Web Application Firewall

User Guide

Issue	06
Date	2024-11-06

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei 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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

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.

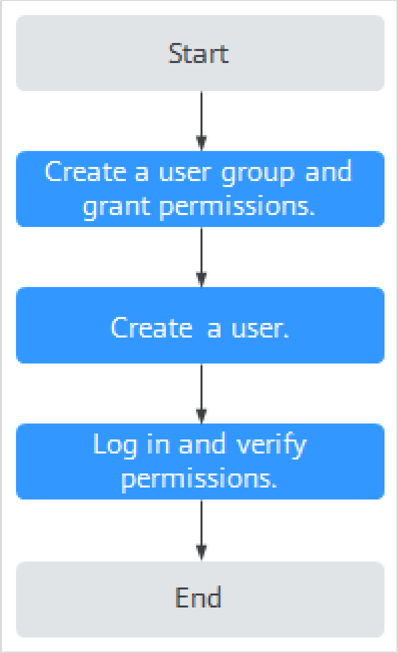
Table 1-1 System policies supported by WAF

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.

Role/Policy Name	Description	Category	Dependencies
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


Start
Create a user group and grant permissions.
Create a user.
Log in and verify permissions.
End

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 the yearly/monthly billing mode, the standard, professional, and platinum editions are available. Each edition offers domain, QPS, and rule expansion packages.

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.
- Expansion package can only be renewed or unsubscribed together with the WAF instance you are using.

Specification Limitations

- A domain package allows you to add 10 domain names to WAF, including one top-level domain and nine subdomains or wildcard domains related to the top-level domain.
- 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.

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.
- Platinum

  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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner and choose **Security** > **Web Application Firewall**.

Step 4 In the upper right corner of the page, click **Buy WAF**.

Step 5 (Optional): Select an enterprise project from the **Enterprise Project** drop-down list.

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 when you purchase WAF under the logged-in account.

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

Step 7 **Billing Mode**: Select **Yearly/Monthly**. Select a region.

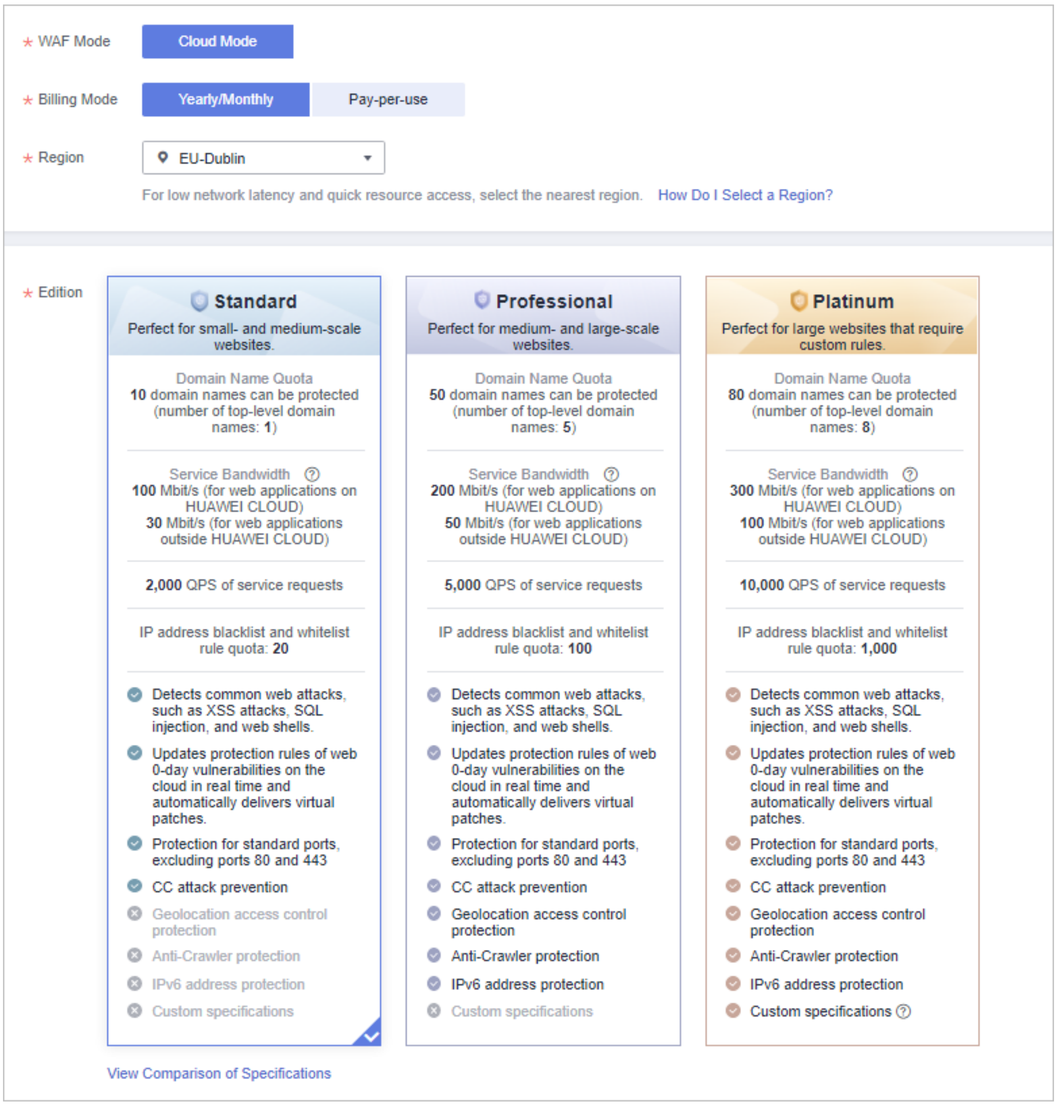
NOTE

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.

Figure 2-1 Selecting WAF edition



* WAF Mode: Cloud Mode

* Billing Mode: Yearly/Monthly | Pay-per-use

* Region: EU-Dublin

For low network latency and quick resource access, select the nearest region. How Do I Select a Region?

* Edition

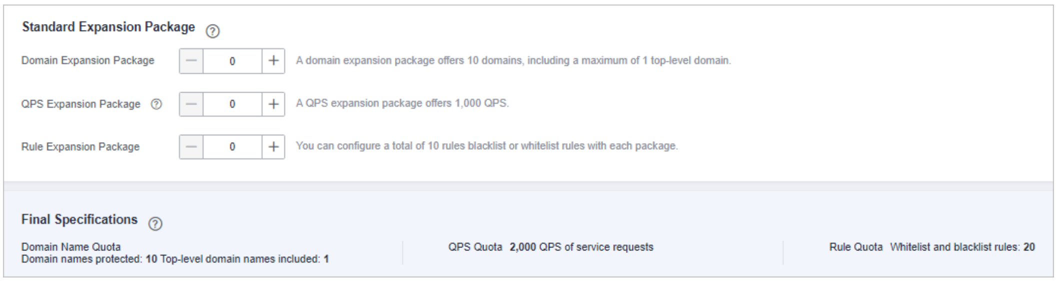
Standard	Professional	Platinum
Perfect for small- and medium-scale websites.	Perfect for medium- and large-scale websites.	Perfect for large websites that require custom rules.
Domain Name Quota **10** domain names can be protected (number of top-level domain names: **1**)	Domain Name Quota **50** domain names can be protected (number of top-level domain names: **5**)	Domain Name Quota **80** domain names can be protected (number of top-level domain names: **8**)
Service Bandwidth **100** Mbit/s (for web applications on HUAWEI CLOUD) **30** Mbit/s (for web applications outside HUAWEI CLOUD)	Service Bandwidth **200** Mbit/s (for web applications on HUAWEI CLOUD) **50** Mbit/s (for web applications outside HUAWEI CLOUD)	Service Bandwidth **300** Mbit/s (for web applications on HUAWEI CLOUD) **100** Mbit/s (for web applications outside HUAWEI CLOUD)
2,000 QPS of service requests	**5,000** QPS of service requests	**10,000** QPS of service requests
IP address blacklist and whitelist rule quota: **20**	IP address blacklist and whitelist rule quota: **100**	IP address blacklist and whitelist rule quota: **1,000**
✓ Detects common web attacks, such as XSS attacks, SQL injection, and web shells.	✓ Detects common web attacks, such as XSS attacks, SQL injection, and web shells.	✓ Detects common web attacks, such as XSS attacks, SQL injection, and web shells.
✓ Updates protection rules of web 0-day vulnerabilities on the cloud in real time and automatically delivers virtual patches.	✓ Updates protection rules of web 0-day vulnerabilities on the cloud in real time and automatically delivers virtual patches.	✓ Updates protection rules of web 0-day vulnerabilities on the cloud in real time and automatically delivers virtual patches.
✓ Protection for standard ports, excluding ports 80 and 443	✓ Protection for standard ports, excluding ports 80 and 443	✓ Protection for standard ports, excluding ports 80 and 443
✓ CC attack prevention	✓ CC attack prevention	✓ CC attack prevention
✗ Geolocation access control protection	✓ Geolocation access control protection	✓ Geolocation access control protection
✗ Anti-Crawler protection	✓ Anti-Crawler protection	✓ Anti-Crawler protection
✗ IPv6 address protection	✓ IPv6 address protection	✓ IPv6 address protection
✗ Custom specifications	✗ Custom specifications	✓ Custom specifications

View Comparison of Specifications

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 2-2 Selecting expansion packages



Standard Expansion Package

Domain Expansion Package − 0 + A domain expansion package offers 10 domains, including a maximum of 1 top-level domain.

QPS Expansion Package − 0 + A QPS expansion package offers 1,000 QPS.

Rule Expansion Package − 0 + You can configure a total of 10 rules blacklist or whitelist rules with each package.

Final Specifications

Domain Name Quota
Domain names protected: **10** Top-level domain names included: **1**

QPS Quota **2,000** QPS of service requests

Rule Quota Whitelist and blacklist rules: **20**

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.

----End

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

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 and choose **Web Application Firewall** under **Security**.

Step 4 In the upper right corner of the page, click **Buy WAF**.

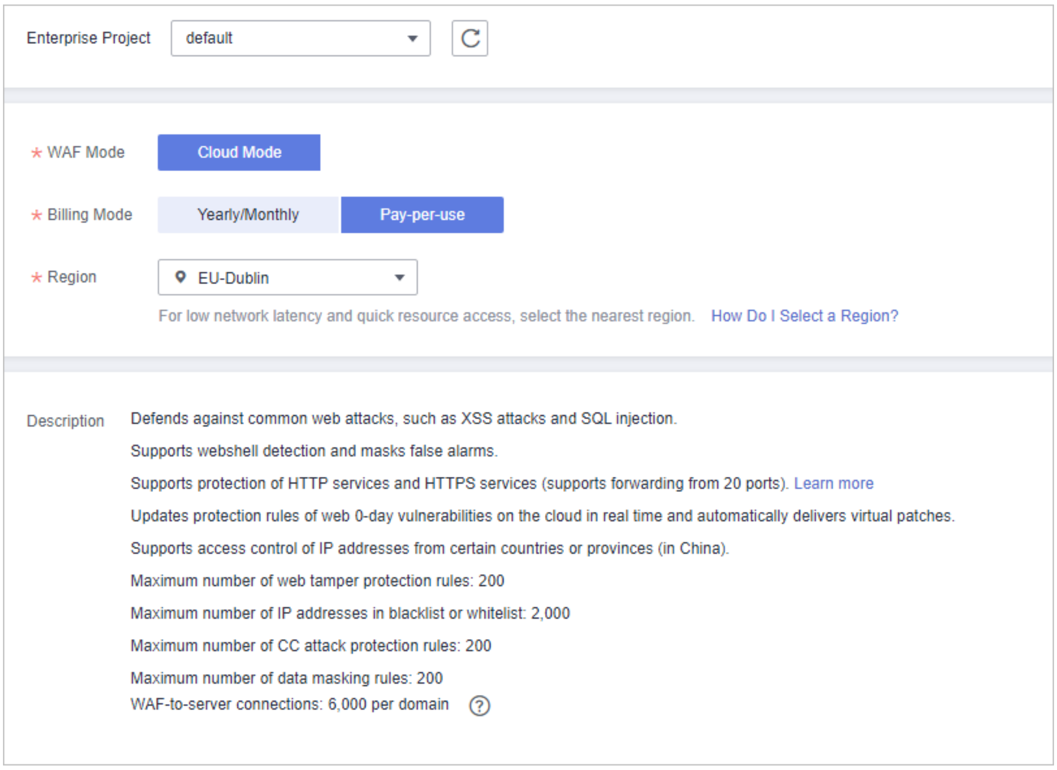
Step 5 On the **Buy Web Application Firewall** page, select **Pay-per-use** for **Billing Mode** and select a region.

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 2-3 Pay-per-use



Enterprise Project: default

* WAF Mode: Cloud Mode

* Billing Mode: Yearly/Monthly | Pay-per-use

* Region: EU-Dublin

For low network latency and quick resource access, select the nearest region. How Do I Select a Region?

Description:
Defends against common web attacks, such as XSS attacks and SQL injection.
Supports webshell detection and masks false alarms.
Supports protection of HTTP services and HTTPS services (supports forwarding from 20 ports). Learn more
Updates protection rules of web 0-day vulnerabilities on the cloud in real time and automatically delivers virtual patches.
Supports access control of IP addresses from certain countries or provinces (in China).
Maximum number of web tamper protection rules: 200
Maximum number of IP addresses in blacklist or whitelist: 2,000
Maximum number of CC attack protection rules: 200
Maximum number of data masking rules: 200
WAF-to-server connections: 6,000 per domain

Step 6 In the lower right corner of the page, click **Next**.

Step 7 Click **Back to Website Settings** and add domain names of websites to be protected.

NOTE

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

----End

Verification

Your WAF instance is purchased when your instance edition and its remaining validity days are shown in the upper right corner of the management console.

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 package can protect 10 domain names, including a maximum of one top-level domain name. If the cloud WAF edition you are using cannot meet your business requirements, you can purchase domain expansion packages to increase the quota. For example, if you are using the standard edition, 10 domain names can be protected, including only one top-level domain name. If you want to protect three top-level domain names, you can purchase two 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, including only one top-level domain name.
- Professional edition: A maximum of 50 domain names can be protected, including five top-level domain names.
- Platinum edition: A maximum of 80 domain names can be protected, including eight top-level domain names.

NOTE

- If only one top-level domain can be added to a WAF instance, you can add one top-level domain and subdomain or wildcard domain names related to the top-level domain. For example, you can add one top-level domain name example.com and a maximum of nine sub-domains or generic domains, for example, www.example.com, *.example.com, mail.example.com, user.pay.example.com, and x.y.z.example.com. Each of these domain names (including the top-level domain name example.com) is counted toward a domain name quota in the domain name package.
- 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 platinum cloud WAF instance billed on a yearly/monthly basis. If you need to protect a larger QPS, 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 platinum 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 a platinum 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.

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 platinum 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. A rule expansion package must be renewed or unsubscribed from along with the associated WAF instance.

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

2.2 Buying a Dedicated WAF Instance

If your service servers are deployed on Huawei Cloud, you can purchase dedicated WAF instances to protect important domain names or web services that have 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
>
> 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.
- The Organizations service is in 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.
- If you enable **Anti-affinity**, a maximum of five dedicated WAF instances can be created.

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 choose **Web Application Firewall** under **Security**.

Step 3 In the upper right corner of the page, click **Buy WAF**.

Step 4 (Optional): Select an enterprise project from the **Enterprise Project** drop-down list.

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.

Step 5 On the **Buy Web Application Firewall** page, select **Dedicated Mode** for **WAF Mode**.

Step 6 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 billing
	Region	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 AZ	Select an AZ in the selected region. **NOTE** After an AZ is selected, it cannot be changed after the purchase.	-
Edition and specifications	Edition selection	Specifications **WI-500** and **WI-100** are available. ● Specifications: WI-500. Referenced performance: – HTTP services - Recommended QPS: 5,000. Maximum QPS: 10,000. – HTTPS services - Recommended QPS: 4,000. Maximum QPS: 8,000. – WebSocket service - Maximum concurrent connections: 5,000 – Maximum WAF-to-server persistent connections: 60,000 ● Specifications: WI-100. Referenced performance: – HTTP services - Recommended QPS: 1,000. Maximum QPS: 2,000. – HTTPS services - Recommended QPS: 800. Maximum QPS: 1,600 – WebSocket service - Maximum concurrent connections: 1,000 – Maximum WAF-to-server persistent connections: 60,000	WI-500

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)**.	**Network Interface**
Network settings	VPC	Select the VPC to which the origin server belongs.	-
	Subnet	Select a subnet configured in the VPC.	-
	Security Group	Select a security group in the region or click **Manage Security Group** to go to the VPC console and create a security group. After you select a security group, the WAF instance will be protected by the access rules of the security group. **NOTICE** ● 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 Retain the default settings. All outgoing network traffic is allowed by default. ● 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.	-

Parameter		Description	Example Value
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
(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
	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.	-

Parameter		Description	Example Value
	Authorization	This parameter is available first time you purchase 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, a maximum of five dedicated WAF instances can be created. ● If you enable this function, dedicated instances will be deployed on different physical servers as much as possible to improve service reliability.	-

Step 7 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 8 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 9 On the payment page, select a payment method and pay for your order.

Step 10 After the payment is successful, click **Back to Dedicated Engine List**. On the **Dedicated Engine** page, view the instance status.

----End

Verification

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.

Related Operations

Managing Dedicated WAF Engines

This topic describes how to manage your dedicated WAF instances (or engines), including viewing instance information, viewing instance monitoring configurations, upgrading the instance edition, or deleting an instance.

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
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.

