Web Application Firewall

User Guide

Issue 156

Date 2025-07-16

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Creating a User Group and Granting Permissions....1
2 Buying WAF....4
2.1 Buying a Cloud WAF Instance....4
2.2 Buying a Dedicated WAF Instance....12
3 Connecting a Website to WAF....22
3.1 Website Connection Overview....22
3.2 Connecting Your Website to WAF (Cloud Mode - CNAME Access)....29
3.2.1 Connecting Your Website to WAF (Cloud Mode - CNAME Access)....29
3.2.2 Example Configuration....50
3.3 Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)....56
3.4 Connecting Your Website to WAF (Dedicated Mode)....62
3.5 Ports Supported by WAF....77
4 Viewing Protection Events....83
4.1 Querying a Protection Event....83
4.2 Handling False Alarms....88
4.3 Using LTS to Log WAF Activities....98
5 Configuring Protection Policies....114
5.1 Protection Configuration Overview....114
5.2 Configuring Basic Web Protection to Defend Against Common Web Attacks....120
5.3 Configuring CC Attack Protection Rules to Defend Against CC Attacks....126
5.4 Configuring Custom Precise Protection Rules....141
5.5 Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses....154
5.6 Configuring Geolocation Access Control Rules to Block or Allow Requests from Specific Locations....166
5.7 Configuring Threat Intelligence Access Control Rules to Block or Allow IP Addresses in a Specified IP Address Library....175
5.8 Configuring Web Tamper Protection Rules to Prevent Static Web Pages from Being Tampered With....178
5.9 Configuring Anti-Crawler Rules....183
5.10 Configuring Information Leakage Prevention Rules to Protect Sensitive Information from Leakage....192
5.11 Configuring a Global Protection Whitelist Rule to Ignore False Alarms....199
5.12 Configuring Data Masking Rules to Prevent Privacy Information Leakage....205

5.13 Configuring a Scanning Blocking Rule to Automatically Block Heavy-Traffic Attacks 210
5.14 Configuring Bot Protection Rules to Defend Against Bot Behavior 214
5.15 Creating a Reference Table to Configure Protection Metrics in Batches 227
5.16 Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration 231
5.17 Condition Field Description 238
5.18 Application Types WAF Can Protect 249
6 Viewing the Dashboard 254
7 Website Settings 265
7.1 Recommended Configurations After Website Connection 265
7.1.1 Configuring PCI DSS/3DS Compliance Check and TLS 265
7.1.2 Enabling the HTTP/2 Protocol 275
7.1.3 Configuring a Response Body Length in Logs 276
7.1.4 Configuring Request and Response Header Forwarding 277
7.1.5 Modifying the Alarm Page 279
7.1.6 Stopping WAF from Inserting Cookie Fields 281
7.1.7 Enabling WAF IPv6 Protection 282
7.1.8 Switching the Load Balancing Algorithm 284
7.1.9 Enabling the Cookie Security Attributes 285
7.1.10 Modifying a Verification Code 286
7.1.11 Configuring a Custom Log Trace ID 286
7.1.12 Configuring a Traffic Identifier for a Known Attack Source 288
7.1.13 Configuring a JA3/JA4 Fingerprint Tag 291
7.1.14 Configuring a Timeout for Connections Between WAF and a Website Server 293
7.1.15 Enabling Break Protection to Protect Origin Servers 295
7.2 Managing Websites 298
7.2.1 Viewing Basic Information of a Website 298
7.2.2 Exporting Website Settings 300
7.2.3 Changing the Protection Mode 301
7.2.4 Changing the Protection Policy for a Protected Website 302
7.2.5 Updating the Certificate Used for a Website 302
7.2.6 Editing Server Information 305
7.2.7 Viewing Protection Information About a Protected Website on Cloud Eye 307
7.2.8 Migrating Domain Names to Other Enterprise Projects 307
7.2.9 Deleting a Protected Website from WAF 309
8 Policy Management 312
8.1 Creating a Protection Policy 312
8.2 Adding a Domain Name to a Policy 314
8.3 Adding Rules to One or More Policies 315
9 Security Reports 317
10 Object Management 323

10.1 Certificate Management....323
10.1.1 Uploading a Certificate to WAF....323
10.1.2 Using a Certificate for a Protected Website in WAF....327
10.1.3 Viewing Certificate Information....328
10.1.4 Sharing a Certificate with Other Enterprise Projects....330
10.1.5 Deleting a Certificate from WAF....332
10.2 Managing IP Address Blacklist and Whitelist Groups....333
10.2.1 Adding an IP Address Group....333
10.2.2 Modifying or Deleting a Blacklist or Whitelist IP Address Group....335
11 Instance Management....338
11.1 Managing Dedicated WAF Engines....338
11.2 Viewing Product Details....349
11.3 Changing the Cloud WAF Edition and Specifications....349
11.4 Enabling Alarm Notifications....353
12 Permissions Management....358
12.1 Authorizing and Associating an Enterprise Project....358
12.2 IAM Permissions Management....359
12.2.1 WAF Custom Policies....359
12.2.2 WAF Permissions and Supported Actions....361
12.3 Permission Dependency of the WAF Console....368
13 Monitoring and Auditing....371
13.1 Using Cloud Eye to Monitor WAF....371
13.1.1 WAF Monitored Metrics....371
13.1.2 Configuring Alarm Monitoring Rules....392
13.1.3 Viewing Monitored Metrics....393
13.2 Using CTS to Audit WAF....394
13.2.1 WAF Operations Recorded by CTS....394
13.2.2 Viewing CTS Traces in the Trace List....400

1 Creating a User Group and Granting Permissions

This topic describes how to use **IAM** to implement fine-grained permissions control for your WAF resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to WAF resources.
- Grant only the permissions required for users to perform a task.
- Entrust an account or cloud service to perform professional and efficient O&M on your WAF resources.

If your account does not require individual IAM users, skip this chapter.

This topic describes the procedure for granting permissions (see **Figure 1-1**).

Prerequisites

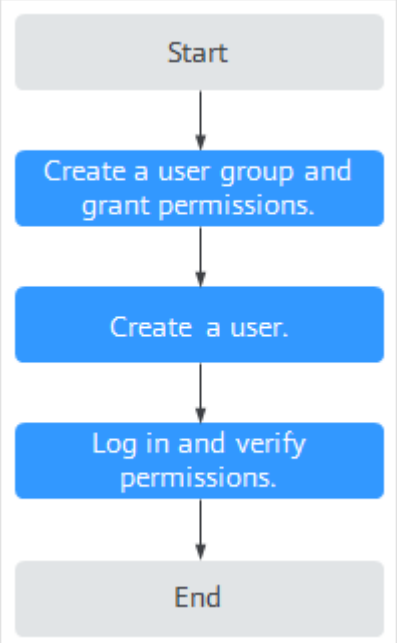
Learn about the permissions supported by WAF in **Table 1-1** and choose policies or roles based on your requirements. For the system policies of other services, see **System Permissions**.

Table 1-1 System policies supported by WAF

Role/Policy Name	Description	Category	Dependencies
WAF Administrator	Administrator permissions for WAF	System-defined role	Dependent on the **Tenant Guest** and **Server Administrator** roles. • **Tenant Guest**: A global role, which must be assigned in the global project. • **Server Administrator**: A project-level role, which must be assigned in the same project.
WAF FullAccess	All permissions for WAF	System-defined policy	None.
WAF ReadOnlyAccess	Read-only permissions for WAF.	System-defined policy	

Process Flow

Figure 1-1 Process for granting permissions



1. **Create a user group and assign permissions**.

Create a user group on the IAM console, and attach the **WAF Administrator** permission to the group.

2. **Create a user and add the user to the user group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in to the management console as the created user** and verify the permissions.

   Log in to the WAF console by using the newly created user, and verify that the user only has **WAF Administrator** permissions for WAF.

   Choose any other service in Service List. If a message appears indicating that you have insufficient permissions to access the service, the **WAF Administrator** policy has already taken effect.

2 Buying WAF

2.1 Buying a Cloud WAF Instance

Cloud WAF instances are billed either on a yearly/monthly (prepaid) or pay-per-use (postpaid) basis. In yearly/monthly billing mode, the standard, professional, and enterprise editions are available. Each edition offers domain, QPS, and rule expansion packages.

NOTE

- To buy pay-per-use WAF instances, **submit a service ticket** to enable the service.
- To use cloud load balancer WAF, you need to **submit a service ticket** to enable it for you first. Cloud load balancer WAF is available in some regions. For details, see **Functions**.
- If you want to use the load balancer access mode, make sure you are using standard, professional, or enterprise cloud WAF. When you are using cloud WAF, the quotas for the domain name, QPS, and rule extension packages are shared between the load balancer access and CNAME access modes.
- WAF APIs are free.

Before You Start

- Only one billing mode can be selected for your WAF instance in an account.
- Switch between yearly/monthly and pay-per-use payments is supported. For details, see **Can I Switch Between Yearly/Monthly and Pay-per-Use Payments for WAF?**
- For a cloud WAF instance billed on a yearly/monthly basis, after it expires or you unsubscribe from it, you can enable another WAF instance billed on either yearly/monthly or pay-per-use basis. The WAF service can save the configuration data of the original WAF instance so that you can use the configuration data without having to configure the new WAF instance only when the following conditions are met:
  - If you choose the pay-per-use billing mode, the new and original WAF instances must be under the same project in the same region.
  - If you choose the yearly/monthly billing mode, the new and original WAF instances must be in the same region.

- For a cloud WAF instance billed on a pay-per-use basis, you can disable the yearly/monthly billing mode and then enable the instance in either yearly/monthly or pay-per-use billing mode.

  NOTICE

  After the pay-per-use billing mode is disabled, the WAF billing stops, the WAF configuration data is saved, and WAF **Mode** changes to **Suspended**. In this situation, WAF forwards your website traffic without inspecting traffic.

Prerequisites

Your account for logging in to the WAF console must have the WAF Administrator and BSS Administrator permissions.

Constraints

- Only one WAF edition can be selected under an account in the same great region such as CN East, including CN East-Shanghai1 and CN East-Shanghai2 regions.

  NOTE

  For details about supported regions, see **In Which Regions Is WAF Available?**

  Generally, a WAF instance purchased in any region can protect web services in all regions. To make a WAF instance forward your website traffic faster, select the region nearest to your services.

- With professional or enterprise WAF, you can protect any non-standard ports for your website. To do so, **submit a ticket** to enable custom non-standard ports.

Specification Limitations

- A domain name expansion package supports a maximum of 10 domain names.
- The QPS limit and bandwidth limit of a QPS expansion package:
  - For web applications deployed on Huawei Cloud

    Service bandwidth: 50 Mbit/s

    QPS: 1,000 (Each HTTP GET request is a query.)
  - For web applications not deployed on Huawei Cloud

    Service bandwidth: 20 Mbit/s

    QPS: 1,000 (Each HTTP GET request is a query.)
- A rule expansion package allows you to configure up to 10 IP address blacklist and whitelist rules.

NOTICE

- If you want to use the load balancer access mode, make sure you are using standard, professional, or enterprise cloud WAF. When you are using cloud WAF, the quotas for the domain name, QPS, and rule expansion packages are shared between the load balancer access and CNAME access modes.
- The bandwidth limit applies only to websites connected to the cloud CNAME access mode. There is no bandwidth limit but only QPS limit for websites connected to WAF in load balancer access mode.

Application Scenarios

Cloud WAF is a good choice if your service servers are deployed on the cloud or on-premises and you plan to protect your website by adding its domain names to WAF.

The application scenarios for different editions are as follows:

- Standard edition

  This edition is suitable for small and medium-sized websites that do not have special security requirements.
- Professional

  This edition is suitable for medium-sized enterprise websites or services that are open to the Internet, focus on data security, and have high security requirements.
- Enterprise

  This edition is suitable for large and medium-sized enterprise websites that have large-scale services or have special security requirements.

Buying Cloud WAF Billed on a Yearly/Monthly Basis

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the upper right corner of the page, click **Buy WAF**.

Step 6 On the **Buy Web Application Firewall** page, select **Cloud Mode** for **WAF Mode**.

Step 7 Select a region.

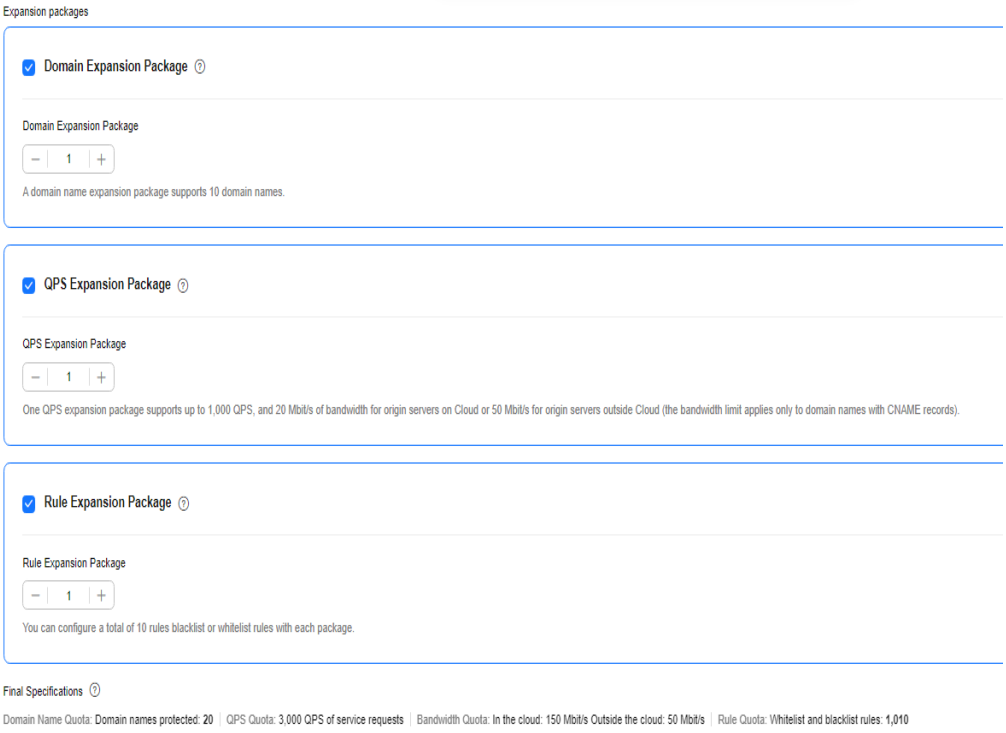
> **NOTE**
>
> Generally, a WAF instance purchased in any region can protect web services in all regions. To make a WAF instance forward your website traffic faster, select the region nearest to your services.
>
> To switch regions, select a region from the drop-down list. Only one WAF edition can be purchased in a region.

Step 8 Select an edition.

Step 9 Specify the number of domain name, QPS, or rule expansion packages.

For details, see **Domain Expansion Package**, **QPS Expansion Package**, and **Rule Expansion Package**.

Figure 2-1 Selecting expansion packages



Step 10 Configure the **Required Duration**. You can select the required duration from one month to three years.

> **NOTE**
>
> Select **Auto-renew** to enable the system to renew your service by the purchased period when the service is about to expire.

Step 11 Confirm the product details and click **Buy Now**.

Step 12 Check the order details and read the *Huawei Cloud WAF Disclaimer*. Then, check the box next to "I have read and agree to the WAF Disclaimer" and click **Pay Now**.

Step 13 On the payment page, select a payment method and pay for your order.

After WAF is enabled, you can go to the WAF console. In the navigation pane on the left, choose **Instance Management** > **Product Details**. On the product details

page, view the details of purchased instances. For details, see **Viewing Product Details**.

----End

Buying a Cloud WAF Instance Billed on a Pay-per-use Basis

To buy pay-per-use WAF instances, **submit a service ticket** to enable the service.

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the upper right corner of the page, click **Buy WAF**.

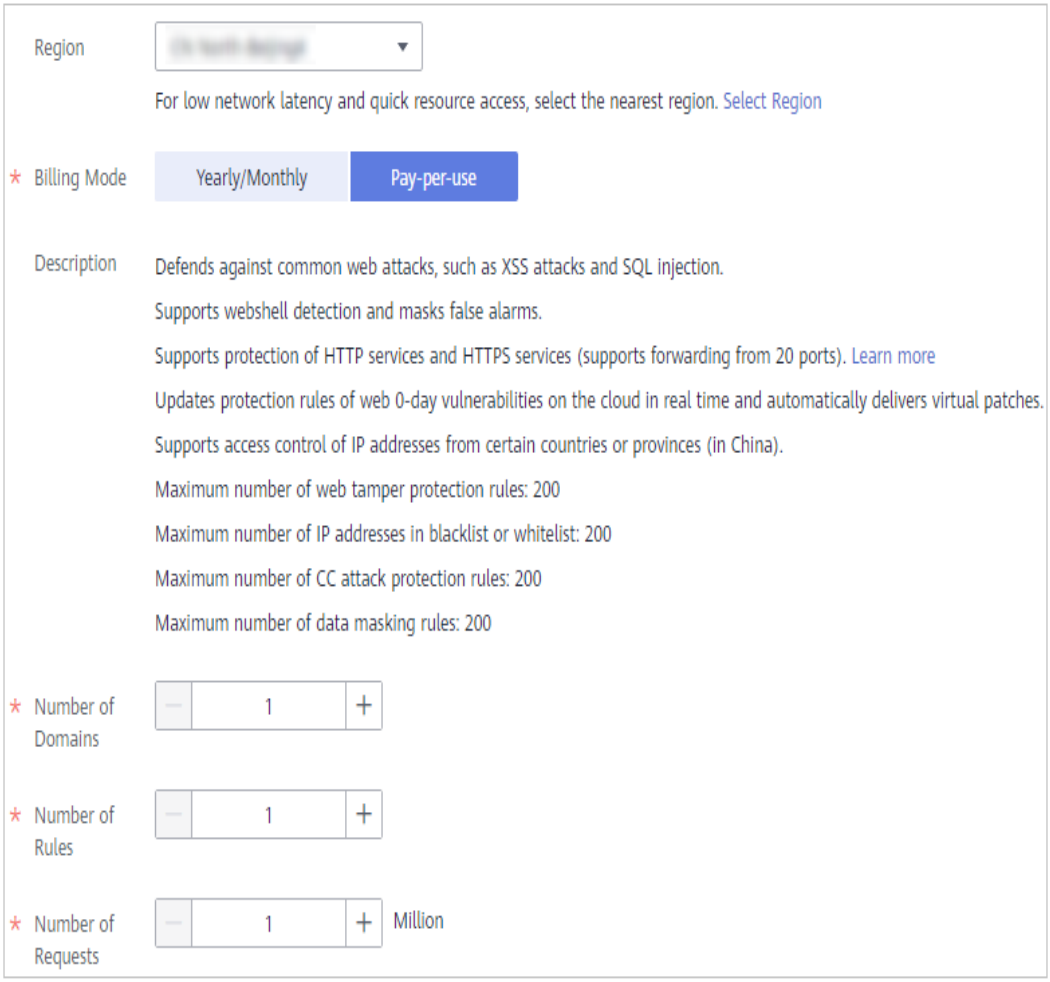
Step 6 On the **Buy Web Application Firewall** page, select **Pay-per-use** for **Billing Mode** and select a region.

NOTE

Generally, a WAF instance purchased in any region can protect web services in all regions. To make a WAF instance forward your website traffic faster, select the region nearest to your services.

To switch regions, select a region from the drop-down list. Only one WAF edition can be purchased in a region.

Figure 2-2 Pay-per-use



Step 7 In the lower right corner of the page, click **Next**.

Step 8 Click **Back to Website Settings** and add domain names of websites to be protected.

If you want to disable WAF, choose **Instance Management** > **Product Details**, and click **Disable Pay-Per-Use Billing** next to **Cloud Mode**.

- If you want to check the WAF edition in use and how long it will expire, choose **Instance Management** > **Product Details** in the navigation pane on the left and view details. For details, see **Viewing Product Details**.
- If you no longer need WAF, click **Disable Pay-Per-Use Billing** next to the **Cloud Mode** column on the **Product Details** page.

----End

Expansion Packages

WAF provides extra domain name, bandwidth, and rule expansion packages. If the domain name, bandwidth, or rule quotas included in the WAF edition you are using cannot meet your service changes, you can buy extra expansion packages.

Domain Expansion Package

One domain name expansion package can protect 10 domain names. If the cloud WAF edition you are using cannot meet your service requirements, you can purchase domain name expansion packages to increase the quota.

Cloud WAF editions offer different domain quotas.

- Standard edition: A maximum of 10 domain names can be protected.
- Professional edition: A maximum of 50 domain names can be protected.
- Enterprise edition: A maximum of 80 domain names can be protected.

NOTE

If a domain name maps to different ports, each port is considered to represent a different domain name. For example, **www.example.com:8080** and **www.example.com:8081** are counted towards your quota as two distinct domain names.

You can also change specifications of your cloud WAF to increase the domain name quota. For details, see **Changing the Edition and Specifications of a Cloud WAF Instance**.

QPS Expansion Package

A certain amount of bandwidth is provided when you buy a standard, professional, or enterprise WAF instance billed on a yearly/monthly basis. For details, see **Edition Differences**. If you have much more workloads to protect, you can buy additional QPS expansion packages.

For example, if your service traffic is 6,000 QPS and you have purchased the WAF professional edition, with a service request limit of 5,000 QPS, you can buy a QPS expansion package of 1,000 QPS to make up the difference. You can **change the edition and specifications of a cloud WAF instance** to increase QPS quota to meet service bandwidth growth requirements.

What Is the Service Bandwidth Limit?

- The service bandwidth limit is the amount of normal traffic a WAF instance can protect. A QPS expansion package protects up to:
  - For web applications deployed on Huawei Cloud

    Service bandwidth: 50 Mbit/s

    QPS: 1,000 (Each HTTP GET request is a query.)
  - For web applications not deployed on Huawei Cloud

    Service bandwidth: 20 Mbit/s

    QPS: 1,000 (Each HTTP GET request is a query.)

  NOTE

  The bandwidth in WAF is calculated by WAF itself and is not associated with the bandwidth or traffic limit of other Huawei Cloud products (such as CDN, ELB, and ECS).
- By default, a certain amount of bandwidth can be protected by the standard, professional, or enterprise WAF instance billed in yearly/monthly mode. If your origin servers (such as ECSs or ELB load balancers) are on Huawei Cloud, more bandwidth can be protected. For example, if you use an enterprise

instance, it can protect up to 300 Mbit/s of bandwidth for origin servers on Huawei Cloud, or protect up to 100 Mbit/s of bandwidth for origin servers outside Huawei Cloud, such as in on-premises data centers.

What Happens If Website Traffic Exceeds the Service Bandwidth or Request Limit?

If your website normal traffic exceeds the service bandwidth or request limit offered by the edition you select, forwarding website traffic may be affected.

For example, traffic limiting and random packet loss may occur. Your website services may be unavailable, frozen, or respond very slowly. Sometimes, your customers may see "Website is under maintenance (Protected by WAF)" when visiting your website.

In this case, upgrade your edition or buy additional QPS expansion packages.

How Many QPS Expansion Packages Do I Need?

Before buying WAF, confirm the total inbound and outbound peak traffic of the websites to be protected by WAF. Ensure that the bandwidth of the WAF edition you select is greater than the total inbound peak traffic or the total outbound peak traffic, whichever is larger.

NOTE

Generally, the outbound traffic is larger than the inbound traffic.

You can estimate the traffic by referring to the traffic statistics on the ECS console or using other monitoring tools.

Attack traffic must be removed in your estimations. For example, if your website is being accessed normally, WAF routes the traffic back to the origin ECS, but if your website is under attack, WAF blocks and filters out the illegitimate traffic, and routes only the legitimate traffic back to the origin ECS. The inbound and outbound traffic of the origin ECS you view on the ECS console is the normal traffic. If there are multiple ECSs, collect statistics on the normal traffic of all ECSs. For example, if you have six sites and the peak outbound traffic of each site does not exceed 2,000 QPS, then the total peak traffic volume does not exceed 12,000 QPS. In this case, you can buy the WAF enterprise edition.

Rule Expansion Package

If you are using yearly/monthly cloud WAF, you can purchase rule expansion packages under the current WAF edition to get more quota for IP address whitelist and blacklist rules.

A rule expansion package allows you to configure up to 10 IP address blacklist and whitelist rules.

Rule expansion packages are available when you purchase or change a cloud WAF instance.

For details, see **Changing the Edition and Specifications of a Cloud WAF Instance**.

Follow-up Operations

1. **Connecting a Website to WAF**: In cloud mode, CNAME and ELB load balancer access methods are supported. You can connect a website to WAF over website domain names or IP addresses using either of the methods.
2. **Viewing Protection Events**: After a domain name or IP address is connected to WAF, by default, WAF enables **General Check** in **Basic Web Protection**, with **Protective Action** set to **Log only** and **Protection Level** to medium, and enables **Scanner** in **Anti-Crawler**, with **Protective Action** set to **Log only**. You can view and handle protection events on the **Events** page.
3. **Configuring Protection Policies**: If default protection rules cannot meet your website security requirements, you can configure custom protection rules.
4. **Querying a Protection Event**: View website protection details.

Related Operations

- **Changing the Cloud WAF Edition and Specifications**: If you are using cloud mode WAF, you can upgrade the WAF edition in use or increase the quotas of expansion packages to protect more domain names or traffic.
- **How Do I Unsubscribe from WAF?**
- **How Do I Renew My WAF Instance?**
- **Can I Switch Between the WAF Cloud and Dedicated Modes?**

2.2 Buying a Dedicated WAF Instance

If your service servers are deployed on Huawei Cloud, you can buy dedicated WAF instances to protect important domain names or web services that are accessible over only IP addresses. To expand the protection capacities and eliminate single points of failure (SPOFs), buy an Elastic Load Balance (ELB) load balancer for your dedicated WAF instances.

Dedicated WAF instances are billed on a pay-per-use basis. You only pay for what you use.

NOTE

Dedicated WAF instances are not available in some regions. For details, see **Notice on Web Application Firewall (Dedicated Mode) Discontinued**.

You are advised to buy at least two WAF instances and use both of them to protect your services. With multiple WAF instances being used for your services, if one of them becomes faulty, WAF automatically switches the traffic to other running WAF instances to ensure continuous protection.

Prerequisites

- The account used to log in to the WAF console must have the **WAF Administrator** or **WAF FullAccess** permission.
- You are advised to use a parent account to purchase dedicated WAF instances. If you want to use an IAM user to purchase dedicated WAF instances, you need to assign the IAM management permission to the IAM user.
  - For first-time buyers, you need to assign IAM system role **Security Administrator** to them.

  - For non-first-time buyers, you need to assign IAM system policy **IAM ReadOnlyAccess** or **custom permissions** to them. The permissions are as follows:
    - iam:agencies:listAgencies
    - iam:agencies:getAgency
    - iam:permissions:listRolesForAgency
    - iam:permissions:listRolesForAgencyOnProject
    - iam:permissions:listRolesForAgencyOnDomain

    For details, see **Creating a User Group and Granting Permissions**.
- A VPC has been created. For details, see **Creating a VPC and Subnet**.
- The Organizations service is under open beta test (OBT). To use organization rules, apply for OBT.

Constraints

- If dedicated WAF instances and origin servers they protect are not in the same VPC, you can use a **VPC peering connection** to connect two VPCs. This method is not recommended as VPC peering connections may be not stable enough sometimes.
- Generally, a WAF instance purchased in any region can protect web services in all regions. To make a WAF instance forward your website traffic faster, select the region nearest to your services. For details about supported regions, see **In Which Regions Is WAF Available?**

Specification Limitations

The specifications of a dedicated WAF instance cannot be modified.

Application Scenarios

Dedicated WAF instances are good choice if your service servers are deployed on Huawei Cloud and you plan to protect your website by adding its domain names or IP addresses to WAF.

This mode is suitable for large enterprise websites that have a large service scale and have customized security requirements.

Buying a Dedicated WAF Instance

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by**

enterprise project drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the upper right corner of the page, click **Buy WAF**.

Step 6 On the **Buy Web Application Firewall** page, select **Dedicated** for **WAF Mode**.

Step 7 Configure instance parameters by referring to **Table 2-1**.

Table 2-1 Parameters of a dedicated WAF instance

Parameter		Description	Example Value
Basic Settings	Billing Mode	Only the pay-per-use billing mode is supported.	Pay-per-use
	Region	For details about supported regions, see **In Which Regions Is WAF Available?** Generally, a WAF instance purchased in any region can protect web services in all regions. To make a WAF instance forward your website traffic faster and reduce latency, select the region nearest to your services.	-
	General	Select an AZ in the selected region. **NOTE** After an AZ is selected, it cannot be changed after the purchase.	-

Parameter		Description	Example Value
Edition	Edition	Specifications **WI-500** and **WI-100** are available. ● Specifications: WI-500. Estimated performance: – HTTP services: 5,000 QPS (recommended) – HTTPS services: 4,000 QPS (recommended) – WebSocket service - Maximum concurrent connections: 5,000 – Maximum WAF-to-server persistent connections: 60,000 ● Specifications: WI-100. Estimated performance: – HTTP services: 1,000 QPS (recommended) – HTTPS services: 800 QPS (recommended) – WebSocket service - Maximum concurrent connections: 1,000 – Maximum WAF-to-server persistent connections: 60,000	WI-500
	Edition	Select a dedicated engine version. The latest dedicated engine version is recommended.	-

Parameter		Description	Example Value
	WAF Instance Type	Select a WAF instance type. Only **Network Interface** is available now. The WAF instance will be connected to your network through a VPC network interface. Only dedicated load balancers can be used for this type of instance. For details, see **Website Connection Process (Dedicated Mode)**. **NOTE** WAF also provides the **ECS** type of WAF instance. This type of WAF instance is deployed on your own ECSs. You can view the ECSs housing your WAF instances on the ECS console. To use this type of WAF instance, **submit a service ticket**. Note that only some regions support this type of WAF instance.	**Network Interface**
Network Settings	VPC	Select the VPC to which the origin server belongs.	-
	Subnet	Select a subnet configured in the VPC.	-

Parameter		Description	Example Value
	Security Group	Select a security group in the region, or click **Create Security Group** and create one. After you select a security group, the WAF instance will be protected by the access rules of the security group. WAF provides three types of security group templates. You can select one that best fits your need. ● **General-purpose web server**: allows all inbound ICMP traffic and inbound traffic on ports **22**, **80**, **443**, and **3389**. This template applies to scenarios where you need to remotely log in to an instance, run the ping command to verify the network connectivity of the instance, and provide website access services for external systems. ● **All ports open**: allows inbound and outbound traffic over any ports. This may introduce security risks. Exercise caution when selecting this option. ● **Fast-add rule**: You can select common protocols and ports to quickly add inbound rules. If you do not select any protocols and ports, no ports will be opened. You can add or modify security group rules as required after a security group is created. Click ⌄ to **Show Default Rule** and view the inbound and outbound rules of the selected security group template.	-

Parameter		Description	Example Value
		NOTICE • You can also create a security group on the VPC console and configure the following access rules: – Inbound rules Add an inbound rule to allow incoming network traffic to pass through over a specified port based on your service requirements. For example, if you want to allow access from port 80, you can add a rule that allows **TCP** and port **80**. – Outbound rules Retain the default settings. All outgoing network traffic is allowed by default. For details, see **Adding a Security Group Rule**. • If your dedicated WAF instance and origin server are not in the same VPC, enable communications between the instance and the subnet of the origin server in the security group.	
(Optional) Advanced Settings	Instance Name Prefix	Set a prefix of the WAF instance name. If you expect to purchase multiple instances, the prefix to each instance name is the same.	WAF
	Enterprise Project	This option is only available if you have logged in using an enterprise account, or if you have enabled enterprise projects. To learn more, see **Enabling the Enterprise Center**. You can use enterprise projects to more efficiently manage cloud resources and project members. **NOTE** • Value **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are listed in the default enterprise project. • The **default** option is available in the **Enterprise Project** drop-down list only after you purchase WAF under the logged-in account.	default

Parameter		Description	Example Value
	Tag	TMS's predefined tag function is recommended for adding the same tag to different cloud resources. If your organization has configured a tag policy for Web Application Firewall (WAF), you need to add tags to dedicated WAF instances based on the tag policy rules. If a tag does not comply with the policies, dedicated WAF instance may fail to be created. Contact your organization administrator to learn more about tag policies.	-
	Authorization	This parameter is required first time you buy a WAF instance. After you enable the authorization, WAF will create an agency in IAM on behalf of you to grant itself related permissions.	-
	Anti-affinity	If you enable this function, dedicated instances will be deployed on different physical servers as much as possible to improve service reliability.	-
Usage Settings	Quantity	Set the number of WAF instances you want to purchase. You are advised to buy at least two WAF instances and use both of them to protect your services. With multiple WAF instances being used for your services, if one of them becomes faulty, WAF automatically switches the traffic to other running WAF instances to ensure continuous protection.	2

Step 8 Confirm the product details and click **Buy Now** in the lower right corner of the page.

NOTE

If you want to use the content moderation check service, click **Buy Now** to go to the purchase page.

Step 9 Check the order details and read the *Huawei Cloud WAF Disclaimer*. Then, check the box next to "I have read and agree to WAF Disclaimer" and click **Pay Now**.

Step 10 On the payment page, select a payment method and pay for your order.

Step 11 After the payment is successful, click **Back to Dedicated Engine List**. On the **Dedicated Engine** page, view the instance status.

- After you purchase a dedicated WAF instance, WAF automatically creates a dedicated engine for you. It takes about 5 minutes to create a dedicated WAF instance. If the instance is in the **Running** status, the instance has been created successfully.

  The billing starts after the instance is created.
- You can choose **Instance Management** > **Dedicated Engine** in the navigation pane on the left and manage instances you have. You can view the instance information, view the instance monitoring information, upgrade the instance version, and delete an instance. For details, see **Managing Dedicated WAF Engines**.

----End

Follow-up Operations

1. **Connecting a Website to WAF**: Connect a website domain name or IP address to your dedicated WAF instances.
2. **Viewing Protection Events**: After a domain name or IP address is connected to WAF, by default, WAF enables **General Check** in **Basic Web Protection**, with **Protective Action** set to **Log only** and **Protection Level** to medium, and enables **Scanner** in **Anti-Crawler**, with **Protective Action** set to **Log only**. You can view and handle protection events on the **Events** page.
3. **Configuring Protection Policies**: If default protection rules cannot meet your website security requirements, you can configure custom protection rules.
4. **Querying a Protection Event**: View website protection details.

Authorizing WAF to Access Data in the VPC Your Website Resides

If you expect to use a dedicated WAF instance, authorize WAF to directly access data in the VPC by enabling certain security rules.

By purchasing a WAF dedicated instance, you agree to authorize WAF to enable such security rules. Currently, the security group rules listed in **Table 2-2** will be automatically enabled for a dedicated WAF instance.

Table 2-2 Security group rules for WAF to access the VPC your website resides

Protocol & Port	Type	Source Address	Description
Inbound rules			
TCP: 22	**IPv4**	100.64.0.0/10	WAF remote O&M
Outbound rules			
TCP: 9011	IPv4	100.125.0.0/16	WAF event logs reporting

Protocol & Port	Type	Source Address	Description
TCP: 9012	IPv4	100.125.0.0/16	WAF event logs reporting
TCP: 9013	IPv4	100.125.0.0/16	WAF event logs reporting
TCP: 9018	IPv4	100.125.0.0/16	WAF policy synchronization
TCP: 9019	IPv4	100.125.0.0/16	WAF heartbeat logs reporting
TCP: 4505	IPv4	100.125.0.0/16	WAF policy synchronization
TCP: 4506	IPv4	100.125.0.0/16	WAF policy synchronization
TCP: 50051	IPv4	100.125.0.0/16	WAF performance logs reporting
TCP: 443	IPv4	100.125.0.0/16	WAF policy synchronization

3 Connecting a Website to WAF

3.1 Website Connection Overview

To use Web Application Firewall (WAF) to protect your web services, the services must be connected to WAF. WAF provides three access modes for you to connect web services to WAF: cloud CNAME, cloud load balancer, and dedicated access modes. You can select a proper access method based on how your web services are deployed. This topic describes how WAF works in different access modes, their differences, and when to use them.

NOTE

Dedicated WAF instances are not available in some regions. For details, see **Notice on Web Application Firewall (Dedicated Mode) Discontinued**.

Application Scenarios

WAF provides the following access modes for you to connect websites to WAF.

- Cloud mode - CNAME access mode
  - Service servers are deployed on any cloud or in on-premises data centers.
  - Protected objects: domain names
  - **Connecting a Website to WAF (Cloud Mode - CNAME Access)**
- Cloud mode - Load balancer access mode
  - Service servers are deployed on Huawei Cloud.

    This mode suitable for large enterprise websites having high security requirements on service stability.
  - Protected object: domain names or IP addresses (public or private IP addresses)
  - **Connecting a Website to WAF (Cloud - ELB Load Balancer Access Mode)**
- Dedicated mode
  - Service servers are deployed on Huawei Cloud.

    This mode is suitable for large enterprise websites that have a large service scale and have customized security requirements.

  - Protected object: domain names or IP addresses (public or private IP addresses)
  - **Connecting a Website to WAF (Dedicated Mode)**

Constraints

There are some restrictions on using different access modes.

Cloud Mode - CNAME Access

When you connect your website to WAF in cloud CNAME access mode, pay attention to the following restrictions.

Constraint	Description
Domain name	• A domain name can only be added to WAF once in cloud mode. Each combination of a domain name and a non-standard port is counted towards the domain name quota of the WAF edition you are using. For example, www.example.com:8080 and www.example.com:8081 use two domain names of the quota. If you want to protect web services over multiple ports with the same domain name, add the domain name and each port to WAF. • Only the domain names that have been registered with Internet Content Provider (ICP) licenses can be added to WAF.
Service edition	• Only the professional and enterprise editions support IPv6 protection, HTTP2, and load balancing algorithms. • If you are using WAF standard edition, only **System-generated policy** can be selected for **Policy**.
Certificate	• Only .pem certificates can be used in WAF. • Currently, certificates purchased in Huawei Cloud SCM can be pushed only to the **default** enterprise project. For other enterprise projects, SSL certificates pushed by SCM cannot be used. • Only accounts with the **SCM Administrator** and **SCM FullAccess** permissions can select SCM certificates.
WebSocket protocol	WAF supports the WebSocket protocol, which is enabled by default.
HTTP/2	HTTP/2 can be used only for access between the client and WAF on the condition that at least one origin server has **HTTPS** used for **Client Protocol**. • To make **Server Configuration** works, there must be at least one server configuration record with **Client Protocol** set to **HTTPS**. • HTTP/2 can work only when the client supports TLS 1.2 or earlier versions.

Constraint	Description
Limitation	After your website is connected to WAF, you can upload a file no larger than 1 GB each time.

Cloud Mode - Load Balancer Access

When you connect your website to WAF in cloud load balancer access mode, pay attention to the following restrictions.

- Only dedicated ELB load balancers with **Specifications** set to **Application load balancing (HTTP/HTTPS)** can be used. Dedicated load balancers with **Specifications** set to **Network load balancing (TCP/UDP)** are not supported.
- Only the professional and enterprise editions allow you to specify a custom policy for **Policy**.
- Limitation: After your website is connected to WAF, you can upload a file no larger than 10 GB each time.

Dedicated Mode

When you connect your website to WAF in dedicated mode, the restrictions are as follows:

Constraint	Description
ELB load balancer	Only dedicated ELB load balancers can be used for dedicated WAF instances. For details, see **Load Balancer Types**. **NOTE** Dedicated WAF instances issued before April 2023 cannot be used with dedicated network load balancers. If you use a dedicated network load balancer (TCP/UDP), ensure that your dedicated WAF instance has been upgraded to the latest version (issued after April 2023). For details, see **Dedicated Engine Version Iteration**.
Domain name	• The wildcard domain name * can be added to WAF. When the domain name is set to *, only non-standard ports except 80 and 443 can be protected. • A protected object can only be added to WAF once. Each combination of a domain name and a non-standard port is counted towards the domain name quota of the WAF edition you are using. For example, www.example.com:8080 and www.example.com:8081 use two domain names of the quota. If you want to protect web services over multiple ports with the same domain name, add the domain name and each port to WAF.

Constraint	Description
Proxy	If a layer-7 proxy server, such as CDN or cloud acceleration, is used before WAF, you need to select **Yes** for **Use Layer-7 Proxy**. By doing this, WAF can obtain real client access IP addresses from the configured header field. For details, see **Configuring a Traffic Identifier for a Known Attack Source**.
Certificate	• Only .pem certificates can be used in WAF. • Currently, certificates purchased in Huawei Cloud SCM can be pushed only to the **default** enterprise project. For other enterprise projects, SSL certificates pushed by SCM cannot be used. • Only accounts with the **SCM Administrator** and **SCM FullAccess** permissions can select SCM certificates.
WebSocket protocol	WAF supports the WebSocket protocol, which is enabled by default.
Limitation	After your website is connected to WAF, you can upload a file no larger than 10 GB each time.

Processes of Connecting a Website to WAF

The process of connecting a website to WAF varied depending on the access mode you select.

Cloud Mode - CNAME Access

When connecting a website to WAF in CNAME access mode, refer to the process shown in **Figure 3-1**.

Figure 3-1 Process of connecting a website to WAF - Cloud Mode (CNAME Access)

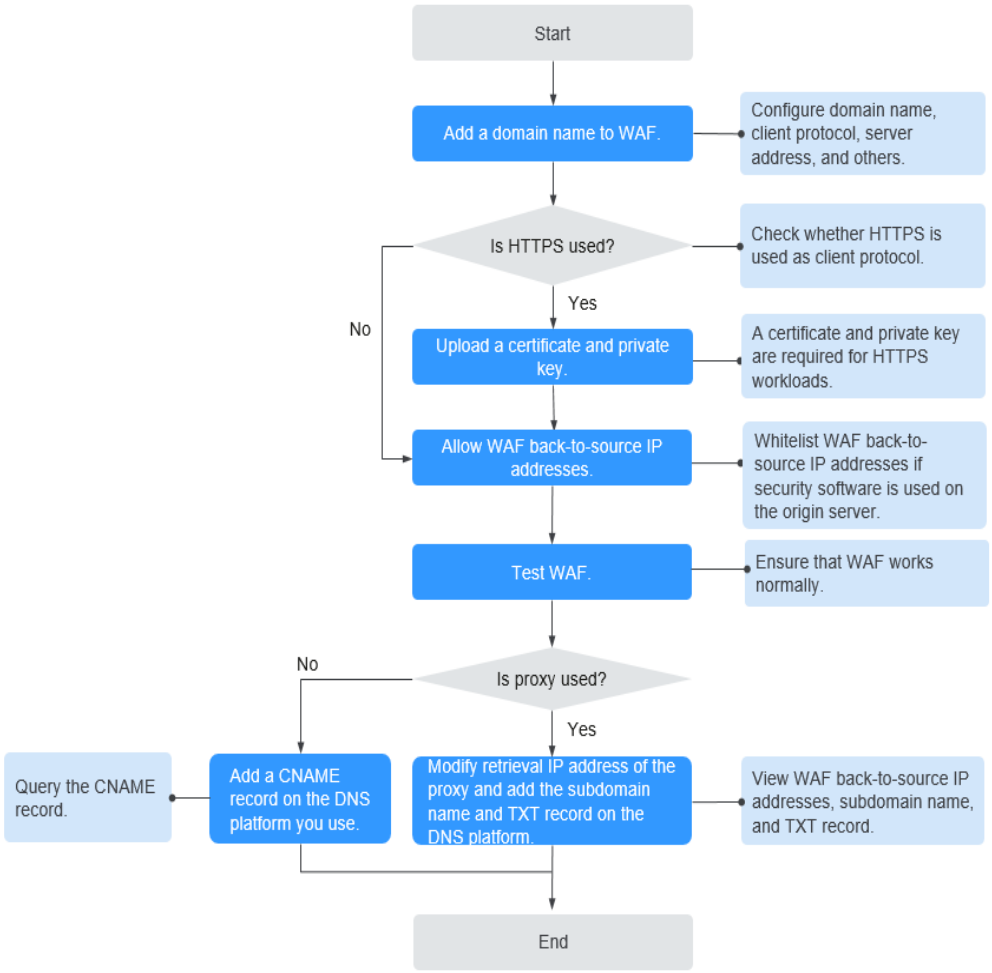


Table 3-1 Process of connecting your website domain name to WAF

Procedure	Description
Adding a Domain Name to WAF	Configure basic information, such as the domain name, protocol, and origin server.
Whitelisting WAF back-to-source IP addresses	If other security software or firewalls are installed on your origin server, whitelist only requests from WAF. This ensures normal access and protects the origin server from hacking.
Testing WAF	To ensure that your WAF instance forwards website traffic normally, test the WAF instance locally and then route traffic destined for the website domain name to WAF by modifying DNS record.

Procedure	Description
Modifying DNS Records for a Domain Name	• No proxy used Configure a CNAME record for the protected domain name on the DNS platform you use. • Proxy (such as advanced anti-DDoS and CDN) used Change the back-to-source IP address of the used proxy, such as advanced anti-DDoS and CDN, to the copied CNAME record.

Cloud Mode - Load Balancer Access

Connect your website to WAF in just a few clicks. For details, see **Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)**.

Dedicated Mode

When connecting a website to WAF in dedicated mode, refer to the process shown in **Figure 3-2**.

Figure 3-2 Process of connecting a website to a dedicated WAF instance

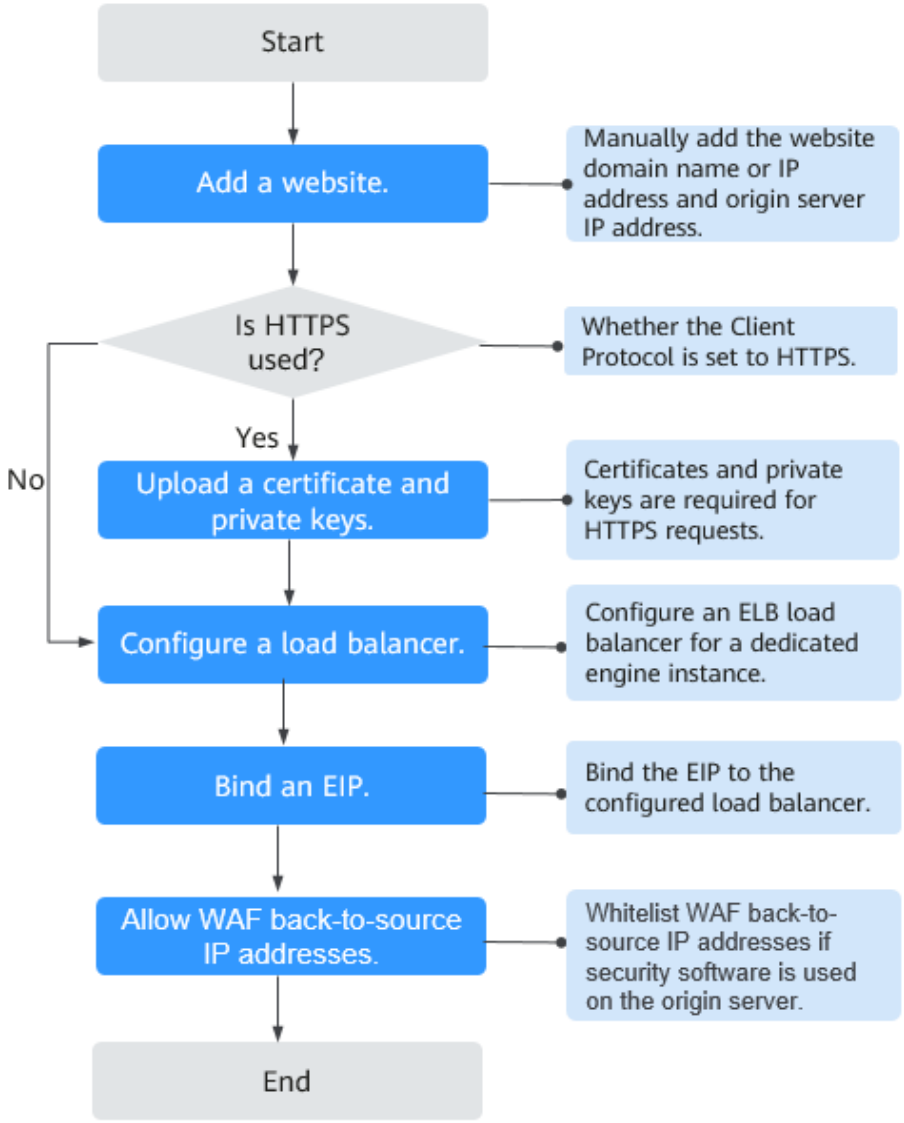


Table 3-2 Process of connecting your website domain name to WAF

Procedure	Description
Adding Your Website to WAF	You need to configure your website (domain name or IP address) details, such as protocol and origin server.
Configuring a Load Balancer for Your Dedicated WAF Instance	To ensure your dedicated WAF instance reliability, after you add a website to it, use Huawei Cloud Elastic Load Balance (ELB) to configure a load balancer and a health check for the dedicated WAF instance.

Procedure	Description
Binding an EIP to the Load Balancer	Unbind an elastic IP address (EIP) from the origin server and bind the EIP to the load balancer configured for the dedicated WAF instance. The request traffic then goes to the dedicated WAF instance for attack detection first and then go to the origin server, ensuring the security, stability, and availability of the origin server.
Allowing Back-to-Source IP Addresses of Dedicated WAF Instances on the Origin Server	The security software on the origin server may most likely regard WAF back-to-source IP addresses as malicious and block them. Once they are blocked, the origin server will deny all WAF requests. As a result, your website may become unavailable or respond very slowly. Therefore, ACL rules must be configured on the origin server to trust only the subnet IP addresses of your dedicated WAF instances.
Testing Dedicated WAF Instances	After adding a website to a dedicated WAF instance, verify that WAF can forward traffic properly and ELB load balancers work well.

3.2 Connecting Your Website to WAF (Cloud Mode - CNAME Access)

3.2.1 Connecting Your Website to WAF (Cloud Mode - CNAME Access)

No matter where your service servers are deployed, on Huawei Cloud, other clouds, or on-premises data centers, you can use WAF cloud CNAME access mode. After WAF is enabled, you need to connect your website to WAF to enable protection. In CNAME access mode, WAF works as a reverse proxy. WAF checks website traffic and forwards only normal traffic back to origin servers of your website over specific back-to-source IP addresses.

NOTE

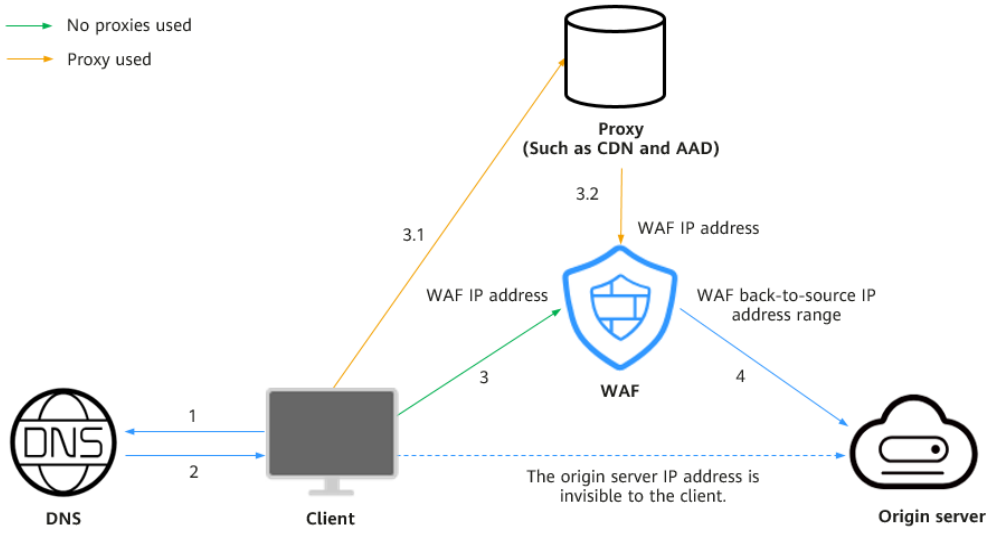
- If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and add websites to be protected in the project.
- If you use the cloud CNAME access mode, do not configure the IP address mapped to the current CNAME record as the protected domain name when configuring the DNS record. To configure a fixed access IP address, select **Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)**.

Solution Overview

In the cloud CNAME access mode, connecting a website to WAF is to point the website traffic to WAF. WAF checks received traffic and forwards only legitimate

traffic to your origin server. **Figure 3-3** shows how your website traffic is forwarded when WAF is used.

Figure 3-3 Website traffic access diagram



The details are as follows:

1. After a visitor enters a domain name in the browser, the client sends a request to the DNS service to query the domain name resolution address.
2. DNS returns the domain name resolution address to the client.
3. If no proxies (such as CDN or AAD) are used, the domain name resolution address returned by DNS is the WAF IP address. The client accesses WAF through the WAF IP address. If a proxy is used:
   a. The domain name resolution address returned by DNS is the IP address of the proxy. The client accesses the proxy through the proxy IP address.
   b. The proxy then accesses WAF over a WAF IP address.
4. WAF checks the traffic, blocks abnormal traffic, and uses WAF back-to-source IP addresses to forward normal traffic to the origin server.

Access Process

You need to perform the following operations based on whether your website uses a proxy (such as AAD, CDN, and cloud acceleration products).

Procedure	Description
Step 1. Add Your Domain Name to WAF	Add a domain name and origin server details to WAF.
Step 2: Whitelist Back-to-Source IP Addresses on Your Origin Server	Obtain and allow back-to-source IP addresses.

Procedure	Description
Step 3: Test WAF	Test website connectivity.
Step 4: Modify the DNS Records of the Domain Name	• No proxies used: Describes how to resolve website domain name to WAF CNAME record on the DNS platform. • Proxy: Describes how to change the back-to-source address of a proxy to the WAF CNAME record.
Step 5: Verify Website Access	Describes how to check whether a domain name is accessible after being connected to WAF and whether basic protection takes effect.

Prerequisites

- You have purchased a cloud WAF instance and understood details about how to connect a website to WAF.
- Make sure your domain names have Internet Content Provider (ICP) licenses, or they cannot be added to WAF.

Step 1. Add Your Domain Name to WAF

To connect your services to WAF, you need to add the domain name and origin server information to WAF.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 In the upper left corner of the website list, click **Add Website**.

Step 7 Select **Cloud Mode - CNAME** and click **Configure Now**.

Step 8 Configure the basic settings by referring to Table 3-3. Figure 3-4 shows an example.

Figure 3-4 Configuring basic information

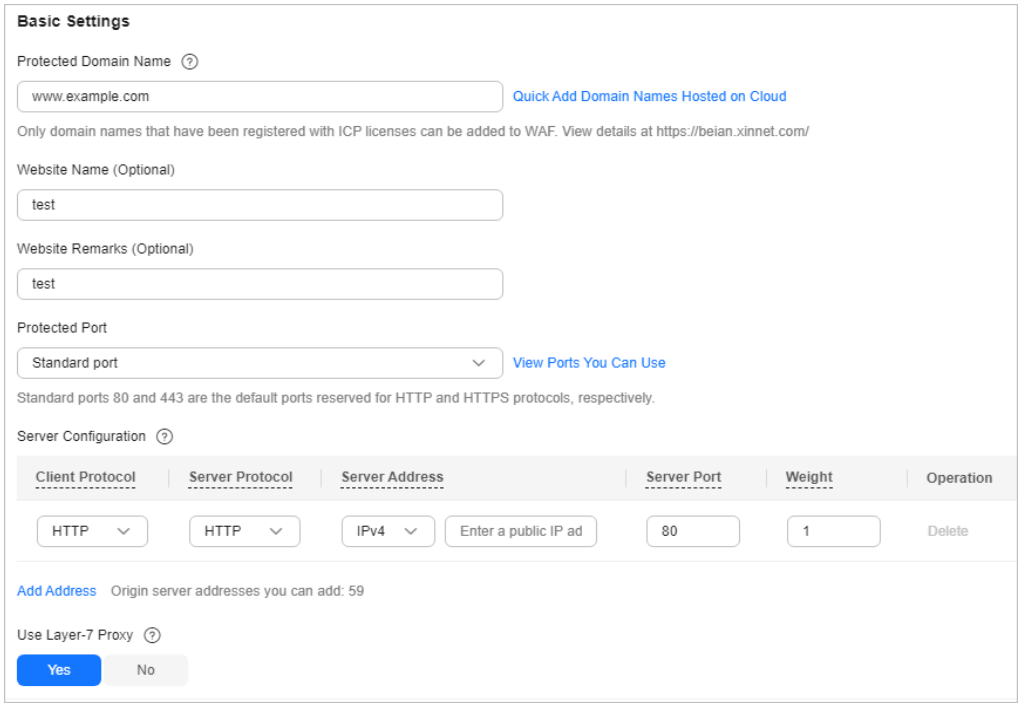


Table 3-3 Parameter description

Parameter	Description	Example Value
Domain Name	The domain name you want WAF to protect. You can enter a top-level single domain name, like example.com, a second-level domain name, like www.example.com, or a wildcard domain name, like *.example.com. **NOTICE** • The starter edition does not support adding wildcard domain names to WAF. • The following are the rules for adding wildcards to domain names: – If the server IP address of each subdomain name is the same, enter a wildcard domain name. For example, if the subdomain names ***a.example.com***, ***b.example.com***, and ***c.example.com*** have the same server IP address, you can add the wildcard domain name ****.example.com*** to WAF to protect all three. – If the server IP addresses of subdomain names are different, add subdomain names as single domain names one by one. • Each combination of a domain name and a port is counted towards the domain name quota of the WAF edition you are using. For example, **www.example.com:8080** and **www.example.com:8081** use two domain names of the quota. • Only the domain names that have been registered with Internet Content Provider (ICP) licenses can be added to WAF.	-
Website Name (Optional)	Website name you specify.	WAF
Website Remarks (Optional)	Remarks of the website.	waftest

Parameter	Description	Example Value
Protected Port	Port to be protected. • To protect port 80 or 443, select **Standard port** from the drop-down list. • To protect other ports, select the one WAF supports. Click **View Ports You Can Use** to view the HTTP and HTTPS ports supported by WAF. For more information, see **Ports Supported by WAF**. **NOTE** If a port other than 80 or 443 is configured, the visitors need to add the non-standard port to the end of the website address when they access the website. Otherwise, a 404 error will occur. If a 404 error occurs, see **How Do I Troubleshoot 404/502/504 Errors?**	81

Parameter	Description	Example Value
Server Configuration	Information about the website server, including the client protocol, server protocol, server address, weight, and server port. • **Client Protocol**: the protocol used by the client to access the server. The option can be **HTTP** or **HTTPS**. Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). HTTPS is widely used to protect privacy and integrity of data in transit and to authenticate website identities. So, if HTTPS is selected, you need to configure a certificate. If you set **Client Protocol** to **HTTPS**, **HTTP/2** can be enabled. For details, see **Enabling HTTP/2**. **NOTE** If **Standard port** is selected for **Protected Port**, by default, port 443 is protected for HTTPS, and port 80 for HTTP. • **Server Protocol**: the protocol supported by your website server. **Server Protocol**: protocol used by WAF to forward client requests. The options are **HTTP** and **HTTPS**. **NOTE** If the client protocol is different from the origin server protocol, WAF forcibly uses the origin server protocol to forward client requests. • **Server Address**: public IP address (generally corresponding to the A record of the domain name configured on the DNS) or domain name (generally corresponding to the CNAME of the domain name configured on the DNS) of the web server that a client accesses. The following IP address formats are supported: – IPv4 address, for example, XXX.XXX.1.1 – IPv6 address, for example, fe80:0000:0000:0000:0000:0000:0000:0000 **NOTICE** Only the professional and enterprise editions support IPv6 protection. • **Server Port**: service port over which the WAF instance forwards client requests to the origin server. • **Weight**: Requests are distributed across backend origin servers based on the load	**Client Protocol**: **HTTP** **Server Protocol**: **HTTP** **Server Address**: XXX.XXX.1.1 **Server Port**: **80**

Parameter	Description	Example Value
	balancing algorithm you select and the weight you assign to each server.	
Certificate	If you set **Client Protocol** to **HTTPS**, select **International** for this parameter. • If you have not created a certificate, click **Import New Certificate**. In the **Import New Certificate** dialog box, set certificate parameters. For more details, see **Uploading a Certificate**. The newly imported certificates will be listed on the **Certificates** page as well. • If a certificate has been created, select a valid certificate from the **Existing certificates** drop-down list. • If you have used a CCM certificate under the same account, you can select an SSL certificate from the drop-down list. The name of the SSL certificate you select must be the same as that in CCM. **NOTICE** • Only .pem certificates can be used in WAF. If the certificate is not in PEM format, convert it into PEM first. For details, see **How Do I Convert a Certificate into PEM Format?** • Currently, certificates purchased in Huawei Cloud SCM can be pushed only to the **default** enterprise project. For other enterprise projects, SSL certificates pushed by SCM cannot be used. • A record is automatically generated for the selected SSL certificate on the **Certificates** page. You can change the certificate name on this page, but the certificate name displayed in CCM will not be changed accordingly. • If your website certificate is about to expire, purchase a new certificate before the expiration date and update the certificate associated with the website in WAF. WAF can send notifications if a certificate expires. You can configure such notifications on the **Notifications** page. For details, see **Enabling Alarm Notifications**. • Each domain name must have a certificate associated. A wildcard domain name can only use a wildcard domain certificate. If you only have single-domain certificates, add domain names one by one in WAF.	-

Parameter	Description	Example Value
Specify **Minimum TLS Version** and **Cipher Suite**.	After selecting a certificate, you need to select the minimum TLS version and cipher suite. In WAF, the minimum TLS version configured is TLS v1.0, and the cipher suite is **Security cipher suite** by default. For more details, see **Configuring PCI DSS/3DS Compliance Check and TLS**.	Minimum TLS version: TLS v1.0 Cipher suite: **Security cipher suite**
Use Layer-7 Proxy	• **Yes**: Web proxy products for layer-7 request forwarding are used, products such as anti-DDoS, CDN, and other cloud acceleration services. • **No**: No layer-7 proxies are used. **NOTICE** • If your website uses a proxy, select **Yes**. Then WAF obtains the actual access IP address from the related field in the configured header. For details, see **Configuring a Traffic Identifier for a Known Attack Source**. • If you deploy AAD before WAF for your website, to let WAF obtain the real IP address of the client, you need to set **IP Tag** to **$remote_addr** in the **Traffic Identifier** area on the basic information page for the protected domain name. For details, see **Configuring a Traffic Identifier for a Known Attack Source**.	No proxy

Step 9 Complete advanced settings. **Figure 3-5** shows an example.

Figure 3-5 Advanced Settings

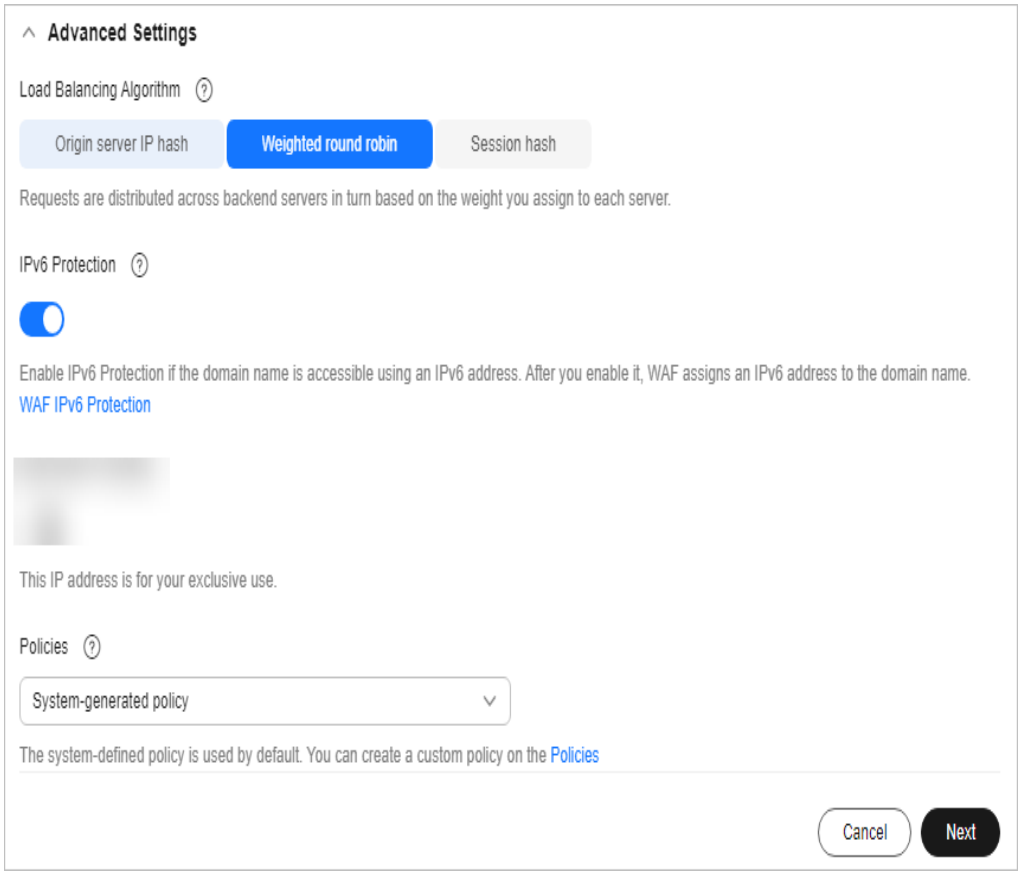


Table 3-4 Advanced settings

Parameter	Description	Example Value
Load Balancing Algorithm	If there are multiple origin server addresses, you need to select a load balancing algorithm so that traffic can be distributed across origin servers in the way you specify. • **Origin server IP hash**: Requests from the same IP address are routed to the same backend server. • Weighted round robin: All requests are distributed across origin servers in turn based on weights set to each origin server. The origin server with a larger weight receives more requests than others. • **Session hash**: Requests with the same session tag are routed to the same origin server. To enable this algorithm, **configure traffic identifiers for known attack sources**, or Session hash algorithm cannot take effect. For more details, see **Switching the Load Balancing Algorithm**.	Weighted round robin
IPv6 Protection	If the domain name is accessible using an IPv6 address, enable **IPv6 Protection**. After you enable it, WAF assigns an IPv6 address to the domain name. For more details, see **Enabling IPv6 Protection**. **NOTE** • Only the professional and enterprise editions support IPv6 protection. • If you select **IPv6** for **Server Address**, **IPv6 Protection** is enabled by default. • If you select **IPv4** for **Server Address** and enable **IPv6 Protection**, WAF will assign an IPv6 address to the domain name so that the website is accessible over the IPv6 address. In this way, requests to the IPv6 address are routed by WAF to the IPv4 address of the origin server. For details, see **How Does WAF Forward Traffic to an IPv6 Origin Server?** • If the origin server uses IPv6 addresses, IPv6 protection is enabled by default. To prevent IPv6 service from interruption, keep the IPv6 protection enabled. If IPv6 protection is not needed, edit the server configuration and delete IPv6 configuration from the origin server first. For details, see **Editing Server Information**.	Enabled

Parameter	Description	Example Value
HTTP/2	If your website needs to support HTTP/2 access, select **Use** for **HTTP/2**. HTTP/2 can be used only for access between the client and WAF on the condition that at least one origin server has **HTTPS** used for **Client Protocol**. **NOTICE** • Only the professional and enterprise editions support HTTP/2. • To make **Server Configuration** works, there must be at least one server configuration record with **Client Protocol** set to **HTTPS**. • HTTP/2 can work only when the client supports TLS 1.2 or earlier versions.	Use
Policy	Select the protection policy you want to use for the website. • **System-generated policy** (default): For details, see **Table 3-5**. If the number of added protection policies reaches the quota, this option will be grayed out. • Custom protection policy: a policy you create based on your security requirements. For more details, see **Configuring a Protection Policy**. **NOTICE** If you are using WAF standard edition, only **System-generated policy** can be selected.	System-generated policy

Table 3-5 Parameters for system-generated policies

Edition	Policy	Description
Standard	Basic web protection (**Log only** mode and common checks)	The basic web protection defends against attacks such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections.

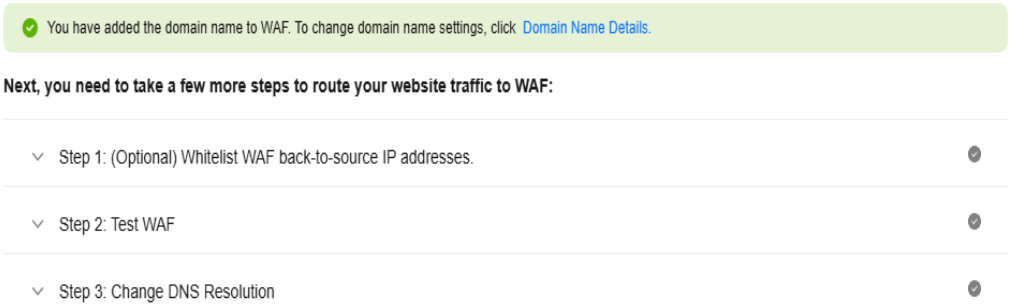
Edition	Policy	Description
Professional/Enterprise edition	Basic web protection (**Log only** mode and common checks)	The basic web protection defends against attacks such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections.
	Anti-crawler (**Log only** mode and **Scanner** feature)	WAF only logs web scanning tasks, such as vulnerability scanning and virus scanning, such as crawling behavior of OpenVAS and Nmap.

NOTE

Log only: WAF only logs detected attacks instead of blocking them.

Step 10 Click **Next** and complete the basic information about the website to be protected. Perform the following operations as prompted on the **Add Website** page:

Figure 3-6 Domain name added



1. **Whitelist WAF Back-to-Source IP Addresses on Your Origin Servers**
2. **Testing WAF**
3. **Modifying DNS Records for a Domain Name**

----End

Step 2: Whitelist Back-to-Source IP Addresses on Your Origin Server

A back-to-source IP address is a source IP address used by WAF to forward client requests to origin servers. To origin servers, all web requests come from WAF, and all source IP addresses are WAF back-to-source IP addresses. The real client IP address is encapsulated into the HTTP X-Forwarded-For (XFF) header field.

If the origin server uses other firewalls, network ACLs, security groups, or antivirus software, they are more likely to block WAF back-to-source IP address as malicious ones. So, you need to configure an access control policy on your origin server to

allow only WAF back-to-source IP addresses to access the origin server over any ports. This prevents hackers from bypassing WAF to attack origin servers.

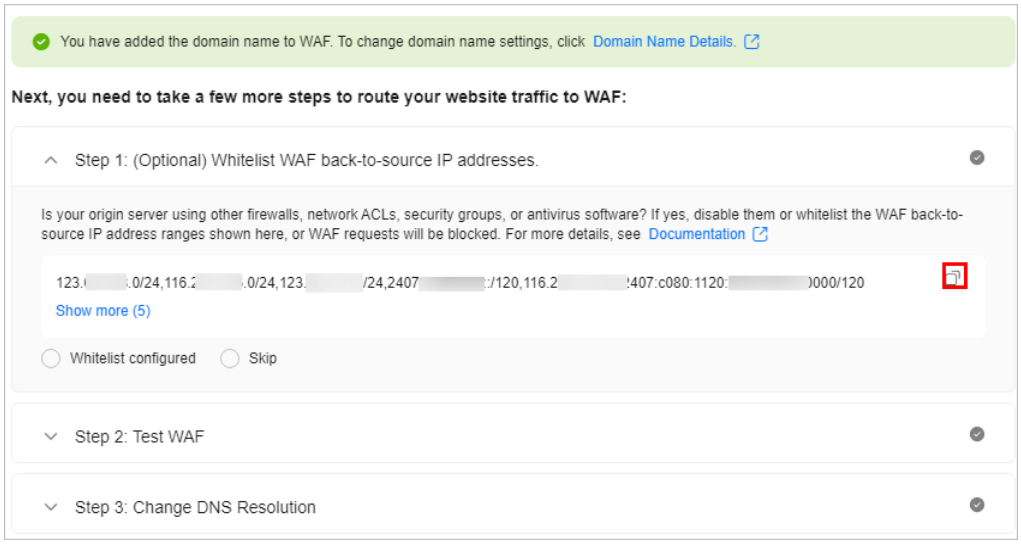
NOTE

- There will be more WAF IP addresses due to scale-out or new clusters. For your legacy domain names, WAF IP addresses usually fall into several class C IP addresses (192.0.0.0 to 223.255.255.255) of two to four clusters.
- Generally, these IP addresses do not change unless clusters in use are changed due to DR switchovers or other scheduling switchovers. Even when WAF cluster is switched over on the WAF background, WAF will check the security group configuration on the origin server to prevent service interruptions.

Step 1 Obtain WAF back-to-source IP addresses.

After **Step 1. Add Your Domain Name to WAF** is complete, expand **Step 1: (Optional) Whitelist WAF back-to-source IP addresses** and click to copy all back-to-source IP addresses. Alternatively, go to the **Website Settings** page, locate the target domain name, and click **Whitelist WAF** in the **Access Status** column. Then, click to copy all back-to-source IP addresses.

Figure 3-7 Copying the back-to-source IP addresses



Step 2 Open the security software on the origin server and add the copied IP addresses to the whitelist.

- If origin servers are deployed on ECSs, see **Whitelisting WAF Back-to-Source IP Addresses on Origin Servers That Are Deployed on ECSs**.
- If origin servers are added to backend servers of an ELB load balancer, see **Whitelisting WAF Back-to-Source IP Addresses on Origin Servers That Use Load Balancers**.
- If you also use Cloud Firewall (CFW) on Huawei Cloud, refer to **Adding a Protection Rule**.
- If your website is deployed on servers on other cloud vendors, whitelist the WAF back-to-source IP addresses in the corresponding security group and access control rules.
- If only the personal antivirus software is installed on the origin server, the software does not have the interface for whitelisting IP addresses. If the origin

server provides external web services, install the enterprise security software on or use Huawei Cloud Host Security Service (HSS) for the server. These products identify the sockets of some IP addresses with a large number of requests and occasionally disconnect the connections. Generally, the IP addresses of WAF are not blocked.

Step 3 After the preceding operations are complete, click **Finished**.

----End

Step 3: Test WAF

You can modify the hosts file on the local server, set the domain name addressing mapping (DNS resolution records that take effect only on the local computer), and point the website domain name to the WAF IP address on the local computer. In this way, you can access the protected domain name from the local computer to verify that the domain name is accessible after it has been added to WAF. This can eliminate website access exceptions caused by abnormal domain name configurations.

NOTICE

Before performing this operation, ensure that:

- The protocol, address, and port used by the origin server (for example, **www.example5.com**) are correctly configured when **adding a domain name to WAF**. If **Client Protocol** is set to **HTTPS**, ensure that the uploaded certificate and private key are correct.
- Operations in **Step 2: Whitelist Back-to-Source IP Addresses on Your Origin Server** have been finished.

Step 1 Obtain the CNAME record.

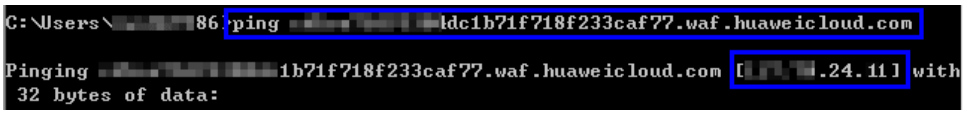
- Method 1: After **Step 2: Whitelist Back-to-Source IP Addresses on Your Origin Server** is complete, expand **Step 2: Test WAF** and copy the CNAME record on the displayed page. Alternatively, go to the **Website Settings** page, locate the target domain name, and click **Test WAF** in the **Access Status** column. On the page displayed, copy the CNAME record.
- Method 2: On the **Website Settings** page, click the target domain name. On the basic information page displayed, click in the **CNAME** row to copy the **CNAME** record.

Step 2 Ping the CNAME record and record the corresponding IP address.

Use **www.example5.com** as an example and its CNAME record is **xxxxxxxdc1b71f718f233caf77.waf.huaweicloud.com**.

Open cmd in Windows or bash in Linux and run the **ping xxxxxxxdc1b71f718f233caf77.waf.huaweicloud.com** command to obtain the WAF access IP addresses. As shown in **Figure 3-8**, the WAF access IP address is displayed.

Figure 3-8 ping cname



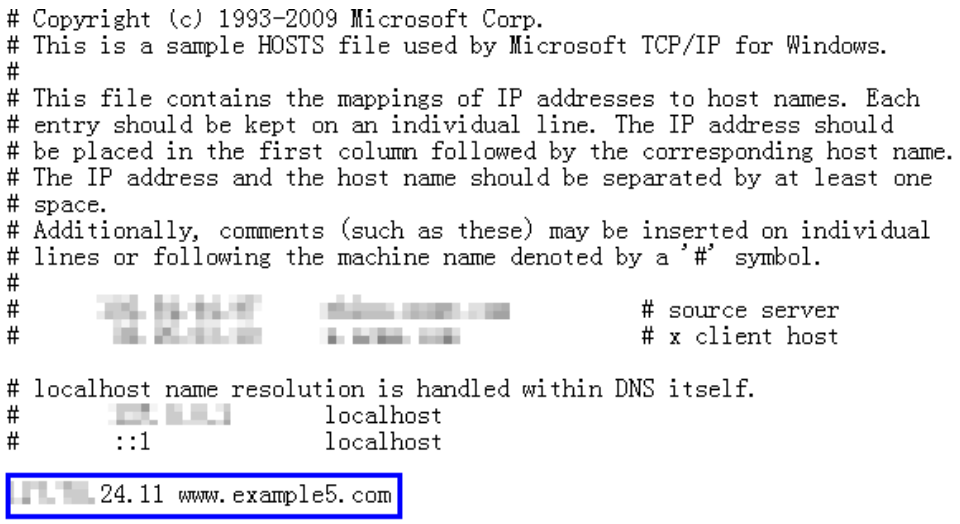
NOTE

If no WAF access IP addresses are returned after you ping the CNAME record, your network may be unstable. You can ping the CNAME record again when your network is stable.

Step 3 Add the domain name and WAF access IP addresses pointed to CNAME to the **hosts** file.

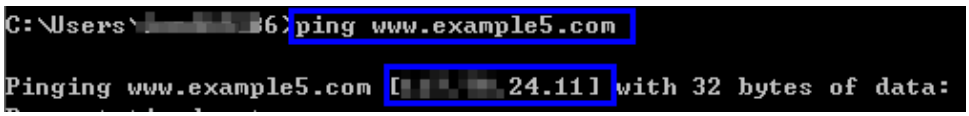
1. Use a text editor to edit the hosts file. In Windows, the location of the hosts file is as follows:
   - Windows: **C:\Windows\System32\drivers\etc**
   - Linux: **/etc/hosts**
2. Add a record like **Figure 3-9** to the **hosts** file. The IP address is the WAF access IP address obtained in **Step 2** and the domain name is the protected domain name.

   Figure 3-9 Adding a record



3. Save the **hosts** file and ping the protected domain name on the local PC.

   Figure 3-10 Pinging the domain name



   It is expected that the resolved IP address is the access IP address of WAF obtained in **Step 3.2**. If the origin server address is returned, refresh the local DNS cache. (Run **ipconfig/flushdns** in Windows cmd or **systemd-resolved** in Linux Bash.)

Step 4 Verify the access.

1. Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

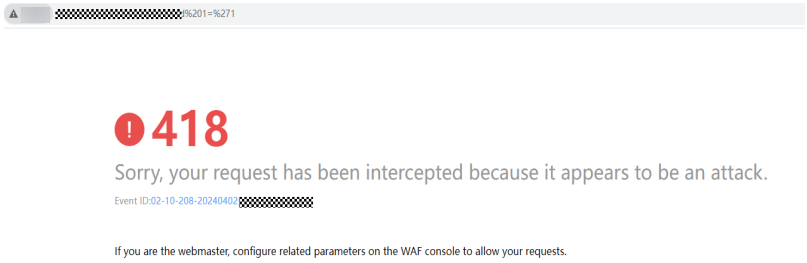
   If the domain name has been resolved to WAF back-to-source IP addresses and WAF configurations are correct, the website is accessible.

