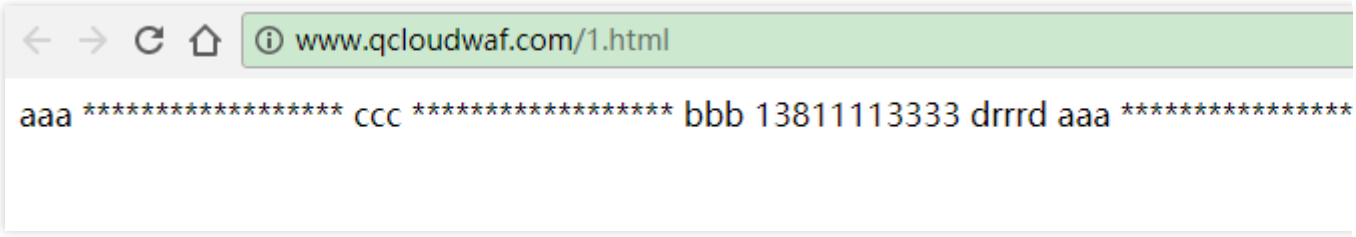
©2013-2022 Tencent Cloud. All rights reserved.

5. Once the rule takes effect, it will begin protecting the sensitive information returned in your web pages as shown in the following example that performs the Replace action (demo content):

Before protection is enabled:



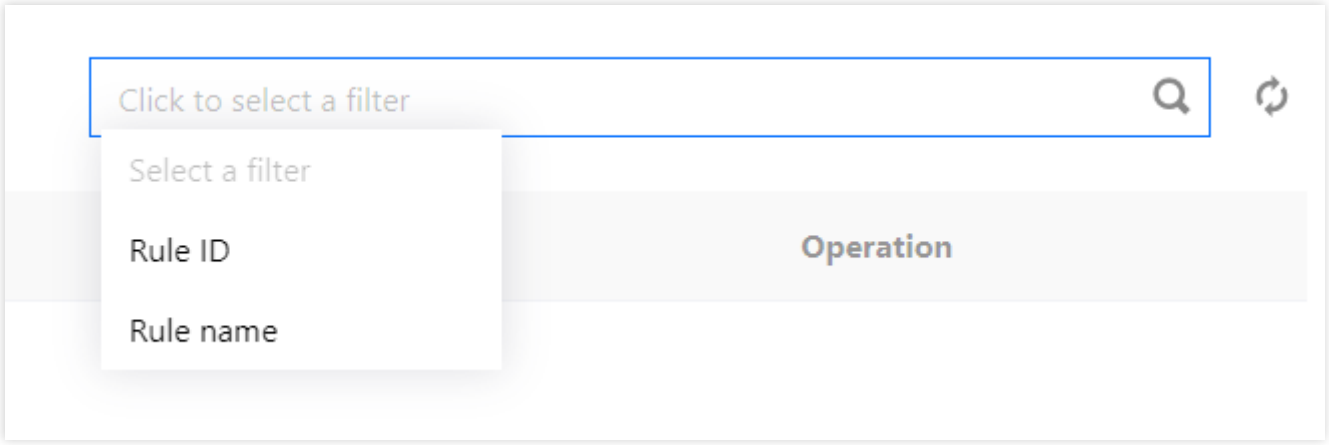
After protection is enabled:



Search rules

1. On the basic security page, select the target domain name in the top-left corner and click **Data leakage prevention**.

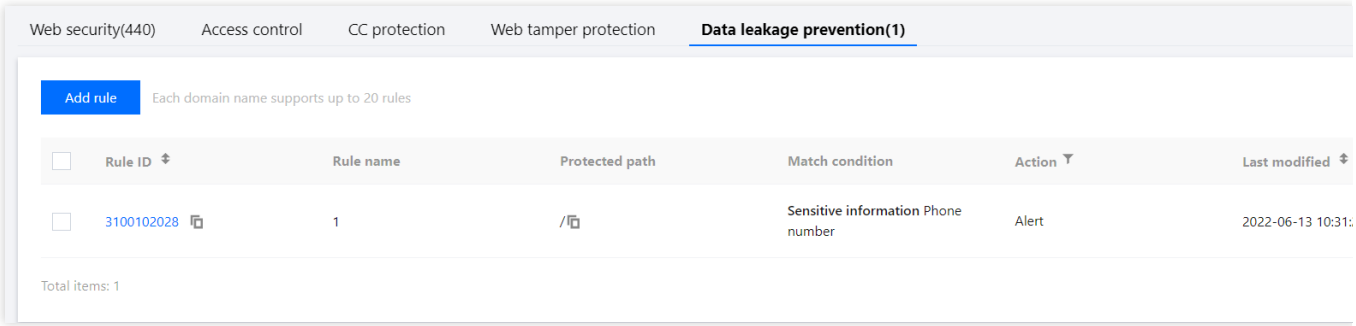
2. On the page displayed, click the search box to filter rules by keywords in a rule ID, rule name, and protected path.



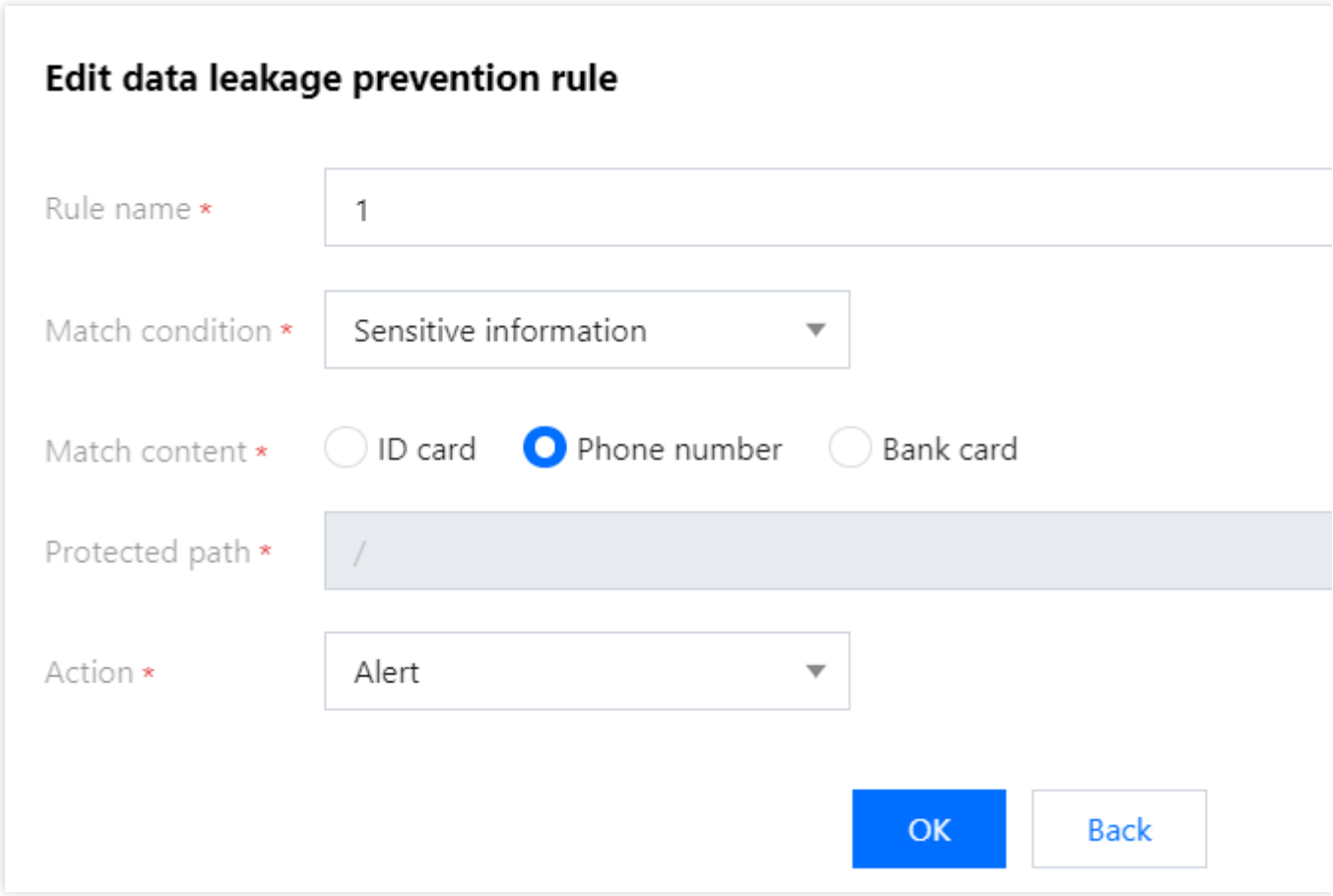
©2013-2022 Tencent Cloud. All rights reserved.

Editing a Rule

1. On the basic security page, select the target domain name in the top-left corner and click **Data leakage prevention**.
2. On the page displayed, select the target rule, click **Edit** in the **Operation** column, and the rule editing window will pop up.



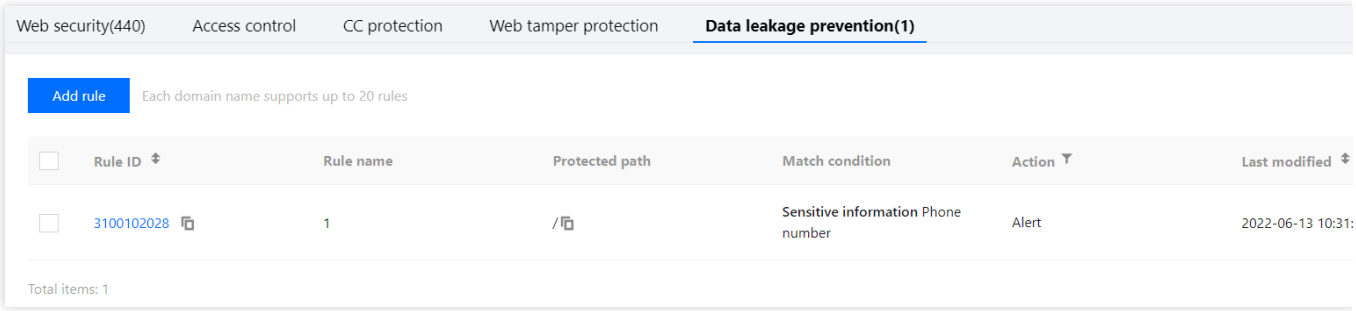
3. In the pop-up window, modify relevant parameters and click **OK**.



©2013-2022 Tencent Cloud. All rights reserved.

Deleting a Rule

1. On the basic security page, select the target domain name in the top-left corner and click **Data leakage prevention**.
2. On the page displayed, select the target rule, click **Delete** in the **Operation** column, and the deletion confirmation window will pop up.



3. In the pop-up window, click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.

API Security

Last updated：2023-12-29 14:42:13

This document describes how to add APIs or API rule files using the API security feature to protect your APIs.

Overview

Using API security, you can add APIs or API rule files, so that WAF will run security checks on the API requests and allow the APIs that meet specified requirements. This module provides protection for APIs by cooperating with the AI engine and bot traffic management modules.

Directions

1. Log in to the WAF console and select **Configuration Center** > **Basic Security** on the left sidebar.
2. On the page displayed, select a target domain name in the upper-left corner, and click **API security**.
3. On the API security page, you can add API security rules by either importing APIs or adding APIs.

Note:

Import API (recommended): You need to import an API file that meet the specified requirements.

Add API: You need to add the API path of a website manually.

Importing APIs (recommended)

1. Select **Basic Security** > **API security**. On the page that appears, click **Import API**.
2. In the pop-up window, select a file to upload, and click **Upload**.

Note:

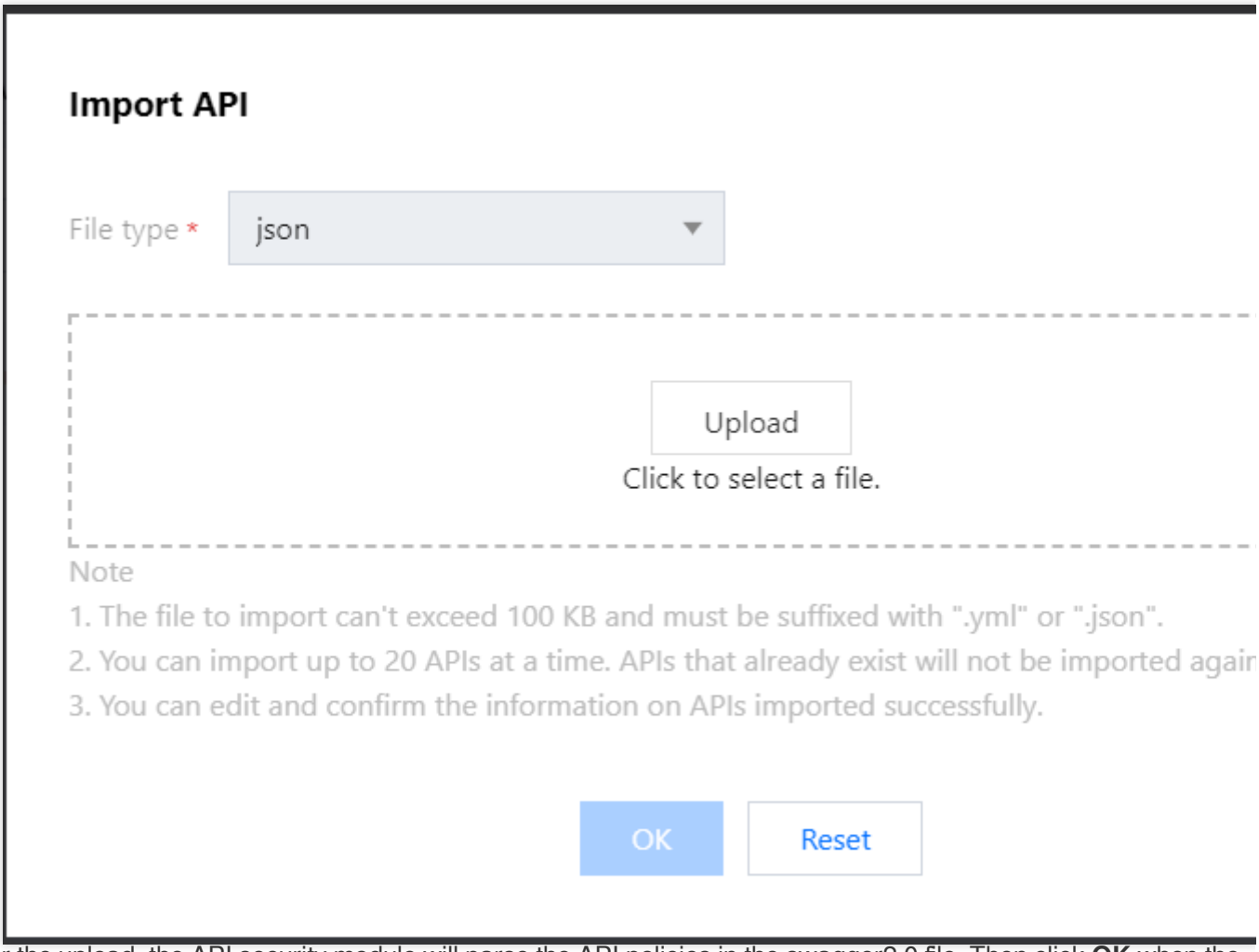
WAF provides support for parsing swagger2.0 files in YML and JSON formats. The file to import should satisfy the following requirements:

Format: The API description file must be suffixed with .yml or .json. The file size cannot exceed 100 KB.

Count: Up to 20 APIs can be imported at a time. APIs that already exist will not be imported again.

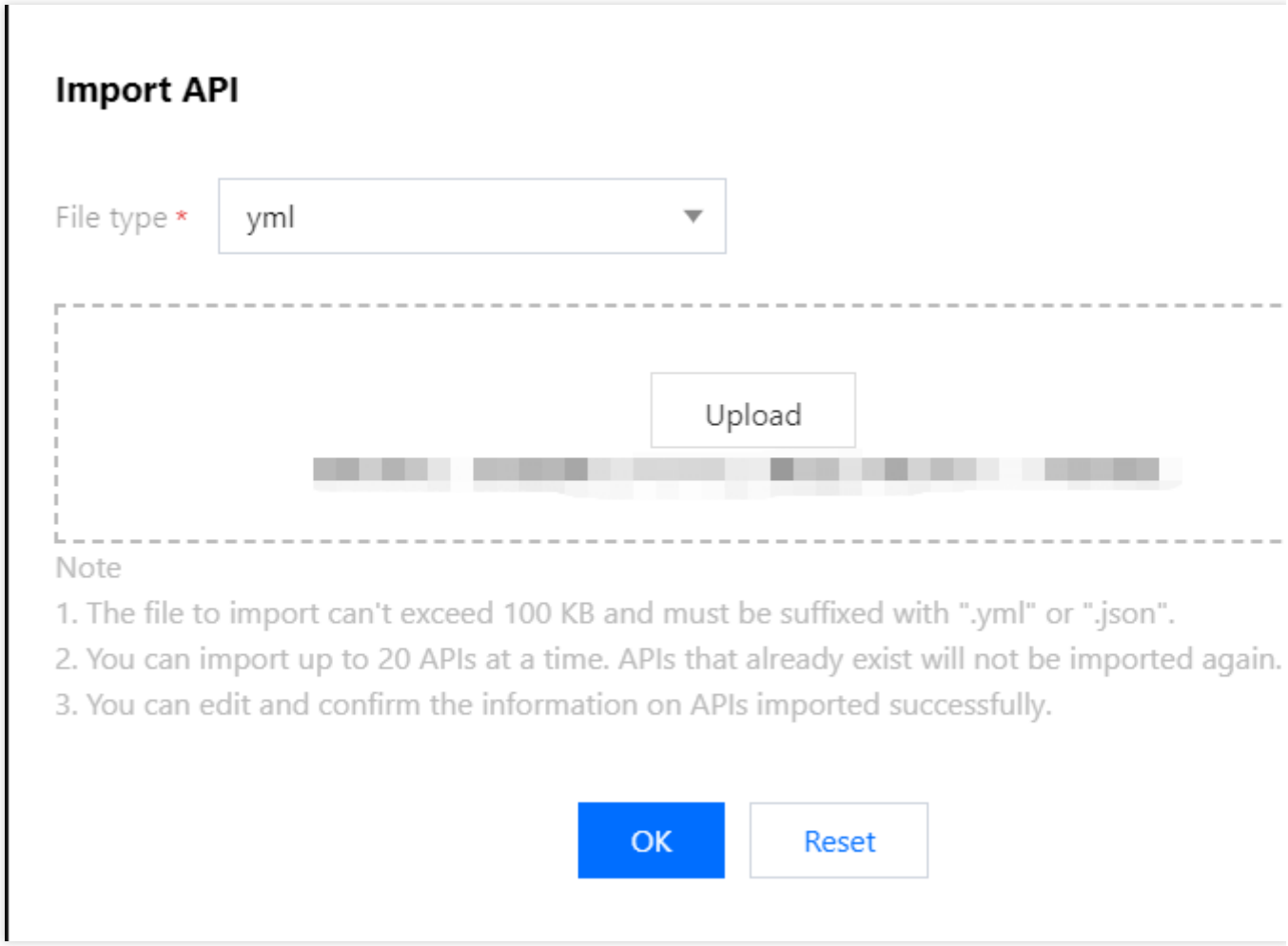
The imported APIs can be reviewed and edited.

©2013-2022 Tencent Cloud. All rights reserved.



3. After the upload, the API security module will parse the API policies in the swagger2.0 file. Then click **OK** when the parsing is complete.

©2013-2022 Tencent Cloud. All rights reserved.

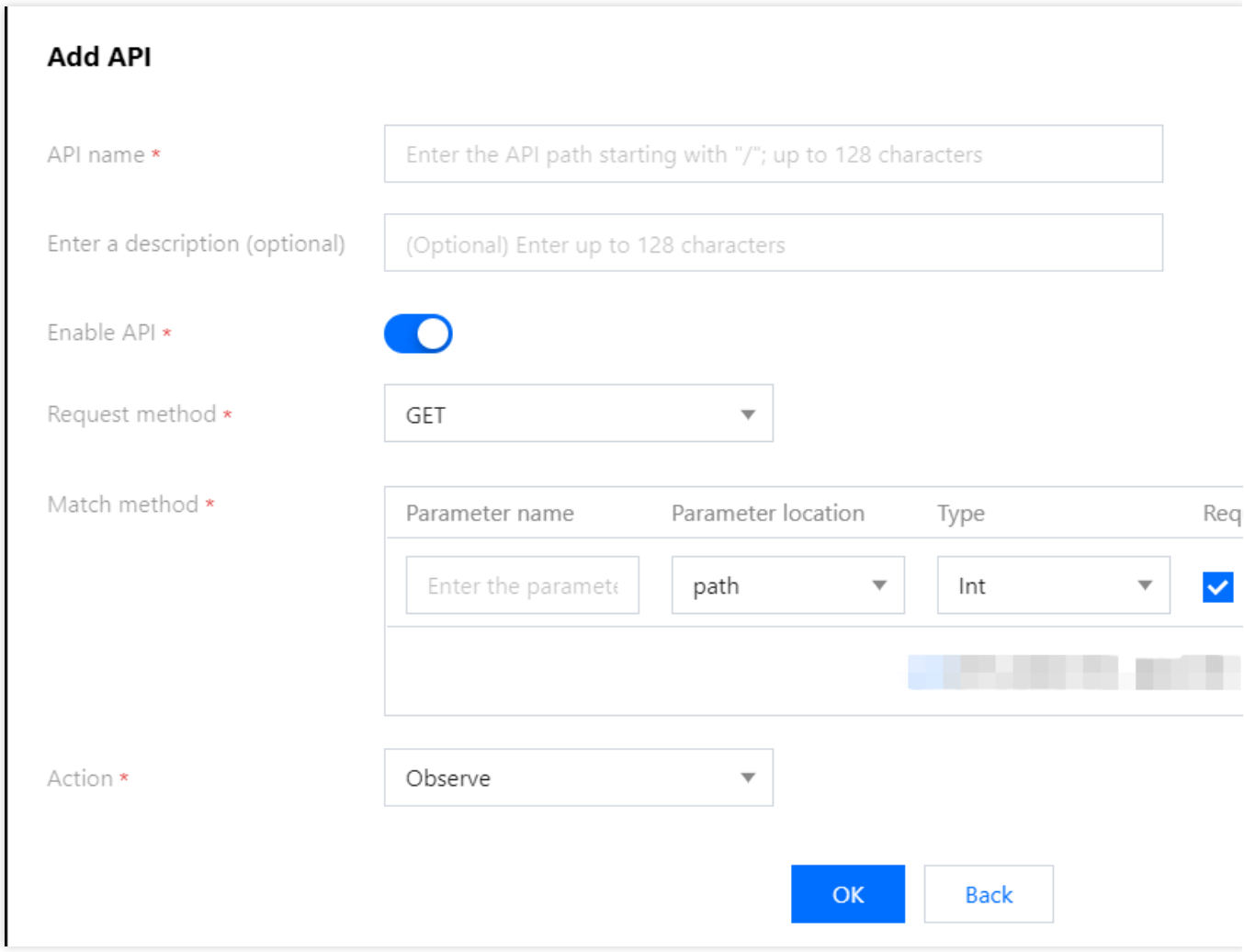


4. You can check the API rules after they are successfully imported.

Adding APIs

1. Select **Basic Security** > **API security**. On the page that appears, click **Add rule**.
2. In the pop-up window, create an API security rule that suits your website needs, and click **Add**.

©2013-2022 Tencent Cloud. All rights reserved.



Field description:

API name: Enter an API path that starts with "/", which cannot be the same as "API name + Request method" in the setting (eg., `/guanjia/waf/config`).

Description: Enter a description of the API rule. This field is optional.

Enable API: The switch controls whether to enable an API rule. The switch is off by default. When it is on, the API rule will be parsed and the action (Observe/Block) configured will be performed.

Request method: Only the following request methods are supported: GET, POST, PUT, and DELETE.

Condition: You need to specify the following parameters: Parameter name, Parameter location (Only `body` , `query` , and `path` values are supported), Parameter type, Required (If it is ticked, WAF will check whether the parameter is contained in the request and block the parameter when it exists), and Remarks (optional field).

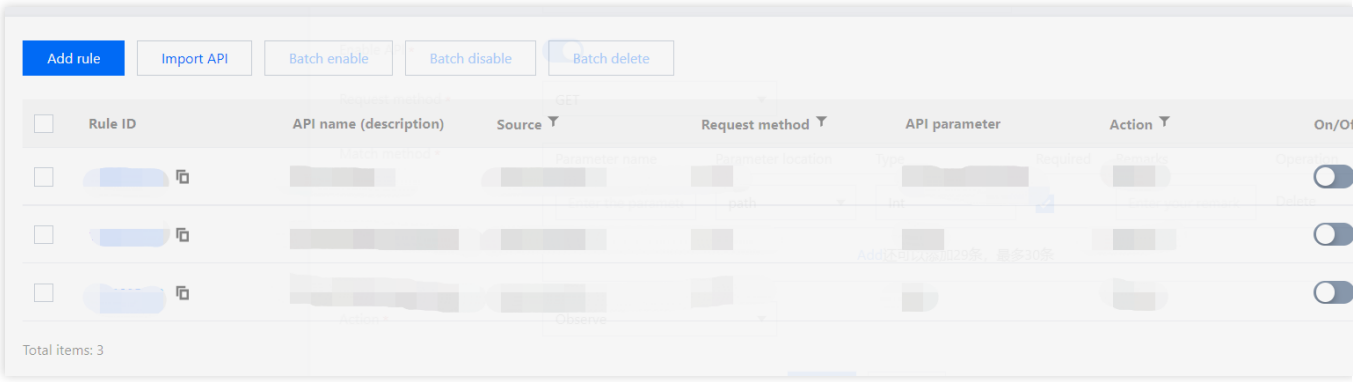
Action: Select the Observe or Block action as needed.

Note:

You are encouraged to set the Observe action, which allows the AI security module to check whether false positives occur in attack logs. If no false positives are caused, then change to the Block action.

3. After the rule is added, the API is added to the API security configuration list.

©2013-2022 Tencent Cloud. All rights reserved.



Field description:

Rule ID: It is a unique identifier for an API rule and is created automatically after the rule is added. You can search logs of the rule by its ID in Attack Logs.

API name (description): It displays the configured API name and description. Note that the API name must be the actual path of the API.

Source: It displays whether an API is parsed from file or added manually.

Request method: The following request methods are supported: GET, POST, PUT, and DELETE.

API parameter: List of API parameters configured, which cannot exceed 30.

Action: It can be set to Observe or Block.

On/Off: The switch controls whether to enable an API rule. To enable or disable multiple switches at the same time, select multiple API rules and click **Batch enable** or **Batch disable**.

Last modified: The last time an API rule is modified.

Operation: It allows you to edit or delete an API rule. If you want to delete API rules in batches, you can select more than one rule and click **Batch delete**.

©2013-2022 Tencent Cloud. All rights reserved.

Bot and Application Security
Bot Settings
Bot Management
Overview

Last updated：2023-12-29 14:42:30

With bot and application security, you can enable and configure modules in bot management, observe and analyze traffic through bot traffic analysis and access logs. Then, you can set refined policies based on the session status to protect core website APIs and businesses from bot attacks.
Bot management supports configuration of bot scenario types, client risk identification (browser bot defense module), threat intelligence module, AI evaluation module, bot flow statistics module, action score, custom rules, token configuration, and legitimate bots. You can configure these modules for refined bot management.

Scenario-based bot configuration

Leveraging Tencent Cloud's years of expertise in bot governance, this feature offers client risk identification (browser bot defense module), threat intelligence module, AI policy module, bot analytics module, action score, session management, legitimate bots, and custom rules specifically for flash sales, price/content crawling, and login scenarios. It simplifies configuration and makes everything easy to use.

Client Risk Identification (Browser Bot Defense Module)

This feature uses the dynamic identity verification technology and generates a unique ID for each client's business request to detect possible bots and malicious crawlers in the access to websites or HTML5 pages.

Threat Intelligence Module

This feature is built on Tencent's nearly 20 years of experience in cybersecurity and big data intelligence. It determines the status of an IP in real time and uses a scoring mechanism to quantify a risk. It precisely identifies the access from a malicious dynamic IP and IDC. In addition, it intelligently identifies the features of a malicious crawler to cope with risky access requests from malicious crawlers, distributed crawlers, proxies, credential stuffing, and bargain hunting.

AI Evaluation Module

This feature builds AI evaluation models from AI technologies and Tencent's experiences in controlling risks and fighting cybercrimes. Through big data analysis and AI modeling of access traffic, it quickly identifies malicious requesters and defends against risky access requests from APT and hidden threat bots.

©2013-2022 Tencent Cloud. All rights reserved.

Bot Flow Statistics Module

Based on big data analysis, this feature automatically classifies customer traffic by characteristic and identifies abnormal and malicious traffic. It automatically adjusts the malicious traffic threshold and handles risky access requests from general and high-frequency bots. With auto-adjustment modeling, it resolves most of the bot behavior bypasses.

Action Setting

This feature leverages the threat intelligence module, AI evaluation module, and bot flow statistics module to provide a comprehensive score ranging from 0 to 100 for the risk level of an access request to a website. The higher the score, the more likely it is from a bot, and the higher the risk level. With the score provided by bot analytics, the risk level of an access request is intelligently identified, and you can precisely block a risky access request based on actions configured for different score ranges.
In addition, it supports configuring a scope so that request data covered by the scope can be handled precisely.

Session Management

This feature allows you to configure the token location of a session to differentiate between access behaviors of different users through the same IP. Therefore, you can precisely handle a user with abnormal access behavior without affecting other users.

Legitimate Bots

This feature allows legitimate bots (such as search engines and feed bots) to get website data so that the website can be normally indexed.

Custom Rules

This feature allows you to precisely handle compliant crawlers and access requests with different characteristics.
In addition, it supports configuring a scope so that request data covered by the scope can be handled precisely.

Bot allowlist

This feature allows you to add the access requests from specified public network users to the allowlist based on the combination of different features, such as HTTP packet session feature, request feature, cookie, HTTP header, scope, IP feature, User-Agent, Referer, and session settings.
Priority from high to low: Bot allowlist > Scenario 1 (priority 1) > Scenario 2 (priority 2) > ... > Scenario n (priority m).

©2013-2022 Tencent Cloud. All rights reserved.

Rule Overview

Last updated：2023-12-29 14:42:42

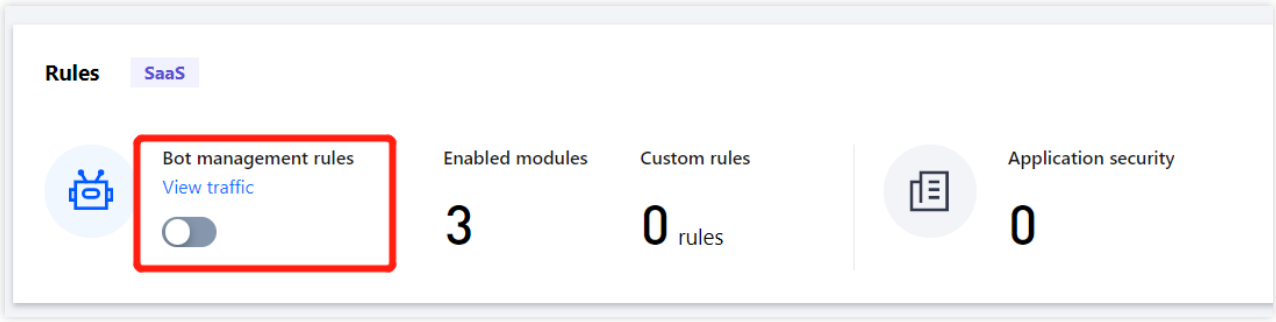
Prerequisites

To connect to bot traffic management, you need to purchase a WAF value-added service.

Directions

1. Log in to the WAF console and select **Configuration center** > **Bot and application security** on the left sidebar.
2. On the **Bot and application security** page, select the target domain name in the top-left corner and click

in **Bot management rules**.



Field description

Enable bot rule management: It is disabled by default and can be enabled as needed.

Note:

The bot traffic analysis feature takes effect only when the WAF switch of the domain name is enabled.

Effective scenario: Displays the number of bot analysis scenario modules enabled currently. They include the browser bot defense module, threat intelligence module, AI evaluation module, and bot flow statistics module.

Total scenarios: Displays the number of bot analysis scenario modules existing under the current domain name.

Current global scenario: Displays the name of the effective global scenario under the current domain name.

©2013-2022 Tencent Cloud. All rights reserved.

Total custom rules: Displays the number of custom bot rules enabled currently.

©2013-2022 Tencent Cloud. All rights reserved.

Advanced

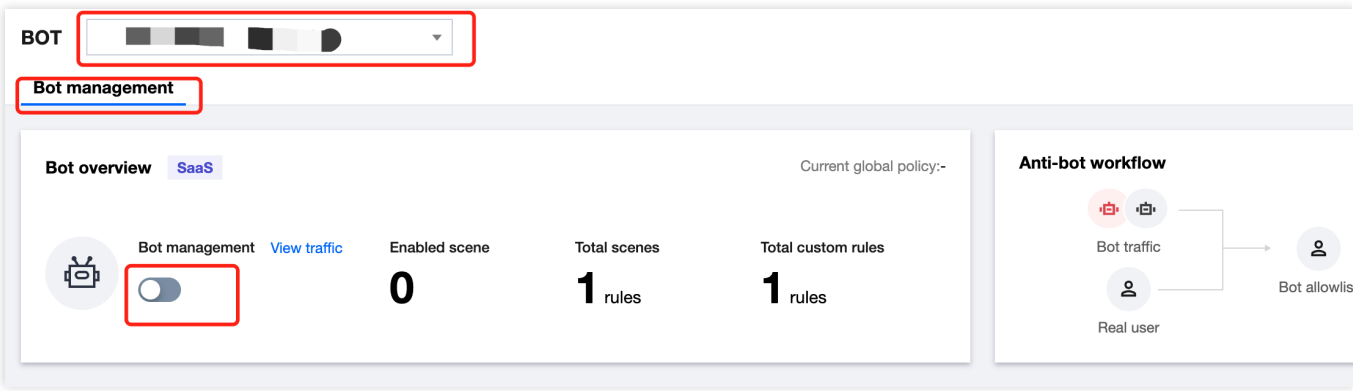
Last updated：2023-12-29 14:44:01

Prerequisites

Purchase a Web Application Firewall (WAF) plan with package for bot traffic management, and enabled bot analytics features for your domain name.

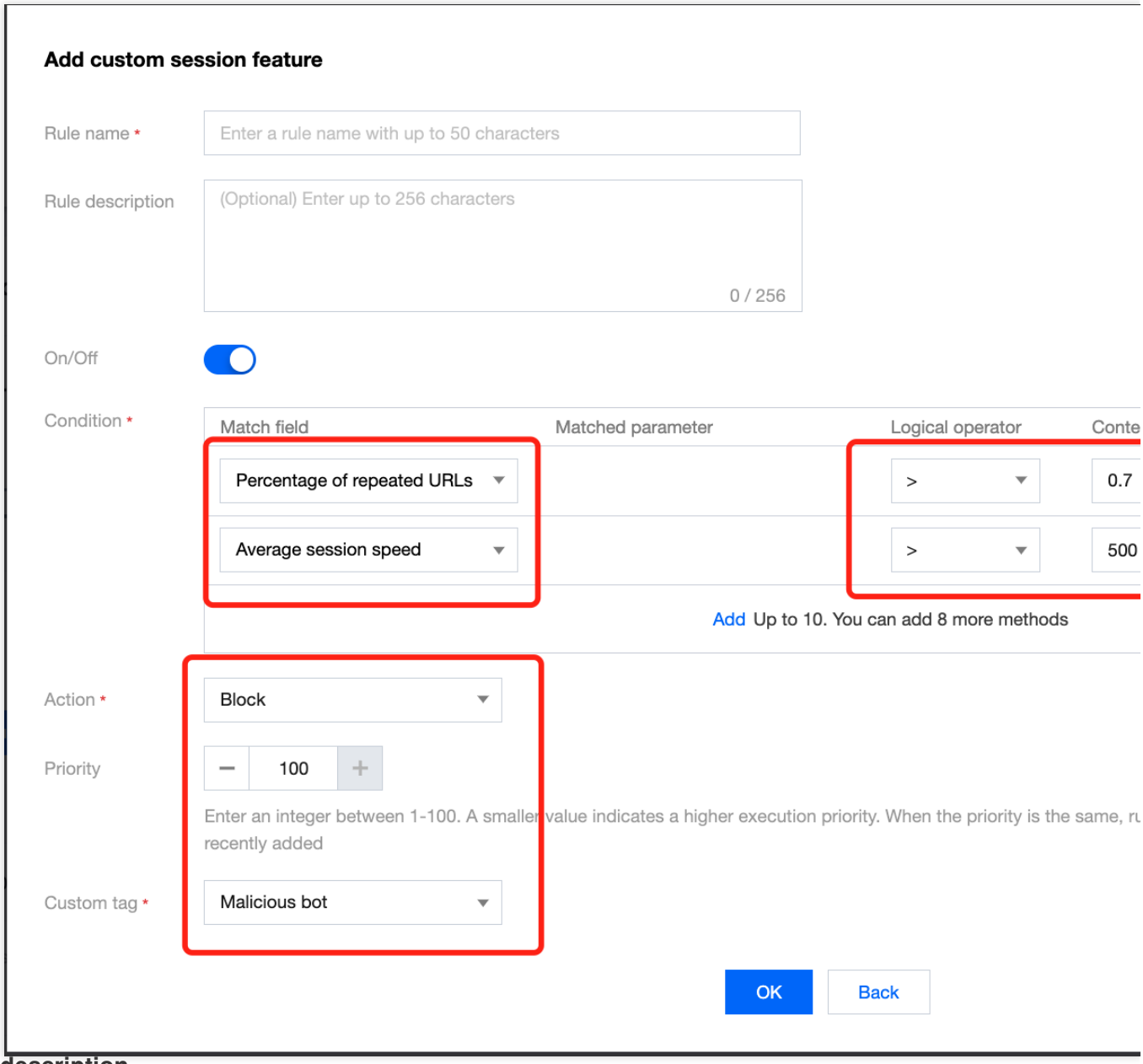
Bot allowlist

1. Log in to the WAF console and select **Configuration Center** > **Bot and Application Security** on the left sidebar.
2. On the **Bot and Application Security** page, select the target domain name in the top-left corner and choose **Bot management** > **Bot allowlist**.



3. On the bot allowlist settings page, click **Add rule**, configure parameters, and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Field description

Rule name:: The rule name.

Rule description: The rule description.

On/Off: Indicates whether the rule is enabled. A rule is enabled by default.

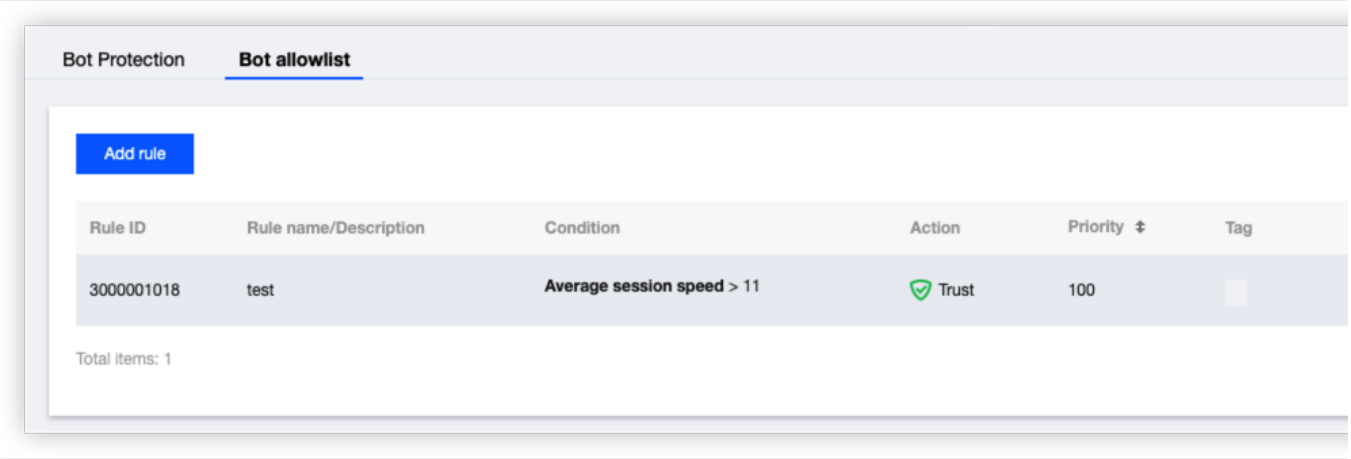
Condition: Conditions for matching bot policies. Up to 10 match conditions can be set, which are connected by the "AND" relationship. When you hover the cursor over a match condition, you can view its description.

Priority: Enter an integer between 1 to 100. A smaller integer indicates a higher priority. If the priority values are the same, the latest rule prevails.

Custom tag: You can set the tag to **Friendly bot** or **Normal traffic**.

4. Now you can view the created rule in the policy list. Click **Edit** or **Delete** to edit or delete it.

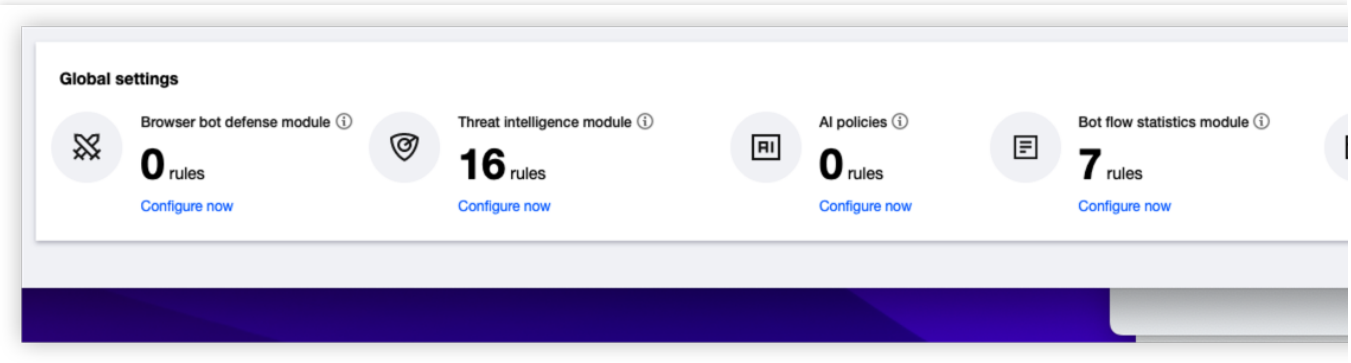
©2013-2022 Tencent Cloud. All rights reserved.



5. Priority from high to low: Bot allowlist > Scenario 1 (priority 1) > Scenario 2 (priority 2) > ... > Scenario n (priority m).

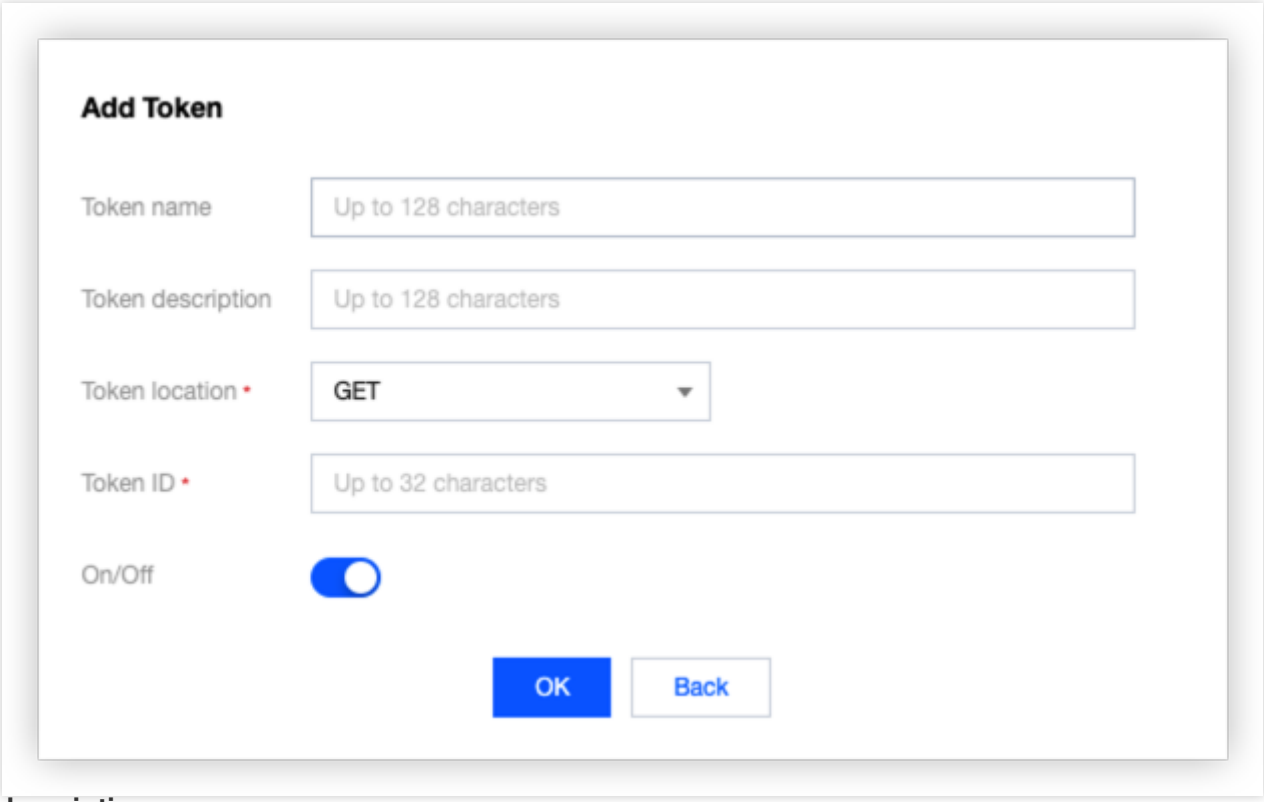
Session Management

This feature is similar to session setting in CC protection. With different token IDs, you can differentiate between access requests from different requesters through the same IP and record their behavior features.
You can also use token IDs to continuously track the access behaviors of different requesters. This helps identify bot access behaviors through residential or public egress IPs and record session features when proxy IPs are frequently changed.
1. Log in to the WAF console and select **Configuration Center** > **Bot and Application Security** on the left sidebar.
2. On the **Bot and Application Security** page, select the target domain name in the top-left corner and choose **Bot management** > **Bot Protection**.
3. On the **Bot Protection** page, click **Configure now** in the **Session management** area.