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)**
- 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 platinum 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. ● WebSocket request inspection is enabled by default if **Client Protocol** is set to **HTTP**. ● WebSockets request inspection is enabled by default if **Client Protocol** is set to **HTTPS**.
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.
Limitation	After your website is connected to WAF, you can upload a file no larger than 1 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**.
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.
Proxy	If a layer-7 proxy server, such as CDN or cloud acceleration, is used before WAF, you need to select **Layer-7 proxy** for **Proxy Configured**. By doing this, WAF can obtain real client access IP addresses from the configured header field.
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. ● WebSocket request inspection is enabled by default if **Client Protocol** is set to **HTTP**. ● WebSockets request inspection is enabled by default if **Client Protocol** is set to **HTTPS**.
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)

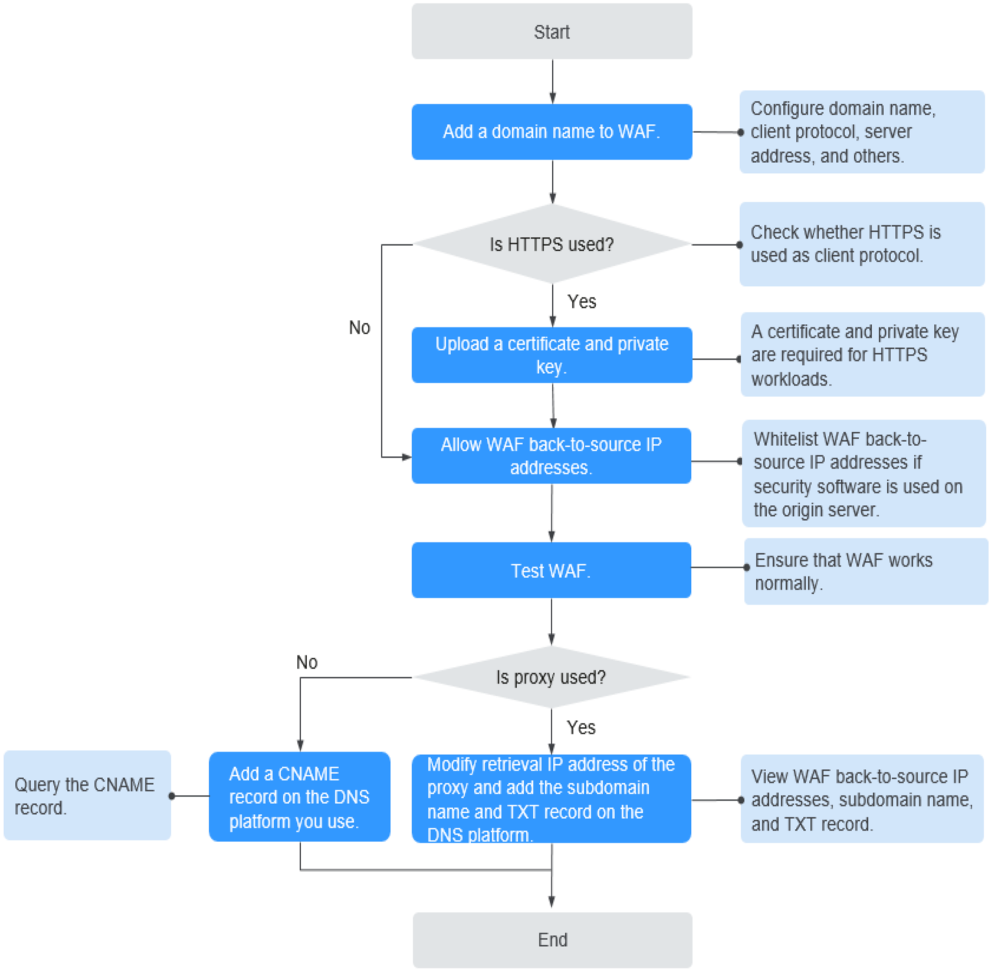

Start
Add a domain name to WAF.
Configure domain name, client protocol, server address, and others.
Is HTTPS used?
Check whether HTTPS is used as client protocol.
Yes
No
Upload a certificate and private key.
A certificate and private key are required for HTTPS workloads.
Allow WAF back-to-source IP addresses.
Whitelist WAF back-to-source IP addresses if security software is used on the origin server.
Test WAF.
Ensure that WAF works normally.
Is proxy used?
No
Yes
Query the CNAME record.
Add a CNAME record on the DNS platform you use.
Modify retrieval IP address of the proxy and add the subdomain name and TXT record on the DNS platform.
View WAF back-to-source IP addresses, subdomain name, and TXT record.
End

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.

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

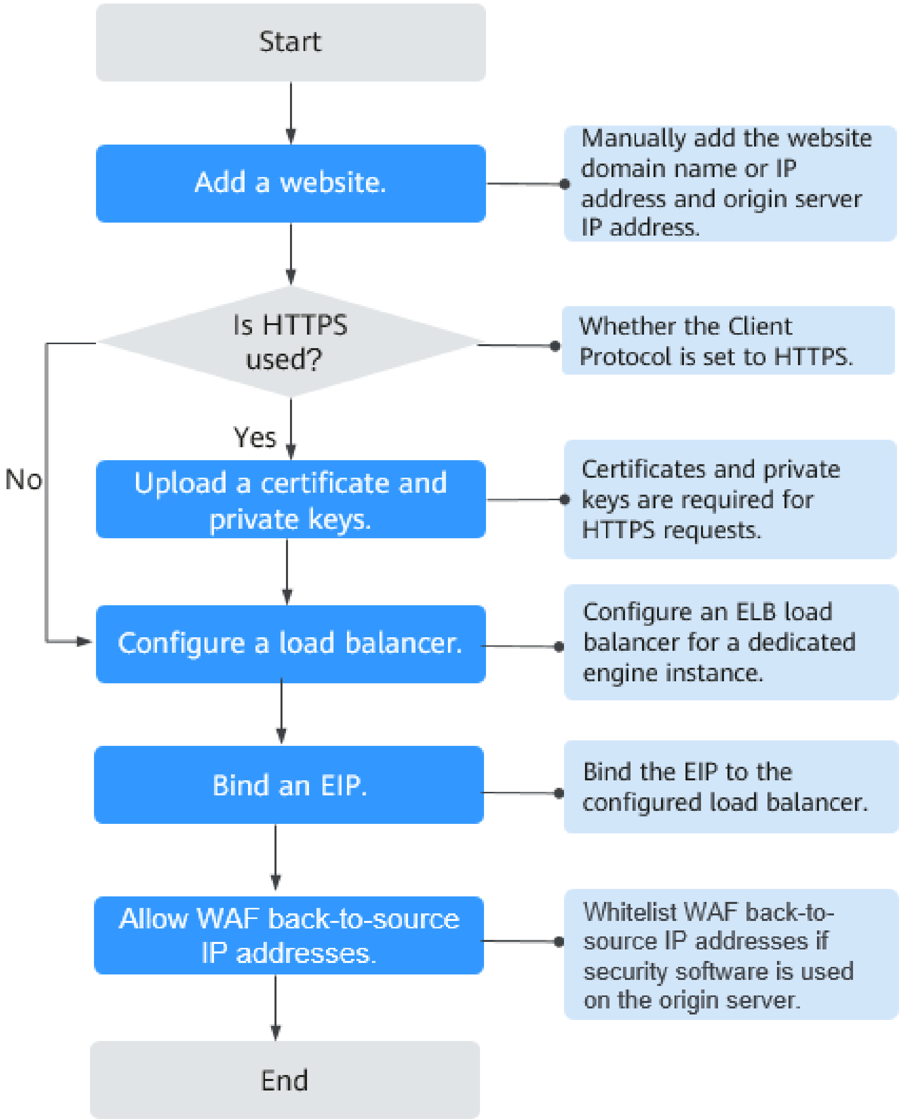

Start
Add a website.
Manually add the website domain name or IP address and origin server IP address.
Is HTTPS used?
Whether the Client Protocol is set to HTTPS.
No
Yes
Upload a certificate and private keys.
Certificates and private keys are required for HTTPS requests.
Configure a load balancer.
Configure an ELB load balancer for a dedicated engine instance.
Bind an EIP.
Bind the EIP to the configured load balancer.
Allow WAF back-to-source IP addresses.
Whitelist WAF back-to-source IP addresses if security software is used on the origin server.
End

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.
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 a Website to WAF (Cloud Mode)

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 load balancer 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.

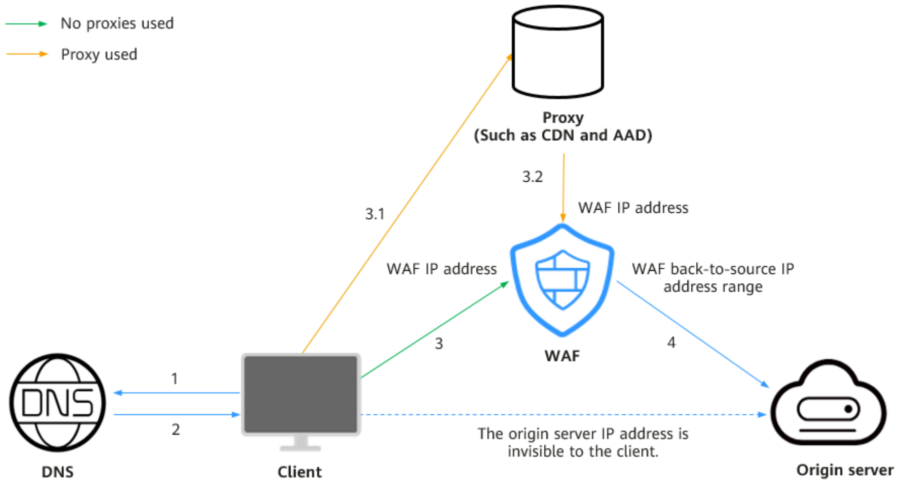
NOTE

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

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.

Procedure	Description
Step 2: Whitelist Back-to-Source IP Addresses on Your Origin Server	Obtain and allow back-to-source IP addresses.
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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane, click **Website Settings**.

Step 5 In the upper left corner of the website list, click **Add Website**.

Step 6 Select **Cloud Mode - CNAME** and click **Configure Now**.

Step 7 Configure the basic settings by referring to **Table 3-3**.

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, 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. **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. ● **Server Port**: service port over which the WAF instance forwards client requests to the origin server.	**Client Protocol**: **HTTP** **Server Protocol**: **HTTP** **Server Address**: XXX.XXX.1.1 **Server Port**: **80**

Parameter	Description	Example Value
Certificate	If you set **Client Protocol** to **HTTPS**, an SSL certificate is required. ● 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?** ● 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.	-
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 cipher suite 1 by default. For more details, see **Configuring PCI DSS/3DS Compliance Check and TLS**.	Minimum TLS version: TLS v1.0 Cipher suite: Cipher suite 1

Parameter	Description	Example Value
Proxy Your Website Uses	- **Layer-7 proxy**: Web proxy products for layer-7 request forwarding are used, products such as anti-DDoS, CDN, and other cloud acceleration services. - **Layer-4 proxy**: Web proxy products for layer-4 forwarding are used, products such as anti-DDoS. - **No proxy**: No proxy products are deployed in front of WAF. NOTICE - If a proxy is deployed before WAF on your website, the WAF working mode cannot be switched to **Bypassed**. For details about how to switch the working mode, see **Switching WAF Working Mode**. - If your website uses a proxy, select **Layer-7 proxy**. 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**.	No proxy

Step 8 Complete advanced settings.

Table 3-4 Advanced settings

Parameter	Description	Example Value
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**.	System-generated policy

Table 3-5 Parameters for system-generated policies

Policy	Description
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.
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.

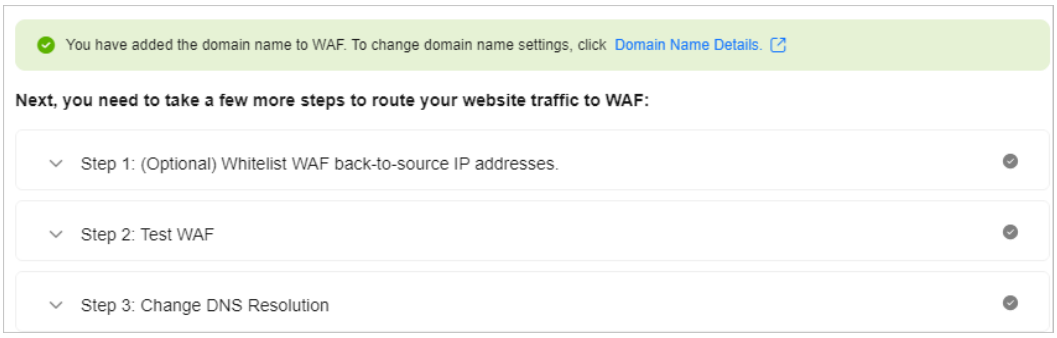
NOTE

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

Step 9 Click **Next**.

Whitelist WAF back-to-source IP addresses, **test WAF**, and **modify DNS record for the domain name** as prompted.

Figure 3-4 Domain name added to WAF.



You have added the domain name to WAF. To change domain name settings, click Domain Name Details.

Next, you need to take a few more steps to route your website traffic to WAF:

Step 1: (Optional) Whitelist WAF back-to-source IP addresses.

Step 2: Test WAF

Step 3: Change DNS Resolution

----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. 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.

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 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 whether the domain name is accessible after it has been added to WAF, preventing 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.

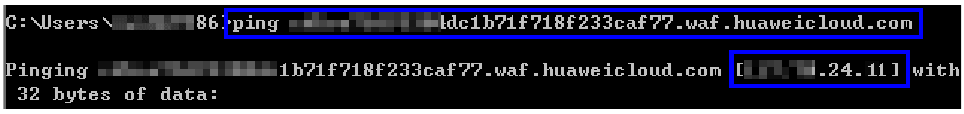
- Method 1: After **Step 2: Whitelist Back-to-Source IP Addresses on Your Origin Server** is complete, expand **Step 2: Test WAF** and copy the CNAME record on the displayed page. Alternatively, go to the **Website Settings** page, locate the target domain name, and click **Test WAF** in the **Access 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 3-5**, the WAF access IP address is displayed.

Figure 3-5 ping cname



```
C:\Users\[redacted]86>ping [redacted]dc1b71f718f233caf77.waf.huaweicloud.com

Pinging [redacted]1b71f718f233caf77.waf.huaweicloud.com [[redacted].24.11] with
 32 bytes of data:
```

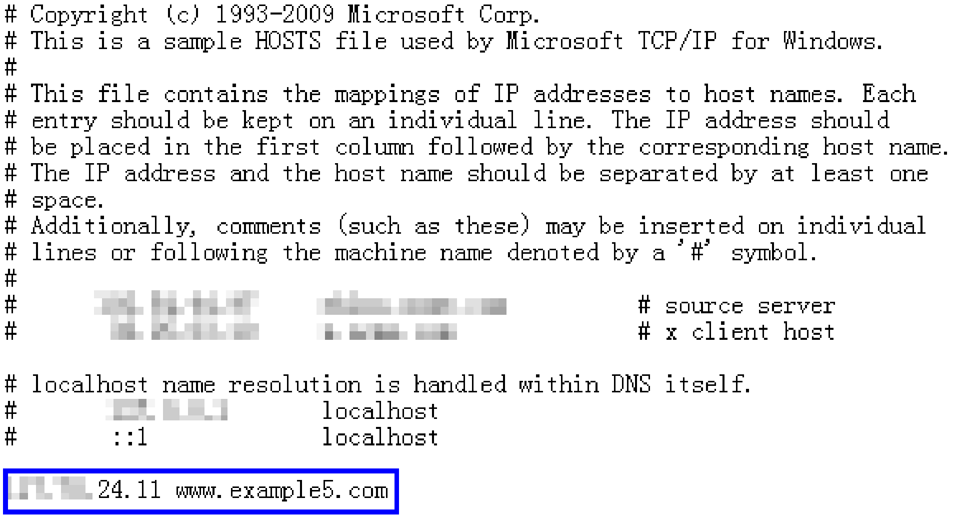
NOTE

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 3-6** 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 3-6 Adding a record



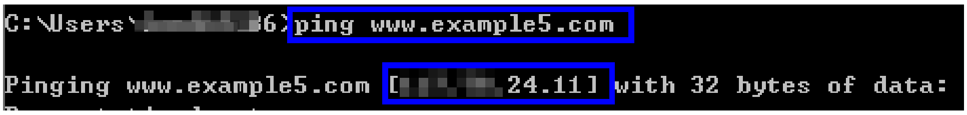
```
# Copyright (c) 1993-2009 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
#       [redacted]      [redacted]          # source server
#       [redacted]      [redacted]          # x client host

# localhost name resolution is handled within DNS itself.
#       [redacted]         localhost
#       ::1                localhost

[redacted]24.11 www.example5.com
```

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

Figure 3-7 Pinging the domain name



```
C:\Users\[redacted]6>ping www.example5.com

Pinging www.example5.com [[redacted]24.11] with 32 bytes of data:
```

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.

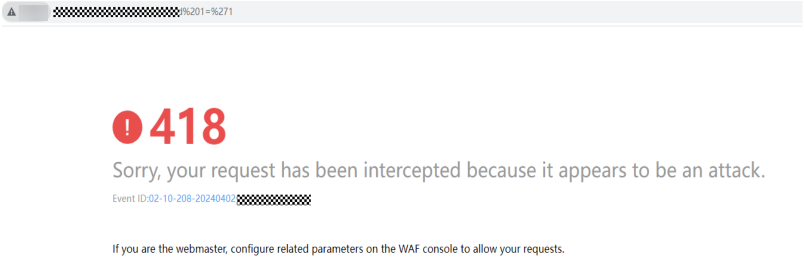
   If the domain name has been resolved to WAF back-to-source IP addresses and WAF configurations are correct, the website is accessible.

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 3-8 Request blocked



[redacted]%201=%271

418

Sorry, your request has been intercepted because it appears to be an attack.

Event ID:02-10-208-20240402[redacted]

If you are the webmaster, configure related parameters on the WAF console to allow your requests.

c. In the navigation pane, 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.

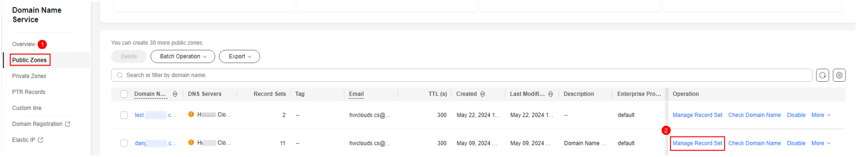
Step 2 Change the DNS records of the domain name to the WAF CNAME record.