2. Simulate simple web attack commands.

   a. Set the mode of **Basic Web Protection** to **Block**. For details, see **Enabling Basic Web Protection**.

   b. Clear the browser cache, enter the test domain name in the address bar, and check whether WAF blocks the simulated SQL injection attack against the domain name.

   Figure 3-11 Request blocked

   c. In the navigation pane on the left, choose **Events** to view test data.

Step 5 Verify that the preceding steps are complete and click **Finished**.

----End

Step 4: Modify the DNS Records of the Domain Name

After a domain name is added to WAF, WAF functions as a reverse proxy between the client and server. The real IP address of the server is hidden, and only the IP address of WAF is visible to web visitors. You must point the DNS resolution of the domain name to the CNAME record provided by WAF. In this way, access requests can be resolved to WAF. After your website connectivity with WAF is tested locally, you can go to the DNS platform hosting your domain name and resolve the domain name to WAF. Then WAF protection can work.

NOTICE

Before modifying the DNS records of a domain name, ensure that:

- Operations in **Step 1. Add Your Domain Name to WAF**, **Step 2: Whitelist Back-to-Source IP Addresses on Your Origin Server**, and **Step 3: Test WAF** have been completed.
- You have the permission to modify domain name resolution settings on the DNS platform hosting your domain name.

No proxies used

Step 1 Obtain the CNAME record of WAF.

- Method 1: After **Step 3: Test WAF** is complete, expand **Step 3: Change DNS Resolution**, and copy the CNAME record on the displayed page. Alternatively, go to the **Website Settings** page, locate the target domain name, and click **Modify DNS** in the **Access Status** column. Then, copy the CNAME record on the page displayed.
- Method 2: On the **Website Settings** page, click the target domain name. On the basic information page displayed, click in the **CNAME** row to copy the **CNAME** record.

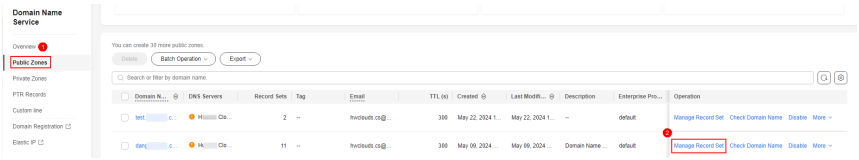
Step 2 Change the DNS records of the domain name to the WAF CNAME record.

Configure the CNAME record at your DNS provider. For details, contact your DNS provider.

The following uses Huawei Cloud DNS as an example to show how to configure a CNAME record. If the following configuration is inconsistent with your configuration, use information provided by the DNS providers.

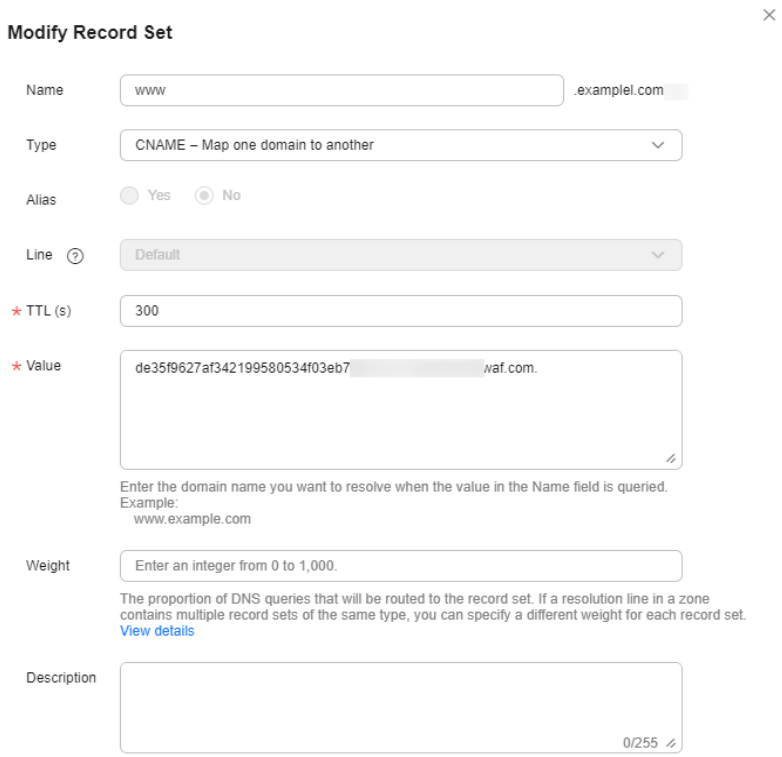
1. Click in the upper left corner of the page and choose **Networking** > **Domain Name Service**.
2. In the navigation pane on the left, choose **Public Zones**.
3. In the **Operation** column of the target domain name, click **Manage Record Set**. The **Record Sets** tab page is displayed.

Figure 3-12 Record sets



4. In the row containing the desired record set, click **Modify** in the **Operation** column.
5. In the displayed **Modify Record Set** dialog box, change the record value.
   - **Name**: Domain name configured in WAF
   - **Type**: Select **CNAME-Map one domain to another**.
   - **Line**: Select **Default**.
   - **TTL (s)**: The recommended value is **5 min**. A larger TTL value will make it slower for synchronization and update of DNS records.
   - **Value**: Change it to the WAF CNAME record copied from WAF.
   - Keep other settings unchanged.

Figure 3-13 Modify Record Set



NOTE

About modifying the resolution record:

- The CNAME record must be unique for the same host record. You need to change the existing CNAME record of your domain name to WAF CNAME record.
- Record sets of different types in the same zone may conflict with each other. For example, for the same host record, the CNAME record conflicts with other records such as A record, MX record, and TXT record. If the record type cannot be directly changed, you can delete the conflicting records and add a CNAME record. Deleting other records and adding a CNAME record should be completed in as short time as possible. If no CNAME record is added after the A record is deleted, domain resolution may fail.

For details about the restrictions on domain name resolution types, see **Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?**

6. Click **OK**.

----End

Proxy used

Step 1 Obtain the WAF CNAME record.

- Method 1: After **Step 3: Test WAF** is complete, click **Step 3: Change the back-to-source IP address of the proxy.**. On the displayed page, copy the CNAME record. Alternatively, go to the **Website Settings** page, click **Change Proxy IP Address** in the **Access Status** column, and copy the CNAME record on the displayed page.

- Method 2: On the **Website Settings** page, click the target domain name. On the basic information page displayed, click in the **CNAME** row to copy the **CNAME** record.

Step 2 Make sure the domain name has been pointed to the proxy and change the back-to-source IP address of the used proxy, such as anti-DDoS and CDN services, to the copied CNAME record.

NOTE

If proxies are used, WAF checks TXT records to **identify the domain name access status**. You are advised to add a subdomain name and TXT record on your DNS service provider.

1. Obtain the subdomain name and TXT record: On the top of the domain name basic information page, click next to **Inaccessible**. In the dialog box displayed, copy the subdomain name and TXT record.
2. Add **Subdomain Name** at the DNS provider and configure **TXT Record** for the subdomain name. For details about the configuration method, see **What Are Impacts If No Subdomain Name and TXT Record Are Configured?**

WAF determines which user owns the domain name based on the configured **Subdomain Name** and **TXT Record**.

----End

Configuration verification

After completing the preceding configurations, you need to check the CNAME record of the domain name.

Step 1 In Windows, choose **Start** > **Run**. Then enter **cmd** and press **Enter**.

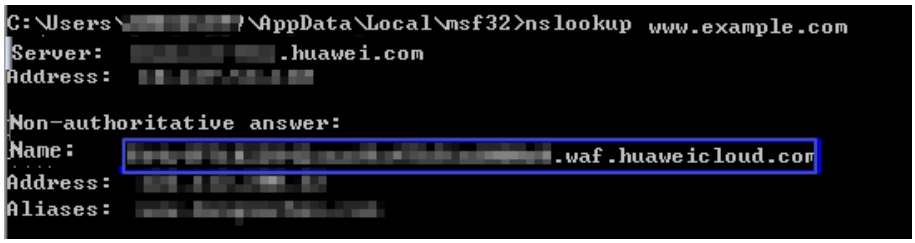
Step 2 Run a **nslookup** command to query the CNAME record.

If the configured CNAME record is returned, the configuration is successful. An example command response is displayed in **Figure 3-14**.

Using www.example.com as an example, the output is as follows:

```
nslookup www.example.com
```

Figure 3-14 Querying the CNAME



Step 3 After the preceding steps are complete, select **Finished**.

----End

Step 5: Verify Website Access

- Checking the access status

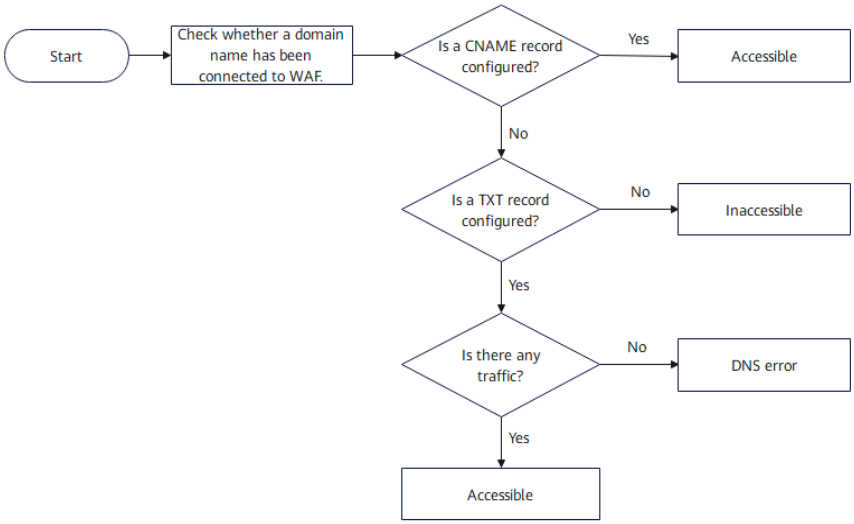
  After the preceding configurations are complete, WAF automatically checks the access status of new or updated domain names every 30 minutes based

on the following conditions: If the domain name was created more than two weeks ago and has not been modified in the past two weeks, you can click in the **Access Status** column to manually refresh the access status.

- Check whether a CNAME record or TXT record is configured for the website domain name if proxies are used.
- Check whether the website has traffic. There are at least 20 requests to the website within 5 minutes, or no traffic can be detected.

Figure 3-15 shows the logic for checking the access status.

Figure 3-15 Access status check logic



Access status description:

- **Inaccessible**: No CNAME or TXT record has been configured for the domain name, and no traffic passes through the domain name. You can allow the back-to-source IP addresses, test WAF, or modify the DNS resolution based on the access status. If the domain name is still **Inaccessible** after you manually refresh the access status, connect the domain name to WAF again by referring to **Why Is My Domain Name or IP Address Inaccessible?**
- **Accessible**: The domain name has been connected to WAF. A CNAME record or a TXT record has been configured for the domain name, and the website has traffic.
- **DNS error**: The website domain name has a TXT record, but the website does not have traffic. You can access the website more than 20 times within 5 minutes, manually refresh the access status, and check whether the access status is updated to **Accessible**.

- Protection Verification

  Simulate simple web attack commands and check whether WAF protection takes effect.

Follow-up Operations

1. (Optional) **Recommended Configurations After Website Connection**: After a domain name is connected to WAF, you need to configure security settings as required.
2. **Configuring Protection Policies**: If default protection rules cannot meet your website security requirements, you can configure custom protection rules.
3. **Querying a Protection Event**: View website protection details.

FAQs

- **What Can I Do If the Message "Illegal server address" Is Displayed When I Add a Domain Name?**
- **Why Am I Seeing the "Someone else has already added this domain name. Please confirm that the domain name belongs to you" Error Message?**
- **Why Cannot I Select an SCM Certificate When Adding a Domain Name to WAF?**
- **How Do I Troubleshoot 404/502/504 Errors?**
- **Why Does the Requested Page Respond Slowly After My Website Is Connected to WAF?**
- **What Can I Do If Files Cannot Be Uploaded After a Website Is Connected to WAF?**
- **Why Cannot the Protection Mode Be Enabled After a Domain Name Is Connected to WAF?**

3.2.2 Example Configuration

When adding a domain name to WAF, the configurations are slightly different based on the service scenarios.

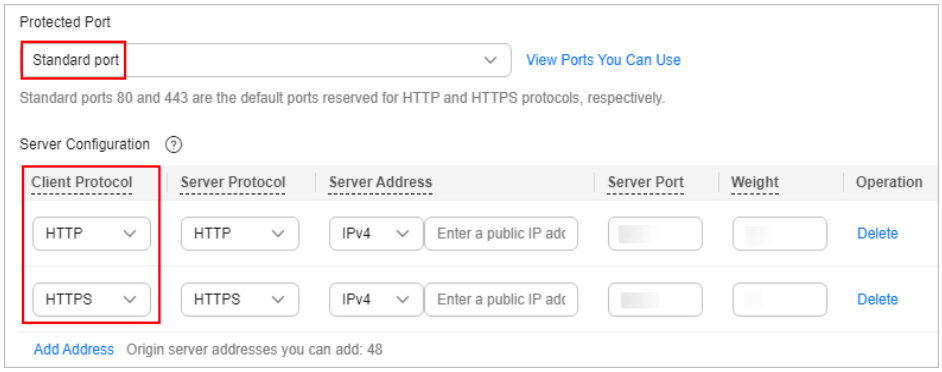
- **Example 1: Configuring Service Protection for Port 80/443**
- **Example 2: Forwarding Client Requests to Different Origin Servers**
- **Example 3: Protection for One Domain Name with Different Protected Ports**
- **Example 4: Configuring Protocols for Different Access Methods**

Example 1: Configuring Service Protection for Port 80/443

Configuration scenario: Protection for web services over port 80 or 443

1. **Protected Port**: Select **Standard port**.
2. **Client Protocol**
   - Protection for port 80: Select **HTTP**.
   - Protection for port 443: Select **HTTPS**.
   - Protection for both ports 80 and 443: Configure two pieces of server information and set **Client Protocol** to **HTTP** and **HTTPS**, respectively, as shown in **Figure 3-16**.

Figure 3-16 Protection for both ports 80 and 443



NOTE

- In **Figure 3-16**, the parameter settings in the red box are fixed. Set other parameters based on site requirements.
- In this case, your website visitors can access the website without adding a port to the end of the domain name. For example, they can enter **http://www.example.com** in the address box of the browser to access the website.

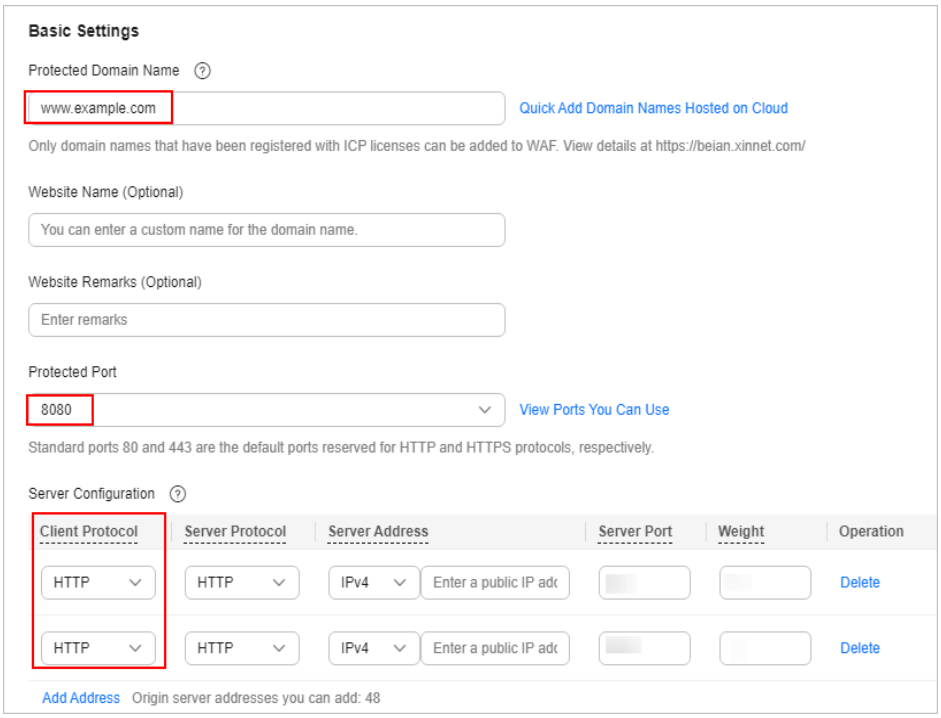
Example 2: Forwarding Client Requests to Different Origin Servers

Configuration scenario: Using WAF to distribute client requests for the same protected object across different origin servers.

For example, you want to add domain name www.example.com and port 8080 to WAF, and want to let WAF forward client requests to two backend servers.

1. **Domain Name**: www.example.com
2. **Protected Port**: 8080
3. **Client Protocol**: WAF auto-fills the client protocol based on the protected port you select. Only HTTP supports port 8080. So, **Client Protocol** must be to **HTTP** for the two pieces of origin server information. **Figure 3-17** shows an example.

Figure 3-17 Forwarding client requests to different origin servers



NOTE

- In **Figure 3-17**, the parameter settings in the red box are fixed. Set other parameters based on site requirements.
- In this scenario, visitors need to add a port number to the end of the domain name when they try to access the website. Otherwise, error 404 will be reported. For example, they need to enter **http://www.example.com:8080** in the address box of the browser to access the website.

Example 3: Protection for One Domain Name with Different Protected Ports

Each combination of a domain name and a non-standard port is counted towards the domain name quota of the WAF edition you are using. For example, www.example.com:8080 and www.example.com:8081 use two domain names of the quota. If you want to protect web services over multiple ports with the same domain name, add the domain name and each port to WAF.

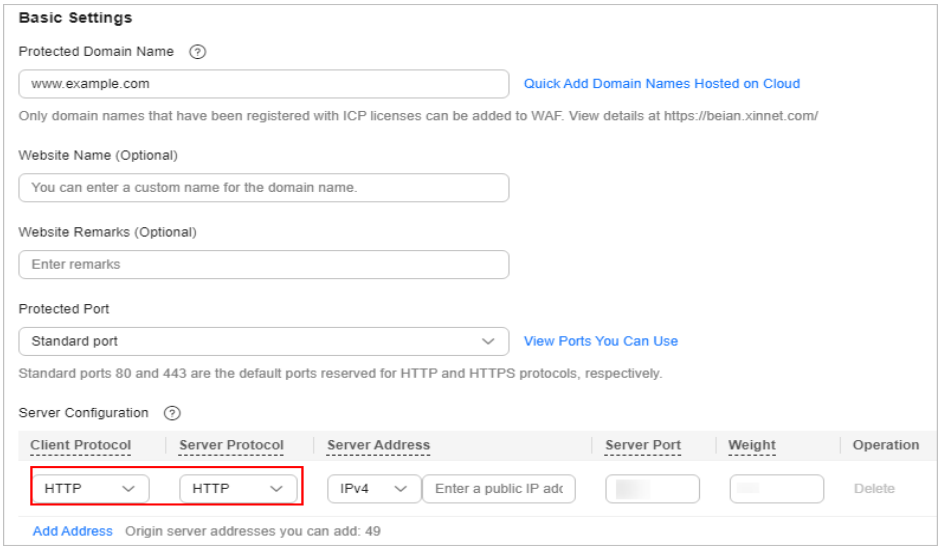
Example 4: Configuring Protocols for Different Access Methods

WAF provides flexible combinations of protocol configurations. If your website is www.example.com, WAF provides the following four access modes:

- In HTTP forwarding mode, set both **Client Protocol** and **Server Protocol** to **HTTP**, as shown in **Figure 3-18**.

  In this scenario, the client accesses the website over HTTP, and WAF forwards requests to the origin server over HTTP. So, this mode is suitable when encrypted transmission is not required.

Figure 3-18 HTTP forwarding



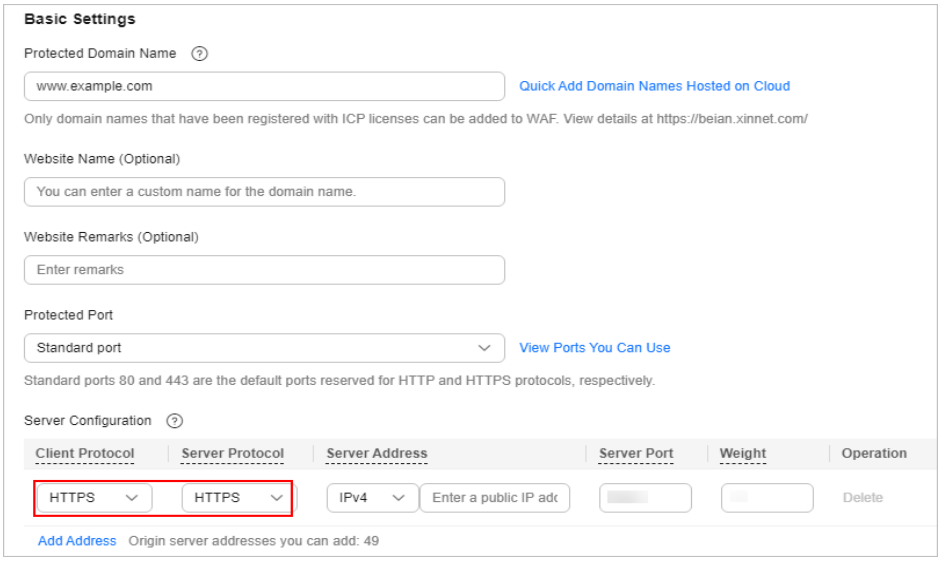
NOTICE

- In **Figure 3-18**, the parameter settings in the red box are fixed. Set other parameters based on site requirements.
- This configuration allows web visitors to access the website over HTTP only. If they access it over HTTPS, they will receive the 302 Found code and be redirected to http://www.example.com.

- In HTTPS forwarding, HTTPS is set to **Client Protocol** and **Server Protocol**, as shown in **Figure 3-19**. This configuration allows web visitors to access your website over HTTPS only. If they access over HTTP, they are redirected to https://www.example.com.

  In this scenario, the client accesses the website over HTTPS, and WAF forwards requests to the origin server over HTTPS as well. So, this mode is suitable when encrypted transmission is required.

Figure 3-19 HTTPS redirection



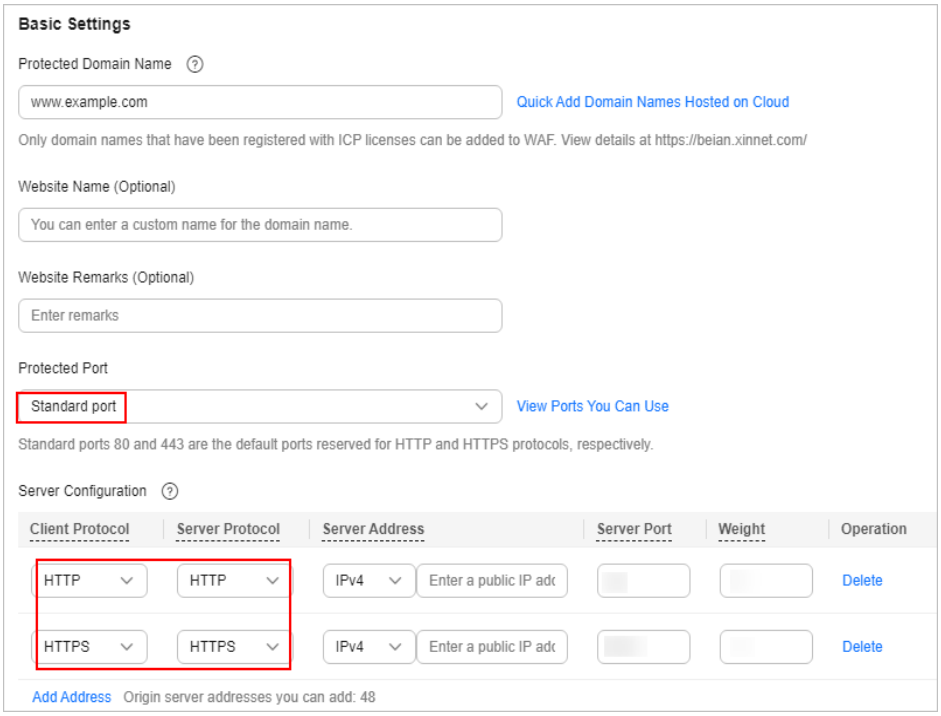
NOTICE

- In **Figure 3-19**, the parameter settings in the red box are fixed. Set other parameters based on site requirements.
- If visitors access your website over HTTPS, the website returns a successful response.
- If visitors access your website over HTTP, they will receive the 301 Found code and are directed to https://www.example.com.

- In HTTP and HTTPS forwarding, configure two pieces of server configurations, one with **Client Protocol** and **Server Protocol** set to **HTTP**, and the other with **Client Protocol** and **Server Protocol** set to **HTTPS**, as shown in **Figure 3-20**.

  This configuration applies only to protection for standard ports 80 and 443.

Figure 3-20 HTTP and HTTPS forwarding



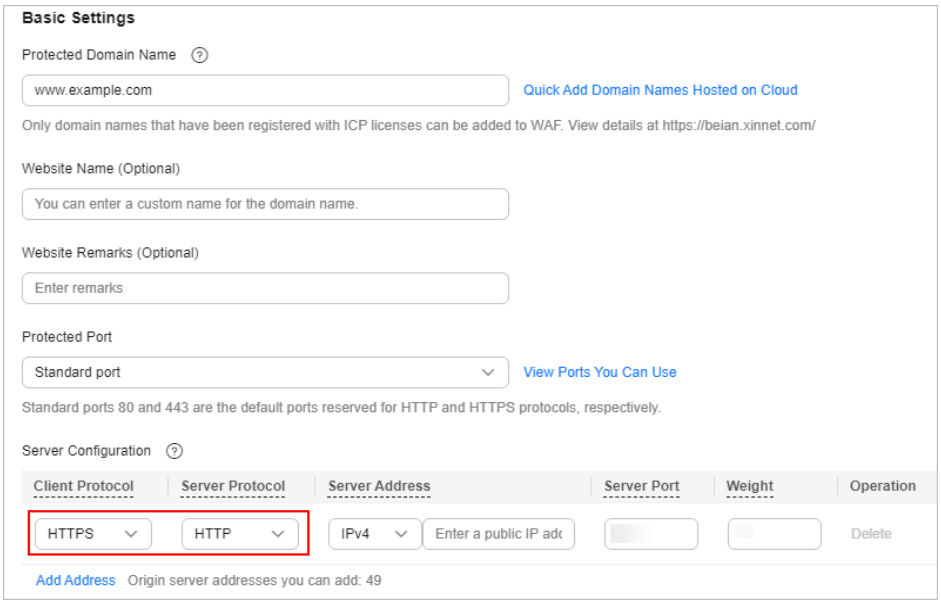
NOTICE

- In **Figure 3-20**, the parameter settings in the red box are fixed. Set other parameters based on site requirements.
- If visitors access your website over HTTP, the website returns a successful response. Communications between the browser and website are not encrypted.
- If visitors access your website over HTTPS, the website returns a successful response and all communications between the browser and website are encrypted.

- If you want to use WAF for HTTPS offloading, select **HTTPS** for **Client Protocol** and **HTTP** for **Server Protocol**, as shown in **Figure 3-21**.

  In this scenario, when a client accesses a website, HTTPS is used for encrypted transmission, and WAF uses HTTP to forward requests to the origin server.

Figure 3-21 HTTPS offloading



NOTICE

- In **Figure 3-21**, the parameter settings in the red box are fixed. Set other parameters based on site requirements.
- If visitors access your website over HTTPS, WAF forwards the requests to your origin server over HTTP.

3.3 Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)

If your service servers are deployed on Huawei Cloud, you can connect your web services to your WAF instance in cloud load balancer access mode.

You can select **Cloud Mode - Load balancer** when connecting a website to WAF only when the website has used a dedicated load balancer to forward traffic. In this mode, WAF works in out-of-path mode and does not forward traffic. Before using this mode, configure a dedicated load balancer first. .

NOTE

If you have enabled enterprise projects, you can select an enterprise project from the **Enterprise Project** drop-down list and add websites to be protected in the project.

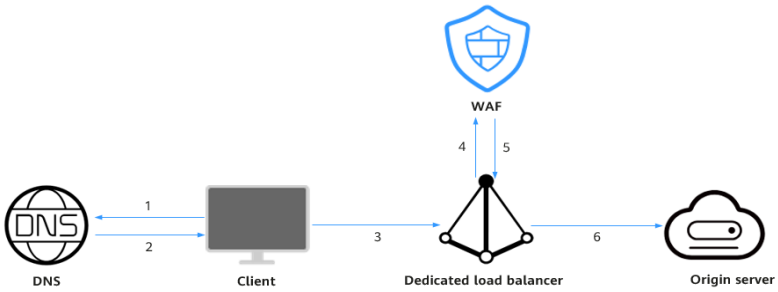
Solution Overview

In cloud load balancer access mode, WAF is integrated into the load balancer gateway through an SDK modular. After your website is connected to WAF, the ELB load balancer mirrors the website traffic to WAF. WAF checks the mirrored traffic and synchronizes the check result to the load balancer. The load balancer determines whether to forward client requests to the origin server based on the

check result it receives. In this method, WAF does not forward traffic. This eliminates compatibility and stability issues that might be caused by additional-layer of traffic forwarding.

Figure 3-22 shows the request forwarding process after a domain name is connected to WAF.

Figure 3-22 Website access diagram



The traffic forwarding details are as follows:

1. After a visitor enters a domain name in the browser, the client sends a request to the DNS service to query the domain name resolution address.
2. DNS returns the domain name resolution address to the client.
3. The client accesses the ELB load balancer over its EIP.
4. The ELB load balancer mirrors traffic to WAF.
5. WAF checks the traffic and synchronizes the check result to the ELB load balancer.
6. The ELB load balancer determines whether to forward traffic to the origin server based on check result WAF sends to it.

Prerequisites

- You have **purchased a cloud WAF instance** and understood details about **how to connect a website to WAF**.

  NOTE

  - To use cloud load balancer WAF, you need to **submit a service ticket** to enable it for you first. Cloud load balancer WAF is available in some regions. For details, see **Functions**.
  - If you want to use the load balancer access mode, make sure you are using standard, professional, or enterprise cloud WAF. When you are using cloud WAF, the quotas for the domain name, QPS, and rule extension packages are shared between the load balancer access and CNAME access modes.

- You have purchased a dedicated load balancer with **Specifications** set to **Application load balancing (HTTP/HTTPS)**. For more details, see **Creating a Dedicated Load Balancer**. Note that you should use the same account to buy the load balancer and dedicated WAF.

Connecting Your Website to WAF (Cloud Mode - Load balancer Access Mode)

Step 1 Create a dedicated load balancer.

- **Specifications**: Select **Application load balancing (HTTP/HTTPS)** .
- Set other parameters based on your service requirements.

Step 2 Add a listener to the load balancer created in **Step 1**. For details, see **Adding an HTTP Listener** or **Adding an HTTPS Listener**.

Step 3 Create a backend server group.

- **Load Balancer**: Select **Associate existing** and select the load balancer created in **Step 1** from the drop-down list.
- Configure the server address of the website you plan to add to WAF in **Step 5** as backend server.

Step 4 Run the following command to check the service connectivity:

curl -kv -H "Host: {Origin server domain name}" {protocol of the listener}://{IP address of the ELB load balancer}:{port of the listener}

If status code **200** is returned, the service has been connected.

Step 5 Configure the websites for which you want WAF to check the traffic.

1. Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.
2. In the navigation pane on the left, choose **Website Settings**.
3. In the upper left corner of the website list, click **Add Website**.
4. Select **Cloud Mode - Load balancer** and click **Configure Now**.
5. On the displayed page, configure basic settings by referring to **Table 3-6**. **Figure 3-23** shows an example.

Figure 3-23 Configuring basic settings of a website

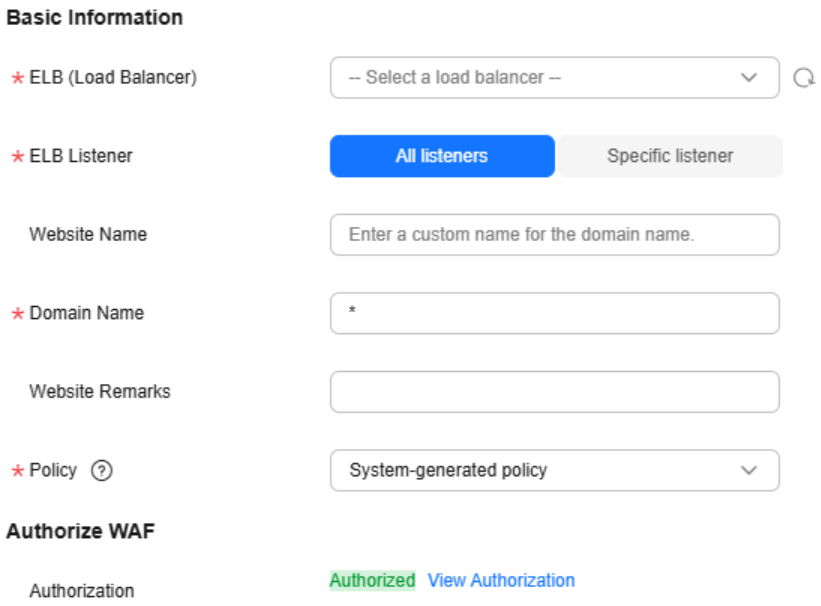


Table 3-6 Parameter description

Parameter	Description	Example Value
ELB (Load Balancer)	Select the load balancer created in **Step 1** and ensure that the server address of the protected website has been added to the load balancer. **NOTE** You can check the ID of the account that the load balancer belongs to. This function is under open beta test (OBT). You can **submit a service ticket** to enable it. If you enable this function, you can click the **ELB (Load Balancer)** drop-down list and move the cursor to the ELB (load balancer) to view its details, including the instance name, ID, number of listeners, account ID, and project ID.	elb-waf-test
ELB Listener	Select the listener configured for the ELB load balancer. You can select an ELB listener of another account. – **All listeners** – **Specific listener**	All listeners
Website Name	(Optional) You can specify a name for your website.	None

Parameter	Description	Example Value
Domain Name	Set this parameter to the domain name or IP address (public or private IP address) you want to protect. Make sure that the domain name has been resolved to the EIP of the load balancer created in **Step 1**. Domain name: Single domain names or wildcard domain names are supported. – Single domain name: Enter a single domain name, for example, www.example.com. – Wildcard domain name ▪ If the server IP address of each subdomain name is the same, enter a wildcard domain name. For example, if the subdomain names ***a.example.com***, ***b.example.com***, and ***c.example.com*** have the same server IP address, you can add the wildcard domain name ****.example.com*** to WAF to protect all three. ▪ If the server IP addresses of subdomain names are different, add subdomain names as single domain names one by one. ▪ A WAF instance with ELB load balancer access mode supports only one wildcard domain name. ▪ Wildcard domain name ***** can be added. **NOTE** WAF can protect both public and private IP addresses. If a private IP address is used, ensure that the corresponding network path is accessible so that WAF can correctly monitor and filter traffic.	Single domain name: **www.example.com** Wildcard domain name: ***.example.com** IP Address: XXX.XXX.1.1
Website Remarks	(Optional) You can enter a description for your website.	-

Parameter	Description	Example Value
Policy	The **system-generated policy** is selected by default. You can select a policy you configured before. You can also customize rules after the domain name is connected to WAF. System-generated policies – Basic web protection (**Log only** mode and common checks) The basic web protection defends against attacks such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections. – Anti-crawler (**Log only** mode and **Scanner** feature) WAF only logs web scanning tasks, such as vulnerability scanning and virus scanning, such as crawling behavior of OpenVAS and Nmap. **NOTE** – **Log only**: WAF only logs detected attacks instead of blocking them. – Only the professional and enterprise editions allow you to specify a custom policy for **Policy**.	System-generated policy
Authorize WAF	When you add a website to WAF for the first time, you need to add an agency and grant it the elb_to_waf_operate_policy permission. This permission allows you to call the ELB API to query the load balancer name.	Authorized

6. Click **OK**.

   You can view the added websites in the protected website list.

----End

Follow-up Operations

- (Optional) **Recommended Configurations After Website Connection**: After a domain name is connected to WAF, you need to configure security settings as required.
- **Configuring Protection Policies**: If default protection rules cannot meet your website security requirements, you can configure custom protection rules.
- **Querying a Protection Event**: View website protection details.

FAQs

- Why Is the Access Status of a Domain Name or IP Address Inaccessible?
- How Do I Troubleshoot 404/502/504 Errors?
- What Can I Do If Files Cannot Be Uploaded After a Website Is Connected to WAF?
- Why Cannot the Protection Mode Be Enabled After a Domain Name Is Connected to WAF?

3.4 Connecting Your Website to WAF (Dedicated Mode)

If your service servers are deployed on Huawei Cloud, you can use dedicated WAF instances to protect your website services as long as your website has domain names or IP addresses.

NOTE

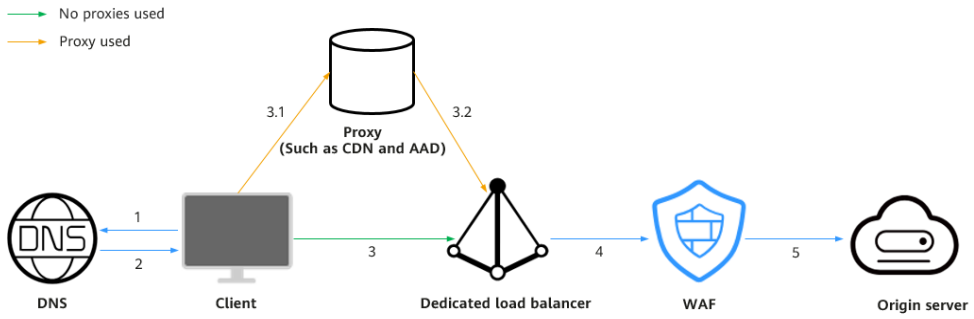
If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and add websites to be protected in the project.

Dedicated WAF instances are not available in some regions. For details, see **Notice on Web Application Firewall (Dedicated Mode) Discontinued**.

Solution Overview

In dedicated mode, after a website is connected to WAF, the website traffic is sent to WAF through the ELB load balancer. WAF blocks abnormal requests and forwards normal requests to the origin server through the back-to-source IP address of the dedicated WAF engine. **Figure 3-24** shows how your website traffic is forwarded when WAF is used.

Figure 3-24 Website access diagram



The details are as follows:

1. After a visitor enters a domain name in the browser, the client sends a request to the DNS service to query the domain name resolution address.
2. DNS returns the domain name resolution address to the client.

3. If no proxies (for example, CDN or AAD) are used, the domain name resolution address returned by the DNS service is the EIP of the load balancer, and the client accesses the load balancer through the EIP. If a proxy is used:
   a. The domain name resolution address returned by DNS is the IP address of the proxy. The client accesses the proxy through the proxy IP address.
   b. The proxy accesses the ELB load balancer over its EIP.
4. The ELB load balancer forwards the traffic to WAF.
5. WAF checks the traffic, blocks abnormal traffic, and forwards normal traffic to the origin server over the back-to-source IP address of the dedicated WAF engine.

Access Process

You need to perform the following operations based on whether your website uses a proxy (such as AAD, CDN, and cloud acceleration products).

Procedure	Description
Step 1. Add a Website to WAF	Add a domain name and origin server details to WAF.
Step 2: Configure a Load Balancer for a Dedicated WAF Instance	Configure a load balancer and health check for a dedicated WAF instance.
Step 3: Bind an EIP to a Load Balancer	Bind an EIP of the origin server to the load balancer configured for a dedicated WAF instance. So that the website request traffic can be forwarded to and checked by the dedicated WAF instance.
Step 4: Whitelist Back-to-Source IP Addresses of Dedicated WAF Instances	Allow the back-to-source IP address of a dedicated engine.
Step 5: Test Dedicated WAF Instances	Check WAF traffic forwarding, ELB load balancer, and WAF basic protection.

Prerequisites

- You have purchased a dedicated load balancer. For details about load balancer types, see **Differences Between Dedicated and Shared Load Balancers**.

  NOTE

  Dedicated WAF instances issued before April 2023 cannot be used with dedicated network load balancers. If you use a dedicated network load balancer (TCP/UDP), ensure that your dedicated WAF instance has been upgraded to the latest version (issued after April 2023). For details, see **Dedicated Engine Version Iteration**.

- Related ports have been enabled in the security group to which the dedicated WAF instance belongs.

  You can configure your security group as follows:

  – Inbound rules

    Add an inbound rule to allow incoming network traffic to pass through over a specified port based on your service requirements. For example, if you want to allow access from port 80, you can add a rule that allows **TCP** and port **80**.

  – Outbound rules

    The value is **Default**. All outgoing network traffic is allowed by default.

  For more details, see **Adding a Security Group Rule**.

Step 1. Add a Website to WAF

To connect your services to WAF, you need to add the domain name and origin server information to WAF.

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 In the upper left corner of the website list, click **Add Website**.

Step 7 Select **Dedicated Mode** and click **Configure Now**.

Step 8 Configure basic information. For details about the parameters, see **Table 3-7**. **Figure 3-25** shows an example.

Figure 3-25 Configuring basic information

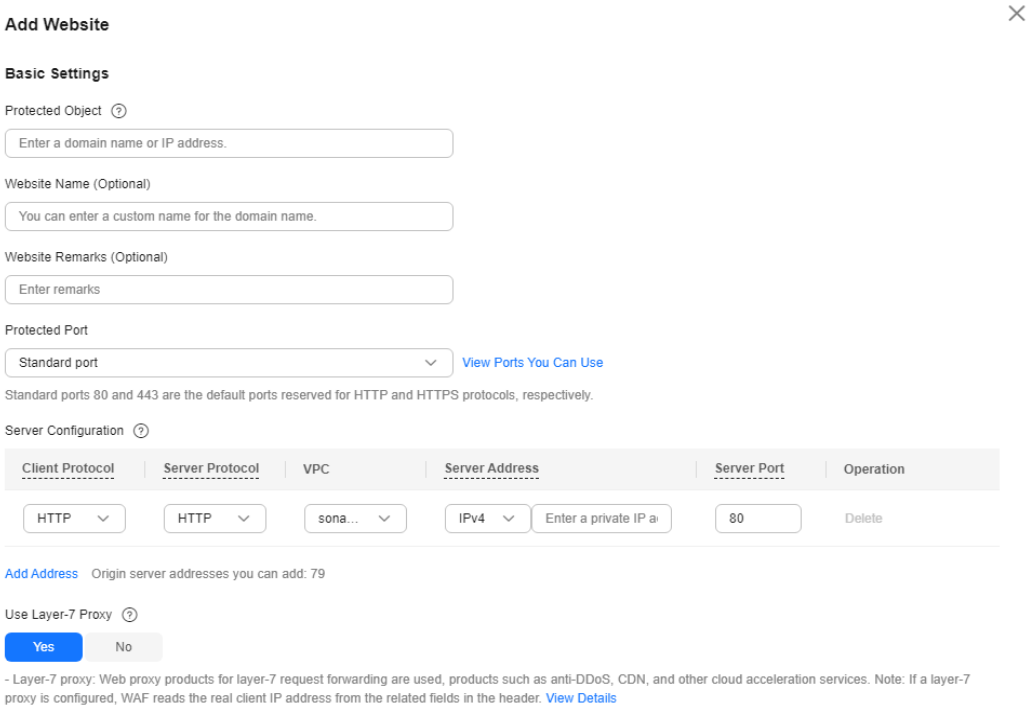


Table 3-7 Parameter description

Parameter	Description	Example Value
Protected Object	The domain name or IP address (public or private IP address) of the website you want to protect. You can enter a single domain name or a wildcard domain name. **NOTE** • The wildcard * can be added to WAF to let WAF protect any domain names. If wildcard (*) is added to WAF, only non-standard ports other than 80 and 443 can be protected. • If the server IP address of each subdomain name is the same, enter a wildcard domain name. For example, if the subdomain names ***a.example.com***, ***b.example.com***, and ***c.example.com*** have the same server IP address, you can add the wildcard domain name ****.example.com*** to WAF to protect all three. • If the server IP addresses of subdomain names are different, add subdomain names as single domain names one by one. • WAF can protect both public and private IP addresses. If a private IP address is used, ensure that the corresponding network path is accessible so that WAF can correctly monitor and filter traffic.	-

Parameter	Description	Example Value
Website Name (Optional)	Website name you specify.	WAF
Website Remarks (Optional)	Remarks of the website.	waftest
Protected Port	Port to be protected. • To protect port 80 or 443, select **Standard port** from the drop-down list. • To protect other ports, select the one WAF supports. Click **View Ports You Can Use** to view the HTTP and HTTPS ports supported by WAF. For more information, see **Ports Supported by WAF**. **NOTE** If a port other than 80 or 443 is configured, the visitors need to add the non-standard port to the end of the website address when they access the website. Otherwise, a 404 error will occur. If a 404 error occurs, see **How Do I Troubleshoot 404/502/504 Errors?**	81

Parameter	Description	Example Value
Server Configuration	Address of the web server. The configuration contains the **Client Protocol**, **Server protocol**, VPC, **Server Address,** and **Server Port**. • **Client Protocol**: protocol used by a client to access a server. The options are **HTTP** and **HTTPS**. • **Server Protocol**: Protocol supported by your website server. **Server Protocol**: protocol used by WAF to forward client requests. The options are **HTTP** and **HTTPS**. **NOTE** – If the client protocol is different from the origin server protocol, WAF forcibly uses the origin server protocol to forward client requests. – WAF can check WebSocket requests. This feature is enabled by default. • **VPC**: Select the VPC to which the dedicated WAF instance belongs. **NOTE** To implement active-active services and prevent single points of failure (SPOFs), you can buy at least two WAF instances and provision them in the same VPC. • **Server Address**: private IP address of the website server. Log in to the ECS or ELB console and view the private IP address of the server in the instance list. **NOTE** The origin server address cannot be the same as that of the protected object. The following IP address formats are supported: – IPv4, for example, XXX.XXX.1.1 – IPv6, for example, fe80:0000:0000:0000:0000:0000:0000:0000 • **Server Port**: service port of the server to which the dedicated WAF instance forwards client requests.	**Client Protocol**: **HTTP** **Server Protocol**: **HTTP** **Server Address**: XXX.XXX.1.1 **Server Port**: **80**

Parameter	Description	Example Value
Certificate Name	If you set **Client Protocol** to **HTTPS**, select **International** for this parameter. • If you have not created a certificate, click **Import New Certificate**. In the **Import New Certificate** dialog box, set certificate parameters. For more details, see **Uploading a Certificate**. The newly imported certificates will be listed on the **Certificates** page as well. • If a certificate has been created, select a valid certificate from the **Existing certificates** drop-down list. • If you have used a CCM certificate under the same account, you can select an SSL certificate from the drop-down list. The name of the SSL certificate you select must be the same as that in CCM. **NOTICE** • Only .pem certificates can be used in WAF. If the certificate is not in PEM format, convert it into pem format first. For details, see **How Do I Convert a Certificate into PEM Format?** • Currently, certificates purchased in Huawei Cloud SCM can be pushed only to the **default** enterprise project. For other enterprise projects, SSL certificates pushed by SCM cannot be used. • If your website certificate is about to expire, purchase a new certificate before the expiration date and update the certificate associated with the website in WAF. WAF can send notifications if a certificate expires. You can configure such notifications on the **Notifications** page. For details, see **Enabling Alarm Notifications**. • Each domain name must have a certificate associated. A wildcard domain name can only use a wildcard domain certificate. If you only have single-domain certificates, add domain names one by one in WAF.	--
Use Layer-7 Proxy	• **Yes**: Web proxy products for layer-7 request forwarding are used, products such as anti-DDoS, CDN, and other cloud acceleration services. • **No**: No layer-7 proxies are used. **NOTICE** If your website uses a proxy, select **Yes**. Then WAF obtains the actual access IP address from the related field in the configured header. For details, see **Configuring a Traffic Identifier for a Known Attack Source**.	Layer-7 proxy

Step 9 Configure the advanced settings.

Policy: The **System-generated policy** is selected by default. You can select a policy you configured before. You can also customize rules after the domain name is connected to WAF.

System-generated policies include:

- Basic web protection (**Log only** mode and common checks)

  The basic web protection defends against attacks such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections.
- Anti-crawler (**Log only** mode and **Scanner** feature)

  WAF only logs web scanning tasks, such as vulnerability scanning and virus scanning, such as crawling behavior of OpenVAS and Nmap.

  NOTE

  Log only: WAF only logs detected attack events instead of blocking them.

Step 10 Click **OK**.

To enable WAF protection, there are still several steps, including configuring a load balancer, binding an EIP to the load balancer, and whitelisting back-to-source IP addresses of your dedicated instance. You can click **Later** in this step. Then, follow the instructions and finish those steps by referring to **Step 2: Configure a Load Balancer for a Dedicated WAF Instance**, **Step 3: Bind an EIP to a Load Balancer**, and **Step 4: Whitelist Back-to-Source IP Addresses of Dedicated WAF Instances**.

----End

Step 2: Configure a Load Balancer for a Dedicated WAF Instance

To ensure your dedicated WAF instance reliability, after you add a website to it, use Huawei Cloud Elastic Load Balance (ELB) to configure a load balancer and a health check for the dedicated WAF instance.

NOTICE

Huawei Cloud ELB is billed by traffic. For details, see **ELB Pricing Details**.

Step 1 Add a listener to the load balancer. For details, see **Adding an HTTP Listener** or **Adding an HTTPS Listener**.

NOTE

When adding a listener, set the parameters as follows:

- **Frontend Port**: the port that will be used by the load balancer to receive requests from clients. You can set this parameter to any port. The origin server port configured in WAF is recommended.
- **Frontend Protocol**: Select HTTP or HTTPS.
- If you select **Weighted round robin** for **Load Balancing Algorithm**, disable **Sticky Session**. If you enable **Sticky Session**, the same requests will be forwarded to the same dedicated WAF instance. If this instance becomes faulty, an error will occur when the requests come to it next time.
- If **Health Check** is configured, the health check result must be **Healthy**, or the website requests cannot be pointed to WAF. For details about how to configure a health check, see **Configuring a Health Check**.

Step 2 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 3 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine**.

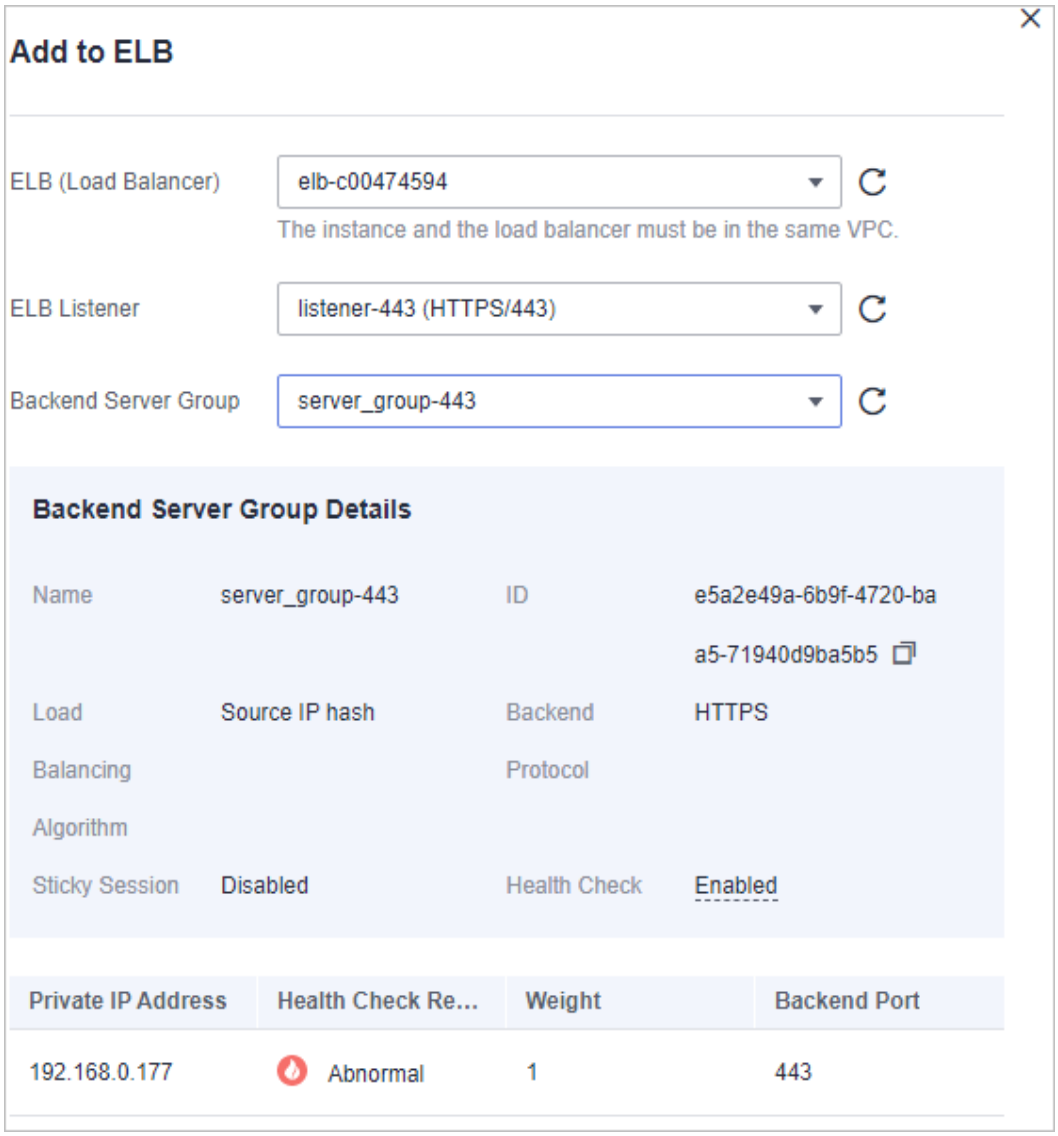
Step 4 In the row containing the instance you want to upgrade, click **More** > **Add to ELB** in the **Operation** column.

NOTE

If you are in the CN East-Shanghai1 or CN North-Ulanqab1 region, you can select multiple running dedicated WAF instances that function as reverse proxies, click **Add to Load Balancer** in the upper left corner of the instance list, and add them to a load balancer to distribute workloads across the dedicated WAF instances.

Step 5 In the **Add to ELB** dialog box, specify **ELB (Load Balancer)**, **ELB Listener**, and **Backend Server Group** based on **Step 1**.

Figure 3-26 Add to ELB



NOTICE

The **Health Check** result must be **Healthy**, or the website requests cannot be pointed to WAF. For details about troubleshooting, see **How Do I Troubleshoot an Unhealthy Backend Server?**

Step 6 Click **OK**. Then, configure service port for the WAF instance, and **Backend Port** must be set to the protected port configured in **Step 1. Add a Website to WAF**.

----End

Step 3: Bind an EIP to a Load Balancer

If you configure a load balancer for your dedicated WAF instance, unbind the EIP from the origin server and then bind this EIP to the load balancer you configured. For details, see **Configuring a Load Balancer**. The request traffic then goes to the

dedicated WAF instance for attack detection first and then go to the origin server, ensuring the security, stability, and availability of the origin server.

This topic describes how to unbind an EIP from your origin server and bind the EIP to a load balancer configured for a dedicated WAF instance.

Step 1 In the upper left corner of the page, click and choose **Networking** > **Elastic Load Balance**. The **Load Balancers** page is displayed.

Step 2 On the **Load Balancers** page, unbind the EIP from the origin server.

- Unbinding an IPv4 EIP: Locate the row that contains the load balancer configured for the origin server. Then, in the **Operation** column, click **More** > **Unbind IPv4 EIP**.
- Unbinding an IPv6 EIP: Locate the row that contains the load balancer configured for the origin server. Then, in the **Operation** column, click **More** > **Unbind IPv6 Address**.

Figure 3-27 Unbinding an EIP

Step 3 In the displayed dialog box, click **Yes**.

Step 4 On the **Load Balancers** page, locate the load balancer configured for the dedicated WAF instance and bind the EIP unbound from the origin server to the load balancer.

- Binding an IPv4 EIP: Locate the row that contains the load balancer configured for the dedicated WAF instance, click **More** in the **Operation** column, and select **Bind IPv4 EIP**.
- Binding an IPv6 EIP: Locate the row that contains the load balancer configured for the dedicated WAF instance, click **More** in the **Operation** column, and select **Bind IPv6 Address**.

Step 5 In the displayed dialog box, select the EIP unbound in **Step 2** and click **OK**.

----End

Step 4: Whitelist Back-to-Source IP Addresses of Dedicated WAF Instances

In dedicated mode, website traffic is pointed to the load balancer configured for your dedicated WAF instances and then to dedicated WAF instances. The latter will filter out malicious traffic and route only normal traffic to the origin server. In this way, the origin server only communicates with WAF back-to-source IP addresses. By doing so, WAF protects the origin server IP address from being attacked. In dedicated mode, the WAF back-to-source IP addresses are the subnet IP addresses of the dedicated WAF instances.

The security software on the origin server may most likely regard WAF back-to-source IP addresses as malicious and block them. Once they are blocked, the origin server will deny all WAF requests. Your website may become unavailable or respond very slowly. So, you need to configure ACL rules on the origin server to trust only the subnet IP addresses of your dedicated WAF instances.

The way to whitelist an IP address varies depending on where your origin servers are provisioned. You can follow the way suitable for you.

Pointing Traffic to an ECS Hosting Your Website

If your origin servers are deployed on Huawei Cloud ECSs, perform the following steps to configure a security group rule to allow only the back-to-source IP address of the dedicated instance to access the origin servers.

Step 1 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 2 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine**.

Step 3 In the **IP Address** column, obtain the IP address of each dedicated WAF instance under your account.

Step 4 In the upper left corner of the page, click and choose **Compute** > **Elastic Cloud Server**.

Step 5 Locate the row containing the ECS hosting your website. In the **Name/ID** column, click the ECS name to go to the ECS details page.

Step 6 Click the **Security Groups** tab. Then, click **Change Security Group**.

Step 7 In the **Change Security Group** dialog box displayed, select a security group or create a security group and click **OK**.

Step 8 Click the security group ID and view the details.

Step 9 Click the **Inbound Rules** tab and click **Add Rule**. Then, specify parameters in the **Add Inbound Rule** dialog box. For details, see **Table 3-8**.

Figure 3-28 Add Inbound Rule

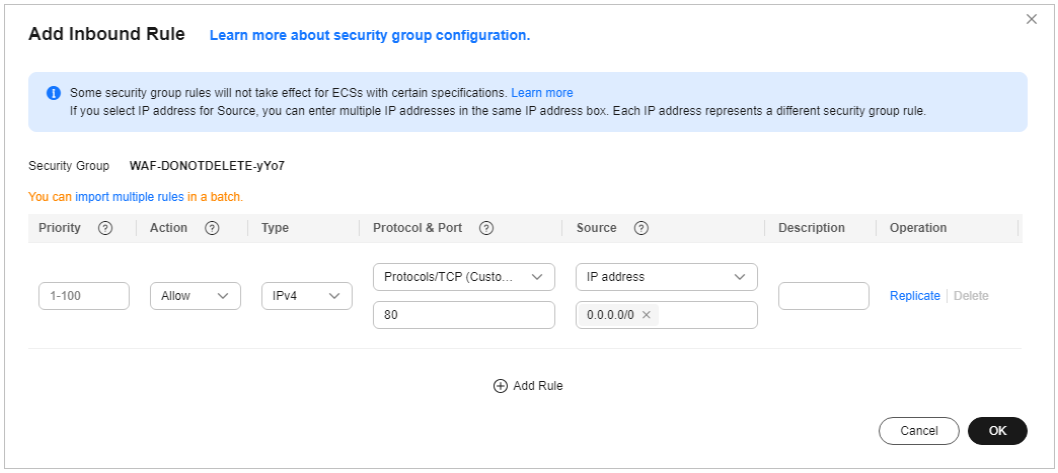


Table 3-8 Inbound rule parameters

Parameter	Configuration Description
Protocol & Port	Protocol and port for which the security group rule takes effect. If you select **TCP (Custom ports)**, enter the origin server port number in the text box below the TCP box.
Server Address	Subnet IP address of each dedicated WAF instance you obtain in **Step 3**. Configure an inbound rule for each IP address. **NOTE** One inbound rule can contain only one IP address. To configure an inbound rule for each IP address, click **Add Rule** to add more rules. A maximum of 10 rules can be configured.

Step 10 Click **OK**.

Now, the security group allows all inbound traffic from the back-to-source IP addresses of all your dedicated WAF instances.

To check whether the configuration takes effect, use the Telnet tool to check whether a connection to the origin server service port bound to the IP address protected by WAF is established.

For example, run the following command to check whether the connection to the origin server service port 443 bound to the IP address protected by WAF is established. If the connection cannot be established over the service port but the website is still accessible, the security group inbound rules take effect.

Telnet *Origin server IP address***443**

----End

Pointing Traffic to a Load Balancer

If your origin server uses Huawei Cloud ELB to distribute traffic, perform the following steps to configure an access control policy to allow only the IP addresses of the dedicated WAF instances to access the origin server:

Step 1 **Log in to the management console**.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine**.

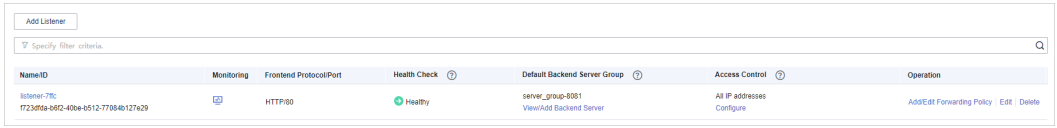
Step 6 In the **IP Address** column, obtain the IP address of each dedicated WAF instance under your account.

Step 7 In the upper left corner of the page, click and choose **Networking** > **Elastic Load Balance**.

Step 8 Locate the row containing the load balancer configured for your dedicated WAF instance and click the load balancer name in the **Name** column.

Step 9 In the **Access Control** row of the target listener, click **Configure**.

Figure 3-29 Listener list



Step 10 In the displayed dialog box, select **Whitelist** for **Access Control**.

1. Click **Create IP Address Group** and add the dedicated WAF instance access IP addresses obtained in **Step 6** to the group being created.
2. Select the IP address group created in **Step 10.1** from the **IP Address Group** drop-down list.

Step 11 Click **OK**.

Now, the access control policy allows all inbound traffic from the back-to-source IP addresses of your dedicated WAF instances.

To check whether the configuration takes effect, use the Telnet tool to check whether a connection to the origin server service port bound to the IP address protected by WAF is established.

For example, run the following command to check whether the connection to the origin server service port 443 bound to the IP address protected by WAF is established. If the connection cannot be established over the service port but the website is still accessible, the security group inbound rules take effect.

Telnet *Origin server IP address***443**

----End

Step 5: Test Dedicated WAF Instances

After adding a website to a dedicated WAF instance, verify that it can forward traffic properly and ELB load balancers work well.

(Optional) Testing a Dedicated WAF Instance

Step 1 Create an ECS that is in the same VPC as the dedicated WAF instance for sending requests.

Step 2 Send requests to the dedicated WAF through the ECS created in **Step 1**.

- Forwarding test

  ```
  curl -kv -H "Host: {protection object added to WAF}"{Client protocol in server configuration}://{IP address of the dedicated WAF instance}:{protection port}
  ```

  For example:

  ```
  curl -kv -H "Host: a.example.com" http://192.168.0.1
  ```


If the response code is 200, the request has been forwarded. If the request failed to be forwarded, rectify the fault by referring to **How Do I Troubleshoot 404/502/504 Errors?**

- Attack blocking test

  a. Ensure that the block mode for basic web protection has been enabled in the policy used for the protected website.

  b. Run the following command:

  ```
  curl -kv -H "Host: {protection object added to WAF}"{Client protocol in server configuration}://{IP address of the dedicated WAF instance}:{protection port}--data "id=1 and 1='1"
  ```

  Example:

  ```
  curl -kv -H "Host: a.example.com" http:// 192.168.X.X --data "id=1 and 1='1"
  ```

  If the response code is 418, the request has been blocked, indicating that the dedicated WAF works properly.

----End

Testing the Dedicated WAF Instance and Dedicated ELB Load Balancer

- Forwarding test (Client protocol: HTTP)

  ```
  curl -kv -H "Host: {Protected object added to WAF}" http://{Private IP address bound to the ELB load balancer}:{ELB listening port}
  ```

  If an EIP is bound to the load balancer, any publicly accessible servers can be used for testing.

  ```
  curl -kv -H "Host: {Protected object added to WAF}" http://{EIP bound to the load balancer}:{ELB listening port}
  ```

  Example:

  ```
  curl -kv -H "Host: a.example.com" http://192.168.X.Y
  curl -kv -H "Host: a.example.com" http://100.10.X.X
  ```

  If the response code is 200, the request has been forwarded.

  If the dedicated WAF instance works but the request fails to be forwarded, check the load balancer settings first. If the load balancer health check result is unhealthy, disable health check and perform the preceding operations again.

- Forwarding test (Client protocol: HTTPS)

  When you use curl to access an HTTPS domain name, SNI is carried by default.

  ```
  curl -kv --resolve {Protected object added to WAF}:{ELB listening port}:{Public IP address of the ELB load balancer} https://{Protected object added to WAF}
  ```

  Example:

  ```
  curl -kv --resolve example.com:443:93.184.X.Y https://example.com
  ```

  If the response code is 200, the request has been forwarded.

  If the dedicated WAF instance works but the request fails to be forwarded, check the load balancer settings first. If the load balancer health check result is unhealthy, disable health check and perform the preceding operations again.

- Attack blocking test

  a. Ensure that the block mode for basic web protection has been enabled in the policy used for the protected website.

b. Run the following command:

```
curl -kv -H "Host: { protected object added to WAF}"{ELB external protocol}://{Private IP address bound to the load balancer}:{ELB listening port}--data "id=1 and 1='1"
```

If an EIP has been bound to the load balancer, any publicly accessible servers can be used for testing.

```
curl -kv -H "Host: { protected object added to WAF}"{ELB external protocol}://{EIP bound to the load balancer}:{ELB listening port}--data "id=1 and 1='1"
```

Example:

```
curl -kv -H "Host: a.example.com" http:// 192.168.0.2 --data "id=1 and 1='1"
curl -kv -H "Host: a.example.com" http:// 100.10.X.X --data "id=1 and 1='1"
```

If the response code is 418, the request has been blocked, indicating that both dedicated WAF instance and ELB load balancer work properly.

Follow-up Operations

1. (Optional) **Recommended Configurations After Website Connection**: After a domain name is connected to WAF, you need to configure security settings as required.
2. **Configuring Protection Policies**: If default protection rules cannot meet your website security requirements, you can configure custom protection rules.
3. **Querying a Protection Event**: View website protection details.

FAQs

- **Why Is the Access Status of a Domain Name or IP Address Inaccessible?**
- **What Can I Do If the Message "Illegal server address" Is Displayed When I Add a Domain Name?**
- **Why Am I Seeing the "Someone else has already added this domain name. Please confirm that the domain name belongs to you" Error Message?**
- **Why Cannot I Select an SCM Certificate When Adding a Domain Name to WAF?**
- **How Do I Troubleshoot 404/502/504 Errors?**
- **Why Does the Requested Page Respond Slowly After My Website Is Connected to WAF?**
- **What Can I Do If Files Cannot Be Uploaded After a Website Is Connected to WAF?**
- **Why Cannot the Protection Mode Be Enabled After a Domain Name Is Connected to WAF?**

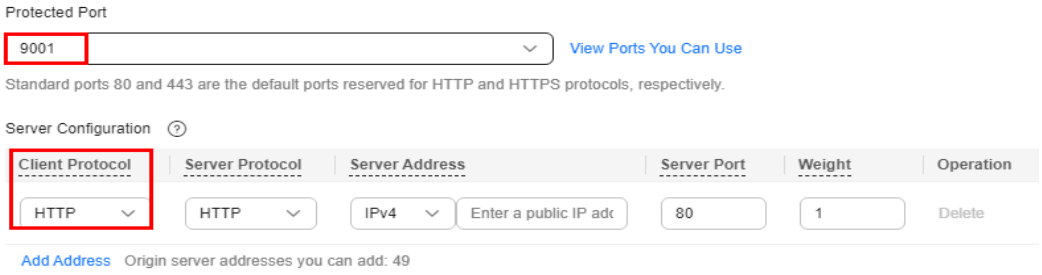
3.5 Ports Supported by WAF

WAF can protect standard and non-standard ports. When you add a website to WAF, you need to specify protection port, which is your service port. WAF will then forward and protect traffic over this port. This section describes the standard and non-standard ports WAF can protect.

For example, as shown in **Table 3-9**, a cloud WAF instance from the standard edition or later and dedicated WAF instances can protect port 9001 over HTTP. If you want to protect port 9001, you can use either a cloud WAF instance from the

standard edition or later or a dedicated WAF instance. Then, configure the instance in **Connecting Your Website to WAF (Cloud Mode - CNAME Access)** by referring to **Figure 3-30**.

Figure 3-30 Port configuration



NOTICE

Note that the supported ports may differ depending on regions.

Standard Ports

WAF can protect the following standard ports.

- Port reserved for HTTP traffic: 80
- Ports reserved for HTTPS traffic: 443

Non-standard ports supported by WAF

WAF can protect non-standard ports in addition to standard ports 80 and 443. Non-standard ports WAF can protect are slightly different depending on WAF modes.

Cloud Mode

Cloud WAF can protect many non-standard ports. Note that these non-standard ports are specified by WAF not the ports you use for your services. Which non-standard ports can be protected by WAF depends on WAF editions you are using.

Table 3-9 Non-standard ports that can be protected by cloud WAF

Edition	Non-standard Port That Can Be Protected	
	HTTP	HTTPS
Standard (pay-per-use)	81, 82, 83, 84, 86, 87, 88, 89, 800, 808, 1091, 1092, 5000, 7009, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8025, 8026, 8061, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8686, 8800, 8888, 8889, 8999, 18085, and 9001	4443, 5048, 5049, 5443, 6443, 7072, 7073, 7443, 8033, 8081, 8082, 8083, 8084, 8443, 8712, 8803, 8804, 8805, 8843, 9443, 8553, 8663, 9553, 9663, 18000, 18110, 18381, 18443, 18980, 8453, 9098,19000, and 28443

Edition	Non-standard Port That Can Be Protected	
	HTTP	HTTPS
Professional	81, 82, 83, 84, 85, 86, 87, 88, 89, 97, 133, 134, 140, 141, 144, 151, 800, 808, 881, 888, 1000, 1090, 1091, 1092, 1135, 1139, 1180, 1688, 3128, 3333, 3501, 3601, 4444, 5000, 5001, 5080, 55222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7080, 77081, 7082, 7083, 7088, 7097, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8004, 8007, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8024, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8182, 8232, 8334, 8336, 8686, 8800, 8813, 8814, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9007, 9020, 9021, 9022, 9023, 9024, 9025, 9026, 9027, 9028, 9029, 9037, 9050, 9077, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 9099, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9802, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9945, 9770, 10000, 10001, 10080, 10087, 11000, 12601, 13000, 14000, 18085, 18081, 18180, 18280, 19101, 19501, 21028, 23333, 27777, 28080, 30002, 30086, 33332, 33334, 33702, 40010, 48299, 48800, 52725, 52726, 60008, 60010, 1091, 1092, 8061, 8301, 8303, 8304, 8306, 9014, 9015, 9104, 9105, 9301, 9302, 9303, 9306, and 18080	90, 447, 882, 1446, 1448, 1451, 1452, 1818, 4006, 4430, 4433, 4443, 5048, 5049, 5100, 5443, 6022, 6130, 6133, 6140, 6141, 6142, 6150, 6443, 7072, 7073, 7443, 8033, 8043, 8079, 8081, 8082, 8083, 8084, 8211, 8221, 8224, 8231, 8243, 8244, 8281, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8810, 8815, 8817, 8836, 8838, 8840, 8842, 8843, 8990, 8991, 9005, 9053, 9090, 9300, 9443, 9553, 9663, 9681, 9682, 9999, 10002, 10003, 10006, 10300, 10301, 11001, 11003, 12340, 12341, 12342, 12343, 12344, 12345, 12346, 12347, 12348, 12349, 12350, 12351, 12352, 12353, 12354, 13001, 13003, 13080, 14003, 14443, 17618, 17718, 17818, 17918, 18000, 18001, 18010, 18110, 18381, 18443, 18980, 19000, 19999, 20000, 28443, 9166, 6091, 6200, 9309, 6019, 6017, 6018, 6020, 6030, 9805, 9806, 9807, 9808, 1443, 3444, 8453, 9098, and 60009

Edition	Non-standard Port That Can Be Protected	
	HTTP	HTTPS
Enterprise	81, 82, 83, 84, 85, 86, 87, 88, 89, 97, 133, 134, 140, 141, 144, 151, 800, 808, 881, 888, 1000, 1090, 1091, 1092, 1135, 1139, 1688, 1180, 3128, 3333, 3501, 3601, 4444, 5000, 5001, 5080, 5222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7081, 7082, 7083, 7088, 7097, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8004, 8006, 8007, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8024, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8182, 8232, 8334, 8336, 8686, 8800, 8813, 8814, 8888, 8889, 8899, 8989, 8999, 9000, 9001, 9002, 9003, 9007, 9020, 9021, 9022, 9023, 9024, 9025, 9026, 9027, 9028, 9029, 9037, 9050, 9077, 9080, 9081, 9082, 9099, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9770, 9802, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9945, 10000, 10001, 10080, 10087, 11000, 12601, 13000, 14000, 18080, 18081, 18180, 18085, 18280, 23333, 27777, 28080, 30086, 33702, 48299, 8061, 8301, 8303, 8304, 8306, 9014, 9015, 9104, 9105, 9301, 9302, 9303, 9306, and 48800	90, 447, 882, 1446, 1448, 1451, 1452, 1818, 4006, 4430, 4433, 4443, 5048, 5049, 5443, 6022, 6130, 6133, 6140, 6141, 6142, 6150, 6443, 7072, 7073, 7443, 8033, 8043, 8079, 8081, 8082, 8083, 8084, 8211, 8221, 8224, 8231, 8243, 8244, 8281, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8810, 8815, 8817, 8836, 8838, 8840, 8842, 8843, 8848, 8910, 8920, 8950, 8990, 8991, 9005, 9053, 9090, 9182, 9184, 9190, 9300, 9443, 9553, 9663, 9681, 9682, 9999, 10002, 10003, 10006, 10300, 10301, 11001, 11003, 12340, 12341, 12342, 12343, 12344, 12345, 12346, 12347, 12348, 12349, 12350, 12351, 12352, 12353, 12354, 13001, 13003, 13080, 14003, 17618, 17718, 17818, 17918, 18000, 18001, 18010, 18110, 18381, 18443, 18980, 19000, 19999, 28443, 9166, 6091, 6200, 9309, 6019, 6017, 6018, 6020, 6030, 9805, 9806, 9807, 9808, 1443, 3444, 8453, 9098, and 60009

Dedicated Mode

If you use dedicated WAF instances, you can select any non-standard ports listed in **Table 3-10**.

Table 3-10 Non-standard ports that can be protected by dedicated waf instances

HTTP	HTTPS
81, 82, 83, 84, 86, 87, 88, 89, 97, 800, 808, 1000, 1090, 3128, 3333, 3501, 3601, 4444, 5000, 5080, 5222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7080, 7081, 7082, 7083, 7088, 7097, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8686, 8800, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9021, 9023, 9027, 9037, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9770, 9802, 9945, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 10000, 10001, 10080, 12601, 19101, 19501, 19998, 21028, 28080, 30002, 33332, 33334, 33702, 40010, 48800, 52725, 52726, 1091, 1092, 60008, and 60010	4443, 5443, 6443, 7072, 7073, 7443, 8033, 8081, 8082, 8083, 8084, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8843, 9443, 9553, 9663, 9999, 18000, 18010, 18110, 18381, 18443, 18980, and 19000, 28443

4 Viewing Protection Events

4.1 Querying a Protection Event

WAF sorts out the attacks, the ten websites attacked the most, ten attack source IP addresses that launched the most attacks, and the ten URLs attacked the most for a selected time range. You can view the blocked or logged events on the **Events** page. You can view details of events generated by WAF, including the occurrence time, client IP address, geographic location of the client IP address, malicious load, and hit rule for an event.

Prerequisites

You have connected the website you want to protect to WAF.

Constraints

- On the WAF console, you can view the event data for all protected domain names over the last 30 days. You can authorize LTS to log WAF activities so that you can view attack and access logs and store all logs for a long time. For more details, see **Using LTS to Log WAF Activities**.
- If you switch the WAF working mode for a website to **Suspended**, WAF only forwards all requests to the website without inspection. It does not log any attack events neither.
- After an attack occurs, it takes about 2 to 3 minutes for the attack to be logged as a protection event.

Viewing Protection Event Logs

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by**

enterprise project drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Events**.

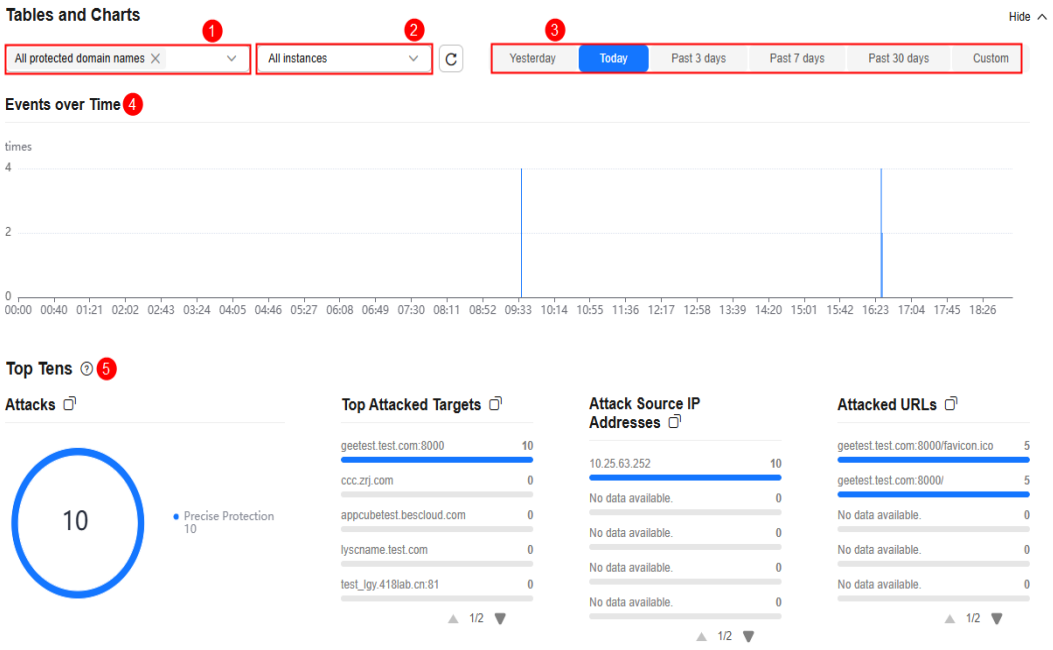
Step 6 On the **Search** tab, view the statistical charts and event details.

----End

Tables and Charts

This area displays the event trends and top 10 events for a specified protected domain name, instance, and time range.

Figure 4-1 Tables and Charts



Step 1 Set search criteria.

- **Domain name** (① in **Figure 4-1**): You can select a specific domain name, multiple domain names, or all domain names to view the security statistics.
- **Instance** (② in **Figure 4-1**): You can select a specific instance or all instances to view security statistics.
- **Query time** (③ in **Figure 4-1**): You can view bot protection statistics for yesterday, today, past 3 days, past 7 days, past 30 days, or any time range within 30 days.

Step 2 View the statistical charts.