4. On the **Session management** page, click **Add a configuration**, configure parameters, and click **OK**.
Note:
A token ID should be a continuous tracking ID, such as the value of `set-cookies` after login.

©2013-2022 Tencent Cloud. All rights reserved.



Field description

Token location: HEADER, COOKIE, GET, or POST. Here, GET and POST are HTTP request parameters rather than HTTP headers.

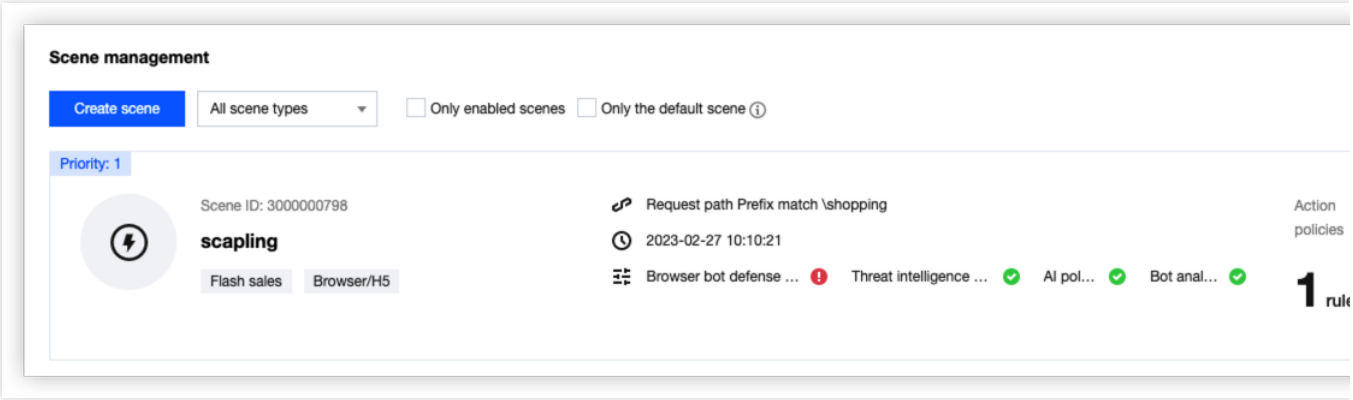
Token ID: Token ID.

5. The configuration will take effect immediately upon completion. Then, bot traffic analysis will analyze traffic according to the field of the session feature.

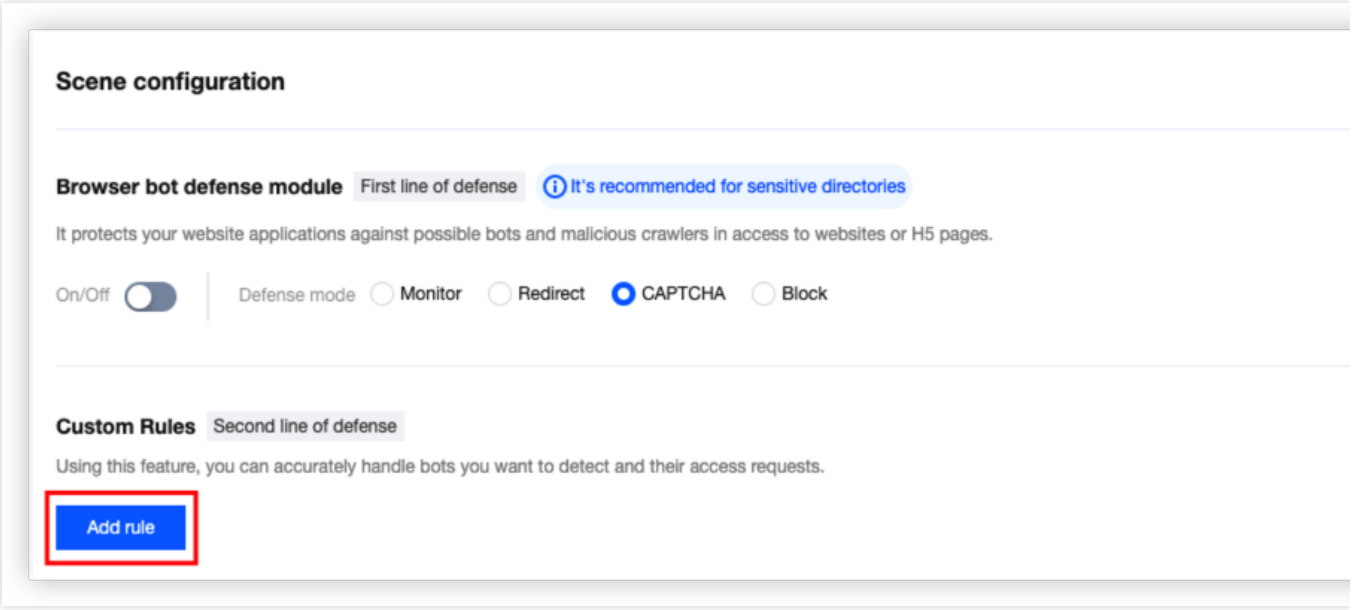
Setting a custom rule

1. Log in to the WAF console and select **Configuration Center** > **Bot and Application Security** on the left sidebar.
2. On the **Bot and Application Security** page, select the target domain name in the top-left corner and choose **Bot management** > **Bot Protection**.
3. In the **Scene management** area, select the target scene, and click **View configuration**.

©2013-2022 Tencent Cloud. All rights reserved.

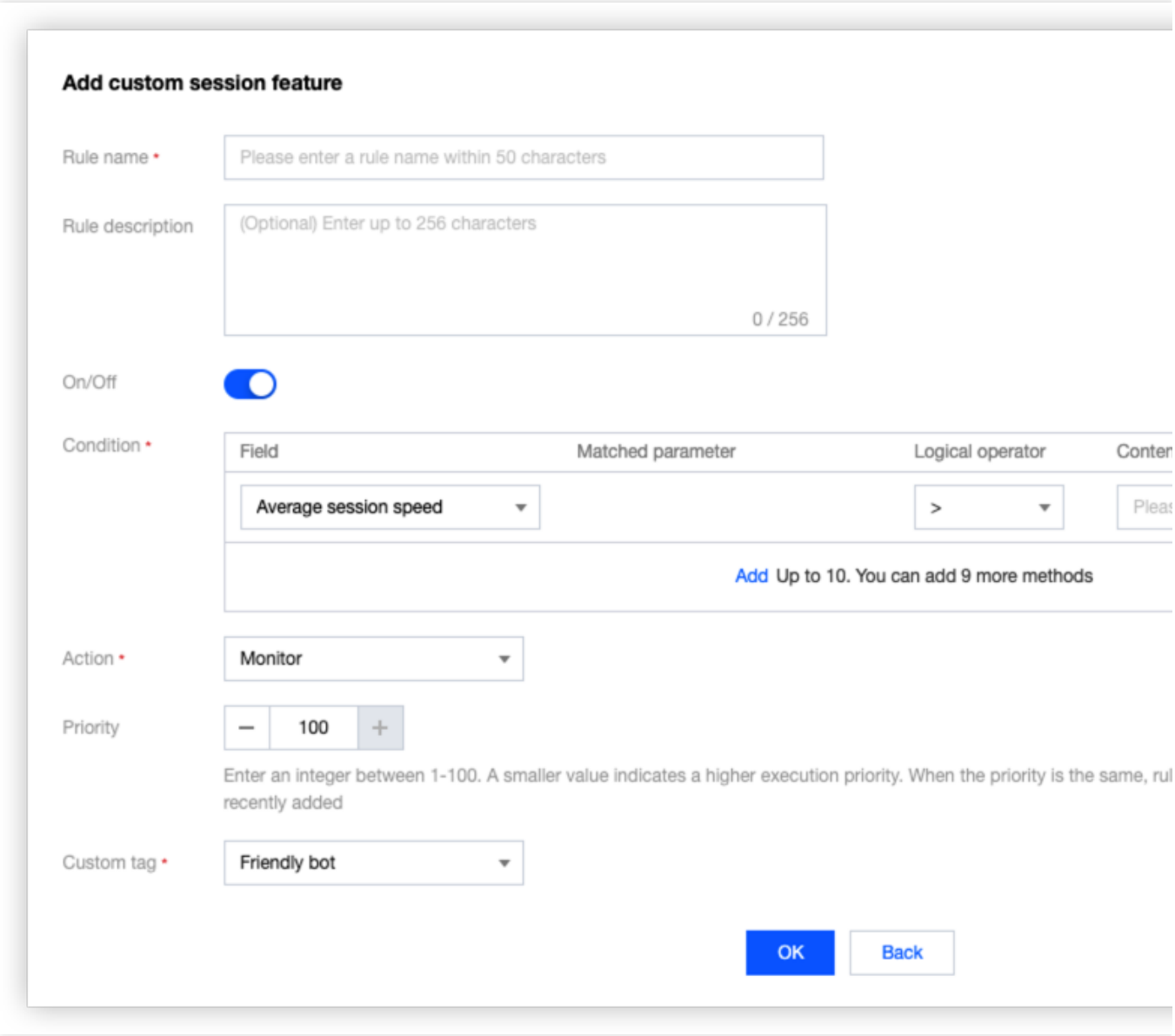


4. On the scene details page, click **Add rule** in the **Custom Rules** area.



5. In the **Add custom session feature** pop-up window, configure relevant parameters and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Field description

Rule name:: The rule name.

Rule description: the rule description.

Rule Switch: enabled by default.

Condition: Conditions to manage detected bots. You can set up to 10 conditions, which are combined with AND. Mouse over a condition to see the details.

Action: Action to be executed.

Action	Description
Trust	Allow hit requests without logging.
Monitor	Allow and log hit requests. You can check details in the **Custom type** of the **Bot details**.

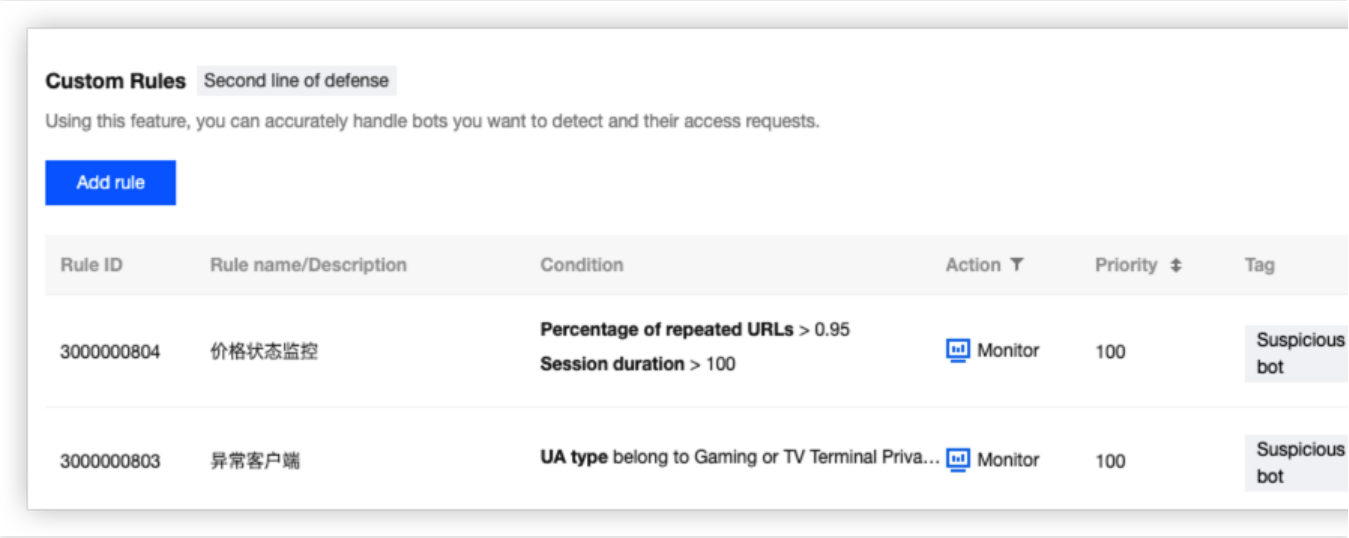
©2013-2022 Tencent Cloud. All rights reserved.

CAPTCHA	This action is applicable only to the access through browsers. Session requests that match the specified conditions will be verified through CAPTCHA. If they fail, they will be blocked. Otherwise, the access is allowed.
Redirect	Session requests that match the specified conditions will be redirected to a specific URL of the current domain name.
Block	Block and log the hit requests. You can check the logs in Attack Logs. To check the blocked IPs, go to IP blocking status.

Priority: Enter an integer between 1 to 100. A smaller integer indicates a higher priority. If the priority values are the same, the latest rule prevails.

Custom tag: You can set the tag to **Friendly bot**, **Malicious bot**, **Normal traffic**, or **Suspicious bot**.

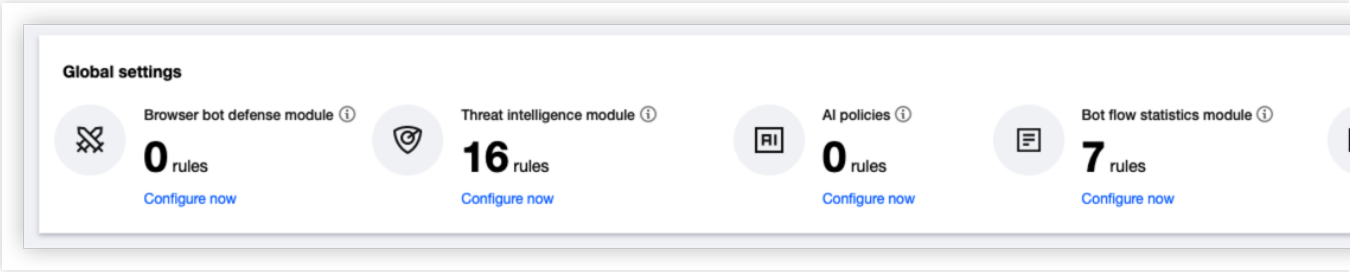
6. Now you can see the created rule in the policy list.



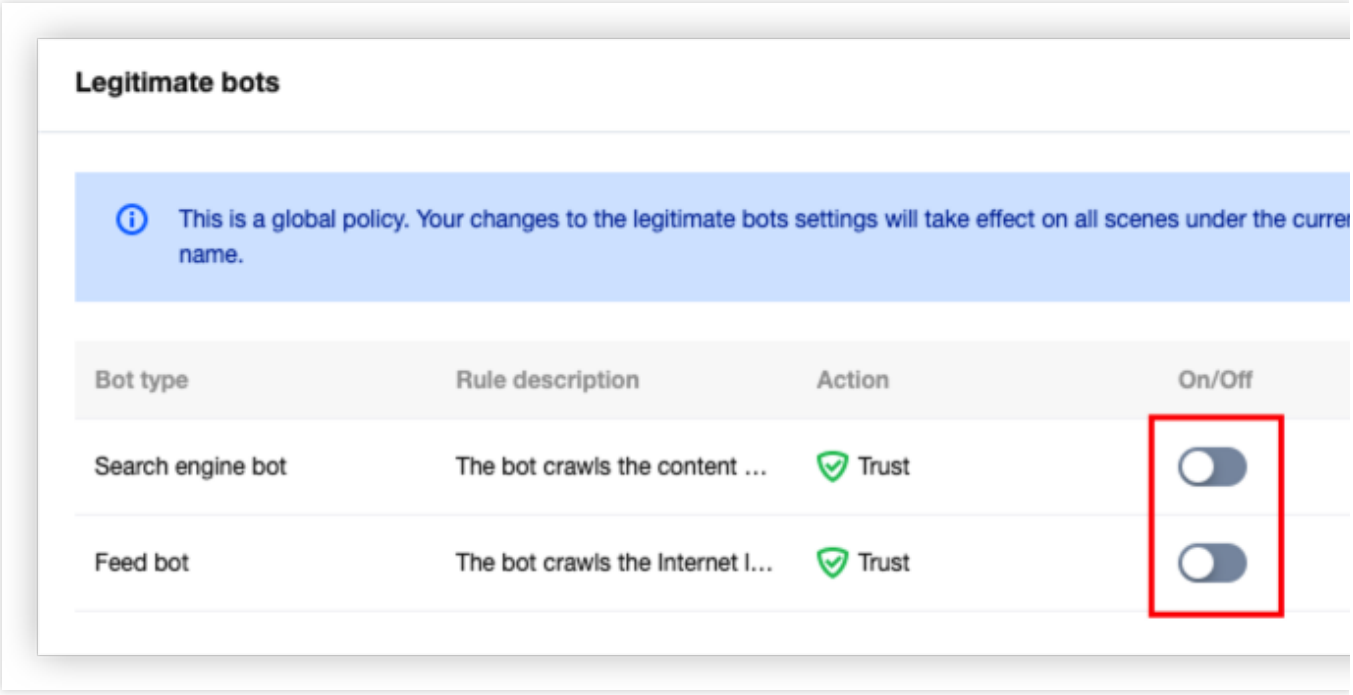
Legitimate Bots

1. Log in to the WAF console and select **Configuration Center** > **Bot and Application Security** on the left sidebar.
2. On the **Bot and Application Security** page, select the target domain name in the top-left corner and choose **Bot management** > **Bot Protection**.
3. On the **Bot Protection** page, click **Configure now** in the **Legitimate bots** area.

©2013-2022 Tencent Cloud. All rights reserved.



4. On the **Legitimate bots** page, toggle on the switch to allow bots useful to the website data, such as search engines and external cooperative crawlers.



©2013-2022 Tencent Cloud. All rights reserved.

Client Risk Identification

Last updated：2023-12-29 14:42:55

This document describes the browser bot defense module in client risk identification. With the dynamic identity verification technology, it will generate a unique ID for each client's business request to detect possible malicious bots and crawlers in access to websites or HTML5 pages.

Background

Compatibility description: The browser bot defense module is applicable to the protection for websites or HTML5 pages. It will dynamically generate client IDs and tokens and identify malicious and crawler requests by detecting the IDs and tokens. In some cases, it may have compatibility issues with POST requests (the content of the `content-type` response body is not `text/html` , and the `<html>` tag is not included). This may cause an exception in the detection. As a countermeasure, you can add the request path or response request to the allowlist.
Perceptible bot defense: The system pops up a CAPTCHA (slider, puzzle, or character comparison) for client requests that meet the conditions to differentiate between access requests from a real person and a bot. Multiple verification failures will lead to blocking. This is applicable to protecting core website APIs (such as shopping cart, payment, and SMS). This capability has been integrated into the actions (observe, CAPTCHA, redirect, and block) of each WAF module for you to use.
Imperceptible bot defense: Client behavior detection is imperceptible to users, applicable to use cases with high requirements for the user experience. This feature leverages the dynamic security technology to generate a unique ID for each client and detect possible click farming and malicious crawling in the access to websites or HTML5 pages. You can perform an action on malicious behaviors as needed.
Note:
The browser bot defense module is applicable to websites and HTML5 pages but not mobile terminals or mini programs.

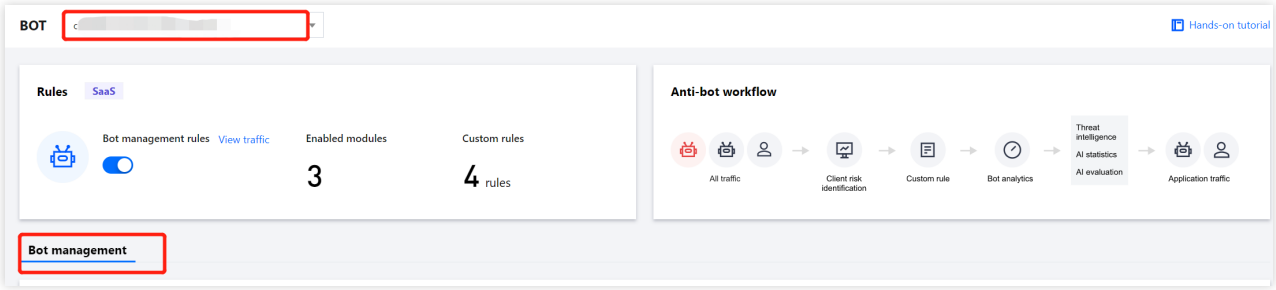
Prerequisites

You have purchased a WAF instance and bot traffic management extra pack.
You have added a protected domain name, the domain name is in normal protection, and bot management rules are on. For more information, see Getting Started.
Note:
The browser bot defense module is not supported for domain names added to CLB WAF instances.
The browser bot defense module is not supported for wildcard domain names added to SaaS WAF instances.

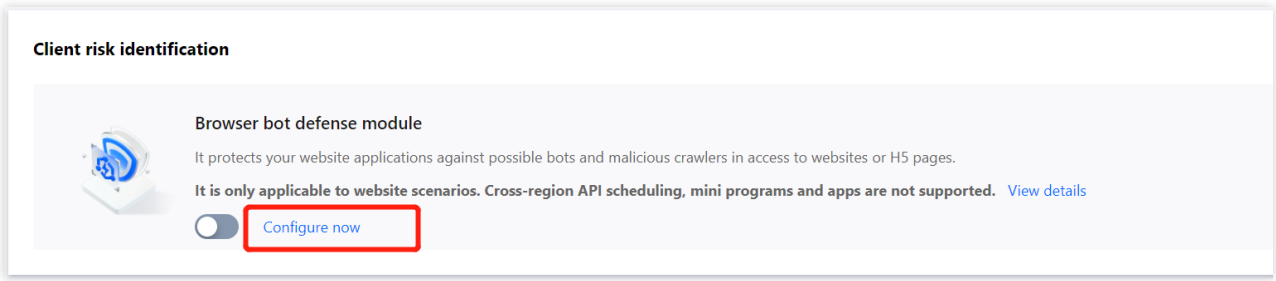
©2013-2022 Tencent Cloud. All rights reserved.

Protection Configuration

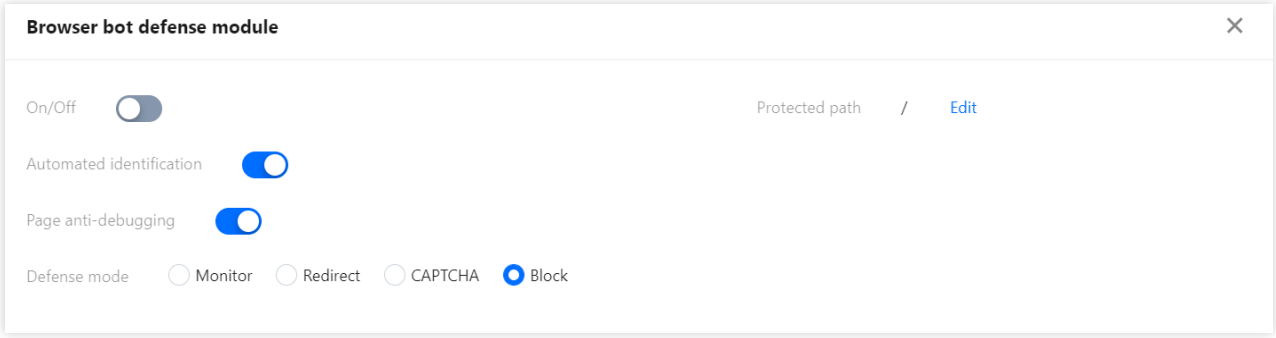
1. Log in to the WAF console and select **Configuration center** > **Bot and application security** on the left sidebar.
2. On the **Bot and application security** page, select the target domain name in the top-left corner and click **Bot management**.



3. In **Global settings**, click **Configure now** in the **Browser bot defense module** section.
4. Set the automated identification, page anti-debugging, and allowlist policy.



5. On the **Browser bot defense module** page, configure page anti-debugging and automated identification.



6. Click the configuration page of a certain scenario, click **Browser bot defense module**, toggle on or off the **On/Off** switch of the **Browser bot defense module**, and select the **Defense mode**.

Field description

©2013-2022 Tencent Cloud. All rights reserved.

On/Off: It is off by default. When it is on, WAF will protect the page specified by the domain name through the browser bot defense module to identify possible crawlers in the client request and take different actions after identification. It is not applicable to applications or mini programs.

Automated identification: It is enabled by default to assist with dynamic threat detection.

Page anti-debugging: It is enabled by default to prevent users from tracking the page logic when they call the developer tool page of the browser.

Note:

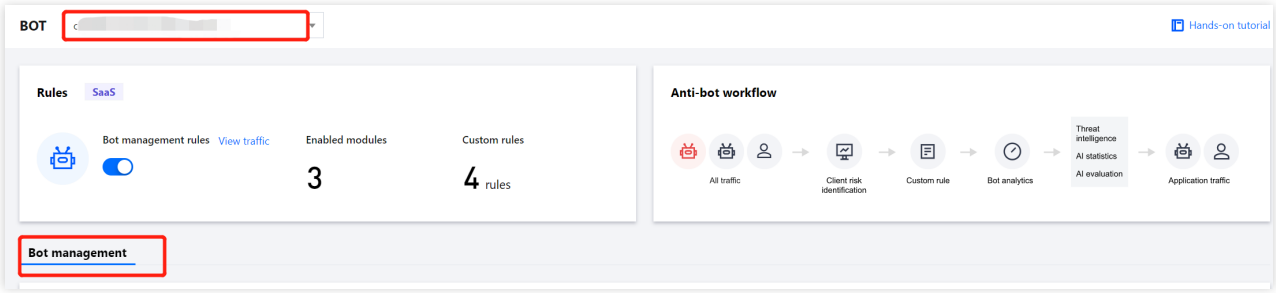
We recommend you enable this feature for the sensitive directory to be protected.

Defense mode: It is **Monitor** by default and can be configured to perform an action on the crawlers detected by the browser bot defense module, such as monitor, CAPTCHA, redirect, or block.

Configuring Allowlist Policy

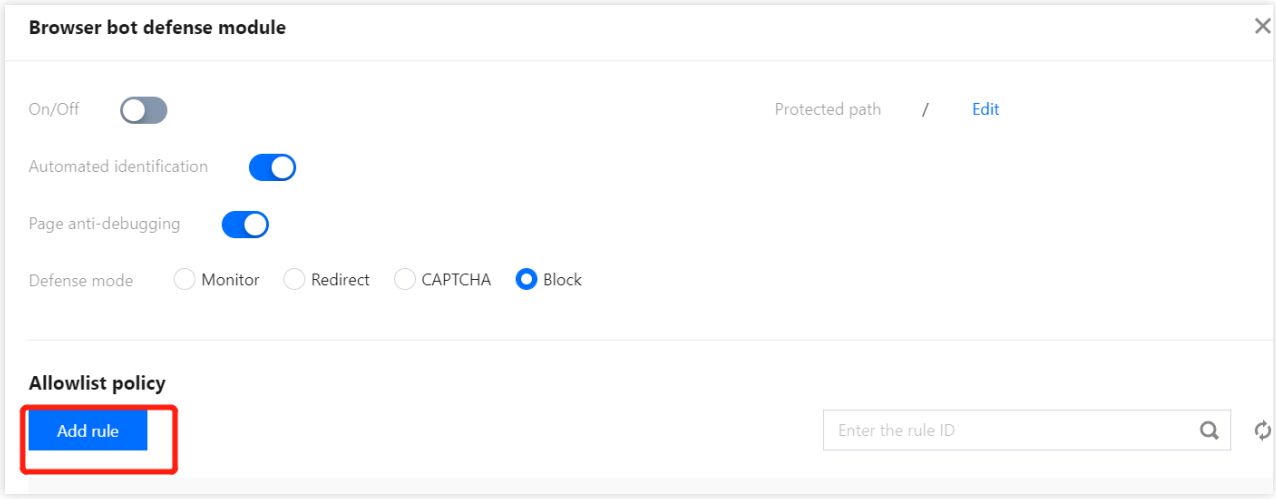
Adding rule

1. Log in to the WAF console and select **Configuration center** > **Bot and application security** on the left sidebar.
2. On the **Bot and application security** page, select the target domain name in the top-left corner. In **Global settings**, click **Configure now** in the **Browser bot defense module** section.

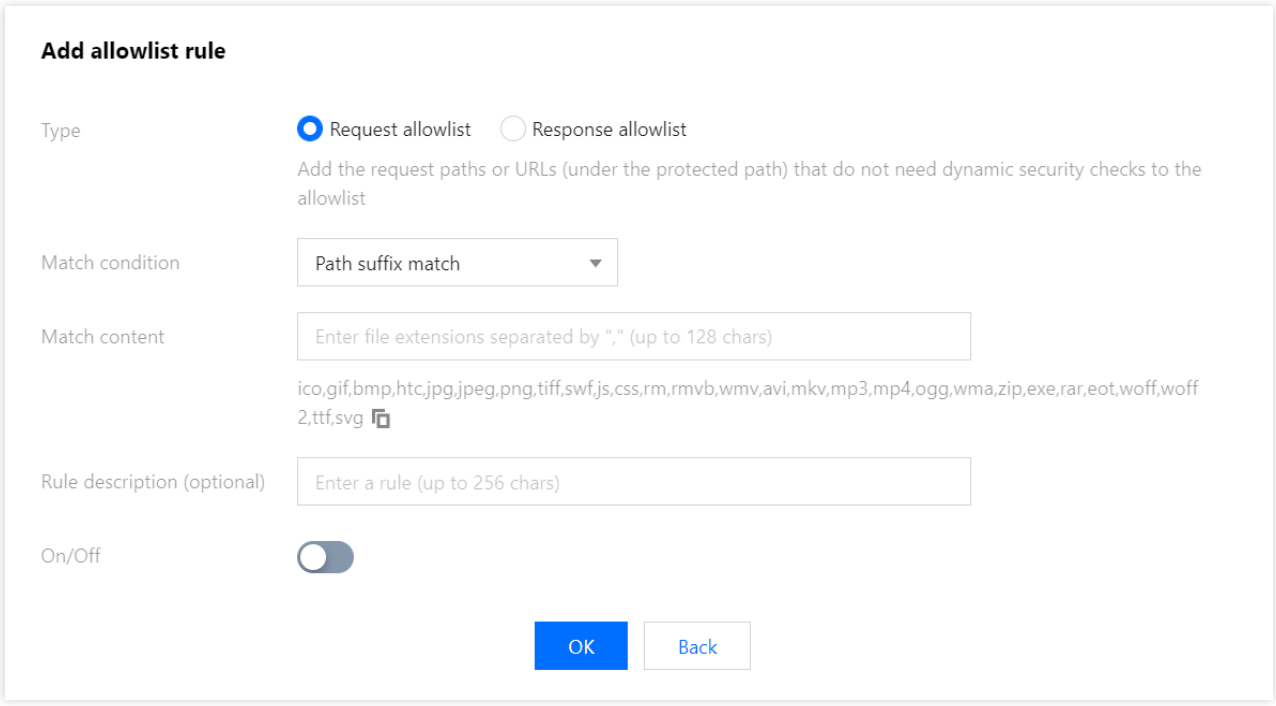


3. On the **Browser bot defense module** page, click **Add rule**.

©2013-2022 Tencent Cloud. All rights reserved.



4. In the **Add allowlist rule** pop-up window, configure parameters and click **OK**.



Field description

Type

Request allowlist: Dynamic security detection is not required for allowed website URLs.

Response allowlist: By default, WAF will insert JavaScript code into a responding page according to the business conditions. It can be configured not to insert JavaScript code into a specified website so as to improve the website compatibility.

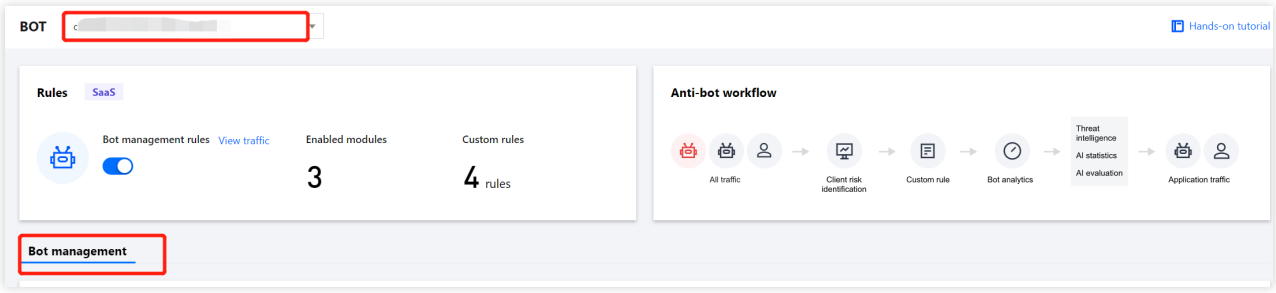
Match condition: **Suffix match** (default), **Prefix match**, **Equal to**, and **Include** are supported.

©2013-2022 Tencent Cloud. All rights reserved.

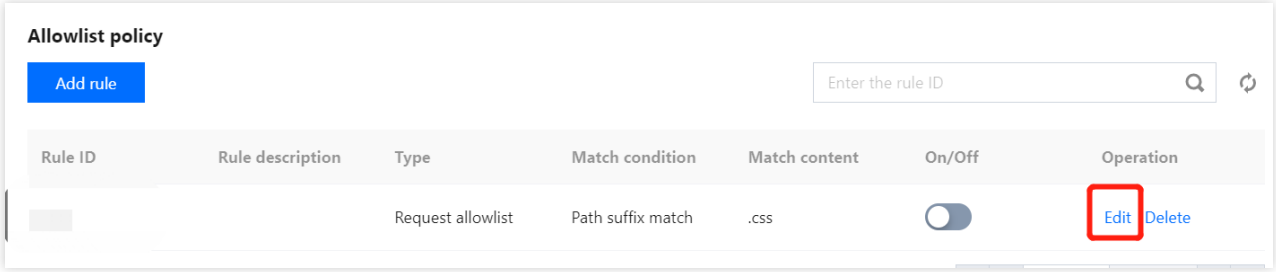
Match content: The current match condition is **Suffix match**. By default, the suffixes of files to be allowed are offered, including ico, gif, bmp, htc, jpg, jpeg, png, tiff, swf, js, css, rm, rmvb, wmv, avi, mkv, mp3, mp4, ogg, wma, zip, exe, rar, eot, woff, woff2, ttf, and svg. You can modify the suffix as needed. If another match condition is selected, enter the allowlist path according to the actual business conditions.
Rule description (optional): Enter the rule description.
On/Off: It is off by default and can be changed as needed.

Editing rule

1. Log in to the WAF console and select **Configuration center** > **Bot and application security** on the left sidebar.
2. On the **Bot and application security** page, select the target domain name in the top-left corner. In **Global settings**, click **Configure now** in the **Browser bot defense module** section.

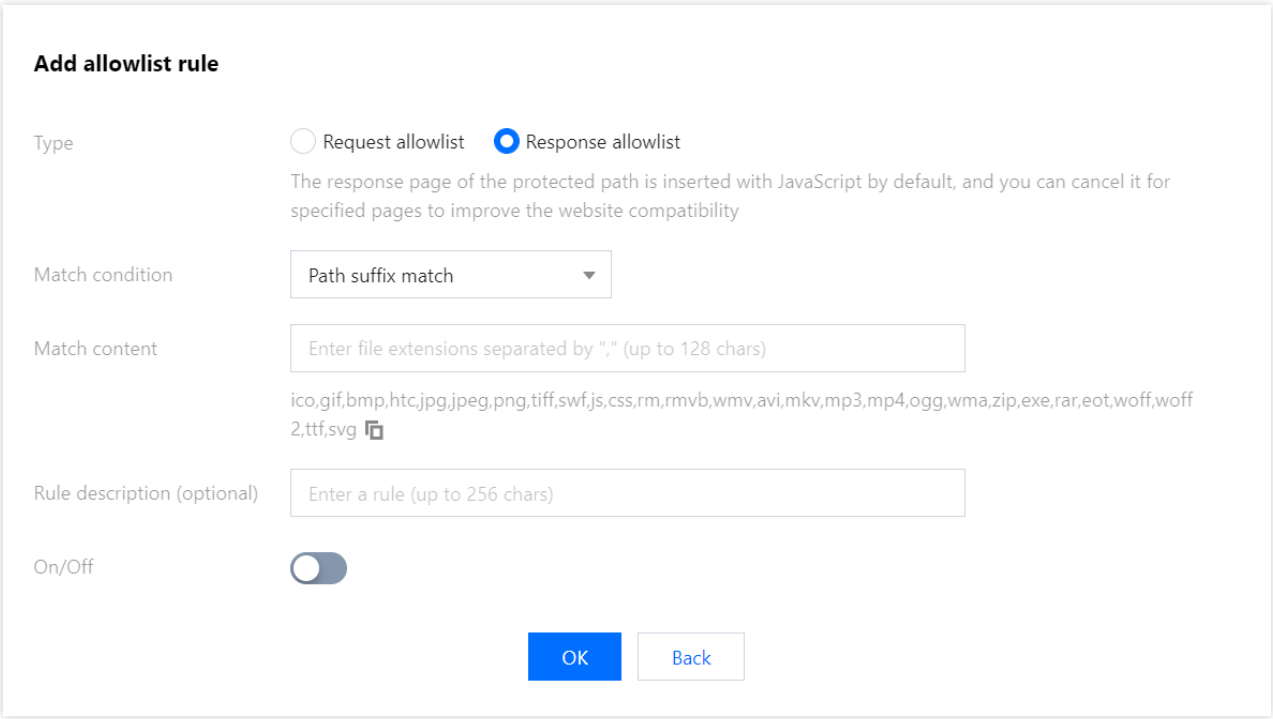


3. On the **Browser bot defense module** page, select the target rule and click **Edit**.



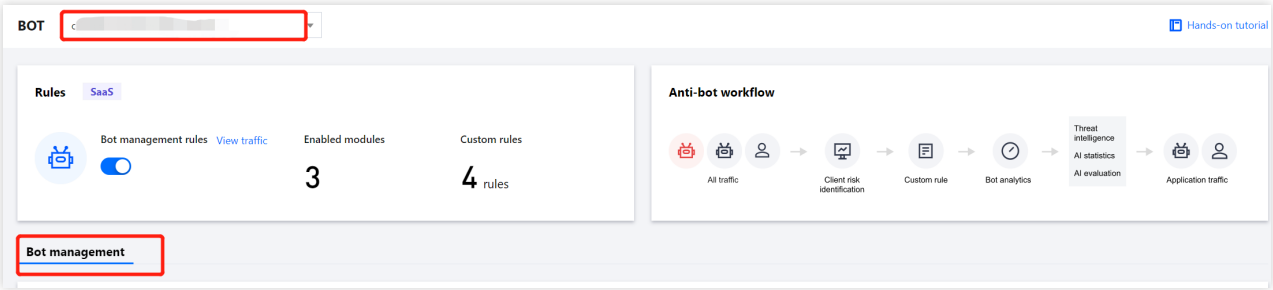
4. In the **Edit allowlist rule** pop-up window, configure parameters and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



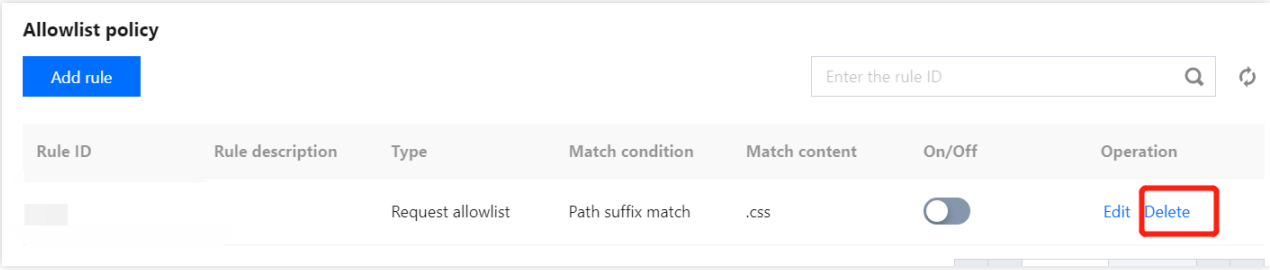
Deleting a rule

1. Log in to the WAF console and select **Configuration center** > **Bot and application security** on the left sidebar.
2. On the **Bot and application security** page, select the target domain name in the top-left corner. In **Global settings**, click **Configure now** in the **Browser bot defense module** section.



3. On the **Browser bot defense module** page, select the target rule and click **Delete**.

©2013-2022 Tencent Cloud. All rights reserved.



4. In the pop-up window, click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.

Bot Analytics
AI Policies

Last updated：2023-12-29 14:43:09

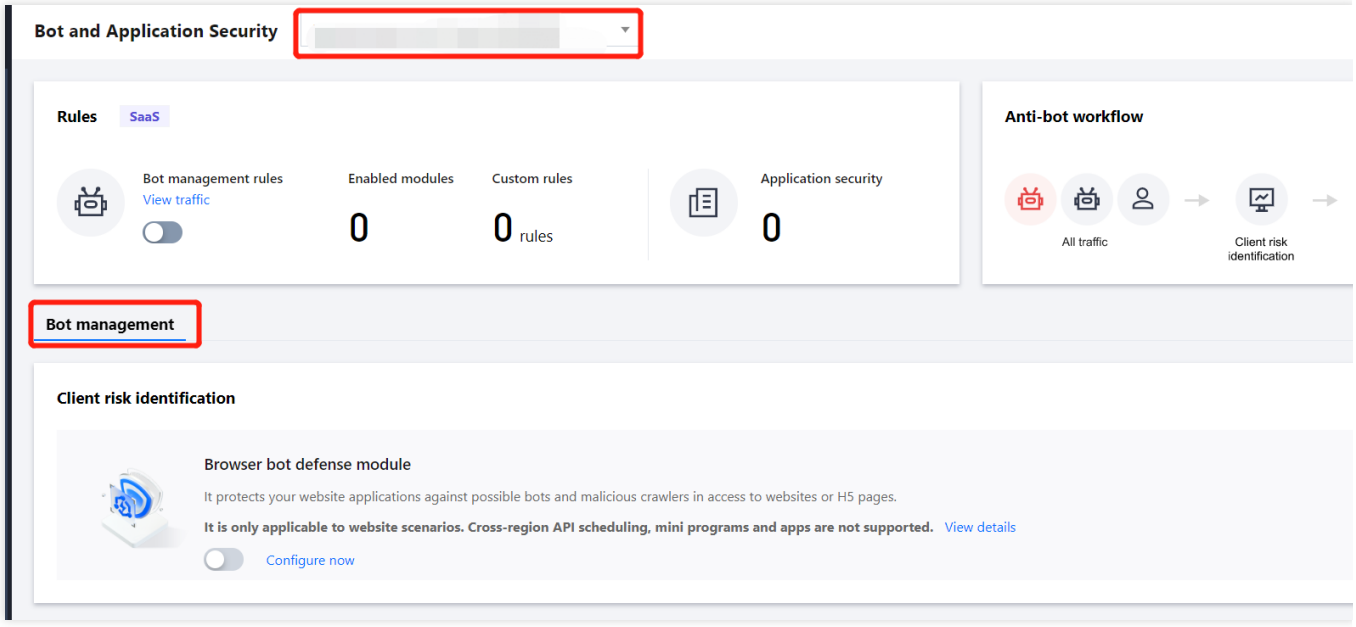
This document describes the AI policy module in bot traffic management. This feature is built on Tencent's nearly 20 years of experience in cybersecurity and bot defense. It applies AI models, built based on AI technology and Tencent's experiences in controlling risks and fighting illegal activities, to quickly identify malicious requests and fight against previous, APT, and distributed bots.