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 3-9 Record sets

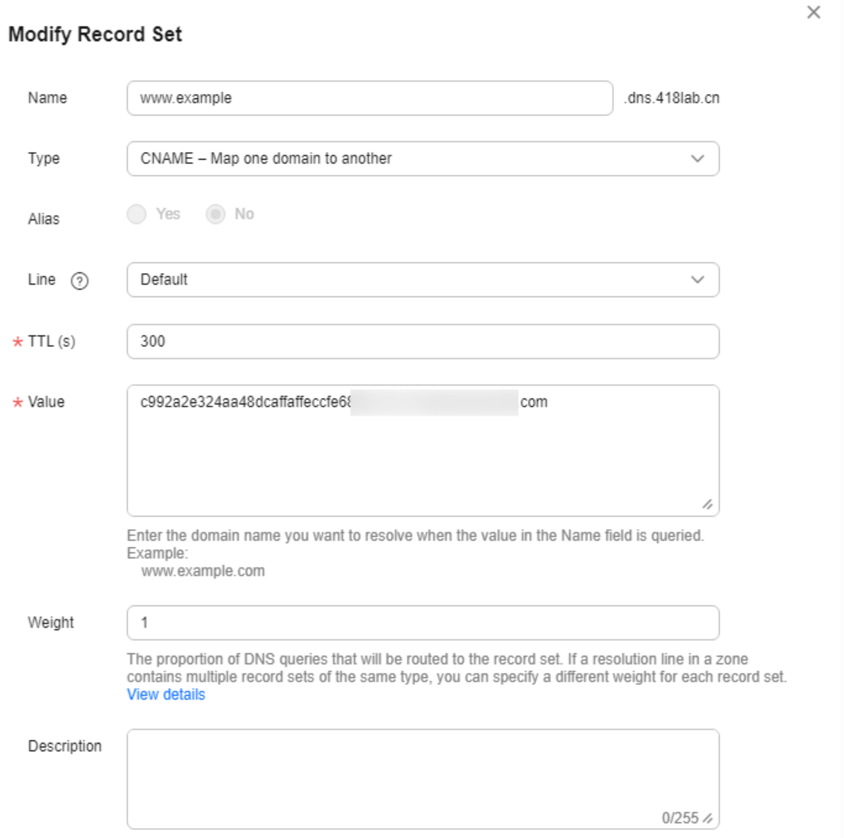


You can create 30 more public zones.

Domain N...	DNS Servers	Record Sets	Tag	Email	TTL (s)	Created	Last Modifi...	Description	Enterprise Pro...	Operation
test.[redacted].c...	H[redacted] Clo...	2	--	hwclouds.cs@...	300	May 22, 2024 1...	May 22, 2024 1...	--	default	Manage Record Set Check Domain Name Disable More
dan[redacted].c...	Hu[redacted] Clo...	11	--	hwclouds.cs@...	300	May 09, 2024 ...	May 09, 2024 ...	Domain Name ...	default	Manage Record Set Check Domain Name Disable More

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 3-10 Modify Record Set



Modify Record Set

Name: www.example .dns.418lab.cn

Type: CNAME – Map one domain to another

Alias: ○ Yes ● No

Line: Default

* TTL (s): 300

* Value: c992a2e324aa48dcaffaffeccfe6[redacted]com

Enter the domain name you want to resolve when the value in the Name field is queried.
Example:
www.example.com

Weight: 1

The proportion of DNS queries that will be routed to the record set. If a resolution line in a zone contains multiple record sets of the same type, you can specify a different weight for each record set.
View details

Description:

0/255

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

To prevent other users from configuring your domain names on WAF in advance (this will cause interference on your domain name protection), add the subdomain name and TXT record on your DNS management platform.

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.

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**.

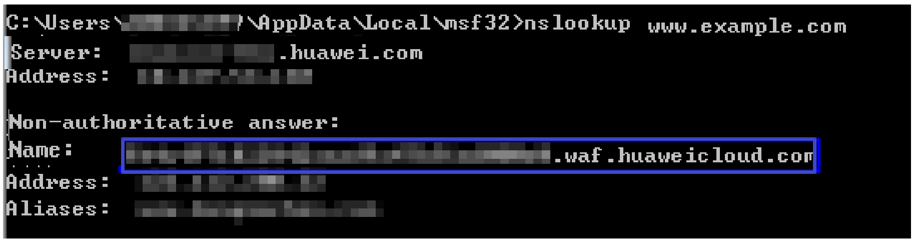
Step 2 Run a **nslookup** command to query the CNAME record.

If the configured CNAME record is returned, the configuration is successful. An example command response is displayed in **Figure 3-11**.

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

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

Figure 3-11 Querying the CNAME



```
C:\Users\[redacted]\AppData\Local\msf32>nslookup www.example.com
Server:  [redacted].huawei.com
Address:  [redacted]

Non-authoritative answer:
Name:    [redacted].waf.huaweicloud.com
Address:  [redacted]
Aliases:  [redacted]
```

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

----End

Step 5: Verify Website Access

- Check the access status.

  Generally, if you have performed domain connection and **Access Status** is **Accessible**, the domain name is connected to WAF.

> NOTE
>
> If the domain name has been connected to WAF but its **Access Status** is still **Inaccessible**, click ⟳ to refresh the status. If the status is still **Inaccessible**, fix the issue by referring to **Why My Domain Name Is Inaccessible?**

- Check the website accessibility.
  - Enter the domain name in the address bar of your browser and check whether the website is accessible.

    > NOTE
    >
    > If a non-standard port 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?**

  - Simulate simple web attack commands and check whether WAF protection takes effect. For details, see **Step 4.2**.

Follow-up Operations

After adding a domain name to WAF, you need to:

- **Complete Recommended Configurations**
- Adjust the protection policy configured for the protected domain name based on protection requirements. For details, see **Protection Configuration Overview**.

3.2.2 Example Configuration

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

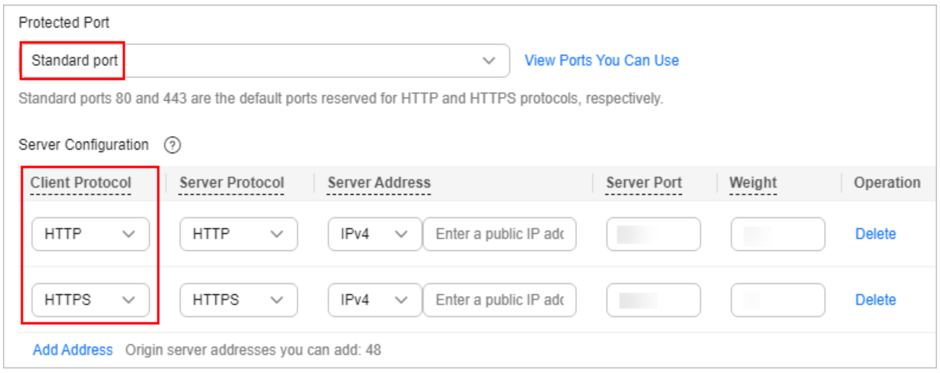
- **Example 1: Configuring Service Protection for Port 80/443**
- **Example 2: Forwarding Client Requests to Different Origin Servers**
- **Example 3: Protection for One Domain Name with Different Protected Ports**
- **Example 4: Configuring Protocols for Different Access Methods**

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 3-12**.

Figure 3-12 Protection for both ports 80 and 443



Protected Port

Standard port

View Ports You Can Use

Standard ports 80 and 443 are the default ports reserved for HTTP and HTTPS protocols, respectively.

Server Configuration

Client Protocol	Server Protocol	Server Address	Server Port	Weight	Operation
HTTP	HTTP	IPv4 Enter a public IP adc			Delete
HTTPS	HTTPS	IPv4 Enter a public IP adc			Delete

Add Address Origin server addresses you can add: 48

NOTE

- In **Figure 3-12**, 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.

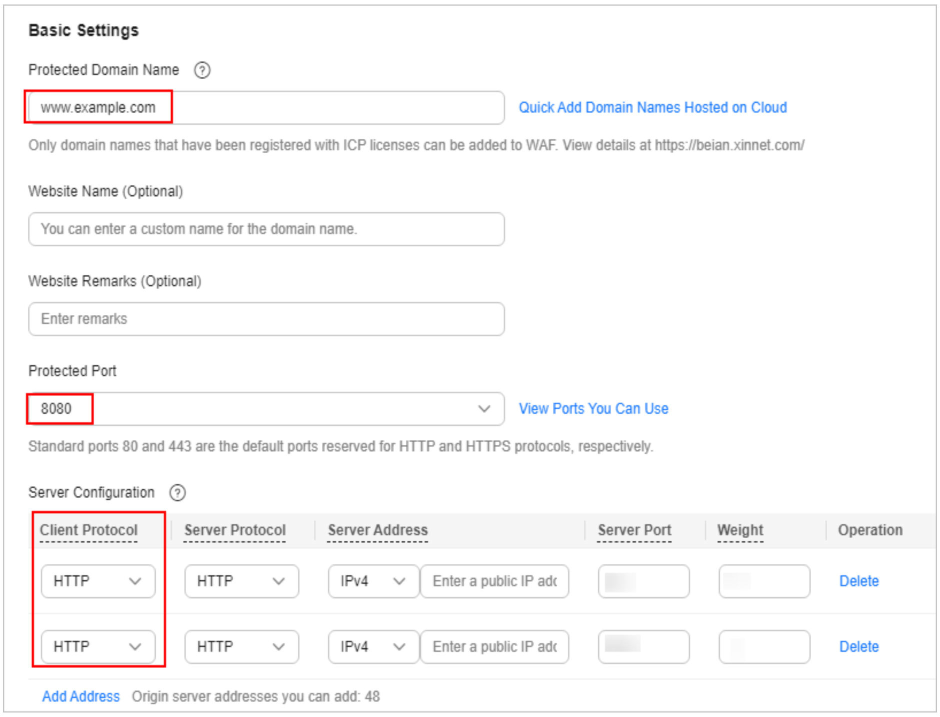
Example 2: Forwarding Client Requests to Different Origin Servers

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**: SecMaster 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 3-13 Forwarding client requests to different origin servers



Basic Settings

Protected Domain Name

www.example.com

Quick Add Domain Names Hosted on Cloud

Only domain names that have been registered with ICP licenses can be added to WAF. View details at https://beian.xinnet.com/

Website Name (Optional)

You can enter a custom name for the domain name.

Website Remarks (Optional)

Enter remarks

Protected Port

8080

View Ports You Can Use

Standard ports 80 and 443 are the default ports reserved for HTTP and HTTPS protocols, respectively.

Server Configuration

Client Protocol	Server Protocol	Server Address	Server Port	Weight	Operation
HTTP	HTTP	IPv4 Enter a public IP adc			Delete
HTTP	HTTP	IPv4 Enter a public IP adc			Delete

Add Address Origin server addresses you can add: 48

NOTE

- In **Figure 3-13**, 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.

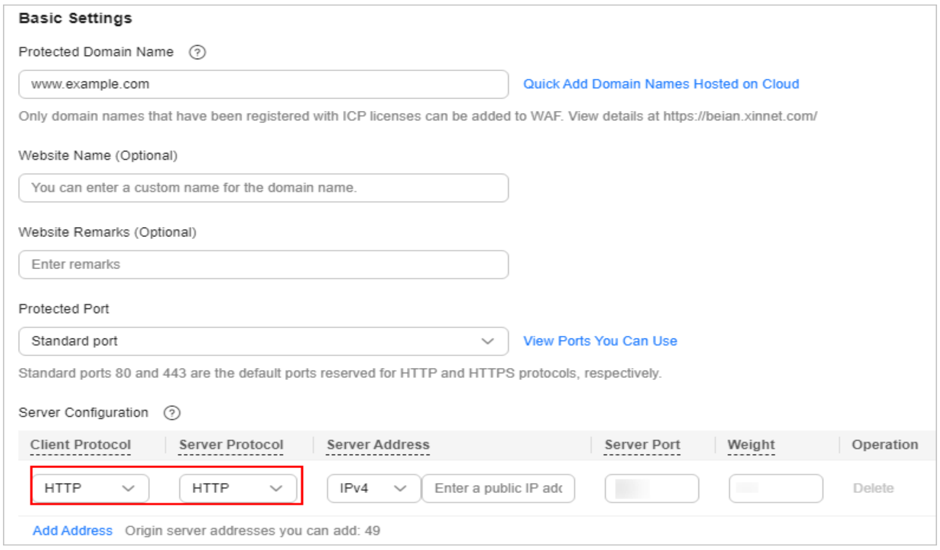
Example 4: Configuring Protocols for Different Access Methods

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 3-14**.

  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 3-14 HTTP forwarding



Basic Settings

Protected Domain Name

www.example.com — Quick Add Domain Names Hosted on Cloud

Only domain names that have been registered with ICP licenses can be added to WAF. View details at https://beian.xinnet.com/

Website Name (Optional)

You can enter a custom name for the domain name.

Website Remarks (Optional)

Enter remarks

Protected Port

Standard port — View Ports You Can Use

Standard ports 80 and 443 are the default ports reserved for HTTP and HTTPS protocols, respectively.

Server Configuration

Client Protocol	Server Protocol	Server Address		Server Port	Weight	Operation
HTTP	HTTP	IPv4	Enter a public IP adc			Delete

Add Address Origin server addresses you can add: 49

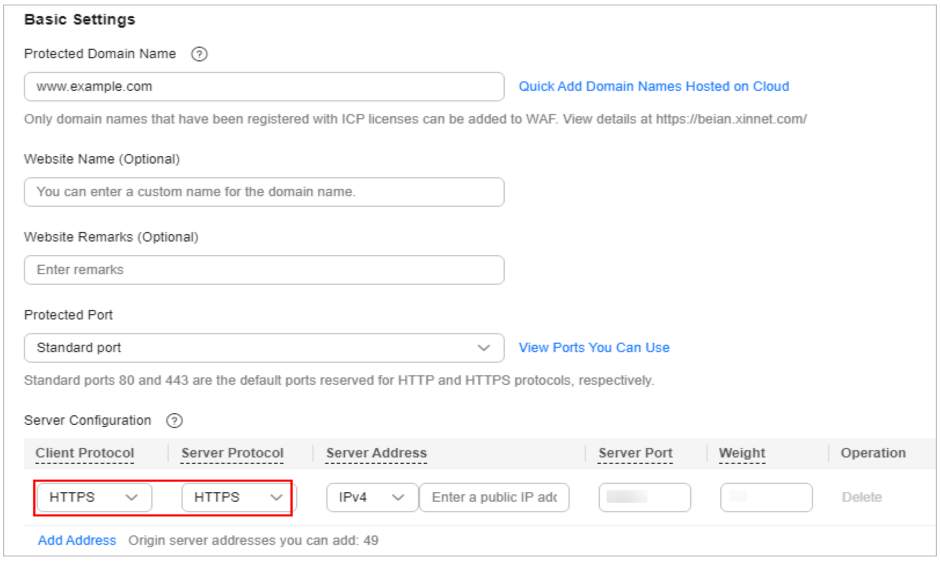
NOTICE

- In **Figure 3-14**, 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 3-15**. 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 3-15 HTTPS redirection



Basic Settings

Protected Domain Name

www.example.com

Quick Add Domain Names Hosted on Cloud

Only domain names that have been registered with ICP licenses can be added to WAF. View details at https://beian.xinnet.com/

Website Name (Optional)

You can enter a custom name for the domain name.

Website Remarks (Optional)

Enter remarks

Protected Port

Standard port

View Ports You Can Use

Standard ports 80 and 443 are the default ports reserved for HTTP and HTTPS protocols, respectively.

Server Configuration

Client Protocol	Server Protocol	Server Address		Server Port	Weight	Operation
HTTPS	HTTPS	IPv4	Enter a public IP adc			Delete

Add Address Origin server addresses you can add: 49

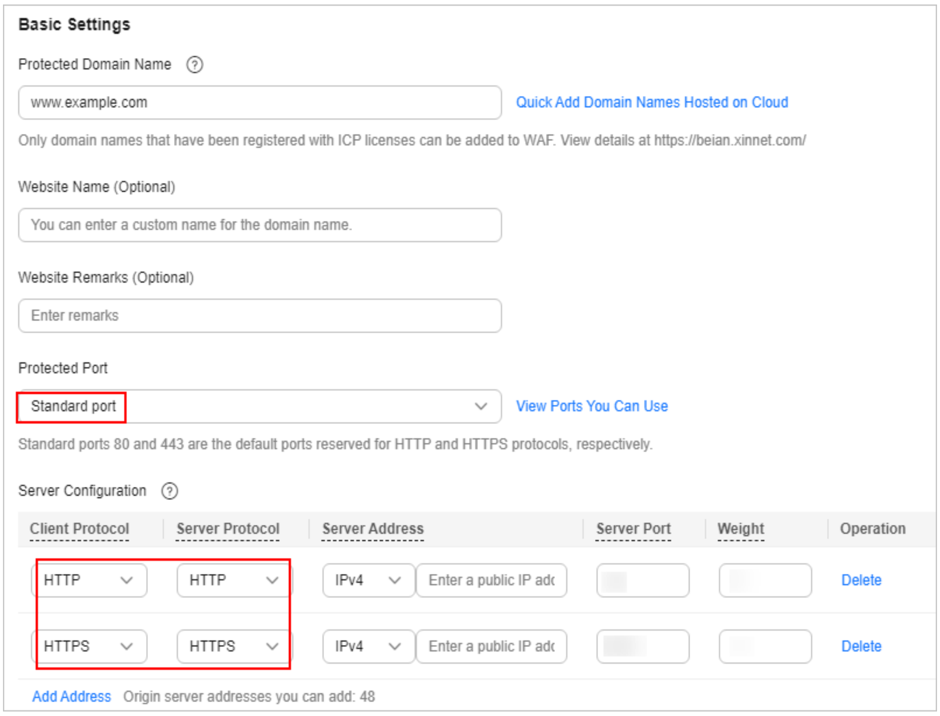
NOTICE

- In **Figure 3-15**, 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 3-16**.

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

Figure 3-16 HTTP and HTTPS forwarding



Basic Settings

Protected Domain Name: www.example.com

Quick Add Domain Names Hosted on Cloud

Only domain names that have been registered with ICP licenses can be added to WAF. View details at https://beian.xinnet.com/

Website Name (Optional): You can enter a custom name for the domain name.

Website Remarks (Optional): Enter remarks

Protected Port: Standard port

View Ports You Can Use

Standard ports 80 and 443 are the default ports reserved for HTTP and HTTPS protocols, respectively.