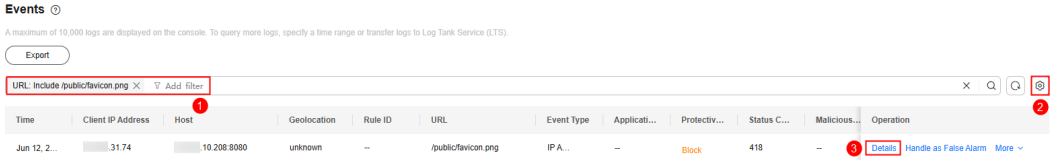
Function Module	Description	Related Operation
Events over Time (④ in **Figure 4-1**)	Displays the WAF protection status for the selected website within a specified period.	--
Top Tens (⑤ in **Figure 4-1**)	Displays the top 10 attack events, attacked objects, attack source IP addresses, and attacked URLs in the selected period.	• **Attacks (1-5)**, **Attacked Targets (1-5)**, **Attack Source IP Addresses (1-5)**, and **Attacked URLs (1-5)** are displayed by default. You can click > next to each area to view **Attacks (6-10)**, **Attacked Targets (6-10)**, **Attack Source IP Addresses (6-10)**, and **Attacked URLs (6-10)**. • You can click next to **Attacks**, **Top Attacked Objects**, **Attack Source IP Addresses**, or **Attacked URLs** to copy the data in the statistical charts. • You can click a domain name, client IP address, or URL listed in **Top Attacked Objects**, **Attack Source IP Addresses**, or **Attacked URLs** charts to make a quick search in the event list, as WAF automatically adds filter criteria to the event search box after you click an object.

----End

Events

A maximum of 10,000 logs are displayed on the console. To query more logs, specify a time range or transfer logs to Log Tank Service (LTS).

Figure 4-2 Events



Step 1 Set matching conditions (① in **Figure 4-2**) based on filter condition fields. The matching conditions you set will be displayed above the event list. For details about the condition fields, see **Table 4-1**.

Table 4-1 Filter condition fields

Parameter	Description
Client IP Address	Public IP address of the web visitor/attacker. By default, **All** is selected. You can view logs of all attack source IP addresses, select an attack source IP address, or enter an attack source IP address to view corresponding attack logs.
Host	Attacked domain name.
Rule ID	ID of a built-in protection rule in WAF basic web protection.
URL	Attacked URL.
Event Type	Type of the attack. By default, **All** is selected. You can view logs of all attack types or select an attack type to view corresponding attack logs.
Protective Action	The options are **Block**, **Log only**, **Verification code**, and **Mismatch**. • **Verification code**: In CC attack protection rules, you can set **Protective Action** to **Verification code**. If a visitor sends too many requests, with the request quantity exceeding the rate limit specified by the CC attack protection rule used, a message is displayed to ask the visitor to provide a verification code. Visitor's requests will be blocked unless they enter a valid verification code. • **Mismatch**: If an access request matches a web tamper protection rule, information leakage prevention rule, or data masking rule, the protective action is marked as **Mismatch**.
Status Code	HTTP status code returned on the block page.
Event ID	ID of the event.

Step 2 Click  (② in **Figure 4-2**) in the upper right corner of the event list to set the fields to be displayed in the event list. For details about the fields, see **Table 4-2**.

Table 4-2 Parameters in the event list

Parameter	Description	Example Value
Time	When the attack occurred.	2021/02/04 13:20:04
Client IP Address	Public IP address of the web visitor/attacker. Click in the **Client IP Address** column to sort the event list in ascending or descending order.	-
Host	Attacked domain name.	www.example.com
Geolocation	Geographic location where the client IP address is located.	-
Rule ID	ID of a built-in protection rule in WAF basic web protection.	-
URL	Attacked URL.	/admin
Event Type	Type of attack.	SQL injection
Application Component	Application component that was attacked.	pgAdmin4
Protective Action	Protective actions configured in the rule. The options are **Block**, **Log only**, and **Verification code**. **NOTE** If an access request matches a web tamper protection rule, information leakage prevention rule, or data masking rule, the protective action is marked as **Mismatch**.	Block
Status Code	HTTP status code returned on the block page.	418
Malicious Load	Location or part of the attack that causes damage or the number of times that the URL was accessed. **NOTE** • In a CC attack, the malicious load indicates the number of times that the URL was accessed. • For blacklist protection events, the malicious load is left blank.	id=1 and 1='1
Enterprise Project	Enterprise project your websites belong to. Click in the **Enterprise Project** column to sort the event list in ascending or descending order.	default

After the preceding configurations are complete, as shown in **Figure 4-2**, you can view the events that meet the search criteria in the event list.

Step 3 Locate the target event and click **Details** in the **Operation** column (③ in **Figure 4-2**) to view details about the event. You can check the event overview, malicious payloads, response details, and request details.

NOTE

You need to **submit a service ticket** to enable the response details function, and configure the length of the response body to be logged. In this way, WAF can display the response details and record the response body based on specified length.

----End

Related Operations

- **Handling False Alarms Triggered by Protection Rules**: If you are sure that an event is a false alarm generated based on a WAF **built-in rule** or **custom protection rule**, you can handle the event as a false alarm.
  - WAF built-in rules include **basic web protection rules**, **known bot detection**, **request signature detection**, **bot behavior detection**, and **proactive feature detection** rules for bot protection, and **feature-based anti-crawler rules**.
  - WAF custom rules include **CC attack protection rules**, **precise protection rules**, **blacklist and whitelist rules**, and **geolocation access control rules** you create.
- **Handling False Positives Based on Client IP Addresses**: If you are sure a client IP address is blocked mistakenly, you can **add the IP address to an address group** and **add the IP address to a blacklist/whitelist rule** to allow it.
- **Exporting protection events**

  In the upper left corner of the event list, click **Export** to export events. If the number of events is less than 200, the events are exported to your local PC.

FAQs

- **How Do I Handle False Alarms as WAF Blocks Normal Requests to My Website?**
- **Why Are There Garbled Characters in Event Data I Exported from WAF?**
- **Why Is the Traffic Statistics on WAF Inconsistent with That on the Origin Server?**
- **Why Is the Number of Logs on the Dashboard Page Inconsistent with That on the Log Settings Tab?**

4.2 Handling False Alarms

If you are sure that a protection event is a false alarm (no malicious link or character was detected), you can handle it as a false alarm, add the client IP address to an address group that is allowed by the policy, add the client IP address to a blacklist/whitelist rule, or disable or delete the hit protection rule. Events that have been handled as false alarms will not be displayed in the event list. You will no longer receive any alarm notifications on the events of this kind.

Scenarios

If legitimate service requests are blocked by WAF, the website may be inaccessible to some visitors. For example, after you connect a web service deployed on Huawei Cloud ECSs to WAF over its public domain name and enable basic web protection for it, if its normal traffic hits a protection rule, the access requests will be blocked. The web service becomes inaccessible over the domain name or returns errors to visitors, but it is still accessible over server IP addresses. It is more likely that the requests were blocked mistakenly, and the event is a false alarm. In this case, you need to handle the event as a false alarm.

You can handle false alarms in the following ways based on how they were generated:

- For a protection event triggered by a WAF built-in rule, you can ignore the corresponding WAF protection in the global protection whitelist rule or disable the corresponding bot rule. For details, see **Handling False Alarms Triggered by Protection Rules**.

  WAF built-in rules include basic web protection rules, known bot detection, request signature detection, bot behavior detection, and proactive feature detection rules for bot protection, and feature-based anti-crawler rules.
- For a protection event triggered by a custom rule, you can disable or delete the corresponding protection rule. For details, see **Handling False Alarms Triggered by Protection Rules**.

  WAF custom rules include **CC attack protection rules**, **precise protection rules**, **blacklist and whitelist rules**, and **geolocation access control rules** you create.
- For a client IP address mistakenly blocked, you can add it to an address group or add it to a blacklist/whitelist rule to allow it. For details, see **Handling False Positives Based on Client IP Addresses**.

Prerequisites

A protection event has been reported and displayed on the **Events** page.

Constraints

- A protection event can only be handled as a false alarm once.
- Dedicated WAF instances earlier than June 2022 do not support **All protection** for **Ignore WAF Protection**. Only **Basic web protection** can be selected.

Handling False Alarms Triggered by Protection Rules

If you are sure that an event is a false alarm generated based on a WAF built-in rule or custom protection rule, you can handle the event as a false alarm.

- WAF built-in rules include **basic web protection rules**, **known bot detection**, **request signature detection**, **bot behavior detection**, and **proactive feature detection** rules for bot protection, and **feature-based anti-crawler rules**.
- WAF custom rules include **CC attack protection rules**, **precise protection rules**, **blacklist and whitelist rules**, and **geolocation access control rules** you create.

Step 1 **Log in to the management console**.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Events**.

Step 6 View protection details of a specified domain name, instance, and time range. For details, see **Querying a Protection Event**.

Step 7 Locate the target protection event and click **Handle as False Alarm** in the **Operation** column.

Step 8 In the **Handle False Alarm** dialog box, handle the event.

- **Ignore the corresponding WAF protection based on the request features hit the rule.**

  If a protection event is triggered by a rule in **Basic Web Protection** or **Feature-based Anti-Crawler**, the associated request features will be displayed in the **Handle False Alarm** dialog box by default. You need to ignore the corresponding WAF protection type and click **OK**. For details about the parameters of the global whitelist rule, see **Table 4-3**.

  Figure 4-3 Handle False Alarm

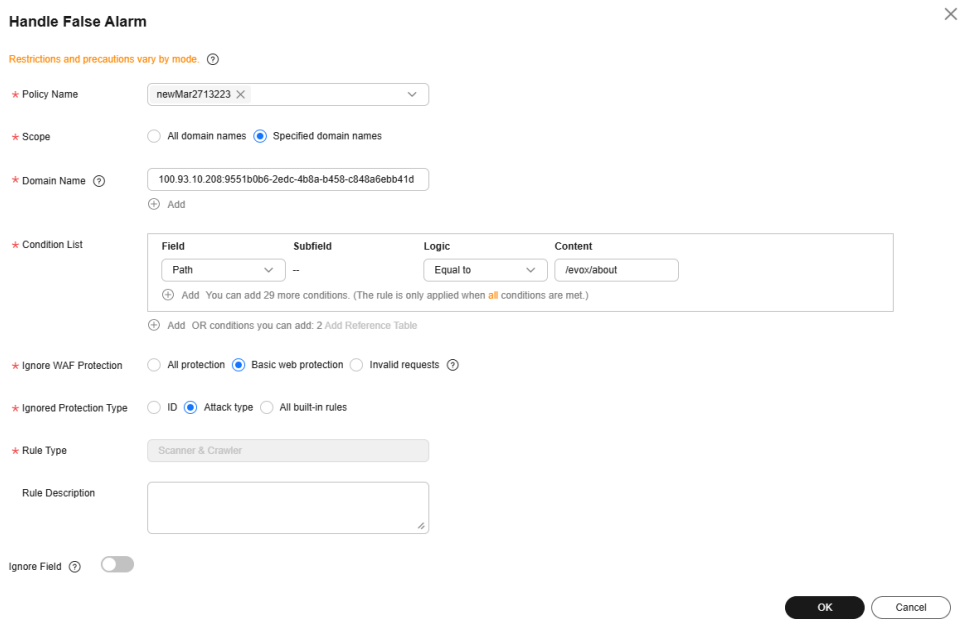


Table 4-3 Parameters

Parameter	Description	Example Value
Scope	– **All domain names**: By default, this rule will be applied to all domain names that are protected by the current policy. – **Specified domain names**: Specify a domain name range this rule applies to.	Specified domain names
Domain Name	This parameter is mandatory when you select **Specified domain names** for **Scope**. Enter a single domain name that matches the wildcard domain name being protected by the current policy. To add more domain names, click **Add** to add them one by one.	www.example.com

Parameter	Description	Example Value
Condition List	– Click **Add** in the condition box to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. – You can click **Add** outside the condition box to add a group of conditions. A maximum of three condition groups can be added. The **OR** logic is used between all condition groups. So, the rule works as long as one condition group is met. Condition parameter description: – **Field** – **Subfield**: Configure this field only when **IPv4**, **IPv6**, **Params**, **Cookie**, **Header** or **Response Header** is selected for **Field**. If **Field** is set to **Response Header** or **Header**, and **Subfield** is not **All** or **Any**, **Case Sensitive** is supported. **NOTICE** A subfield cannot exceed 2,048 characters. – **Logic**: Select a logical relationship from the drop-down list. – **Content**: Enter or select the content that matches the condition.	**Field** is set to **Path**. **Logic** is set to **Include**. **Content** is set to **/product**.

Parameter	Description	Example Value
Ignore WAF Protection	– **All protection**: All WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule. – **Basic web protection**: You can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, if XSS check is not required for a URL, you can whitelist XSS rule. – **Invalid requests**: WAF can allow invalid requests. **NOTE** A request is invalid if: ■ The request header contains more than 512 parameters. ■ The URL contains more than 2,048 parameters. ■ The request header contains "Content-Type:application/x-www-form-urlencoded", and the request body contains more than 8,192 parameters.	Basic web protection
Ignored Protection Type	If you select **Basic web protection** for **Ignored WAF Protection**, select one of the following for **Ignored Protection Type**: – **ID**: Configure the rule by event ID. – **Attack type**: Configure the rule by attack type, such as XSS and SQL injection. One type contains one or more rule IDs. – **All built-in rules**: all checks enabled in **Basic Web Protection**.	Attack type
Rule ID	This parameter is mandatory when you select **ID** for **Ignored Protection Type**. Rule ID of a misreported event in **Events** whose type is not **Custom**. You are advised to handle false alarms on the **Events** page.	041046

Parameter	Description	Example Value
Rule Type	This parameter is mandatory when you select **Attack type** for **Ignored Protection Type**. Select an attack type from the drop-down list box. WAF can defend against XSS attacks, web shells, SQL injection attacks, malicious crawlers, remote file inclusions, local file inclusions, command injection attacks, and other attacks.	SQL injection
Rule Description	A brief description of the rule. This parameter is optional.	SQL injection attacks are not intercepted.
Ignore Field	To ignore attacks of a specific field, specify the field in the **Advanced Settings** area. After you add the rule, WAF will stop blocking attacks matching the specified field. Select a target field from the first drop-down list box on the left. The following fields are supported: **Params**, **Cookie**, **Header**, **Body**, and **Multipart**. – If you select **Params**, **Cookie**, or **Header**, you can select **All** or **Field** to configure a subfield. – If you select **Body** or **Multipart**, you can select **All**. – If you select **Cookie**, the **Domain Name** box for the rule can be empty. **NOTE** If **All** is selected, WAF will not block all attack events of the selected field.	Params All

- **Disabling a bot protection rule**

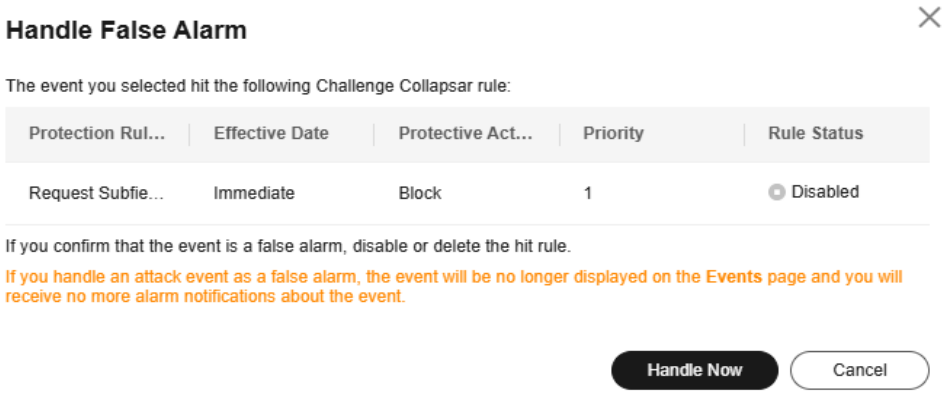
  For a protection event triggered by a bot protection rule, the hit bot protection rule is displayed in the **Handle False Alarm** dialog box. You can click **Handle Now** in the dialog box and disable the rule on the displayed page. For details about bot protection rules, see **Configuring Bot Protection Rules to Defend Against Bot Behavior**.

- Disabling or deleting a custom protection rule

  For a protection event triggered by a custom protection rule (such as a CC attack protection rule or precise protection rule), the custom protection rule is displayed in the **Handle False Alarm** dialog box. You can click **Handle Now**

to go to the custom protection rule page. Then, click **Disable** or **Delete** in the **Operation** column of the target rule.

Figure 4-4 Disabling or deleting a custom protection rule



----End

Handling False Positives Based on Client IP Addresses

If you are sure a client IP address is blocked mistakenly, you can **add the IP address to an address group** and **add the IP address to a blacklist/whitelist rule** to allow it.

Step 1 **Log in to the management console**.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

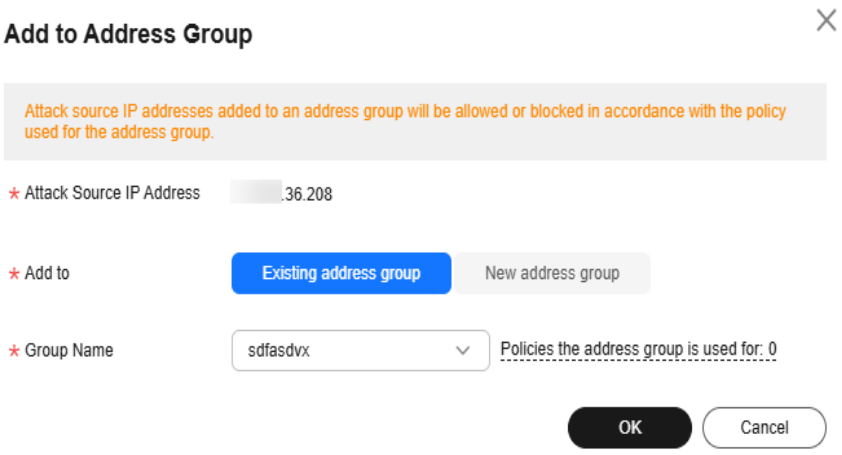
Step 5 In the navigation pane on the left, click **Events**.

Step 6 View protection details of a specified domain name, instance, and time range. For details, see **Querying a Protection Event**.

Step 7 Locate the target client IP address and click **Add to Address Group** or **Add to Blacklist/Whitelist**.

- Adding a client IP address to an address group
  a. In the **Operation** column of the target client IP address, choose **More** > **Add to Address Group**.
  b. In the **Add to Address Group** dialog box, add the client IP address to an existing address group or a new address group.

Figure 4-5 Add to Address Group



c. Associate the address group with a protection policy. If the address group has been associated with a protection policy, skip this step.

   After the preceding configurations are complete, WAF blocks or allows the client IP addresses based on the protection policy associated with the address group.

- Adding a client IP address to a blacklist or whitelist

  a. In the **Operation** column of the target client IP address, choose **More** > **Add to Blacklist/Whitelist**.

  b. In the **Add to Blacklist/Whitelist** dialog box, add the client IP address to an existing rule or a new rule. For more details about a blacklist/whitelist rule, see **Table 4-4**.

Figure 4-6 Add to Blacklist/Whitelist

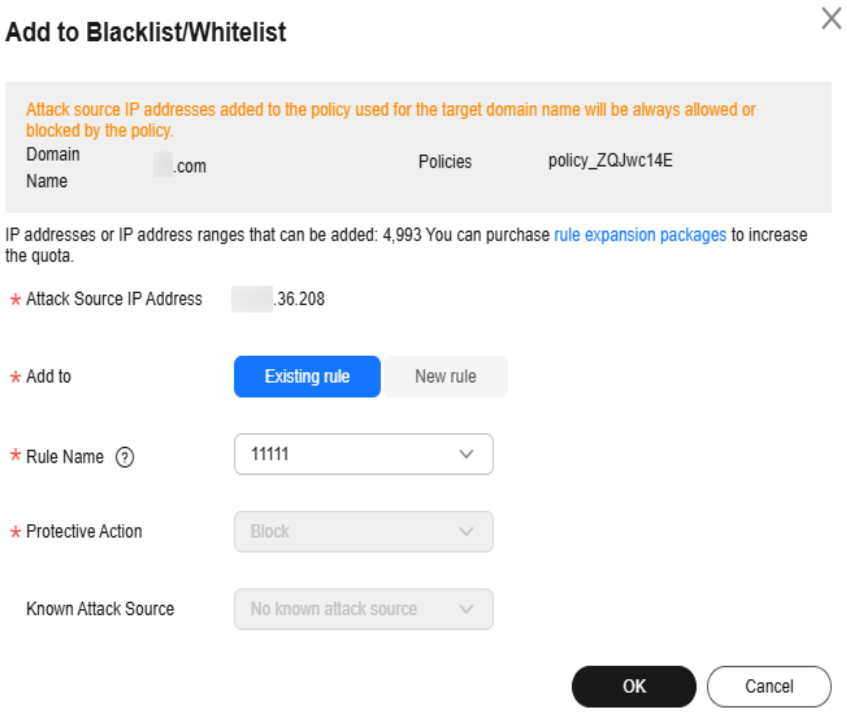


Table 4-4 Parameter descriptions

Parameter	Description
Add to	▪ **Existing rule**: Add the client IP address to an existing blacklist or whitelist rule used for the protected domain name. ▪ **New rule**: Create a blacklist or whitelist rule for the protected domain name and add the client IP address to the rule.
Rule Name	▪ If you select **Existing rule** for **Add to**, select a rule name from the drop-down list. ▪ If you select **New rule** for **Add to**, customize a blacklist or whitelist rule.
IP Address/ Range/Group	Add an IP address, IP address range, or address group. This parameter is mandatory only when you select **New rule** for **Add to**. ▪ **IP address/range**: Add the client IP address to the blacklist or whitelist. ▪ **Address group**: Add the client IP address to the address group associated with the blacklist or whitelist rule. If you select **Address Group**, you need to select an existing address group or create a new address group. For details, see **Adding an IP Address Group**.
Protective Action	Select the protective action for the rule. This parameter is mandatory only when you select **New rule** for **Add to**. ▪ **Block**: Select **Block** if you want to black the IP address or IP address range you configure previously. ▪ **Allow**: Select **Allow** if you want to allow the IP address or IP address range you configure previously. ▪ **Log only**: Select **Log only** if you want to observe the traffic from the IP address or IP address range you configure previously.

Parameter	Description
Known Attack Source	If you select **Block** for **Protective Action**, you can configure a known attack source rule. Then, WAF blocks the requests matching the configured **IP**, **Cookie**, or **Params** for a period configured by the known attack source rule. For details about know attack source rules, see **Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration**.
Rule Description	Description of the rule.

After the preceding configurations are complete, WAF blocks or allows client IP addresses based on the blacklist and whitelist rule you configure.

----End

Operation Result Verification

It takes about one minute for the operation works. Handled false alarms will no longer be displayed in the event list. You can refresh the browser cache, access the page for which the global whitelist rule is configured, and check whether the configuration is successful.

Related Operations

- If an event is handled as a false alarm, the rule hit will be added to the global protection whitelist rule list. You can go to the **Policies** page and then switch to the **Global Protection Whitelist** page to manage the rule, including querying, disabling, deleting, and modifying the rule. For details, see **Configuring a Global Protection Whitelist Rule**.
- If the **Handle as False Alarm** button is grayed out, see **Why Is the Handle as False Alarm Button Grayed Out?**

4.3 Using LTS to Log WAF Activities

After you authorize WAF to access Log Tank Service (LTS), you can use the WAF logs recorded by LTS for quick and efficient real-time analysis, device O&M management, and analysis of service trends.

LTS analyzes and processes a large number of logs. It enables you to process logs in real-time, efficiently, and securely. Logs can be stored in LTS for 30 days by default but you can configure LTS for up to 365 days if needed. Logs earlier than storage duration are automatically deleted. However, you can configure LTS to dump those logs to an Object Storage Service (OBS) bucket or enable Data Ingestion Service (DIS) for long-term storage.

NOTICE

- On the WAF console, you can view protection event logs generated over the last 30 days.
- LTS is billed by traffic and is billed separately from WAF. For details about LTS pricing, see **LTS Pricing Details**.
- If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select the project from the **Enterprise Project** drop-down list and configure WAF logging.

Prerequisites

- **You have purchased a WAF instance.**
- **You have connected the website you want to protect to WAF.**

Impact on the System

Enabling LTS for WAF does not affect WAF performance.

Enabling LTS for WAF Protection Event Logging

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Events**.

Step 6 Click the **Configure Logs** or **Log Settings** tab, enable LTS (), and select a log group and log stream. **Table 4-5** describes the parameters.

Figure 4-7 Log settings

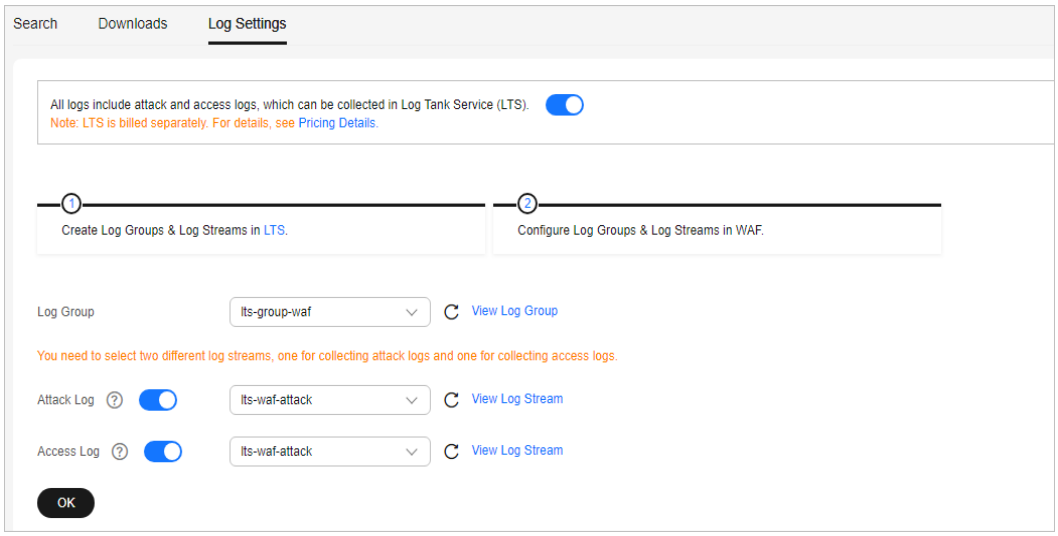


Table 4-5 Log configuration

Parameter	Description	Example Value
Log Group	Select a log group or click **View Log Group** to go to the LTS console and create a log group.	lts-group-waf
Attack Log	Select a log stream or click **View Log Stream** to go to the LTS console and create a log stream. An attack log includes information about event type, protective action, and attack source IP address of each attack.	lts-topic-waf-attack
Access Log	Select a log stream or click **View Log Stream** to go to the LTS console and create a log stream. An access log includes key information about access time, client IP address, and resource URL of each HTTP access requests.	lts-topic-waf-access

Step 7 Click **OK**.

You can view WAF protection event logs on the LTS console.

----End

Checking and Downloading WAF Protection Event Logs on LTS

After enabling LTS, you can go to the LTS console and check, analyze, and download WAF logs.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Management & Governance** > **Log Tank Service**.

Step 4 In the log group list, click to expand the WAF log group (for example, **lts-group-waf**).

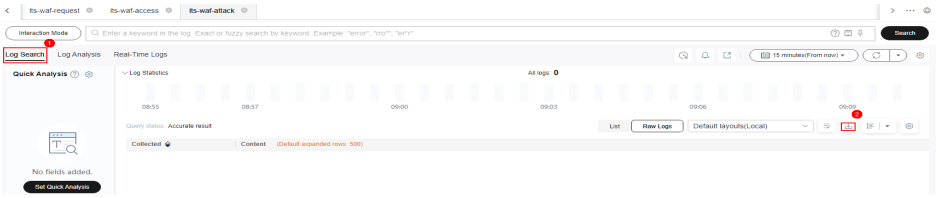
Step 5 In the log stream list, click the log stream name to go to the log stream log page. Then, you can check and analyze logs.

Step 6 On the **Log Search** tab, click to download logs reported in the log stream.

Direct Download: Download log files to the local PC. Up to 5,000 logs can be downloaded at a time.

Select **.csv** or **.txt** from the drop-down list and click **Download** to export logs to the local PC.

Figure 4-8 Download Logs



----End

WAF access_log Field Description

Field	Type	Field Description	Description
access_log.requestid	String	Random ID	The value is the same as the last eight characters of the **req_id** field in the attack log.
access_log.time	String	Access time	GMT time a log is generated.
access_log.connection_requests	String	Sequence number of the request over the connection	-

Field	Type	Field Description	Description
access_log.eng_ip	String	IP address of the WAF engine	-
access_log.pid	String	The engine that processes the request	Engine (worker PID).
access_log.hostid	String	Domain name identifier of the access request.	Protected domain name ID (upstream_id).
access_log.tenantid	String	Account ID	Each Huawei Cloud account corresponds to a tenant ID.
access_log.projectid	String	ID of the project the protected domain name belongs to	Project ID of a user in a specific region.
access_log.remote_ip	String	Remote IP address of the request at layer 4	IP address from which a client request originates. **NOTICE** If a layer-7 proxy is deployed in front of WAF, this field indicates the IP address of the proxy node closest to WAF. The real IP address of the visitor is specified by the **x-forwarded-for** and **x_real_ip** fields.
access_log.remote_port	String	Remote port of the request at layer 4	Port used by the IP address from which a client request originates
access_log.sip	string	IP address of the client that sends the request	For example, XFF.
access_log.scheme	String	Request protocol	Protocols that can be used in the request: • HTTP • HTTPS
access_log.response_code	String	Response code	Response status code returned by the origin server to WAF.

Field	Type	Field Description	Description
access_log.method	String	Request method.	Request type in a request line. Generally, the value is **GET** or **POST**.
access_log.http_host	String	Domain name of the requested server.	Address, domain name, or IP address entered in the address bar of a browser.
access_log.url	String	Request URL.	Path in a URL (excluding the domain name).
access_log.request_length	String	Request length.	The request length includes the access request address, HTTP request header, and number of bytes in the request body.
access_log.bytes_send	String	Total number of bytes sent to the client.	Number of bytes sent by WAF to the client.
access_log.body_bytes_sent	String	Total number of bytes of the response body sent to the client	Number of bytes of the response body sent by WAF to the client
access_log.upstream_addr	String	Address of the backend server.	IP address of the origin server for which a request is destined. For example, if WAF forwards requests to an ECS, the IP address of the ECS is returned to this parameter.
access_log.request_time	String	Request processing time	Processing time starts when the first byte of the client is read (unit: s).
access_log.upstream_response_time	String	Backend server response time	Time the backend server responds to the WAF request (unit: s).
access_log.upstream_status	String	Backend server response code	Response status code returned by the backend server to WAF.

Field	Type	Field Description	Description
access_log.upstream_connect_time	String	Time for the origin server to establish a connection to its backend services. Unit: second.	When SSL is used, the time for the handshake process is also recorded. Time used for establishing a connection for a request. Use commas (,) to separate the time used for each request.
access_log.upstream_header_time	String	Time used by the backend server to receive the first byte of the response header. Unit: second	Response time for multiple requests. Use commas (,) to separate the time used for each response.
access_log.bind_ip	String	WAF engine back-to-source IP address.	The IP address of the NIC used by the engine for forwarding requests to the origin server. This value is not the EIP bound to the engine even if the engine forwards requests over the EIP.
access_log.group_id	String	LTS log group ID	ID of the log group for interconnecting WAF with LTS.
access_log.access_stream_id	String	Log stream ID.	ID of **access_stream** of the user in the log group identified by the **group_id** field.
access_log.engine_id	String	WAF engine ID	Unique ID of the WAF engine.
access_log.time_iso8601	String	ISO 8601 time format of logs.	-
access_log.sni	String	Domain name requested through SNI.	-
access_log.tls_version	String	Protocol versioning an SSL connection.	TLS version used in the request.

Field	Type	Field Description	Description
access_log.ssl_curves	String	Curve group list supported by the client.	-
access_log.ssl_session_reused	String	SSL session reuse	Whether the SSL session can be reused **r**: Yes **.**: No
access_log.process_time	String	Engine attack detection duration (unit: ms)	-
access_log.args	String	The parameter data in the URL	-
access_log.x_forwarded_for	String	IP address chain for a proxy when the proxy is deployed in front of WAF.	The sting includes one or more IP addresses. The leftmost IP address is the originating IP address of the client. Each time the proxy server receives a request, it adds the source IP address of the request to the right of the originating IP address.
access_log.cdn_src_ip	String	Client IP address identified by CDN when CDN is deployed in front of WAF	This field specifies the real IP address of the client if CDN is deployed in front of WAF. **NOTICE** Some CDN vendors may use other fields. WAF records only the most common fields.
access_log.x_real_ip	String	Real IP address of the client when a proxy is deployed in front of WAF.	Real IP address of the client, which is identified by the proxy.

Field	Type	Field Description	Description
access_log.intel_crawler	String	Used for intelligence anti-crawler analysis.	-
access_log.ssl_ciphers_md5	String	MD5 value of the SSL cipher (ssl_ciphers).	-
access_log.ssl_cipher	String	SSL cipher used.	-
access_log.web_tag	String	Website name.	-
access_log.user_agent	String	User agent in the request header.	-
access_log.upstream_response_length	String	Backend server response size.	-
access_log.region_id	String	Region where the request is received.	-
access_log.enterprise_project_id	String	ID of the enterprise project that the requested domain name belongs to.	-
access_log.referer	String	Referer content in the request header.	The value can contain a maximum of 128 characters. Characters over 128 characters will be truncated.
access_log.rule	String	Protection rule that the request matched.	If multiple rules are matched, only one rule is displayed.

Field	Type	Field Description	Description
access_log.category	String	Log category matched by the request.	-
access_log.waf_time	String	Time an access request is received.	-
access_log.geo	String	Mark of geographical location.	• **c**: Country name • **r**: name of a specific geographical location.

WAF attack_log Field Description

Field	Type	Field Description	Description
attack_log.category	String	Log category	The value is **attack**.
attack_log.time	String	Log time	-
attack_log.time_iso8601	String	ISO 8601 time format of logs.	-
attack_log.policy_id	String	Policy ID	-
attack_log.level	String	Protection level	Protection level of a built-in rule in basic web protection • **1**: Low • **2**: Medium • **3**: High

Field	Type	Field Description	Description
attack_log.attack	String	Type of attack	Attack type. This parameter is listed in attack logs only. • **default**: default attacks • **sqli**: SQL injections • **xss**: cross-site scripting (XSS) attacks • **webshell**: web shells • **robot**: malicious crawlers • **cmdi**: command injections • **rfi**: remote file inclusion attacks • **lfi**: local file inclusion attacks • **illegal**: unauthorized requests • **vuln**: exploits • **default_cc**: attacks that hit a default CC attack protection rule • **cc**: attacks that hit a CC protection rule • **custom_custom**: attacks that hit a precise protection rule • **custom_whiteblackip**: attacks that hit an IP address blacklist or whitelist rule • **custom_geoip**: attacks that hit a geolocation access control rule • **antitamper**: attacks that hit a web tamper protection rule • **anticrawler**: attacks that hit the JS challenge anti-crawler rule • **leakage**: vulnerabilities that hit an information leakage prevention rule • **antiscan_high_freq_scan**: attacks that hit malicious scanning rules. • **antiscan_dir_traversal**: directory scanning attacks • **custom_idc_ip**: attacks that hit a threat intelligence access control rule • **botm**: attacks that hit a bot protection rule • **followed_action**: The source is marked as a known attack source.

Field	Type	Field Description	Description
			For details, see **Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration**.
attack_log.action	String	Protective action	WAF defense action. • **block**: WAF blocks attacks. • **log**: WAF only logs detected attacks. • **captcha**: Verification code
attack_log.sub_type	String	Crawler types	When **attack** is set to **robot**, this parameter cannot be left blank. • **script_tool**: Script tools • **search_engine**: Search engines • **scanner:** Scanning tools • **uncategorized**: Other crawlers
attack_log.rule	String	ID of the triggered rule or the description of the custom policy type.	-
attack_log.rule_name	String	Description of a custom rule type.	This field is empty when a basic protection rule is matched.
attack_log.location	String	Location triggering the malicious load	-
attack_log.req_body	sting	Request body.	-
attack_log.resp_headers	String	Response header	-
attack_log.hit_data	String	String triggering the malicious load	-
attack_log.resp_body	String	Response body	-
attack_log.backend.protocol	String	Backend protocol.	-
attack_log.backend.alive	String	Backend server status.	-

Field	Type	Field Description	Description
attack_log.backend.port	String	Backend server port.	-
attack_log.backend.host	String	Backend server host value.	-
attack_log.backend.type	String	Backend server type.	IP address or domain name.
attack_log.backend.weight	number	Backend server weight.	-
attack_log.status	String	Response status code	-
attack_log.upstream_status	String	Origin server response code.	-
attack_log.reqid	String	Random ID	The value consists of the engine IP address suffix, request timestamp, and request ID allocated by Nginx.
attack_log.requestid	String	Unique ID of the request.	Request ID allocated by Nginx.
attack_log.id	String	Attack ID	ID of the attack
attack_log.method	String	Request method	-
attack_log.sip	String	Client request IP address	-
attack_log.sport	String	Client request port	-
attack_log.host	String	Requested domain name	-
attack_log.http_host	String	Domain name of the requested server.	-
attack_log.hport	String	Port of the requested server.	-
attack_log.uri	String	Request URL.	The domain is excluded.

Field	Type	Field Description	Description
attack_log.header	A JSON string. A JSON table is obtained after the string is decoded.	Request header	-
attack_log.mutipart	A JSON string. A JSON table is obtained after the string is decoded.	Request multipart header	This parameter is used to upload files.
attack_log.cookie	A JSON string. A JSON table is obtained after the string is decoded.	Cookie of the request	-

Field	Type	Field Description	Description
attack_log.params	A JSON string. A JSON table is obtained after the string is decoded.	Params value following the request URI.	-
attack_log.body_bytes_sent	String	Total number of bytes of the response body sent to the client.	Total number of bytes of the response body sent by WAF to the client.
attack_log.upstream_response_time	String	Time elapsed since the backend server received the response content from the upstream service. Unit: second.	Response time for multiple requests. Use commas (,) to separate the time used for each response.
attack_log.engine_id	String	Unique ID of the engine	-
attack_log.region_id	String	ID of the region where the engine is located.	-
attack_log.engine_ip	String	Engine IP address.	-
attack_log.process_time	String	Detection duration	-
attack_log.remote_ip	String	Layer-4 IP address of the client that sends the request.	-

Field	Type	Field Description	Description
attack_log.x_forwarded_for	String	Content of **X-Forwarded-For** in the request header.	-
attack_log.cdn_src_ip	String	Content of **Cdn-Src-Ip** in the request header.	-
attack_log.x_real_ip	String	Content of **X-Real-IP** in the request header.	-
attack_log.group_id	String	Log group ID	LTS log group ID
attack_log.attack_stream_id	String	Log stream ID	ID of **access_stream** of the user in the log group identified by the **group_id** field.
attack_log.hostid	String	Protected domain name ID (upstream_id).	-
attack_log.tenantid	String	Account ID	-
attack_log.projectid	String	ID of the project the protected domain name belongs to	-
attack_log.enterprise_project_id	String	ID of the enterprise project that the requested domain name belongs to.	-
attack_log.web_tag	String	Website name.	-
attack_log.req_body	String	Request body. (If the request body larger than 1 KB, it will be truncated.)	-

5 Configuring Protection Policies

5.1 Protection Configuration Overview

This topic walks you through how to configure WAF protection policies, how WAF engine works, and protection rule priorities.

Protection Rule Overview

After your website is connected to WAF, you need to configure a protection policy for it.

Table 5-1 Configurable protection rules

Protection Rule	Description	Reference
Basic web protection rules	With an extensive reputation database, WAF defends against Open Web Application Security Project (OWASP) top 10 threats, and detects and blocks threats, such as malicious scanners, IP addresses, and web shells.	**Configuring Basic Web Protection to Defend Against Common Web Attacks**
CC attack protection rules	CC attack protection rules can be customized to restrict access to a specific URL on your website based on a unique IP address, cookie, or referer field, mitigating CC attacks.	**Configuring CC Attack Protection Rules to Defend Against CC Attacks**
Precise protection rules	You can customize protection rules by combining HTTP headers, cookies, URLs, request parameters, and client IP addresses.	**Configuring Custom Precise Protection Rules**

Protection Rule	Description	Reference
Blacklist and whitelist rules	You can configure blacklist and whitelist rules to block, log only, or allow access requests from specified IP addresses.	**Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses**
Known attack source rules	These rules can block the IP addresses from which blocked malicious requests originate. These rules are dependent on other rules.	**Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration**
Geolocation access control rules	You can customize these rules to allow or block requests from a specific country or region.	**Configuring Geolocation Access Control Rules to Block or Allow Requests from Specific Locations**
Threat intelligence access control rules	Access control is performed based on the IP address library of the Internet Data Center (IDC).	**Configuring Threat Intelligence Access Control Rules to Block or Allow IP Addresses in a Specified IP Address Library**
Web tamper protection rules	You can configure these rules to prevent a static web page from being tampered with.	**Configuring Web Tamper Protection Rules to Prevent Static Web Pages from Being Tampered With**
Website anti-crawler protection	This function dynamically analyzes website service models and accurately identifies crawler behavior based on data risk control and bot identification systems, such as JS Challenge.	**Configuring Anti-Crawler Rules**

Protection Rule	Description	Reference
Information leakage prevention rules	You can add two types of information leakage prevention rules. • Sensitive information filtering: prevents disclosure of sensitive information (such as ID numbers, phone numbers, and email addresses). • Response code interception: blocks the specified HTTP status codes.	**Configuring Information Leakage Prevention Rules to Protect Sensitive Information from Leakage**
Global protection whitelist rules	You can configure these rules to let WAF ignore certain rules for specific requests.	**Configuring a Global Protection Whitelist Rule to Ignore False Alarms**
Data masking rules	You can configure data masking rules to prevent sensitive data such as passwords from being displayed in event logs.	**Configuring Data Masking Rules to Prevent Privacy Information Leakage**
Scanning protection rules	The scanning protection module identifies scanning behaviors and scanner features to prevent attackers or scanners from scanning websites at scale. WAF will automatically block heavy traffic web attacks and directory traversal attacks and block the source IP addresses for a period of time, helping reduce intrusion risks and junk traffic.	**Configuring a Scanning Blocking Rule to Automatically Block Heavy-Traffic Attacks**

Protection Rule	Description	Reference
Bot rules	Supports detection of known bots, signature-based requests, and bot behavior. With such layered bot detection, WAF can accurately identify and manage bot behavior in website traffic, effectively reducing risks such as data leakage and performance deterioration caused by bot attacks.	**Configuring Bot Protection Rules to Defend Against Bot Behavior**

WAF Rule Priorities

The built-in protection rules of WAF help you defend against common web application attacks, including XSS attacks, SQL injection, crawlers, and web shells. You can customize protection rules to let WAF better protect your website services using these custom rules. **Figure 5-1** shows how WAF engine built-in protection rules work. **Figure 5-2** shows the detection sequence of rules you configured.

NOTE

On the protection configuration page, select **Sort by check sequence**. All protection rules will be displayed by the WAF check sequence.

Figure 5-1 WAF engine work process

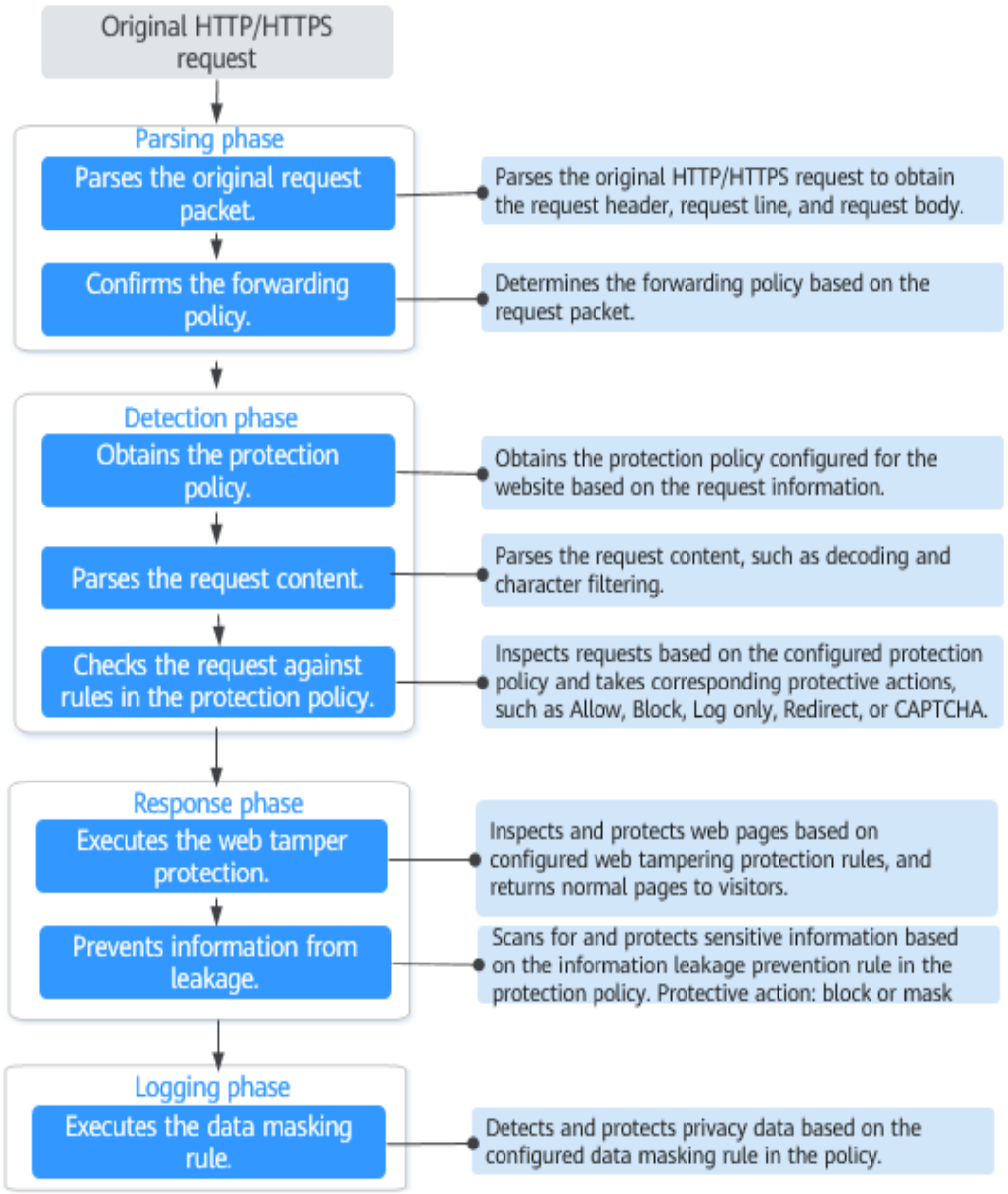
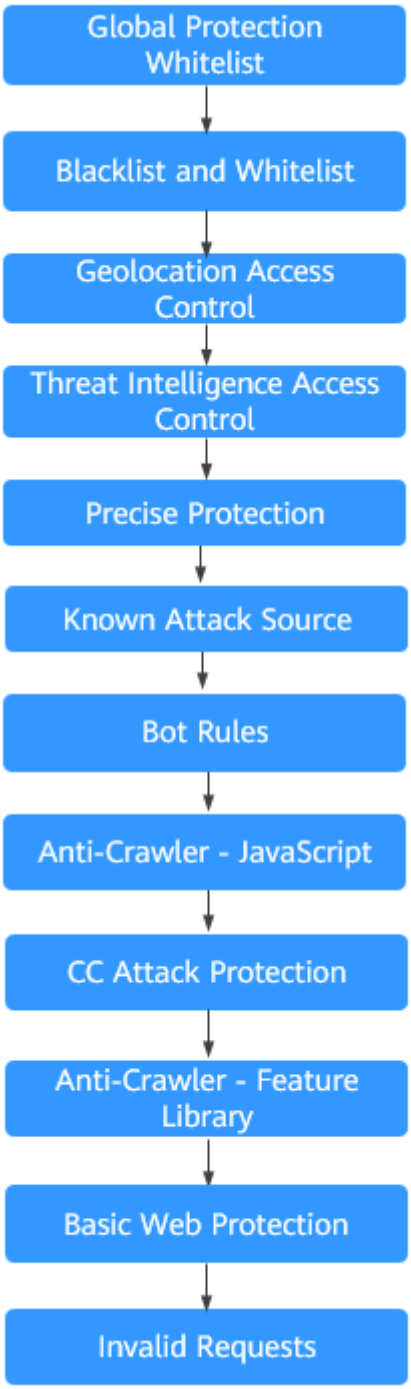


Figure 5-2 Priorities of protection rules



Response actions

- Pass: The current request is unconditionally permitted after a protection rule is matched.
- Block: The current request is blocked after a rule is matched.
- CAPTCHA: The system will perform human-machine verification after a rule is matched.

- Redirect: The system will notify you to redirect the request after a rule is matched.
- Log: Only attack information is recorded when a rule is matched.
- Mask: The system will anonymize sensitive information after a rule is matched.

Tutorial Video

This video introduces core functions and advanced protection capabilities of WAF.

5.2 Configuring Basic Web Protection to Defend Against Common Web Attacks

After this function is enabled, WAF can defend against common web attacks, such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections. You can also enable other checks in basic web protection, such as web shell detection, deep inspection against evasion attacks, and header inspection.

Suggestions

- If you are not clear about your service traffic characteristics, you are advised to switch to the **Log only** mode first and observe the WAF protection for a period of time. Generally, you need to observe service running for one to two weeks, and then analyze the attack logs.
  - If no record of blocking legitimate requests is found, switch to the **Block** mode.
  - If legitimate requests are blocked, adjust the protection level or configure global protection whitelist rules to prevent legitimate requests from being blocked.
- Note the following points in your operations:
  - Do not transfer the original SQL statement or JavaScript code in a legitimate HTTP request.
  - Do not use special keywords (such as UPDATE and SET) in a legitimate URL. For example, **https://www.example.com/abc/update/mod.php?set=1**.
  - Use Object Storage Service (OBS) or other secure methods to upload files that exceed 50 MB rather than via a web browser.

Prerequisites

- You have added the website you want to protect to WAF or **added a protection policy**.
  - For cloud CNAME access mode, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)**.
  - For cloud load balancer access mode, see **Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)**.

  - For dedicated mode, see **Connecting Your Website to WAF (Dedicated Mode)**.
- If you use a dedicated WAF instance, ensure that it has been upgraded to the latest version. For details, see **Managing Dedicated WAF Engines**.

Constraints

- Basic web protection has two modes: **Block** and **Log only**.
- If you select **Block** for **Basic Web Protection**, you can **configure access control criteria for a known attack source**. WAF will block requests matching the configured IP address, cookie, or params for a length of time configured as part of the rule.
- Currently, Shiro decryption detection is not available in regions CN East-Qingdao and AP-Manila.
- HTTP/2 packets do not support web shell detection.

Enabling Basic Web Protection Rules

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

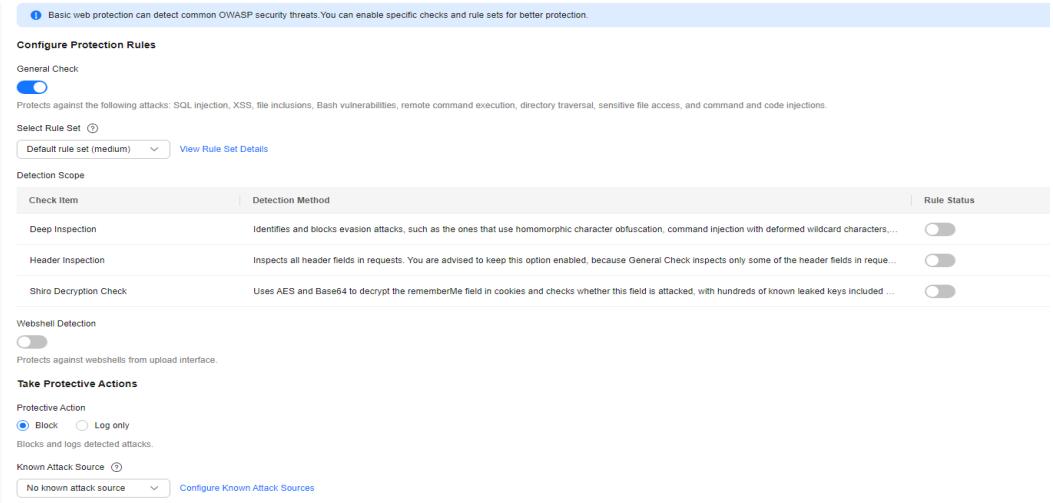
Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Click the **Basic Web Protection** configuration area and toggle it on or off if needed.

-  : enabled.
-  : disabled.

Step 8 Configure a basic web protection rule, as shown in **Figure 5-3**.

Figure 5-3 Rule Configuration



1. **General Check** is enabled by default. WAF defends against attacks such as SQL injections, XSS, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections. SQL injection attacks are mainly detected based on semantics.
2. Select a protection level.

   There are three protection levels: **Default rule set (loose)**, **Default rule set (medium)**, and **Default rule set (tight)**. **Default rule set (medium)** is selected by default.

   Table 5-2 Protection levels

Protection Level	Description
Default rule set (loose)	WAF only blocks the requests with obvious attack signatures. If a large number of false alarms are reported, the loose one is recommended.
Default rule set (medium)	This one is selected by default. It meets a majority of web protection requirements.
Default rule set (tight)	At this level, WAF provides the finest granular protection and can intercept attacks with complex bypass features, such as Jolokia cyber attacks, common gateway interface (CGI) vulnerability detection, and Druid SQL injection attacks. To let WAF defend against more attacks but make minimum effect on normal requests, observe your workloads for a period of time first. Then, configure a global protection whitelist rule and select the tight level.

Click **View Rule Set Details** to view details about all basic web protection rules. You can know which rules are loose, which are medium, and which are tight.

NOTE

Click to search for a rule by **CVE ID**, **Risk Severity**, **Application Type**, or **Protection Type**.

Table 5-3 Protection rule description

Parameter	Description
Rule ID	The protection rule ID, which is generated automatically.
Rule Description	Details of attacks the protection rule is configured for.
CVE ID	Common Vulnerabilities & Exposures (CVE) ID, which corresponds to the protection rule. For non-CVE vulnerabilities, a double dash (--) is displayed.
Risk Severity	The severity of the vulnerability, including: – High – Medium – Low
Application Type	The application type the protection rule is used for. For details about applications types WAF can protect, see **Application Types WAF Can Protect**.
Protection Type	The type of the protection rule. WAF can discover SQL injection, command injection, XSS attacks, XML external entity (XXE) injection, Expression Language (EL) Injection, SSRF, local file inclusion, remote file inclusion, website Trojans, malicious crawlers, session fixation attacks, deserialization vulnerabilities, remote command execution, information leakage, DoS attacks, source code/data leakage.

3. Enable the check items in **Detection Scope** based on service requirements.

Table 5-4 Check item description

Type	Description
Deep Inspection	Identifies and blocks evasion attacks, such as the ones that use homomorphic character obfuscation, command injection with deformed wildcard characters, UTF7, data URI scheme, and other techniques. **NOTE** If you enable **Deep Inspection**, WAF detects and defends against evasion attacks in depth.

Type	Description
Header Inspection	This function is disabled by default. When it is disabled, General Check will check some of the header fields, such as User-Agent, Content-type, Accept-Language, and Cookie. **NOTE** If you enable this function, WAF checks all header fields in the requests.
Shiro Decryption Check	This function is disabled by default. After this function is enabled, WAF uses AES and Base64 to decrypt the rememberMe field in cookies and checks whether this field is attacked. There are hundreds of known leaked keys included and checked for. **NOTE** If your website uses Shiro 1.2.4 or earlier, or your website uses Shiro 1.2.5 or later but no AES keys are not configured, it is strongly recommended that you enable Shiro decryption detection to prevent attackers from using leaked keys to construct attacks.

4. Configure **Webshell Detection**.

   If you enable **Webshell Detection**, WAF detects web page Trojan horses inserted through the upload interface.

   NOTE

   HTTP/2 packets do not support web shell detection.

Step 9 Configure a protective action. You can select:

- **Block**: WAF blocks and logs detected attacks.

  If you select **Block**, you can select a known attack source rule to let WAF block requests accordingly. For details, see **Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration**.
- **Log only**: WAF only logs detected attacks.

----End

Protection Verification

To verify that WAF is protecting your website (**www.example.com**) based on basic web protection (with **General Check** enabled and **Mode** set to **Block**), take the following steps:

Step 1 Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

- If the website is inaccessible, connect the website domain name to WAF by following the instructions in **Website Settings**.
- If the website is accessible, go to **Step 2**.

Step 2 Clear the browser cache and enter **http://www.example.com?id=1%27%20or%201=1** in the address box of the browser to simulate an SQL injection attack.

Step 3 Return to the WAF console. In the navigation pane on the left, click **Events**. On the displayed page, check event logs.

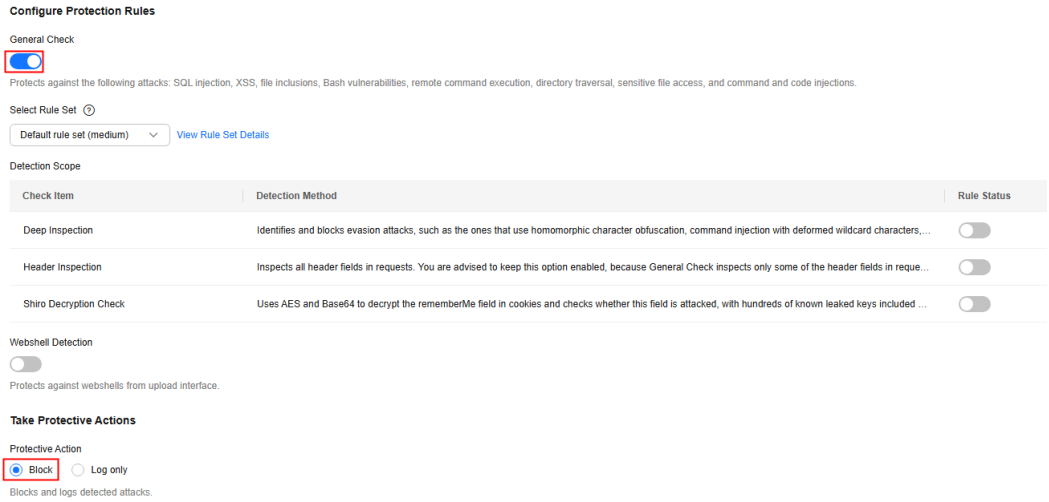
----End

Configuration Example - Blocking SQL Injection Attacks

If domain name **www.example.com** has been connected to WAF, perform the following steps to verify that WAF can block SQL injection attacks.

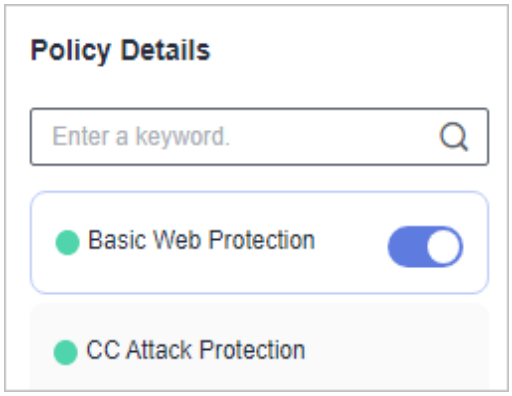
Step 1 Enable **General Check** in **Basic Web Protection** and set the protection mode to **Block**.

Figure 5-4 Enabling General Check



Step 2 Enable WAF basic web protection.

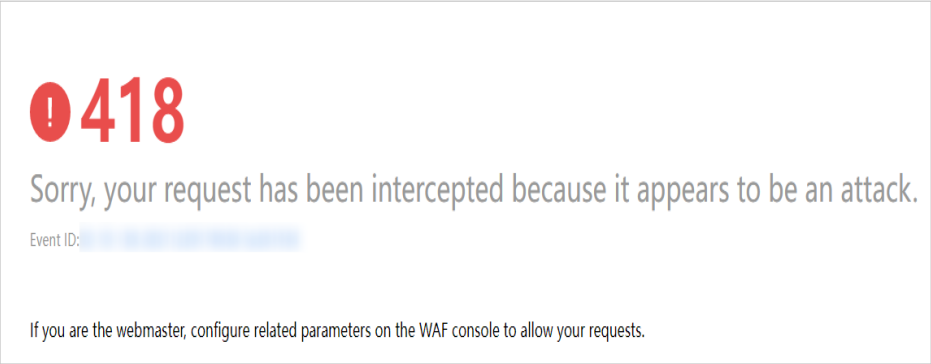
Figure 5-5 Basic Web Protection configuration area



Step 3 Clear the browser cache and enter a simulated SQL injection (for example, http://www.example.com?id=' or 1=1) in the address box.

WAF blocks the access request. **Figure 5-6** shows an example block page.

Figure 5-6 Block page



Step 4 Go to the WAF console. In the navigation pane on the left, choose **Events**. View the event on the **Events** page.

----End

5.3 Configuring CC Attack Protection Rules to Defend Against CC Attacks

CC attack protection can limit the access to a protected website based on a single IP address, cookie, or referer. Beyond that, CC attack protection can also limit access rate based on policies, domain names, and URLs to precisely mitigate CC attacks. In policy-based rate limiting, the number of requests for all domain names in the same policy are counted for triggering the rule. In domain-based rate limiting, the total number of requests for each domain name is counted separately for triggering the rule. In URL-based rate limiting, the number of requests for each URL is counted separately for triggering the rule. To use this protection, ensure that you have toggled on **CC Attack Protection** ( ).

A reference table can be added to a CC attack protection rule. The reference table takes effect for all protected domain names.

Prerequisites

- You have added the website you want to protect to WAF or **added a protection policy**.
  - For cloud CNAME access mode, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)**.
  - For cloud load balancer access mode, see **Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)**.
  - For dedicated mode, see **Connecting Your Website to WAF (Dedicated Mode)**.
- If you use a dedicated WAF instance, ensure that it has been upgraded to the latest version. For details, see **Managing Dedicated WAF Engines**.

Constraints

- Managing reference tables is not supported in the standard edition cloud WAF.
- If you set **Logic** to **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any of them**, **Suffix is any value**, or **Suffix is not any of them**, select an existing reference table. For details, see **Creating a Reference Table to Configure Protection Metrics in Batches**.
- Counting requests to **All WAF instances** is only supported by cloud CNAME access mode.

  NOTE

  In the CN East-Shanghai1 or CN North-Ulanqab1 region, you need to **submit a service ticket** to enable **All WAF instances** for all dedicated WAF instances.
- If you are using a cloud WAF edition and your website uses proxies such as anti-DDoS, Content Delivery Network (CDN), and cloud acceleration services, select **Source** for **Rate Limit Mode** and then **Per user** and enable **All WAF instances**.

  NOTE

  If a website has used other proxy services, such as CDN and advanced anti-DDoS in front of WAF, the access requests to WAF will be distributed to each WAF instance for traffic forwarding. By default, WAF counts requests on each WAF instance separately. To set a proper rate limit frequency, follow the following principles:

  - Cloud mode - CNAME access: This mode supports counting requests to **All WAF instances**. That means WAF aggregates requests to all WAF nodes for rate limiting. You can just enable this function during configuration.
  - Dedicated mode:
    - Generally, this mode does not support global counting for all WAF instances. The **Rate Limit** can be set to the maximum access requests allowed for a website visitor divided by the number of WAF instances used to protect the website.

      For example, if you use two WAF dedicated instances to protect you website, and want to limit the requests for a single web visitor to no more than 1,000, set **Rate Limit** to **500**, which is obtained by dividing 1,000 by 2.
    - This mode supports **All WAF instances**. If you want to enable this function, **submit a service ticket**. Before using this function, note that the global counting (**All WAF instances**) is not an accurate rate limit. In some cases, a delay may occur as it may take several seconds for the internal counter to update. Due to this type of delay, part of requests exceeding the threshold may still reach the origin server before WAF protective actions (such as block) work.
- The **Response Code**, **Response Length**, **Response Time**, **Response Header**, and **Response Body** fields are not supported by the **Cloud Mode - Load balancer** access mode. In the **Cloud Mode - CNAME** access mode, response fields are supported only by WAF enterprise edition.
- It takes several minutes for a new rule to take effect. After a rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- For the same rule, only one CC attack log is generated every minute for requests sharing the same attributes as defined in the rate limiting type.

Configuring a CC Attack Protection Rule

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Click the **CC Attack Protection** configuration area and toggle it on or off if needed.

-  : enabled.
-  : disabled.

Step 8 In the upper left corner above the **CC Attack Protection** rule list, click **Add Rule**.

Step 9 In the displayed dialog box, configure a CC attack protection rule by referring to Table 5-5.

For example, you can configure a CC attack protection rule to block requests from a visit for 600 seconds by identifying their cookie (name field) if the visitor accessed a URL (for example, /admin*) of your website over 10 times within 60 seconds.

Figure 5-7 Adding a CC attack protection rule

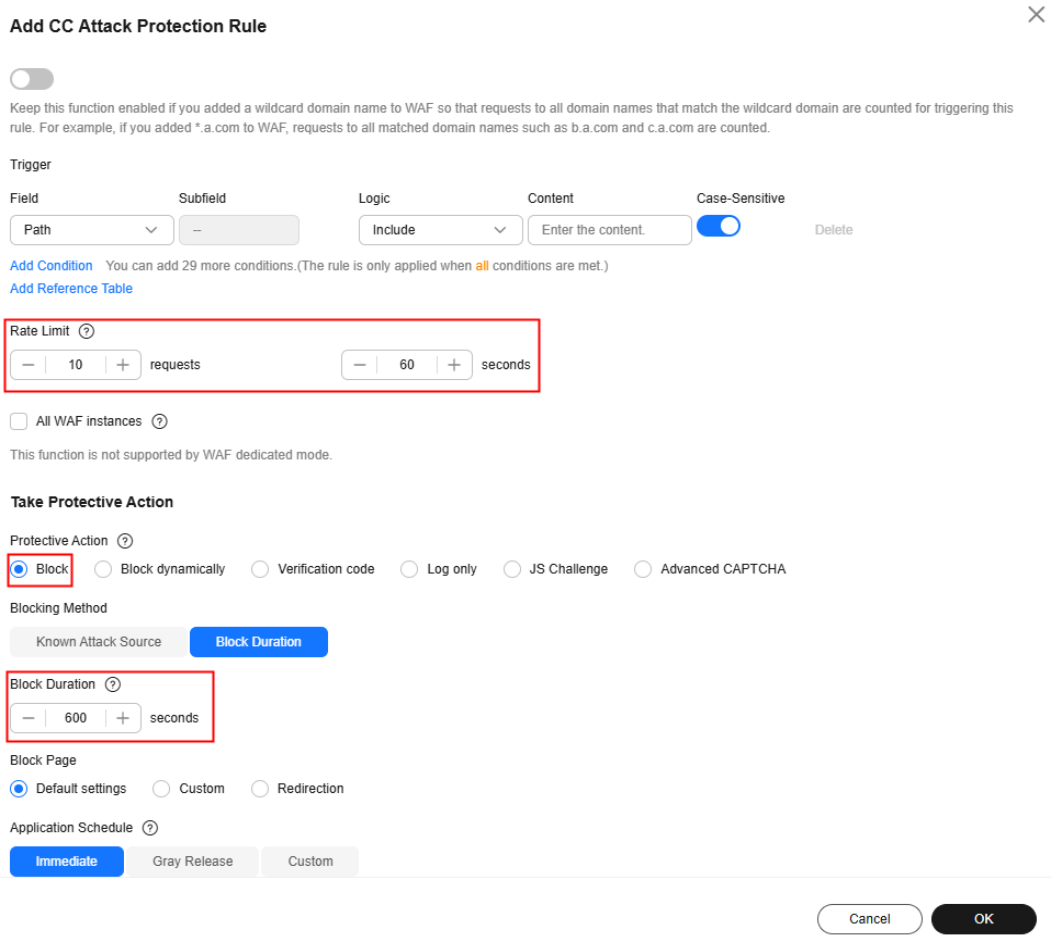


Table 5-5 Rule parameters

Parameter	Description	Example Value
Rule Name	Name of the rule.	waftest
Rule Description	A brief description of the rule. This parameter is optional.	--

Parameter	Description	Example Value
Rate Limit Mode	• **Source**: Requests from a specific source are limited. For example, if traffic from an IP address (or user) exceeds the rate limit you configure in this rule, WAF limits traffic rate of the IP address (or user) in the way you configure. – **Per IP address**: A website visitor is identified by the IP address. – **Per user**: A website visitor is identified by the key value of **Cookie** or **Header**. – **Other**: A website visitor is identified by the Referer field (user-defined request source). **NOTE** If you set **Rate Limit Mode** to **Other**, set **Content** of **Referer** to a complete URL containing the domain name. The **Content** field supports prefix match and exact match only, but cannot contain two or more consecutive slashes, for example, **///admin**. If you enter **///admin**, WAF will convert it to **/admin**. For example, if you do not want visitors to access www.test.com, set **Referer** to **http://www.test.com**. • **Destination**: If this parameter is selected, the following rate limit types are available: – **By rule**: If this rule is used by multiple domain names, requests for all these domain names are counted for this rule no matter what IP addresses these requests originate from. If you have added a wildcard domain name to WAF, requests to all domain names matched the wildcard domain name are counted for triggering this rule no matter what IP addresses these requests originate from. – **By domain name**: Requests for each domain name are counted separately. If the number exceeds the threshold you configure, the protective action is triggered no matter what IP addresses these requests originate from.	--

Parameter	Description	Example Value
	– **By URL**: Requests for each URL are counted separately. If the number exceeds the threshold you configure, the protective action is triggered no matter what IP addresses these requests originate from.	
User Identifier	This parameter is mandatory when you select **Source** and **Per user** for **Rate Limit Mode**. • **Cookie**: A cookie field name. You need to configure an attribute variable name in the cookie that can uniquely identify a web visitor based on your website requirements. This field does not support regular expressions. Only complete matches are supported. For example, if a website uses the **name** field in the cookie to uniquely identify a web visitor, enter **name**. • **Header**: Set the user-defined HTTP header you want to protect. You need to configure the HTTP header that can identify web visitors based on your website requirements.	name
Request Aggregation	This parameter is not required when you select **Destination** and **By rule** for **Rate Limit Mode**. This function is disabled by default. Keep this function enabled so that requests to all domain names that match a protected wildcard domain are counted for triggering this rule. For example, if you added *.a.com to WAF, requests to all matched domain names such as b.a.com and c.a.com are counted.	--

Parameter	Description	Example Value
Trigger	The request features to be matched by the rule. If a request matches the features, WAF handles the request according to the configured rule. • At least one condition is required for the rule to take effect. If multiple conditions are configured, the rule takes effect only when all conditions are met. • Click **Add Condition** to add a condition. You can add up to 30 conditions. • You can add a rate limit condition group. This function is under open beta test (OBT). You can **submit a service ticket** to enable it. – How a condition group takes effect: A condition group takes effect as long as one of the conditions in the group is met. Click **Add Condition** and add a rate limit condition in the group. – How condition groups take effect: ▪ **and**: The combination of an and group takes effect when all AND groups are met. You can click **Add and Group** to add an AND group. ▪ **or**: The combination of an OR group takes effect as long as one group is met. You can click **Add or Group** to add an OR group. Condition parameter description: • **Field**: For details, see **Condition Field Description**. • **Subfield**: Configure this field only when **IPv4**, **IPv6**, **Cookie**, **Header**, or **Params** is selected for **Field**. **NOTICE** A subfield cannot exceed 2,048 characters. • **Logic**: Select a logical relationship from the drop-down list.	**Field**: Set to **Path**. **Logic**: Set to **Include**. **Content**: Set to **/admin/**.

Parameter	Description	Example Value
	NOTE If you set **Logic** to **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any of them**, **Suffix is any value**, or **Suffix is not any of them**, select an existing reference table. For details, see **Creating a Reference Table to Configure Protection Metrics in Batches**. • **Content**: Enter or select the content that matches the condition. • **Case Sensitive**: If **Field** is set to **Path**, **User Agent**, **Params**, **Cookie**, **Referer**, **Header**, **Response Header**, or **Response Body**, you can enable case-sensitive matching for conditions. If you enable this, the system matches the case-sensitive content. It helps the system precisely identify requests and respond to them accurately, making protection policies work better.	

Parameter	Description	Example Value
Rate Limit	The number of requests allowed from a website visitor in the rate limit period. If the number of requests exceeds the rate limit, WAF takes the action you configure for **Protective Action**. **All WAF instances**: Requests to one or more WAF instances will be counted together according to the rate limit mode you select. By default, requests to each WAF instance are counted. If you enable this, WAF will count requests to all your WAF instances for triggering this rule. To enable user-based rate limiting, **Per user** or **Other** (**Referer** must be configured) instead of **Per IP address** must be selected for **Rate Limit Mode**. This is because IP address-based rate limiting cannot limit the access rate of a specific user. However, in user-based rate limiting, requests may be forwarded to one or more WAF instances. So **All WAF instances** must be enabled for triggering the rule precisely.	**10** requests allowed in **60** seconds

Parameter	Description	Example Value
	NOTE If a website has used other proxy services, such as CDN and advanced anti-DDoS in front of WAF, the access requests to WAF will be distributed to each WAF instance for traffic forwarding. By default, WAF counts requests on each WAF instance separately. To set a proper rate limit frequency, follow the following principles: • Cloud mode - CNAME access: This mode supports counting requests to **All WAF instances**. That means WAF aggregates requests to all WAF nodes for rate limiting. You can just enable this function during configuration. • Dedicated mode: – Generally, this mode does not support global counting for all WAF instances. The **Rate Limit** can be set to the maximum access requests allowed for a website visitor divided by the number of WAF instances used to protect the website. For example, if you use two WAF dedicated instances to protect you website, and want to limit the requests for a single web visitor to no more than 1,000, set **Rate Limit** to **500**, which is obtained by dividing 1,000 by 2. – This mode supports **All WAF instances**. If you want to enable this function, **submit a service ticket**. Before using this function, note that the global counting (**All WAF instances**) is not an accurate rate limit. In some cases, a delay may occur as it may take several seconds for the internal counter to update. Due to this type of delay, part of requests exceeding the threshold may still reach the origin server before WAF protective actions (such as block) work.	

Parameter	Description	Example Value
Protective Action	The action that WAF will take if the number of requests exceeds **Rate Limit** you configured. The options are as follows: • **Verification code**: WAF allows requests that trigger the rule as long as your website visitors complete the required verification. **NOTE** The cloud load balancer access mode does not support this protective action. • **Block**: WAF blocks requests that trigger **Rate Limit** set in the rule. • **Block dynamically**: WAF blocks requests that trigger the rule based on **Allowable Frequency**, which you configure after the first rate limit period is over. • **Log only**: WAF only logs requests that trigger **Rate Limit** set in the rule. • **JS Challenge**: WAF returns a piece of JavaScript code that can be automatically executed by a normal browser to the client. If the client properly executes the JavaScript code, WAF allows all requests from the client within a period of time (30 minutes by default). During this period, no verification is required. If the client fails to execute the code, WAF blocks the requests. **NOTE** – The cloud load balancer access mode does not support this protective action. – If the referer in the request is different from the current host, the JS challenge does not work. • **Advanced CAPTCHA**: If your website visitor triggers **Rate Limit** you set, CAPTCHA verification is required. If the verification is successful, the request is allowed within the validity period. If the verification fails, the CAPTCHA code is updated and the verification is required again. Compared with verification code, advanced CAPTCHA provides better experience and is more secure.	Block

Parameter	Description	Example Value
	NOTE – The cloud load balancer access mode does not support this protective action. – If you want to select **Advanced CAPTCHA** for **Protective Action**, make sure requests from a client IP address are forwarded to one WAF engine, or the authentication will fail due to repeated authentications. – After a successful verification, the client obtains a token, which grants access to all requests within its validity period. To prevent replay attacks, you can configure a policy to block requests exceeding a specified threshold.	
Token Lifespan	If **Protective Action** is set to **JS challenge** or **Advanced CAPTCHA**, the default validity period of a token is 1,800s. You can set it to a value ranging from 60 to 86,400 seconds.	60s
Application Schedule **NOTE** Periodic and gray application schedules are under OBT now. You need to **submit a service ticket** to enable them.	• **Immediate**: The rule works immediately after it is enabled. • **Periodic**: You can specify a time range in a time zone to let the rule work at the time range every day. • **Gray release**: In the specified period, the probability that client requests trigger the rule increases linearly from 0% to 100%. • **Custom**: You can select a time range for the rule to work.	Immediate
Allowable Frequency	This parameter can be set if you select **Block dynamically** for **Protective Action**. WAF blocks requests that trigger the rule based on **Rate Limit** first. Then, in the following rate limit period, WAF blocks requests that trigger the rule based on **Allowable Frequency** you configure. **Allowable Frequency** cannot be larger than **Rate Limit**. **NOTE** If you set **Allowable Frequency** to **0**, WAF blocks all requests that trigger the rule in the next rate limit period.	**8** requests allowed in **60** seconds

Parameter	Description	Example Value
Block Method	If **Protective Action** is set to **Block**, two blocking methods are available. • **Known Attack Source**: WAF will block requests matching the configured IP address, Cookie, or Params for a length of time configured as part of the rule. WAF supports one-click unblocking of known attack sources. For details, see **One-Click Unblocking a Known Attack Source Rule**. • **Block Duration**: how long you want WAF to block the requests hit the rule.	Block Duration
Block Duration	Period of time for which to block the item when you set **Protective Action** to **Block**.	**600** seconds
Block Page	The page displayed if the request limit has been reached. This parameter is configured only when **Protective Action** is set to **Block**. • If you select **Default settings**, the default block page is displayed. • If you select **Custom**, you can write a custom error message, so that WAF will return this message to website visitors when their requests are blocked. • To configure a redirection URL, select **Redirection**.	Custom
HTTP Return Code	HTTP return codes can be configured when **Block Page** is set to **Custom**.	418
Response Header	Response headers can be configured when **Block Page** is set to **Custom**. Click **Add Response Header Field** and configure response header parameters.	-
Block Page Type	If you select **Custom** for **Block Page**, select a type of the block page among options **application/json**, **text/html**, and **text/xml**.	text/html

Parameter	Description	Example Value
Page Content	If you select **Custom** for **Block Page**, configure the content to be returned.	Page content styles corresponding to different page types are as follows: • **text/html**: <html><body>Forbidden</body></html> • **application/json**: {"msg": "Forbidden"} • **text/xml**: <?xml version="1.0" encoding="utf-8"?><error><msg>Forbidden</msg></error>

Step 10 Click **OK**. You can then view the added CC attack protection rule in the CC rule list.

- After the configuration is complete, you can view the added rule in the protection rule list. **Rule Status** is **Enabled** by default.
- If you do not want the rule to take effect, click **Disable** in the **Operation** column of the rule.
- To delete a rule you no longer need, click **Delete** in the **Operation** column of the rule.
- To modify or copy a rule, click **More** > **Modify** or **More** > **Copy** in the **Operation** column of the target rule, respectively.

----End

Protection Verification

If you have configured a CC attack protection rule as required in **Figure 5-7** (with **Protective Action** set to **Block**) by referring to **Table 5-5** for your domain name **www.example.com**, take the following steps to verify the protection effect:

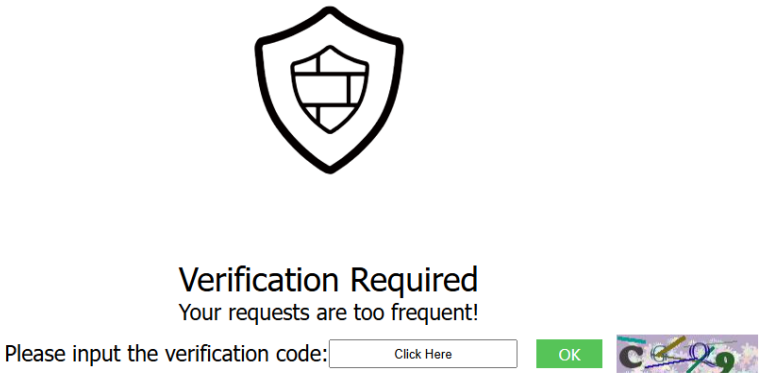
Step 1 Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

- If the website is inaccessible, connect the website domain name to WAF by following the instructions in **Website Settings**.
- If the website is accessible, go to **Step 2**.