Prerequisites

You have purchased a WAF instance and bot traffic management extra pack and enabled bot rule management for WAF-connected domain names.

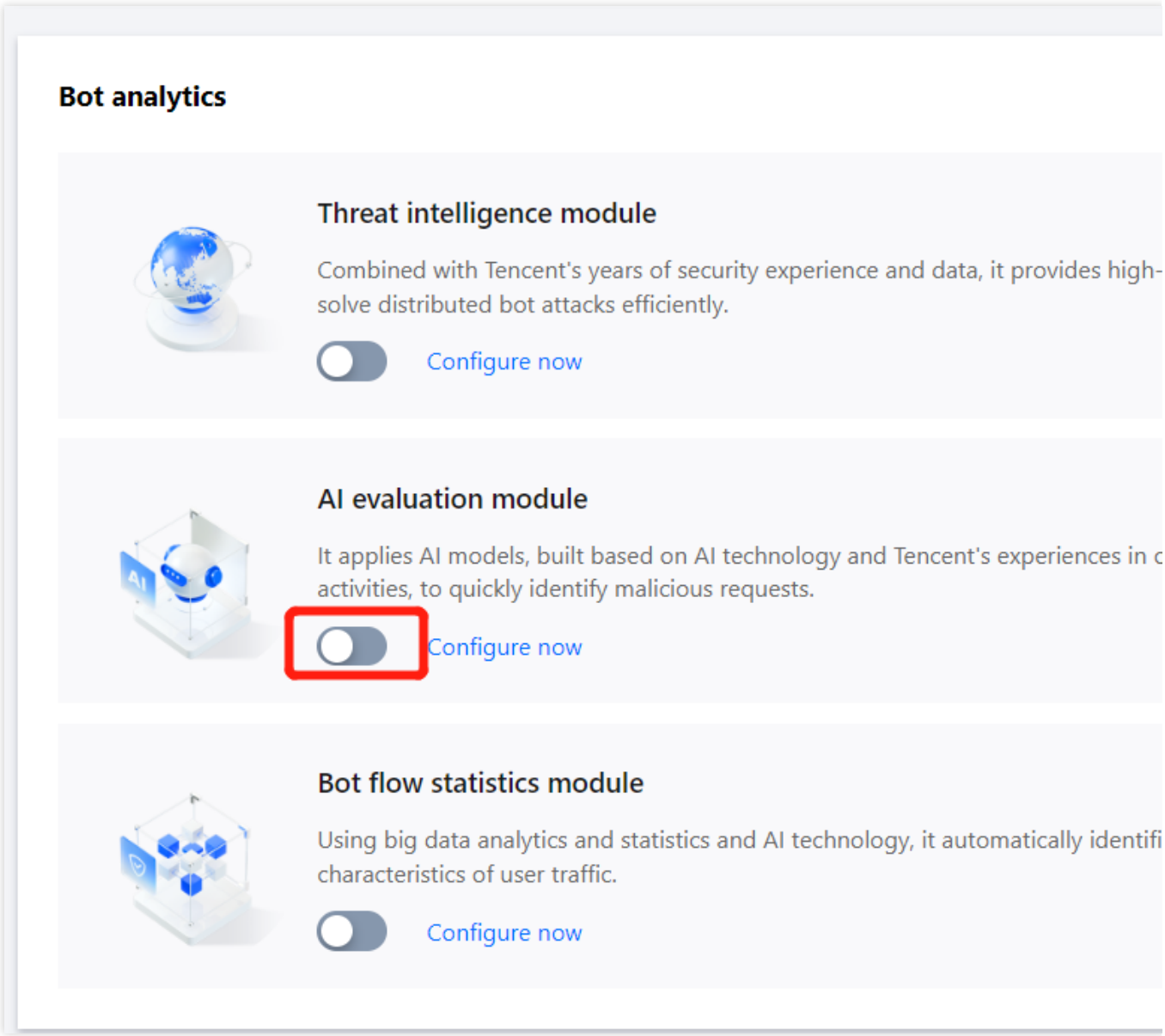
Protection Configuration

1. Log in to the WAF console and select **Configuration center** > **Bot and application security** on the left sidebar.
2. On the **Bot and application security** page, select the target domain name in the top-left corner and click **Bot management**.

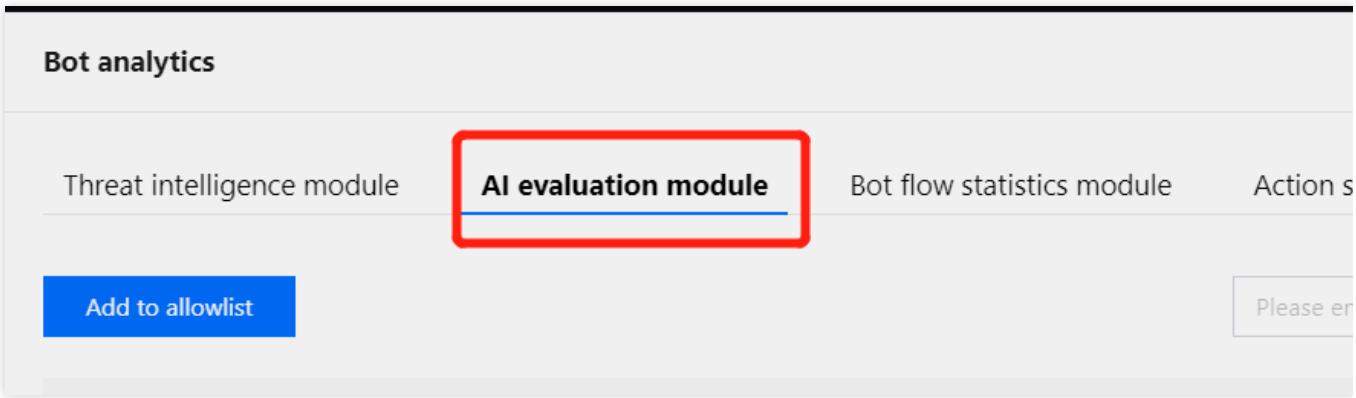


3. In global settings, click **Configure now** in the **Browser bot defense module** section.

©2013-2022 Tencent Cloud. All rights reserved.



4. Click **Add to allowlist** to add certain URLs to the allowlist to reduce false positives detected by AI.



5. On the AI policy page, you can add URLs to the allowlist, so that core business will not be blocked due to frequent access to core business/callback business. You can also add certain URLs to the allowlist so that they will not be

©2013-2022 Tencent Cloud. All rights reserved.

blocked by mistake.

Note:

Here, the allowlist applies only to the AI policy module but not other modules.

Parameter description:

Policy name: Policy name.

Rule description: Policy description.

Allowed URL: URL allowed by the AI policy module, which affects the score of the AI policy module.

On/**Off**: You can enable/disable an allowlist in the AI policy module. When this option is on, the AI policy module will not add the score of the URL that hits the allowlist. The score will be provided by the threat intelligence module and bot flow statistics module.

6. After configuring the AI policy module, click the configuration page of a certain scenario and click of the AI policy module.

Best practices

The AI policy module leverages the bot defense experience and the accumulation of the bot attack/defense lab to quickly identify general and APT bots. Therefore, we recommend you enable it and add the business callback API to the allowlist under any circumstances.

©2013-2022 Tencent Cloud. All rights reserved.

Threat Intelligence Module

Last updated：2023-12-29 14:43:24

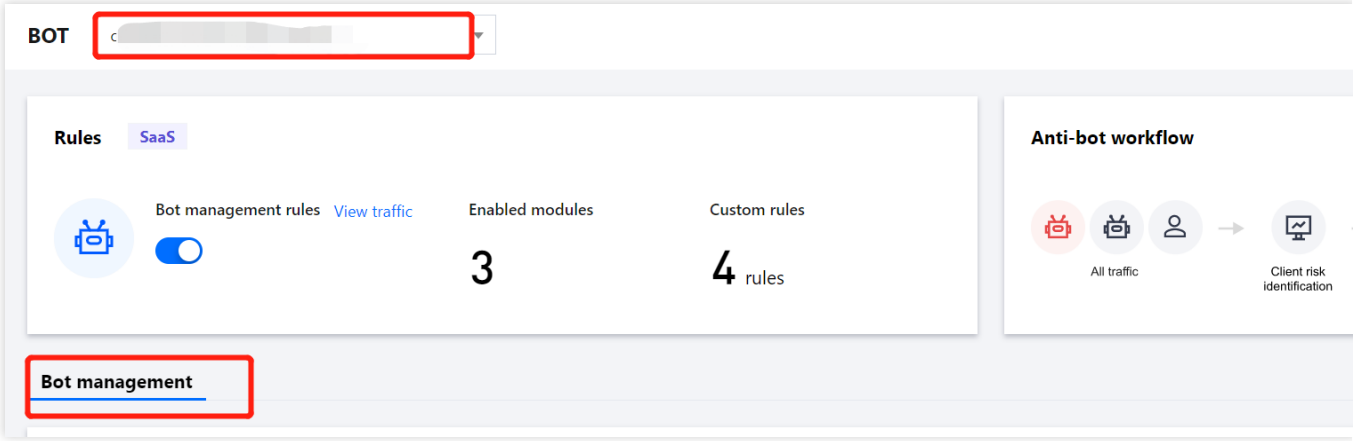
This document describes how to set the threat intelligence module in the bot analytics section of bot traffic management. This feature is built on Tencent's nearly 20 years of experience in cybersecurity and big data intelligence. It determines the status of an IP in real time and uses a scoring mechanism to quantify a risk. It precisely identifies the access from a malicious dynamic IP and IDC. In addition, it intelligently identifies the characteristics of a malicious crawler to cope with risky access requests from malicious crawlers, distributed crawlers, proxies, credential stuffing, and bargain hunting.

Prerequisites

You have purchased a WAF instance and bot traffic management extra pack and enabled bot analysis for WAF-connected domain names.

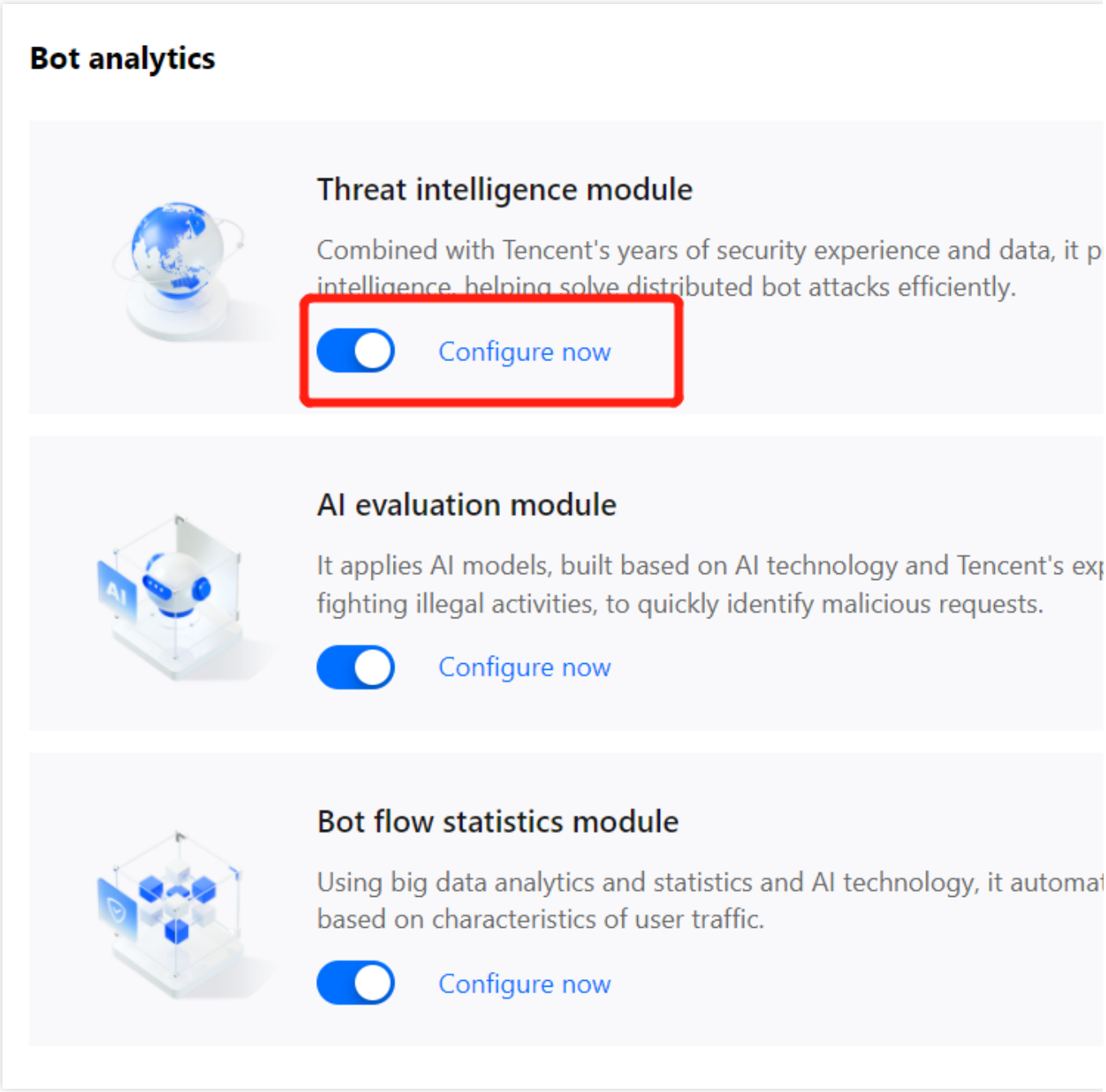
Protection Configuration

1. Log in to the WAF console and select **Configuration center** > **Bot and application security** on the left sidebar.
2. On the **Bot and application security** page, select the target domain name in the top-left corner and click **Bot management**.



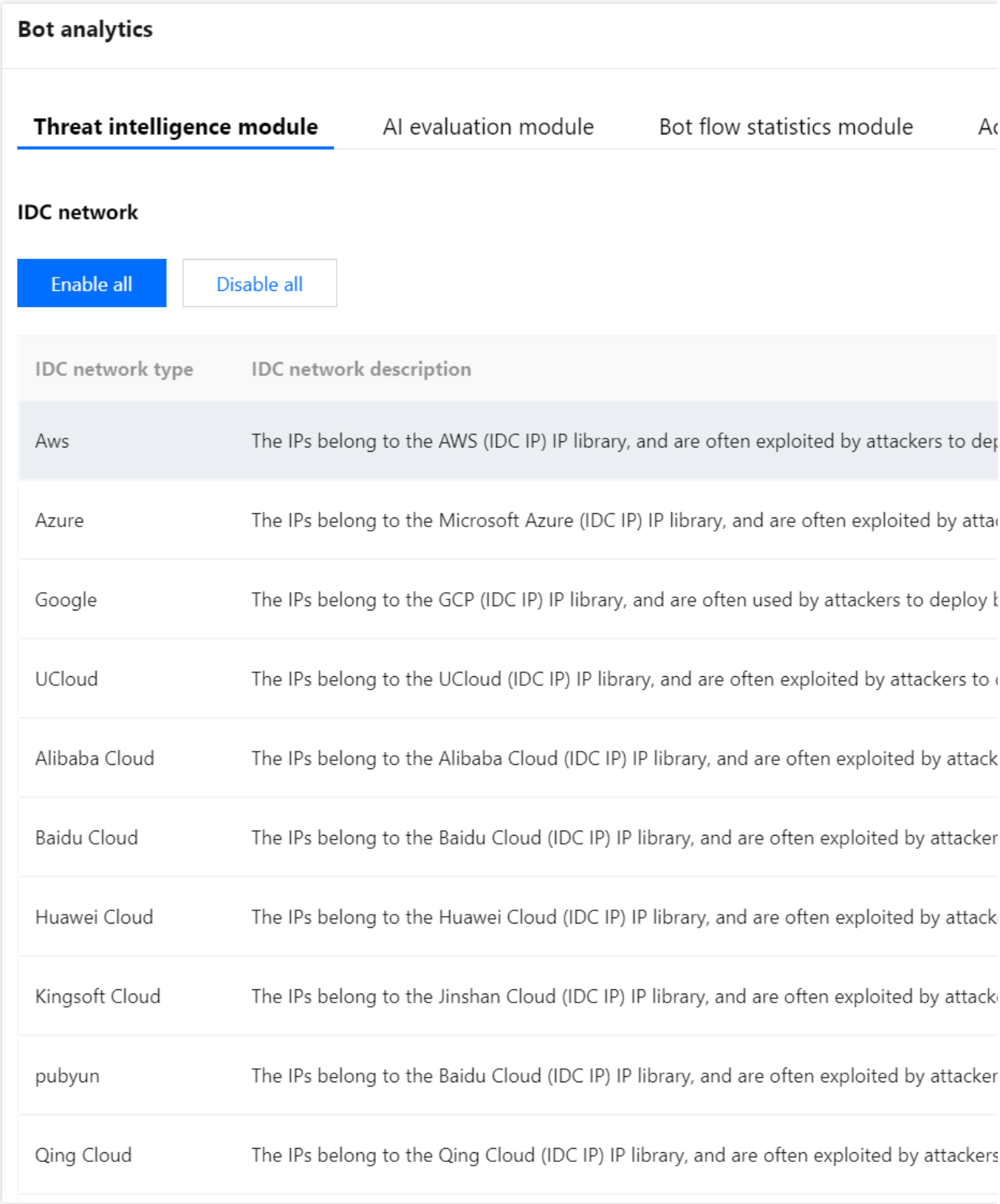
3. In **Global settings**, click **Configure now** in the **Threat intelligence module** section.

©2013-2022 Tencent Cloud. All rights reserved.



4. On the configuration page, enable or disable an identification item or enable or disable all the items.

©2013-2022 Tencent Cloud. All rights reserved.



Parameter description:

Enable/Disable all: Enable/Disable all the rules of the current type.

IDC type: IPs belong to IP libraries of the corresponding type. These IP ranges are often exploited by attackers to deploy bots or proxies rather than normal users. When this item is enabled, the threat intelligence module will identify

©2013-2022 Tencent Cloud. All rights reserved.

the access source from this IDC.

Threat intelligence library:

Bot: The IPs tagged by this intelligence provided by Tencent Security Threat Intelligence and the bot IPs detected by WAF in real time will not be exploited by normal users. After this item is enabled, the threat intelligence module will identify the access sources of bots in Tencent Security Threat Intelligence.

Web attacks: The IPs tagged by this inbound threat intelligence provided by Tencent Security Threat Intelligence launch a large number of attacks containing malicious scans within the intelligence validity. Such IPs will not be exploited by normal users. After this item is enabled, the threat intelligence module will identify the access sources of web attacks in Tencent Security Threat Intelligence.

Web proxy: The IPs tagged by this intelligence provided by Tencent Security Threat Intelligence are exploited by attackers rather than normal users. After this item is enabled, the threat intelligence module will identify the access sources of bots in Tencent Security Threat Intelligence.

Scanner: The IPs tagged by this intelligence provided by Tencent Security Threat Intelligence launch malicious scans on the entire network. After this item is enabled, the threat intelligence module will identify the access sources of scanners in Tencent Security Threat Intelligence.

Account takeover: The IPs tagged by this intelligence launched online identity theft, account blasting, credential stuffing, and other attacks in the past period of time. After this item is enabled, the threat intelligence module will identify the access sources of account takeover attacks in Tencent Security Threat Intelligence.

5. After the configuration, click the configuration page of a certain scenario, and click

in the **Threat intelligence module** section. When the module is enabled for the first time, all the identification items will be enabled. If you enable certain items, you can identify the access sources at different risk levels from the threat intelligence module and IDC.

Best Practices in Configuring Threat Intelligence Module for B2C Website

Overview

B2C feature: B2C faces a large number of users, and user businesses are mainly launched from residential/base station IPs.

Note:

Some businesses have callback APIs that initiate access requests from the IDC side. The number of callback APIs is the collection of multiple users.

Business scheduling APIs may initiate access requests from specific IPs/IDCs.

Users at some of the enterprise egresses will initiate access requests from the IDC.

©2013-2022 Tencent Cloud. All rights reserved.

Configuration process

1. Enable the threat intelligence module.
2. Configure a session policy to identify proxy/IDC access requests through a CAPTCHA.
3. Configure a session policy and set callback API address/business IDC address to **Trust**. This is to avoid blocking business APIs by mistake and thus affecting the business while ensuring the website security.
4. Enable CAPTCHA for applications or sites as needed.

Best Practices in Configuring Threat Intelligence Module for B2B Website

B2B feature: B2B faces a large number of businesses, and customer businesses are mainly launched from the IDC/enterprise egress. A few access sources are from residential/base station IPs.

Note:

Some businesses have callback APIs that initiate access requests from the IDC side. The number of callback APIs is the collection of multiple users.

Business scheduling APIs initiate access requests from specific IPs/IDCs.

Users at some of the enterprise egresses will launch access requests from residential IPs.

Configuration process

1. Enable the threat intelligence module and disable the expected IDC.
2. Configure a session policy to identify residential IP access requests through a CAPTCHA.
3. Configure a session policy and set callback API address/business IDC address to **Trust**. This is to avoid blocking business APIs by mistake and thus affecting the business while ensuring the website security.
4. Enable CAPTCHA for applications or sites as needed.

©2013-2022 Tencent Cloud. All rights reserved.

Bot Flow Statistics Module

Last updated：2023-12-29 14:43:37

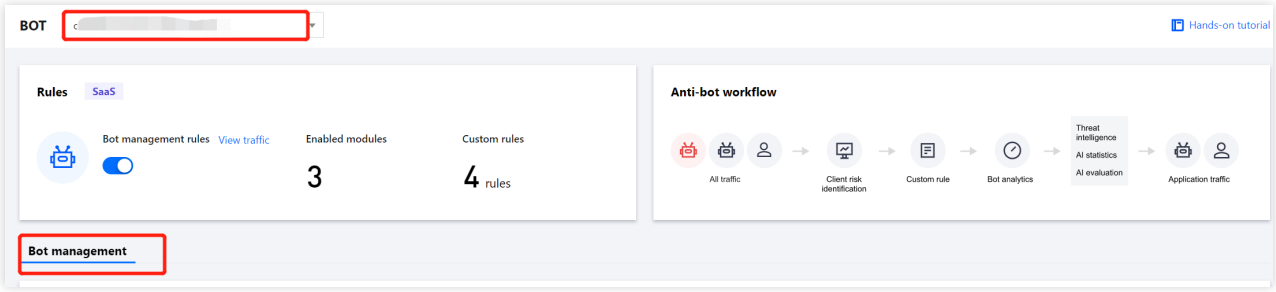
This document describes how to configure the bot flow statistics module in the bot analytics section of bot traffic management. Using big data analytics and statistics and AI technology, it automatically identifies malicious users based on characteristics of user traffic.

Prerequisites

You have purchased a WAF instance and bot traffic management extra pack and enabled bot analysis for WAF-connected domain names.

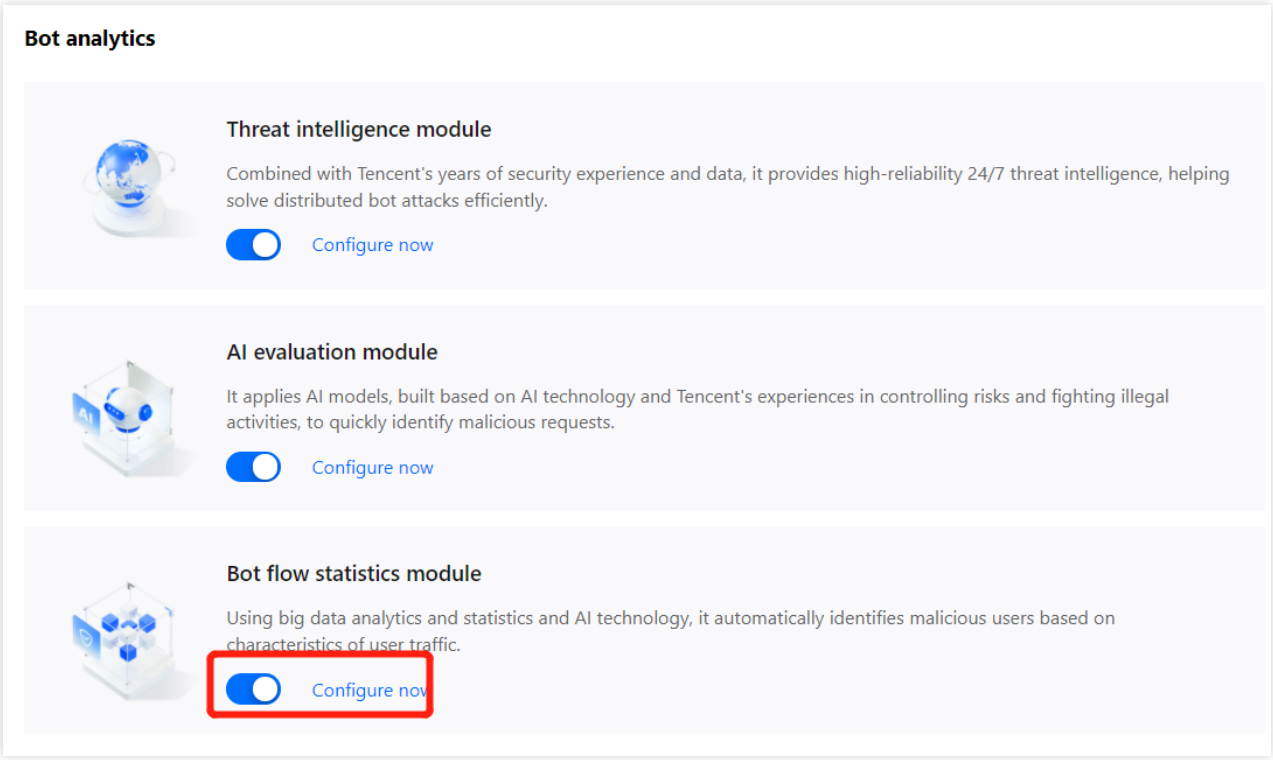
Protection Configuration

1. Log in to the WAF console and select **Configuration center** > **Bot and application security** on the left sidebar.
2. On the **Bot and application security** page, select the target domain name in the top-left corner and click **Bot management**.



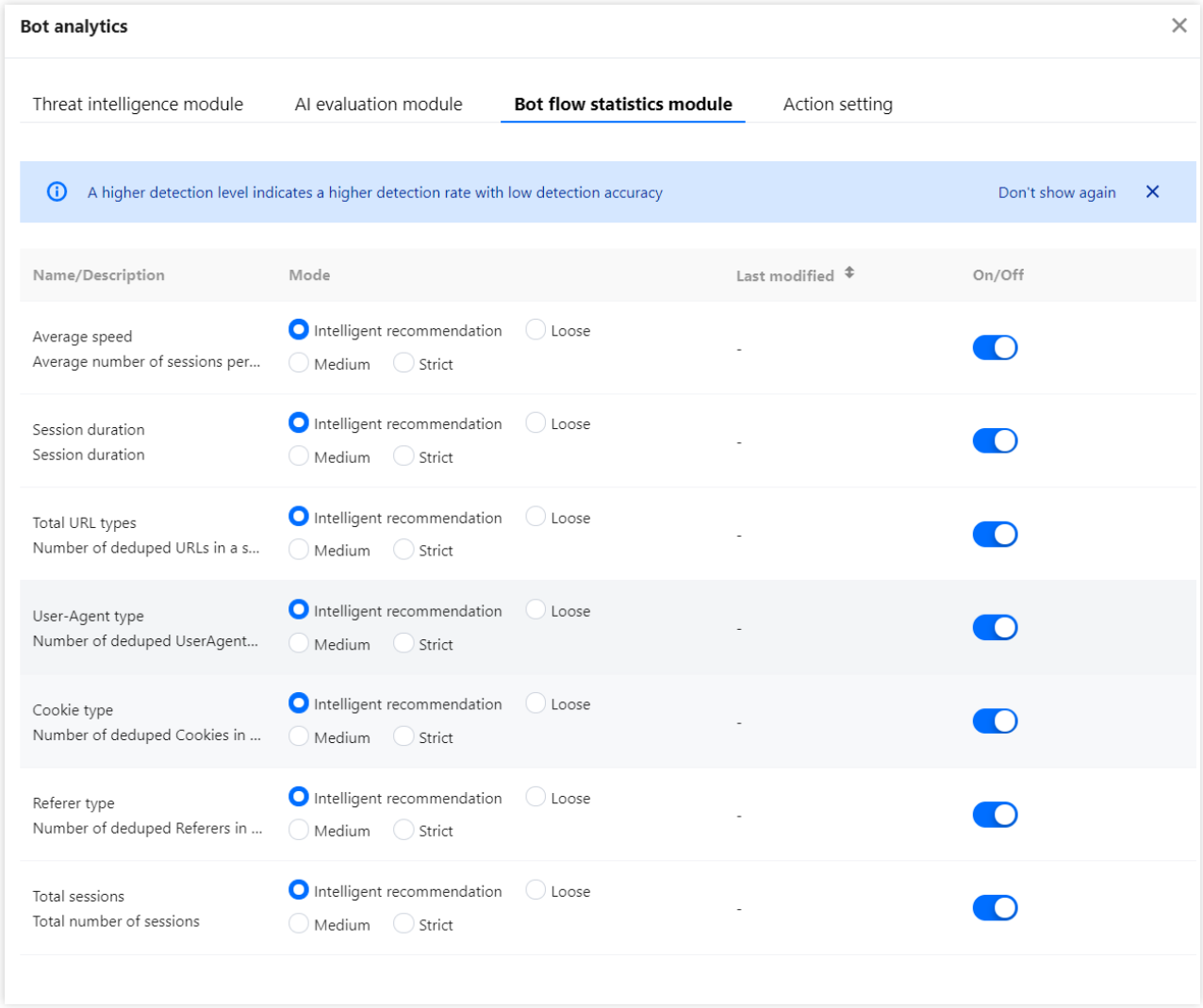
3. In **Global settings**, click **Configure now** in the **Bot flow statistics module** section.

©2013-2022 Tencent Cloud. All rights reserved.



4. On the **Bot flow statistics module** page, you can configure the detection level of different features.

©2013-2022 Tencent Cloud. All rights reserved.



Parameter description:

Name/Description:

Referer type: The number of deduped Referers in a session request is detected, with different thresholds for detecting an access request with a higher value than the corresponding threshold.

Total URL types: The number of deduped URLs in a session request is detected, with different thresholds for detecting an access request with a higher value than the corresponding threshold.

User-Agent type: The number of deduped User-Agents in a session request is detected, with different thresholds for detecting an access request with a higher value than the corresponding threshold.

Cookie type: The number of deduped cookies in a session request is detected, with different thresholds for detecting an access request with a higher value than the corresponding threshold.

Total sessions: The total number of sessions is detected, with different thresholds for detecting an access request with a higher value than the corresponding threshold.

Average speed: The average number of sessions per minute is detected, with different thresholds for detecting an access request with a higher value than the corresponding threshold.

©2013-2022 Tencent Cloud. All rights reserved.

Session duration: The session duration is detected, with different thresholds for detecting an access request with a higher value than the corresponding threshold.
Mode: Different detection levels correspond to different thresholds, which fluctuate with the number of website access requests.
A higher detection level indicates a higher detection rate with a lower detection accuracy.
A lower detection level indicates a lower detection rate with a higher detection accuracy.
Intelligent recommendation automatically learns the historical traffic of your website to generate a recommended detection level in Tencent Security bot traffic management. The detection level is either loose or medium according to the current bot situation at your website.
On/Off: You can enable or disable the detection type of the current option. After this option is disabled, the detection item will not contribute to the bot score.
5. After the configuration, click the configuration page of a certain scenario, and click

of the **Bot flow statistics module**.

Best Practices of Bot Flow Statistics Module

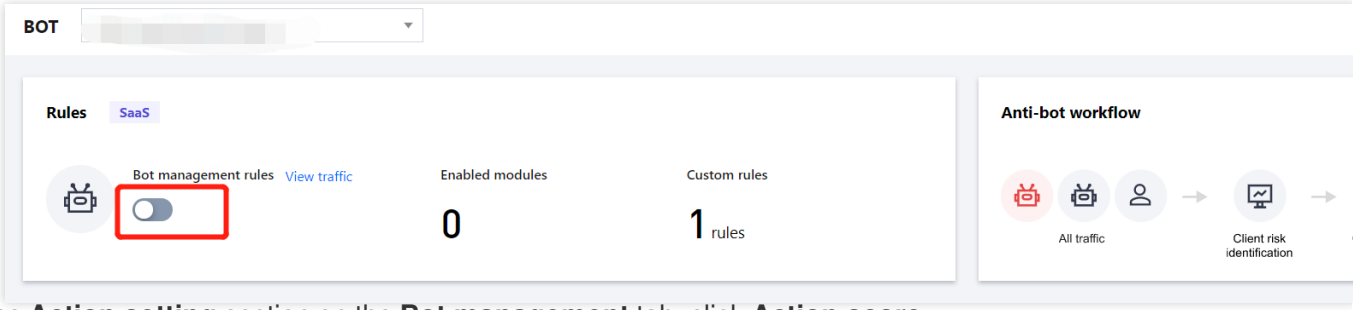
The bot flow statistics module leverages the bot defense experience and accumulation of the bot attack/defense lab to quickly identify abnormal access behaviors. Therefore, we recommend you enable it and set **Rule level** to **Intelligent recommendation** under any circumstances.

©2013-2022 Tencent Cloud. All rights reserved.

Action Settings

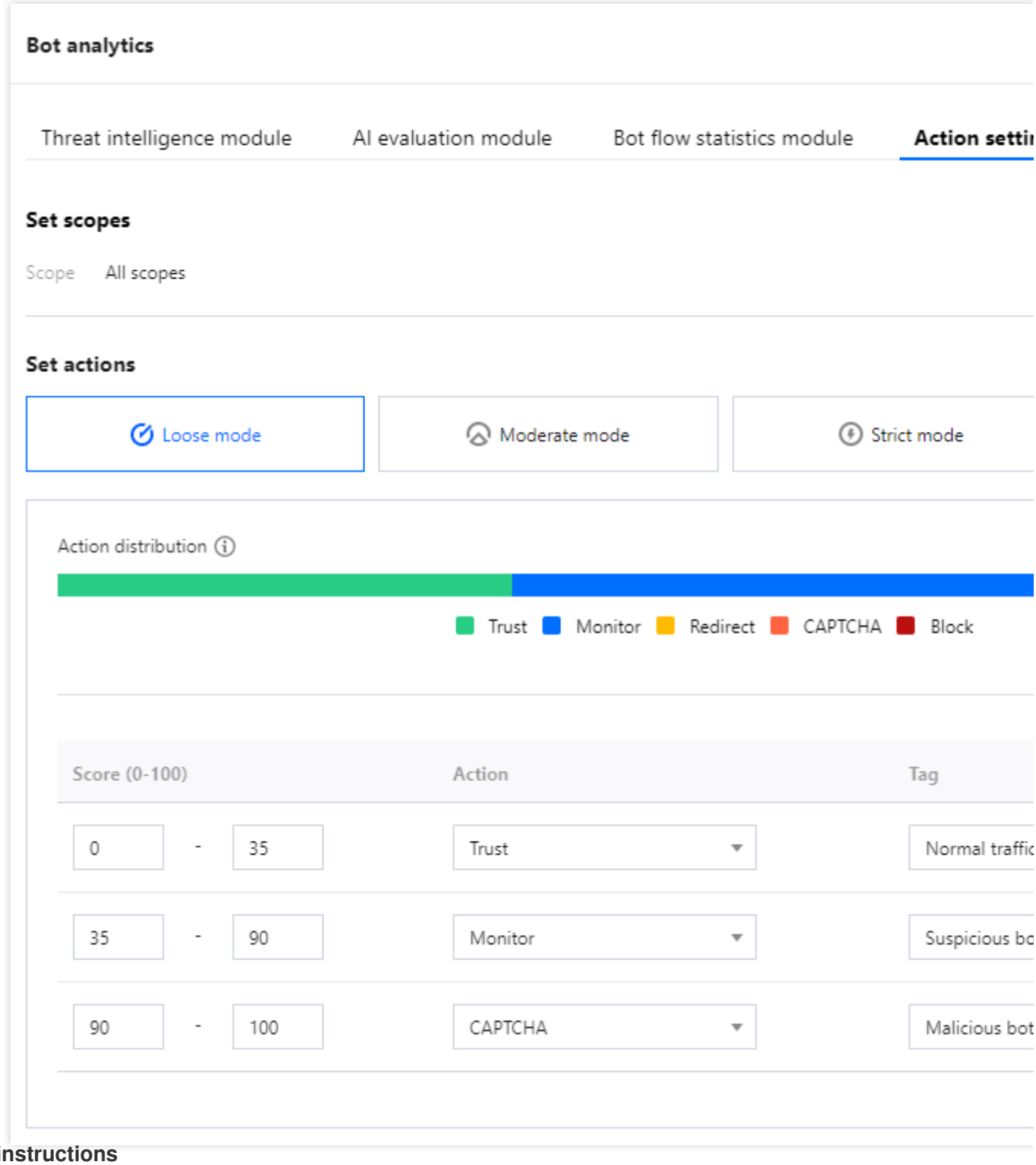
Last updated：2023-12-29 14:43:49

1. Log in to the WAF console and select **Configuration center** > **Bot and application security** on the left sidebar.
2. On the **Bot and application security** page, select the target domain name in the top-left corner and click **Bot management**.



3. In the **Action setting** section on the **Bot management** tab, click **Action score**.
4. On the **Action setting** tab, you can configure different action policies, the scope of each action policy, and actions in different score ranges to precisely block risky access requests.

©2013-2022 Tencent Cloud. All rights reserved.



Use instructions

Action policy: Currently, you can select multiple action policies for one bot scenario.

Scope: It can be **All scopes** or **Custom scope**. Traffic hitting the scope will be precisely blocked based on the actions in different score ranges.

Mode: By default, there are loose, moderate, strict, and custom modes. The first three modes are preset, representing different recommended categories and handling policies for bots at different risk levels in bot behavior management. Once modified, they become the custom mode.

©2013-2022 Tencent Cloud. All rights reserved.

Score range: A score ranges from 0 to 100. Ten score entries can be added to each range, which is left-closed and right-open and cannot be overlapped. You can set a range to null, and then no action will be processed in it.
Action: You can set an action to **Trust**, **Monitor**, **Redirect** (to a certain website URL), **CAPTCHA**, or **Block**.
Tag: You can set a tag of **Friendly bots**, **Malicious bots**, **Normal traffic**, or **Suspicious bots**.
Friendly bots: The bot is friendly and legal for the website by default.
Suspicious bots: The system finds the access source traffic suspicious but cannot determine if it is malicious to the website.
Normal traffic: The access traffic is regarded as from a real user.
Malicious bots: The bot has malicious traffic and is unfriendly to the website.
5. After completing the configuration, click **Publish** in the bottom-left corner of the page.

©2013-2022 Tencent Cloud. All rights reserved.

Bot Traffic Analysis

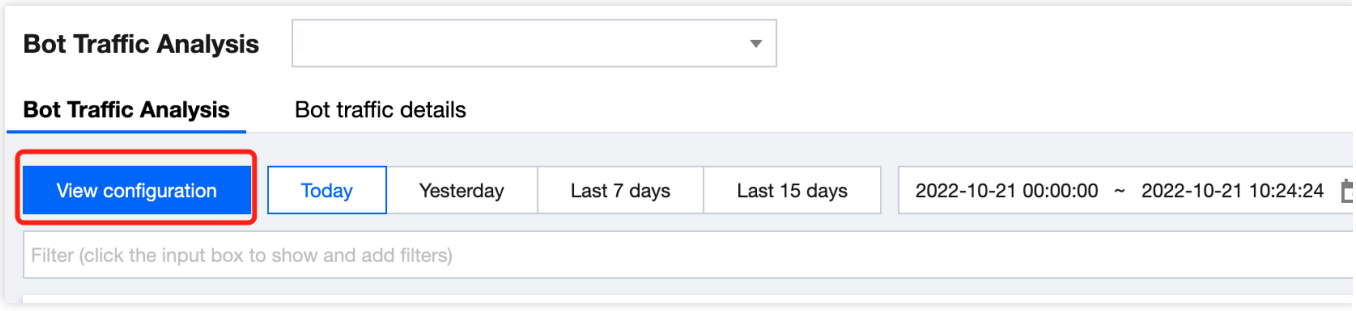
Last updated：2023-12-29 14:44:17

Background

The bot traffic management feature can differentiate between friendly and malicious bots and crawlers and implement corresponding management policies such as letting through the traffic of search engine bots, blocking the traffic of malicious item information crawlers, delaying responses, or adopting different response time periods. This feature reduces resource consumption, information leakage, and failed marketing caused by malicious bots and crawlers on the one hand and ensures normal operations of friendly ones (such as search engine bots and advertising programs) on the other hand.
With bot traffic analysis, you can collect data from bot traffic management and quickly understand how a selected domain name with bot traffic analysis enabled is affected by bots. You can also view the bot classification trend, action trend, bot score distribution, top statistics by request count, and list of URLs vulnerable to attacks.

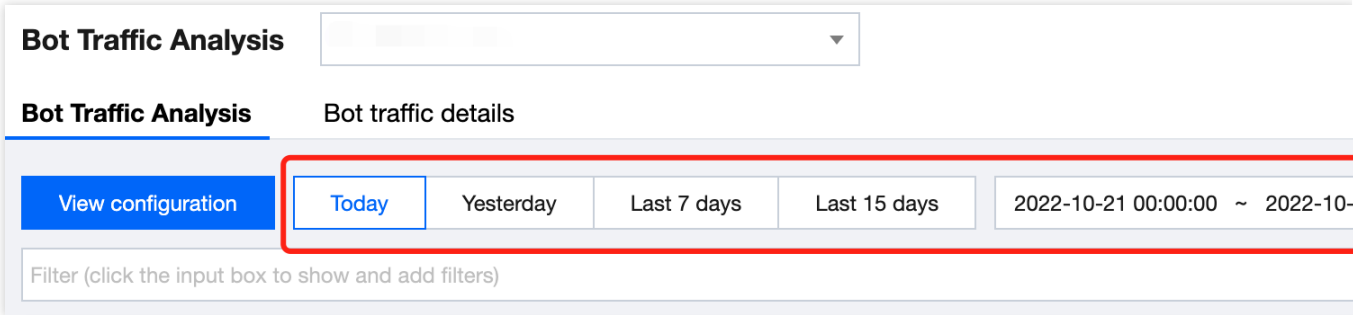
Directions

1. Log in to the WAF console and select **Bot traffic analysis** on the left sidebar.
2. On the **Bot traffic analysis** page, click the **All domain names** drop-down list in the top-left corner and select the target domain name.
3. Select **Not all domain names** and click **View configuration** in the top-left corner to enter the **Bot and application security** page for the corresponding domain name.

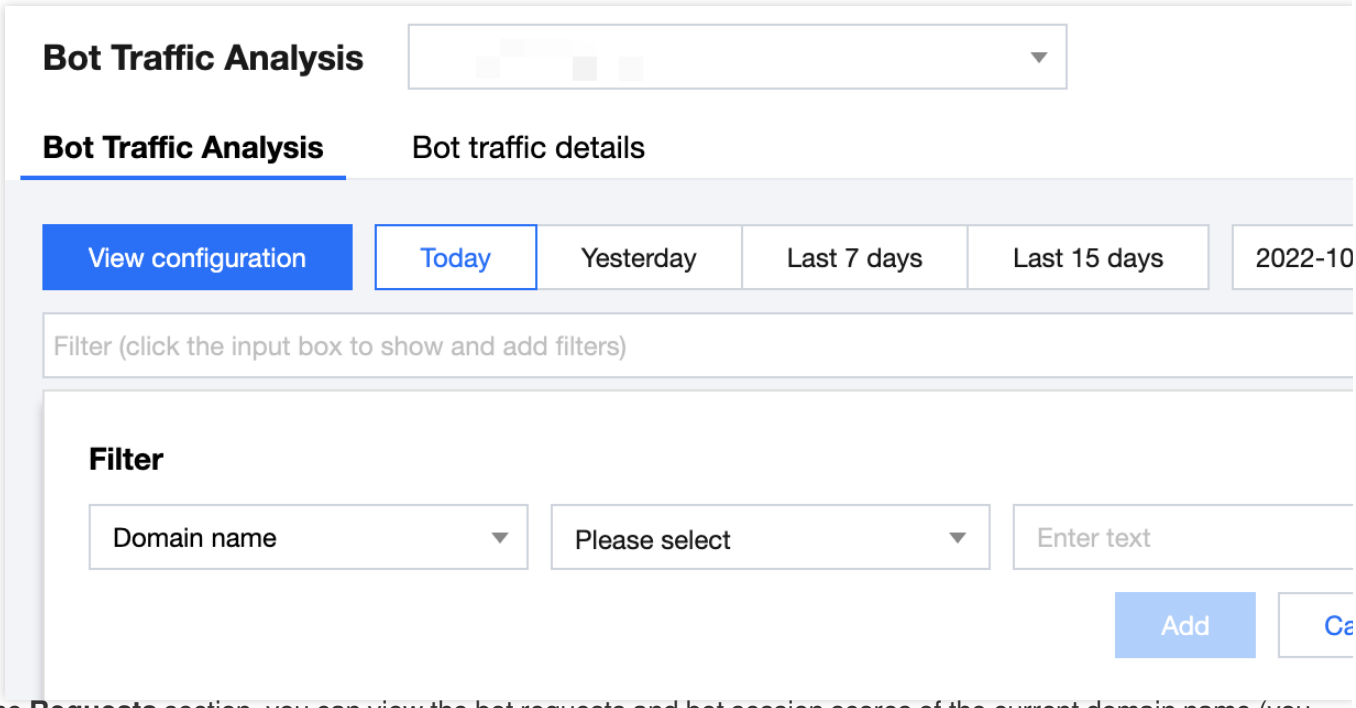


4. On the **Bot traffic analysis** page, search for the protection data of a domain name by **Time** or **Filter**.
You can search for the bot protection effect data of a domain name in the specified time period.