Server Configuration

Client Protocol	Server Protocol	Server Address		Server Port	Weight	Operation
HTTP	HTTP	IPv4	Enter a public IP adc			Delete
HTTPS	HTTPS	IPv4	Enter a public IP adc			Delete

Add Address   Origin server addresses you can add: 48

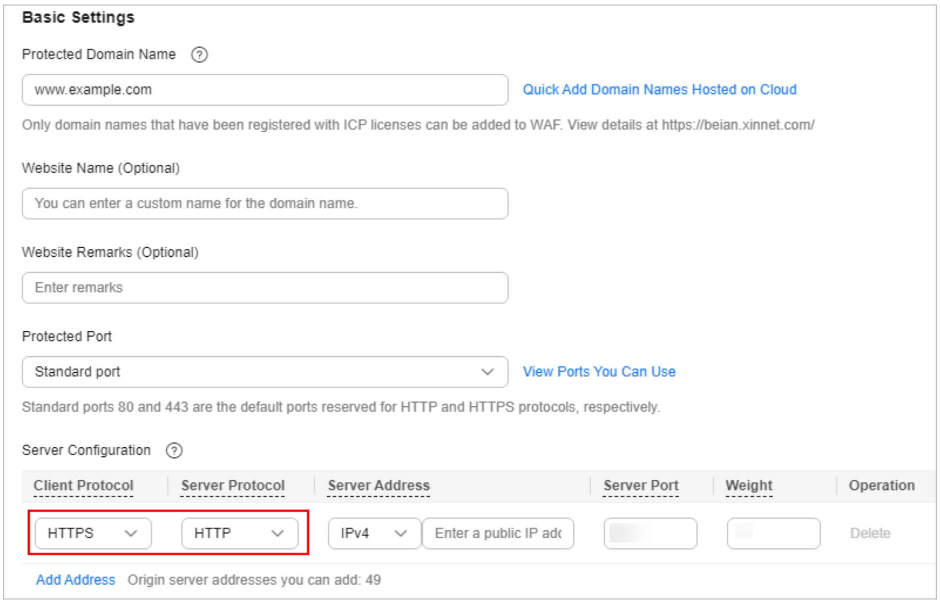
NOTICE

- In **Figure 3-16**, 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 3-17**.

  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 3-17 HTTPS offloading



Basic Settings

Protected Domain Name

www.example.com

Quick Add Domain Names Hosted on Cloud

Only domain names that have been registered with ICP licenses can be added to WAF. View details at https://beian.xinnet.com/

Website Name (Optional)

You can enter a custom name for the domain name.

Website Remarks (Optional)

Enter remarks

Protected Port

Standard port

View Ports You Can Use

Standard ports 80 and 443 are the default ports reserved for HTTP and HTTPS protocols, respectively.

Server Configuration

Client Protocol	Server Protocol	Server Address		Server Port	Weight	Operation
HTTPS	HTTP	IPv4	Enter a public IP adc			Delete

Add Address Origin server addresses you can add: 49

NOTICE

- In **Figure 3-17**, 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 (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.

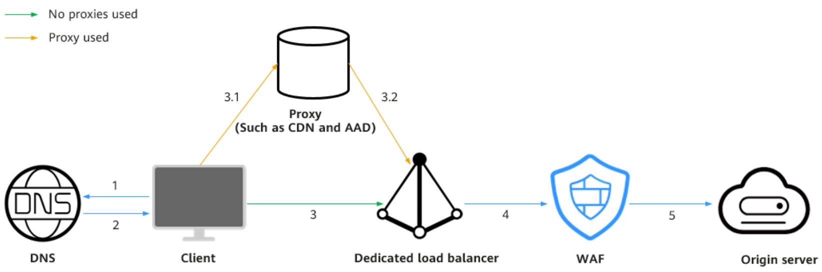
NOTE

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.

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 3-18** shows how your website traffic is forwarded when WAF is used.

Figure 3-18 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.

Procedure	Description
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 WAF instance**.
- 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).
- 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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner and choose **Web Application Firewall** under **Security**.

Step 4 In the navigation pane, choose **Website Settings**.

Step 5 In the upper left corner of the website list, click **Add Website**.

Step 6 Select **Dedicated Mode** and click **Configure Now**.

Step 7 , including domain name and origin server settings. For details about the parameters, see **Table 3-6**.

Table 3-6 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.	-
Website Name	Website name you specify.	WAF
Website Remarks	Remarks of the website.	waftest

Paramete r	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	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 and WebSockets requests, which 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), it is recommended that at least two WAF instances be configured 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. ● **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**, an SSL certificate is required. ● 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?** ● 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
Proxy Your Website Uses	● **Layer-7 proxy**: Web proxy products for layer-7 request forwarding are used, products such as anti-DDoS, CDN, and other cloud acceleration services. ● **Layer-4 proxy**: Web proxy products for layer-4 forwarding are used, products such as anti-DDoS. ● **No proxy**: No proxy products are used for the website. NOTICE If your website uses a proxy, select **Layer-7 proxy**. 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 8 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 9 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 health check, see **Configuring a Health Check**.

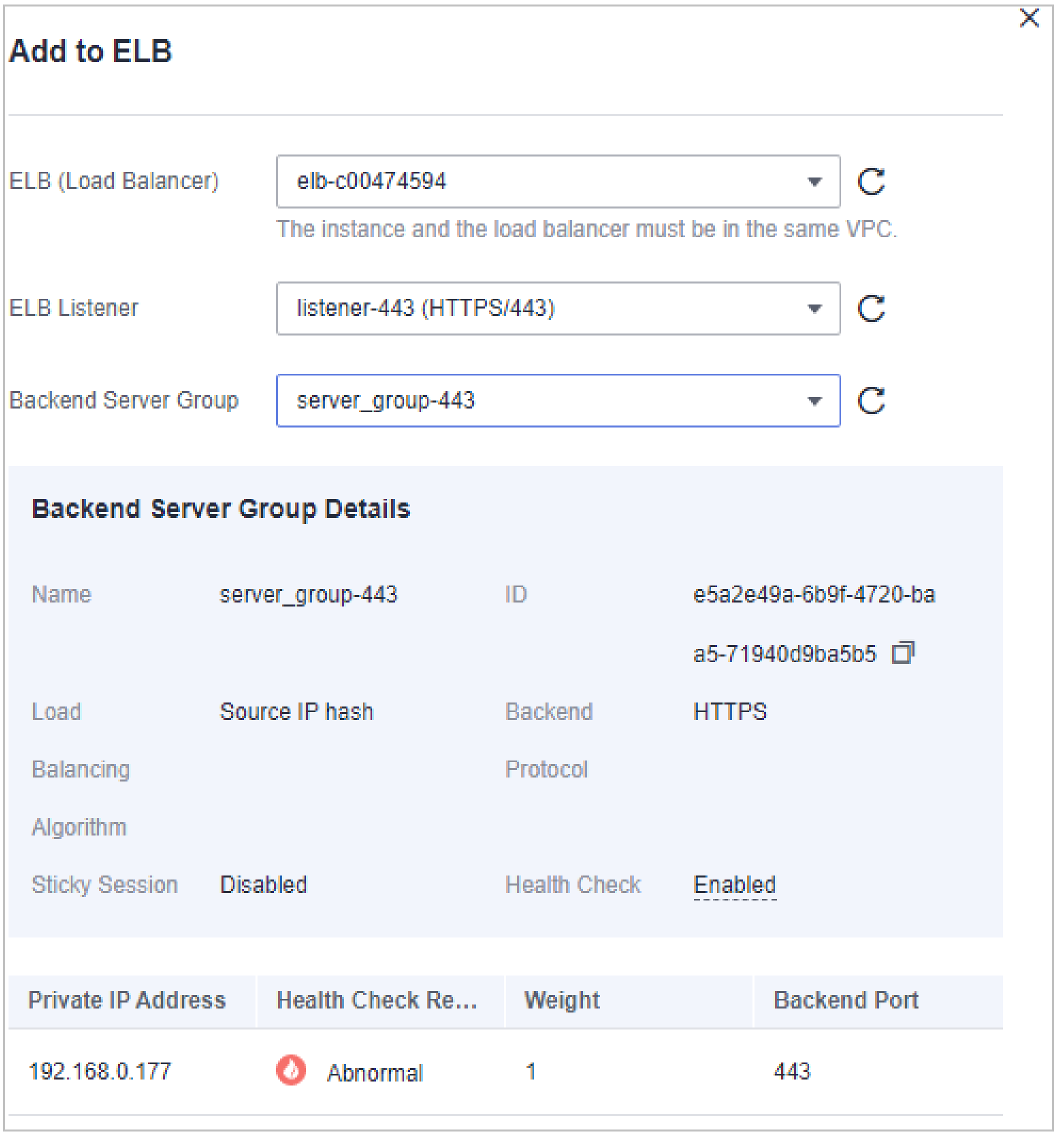
Step 2 Click ☰ in the upper left corner and choose **Web Application Firewall** under **Security**.

Step 3 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.

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

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

Figure 3-19 Add to ELB



Add to ELB

ELB (Load Balancer): elb-c00474594
The instance and the load balancer must be in the same VPC.

ELB Listener: listener-443 (HTTPS/443)

Backend Server Group: server_group-443

Backend Server Group Details

Name	server_group-443	ID	e5a2e49a-6b9f-4720-baa5-71940d9ba5b5
Load Balancing Algorithm	Source IP hash	Backend Protocol	HTTPS
Sticky Session	Disabled	Health Check	Enabled

Private IP Address	Health Check Re...	Weight	Backend Port
192.168.0.177	Abnormal	1	443

NOTICE

The **Health Check** result must be **Healthy**, or the website requests cannot be pointed to WAF.

Step 6 Click **Confirm**. Then, configure service port for the WAF instance, and **Backend Port** must be set to the 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.

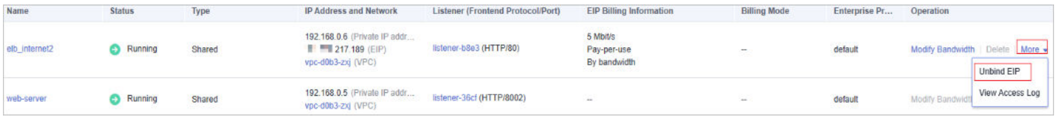
This topic describes how to unbind an EIP from your origin server and bind the EIP to a load balancer configured for a dedicated WAF instance.

Step 1 Click ☰ in the upper left corner of the page and choose **Elastic Load Balance** under **Network** to go to the **Load Balancers** page.

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 3-20 Unbinding an EIP



Name	Status	Type	IP Address and Network	Listener (Frontend Protocol/Port)	EIP Billing Information	Billing Mode	Enterprise Pr...	Operation
elb_internet2	Running	Shared	192.168.0.6 (Private IP addr... [redacted] 217.189 (EIP) vpc-d0b3-zxj (VPC)	listener-b8e3 (HTTP/80)	5 Mbit/s Pay-per-use By bandwidth	--	default	Modify Bandwidth | Delete | More
web-server	Running	Shared	192.168.0.5 (Private IP addr... vpc-d0b3-zxj (VPC)	listener-36cf (HTTP/8002)	--	--	default	Modify Bandwidth

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.

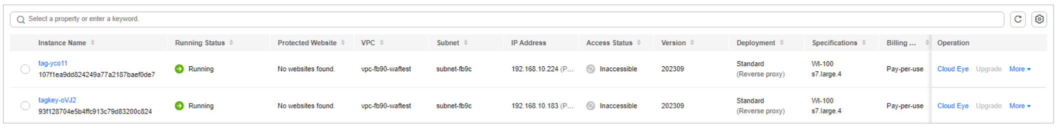
Pointing Traffic to an ECS Hosting Your Website

If your origin server is deployed on an ECS, 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 server.

Step 1 Click ☰ in the upper left corner and choose **Security** > **Web Application Firewall**.

Step 2 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.

Figure 3-21 Dedicated engine list



Select a property or enter a keyword.

	Instance Name	Running Status	Protected Website	VPC	Subnet	IP Address	Access Status	Version	Deployment	Specifications	Billing ...	Operation
○	tag-yco11 107f1ea9dd824249a77a2187baef0de7	Running	No websites found.	vpc-fb90-waftest	subnet-fb9c	192.168.10.224 (P...	Inaccessible	202309	Standard (Reverse proxy)	WI-100 s7.large.4	Pay-per-use	Cloud Eye Upgrade More ▾
○	tagkey-oVJ2 93f128704e5b4ffc913c79d83200c824	Running	No websites found.	vpc-fb90-waftest	subnet-fb9c	192.168.10.183 (P...	Inaccessible	202309	Standard (Reverse proxy)	WI-100 s7.large.4	Pay-per-use	Cloud Eye Upgrade More ▾

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

Step 4 Click ☰ in the upper left corner of the page 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.

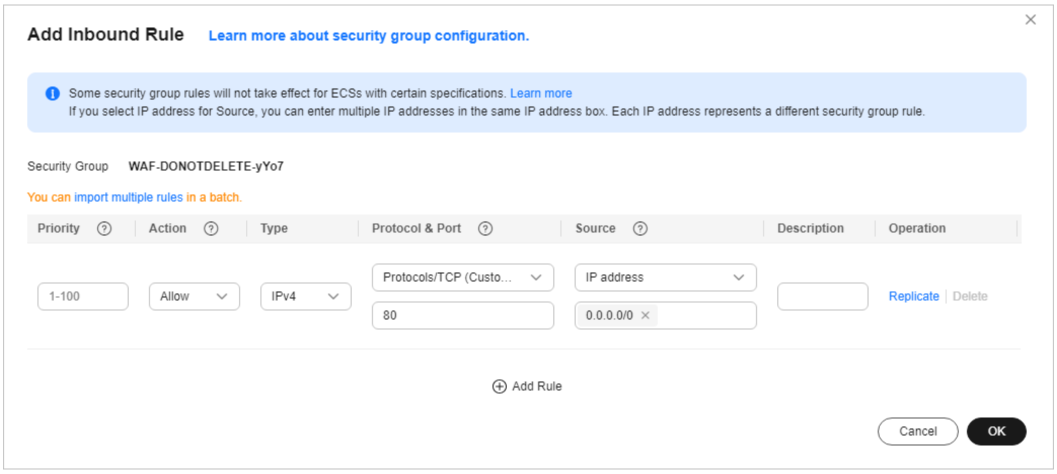
Step 6 Click the **Security Groups** tab. Then, click **Change Security Group**.

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 3-7**.

Figure 3-22 Add Inbound Rule



Add Inbound Rule Learn more about security group configuration.

Some security group rules will not take effect for ECSs with certain specifications. Learn more
If you select IP address for Source, you can enter multiple IP addresses in the same IP address box. Each IP address represents a different security group rule.

Security Group WAF-DONOTDELETE-yYo7

You can import multiple rules in a batch.

Priority	Action	Type	Protocol & Port	Source	Description	Operation
1-100	Allow	IPv4	Protocols/TCP (Custo... 80	IP address 0.0.0.0/0 ×		Replicate | Delete

Table 3-7 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 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:

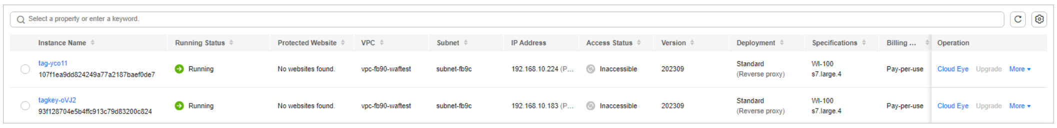
Step 1 Log in to the management console.

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

Step 3 Click ☰ in the upper left corner and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.

Figure 3-23 Dedicated engine list



Select a property or enter a keyword.

	Instance Name	Running Status	Protected Website	VPC	Subnet	IP Address	Access Status	Version	Deployment	Specifications	Billing ...	Operation
○	tag-yco11 107f1ea9dd824249a77a2187baef0de7	Running	No websites found.	vpc-fb90-waftest	subnet-fb9c	192.168.10.224 (P...	Inaccessible	202309	Standard (Reverse proxy)	WI-100 s7.large.4	Pay-per-use	Cloud Eye Upgrade More ▾
○	tagkey-oVJ2 93f128704e5b4ffc913c79d83200c824	Running	No websites found.	vpc-fb90-waftest	subnet-fb9c	192.168.10.183 (P...	Inaccessible	202309	Standard (Reverse proxy)	WI-100 s7.large.4	Pay-per-use	Cloud Eye Upgrade More ▾

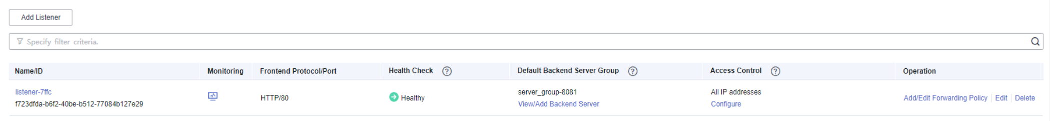
Step 5 In the **IP Address** column, obtain the IP address of each dedicated WAF instance under your account.

Step 6 Click ☰ in the upper left corner of the page and choose **Networking** > **Elastic Load Balance**.

Step 7 Locate the row containing the load balancer configured for your dedicated WAF instance and click the load balancer name in the **Name** column.

Step 8 In the **Access Control** row of the target listener, click **Configure**.

Figure 3-24 Listener list



Name/ID	Monitoring	Frontend Protocol/Port	Health Check	Default Backend Server Group	Access Control	Operation
listener-7ffc f723dfda-b6f2-40be-b512-77084b127e29		HTTP/80	Healthy	server_group-8081 View/Add Backend Server	All IP addresses Configure	Add/Edit Forwarding Policy | Edit | Delete

Step 9 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 5** to the group being created.
2. Select the IP address group created in **Step 9.1** from the **IP Address Group** drop-down list.

Step 10 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.