Step 2 Clear the browser cache, enter **http://www.example.com/admin** in the address bar, and refresh the page 10 times within 60 seconds. In normal cases, the custom block page will be displayed the eleventh time you refresh the page, and the requested page will be accessible when you refresh the page 60 seconds later.

If you select **Verification code** for protective action, a verification code is required for visitors to continue the access if they exceed the configured rate limit.

Figure 5-8 Verification code



Step 3 Return to the WAF console. In the navigation pane on the left, click **Events**. On the displayed page, check event logs.

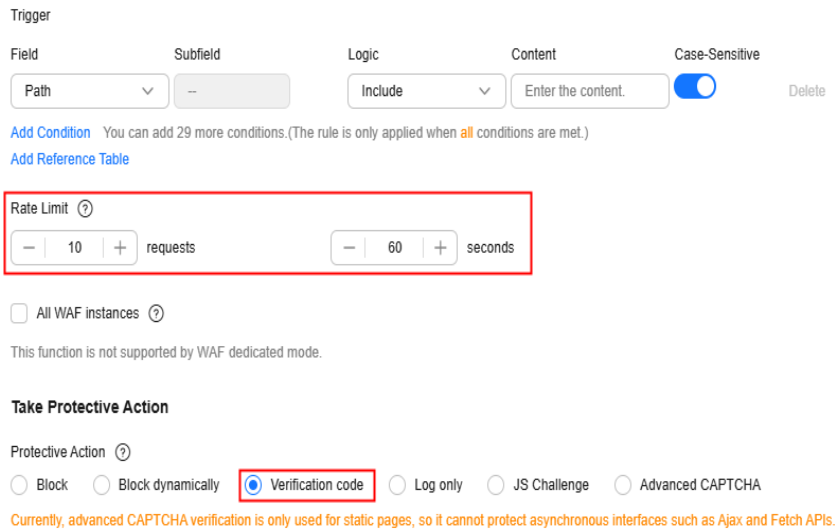
----End

Configuration Example - Verification Code

You can take the following steps to verify that CAPTCHA verification is enabled for your website (**www.example.com**) protected by WAF.

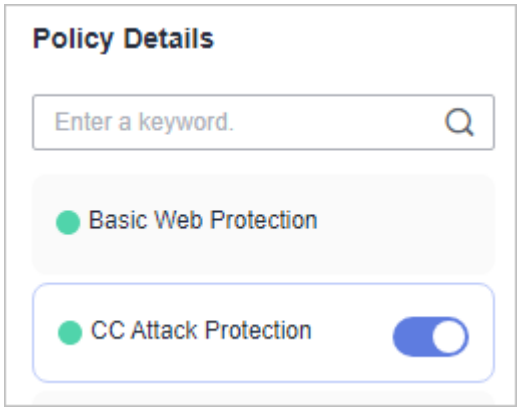
Step 1 Add a CC attack protection rule with **Protection Action** set to **Verification code**.

Figure 5-9 Verification code



Step 2 Enable CC attack protection.

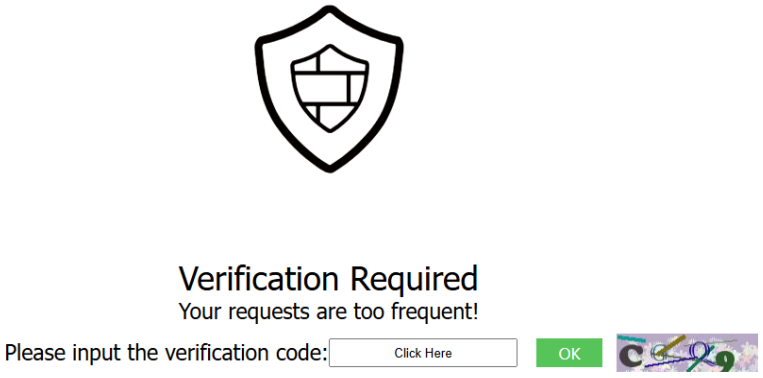
Figure 5-10 Enabling CC Attack Protection



Step 3 Clear the browser cache and access http://www.example.com/admin/.

If you access the page 10 times within 60 seconds, a verification code is required when you attempt to access the page for the eleventh time. You need to enter the verification code to continue the access.

Figure 5-11 Verification code



Step 4 Go to the WAF console. In the navigation pane on the left, choose **Events**. View the event on the **Events** page.

----End

FAQs

Why Cannot the Verification Code Be Refreshed When Verification Code Is Configured in a CC Attack Protection Rule?

5.4 Configuring Custom Precise Protection Rules

You can combine common HTTP fields, such as **IP**, **Path**, **Referer**, **User Agent**, and **Params** in a protection rule to let WAF allow, block, or only log the requests that match the combined conditions. In addition, **JavaScript challenge** verification is supported. WAF returns a piece of JavaScript code that can be automatically executed by a normal browser to the client. If the client properly executes JavaScript code, WAF allows all requests from the client within a period of time

(30 minutes by default). During this period, no verification is required. If the client fails to execute the code, WAF blocks the requests.

A reference table can be added to a precise protection rule. The reference table takes effect for all protected domain names.

Prerequisites

- You have added the website you want to protect to WAF or **added a protection policy**.
  - For cloud CNAME access mode, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)**.
  - For cloud load balancer access mode, see **Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)**.
  - For dedicated mode, see **Connecting Your Website to WAF (Dedicated Mode)**.
- If you use a dedicated WAF instance, ensure that it has been upgraded to the latest version. For details, see **Managing Dedicated WAF Engines**.

Constraints

- **Full Detection** is not included in the WAF standard edition or cloud WAF billed on a pay-per-use basis.
- The reference table function is not included in the WAF standard edition or cloud WAF billed on a pay-per-use basis.
- The **Response Code**, **Response Length**, **Response Time**, **Response Header**, and **Response Body** fields are not supported by the **Cloud Mode - Load balancer** access mode. In the **Cloud Mode - CNAME** access mode, response fields are supported only by WAF enterprise edition.
- If you configure **Protective Action** to **Block** for a precise protection rule, you can configure a known attack source rule by referring to **Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration**. WAF will block requests matching the configured IP address, Cookie, or Params for a length of time configured as part of the rule.
- The path content cannot contain the following special characters: (<>*)
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- With dedicated mode, if a layer-7 reverse proxy (for example, ELB load balancer) is deployed in front of WAF and the reverse proxy's fingerprints are transferred to WAF with request headers, you need to **configure JA3/JA4 fingerprint tags** for the protected domain name, or the rule with **Condition** set to **TLS fingerprint (JA3)** or **TLS fingerprint (JA4)** cannot work.

Application Scenarios

Precise protection rules are used for anti-leeching and website management background protection.

Configuring a Precise Protection Rule

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Click the **Precise Protection** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

Step 8 On the **Precise Protection** page, set **Detection Mode**.

Two detection modes are available:

- **Instant detection**: If a request matches a configured precise protection rule, WAF immediately ends threat detection and blocks the request.
- **Full detection**: If a request matches a configured precise protection rule, WAF finishes its scan first and then blocks all requests that match the configured precise protection rule.

Step 9 In the upper left corner above the **Precise Protection** rule list, click **Add Rule**.

Step 10 In the displayed dialog box, add a rule by referring to **Table 5-6**.

The settings shown in **Figure 5-12** are used as an example. If a visitor tries to access a URL containing **/admin**, WAF will block the request.

NOTICE

To ensure that WAF blocks only attack requests, configure **Protective Action** to **Log only** first and check whether normal requests are blocked on the **Events** page. If no normal requests are blocked, configure **Protective Action** to **Block**.

Figure 5-12 Add Precise Protection Rule

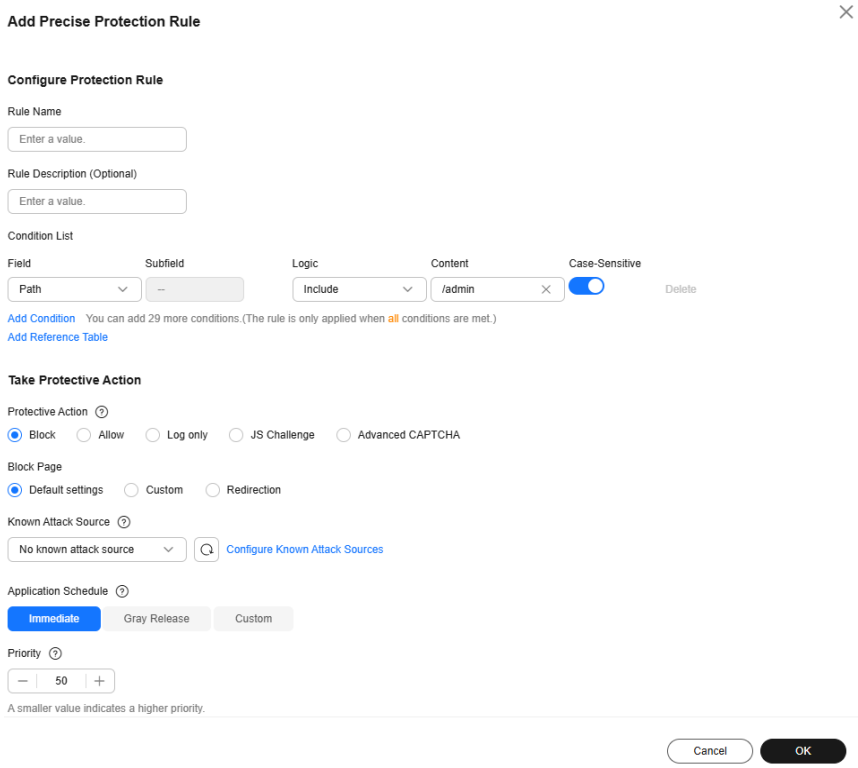


Table 5-6 Rule parameters

Parameter	Description	Example Value
Rule Name	Name of the rule.	waftest
Rule Description	A brief description of the rule. This parameter is optional.	None

Parameter	Description	Example Value
Condition List	The request features to be matched by the rule. If a request matches the features, WAF handles the request according to the configured rule. • At least one condition is required for the rule to take effect. If multiple conditions are configured, the rule takes effect only when all conditions are met. • Click **Add Condition** to add a condition. You can add up to 30 conditions. • You can add a rate limit condition group. This function is under open beta test (OBT). You can **submit a service ticket** to enable it. – How a condition group takes effect: A condition group takes effect as long as one of the conditions in the group is met. Click **Add Condition** and add a rate limit condition in the group. – How condition groups take effect: ▪ **and**: The combination of an and group takes effect when all AND groups are met. You can click **Add and Group** to add an AND group. ▪ **or**: The combination of an OR group takes effect as long as one group is met. You can click **Add or Group** to add an OR group. Condition parameter description: • **Field** With dedicated mode, if a layer-7 reverse proxy (for example, ELB load balancer) is deployed in front of WAF and the reverse proxy's fingerprints are transferred to WAF with request headers, you need to **configure JA3/JA4 fingerprint tags** for the protected domain name, or the rule with **Condition**	• **Field** is set **Path**, **Logic** to **Include**, and **Content** to **/admin/**. • **Field** is set to **User Agent**, **Logic** to **Prefix is not**, and **Content** to **mozilla/5.0**. • **Field** is set to **IP**, **Logic** to **Equal**, and **Content** to **192.168.2.3**. • **Field** is set to **Cookie[key1]**, **Logic** to **Prefix is not**, and **Content** to **jsessionid**.

Parameter	Description	Example Value
	set to **TLS fingerprint (JA3)** or **TLS fingerprint (JA4)** cannot work. • **Subfield**: Configure this field only when **IPv4**, **IPv6**, **Params**, **Cookie**, **Response Header**, or **Header** is selected for **Field**. If **Field** is set to **Response Header** or **Header**, and **Subfield** is not **All** or **Any**, **Case Sensitive** is supported. **NOTICE** A subfield cannot exceed 2,048 characters. • **Logic**: Select a logical relationship from the drop-down list. **NOTE** – If **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any of them**, **Suffix is any value**, or **Suffix is not any of them** is selected, select an existing reference table in the **Content** drop-down list. For details, see **Creating a Reference Table to Configure Protection Metrics in Batches**. – **Exclude any value**, **Not equal to any value**, **Prefix is not any of them**, and **Suffix is not any of them** indicates, respectively, that WAF takes the protective action (**Block**, **Allow**, or **Log only**) when the field in an access request does not contain, is not equal to, or the prefix or suffix is not any value set in the reference table. For example, assume that **Path** field is set to **Exclude any value** and the **test** reference table is selected. If *test1*, *test2*, and *test3* are set in the **test** reference table, WAF performs the protection action when the path of the access request does not contain *test1*, *test2*, or *test3*. • **Content**: Enter or select the content that matches the condition. If **Field** is set to **Path**, **User Agent**, **Params**, **Cookie**, **Referer**, **Header**, **Response Header**, **Response Body**, or **Request Body**, **Case**	

Parameter	Description	Example Value
	Sensitive is supported. If you enable this, the system matches the case-sensitive content. It helps the system precisely identify requests and respond to them accurately, making protection policies work better. **NOTE** For more details, see **Table 5-20**.	
Deep Inspection	Assume that you set **Field** in the condition list to one of the following: • **Path**: **Content** supports **Case-Sensitive**. • **User Agent**: **Content** supports **Case-Sensitive**. • **Params**: **Content** supports **Case-Sensitive**. • **Cookie**: **Content** supports **Case-Sensitive**. • **Cookie**: **Content** supports **Case-Sensitive**. • **Header**: **Subfield** supports **Case-Sensitive**, and **Content** also supports **Case-Sensitive**. If you enable **Deep Inspection**, the **Subfield** and **Content** will be decoded and matched conditions in a case-insensitive manner. Deep Inspection supports Base64 decoding.	-

Parameter	Description	Example Value
Protective Action	• **Block**: Requests that hit the rule will be blocked and a block response page is returned to the client that initiates the requests. By default, WAF uses a unified block response page. You can also customize this page. • **Allow**: Requests that hit the rule are forwarded to backend servers. • **Log only**: Requests that hit the rule are not blocked, but will be logged. You can use WAF logs to query requests that hit the current rule and analyze the protection results of the rule. For example, check whether there are requests that are blocked mistakenly. • **JS Challenge**: WAF returns a piece of JavaScript code that can be automatically executed by a normal browser to the client. If the client properly executes the JavaScript code, WAF allows all requests from the client within a period of time (30 minutes by default). During this period, no verification is required. If the client fails to execute the code, WAF blocks the requests. **NOTE** – The cloud load balancer access mode does not support this protective action. – If the referer in the request is different from the current host, the JS challenge does not work. • **Advanced CAPTCHA**: If your website visitor triggers **Rate Limit** you set, CAPTCHA verification is required. If the verification is successful, the request is allowed within the validity period. If the verification fails, the CAPTCHA code is updated and the verification is required again. Compared with verification code, advanced CAPTCHA provides better experience and is more secure.	Block

Parameter	Description	Example Value
	NOTE – The cloud load balancer access mode does not support this protective action. – If you want to select **Advanced CAPTCHA** for **Protective Action**, make sure requests from a client IP address are forwarded to one WAF engine, or the authentication will fail due to repeated authentications. – After a successful verification, the client obtains a token, which grants access to all requests within its validity period. To prevent replay attacks, you can configure a policy to block requests exceeding a specified threshold.	
Token Lifespan	If **Protective Action** is set to **JS challenge** or **Advanced CAPTCHA**, the default validity period of a token is 1,800s. You can set it to a value ranging from 60 to 86,400 seconds.	60s
Known Attack Source	If you select **Block** for **Protective Action**, you can select a blocking type of a known attack source rule. Then, WAF blocks requests matching the configured **IP**, **Cookie**, or **Params** for a length of time that depends on the selected blocking type. WAF supports one-click unblocking of known attack sources. For details, see **One-Click Unblocking a Known Attack Source Rule**.	**Long-term IP address blocking**
Priority	Rule priority. If you have added multiple rules, rules are matched by priority. The smaller the value you set, the higher the priority. **NOTICE** If multiple precise access control rules have the same priority, WAF matches the rules in the sequence of time the rules are added.	**5**
Application Schedule	Select **Immediate** to enable the rule immediately, or select **Custom** to configure when you wish the rule to be enabled.	**Immediate**

Parameter	Description	Example Value
Block Page	If you select **Block** for **Protective Action**, you can configure an error page you want to return to your website visitors. • If you select **Default settings**, the default block page is returned. • If you select **Custom**, you can write a custom error message, so that WAF will return this message to website visitors when their requests are blocked. • To configure a redirection URL, select **Redirection**.	Custom
HTTP Return Code	HTTP return codes can be configured if **Block Page** is set to **Custom**.	418
Response Header	HTTP response headers can be configured if **Block Page** is set to **Custom**. Click **Add Response Header Field** and configure response header parameters.	-
Block Page Type	If you select **Custom** for **Block Page**, select a type of the block page among options **application/json**, **text/html**, and **text/xml**.	text/html
Page Content	If you select **Custom** for **Block Page**, configure the content to be returned.	Page content styles corresponding to different page types are as follows: • **text/html**: <html><body>Forbidden</body></html> • **application/json**: {"msg": "Forbidden"} • **text/xml**: <?xml version="1.0" encoding="utf-8"?><error><msg>Forbidden</msg></error>

Step 11 Click **OK**. You can then view the added precise protection rule in the protection rule list.

- After the configuration is complete, you can view the added rule in the protection rule list. **Rule Status** is **Enabled** by default.
- If you do not want the rule to take effect, click **Disable** in the **Operation** column of the rule.
- To delete a rule you no longer need, click **Delete** in the **Operation** column of the rule.
- To modify or copy a rule, click **More** > **Modify** or **More** > **Copy** in the **Operation** column of the target rule, respectively.

----End

Protection Verification

To verify that WAF is protecting your website (**www.example.com**) according to the precise protection rule as shown in **Figure 5-12**, take the following steps:

Step 1 Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

- If the website is inaccessible, connect the website domain name to WAF by following the instructions in **Website Settings**.
- If the website is accessible, go to **Step 2**.

Step 2 Clear the browser cache and enter **http://www.example.com/admin** (or any page containing **/admin**) in the address bar. Normally, WAF blocks the requests that meet the conditions and returns the block page.

Step 3 Return to the WAF console. In the navigation pane on the left, click **Events**. On the displayed page, check event logs.

----End

Configuration Example: Blocking a Certain Type of Attack Requests

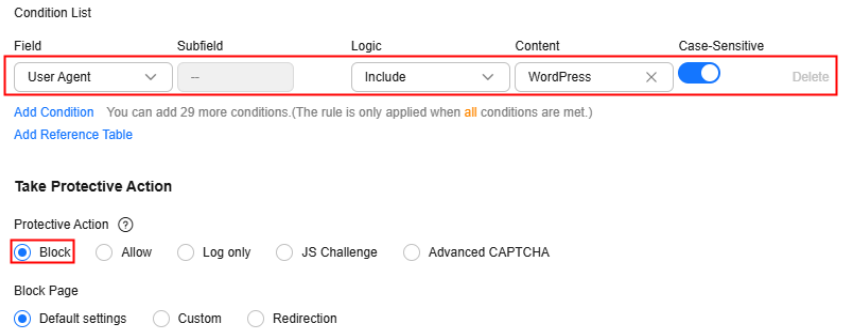
Analysis of a specific type of WordPress pingback attack shows that the **User Agent** field contains WordPress.

Figure 5-13 WordPress pingback attack

UA
WordPress/4.2.10; http://[redacted]s.vn; verifying pingback from [redacted]249.54
WordPress/4.0.1; http://[redacted]90; verifying pingback from [redacted].249.54
WordPress/4.6.1; https://[redacted]sabt.com; verifying pingback from [redacted].249.54
WordPress/4.5.3; http://[redacted].lib.umd.edu; verifying pingback from [redacted]9.54
WordPress/3.5.1; http://[redacted]o.com
WordPress/4.2.4; http://[redacted]t.tw; verifying pingback from [redacted]249.54
WordPress/4.6.1; http:/[redacted]om; verifying pingback from [redacted].249.54

A precise rule as shown in the figure can block this type of attack.

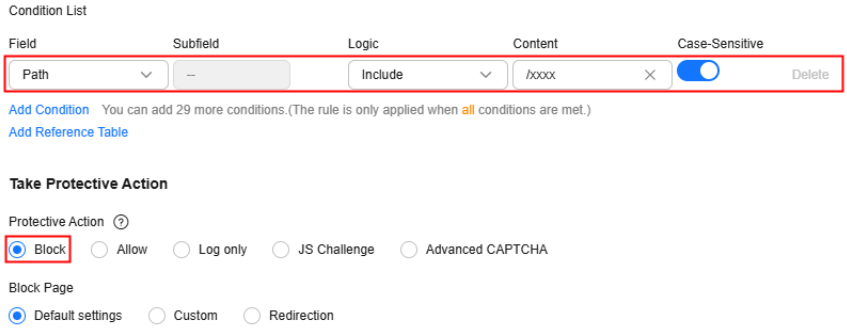
Figure 5-14 User Agent configuration



Configuration Example: Blocking Requests to a Certain URL

If a large number of IP addresses are accessing a URL that does not exist, configure the following protection rule to block such requests to reduce resource usage on the origin server. **Figure 5-15** shows an example.

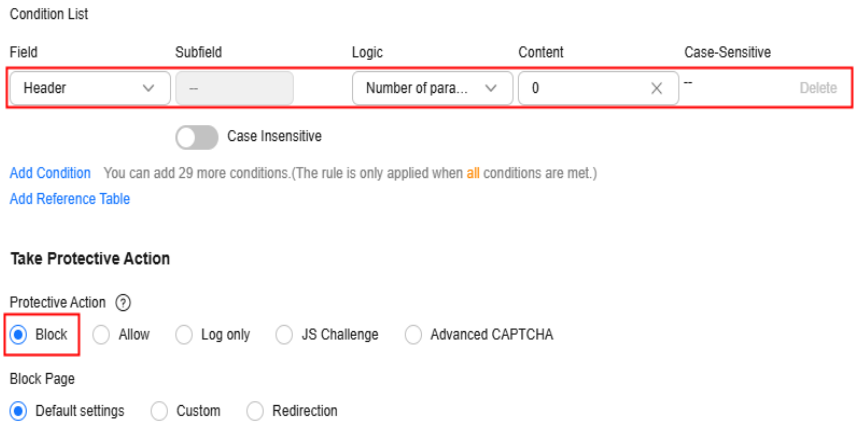
Figure 5-15 Blocking requests to a specific URL



Blocking Requests with null Fields

You can configure precise protection rules to block requests having null fields. **Figure 5-16** shows an example.

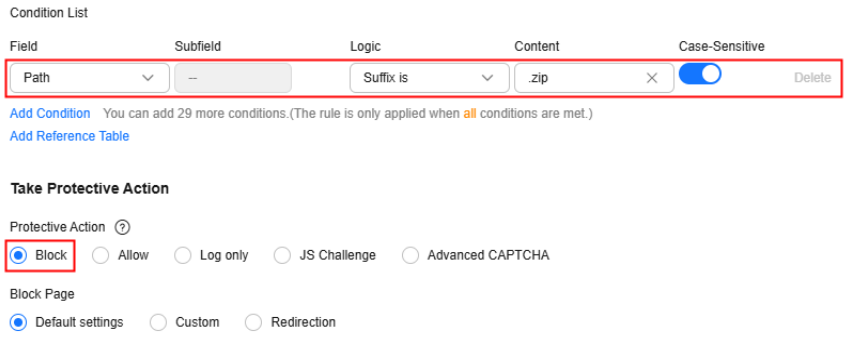
Figure 5-16 Blocking requests with empty Referer



Blocking Specified File Types (ZIP, TAR, and DOCX)

You can configure file types that match the path field to block specific files of certain types. For example, if you want to block .zip files, you can configure a precise protection rule as shown in **Figure 5-17** to block access requests of .zip files.

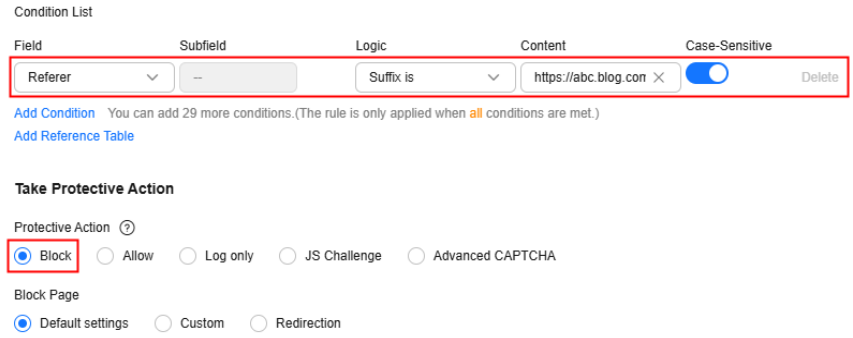
Figure 5-17 Blocking requests of specific file types



Configuration Example: Preventing Hotlinking

You can configure a protection rule based on the Referer field to enable WAF to block hotlinking from a specific website. If you find out that, for example, requests from **https://abc.blog.com** are stealing images from your site, you can configure a rule to block such requests.

Figure 5-18 Preventing hotlinking



Configuration Example: Allowing a Specified IP Address to Access Your Website

You can configure two precise protection rules, one to block all requests, as shown in **Figure 5-19**, but then another one to allow the access from a specific IP address, as shown in **Figure 5-20**.

Figure 5-19 Blocking all requests

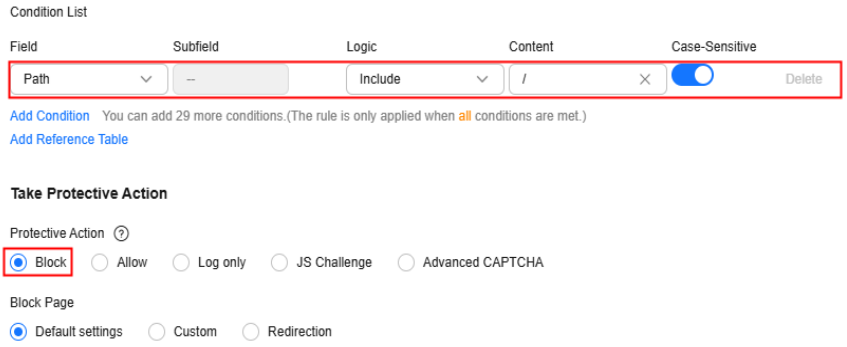
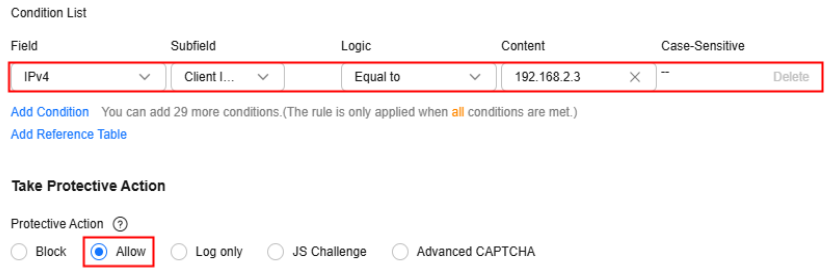


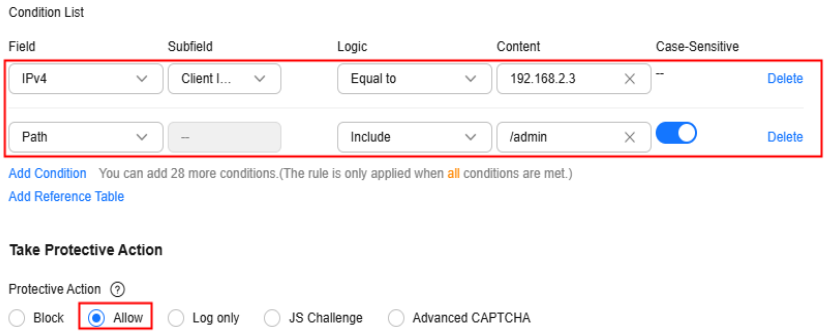
Figure 5-20 Allowing the access of a specified IP address



Configuration Example: Allowing a Specific IP Address to Access a Certain URL

You can configure multiple conditions in the **Condition List** field. If an access request meets the conditions in the list, WAF will allow the request from a specific IP address to access a specified URL.

Figure 5-21 Allowing specific IP addresses to access specified URLs



5.5 Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses

By default, all IP addresses are allowed to access your website. You can configure blacklist and whitelist rules to block, log only, or allow access requests from specific IP addresses or IP address ranges. Whitelist rules have a higher priority than blacklist rules. You can add a single IP address or import an IP address group to the blacklist or whitelist.

Prerequisites

- You have added the website you want to protect to WAF or **added a protection policy**.
  - For cloud CNAME access mode, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)**.
  - For cloud load balancer access mode, see **Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)**.
  - For dedicated mode, see **Connecting Your Website to WAF (Dedicated Mode)**.
- If you use a dedicated WAF instance, ensure that it has been upgraded to the latest version. For details, see **Managing Dedicated WAF Engines**.

Constraints

- When you add a website through **Cloud Mode - Load balancer** and set **Frontend Protocol** of the listener of your ELB load balancer to **TCP**, **UDP**, or **QUIC**, this type of rule does not take effect.
- WAF supports batch import of IP address blacklists and whitelists. You can use address groups to add multiple IP addresses/ranges quickly to a blacklist or whitelist rule. For details, see **Adding an IP Address Group**.
- The dedicated mode and cloud load balancer access mode support IPv6 addresses and IPv6 address ranges as long as the load balancers used for the dedicated mode or cloud load balancer access mode support IPv6.
- You can configure 0.0.0.0/0 and ::/0 IP address ranges in WAF blacklist and whitelist rules to block all IPv4 and IPv6 traffic, respectively. A whitelist rule has a higher priority than a blacklist rule. If you want to allow only a specific IP address within a range of blocked addresses, add a blacklist rule to block the range and then add a whitelist rule to allow the individual address you wish to allow.

  NOTICE

  If you want to allow only specified IP addresses to access the protected website, you can also configure rules b referring to **How Do I Allow Only Specified IP Addresses to Access the Protected Website?**

- If you set **Protective Action** to **Block** for a blacklist or whitelist rule, you can **set a known attack source** to block the visitor for a certain period of time; however, the known attack source with **Long-term IP address blocking** or **Short-term IP address blocking** configured cannot be set for a blacklist or whitelist rule. WAF will block requests matching the configured Cookie or Params for a block duration you specify.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.

Specification Limitations

- For details about the quota for IP address blacklist and whitelist rules, see **Edition Differences**.
- If the quota for IP address whitelist and blacklist rules of your cloud WAF instance cannot meet your requirements, you can purchase rule expansion packages under the current WAF instance edition or upgrade your WAF instance edition to increase such quota.

  A rule expansion package allows you to configure up to 10 IP address blacklist and whitelist rules. For details about how to upgrade WAF specifications, see **Upgrading the WAF Edition and Specifications**.

Impact on the System

If an IP address is added to a blacklist or whitelist, WAF blocks or allows requests from that IP address without checking whether the requests are malicious.

Configuring an IP Address Blacklist or Whitelist Rule

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Click the **Blacklist and Whitelist** configuration area and toggle it on or off if needed.

-  : enabled.
-  : disabled.

Step 8 In the upper left corner above the **Blacklist and Whitelist** list, click **Add Rule**.

Step 9 In the **Add Blacklist/Whitelist Rule** dialog box, add a blacklist or whitelist rule, as shown in **Figure 5-22** and **Figure 5-23**. For details about the parameters, see **Table 5-7**.

NOTE

- If you select **Log only** for **Protective Action** for an IP address, WAF only identifies and logs requests from the IP address.
- Other IP addresses are evaluated based on other configured WAF protection rules.

Figure 5-22 Adding an IP address/Range to a blacklist or whitelist rule

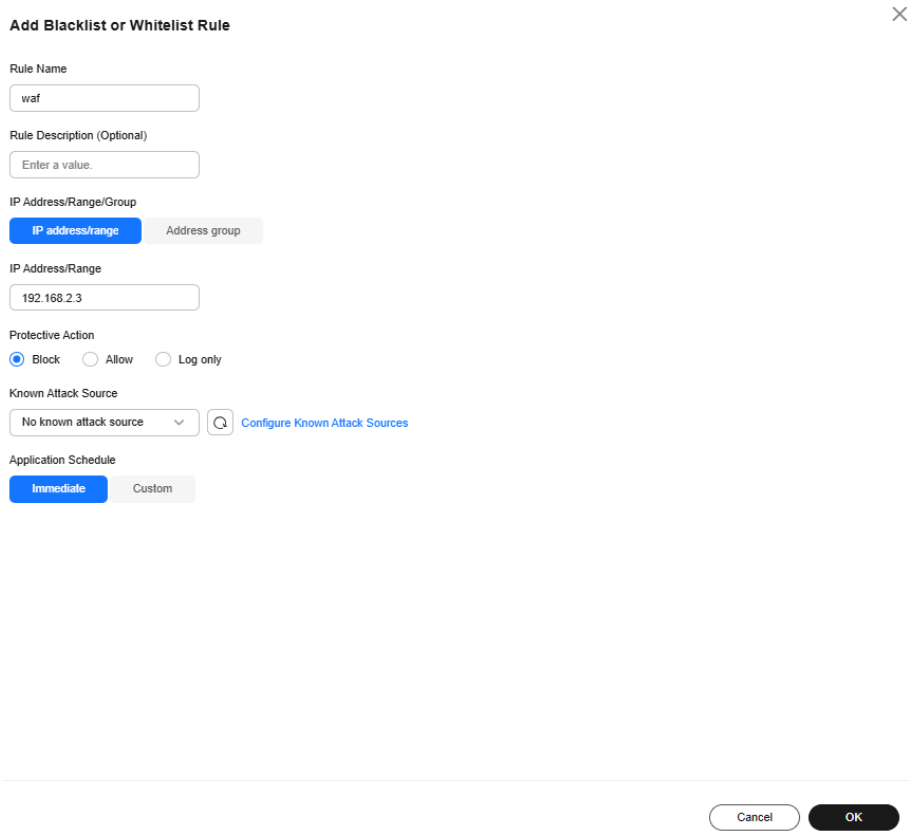


Figure 5-23 Batching adding IP addresses/Ranges to a blacklist or whitelist rule

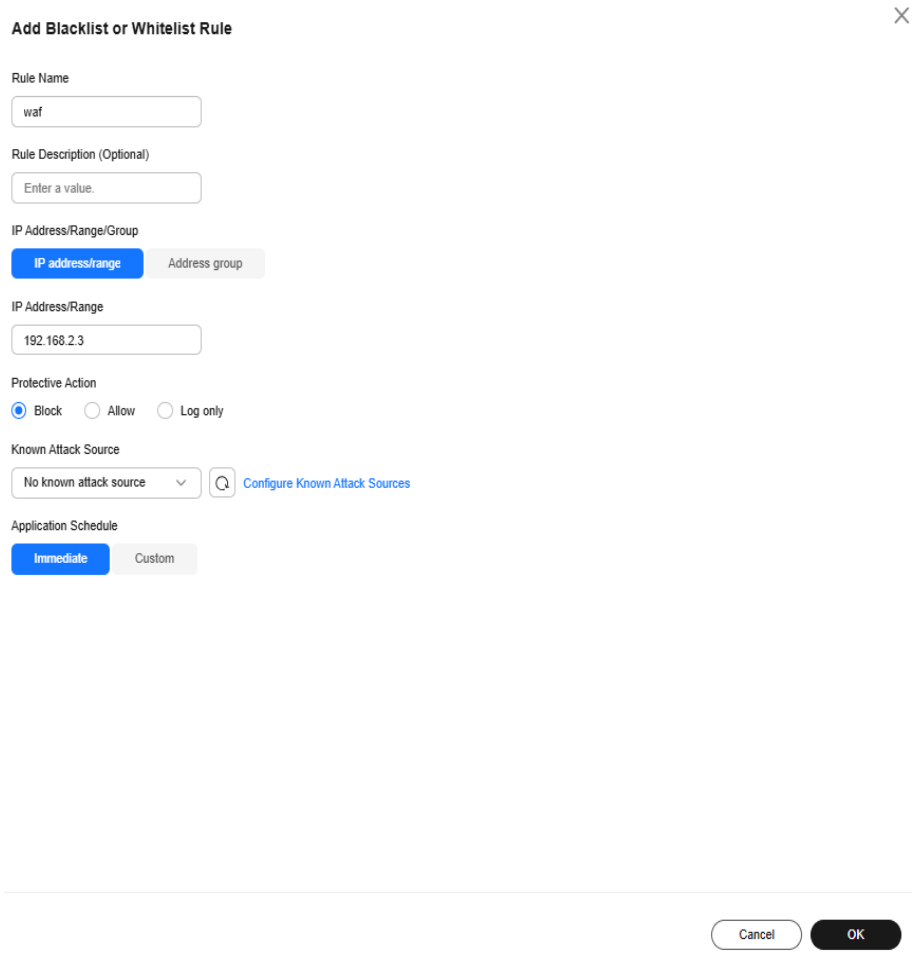


Table 5-7 Rule parameters

Parameter	Description	Example Value
Rule Name	Enter the name of the blacklist or whitelist rule.	waf
Rule Description (Optional)	Enter remarks for the blacklist or whitelist rule.	None
IP Address/ Range/Group	You can select **IP address/ Range** or **Address Group** to add IP addresses a blacklist or whitelist rule.	IP Address/Range

Parameter	Description	Example Value
IP Address/ Range	This parameter is mandatory if you select **IP address/range** for **IP Address/Range/Group**. IP addresses or IP address ranges are supported. • IP address: IP address to be added to the blacklist or whitelist • IP address range: IP address and subnet mask defining a network segment **NOTICE** IPv6 protection is supported by only professional and enterprise editions.	• IPv4 format: – 192.168.2.3 – 10.1.1.0/24 • IPv6 format: – fe80:0000:0000:0000:0000:0000:0000:0000 – ::/0 XXX.XXX.2.3

Parameter	Description	Example Value
Address Groups	This parameter is mandatory if you select **Address group** for **IP Address/Range/Group**. 1. (Optional) Click **Add Address Group** and enter the address group name, IP addresses/IP address ranges, and description. If you have an address group already, skip this step and select the address group from the address group list. **NOTE** – If the existing address group does not meet service requirements, click **Modify** in the **Operation** column to modify it. – If you no longer need an address group, disassociate it from the blacklist or whitelist rules and click **Delete** in the **Operation** column to delete it. – Address groups you add in this step will be synchronized to the **Address Groups** page. For more details, see **Managing IP Address Blacklist and Whitelist Groups**. 2. Select an address group you have added before.	--

Parameter	Description	Example Value
Protective Action	• **Block**: Select **Block** if you want to blacklist an IP address or IP address range. • **Allow**: Select **Allow** if you want to whitelist an IP address or IP address range. • **Log only**: Select **Log only** if you want to observe an IP address or IP address range. Then, WAF determines whether the IP address or IP address range are blacklisted or whitelisted based on the events data.	Block
Known Attack Source	If you select **Block** for **Protective Action**, you can select a blocking type of a known attack source rule. WAF will block requests matching the configured Cookie or Params for a length of time configured as part of the rule. **NOTE** Do not select the **Long-term IP address blocking** for a long time or **Short-term IP address blocking** for **Blocking Type**.	**Long-term Cookie blocking**
Effective Date	You can select **Immediate** or set a custom time range. If the configured effective time expires, the **Rule Status** of the rule will change to **Enabled (Invalid)**. You can change the effective time to make the rule work again or delete the rule.	Immediate

Step 10 Click **OK**. You can then view the added rule in the list of blacklist and whitelist rules.

- After the configuration is complete, you can view the added rule in the protection rule list. **Rule Status** is **Enabled** by default.

- If you do not want the rule to take effect, click **Disable** in the **Operation** column of the rule.
- To delete or modify a rule, click **Delete** or **Modify** in the **Operation** column of the rule.

----End

Protection Verification

Assume that the domain name **www.example.com** has been added and the IP address blacklist and whitelist protection rules have been configured by referring to the value example in **Table 5-7**. Take the following steps to verify the protection effect:

Step 1 Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

- If the website is inaccessible, connect the website domain name to WAF by following the instructions in **Website Settings**.
- If the website is accessible, go to **Step 2**.

Step 2 Blacklist the IP address of a client according to the instructions in **Configuring an IP Address Blacklist or Whitelist Rule**.

Step 3 Clear the browser cache and access **http://www.example.com** using configured IP address 192.168.2.3. Normally, WAF blocks the request and returns the block page.

Step 4 Return to the WAF console. In the navigation pane on the left, click **Events**. On the displayed page, check event logs.

----End

Example Configuration: Allowing a Specified IP Addresses

To verify that a specific IP address can be allowed to access your website domain name (*www.example.com*), take the following steps:

Step 1 Add a rule to block all source IP addresses.

- **Method 1**: Add the following two blacklist rules to block all source IP addresses, as shown in **Figure 5-24** and **Figure 5-25**.

Figure 5-24 Blocking IP address range 1.0.0.0/1

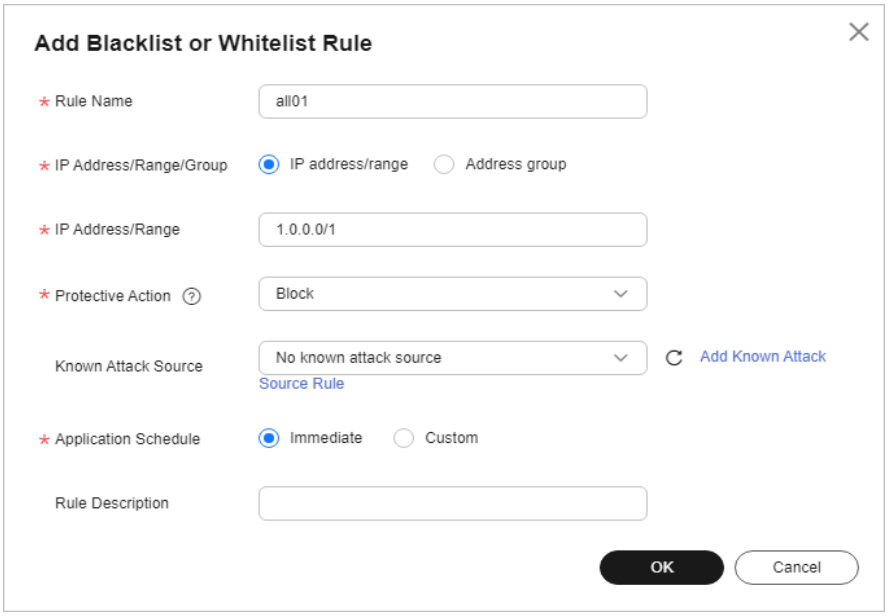
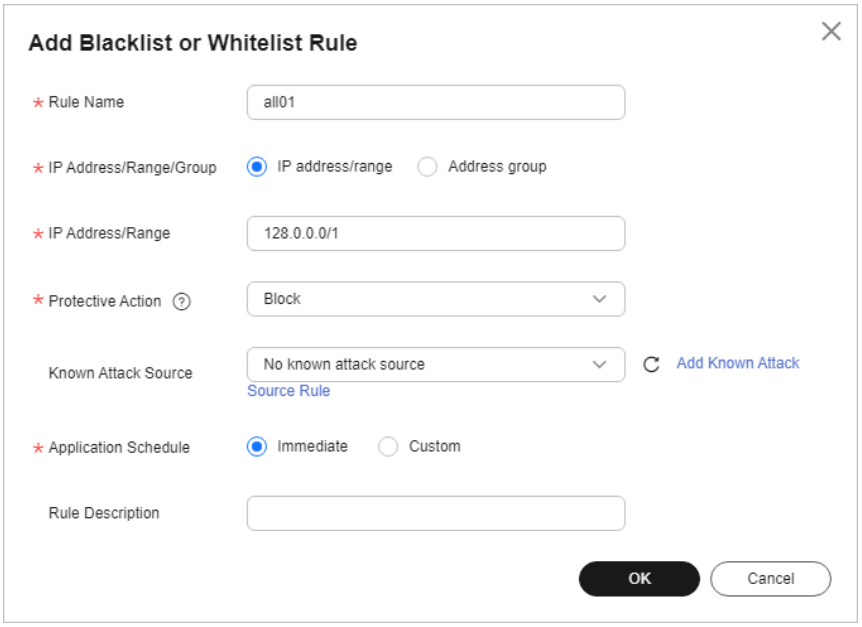
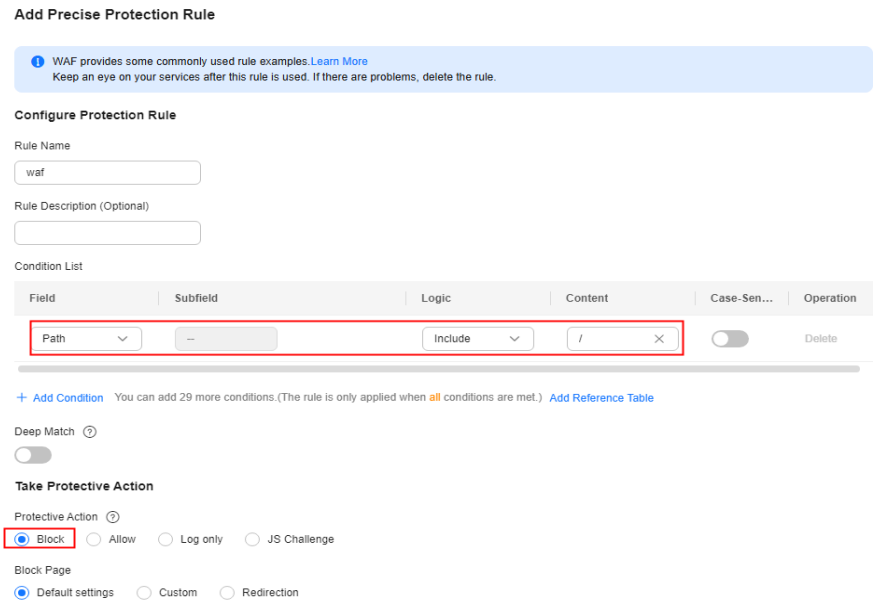


Figure 5-25 Blocking IP address range 128.0.0.0/1



- **Method 2**: Add a precise protection rule to block all access requests, as shown in **Figure 5-26**.

Figure 5-26 Blocking all access requests



- **Method 3**: Add 0.0.0.0/0 and::/0 to block all IPv4 and IPv6 traffic.

Figure 5-27 Blocking all IPv4 traffic

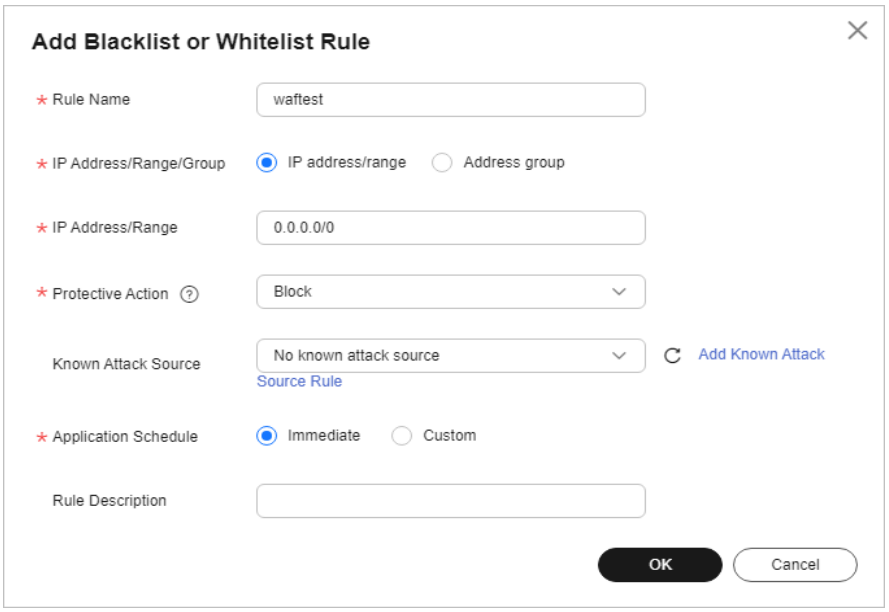
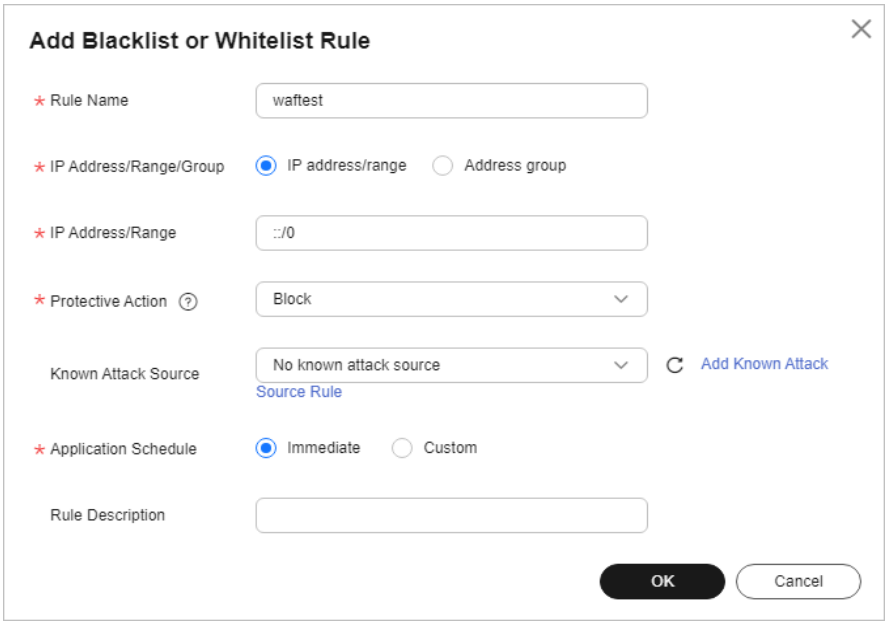
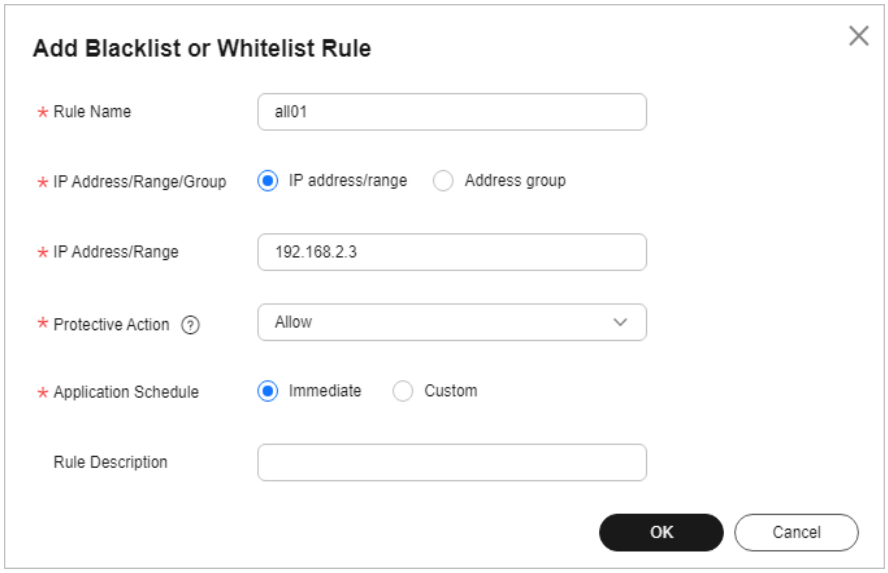


Figure 5-28 Blocking all IPv6 traffic



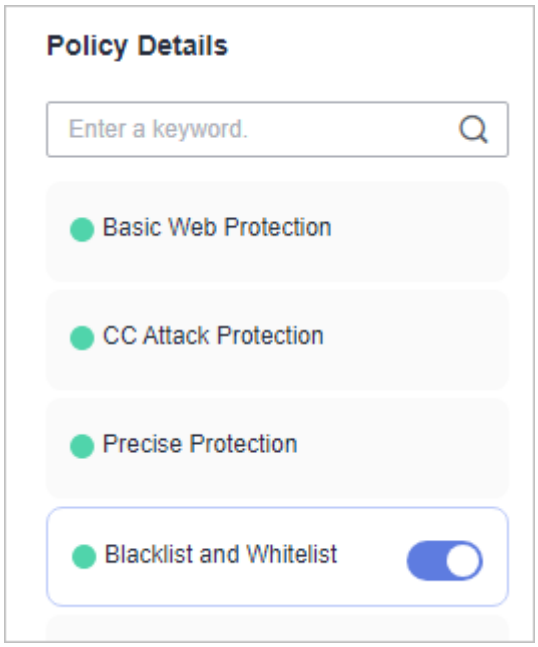
Step 2 Refer to **Figure 5-29** and add a whitelist rule to allow a specified IP address, for example, *192.168.2.3*.

Figure 5-29 Allowing the access of a specified IP address



Step 3 Enable the white and blacklist protection.

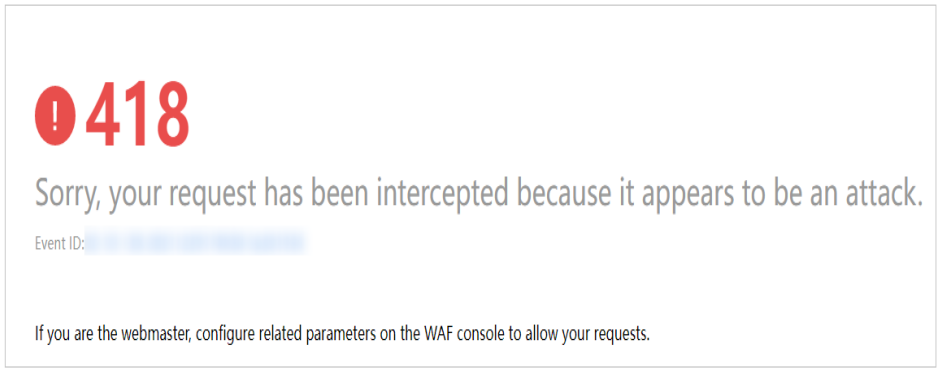
Figure 5-30 Blacklist and Whitelist configuration area



Step 4 Clear the browser cache and access http://www.example.com.

If the IP address of a visitor is not the one specified in **Step 2**, WAF blocks the access request. **Figure 5-31** shows an example of the block page.

Figure 5-31 Block page



Step 5 Go to the WAF console. In the navigation pane on the left, choose **Events**. View the event on the **Events** page.

----End

5.6 Configuring Geolocation Access Control Rules to Block or Allow Requests from Specific Locations

WAF can identify where a request originates. You can set geolocation access control rules in just a few clicks and let WAF block or allow requests from a certain region. A geolocation access control rule allows you to allow or block requests from IP addresses from specified countries or regions.

To allow only the IP addresses in a certain region to access the protected website, configure a rule by referring to **Configuration Example: Allowing Only IP Addresses from a Specified Location**.

Prerequisites

- You have added the website you want to protect to WAF or **added a protection policy**.
  - For cloud CNAME access mode, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)**.
  - For cloud load balancer access mode, see **Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)**.
  - For dedicated mode, see **Connecting Your Website to WAF (Dedicated Mode)**.
- If you use a dedicated WAF instance, ensure that it has been upgraded to the latest version. For details, see **Managing Dedicated WAF Engines**.

Constraints

- This function is not supported in the standard edition.
- If you are using dedicated WAF instances, **upgrade them to the latest version** and add IPv6 addresses for **IP Address Range**, or the settings cannot work.
- When you add a website through **Cloud Mode - Load balancer** and set **Frontend Protocol** of the listener of your ELB load balancer to **TCP**, **UDP**, or **QUIC**, this type of rule does not take effect.
- One region can be configured in only one geolocation access control rule. For example, if you have blocked requests from Shanghai with a geolocation access control rule, then Shanghai cannot be added to other geolocation access control rules.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.

Configuring a Geolocation Access Control Rule

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Click the **Geolocation Access Control** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

Step 8 In the upper left corner above the **Geolocation Access Control** list, click **Add Rule**.

Step 9 In the displayed dialog box, add a geolocation access control rule by referring to **Table 5-8**.

Figure 5-32 Adding a geolocation access control rule

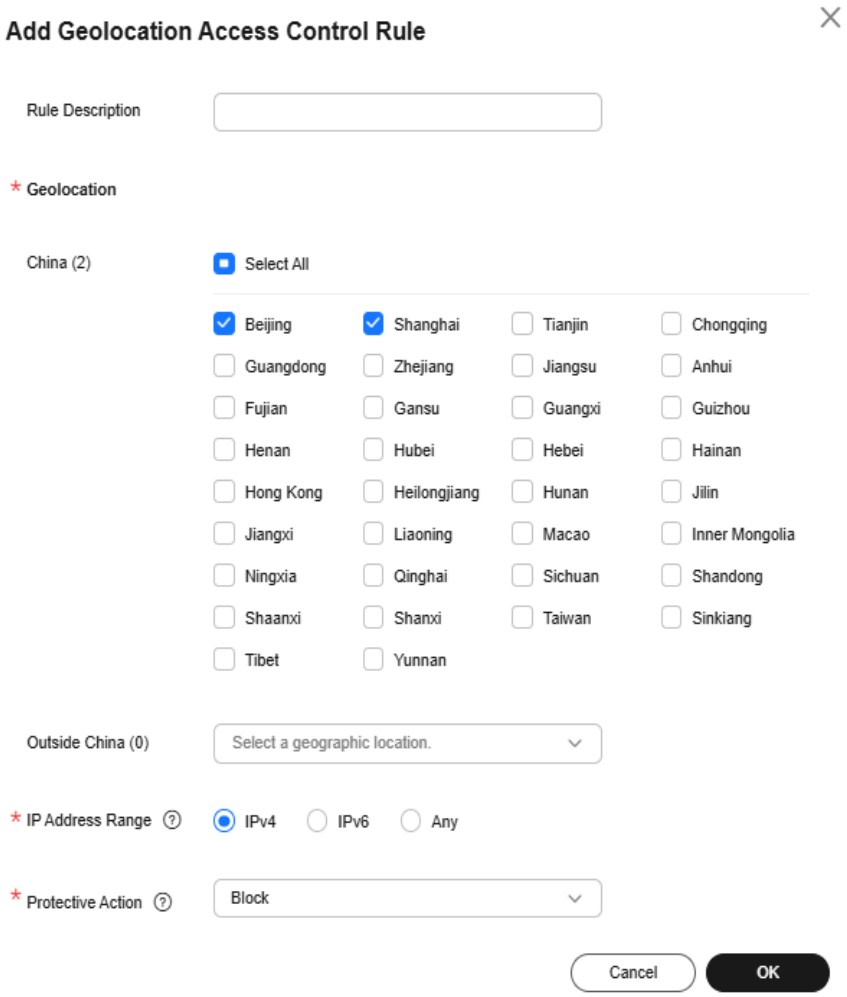


Table 5-8 Rule parameters

Parameter	Description	Example Value
Rule Name	Rule name you configured	-
Rule Description	A brief description of the rule. This parameter is optional.	waf

Parameter	Description	Example Value
Geolocation	Geographical scope of the IP address. You can select a location inside **China** or **Outside China**. A geographical location cannot be added to multiple protection policies.	**China**: **Shanghai**
IP Address Range	• **IPv4** • **IPv6** • Any (IPv4 or IPv6 address) **NOTE** If you are using dedicated WAF instances, **upgrade them to the latest version** and add IPv6 addresses for **IP Address Range**, or the settings cannot work.	**IPv4**
Protective Action	Action WAF will take if the rule is hit. You can select **Block**, **Allow**, or **Log only**.	**Block**

Step 10 Click **OK**. You can then view the added rule in the list of the geolocation access control rules.

- After the configuration is complete, you can view the added rule in the protection rule list. **Rule Status** is **Enabled** by default.
- If you do not want the rule to take effect, click **Disable** in the **Operation** column of the rule.
- To delete or modify a rule, click **Delete** or **Modify** in the **Operation** column of the rule.

----End

Protection Verification

To verify that WAF is protecting your domain name (**www.example.com**) according to the geolocation access control protection rule configured by referring to **Table 5-8**, take the following steps:

Step 1 Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

- If the website is inaccessible, connect the website domain name to WAF by following the instructions in **Website Settings**.
- If the website is accessible, go to **Step 2**.

Step 2 Clear the browser cache. Then, use an IP address from **Shanghai** to access the **http://www.example.com** page. If WAF blocks the access request from the IP address and returns the block page, the rule works.

Step 3 Return to the WAF console. In the navigation pane on the left, click **Events**. On the displayed page, check event logs.

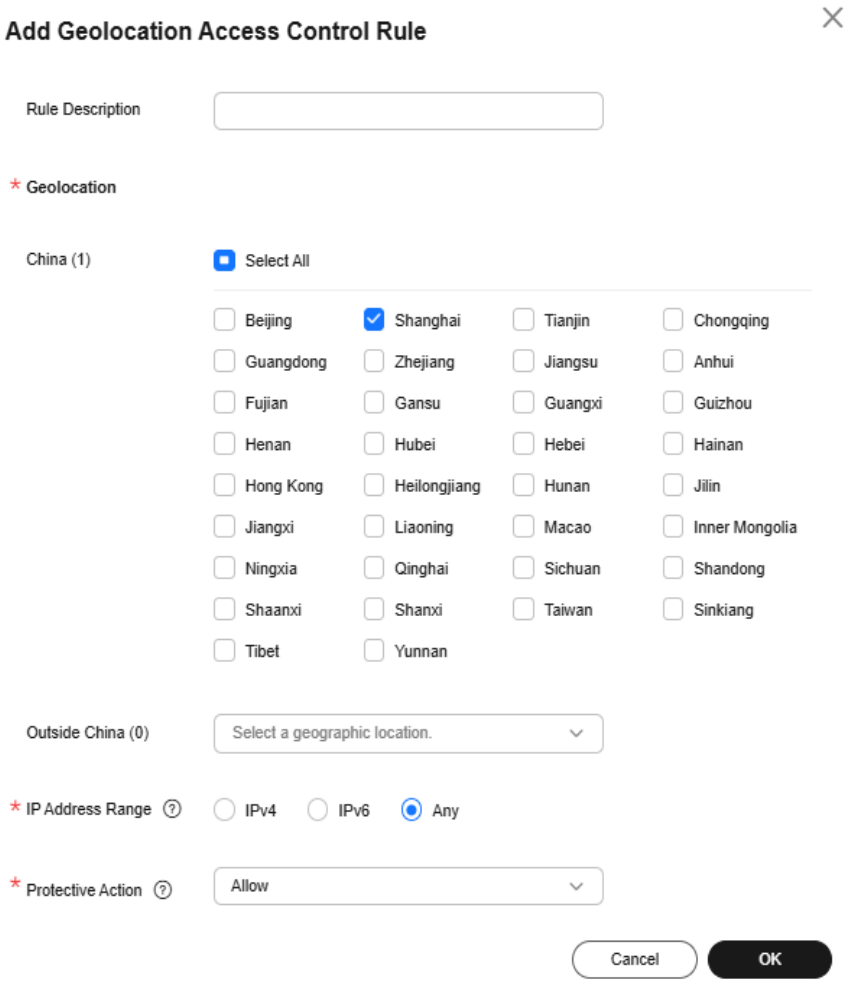
----End

Configuration Example: Allowing Only IP Addresses from a Specified Location

If you want to allow only IP addresses from **Shanghai, China** to access the domain name, configure a rule as follows:

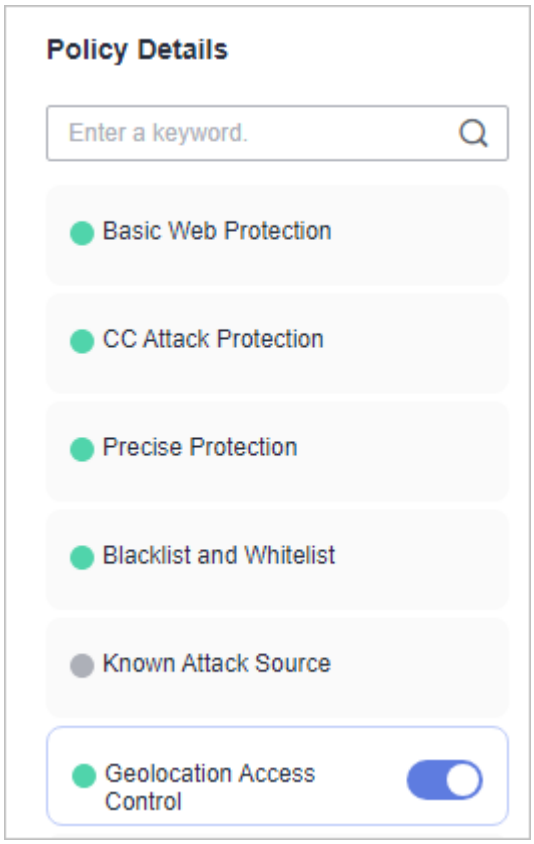
Step 1 Add a geolocation access control rule: Select **Shanghai** for **Geolocation** and select **Allow** for **Protective Action**.

Figure 5-33 Selecting **Allow** for **Protective Action**



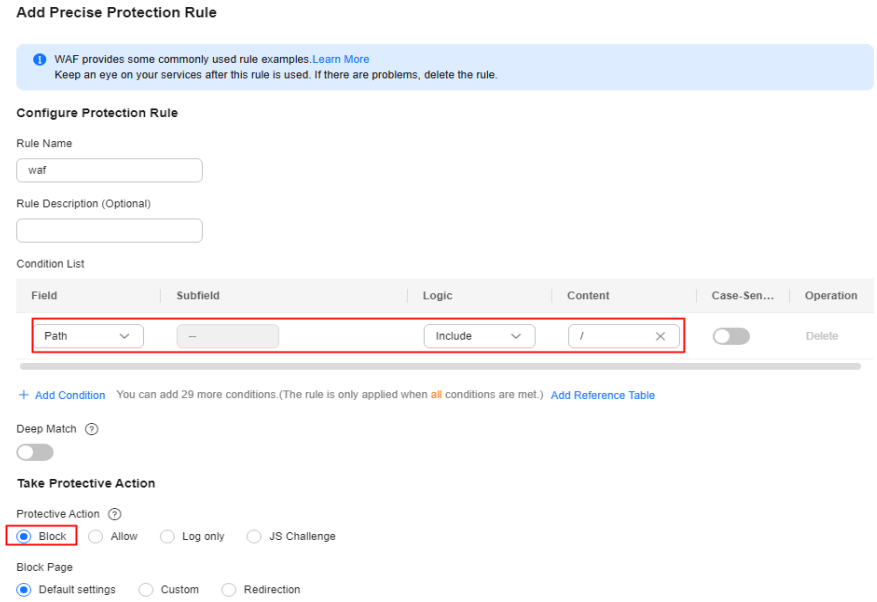
Step 2 Enable geolocation access control.

Figure 5-34 Geolocation Access Control configuration area



Step 3 Configure a precise protection rule to block all requests.

Figure 5-35 Blocking all access requests

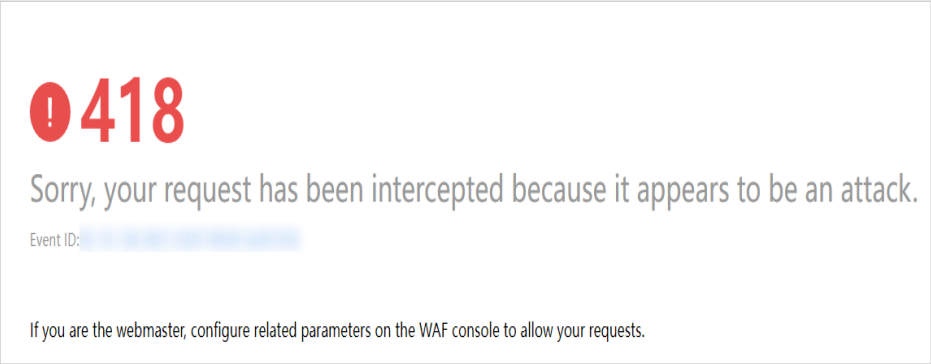


For details, see **Configuring Custom Precise Protection Rules**.

Step 4 Clear the browser cache and access **http://www.example.com**.

When an access request from IP addresses outside **Shanghai** accesses the page, WAF blocks the access request.

Figure 5-36 Block page



Step 5 Go to the WAF console. In the navigation pane on the left, choose **Events**. View the event on the **Events** page. You will see that all requests not from **Shanghai** have been blocked.

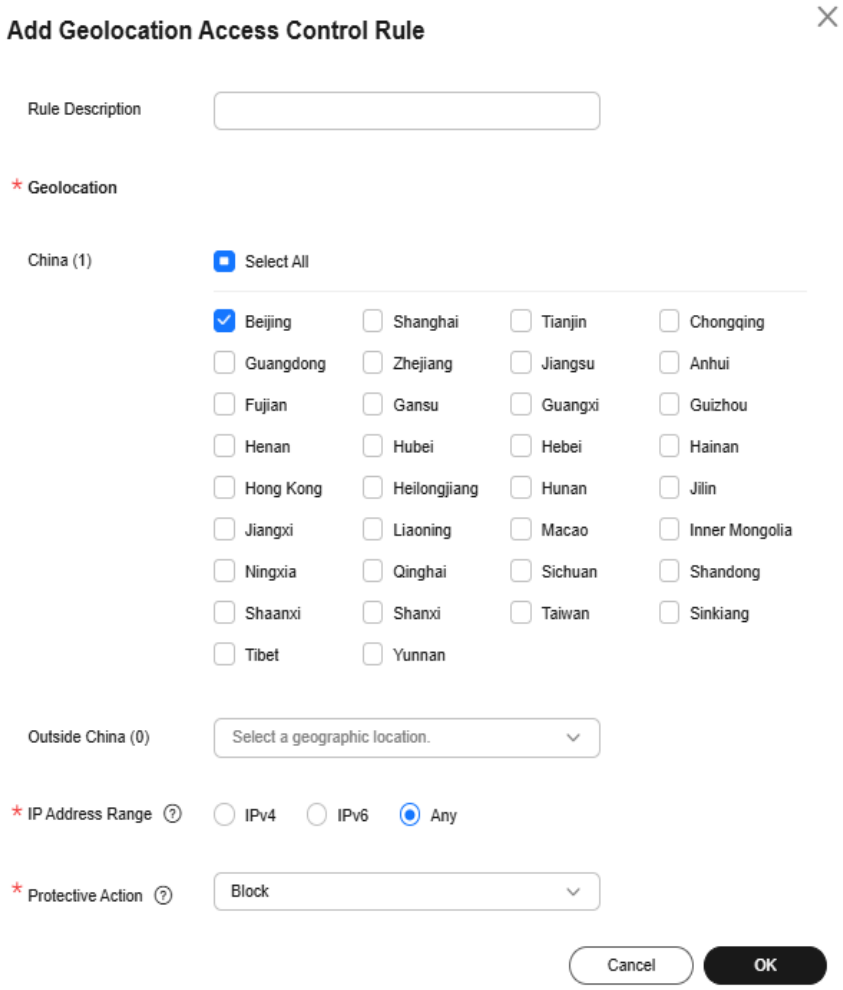
----End

Configuration Example: Blocking IP Addresses from a Specified Location

If you want to block all IP addresses from **Beijing**, configure a rule as follows:

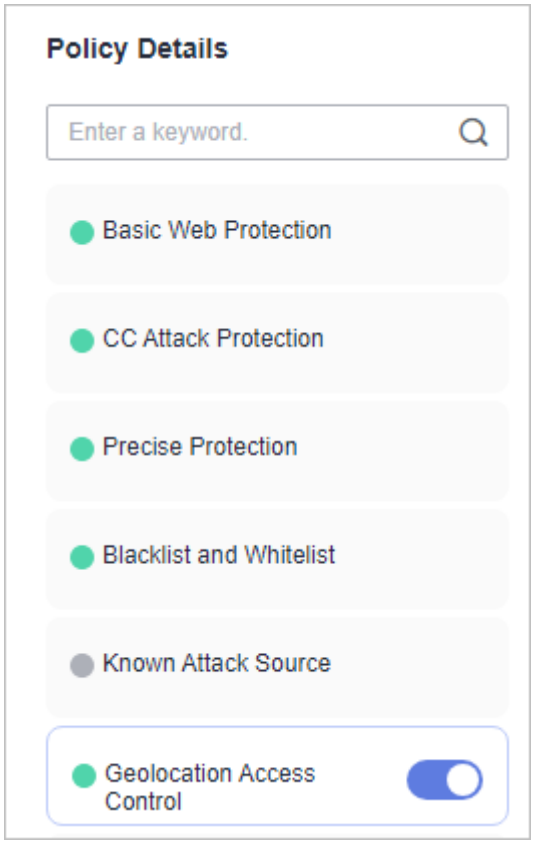
Step 1 Add a geolocation access control rule: Select **Beijing** for **Geolocation** and **Block** for **Protective Action**.

Figure 5-37 Blocking access requests from a specific region



Step 2 Enable geolocation access control.

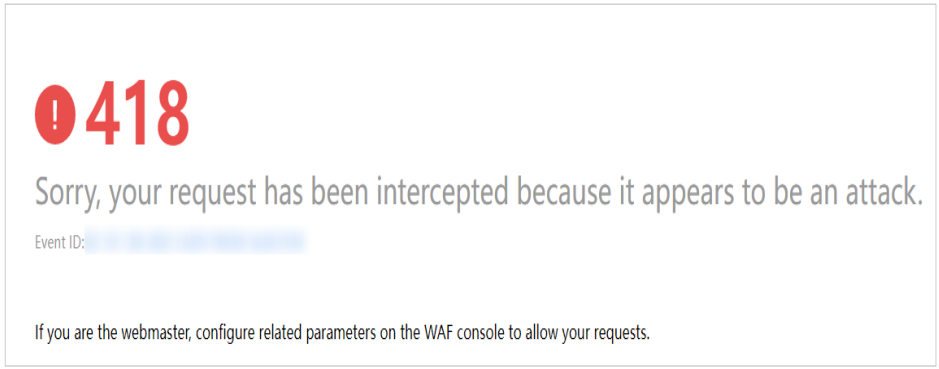
Figure 5-38 Geolocation Access Control configuration area



Step 3 Clear the browser cache and access http://www.example.com.

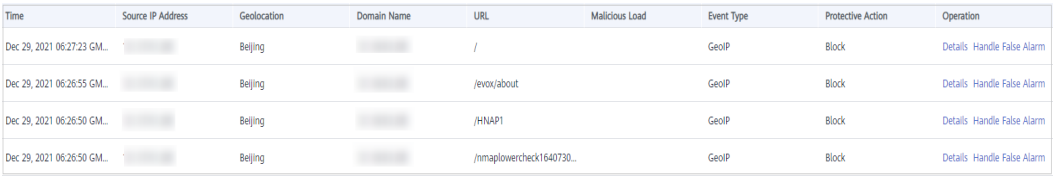
When an access request from IP addresses inside **Beijing** accesses the page, WAF blocks the access request.

Figure 5-39 Block page



Step 4 Go to the WAF console. In the navigation pane on the left, choose **Events**. View the event on the **Events** page.

Figure 5-40 Viewing events - blocking access requests from IP addresses in a region



----End

5.7 Configuring Threat Intelligence Access Control Rules to Block or Allow IP Addresses in a Specified IP Address Library

Access is controlled based on the IP address library of an Internet Data Center (IDC). The available IP address library platforms include Dr. Peng, Google, Tencent, and Meituan. With this protection, when a source IP address in the target IP address library initiates an access request to any path under the protected domain name, the configured access control rule is triggered, and the request is blocked, allowed, or logged only.

Prerequisites

- You have added a website to WAF or **added a protection policy**.
  - For cloud CNAME access mode, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)**.
  - For dedicated access mode, see **Connecting Your Website to WAF (Dedicated Mode)**.
- If you use a dedicated WAF instance, make sure it has been upgraded to the latest version. For details, see **Managing Dedicated WAF Engines**.

Constraints

- In cloud mode, threat intelligence access control rules are available only in the professional and enterprise editions.
- In dedicated mode, only dedicated instances released in September 2022 and later support threat intelligence access control rules. For details about dedicated instance versions, see **Dedicated Engine Version Iteration**.
- ELB-mode WAF does not support threat intelligence access control rules.

Configuring a Threat Intelligence Access Control Rule

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Click the **Threat Intelligence Access Control** configuration area and toggle it on or off if needed.

-  : enabled.
-  : disabled.

Step 8 In the upper left corner above the rule list, click **Add Rule**.

Step 9 In the dialog box displayed, add a threat intelligence access control rule. **Table 5-9** describes the parameters.

Figure 5-41 Add Threat Intelligence Access Rule

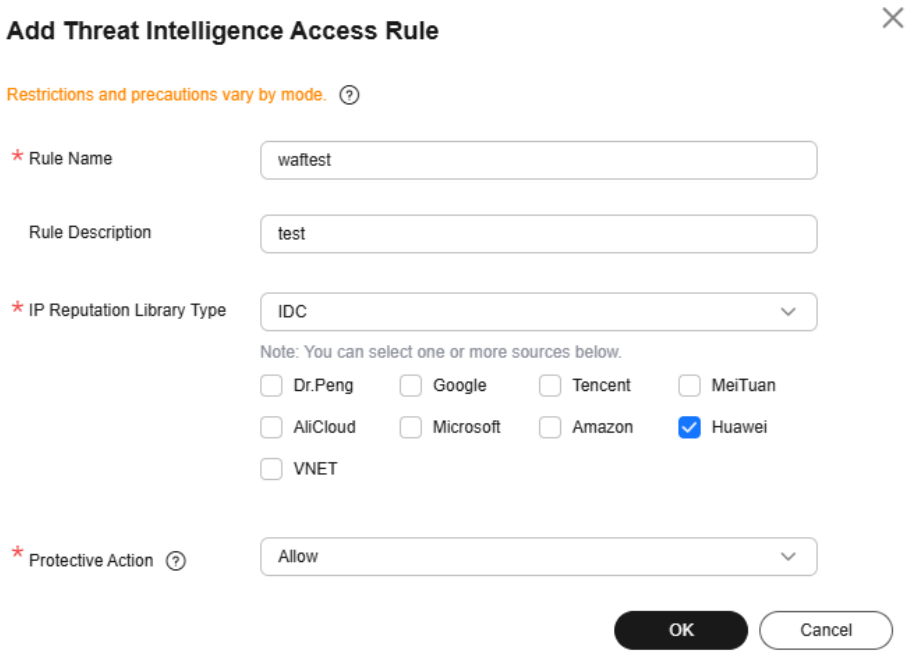


Table 5-9 Parameter description

Parameter	Description	Example Value
Rule Name	Name of the rule.	WAFtest
Rule Description	A brief description of the rule. This parameter is optional.	--

Parameter	Description	Example Value
IP Reputation Library Type	Select **IDC** from the drop-down list box and select the IP database platform. You can select IP library platform **Dr. Peng**, **Google**, **Tencent**, **Meituan**, and more.	IDC Huawei
Protective Action	Action WAF will take if the rule is hit. You can select **Block**, **Allow**, or **Log only**. • **Block**: Requests that hit the rule will be blocked and a block response page is returned to the client that initiates the requests. By default, WAF uses a unified block response page. You can also customize this page. • **Allow**: Requests that hit the rule are forwarded to backend servers. • **Log only**: Requests that hit the rule are not blocked, but will be logged.	Allow

Step 10 Click **OK**. You can view the added threat intelligence access control rule in the rule list.

- After the configuration is complete, you can view the added rule in the protection rule list. **Rule Status** is **Enabled** by default.
- If you do not want the rule to take effect, click **Disable** in the **Operation** column of the rule.
- To delete or modify a rule, click **Delete** or **Modify** in the **Operation** column of the rule.

----End

Protection Verification

To verify that WAF is protecting your domain name (**www.example.com**) according to the protection rule configured by referring to example values in **Table 5-9**, take the following steps:

Step 1 Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

- If the website is inaccessible, connect the website domain name to WAF by following the instructions in **Website Settings**.
- If the website is accessible, go to **Step 2**.