©2013-2022 Tencent Cloud. All rights reserved.



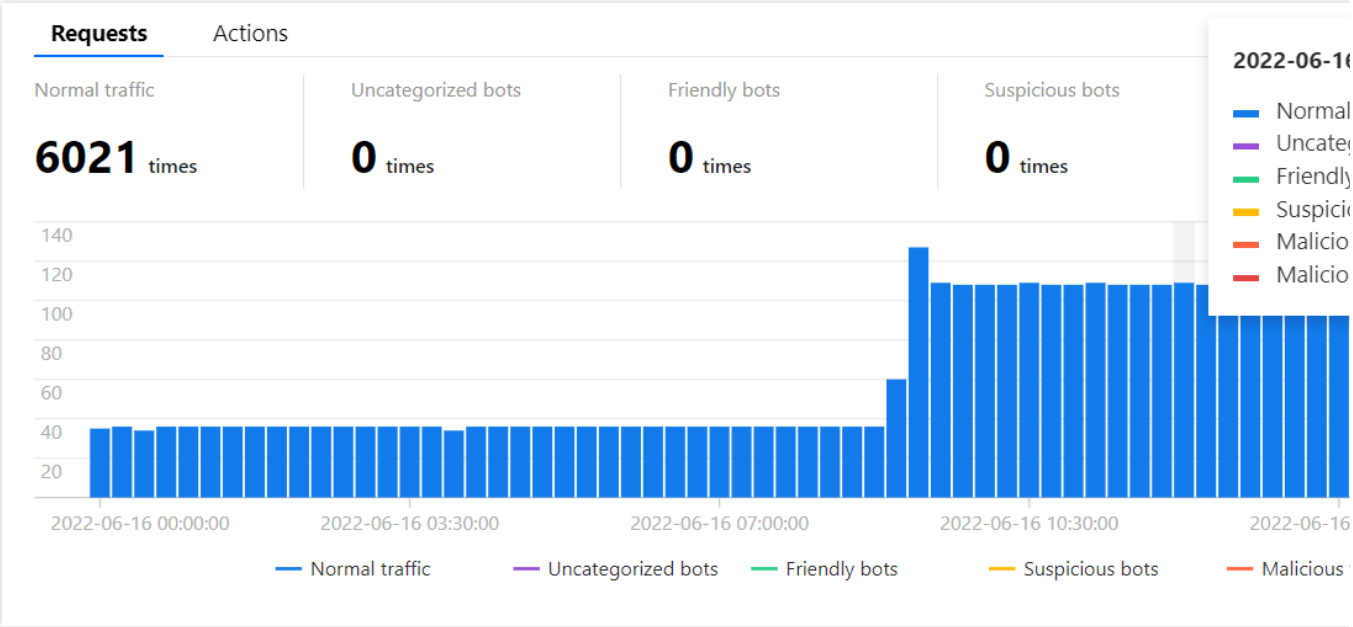
Click **Filter** to display the bot traffic analysis filter.



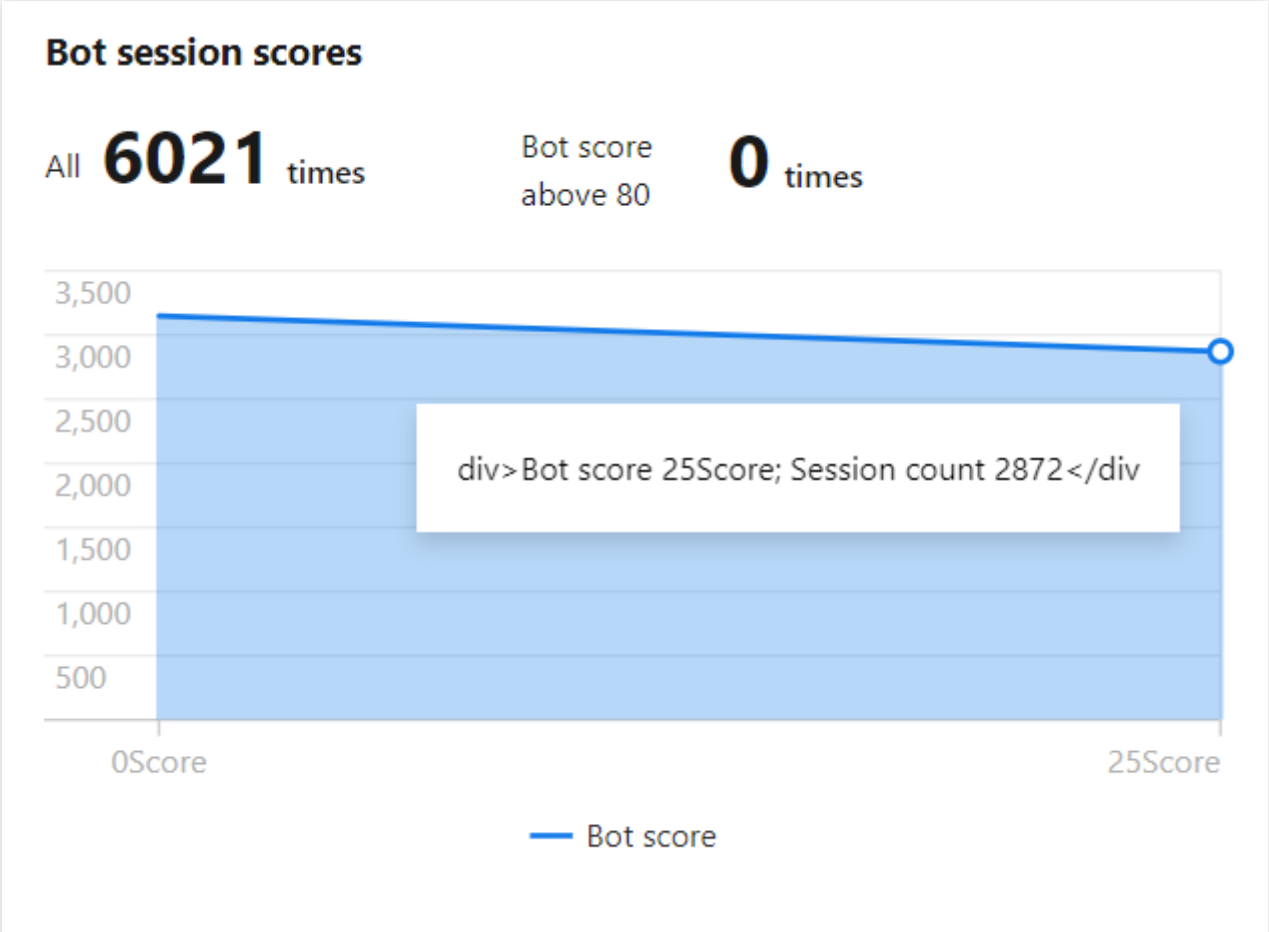
5. In the **Requests** section, you can view the bot requests and bot session scores of the current domain name (you can select a global domain name).

Bot requests chart: Group different bot scores into different ranges according to the configured action and tag, score and tag each traffic request accessing the website, and display the result on the chart.

©2013-2022 Tencent Cloud. All rights reserved.

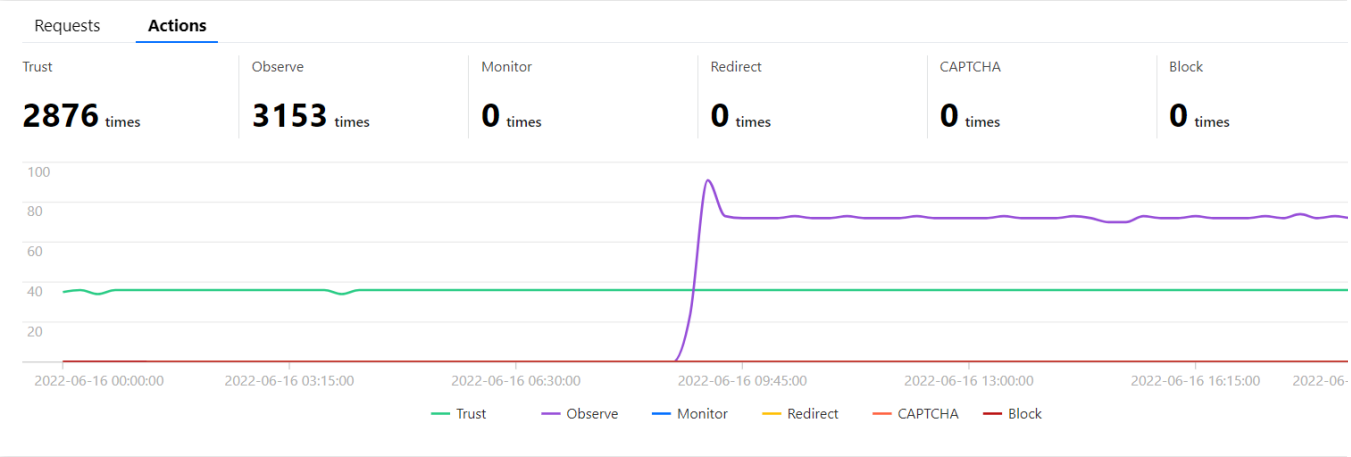


Bot session scores: It's a chart displaying the bot traffic risk distribution in a domain name of the current user, including the access traffic trend. You can set bot scores accordingly. The higher the scores, the larger the impact of the bots.

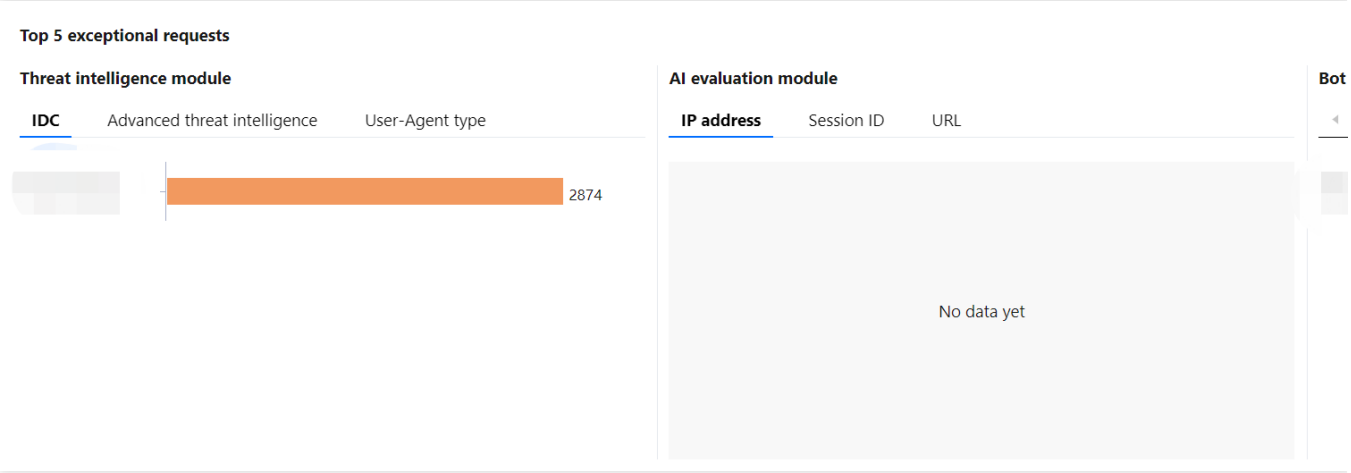


6. Click **Actions** to view the actions on traffic of the current domain name (or a global domain name) by bot traffic management and its percentage to the actions on all the request traffic.

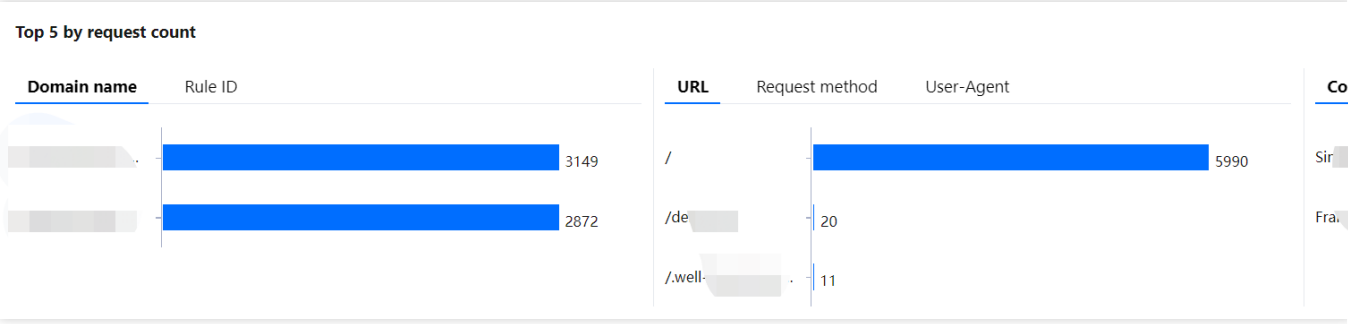
©2013-2022 Tencent Cloud. All rights reserved.



7. The **Top 5 exceptional requests** section displays the top 5 key-value pairs and quantity of abnormal bot features in a certain time period. The statistical chart is subject to the filter and the time of the traffic trend comparison chart. Click **Bar chart** to view the key-value pair information. Click **Filter** or **Exclude** to quickly add a filter.

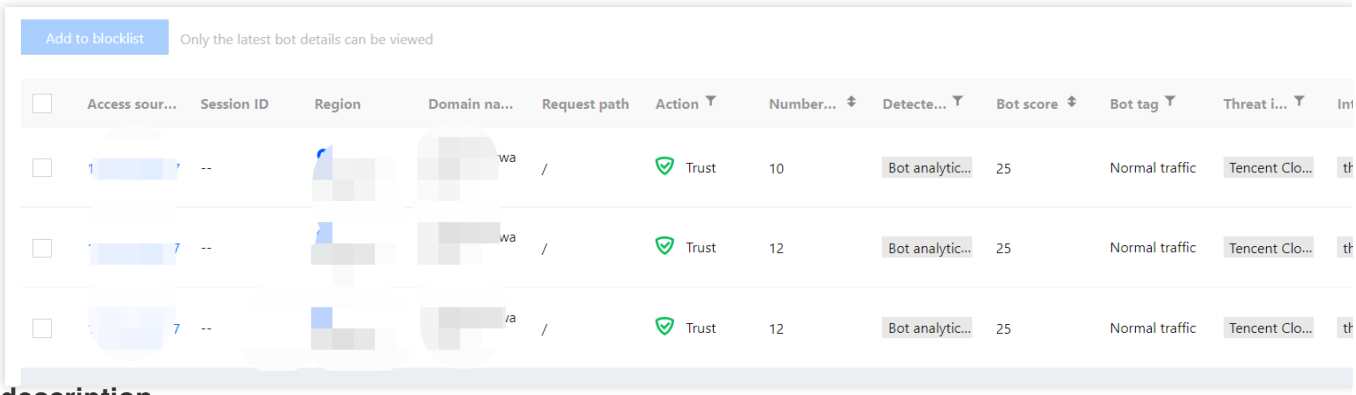


8. The **Top 5 by request count** section displays the top 5 key-value pairs and number of bot features in a certain time period. The statistical chart is subject to the filter and the time of the traffic trend comparison chart. Click **Bar chart** to view the key-value pair information. Click **Filter** or **Exclude** to quickly add a filter.



©2013-2022 Tencent Cloud. All rights reserved.

9. The affected asset statistical list displays the URLs most affected by bots and the actions performed by bot traffic management. The entries are aggregated once every five minutes.



Field description

Access source: Source of the access request.

Session: A single connection establishment session.

Region: Geographical location of the access request.

Domain name: Access domain name.

Request path: URI of the access request.

Action: Action performed by bot traffic management.

Access count: Number of sessions.

Detected module: Hit modules.

Bot score: Bot score of the current access request in the aggregated dimension.

Bot tag: Bot tag hit by the current access request in the aggregated dimension.

Threat intelligence module: Match tag hit by the current bot in the threat intelligence module.

Analysis of hits: Displays the exceptions in the current access request that hit the bot analytics module in the aggregated dimension.

Type of exceptions: Displays the exceptions discovered by the bot flow statistics module in the aggregated dimension.

Logging time: Time when bot access is discovered.

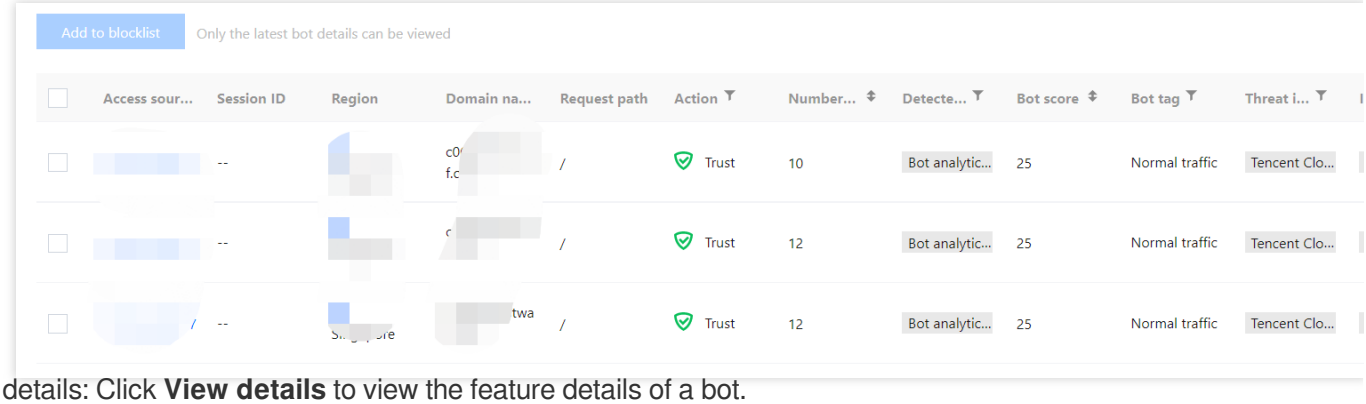
Operation:

View logs: Click **View logs** to view the access log of a bot.

Note:

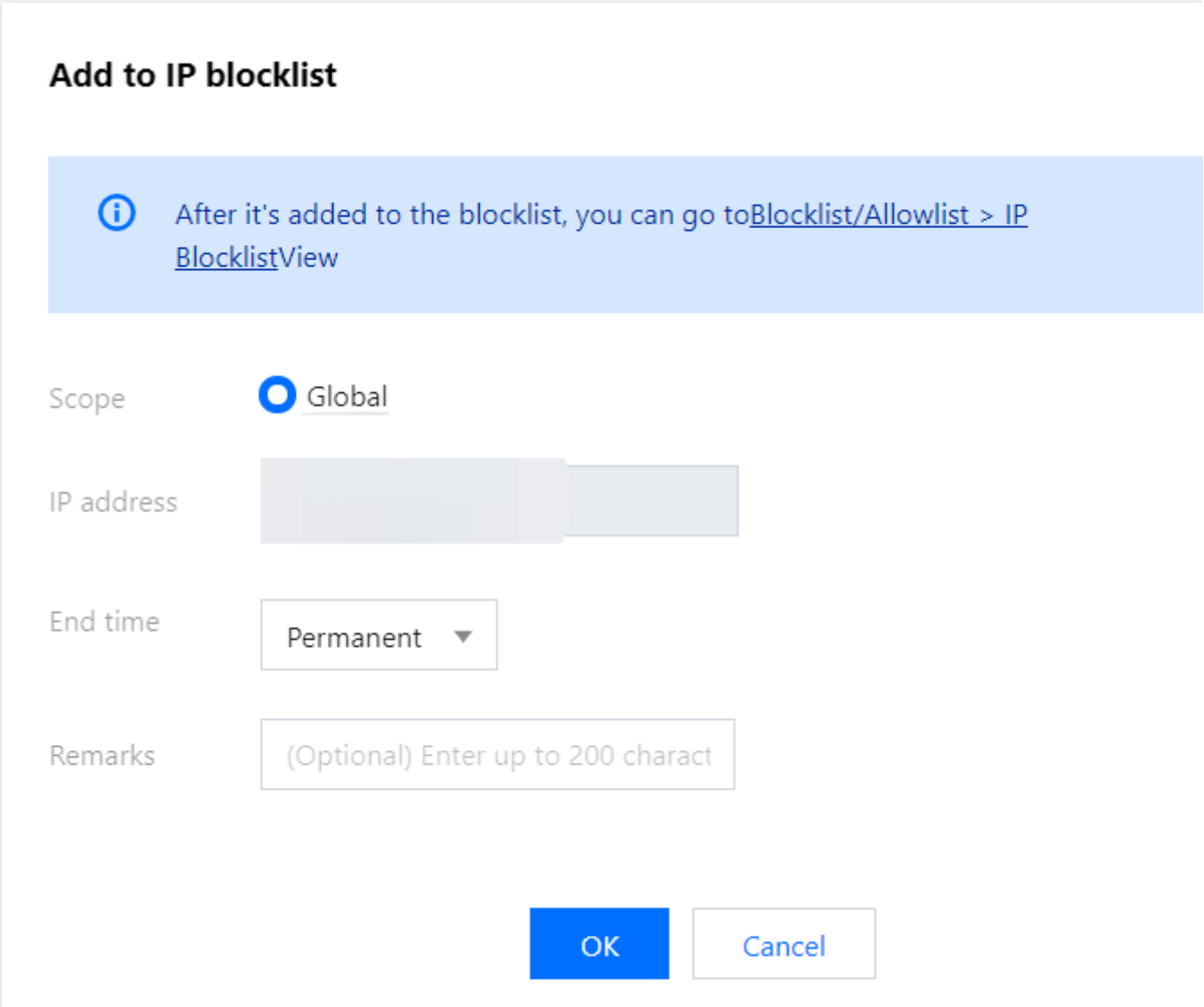
To view access logs, you need to subscribe to the access logging service.

©2013-2022 Tencent Cloud. All rights reserved.



View details: Click **View details** to view the feature details of a bot.

Add to blocklist: Click **Add to blocklist**, configure parameters, and click **OK**.



©2013-2022 Tencent Cloud. All rights reserved.

Bot Traffic Details

Last updated：2023-12-29 14:44:34

Overview

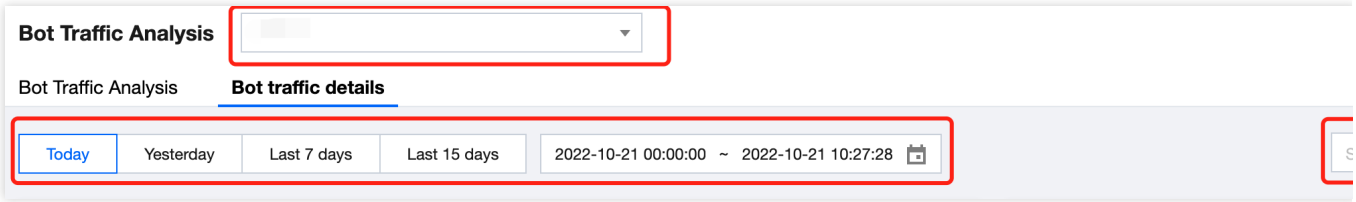
With data provided by the bot traffic management module, bot traffic analysis quickly analyzes the bot impacts on domain names in terms of bot feature metrics, including the types of bots, proportion of actions, bot score distribution, top data by request count and URLs that may be affected. You can click **View details** to view the bot details of an access source, and its access characteristics and exceptions detected.
The bot traffic details section displays the bot traffic details of top 10 access sources. You can also view their session access information and logs if session settings are configured, and the information of these access sources/IPs by retrieval.

Prerequisites

You have subscribed to the bot traffic management service and enabled bot traffic analysis.

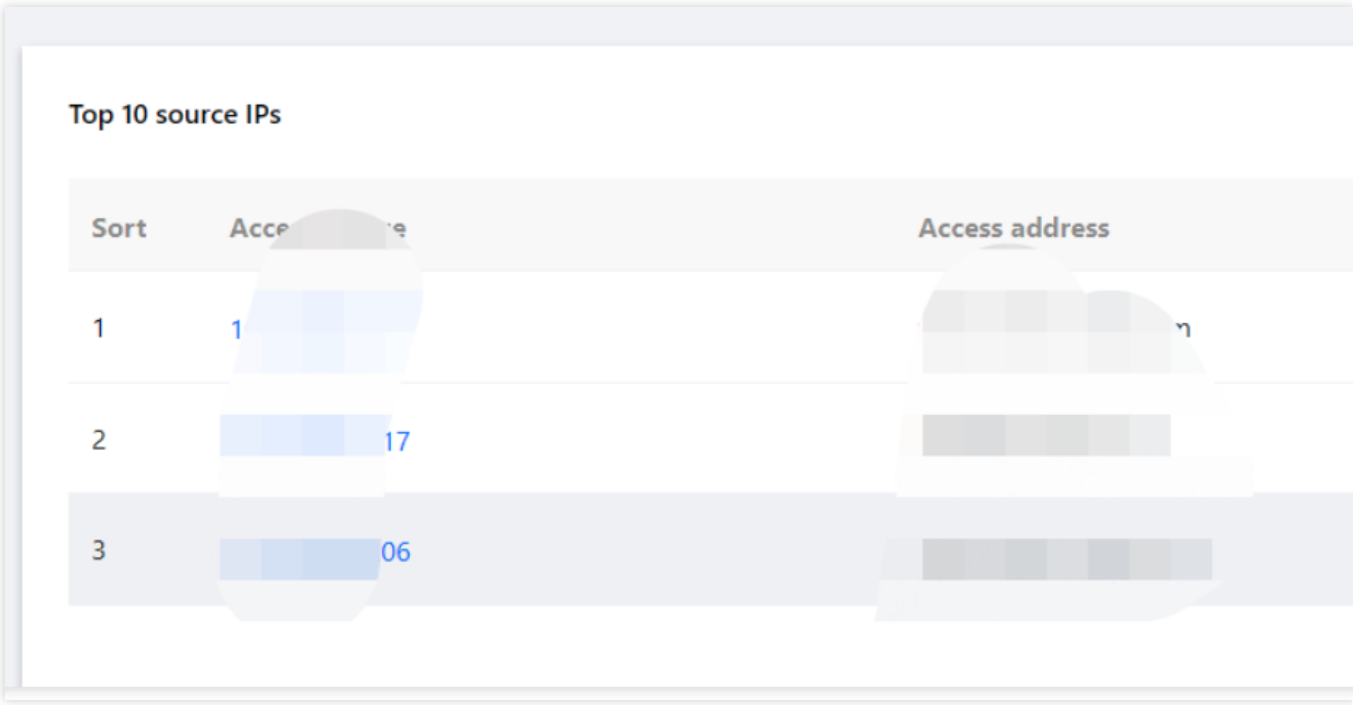
Directions

1. Log in to the WAF console and select **Bot Traffic Analysis** on the left sidebar. Open the **Bot traffic details** tab.
2. On the page displayed, click the drop-down list in the upper-left corner and select a domain name.
3. Specify a date or use the filter to search top 10 access sources of all domain names or a specific domain name. Then click **View logs** of the access source you want to view.



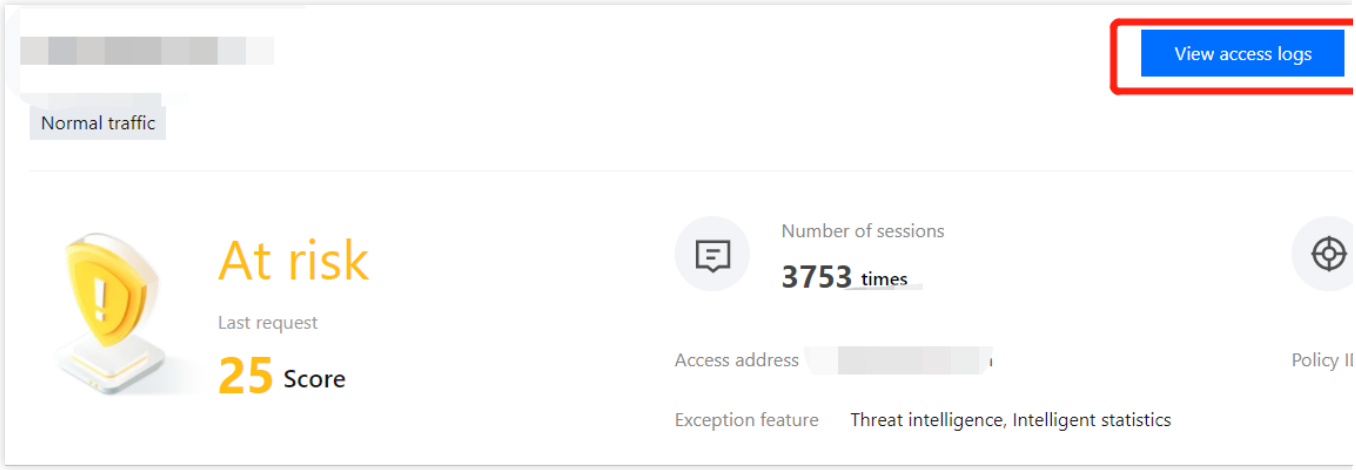
4. To view traffic details of an access source, click **View details** on the right.

©2013-2022 Tencent Cloud. All rights reserved.



Viewing access overview

The bot traffic details page shows you the estimated risk value of the access source and the information of the hit policy, and allows you to take measures such as adding the access source to the allowlist/blocklist and creating custom rules targeting the access source.



Field description:

IP address and tag: It displays the IP address of an access source and the hit tag that identifies the bot category.

Last request: It displays the score of the last access request from the access source and the risk level.

Session count: It displays the number of continuous sessions on the website accessed occurred in the last access request.

Access address: It displays the domain name of the access source.

©2013-2022 Tencent Cloud. All rights reserved.

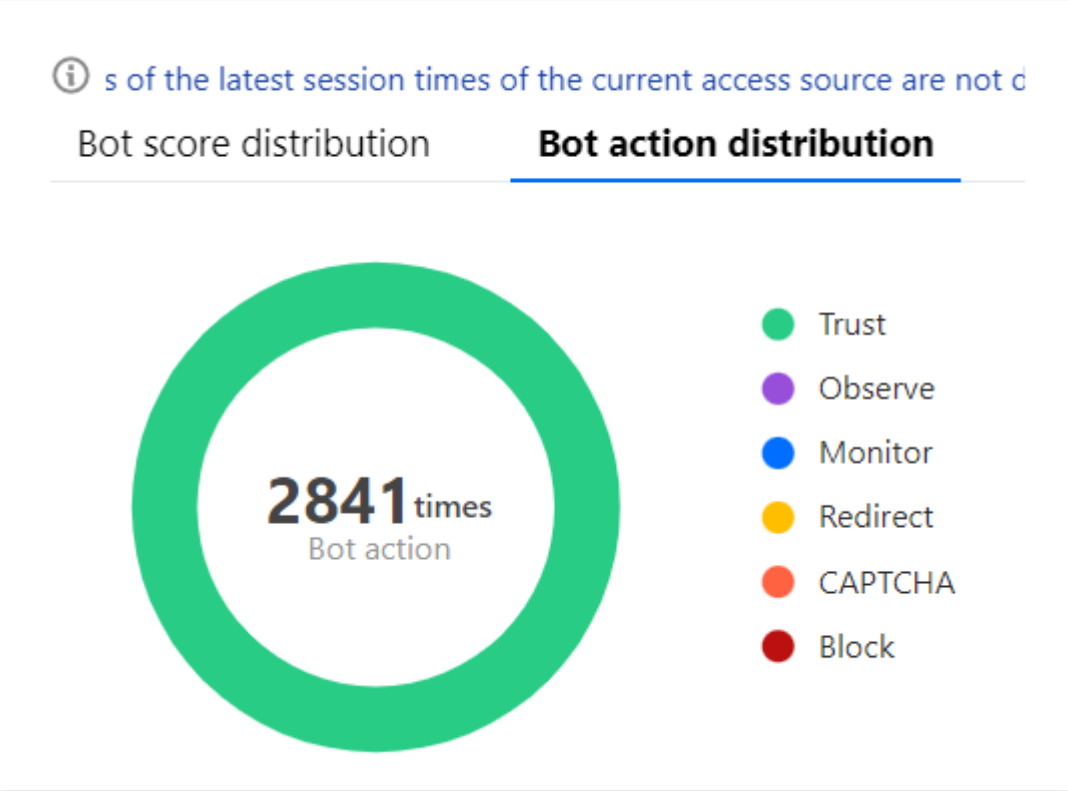
Exception feature: It displays modules that detect exceptional features of the access source.
Hit modules: It displays modules that take actions to combat bots.
Policy ID: It is the ID of a hit policy.
View access logs: It redirects you to the access logs page where you can view the access details of the access source.
Add to allowlist: It allows you to add the access source to the allowlist.
Add to blocklist: It allows you to add the access source to the blocklist.
Add custom rules: It allows you to add custom rules targeting the access source.

Viewing bot scores

In the bot score distribution and bot action distribution sections, you can view the distribution of bot scores and bot actions within the selected period, helping you determine the risk level of the access source.

Viewing bot information

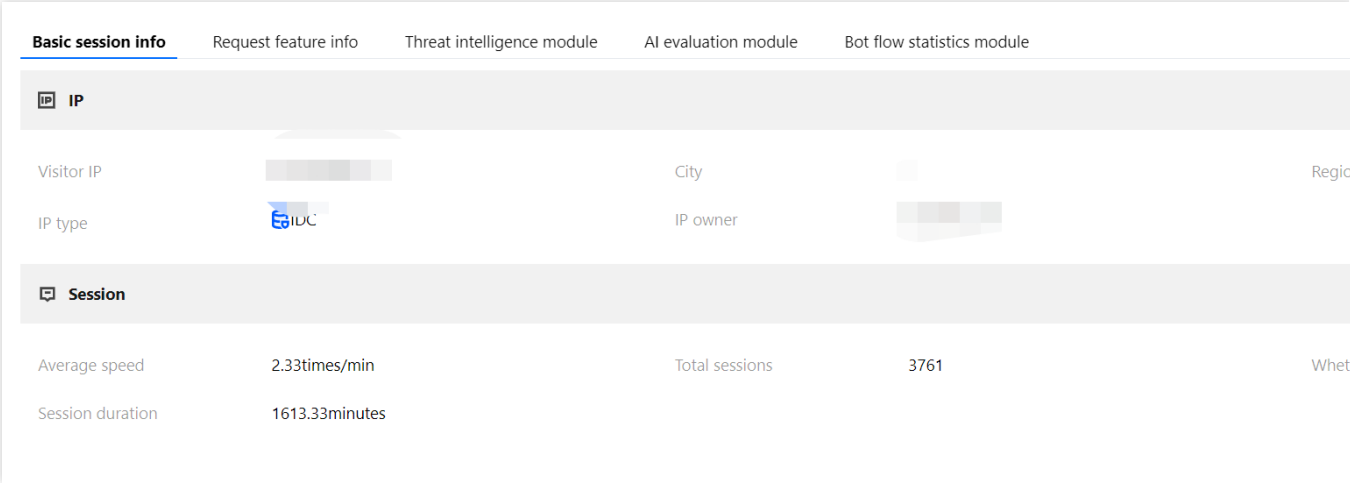
The bot traffic details page also displays information of the automated access source including the features of the bot and access request, threat intelligence and AI evaluation information, bot flow statistics and sessions. Using this data, you can quickly identify exceptions in the access request and take measures against the bot.



Basic session information

On the basic session information tab, you can view the information of the access source IP and session separately.

©2013-2022 Tencent Cloud. All rights reserved.



Field description:

IP information

Access source IP: IP address of an access source.

City: City where the access source is located.

Region: Country where the access source is located.

IP type: IP type of the access source.

IP owner: IP owner of the access source.

Session information

Session average speed: The average session speed of the access source in the latest session, which is calculated by the total number of session requests/session duration. Unit: times/minute.

Total sessions: The total number of sessions of the access source in the latest session.

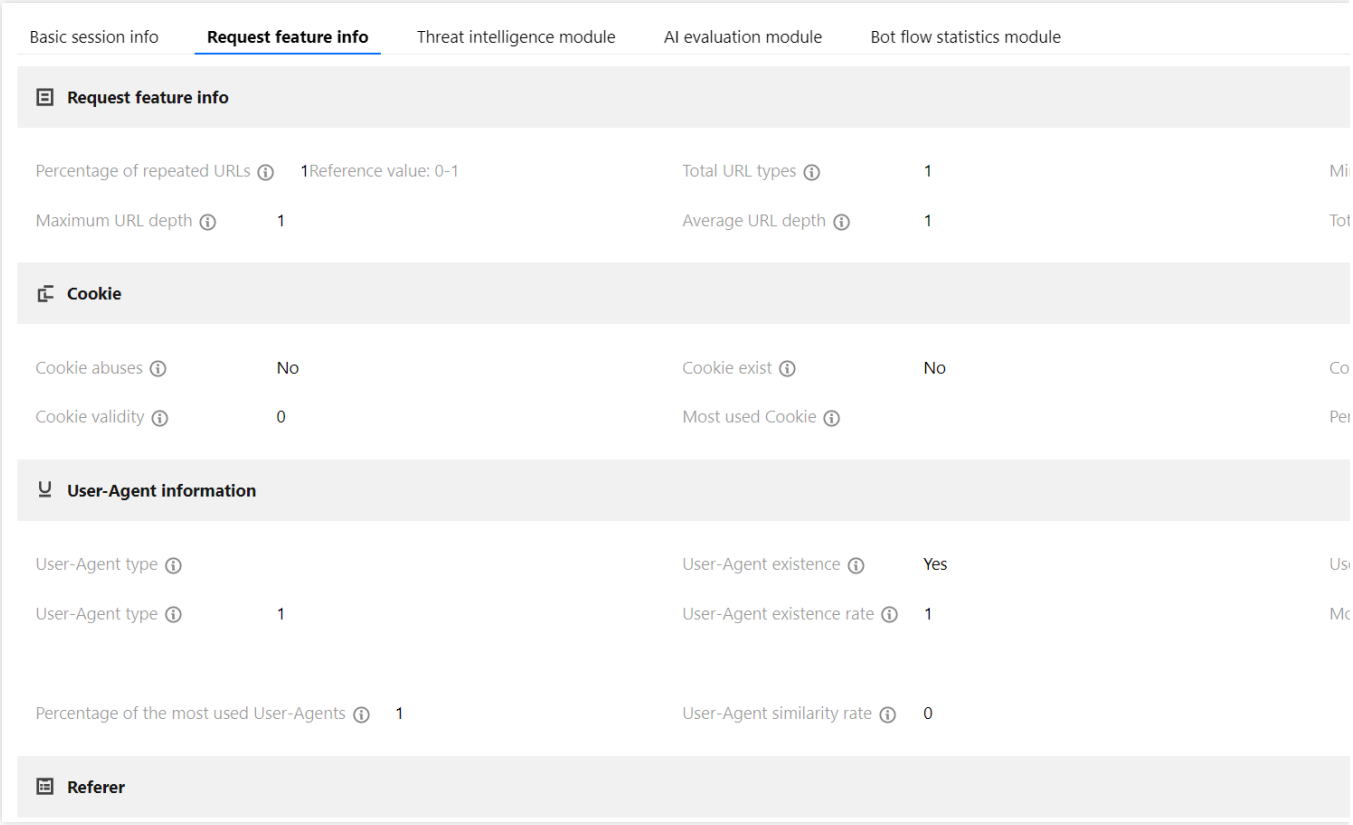
Whether Robots.txt exists: Whether the access source has accessed the Robots.txt file, which is often accessed by bot sessions.

Session duration: Amount of time the latest session initiated by the access source.

Request feature information

On the request feature information tab, you can view the information of the request features, Cookie, User-Agent, Referer, and Query in the session request.

©2013-2022 Tencent Cloud. All rights reserved.



Field description:

Type	Metric	Description
Request feature information	Percentage of repeated URLs	Percentage of the repeated URLs in a session request. The value range is 0-1. Set this parameter based on your actual business needs. A value that is too high or too low suggests an exception (which must be determined based on the actual business conditions).
	Total URL types	Number of deduplicated URLs in a session request.
	Minimum URL depth	Minimum directory levels of URLs in a session request.
	Maximum URL depth	Maximum directory levels of URLs in a session request.
	Average URL depth	Average directory levels of URLs in a session request.
	Total URLs	Total number of URLs visited in a session request (including duplicates).
Cookie information	Whether Cookie is	Different types of UAs use the same Cookie.

©2013-2022 Tencent Cloud. All rights reserved.

	abused	
	Cookie exist	Whether the Cookie exists in all session requests.
	Percentage of repeated Cookies	Percentage of the repeated Cookies in a session request. The value ranges from 0-1.
	Cookie validity	Percentage of the Cookies that can be parsed in a session request.
	Most used Cookie	Most used Cookies in a session request.
	Percentage of the most used Cookies	Percentage of the most used Cookies in a session request.
User-Agent information	User-Agent type	User-Agent type of the request user in a session request.
	User-Agent exist	Whether User-Agent exists in a session request.
	User-Agent randomness index	Random distribution of User-Agents in a session request. When the reference value threshold exceeds 0.6, an exception is suspected; when it exceeds 0.92, an exception is basically confirmed.
	User-Agent type	Number of deduplicated User-Agents in a session request, which is valid only for non-proxy IPs. A value that is too high suggests an exception (which must be determined based on the actual business conditions).
	User-Agent existence rate	Existence rate of UAs in a session request, which ranges from 0 to 1. A value too small may be suspected as an exception (which must be determined based on the actual business conditions).
	Most used User-Agent	Most used value of the HTTP User-Agent in a session request.
	Percentage of the most used User-Agents	Percentage of the most used HTTP User-Agent values in a session request.
	User-Agent similarity rate	Similarity between the most used value and the rest in a session request.
Referer information	Percentage of repeated Referers	Percentage of repeated Referers in a session request, which is valid only for access through

©2013-2022 Tencent Cloud. All rights reserved.

		browsers and ranges from 0 to 1. A value that is too high suggests an exception (which must be determined based on the actual business conditions).
	Referer exist	Existence rate of Referers in a session request, which ranges from 0 to 1. A value too small may be suspected as an exception. It's available for browser access.
	Referer existence rate	Existence rate of Referers in a session request, which ranges from 0 to 1. A value too small may be suspected as an exception. It's available for browser access.
	Whether Referer is abused	Different types of UAs use the same Referer.
	Most used Referer	Most used value of the HTTP Referer in a session request.
	Percentage of the most used Referers	Percentage of the most used HTTP Referer values in a session request.
Query information	Percentage of repeated Query parameters	Percentage of repeated GET request parameters (`Query` content) or POST request parameters (`Body` content) in a session request, which ranges from 0 to 1. Set this parameter based on your actual business needs. A value that is too high or too low suggests an exception (which must be determined based on the actual business conditions).
	Total query parameter types	Most used parameters in a session request, which may be GET request parameters (`Query` content) or POST request parameters (`Body` content).