- 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

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

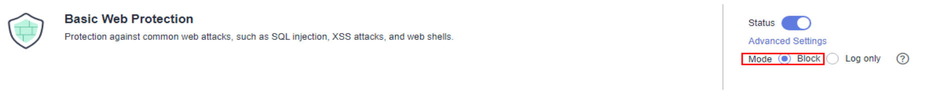
  Example:

  ```
  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.

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



Basic Web Protection

Protection against common web attacks, such as SQL injection, XSS attacks, and web shells.

Status

Advanced Settings

Mode ● Block ○ Log only

  b. Run the following command:

     ```
     curl -kv -H "Host: { protection 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: { protection 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

- The initial **Access Status** of a website is **Unaccessed**. When a request reaches the WAF instance configured for the website, the access status automatically changes to **Accessed**. To address access failure, see **Why Is the Access Status of a Domain Name or IP Address Inaccessible?**
- **Complete Recommended Configurations**
- Adjust the protection policy configured for the protected domain name based on protection requirements. For details, see **Protection Configuration Overview**.

3.4 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.

Standard Ports

WAF can protect the following standard ports.

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

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 3-8 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, 5000, 7009, 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, 8999, 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, 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, 1135, 1139, 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, 18080, 18180, 18280, 19101, 19501, 21028, 23333, 27777, 28080, 30002, 30086, 33332, 33334, 33702, 40010, 48299, 48800, 52725, 52726, 60008, 60010	447, 882, 1818, 4006, 4430, 4443, 5048, 5049, 5100, 5443, 6443, 7072, 7073, 7443, 8033, 8043, 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, 9005, 9053, 9090, 9443, 9553, 9663, 9681, 9682, 9999, 10002, 10300, 10301, 11001, 11003, 13001, 13003, 13080, 14003, 14443, 17618, 17718, 17818, 18000, 18001, 18010, 18110, 18381, 18443, 18980, 19000, 20000, 28443, and 60009

Edition	Non-standard Port That Can Be Protected	
	HTTP	HTTPS
Platinum	81, 82, 83, 84, 85, 86, 87, 88, 89, 97, 133, 134, 140, 141, 144, 151, 800, 808, 881, 888, 1000, 1090, 1135, 1139, 1688, 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, 18180, 18280, 23333, 27777, 28080, 30086, 33702, 48299, 48800	447, 882, 1818, 4006, 4430, 4443, 5048, 5049, 5443, 6443, 7072, 7073, 7443, 8033, 8043, 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, 9005, 9053, 9090, 9182, 9184, 9190, 9443, 9553, 9663, 9681, 9682, 9999, 10002, 10300, 10301, 11001, 11003, 13001, 13003, 13080, 14003, 17618, 17718, 17818, 18000, 18001, 18010, 18110, 18381, 18443, 18980, 19000, 28443, and 60009

Dedicated Mode

If you use dedicated WAF instances, you can select any non-standard ports listed in **Table 3-9**.

Table 3-9 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, 60008, 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, 19000, and 28443

4 Viewing Protection Events

4.1 Querying a Protection Event

On the **Events** page, you can view events generated for blocked attacks and logged-only attacks. You can view details of events generated by WAF, including the occurrence time, attack source IP address, geographic location of the attack source IP address, malicious load, and hit rule for an event.

Prerequisites

The website you want to protect has been connected to WAF.

Constraints

- On the WAF console, you can view the event data for all protected domain names over the last 30 days.
- 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.
- If the security software installed on your server blocks the event file from being downloaded, close the software and download the file again.

Viewing Protection Event 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.

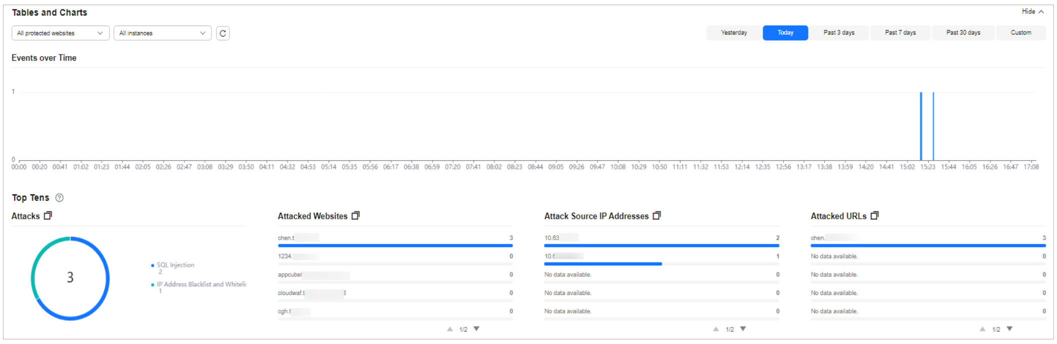
Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Events**.

Step 5 Click the **Search** tab. In the website or instance drop-down list, select a website to view corresponding event logs. The query time can be **Yesterday**, **Today**, **Past 3 days**, **Past 7 days**, **Past 30 days**, or a time range you configure.

- **Events over Time**: displays the WAF protection status of the selected website within the selected time range.
- **Top Tens**: displays top 10 attacks, attacked websites, attack source IP addresses, and attacked URLs for a selected time range. You can click ❐ to copy the data in the corresponding chart.

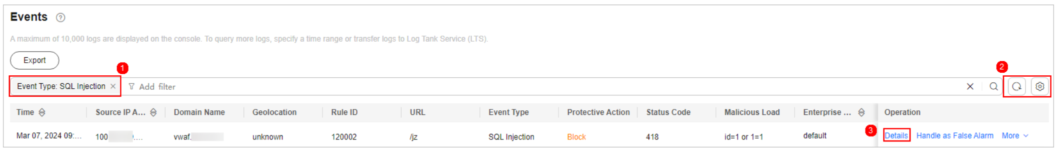
Figure 4-1 Events



Step 6 In the **Events** area, view the event details.

- Configure a filter by combining several conditions. Then, click **OK**. Conditions will be displayed above the event list. Table 4-2 lists parameters for filter conditions.
- In the upper left corner of the event list, click **Export** to export events. A maximum of 200 events can be exported once.
- Click ⚙ to select fields you want to display in the event lists.
- To view event details, locate the row containing the event and click **Details** in the **Operation** column.

Figure 4-2 Events



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).

Export

1 Event Type: SQL Injection × Add filter

2

Time	Source IP A...	Domain Name	Geolocation	Rule ID	URL	Event Type	Protective Action	Status Code	Malicious Load	Enterprise ...	Operation
Mar 07, 2024 09:...	100....	vwaf.	unknown	120002	/jz	SQL Injection	Block	418	id=1 or 1=1	default	3 Details Handle as False Alarm More

Table 4-1 Filter condition fields

Parameter	Description
Event ID	ID of the event.
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.
Rule ID	ID of a built-in protection rule in WAF basic web protection.

Parameter	Description
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**.
Source 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.
URL	Attacked URL.

Table 4-2 Parameters in the event list

Parameter	Description	Example Value
Time	When the attack occurred.	2021/02/04 13:20:04
Source IP Address	Public IP address of the web visitor/attacker.	-
Domain Name	Attacked domain name.	www.example.com
Geolocation	Location where the IP address of the attack originates from.	-
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

Parameter	Description	Example Value
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

----End

4.2 Handling False Alarms

If you confirm that an attack event on the **Events** page is a false alarm, you can handle the event as false alarm by ignoring the URL and rule ID in basic web protection, or by deleting or disabling the corresponding protection rule you configured. You can also add the attack source IP addresses to a whitelist or blacklist to handle the false alarm. After an attack event is handled as a false alarm, the event will not be displayed on the **Events** page anymore. You will no longer receive any alarm notifications about the events of this kind.

WAF detects attacks by using built-in basic web protection rules, built-in features in anti-crawler protection, and custom rules you configured (such as CC attack protection, precise access protection, blacklist, whitelist, and geolocation access control rules). WAF will respond to detected attacks based on the protective actions (such as **Block** and **Log only**) defined in the rules and display attack events on the **Events** page.

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 handle false alarms in the project.

Prerequisites

There is at least one false alarm event in the event list.

Constraints

- Only attack events blocked or recorded by built-in basic web protection rules and features in anti-crawler protection can be handled as false alarms.
- For events generated based on custom rules (such as a CC attack protection rule, precise protection rule, blacklist rule, whitelist rule, or geolocation access control rule), they cannot be handled as false alarms. To ignore such an event, delete or disable the custom rule hit by the event.
- An attack event can only be handled as a false alarm once.
- After an attack event is handled as a false alarm, the attack event will not be displayed on the **Events** page. You will no longer receive any alarm notifications about the events of this kind.
- Dedicated WAF instances earlier than June 2022 do not support **All protection** for **Ignore WAF Protection**. Only **Basic web protection** can be selected.

Application Scenarios

Sometimes normal service requests may be blocked by WAF. For example, suppose you deploy a web application on an ECS and then add the public domain name associated with that application to WAF. If you enable basic web protection for that application, WAF may block the access requests that match the basic web protection rules. As a result, the website cannot be accessed through its domain name. However, the website can still be accessed through the IP address. In this case, you can handle the false alarms to allow normal access requests to the application.

Handling False Alarms

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 **Security** > **Web Application Firewall**.

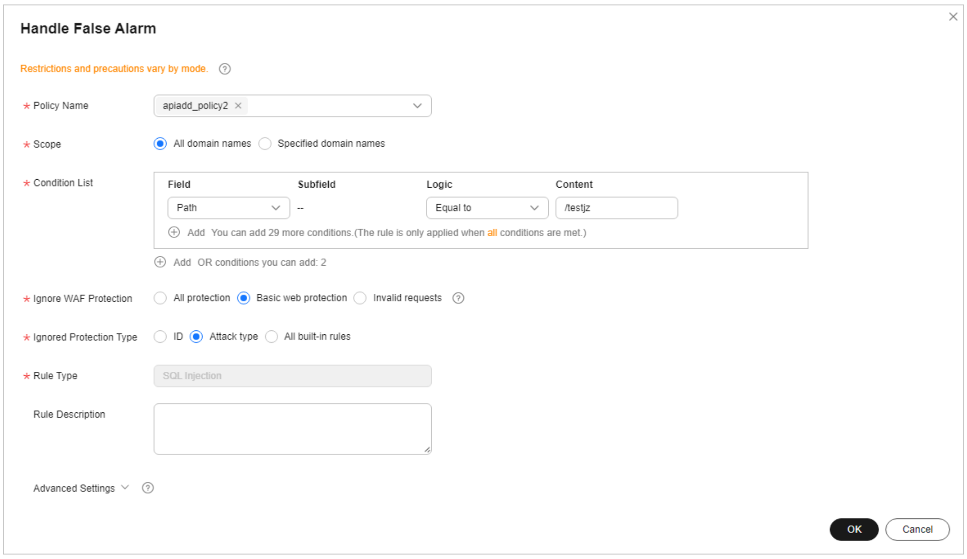
Step 4 In the navigation pane on the left, choose **Events**.

Step 5 Click the **Search** tab. In the website or instance drop-down list, select a website to view corresponding event logs. The query time can be **Yesterday**, **Today**, **Past 3 days**, **Past 7 days**, **Past 30 days**, or a time range you configure.

Step 6 In the event list, handle events.

- If you confirm that an event is a false alarm, locate the row containing the event. In the **Operation** column, click **Handle as False Alarm** and handle the hit rule.

Figure 4-3 Handling a false alarm



Handle False Alarm

Restrictions and precautions vary by mode.

* Policy Name: apiadd_policy2

* Scope: ● All domain names ○ Specified domain names

* Condition List

Field	Subfield	Logic	Content
Path	--	Equal to	/testjz

Add You can add 29 more conditions.(The rule is only applied when all conditions are met.)

Add OR conditions you can add: 2