Step 2 Add a rule where **IP Reputation Library Type** is **Huawei** and **Protective Action** is **Block**. For details, see **Configuring a Geolocation Access Control Rule**.

Step 3 Clear the browser cache and access **http://www.example.com** using an IP address from Huawei IP address library. If WAF blocks the request and returns the block page, the rule takes effect.

Step 4 Return to the WAF console. In the navigation pane on the left, click **Events**. On the displayed page, check event logs.

----End

5.8 Configuring Web Tamper Protection Rules to Prevent Static Web Pages from Being Tampered With

You can set web tamper protection rules to protect specific website pages (such as the ones contain important content) from being tampered with. If a web page protected with such a rule is requested, WAF returns the origin page it has cached based on the rule so that visitors always receive the authenticate web pages.

How It Works

- Return directly the cached web page to the normal web visitor to accelerate request response.
- Return the cached original web pages to visitors if an attacker has tampered with the static web pages. This ensures that your website visitors always get the right web pages.
- Protect all resources in the web page path. For example, if a web tamper protection rule is configured for a static page pointed to *www.example.com/index.html*, WAF protects the web page pointed to */index.html* and related resources associated with the web page.

  So, if the URL in the **Referer** header field is the same as the configured anti-tamper path, for example, **/index.html**, all resources (resources ending with png, jpg, jpeg, gif, bmp, css or js) matching the request are also cached.
- WAF can cache user-defined header fields. In the upper part of the page, click **Modify Field** to configure the header fields you want WAF to cache.

Prerequisites

You have added the website you want to protect to WAF or **added a new protection policy**.

- For cloud CNAME access mode, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)**.
- For dedicated access mode, see **Connecting Your Website to WAF (Dedicated Mode)**.

Constraints

- The cloud load balancer access mode does not support this type of protection rule.

- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- Ensure that the origin server response contains the **Content-Type** response header, or WAF may fail to cache the origin server response.

Application Scenarios

- Quicker response to requests

  After a web tamper protection rule is configured, WAF caches static web pages on the server. When receiving a request from a web visitor, WAF directly returns the cached web page to the web visitor.

- Web tamper protection

  If an attacker modifies a static web page on the server, WAF still returns the cached original web page to visitors. Visitors never see the pages that were tampered with.

  WAF randomly extracts requests from a visitor to compare the page they received with the page on the server. If WAF detects that the page has been tampered with, it notifies you by SMS or email, depending on what you configure. For more details, see **Enabling Alarm Notifications**.

Configuring a Web Tamper Protection Rule

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Click the **Web Tamper Protection** configuration area and toggle it on or off if needed.

-  : enabled.
-  : disabled.

Step 8 In the upper left corner above the **Web Tamper Protection** rule list, click **Add Rule**.

Step 9 In the displayed dialog box, specify the parameters by referring to **Table 5-10**.

Figure 5-42 Adding a web tamper protection rule

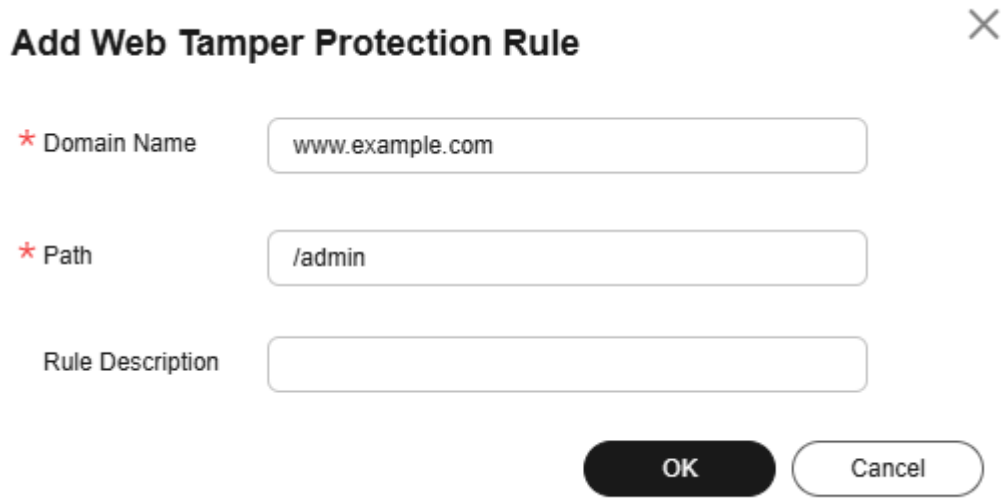


Table 5-10 Parameter description

Parameter	Description	Example Value
Domain Name	Domain name of the website to be protected	**www.example.com**
Path	Path of the URL for which you want to enable web tamper protection. A URL is the address of a web page. The common URL format is *Protocol name*://*Domain name or IP address[:Port number]*/*[Path name/... /File name]*, for example, http://www.example.com/admin. Path configuration requirements: • The path cannot contain a domain name. For example, the path in the example URL is **/admin**. • Regular expressions are not supported. • The path cannot contain two or more consecutive slashes. For example, **///admin**. If you enter **///admin**, WAF converts **///** to **/**.	**/admin**

Parameter	Description	Example Value
Rule Description	A brief description of the rule. This parameter is optional.	None

Step 10 Click **OK**. You can view the rule in the list of web tamper protection rules.

- After the configuration is complete, you can view the added rule in the protection rule list. **Rule Status** is **Enabled** by default.
- If you do not want the rule to take effect, click **Disable** in the **Operation** column of the rule.
- To delete or modify a rule, click **Delete** or **Modify** in the **Operation** column of the rule.
- To update cache of a protected web page, click **Update Cache** in the row containing the corresponding web tamper protection rule. If the rule fails to be updated, WAF will return the recently cached page but not the latest page.

----End

Protection Verification

To verify that WAF is protecting your domain name (**www.example.com**) according to the protection rule configured by referring to example values in **Table 5-10**, take the following steps:

Step 1 Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

- If the website is inaccessible, connect the website domain name to WAF by following the instructions in **Website Settings**.
- If the website is accessible, go to **Step 2**.

Step 2 Access the **http://www.example.com/admin** page. The initial page is displayed.

Step 3 Simulate the attack to tamper with the **http://www.example.com/admin** web page.

Step 4 Access the **http://www.example.com/admin** page in the browser. The initial page that is not tampered with is displayed.

Step 5 Return to the WAF console. In the navigation pane on the left, click **Events**. On the displayed page, check event logs.

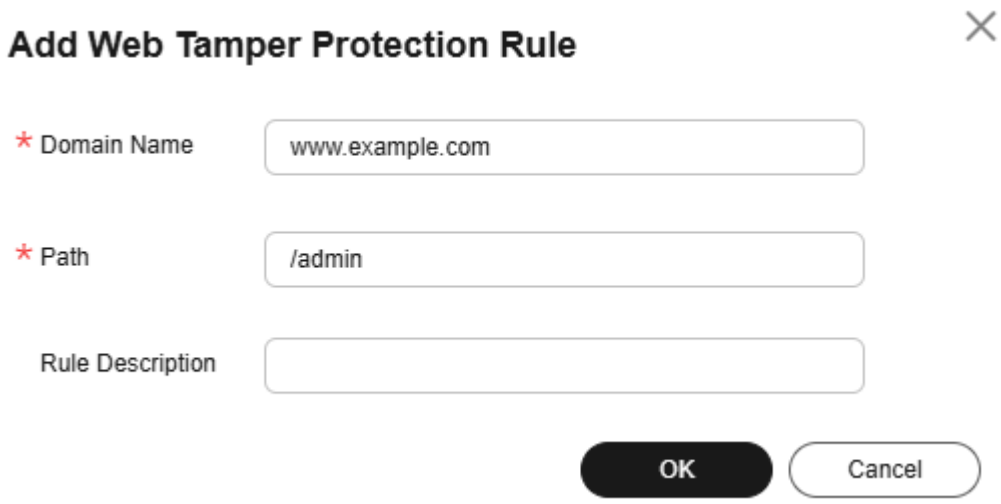
----End

Configuration Example: Static Web Page Tamper Prevention

To verify that WAF is protecting a static page **/admin** on your website **www.example.com** from being tampered with, take the following steps:

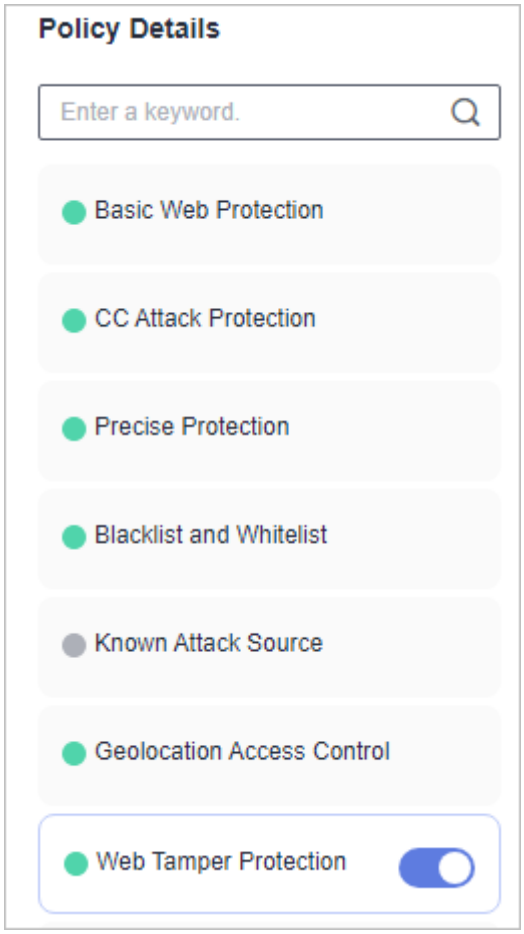
Step 1 Add a web tamper prevention rule to WAF.

Figure 5-43 Adding a web tamper protection rule



Step 2 Enable WTP.

Figure 5-44 Web Tamper Protection configuration area



Step 3 Simulate the attack to tamper with the **http://www.example.com/admin** web page.

Step 4 Use a browser to access **http://www.example.com/admin**. WAF will cache the page.

Step 5 Access the page again.

The intact page is returned.

----End

FAQs

Why Does the Page Fail to Be Refreshed After WTP Is Enabled?

5.9 Configuring Anti-Crawler Rules

You can configure website anti-crawler protection rules to protect against search engines, scanners, script tools, and other crawlers, and use JavaScript to create custom anti-crawler protection rules.

Prerequisites

- You have added the website you want to protect to WAF or **added a protection policy**.
  - For cloud CNAME access mode, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)**.
  - For cloud load balancer access mode, see **Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)**.
  - For dedicated mode, see **Connecting Your Website to WAF (Dedicated Mode)**.
- If you use a dedicated WAF instance, ensure that it has been upgraded to the latest version. For details, see **Managing Dedicated WAF Engines**.

Constraints

- Cookies must be enabled and JavaScript supported by any browser used to access a website protected by anti-crawler protection rules.
- If your service is connected to CDN, exercise caution when using the JS anti-crawler function.

  CDN caching may impact JS anti-crawler performance and page accessibility.
- The JavaScript anti-crawler function is unavailable for pay-per-use WAF instances.
- This function is not supported in the standard edition.
- JS anti-crawler protection is not supported in **Cloud - Load balancer** WAF.
- If JavaScript anti-crawler event logs cannot be viewed, see **Why Are There No Protection Logs for Some Requests Blocked by WAF JavaScript Anti-Crawler Rules?**
- The protective action for website anti-crawler JavaScript challenge is **Log only**, and that for JavaScript authentication is **Verification code**. If a visitor fails the JavaScript authentication, a verification code is required for access.

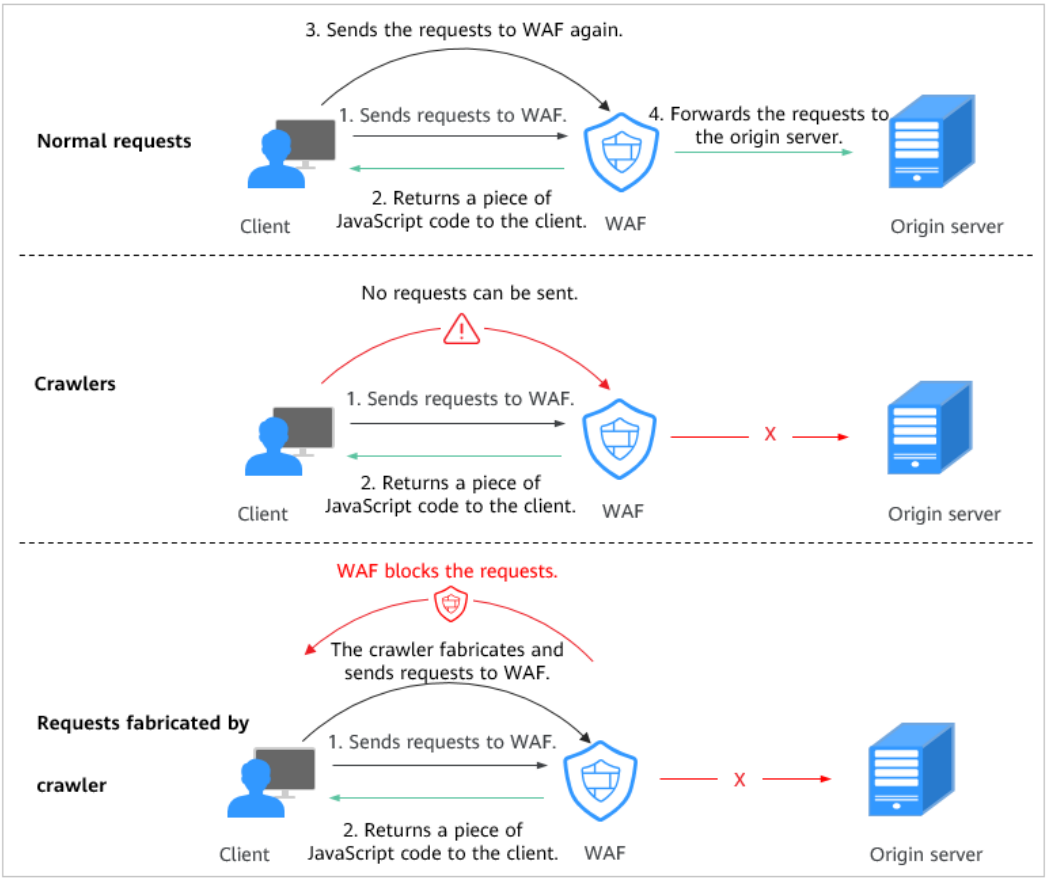
Requests will be forwarded as long as the visitor enters a valid verification code.

- WAF JavaScript-based anti-crawler rules only check GET requests and do not check POST requests.

How JavaScript Anti-Crawler Protection Works

Figure 5-45 shows how JavaScript anti-crawler detection works, which includes JavaScript challenges (step 1 and step 2) and JavaScript authentication (step 3).

Figure 5-45 JavaScript Anti-Crawler protection process

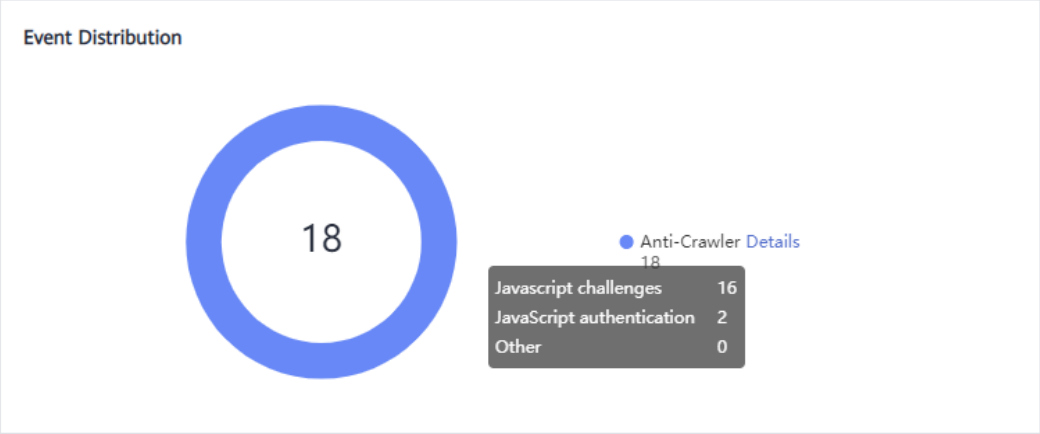


If JavaScript anti-crawler is enabled when a client sends a request, WAF returns a piece of JavaScript code to the client.

- If the client sends a normal request to the website, triggered by the received JavaScript code, the client will automatically send the request to WAF again. WAF then forwards the request to the origin server. This process is called JavaScript verification.
- If the client is a crawler, it cannot be triggered by the received JavaScript code and will not send a request to WAF again. The client fails JavaScript authentication.
- If a client crawler fabricates a WAF authentication request and sends the request to WAF, the WAF will block the request. The client fails JavaScript authentication.

By collecting statistics on the number of JavaScript challenges and authentication responses, the system calculates how many requests the JavaScript anti-crawler defends. In **Figure 5-46**, the JavaScript anti-crawler has logged 18 events, 16 of which are JavaScript challenge responses, and 2 of which are JavaScript authentication responses. **Other** indicates the number of WAF authentication requests fabricated by the crawler.

Figure 5-46 Parameters of a JavaScript anti-crawler protection rule



NOTICE

The protective action for website anti-crawler JavaScript challenge is **Log only**, and that for JavaScript authentication is **Verification code**. If a visitor fails the JavaScript authentication, a verification code is required for access. Requests will be forwarded as long as the visitor enters a valid verification code.

Configuring an Anti-Crawler Rule

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Click the **Anti-Crawler** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

Step 8 Select the **Feature Library** tab and enable the protection by referring to **Table 5-11**. **Figure 5-47** shows an example.

A feature-based anti-crawler rule has two protective actions:

- **Block**

  WAF blocks and logs detected attacks.

  CAUTION

  Enabling this feature may have the following impacts:

  – Blocking requests of search engines may affect your website SEO.

  – Blocking scripts may block some applications because those applications may trigger anti-crawler rules if their user-agent field is not modified.

- **Log only**

  Detected attacks are logged only. This is the default protective action.

Scanner is enabled by default, but you can enable other protection types if needed.

Figure 5-47 Feature Library

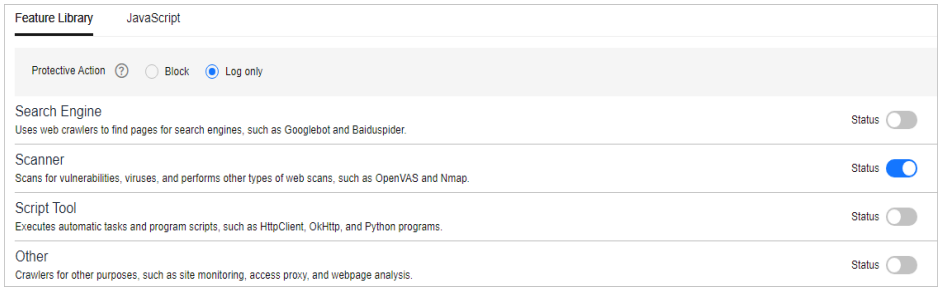


Table 5-11 Anti-crawler detection features

Type	Description	Remarks
Search Engine	This rule is used to block web crawlers, such as Googlebot and Baiduspider, from collecting content from your site.	If you enable this rule, WAF detects and blocks search engine crawlers. **NOTE** If **Search Engine** is not enabled, WAF does not block POST requests from Googlebot or Baiduspider. If you want to block POST requests from Baiduspider, use the configuration described in **Configuration Example: Search Engine**.

Type	Description	Remarks
Scanner	This rule is used to block scanners, such as OpenVAS and Nmap. A scanner scans for vulnerabilities, viruses, and other jobs.	After you enable this rule, WAF detects and blocks scanner crawlers.
Script Tool	This rule is used to block script tools. A script tool is often used to execute automatic tasks and program scripts, such as HttpClient, OkHttp, and Python programs.	If you enable this rule, WAF detects and blocks the execution of automatic tasks and program scripts. **NOTE** If your application uses scripts such as HttpClient, OkHttp, and Python, disable **Script Tool**. Otherwise, WAF will identify such script tools as crawlers and block the application.
Other	This rule is used to block crawlers used for other purposes, such as site monitoring, using access proxies, and web page analysis. **NOTE** To avoid being blocked by WAF, crawlers may use a large number of IP address proxies.	If you enable this rule, WAF detects and blocks crawlers that are used for various purposes.

Step 9 Select the **JavaScript** tab and change **Status** if needed.

JavaScript anti-crawler is disabled by default. To enable it, click  and then click **OK** in the displayed dialog box to toggle on  .

Protective Action: **Block** or **Log only**. You can also select **Verification code**. If the JavaScript challenge fails, a verification code is required. As long as the visitor provides a valid verification code, their request will not be restricted.

NOTICE

- Cookies must be enabled and JavaScript supported by any browser used to access a website protected by anti-crawler protection rules.
- If your service is connected to CDN, exercise caution when using the JS anti-crawler function.

  CDN caching may impact JS anti-crawler performance and page accessibility.

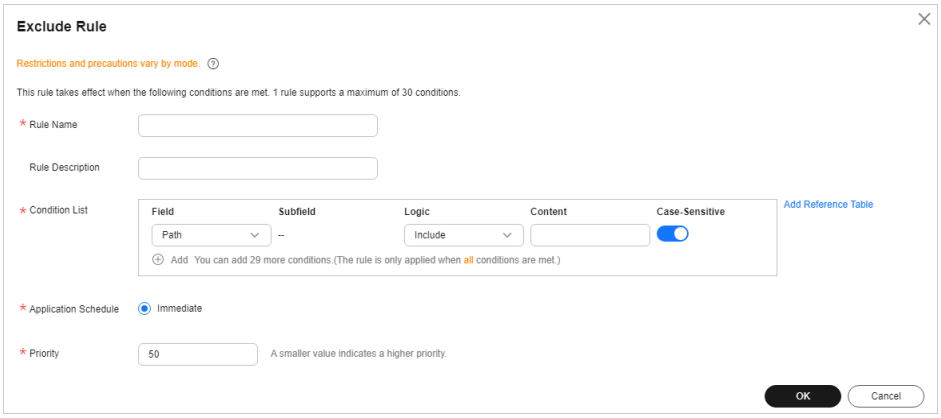
Step 10 Configure a JavaScript-based anti-crawler rule by referring to **Table 5-12**.

Two protective actions are provided: **Protect all requests** and **Protect specified requests**.

- To protect all requests except requests that hit a specified rule

  Set **Protection Mode** to **Protect all requests**. Then, click **Exclude Rule**, configure the request exclusion rule, and click **OK**.

  Figure 5-48 Exclude Rule



- To protect a specified request only

  Set **Protection Mode** to **Protect specified requests**, click **Add Rule**, configure the request rule, and click **OK**.

  Figure 5-49 Add Rule

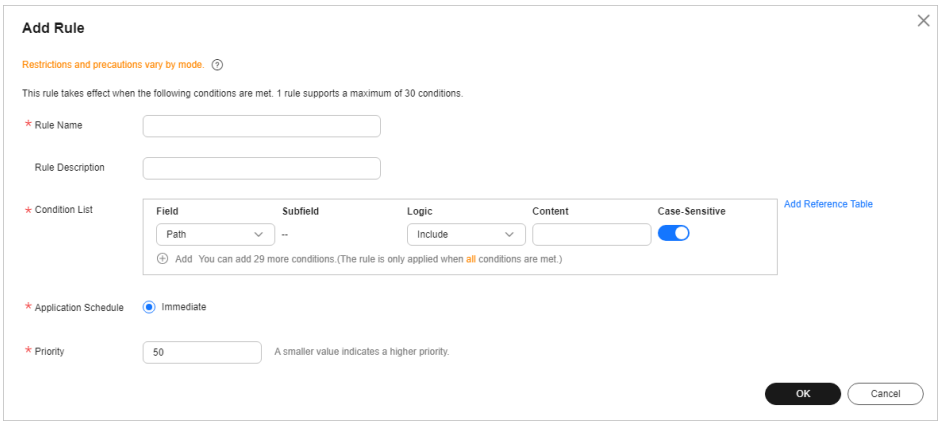


Table 5-12 Parameters of a JavaScript-based anti-crawler protection rule

Parameter	Description	Example Value
Rule Name	Name of the rule.	waf
Rule Description	A brief description of the rule. This parameter is optional.	-
Effective Date	Time the rule takes effect.	Immediate

Parameter	Description	Example Value
Condition List	Condition parameter description: • **Field**: Select the field you want to protect from the drop-down list. Currently, only **Path** and **User Agent** are included. • **Subfield** • **Logic**: Select a logical relationship from the drop-down list. **NOTE** If you set **Logic** to **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any of them**, **Suffix is any value**, or **Suffix is not any of them**, you need to select a reference table. • **Content**: Enter or select the content that matches the condition. • **Case-Sensitive**: This parameter can be configured if **Path** is selected for **Field**. If you enable this, the system matches the case-sensitive path. It helps the system accurately identify and handle various crawler requests, improving the accuracy and effectiveness of anti-crawler policies.	**Path Include /admin**
Priority	Rule priority. If you have added multiple rules, rules are matched by priority. The smaller the value you set, the higher the priority.	5

- After the configuration is complete, you can view the added rule in the protection rule list. **Rule Status** is **Enabled** by default.
- If you do not want the rule to take effect, click **Disable** in the **Operation** column of the rule.
- To delete or modify a rule, click **Delete** or **Modify** in the **Operation** column of the rule.

----End

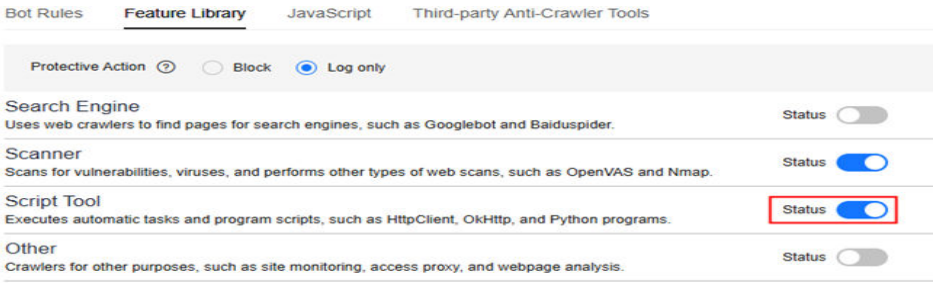
Configuration Example: Logging Script Crawlers Only

You can take the following steps to verify that WAF is protecting your website domain name (**www.example.com**) against an anti-crawler rule.

Step 1 Execute a JavaScript tool to crawl web page content.

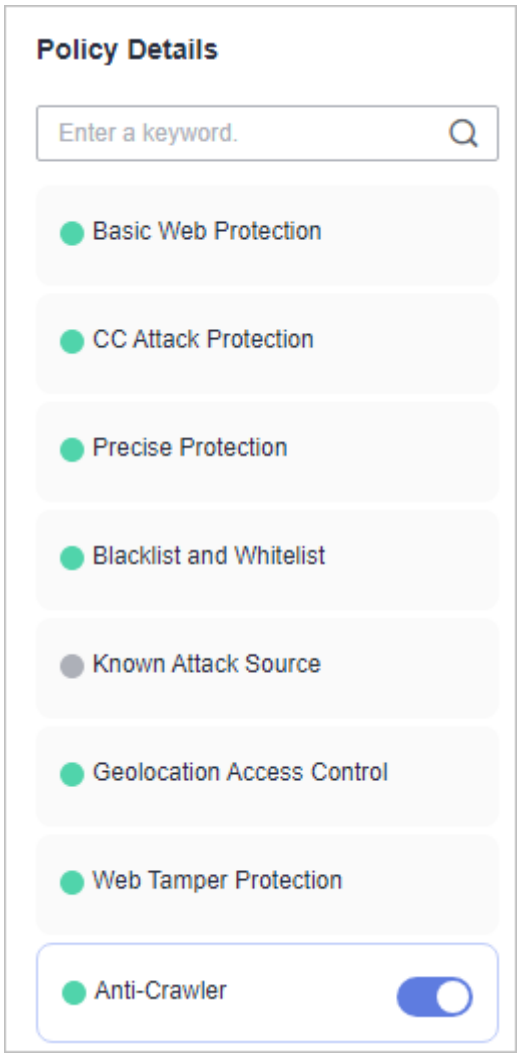
Step 2 On the **Feature Library** tab, enable **Script Tool** and select **Log only** for **Protective Action**. (If WAF detects an attack, it logs the attack only.)

Figure 5-50 Enabling Script Tool



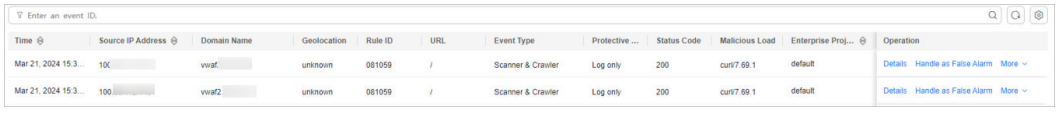
Step 3 Enable anti-crawler protection.

Figure 5-51 Anti-Crawler configuration area



Step 4 In the navigation pane on the left, choose **Events** to go to the **Events** page.

Figure 5-52 Viewing Events - Script crawlers



----End

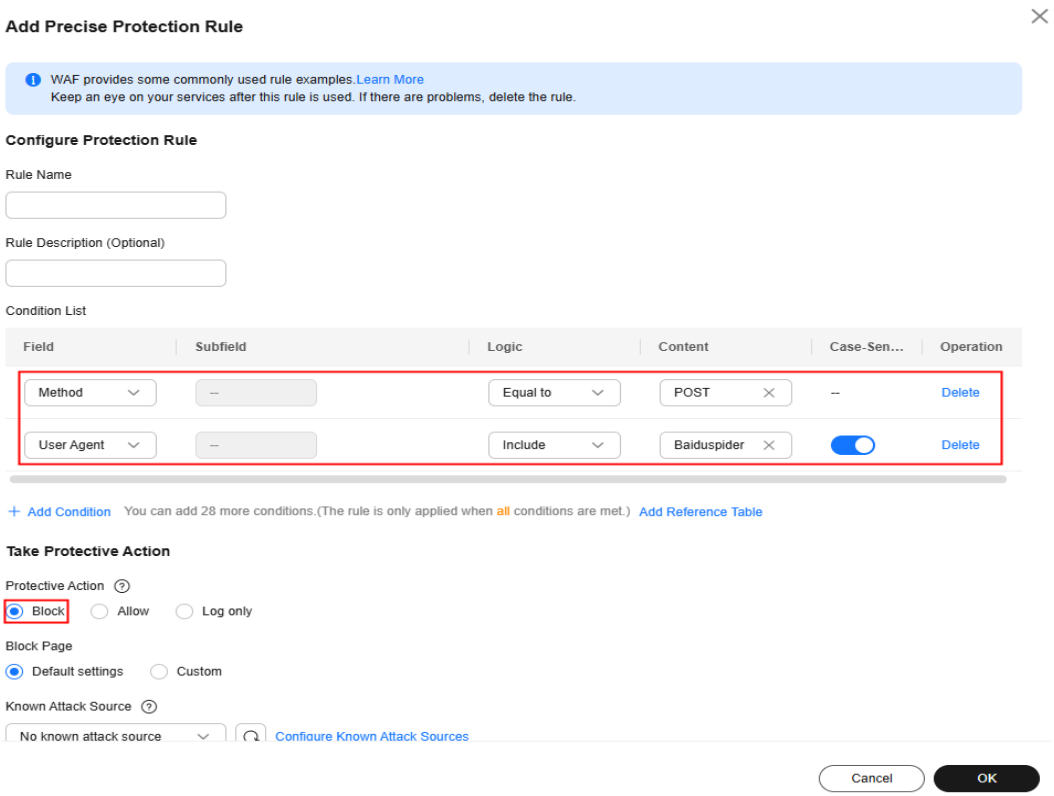
Configuration Example: Search Engine

To allow the search engine of Baidu or Google and block the POST request of Baidu:

Step 1 Set **Status** of **Search Engine** to  by referring to **Step 7**.

Step 2 Configure a precise protection rule by referring to **Configuring Custom Precise Protection Rules**.

Figure 5-53 Blocking POST requests



----End

FAQs

Why Does a Requested Page Fail to Respond to the Client After the JavaScript-based Anti-Crawler Is Enabled?

5.10 Configuring Information Leakage Prevention Rules to Protect Sensitive Information from Leakage

You can add two types of information leakage prevention rules.

- Sensitive information filtering: prevents disclosure of sensitive information, such as ID numbers, phone numbers 11-digit phone numbers registered in China, and email addresses.
- Response code interception: blocks the specified HTTP status codes.

Prerequisites

You have added the website you want to protect to WAF or **added a new protection policy**.

- For cloud CNAME access mode, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)**.
- For dedicated access mode, see **Connecting Your Website to WAF (Dedicated Mode)**.

Constraints

- This function is not supported by the cloud standard edition, or the cloud load balancer access mode.
- This function is not supported by the professional edition.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.

Configuring an Information Leakage Prevention Rule

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Click the **Information Leakage Prevention** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

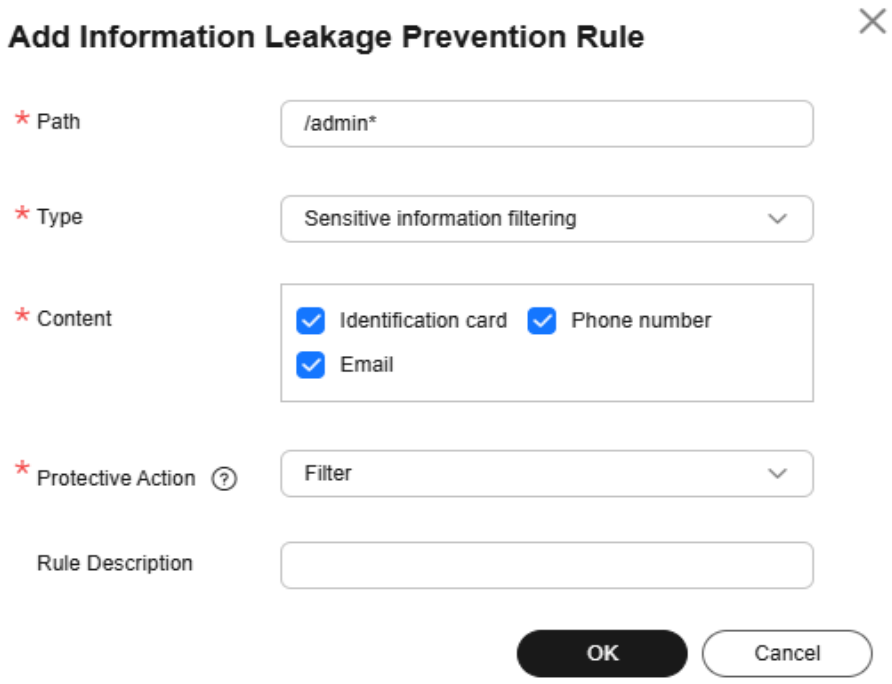
Step 8 In the upper left corner above the **Information Leakage Prevention** rule list, click **Add Rule**.

Step 9 In the dialog box displayed, add an information leakage prevention rule by referring to **Table 5-13**. **Figure 5-54** and **Figure 5-55** show the examples.

Information leakage prevention rules prevent sensitive information (such as ID numbers, phone numbers, and email addresses) from being disclosed. This type of rule can also block specified HTTP status codes.

Sensitive information filtering: Configure rules to mask sensitive information, such as phone numbers and ID numbers, from web pages. For example, you can set the following protection rules to mask sensitive information, such as ID numbers, phone numbers, and email addresses:

Figure 5-54 Sensitive information leakage



Response code interception: An error page of a specific HTTP response code may contain sensitive information. You can configure rules to block such error pages to prevent such information from being leaked out. For example, you can set the following rule to block error pages of specified HTTP response codes 404, 502, and 503.

Figure 5-55 Response code interception

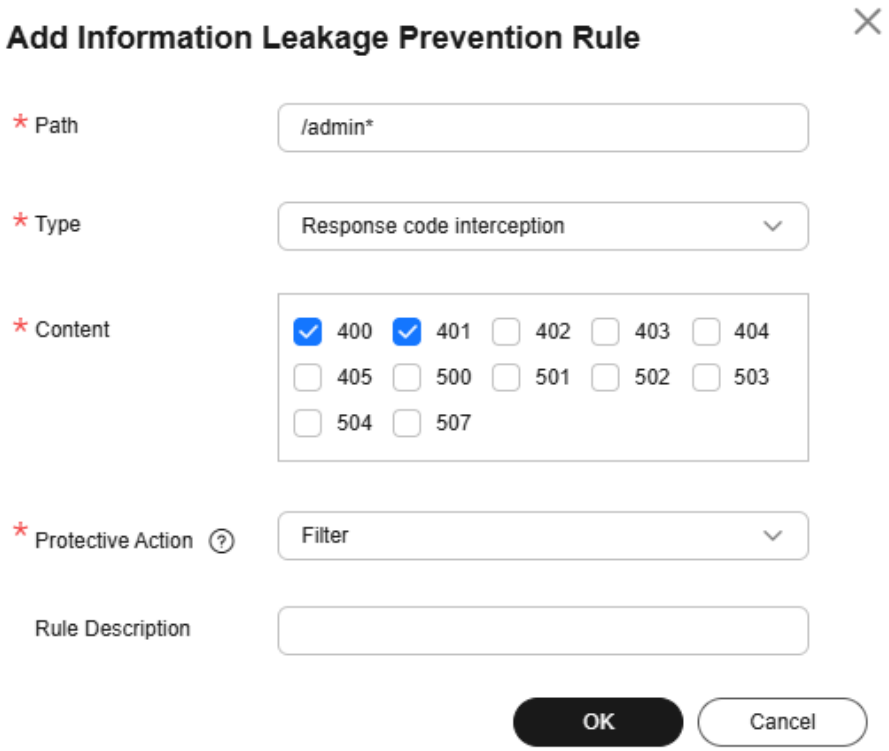


Table 5-13 Parameter description

Parameter	Description	Example Value
Path	A part of the URL that does not include the domain name. The URL can contain sensitive information (such as ID numbers, phone numbers, and email addresses) or a blocked error code. • Prefix match: Only the prefix of the path to be entered must match that of the path to be protected. If the path to be protected is **/admin**, set **Path** to **/admin***. • Exact match: The path to be entered must match the path to be protected. If the path to be protected is **/admin**, set **Path** to **/admin**. **NOTE** – The path supports prefix and exact matches only. Regular expressions are not supported. – The path cannot contain two or more consecutive slashes. For example, **///admin**. If you enter **///admin**, the WAF engine converts /// to /.	**/admin***

Parameter	Description	Example Value
Type	• **Sensitive information filtering** • **Response code interception**: Enable WAF to block the specified HTTP response code page.	**Sensitive information filtering**
Content	Information to be protected. Options are **Identification card**, **Phone number**, and **Email**.	**Identification card**
Protective Action	Action the rule takes. You can select **Filter** or **Log only**.	Filter
Rule Description	A brief description of the rule. This parameter is optional.	None

Step 10 Click **OK**. The added information leakage prevention rule is displayed in the list of information leakage prevention rules.

- After the configuration is complete, you can view the added rule in the protection rule list. **Rule Status** is **Enabled** by default.
- If you do not want the rule to take effect, click **Disable** in the **Operation** column of the rule.
- To delete or modify a rule, click **Delete** or **Modify** in the **Operation** column of the rule.

----End

Protection Verification

To verify that WAF is protecting your domain name (**www.example.com**) according to the protection rule configured by referring to example values in **Table 5-6**, take the following steps:

Step 1 Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

- If the website is inaccessible, connect the website domain name to WAF by following the instructions in **Website Settings**.
- If the website is accessible, go to **Step 2**.

Step 2 Clear the browser cache and access the **http://www.example.com/admin** page. If the sensitive information on the page is masked, the rule takes effect.

Step 3 Return to the WAF console. In the navigation pane on the left, click **Events**. On the displayed page, check event logs.

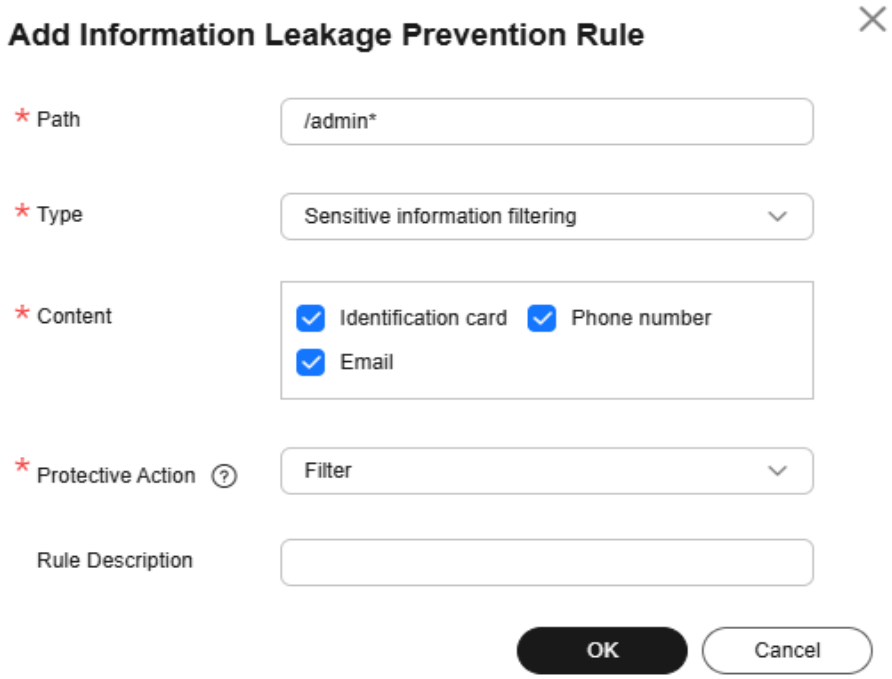
----End

Configuration Example: Masking Sensitive Information

You can take the following steps to verify that WAF is protecting your website domain name (**www.example.com**) based on the information leakage prevention rule you configure.

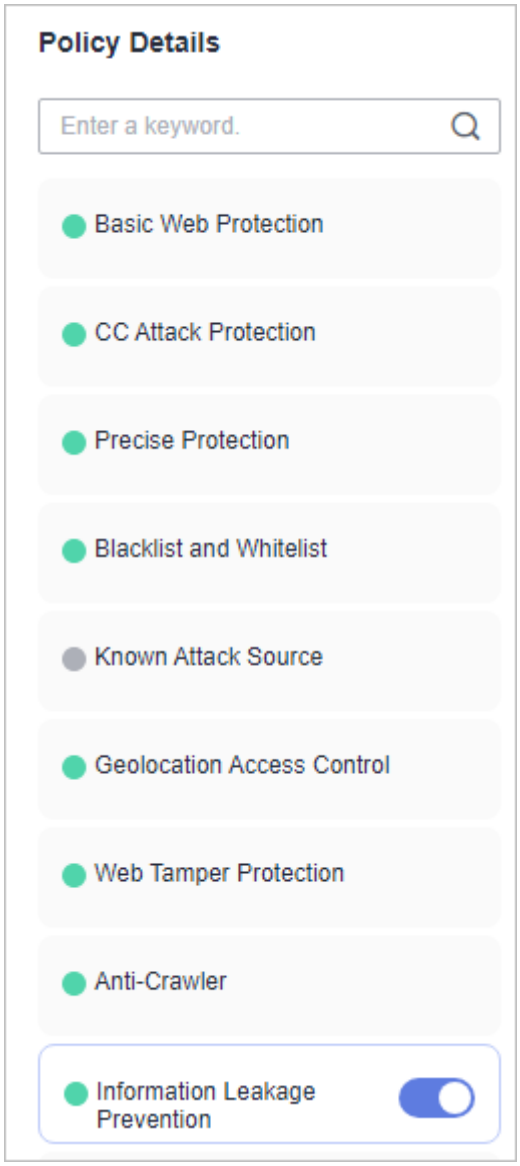
Step 1 Add an information leakage prevention rule.

Figure 5-56 Sensitive information leakage



Step 2 Enable information leakage prevention.

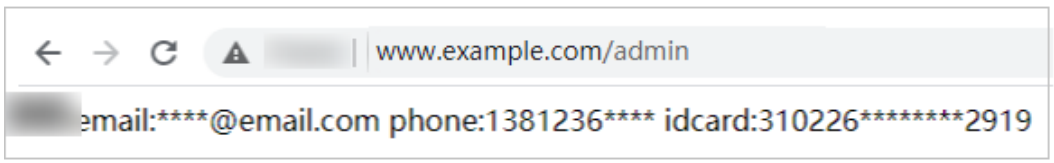
Figure 5-57 Information Leakage Prevention configuration area



Step 3 Clear the browser cache and access http://www.example.com/admin/.

The email address, phone number, and identity number on the returned page are masked.

Figure 5-58 Sensitive information masked



----End

5.11 Configuring a Global Protection Whitelist Rule to Ignore False Alarms

Once an attack hits a WAF basic web protection rule or a feature-library anti-crawler rule, WAF will respond to the attack immediately according to the protective action (**Log only** or **Block**) you configured for the rule and display an event on the **Events** page.

You can add false alarm masking rules to let WAF ignore certain rule IDs or event types (for example, skip XSS checks for a specific URL).

- If you select **All protection** for **Ignore WAF Protection**, all WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule.
- If you select **Basic Web Protection** for **Ignore WAF Protection**, you can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, if XSS check is not required for a URL, you can whitelist XSS rule.
- If you select **Invalid requests** for **Ignore WAF Protection**, WAF will whitelist invalid requests.

Prerequisites

- You have added the website you want to protect to WAF or **added a protection policy**.
  - For cloud CNAME access mode, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)**.
  - For cloud load balancer access mode, see **Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)**.
  - For dedicated mode, see **Connecting Your Website to WAF (Dedicated Mode)**.
- If you use a dedicated WAF instance, ensure that it has been upgraded to the latest version. For details, see **Managing Dedicated WAF Engines**.

Constraints

- If you select **All protection** for **Ignore WAF Protection**, all WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule.
- If you select **Basic web protection** for **Ignore WAF Protection**, global protection whitelist rules take effect only for events triggered against WAF built-in rules in **Basic Web Protection** and anti-crawler rules under **Feature Library**.
  - Basic web protection rules

    Basic web protection defends against common web attacks, such as SQL injection, XSS attacks, remote buffer overflow attacks, file inclusion, Bash vulnerability exploits, remote command execution, directory traversal, sensitive file access, and command and code injections. Basic web protection also detects web shells and evasion attacks.

  - Feature-based anti-crawler protection

    Feature-based anti-crawler identifies and blocks crawler behavior from search engines, scanners, script tools, and other crawlers.

- You can configure a global protection whitelist rule by referring to **Handling False Alarms**. After handling a false alarm, you can view the rule in the global protection whitelist rule list.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.

Configuring a Global Protection Whitelist

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Click the **Blacklist and Whitelist** configuration area and toggle it on or off if needed.

-  : enabled.
-  : disabled.

Step 8 In the upper left corner above the **Global Protection Whitelist** rule list, click **Add Rule**.

Step 9 Add a global whitelist rule by referring to **Table 5-14**.

Figure 5-59 Add Global Protection Whitelist Rule

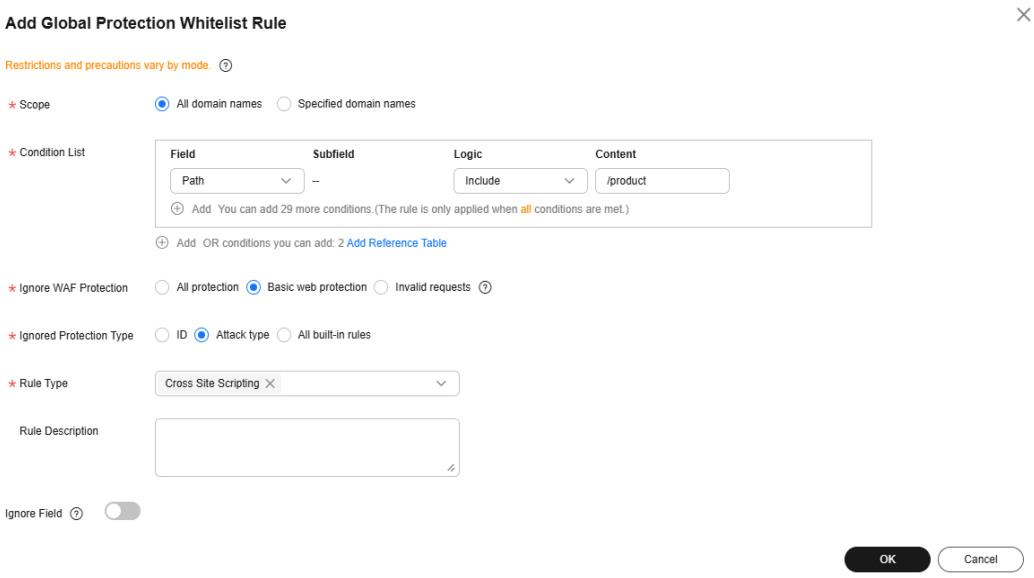


Table 5-14 Parameters

Parameter	Description	Example Value
Scope	• **All domain names**: By default, this rule will be applied to all domain names that are protected by the current policy. • **Specified domain names**: Specify a domain name range this rule applies to.	Specified domain names
Domain Name	This parameter is mandatory when you select **Specified domain names** for **Scope**. Enter a single domain name that matches the wildcard domain name being protected by the current policy. To add more domain names, click **Add** to add them one by one.	www.example.com

Parameter	Description	Example Value
Condition List	• Click **Add** in the condition box to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. • You can click **Add** outside the condition box to add a group of conditions. A maximum of three condition groups can be added. The **OR** logic is used between all condition groups. So, the rule works as long as one condition group is met. Condition parameter description: • **Field** • **Subfield**: Configure this field only when **IPv4**, **IPv6**, **Params**, **Cookie**, **Header** or **Response Header** is selected for **Field**. If **Field** is set to **Response Header** or **Header**, and **Subfield** is not **All** or **Any**, **Case Sensitive** is supported. **NOTICE** A subfield cannot exceed 2,048 characters. • **Logic**: Select a logical relationship from the drop-down list. • **Content**: Enter or select the content that matches the condition.	**Field** is set to **Path**. **Logic** is set to **Include**. **Content** is set to **/product**.

Parameter	Description	Example Value
Ignore WAF Protection	• **All protection**: All WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule. • **Basic web protection**: You can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, if XSS check is not required for a URL, you can whitelist XSS rule. • **Invalid requests**: WAF can allow invalid requests. **NOTE** A request is invalid if: – The request header contains more than 512 parameters. – The URL contains more than 2,048 parameters. – The request header contains "Content-Type:application/x-www-form-urlencoded", and the request body contains more than 8,192 parameters.	Basic web protection
Ignored Protection Type	If you select **Basic web protection** for **Ignored WAF Protection**, select one of the following for **Ignored Protection Type**: • **ID**: Configure the rule by event ID. • **Attack type**: Configure the rule by attack type, such as XSS and SQL injection. One type contains one or more rule IDs. • **All built-in rules**: all checks enabled in **Basic Web Protection**.	Attack type
Rule ID	This parameter is mandatory when you select **ID** for **Ignored Protection Type**. Rule ID of a misreported event in **Events** whose type is not **Custom**. You are advised to handle false alarms on the **Events** page.	041046

Parameter	Description	Example Value
Rule Type	This parameter is mandatory when you select **Attack type** for **Ignored Protection Type**. Select an attack type from the drop-down list box. WAF can defend against XSS attacks, web shells, SQL injection attacks, malicious crawlers, remote file inclusions, local file inclusions, command injection attacks, and other attacks.	SQL injection
Rule Description	A brief description of the rule. This parameter is optional.	SQL injection attacks are not intercepted.
Ignore Field	To ignore attacks of a specific field, specify the field in the **Advanced Settings** area. After you add the rule, WAF will stop blocking attacks matching the specified field. Select a target field from the first drop-down list box on the left. The following fields are supported: **Params**, **Cookie**, **Header**, **Body**, and **Multipart**. • If you select **Params**, **Cookie**, or **Header**, you can select **All** or **Field** to configure a subfield. • If you select **Body** or **Multipart**, you can select **All**. • If you select **Cookie**, the **Domain Name** box for the rule can be empty. **NOTE** If **All** is selected, WAF will not block all attack events of the selected field.	Params All

Step 10 Click **OK**.

- After the configuration is complete, you can view the added rule in the protection rule list. **Rule Status** is **Enabled** by default.
- If you do not want the rule to take effect, click **Disable** in the **Operation** column of the rule.
- To delete or modify a rule, click **Delete** or **Modify** in the **Operation** column of the rule.

----End

Protection Verification

To verify that WAF is protecting your domain name (**www.example.com**) according to the protection rule configured by referring to example values in **Table 5-14**, take the following steps:

Step 1 Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

- If the website is inaccessible, connect the website domain name to WAF by following the instructions in **Website Settings**.
- If the website is accessible, go to **Step 2**.

Step 2 Simulate an XSS attack.

Step 3 Return to the WAF console. In the navigation pane on the left, click **Events**. On the displayed page, check event logs.

----End

5.12 Configuring Data Masking Rules to Prevent Privacy Information Leakage

This topic describes how to configure data masking rules. You can configure data masking rules to prevent sensitive data such as passwords from being displayed in event logs.

Prerequisites

- You have added the website you want to protect to WAF or **added a protection policy**.
  - For cloud CNAME access mode, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)**.
  - For cloud load balancer access mode, see **Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)**.
  - For dedicated mode, see **Connecting Your Website to WAF (Dedicated Mode)**.
- If you use a dedicated WAF instance, ensure that it has been upgraded to the latest version. For details, see **Managing Dedicated WAF Engines**.

Constraints

It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.

Impact on the System

Sensitive data in the events will be masked to protect your website visitor's privacy.

Configuring a Data Masking Rule

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Click the **Data Masking** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

Step 8 In the upper left corner above the **Data Masking** rule list, click **Add Rule**.

Step 9 In the displayed dialog box, specify the parameters described in Table 5-15.

Figure 5-60 Adding a data masking rule

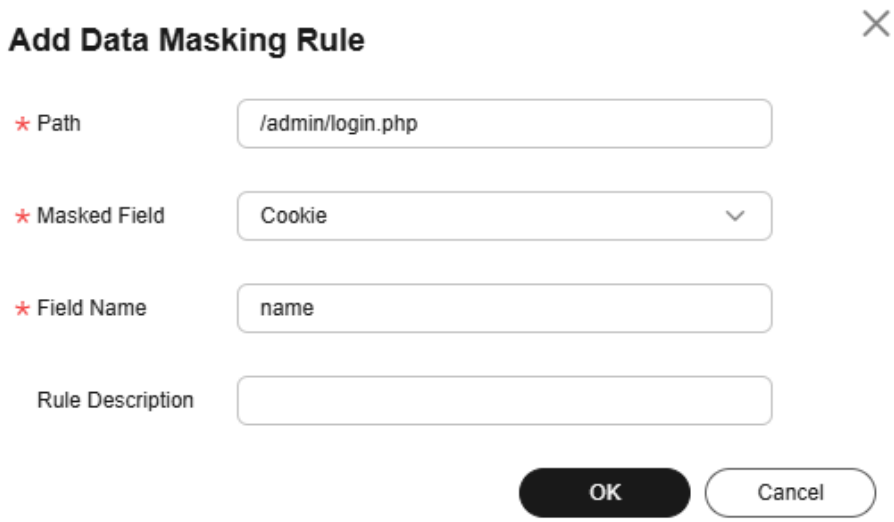


Table 5-15 Rule parameters

Parameter	Description	Example Value
Path	Part of the URL that does not include the domain name. • Prefix match: The path ending with * indicates that the path is used as a prefix. For example, if the path to be protected is **/admin/test.php** or **/adminabc**, set **Path** to **/admin***. • Exact match: The path to be entered must match the path to be protected. If the path to be protected is **/admin**, set **Path** to **/admin**. **NOTE** • The path supports prefix and exact matches only and does not support regular expressions. • The path cannot contain two or more consecutive slashes. For example, **///admin**. If you enter **///admin**, WAF converts **///** to **/**.	/admin/login.php For example, if the URL to be protected is **http://www.example.com/admin/login.php**, set **Path** to **/admin/login.php**.
Masked Field	A field set to be masked • **Params**: A request parameter • **Cookie**: A small piece of data to identify web visitors • **Header**: A user-defined HTTP header • **Form**: A form parameter	• If **Masked Field** is **Params** and **Field Name** is **id**, content that matches **id** is masked. • If **Masked Field** is **Cookie** and **Field Name** is **name**, content that matches **name** is masked.
Field Name	Set the parameter based on **Masked Field**. The masked field will not be displayed in logs.	
Rule Description	A brief description of the rule. This parameter is optional.	None

Step 10 Click **OK**. The added data masking rule is displayed in the list of data masking rules.

- After the configuration is complete, you can view the added rule in the protection rule list. **Rule Status** is **Enabled** by default.
- If you do not want the rule to take effect, click **Disable** in the **Operation** column of the rule.
- To delete or modify a rule, click **Delete** or **Modify** in the **Operation** column of the rule.

----End

Protection Verification

To verify that WAF is protecting your domain name (**www.example.com**) according to the protection rule configured by referring to example values in **Table 5-15**, take the following steps:

Step 1 Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

- If the website is inaccessible, connect the website domain name to WAF by following the instructions in **Website Settings**.
- If the website is accessible, go to **Step 2**.

Step 2 Clear the browser cache and access the **http://www.example.com/admin** page. If the configured **jsessionid** cookie field is masked in the **/admin** directory, the rule takes effect.

Step 3 Return to the WAF console. In the navigation pane on the left, click **Events**. On the displayed page, check event logs.

----End

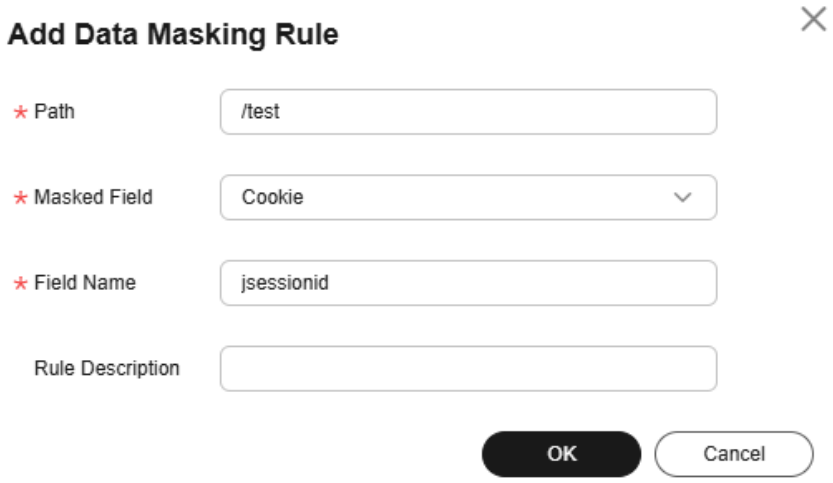
Configuration Example: Masking the Cookie Field

You can take the following steps to verify that WAF is protecting your website domain name (**www.example.com**).

The cookie field **jsessionid** is masked.

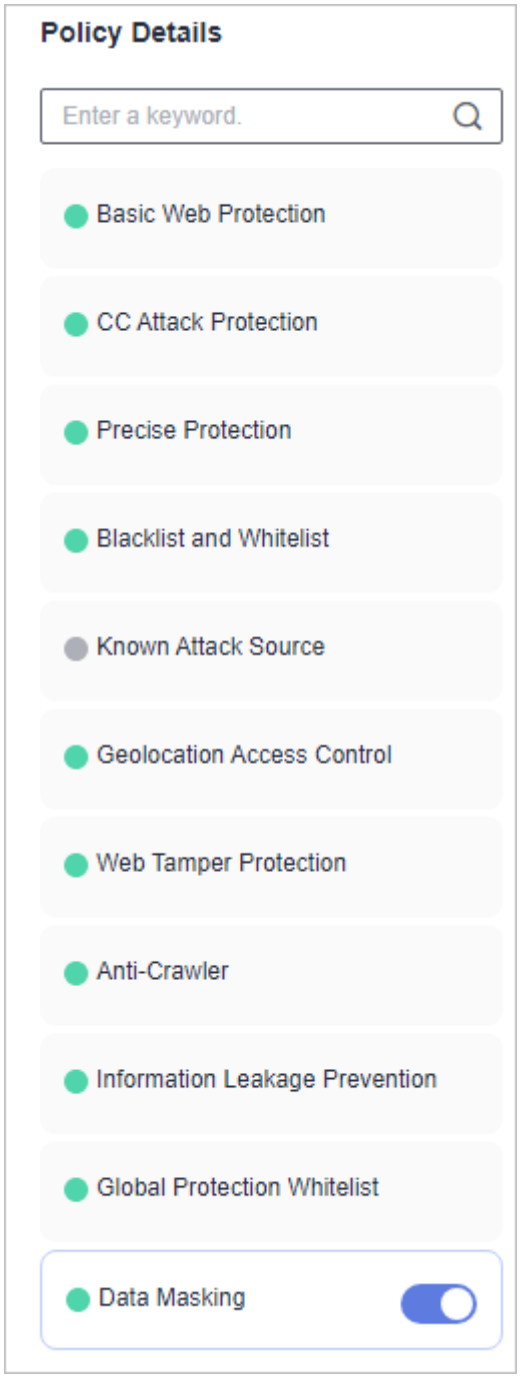
Step 1 Add a data masking rule.

Figure 5-61 Select **Cookie** for **Masked Field** and enter **jsessionid** in **Field Name**.



Step 2 Enable data masking.

Figure 5-62 Data Masking configuration area

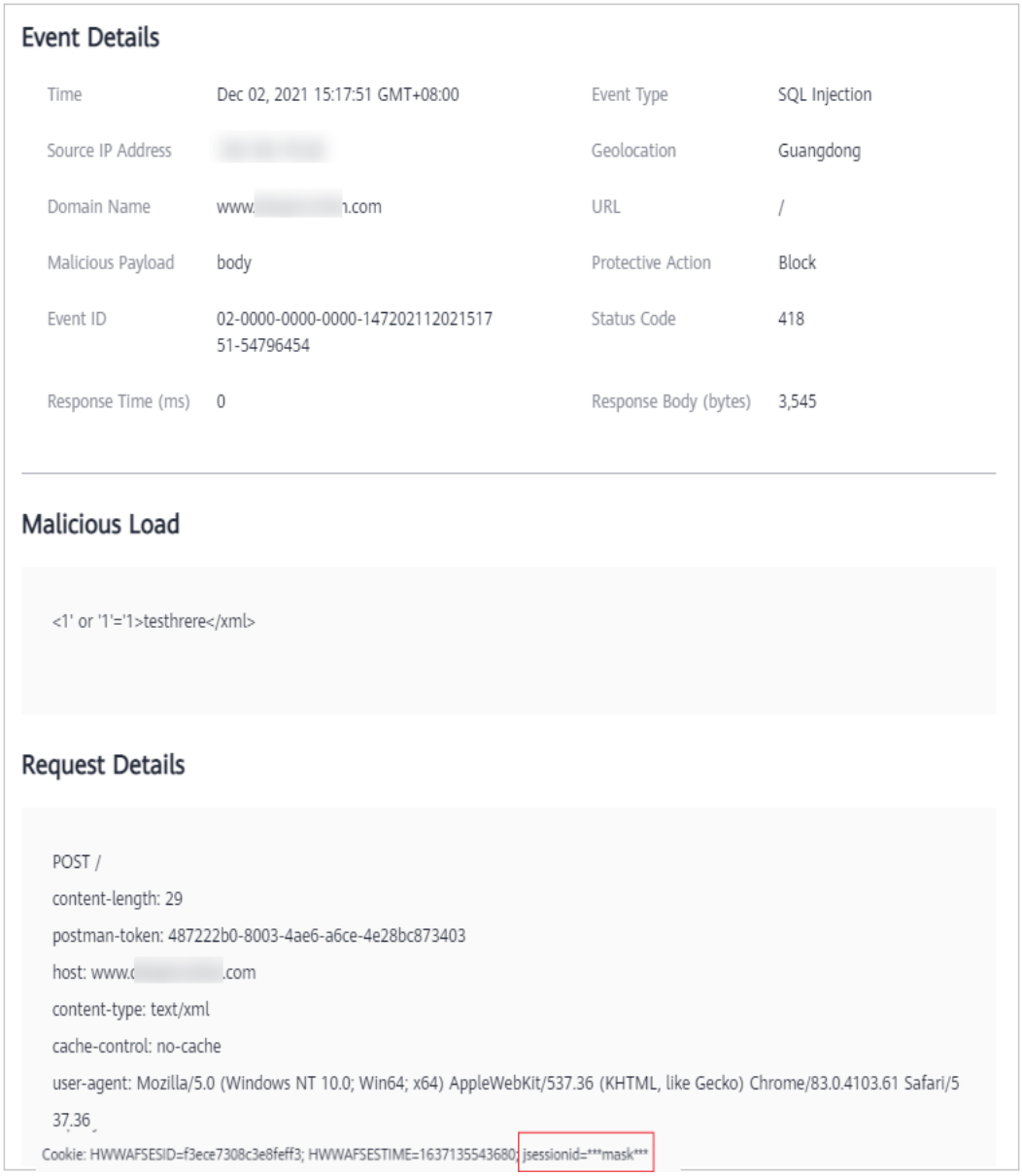


Step 3 In the navigation pane on the left, choose **Events**.

Step 4 In the row containing the event hit the rule, click **Details** in the **Operation** column and view the event details.

Data in the **jsessionid** cookie field is masked.

Figure 5-63 Viewing events - privacy data masking



----End

5.13 Configuring a Scanning Blocking Rule to Automatically Block Heavy-Traffic Attacks

The scanning protection module identifies scanning behaviors and scanner features to prevent attackers or scanners from scanning websites at scale. WAF will automatically block heavy traffic web attacks and directory traversal attacks and block the source IP addresses for a period of time, helping reduce intrusion risks and junk traffic.

- **Scanning Blocking**: If an attack source triggers basic protection rules for more than the threshold you specify, WAF blocks the source for a duration you configure.

- **Directory Traversal Protection**: If an attack source requests a large number of non-existent directories within a short period, which triggers too many 404 responses, WAF blocks the source for a length of time you configure.

Prerequisites

You have added a website to WAF or **added a protection policy**.

- For cloud CNAME access mode, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)**.
- For dedicated mode, see **Connecting Your Website to WAF (Dedicated Mode)**.

Constraints

- This function is not supported by the cloud standard edition, or the cloud load balancer access mode.
- It takes several minutes for a new rule to take effect. After a rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.

Configuring a Scanning Protection Rule

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Click the **Scanning Protection** configuration area and toggle it on or off if needed.

-  : enabled.
-  : disabled.

Step 8 Configure **Scanning Blocking**.

If an attack source triggers basic protection rules for more than the threshold you specify, WAF blocks the source for a duration you configure.

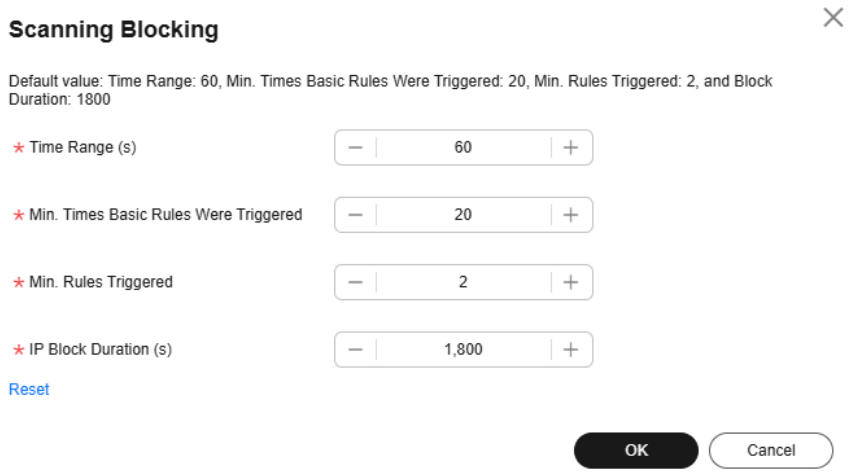
1. Click  to enable **Scanning Blocking**.
2. Select a protective action.
   - **Block**: WAF blocks and logs detected attacks.
   - **Log only**: WAF only logs detected attacks.

3. Click and edit the rule information.

   Default value: **Time Range**: 60 seconds; **Min. Times Basic Rules Were Triggered**: 20, **Min. Rules Triggered**: 2; and **Block Duration**: 1,800 seconds. So, if more than two types of basic web protection rules were triggered for more than 20 times within 60 seconds, the source IP address will be blocked for 1,800 seconds.

   You can adjust the value as required.

Figure 5-64 Scanning Blocking



Step 9 Configure **Directory Traversal Protection**.

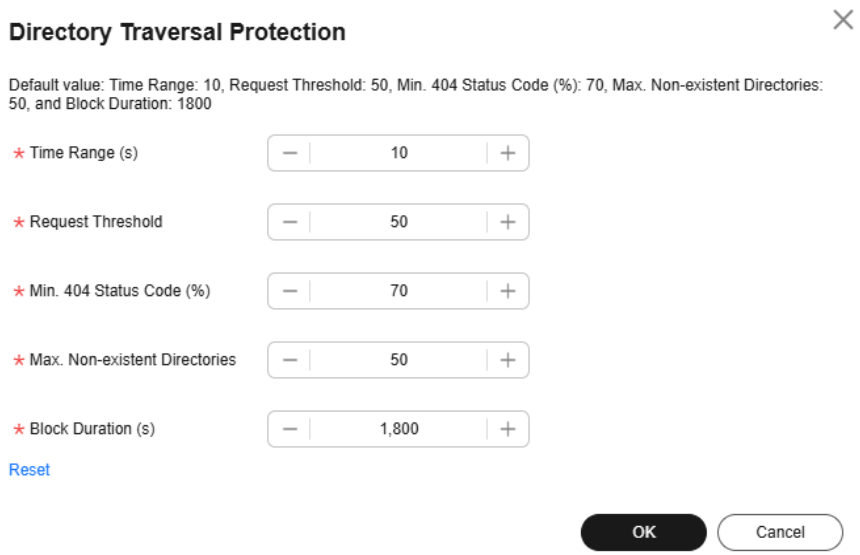
WAF will block attack sources that trigger the basic protection rule configured for the protected website many times for a period.

1. Click to enable directory traversal protection.
2. Select a protective action.
   - **Block**: WAF blocks and logs detected attacks.
   - **Log only**: WAF only logs detected attacks.
3. Click and edit the rule information.

   Default value: **Time Range**: 10 seconds; **Request Threshold**: 50 requests; **Min 404 Status Code (%)**: 70%; **Max. Non-existent Directories**: 50; and **Block Duration**: 1,800 seconds. So, for the protected object, if there are more than 50 requests, with 404 requests accounting for over 70%, and 50 non-existent directories detected, the source IP address will be blocked for 1,800 seconds.

   You can adjust the value as required.

Figure 5-65 Directory Traversal Protection



----End

One-Click Unblocking Scanning Blocking and Directory Traversal Protection

This operation will unblock all blocked IP addresses triggered by **Scanning Blocking** or **Directory Traversal Protection** for the current policy. These IP addresses will still be blocked in other policies.

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 On the **Protection Status** tab, click the **Scanning Protection** configuration box. In the upper right corner of the **Scanning Protection** list, click **One-Click Unblocking**.

CAUTION

This operation will unblock all IP addresses that trigger IP address scanning blocking in the current policy. If an IP address triggers the scanning protection rule again, the IP address will be blocked for a period of time according to the rule.

Step 7 In the **One-Click Unblocking** dialog box, click **OK**.

All IP addresses that triggered scanning blocking in the current policy will be unblocked.

----End

Protection Verification

To verify that WAF is protecting your domain name (**www.example.com**) according to the protection rule configured by referring to example values in **Table 5-15**, take the following steps:

Step 1 Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

- If the website is inaccessible, connect the website domain name to WAF by following the instructions in **Website Settings**.
- If the website is accessible, go to **Step 2**.

Step 2 Clear the browser cache and access the **http://www.example.com** page for 20 times within 60 seconds. If the access is blocked for 1,800 seconds, the rule takes effect.

Step 3 Return to the WAF console. In the navigation pane on the left, click **Events**. On the displayed page, check event logs.

----End

5.14 Configuring Bot Protection Rules to Defend Against Bot Behavior

There are four bot protection checks: known bot detection, signature-based request detection, bot behavior detection, and proactive feature detection. With such layered bot detection, WAF can accurately identify and manage bot behavior in website traffic, effectively reducing risks such as data leakage and performance deterioration caused by bot attacks.

NOTE

To enable this function, **submit a service ticket**.

Function

WAF bot protection provides the following functions.

Custom Protected Objects

If you enable bot protection, WAF protects all URLs of the protected domain name by default. You can specify protected objects for bot protection rules if you want WAF to protect specific service scenarios, such as login and registration.

The following table lists the conditions that can be used to specify protected objects for bot protection rules.

Table 5-16 Condition list

Field	Field Description	Subfield	Logic	Content
Path	The path of a resource requested by the client. A path is part of a URL.	--	The following logical relationships are supported: **Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, and **Prefix is not any value**. **NOTE** If the logical relationship is **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, or **Prefix is not any value**, you can select an existing reference table for **Content**. For details about how to add and manage a reference table, see **Creating a Reference Table to Configure Protection Indicators in Batches**.	Enter the path to be protected. Configuration description: • The path does not contain a domain name and supports only exact match. So, the path to be protected must be the same as the path you configure. If the path to be protected is **/admin**, set **Path** to **/admin**. • If **Path** is set to **/**, all paths of the website are protected. • The path content cannot contain the following special characters: (<>*)
Method	The request method.	--	The following logical relationships are supported: **Equal to** and **Not equal to**.	Enter the request method, for example, GET, POST, PUT, DELETE, or PATCH.

Field	Field Description	Subfield	Logic	Content
Cookie	The cookie in the request.	Custom subfield. Length: 1 to 2,048 characters.	The following logical relationships are supported: **Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, **Suffix is not**, **Has**, **Does not have**, **Equal to any value**, **Not equal to any value**, and **Exclude any value**. **NOTE** If the logical operator is **Equal to any value**, **Not equal to any value**, or **Exclude any value**, you can select an existing reference table for **Content**. For details about how to add and manage a reference table, see **Creating a Reference Table to Configure Protection Indicators in Batches**.	Enter the cookie value of the request, for example, jsessionid.
Header	The request header content.			Enter the request header content, for example, *text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8*.
Params	The query parameter in the URL. The query parameter is the content following the question mark (?).			Enter the query parameter, for example, 201901150929.
Referer	The source of the access request.	--		Enter the request access source. For example, if the protected path is **/admin/xxx** and you do not want visitors to be able to access the page from **www.test.com**, set **Content** for **Referer** to **http://www.test.com**.

Known Bot Detection

Known bot detection is the first step. It compares the user agent (UA) keywords carried in user requests with the UA signature database in bot protection. If a request is from a known bot (known client), the request will be handled based on the configured protective action.

Based on the open-source UA signature intelligence on the Internet and the UA signature library of WAF for anti-crawler protection, WAF can detect 10 types of known bots.

Type	Description
Search engine bots	Search engines use web crawlers to aggregate and index online content (such as web pages, images, and other file types). They provide search results in real time.
Online scanners	An online scanner typically scans assets on the Internet for viruses or vulnerabilities that are caused by configuration errors or programming defects and exploits such weak points to launch attacks. Typical scanners include Nmap, sqlmap, and WPSec.
Web crawlers	Popular crawler tools or services on the Internet. They are often used to capture any web page and extract content to meet user requirements. Scrapy, Pyspider, and Prerender are typical ones.
Website development and monitoring bots	Some companies use robots to provide services and help web developers monitor status of their sites. These bots can check the availability of links and domain names, connections and web page loading time for requests from different geographical locations, DNS resolution issues, and other functions.
Business analysis and marketing bots	A company offering business analysis and marketing services utilizes bots to evaluate website content, conduct audience and competitor analysis, support online advertising and marketing campaigns, and optimize website or web page rankings in search engine results.
News and social media bots	News and social media platforms allow users to browse hot news, share ideas, and interact with each other online. Many enterprises' marketing strategies include operating pages on these websites and interacting with consumers about products or services. Some companies use robots to collect data from these platforms for insights into media trends and products, enriching network experience.
Screenshot bots	Some companies use bots to provide website screenshot services. It can take complete long-screen screenshots of online content such as posts on websites and social networks, news, and posts on forums and blogs.
Academic and research bots	Some universities and companies use bots to collect data from various websites for academic or research purposes, including reference search, semantic analysis, and specific types of search engines.
RSS feed reader	RSS uses the standard XML web feed format to publish content. Some Internet services use bots to aggregate information from RSS feeds.

Type	Description
Online archiver	Some organizations such as Wikipedia use bots to periodically crawl and archive valuable online information and content copies. These web archiving services are very similar to search engines, but the data provided is not up-to-date. They are mainly used for research.

Signature-based Request Detection

Signature-based request detection is the second step. This approach identifies the HTTP request header features in user requests, matches mainstream development frameworks and HTTP libraries, stimulates known bots, and uses automated programs to detect bots. If a request matches a bot signature, the request will be handled based on the configured protective action.

Type	Description
Abnormal request header	A request header that does not contain User Agent or whose User Agent is empty is abnormal.
Impersonators of known bots	If this function is enabled, the system checks whether the source IP address of a known bot request is its valid client IP address to prevent spoofing.
Development frameworks and HTTP libraries	A mainstream development framework and HTTP library have the following features: aiohttp, Apache-HttpClient, Apache-HttpAsyncClient, Commons-HttpClient, HttpComponents, PhantomJS, CakePHP, curl, Jetty, wget, http-kit, python-requests, Ruby, WebClient, WinHttpRequest, HttpUrlConnection, OxfordCloudService, http_request2, PEAR HTTPRequest, Python-urllib, RestSharp, Mojolicious (Perl), PHP, libwww-perl, okhttp, HTMLParser, Go-http-client, axios, Dispatch, LibVLC, node-superagent, curb, Needle, IPWorks, lwp-trivial, Custom-AsyncHttpClient, Convertify, AsyncHttpClient, Embed PHP Library, Apache Synapse, node-fetch, electron-fetch, asynchttp, Dolphin http client, EventMachine HttpClient, httpunit, Zend_Http_Client, Python-httplib2, spray-can, http_requester, AndroidDownload-Manager, bluefish, Java, git, and Prerender.cloud
Automation program	The service can detect automation programs with crawler behavior characteristics but unclear purposes.

Bot Behavior Detection

Bot behavior detection is the third step. WAF uses an AI protection engine to analyze and automatically learn requests, and then handles the attack behavior based on the configured behavior detection score and protective action.

You can set three score ranges for bot behavior detection. Score range: 0 to 100. A score closer to 0 indicates that the request feature is more like a normal request, and a score closer to 100 indicates that the request feature is more like a bot.

Proactive Feature Detection

⚠ CAUTION

- Currently, proactive feature detection can check traffic of websites that are connected to WAF in cloud CNAME access mode or dedicated mode. **Currently, proactive feature detection is not supported in cloud load balance access mode.**
- Currently, proactive feature detection supports only web browser services. Before enabling this function, ensure that the protected object is a browser client. Alternatively, configure matching conditions to ensure that the resources can be accessed only by web browsers. Otherwise, mobile app access may be affected.

Proactive feature detection is the fourth phase during bot detection. The system injects JavaScript code into HTML responses to monitor and verify the client browser's runtime environment, including keyboard and mouse interaction behaviors. In this way, the system can identify requests from tools and normal requests, and handle bot attacks based on the **interaction confidence** and protective action.

Interaction confidence indicates the frequency of interactions (such as keyboard and mouse operations) generated by a client within a period of time. A lower confidence level indicates a lower frequency of client interactions and a higher probability that the client is an automation program. A higher confidence level indicates a higher probability that the client is a normal user operation.