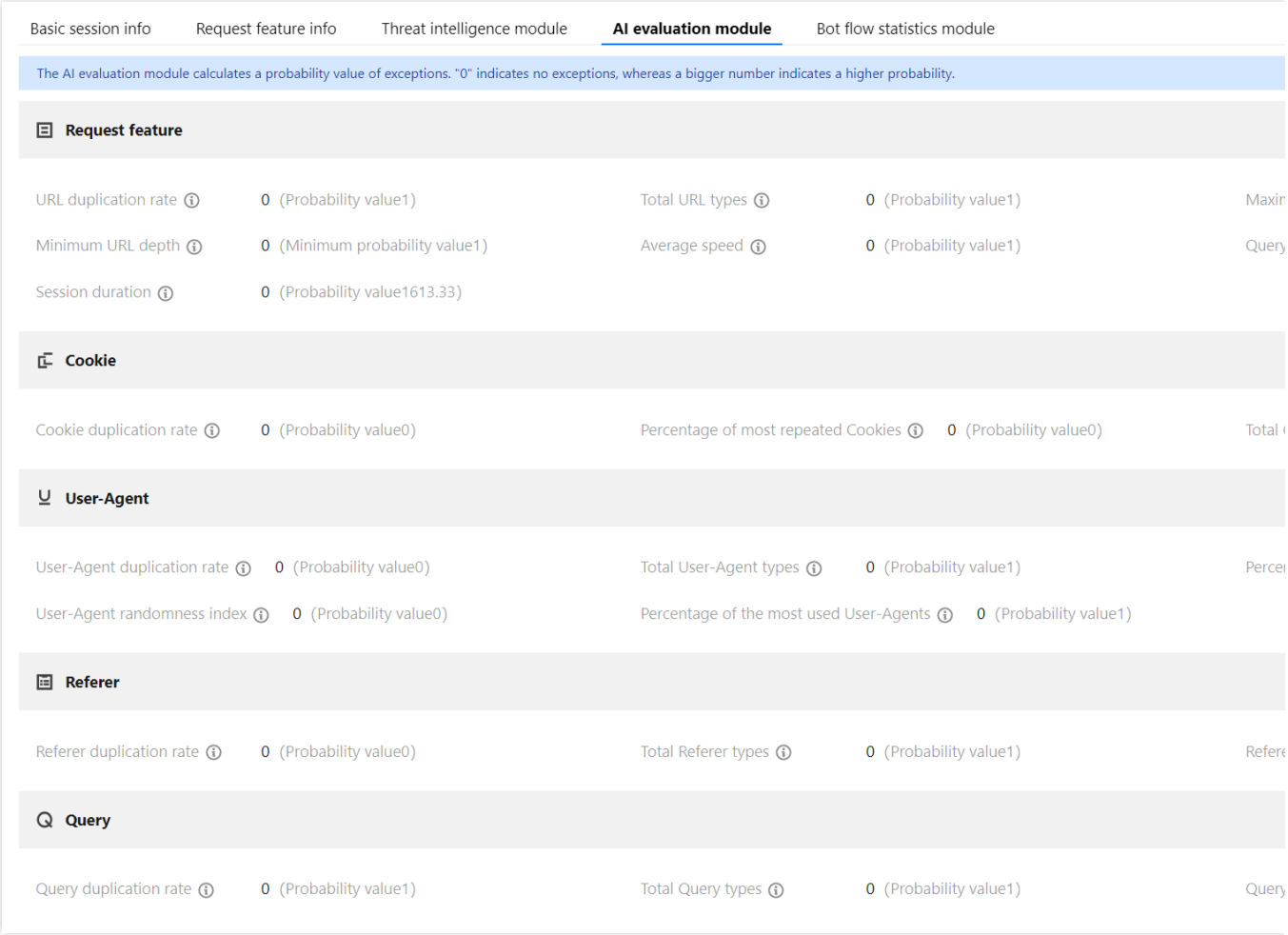
Threat intelligence

The threat intelligence tab displays the known information that matches the current access source IP/session ID, such as the IDC details of the access source.
IDC details: If the information of the access source includes the IDC, the IDC information will be displayed.
Threat Intelligence: If the IP information of the access source is matched, the matched tag and its definition will be displayed.

AI evaluation

©2013-2022 Tencent Cloud. All rights reserved.

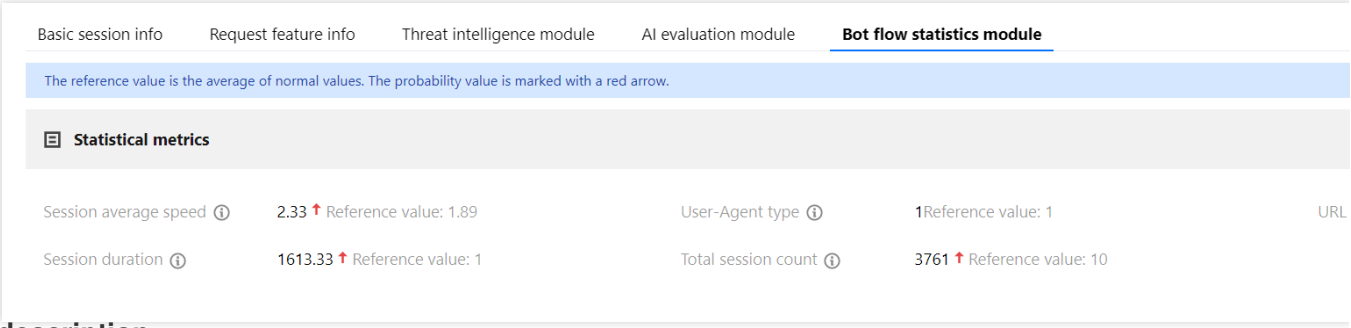
The AI evaluation tab displays the following feature metrics detected exceptionally and the corresponding probability values, including information of Cookie, User-Agent, Referer, and Query. If a metric's value larger than 0, this metric is considered exceptional.



Bot flow statistics

The bot flow statistics tab displays the feature metrics detected exceptionally, and the corresponding values estimated, as well as the reference values.

©2013-2022 Tencent Cloud. All rights reserved.



Field description:

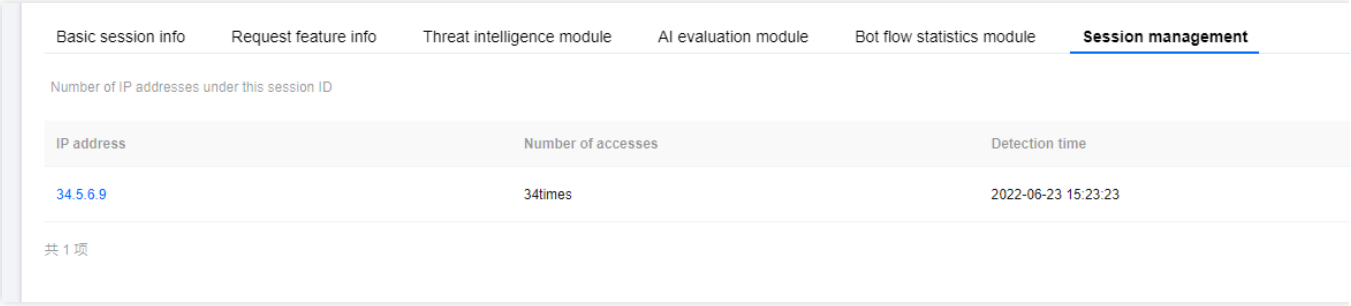
Metric	Description
Session average speed	This metric indicates that the session average speed is considered exceptional, and gives a probability threshold to confirm the exception.
User-Agent type	This metric indicates that the User-Agent type is considered exceptional, and gives a probability threshold to confirm the exception.
URL type	This metric indicates that the URL type is considered exceptional, and gives a probability threshold to confirm the exception.
Session duration	This metric indicates that the session duration is considered exceptional, and gives a probability threshold to confirm the exception.
Total session count	This metric indicates that the total session count is considered exceptional, and gives a probability threshold to confirm the exception.

Session management

The session management tab displays the IP addresses accessed by the current session, the number of accesses by each IP address, and the access logs of the current session ID.

Note:

When session settings are configured, the session management tab will be displayed.



©2013-2022 Tencent Cloud. All rights reserved.

Blocklist/Allowlist Protection Settings Features

Last updated：2023-12-29 14:45:14

The blocklist/allowlist feature of WAF allows you to add access source IPs that pass WAF-protected domains to the blocklist or allowlist and add multiple HTTP sections to the precise allowlist. Key features include IP blocklist/allowlist settings and precise allowlist settings.

IP blocklist/allowlist setting: You can set domain name-specific, IP range-specific, or global IP blocklist/allowlist rules.

Precise allowlist setting: You can add the access requests from specified public network users to the allowlist by combining and matching HTTP message sections such as request path, GET parameters, POST parameters, `Referer`, and `User-Agent`.

Meanwhile, you can add a domain name-specific or global blocklist/allowlist which will take effect in the following priority order:

The priority of the blocklist/allowlist is only lower than that of the custom precise allowlist, but higher than that of other detection logic.

The priority of blocklist/allowlist settings is in descending order: precise allowlist > global allowlist > domain name-specific allowlist > domain name-specific blocklist > global blocklist > other WAF module logic.

©2013-2022 Tencent Cloud. All rights reserved.

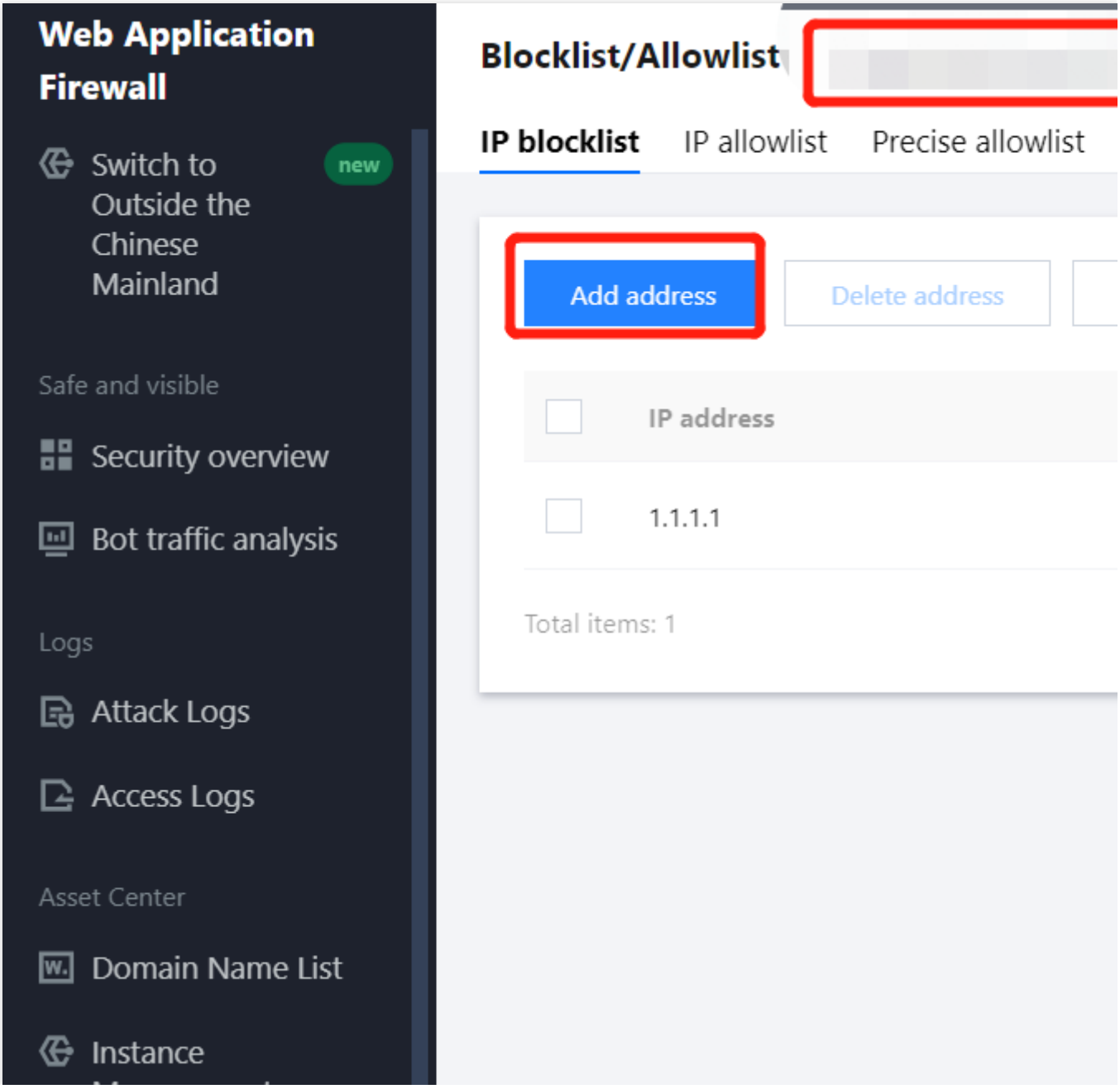
IP Blocklist

Last updated：2023-12-29 14:45:25

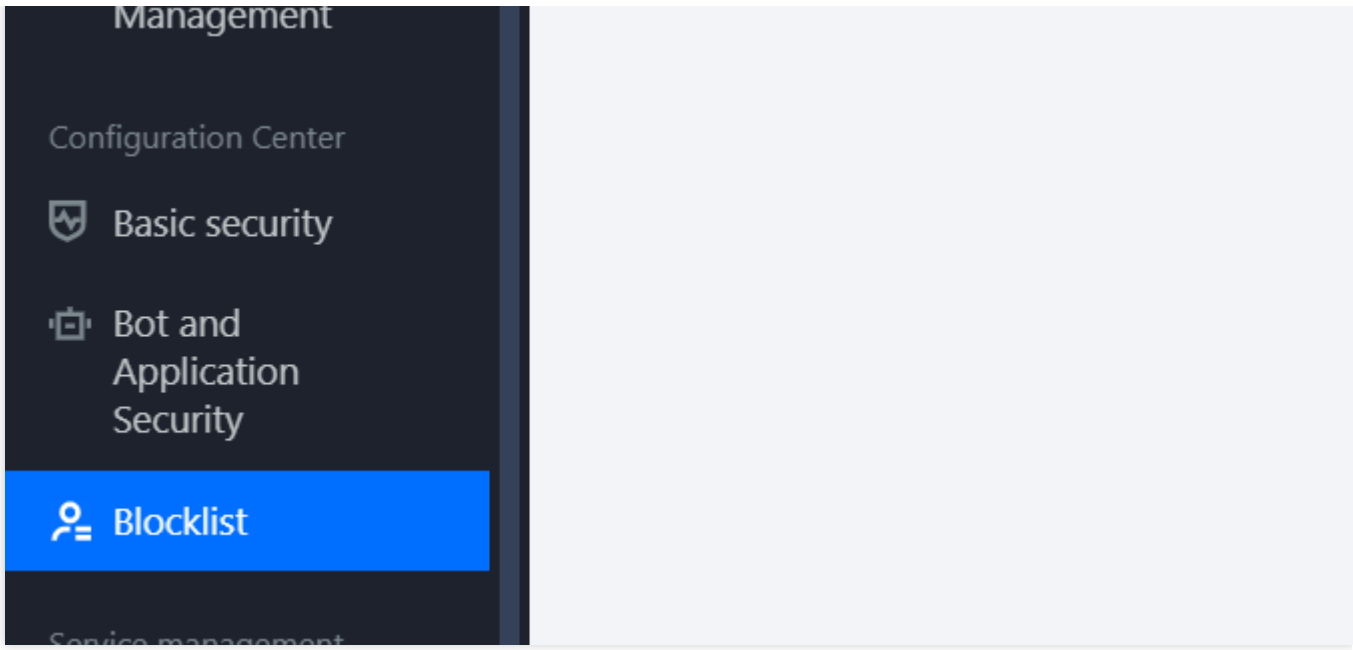
Adding IPs to Blocklist

Adding IPs manually

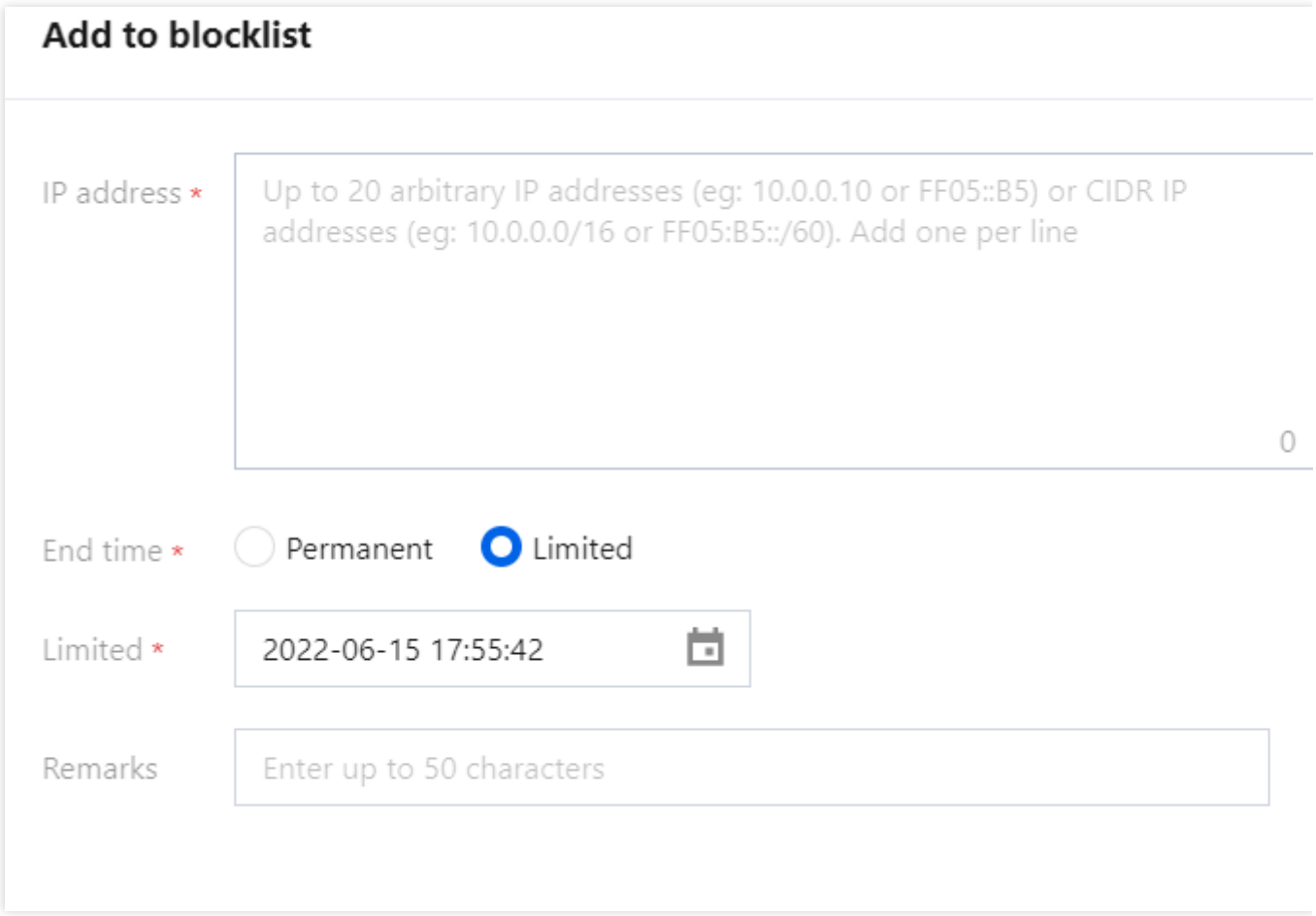
1. Log in to the WAF console and select **Configuration Center** > **Blocklist/Allowlist** on the left sidebar.
2. On the blocklist/allowlist page, select a target domain name in the top-left corner and click **IP blocklist**.
3. On the IP blocklist page, click **Add address**.



©2013-2022 Tencent Cloud. All rights reserved.



4. On the page that appears, configure relevant parameters and click **OK**.



Field description:

IP address: IP address such as `10.0.0.10` or `FF05::B5` . CIDR blocks are supported, such as `10.0.0.0/16` or `FF05:B5::/60` . You can enter up to 20 items and separate them with line breaks.

©2013-2022 Tencent Cloud. All rights reserved.

Note:

If you select **All** for the domain name, the added IP address or range will be blocked/allowed globally.

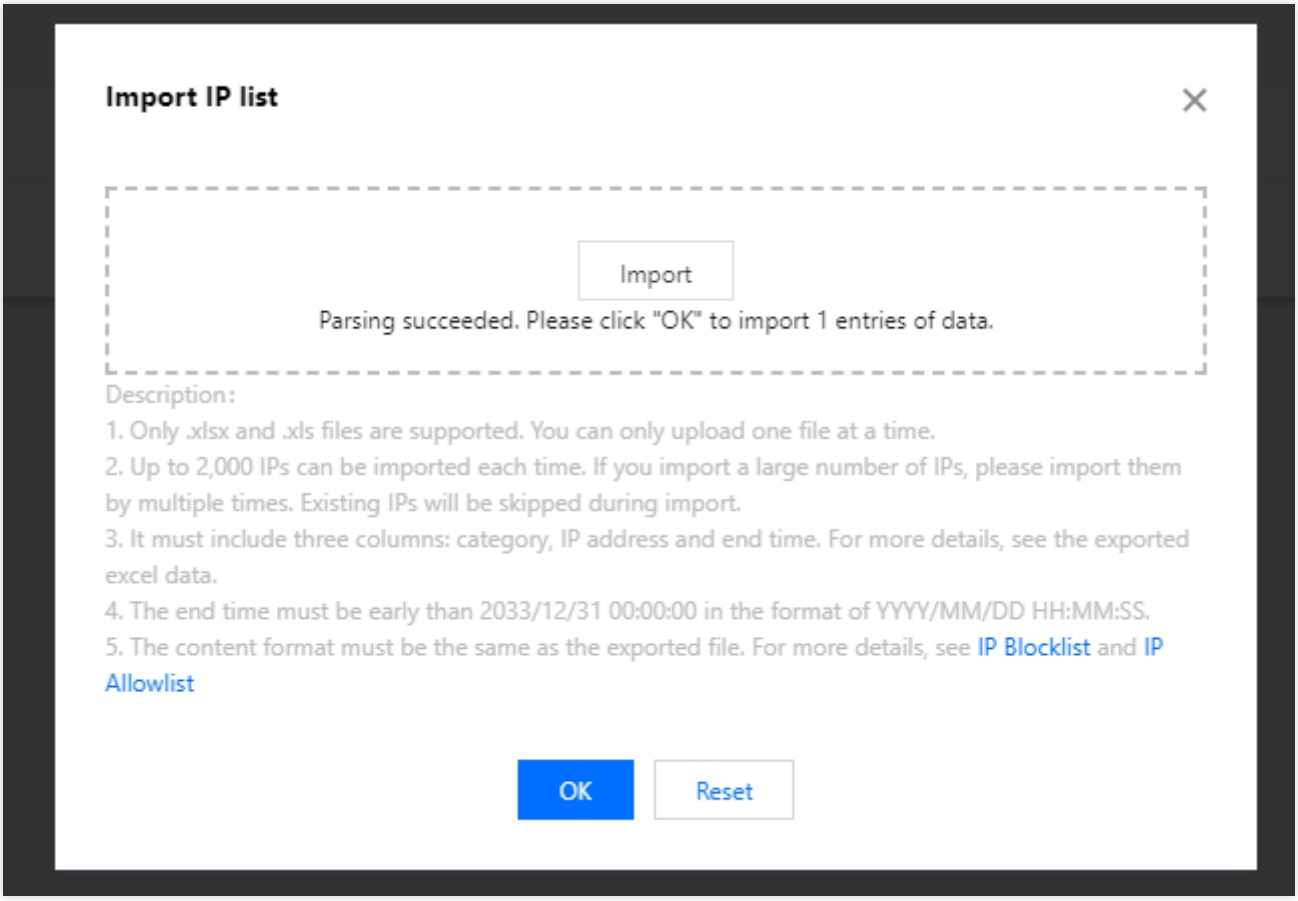
The domain name quotas in each edition are as follows: Premium Edition: 1,000 entries/domain name; Enterprise Edition: 5,000 entries/domain name; Ultimate Edition: 20,000 entries/domain. Each IP address or range occupies one entry in the quota.

Expiration time:Never expire or a specified date.

Remarks: Custom remarks, which can contain up to 50 characters.

Importing IPs

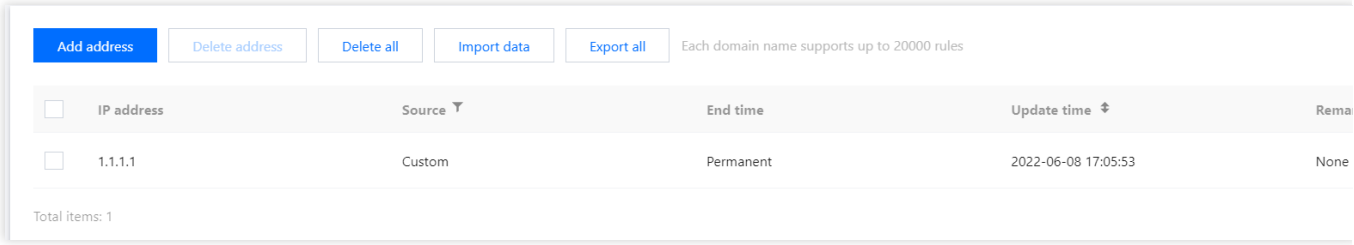
1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click **IP blocklist**.
2. On the IP blocklist page, click **Import data** > **Import**. After the data is parsed successfully, click **OK**.



Editing IP Blocklist

1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click **IP blocklist**.
2. On the IP blocklist page, select a target IP address, click **Edit** in the **Operation** column, modify the expiration time and remarks, and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



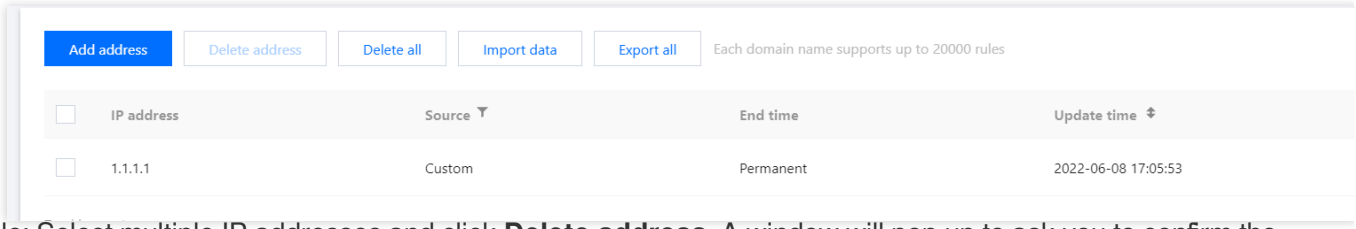
Deleting IPs from IP Blocklist

1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click **IP blocklist**.
2. You can delete one, multiple, or all IP addresses on the IP blocklist page as follows:

One: Select an IP address and click **Delete address** or **Delete** in the **Operation** column. A window will pop up to ask you to confirm the deletion operation.

Note:

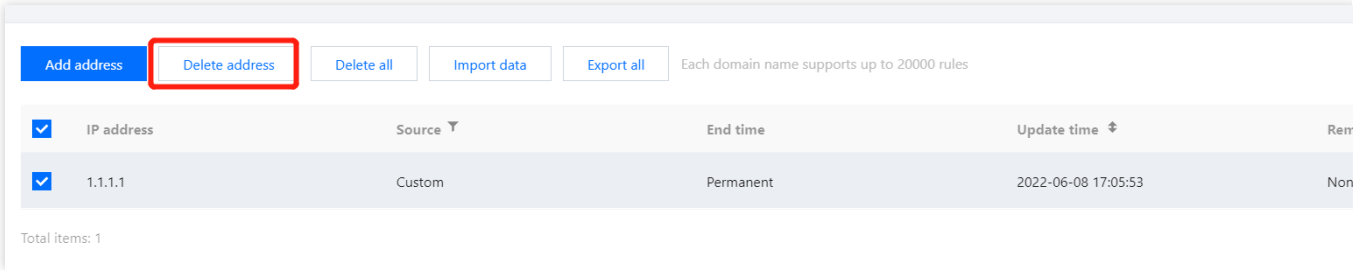
Once deleted, it cannot be restored and can take effect only after being added again.



Multiple: Select multiple IP addresses and click **Delete address**. A window will pop up to ask you to confirm the deletion operation.

Note:

Once deleted, it cannot be restored and can take effect only after being added again.



All: Click **Delete all**. A window will pop up to ask you to confirm the deletion operation.

Note:

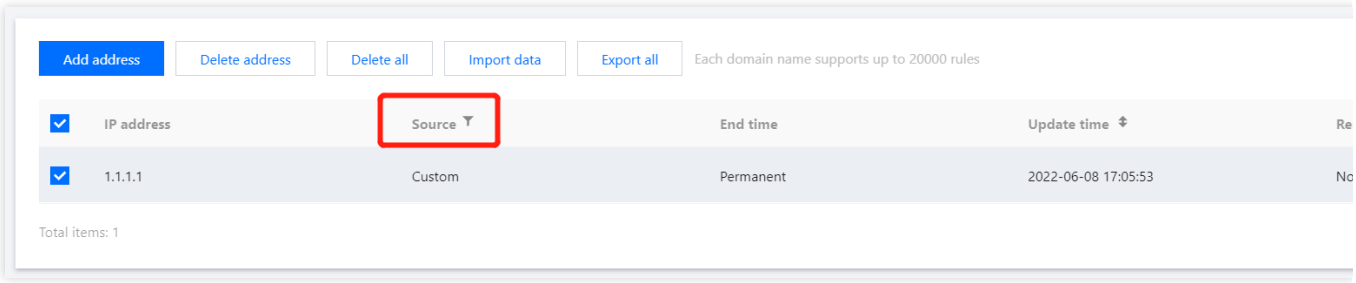
This operation will clear all IP blocklist/allowlist information under the current domain name. Therefore, proceed with caution. Once deleted, the addresses cannot be restored and can take effect only after being added again.

3. In the pop-up window, click **OK**.

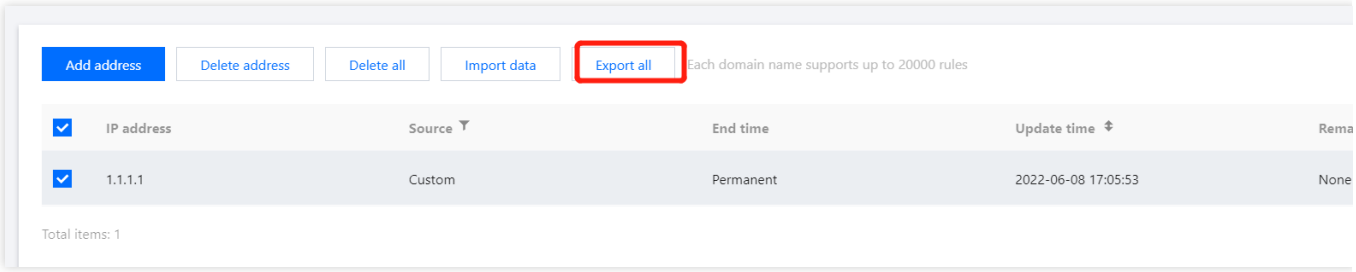
©2013-2022 Tencent Cloud. All rights reserved.

Exporting All Filtered Results

1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click **IP blocklist**.
2. On the IP blocklist page, click the search box to filter IPs by **IP address** or click **Source** to filter IPs by source type.



3. After filtering required IPs, click **Export all**.



©2013-2022 Tencent Cloud. All rights reserved.

IP Allowlist

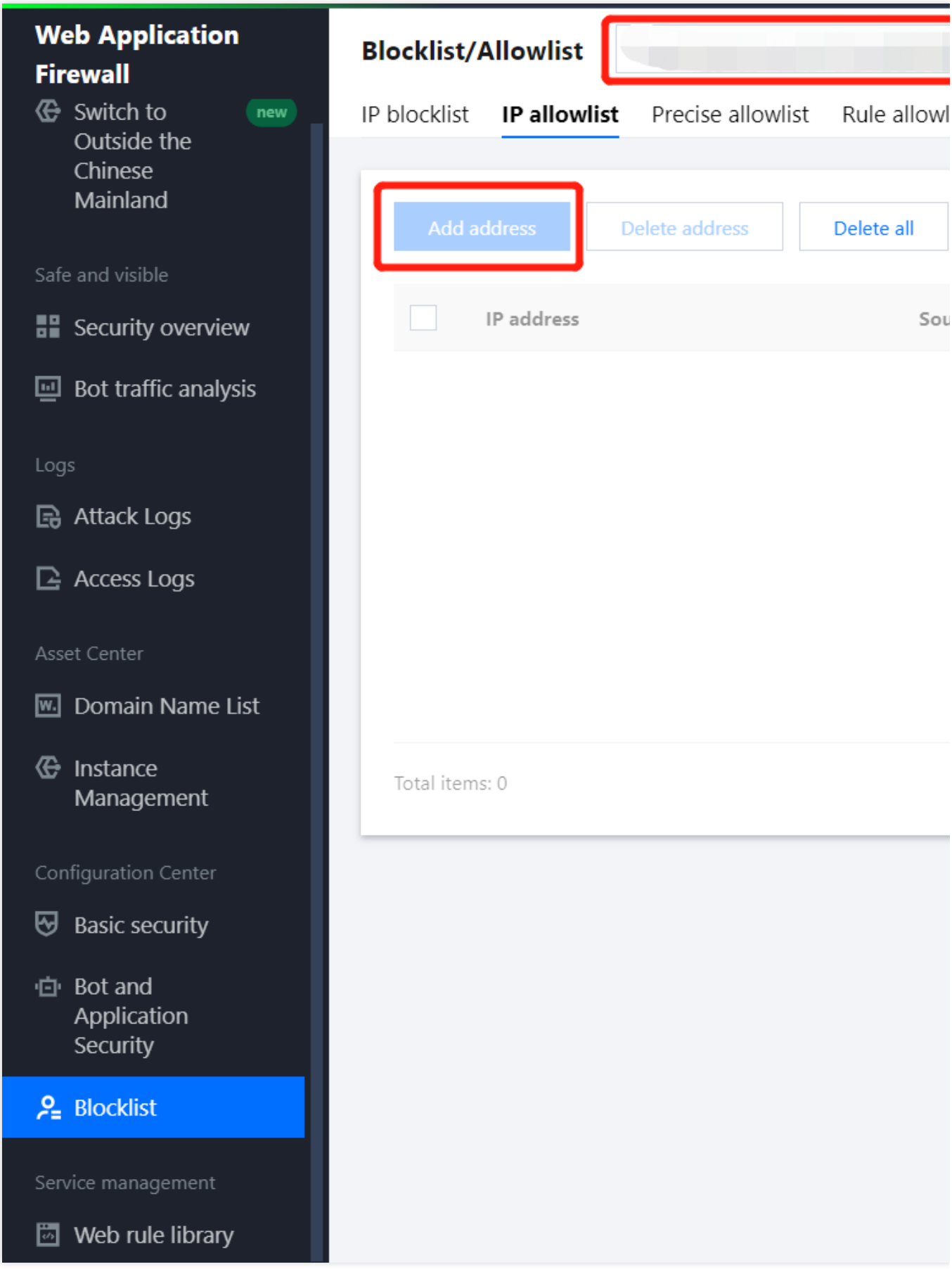
Last updated：2023-12-29 14:45:40

Adding IPs to Allowlist

Adding IPs manually

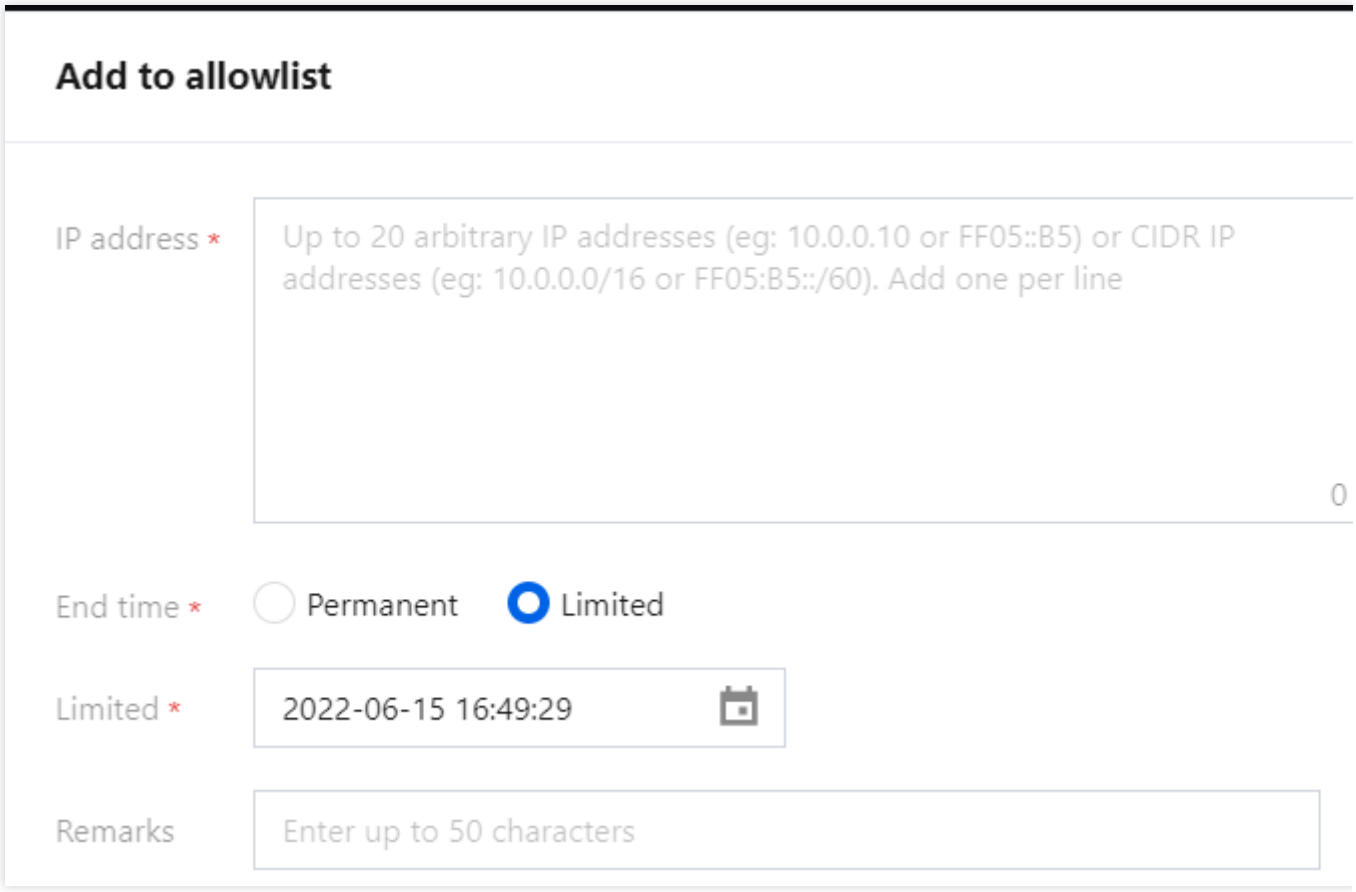
1. Log in to the WAF console and select **Configuration Center** > **Blocklist/Allowlist** on the left sidebar.
2. On the blocklist/allowlist page, select a target domain name in the top-left corner and click **IP allowlist**.
3. On the IP allowlist page, click **Add address**.

©2013-2022 Tencent Cloud. All rights reserved.



4. On the allowlist IP adding page, configure relevant parameters and click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Field description

IP address: IP address such as `10.0.0.10` or `FF05::B5` . CIDR blocks are supported, such as `10.0.0.0/16` or `FF05:B5::/60` . You can enter up to 20 items and separate them with line breaks.

Note:

If you select **All** for the domain name, the added IP address or range will be allowed globally.

The domain name quotas in each edition are as follows: Premium Edition: 1,000 entries/domain name; Enterprise Edition: 5,000 entries/domain name; Ultimate Edition: 20,000 entries/domain. Each IP address or range occupies one entry in the quota.

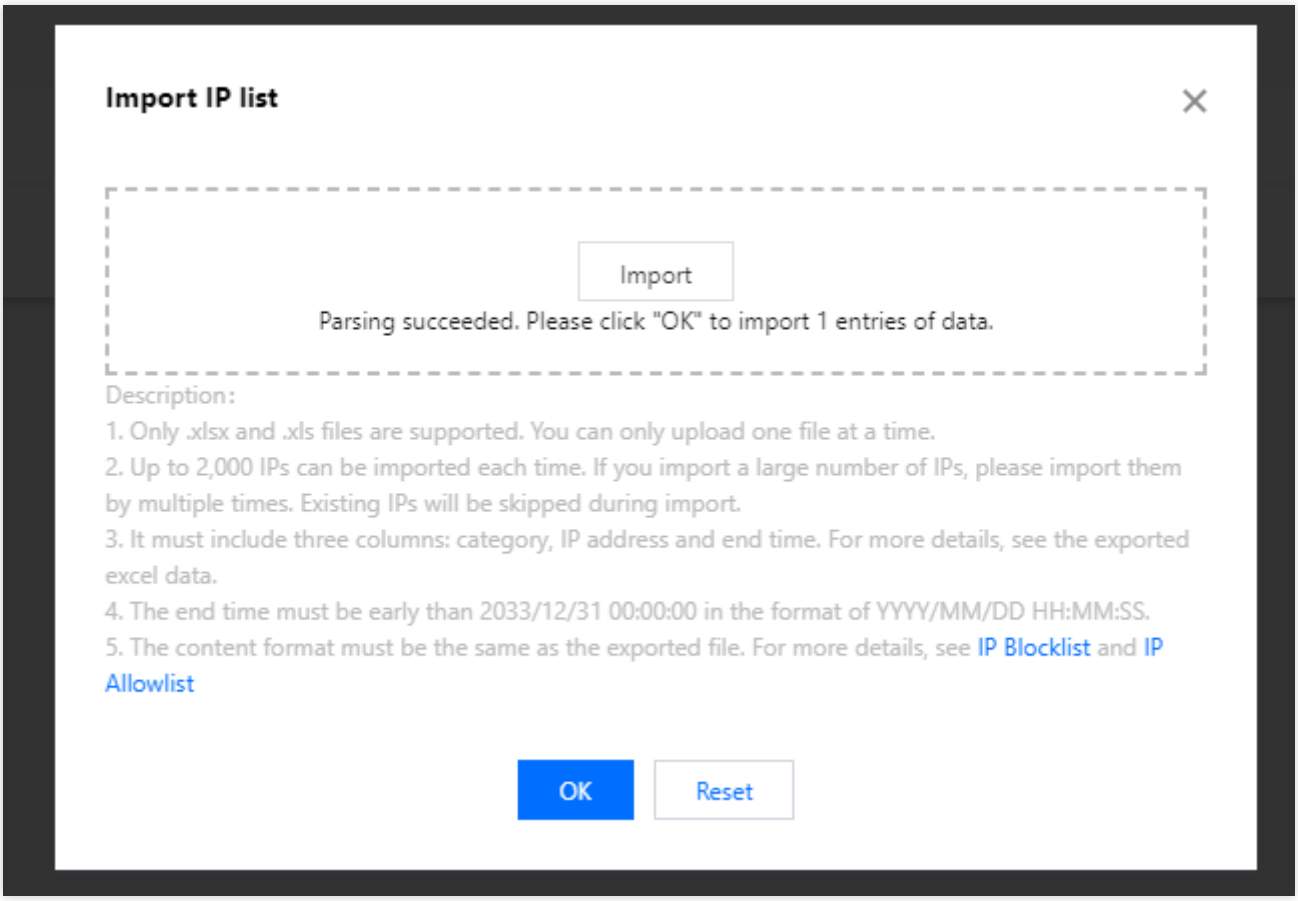
Expiration time:Never expire or a specified date.

Remarks: Custom remarks, which can contain up to 50 characters.

Importing IPs

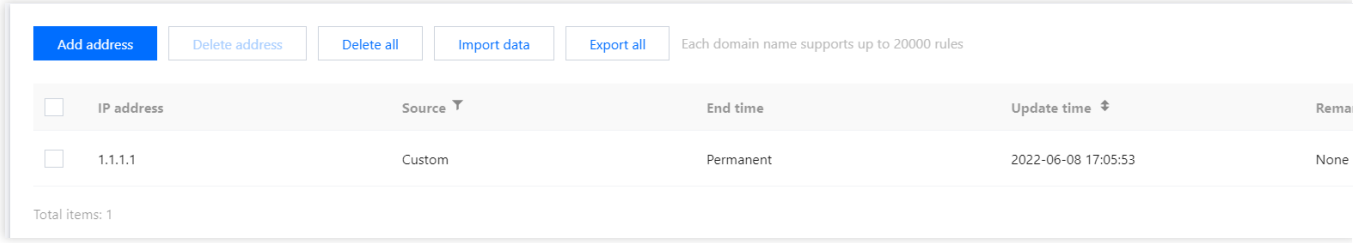
1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click **IP allowlist**.
2. On the IP allowlist page, click **Import data** > **Import**. After the data is parsed successfully, click **OK**.

©2013-2022 Tencent Cloud. All rights reserved.



Editing IP Allowlist

1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click **IP allowlist**.
2. On the IP allowlist page, select a target IP address, click **Edit** in the **Operation** column, modify the expiration time and remarks, and click **OK**.