* Ignore WAF Protection: ○ All protection ● Basic web protection ○ Invalid requests

* Ignored Protection Type: ○ ID ● Attack type ○ All built-in rules

* Rule Type: SQL Injection

Rule Description

Advanced Settings

Table 4-3 Parameters

Parameter	Description	Example Value
Scope	– **All domain names**: By default, this rule will be used 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.	www.example.com

Parameter	Description	Example Value
Condition List	Click **Add** 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. A condition includes the following parameters: Parameters for configuring a condition are described as follows: – **Field** – **Subfield**: Configure this field only when **Params**, **Cookie**, or **Header** is selected for **Field**. **NOTICE** The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed. – **Logic**: Select a logical relationship from the drop-down list. – **Content**: Enter or select the content that matches the condition.	Path, Include, /product

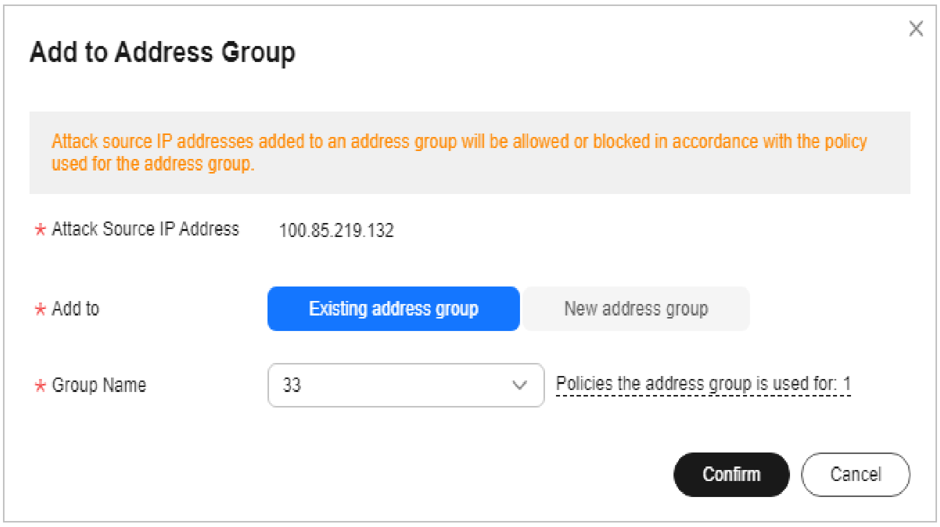
Parameter	Description	Example Value
Ignore WAF Protection	– **All protection**: All WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule. – **Basic web protection**: You can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, 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 Protection Type**, specify the following parameters: – **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 attack events of 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

- Add the source IP address to an address group. Locate the row containing the desired event, in the **Operation** column, click **More** > **Add to Address Group**. The source IP address triggering the event will be blocked or allowed based on the policy used for the address group.

  Add to: You can select an existing address group or create an address group.

Figure 4-4 Add to Address Group



Add to Address Group

Attack source IP addresses added to an address group will be allowed or blocked in accordance with the policy used for the address group.

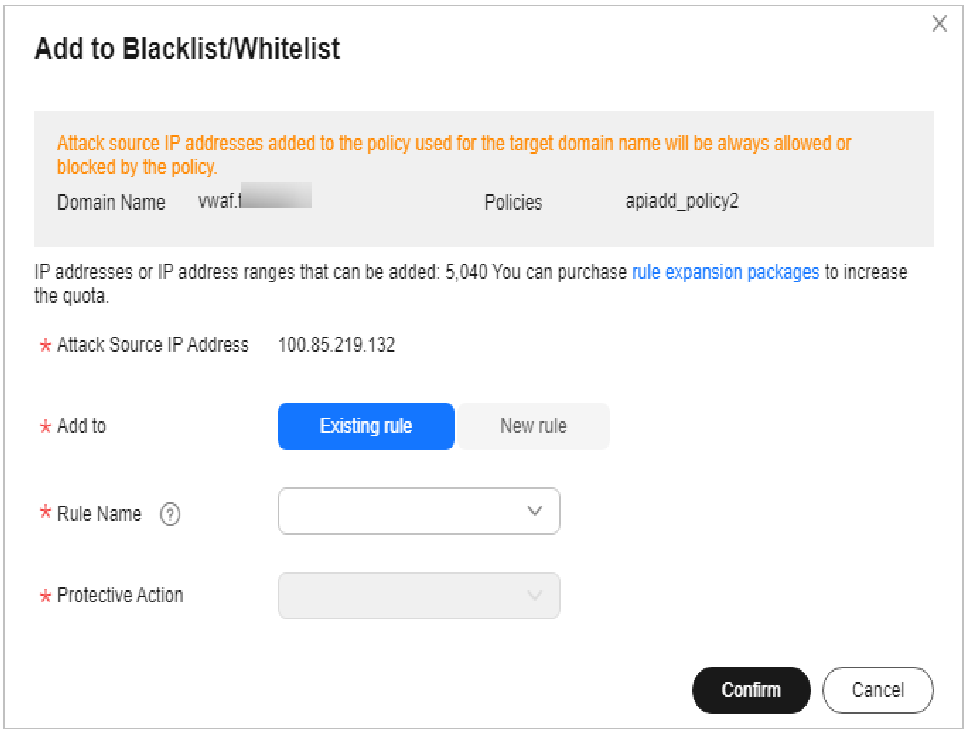
* Attack Source IP Address: 100.85.219.132

* Add to: Existing address group | New address group

* Group Name: 33 — Policies the address group is used for: 1

- Add the source IP address to a blacklist or whitelist rule of the corresponding protected domain name. Locate the row containing the desired event. In the **Operation** column, click **More** > **Add to Blacklist/Whitelist**. Then, the source IP address will be blocked or allowed based on the protective action configured in the blacklist or whitelist rule.

Figure 4-5 Add to Blacklist/Whitelist



Add to Blacklist/Whitelist

Attack source IP addresses added to the policy used for the target domain name will be always allowed or blocked by the policy.

Domain Name: vwaf.[redacted]   Policies: apiadd_policy2

IP addresses or IP address ranges that can be added: 5,040 You can purchase rule expansion packages to increase the quota.

* Attack Source IP Address: 100.85.219.132

* Add to: Existing rule | New rule

* Rule Name:

* Protective Action:

Table 4-4 Parameter descriptions

Parameter	Description
Add to	– Existing rule – New 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	This parameter is mandatory when you select **New rule** for **Add to**. You can select **IP address/Range** or **Address Group** to add IP addresses a blacklist or whitelist rule.
Group Name	This parameter is mandatory when you select **Address group** for **IP Address/Range/Group**. Select an address group from the drop-down list. You can also click **New address group** to create an address group. For details, see **Adding an IP Address Group**.
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.
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 IP address, Cookie, or Params for a length of time configured as part of the rule.
Rule Description	A brief description of the rule. This parameter is optional.

----End

Verification

A false alarm will be deleted within about a minute after the handling configuration is done. It will no longer be displayed in the attack event details list. You can refresh the browser cache and access the page for which the global whitelist rule is configured again to 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**.

4.3 Downloading Events Data

This topic describes how to download events (logged and blocked events) data for the last five days. One or more CSV files containing the event data of the current day will be generated at the beginning of the next day.

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 download protection event logs in the project.

Prerequisites

- **The website you want to protect has been connected to WAF.**
- An event file has been generated.

Specification Limitations

- Each file can include a maximum of 5,000 events. If there are more than 5,000 events, another file is generated.
- Only event data for the last five days can be downloaded through the WAF console.

Downloading Events Data

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 **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Events**.

Step 5 Click the **Downloads** tab and download the desired protection data. **Table 4-5** describes the parameters.

Table 4-5 Parameter description

Parameter	Description
File Name	The format is *file-name*.**csv**.

Parameter	Description
Number of Events	Total number of blocked and logged events **NOTE** Each file can include a maximum of 5,000 events. If there are more than 5,000 events, another file is generated.

Step 6 In the **Operation** column, click **Download** to download data to the local PC.

----End

Fields in a Protection Event Data File

Field	Description	Example Value
action	Protective action taken in response to the event	block
attack	Attack type	SQL Injection
body	Request content of the attack	N/A
cookie	Cookie of the attacker	N/A
headers	Header of the attacker	N/A
host	Domain name or IP address of the protected website	www.example.com
id	ID of the event.	02-11-16-20201121060347-feb42002
payload	The part of the attack that causes damage to the protected website	python-requests/2.20.1
payload_location	The location of the attack that causes damage or the number of times that the URL is accessed by the attacker	user-agent
policyid	Policy ID.	d5580c8f6cd4403ebbf85892d4bbb8e4
request_line	Request line of the attack	GET /
rule	ID of the rule against which the event is generated.	81066
sip	Public IP address of the web visitor/attacker	N/A

Field	Description	Example Value
time	When the event occurred.	2020/11/21 0:20:44
url	URL of the protected domain name	N/A

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**
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**
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**

Protection Rule	Description	Reference
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**

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

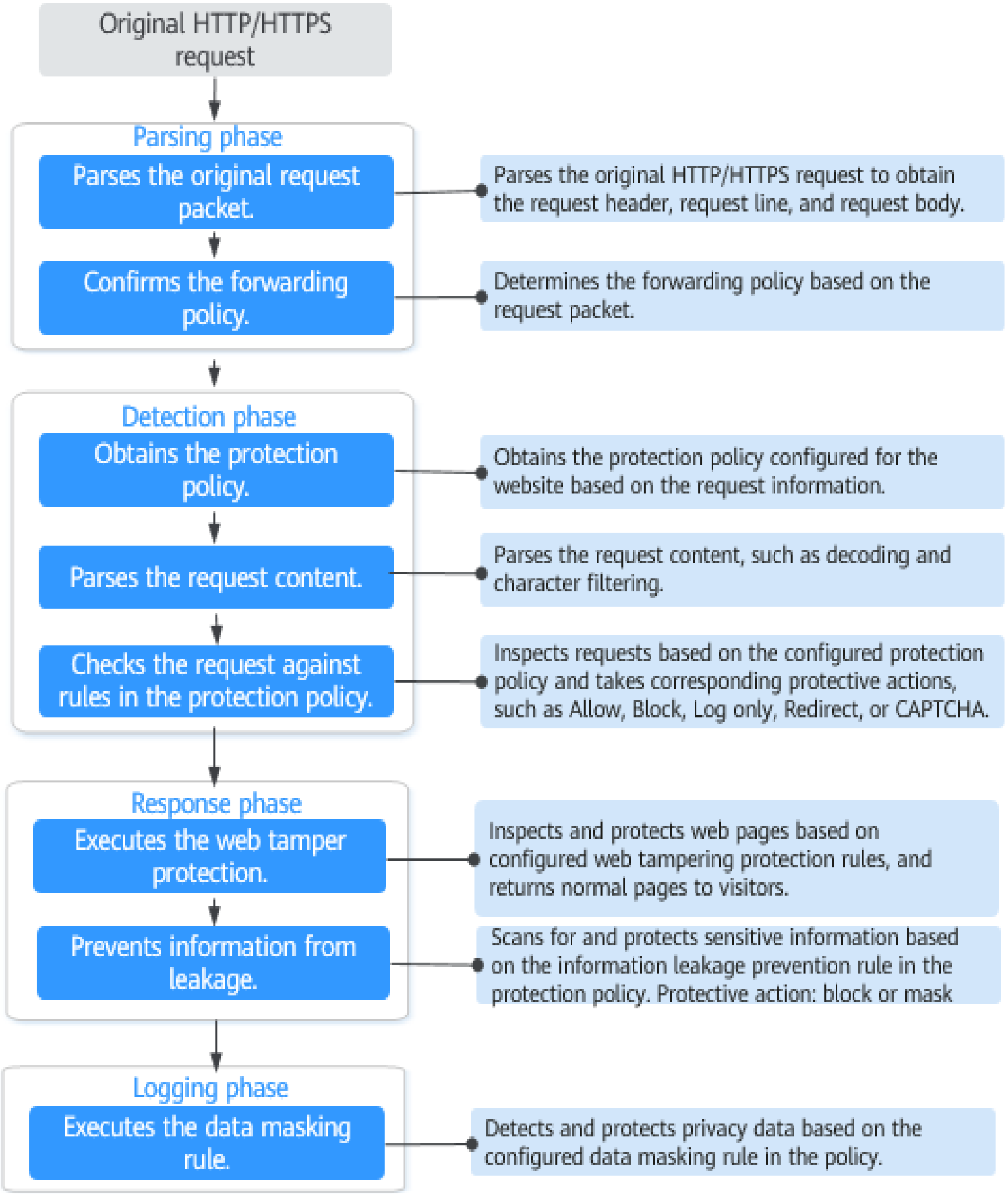
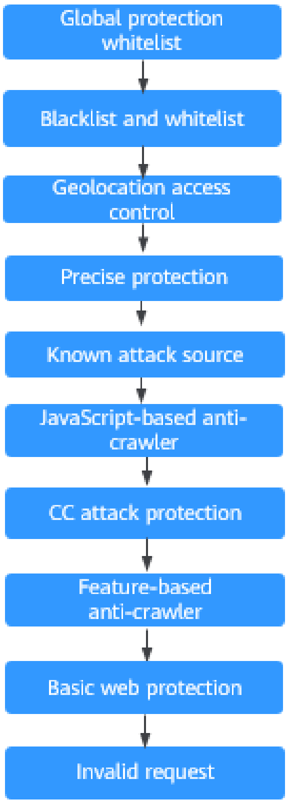

Original HTTP/HTTPS request
Parsing phase
Parses the original request packet.
Confirms the forwarding policy.
Parses the original HTTP/HTTPS request to obtain the request header, request line, and request body.
Determines the forwarding policy based on the request packet.
Detection phase
Obtains the protection policy.
Parses the request content.
Checks the request against rules in the protection policy.
Obtains the protection policy configured for the website based on the request information.
Parses the request content, such as decoding and character filtering.
Inspects requests based on the configured protection policy and takes corresponding protective actions, such as Allow, Block, Log only, Redirect, or CAPTCHA.
Response phase
Executes the web tamper protection.
Prevents information from leakage.
Inspects and protects web pages based on configured web tampering protection rules, and returns normal pages to visitors.
Scans for and protects sensitive information based on the information leakage prevention rule in the protection policy. Protective action: block or mask
Logging phase
Executes the data masking rule.
Detects and protects privacy data based on the configured data masking rule in the policy.

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 after a rule is matched.
- Mask: The system will anonymize sensitive information after a rule is matched.

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.

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 the project.

Prerequisites

A website has been added to WAF.

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.

Enabling Basic Web Protection Rules

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 **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.

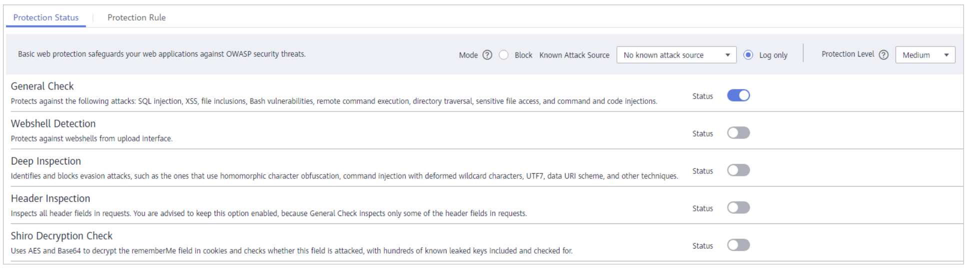
Step 5 Click the name of the target policy to go to the protection configuration page.

Step 6 Click the **Basic Web Protection** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

Step 7 Click the **Protection Status** tab, and enable protection types one by one by referring to **Table 5-3**.

Figure 5-3 Basic web protection



Protection Status | Protection Rule

Basic web protection safeguards your web applications against OWASP security threats.

Mode ⓘ ○ Block Known Attack Source: No known attack source ◉ Log only | Protection Level ⓘ: Medium

General Check
Protects against the following attacks: SQL injection, XSS, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command and code injections.
Status: on

Webshell Detection
Protects against webshells from upload interface.
Status: off

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.
Status: off

Header Inspection
Inspects all header fields in requests. You are advised to keep this option enabled, because General Check inspects only some of the header fields in requests.
Status: off

Shiro Decryption Check
Uses AES and Base64 to decrypt the rememberMe field in cookies and checks whether this field is attacked, with hundreds of known leaked keys included and checked for.
Status: off

1. Set the protective action.
   - **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.
2. Set the protection level.