The confidence levels are as follows:

- **Skip**: Do not detect interactions. For example, if you enable proactive feature detection rules and set the interaction confidence to **Skip**, the system does not count the keyboard and mouse interactions of the client. If the interaction confidence is set to a low value, the client that has not generate keyboard and mouse interactions will be blocked.
- **High**: More than 10 interactions are generated within 600s.
- **Medium**: More than 5 interactions are generated within 600s.
- **Low**: More than 0 interactions are generated within 600s.

If a client accesses the protected website for the first time or does not send any requests to the website within 600 seconds, the request is allowed.

Constraints

This type of protection rule is only supported by cloud WAF and dedicated WAF instances of the network interface type. This type of protection rule is not supported by dedicated WAF instances of the ECS type.

Prerequisites

- You have connected the website you want to protect to WAF. For details, see **Connecting a Website to WAF**.
- At least one protection rule has been configured for the domain name. For details, see **Configuring Protection Policies**.
- You have created a policy, and this policy has not been shared with others.

  This function cannot be configured in shared policies.

Configuring a Bot Protection Rule

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 On the **Protection Status** tab, toggle **Bot Rules** on.

 : enabled.

Step 8 On the **Custom Protected Objects** tab, click **Add Protected Object Feature**, set **Field**, **Subfield**, **Logic**, and **Content**, and click **Save**.

If you enable bot protection, WAF protects all URLs of the protected domain name by default. You can specify protected objects for bot protection rules if you want WAF to protect specific service scenarios, such as login and registration.

- The following table lists the conditions that can be matched by protected objects in bot rules.

Table 5-17 Condition list

Field	Field Description	Subfield	Logic	Content
Path	The path of a resource requested by the client. A path is part of a URL.	--	The following logical relationships are supported: **Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, and **Prefix is not any value**. **NOTE** If the logical relationship is **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, or **Prefix is not any value**, you can select an existing reference table for **Content**. For details about how to add and manage a reference table, see **Creating a Reference Table to Configure Protection Indicators in Batches**.	Enter the path to be protected. Configuration description: – The path does not contain a domain name and supports only exact match. So, the path to be protected must be the same as the path you configure. If the path to be protected is **/admin**, set **Path** to **/admin**. – If **Path** is set to **/**, all paths of the website are protected. – The path content cannot contain the following special characters: (<>*)
Method	The request method.	--	The following logical relationships are supported: **Equal to** and **Not equal to**.	Enter the request method, for example, GET, POST, PUT, DELETE, or PATCH.

Field	Field Description	Subfield	Logic	Content
Cookie	The cookie in the request.	Custom subfield. Length: 1 to 2,048 characters.	The following logical relationships are supported: **Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, **Suffix is not**, **Has**, **Does not have**, **Equal to any value**, **Not equal to any value**, and **Exclude any value**. **NOTE** If the logical operator is **Equal to any value**, **Not equal to any value**, or **Exclude any value**, you can select an existing reference table for **Content**. For details about how to add and manage a reference table, see **Creating a Reference Table to Configure Protection Indicators in Batches**.	Enter the cookie value of the request, for example, jsessionid.
Header	The request header content.			Enter the request header content, for example, *text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8*.
Params	The query parameter in the URL. The query parameter is the content following the question mark (?).			Enter the query parameter, for example, 201901150929.
Referer	The source of the access request.	--		Enter the request access source. For example, if the protected path is **/admin/xxx** and you do not want visitors to be able to access the page from **www.test.com**, set **Content** for **Referer** to **http://www.test.com**.

- Click **Add Rule** and add more than one protected object. A maximum of 10 protected objects can be added.
- If there are multiple rules, the **AND** operator is used. The feature cannot be matched unless all rules are met.

After the preceding configurations are complete, you can **view**, **modify**, or **delete** the configured rules in the protected object feature list.

Step 9 On the **Known bots**, **Signature-based requests**, **Proactive feature detection**, or **Bot behavior** card, configure rules.

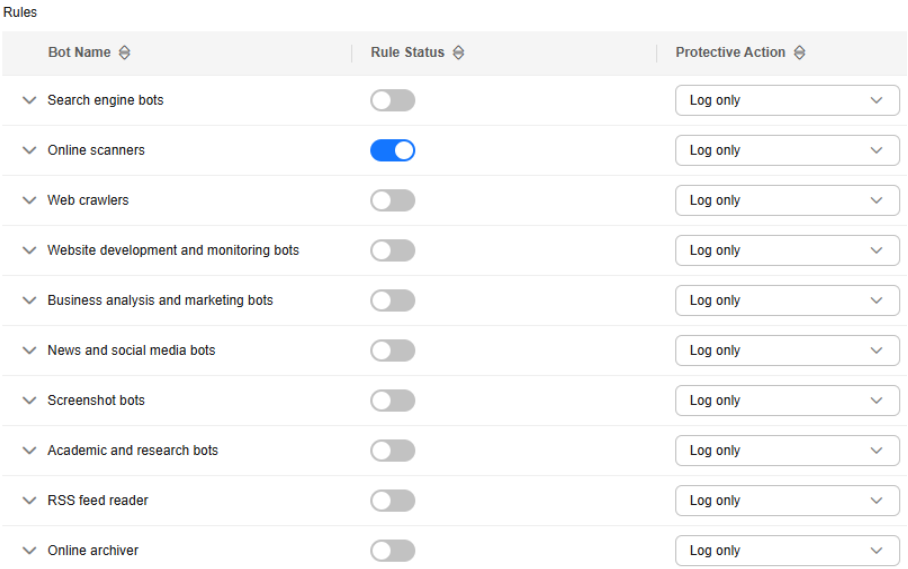
----End

Known Bot Detection

Step 1 Click the **Known bots** card and toggle **Status** on.

- Figure 5-66 shows the default configurations after you enable this function.

Figure 5-66 Known bots



- Click ⌄ on the left of the protection rule to view the details about and features of the protection rule.

Step 2 Enable or disable a specific rule and configure protective actions based on your service requirements.

The protective actions are as follows:

- **Log only**: WAF only logs requests that match the features.
- **JS Challenge**: After identifying the feature, WAF returns a segment of JavaScript code that can be automatically executed by a normal browser to the client. If the client properly executes the JavaScript code, WAF allows all requests from the client within a period of time (30 minutes by default). During this period, no verification is required. If the client fails to execute the code, WAF blocks the requests.

  NOTE

  If the referer in the request is different from the current host, the JS challenge does not work.

- **Block**: WAF blocks requests that match the features.
- **Advanced CAPTCHA**: After a request matches feature conditions, CAPTCHA is required for the visitor. If the verification is successful, the request is allowed in a period of time (default: 30 minutes). If the verification fails, the CAPTCHA code is updated and a new-round verification is required again.

NOTE

- The cloud load balancer access mode does not support this protective action.
- If you want to select **Advanced CAPTCHA** for **Protective Action**, make sure requests from a client IP address are forwarded to one WAF engine, or the authentication will fail due to repeated authentications.
- After a successful verification, the client obtains a token, which grants access to all requests within its validity period. To prevent replay attacks, you can configure a policy to block requests exceeding a specified threshold.

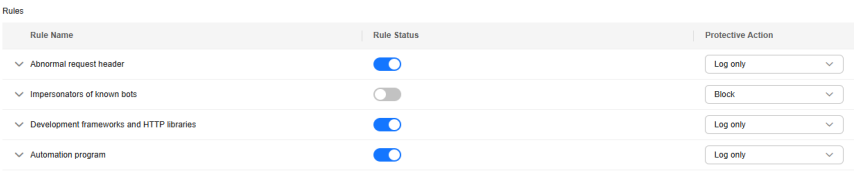
----End

Signature-based Request Detection

Step 1 Click the **Signature-based requests** card and toggle **Status** on.

- Figure 5-67 shows the default configurations after you enable this function.

Figure 5-67 Signature-based requests



- Click ⌄ on the left of the protection rule to view the details about the protection rule.

Step 2 Enable or disable a specific rule and configure protective actions based on your service requirements.

The protective actions are as follows:

- **Log only**: WAF only logs requests that match the features.
- **JS Challenge**: After identifying the feature, WAF returns a segment of JavaScript code that can be automatically executed by a normal browser to the client. If the client properly executes the JavaScript code, WAF allows all requests from the client within a period of time (30 minutes by default). During this period, no verification is required. If the client fails to execute the code, WAF blocks the requests.

  NOTE

  If the referer in the request is different from the current host, the JS challenge does not work.
- **Block**: WAF blocks requests that match the features.
- **Advanced CAPTCHA**: After a request matches feature conditions, CAPTCHA is required for the visitor. If the verification is successful, the request is allowed in a period of time (default: 30 minutes). If the verification fails, the CAPTCHA code is updated and a new-round verification is required again.

NOTE

- The cloud load balancer access mode does not support this protective action.
- If you want to select **Advanced CAPTCHA** for **Protective Action**, make sure requests from a client IP address are forwarded to one WAF engine, or the authentication will fail due to repeated authentications.
- After a successful verification, the client obtains a token, which grants access to all requests within its validity period. To prevent replay attacks, you can configure a policy to block requests exceeding a specified threshold.

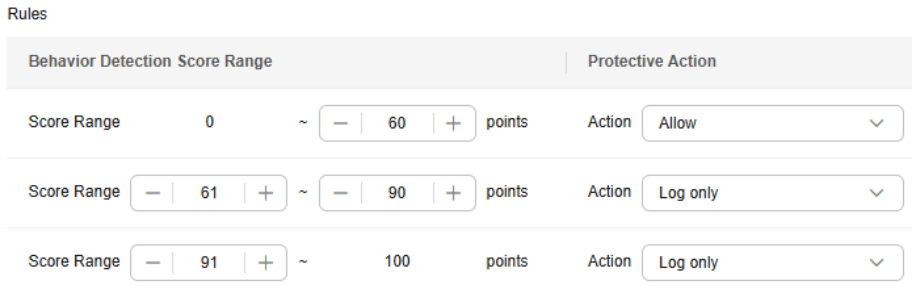
----End

Bot Behavior Detection

Step 1 Click the **BOT behavior** card and enable **AI-based behavior detection**.

Figure 5-68 shows the default configurations after you enable this function.

Figure 5-68 Bot behavior



Step 2 Set three behavior detection score ranges based on service requirements. Score range: 0 to 100. A score closer to 0 indicates that the request feature is more like a normal request, and a score closer to 100 indicates that the request feature is more like a bot.

Step 3 Configure a protective action for each score range.

The protective actions are as follows:

- **Allow**: WAF allows requests that match the features to pass.
- **Log only**: WAF only logs requests that match the features.
- **JS Challenge**: After identifying the feature, WAF returns a segment of JavaScript code that can be automatically executed by a normal browser to the client. If the client properly executes the JavaScript code, WAF allows all requests from the client within a period of time (30 minutes by default). During this period, no verification is required. If the client fails to execute the code, WAF blocks the requests.

  NOTE

  If the referer in the request is different from the current host, the JS challenge does not work.
- **Block**: WAF blocks requests that match the features.
- **Advanced CAPTCHA**: After a request matches feature conditions, CAPTCHA is required for the visitor. If the verification is successful, the request is allowed in a period of time (default: 30 minutes). If the verification fails, the CAPTCHA code is updated and a new-round verification is required again.

NOTE

- The cloud load balancer access mode does not support this protective action.
- If you want to select **Advanced CAPTCHA** for **Protective Action**, make sure requests from a client IP address are forwarded to one WAF engine, or the authentication will fail due to repeated authentications.
- After a successful verification, the client obtains a token, which grants access to all requests within its validity period. To prevent replay attacks, you can configure a policy to block requests exceeding a specified threshold.

----End

Proactive Feature Detection

CAUTION

- Currently, proactive feature detection can check traffic of websites that are connected to WAF in cloud CNAME access mode or dedicated mode. **Currently, proactive feature detection is not supported in cloud load balance access mode.**
- Currently, proactive feature detection supports only web browser services. Before enabling this function, ensure that the protected object is a browser client. Alternatively, configure matching conditions to ensure that the resources can be accessed only by web browsers. Otherwise, mobile app access may be affected.

Step 1 Click the **Proactive feature detection** card and toggle **Status** on.

Figure 5-69 shows the default configurations after you enable this function.

Figure 5-69 Proactive feature detection

Step 2 Set **Confidence** for detection based on actual service requirements.

A lower confidence level indicates a lower frequency of client interactions and a higher probability that the client is an automation program. A higher confidence level indicates a higher probability that the client is a normal user operation. Proactive feature detection supports the following confidence levels:

- **Skip**: Do not detect interactions. For example, if you enable proactive feature detection rules and set the interaction confidence to **Skip**, the system does not count the keyboard and mouse interactions of the client. If the interaction confidence is set to a low value, the client that has not generate keyboard and mouse interactions will be blocked.
- **High**: More than 10 interactions are generated within 600s.
- **Medium**: More than 5 interactions are generated within 600s.

- **Low**: More than 0 interactions are generated within 600s.

Step 3 Configure a protective action for each confidence level.

The protective actions are as follows:

- **Log only**: WAF only logs requests that match the features.
- **Block**: WAF blocks requests that match the features.

----End

Protection Verification

To verify that WAF is protecting your domain name (**www.example.com**) according to the default settings (with **Protective Action** set to **Block**), take the following steps:

Step 1 Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

- If the website is inaccessible, connect the website domain name to WAF by following the instructions in **Website Settings**.
- If the website is accessible, go to **Step 2**.

Step 2 Simulate a bot behavior.

Step 3 Return to the WAF console. In the navigation pane on the left, click **Events**. On the displayed page, check event logs.

----End

Related Operations

- **Bot Protection Statistics**: You can learn of bot protection statistics, including traffic distribution, action distribution, traffic trends, BOT score distribution, and top event source statistics.
- **Querying a Protection Event**: Click **Details** in the **Operation** column of the target event to view event details.
- You can disable **Known bots**, **Signature-based request**, **BOT behavior**, or **Proactive feature detection** to disable all rules under the detection. Your settings will be retained even if you disable the corresponding detection.

5.15 Creating a Reference Table to Configure Protection Metrics in Batches

This topic describes how to create a reference table to batch configure protection metrics of a single type, such as **Path**, **User Agent**, **IP**, **Params**, **Cookie**, **Referer**, and **Header**. A reference table can be referenced by CC attack protection rules, bot rules, anti-crawler protection rules, and precise protection rules.

When you configure a CC attack protection rule, bot rule,, anti-crawler rule, or precise protection rule, if the **Logic** field in the **Trigger** list is set to **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any value**, **Suffix is any value**, or **Suffix is not any**

value, you can select an appropriate reference table from the **Content** drop-down list.

Prerequisites

- You have added the website you want to protect to WAF or **added a protection policy**.
  - For cloud CNAME access mode, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)**.
  - For cloud load balancer access mode, see **Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)**.
  - For dedicated mode, see **Connecting Your Website to WAF (Dedicated Mode)**.
- If you use a dedicated WAF instance, ensure that it has been upgraded to the latest version. For details, see **Managing Dedicated WAF Engines**.

Constraints

This function is not supported in the standard edition.

Application Scenarios

Reference tables can be used for configuring multiple protection fields in CC attack protection, bot rule, anti-crawler, and precise protection rules.

Creating a Reference Table

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Select **CC Attack Protection**, **Bot Rule**, or **Precise Protection**.

Step 8 Click **Reference Table Management** in the upper left corner of the list.

To add a reference table to a bot rule, click the **Custom Protected Objects** tab and click **Reference Table Management** in the upper left corner of the list.

Step 9 On the **Reference Table Management** page, click **Add Reference Table**.

Step 10 In the **Add Reference Table** dialog box, specify the parameters by referring to **Table 5-18**.

Figure 5-70 Adding a reference table

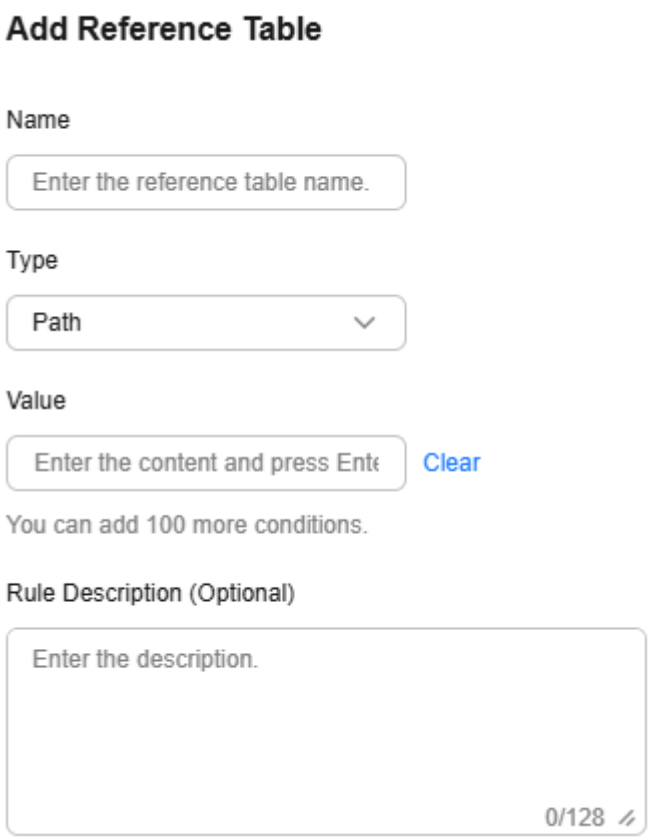


Table 5-18 Parameter description

Parameter	Description	Example Value
Name	Table name you entered	test

Parameter	Description	Example Value
Type	• **Path**: A URL to be protected, excluding a domain name • **User Agent**: A user agent of the scanner to be protected • **IP**: An IP address of the visitor to be protected. **NOTICE** – In cloud mode, IPv6 protection is available only in the professional and enterprise editions. – You can configure 0.0.0.0/0 and ::/0 IP address ranges to block all IPv4 and IPv6 traffic, respectively. • **Params**: A request parameter to be protected • **Cookie**: A small piece of data to identify web visitors • **Referer**: A user-defined request resource For example, if the protected path is **/admin/xxx** and you do not want visitors to be able to access it from *www.test.com*, set **Value** to **http://www.test.com**. • **Header**: A user-defined HTTP header. • **Request Body**: data contained in an HTTP request. • **Response Code**: status code returned to the request. • **Response Body**: response message body • **Response Header**: response header.	Path
Value	Value of the corresponding **Type**. Wildcards are not allowed. You can add multiple values in batches and use line breaks as separators.	**/buy/phone/**

Parameter	Description	Example Value
Rule Description	Description of the rule.	-

Step 11 Click **OK**. You can then view the added reference table in the reference table list.

- After the preceding configurations are complete, you can view the added reference table in the reference table list.
- To delete or modify a reference table, click **Delete** or **Modify** in the **Operation** column of the reference table.

----End

Related Operations

- To modify a reference table, click **Modify** in the row containing the reference table.
- To delete a reference table, click **Delete** in the row containing the reference table.

5.16 Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration

If WAF blocks a malicious request by IP address, Cookie, or Params, you can configure a known attack source rule to let WAF automatically block all requests from the attack source for a blocking duration set in the known attack source rule. For example, if a blocked malicious request originates from a client IP address (192.168.1.1) and you set the blocking duration to 500 seconds, WAF will block the IP address for 500 seconds after the known attack source rule takes effect.

Known attack source rules can be used by basic web protection, CC attack protection, precise protection, IP address blacklist, IP address whitelist, and other rules. You can use known attack source rules in basic web protection, CC attack protection, precise protection, and IP blacklist or whitelist rules as long as you set **Protective Action** to **Block** for these rules.

Prerequisites

- You have added the website you want to protect to WAF or **added a protection policy**.
  - For cloud CNAME access mode, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)**.
  - For cloud load balancer access mode, see **Connecting Your Website to WAF (Cloud Mode - Load Balancer Access)**.
  - For dedicated mode, see **Connecting Your Website to WAF (Dedicated Mode)**.
- If you use a dedicated WAF instance, ensure that it has been upgraded to the latest version. For details, see **Managing Dedicated WAF Engines**.

Constraints

- For a known attack source rule to take effect, it must be enabled when you configure basic web protection, CC attack protection, precise protection, or blacklist/whitelist protection rules.

  NOTICE

  For blacklist and whitelist rules, a known attack source with **Long-term IP address blocking** or **Short-term IP address blocking** configured cannot be selected.

- Before adding a known attack source rule for malicious requests blocked based on Cookie or Params, a traffic identifier must be configured for the corresponding domain name. For more details, see **Configuring a Traffic Identifier for a Known Attack Source**.
- Known attack source rules can only apply to existing WAF engines. New engines do not synchronize the known attack sources configured previously. So known attack sources in requests passing through the new engines cannot be blocked.

  For example, if you configure a known attack source rule for an IP address and set the blocking duration to 100 seconds, all requests from this IP address will be blocked for 100 seconds. If a new engine is added and receives requests over the IP address, the known attack source rule will not be triggered, and the requests will not be blocked.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.

Specification Limitations

- You can configure up to six blocking types. Each type can have one known attack source rule configured.
- Maximum blocking duration:
  - Long-term blocking (including **Long-term IP address blocking**, **Long-term Cookie blocking**, and **Long-term Params blocking**): 3 months
  - Short-term blocking (including **Short-term IP address blocking**, **Short-term Cookie blocking**, and **Short-term Params blocking**): 1,800 seconds

Configuring a Known Attack Source Rule

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by**

enterprise project drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Enable **Known Attack Source** if needed.

-  : enabled.
-  : disabled.

Step 8 If you add a known attack source for the first time, click **Add Known Attack Source Rule**. Configure the parameters by referring to **Table 5-19**.

NOTE

You can click **Add Rule** and add more known attack source rules.

Figure 5-71 Configure Known Attack Source Rule

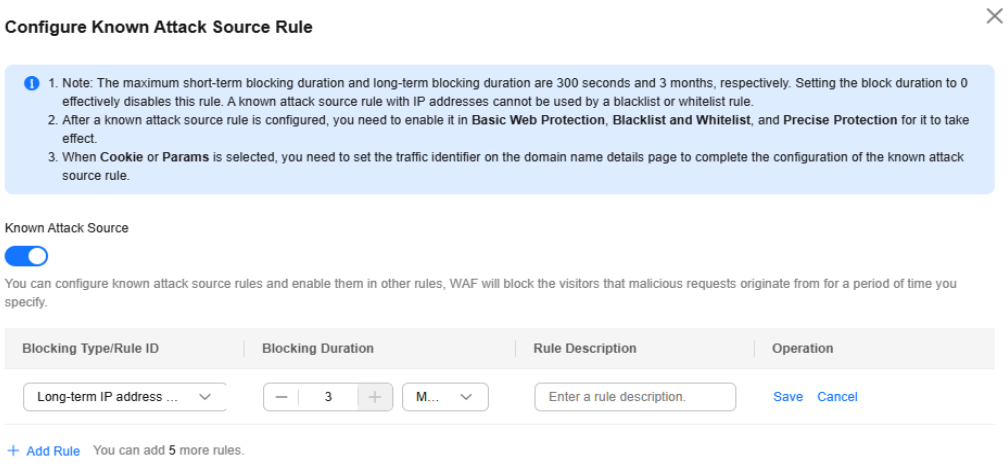


Table 5-19 Known attack source parameters

Parameter	Description	Example Value
Blocking Type	The blocking type for the rule. The options are: • **Long-term IP address blocking** • **Short-term IP address blocking** • **Long-term Cookie blocking** • **Short-term Cookie blocking** • **Long-term Params blocking** • **Short-term Params blocking** **NOTICE** For blacklist and whitelist rules, a known attack source with **Long-term IP address blocking** or **Short-term IP address blocking** configured cannot be selected.	**Long-term IP address blocking**
Blocking Duration (s)	The blocking duration must be an integer and range from: • Short-term blocking: The **Blocking Type** can be set to **Short-term IP address blocking**, **Short-term Cookie blocking**, or **Short-term Params blocking**. The blocking duration is calculated by the second. Value range: 1 to 300 seconds. • Long-term blocking: The **Blocking Type** can be **Long-term IP address blocking**, **Long-term Cookie blocking**, or **Long-term Params blocking**. The blocking duration can be calculated by the **Second**, **Minute**, **Hour**, **Day**, or **Month**. Value ranges are as follows: – **Second**: 301 to 7,776,000 – **Minute**: 6 to 129,600 – **Hour**: 1 to 2,160 – **Day**: 1 to 90 – **Month**: 1 to 3	3 months
Rule Description	A brief description of the rule. This parameter is optional.	-

Step 9 Click **Save**. You can then view the added known attack source rule in the list.

- After the configuration is complete, you can view the added rule in the protection rule list. **Rule Status** is **Enabled** by default.
- If you do not want the rule to take effect, click **Disable** in the **Operation** column of the rule.
- To delete or modify a rule, click **Delete** or **Modify** in the **Operation** column of the rule.

----End

One-Click Unblocking a Known Attack Source Rule

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Click the name of the target policy to go to the protection configuration page.

Step 7 Click the **CC Attack Protection** or **Precise Protection** configuration box. In the upper right corner of the rule list, click **One-Click Unblocking**.

> ⚠ CAUTION
>
> **One-Click Unblocking** unblocks all known attack source rules triggered in the current module. All IP addresses, cookies, and params previously blocked by these rules will be unblocked. If the protection rule is triggered again, the associated known attack source rule is triggered as well. The IP addresses, cookies, or parameters will be blocked for a time period you configure in the rule.

Step 8 Click **One-Click Unblocking** in the displayed dialog box and click **OK** to unblock all known attack source rules triggered by the current protection module.

Then, the IP addresses, cookies, or parameters that have been blocked are unblocked until the protection rule associated with the known attack sources is triggered again.

----End

Protection Verification

To verify that WAF is protecting your domain name (**www.example.com**) according to the protection rule configured by referring to example values in **Table 5-19**, take the following steps:

Step 1 Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

- If the website is inaccessible, connect the website domain name to WAF by following the instructions in **Website Settings**.
- If the website is accessible, go to **Step 2**.

Step 2 Clear the browser cache and access the **http://www.example.com/admin** page. If client IP address *XXX.XXX.248.195* is blocked by WAF for three months, the rule takes effect.

Step 3 Return to the WAF console. In the navigation pane on the left, click **Events**. On the displayed page, check event logs.

----End

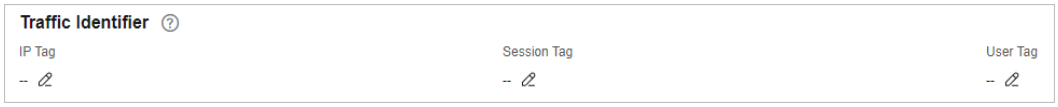
Configuration Example: Blocking Known Attack Source Identified by Cookie

Assume that domain name *www.example.com* has been connected to WAF and a visitor has sent one or more malicious requests through IP address *XXX.XXX.248.195*. You want to block access requests from this IP address and whose cookie is **jsessionid** for 10 minutes.

Step 1 On the **Website Settings** page, click *www.example.com* to go to its basic information page.

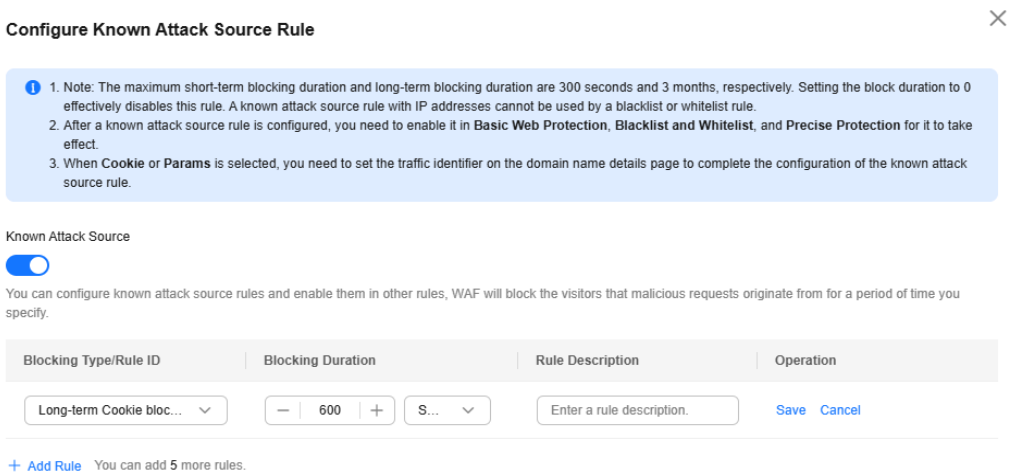
Step 2 In the **Traffic Identifier** area, configure the cookie in the **Session Tag** field.

Figure 5-72 Traffic Identifier



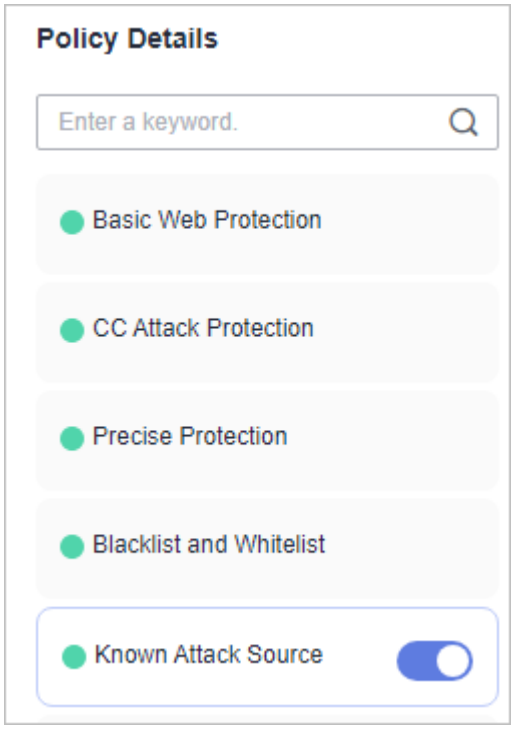
Step 3 Add a known attack source, select **Long-term Cookie blocking** for **Blocking Type**, and set block duration to 600 seconds.

Figure 5-73 Adding a Cookie-based known attack source rule



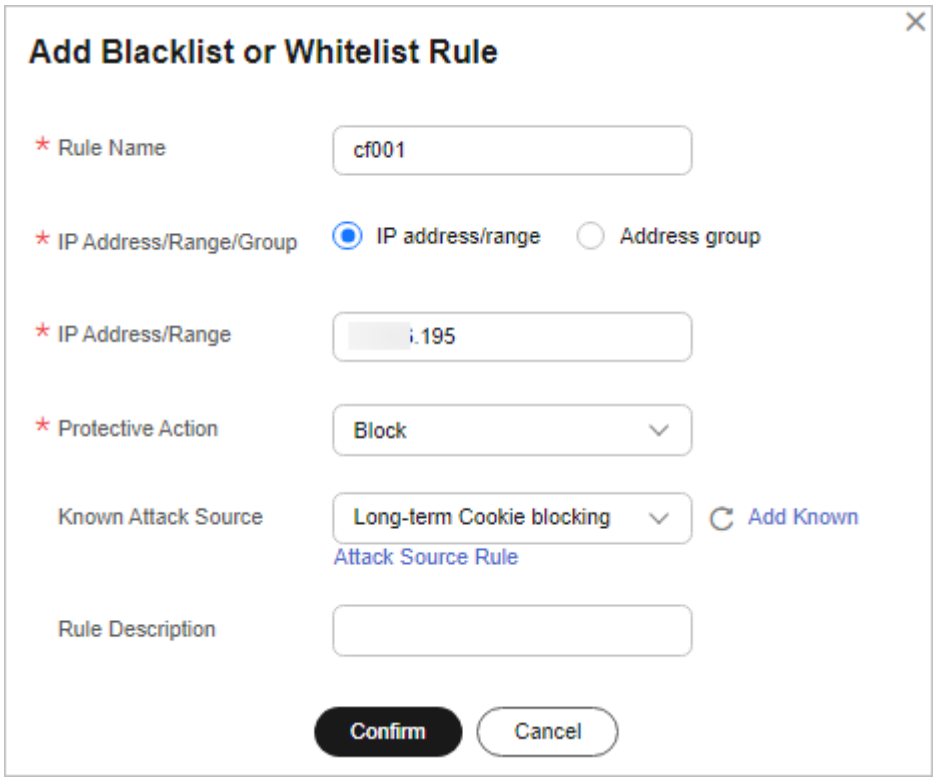
Step 4 Enable the known attack source protection.

Figure 5-74 Known Attack Source configuration area



Step 5 Add a blacklist and whitelist rule to block *XXX.XXX.248.195*. Select **Long-term Cookie blocking** for **Known Attack Source**.

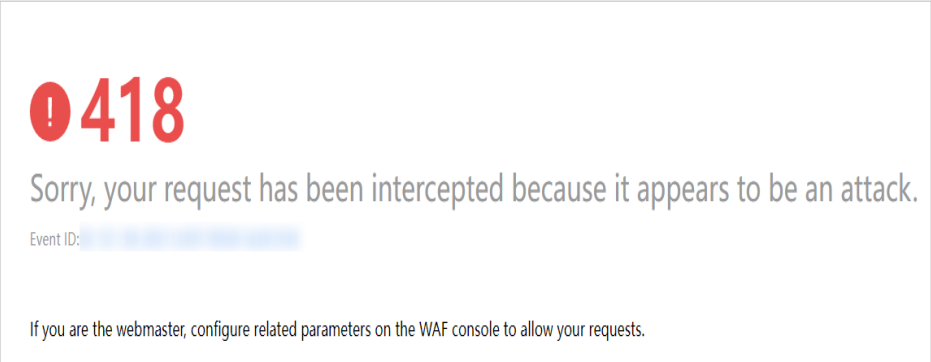
Figure 5-75 Specifying a known attack source rule



Step 6 Clear the browser cache and access http://www.example.com.

When a request from client IP address *XXX.XXX.248.195*, WAF blocks the access. If WAF detects that the cookie of the access request from the client IP address is **jsessionid**, WAF blocks the access request for 10 minutes.

Figure 5-76 Block page



Step 7 Go to the WAF console. In the navigation pane on the left, choose **Events**. View the event on the **Events** page.

----End

5.17 Condition Field Description

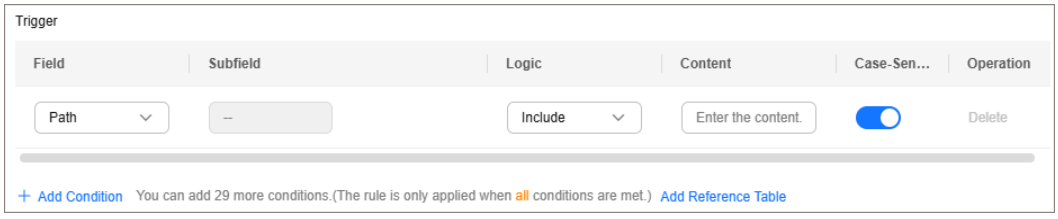
When setting a precise access, CC attack protection, or global protection whitelist rule, configure some fields in the condition list area. These fields together are used to define the request attributes to trigger the rule. This topic describes the fields that you can specify in conditions to trigger a rule.

What Is a Condition Field?

A condition field specifies the request attribute WAF checks based on protection rules. When configuring a **CC attack protection rule**, **precise access protection rule**, or **global protection whitelist**, you can define condition fields to specify request attributes to trigger the rule.

If a request meets the conditions set in a rule, the request hits the rule. WAF will then handle the request based on the action (**Allow**, **Block**, or **Log only**) configured for the rule.

Figure 5-77 Condition field



A condition field consists of **Field**, **Subfield**, **Logic**, and **Content**. Example:

- Example 1: If **Field** is set to **Path**, **logic** to **Include**, and **Content** to **/admin**, a request matches the rule when the requested path contains **/admin**.
- Example 2: If **Field** is set to **IPv4**, **Subfield** to **Client IP Address**, **Logic** to **Equal to**, and **Content** to **192.XX.XX.3**. When the client IP address is 192.XX.XX.3, the request hits the rule.

Supported Condition Fields

Table 5-20 Condition list configurations

Field	Description	Subfield	Logic	Content (Example)
Path	The path of a resource requested by the client. A path is part of a URL. Configuration description: • The path does not contain a domain name and supports only exact match. So, the path to be protected must be the same as the path you configure. If the path to be protected is **/admin**, set **Path** to **/admin**. • If **Path** is set to **/**, all paths of the website are protected. • The path content cannot contain the following special characters: (<>*)	--	The following logical relationships are supported: • **Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, or **Suffix is not** • **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any value**, **Suffix is any value**, or **Suffix is not any value** If you select any logical relationship listed above, you can specify **Reference Table** for **Content**. For details about how to add a reference table and manage reference tables, see **Creating a Reference Table to Configure Protection Metrics in Batches**. • **Subfield length equal to**, **Subfield length not equal to**,	/buy/phone/
User Agent	The client type, for example, browser, crawler, and mobile app.	--		*Mozilla/5.0 (Windows NT 6.1)*
Referer	The source from which the request is sent. If you do not want visitors to access the page from **www.test.com**, set **Content** corresponding to **Referer** to **http://www.test.com**.	--		**/admin/xxx**

Field	Description	Subfield	Logic	Content (Example)
			Subfield length greater than, or **Subfield length less than**	
IPv4	The IPv4 address of the client.	• Client IP Address • X-Forwarded-For • TCP connection IP address • Layer 3 source IP address	The following logical relationships are supported: • **Equal to** or **Not equal to** • **Equal to any value** or **Not equal to any value** If you select any logical relationship listed above, you can specify **Reference Table** for **Content**. For details about how to add a reference table and manage reference tables, see **Creating a Reference Table to Configure Protection Metrics in Batches**.	*192.168.1.1*
IPv6	The IPv6 address of the client. Only the professional and enterprise editions for cloud mode support IPv6 protection.			*fe80:0000:0000:0000:0000:0000:0000:0000*

Field	Description	Subfield	Logic	Content (Example)
Params	The query parameter in the URL. The query parameter is the content following the question mark (?).	• All fields • Any subfield • Custom	The following logical relationships are supported: • **Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, or **Suffix is not** • **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any value**, **Suffix is any value**, or **Suffix is not any value** If you select any logical relationship listed above, you can specify **Reference Table** for **Content**. For details about how to add a reference table and manage reference tables, see **Creating a Reference Table to Configure Protection Metrics in Batches**. • **Subfield length equal to**, **Subfield length not equal to**, **Subfield length greater than**, **Subfield length less than**,	*2019011 50929*
Cookie	The cookie in the request.	• All fields • Any subfield • Custom		*jsessionid*
Header	The request header content.	• All fields • Any subfield • Custom		*text/ html,application /xhtml +xml,application / xml;q=0.9,image/ webp,image/ apng,*/ *;q=0.8*

Field	Description	Subfield	Logic	Content (Example)
			Number of params not equal to, **Number of params greater than**, **Number of params less than**, **Has**, or **Does not have**	
Method	The request method.	--	The following logical relationships are supported: • **Equal to** • **Not equal to**	**GET**, **POST**, **PUT**, **DELETE**, and **PATCH**
Protocol	The request protocol.	--		**HTTP** and **HTTPS**
Request Line	The request line length. The value must be an integer ranging from 0 to 65,535.	--	The following logical relationships are supported: • **Subfield length equal to** • **Subfield length not equal to** • **Subfield length greater than** • **Subfield length less than**	**50**
Request	The request length. The value must be an integer ranging from 0 to 2,147,483,647. The maximum value for cloud load balancer access mode is 4,000 bytes. If the value exceeds the maximum, the configuration does not take effect.	--		*50*

Field	Description	Subfield	Logic	Content (Example)
Response Length	The response length. The value must be an integer ranging from 0 to 2,147,483,647. • Response detection occurs after the response header is returned. The response header cannot be modified when it is blocked. • A response body returned from the origin server may be included in protection events. As the response body is streamed, WAF cannot change it once it has been sent.	--	The following logical relationships are supported: • **Subfield length equal to** • **Subfield length not equal to** • **Subfield length greater than** • **Subfield length less than**	*50*
Response Time	The response time. The value must be an integer ranging from 0 to 60,000, in ms. • Response detection occurs after the response header is returned. The response header cannot be modified when it is blocked. • A response body returned from the origin server may be included in protection events. As the response body is streamed, WAF cannot change it once it has been sent.	--		*100*

Field	Description	Subfield	Logic	Content (Example)
Geolocation	The geolocation of the visitor (client). **NOTE** This function is under open beta test (OBT). You can **submit a service ticket** to enable it.	• **IPv4** • **IPv6** • **Any** (IPv4 or IPv6 address)	The following logical relationships are supported: • **Included** • **Excluded**	**Shanghai**
Known feature crawler	Common web crawlers: • Search Engine • Scanner • Script Tool • Other **NOTE** This function is under open beta test (OBT). You can **submit a service ticket** to enable it.	--	The following logical relationships are supported: • Match • Mismatch	Search Engine
Response Code	The status code returned to the request. For requests sent after this rule is triggered, WAF stops checking their HTTP response code until the current traffic limit duration you configure in the rule ends.	--	The following logical relationships are supported: • **Equal to** or **Not equal to** • **Equal to any value** or **Not equal to any value** If you select any logical relationship listed above, you can specify **Reference Table** for **Content**. For details about how to add a reference table and manage reference tables, see **Creating a Reference Table to Configure Protection Metrics in Batches**.	*404*

Field	Description	Subfield	Logic	Content (Example)
Response Header	The response header. WAF checks responses after response headers are returned. If WAF needs to block responses, response headers cannot be changed.	• All fields • Any subfield • Custom	The following logical relationships are supported: • **Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, or **Suffix is not** • **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any value**, or **Suffix is any value**, If you select any logical relationship listed above, you can specify **Reference Table** for **Content**. For details about how to add a reference table and manage reference tables, see **Creating a Reference Table to Configure Protection Metrics in Batches**.	--

Field	Description	Subfield	Logic	Content (Example)
Response Body	The response message body. WAF checks responses after response headers are returned. If WAF needs to block responses, response headers cannot be changed.	--	The following logical relationships are supported: • **Include** or **Exclude** • **Include any value** or **Exclude any value** If you select any logical relationship listed above, you can specify **Reference Table** for **Content**. For details about how to add a reference table and manage reference tables, see **Creating a Reference Table to Configure Protection Metrics in Batches**.	--

Field	Description	Subfield	Logic	Content (Example)
Request Body	The request message body.	--	The following logical relationships are supported: • **Include** or **Not Include** • **Include any value** or **Exclude any value** If you select any logical relationship listed above, you can specify **Reference Table** for **Content**. For details about how to add a reference table and manage reference tables, see **Creating a Reference Table to Configure Protection Metrics in Batches**.	--

Field	Description	Subfield	Logic	Content (Example)
TLS fingerprint (JA3)	The JA3 fingerprint generated during TLS handshake. It is used to identify device types and malicious tools.	--	The following logical relationships are supported: • **Equal to** or **Not equal to** • **Equal to any value** or **Not equal to any value** If you select any logical relationship listed above, you can specify **Reference Table** for **Content**. For details about how to add a reference table and manage reference tables, see **Creating a Reference Table to Configure Protection Metrics in Batches**.	**X-Forwarded-Tls-Ja3**
TLS fingerprint (JA4)	The JA4 fingerprint generated during TLS handshake. It is used to identify device types and malicious tools.	--		**X-Forwarded-Tls-Ja4**
Header Content Length	The request header content length. The value must be an integer ranging from 0 to 2,147,483,647. The maximum value for cloud load balancer access mode is 4,000 bytes. If the value exceeds the maximum, the configuration does not take effect.	--	The following logical relationships are supported: • Greater than • Equal to • Less than	*123*

5.18 Application Types WAF Can Protect

Table 5-21 lists the application types that can be protected by basic web protection rules.

Table 5-21 Application types WAF can protect

4images	Dragon-Fire IDS	Log4j2	ProjectButler
A1Stats	Drunken Golem GP	Loggix	Pulse Secure
Achievo	Drupal	lpswitch IMail	Quest CAPTCHA
Acidcat CMS	DS3	Lussumo Vanilla	QuickTime Streaming Server
Activist Mobilization Platform	Dubbo	MAGMI	R2 Newsletter
AdaptBB	DynPG CMS	ManageEngine ADSelfService Plus	Radware AppWall
Adobe	DZCP basePath	MassMirror Uploader	Rezervi root
Advanced Comment System	ea-gBook inc ordner	Mavili	Ruby
agendax	EasyBoard	MAXcms	RunCMS
Agora	EasySiteEdit	ME Download System	Sahana-Agasti
AIOCP	e-cology	Mevin	SaurusCMS CE
AjaxFile	E-Commerce	Microsoft Exchange Server	School Data Navigator
AJSquare	Elvin	Moa Gallery MOA	Seagull
Alabanza	Elxis-CMS	Mobius	SGI IRIX
Alfresco Community Edition	EmpireCMS	Moodle	SilverStripe
AllClubCMS	EmuMail	Movabletype	SiteEngine
Allwebmenus Wordpress	eoCMS	Multi-lingual E-Commerce	Sitepark
Apache	E-Office	Multiple PHP	Snipe Gallery
Apache APISIX Dashboard	EVA cms	mxCamArchive	SocialEngine
Apache Commons	eXtropia	Nakid CMS	SolarWinds

Apache Druid	EZPX Photoblog	NaviCOPA Web Server	SQuery
Apache Dubbo	F5 TMUI	NC	Squid
Apache Shiro	Faces	NDS iMonitor	StatCounteX
Apache Struts	FAQEngine	Neocrome Seditio	Subdreamer-CMS
Apache Tomcat	FASTJSON or JACKSON	NetIQ Access Manager	Sumsung IOT
Apache-HTTPD	FCKeditor	Netwin	Sun NetDynamics
Apple QuickTime	FileSeek	Nginx	SuSE Linux Sdbsearch
ardeaCore	fipsCMSLight	Nodesforum	SweetRice-2
AROUNDMe	fipsForum	Nucleus Plugin Gallery	Tatantella
Aurora Content Management	Free PHP VX Guestbook	Nucleus Plugin Twitter	Thecartpress Wordpress
AWCM final	FreeSchool	Nukebrowser	Thinkphp
AWStats	FreshScripts	NukeHall	ThinkPHP5 RCE
Baby Gekko	FSphp	Nullsoft	Tiki Wiki
BAROSmini Multiple	FusionAuth	Ocean12 FAQ Manager	Tomcat
Barracuda Spam	Gallo	OCPortal CMS	Trend Micro
BizDB	GetSimple	Open Education	Trend Micro Virus Buster
Blackboard	GetSimple CMS	OpenMairie openAnnuaire	Tribal Tribiq CMS
BLNews	GLPI	OpenPro	TYPO3 Extension
Caldera	GoAdmin	openUrgence Vaccin	Uebimiau
Cedric	Gossamer Threads DBMan	ORACLE Application Server	Uiga Proxy
Ciamos CMS	Grayscalecms	Oramon	Ultrize TimeSheet
ClearSite Beta	Hadoop	OSCommerce	VehicleManager
ClodFusion Tags	Haudenschilt Family	PALS	Visitor Logger

CMS S Builder	Havalite	Pecio CMS	VMware
ColdFusion	HIS Auktion	PeopleSoft	VoteBox
ColdFusion Tags	HP OpenView Network Node Manager	Persism Content Management	WayBoard
Commvault CommCell CVSearchService	HPInsightDiagnostics	PhotoGal	WebBBS
Concrete5	Huawei D100	PHP Ads	WebCalendar
Confluence Server and Data Center	HUBScript	PHP Classifieds	WEB-CGI
Coremail	IIS	PHP CMS	WebFileExplorer
Cosmicperl Directory Pro	iJoomla Magazine	PHP Paid 4 Mail Script	WebGlimpse
CPCommerce	ILIAS	PHPAddressBook	webLogic
DataLife Engine	Indexu	PHP-Calendar	WebLogic Server wls9-async
DCScripts	IRIX	phpCow	Webmin
DDL CMS	JasonHines PHPWebLog	PHPGenealogy	WEB-PHP Invision Board
DELL TrueMobile	JBOSS	PHPGroupWare	WebRCSdiff
Digitaldesign CMS	JBossSeam	phpMyAdmin	Websense
Dir2web	Joomla	phpMyAdmin Plugin	WebSphere
Direct News	JRE	PHPMyGallery	WikyBlog WBmap
Discourse	jsfuck	PHPNews	WordPress
Diskos CMS Manager	justVisual	Pie Web Masher	WORK system
DiY-CMS	Katalog Stron Hurricane	PlaySMS	Wpeasystats Wordpress
D-Link	KingCMS	Plogger	XOOPS

DMXReady Registration Manager	koesubmit	Plone	Xstream
DoceboLMS	Kontakt Formular	PointComma	YABB SE
Dokuwiki	KR-Web	Postgres	YP Portal MS-Pro Surumu
dompdf	Landray	PrestaShop	ZenTao
DotNetNuke	Livesig Wordpress	ProdLer	Zingiri Web Shop Wordpress
ZOHO ManageEngine	-	-	-

6 Viewing the Dashboard

If you have connected websites to WAF, you can have a glance at their security on the **Dashboard** page. You will learn of WAF updates, protection overview, product details, as well as the security statistics of protected websites and instances you have for up to 30 days. You can also check event source statistics and bot protection statistics.

Statistics on the **Dashboard** page are updated every two minutes.

Prerequisites

- You have connected the website you want to protect to WAF. For details, see **Connecting a Website to WAF**.
- At least one protection rule has been configured for the domain name. For details, see **Configuring Protection Policies**.

Specification Limitations

You can view the protection data of a maximum of 30 days.

Checking the Overview Information

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Dashboard**.

Step 6 On the **Dashboard** page, view the following information.

Table 6-1 Dashboard overview

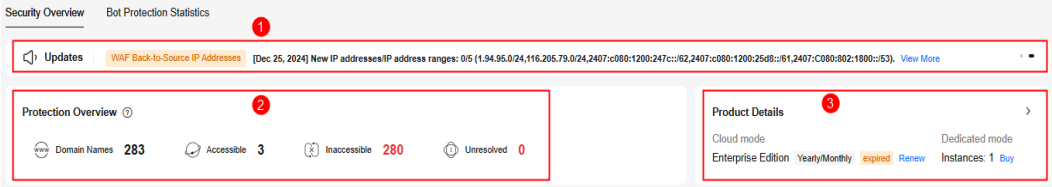
Tab	Function Module	Description
Dashboard	**Updates**	This area displays the latest information about WAF back-to-source IP address ranges, rule updates, and risk found recently.
	Protection Overview	This area displays the domain name access status.
	Product Details	This area displays the details about instances you buy. You can check the WAF edition and specifications you are using.
	Security Event Statistics	In this area, you can view the protection event logs by website or instance. You can select a specific time range, including yesterday, today, past 3 days, past 7 days, or past 30 days. You can also specify a time range no longer than 30 days.
	Event Source Statistics	This area displays information such as event distribution, attacked objects, attack source IP addresses, attacked URLs, attack source locations, and error pages.
Bot Protection Statistics	**Bot Protection Statistics**	On this tab, you will learn of bot protection statistics, including traffic distribution, action distribution, traffic trends, BOT score distribution, and top event source statistics.
Bot protection statistics description: You need to **submit a service ticket** and **configure a bot protection rule**. Then, you can view **Bot Protection Statistics** on the **Dashboard** page. Otherwise, the **Dashboard** page displays only information such as **Updates**, **Protection Overview**, **Product Details**, **Security Event Statistics**, and **Event Source Statistics**.		

----End

Updates, Protection Overview, and Product Details

In these areas, you can check the latest WAF back-to-source IP address ranges, rule updates, risks found recently, domain name access status statistics, and details about products you have.

Figure 6-1 Updates



Function Module	Description	Related Operation
Updates (① in **Figure 6-1**)	**WAF Back-to-Source IP Addresses**: You can check new WAF back-to-source IP addresses. A notification will be sent one month in advance if there are new WAF back-to-source IP addresses.	On the **Updates** bar, you can click **View More** next to **WAF Back-to-Source IP Addresses** to check and copy WAF back-to-source IP address ranges.
	Updated Rules: In this area, you can check notifications about built-in rule library updates, including emerging vulnerabilities such as zero-day vulnerabilities these rules can defend against. You can also check notifications about new functions, billing details, and critical alarms, such as alarms generated when requests to your domain name bypass WAF.	• On the **Updates** bar, you can click **More** next to **Updated Rules** to view the rule update details. • Click **View Details** to go to the **Built-in Rule Sets** page. You can view all built-in rules. All default rules are sorted by update time.
	Risks Found: If you use dedicated WAF instances, you will get notifications on the latest risks your dedicated WAF instances have. You can then handle related risks in a timely manner to prevent services from being affected.	• Click **View Details**. In the displayed dialog box, check risks and upgrade dedicated WAF instances as needed. • If the multi-active architecture is not used, click the **Multi-active architecture not** tab, buy another dedicated WAF instance, and deploy two instances to implement the multi-active architecture, preventing risks caused by single points of failure (SPOFs).
Protection Overview (② in **Figure 6-1**)	This area displays the total number of website domain names, number of domain names that have been connected to WAF, number of domain names that fail to be connected to WAF, and number of domain names that fail to be resolved by DNS.	You can click the number to go to the **Website Settings** page. In the domain name list, the system automatically filters the domain names based on the number you click, making it easier to locate websites you need to connect to WAF.

Function Module	Description	Related Operation
Product Details (③ in **Figure 6-1**)	This area displays the details about instances you buy. You can check the edition, billing mode, and number of dedicated engines you buy	• You can click › to go to the **Product Details** page and view the edition and quota details. • Click **Details** in the cloud mode area. On the **Cloud Mode Details** panel, perform the following operations: – View the in-use cloud edition details, such as specifications and advanced functions. – Click **Change Edition** in the **Edition** row to change the specifications. For details, see **Changing the Cloud WAF Edition and Specifications**. – Choose **Advanced Functions** > **Expansion Packages**, click **Change** under **Domain Expansion Package**, **QPS Expansion Package**, or **Rule Expansion Package** to buy packages to meet your service needs. For details, see **Expansion Packages**. • Click **Buy** in the dedicated mode to buy dedicated WAF instances based on service requirements.

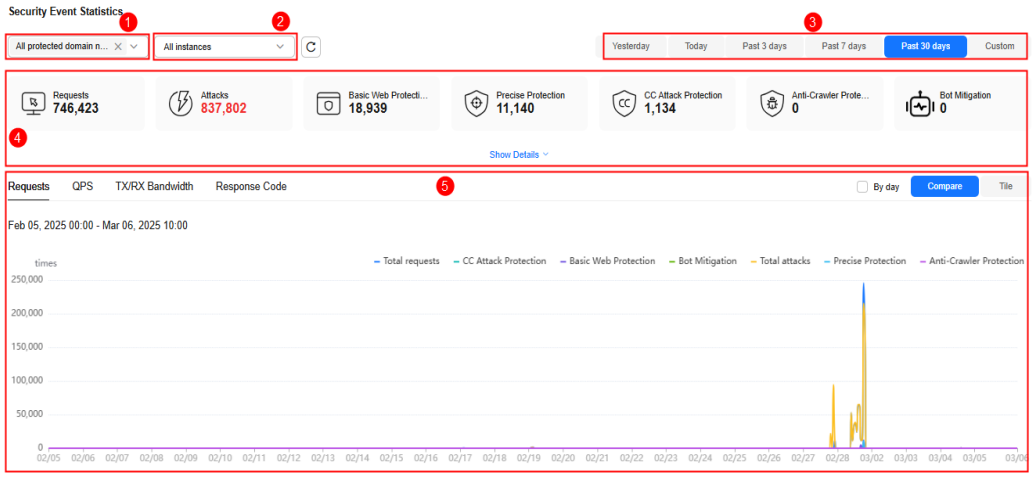
Security Event Statistics

In the **Security Event Statistics** area, you can view the protection event logs by website or instance. You can select a specific time range, including yesterday, today, past 3 days, past 7 days, or past 30 days. You can also specify a time range no longer than 30 days. On this page, protection event logs are displayed by different dimensions, including the number of requests and attack types, QPS, bandwidth, response code, event distribution, top 5 attacked domain names, top 5 attack source IP addresses, and top 5 attacked URLs.

If no enterprise project is selected, WAF collects security data of all websites added to WAF in all enterprise projects under the account by default. Before viewing the data, you can set the following information based on service requirements:

- **Domain name** (① in Figure 6-2): You can select a specific domain name, multiple domain names, or all domain names to view the security statistics.
- **Instance** (② in Figure 6-2): You can select a specific instance or all instances to view security statistics.
- **Query time** (③ in Figure 6-2): You can view security statistics for yesterday, today, past 3 days, past 7 days, past 30 days, or any time range within 30 days. The statistics collection frequency in each time range is as follows:
  - **Yesterday** and **Today**: Security data is gathered every minute.
  - **Past 3 days**: Security data is gathered every 5 minutes.
  - **Past 7 days**: Security event data is gathered every 10 minutes.
  - **Past 30 days**: Security data is gathered every hour.

Figure 6-2 Security Event Statistics



Function Module	Description	Related Operation
Security statistics (④ in Figure 6-2)	**Requests**: shows the page views of the website, making it easy for you to view the total number of pages accessed by visitors in a certain period of time.	You can click **Show Details** to view the details about the 10 domain names with the most requests, attacks, and basic web protection, precise protection, CC attack protection, bot mitigation, and anti-crawler protection actions.
	Attacks: indicates the total number of attacks, including blocked attacks and logged attacks, at your website.	
	Protection details: displays details about attacks that match each protection rule, including the number of times that the attack is blocked by the protection rule and the number of times that the attack is logged.	

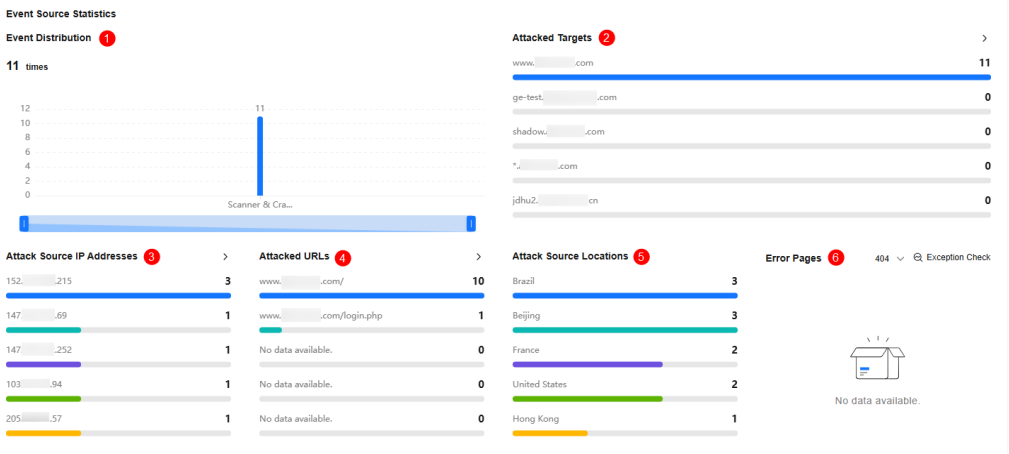
Function Module	Description	Related Operation
Security statistics trend (⑤ in Figure 6-2)	**Requests**: This tab displays statistics on the total number of requests to a domain name and details about each protection rule.	• **By day**: You can select this option to view the data gathered by the day. If you leave this option unselected, the data is displayed by the time range you select. • You can select **Compare** or **Tile** to view data.
	QPS: You can check the average number of requests per second for the domain name. This tab displays the total number of requests to the domain name, and the average and peak QPS values by protection rule. The QPS calculation method varies depending on the time range you specify. The average and peak QPS values for each time range are calculated in the following way: • Average QPS description – **Yesterday** and **Today**: The average value is obtained at an interval of 1 minute. – **Past 3 days**: The QPS curve is made with the average QPS in every five minutes. – **Past 7 days**: The QPS curve is made with the maximum value among the average QPS in every five minutes at a 10-minute interval. – **Past 30 days**: The QPS curve is made with the maximum value among the average QPS in every five minutes at a one-hour interval. • Peak QPS description – **Yesterday** and **Today**: The maximum value is obtained at a one-minute interval. – **Past 3 days**: The QPS curve is made with the maximum QPS in every five minutes. – **Past 7 days**: The QPS curve is made with each peak QPS in every 10 minutes. – **Past 30 days**: The QPS curve is made with the peak QPS in every hour.	

Function Module	Description	Related Operation
	TX/RX Bandwidth: shows the bandwidth usage of domain names. You can view the average value and peak value. The value of sent and received bytes is calculated by adding the values of **request_length** and **upstream_bytes_received** by time, so the value is different from the network bandwidth monitored on the EIP. This value is also affected by web page compression, connection reuse, access mode, and TCP retransmission. For details, see **Why Is the Traffic Statistics on WAF Inconsistent with That on the Origin Server?**	
	Response Code: Response codes returned by WAF to the client or returned by the origin server to WAF along with the corresponding number of responses. You can click **WAF to Client** or **Origin Server to WAF** to view the corresponding information. The number of response codes is accumulated based on the sequence of response codes (from left to right) in the lower part of the chart. The number of response codes is the difference between two lines. If the value of a response code is 0, the line of the response code overlaps that of the previous response code.	

Event Source Statistics

This area displays the following information: event distribution, attacked objects, attack source IP addresses, attack source locations, error pages, and attacked URLs.

Figure 6-3 Event Source Statistics



Parameter	Description	Related Operation
Event Distribution (① in **Figure 6-3**)	Types of attack events.	You can click an area in the **Event Distribution** area to view the type, number, and proportion of an attack.
Attacked Targets (② in **Figure 6-3**)	The five most attacked domain names and the number of attacks at each domain name.	You can click > to go to the **Events** page and view more protection details.
Attack Source IP Addresses (③ in **Figure 6-3**)	The five IP addresses that initiate most attacks and the number of attacks from each IP address. **NOTE** **49.4.121.70** is the WAF dialing test IP address. If the requests of this IP address are blocked and the number of block times is ranked top 5, the IP address will be also displayed in the attack source IP address list.	You can click > to go to the **Events** page and view more protection details.
Attacked URLs (④ in **Figure 6-3**)	The five most attacked URLs and the number of attacks at each URL.	You can click > to go to the **Events** page and view more protection details.
Attack Source Locations (⑤ in **Figure 6-3**)	The five locations generating the most attacks and the number of attacks from each location.	N/A

Parameter	Description	Related Operation
Error Pages (⑥ in **Figure 6-3**)	The five websites with the most service exceptions. Websites with **404**, **500**, or **502** errors can be viewed.	You can click **Exception Check** and find corresponding solutions to rectify service interruptions.

Bot Protection Statistics

You need to **submit a service ticket** to enable bot protection. If you enable bot protection and **configured bot rules**, you can check the **Bot Protection Statistics** tab on the **Dashboard** page. You will view the traffic distribution, action distribution, traffic trends, bot score distribution, and top event source statistics.

If no enterprise project is selected, WAF collects security data of all websites added to WAF in all enterprise projects under the account by default. Before viewing data, you can set the following parameters based on service requirements:

- **Domain name** (① in **Figure 6-4**): You can select a specific domain name, multiple domain names, or all domain names to view the bot protection statistics.
- **Query time** (② in **Figure 6-4**): You can view bot protection statistics for yesterday, today, past 3 days, past 7 days, past 30 days, or any time range within 30 days.

Viewing bot protection data and trends

Figure 6-4 Bot protection data and trends

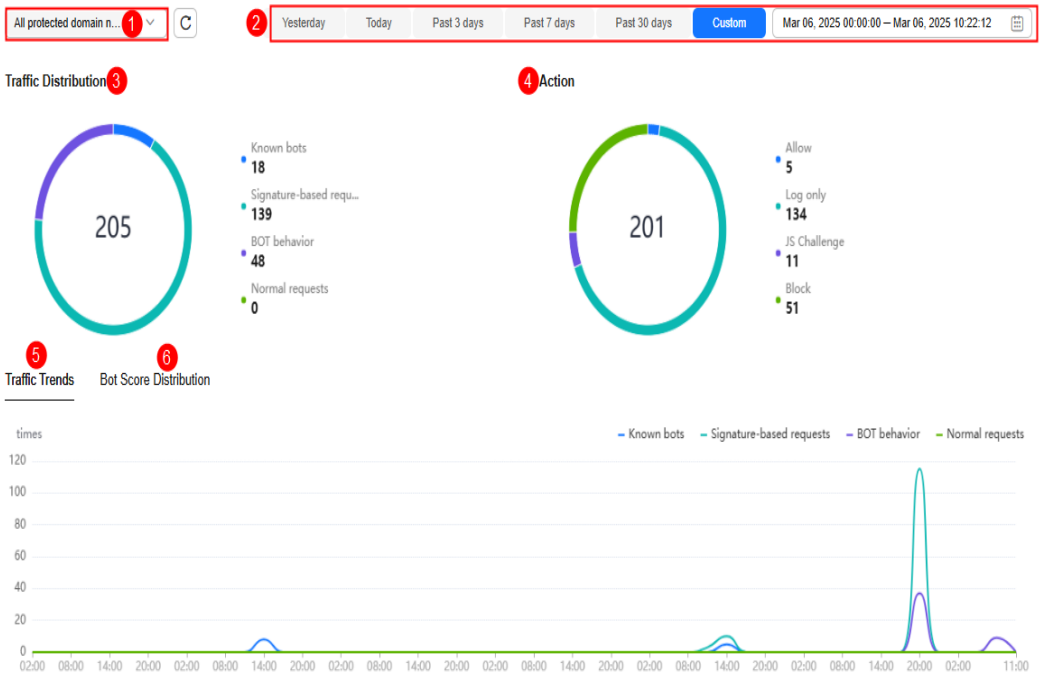


Table 6-2 Parameters of bot protection statistics

Function Module	Description
Traffic Distribution (③ in **Figure 6-4**)	• **Known bots**: shows the number of requests that match known bot rules in a specified time range. • **Signature-based requests**: shows the number of requests that hit the request signature detection in a specified time range. • **BOT behavior**: shows the number of requests that hit bot behavior detection in a specified time range. • **Normal requests**: shows the number of normal requests for accessing a website in a specified time range.
Action (④ in **Figure 6-4**)	WAF counts the number of requests that are identified based on bot detection rules within a period of time. WAF also displays protective actions (**Allow**, **Log only**, **JS Challenge**, and **Block**) taken to those requests.
Traffic Trends (⑤ in **Figure 6-4**)	On this tab, you will learn of traffic trends of known bots, signature-based requests, bot behavior, and normal requests.
Bot Score Distribution (⑥ in **Figure 6-4**)	Bot behavior detection scores. BOT behavior detection scores each request of the client to evaluate the probability that the request comes from a bot. A value closer to 0 indicates that the request feature is more like a normal request, and a value closer to 100 indicates that the request feature is more like a bot.

Viewing Top Event Source Statistics

Figure 6-5 Top Event Source Statistics

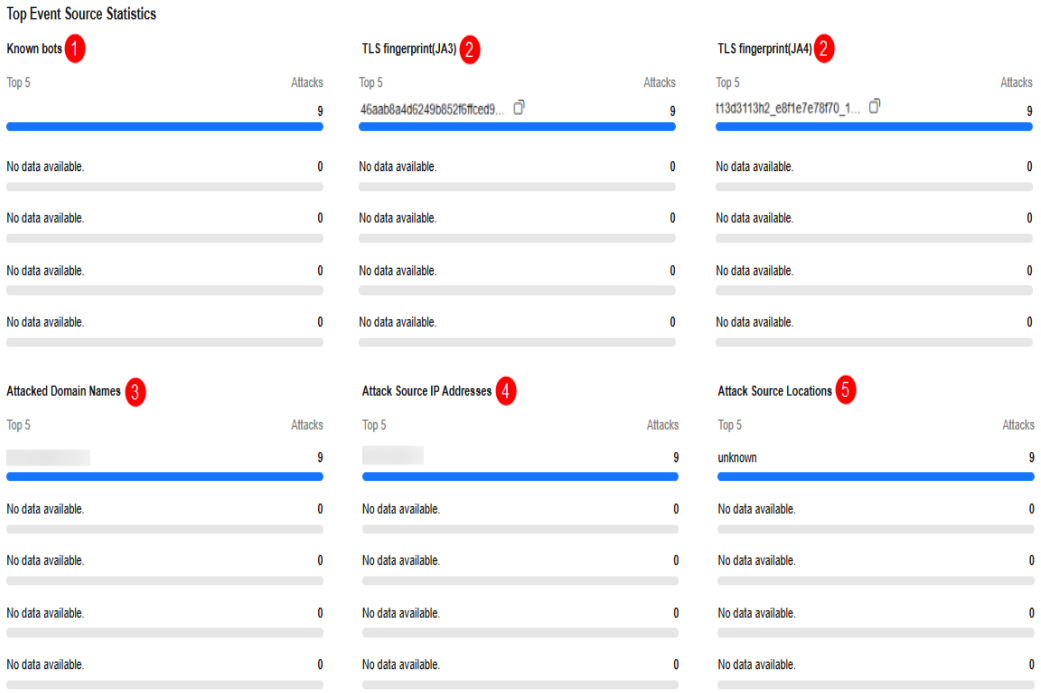


Table 6-3 Top event source statistics parameters

Parameter	Description
Known bots (① in **Figure 6-5**)	The five known bots with the most attacks and the number of attacks from each bot.
TLS fingerprint (② in **Figure 6-5**)	The five TLS fingerprints (JA3 and JA4) with the most attacks and the number of attacks.
Attacked Domain Names (③ in **Figure 6-5**)	The five most attacked domain names and the number of attacks at each domain name.
Attack Source IP Addresses (④ in **Figure 6-5**)	The five IP addresses where the most attacks initiate and the number of attacks from each IP address.
Attack Source Locations (⑤ in **Figure 6-5**)	The five locations where the most attacks originate, along with the number of attacks from each.

7 Website Settings

7.1 Recommended Configurations After Website Connection

7.1.1 Configuring PCI DSS/3DS Compliance Check and TLS

Transport Layer Security (TLS) provides confidentiality and ensures data integrity for data sent between applications over the Internet. HTTPS is a network protocol constructed based on TLS and HTTP and can be used for encrypted transmission and identity authentication. If you select **Cloud** or **Dedicated** for **Protection** and set **Client Protocol** to **HTTPS**, set the minimum TLS version and cipher suite for your domain name, so that WAF can block requests that use a TLS version earlier than the one you configure. A cipher suite is a set of multiple cryptographic algorithms.

In WAF, the minimum TLS version configured is TLS v1.0, and the cipher suite is **Security cipher suite** by default.

WAF allows you to enable PCI DSS and PCI 3DS certification checks. After PCI DSS or PCI 3DS certification check is enabled, the minimum TLS version is automatically set to TLS v1.2 to meet the PCI DSS and PCI 3DS certification requirements. The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. PCI 3-Domain Secure (PCI 3DS) is a PCI Core Security Standard.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select the enterprise project from the **Enterprise Project** drop-down list and configure PCI DSS or PCI 3DS and TLS for the domain names.

Prerequisites

You have **added the website to WAF** and selected HTTPS for **Client Protocol**.

Constraints

- You have selected **Cloud Mode - CNAME** or **Dedicated Mode** for protection when adding the website to WAF.

  NOTE

  If you use **cloud mode - load balancer** access mode, you need to **configure TLS security policies** on the ELB console.

- If **Client Protocol** for the website you want to protect is set to **HTTP**, TLS is not required, and you can skip this topic.
- If you configure multiple combinations of server information, PCI DSS and PCI 3DS compliance certification checks can be set only when **Client Protocol** is set to **HTTPS** in all of those combinations.
- If PCI DSS/3DS compliance check is enabled, the client protocol cannot be changed, and no servers can be added.

Application Scenarios

By default, the minimum TLS version configured for WAF is **TLS v1.0**. To ensure website security, configure the right TLS version for your service requirements. **Table 7-1** lists the minimum TLS versions supported for different scenarios.

Table 7-1 Minimum TLS versions supported

Scenario	Minimum TLS Version (Recommended)	Protection Effect
Websites that handle critical business data, such as sites used in banking, finance, securities, and e-commerce.	TLS v1.2	WAF automatically blocks website access requests that use TLS v1.1 or TLS v1.1.
Websites with basic security requirements, for example, small and medium-sized enterprise websites.	TLS v1.1	WAF automatically blocks website access requests that use TLS v1.0.
Client applications with no special security requirements	TLS v1.0	Requests using any TLS protocols can access the website.

NOTE

Before you configure TLS, **check the TLS version of your website**.

The recommended cipher suite in WAF is **Security cipher suite**. It offers a good mix of browser compatibility and security. For details about each cipher suite, see **Table 7-2**.

Table 7-2 Description of cipher suites

Cipher Suite Name	Cryptographic Algorithm Supported	Cryptographic Algorithm Not Supported	Description
Classic cipher suite **NOTE** By default, **Security cipher suite** is configured for websites. However, if the request does not carry the server name indication (SNI), WAF uses the **Classic cipher suite**.	• ECDHE-RSA-AES256-SHA384 • AES256-SHA256 • RC4 • HIGH	• MD5 • aNULL • eNULL • NULL • DH • EDH • AESGCM	• Compatibility: Good. A wide range of browsers are supported. • Security: Average
Cipher suite 1	• ECDHE-ECDSA-AES256-GCM-SHA384 • HIGH	• MEDIUM • LOW • aNULL • eNULL • DES • MD5 • PSK • RC4 • kRSA • 3DES • DSS • EXP • CAMELLIA	Recommended configuration. • Compatibility: Good. A wide range of browsers are supported. • Security: Good
Cipher suite 2	• EECDH+AESGCM • EDH+AESGCM	-	• Compatibility: Average. Strict compliance with forward secrecy requirements of PCI DSS and excellent protection, but browsers of earlier versions may be unable to access the website. • Security: Excellent

Cipher Suite Name	Cryptographic Algorithm Supported	Cryptographic Algorithm Not Supported	Description
Cipher suite 3	• ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-SHA384 • RC4 • HIGH	• MD5 • aNULL • eNULL • NULL • DH • EDH	• Compatibility: Average. Earlier versions of browsers may be unable to access the website. • Security: Excellent. Multiple algorithms, such as ECDHE, DHE-GCM, and RSA-AES-GCM, are supported.
Cipher suite 4	• ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • AES256-SHA256 • RC4 • HIGH	• MD5 • aNULL • eNULL • NULL • EDH	• Compatibility: Good. A wide range of browsers are supported. • Security: Average. The GCM algorithm is supported.
Cipher suite 5	• AES128-SHA:AES256-SHA • AES128-SHA256:AES256-SHA256 • HIGH	• MEDIUM • LOW • aNULL • eNULL • EXPORT • DES • MD5 • PSK • RC4 • DHE	Supported algorithms: RSA-AES-CBC only

Cipher Suite Name	Cryptographic Algorithm Supported	Cryptographic Algorithm Not Supported	Description
Cipher suite 6	• ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256	-	• Compatibility: Average • Security: Good

Cipher Suite Name	Cryptographic Algorithm Supported	Cryptographic Algorithm Not Supported	Description
Security cipher suite	• ECDHE-ECDSA-AES256-GCM-SHA384 • HIGH	• MEDIUM • LOW • aNULL • eNULL • DES • MD5 • PSK • RC4 • kRSA • SRP • 3DES • DSS • EXP • CAMELLIA • SHA1 • SHA256 • SHA384	This cipher suite supports all algorithms in cipher suite 1, except for the CBC algorithm. Recommended. This cipher suite can meet security requirements in most scenarios. • Compatibility: Average. Core suite: ECDHE-ECDSA-AES256-GCM-SHA384. Old protocols and weak algorithms are disabled. Browsers of earlier versions may fail to access the system. • Security: Excellent
Cipher suite 8	• AESGCM • HIGH • ECDHE • RSA	• DH • EXPORT • RC4 • MEDIUM • LOW • aNULL • eNULL	Supports AES-GCM, providing strong encryption and data integrity protection. • Compatibility: Good. A wide range of browsers are supported. • Security: Good

The TLS cipher suites in WAF are compatible with all browsers and clients of later versions but are incompatible with some browsers of earlier versions. **Table 7-3** lists the incompatible browsers and clients if the TLS v1.0 protocol is used.

NOTICE

It is recommended that compatibility tests should be carried out on the service environment to ensure service stability.

Table 7-3 Incompatible browsers and clients for cipher suites under TLS v1.0

Browser/ Client	Classic Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4	Cipher Suite 5	Cipher Suite 6	Security Cipher Suite	Cipher Suite 8
Google Chrome 63 / macOS High Sierra 10.13.2	Not compatible	Compatible	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	√
Google Chrome 49/ Windows XP SP3	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Compatible	Compatible	Not compatible	√
Internet Explorer 6 /Windows XP	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
Internet Explorer 8 /Windows XP	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
Safari 6/iOS 6.0.1	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	Compatible	Not compatible	√
Safari 7/iOS 7.1	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible
Safari 7/OS X 10.9	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible

Browser/ Client	Classic Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4	Cipher Suite 5	Cipher Suite 6	Security Cipher Suite	Cipher Suite 8
Safari 8/iOS 8.4	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible
Safari 8/OS X 10.10	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	Compatible	Compatible	Compatible
Internet Explorer 7/Windows Vista	Compatible	Compatible	Not compatible	Compatible	Compatible	Not compatible	√	Not compatible	√
Internet Explorer 8, 9, or 10 /Windows 7	Compatible	Compatible	Not compatible	Compatible	Compatible	Not compatible	√	Not compatible	√
Internet Explorer 10 /Windows Phone 8.0	Compatible	Compatible	Not compatible	Compatible	Compatible	Not compatible	√	Not compatible	√
Java 7u25	Compatible	Compatible	Not compatible	Compatible	Compatible	Not compatible	√	Not compatible	√
OpenSSL 0.9.8y	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	√
Safari 5.1.9/OS X 10.6.8	Compatible	Compatible	Not compatible	Compatible	Compatible	Not compatible	√	Not compatible	√

Browser/ Client	Classic Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4	Cipher Suite 5	Cipher Suite 6	Security Cipher Suite	Cipher Suite 8
Safari 6.0.4/OS X 10.8.4	Compatible	Compatible	Not compatible	Compatible	Compatible	Not compatible	√	Not compatible	√

Impact on the System

- If you enable the PCI DSS certification check:
  - The minimum TLS version and cypher suite are automatically set to **TLS v1.2** and **EECDH+AESGCM:EDH+AESGCM**, respectively, and cannot be changed.
  - To change the minimum TLS version and cipher suite, disable the check.
- If you enable the PCI 3DS certification check:
  - The minimum TLS version is automatically set to **TLS v1.2** and cannot be changed.
  - The check cannot be disabled.

Configuring PCI DSS/3DS Compliance Check and TLS

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

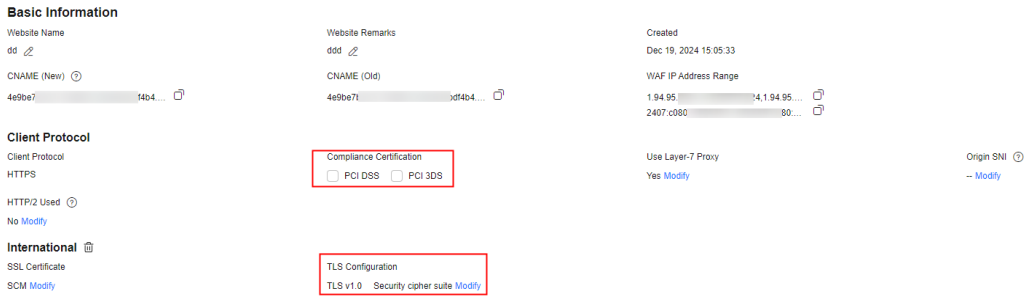
Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **Compliance Certification** row, you can select **PCI DSS** and/or **PCI 3DS** to allow WAF to check your website for the corresponding PCI certification compliance. In the **TLS Configuration** row, click  to complete TLS configuration.

Figure 7-1 TLS configuration modification



- Select **PCI DSS**. In the displayed **Warning** dialog box, click **OK** to enable the PCI DSS certification check.

  NOTICE

  If PCI DSS certification check is enabled, the minimum TLS version and cypher suite cannot be changed.

- Select **PCI 3DS**. In the displayed **Warning** dialog box, click **OK** to enable the PCI 3DS certification check.