Deleting IPs from IP Allowlist

1. On the blocklist/allowlist page, select a target domain name in the top-left corner and click **IP allowlist**.

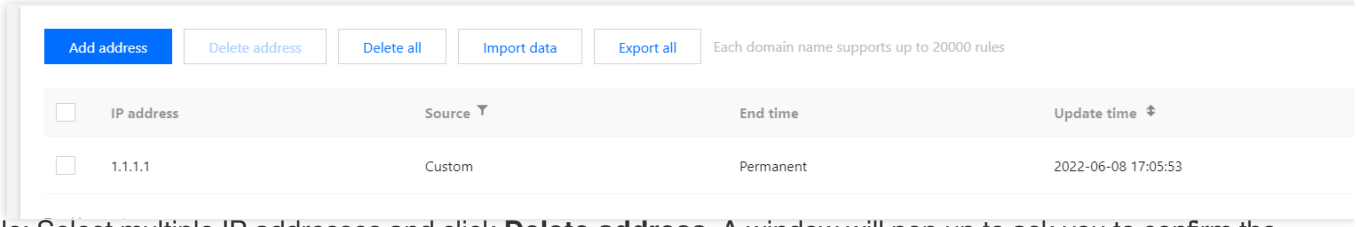
©2013-2022 Tencent Cloud. All rights reserved.

2. You can delete one, multiple, or all IP addresses on the IP allowlist page as follows:

One: Select an IP address, and click **Delete address** or **Delete** in the **Operation** column. A window will pop up to ask you to confirm the deletion operation.

Note:

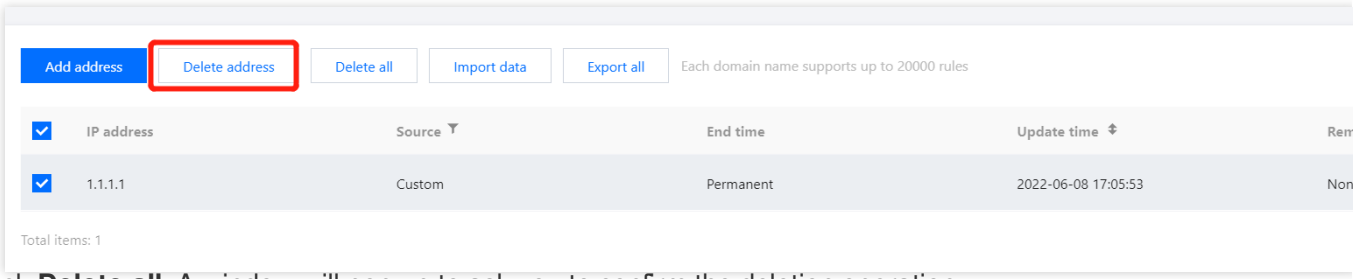
Once deleted, it cannot be restored and can take effect only after being added again.



Multiple: Select multiple IP addresses and click **Delete address**. A window will pop up to ask you to confirm the deletion operation.

Note:

Once deleted, it cannot be restored and can take effect only after being added again.



All: Click **Delete all**. A window will pop up to ask you to confirm the deletion operation.

Note:

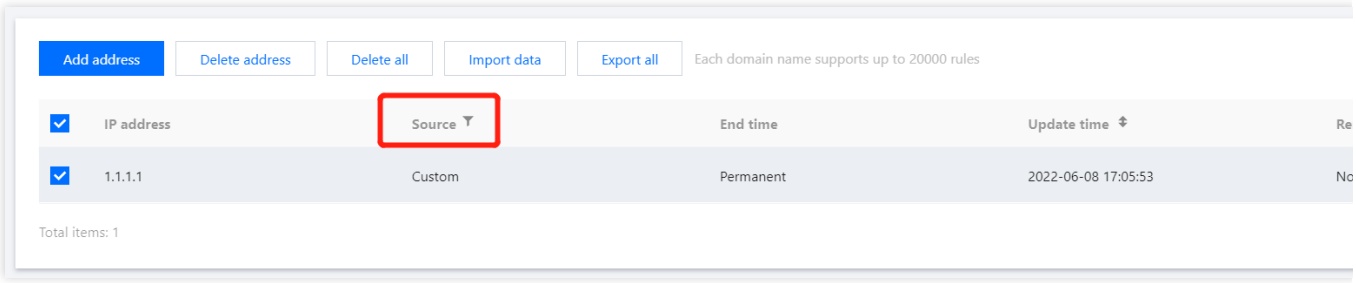
This operation will clear all IP blocklist/allowlist information under the current domain name. Therefore, proceed with caution. Once deleted, the addresses cannot be restored and can take effect only after being added again.

3. In the pop-up window, click **OK**.

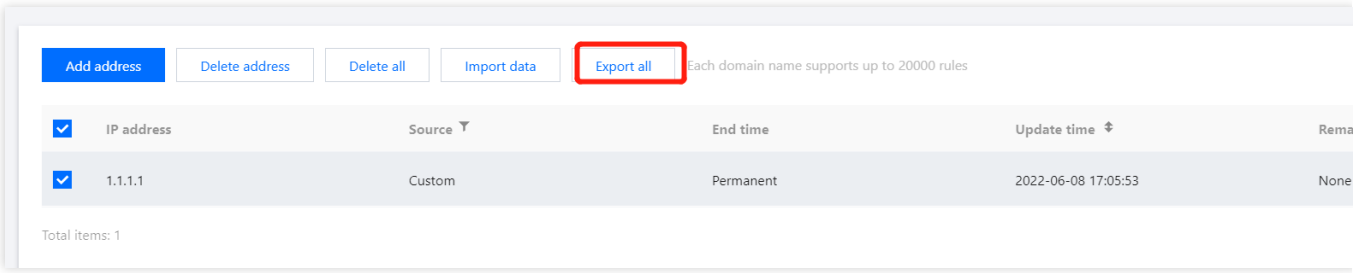
Exporting All Filtered Results

1. On the blocklist/allowlist page, select the target domain name in the top-left corner and click **IP Allowlist**.
2. On the IP allowlist page, click the search box to filter IPs by **IP address** or click **Source** to filter IPs by source type.

©2013-2022 Tencent Cloud. All rights reserved.



3. After filtering required IPs, click **Export all**.



©2013-2022 Tencent Cloud. All rights reserved.

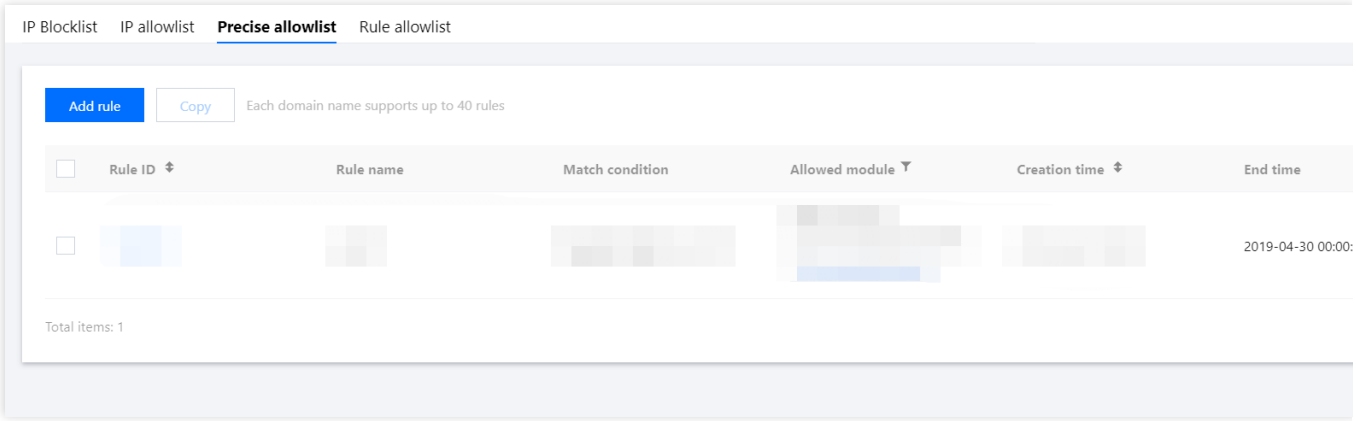
Precise Allowlist Management

Last updated：2023-12-29 14:45:58

You can add IPs to the precise allowlist to allow access requests of specific public network users to the specified sites.

Adding to Precise Allowlist

1. Log in to the WAF console and select **Configuration Center** > **IP Blocklist/Allowlist** on the left sidebar to enter the IP blocklist/allowlist page.
2. On the blocklist/allowlist page, select the target domain name in the top-left corner and click **Precise allowlist**.
3. On the precise allowlist page, click **Add address**, and the IP adding window will pop up.



4. In the pop-up window, configure relevant parameters and click **OK**.

Note:

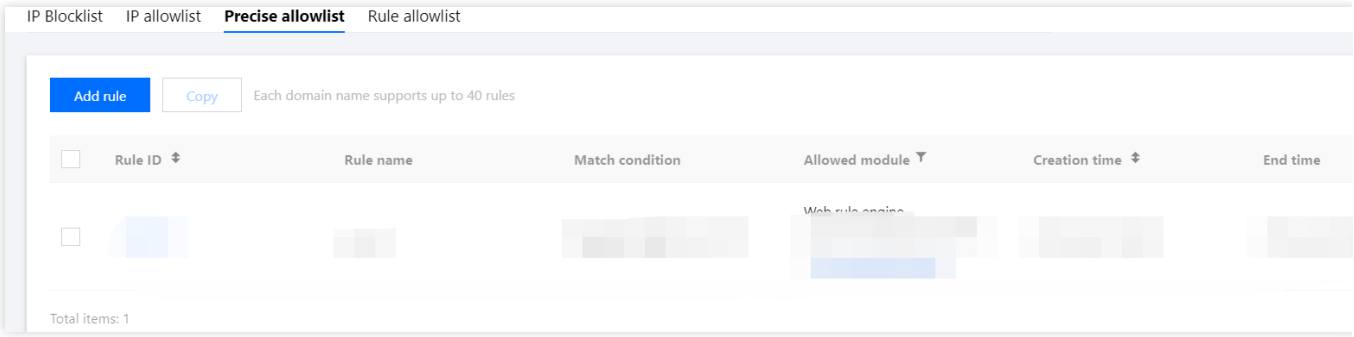
WAF precise allowlist enables you to use masks to allow access requests from source IPs within a range. We can enter a specific IP range (e.g. `10.10.10.0/24`) in **Content**.

5. Now the rule will take effect immediately, and allow all HTTP access requests from specific source IPs.

Editing Precise Allowlist

1. On the blocklist/allowlist page, select the target domain name in the top-left corner and click **Precise allowlist**.
2. On the precise allowlist page, select the target rule, click **Edit**, and the editing window will pop up.

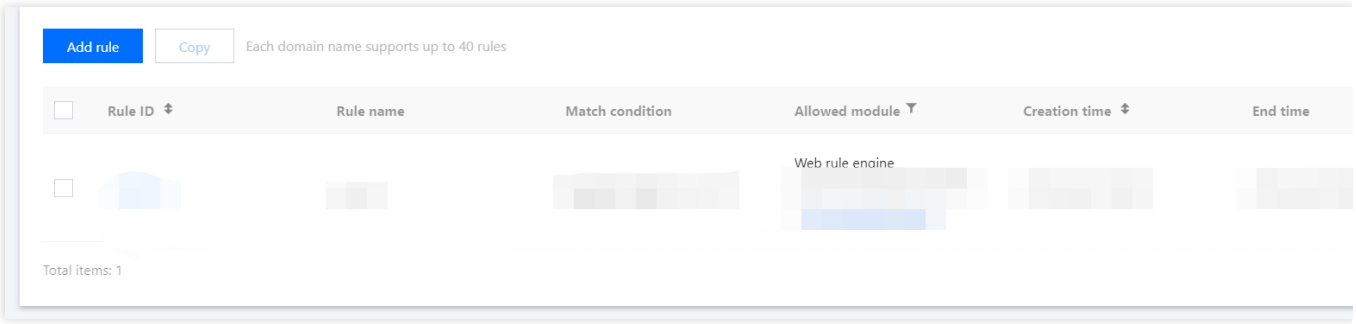
©2013-2022 Tencent Cloud. All rights reserved.



3. In the pop-up window, modify relevant parameters and click **OK**.

Removing from Precise Allowlist

1. On the blocklist/allowlist page, select the target domain name in the top-left corner and click **Precise allowlist**.
2. On the precise allowlist page, select the target rule, click **Delete**, and the deletion confirmation window will pop up.



3. In the pop-up window, click **OK**.

Note:

Once deleted, it cannot be restored and takes effect only after being added again.

©2013-2022 Tencent Cloud. All rights reserved.

Rule Allowlist

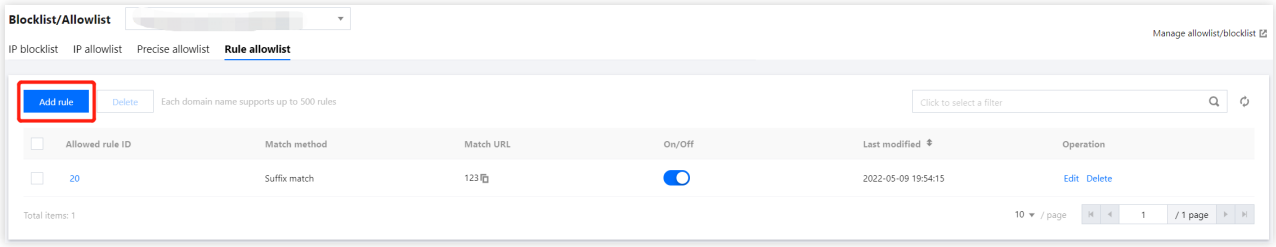
Last updated：2023-12-29 14:46:11

Scenarios

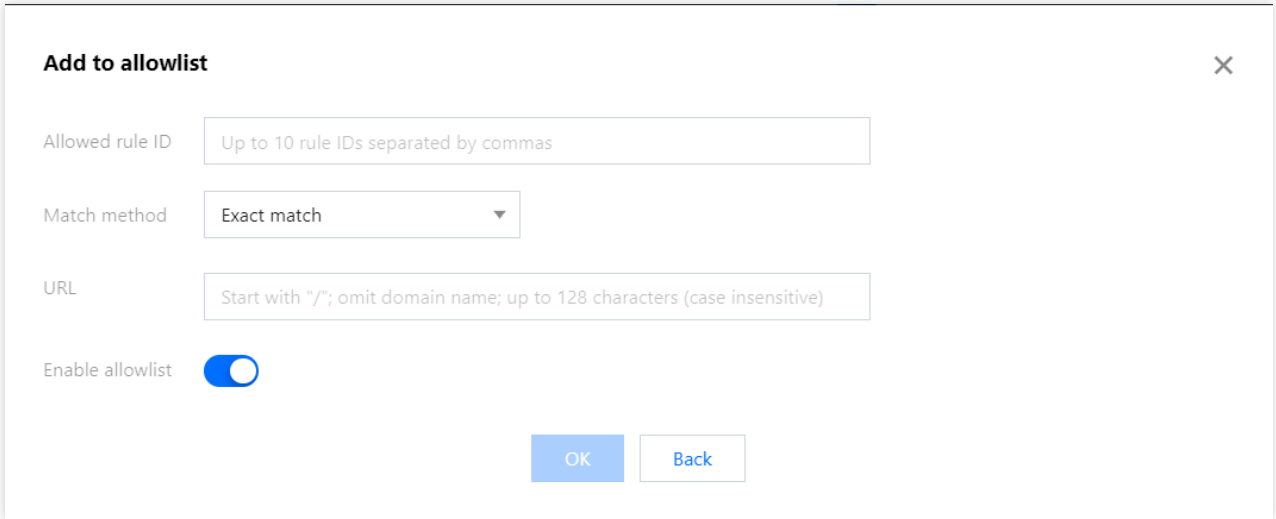
If normal access traffic is blocked by the WAF rule engine, you can create rules to allow the access traffic using the blocklist/allowlist feature.

Directions

1. Log in to the WAF console and select **Configuration Center** > **IP Blocklist/Allowlist** on the left sidebar to enter the IP blocklist/allowlist page.
2. On the blocklist/allowlist page, select the target domain name in the top-left corner and click **Rule allowlist**.
3. On the page that appears, click **Add rule**.



4. In the pop-up window, configure the required parameters and click **OK**.



©2013-2022 Tencent Cloud. All rights reserved.

Field description:

Rule ID: ID of the rule to be allowed. You can add up to 10 rule IDs for each policy.

Match method: Match method of the URL to be allowed. You can select "Exact match" (default value), "Prefix match", or "Suffix match".

URL: URI path to be allowed. The URI must be unique under one domain name.

Enable allowlist: It specifies whether to enable allowlist. The switch is enabled by default.

©2013-2022 Tencent Cloud. All rights reserved.

Traffic Inspection

Last updated：2024-06-18 14:42:15

Overview

The traffic inspection feature enables an analysis of the traffic risks associated with the currently protected services. It assists you in efficiently summarizing the connected assets, detecting risks in business traffic, reviewing the WAF configurations, and generating a detailed Traffic Inspection report. This aids in enhancing website protection effectiveness and ensuring the stable operation of your business.

Traffic Inspection Introduction:

Free trial: Traffic inspection is currently a beta feature, and it is available for use after WAF is purchased.

Log recording: Once the traffic inspection starts, it will check for web risk, bot risk, and API asset risk for the check domain. **If any risk is detected, attack logs and access logs will be recorded with actions of observation (monitoring without interception). It ensures there is no impact or interception of business access.**

Data source: The traffic inspection display data comes from the WAF product you are currently using. If some value-added features are not enabled, the statistics may slightly deviate from the actual access situation. It is recommended that you purchase and enable these features before conducting another check.

Directions

1. Log in to the WAF console, and choose **Traffic Inspection** in the left sidebar.
2. On the traffic Inspection page, you can initiate a check, view the top 5 key issues of concern, and download historical check reports.

Initiating a Traffic Inspection

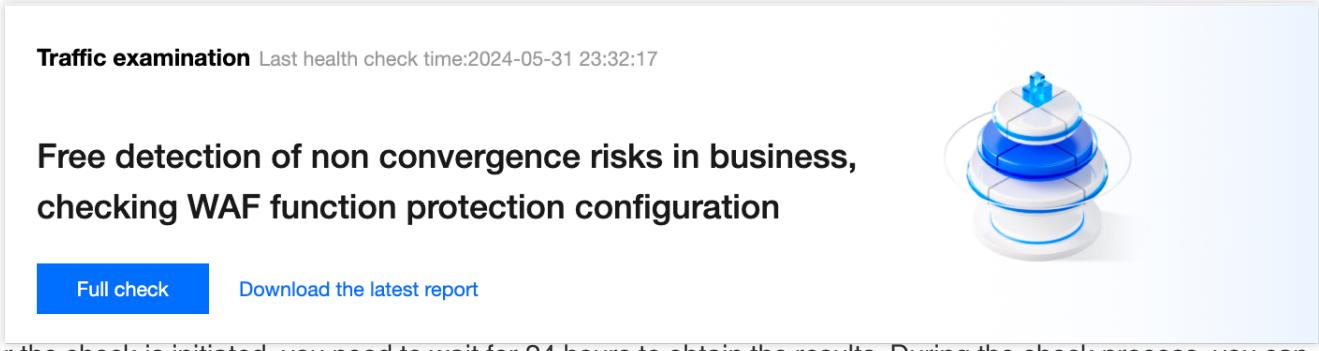
1. On the traffic Inspection card, click **Full check** to initiate the check task.

Check scope: Supports the check of up to 100 domain names within 20,000 QPS. Exceeding this limit will result in a random selection of some domain names for check.

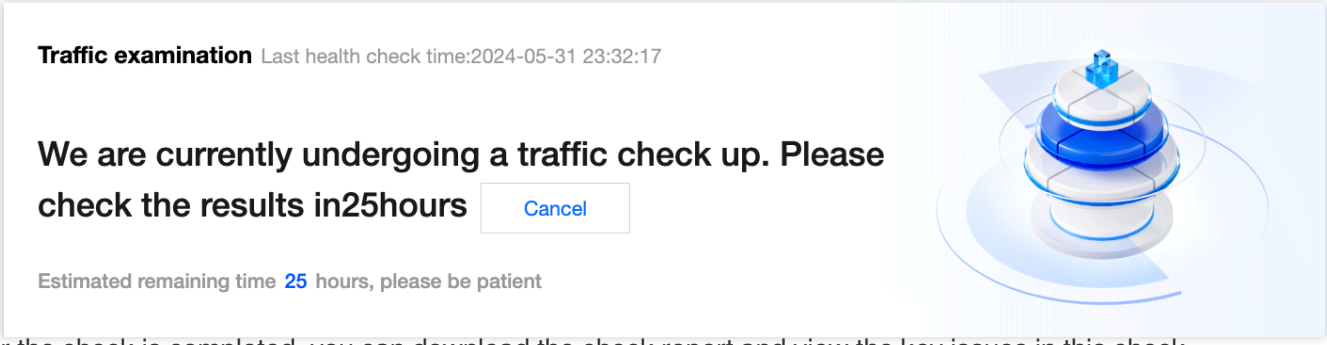
Check cycle: Supports check once every 7 days.

Check duration: Each check cycle is expected to span approximately 24 hours. Once it is initiated, the check will only analyze abnormal traffic data from the most recent 24-hour period. The check ends with the generation of a check report and key issues.

©2013-2022 Tencent Cloud. All rights reserved.



2. After the check is initiated, you need to wait for 24 hours to obtain the results. During the check process, you can click **Cancel** to terminate the check task.



3. After the check is completed, you can download the check report and view the key issues in this check.

Viewing Key Issues

After the check is completed, you can view the top 5 key issues at the bottom of the page, and handle key risks accordingly.

Priority: The priority of risk disposal, divided into high, medium, and low levels, is evaluated based on the degree of risk and impact scope.

Statistics data: Collects risk data within the check cycle, and displays the increase/decrease changes in risk compared to the results of the last check.

©2013-2022 Tencent Cloud. All rights reserved.

Downloading Reports

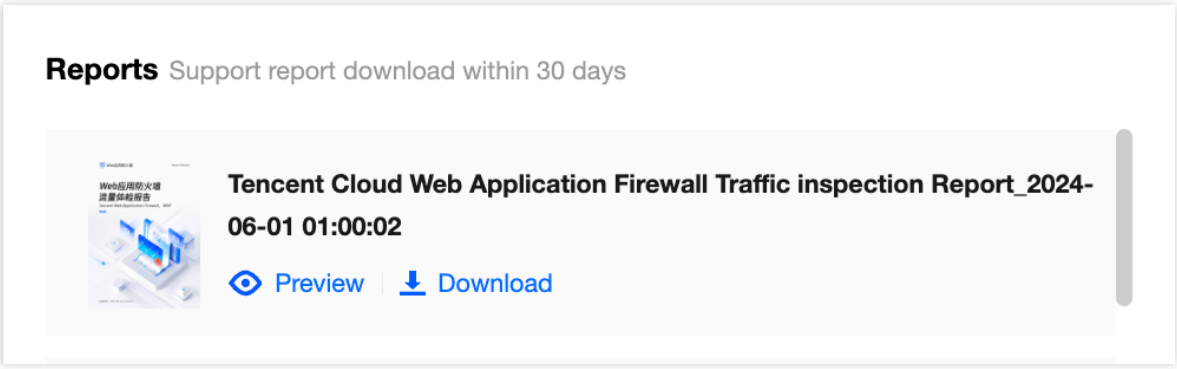
After the check is completed, you can download a detailed traffic Inspection report. The report **is only saved for 30 days**.

Note:

Due to the limited length of the report, only the top 5 items are displayed for each check item detail list. For complete details, see the report guide and view on the corresponding page in the console.

On the report download card, click **Preview** to view the content of the check report online.

On the report download card, click **Download** to download the physical check report in PDF format.



Introduction of Check Items of Traffic Inspection

Check Module	Check Item	Check Content
Connected Asset Summary	Domain asset summary	Summarizes the total number of domains, the total number of domains connected to the WAF, and the total number of domains with WAF protection enabled.

©2013-2022 Tencent Cloud. All rights reserved.

		Displays the list of domains not yet protected by the WAF.
	API asset summary	Summarizes the total number of API assets found in the connected domains and the business scenarios involved. Displays the top 5 API QPS peak values from the day before and the list of domains with a high number of active APIs.
Traffic Risk Summary	Trend of business access	Analyzes business access trends and identifies any risks of excessive traffic volume.
	Trend of attack traffic	Analyzes the distribution of attack types within the access business check cycle.
	Bot attack risk	Determines if there is bot risk in the access traffic; if so, further analyzes the types/purposes, maliciousness, and access trend of the relevant bots.
	API risk summary	Analyzes if there are risks associated with API assets found in the access traffic; if so, further analyzes the sensitivity involvement, risk events, and the total number of accesses, QPS, and the business scenarios of the related assets.
WAF Configuration Summary	WAF configuration summary	Checks the configuration of key product features, including statuses of asset connectivity, protection switch status, protection configuration, and log storage configuration.

©2013-2022 Tencent Cloud. All rights reserved.

Statistics and Logs
Attack Logs

Last updated：2023-12-29 14:46:24

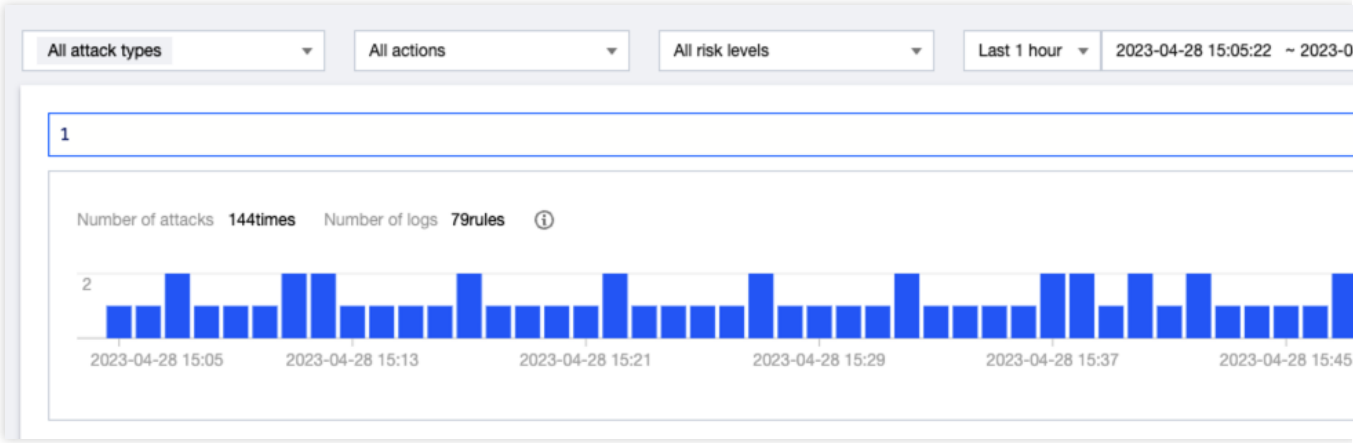
This guide describes how to search and analyze attack logs.

Background

WAF collects attack logs that record information about the attack time, attacker IP and attack type, and allows you to query and download logs for up to 30 days in the past by full-text search, fuzzy search and filter search (which support downloading million of logs).

Searching Attack Logs

1. Log in to the WAF console. Select **Attack Logs** on the left sidebar and then the **Log service** tab.
2. Select the instance, domain name, attack type, action and attack time to search attack logs.

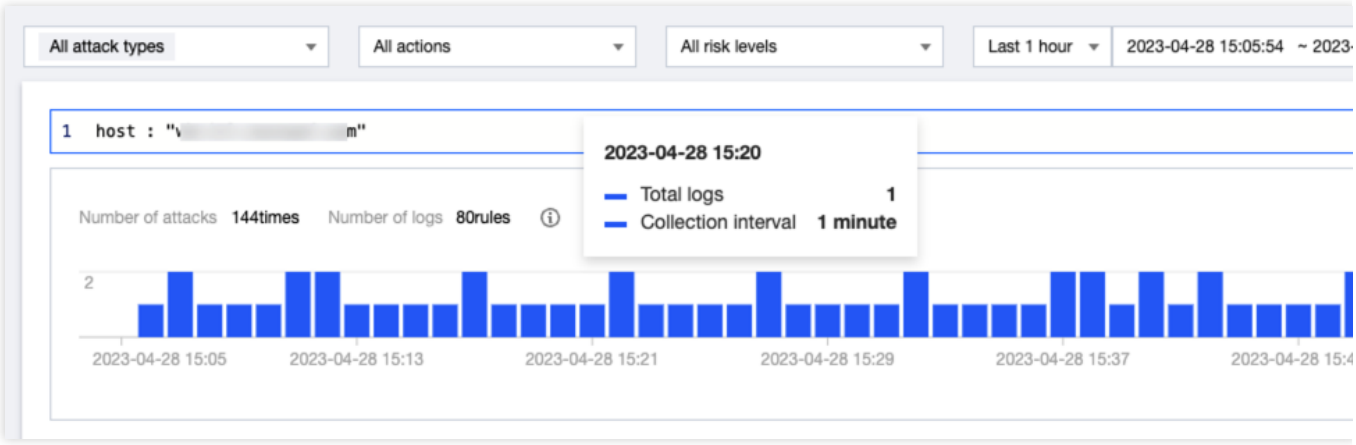


Field Name	Description
Instance	Select instances. By default, all instances are selected.
Domain name	Select domain names. By default, all domain names are selected.
Attack type	Select attack types observed/blocked by security modules. By default, all attack types are selected.

©2013-2022 Tencent Cloud. All rights reserved.

Action	Select **Observe** or **Block**. By default, all actions are selected.
Risk level	Select **High risk**, **Medium risk** or **Low risk**. By default, all risk levels are selected.
Time period	Select a time period for the logs you want to search. If this field is not specified, **Last 1 hour** is selected by default.
Auto-refresh	Automatically refresh the page at the specified frequency. This feature is disabled by default.

3. Specify the search filters prior to clicking **Search**.

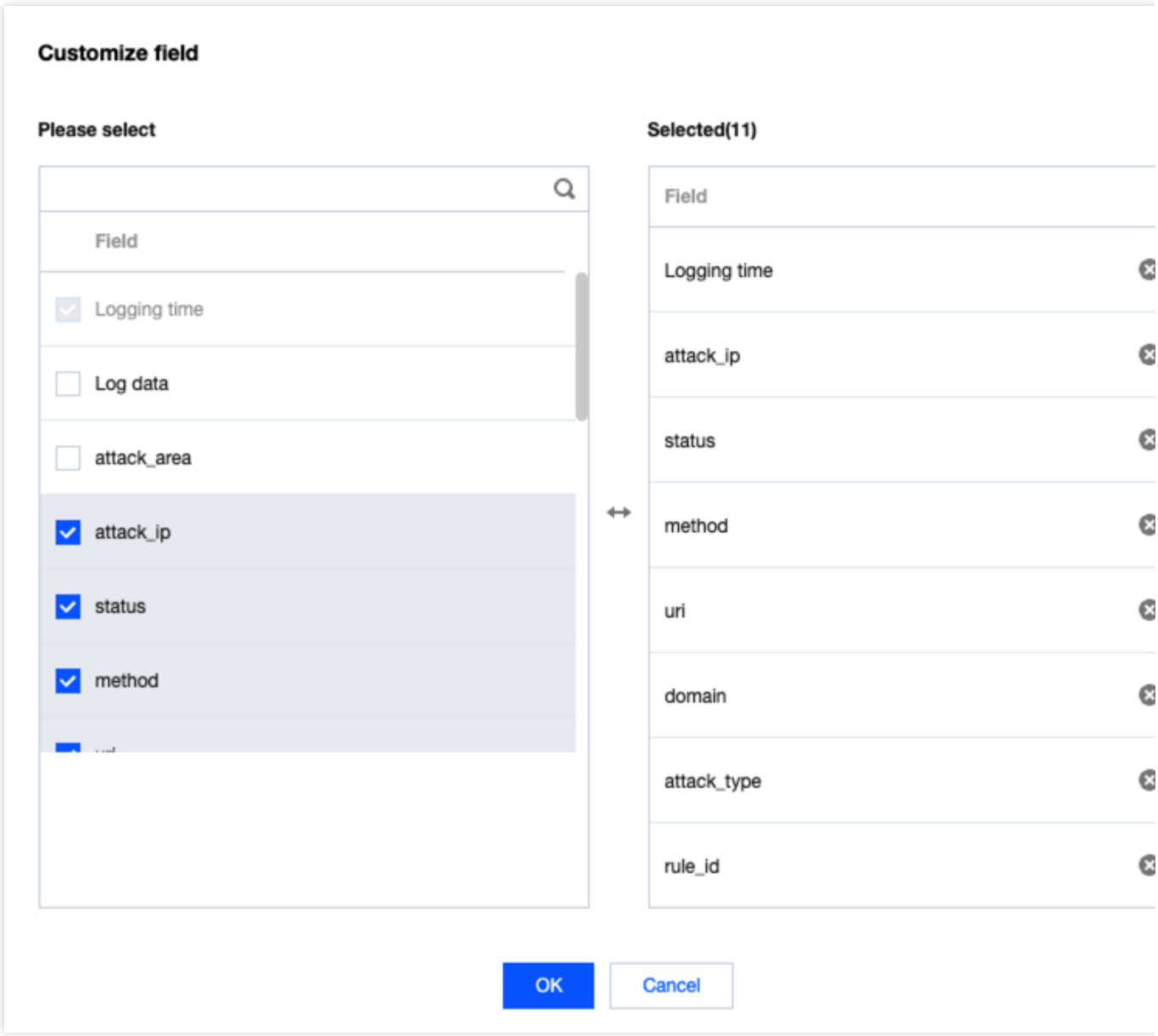


Analyzing Attack Logs

1. On the top right of the log list, click

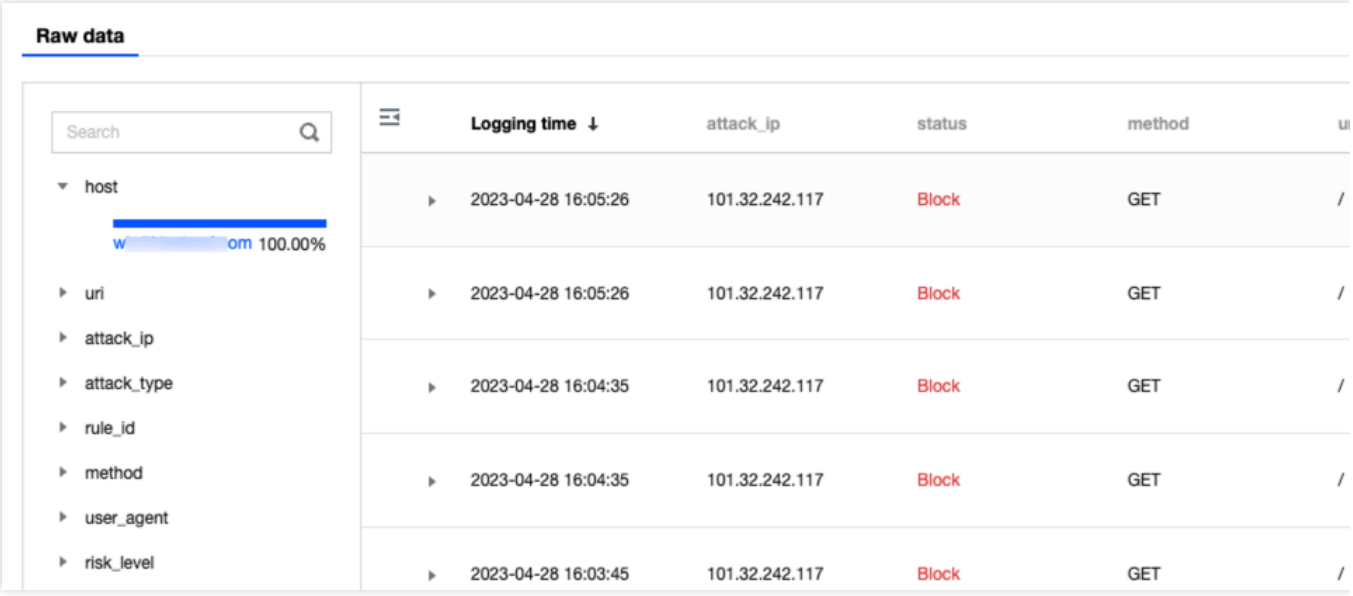
to select fields, and then click **OK**. To know more about the log fields, refer to Log field description.

©2013-2022 Tencent Cloud. All rights reserved.



2. On the left of the **Raw data** section, select the field you want to view its percentage. Then select the value to filter the log results.

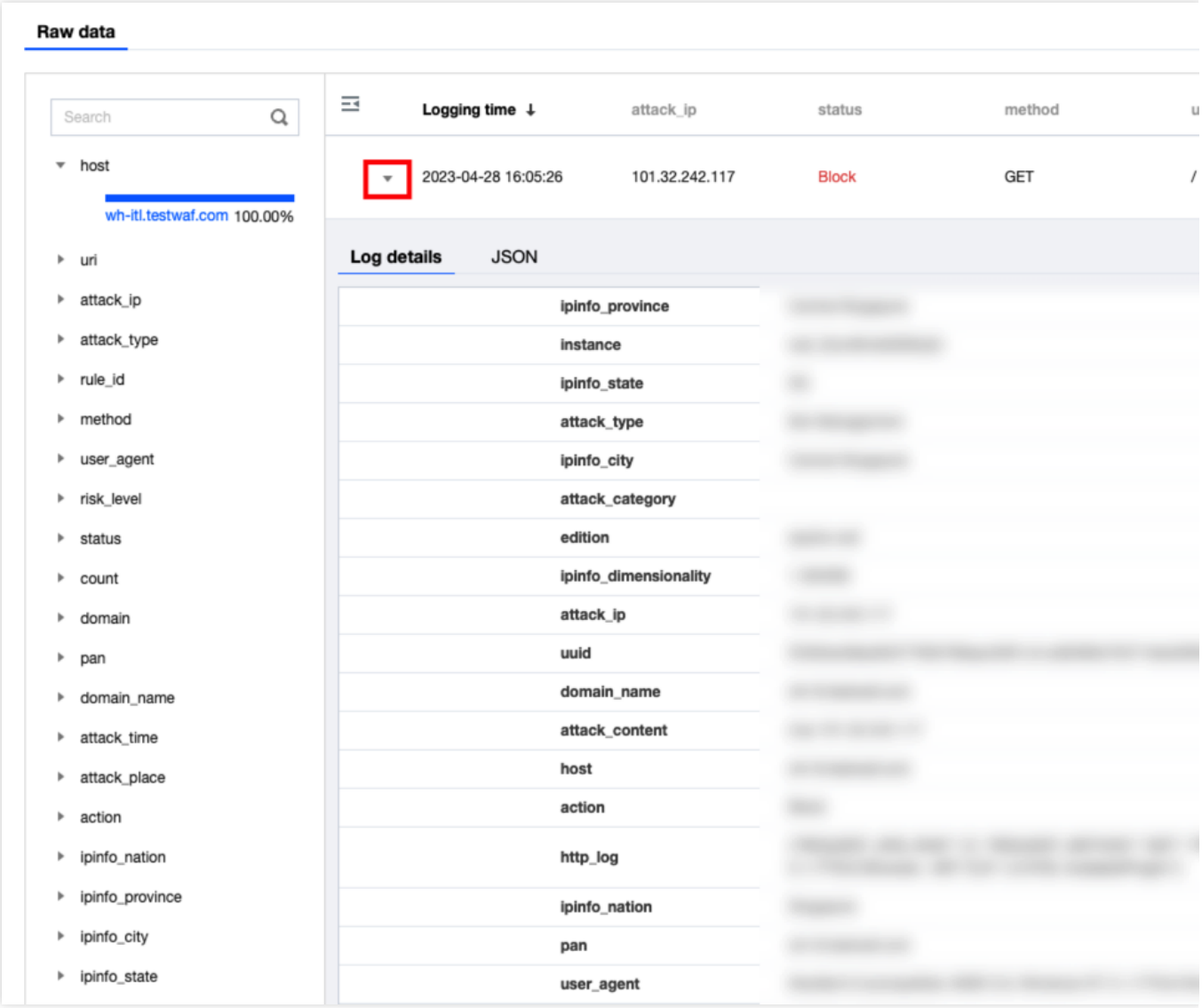
©2013-2022 Tencent Cloud. All rights reserved.



3. Click

to expand log details, where you can select the field value to find the log results. To view logs in JSON format, click **JSON**.

©2013-2022 Tencent Cloud. All rights reserved.



Downloading Attack Logs

1. On the top right of the log list, click

to view your download tasks.

Note

By default, your log results are downloaded.

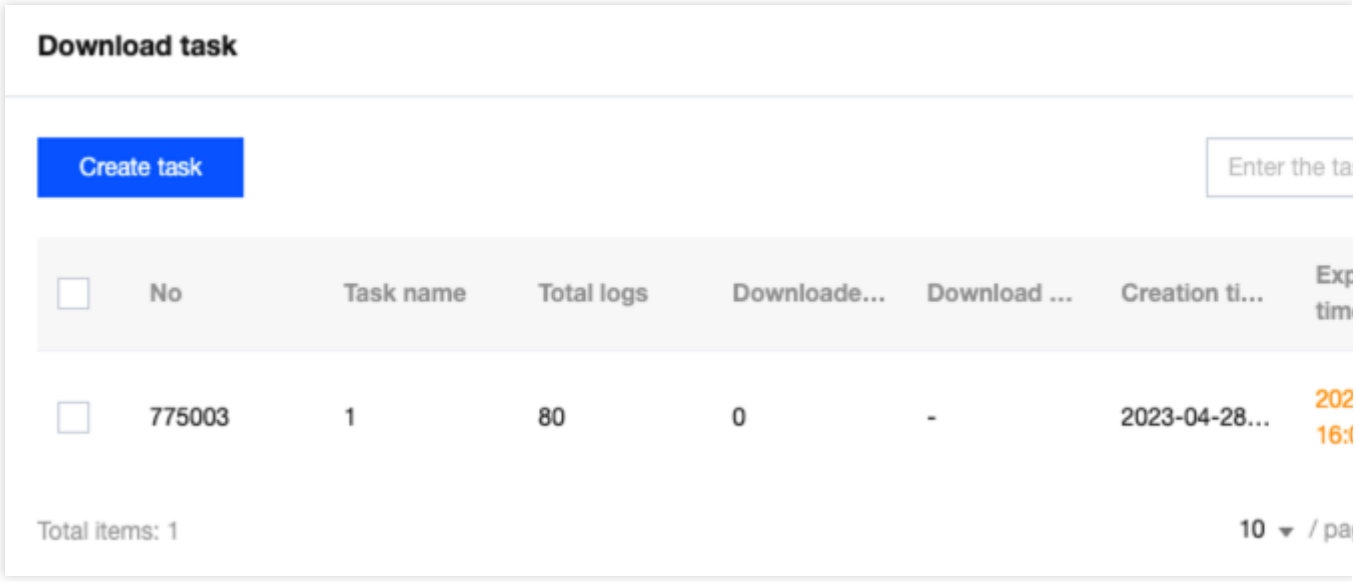
Only one download task can be created at a time.

One download task can contain up to 1 million logs. If you need to download more, it is recommended to create multiple tasks one by one, or contact us for support.

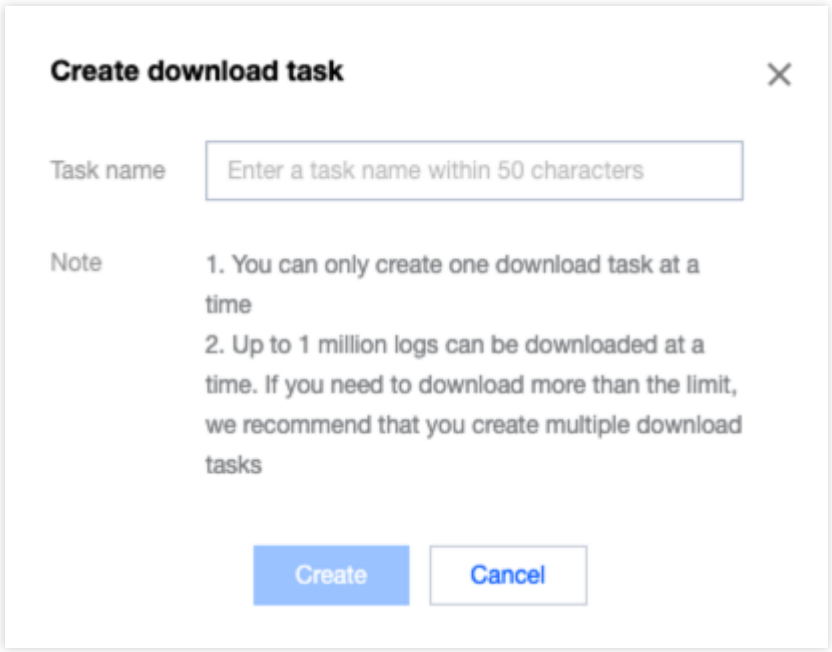
©2013-2022 Tencent Cloud. All rights reserved.