   In the upper part of the page, set **Protection Level** to **Low**, **Medium**, or **High**. The default value is **Medium**.

Table 5-2 Protection levels

Protection Level	Description
Low	WAF only blocks the requests with obvious attack signatures. If a large number of false alarms are reported, **Low** is recommended.
Medium	The default level is **Medium**, which meets a majority of web protection requirements.
High	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 **High**.

3. Set the protection type.

NOTICE

By default, **General Check** is enabled. You can enable other protection types by referring to **Table 5-3**.

Table 5-3 Protection types

Type	Description
General Check	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. SQL injection attacks are mainly detected based on semantics. **NOTE** If you enable **General Check**, WAF checks your websites based on the built-in rules.
Webshell Detection	Protects against web shells from upload interface. **NOTE** If you enable **Webshell Detection**, WAF detects web page Trojan horses inserted through the upload interface.
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.
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.

----End

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.

Protection Effect

If **General Check** is enabled and **Mode** is set to **Block** for your domain name, to verify WAF is protecting your website (**www.example.com**) against general check items:

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, click **Events**. On the displayed page, view the event log.

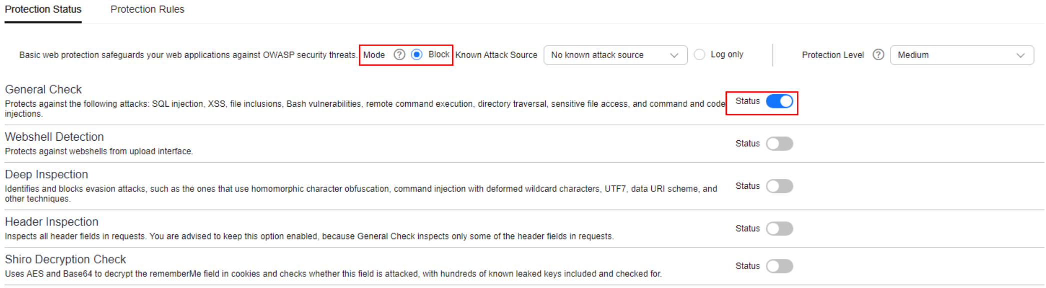
----End

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



Protection Status | Protection Rules

Basic web protection safeguards your web applications against OWASP security threats. Mode ● Block Known Attack Source: No known attack source ○ Log only | Protection Level: Medium

General Check
Protects against the following attacks: SQL injection, XSS, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command and code injections.
Status: on

Webshell Detection
Protects against webshells from upload interface.
Status: off

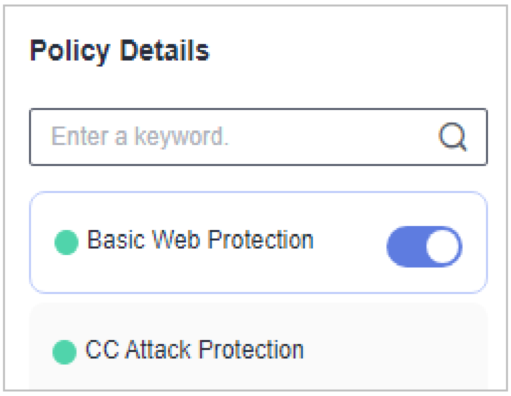
Deep Inspection
Identifies and blocks evasion attacks, such as the ones that use homomorphic character obfuscation, command injection with deformed wildcard characters, UTF7, data URI scheme, and other techniques.
Status: off

Header Inspection
Inspects all header fields in requests. You are advised to keep this option enabled, because General Check inspects only some of the header fields in requests.
Status: off

Shiro Decryption Check
Uses AES and Base64 to decrypt the rememberMe field in cookies and checks whether this field is attacked, with hundreds of known leaked keys included and checked for.
Status: off

Step 2 Enable WAF basic web protection.

Figure 5-5 Basic Web Protection configuration area



Policy Details

Enter a keyword.

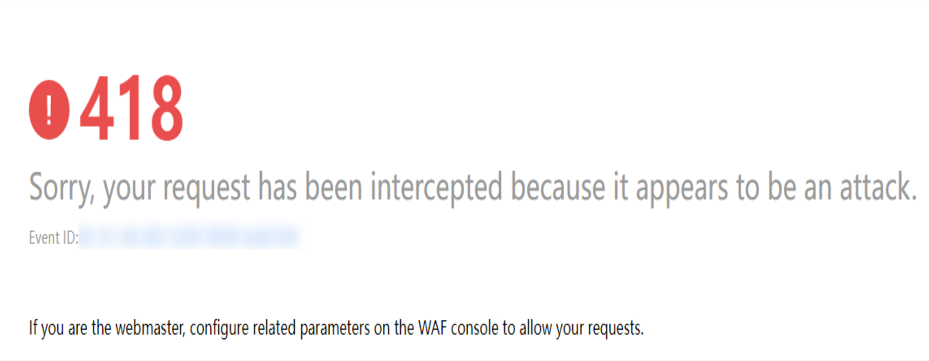
● Basic Web Protection (on)

● CC Attack Protection

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



418

Sorry, your request has been intercepted because it appears to be an attack.

Event ID: [redacted]

If you are the webmaster, configure related parameters on the WAF console to allow your requests.

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.

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 the project.

Prerequisites

A website has been added to WAF.

Constraints

- 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**.
- 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 CC Attack Protection Rule

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 **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 Click the name of the target policy to go to the protection configuration page.

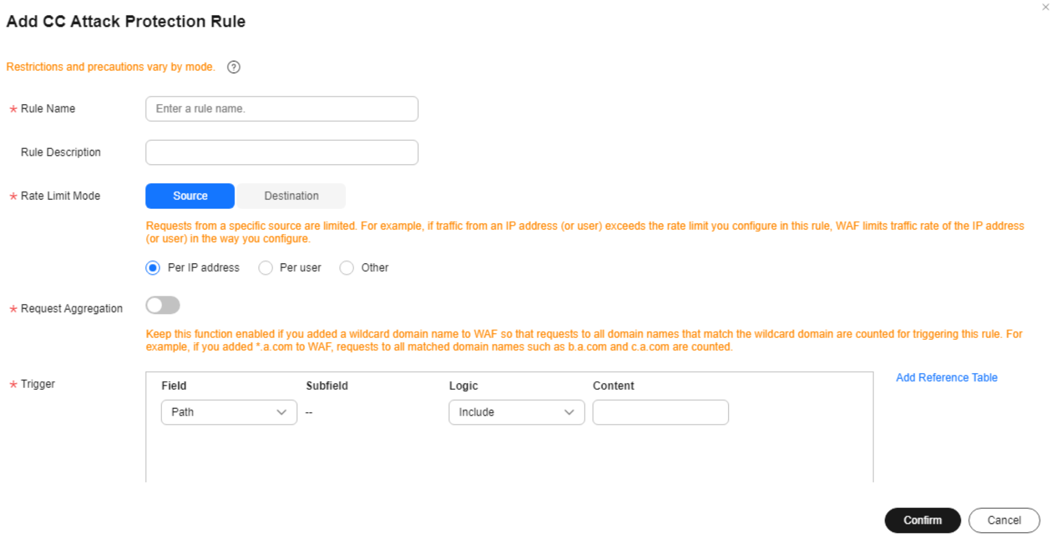
Step 6 Click the **CC Attack Protection** configuration area and toggle it on or off if needed.

- ●: enabled.
- ○: disabled.

Step 7 In the upper left corner above the **CC Attack Protection** rule list, click **Add Rule**.

Step 8 In the displayed dialog box, configure a CC attack protection rule by referring to **Table 5-4**.

Figure 5-7 Adding a CC attack protection rule



Add CC Attack Protection Rule

Restrictions and precautions vary by mode.

* Rule Name: Enter a rule name.

Rule Description:

* Rate Limit Mode: Source | Destination

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 ○ Per user ○ Other

* Request Aggregation: ○

Keep this function enabled if you added a wildcard domain name to WAF so that requests to all domain names that match the 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.

* Trigger

Field	Subfield	Logic	Content
Path	--	Include	

Table 5-4 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 for 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	Click **Add** and add conditions. At least one condition is required, but up to 30 conditions are allowed. If you add more than one condition, the rule will only take effect when all conditions are met. ● **Field** ● **Subfield**: Configure this field only when **IPv4**, **Cookie**, **Header**, or **Params** is selected for **Field**. NOTICE A subfield cannot exceed 2,048 bytes. ● **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**, 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.	**Path Include / admin**
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**.	**10** requests allowed in **60** seconds
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. ● **Block**: WAF blocks requests that trigger 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 the rule.	Block

Parameter	Description	Example Value
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
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**, a custom error message is displayed.	Custom
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 9 Click **Confirm**. You can then view the added CC attack protection rule in the CC rule list.

- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

----End

Protection Effect

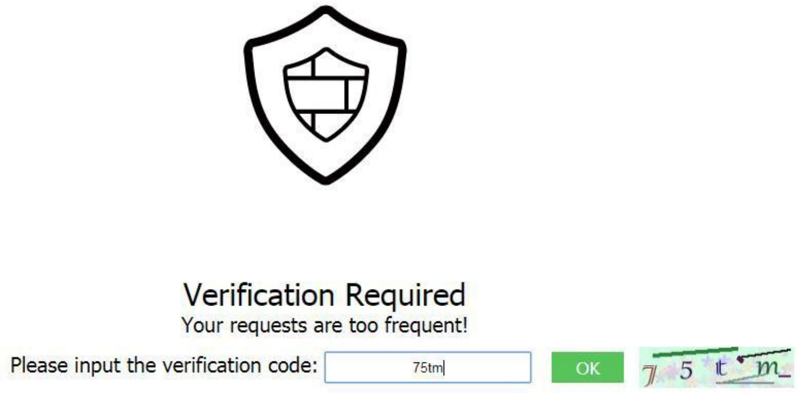
If you have configured a CC attack protection rule like **Figure 5-7** (with **Protective Action** set to **Block**) for your domain name **www.example.com**, take the following steps to verify the protection effect:

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 referring to **Website Settings**.
- If the website is accessible, go to **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.



Verification Required

Your requests are too frequent!

Please input the verification code: 75tm

Step 3 Return to the WAF console. In the navigation pane, click **Events**. On the displayed page, view the event log.

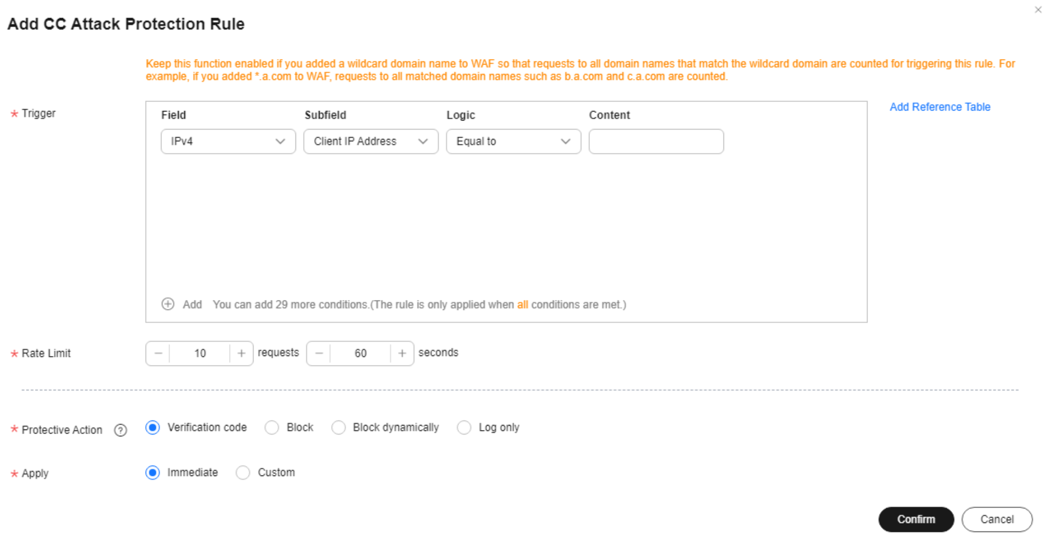
----End

Configuration Example - Verification Code

If domain name **www.example.com** has been connected to WAF, perform the following steps to verify that WAF CAPTCHA verification is enabled.

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

Figure 5-8 Verification code



Add CC Attack Protection Rule

Keep this function enabled if you added a wildcard domain name to WAF so that requests to all domain names that match the 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.

* Trigger

Field	Subfield	Logic	Content
IPv4	Client IP Address	Equal to	

⊕ Add You can add 29 more conditions.(The rule is only applied when all conditions are met.)

Add Reference Table

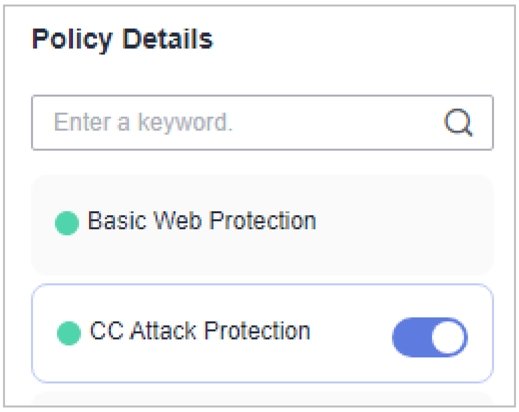
* Rate Limit: 10 requests 60 seconds

* Protective Action: ● Verification code ○ Block ○ Block dynamically ○ Log only

* Apply: ● Immediate ○ Custom

Step 2 Enable CC attack protection.

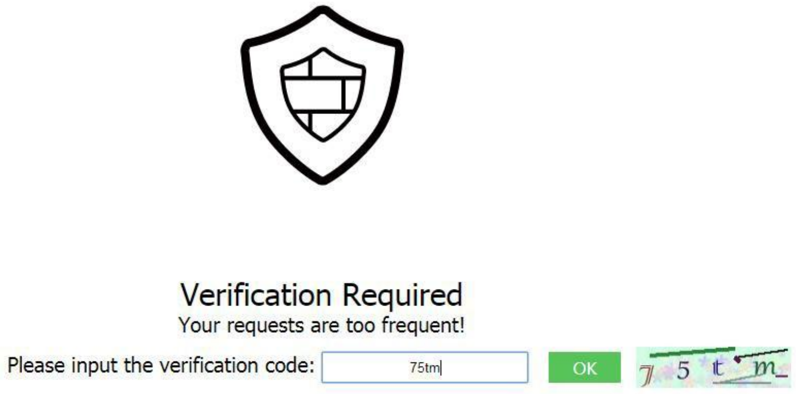
Figure 5-9 Enabling CC Attack Protection



Policy Details

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.



Verification Required

Your requests are too frequent!

Please input the verification code: 75tm

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

----End

5.4 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.

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

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 the project.

Prerequisites

A website has been added to WAF.

Constraints

- 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.

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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 Click the name of the target policy to go to the protection configuration page.

Step 6 Click the **Precise Protection** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

Step 7 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 8 In the upper left corner above the **Precise Protection** rule list, click **Add Rule**.

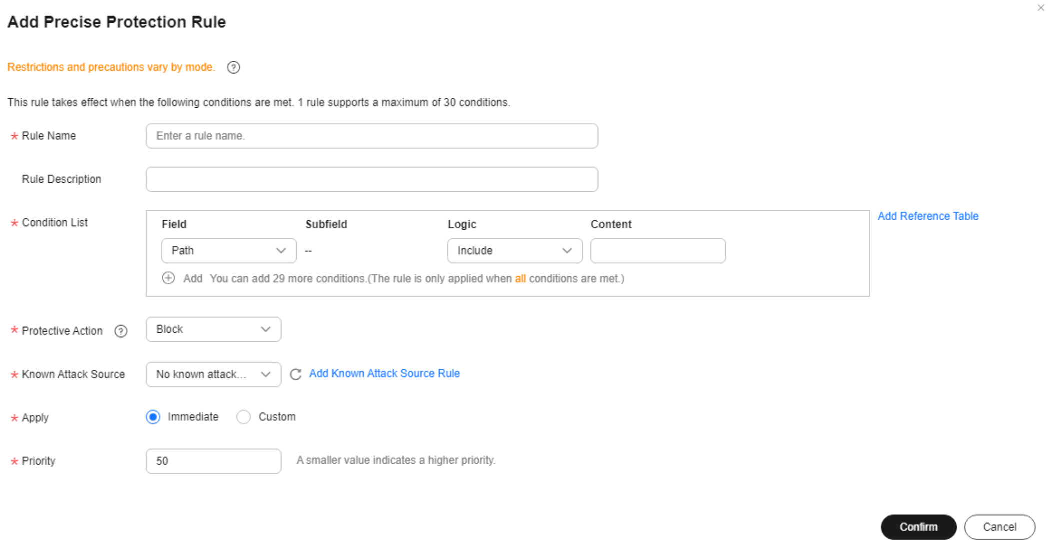
Step 9 In the displayed dialog box, add a rule by referring to **Table 5-5**.

The settings shown in **Figure 5-10** 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 5-10 Add Precise Protection Rule



Add Precise Protection Rule

Restrictions and precautions vary by mode.

This rule takes effect when the following conditions are met. 1 rule supports a maximum of 30 conditions.

* Rule Name: Enter a rule name.

Rule Description:

* Condition List

Field	Subfield	Logic	Content
Path	--	Include	

Add You can add 29 more conditions.(The rule is only applied when all conditions are met.)

Add Reference Table

* Protective Action: Block

* Known Attack Source: No known attack... Add Known Attack Source Rule

* Apply: ● Immediate ○ Custom

* Priority: 50 A smaller value indicates a higher priority.

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.	None

Parameter	Description	Example Value
Condition List	Click **Add** and add conditions. At least one condition is required for a rule, but up to 30 conditions are allowed. If you add more than one condition, the rule will only take effect when all conditions are met. Parameters for configuring a condition are described as follows: ● **Field** ● **Subfield**: Configure this field only when **IPv4**, **Params**, **Cookie**, **Response Header**, or **Header** is selected for **Field**. NOTICE A subfield cannot exceed 2,048 bytes. ● **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 performs the protection action (block, allow, or log only) when the field in the 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 of condition matching.	● **Path Include /admin** ● **User Agent Prefix is not mozilla/5.0** ● **IP Equal to 192.168.2.3** ● **Cookie key1 Prefix is not jsessionid**