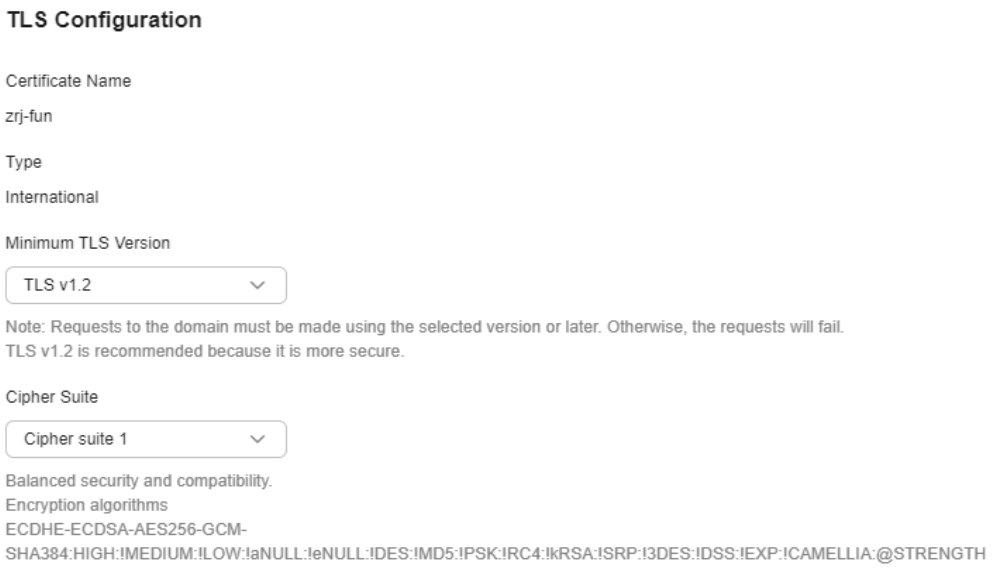
  NOTICE

  - If PCI 3DS certification check is enabled, the minimum TLS version cannot be changed.
  - Once enabled, the PCI 3DS certification check cannot be disabled.

Step 8 Click **Modify** next to a TLS cipher suite in the row of **International**.

Step 9 In the displayed **TLS Configuration** dialog box, select the minimum TLS version and cipher suite.

Figure 7-2 TLS Configuration



Select the minimum TLS version you need. The options are as follows:

- **TLS v1.0**: the default version. Requests using TLS v1.0 or later can access the domain name.
- **TLS v1.1**: Only requests using TLS v1.1 or later can access the domain name.
- **TLS v1.2**: Only requests using TLS v1.2 or later can access the domain name.

Step 10 Click **OK**.

If the configuration works, requests using TLS versions earlier than v1.2 will fail, and requests using TLS v1.2 or later will succeed.

----End

7.1.2 Enabling the HTTP/2 Protocol

If your website is accessible over the HTTP/2 protocol, enable HTTP/2 in WAF. The HTTP/2 protocol can be used only for access between the client and WAF on the condition that at least one origin server has **HTTPS** used for **Client Protocol**.

Prerequisites

You have **added the website to WAF** and selected HTTPS for **Client Protocol**.

Constraints

- The **Cloud Mode - CNAME** mode is used when you connect the website to WAF. Only professional and enterprise editions support HTTP/2.
- HTTP/2 is automatically enabled for dedicated WAF instances provisioned in May 2023 and later.
- For details about the regions that support HTTP/2, see **Functions**.

Enabling the HTTP/2 Protocol

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **HTTP/2 Used** row, click **Modify**. Then, select **Yes** and click **OK**.

If the configuration works, HTTP/2 access to the website will be supported.

----End

7.1.3 Configuring a Response Body Length in Logs

If WAF blocks or only logs an attack, the response details are displayed in the event list. If this function is not enabled and the length of the response body in logs is not configured, the response details are empty. If you enable the response details function and configure a specific length for the response body in logs, the response details will record the response body information up to the configured length. You can configure the response body length based on site requirements to make sure response bodies are recorded in event logs.

WAF logs response bodies by domain name. The default response body length is 2,048 bytes. You can configure a value ranging from 1 to 8,192 bytes.

NOTE

This function is under open beta test (OBT). You can **submit a service ticket** to enable it.

Prerequisites

You have **added your website to WAF**.

Configuring a Response Body Length in Logs

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by**

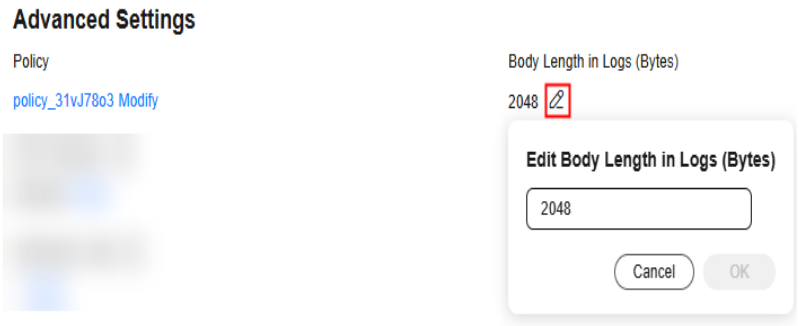
enterprise project drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **Advanced Settings** area, click next to **Body Length in Logs (Bytes)**, set a response body length (ranging from 1 to 8,192 bytes), and click **OK**.

Figure 7-3 Configuring a response body length in logs



After the configuration is complete, WAF displays response body details based on the configured response body length on the details page for new event logs.

To view response body details, choose **Events** in the navigation pane on the left. In the event list, locate the target event and click **Details** in the **Operation** column, and click the **Response Details** tab.

----End

7.1.4 Configuring Request and Response Header Forwarding

If you enable and configure request and response header forwarding, WAF will insert fields you specify into the header field of requests and responses, and forwards the requests to your origin server, and the responses to the client. This helps you distinguish requests from different sources and better analyze website operational status.

Prerequisites

You have **added the website you want to protect to WAF** in **Cloud Mode - CNAME** or **Dedicated Mode**.

Constraints

- You can configure request header and response header forwarding as long as **Cloud Mode - CNAME** or **Dedicated Mode** is in use.
- Forwarding custom request and response header fields is supported in some regions. For details, see **Functions**.
- You can configure up to eight key/value pairs.
- Dots (.) cannot be specified in the request header or response header for forwarding.

- The value can be set to a custom string or a variable starting with $. Variables starting with $ support only the following fields:

```
$time_local
$request_id
$connection_requests
$tenant_id
$project_id
$remote_addr
$remote_port
$scheme
$request_method
$http_host
$origin_uri
$request_length
$ssl_server_name
$ssl_protocol
$ssl_curves
$ssl_session_reused
```

Configuring Request and Response Header Forwarding

Step 1 **Log in to the management console**.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **Advanced Settings** area, click **Modify** next to **Request Header Field Forwarding** or **Response Header Field Forwarding**.

Step 8 In the displayed dialog box, enter a key/value pair and click **Add** to add multiple fields.

Figure 7-4 Request Header Field Forwarding

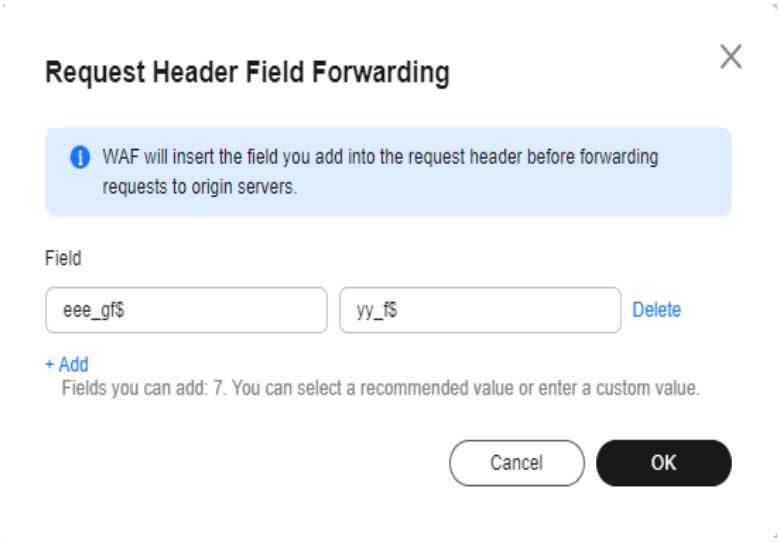
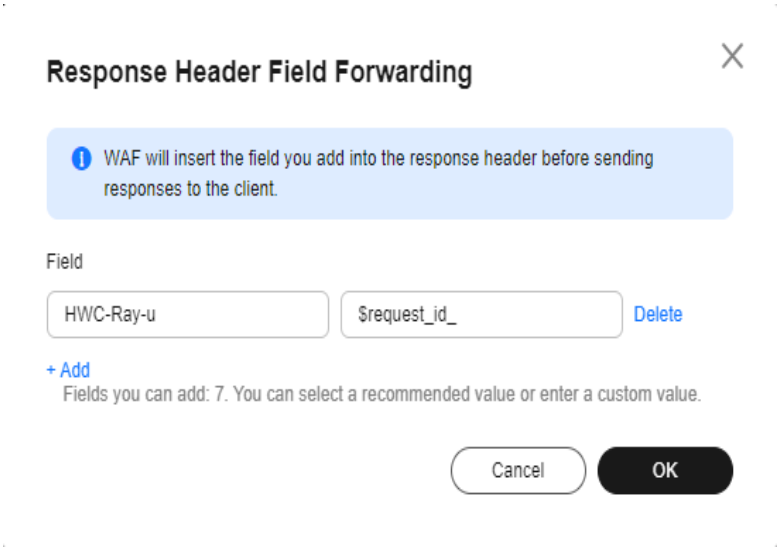


Figure 7-5 Response Header Field Forwarding



Step 9 After fields are added, click **OK**.

After the configuration is complete, check whether the configured request header forwarding fields are recorded in request headers and whether the configured response header forwarding fields are recorded in response headers.

----End

7.1.5 Modifying the Alarm Page

If a visitor is blocked by WAF, the **Default** block page of WAF is returned by default. You can also configure **Custom** or **Redirection** for the block page to be returned as required.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select the enterprise project from the **Enterprise Project** drop-down list and customize alarm pages for the domain names.

Prerequisites

You have connected the website you want to protect to WAF.

Constraints

- The **Redirection** mode is not supported if you select **Cloud Mode - Load balancer** for the protected website.
- The content of the text/html, text/xml, and application/json pages can be configured on the **Custom** block page to be returned.
- The root domain name of the redirection address must be the same as the currently protected domain name (including a wildcard domain name). For example, if the protected domain name is **www.example.com** and the port is 8080, the redirection URL can be set to **http://www.example.com:8080/error.html**.

Editing Response Page for Blocked Requests

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

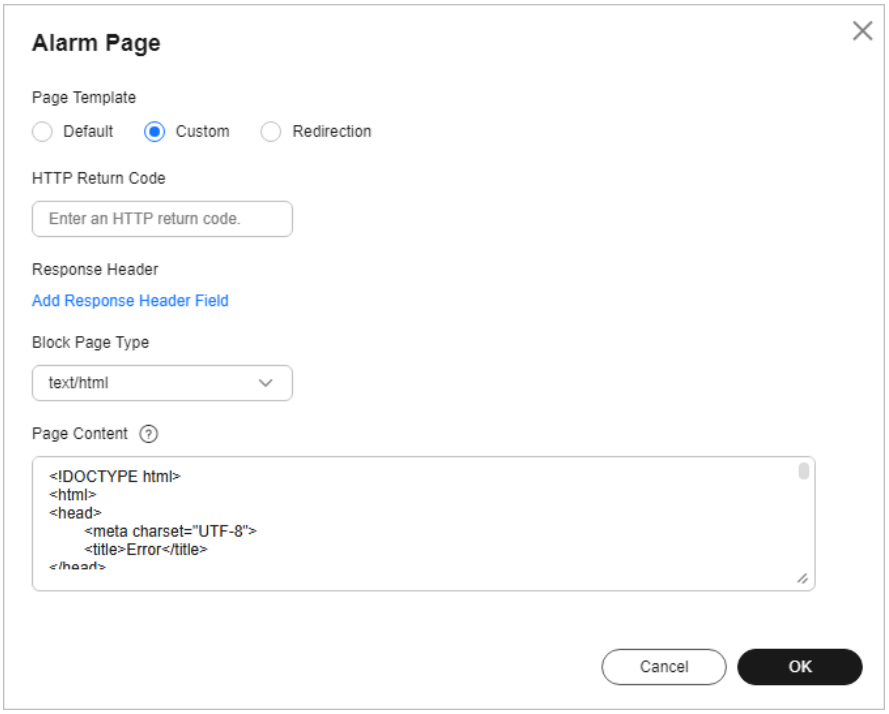
Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 Click **Modify** next to the page template name in the row of **Alarm Page**. In the displayed **Alarm Page** dialog box, specify **Page Template**.

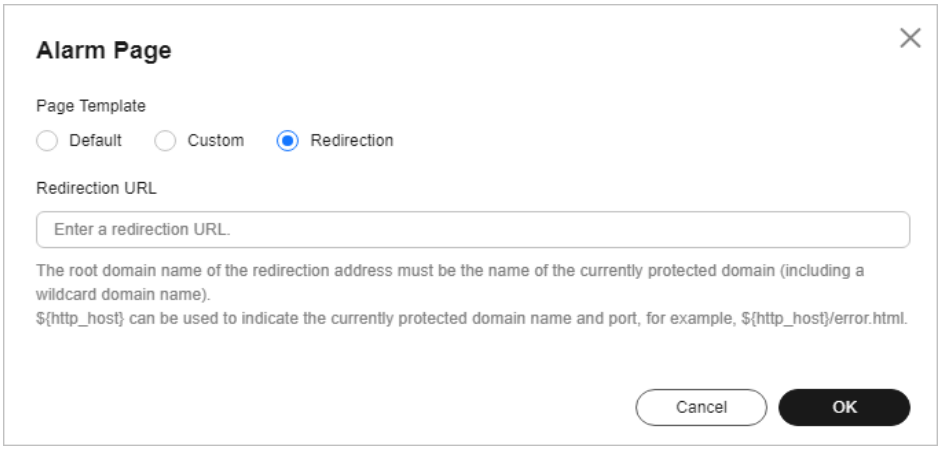
- To use the built-in page, select **Default**. An HTTP code 418 is returned.
- To customize the alarm page, select **Custom** and configure following parameters. Figure 7-6 shows an example.
  - **HTTP Return Code**: return code configured on a custom page.
  - **Response Header**: Click **Add Response Header Field** and configure response header parameters.
  - **Block Page Type**: The options are **text/html**, **text/xml**, and **application/json**.
  - **Page Content**: Configure the page content based on the selected value for **Block Page Type**.

Figure 7-6 Custom alarm page



- To configure a redirection URL, select **Redirection**.

  Figure 7-7 Redirection alarm page

  The root domain name of the redirection URL must be the same as the currently protected domain name (including a wildcard domain name). For example, if the protected domain name is **www.example.com** and the port is 8080, the redirection URL can be set to **http://www.example.com:8080/error.html**.

Step 8 Click **OK**.

After the above configuration is complete, you can enable basic web protection by referring to **Configuring Basic Web Protection to Defend Against Common Web Attacks** (with **Protective Action** set to **Block**) and verify the protection by referring to **Protection Verification**.

----End

7.1.6 Stopping WAF from Inserting Cookie Fields

This topic describes how to stop WAF from inserting the HWWAFSESTIME and HWWAFSESID fields into cookies. However, you should exercise caution when enabling this function. If WAF does not insert the HWWAFSESTIME and HWWAFSESID fields into cookies, CC attack protection rules (verification code), known attack source rules, and dynamic anti-crawler rules will be unable to work.

Prerequisites

You have selected **Dedicated Mode** or **Cloud Mode - Load balancer** when adding the website to WAF.

Procedure

Step 1 **Log in to the management console**.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **Do Not Insert the Cookie Field** column, click  to enable the function.

After the above configuration is complete, access the protected website. If the configuration works, the returned response cookie does not contain the **HWWAFSESTIME** or **HWWAFSESID** fields.

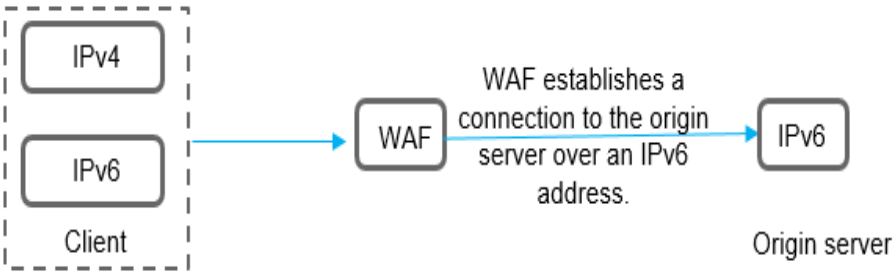
----End

7.1.7 Enabling WAF IPv6 Protection

You can enable IPv6 protection if needed. If IPv6 protection is enabled, WAF assigns an IPv6 access address to your domain name. WAF adds IPv6 address resolution to CNAME record sets by default. All IPv6 access requests are first forwarded to WAF. WAF detects and filters out malicious traffic and returns legitimate traffic to the origin server. This can keep origin servers secure, stable, and available.

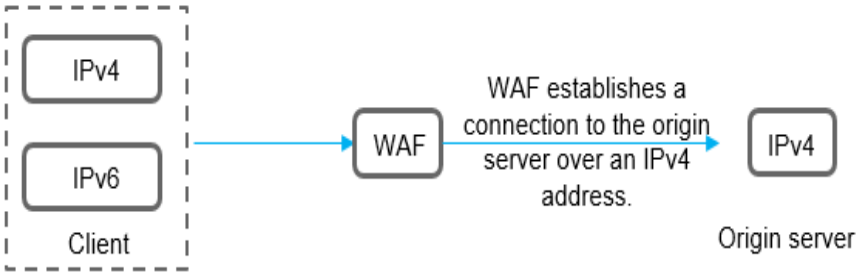
- If the origin server address of the protected website is an IPv6 address, IPv6 protection is enabled by default. WAF uses the IPv6 back-to-source address to establish a connection to the origin server.

  Figure 7-8 Only IPv6 addresses set for origin server addresses

- If the origin server address of the protected website is set to an IPv4 address, after you manually enable IPv6 protection, WAF uses the NAT64 mechanism to translate the external IPv6 traffic to internal IPv4 traffic. NAT64 is a network address translation (NAT) mechanism that enables communications between IPv6 and IPv4 servers. WAF uses the IPv4 back-to-source address to establish a connection to the origin server.

Figure 7-9 Only IPv4 addresses set for origin server addresses



Prerequisites

You have connected the website you want to protect to WAF.

Constraints

- The **Cloud Mode - CNAME** mode is used when you connect the website to WAF. Only professional and enterprise editions support IPv6 protection.
- For details about the regions that support IPv6 protection, see **Features**.
- If the origin server uses IPv6 addresses, IPv6 protection is enabled by default. To prevent IPv6 service from interruption, keep the IPv6 protection enabled. If IPv6 protection is not needed, edit the server configuration and delete IPv6 configuration from the origin server first. For details, see **Editing Server Information**.

Enabling WAF IPv6 Protection

Step 1 **Log in to the management console**.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **IPv6 Protection** row, click **Modify**. In the dialog box displayed, select **Enable** and click **OK**.

If the above configuration works, the website is accessible using an IPv6 address.

----End

7.1.8 Switching the Load Balancing Algorithm

If you configure one or more origin server addresses, you can use a load balancing algorithm to distribute traffic across these origin servers. WAF supports the following algorithms:

- **Origin server IP hash**: Requests from the same IP address are routed to the same backend server.
- Weighted round robin: All requests are distributed across origin servers in turn based on weights set to each origin server. The origin server with a larger weight receives more requests than others.
- **Session hash**: Requests with the same session tag are routed to the same origin server. To enable this algorithm, **configure traffic identifiers for known attack sources**, or Session hash algorithm cannot take effect.

Prerequisites

The website you want to protect has been connected to WAF.

Constraints

- The **Cloud Mode - CNAME** mode is used when you connect the website to WAF. Only professional and enterprise editions support using of a load balancing algorithm.
- You have selected the **dedicated mode** for your website.
- Configuring load balancing algorithms is supported in some regions. For details, see **Functions**.

Switching the Load Balancing Algorithm

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **Load Balancing Algorithm** field, click **Modify** . In the dialog box displayed, select a load balancing algorithm and click **OK**.

----End

7.1.9 Enabling the Cookie Security Attributes

If you set **Client Protocol** to **HTTPS**, you can enable **Cookie Security Attributes**. If you enable this, the HttpOnly and Secure attributes of cookies will be set to true.

Cookies are inserted by back-end web servers and can be implemented through framework configuration or set-cookie. Secure and HttpOnly in cookies help defend against attacks, such as XSS attacks to obtain cookies, and help defend against cookie hijacking.

If the AppScan scanner detects that the customer site does not insert security configuration fields, such as HttpOnly and Secure, into the cookie of the scan request, it records them as security threats.

Prerequisites

You have selected **Dedicated Mode** or **Cloud Mode - CNAME** and **added the website you want to protect to WAF**.

Constraints

- This function is not supported in **Cloud Mode - Load balancer** access mode.
- If the **Client Protocol** is set to **HTTP**, the **Cookie Security Attributes** function is disabled by default and cannot be enabled.

Enabling Cookie Security Attributes

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

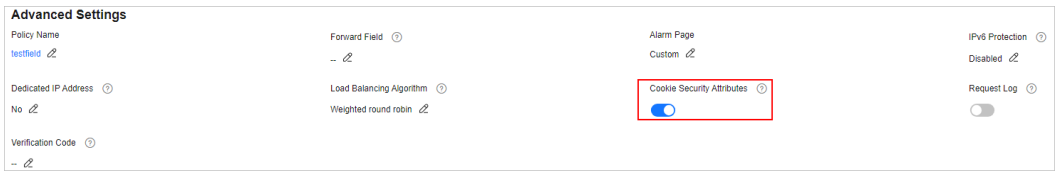
Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **Advanced Settings** area, click  next to **Cookie Security Attributes** to enable it.

Figure 7-10 Cookie Security Attributes



After completing the above configuration, enter the protected domain name in the address box of a browser, open the developer tool, and check whether the **HttpOnly** and **Secure** attributes of the cookie are set to **true**.

----End

7.1.10 Modifying a Verification Code

If **Protective Action** in a policy is set to **Verification code**, you can modify the response code on the verification page.

NOTE

This function is under open beta test (OBT). You can **submit a service ticket** to enable it.

Procedure

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **Advanced Settings** area, click  next to the **Verification Code** row, set a verification code, and click **OK**.

After the above configuration is complete, you can configure a CC attack protection rule (with **Protective Action** set to **Verification code**) by referring to **Configuring CC Attack Protection Rules to Defend Against CC Attacks** and verify the protection effect by referring to **Protection Verification**. After the verification is triggered, check whether the returned status code is the configured one.

----End

7.1.11 Configuring a Custom Log Trace ID

You can configure a custom log trace ID and record a specific header field in requests or responses to the **custom_traceid** field in the log.

NOTE

This function is under open beta test (OBT). You can **submit a service ticket** to enable it.

Constraints

This function is not supported if **Cloud Mode - Load balancer** access mode is in use.

Prerequisites

You have connected your website to WAF using **Cloud Mode - CNAME** or **Dedicated Mode**. For details, see **Connecting Your Website to WAF (Cloud Mode - CNAME Access)** and **Connecting Your Website to WAF (Dedicated Mode)**.

Configuring a Custom Log Trace ID

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

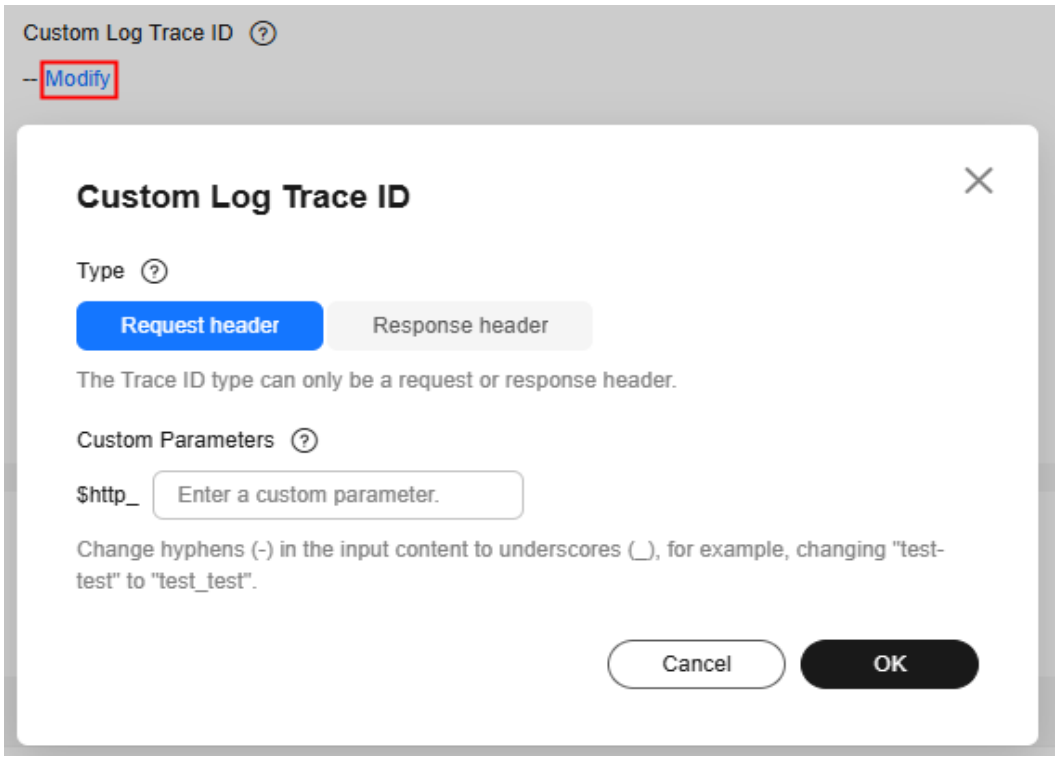
Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **Advanced Settings** area, click **Modify** under **Custom Log Trace ID**, specify **Type**, and configure **Custom Parameters**.

Figure 7-11 Custom Log Trace ID



After the above configuration is complete, access the protected website and check whether the **custom_traceid field** is displayed in the access logs in LTS and whether the value of the field is the configured value. For details about how to view access logs in LTS, see **Using LTS to Log WAF Activities**.

----End

7.1.12 Configuring a Traffic Identifier for a Known Attack Source

WAF allows you to configure traffic identifiers by IP address, session, or user tag to block possibly malicious requests from known attack sources based on **IP address**, **Cookie**, or **Params**.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select the project from the **Enterprise Project** drop-down list and configure known attack source traffic identifiers for the domain names.

Prerequisites

You have connected the website you want to protect to WAF.

Constraints

- If the IP address tag is configured, ensure that the protected website has a layer-7 proxy configured in front of WAF and that **Use Layer-7 Proxy** is set to **Yes** for the protected website.

If the IP address tag is not configured, WAF identifies the client IP address by default.

- Before enabling cookie- or params-based known attack source rules, configure a session or user tag for the corresponding website domain name.

Configuring a Traffic Identifier for a Known Attack Source

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **Traffic Identifier** area, click  next to **IP Tag**, **Session Tag**, or **User Tag** and configure a traffic identifier by referring to **Table 7-4**.

Figure 7-12 Traffic Identifier

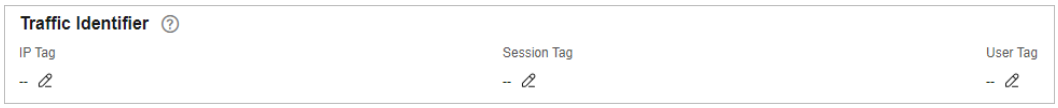


Table 7-4 Traffic identifier parameters

Tag	Description	Example Value
IP Tag	HTTP request header field of the original client IP address. Ensure that the protected website has a layer-7 proxy configured in front of WAF and that **Use Layer-7 Proxy** under the website basic information settings is set to **Yes** for this parameter to take effect. This field is used to store the real IP address of the client. You can customize the field name and configure multiple fields (separated by commas). After the configuration, WAF preferentially reads the configured field to obtain the real IP address of the client. If multiple fields are configured, WAF reads the IP address from left to right. **NOTICE** • If you want to use a TCP connection IP address as the client IP address, set **IP Tag** to **$remote_addr**. • If WAF does not obtain the real IP address of a client from fields you configure, WAF reads the **cdn-src-ip**, **x-real-ip**, **x-forwarded-for**, and **$remote_addr** fields in sequence to read the client IP address.	X-Forwarded-For
Session Tag	This tag is used to block possibly malicious requests based on the cookie attributes of an attack source. Configure this parameter to block requests based on cookie attributes.	sessiontest

Tag	Description	Example Value
User Tag	This tag is used to block possibly malicious requests based on the Params attribute of an attack source. Configure this parameter to block requests based on the Params attributes.	Params

Step 8 Click **OK**.

----End

Related Operations

Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration

7.1.13 Configuring a JA3/JA4 Fingerprint Tag

JA3/JA4 is a fingerprinting technology for SSL/TLS client identification. By analyzing TLS handshake metadata, it generates unique fingerprints to distinguish different client applications. With dedicated mode, if a layer-7 reverse proxy (for example, ELB) is deployed in front of WAF and its fingerprint is transferred to WAF with the header field, you can configure the JA3/JA4 fingerprint tags for the domain name protected by WAF. Then, the fingerprints along with tags will be transferred to WAF. WAF processes requests based on the TLS fingerprint (JA3) and TLS fingerprint (JA4) configured in the precise protection rule. This can mitigate JA3/JA4 fingerprinting attacks.

Prerequisites

You have connected your website to WAF in **dedicated mode**. For details, see **Connecting a Website to WAF (Dedicated Mode)**.

Constraints

This function is available only in dedicated mode.

Configuring a JA3/JA4 Fingerprint Tag

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

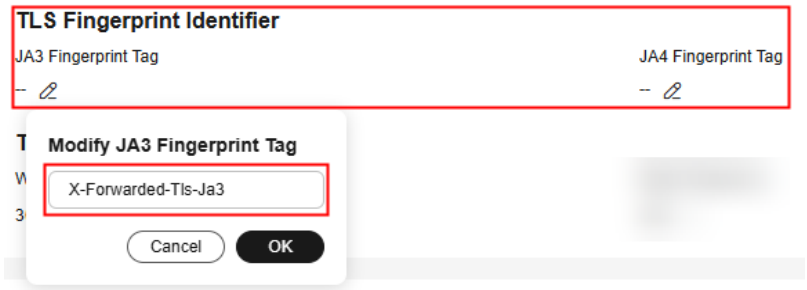
Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 Choose **Advanced Settings** > **TLS Fingerprint Identifier**, click ✎ under **JA3 Fingerprint Tag** or **JA4 Fingerprint Tag**, and enter the corresponding fingerprint tags.

- Set **JA3 Fingerprint Tag** to **X-Forwarded-Tls-Ja3**.
- Set **JA4 Fingerprint Tag** to **X-Forwarded-Tls-Ja4**.

Figure 7-13 TLS Fingerprint Identifier



----End

Follow-up Operations

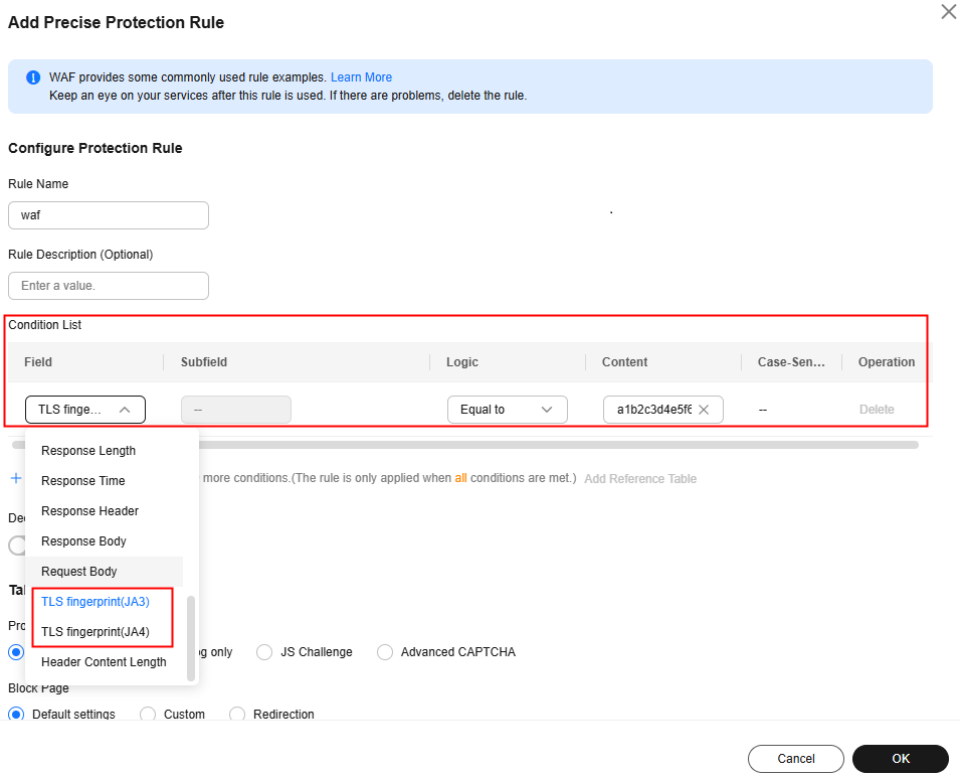
You can add a precise protection rule and configure TLS fingerprint (JA3) and TLS fingerprint (JA4) tags for the rules to process requests carrying JA3 and JA4 fingerprints.

Step 1 Return to the management console. In the navigation pane on the left, choose **Policies**.

Step 2 Click the target policy and enable **Precise Protection**.

Step 3 Click **Add Rule** and specify parameters.

Figure 7-14 Adding **TLS Fingerprint (JA3)** or **TLS Fingerprint (JA4)** tag for a rule



- **Condition**: Set **Field** to **TLS fingerprint (JA3)** or **TLS fingerprint (JA4)**, and set **Logic** and **Content** as required.
- Configure other parameters by referring to **Configuring a Precise Protection Rule**.

----End

Operation Result Verification

1. Clear the browser cache and access the protected website. The request is blocked.
2. Return to the WAF console. In the navigation pane on the left, choose **Events**. On the displayed page, view the event log.

7.1.14 Configuring a Timeout for Connections Between WAF and a Website Server

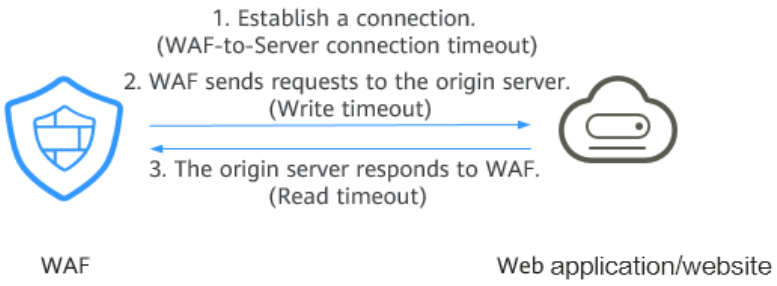
If you want to set a timeout duration for each request between your WAF instance and origin server, enable **Timeout Settings** and specify **WAF-to-Server connection timeout (s)**, **Read timeout (s)**, and **Write timeout (s)**. This function cannot be disabled once it is enabled.

- **WAF-to-Server Connection Timeout**: timeout for WAF and the origin server to establish a TCP connection.
- **Write Timeout**: Timeout set for WAF to send a request to the origin server. If the origin server does not receive a request within the specified write timeout, the connection times out.

- **Read Timeout**: Timeout set for WAF to read responses from the origin server. If WAF does not receive any response from the origin server within the specified read timeout, the connection times out.

Figure 7-15 shows the three steps for WAF to forward requests to an origin server.

Figure 7-15 WAF forwarding requests to origin servers.



NOTE

- The timeout for connections from a browser to WAF is 120 seconds. The value varies depending on your browser settings and cannot be changed on the WAF console.
- The default timeout for connections between WAF and your origin server is 30 seconds. You can customize this timeout. If you are using a dedicated WAF instance or professional or enterprise edition cloud WAF instance, you can configure connection timeout, read timeout, and write timeout.

Prerequisites

You have connected the website you want to protect to WAF.

Constraints

- You have selected **Cloud Mode - CNAME** or **Dedicated Mode** when adding the website to WAF.
- In cloud mode, only professional and enterprise editions support custom connection timeouts.
- The timeout duration for connections between a browser and WAF cannot be modified. Only timeout duration for connections between WAF and your origin server can be modified.
- This function cannot be disabled once it is enabled.
- For details about regions where you can configure a connection timeout, see **Functions**.

Configuring a Timeout for Connections Between WAF and a Website Server

Step 1 **Log in to the management console**.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **Timeout Settings** row, toggle  on if needed.

Step 8 Click  , specify **WAF-to-Server connection timeout (s)**, **Read timeout (s)**, and **Write timeout (s)**, and click **OK** to save settings.

----End

7.1.15 Enabling Break Protection to Protect Origin Servers

If a large number of 502 Bad Gateway and 504 Gateway Timeout errors are detected, you can enable WAF breakdown protection and connection protection to let WAF suspend your website and protect your origin servers from being crashed. When the 502/504 error requests and pending URL requests reach the thresholds you configure, WAF enables corresponding protection for your website.

Prerequisites

- You have **added the website to WAF**.
- You have upgraded the dedicated WAF instance to the latest version. For details, see **Upgrading a Dedicated WAF Instance**.

Constraints

- You have selected **Dedicated mode** for your website deployment.
- Before enabling **Break Protection**, make sure **you have updated dedicated WAF instances to the latest version,**, or your services might be affected.
- Connection Protection is available in some regions. For details, see **Functions**.

Enabling Break Protection

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **Break Protection** area, click the status icon to toggle it on.

Figure 7-16 Break Protection

Step 8 Click next to each parameter, edit **Breakdown Protection** and **Connection Protection** parameters to meet your requirements, and click **OK** to save settings. **Table 7-5** describes these parameters.

Table 7-5 Connection Protection parameters

Parameter		Description	Example Value
Breakdown Protection	502/504 Error Threshold	30s 502/504 Error Threshold	1000
	502/504 Error Percentage (%)	A breakdown is triggered when the 502/504 error threshold and percentage threshold have been reached.	90
	Initial Downtime (s)	Protection period upon the first breakdown. During this period, WAF stops forwarding client requests.	180

Parameter		Description	Example Value
	Multiplier for Consecutive Breakdowns	The maximum multiplier you can use for consecutive breakdowns. The number of breakdowns are counted from 0 every time the accumulated breakdown protection duration reaches 3,600s. For example, assume that **Initial Downtime (s)** is set to 180s and **Multiplier for Consecutive Breakdowns** is set to 3. ● If the breakdown is triggered for the second time, that is, less than 3, the protection duration is 360s (180s x 2). ● If the breakdown is triggered for the third or fourth time, that is, greater than or equal to 3, the protection duration is 540s (180s x 3). ● The breakdowns are counted from 0 when the total downtime duration exceeds one hour (3,600s).	3
Connection Protection	Pending URL Request Threshold	Connection Protection is triggered when the number of read URL requests reaches the threshold you configure.	6,000
	Duration (s)	Protection duration. During this period, WAF stops forwarding client requests.	60

NOTE

Use **Figure 7-16** as an example:

- **Breakdown Protection**: When the number of 502/504 errors returned by the protected website exceeds 1,000 and accounts for 90% or more of the total access requests of the website for the first time, the first breakdown protection is triggered. During the first breakdown protection, WAF stops forwarding client requests for 180s (that is, blocks visitors access to the website for 180s). If a second consecutive breakdown protection is triggered, WAF stops forwarding client requests for 360s (180 x 2). If a third or more consecutive breakdowns are triggered, WAF stops forwarding client requests for 540s (180s x 3). The breakdowns are counted from 0 when the total downtime duration exceeds one hour (3,600s).
- **Connection Protection**: When the number of read URL requests in the waiting queue exceeds 6,000, WAF stops forwarding client requests for 60s and returns the maintenance page of the website to visitors.

----End

7.2 Managing Websites

7.2.1 Viewing Basic Information of a Website

This topic describes how to view client protocol, policy name, alarm page, CNAME record, and CNAME IP address configured for a protected domain name.

Prerequisites

You have connected the website you want to protect to WAF.

Viewing Basic Information of a Website

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 View the protected website list. For details about parameters, see **Table 7-6**.

Figure 7-17 Website list

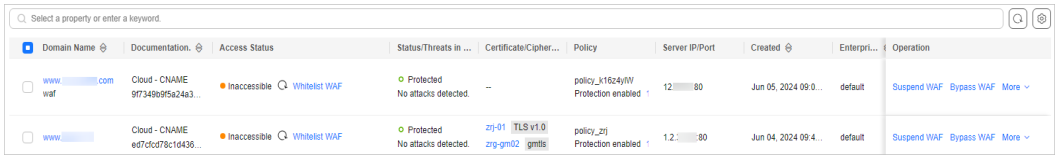


Table 7-6 Parameter descriptions

Parameter	Description
Domain Name	Protected domain name or IP address.
Protection	WAF protection configured for your website. You can select **Cloud Mode - CNAME**, **Cloud Mode - Load balancer**, or **Dedicated Mode**.
Access Status	The progress of connecting your website to WAF or the website access status. • **Inaccessible**: The website has not been connected to WAF yet or failed to connect to WAF. • **Accessible**: The website has been connected to WAF. • **DNS error**: If the **Access Mode** is **Cloud mode - CNAME access**, the DNS service resolves the website domain name to a proxy, such as CDN, that is deployed before WAF, and no website traffic can pass through WAF. **NOTICE** The initial **Access Status** of a website protected in **Dedicated Mode** or **Cloud Mode - Load balancer** is **Inaccessible**. When a request reaches your WAF instance, the initial access status automatically changes to **Accessible**.
Status/Threats in Last 3 Days	WAF protection status and security situation of the domain name for the past three days. WAF supports the following protection modes: • **Protected**: The WAF protection is enabled. • **Unprotected**: The WAF protection is disabled. If a large number of normal requests are blocked, for example, status code 418 is frequently returned, then you can switch the mode to **Suspended**. In this mode, your website is not protected because WAF only forwards requests. It does not scan for attacks. This mode is risky. You are advised to use the global protection whitelist rules to reduce false alarms.
Certificate/Cipher Suite	Certificate and cipher suite used for the domain name. You can click the certificate name to go to the **Certificates** page.
Policy	Number of types of WAF protection enabled for the domain name. Policy applied to the domain name. You can click the number to go to the rule configuration page and configure specific protection rules. For details, see **Configuring Protection Policies**.
Server IP/Port	Public IP address of the website server accessed by the client and the service port used by WAF to forward client requests to the server.
Created	Time the website was added to WAF.

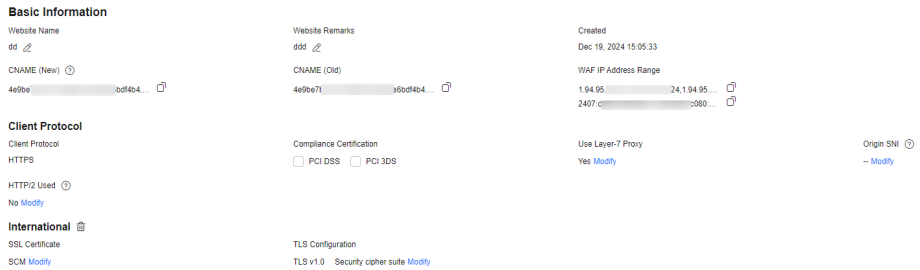
Parameter	Description
Enterprise Project	Enterprise project the domain name belongs to.

Step 8 In the **Domain Name** column, click the domain name of the website to go to the basic information page.

Step 9 View the basic information about the protected website.

To modify a parameter, locate the row that contains the target parameter and click the edit icon.

Figure 7-18 Basic Information



----End

7.2.2 Exporting Website Settings

You can export settings of all websites protected by WAF in your account on the **Website Settings** page.

Prerequisites

You have connected the website you want to protect to WAF.

Exporting Website Settings

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 In the upper right corner above the website list, click **Export** to export the website information list.

----End

7.2.3 Changing the Protection Mode

After a website is connected to WAF, WAF protection is enabled by default. WAF detects traffic based on the protection policy you configure for the website. If a large number of normal requests are blocked, for example, status code 418 is frequently returned, you can suspend WAF. If you suspend WAF protection, WAF only forwards requests to origin servers. It does not scan for or log attacks.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select the enterprise project from the **Enterprise Project** drop-down list and switch WAF working mode for a specific domain name.

Prerequisites

You have connected the website you want to protect to WAF.

Impact on the System

If you suspend WAF protection, WAF does not scan for attacks and only forwards requests to origin servers. This is risky. To avoid normal requests from being blocked, configure global protection whitelist rules, instead of suspending WAF protection.

Changing the Protection Mode (Enabling/Suspending WAF Protection)

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 Change the protection mode.

- Enabling protection: In the row containing the target domain name, click **Enable WAF** in the **Operation** column. In the displayed dialog box, click **OK**. If you **Enable WAF**, the **Status** of the domain name changes to **Protected**.
- Suspending protection: In the row containing the target domain name, click **Suspend WAF** in the **Operation** column. In the displayed dialog box, click **OK**. If you **Suspend WAF**, the **Status** of the domain name changes to **Unprotected**.

----End

Related Operations

- Handling False Alarms
- How Do I Troubleshoot 404/502/504 Errors?

7.2.4 Changing the Protection Policy for a Protected Website

This topic walks you through how to change the protection policy used for a website.

Prerequisites

You have used a protection policy for a website. For details, see **Policy Management**.

Constraints

In **Cloud Mode - CNAME** access mode, only the professional and enterprise editions support changing the protection policy for a website.

Changing the Protection Policy for a Protected Website

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **Advanced Settings** area, click **Modify** in the **Policy** column. In the dialog box displayed, select a policy and click **OK**.

----End

7.2.5 Updating the Certificate Used for a Website

If you select **Cloud Mode - CNAME** or **Dedicated Mode** as the access mode and set **Client Protocol** to **HTTPS**, a certificate is required for your website.

- If your website certificate is about to expire, purchase a new certificate before the expiration date and update the certificate associated with the website in WAF.

  WAF can send notifications if a certificate expires. You can configure such notifications on the **Notifications** page. For details, see **Enabling Alarm Notifications**.

- If you plan to update the certificate associated with the website, associate a new certificate with your website on the WAF console.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select the enterprise project from the **Enterprise Project** drop-down list and update certificates.

Prerequisites

You have **added the website to WAF** and selected HTTPS for **Client Protocol**.

Constraints

- Each domain name must have a certificate associated. A wildcard domain name can only use a wildcard domain certificate. If you only have single-domain certificates, add domain names one by one in WAF.
- Only .pem certificates can be used in WAF. If the certificate is not in .pem, before uploading it, convert it to .pem by referring to **Step 7**.
- Only accounts with the **SCM Administrator** and **SCM FullAccess** permissions can select SCM certificates.
- Before updating the certificate, ensure that your WAF instance and the certificate you want to upload belong to the same account.

Impact on the System

- It is recommended that you update the certificate before it expires. Otherwise, all WAF protection rules will fail to take effect, and there can be massive impacts on the origin server, even more severe than a crashed host or website access failures.
- Updating certificates does not affect services. The old certificate still works during the certificate replacement. The new certificate will take over the job once it has been uploaded and successfully associated with the domain name.
- Access to your website may be affected when you update the configurations of certificates used for backend servers or for domain names of your websites protected by WAF. To minimize these impacts, update the certificates during off-peak hours.

Updating the Certificate Used for a Website

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 Click **Modify** next to the certificate name. In the **Update Certificate** dialog box, import a new certificate or select an existing certificate.

- If you select **Import new certificate** for **Update Method**, enter a certificate name, and copy and paste the certificate file and private key into the corresponding text boxes.

  The newly imported certificates will be listed on the **Certificates** page. For more details, see **Uploading a Certificate to WAF**.

  NOTE

  WAF encrypts and saves the private key to keep it safe.

  Only .pem certificates can be used in WAF. If the certificate is not in .pem format, convert it into .pem locally by referring to **Table 7-7** before uploading it.

Table 7-7 Certificate conversion commands

Format	Conversion Method
CER/CRT	Rename the **cert.crt** certificate file to **cert.pem**.
PFX	– Obtain a private key. For example, run the following command to convert **cert.pfx** into **key.pem**: **openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes** – Obtain a certificate. For example, run the following command to convert **cert.pfx** into **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. Convert a certificate. For example, run the following command to convert **cert.p7b** into **cert.cer**: **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. Rename certificate file **cert.cer** to **cert.pem**.
DER	– Obtain a private key. For example, run the following command to convert **privatekey.der** into **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** – Obtain a certificate. For example, run the following command to convert **cert.cer** into **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTE

- Before running an OpenSSL command, ensure that the **OpenSSL** tool has been installed on the local host.
- If your local PC runs a Windows operating system, go to the command line interface (CLI) and then run the certificate conversion command.

- If you select **Select existing certificate** for **Update Method**, select an existing certificate from the **Certificate** drop-down list.

  NOTE

  If there are no certificates available, click **Purchase Certificate** and purchase a certificate and push it to WAF.

- If you select **SCM certificate** for **Update Method**, select a certificate managed in CCM. It can be a certificate you purchased through CCM or an external certificate you uploaded to CCM.

  CAUTION

  The SCM certificate domain name must be the same as the one you added to WAF.

Step 8 Click **OK**.

----End

Related Operations

Uploading a Certificate to WAF

7.2.6 Editing Server Information

If you select **Cloud Mode - CNAME** or **Dedicated Mode** when adding a website to WAF, you can edit the server information of your website.

Applicable scenarios:

- Edit server information.
  - Cloud Mode - CNAME access: You can modify configurations for **Client Protocol**, **Server Protocol**, **Server Address**, **Weight**, and **Server Port**.
  - Dedicated mode: You can modify configurations for **Client Protocol**, **Server Protocol**, **Server Address**, **VPC**, **Weight**, and **Server Port**.
- Add server configurations.
- Update a certificate by referring to **Updating the Certificate Used for a Website**.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select the enterprise project from the **Enterprise Project** drop-down list and configure server information for the domain names.

Prerequisites

You have connected the website you want to protect to WAF.

Constraints

- If PCI DSS/3DS compliance check is enabled, the client protocol cannot be changed, and no origin server addresses can be added.
- Server configuration information can be modified in batches only for domain names connected to WAF in the same access mode.

Impact on the System

Modifying the server configuration does not affect services.

Modifying Server Information of One Website

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 On the **Website Settings** page, click the target website domain name.

Step 7 In the **Origin Servers** area, click **Edit**.

Step 8 In the **Edit Server Information** dialog box, edit the server configurations and associated certificates as needed.

- For details about certificate, see **Updating the Certificate Used for a Website**.
- WAF supports configuring of multiple backend servers. To add a backend server, click **Add**.
- You can click **Enable** in the **IPv6 Protection** row if needed.

Step 9 Click **OK**.

----End

Batch Modifying Origin Server Information of Websites

Batch modifying origin server information is supported only for domain names connected to WAF in the same access mode.

Step 1 In the navigation pane on the left, choose **Website Settings**.

Step 2 Select domain names whose server configurations need to be modified. In the upper part of the website list, click **Modify**.

Step 3 Edit the server configurations and associated certificates as needed.

WAF supports configuring of multiple backend servers. To add a backend server, click **Add**.

Step 4 Click **OK**.

This action will take a while. Please be patient. After the modification is successful, the domain names with server information modified will be displayed.

----End

Verification

After the server information is modified, it takes about two minutes for the modification to take effect.

7.2.7 Viewing Protection Information About a Protected Website on Cloud Eye

You can go to Cloud Eye to view protection details about your websites protected with WAF.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select the enterprise project from the **Enterprise Project** drop-down list and view details about protected websites on Cloud Eye.

Prerequisites

You have connected the website you want to protect to WAF.

Viewing Protection Details About a Protected Website on Cloud Eye

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 In the row containing the protected domain name, click **More** > **Cloud Eye** in the **Operation** column to go to the Cloud Eye console and view the monitoring information.

----End

7.2.8 Migrating Domain Names to Other Enterprise Projects

WAF allows you to migrate domain names from an enterprise project to another one. Note that the migrated domain names will not be listed in the original enterprise project.

Certificates and policies are not migrated along with domain names. You need to configure them during the migration.

Prerequisites

You have connected the website you want to protect to WAF.

Constraints

- In cloud mode, only the professional and enterprise editions support migrating domain names to other enterprise projects.
- In **dedicated mode**, before migrating a website to other enterprise project, ensure that there is a dedicated WAF instance available in the destination enterprise project.
- Certificates and policies are not migrated along with domain names. You need to configure them during the migration.

Migrating Domain Names to Other Enterprise Projects

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

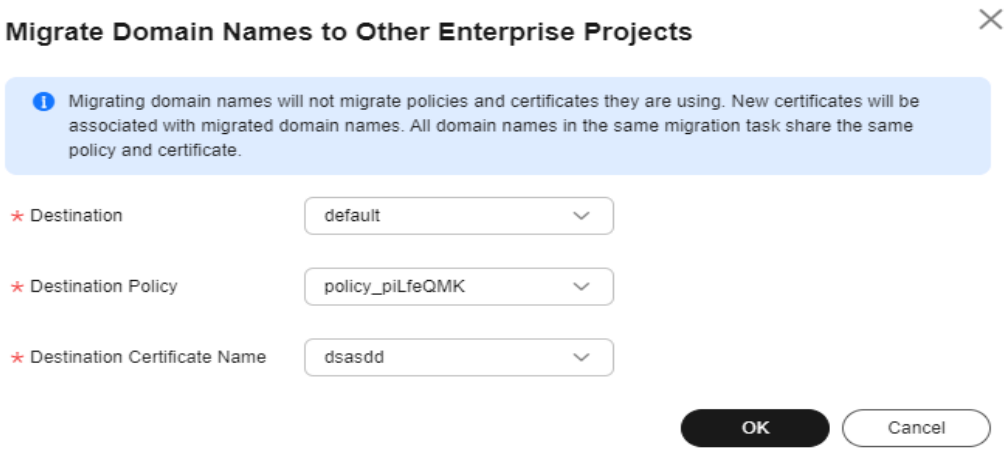
Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 Select the domain names you want to migrate. In the upper right corner of the website list, click **Migrate Domain Name**.

- **Destination**: Select the enterprise project you want to migrate domain names to.
- **Destination Policy**: Select a policy for domain names you are migrating. This is because policies are not migrated along with domain names.
- **Destination Certificate Name**: Select a certificate for domain names you are migrating. This is because certificates are not migrated along with domain names.

Figure 7-19 Migrate Domain Names to Other Enterprise Projects



----End

7.2.9 Deleting a Protected Website from WAF

This topic describes how to remove a website from WAF if you no longer need to protect it.

In cloud CNAME access mode, before removing a website from WAF, you need to resolve your domain name to the IP address of the origin server, or the traffic to your domain name cannot be routed to the origin server.

If you want to add a website you deleted before to WAF again, follow the process in **Connecting a Website to WAF**.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select your enterprise project from the **Enterprise Project** drop-down list and delete protected domain names.

Prerequisites

You have connected the website you want to protect to WAF.

Impact on the System

- In cloud CNAME access mode, before removing a website from WAF, you need to resolve the domain name to the origin server IP address on the DNS platform, or the traffic to your domain name cannot be routed to the origin server.
- If you select **Forcible delete the WAF CNAME record.**, WAF will not check your domain name resolution and delete WAF CNAME record immediately. Before enabling this option, make sure you have resolved the domain name to the origin server, or your website will become inaccessible.

  NOTE

  If you do not select **Forcibly delete the WAF CNAME record**, WAF will retain the CNAME record of the domain name for about 30 days before deleting it.

- It takes about a minute to remove a website from WAF, but once this action is started, it cannot be cancelled. Exercise caution when removing a website from WAF.

Deleting a Protected Website from WAF

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Website Settings**.

Step 6 Locate the row of the target domain name. In the **Operation**, click **More** > **Delete**.

Step 7 In the displayed confirmation dialog box, confirm the deletion.

- Cloud mode
  - No proxy used

    NOTE

    - Ensure that related configurations are completed and select **The CNAME of the domain name has been deleted from the DNS provider, and an A record has been configured to the origin server IP address, or services carried on the domain name have been brought offline**.
    - If you select **Forcible delete the WAF CNAME record.**, WAF will not check your domain name resolution and delete WAF CNAME record immediately. Before enabling this option, make sure you have resolved the domain name to the origin server, or your website will become inaccessible.
    - If you want to retain the policy applied to the domain name, select **Retain the policy of this domain name**.
  - Proxy used

    NOTE

    - Ensure that related configurations are completed and select **The domain name has been pointed to the origin server on the Advanced Anti-DDoS, CDN, or cloud acceleration product side, or services carried on the domain name have been brought offline**.
    - If you select **Forcible delete the WAF CNAME record.**, WAF will not check your domain name resolution and delete WAF CNAME record immediately. Before enabling this option, make sure you have resolved the domain name to the origin server, or your website will become inaccessible.
    - If you want to retain the policy applied to the domain name, select **Retain the policy of this domain name**.

- Cloud mode - Load balancer access/Dedicated mode

  If you want to retain the policy applied to the domain name, select **Retain the policy of this domain name**.

Step 8 Click **OK**. If **Domain name deleted successfully** is displayed in the upper right corner, the domain name of the website was deleted.

----End

Related Operations

To delete domain names in batches, select the domain names and click **Delete** above the website list.

8 Policy Management

8.1 Creating a Protection Policy

A policy is a combination of rules, such as basic web protection, blacklist, whitelist, and precise protection rules. A policy can be applied to multiple domain names, but only one policy can be used for a domain name. This topic describes how to add a policy for your WAF instance.

NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and add protection policies in the project.

Constraints

- This function is not supported in the standard edition.
- A protected website domain name can use only one policy.
- You can copy policies in the same enterprise project.

Procedure

You can add a protection policy in either of the following ways.

Adding a Protection Policy

A protection policy can be applied to multiple protected domain names, but a protected domain name can have only one protection policy.

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by**

enterprise project drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 In the upper left corner, click **Add Policy**.

Step 7 In the displayed dialog box, enter the policy name and click **OK**. The added policy will be displayed in the policy list.

Step 8 In the **Policy Name** column, click the policy name. On the displayed page, add rules to the policy by referring to **Rule Configurations**.

After completing the preceding configuration, you can view the added policy in the policy list.

----End

Copying a Protection Policy

You can copy policies in the same enterprise project.

NOTE

If your policy has a known attack source rule configured, configure it again after you copy the policy as known attack source rules configured in dependent rules will become invalid in the new policy.

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 Locate the row containing the policy you want to copy. In the **Operation** column, click **Copy**.

Step 7 In the dialog box displayed, enter a policy name, specify the enterprise project, and click **OK**.

----End

Related Operations

- To modify a policy name, click  next to the policy name. In the dialog box displayed, enter a new policy name.
- To delete a rule, locate the row containing the rule. In the **Operation** column, click **More** > **Delete**.
- To delete protection policies in batches, select all policies you want to delete and click **Delete** above the policy list.

8.2 Adding a Domain Name to a Policy

You can add a domain name to a new policy you think applicable. Then, the original policy applied to the domain name stops working on this domain name.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select the project from the **Enterprise Project** drop-down list and configure protection policies for the domain names in batches.

Prerequisites

You have connected the website you want to protect to WAF.

Constraints

This function is not supported in the standard edition.

Adding a Domain Name to a Policy

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

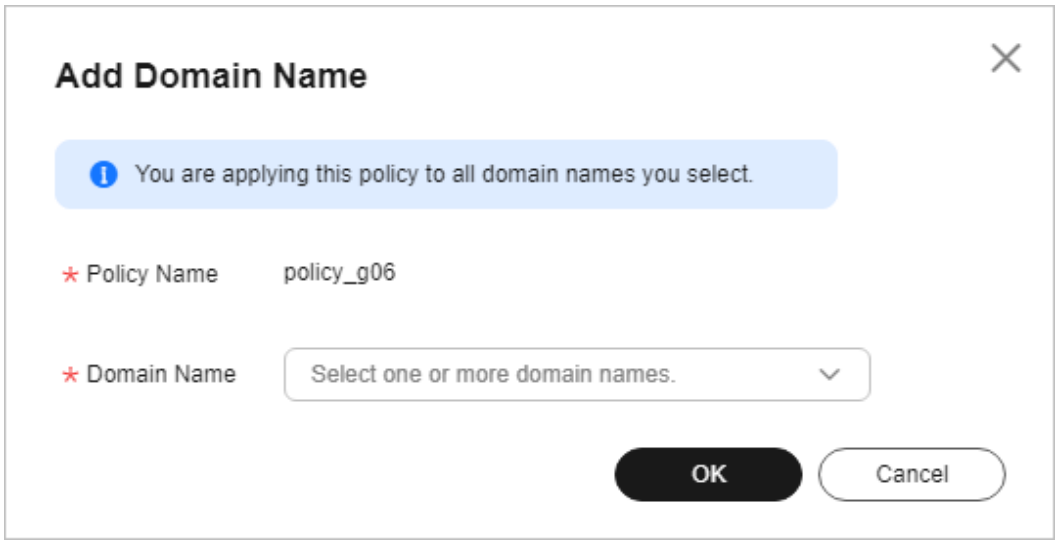
Step 6 In the row containing the target policy, click **Add Domain Name** in the **Operation** column.

Step 7 Select one or more domain names from the **Domain Name** drop-down list.

NOTICE

- A protected domain name can use only one policy, but one policy can be applied to multiple domain names.
- To delete a policy that has been applied to domain names, add these domain names to other policies first. Then, click **More** > **Delete** in the **Operation** column of the policy you want to delete.

Figure 8-1 Selecting one or more domain names



Step 8 Click **OK**.

----End

8.3 Adding Rules to One or More Policies

This topic describes how to add rules to one or more policies.

Constraints

If **Enterprise Project** is set to **All projects**, no rules can be added to a policy.

Adding Rules to One or More Policies

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, click **Policies**.

Step 6 In the upper left corner of the policy list, click **View All Policies & Rules**.

Step 7 In the upper left corner above a list of a type of rule, click **Add Rule**.

Step 8 Select one or more policies from the **Policies** drop-down list.

Step 9 Set other parameters in addition to **Policies**.

- To add a CC attack protection rule, see **Table 5-5**.

- To add a precise protection rule, see **Table 5-6**.
- To add a blacklist or whitelist rule, see **Table 5-7**.
- To add a geolocation access control rule, see **Table 5-8**.
- To add a WTP rule, see **Table 5-10**.
- To add an information leakage prevention rule, see **Table 5-13**.
- To add a global protection whitelist rule, see **Table 5-14**.
- To add a data masking rule, see **Table 5-15**.

Step 10 Click **OK**.

----End

Related Operations

- After a rule is added, the rule is **Enabled** by default. To disable it, click **Disable** in the **Operation** column of the target rule. You can also select multiple rules and click **Disable** above the rule list to disable them all together.
- To modify a rule, locate the row that contains the rule and click **Modify** in the **Operation** column. You can also select multiple rules and click **Modify** above the list to modify them all together.
- To delete a rule, locate the row that contains the rule and click **Delete** in the **Operation** column. You can also select multiple rules and click **Delete** above the list to delete them all together.
- To enable multiple rules, select them and click **Enable** above the list.

9 Security Reports

WAF can generate daily, weekly, monthly, or custom reports based on the report templates you have created. Reports will be sent to you in the way and within the time range you configure.

Prerequisites

You have connected the website you want to protect to WAF.

Constraints

- WAF offers a quota for creating report templates.
  - Cloud mode - professional edition: 10
  - Cloud mode - enterprise edition or dedicated mode: 20
  - Cloud mode - standard edition: 5
- WAF stores security reports for six months only. You are advised to regularly download reports to meet compliance and audit requirements.

Creating a Report Template

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 4 In the navigation pane on the left, click **Reports**.

Step 5 In the upper left corner of the list, click **Create Report Template**. **Table 9-1** describes the parameters.

NOTE

- Currently, security reports cannot be filtered by enterprise project in the upper part of the navigation pane. To filter resources by enterprise project, select the enterprise project the report belongs to and the enterprise project from which the report data comes when creating a report template.
- If the security report quota has been used up, the **Create Report Template** button will be grayed out. You should delete the security report templates that are not frequently used in a timely manner to make sure you have available report quota.

Figure 9-1 Create Report Template

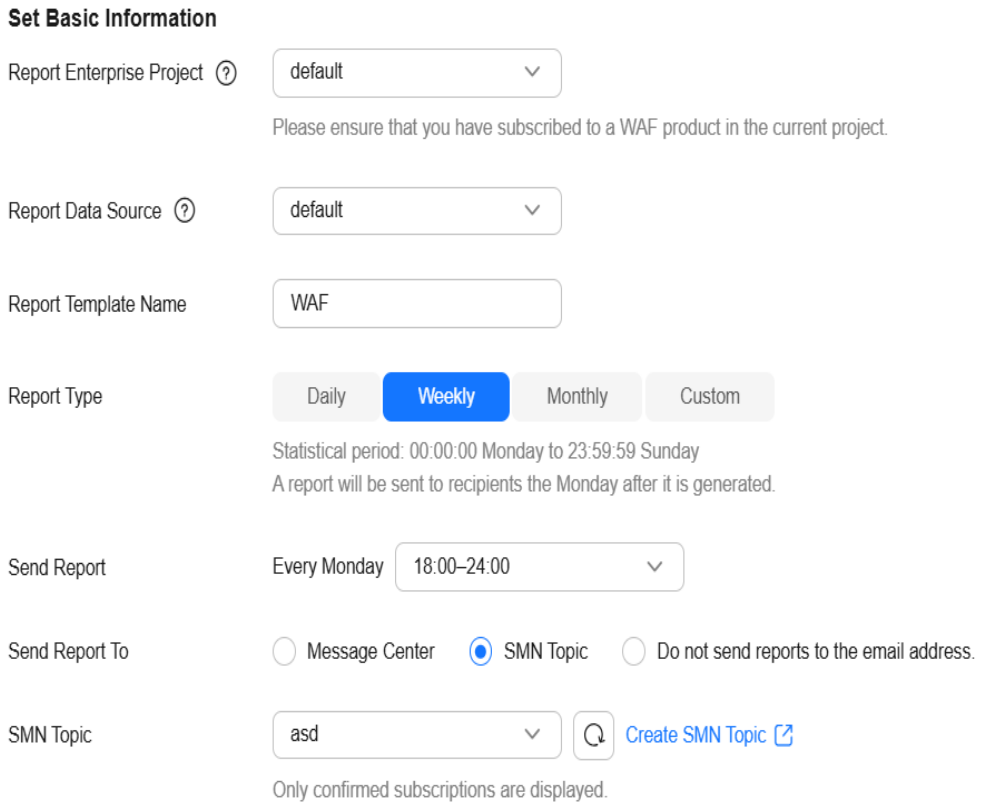


Table 9-1 Parameters for creating a report template

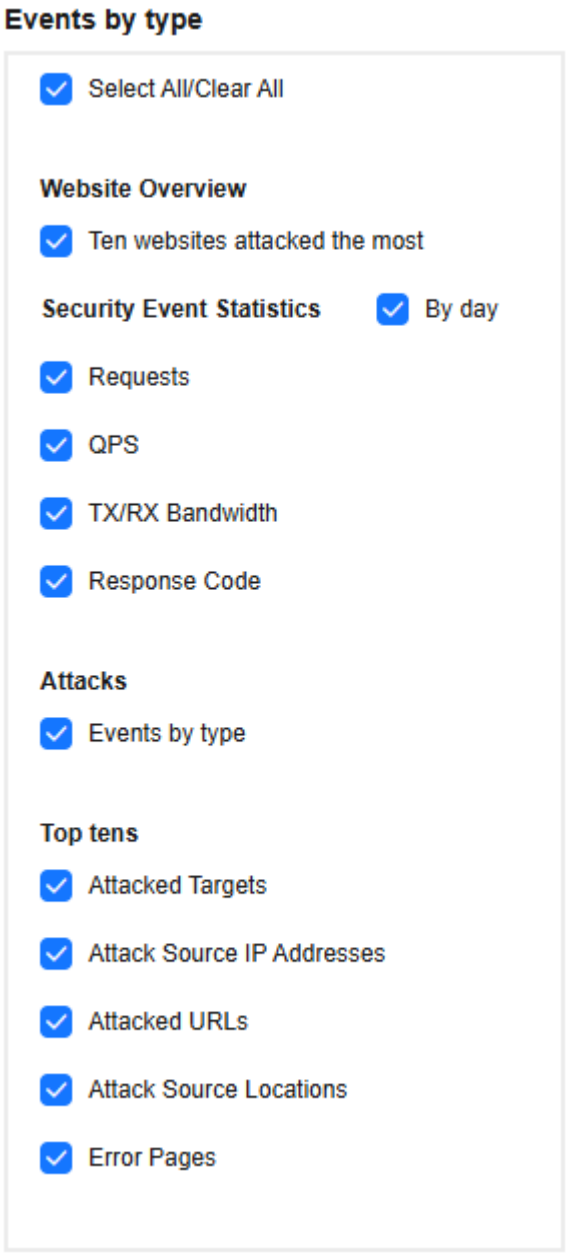
Parameter	Description	Example Value
Report Data Source	Enterprise projects the current report covers.	All projects
Report Template Name	Name of the custom security report template.	WAF
Report Enterprise Project	Enterprise project the report you are creating belongs to.	default

Parameter	Description	Example Value
Report Data Source	Enterprise project scope of the security report. You can select all projects or the project that the current report belongs to.	default
Report Template Name	Name of the custom security report template.	WAF
Report Type	• Daily Statistical period: 00:00:00 to 23:59:59 every day A report will be sent to the recipients the day after it is generated. • Weekly Statistical period: 00:00:00 on Monday to 23:59:59 on Sunday A report will be sent to the recipients the next Monday after it is generated. • Monthly Statistical period: 00:00:00 on the first day of each month to 23:59:59 on the last day of that month A report will be sent to the recipients on the first day of the month after it is generated. • Custom If you select **Custom**, configure **Statistical Period**. The system can collect statistics on security reports of the last 30 days at most.	Weekly
Send Report	Set the time range for sending daily reports. • Daily, weekly, and monthly reports: WAF sends protection log reports to recipients every day, every Monday, and on the first day of each month, respectively. • **Custom**: The report will be sent after it is generated.	18:00~24:00

Parameter	Description	Example Value
Send Report To	You can enable either of the following ways, or both, to receive security reports: • **Message Center**: Click  in the upper right corner of the page to access the message center and add recipient information. • **SMN Topic**: Select a topic from the drop-down list or click **Create SMN Topic** to create one and configure recipients. • **Do not send reports to the email address**: Reports will not be sent to the specified email address.	SMN Topic

Step 6 Click **Next: Set Report Content** and select the content you want the report to include.

Figure 9-2 Select Report Content



Step 7 Click **Save Report**.

----End

Downloading a Report

WAF stores security reports for six months only. You are advised to regularly download reports to meet compliance and audit requirements.

Step 1 **Log in to the management console**.

Step 2 Click in the upper left corner and select a region or project.

Step 3 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by**

enterprise project drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 4 In the navigation pane on the left, click **Reports**.

Step 5 In the row containing the desired report template, click **Download New Report** in the **Operation** column.

----End

Related Operations

- By default, report templates are enabled once they are created. To disable a report template, locate the row containing the report template you want to disable and choose **More** > **Disable** in the **Operation** column.
- To delete a report template, locate the row containing the report template you want to delete and choose **More** > **Delete** in the **Operation** column.
- To copy a report template, locate the row containing the report template you want to copy and choose **More** > **Copy** in the **Operation** column.
- To edit a report template, locate the row containing the report template you want to edit and choose **More** > **Edit** in the **Operation** column.

10 Object Management

10.1 Certificate Management

10.1.1 Uploading a Certificate to WAF

If you select **Cloud Mode - CNAME** or **Dedicated Mode** as the access mode and set **Client Protocol** to **HTTPS**, a certificate is required for your website.

If you upload a certificate to WAF, you can directly select the certificate when adding a website to WAF.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select your enterprise project from the **Enterprise Project** drop-down list and upload certificates in the project.

Prerequisites

You have obtained the certificate file and certificate private key.

Specification Limitations

You can upload as many certificates in WAF as the number of domain names that can be protected by your WAF instances in the same account. For example, if you purchase a standard edition WAF instance, which can protect 10 domain names, and a domain name expansion package, which can protect 20 domain names, your WAF instance can protect 30 domain names total. In this case, you can upload 30 certificates.

Constraints

- If you purchase a certificate on the SCM console and push it to WAF, the certificate is added to the certificate list on the **Certificates** page on the WAF console. This certificate is also counted towards your total certificate quota. For details about how to push an SSL certificate in SCM to WAF, see **Pushing an SSL Certificate to Other Cloud Services**.

NOTICE

Currently, certificates purchased in Huawei Cloud SCM can be pushed only to the **default** enterprise project. For other enterprise projects, SSL certificates pushed by SCM cannot be used.

- If you import a new certificate when adding a protected website or updating a certificate, the certificate is added to the certificate list on the **Certificates** page, and the imported certificate is also counted towards your total certificate quota.

Application Scenario

If you select **HTTPS** for **Client Protocol**, a certificate is required.

Uploading a Certificate to WAF

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

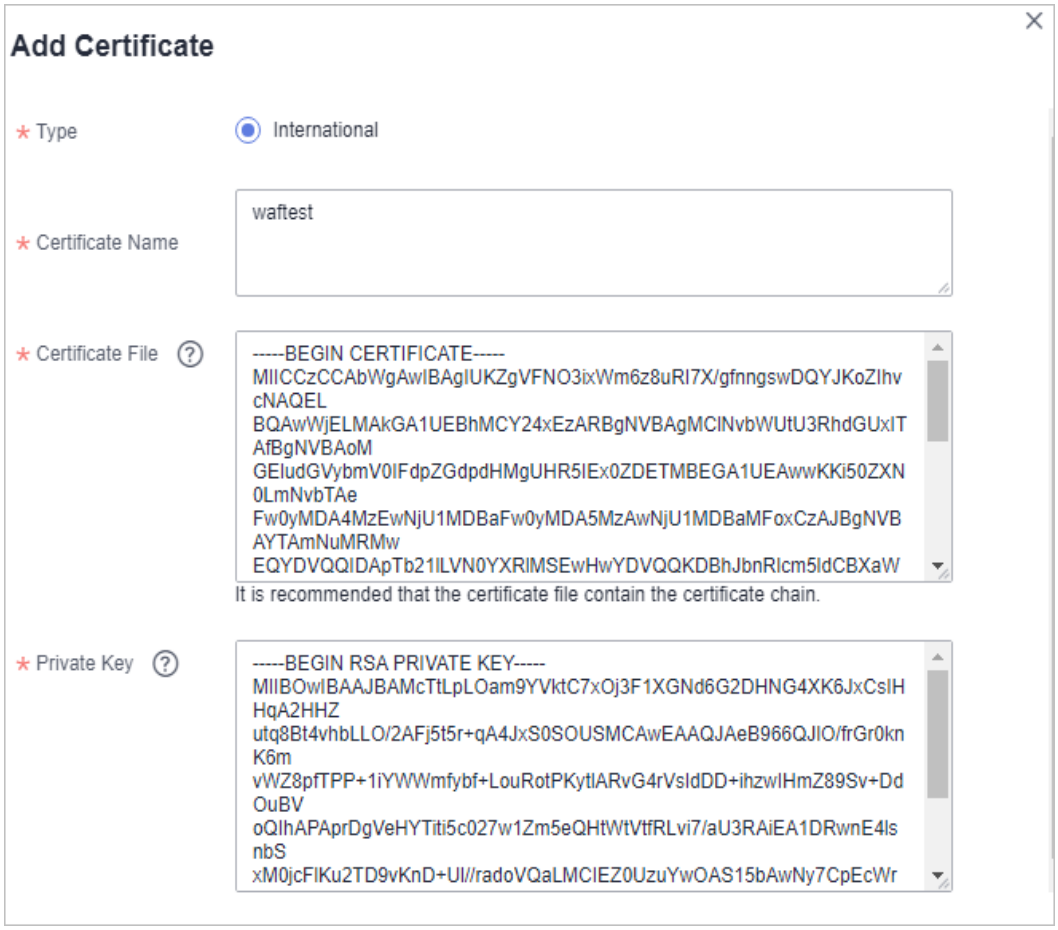
Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Objects** > **Certificates**.

Step 6 Click **Add Certificate**.

Step 7 In the displayed dialog box, enter a certificate name, and copy and paste the certificate file and private key to the corresponding text boxes.

Figure 10-1 Uploading an international certificate



Only .pem certificates can be used in WAF. If the certificate is not in .pem format, convert it into .pem locally by referring to **Table 10-1** before uploading it.

Table 10-1 Certificate conversion commands

Format	Conversion Method
CER/CRT	Rename the **cert.crt** certificate file to **cert.pem**.
PFX	• Obtain a private key. For example, run the following command to convert **cert.pfx** into **key.pem**: **openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes** • Obtain a certificate. For example, run the following command to convert **cert.pfx** into **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. Convert a certificate. For example, run the following command to convert **cert.p7b** into **cert.cer**: **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. Rename certificate file **cert.cer** to **cert.pem**.

Format	Conversion Method
DER	• Obtain a private key. For example, run the following command to convert **privatekey.der** into **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** • Obtain a certificate. For example, run the following command to convert **cert.cer** into **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTE

- Before running an OpenSSL command, ensure that the **OpenSSL** tool has been installed on the local host.
- If your local PC runs a Windows operating system, go to the command line interface (CLI) and then run the certificate conversion command.

Step 8 Click **OK**.

You can then view the uploaded certificate in the certificate list. The certificate you add will also be synchronized to the drop-down list of existing certificates for you to configure or modify website certificates through the **Website Settings** page.

----End

Related Operations

- To change the certificate name, move the cursor over the name of the certificate, click  , and enter a certificate name.

  NOTICE

  If the certificate is in use, unbind the certificate from the domain name first. Otherwise, the certificate name cannot be changed.

- To view details about a certificate, click **View** in the **Operation** column of the certificate.
- In the row containing the certificate you want, click **Use** in the **Operation** column to use the certificate to the corresponding domain name.
- To delete a certificate, locate the row of the certificate and click **More** > **Delete** in the **Operation** column.
- To update a certificate, locate the row of the certificate and click **More** > **Update** in the **Operation** column.
- To share a certificate with other enterprise projects, locate the row containing the certificate and click **More** > **Share** in the **Operation** column.
- To stop sharing a certificate with other enterprise projects, locate the row containing the certificate and click **More** > **Stop Sharing** in the **Operation** column.

FAQs

- How Do I Fix an Incomplete Certificate Chain?
- How Do I Fix a Certificate and Key Mismatch?
- Why Are HTTPS Requests Denied on Some Mobile Phones?
- What Do I Do If the Protocol Is Not Supported and the Client and Server Do Not Support Common SSL Protocol Versions or Cipher Suites?
- Why Is the Bar Mitzvah Attack on SSL/TLS Detected?

10.1.2 Using a Certificate for a Protected Website in WAF

If you configure **Client Protocol** to **HTTPS** for your website, the website needs an SSL certificate. This topic describes how to bind an SSL certificate that you have uploaded to WAF to a website.

NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and bind certificates to websites in the project.

Prerequisites

- Your certificate is still valid.
- Your website uses HTTPS as the client protocol.

Constraints

- An SSL certificate can be used for multiple protected websites.
- A protected website can use only one SSL certificate.

Application Scenario

If you configure **Client Protocol** to **HTTPS**, a certificate is required.

Using a Certificate for a Protected Website in WAF

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Objects** > **Certificates**.

Step 6 In the row containing the certificate you want to use, click **Use** in the **Operation** column.

Step 7 In the displayed **Domain Name** dialog box, select the website you want to use the certificate to.

Step 8 Click **OK**.

----End

Verification

The protected website is listed in the **Domain Name** column of the certificate.

Related Operations

- To change the certificate name, move the cursor over the name of the certificate, click  , and enter a certificate name.