If you select a wildcard domain name (for example, *.abc.com), logs of all its associated subdomain names such as those suffixed with `.abc.com` will also be downloaded.

2. On the **Download task** page, click **Create task**.



3. Enter a task name and click **Create**.



4. After the task is created, you can view the total number of logs, download progress, download status, creation time, and expiration time. Click **Download** to export the logs in CSV format.

Note

Logs downloaded are retained for 3 days.

©2013-2022 Tencent Cloud. All rights reserved.

See Also

Log field description

Basic Information

Field Name	Description
host	The domain name accessed by the client.
uri	The request URI, which is a character string for identifying resources.
attack_ip	The source IP of the attack.
attack_type	The attack type.
rule_id	ID of the protection rule applied. Note that ID of the AI engine rule is 0.
method	The request method used in the attack request.
user_agent	User-Agent that records information about the browser type and operating system used by the attacker IP.
risk_level	Risk level of the attack.
status	The action taken on the attack request. Valid values are `0` (Observe) and `1` (Block).
count	Number of attacks from the same attacker IP every 10 seconds.
domain	The domain name attacked by the client.
pan	The domain name accessed by the client.
domain_name	The domain name accessed by the client.
attack_time	The time that the attack is launched.
attack_place	The attack location in the HTTP request.
action	The action to take on the attack request. Valid values are `0` (Observe) and `1` (Block).
ipinfo_nation	Country of the attacker IP.
ipinfo_province	Province/State of the attacker IP.
ipinfo_city	City of the attacker IP.

©2013-2022 Tencent Cloud. All rights reserved.

ipinfo_state	Country of the attacker IP.
ipinfo_dimensionality	Latitude of the attacker IP.
instance	Name of the WAF instance accessed by the domain name.
attack_category	The attack category (unavailable currently).
edition	Edition of the WAF instance. Valid values are sparta-waf (SaaS WAF) and clb-waf (CLB WAF).
uuid	Unique ID of the log.
attack_content	The content that was attacked.
http_log	The log files recording HTTP requests and responses.
headers	The protocol headers, including custom headers.
rule_name	The rule name (unavailable currently).
count	Number of attacks of the same type from the same attacker IP every 10 seconds.
args_name	Parameters in the HTTP request.
ipinfo_isp	ISP of the attacker IP.
appid	APPID of the Tencent Cloud account.
ipinfo_longitude	Longitude of the attacker IP.

©2013-2022 Tencent Cloud. All rights reserved.

Access Logs

Last updated：2023-12-29 14:46:39

Overview

Access logging is used to record access logs of domain names protected by WAF. It allows you to query and download access logs generated in the last 30 days and retain them for up to 180 days. After enabling this feature, you can query and download access logs as needed to meet your security compliance and OPS requirements.

Note:

To use access logging, you need to purchase an extra log services pack and enable access logging as instructed in Directions. Only after this feature is enabled for a domain name can its access requests be logged by WAF.

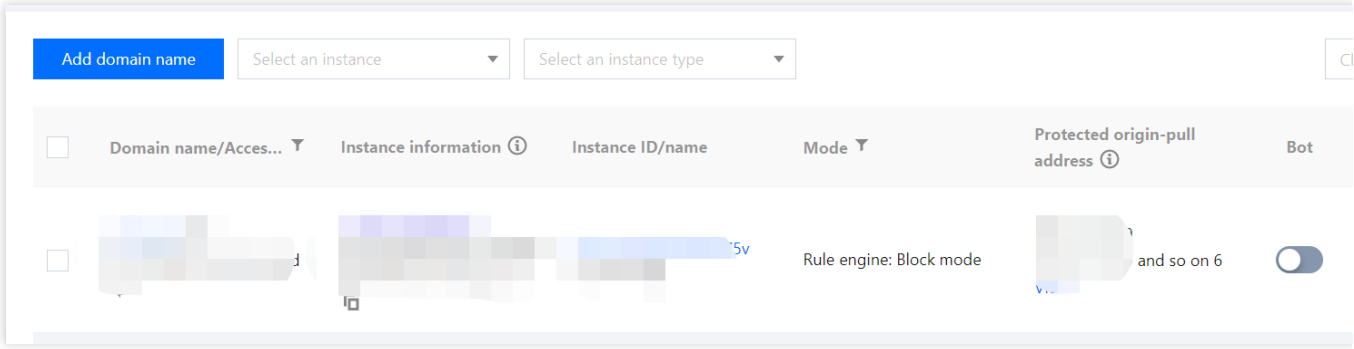
To disable access logging: You can delete the corresponding billable item in Renewal Management. Note that access logging will be stopped within 2 hours and the history will be cleared within 24 hours once the billable item is removed.

To expand logging capacity: When the required log storage exceeds the purchased log pack's capacity, new access logs will not be stored, and the historical access logs will be deleted when the retention period reaches. To avoid loss of access logs from insufficient capacity, we recommend checking your log usage and expanding the capacity in advance.

Directions

Enabling access logging

Log in to the WAF console and select **Domain Name List** on the left sidebar. Then toggle on the access logging switch for the domain name you choose.

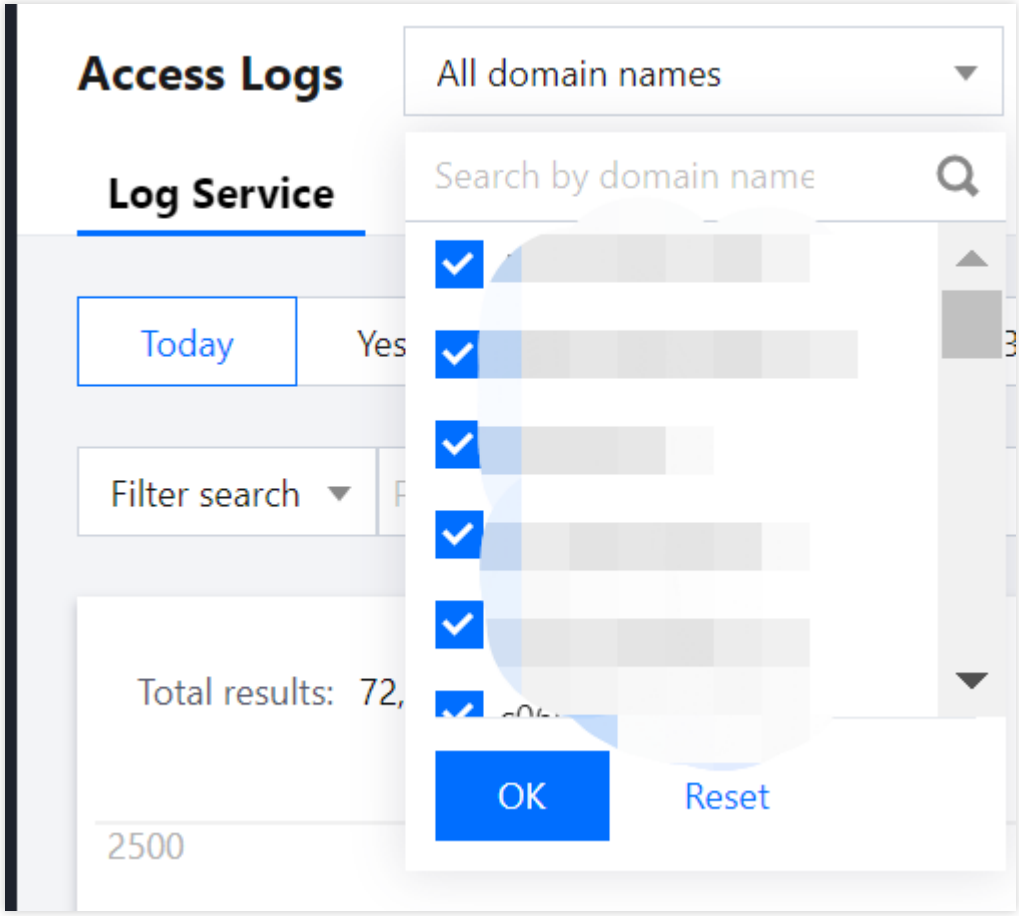


Viewing logs

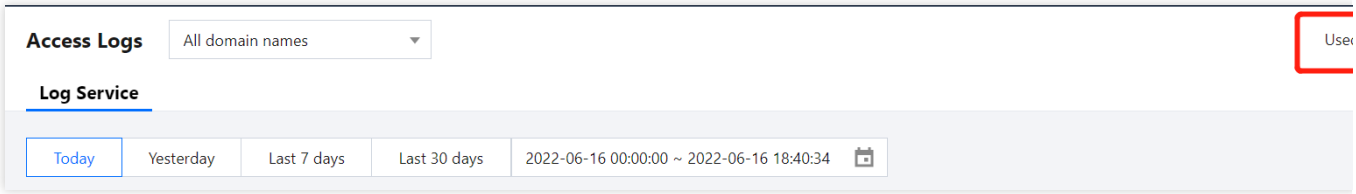
1. Log in to the WAF console and select **Access Logs** on the left sidebar. Then open the **Log service** tab.

©2013-2022 Tencent Cloud. All rights reserved.

2. Click the drop-down list in the top left corner of the page to select domain names, and click **OK**.



3. The usage capacity is displayed in top right corner. For more details about WAF billing, click **Learn more**.

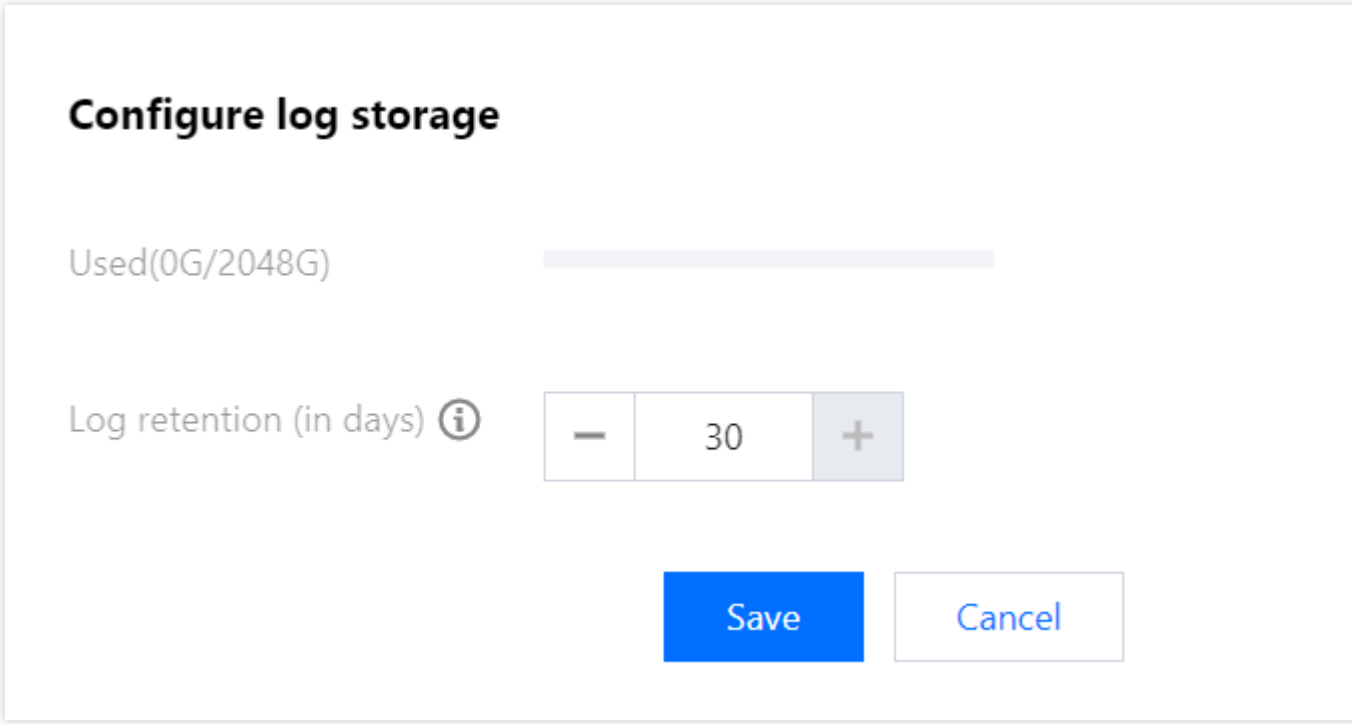


4. To view usage capacity and set the retention period at the same time, click **Storage configuration**, and then click **Save** to save your setting.

Note:

The retention period ranges from 1 to 30 days.

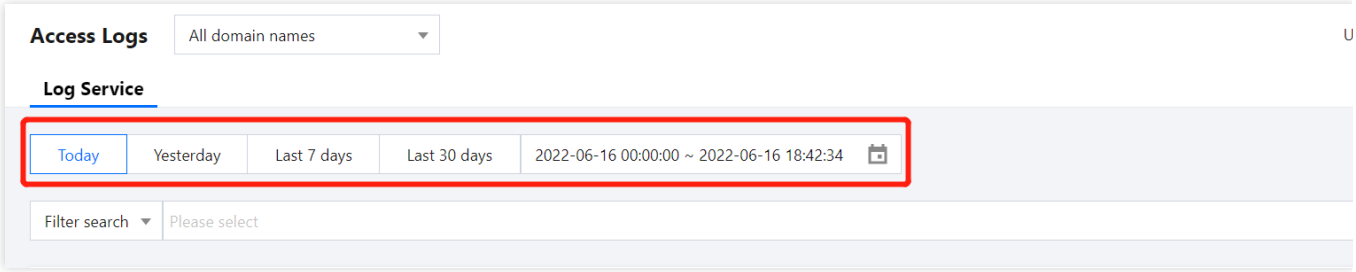
©2013-2022 Tencent Cloud. All rights reserved.



Querying logs

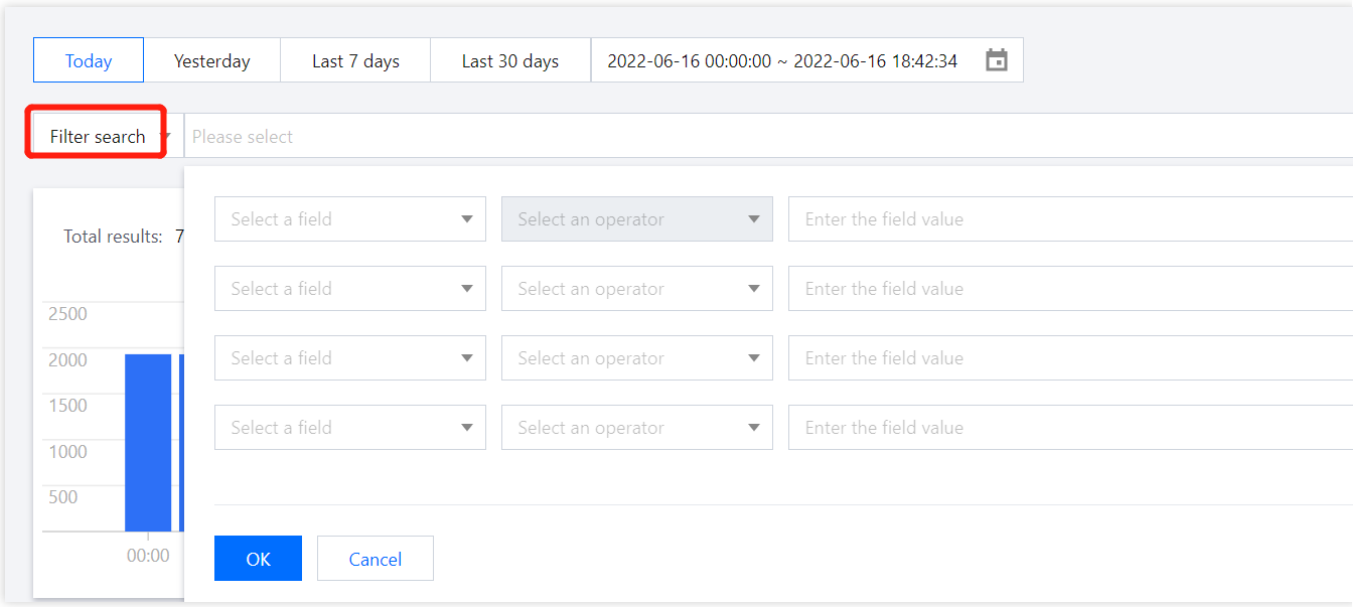
1. Log in to the WAF console and select **Access Logs** on the left sidebar. Then open the **Log service** tab.
2. Search logs by using quick search, filters, or statements.

Quick search: It allows you to search logs quickly be specifying a period.



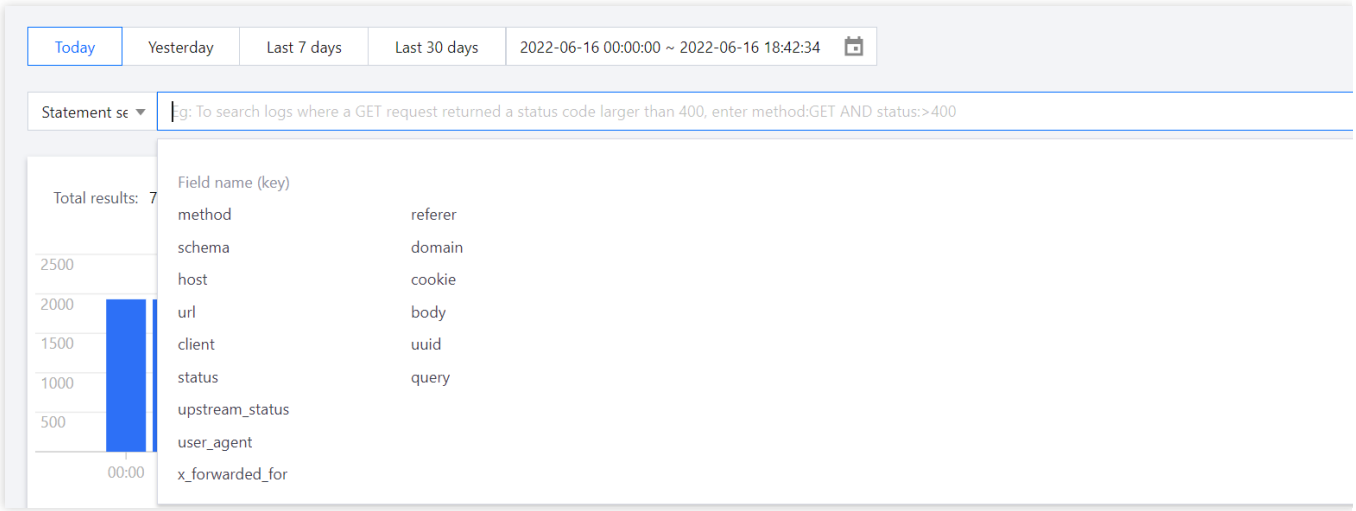
Search by filter: Select fields and operators, enter the filed values, and click **OK**. You can select multiple fields.

©2013-2022 Tencent Cloud. All rights reserved.



Search by statement: It supports professional searches by statement and enables you to run more complex log queries. Enter the required information, and then click

.



Search statement

Reserved Character	Description
AND	"AND" logical operator, such as level:ERROR AND pid:1234
OR	"OR" logical operator, such as level:ERROR OR level:WARNING
NOT	"NOT" logical operator, such as level:ERROR NOT pid:1234

©2013-2022 Tencent Cloud. All rights reserved.

TO	"TO" logical operator, such as request_time:[0.1 TO 1.0]
""	Double quotation mark, which quotes a phrase, such as name:"john Smith"
:	Colon, which is used for key-value search, such as level:ERROR
*	Wildcard, which is used to replace zero, one, or more characters, such as host:www.test*.com
?	Wildcard, which is used to replace one character, such as host:www.te?t.com
()	Parentheses, which is used to group clauses to form sub queries and control the logic operations, such as (ERROR OR WARNING) AND pid:1234
>	Range operator, which indicates the left operand is greater than the right operand, such as status:>400
>=	Range operator, which indicates the left operand is greater than or equal to the right operand, such as status:>=400
<	Range operator, which indicates the left operand is less than the right operand, such as status:<400
<=	Range operator, which indicates the left operand is less than or equal to the right operand, such as status:<=400
[]	Range operator, which includes the upper and lower boundary values, such as age:[20 TO 30]
{}	Range operator, which excludes the upper and lower boundary values, such as age:{20 TO 30}
\\	Escape character. An escaped character represents the literal meaning of the character, such as url:\\/images\\/favicon.ico. You can also use "" to wrap special characters as a whole, e.g., url:"/images/favicon.ico". For details about the difference between these two search methods, see Configuring Indexes.
+	Logical operator (similar to AND). The term +A indicates A must exist, such as +level:ERROR +pid:1234.
-	Logical operator (similar to NOT). The term -A indicates A does not exist, such as +level:ERROR -pid:1234.
&&	Logical operator (similar to AND), such as level:ERROR && pid:1234

©2013-2022 Tencent Cloud. All rights reserved.

!	Logical operator (similar to NOT), such as level:ERROR !pid:1234
/	Regular expression identifier in the format of /${regExp}/, e.g., /[mb]oat/ returns results containing moat or boat.
exists	_exists_:key returns results where the `key` value is not empty, e.g., _exists_:userAgent returns results where the userAgent value is not empty.
~	Fuzzy search, e.g., level:errro~ returns results where level contains error.

Note:

The operators are case-sensitive. For example, `AND` and `OR` represent logical search operators, while `and` and `or` are regarded as common words.

When multiple search statements are connected with spaces, they are regarded as in the `OR` logic. For example, `warning error` indicates to return results containing the `warning` keyword or `error` keyword.

The following special characters must be escaped: +, -, &&, ||, !, ( ), { }, [ ], ^, ", ~, *, ?, :, \\

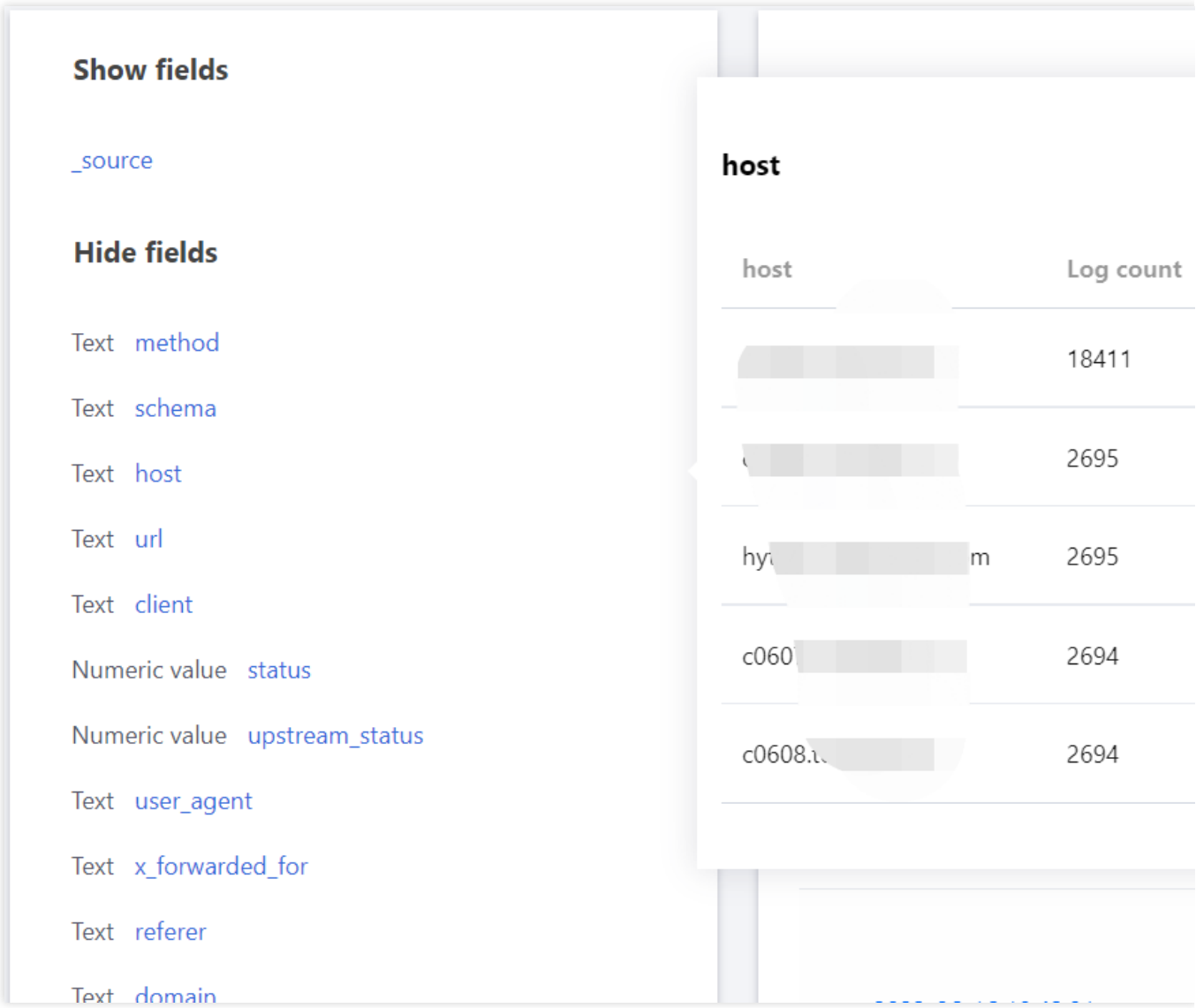
Before performing a `key:value` search, make sure the key is configured in the index configuration of the log topic.

Use () to group search conditions and clarify the precedency when using the "AND" and "OR" operators, such as `(ERROR OR WARNING) AND pid:1234`.

Displaying logs

1. Log in to the WAF console and select **Access Logs** on the left sidebar. Then open the **Log service** tab.
2. Click **Filed name** to display the top five logs that match the filed.

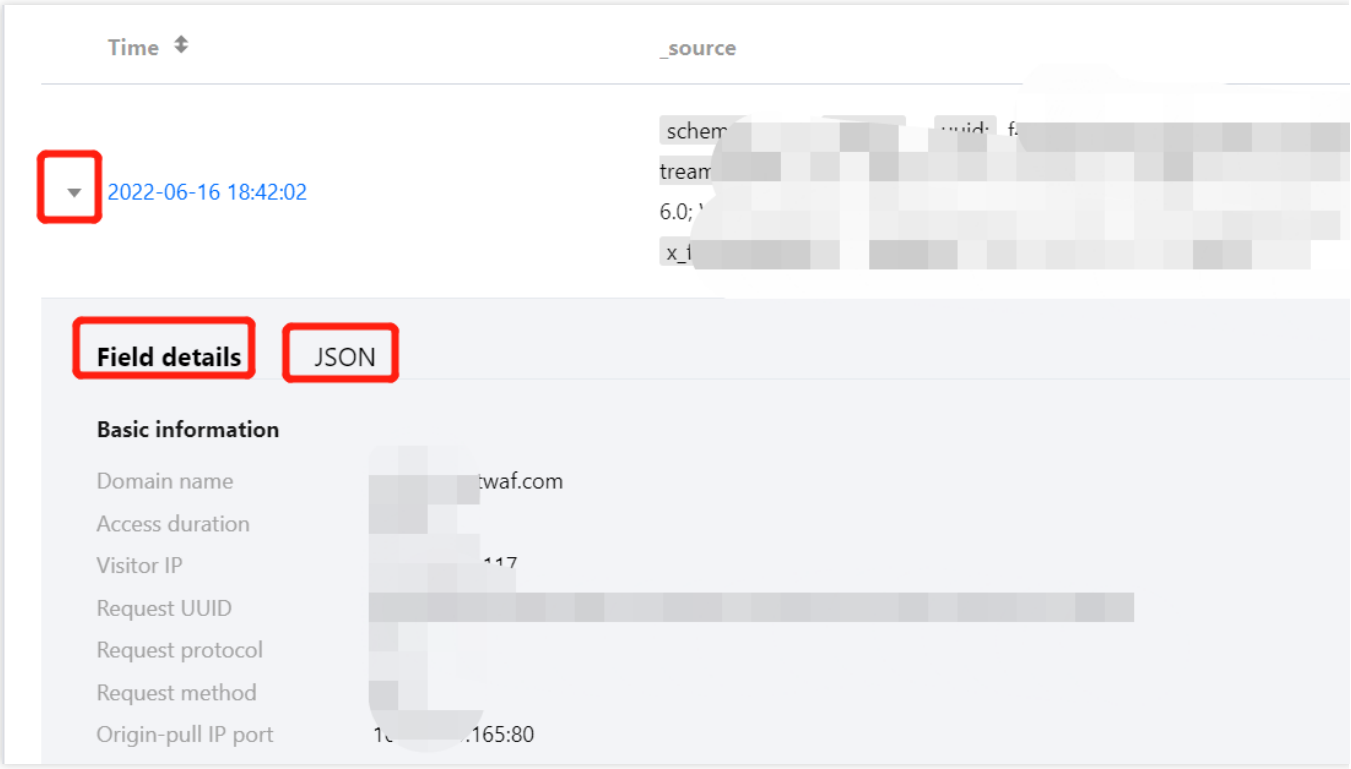
©2013-2022 Tencent Cloud. All rights reserved.



3. Click

on the left of the date that the log is generated to view filed details. If you want to view details in JSON format, click **JSON**.

©2013-2022 Tencent Cloud. All rights reserved.



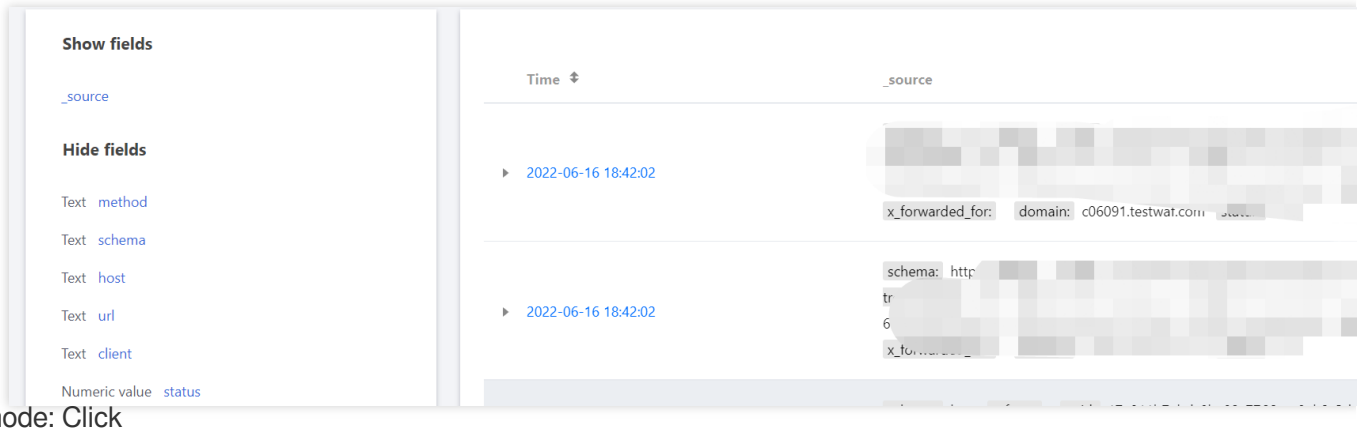
JSON field description

Field	Description
domain	Wildcard domain name
request_time	Time that the client takes to send a request to WAF and receive a response
uuid	Unique identifier of an HTTP request
schema	Request protocol: HTTP or HTTPS
method	Client request method
url	Request URI, which resides between "/" and "?" in the client's request path
host	Client domain name
http_user_agent	Request UA
headers	HTTP request header
upstream_status	Response code returned to WAF from the origin server
status	Response code returned to the client from WAF For CLB WAF, the response code 624 indicates the request is blocked and 600 indicates the request is allowed.

©2013-2022 Tencent Cloud. All rights reserved.

	For SAAS WAF, the response code 403 indicates the request is blocked and 200 indicates the request is allowed.
body_bytes_sent	Response body size
upstream_response_time	Time that WAF takes to receive the client request from the real server
ip_info.country	Country/Region
ip_info.city	City
ip_info.province	Province
ip_info.operator	ISP
ip_info.ip_type	IP type
ip_info.idc	IDC data center
ip_info.longtitude	Longitude
ip_info.dimensionality	Latitude

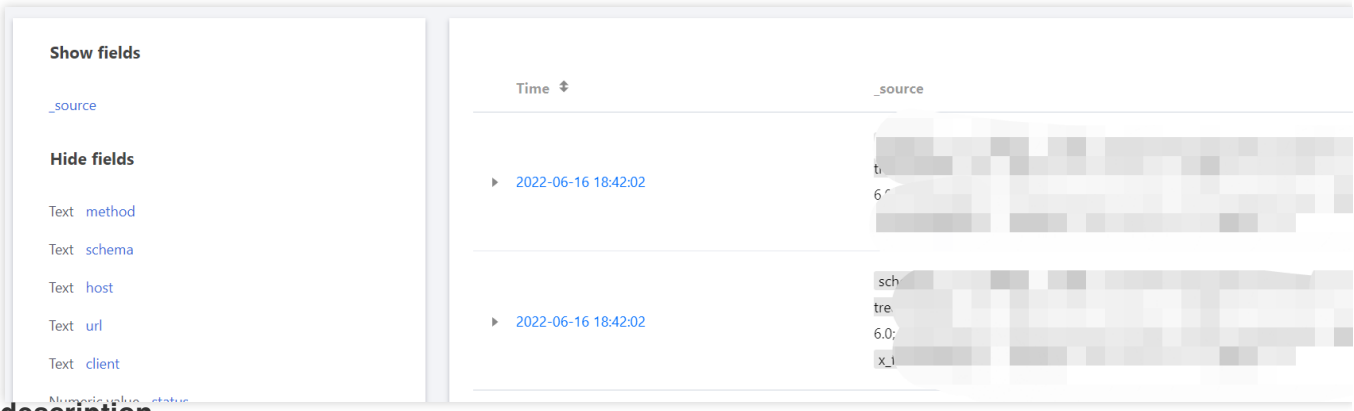
4. Display the filtered log content in the list mode or field mode.
Field mode: This is the default display mode. You can change to the other mode by clicking the icon in the top right corner.



List mode: Click

to change to list view.

©2013-2022 Tencent Cloud. All rights reserved.



Field description

Field	Description
msec	Timestamp of when the request is sent
schema	Request protocol: HTTP or HTTPS
method	Client request method
host	Client domain name
url	Request URI, which resides between "/" and "?" in the client's request path
query	HTTP Query String. The maximum length is 1 KB.
body	Request body data
http_referer	Page source
http_user_agent	Request UA
http_x_forwarded_for	All the proxies that pass the request
cookie	Request cookie. The maximum length is 1 KB.
upstream_status	Response code returned to WAF from the origin server
upstream_response_time	Time that WAF takes to receive the client request from the origin server
upstream_addr	Upstream server IP
status	Response code returned to the client from WAF
upstream_status	Response code returned to WAF from the origin server
upstream_response_length	Response length returned from the upstream server
edition	WAF versions: `sparta-waf`, `clb-waf`, `cdn-waf`

©2013-2022 Tencent Cloud. All rights reserved.

Downloading access logs

1. Log in to the WAF console and select **Access Logs** on the left sidebar. Then open the **Log service** tab.
2. Click to enter the download page. Click **OK** to create a download task.

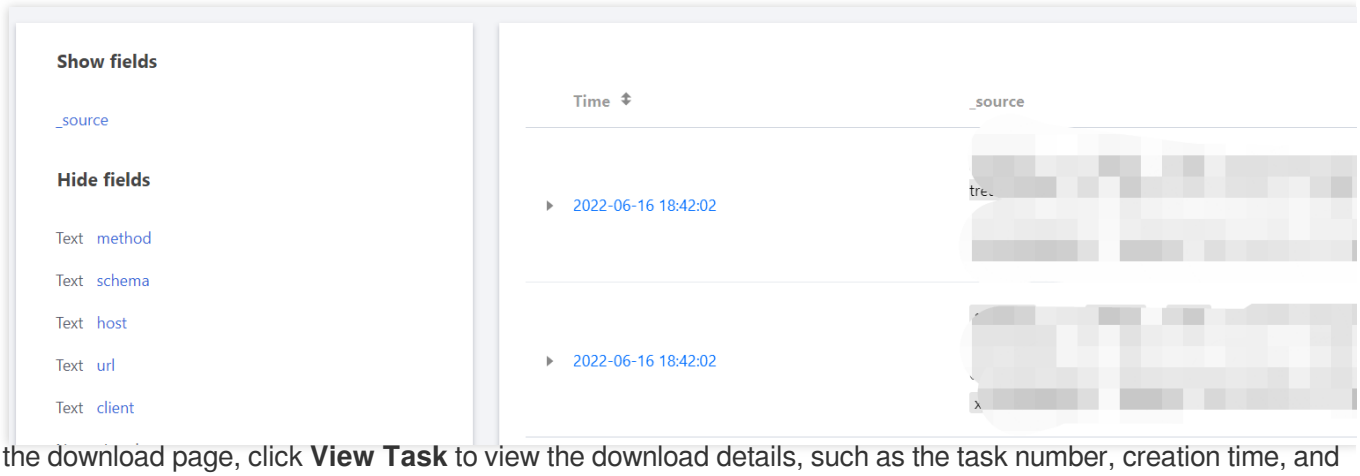
Note:

You cannot create more than one download task simultaneously.

Up to 1 million logs can be downloaded at a time. To download more logs, it is recommended that you create multiple tasks to download them in batches.

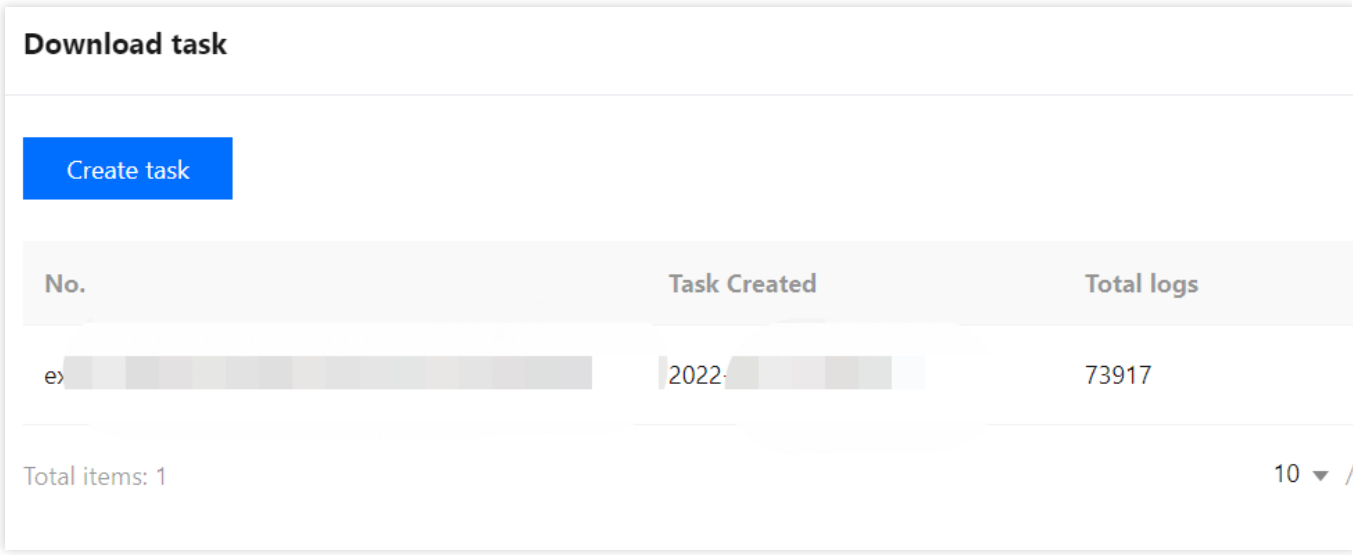
If you select a wildcard domain name (for example, *.abc.com), logs of all associated subdomain names such as those suffixed with .abc.com will also be downloaded.

Up to five download tasks can be created.



3. On the download page, click **View Task** to view the download details, such as the task number, creation time, and total number of logs.

©2013-2022 Tencent Cloud. All rights reserved.



Log field description

Field	Description
domain	Wildcard domain name
bytes_sent	Response size, including response headers (in bytes) and downstream bandwidth
method	Client request method
request_time	Time that the client takes to send a request to WAF and receive a response
http_connection	HTTP request header Connection
upstream_connect_time	Time that WAF takes to send the client request to the real server
uuid	Unique identifier of an HTTP request
upstream_addr	Upstream server IP
host	Client domain name
upstream_response_length	Response length returned from the upstream server
schema	Request protocol: HTTP or HTTPS
http_user_agent	Request UA
headers	HTTP request header
url	Request URI, which resides between "/" and "?" in the client's request path
http_x_forwarded_for	All the proxies that pass the request

©2013-2022 Tencent Cloud. All rights reserved.

http_referer	Page source
body	Request body data
remote_addr	Requester IP
cookie	Request cookie. The maximum length is 1 KB.
bot_client_ip	Client IP, which is typically the same as `remote_addr`
request_length	Request length
http_accept	HTTP request header Accept
status	Status code returned to the client from WAF
protocol	HTTP protocol, such as 1.1、1.0 and 2.0
msec	Timestamp of when the request is sent
pipe	Nginx built-in variable
content_type	HTTP request header Content-Type
time_local	Nginx readable local time string
upstream_response_time	Time that WAF takes to receive the client request from the real server
server_addr	WAF private IP
edition	WAF versions: `sparta-waf`, `clb-waf`, `cdn-waf`
upstream_status	Status code returned to WAF from the real server
body_bytes_sent	Response body size
query	HTTP Query String. The maximum length is 1 KB.

©2013-2022 Tencent Cloud. All rights reserved.

Log Shipping

Last updated：2023-12-29 14:51:09

Log Shipping

Log shipping allows you to send logs to CLS and CKafka, helping you gain more out of logs and meet user needs for operation and maintenance. To ship custom fields for your access logs, submit a ticket.

Note

For any exception with log shipping, contact us.

To ship attack logs/access logs, activate the paid you need.

After the shipping destination is configured, enable log shipping as instructed.

Log shipping can be used with log service. Enable these features as needed.

Shipping Logs to CLS

To ship logs to CLS, you need to activate CLS and grant WAF required permissions.

Note

If CLS is already activated, skip to Step 3.

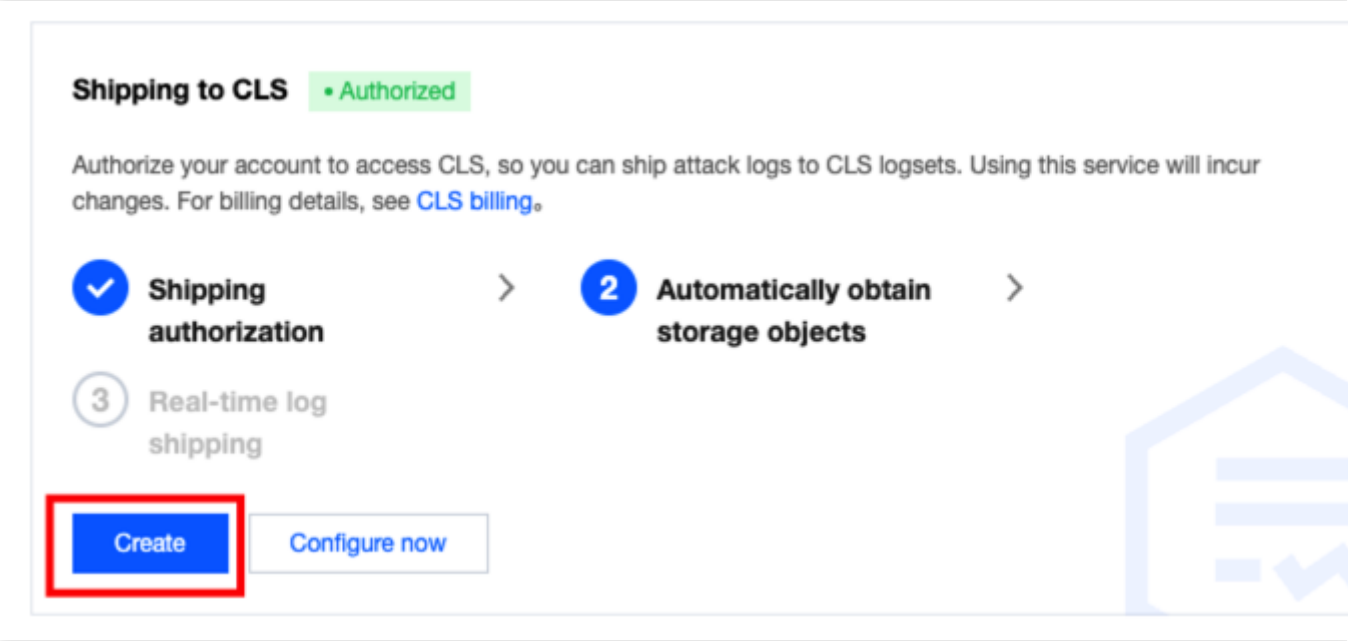
1. Log in to the WAF console. Select **Access Logs**/**Attack Logs** on the left sidebar and the **Log shipping** tab.