  NOTICE

  If the certificate is in use, unbind the certificate from the domain name first. Otherwise, the certificate name cannot be changed.

- To view details about a certificate, click **View** in the **Operation** column of the certificate.
- To delete a certificate, locate the row of the certificate and click **More** > **Delete** in the **Operation** column.
- To update a certificate, locate the row of the certificate and click **More** > **Update** in the **Operation** column.
- To share a certificate with other enterprise projects, locate the row containing the certificate and click **More** > **Share** in the **Operation** column.
- To stop sharing a certificate with other enterprise projects, locate the row containing the certificate and click **More** > **Stop Sharing** in the **Operation** column.

10.1.3 Viewing Certificate Information

This topic describes how to view certificate details, including the certificate name, domain name a certificate is used for, and expiration time.

NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and view certificates in the project.

Prerequisites

You have obtained certificates from Huawei Cloud CCM, or **uploaded certificates** to WAF.

Constraints

- To receive certificate expiration notifications, you need to configure certificate expiration notifications on the **Instance Management** > **Notifications** page.
- If you update or import a certificate when adding a website to WAF, the **Certificate Source** column for this type of certificate is **SCM**. For those

certificates, only **Use** and **Delete** buttons are available in the **Operation** column.

Checking Certificate Details

Step 1 **Log in to the management console**.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Objects** > **Certificates**.

Step 6 View the certificate information. For details about related parameters, see **Table 10-2**.

Figure 10-2 Certificate list

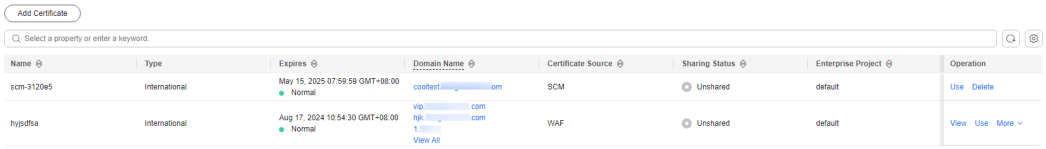


Table 10-2 Certificate parameters

Parameter	Description
Name	Certificate name.
Type	**International** certificates are supported.
Expires	Certificate expiration time. It is recommended that you update the certificate before it expires. Otherwise, all WAF protection rules will be unable to take effect, and there can be massive impacts on the origin server, even more severe than a crashed host or website access failures. For more details, see **Updating the Certificate Used for a Website**.
Domain Name	The domain names protected by the certificate. Each domain name must be bound to a certificate. One certificate can be used for multiple domain names.

Parameter	Description
Certificate Source	• **WAF**: The certificate is added to the WAF console. • **SCM**: Certificates WAF obtained when you import or update certificates during website connection. You can only **Use** and **Delete** this type of certificate in WAF.
Enterprise Project	The enterprise project that the certificate belongs to.
Sharing Status	Whether the certificate is shared with other enterprise projects. • Shared • Unshared

----End

Related Operations

- To change the certificate name, move the cursor over the name of the certificate, click  , and enter a certificate name.

  NOTICE

  If the certificate is in use, unbind the certificate from the domain name first. Otherwise, the certificate name cannot be changed.

- To view details about a certificate, click **View** in the **Operation** column of the certificate.
- In the row containing the certificate you want, click **Use** in the **Operation** column to use the certificate to the corresponding domain name.
- To delete a certificate, locate the row of the certificate and click **More** > **Delete** in the **Operation** column.
- To update a certificate, locate the row of the certificate and click **More** > **Update** in the **Operation** column.
- To share a certificate with other enterprise projects, locate the row containing the certificate and click **More** > **Share** in the **Operation** column.
- To stop sharing a certificate with other enterprise projects, locate the row containing the certificate and click **More** > **Stop Sharing** in the **Operation** column.

10.1.4 Sharing a Certificate with Other Enterprise Projects

This topic walks you through how to share a certificate with other enterprise projects.

NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and view certificates in the project.

Prerequisites

You have **uploaded a certificate** on the WAF console.

Constraints

SSL certificates pushed by CCM to WAF cannot be shared within an enterprise project.

Sharing a Certificate with Other Enterprise Projects

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Objects** > **Certificates**.

Step 6 In the row containing the certificate you want to share, click **More** > **Share** in the **Operation** column.

Step 7 In the displayed dialog box, select a handling method, and click **OK**.

----End

Related Operations

- To change the certificate name, move the cursor over the name of the certificate, click  , and enter a certificate name.

  NOTICE

  If the certificate is in use, unbind the certificate from the domain name first. Otherwise, the certificate name cannot be changed.

- To view details about a certificate, click **View** in the **Operation** column of the certificate.
- In the row containing the certificate you want, click **Use** in the **Operation** column to use the certificate to the corresponding domain name.
- To delete a certificate, locate the row of the certificate and click **More** > **Delete** in the **Operation** column.

- To update a certificate, locate the row of the certificate and click **More** > **Update** in the **Operation** column.
- To stop sharing a certificate with other enterprise projects, locate the row containing the certificate and click **More** > **Stop Sharing** in the **Operation** column.

10.1.5 Deleting a Certificate from WAF

This topic describes how to delete an expired or invalid certificate.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select the project from the **Enterprise Project** drop-down list and delete a certificate.

Prerequisites

The certificate you want to delete is not bound to a protected website.

Constraints

If a certificate to be deleted is bound to a website, unbind it from the website before deletion.

Impact on the System

- Deleting certificates does not affect services.
- Deleted certificates cannot be recovered. Exercise caution when performing this operation.

Deleting a Certificate from WAF

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Objects** > **Certificates**.

Step 6 In the row of the certificate, click **More** > **Delete** in the **Operation** column.

Step 7 In the displayed dialog box, click **OK**.

----End

Related Operations

If a certificate to be deleted is bound to a website, unbind it from the website before deletion.

To unbind a certificate from a website domain name, perform the following steps:

Step 1 In the **Domain Name** column of the row containing the desired certificate, click the domain name to go to the basic information page.

Step 2 Click  next to the certificate name. In the displayed dialog box, upload a new certificate or select an existing certificate.

----End

10.2 Managing IP Address Blacklist and Whitelist Groups

10.2.1 Adding an IP Address Group

With IP address groups, you can quickly add IP addresses or IP address ranges to a blacklist or whitelist rule.

NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and add IP address/range groups in the project.

Prerequisites

You have purchased WAF.

Constraints

- For dedicated and cloud load balancer WAF instances, if the load balancers they use support IPv6 addresses, those WAF instances also support IPv6 addresses and IPv6 address ranges.
- Before adding an address group to a blacklist or whitelist rule, make sure that your IP address blacklist and whitelist rule quota has not been used up.

  NOTE

  - For details, see **Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses**.

    For details about specifications, see **Edition Differences**.
  - If the quota for IP address whitelist and blacklist rules of your cloud WAF cannot meet your requirements, you can purchase rule expansion packages under the current WAF instance edition or upgrade your WAF instance edition to increase such quota. A rule expansion package allows you to configure up to 10 IP address blacklist and whitelist rules.

    For details, see **Upgrading Cloud WAF Edition and Specifications**

Adding a Blacklist or Whitelist IP Address Group

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Objects** > **Address Groups**.

Step 6 Click the **My Address Groups** tab.

Step 7 On the upper left of the address group list, click **Add Address Group**.

Step 8 On the **Add Address Group** panel displayed, complete the following configurations.

Table 10-3 Address group parameters

Parameter	Description	Example Value
Group Name	Enter the name of the address group. An address group name can contain a maximum of 128 characters. Only letters, digits, underscores (_), hyphens (-), colons (:), and periods (.) are allowed.	waf

Parameter	Description	Example Value
IP Address/ Range	Enter the IP addresses or IP address ranges you want to add. • Adding many IP addresses all at once 1. In the **IP Address/Range** configuration area, enter the IP addresses or IP address ranges you want to add and click **Add to List**. You can use commas (,), semicolons (;), carriage returns (Enter), tab characters (Tab), or spaces to separate IP addresses or IP address ranges. IPv4 and IPv6 addresses are supported. ▪ For dedicated and cloud load balancer WAF instances, if the load balancers they use support IPv6 addresses, the corresponding WAF instances also support IPv6 addresses and IPv6 address ranges. 2. In the IP address or IP address range list, check the IP address or IP address range information and enter the description. • Adding IP addresses one by one Above the IP address or IP address range list, click **Add** and enter an IP address and description. You can enter IPv4 and IPv6 addresses.	• IPv4 format: – 192.168.2.3 – 10.1.1.0/24 • IPv6 format: – fe80:0000:0000:0000:0000:0000:0000:0000 – ::/0

Step 9 Click **OK**.

After the above configuration is complete, you can view the added address group in the address group list. The address group you add will also be synchronized to the address group list on the **Policies** > **Blacklist and Whitelist** page.

----End

10.2.2 Modifying or Deleting a Blacklist or Whitelist IP Address Group

This topic describes how to modify or delete an IP address group.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select the project from the **Enterprise Project** drop-down list and modify or delete an IP address group.

Constraints

Only address groups not used by any rules can be deleted. Before you delete an address group that is being used by a blacklist or whitelist rule, remove the address group from the rule first.

Modifying or Deleting a Blacklist or Whitelist IP Address Group

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Objects** > **Address Groups**.

Step 6 Click the **My Address Groups** tab.

Step 7 In the address group list, view the address group information.

Table 10-4 Parameter description

Parameter	Description
Group Name	Address group name you configured. You can click  next to an address group name to modify the address group name.
IP Addresses/ Ranges	The number of IP addresses or IP address ranges added to the address group.
Rule	Rules that are using the address group.
Description	Supplementary information about the address group.

Step 8 Modify or delete an IP address group.

- Modify an IP address or IP address range.

  In the row containing the address group you want to modify, click **Change IP Address/Range** in the **Operation** column. In the dialog box displayed, add a new IP address/range and click **Confirm**. You can also click **Delete** to remove an IP address or IP address range.

- Modify an address group.

  In the row containing the address group you want to modify, click **Modify Address Group** in the **Operation** column. On the **Address Group Details** panel displayed, you can modify the address group name and description, add an IP address or IP address range, modify the IP address or IP address range description, or delete an IP address or IP address range.

- Delete an address group.

  In the row containing the address group you want to delete, click **Delete** in the **Operation** column. In the displayed dialog box, click **OK**.

----End

11 Instance Management

11.1 Managing Dedicated WAF Engines

This topic describes how to manage your dedicated WAF instances (or engines). You can view instance information, view instance monitoring configurations, upgrade the edition of an instance, and delete an instance.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instances locate. Then, you can select the project from the **Enterprise Project** drop-down list and manage dedicated WAF instances in the project.

Prerequisites

- **You have purchased a dedicated WAF instance.**
- Your login account has the **IAM ReadOnly** permission.

Dedicated Engine Version Iteration

You can view the WAF instance version in the **Version** column of the dedicated WAF instance list.

Table 11-1 Dedicated WAF versions

Engine Version	Feature
202502 **NOTE** If you want to upgrade your instances to this version, **submit a service ticket** for consultation.	• Custom headers can be used as trace IDs. • Counting requests to all WAF instances is supported in CC attack protection rules. You need to **submit a service ticket** to enable this function. • Advanced JS challenge is supported. • Known issues have been fixed.

Engine Version	Feature
202412	• IPv6 addresses are supported for geolocation access control rules. • WAF supports in-house bot mitigation. • Custom response headers can be forwarded. • Known issues have been fixed.
202410	• Customizable response headers on the custom block pages • Obtaining and processing the TOA field
202408	Known issues have been fixed.
202407	• In-depth decoding supported in precise protection rules • Known issues have been fixed.
202405	• The **health-check** API is supported. • Cookies can be checked for invalid characters. • The **Protective Action** in CC attack protection rules can be set to **JS Challenge**. • **Known feature crawler** can be set in the condition list of precise protection rules. • When and how to execute a precise rule can be set in the **Apply** parameter. • Requests for only error response codes *4xx* and *5xx* can be logged. Function parameter: **upstream.extend.only_log_abnormal_status**. • In dedicated mode, the default values of **X-Real-IP** and **X-Hwwaf-Real-IP** are returned from **$client_ip** instead of **$remote_addr**.
202312	• A global protection whitelist rule can be set to **ignore invalid requests**. • JavaScript-based anti-crawler rules support more protective actions, including **Block**, **Log only**, and **Verification code**.
202308	• The **$remote_addr** field is added to the IP identifier, which can be directly set to the IP address of the TCP connection. • IP addresses used in TCP connections can be identified by CC, precise protection, blacklist, and whitelist rules. • A block duration can be set if **Protective Action** is set to **Verification code** in a CC attack protection rule.

Engine Version	Feature
202305	• HTTP2 is enabled globally by default. There is no need to enable it manually. • By default, a request can pass through WAF four times before it goes to the origin server. Error code 523 will be returned if the request exceeds this limit. • Strict multipart format verification is supported. • Dedicated ELB network load balancers are supported. (In earlier versions, only shared load balancers and dedicated application load balancers are supported.)
202211	• Built-in tags can be added to attack logs (hit_data) when built-in rules are hit. • Destination rate limiting and response code conditions can be configured in CC attack protection rules.
202209	• TLS v1.3 is supported. • Protection for on-premises web servers is supported. • More types of statistics are added to heartbeat logs for attacks. • HTTPS ports 60700 to 60999 (300 ports) are added to the protection port list.
202207	• The wildcard domain name matching logic is supported. • The global protection whitelist is supported.
202205	Configuring the earliest TLS version based on instances is supported.
202204	• Rules can be updated and delivered from the management plane. • False alarm masking rules can work for all domain names and specified domain names. • All conditions can be configured for false alarm masking.
202202	The request logging methods are optimized.
202201	Some regular expression matching rules are optimized.
202111	• The log only mode is supported for information leakage rules. • Attack logs of invalid requests are added. • Precise protection rules can work to each IP address (only for IPv4 format) in the XFF request header. • Timeout duration can be set for specified domain names. • Some functions are optimized.

Engine Version	Feature
202110	The performance of some functions is improved.
202109	• Precise protection rules can work to the **request body** field. • Precise protection rules support regular expression matching and all subfields. • Some logs can be interconnected with LTS.
202106	• The HTTPS port supports HTTP/2. • The **region ID** field is added to access logs. • The **region ID** field and engine IP address are added to attack logs.

Viewing Information About a Dedicated WAF Instance

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine**.

Step 6 On the **Dedicated Engine** page, view the details about dedicated engine instances. Table 11-2 shows an example.

Figure 11-1 Dedicated engine list

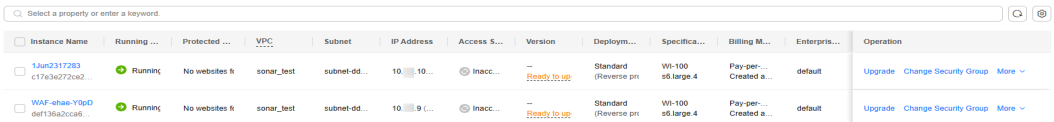


Table 11-2 Key parameters of dedicated WAF instances

Parameter	Description	Example Value
Instance Name	Name automatically generated when an instance is created.	None
Protected Website	Domain name of the website protected by the instance.	www.example.com

Parameter	Description	Example Value
VPC	VPC where the instance resides	vpc-waf
Subnet	Subnet where an instance resides	subnet-62bb
IP Address	IP address of the subnet in the VPC where the WAF instance is deployed.	192.168.0.186
Access Status	Connection status of the instance.	Accessible
Running Status	Status of the instance.	Running
Version	Dedicated WAF version.	202304
Deployment	How the instance is deployed.	Standard mode (reverse proxy)
Specifications	Specifications of resources hosting the instance.	WI-500 (specifications of dedicated engine instances) x1.8u.32g (Specifications of the ECS housing the dedicated engine. Specifications: x86: 8 vCPUs | 32 GB)

----End

Viewing Metrics of a Dedicated WAF Instance

When a WAF instance is in the **Running** status, you can view the monitored metrics about the instance.

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine**.

Step 6 In the row of the instance, click **Cloud Eye** in the **Operation** column to go to the Cloud Eye console and view the monitoring information, such as CPU, memory, and bandwidth.

----End

Updating the Specifications for a Dedicated Engine

The specifications of ECSs housing dedicated WAF instances have been updated. Before upgrading a dedicated WAF instance version, check the ECS specifications for the instance. If the specifications are not the latest, the dedicated instance may fail to be upgraded. You need to buy a new dedicated WAF instance with updated ECS specifications first.

NOTICE

- Dedicated WAF instances are billed on a pay-per-use basis. This is a postpaid mode. So, if the instance specifications and quantity of the new dedicated engine are consistent with the original one, there are no price changes.
- After buying new dedicated WAF instances, you need to connect your website to WAF again.

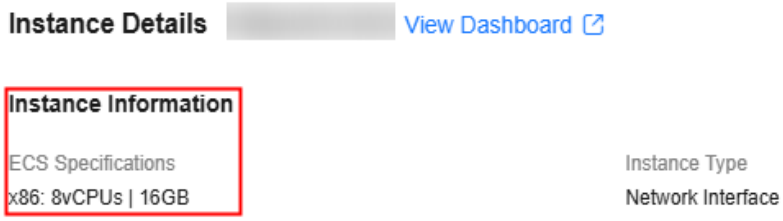
Specifications of ECSs housing dedicated WAF instances

Table 11-3 Specifications description

Instance Specification	Original ECS Specification	New ECS Specification
WI-100	2 vCPUs | 4 GB	2 vCPUs | 8 GB
WI-500	8 vCPUs | 16 GB	8 vCPUs | 32 GB

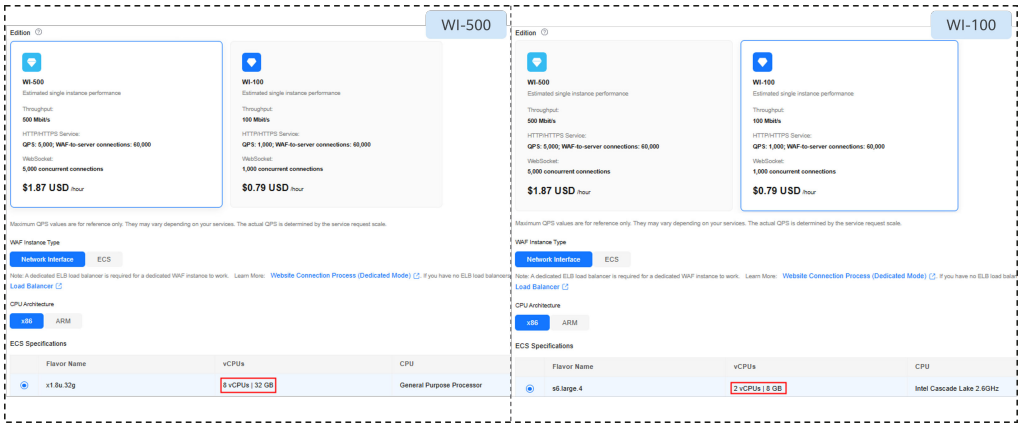
Step 1 On the **Dedicated Engine** page, click the target instance name to view the ECS specifications for the instance. If the ECS specifications are not updated, perform the following steps. To check instance details, see **Viewing Information About a Dedicated WAF Instance**.

Figure 11-2 ECS Specifications



Step 2 **Buy a dedicated WAF instance** based on the current specifications. Ensure that the ECS specifications for the new dedicated WAF instance have been updated.

Figure 11-3 vCPUs of the dedicated engine



Step 3 **Configure a load balancer for your dedicated WAF instance**.

1. Check **ELB (Load Balancer)**, **ELB Listener**, and **Backend Server Group** of the load balancer configured for the old dedicated WAF instance. For details, see **Managing Listeners**.
2. Add the new dedicated engine to the ELB load balancer. For details, see **Step 5**.

Step 4 **Test your dedicated WAF instance**.

NOTE

If you have multiple dedicated engines, repeat **Step 1** to **Step 4** to buy new dedicated engines and connect services to WAF.

Step 5 **Delete old dedicated WAF instances.**

----End

Upgrading a Dedicated WAF Instance

Only dedicated WAF instances in the **Running** status can be upgraded to the latest version.

Before the upgrade, check the ECS specifications of the dedicated WAF instance you want to upgrade. If the specifications are not the latest, the dedicated instance may fail to be upgraded. You need to buy a new dedicated WAF instance with updated ECS specifications first. For details, see **Updating the Specifications for a Dedicated Engine**.

Select an upgrade method based on the number of dedicated WAF instances you have.

Upgrading a Dedicated WAF Instance

If you have deployed only one dedicated WAF instance for your workloads, take the following steps to complete the upgrade:

Step 1 Apply for another dedicated WAF instance.

- The new dedicated WAF instance is of the latest version. So its **Upgrade** button is grayed out.

- The VPC, subnet, security group, and other settings of the new instance must be the same as those of the original one. In this way, the new instance automatically synchronizes all WAF protection configurations of the original instance.

Step 2 Run the curl command on any ECS in the VPC the original dedicated WAF instance locates to check whether the workloads are normal.

- HTTP workloads

  curl http://*IP-address-of-the-dedicated-WAF-instance*:*Service-port* **-H "host:***Service-domain-name***" -H "User-Agent: Test"**

- HTTPS workloads

  curl https://*IP-address-of-the-dedicated-WAF-instance*:*Service-port* **-H "host:***Service-domain-name***" -H "User-Agent: Test"**

Check whether the service is normal. If the service is normal, go to **Step 3**. If the service is abnormal, rectify the fault. After the fault is fixed, go to **Step 3**. For details about fault rectification, see **Why Is the Access Status of a Domain Name or IP Address Inaccessible?** and **How Do I Troubleshoot 404/502/504 Errors?**

NOTE

To run a curl command, your server must meet the following requirements:

- The network communication is normal.
- A curl command line tool has been installed. **curl** must be manually installed on the host running the Windows operating system. **curl** is installed along with other operating systems.

Step 3 Add the new dedicated WAF instance to the backend server group of the ELB load balancer you are using.

The following uses a shared load balancer to show how to add an instance to a backend server group.

1. Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.
2. In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.
3. In the row containing the instance you want to upgrade, click **More** > **Add to ELB** in the **Operation** column.

   NOTE

   You can also select multiple dedicated instances and click **Upgrade** in the upper left corner above the list to upgrade them all at once.
4. In the **Add to ELB** dialog box, specify **ELB (Load Balancer)**, **ELB Listener**, and **Backend Server Group** you configure for the original dedicated instance.
5. Click **OK**. Then, configure service port for the WAF instance. In this example, configure **Backend Port** to the one we configured for the original dedicated instance.

Step 4 On the ELB console, set the weight of the original dedicated instance to **0**. For details, see **Changing Backend Server Weights**.

Requests are not forwarded to a backend server if its weight is set to 0.

Step 5 Delete the original dedicated WAF instance during off-peak hours.

You can **view metrics of the dedicated WAF instance on Cloud Eye**. If the number of new connections is small (for example, less than 5), your workloads have decreased.

1. In the navigation pane on the left on the WAF console, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.
2. In the row of the instance, click **More** > **Delete** in the **Operation** column.
3. Click **OK**.

   Resources on deleted instance are released and cannot be restored.

----End

Upgrading Multiple Dedicated WAF Instances

If you have deployed multiple dedicated WAF instances for your workloads, take the following steps to upgrade them:

Step 1 On the ELB console, obtain the weight of a dedicated instance and then change the weight to **0**. For details, see **Changing Backend Server Weights**.

Requests are not forwarded to a backend server if its weight is set to 0.

Step 2 Upgrade the dedicated WAF instance during off-peak hours.

You can **view metrics of the dedicated WAF instance on Cloud Eye**. If the number of new connections is small (for example, less than 5), your workloads have decreased.

1. In the navigation pane on the left on the WAF console, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.
2. In the row containing the instance you want to upgrade, click **Upgrade** in the **Operation** column.
3. Confirm the upgrade conditions and click **OK**.

   It takes about 5 minutes for the upgrade.

Step 3 Run the curl command on any ECS in the VPC the dedicated WAF instance locates to check whether the workloads are normal.

- HTTP workloads

  curl http://*IP-address-of-the-dedicated-WAF-instance***:***Service-port* **-H "host:***Service-domain-name***" -H "User-Agent: Test"**

- HTTPS workloads

  curl https://*IP-address-of-the-dedicated-WAF-instance***:***Service-port* **-H "host:***Service-domain-name***" -H "User-Agent: Test"**

Check whether the service is normal. If the service is normal, go to **Step 4**. If the service is abnormal, rectify the fault by referring to **Why Is the Access Status of a Domain Name or IP Address Inaccessible?** and **How Do I Troubleshoot 404/502/504 Errors?** After the fault is fixed, go to **Step 3**.

NOTE

To run a curl command, your server must meet the following requirements:

- The network communication is normal.
- A curl command line tool has been installed. **curl** must be manually installed on the host running the Windows operating system. **curl** is installed along with other operating systems.

Step 4 On the ELB console, change the weight of the dedicated instance from **0** to the one you obtain in **Step 1**. For details, see **Configuring Weights for Backend Servers**.

Step 5 Upgrade other dedicated WAF instances one by one by referring to **Step 1** to **Step 4**.

----End

Rolling Back a Dedicated WAF Instance

The version can be rolled back only to the original version.

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine**.

Step 6 In the row of the instance, click **More** > **Roll Back** in the **Operation** column.

Step 7 In the dialog box displayed, confirm that the following conditions are met and select the following three conditions. Then, click **OK**.

An instance can be rolled back only when the following conditions are met:

- Multiple active instances are available or no services are connected to the instance.
- ELB HTTP/HTTPS health check has been enabled.
- ELB sticky session has been disabled.

----End

Change Security Group for a Dedicated WAF Instance

If you select **Network Interface** for **Instance Type**, you can change the security group to which your dedicated instance belongs. After you select a security group, the WAF instance will be protected by the access rules of the security group.

Step 1 **Log in to the management console**.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine**.

Step 6 In the row containing the instance, choose **More** > **Change Security Group** in the **Operation** column.

Step 7 In the dialog box displayed, select the new security group and click **OK**.

----End

Deleting a Dedicated WAF Instance

You can delete a dedicated WAF instance at any time. After it is deleted, the billing ends.

NOTICE

Resources on deleted instance are released and cannot be restored. Exercise caution when performing this operation.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine**.

Step 6 In the row containing the instance, click **More** > **Delete** in the **Operation** column.

NOTE

You can also select multiple dedicated instances and click **Delete** in the upper left corner above the list to delete them all at once.

Step 7 In the displayed dialog box, enter **DELETE** and click **OK**.

----End

11.2 Viewing Product Details

On the **Product Details** page, you can view information about all your WAF instances, including the edition, domain quotas, and specifications.

NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and view products in the project.

Prerequisites

You have purchased WAF.

Viewing Product Details

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Instance Management** > **Product Details**.

Step 6 On the **Product Details** page, view the WAF edition you are using, specifications, and expiration time.

- To view details about the WAF edition you are using, click **Details**.
- To disable a cloud WAF instance billed on a pay-per-use basis, click **Disable Pay-Per-Use Billing** for it and finish operations as prompted.
- To renew a WAF instance, click **Renew** next to the instance.
- To change the edition and purchase an expansion package, in the cloud mode configuration area, click **Change Specifications**. Then, change whatever you want.
- To unsubscribe a resource, click **Unsubscribe** in the **Order Info** column.
- To release expired resources, click **Release** in the **Order Info** column. For more details, see **Releasing Resources**.

----End

11.3 Changing the Cloud WAF Edition and Specifications

You can change the edition of your cloud instance to a higher or lower edition. Beyond that, you can subscribe to more or unsubscribe from some domain name,

QPS, and rule expansion packages without changing the WAF edition you are using.

Prerequisites

- You have obtained management console login credentials for an account with the **WAF Administrator** and **BSS Administrator** permissions.
- **You have purchased a cloud WAF instance.**

Specification Limitations

- Changing specifications does not change the billing mode or expiration date.
- A domain name expansion package can protect a maximum of 10 domain names.
- The QPS limit and bandwidth limit of a QPS expansion package:
  - For web applications deployed on Huawei Cloud

    Service bandwidth: 50 Mbit/s

    QPS: 1,000 (Each HTTP GET request is a query.)
  - For web applications not deployed on Huawei Cloud

    Service bandwidth: 20 Mbit/s

    QPS: 1,000 (Each HTTP GET request is a query.)
- A rule expansion package allows you to configure up to 10 IP address blacklist and whitelist rules.

Constraints

- Specifications of an expired WAF instance cannot be changed. To do that, renew the WAF instance first.
- Changing WAF editions or specifications is not supported if you have used some functions of the WAF edition, or you have no extra domain name, QPS, or IP blacklist and whitelist rules to unsubscribe from.

Application Scenarios

- **Scenario 1**: If the current cloud WAF edition does not support some functions, or cannot meet your protection requirements for domain names, QPS, or IP address blacklist and whitelist rules, you can use this function to upgrade service specifications. For details about WAF editions, see **Edition Differences**.
- **Scenario 2**: If the WAF edition you are using has much more protection capabilities or domain name, QPS, and rule expansion packages than what you actually need, you can change the WAF edition to a lower one or unsubscribe from some packages.

Impact on the System

Changing a WAF edition or quantity of domain, QPS, or rule expansion packages has no impact on protected website services.

Changing the Cloud WAF Edition

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Instance Management** > **Product Details**.

Step 6 Click **Change Specifications**. The **Change WAF Specifications** page is displayed.

- To change WAF edition: In the **Edition** row, click **Change Edition** in the **Details** column. In the displayed **Change Edition** pane, select an edition and click **OK**.
- To change expansion packages: In the **Details** column of the **Domain Name Quota**, **QPS Quota**, and **Rule Quota** rows, increase or decrease the number of expansion packages, respectively.

  By default, the number of expansion packages cannot be reduced to 0. To do so, **submit a service ticket** and click **Unsubscribe**.
- Billing information: Changing specifications does not change the billing mode or expiration date.

Step 7 In the lower right corner of the page, click **Next**.

Step 8 Check the order details and read the *Web Application Firewall Disclaimer*. Then, select *I have read and agree to the WAF Disclaimer*, and click **Pay Now**.

Step 9 On the payment page, select a payment method and pay for your order or select a refund method to get your money refunded.

----End

Changing Expansion Package Specifications

You can change the quantity of domain name, QPS, or rule expansion packages.

Changing Domain Expansion Package Specifications

The following procedure describes how to increase or decrease the number of domain expansion packages.

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Instance Management** > **Product Details**.

Step 6 In the **Domain Expansion Package** column, click **Buy Expansion Package**.

Step 7 In the **Details** column, increase or decrease the number of the expansion packages.

Step 8 In the lower right corner of the page, click **Next**.

Step 9 Check the order details and read the *Web Application Firewall Disclaimer*. Then, select *I have read and agree to the WAF Disclaimer*, and click **Pay Now**.

Step 10 On the payment page, select a payment method and pay for your order or select a refund method to get your money refunded.

----End

Changing the QPS Expansion Package Quantity

The following procedure describes how to increase or decrease the number of QPS expansion packages.

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Instance Management** > **Product Details**.

Step 6 In the **QPS Expansion Package** column, click **Buy Expansion Package**.

Step 7 In the **Details** column, increase or decrease the number of the expansion packages.

Step 8 In the lower right corner of the page, click **Next**.

Step 9 Check the order details and read the *Web Application Firewall Disclaimer*. Then, select *I have read and agree to the WAF Disclaimer*, and click **Pay Now**.

Step 10 On the payment page, select a payment method and pay for your order or select a refund method to get your money refunded.

----End

Changing the Rule Expansion Package Quantity

The following procedure describes how to increase or decrease the number of rule expansion packages.

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Instance Management** > **Product Details**.

Step 6 In the **Rule Expansion Package** column, click **Buy Expansion Package**.

Step 7 In the **Details** column, increase or decrease the number of the expansion packages.

Step 8 In the lower right corner of the page, click **Next**.

Step 9 Check the order details and read the *Web Application Firewall Disclaimer*. Then, select *I have read and agree to the WAF Disclaimer*, and click **Pay Now**.

Step 10 On the payment page, select a payment method and pay for your order or select a refund method to get your money refunded.

----End

11.4 Enabling Alarm Notifications

This topic describes how to enable notifications for attack logs. Once this function is enabled, WAF sends you SMS or email notifications if an attack is detected.

You can configure certificate expiration reminders. When a certificate is about to expire, WAF notifies you by the way you configure, such as email or SMS.

NOTE

- Simple Message Notification (SMN) is a paid service. For details, see **Product Pricing Details**.
- Before setting alarm notifications, create a message topic in SMN.

Constraints

- Certificate notifications are available only for the **cloud mode CNAME** access mode of professional and enterprise editions and the **dedicated** access mode.
- This service depends on the Simple Message Notification (SMN) service. SMN is billed based on the actual usage. For details, see **SMN Pricing Details**.
- Alarm notifications are sent if the number of attacks reaches the threshold you configure.

- Only one alarm notification of the same type can be configured in an enterprise project.

Enabling Alarm Notifications

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Web Application Firewall** under **Security & Compliance**.

Step 4 (Optional) If you have enabled the enterprise project function, in the upper part of the navigation pane on the left, select your enterprise project from the **Filter by enterprise project** drop-down list. Then, WAF will display the related security data in the enterprise project on the page.

Step 5 In the navigation pane on the left, choose **Instance Management** > **Notifications**.

Step 6 In the navigation pane on the left, choose **Instance Management** > **Notifications**.

Step 7 Click **Create** and configure alarm notification parameters. Table 11-4 lists the parameters.

Figure 11-4 Create Notification

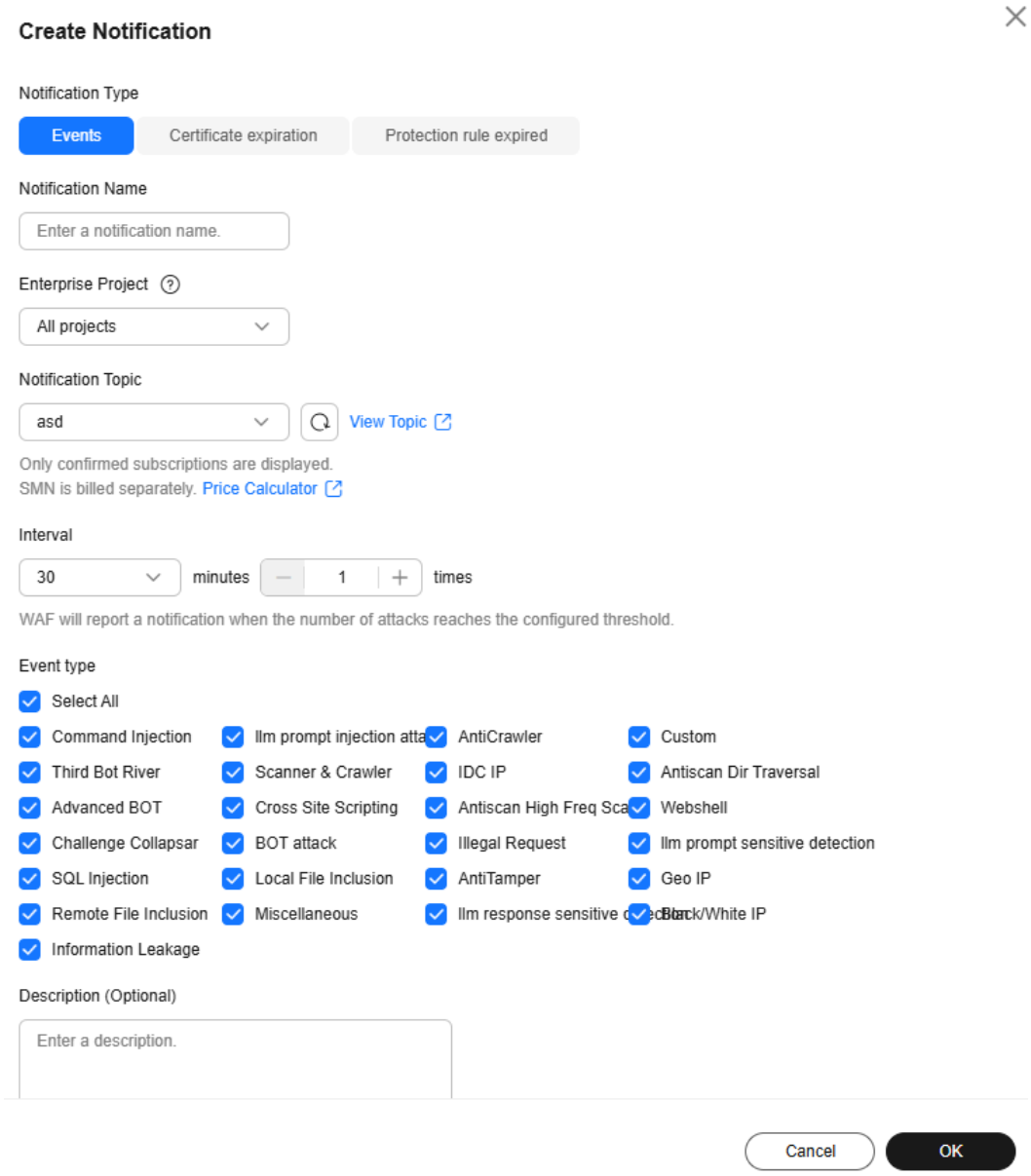


Table 11-4 Description of notification setting parameters

Parameter	Description
Notification Type	Select a notification type. • **Events**: WAF sends attack logs to you in the way you configure (such as SMS or email) once it detects log-only or blocked events. • **Certificate expiration**: When a certificate is about to expire, WAF notifies you by the way you configure, such as email or SMS. • **Protection rule expired**: When a protection rule is about to expire, WAF notifies you by the way you configure, such as email or SMS.

Parameter	Description
Notification Name	Name of the alarm notification.
Enterprise Project	Select an enterprise project from the drop-down list. The notification takes effect in the selected enterprise project.
Notification Topic	Select a topic from the drop-down list. If there are no topics, click **View Topic** and perform the following steps to create a topic: 1. Create a topic. For details, see **Creating a Topic**. 2. Add one or more subscriptions to the topic. You will need to provide a phone number, email address, function, platform application endpoint, DMS endpoint, or HTTP/HTTPS endpoint for receiving alarm notifications. For details, see **Adding a Subscription**. 3. Confirm the subscription. After the subscription is added, confirm the subscription. For details about topics and subscriptions, see the *Simple Message Notification User Guide*.
Protection Rules	If you select **Protection rule expired** for **Notification Type**, you need to select the protection rules for the notification. You can select CC attack protection, precise protection, and blacklist and whitelist rules.
Interval	If you select **Events** for **Notification Type**, **Interval** must be configured. **NOTE** Alarm notifications are sent if the number of attacks reaches the threshold configured for a certain period.
Event Type	If you select **Events** for **Notification Type**, **Event Type** must be configured. By default, **All** is selected. To specify event types, click **Custom**.
Notification Before Expiration	This parameter must be configured if you select **Certificate expiration** or **Protection rule expired** for **Notification Type**. Select how long before a certificate expire WAF can send notifications. You can select **1 week**, **1 month**, or **2 months**. For example, if you select **1 week**, WAF will send you an SMS message or email one week before the certificate expires.

Parameter	Description
Interval	This parameter must be configured if you select **Certificate expiration** or **Protection rule expired** for **Notification Type**. How often WAF sends certificate expiration notifications to you. You can select **Weekly** or **Daily**.
Description	(Optional) A description of the purposes of the alarm.

Step 8 Click **OK**.

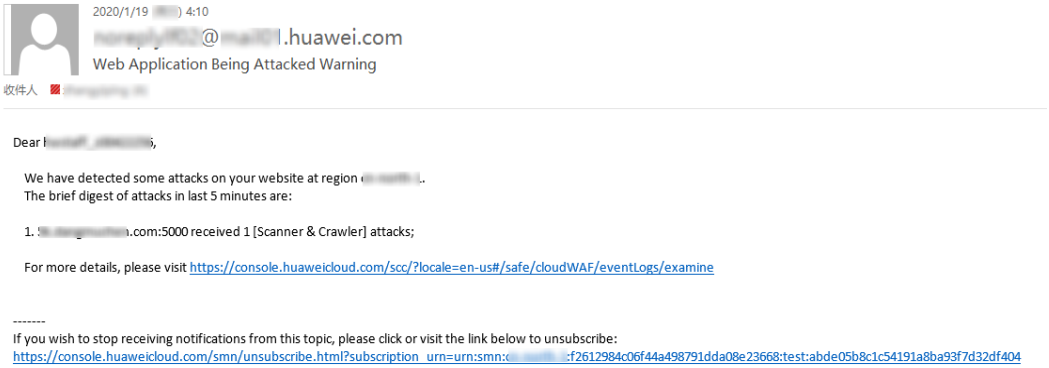
- To disable a notification, locate the row containing the notification and click **Disable** in the **Operation** column.
- To delete a notification, locate the row containing the notification and click **Delete** in the **Operation** column.
- To modify a notification, locate the row containing the notification and click **Modify** in the **Operation** column.

----End

Example Alarm Notification Email

If you have enabled alarm notifications and configured email alarm notifications, WAF emails you reports of any attacks that occur. **Figure 11-5** shows an alarm notification email.

Figure 11-5 Alarm notification email



12 Permissions Management

12.1 Authorizing and Associating an Enterprise Project

Huawei Cloud Enterprise Management service provides unified cloud resource management based on enterprise projects, and resource and personnel management within enterprise projects. Enterprise projects can be managed by one or more user groups. You can create WAF enterprise projects on the Enterprise Management console to manage your WAF resources centrally.

Creating an Enterprise Project and Assigning Permissions

- Creating an enterprise project

  On the management console, click **Enterprise** in the upper right corner to go to the **Enterprise Management** page. Click **Create Enterprise Project** and enter a name.

  NOTE

  Enterprise is available on the management console only if you have enabled the enterprise project, or you have an enterprise account. To use this function, enable it by referring to **Enabling the Enterprise Center**.

- Authorization

  You can add a user group to an enterprise project and configure a policy to associate the enterprise project with the user group. You can add users to a user group to control which projects they can access and what resources they can perform operations on. To do so, perform the following operations:

  a. On the **Enterprise Management** console, click the name of an enterprise project to go to the enterprise project details page.

  b. On the **Permissions** tab, click **Authorize User Group** to go to the **User Groups** page on the IAM console. Associate the enterprise project with a user group and assign permissions to the group. For details, see **Creating a User Group and Granting Permissions**.

- Associating the resource with enterprise projects

  To use an enterprise project to manage cloud resources, associate resources with the enterprise project.

- Associate a WAF instance with an enterprise project when purchasing WAF

  On the page for buying WAF, select an enterprise project from the **Enterprise Project** drop-down list.
- Add WAF instances to an enterprise project after a WAF instance is purchased.

  On the **Enterprise Project Management** page, add WAF instances you buy under your account to an enterprise project.

  Value **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are listed in the default enterprise project.

NOTICE

WAF instances billed on a pay-per-use basis cannot be added to enterprise projects.

For more information about enterprise project, see **Enterprise Management User Guide**.

12.2 IAM Permissions Management

12.2.1 WAF Custom Policies

If the system-defined policies of WAF cannot meet your needs, you can create custom policies.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**.

CAUTION

WAF does not support the **g:RequestedRegion** request condition key. Do not select this condition key when adding a request condition. Otherwise, the custom policy does not take effect.

If the WAF console displays a message indicating that you do not have the permission to perform an operation, check whether the **g:RequestedRegion** condition key has been added to the request condition. If yes, deselect **g:RequestedRegion** from the visual editor or delete **g:RequestedRegion** from the JSON editor.

For details about the actions supported by custom policies, see **WAF Permissions and Supported Actions**.

WAF Example Custom Policies

You can configure custom policies by referring to the following examples.

Example 1: Allowing Users to Query the Protected Domain List

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "waf:instance:list"
                                ]
        }
    ]
}
```

Example 2: Denying the user request of deleting web tamper protection rules

A deny policy must be used together with other policies. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

The following method can be used if you need to assign permissions of the **WAF FullAccess** policy to a user but also forbid the user from deleting web tamper protection rules (**waf:antiTamperRule:delete**). Create a custom policy with the action to delete web tamper protection rules, set its **Effect** to **Deny**, and assign both this policy and the **WAF FullAccess** policy to the group the user belongs to. Then the user can perform all operations on WAF except deleting web tamper protection rules. The following is a policy for denying web tamper protection rule deletion.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "waf:antiTamperRule:delete"
            ]
        },
    ]
}
```

Multi-Action Policies

A custom policy can contain the actions of multiple services that are of the project-level type. The following is an example policy containing actions of multiple services:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "waf:instance:get",
                "waf:certificate:get"
            ]
        },
```



```
        {
            "Effect": "Allow",
            "Action": [
                "hss:hosts:switchVersion",
                "hss:hosts:manualDetect",
                "hss:manualDetectStatus:get"
            ]
        }
    ]
}
```

12.2.2 WAF Permissions and Supported Actions

This topic describes fine-grained permissions management for your WAF instances. If your Huawei ID does not need individual IAM users, then you may skip over this section.

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign permissions policies to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

You can grant users permissions by using **roles** and **policies**. Roles are provided by IAM to define service-based permissions depending on user's job responsibilities. Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions.

Supported Actions

WAF provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control.

- Permission: A statement in a policy that allows or denies certain operations.
- Action: Specific operations that are allowed or denied.

Permission	Action	IAM Project	Enterprise Project
Querying the list of protected domain names	waf:host:list	√	√
Adding a domain name to WAF	waf:host:create	√	√
Querying a protected domain name	waf:host:get	√	√
Modifying a protected domain name	waf:host:put	√	√

Permission	Action	IAM Project	Enterprise Project
Deleting a protected domain from WAF	waf:host:delete	√	√
Querying an information leakage prevention rule	waf:antiLeakageRule:get	√	√
Querying a web tamper protection rule	waf:antiTamperRule:get	√	√
Querying a CC attack protection rule	waf:ccRule:get	√	√
Querying a precise protection rule	waf:preciseProtection-Rule:get	√	√
Querying a global protection whitelist rule	waf:falseAlarmMaskRule:get	√	√
Querying a data masking rule	waf:privacyRule:get	√	√
Querying a blacklist or whitelist rule	waf:whiteBlackIpRule:get	√	√
Querying a geolocation access control rule	waf:geoIpRule:get	√	√
Querying a certificate	waf:certificate:get	√	√
Modifying WAF certificates	waf:certificate:put	√	√
Applying a certificate to a domain name	waf:certificate:apply	√	√
Querying a protection event	waf:event:get	√	√
Querying a protected domain	waf:instance:get	√	√

Permission	Action	IAM Project	Enterprise Project
Querying a protection policy	waf:policy:get	√	√
Querying quota package information	waf:bundle:get	√	√
Querying the protection event download link	waf:dumpEventLink:get	√	√
Querying configurations	waf:consoleConfig:get	√	√
Querying the back-to-source IP address range	waf:sourceIp:get	√	√
Updating an information leakage prevention rule	waf:antiLeakageRule:put	√	√
Updating a web tamper protection rule	waf:antiTamperRule:put	√	√
Updating a CC attack protection rule	waf:ccRuleRule:put	√	√
Updating a precise protection rule	waf:preciseProtection-Rule:put	√	√
Updating a global protection whitelist rule	waf:falseAlarmMaskRule:put	√	√
Updating a data masking rule	waf:privacyRule:put	√	√
Updating an IP address blacklist or whitelist rule	waf:whiteBlackIpRule:put	√	√
Updating a geolocation access control rule	waf:geoIpRule:put	√	√
Updating a protected domain	waf:instance:put	√	√

Permission	Action	IAM Project	Enterprise Project
Updating a protection policy	waf:policy:put	√	√
Deleting an information leakage prevention rule	waf:antiLeakageRule:delete	√	√
Deleting a web tamper protection rule	waf:antiTamperRule:delete	√	√
Deleting a CC attack protection rule	waf:ccRule:delete	√	√
Configuring a precise protection rule	waf:preciseProtection-Rule:delete	√	√
Deleting a global protection whitelist rule	waf:falseAlarmMaskRule:delete	√	√
Deleting a data masking rule	waf:privacyRule:delete	√	√
Deleting a blacklist or whitelist rule	waf:whiteBlackIpRule:delete	√	√
Deleting a geolocation access control rule	waf:geoIpRule:delete	√	√
Deleting a protected domain from WAF	waf:instance:delete	√	√
Deleting a protection policy	waf:policy:delete	√	√
Adding an information leakage prevention rule	waf:antiLeakageRule:create	√	√
Adding a web tamper protection rule	waf:antiTamperRule:create	√	√

Permission	Action	IAM Project	Enterprise Project
Adding a CC attack protection rules	waf:ccRule:create	√	√
Adding a precise protection rule	waf:preciseProtection-Rule:create	√	√
Querying bot rules	waf:anticrawlerRule:list	√	√
Updating configuration of bot rules	waf:anticrawlerRule:put	√	√
Creating a global protection whitelist rule	waf:falseAlarmMaskRule:create	√	√
Adding a data masking rule	waf:privacyRule:create	√	√
Adding a blacklist or whitelist rule	waf:whiteBlackIpRule:create	√	√
Adding a geolocation access control rule	waf:geoIpRule:create	√	√
Adding a certificate	waf:certificate:create	√	√
Adding a domain	waf:instance:create	√	√
Adding a policy	waf:policy:create	√	x
Querying information leakage prevention rules	waf:antiLeakageRule:list	√	√
Querying web tamper protection rules	waf:antiTamperRule:list	√	√
Querying CC attack protection rules	waf:ccRuleRule:list	√	√
Querying precise protection rules	waf:preciseProtection-Rule:list	√	√

Permission	Action	IAM Project	Enterprise Project
Querying the global protection whitelist rule list	waf:falseAlarmMaskRule:list	√	√
Querying data masking rules	waf:privacyRule:list	√	√
Querying blacklist and whitelist rules	waf:whiteBlackIpRule:list	√	√
Querying geolocation access control rules	waf:geoIpRule:list	√	√
Querying the protection domains	waf:instance:list	√	√
Querying protection policies	waf:policy:list	√	√
Querying cloud-mode billing items	waf:subscription:get	√	√
Querying alarm notification configuration	waf:alert:get	√	√
Updating alarm notification configuration	waf:alert:put	√	√
Querying log quotas	waf:ltsConfig:get	√	√
Updating log quotas	waf:ltsConfig:put	√	√
Creating a yearly/monthly order for a cloud-mode instance	waf:prepaid:create	√	√
Enabling the pay-per-use billing for a WAF cloud-mode instance	waf:postpaid:create	√	√

Permission	Action	IAM Project	Enterprise Project
Disabling the pay-per-use billing for a WAF cloud-mode instance	waf:postpaid:delete	√	√
Viewing details of a WAF instance group	waf:pool:get	√	√
Modifying WAF instance group configuration	waf:pool:put	√	√
Creating a WAF instance group	waf:pool:create	√	√
Deleting a WAF instance group	waf:pool:delete	√	√
Viewing the WAF instance group list	waf:pool:list	√	√
Querying binding details of a WAF instance group	waf:poolBinding:get	√	√
Binding a WAF instance group	waf:poolBinding:create	√	√
Unbinding a WAF instance group	waf:poolBinding:delete	√	√
Querying binding details of a WAF instance group	waf:poolBinding:list	√	√
Querying health check configurations of a WAF instance group	waf:poolHealthMonitor:get	√	√
Modifying the health check configuration of a WAF instance group	waf:poolHealthMonitor:put	√	√

Permission	Action	IAM Project	Enterprise Project
Configuring health check for a WAF instance group	waf:poolHealthMonitor:create	√	√
Deleting health check configuration for a WAF instance group	waf:poolHealthMonitor:delete	√	√
Querying health check configurations for WAF instance groups	waf:poolHealthMonitor:list	√	√
Modifying a shared IP address group	waf:ipGroupShare:put	√	√
Batch updating known attack source rules	waf:punishmentRule:batch-delete	√	√
Querying DNS domain names	waf:dnsDomain:get	√	√
Querying IP address groups with the same names	waf:duplicateIpGroup:list	√	√

12.3 Permission Dependency of the WAF Console

When using WAF, you may need to view resources of or use other cloud services. So you need to obtain required permissions for dependent services so that you can view resources or use WAF functions on WAF Console. To that end, make sure you have the WAF FullAccess or WAF ReadOnlyAccess assigned first. For details, see **Creating a User Group and Granting Permissions**.

Dependency Policy Configuration

To grant an IAM user the permissions to view or use resources of other cloud services on the WAF console, you must first grant the WAF Administrator, WAF FullAccess, or WAF ReadOnlyAccess policy to the user group to which the user belongs and then grant the dependency policies listed in **Table 12-1** to the user. These dependency policies will allow the IAM user to access resources of other cloud services.

Table 12-1 WAF console dependency policies and roles

Console Function	Dependent Services	Policy/Role Required
Dashboard	Enterprise Project Management Service (EPS)	You can view the data on the Dashboard page of an enterprise project only after obtaining the EPS ReadOnlyAccess system policy.
Buying a WAF instance (for Dedicated Cloud)	Elastic Volume Service (EVS)	The EVS ReadOnlyAccess system policy is required to query EVS disks you have.
Dedicated WAF engine management	Network Console VPC Elastic IP (EIP) Elastic Load Balance (ELB)	• The VPC ReadOnlyAccess system policy is required to query VPCs you have. • The EIP ReadOnlyAccess system policy is required to query EIPs bound to dedicated WAF instance. • The ELB ReadOnlyAccess system policy is required to query information about ELB load balancers bound to dedicated WAF instance.
Adding a website to WAF (ELB mode)	Elastic Load Balance (ELB)	• The Elastic Load Balance (ELB) Administrator system role is required. You need to assign ELB administrator role together with the ELB FullAccess and ELB ReadOnlyAccess permissions to IAM users. You can read and modify ELB configuration information only after the preceding operations are complete.
Instance group management	Elastic Load Balance (ELB)	The ELB ReadOnlyAccess system policy is required to query load balancers used for a WAF instance group.
Adding a website to WAF (cloud and dedicated modes)	Cloud Certificate Manager (CCM)	The SCM ReadOnlyAccess system policy is required to query certificate details.
Editing server information	Cloud Certificate Manager (CCM)	
Website settings	Cloud Certificate Manager (CCM)	
Notifications	Simple Message Notification (SMN)	The SMN ReadOnlyAccess system policy is required to obtain SMN topic groups.

Console Function	Dependent Services	Policy/Role Required
Enabling LTS for WAF logging	Log Tank Service (LTS)	The LTS ReadOnlyAccess system policy is required to select log group and log stream names created in LTS.

13 Monitoring and Auditing

13.1 Using Cloud Eye to Monitor WAF

13.1.1 WAF Monitored Metrics

Function Description

This topic describes metrics reported by WAF to Cloud Eye as well as their namespaces and dimensions. You can use APIs provided by Cloud Eye to query the metrics of the monitored object and alarms generated for WAF. You can also query them on the Cloud Eye console.

namespaces

SYS.WAF

NOTE

A namespace is an abstract collection of resources and objects. Multiple namespaces can be created in a single cluster with the data isolated from each other. This enables namespaces to share the same cluster services without affecting each other.

Monitored Metrics for Protected Domain Names

Table 13-1 Monitored metrics for domain names protected with WAF

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
requests	Number of Requests	Number of requests returned by WAF in the last 5 minutes Collection method: The total number of requests for the domain name are collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes
waf_http_2xx	WAF Status Code (2XX)	Number of 2XX status codes returned by WAF in the last 5 minutes Collection method: Number of 2XX status codes returned	≥0 Value type: Float	Count	N/A	Protected domain dame	5
waf_http_3xx	WAF Status Code (3XX)	Number of 3XX status codes returned by WAF in the last 5 minutes Collection method: Number of 3XX status codes returned	≥0 Value type: Float	Count	N/A	Protected domain dame	5

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
waf_http_4xx	WAF Status Code (4XX)	Number of 4XX status codes returned by WAF in the last 5 minutes Collection method: Number of 4XX status codes returned	≥0 Value type: Float	Count	N/A	Protected domain dame	5
waf_http_5xx	WAF Status Code (5XX)	Number of 5XX status codes returned by WAF in the last 5 minutes Collection method: Number of 5XX status codes returned	≥0 Value type: Float	Count	N/A	Protected domain dame	5
waf_fused_counts	WAF Traffic Threshold	Number of requests destined for the website in the last 5 minutes during breakdown protection duration Collection method: Number of requests to the protected domain name while the website was down	≥0 Value type: Float	Count	N/A	Protected domain dame	5

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
inbound_traffic	Total Inbound Traffic	Total inbound traffic in the last 5 minutes Collection method: Total inbound traffic in the last 5 minutes	≥0 Mbit Value type: Float	Mbit	1000	Protected domain dame	5
outbound_traffic	Total Outbound Traffic	Total outbound traffic in the last 5 minutes Collection method: Total outbound traffic in the last 5 minutes	≥0 Mbit Value type: Float	Mbit	1000	Protected domain dame	5
waf_process_time_0	WAF Latency [0-10) ms	This metric is used to collect how many requests are processed by WAF at latencies from 0 ms (included) to 10 ms (excluded) in the last 5 minutes. Collection method: The number of requests processed by WAF at latencies from 0 ms (included) to 10 ms (excluded) in the last 5 minutes are collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
waf_process_time_10	WAF Latency [10-20) ms	This metric is used to collect how many requests are processed by WAF at latencies in the 10 ms to less than 20 ms range in the last 5 minutes. Collection method: The number of requests processed by WAF at latencies in the 10 ms to less than 20 ms range in the last 5 minutes are collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
waf_process_time_20	WAF Latency [20-50) ms	This metric is used to collect how many requests are processed by WAF at latencies from 20 ms (included) to 50 ms (excluded) in the last 5 minutes. Collection method: The number of requests processed by WAF at latencies from 20 ms (included) to 50 ms (excluded) in the last 5 minutes are collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
waf_process_time_50	WAF Latency [50-100) ms	This metric is used to collect how many requests are processed by WAF at latencies from 50 ms (included) to 100 ms (excluded) in the last 5 minutes. Collection method: The number of requests processed by WAF at latencies from 50 ms (included) to 100 ms (excluded) in the last 5 minutes are collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
waf_process_time_100	WAF Latency [100, 1,000) ms	This metric is used to collect how many requests are processed by WAF at latencies in the 100 ms to less than 1,000 ms range in the last 5 minutes. Collection method: The number of requests processed by WAF at latencies in the 100 ms to less than 1,000 ms range in the last 5 minutes are collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes
waf_process_time_1000	WAF Latency [1,000, above) ms	This metric is used to collect how many requests are processed by WAF at latencies above 1000 ms in the last 5 minutes. Collection method: The number of requests processed by WAF at latencies above 1000 ms in the last 5 minutes are collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
qps_peak	Peak QPS	This metric is used to collect the peak QPS of the domain name in the last 5 minutes. Collection method: The peak QPS of the domain name in the last 5 minutes is collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes
qps_mean	Average QPS	This metric is used to collect the average QPS of the domain name in the last 5 minutes. Collection method: The average QPS of the domain name in the last 5 minutes is collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
waf_http_0	No WAF Status Code	This metric is used to collect how many requests with no status code returned by WAF in the last 5 minutes. Collection method: The number of requests with no WAF status code returned in the last 5 minutes is collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes
upstream_code_2xx	Status Code Returned to the Client (2XX)	This metric is used to collect how many requests with *2XX* status code are returned by the origin server in the last 5 minutes. Collection method: The number of requests with *2XX* status code returned by the origin server in the last 5 minutes is collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
upstream_code_3xx	Status Code Returned by the Origin Server (3XX)	This metric is used to collect how many requests with *3XX* status code are returned by the origin server in the last 5 minutes. Collection method: The number of requests with *3XX* status code returned by the origin server in the last 5 minutes is collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes
upstream_code_4xx	Status Code Returned by the Origin Server (4XX)	This metric is used to collect how many requests with *4XX* status code are returned by the origin server in the last 5 minutes. Collection method: The number of requests with *4XX* status code returned by the origin server in the last 5 minutes is collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
upstream_code_5xx	Status Code Returned by the Origin Server (5XX)	This metric is used to collect how many requests with *5XX* status code are returned by the origin server in the last 5 minutes. Collection method: The number of requests with *5XX* status code returned by the origin server in the last 5 minutes is collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes
upstream_code_0	No Origin Server Status Code	This metric is used to collect how many requests with no status code returned by the origin server in the last 5 minutes. Collection method: The number of requests with no status code returned by the origin server in the last 5 minutes is collected.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
inbound_traffic_peak	Peak Inbound Bandwidth	This metric is used to collect the peak inbound bandwidth to the domain name in the last 5 minutes. Collection method: The peak inbound bandwidth to the domain name in the last 5 minutes is collected.	≥0 Value type: Float	Mbit/s	1000	Protected domain dame	5 minutes
inbound_traffic_mean	Average Inbound Bandwidth	This metric is used to collect the average inbound bandwidth to the domain name in the last 5 minutes. Collection method: The average inbound bandwidth to the domain name in the last 5 minutes is collected.	≥0 Value type: Float	Mbit/s	1000	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
outbound_traffic_peak	Peak Outbound Bandwidth	This metric is used to collect the peak outbound bandwidth from the domain name in the last 5 minutes. Collection method: The peak outbound bandwidth from the domain name in the last 5 minutes is collected.	≥0 Value type: Float	Mbit/s	1000	Protected domain dame	5 minutes
outbound_traffic_mean	Average Outbound Bandwidth	This metric is used to collect the average outbound bandwidth from the domain name in the last 5 minutes. Collection method: The average outbound bandwidth from the domain name in the last 5 minutes is collected.	≥0 Value type: Float	Mbit/s	1000	Protected domain dame	5

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
attacks	Number of Attack Requests	This metric is used to collect the total number of attacks against the domain name in the last 5 minutes. Collection method: The system collects the number of attacks against the domain name in the last 5 minutes.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes
crawlers	Crawler Requests	This metric is used to collect the crawler attacks against the domain name in the last 5 minutes. Collection method: The system collects the number of crawler attacks against the domain name in the last 5 minutes.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
base_protection_counts	Basic Web Protection Actions	This metric is used to collect the number of attacks defended by basic web protection rules over the last 5 minutes. Collection method: The system collects the number of attacks hit basic web protection rules over the last 5 minutes.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes
precise_protection_counts	Precise Protection Actions	This metric is used to collect the number of attacks defended by precise protection rules over the last 5 minutes. Collection method: The system collects the number of attacks hit precise protection rules over the last 5 minutes.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Minute)
cc_protection_counts	CC Attacks Blocked	This metric is used to collect the number of attacks blocked by CC attack protection rules over the last 5 minutes. Collection method: The system collects the number of attacks hit CC attack protection rules over the last 5 minutes.	≥0 Value type: Float	Count	N/A	Protected domain name	5 minutes
white_black_ip_protection_counts	Blacklist and Whitelist IP Protection Count	This metric is used to collect the number of attacks defended by IP address blacklist and whitelist rules over the last 5 minutes. Collection method: The system collects the number of attacks hit blacklist and whitelist rules over the last 5 minutes.	≥0 Value type: Float	Count	N/A	Protected domain dame	5 minutes

Metrics for Dedicated WAF Instances

Table 13-2 Metrics for dedicated waf instances

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
cpu_util	CPU Usage	CPU consumed by the monitored object Collection method: 100% minus idle CPU usage percentage	0–100 Value type: Float	%	N/A	Dedicated WAF instances	1
mem_util	Memory Usage	Memory usage of the monitored object Collection method: 100% minus idle memory percentage	0–100 Value type: Float	%	N/A	Dedicated WAF instances	1
disk_util	Disk Usage	Disk usage of the monitored object Collection method: 100% minus idle disk space percentage	0–100 Value type: Float	%	N/A	Dedicated WAF instances	1
disk_avail_size	Available Disk Space	Available disk space of the monitored object Collection mode: size of free disk space	≥0 Value type: Float	Byte, KB, MB, GB, TB, and PB	1024	Dedicated WAF instances	1

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
disk_read_bytes_rate	Disk Read Rate	Number of bytes the monitored object reads from the disk per second Collection mode: number of bytes read from the disk per second	≥0 Value type: Float	Byte/s, KB/s, MB/s, and GB/s	1024	Dedicated WAF instances	1
disk_write_bytes_rate	Disk Write Rate	Number of bytes the monitored object writes into the disk per second Collection mode: number of bytes written into the disk per second	≥0 Value type: Float	Byte/s, KB/s, MB/s, and GB/s	1024	Dedicated WAF instances	1
disk_read_requests_rate	Disk Read Requests	Number of requests the monitored object reads from the disk per second Collection mode: number of read requests processed by the disk per second	≥0 Value type: Float	request/s	N/A	Dedicated WAF instances	1

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
disk_write_requests_rate	Disk Write Requests	Number of requests the monitored object writes into the disk per second Collection method: Number of write requests processed by the disk per second	≥0 Value type: Float	request/s	N/A	Dedicated WAF instances	1
network_incoming_bytes_rate	Incoming Traffic	Incoming traffic per second on the monitored object Collection method: Incoming traffic over the NIC per second	≥0 Value type: Float	Byte/s, KB/s, MB/s, and GB/s	1024	Dedicated WAF instances	1
network_outgoing_bytes_rate	Outgoing Traffic	Outgoing traffic per second on the monitored object Collection method: Outgoing traffic over the NIC per second	≥0 Value type: Float	Byte/s, KB/s, MB/s, and GB/s	1024	Dedicated WAF instances	1
network_incoming_packets_rate	Incoming Packet Rate	Incoming packets per second on the monitored object Collection method: Incoming packets over the NIC per second	≥0 Value type: Int	Packet/s	N/A	Dedicated WAF instances	1

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
network_outgoing_packets_rate	Outgoing Packet Rate	Outgoing packets per second on the monitored object Collection method: Outgoing packets over the NIC per second	≥0 Value type: Int	Packet/s	N/A	Dedicated WAF instances	1
concurrent_connections	Concurrent Connections	Number of concurrent connections being processed Collection method: Number of concurrent connections in the system	≥0 Value type: Int	Count	N/A	Dedicated WAF instances	1
active_connections	Active Connections	Number of active connections Collection method: Number of active connections in the system	≥0 Value type: Int	Count	N/A	Dedicated WAF instances	1
latest_policy_sync_time	Latest Rule Synchronization	Time elapsed for the WAF to synchronize the latest custom rules Collection method: Time elapsed for synchronizing to the last policies	≥0 Value type: Int	ms	N/A	Dedicated WAF instances	1

Dimensions

Key	Value
instance_id	ID of the dedicated WAF instance
waf_instance_id	ID of the website protected with WAF

Example of Raw Data Format of Monitored Metrics

```
[
   {
      "metric": {
          // Namespace
         "namespace": "SYS.WAF",
         "dimensions": [
            {
               // Dimension name, for example, protected website
               "name": "waf_instance_id",
               // ID of the monitored object in this dimension, for example, ID of the protected website
               "value": "082db2f542e0438aa520035b3e99cd99"
            }
         ],
        //Metric ID
         "metric_name": "waf_http_2xx"
      },
// Time to live, which is predefined for the metric
      "ttl": 172800,
       // Metric value
      "value": 0.0,
     // Metric unit
      "unit": "Count",
       // Metric value type
      "type": "float",
      // Collection time for the metric
      "collect_time": 1637677359778
   }
]
```

13.1.2 Configuring Alarm Monitoring Rules

You can set WAF alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, metric, threshold, monitoring scope, and whether to send notifications. This helps you learn the WAF protection status in a timely manner.

Prerequisites

You have connected the website you want to protect to WAF.

Configuring Alarm Monitoring Rules

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.

Step 5 In the upper right corner of the page, click **Create Alarm Rule**.

Step 6 Configure related parameters.

- **Name**: Enter a name.
- **Alarm Type**: Select **Metric**.
- **Cloud product**: Select **Web Application Firewall - Dedicated WAF Instance** or **Web Application Firewall - Domains**.
  - For dedicated instance metrics, select **Web Application Firewall - Dedicated WAF Instance** as the monitored metric.
  - For protected domain names, select **Web Application Firewall - Domains**.
- **Monitoring Scope**: Select **All resources**.
- **Method**: Select **Associated template** or create a custom template.
- **Alarm Notification**: If you want to receive alarms in real time, enable this option and select a notification mode.
- Other parameters: Set them based on site requirements.

Step 7 Click **Create**. In the displayed dialog box, click **OK**.

----End

13.1.3 Viewing Monitored Metrics

You can view WAF metrics on the Cloud Eye console. You will learn about the WAF protection status in a timely manner and set protection policies based on the metrics.

Prerequisites

WAF alarm rules have been configured in Cloud Eye. For more details, see **Configuring Alarm Monitoring Rules**.

Viewing Monitored Metrics

Step 1 **Log in to the management console**.

Step 2 Click  in the upper left corner and select a region or project.

Step 3 Click  in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Cloud Service Monitoring**.

Step 5 Search for **Web Application Firewall WAF** by **Dashboard** in the search box. In the **Dashboard** column, click **Web Application Firewall WAF** to go to the **Details** page.

Step 6 On the **Overview** tab, you can view metrics related to resource overview and alarm statistics.

Step 7 Click the **Resources** tab. In the **Operation** column of the instance list, click **View Metric**.

NOTE

To view the monitoring information about a specific website, you can go to the **Website Settings** page, locate the row containing the target domain name and click **Cloud Eye** in the **Operation** column.

----End

13.2 Using CTS to Audit WAF

13.2.1 WAF Operations Recorded by CTS

CTS provides records of operations on WAF. With CTS, you can query, audit, and backtrack these operations. For details, see the *Cloud Trace Service User Guide*.

Table 13-3 WAF Operations Recorded by CTS

Operation	Resource Type	Trace Name
Adding a domain name to the cloud WAF	instance	createInstance
Deleting a domain name from the cloud WAF	instance	deleteInstance
Modifying the protection status of a domain name in cloud mode	instance	modifyProtectStatus
Modifying the access status of a domain name in cloud mode	instance	modifyAccessStatus
Changing a domain name in cloud mode	instance	modifyInstance
Modifying DNS records for quick access to WAF	instance	quickAccessInstance
Adding a domain name to WAF (dedicated/ELB mode)	Host	createHost
Changing a domain name added to WAF (dedicated/ELB mode)	Host	modifyHost

Operation	Resource Type	Trace Name
Deleting a domain name from WAF (dedicated/ELB mode)	Host	deleteHost
Changing WAF protection status (dedicated/ELB mode)	Host	modifyProtectStatus
Changing domain name access status (dedicated/ELB mode)	Host	modifyAccessStatus
Changing domain name access settings (dedicated/ELB mode)	Host	modifyAccessProgress
Migrating domain names	migrate-host	migrateHosts
Uploading a certificate	certificate	createCertificate
Modifying a certificate	certificate	updateCertificate
Deleting a certificate from WAF	certificate	deleteCertificate
Applying a certificate to a domain name	certificate	applyCertificate
Sharing a certificate	certificate-sharing	createCertificateSharing
Disabling certificate sharing	certificate-sharing	deleteCertificateSharing
Creating a WAF policy	policy	createPolicy
Applying a WAF policy	policy	applyToHost
Modifying a policy	policy	modifyPolicy
Deleting a WAF policy	policy	deletePolicy

Operation	Resource Type	Trace Name
Adding a CC attack protection rule	policy	createCc
Modifying a CC attack protection rule	policy	modifyCc
Deleting a CC attack protection rule	policy	deleteCc
Adding a precise protection rule	policy	createCustom
Modifying a precise protection rule	policy	modifyCustom
Deleting a precise protection rule	policy	deleteCustom
Adding an IP address blacklist or whitelist rule	policy	createWhiteblackip
Modifying an IP address blacklist or whitelist rule	policy	modifyWhiteblackip
Deleting an IP address blacklist or whitelist rule	policy	deleteWhiteblackip
Creating/updating a web tamper protection rule	policy	createAntitamper
Enabling or disabling a web tamper protection rule	policy	modifyAntitamper
Deleting a web tamper protection rule	policy	deleteAntitamper
Creating a global whitelist rule	policy	createIgnore
Modifying a global protection whitelist rule	policy	modifyIgnore
Deleting a global protection whitelist rule	policy	deleteIgnore

Operation	Resource Type	Trace Name
Adding a data masking rule	policy	createPrivacy
Modifying a data masking rule	policy	modifyPrivacy
Deleting a data masking rule	policy	deletePrivacy
Creating a known attack source rule	policy	createPunishment
Modifying a known attack source rule	policy	modifyPunishment
Deleting a known attack source rule	policy	deletePunishment
Adding a geolocation access control rule	policy	createGeoip
Modifying a geolocation access control rule	policy	modifyGeoip
Deleting a geolocation access control rule	policy	deleteGeoip
Creating an anti-crawler rule	policy	createAnticrawler
Modifying an anti-crawler rule	policy	modifyAnticrawler
Deleting an anti-crawler rule	policy	deleteAnticrawler
Creating an information leakage prevention rule	policy	createAntileakage
Modifying an information leakage prevention rule	policy	modifyAntileakage
Deleting an information leakage prevention rule	policy	deleteAntileakage
Batch creating CC attack protection rules	policy	batchCreateCc

Operation	Resource Type	Trace Name
Batch modifying CC attack protection rules	policy	batchUpdateCc
Batch deleting CC attack protection rules	policy	batchDeleteCc
Batch creating precise protection rules	policy	batchCreateCustom
Batch modifying precise protection rules	policy	batchUpdateCustom
Batch deleting precise protection rules	policy	batchDeleteCustom
Batch creating IP address blacklist and whitelist rules	policy	batchCreateWhiteblackip
Batch modifying IP address blacklist or whitelist rules	policy	batchUpdateWhiteblackip
Batch deleting IP address blacklist or whitelist rules	policy	batchDeleteWhiteblackip
Batch creating geolocation access control rules	policy	batchCreateGeoip
Batch modifying geolocation access control rules	policy	batchUpdateGeoip
Batch deleting geolocation access control rules	policy	batchDeleteGeoip
Batch creating/ updating web tamper protection rules	policy	batchCreateAntitamper
Batch enabling or disabling web tamper protection rules	policy	batchUpdateAntitamper

Operation	Resource Type	Trace Name
Batch deleting web tamper protection rules	policy	batchDeleteAntitamper
Batch creating information leakage prevention rules	policy	batchCreateAntileakage
Batch modifying information leakage prevention rules	policy	batchUpdateAntileakage
Batch deleting information leakage prevention rules	policy	batchDeleteAntileakage
Batch creating global protection whitelist rules	policy	batchCreateIgnore
Batch modifying global protection whitelist rules	policy	batchUpdateIgnore
Batch deleting global protection whitelist rules	policy	batchDeleteIgnore
Batch creating data masking rules	policy	batchCreatePrivacy
Batch modifying data masking rules	policy	batchUpdatePrivacy
Batch deleting data masking rules	policy	batchDeletePrivacy
Creating alarm notifications	alertNoticeConfig	createAlertNoticeConfig
Modifying alarm notifications	alertNoticeConfig	modifyAlertNoticeConfig
Deleting alarm notifications	alertNoticeConfig	deleteAlertNoticeConfig
Batch deleting alarm notifications	alertNoticeConfig	batchDeleteAlertNoticeConfig
Deleting a dedicated WAF instance	instance	deleteInstance

Operation	Resource Type	Trace Name
Creating a dedicated WAF instance	instance	createInstance
Updating a dedicated WAF instance	instance	upgradeInstance
Changing the instance name	instance	alterInstanceName
Adding an address group	ip-group	createIPGroup
Modifying an address group	ip-group	modifyIPGroup
Deleting an address group	ip-group	deleteIPGroup
Creating a reference table	valueList	createValueList
Modifying a reference table	valueList	modifyValueList
Deleting a reference table	valueList	deleteValueList
Creating a Report Template	SecurityReport	createSecurityReportSubscription
Modifying a security report template	SecurityReport	updateSecurityReportSubscription
Deleting a security report template	SecurityReport	deleteSecurityReportSubscription

13.2.2 Viewing CTS Traces in the Trace List

Scenarios

After you enable Cloud Trace Service (CTS) and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, CTS starts recording operations on data in Object Storage Service (OBS) buckets. CTS stores operation records (traces) generated in the last seven days.

This section describes how to query or export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for longer than seven days, configure transfer to OBS or Log Tank Service (LTS) so that you can view them in OBS buckets or LTS log groups.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces 5 minutes later.
- These operation records are retained for seven days on the CTS console and are automatically deleted upon expiration. Manual deletion is not supported.

Viewing Real-Time Traces in the Trace List of the New Edition

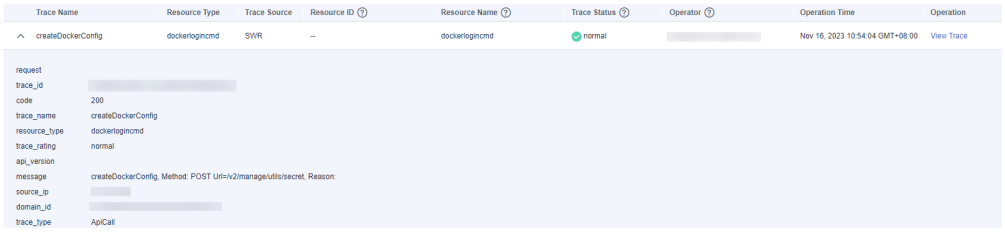
1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
   - **Trace Name**: Enter a trace name.
   - **Trace ID**: Enter a trace ID.
   - **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
   - **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
   - **Trace Source**: Select a cloud service name from the drop-down list.
   - **Resource Type**: Select a resource type from the drop-down list.
   - **Operator**: Select one or more operators from the drop-down list.
   - **Trace Status**: Select **normal**, **warning**, or **incident**.
     - **normal**: The operation succeeded.
     - **warning**: The operation failed.
     - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
   - **Enterprise Project ID**: Enter an enterprise project ID.
   - **Access Key**: Enter a temporary or permanent access key ID.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.

- Enter any keyword in the search box and press **Enter** to filter desired traces.
- Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
- Click to view the latest information about traces.
- Click to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled ( ), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.

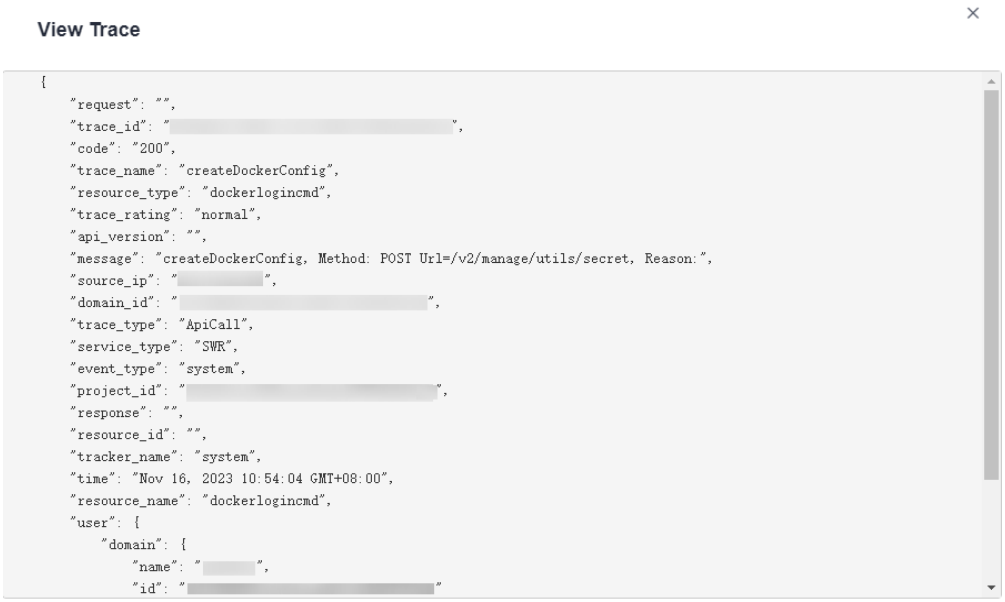
6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

1. Log in to the management console.
2. Click in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available.
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.
     - If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range within the last seven days.
6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.
   - Click to view the latest information about traces.
8. Click on the left of a trace to expand its details.



9. Click **View Trace** in the **Operation** column. The trace details are displayed.



10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces** in the *CTS User Guide*.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