2. If you have not activated CLS, click **Activate now**. For details, see Cloud Log Service.

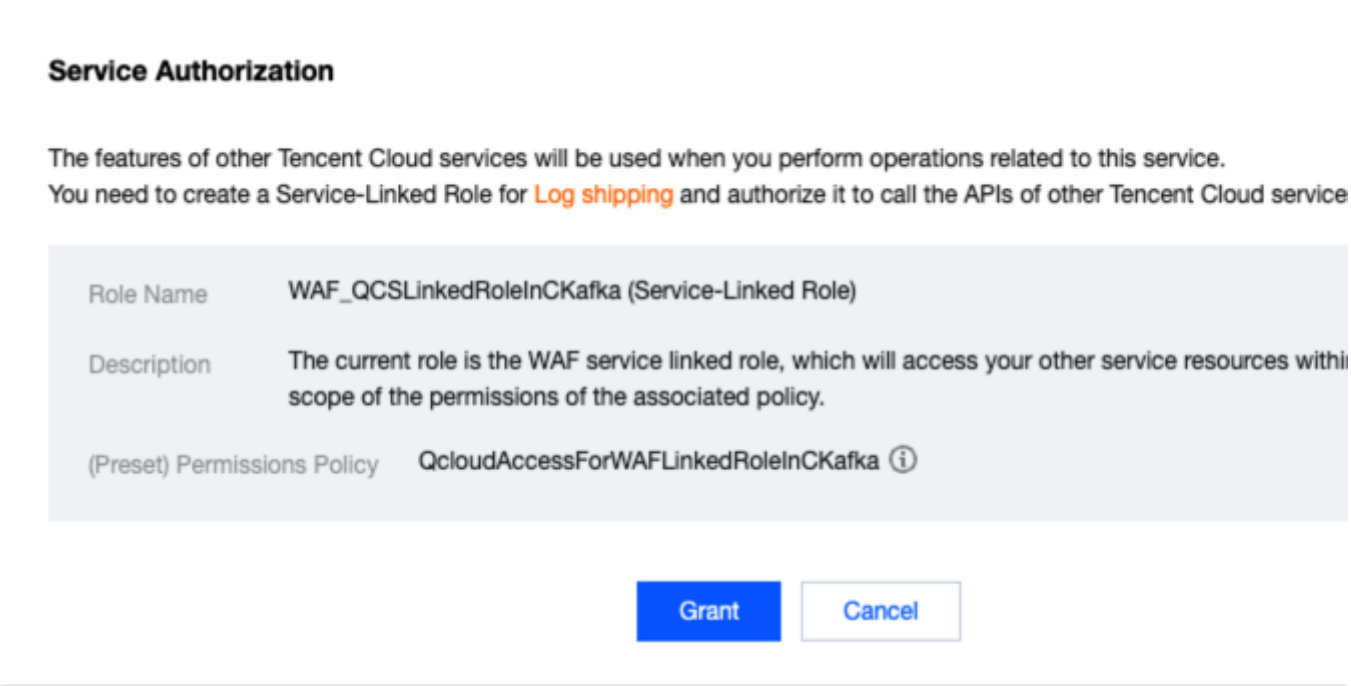
3. Authorize WAF to ship data to CLS.

3.1 In the **Shipping to CLS** section, click **Configure**.

©2013-2022 Tencent Cloud. All rights reserved.



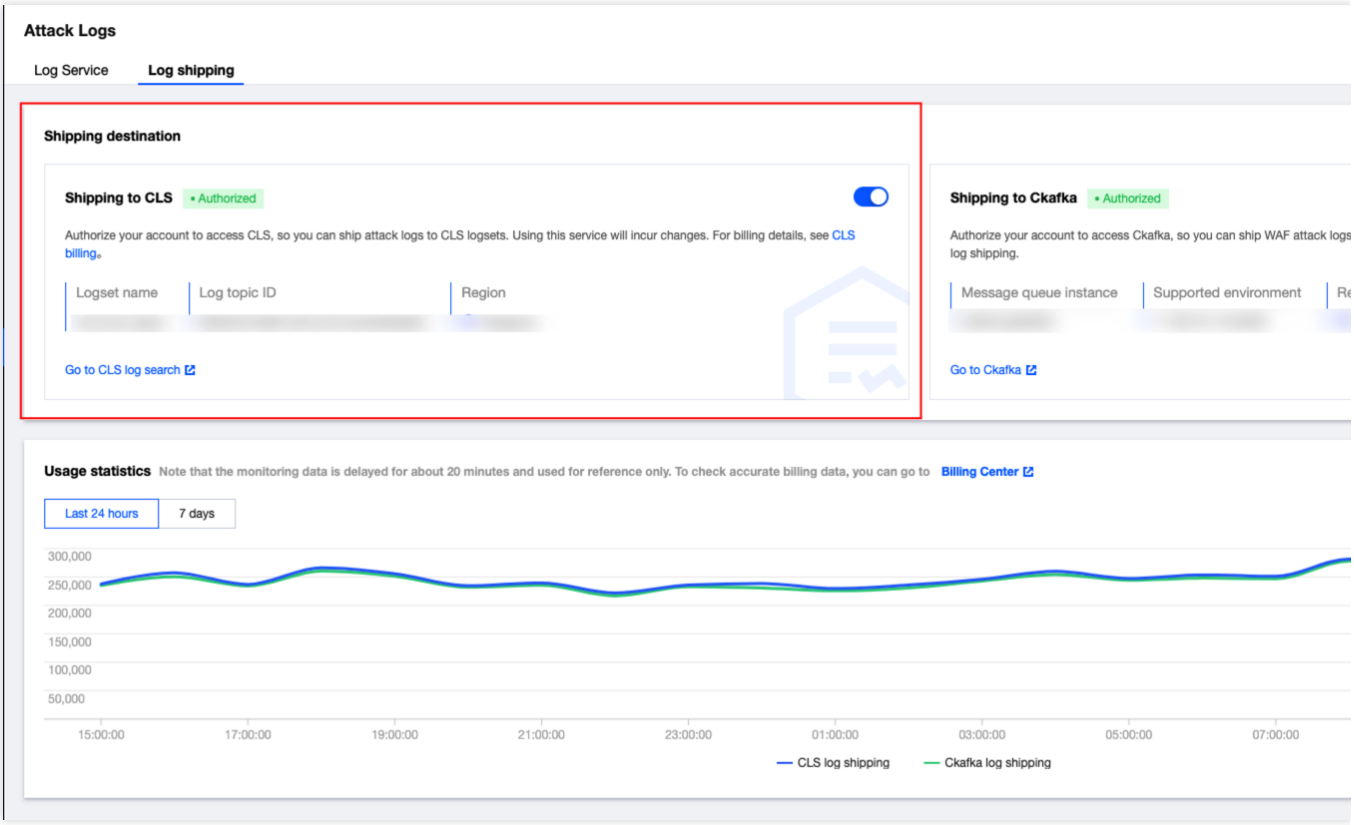
3.2 In the pop-up window, click **Authorize now**.



3.3 On the CAM authorization page, click **Authorize** to allow WAF to ship logs to CLS. If you encounter problems during the process, see Cloud Access Management.

3.4 Return to the log shipping page and click **Configure now**. Select the shipping region and log topic and then click **OK**. Alternatively, click **Create** to automatically create a WAF logset waf_post_logset. See the CLS console for details.

©2013-2022 Tencent Cloud. All rights reserved.



3.5 After logs are sent to CLS, you can enable log shipping for the desired domain names. For details, see Enabling Log Shipping.

Note

For any exception with authorization, submit a ticket.

Shipping Logs to CKafka

Prerequisites

You have purchased CKafka instances, and set the instance bandwidth based on actual log usage.

A ticket is required for connecting your supported environment to CKafka.

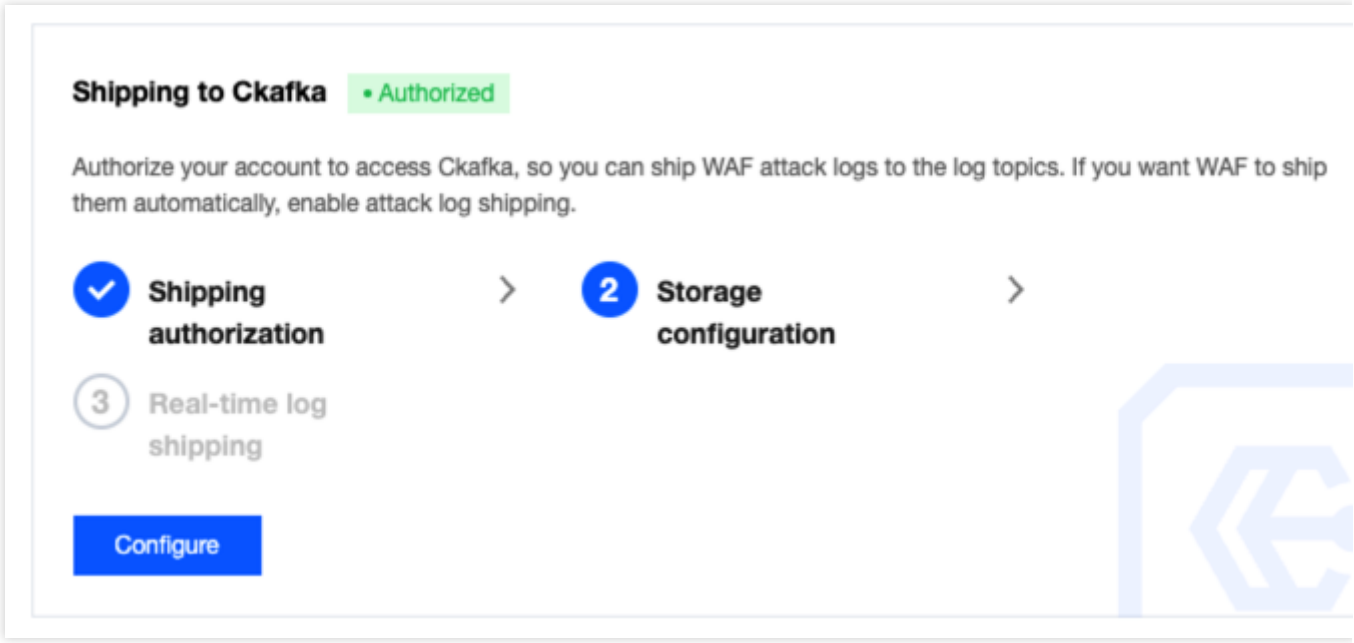
Directions

1. Log in to the WAF console. Navigate to **Access Logs**>**Log shipping**.

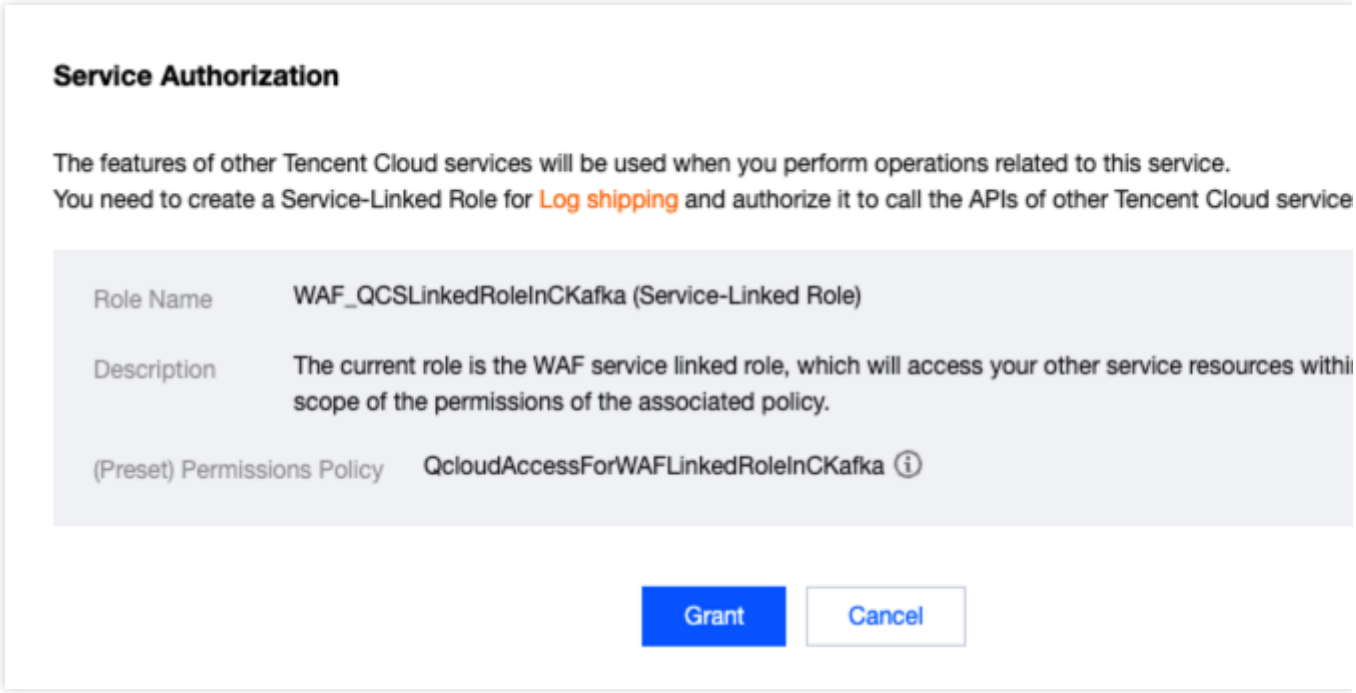
2. Authorize WAF to ship logs to the specified CKafka instance.

2.1 On the log shipping page, click **Configure now** to open an authorization pop-up window.

©2013-2022 Tencent Cloud. All rights reserved.

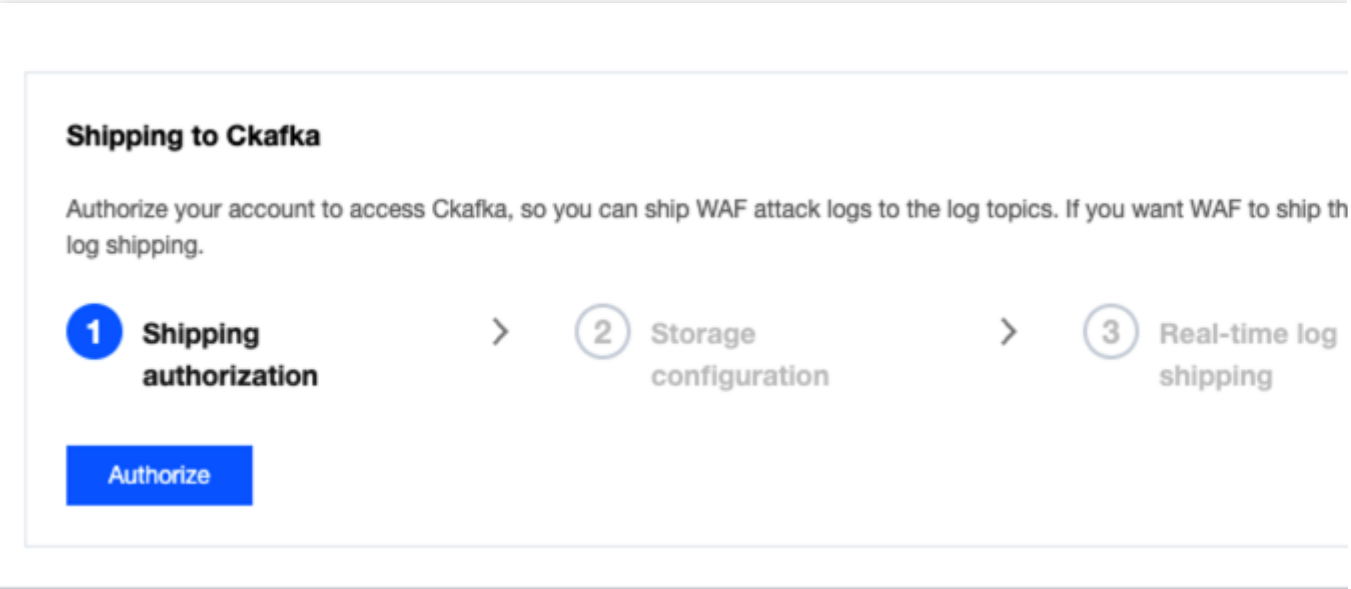


2.2 In the pop-up window, click **Authorize now**.



2.3 On the CAM authorization page, click **Authorize** to allow CKafka to send data to WAF. If you encounter problems during the process, see Cloud Access Management.

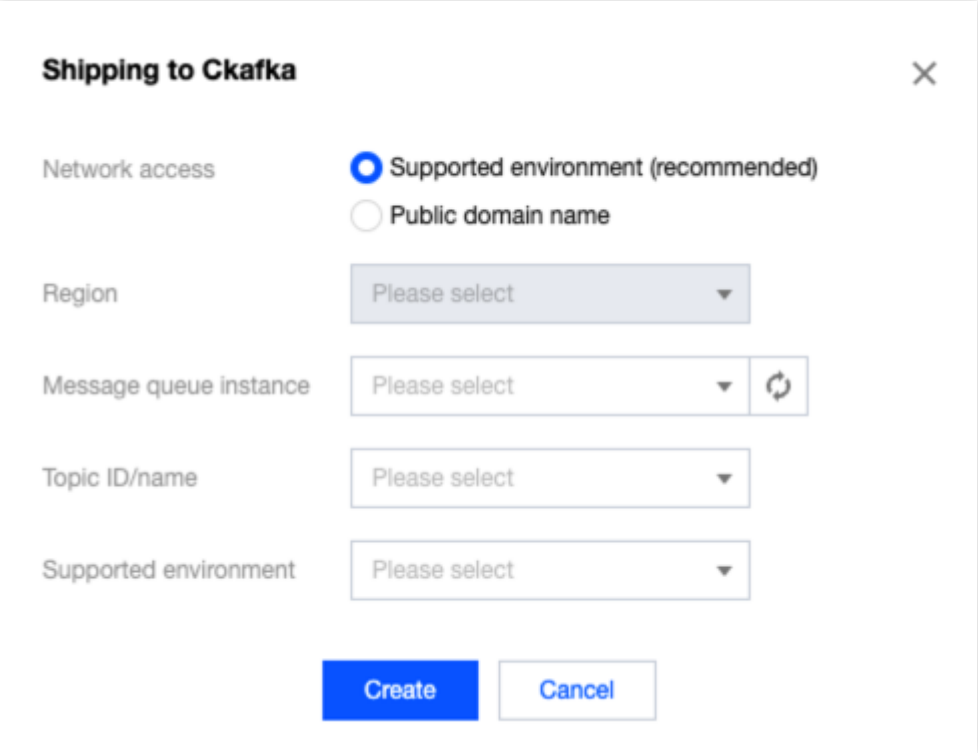
©2013-2022 Tencent Cloud. All rights reserved.



2.4 After the authorization is complete, go back to the log shipping page and click **Configure now**.

3. In the pop-up window, set the required parameters and click **OK**.

Supportive environment: Select Tencent Cloud products that you purchased and can be used with CKafka, and then select a CKafka instance and IP port.

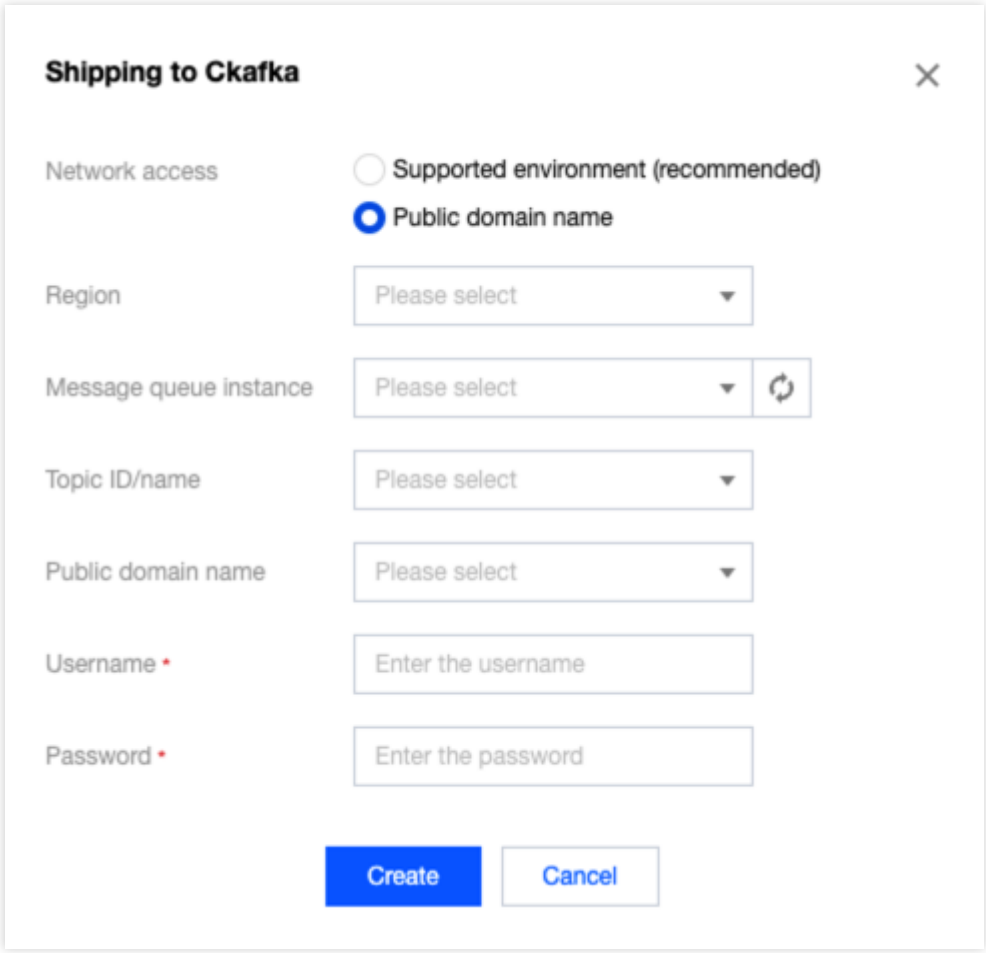


Parameter	Description	Remarks
Region	For more information about CKafka supported regions, see Regions and	To connect your supportive environment to CKafka, submit a ticket.

©2013-2022 Tencent Cloud. All rights reserved.

	AZs.
Instance	The CKafka instance running in the current region.
Topic ID/name	The topic ID and name.
Supportive environment	The route specified to connect the supportive environment.

Public domain name: Select a CKafka instance and public domain name and enter the username and password of the instance.



Parameter	Description
Region	For more information about CKafka supported regions, see Regions and AZs.
Instance	The CKafka instance running in the current region.
Topic ID/name	The topic ID and name.

©2013-2022 Tencent Cloud. All rights reserved.

Supportive environment	The route specified to connect the supportive environment.
Username	The SASL username.
Password	The SASL password.

4. After logs are sent to CKafka, you can enable log shipping for the desired domain names.

Enabling Log Shipping

After shipping logs to CLS or shipping logs to Ckafka, you need to enable log delivery for the specified domain name/instance.

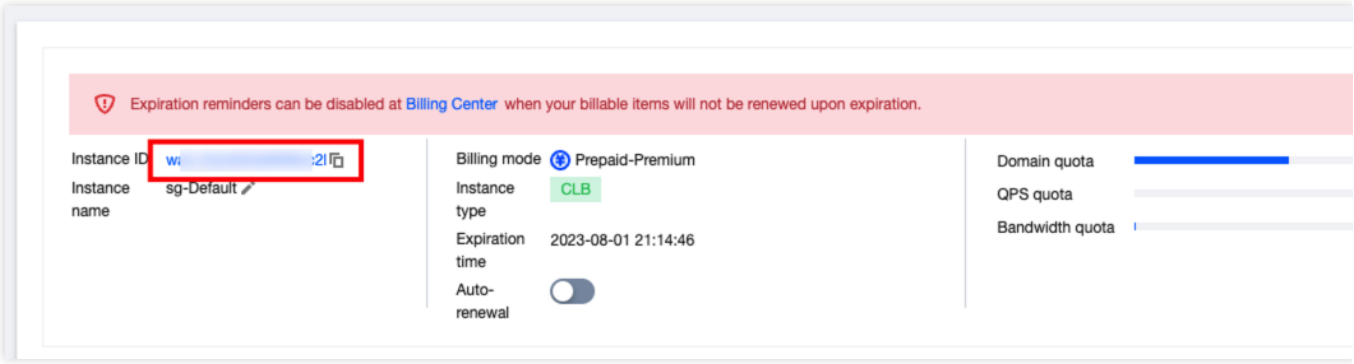
Note

Shipping attack logs is enabled at the instance level. This feature is only available for instances of Enterprise and above editions.

Shipping access logs is enabled at the domain level. This feature is available for all instances, regardless of the edition.

Enabling attack log shipping

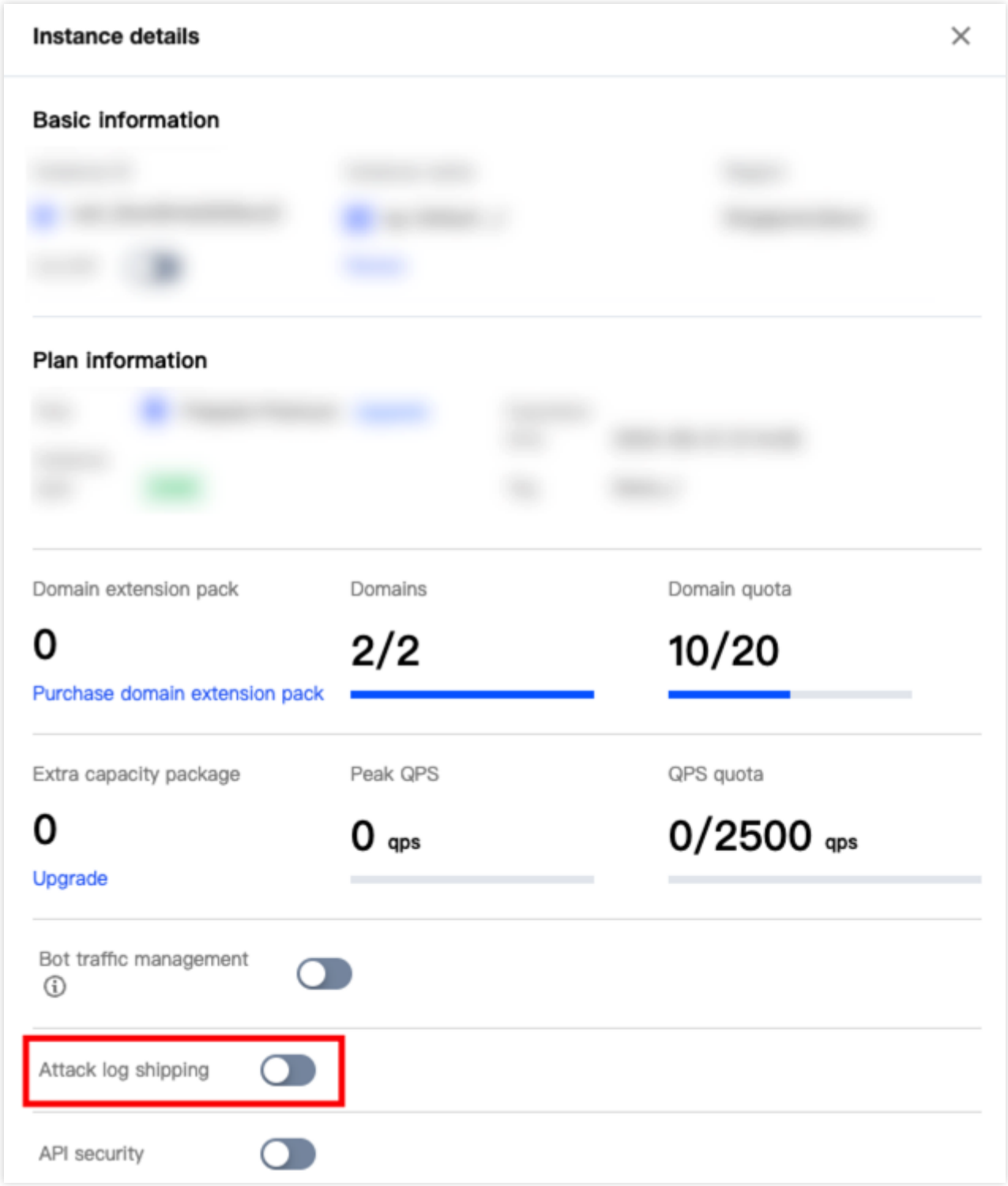
1. Log in to the WAF console and select **Instance Management** on the left sidebar.
2. On the instance management page, click **Instance name** to bring up the sidebar.



3. In the instance details, click

to enable attack log shipping for the current instance.

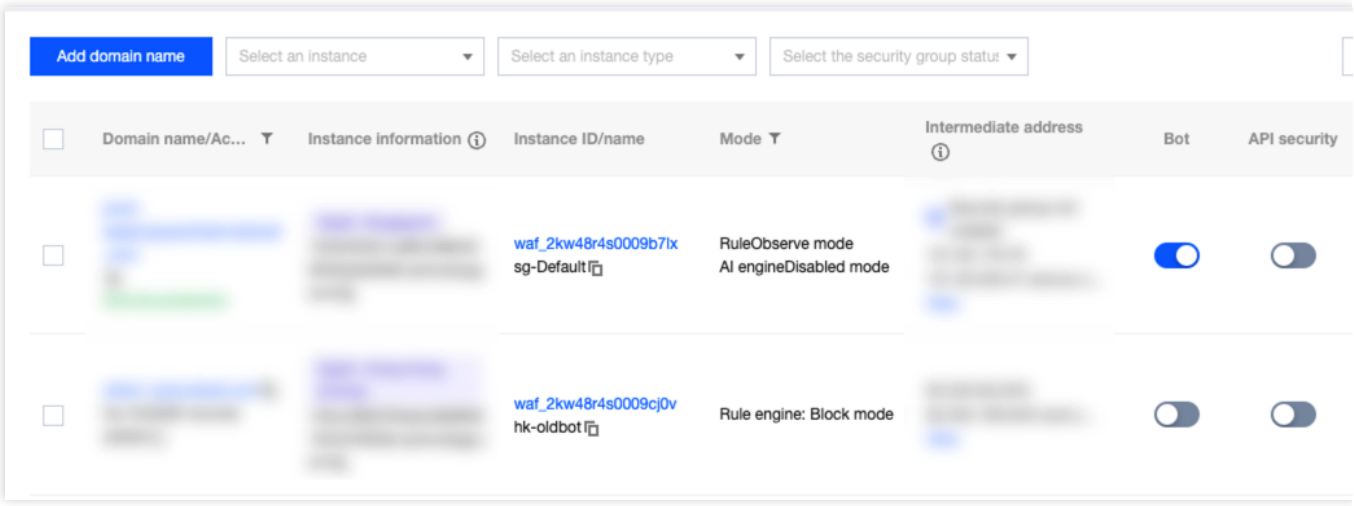
©2013-2022 Tencent Cloud. All rights reserved.



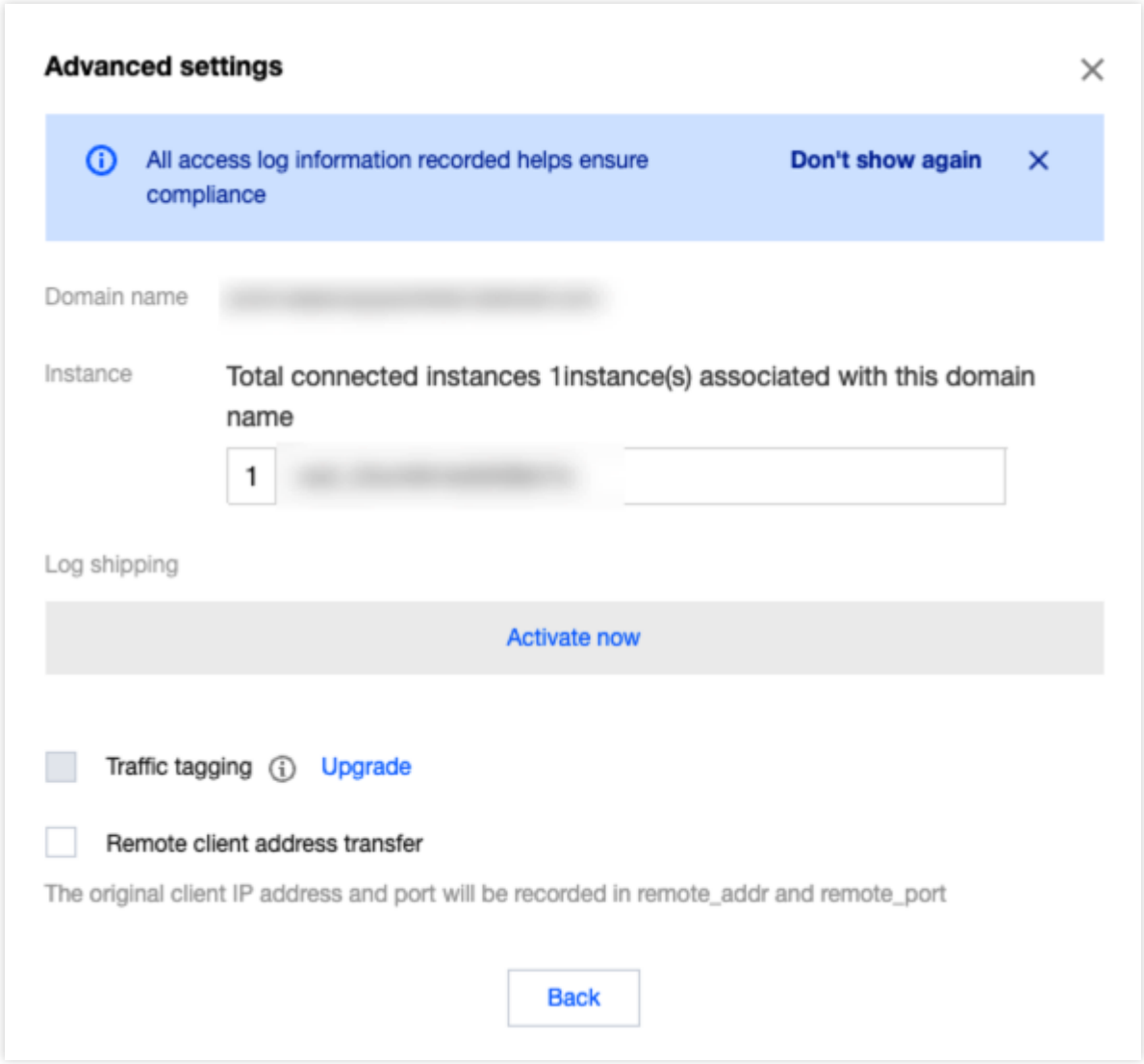
Enabling access log shipping

1. Log in to the WAF console and navigate to **Connection Management** > **Domain names**.
2. On the page displayed, select a target domain name and click **More** > **Log shipping**.

©2013-2022 Tencent Cloud. All rights reserved.



3. In the advanced settings window, select logs to ship and click **Save**.



©2013-2022 Tencent Cloud. All rights reserved.

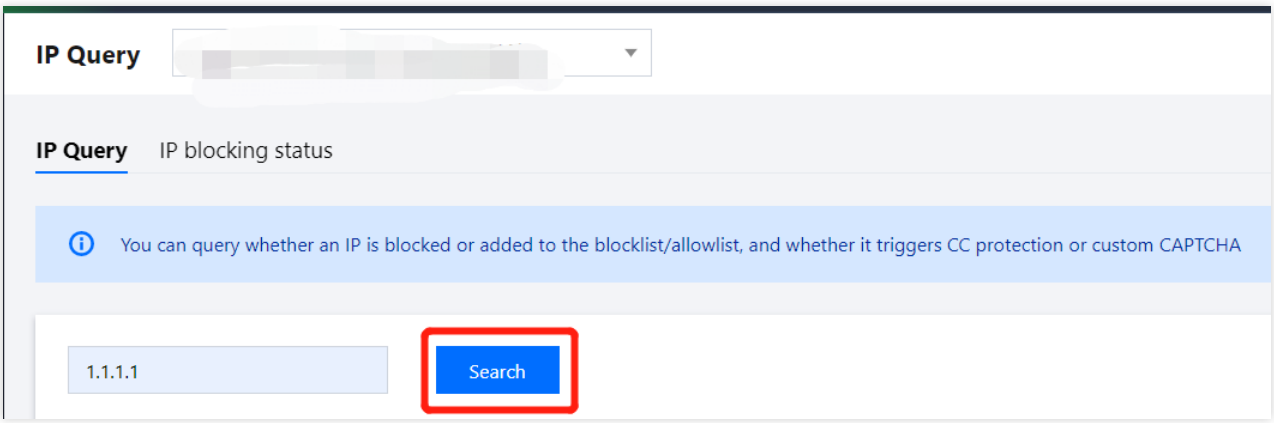
IP Query

Last updated：2023-12-29 14:52:09

This document describes how to view the IP information and blocking status using the IP query feature.

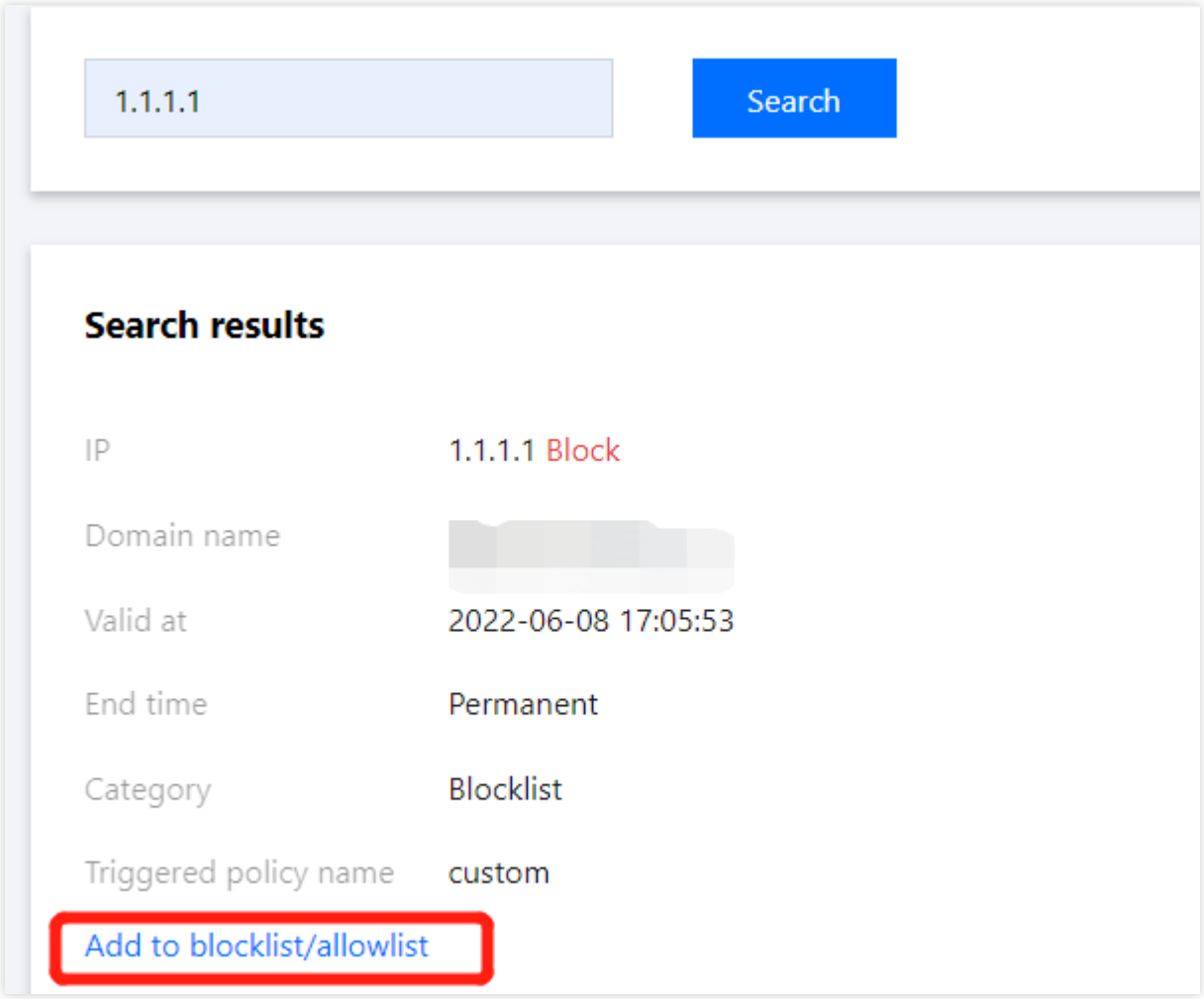
IP Query

1. Log in to the WAF console and click **IP Query** on the left sidebar.
2. On the page that appears, click a target domain name and enter an IP to search. Then click **Search**.



3. In the query results, you can view the specific IP details, and click **Add to blocklist/allowlist** to manually add the IP to the blocklist/allowlist.

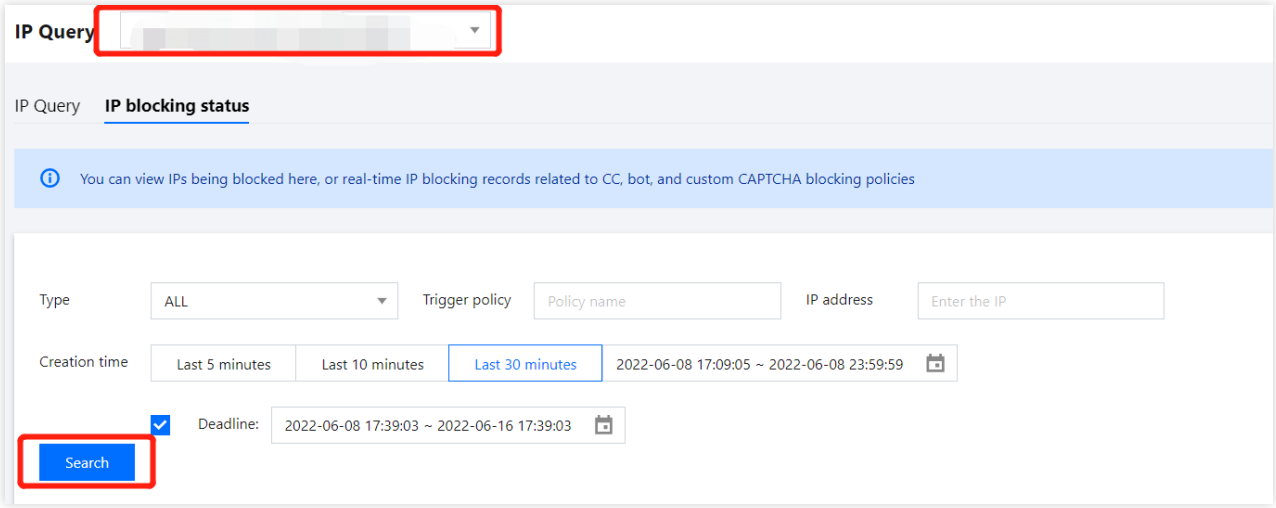
©2013-2022 Tencent Cloud. All rights reserved.



IP Blocking Status

1. Log in to the WAF console and select **IP Query** on the left sidebar. Open the **IP blocking status** tab.
2. On the IP blocking status page, specify the IP type, triggering policy, IP address, creation time or expiration time, and click **Search**.

©2013-2022 Tencent Cloud. All rights reserved.



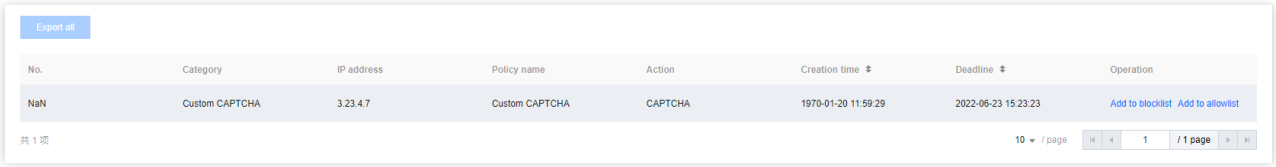
3. Click **Export all**. In the pop-up window, click **Export record** to export the query results.

Note:

A large export may take longer time to process.

Up to 10,000 entries can be exported.

4. In the list of query results, select an IP that you want to add to the blocklist/allowlist, and click **Add to blocklist** or **Add to allowlist**.



©2013-2022 Tencent Cloud. All rights reserved.