Parameter	Description	Example Value
	NOTE For more details about the configurations in general, see **Table 5-16**.	
Protective Action	● **Block**: The request that hit the rule will be blocked and a block response page is returned to the client that initiates the request. 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.	**Block**
Known Attack Source	If you set **Protective Action** to **Block**, you can select a blocking type for 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.	**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**

Step 10 Click **Confirm**. You can then view the added precise protection rule in the protection rule list.

- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.

- To delete a rule, click **Delete** in the row containing the rule.

----End

Protection Effect

To verify WAF is protecting your website (**www.example.com**) against the rule as shown in **Figure 5-10**:

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.

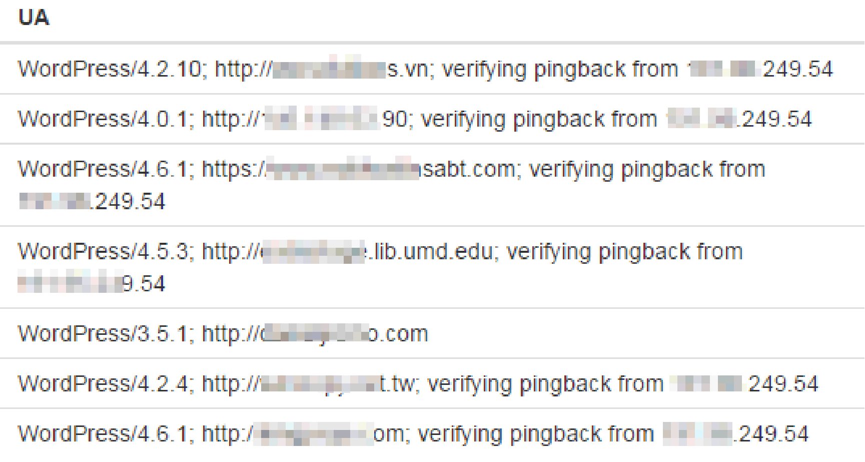
Step 3 Return to the WAF console. In the navigation pane, choose **Events**. On the displayed page, view the event log.

----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.

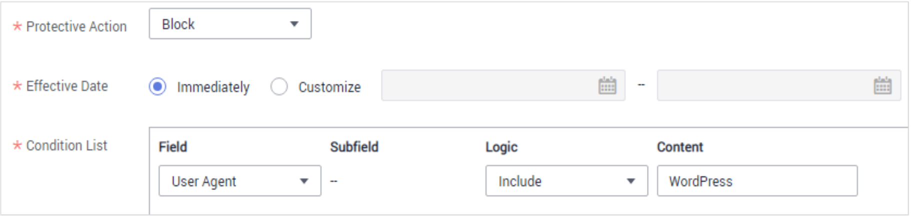
Figure 5-11 WordPress pingback attack



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 5-12 User Agent configuration



* Protective Action: Block

* Effective Date: ● Immediately ○ Customize

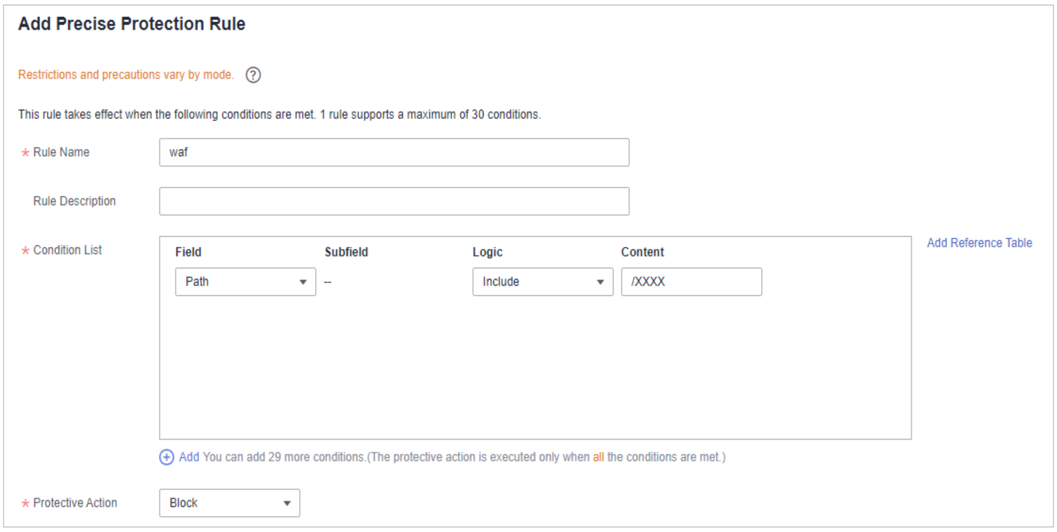
* Condition List

Field	Subfield	Logic	Content
User Agent	--	Include	WordPress

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 5-13 Blocking requests to a specific URL



Add Precise Protection Rule

Restrictions and precautions vary by mode.

This rule takes effect when the following conditions are met. 1 rule supports a maximum of 30 conditions.

* Rule Name: waf

Rule Description:

* Condition List:

Field	Subfield	Logic	Content
Path	--	Include	/XXXX

Add Reference Table

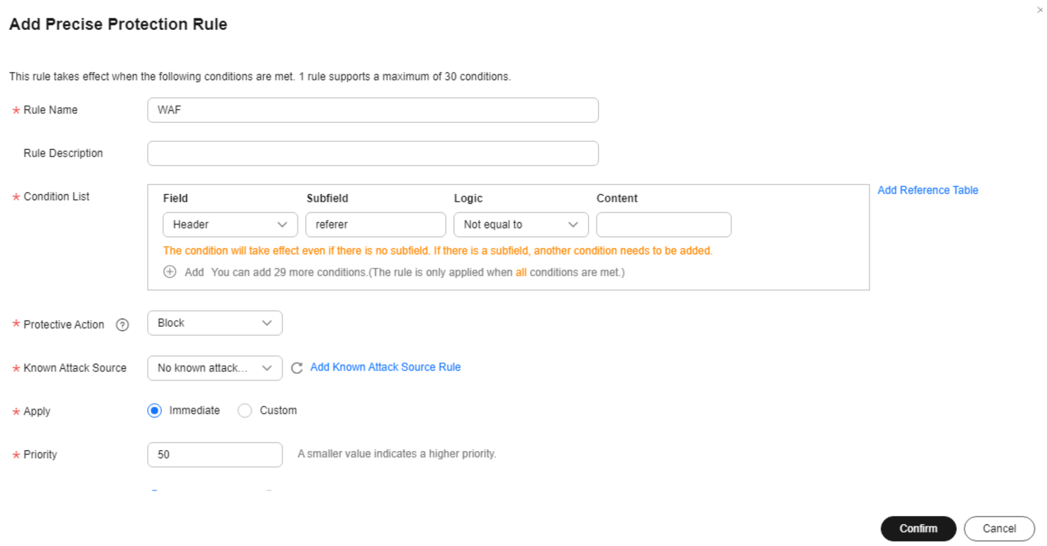
Add You can add 29 more conditions.(The protective action is executed only when all the conditions are met.)

* Protective Action: Block

Configuration Example - Blocking Requests with null Fields

You can configure precise protection rules to block requests having null fields.

Figure 5-14 Blocking requests with empty Referer



Add Precise Protection Rule

This rule takes effect when the following conditions are met. 1 rule supports a maximum of 30 conditions.

* Rule Name: WAF

Rule Description:

* Condition List:

Field	Subfield	Logic	Content
Header	referer	Not equal to	

The condition will take effect even if there is no subfield. If there is a subfield, another condition needs to be added.

Add You can add 29 more conditions.(The rule is only applied when all conditions are met.)

Add Reference Table

* Protective Action: Block

* Known Attack Source: No known attack... Add Known Attack Source Rule

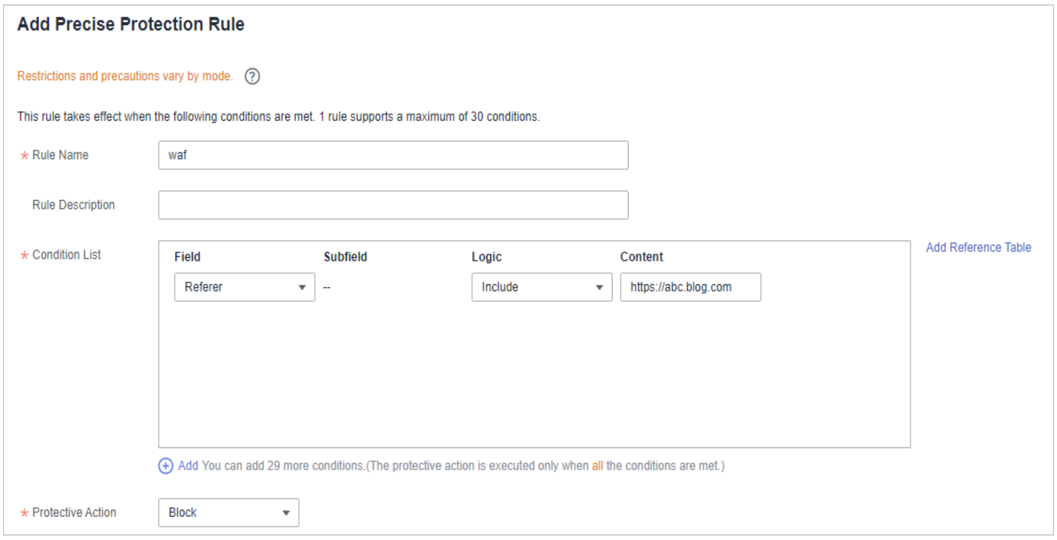
* Apply: ● Immediate ○ Custom

* Priority: 50 A smaller value indicates a higher priority.

Configuration Example - 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 5-15** to block access requests of .zip files.

Figure 5-15 Blocking requests of specific file types



Add Precise Protection Rule

Restrictions and precautions vary by mode.

This rule takes effect when the following conditions are met. 1 rule supports a maximum of 30 conditions.

* Rule Name: waf

Rule Description:

* Condition List:

Field	Subfield	Logic	Content
Referer	--	Include	https://abc.blog.com

Add Reference Table

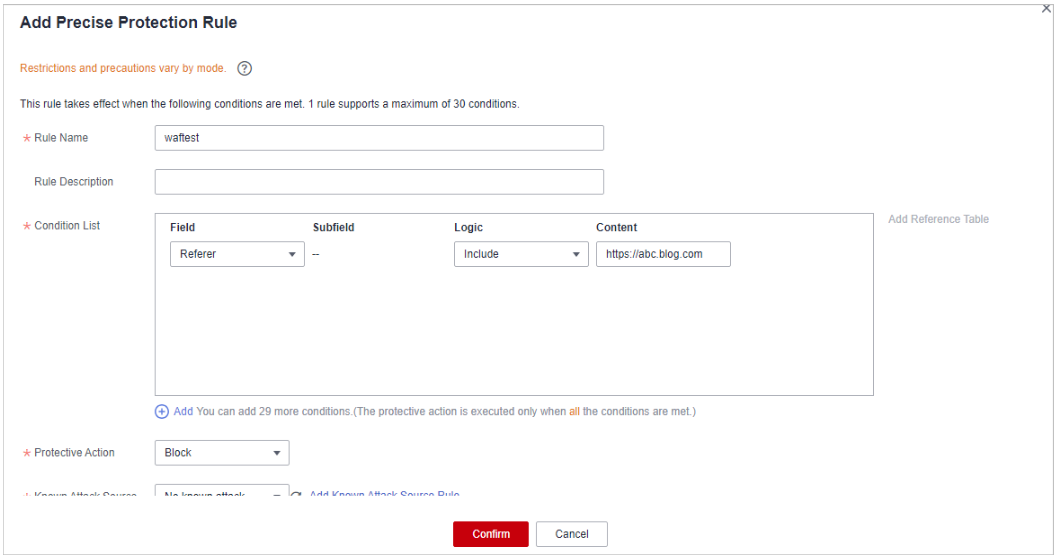
Add You can add 29 more conditions.(The protective action is executed only when all the conditions are met.)

* Protective Action: Block

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 5-16 Preventing hotlinking



Add Precise Protection Rule

Restrictions and precautions vary by mode.

This rule takes effect when the following conditions are met. 1 rule supports a maximum of 30 conditions.

* Rule Name: waftest

Rule Description:

* Condition List:

Field	Subfield	Logic	Content
Referer	--	Include	https://abc.blog.com

Add Reference Table

Add You can add 29 more conditions.(The protective action is executed only when all the conditions are met.)

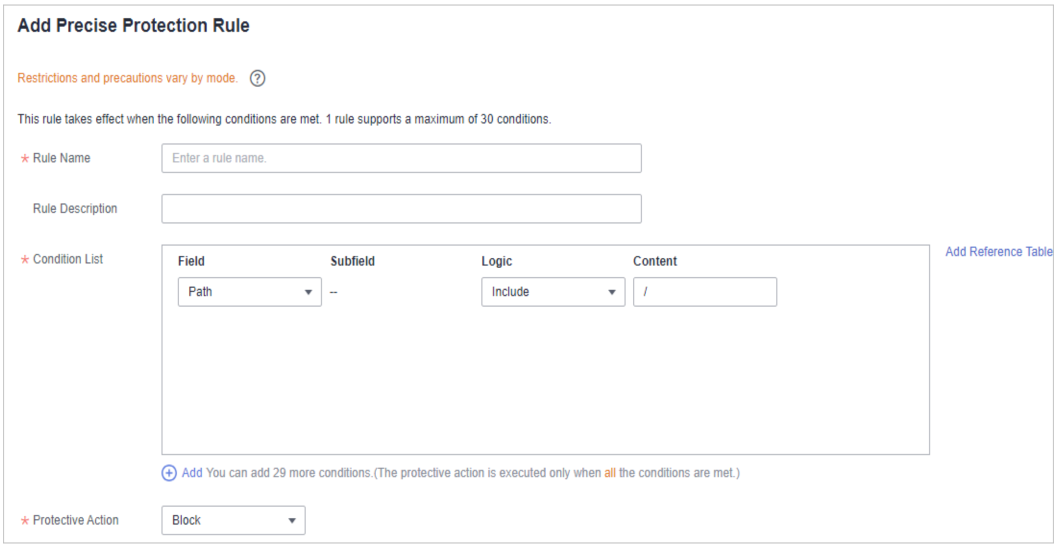
* Protective Action: Block

* Known Attack Source: No known attack Add Known Attack Source Rule

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 5-17**, but then another one to allow the access from a specific IP address, as shown in **Figure 5-18**.

Figure 5-17 Blocking all requests


Add Precise Protection Rule

Restrictions and precautions vary by mode.

This rule takes effect when the following conditions are met. 1 rule supports a maximum of 30 conditions.

* Rule Name: Enter a rule name.

Rule Description:

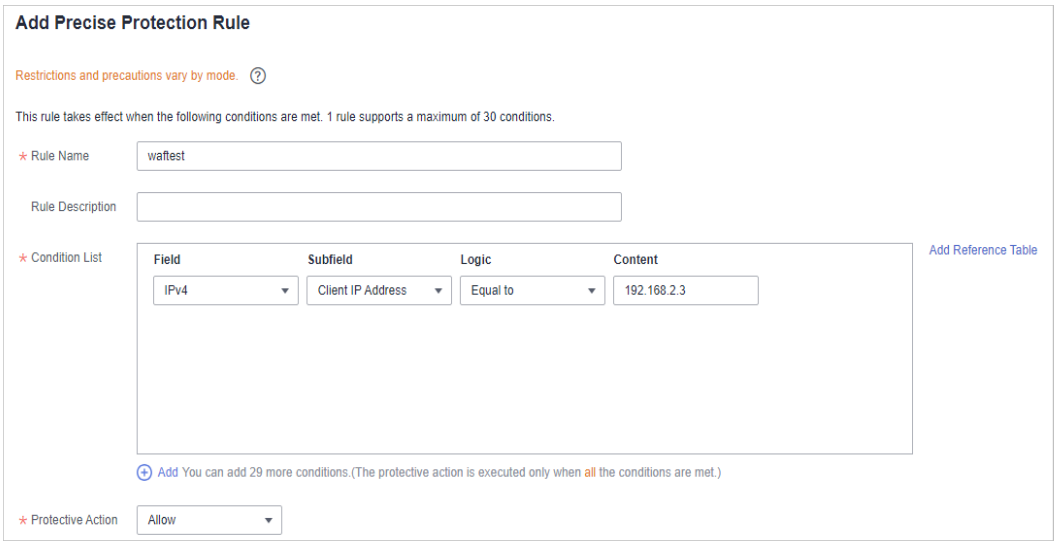
* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/

Add You can add 29 more conditions.(The protective action is executed only when all the conditions are met.)

* Protective Action: Block

Figure 5-18 Allowing the access of a specified IP address


Add Precise Protection Rule

Restrictions and precautions vary by mode.

This rule takes effect when the following conditions are met. 1 rule supports a maximum of 30 conditions.

* Rule Name: waftest

Rule Description:

* Condition List

Field	Subfield	Logic	Content
IPv4	Client IP Address	Equal to	192.168.2.3

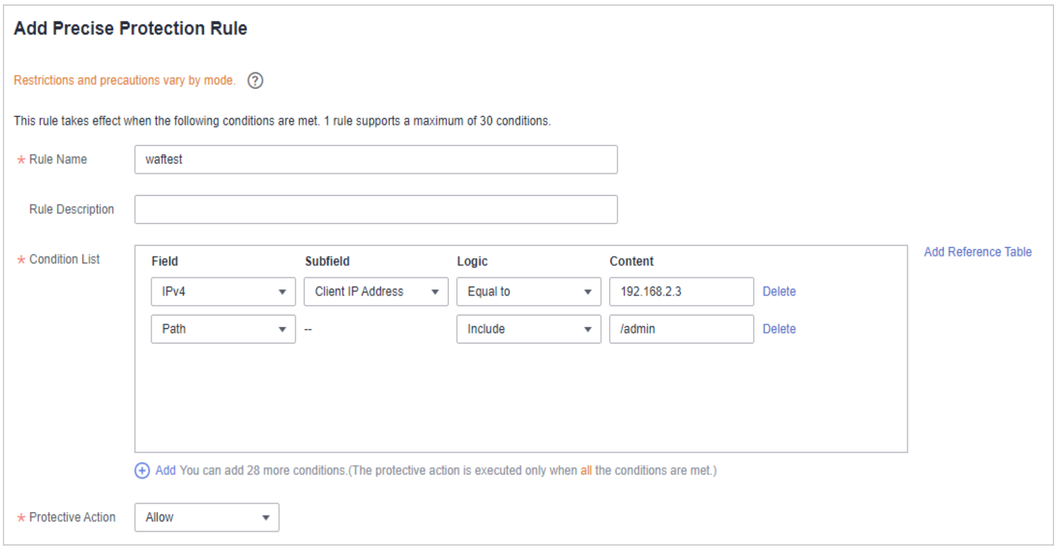
Add You can add 29 more conditions.(The protective action is executed only when all the conditions are met.)

* Protective Action: Allow

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 5-19 Allowing specific IP addresses to access specified URLs



Add Precise Protection Rule

Restrictions and precautions vary by mode.

This rule takes effect when the following conditions are met. 1 rule supports a maximum of 30 conditions.

* Rule Name: waftest

Rule Description:

* Condition List

Field	Subfield	Logic	Content	
IPv4	Client IP Address	Equal to	192.168.2.3	Delete
Path	--	Include	/admin	Delete

Add You can add 28 more conditions.(The protective action is executed only when all the conditions are met.)

* Protective Action: Allow

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.

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 the project.

Prerequisites

A website has been added to WAF.

Constraints

- 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 address 0.0.0.0/0 cannot be added to a WAF IP address blacklist or whitelist, and if a whitelist conflicts with a blacklist, the whitelist rule takes priority. 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.
- 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.

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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 Click the name of the target policy to go to the protection configuration page.

Step 6 Click the **Blacklist and Whitelist** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

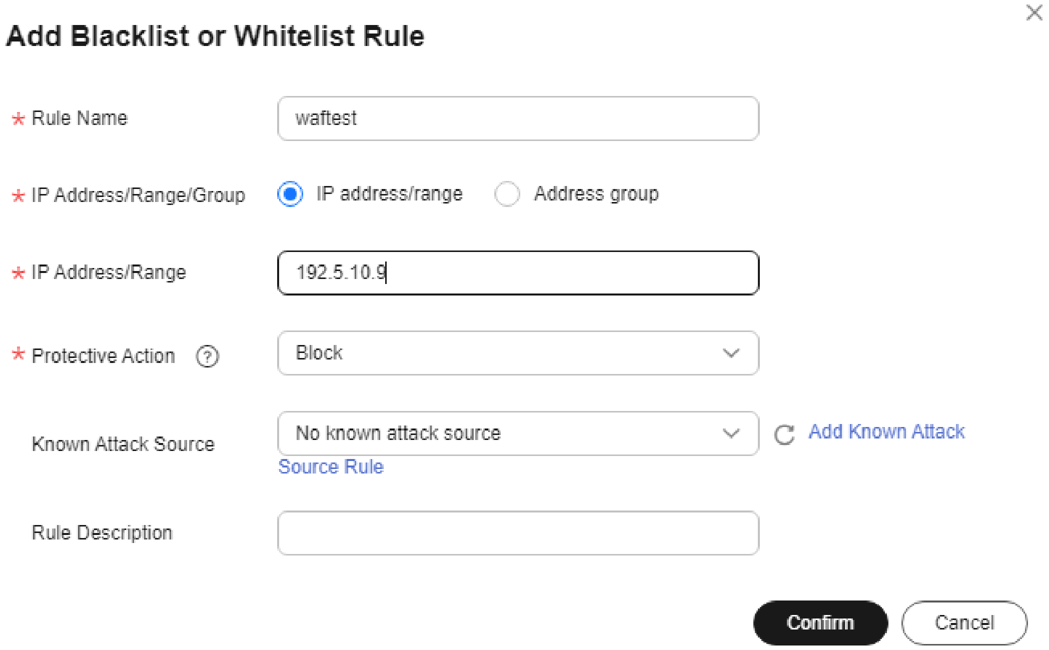
Step 7 In the upper left corner above the **Blacklist and Whitelist** list, click **Add Rule**.

Step 8 In the displayed dialog box, specify the parameters by referring to **Table 5-6**. **Figure 5-20** and **Figure 5-21** show two examples.

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 5-20 Adding an IP address/Range to a blacklist or whitelist rule



Add Blacklist or Whitelist Rule

* Rule Name: waftest

* IP Address/Range/Group: ● IP address/range ○ Address group

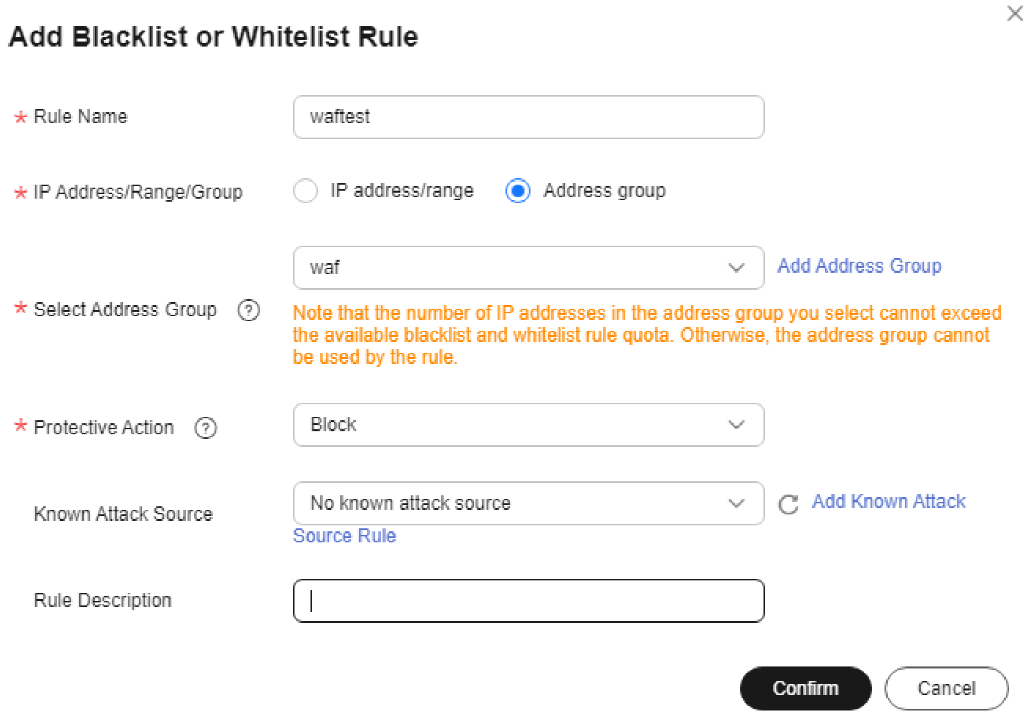
* IP Address/Range: 192.5.10.9

* Protective Action: Block

Known Attack Source: No known attack source

Rule Description:

Figure 5-21 Batching adding IP addresses/Ranges to a blacklist or whitelist rule



Add Blacklist or Whitelist Rule

* Rule Name: waftest

* IP Address/Range/Group: ○ IP address/range ● Address group

* Select Address Group: waf

Note that the number of IP addresses in the address group you select cannot exceed the available blacklist and whitelist rule quota. Otherwise, the address group cannot be used by the rule.

* Protective Action: Block

Known Attack Source: No known attack source

Rule Description:

Table 5-6 Rule parameters

Parameter	Description	Example Value
Rule Name	Rule name you entered.	waftest

Parameter	Description	Example Value
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
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	XXX.XXX.2.3
Select Address Group	This parameter is mandatory if you select **Address group** for IP **Address/Range/Group**. Select an IP address group from the drop-down list. You can also click **Add Address Group** to create an address group. For details, see **Adding an IP Address Group**.	groupwaf
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

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

Step 9 Click **Confirm**. You can then view the added rule in the list of blacklist and whitelist rules.

- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

----End

Protection Effect

To verify WAF is protecting your website (**www.example.com**) against a rule:

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 referring to **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**. Normally, WAF blocks such requests and returns the block page.

Step 4 Return to the WAF console. In the navigation pane, click **Events**. On the displayed page, view the event log.

----End

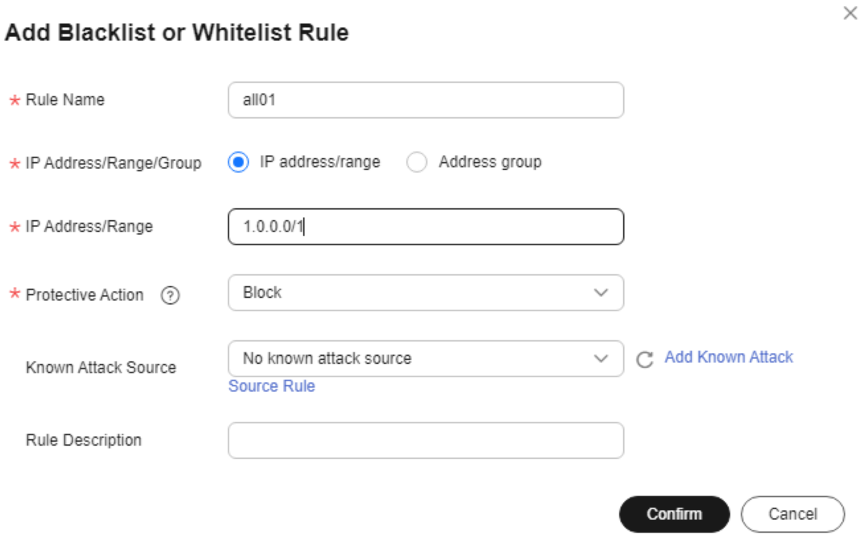
Example Configuration - Allowing a Specified IP Addresses

If domain name *www.example.com* has been connected to WAF, you can perform the following steps to verify the rule takes effect:

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 5-22** and **Figure 5-23**.

Figure 5-22 Blocking IP address range 1.0.0.0/1



Add Blacklist or Whitelist Rule

* Rule Name: all01

* IP Address/Range/Group: ● IP address/range ○ Address group

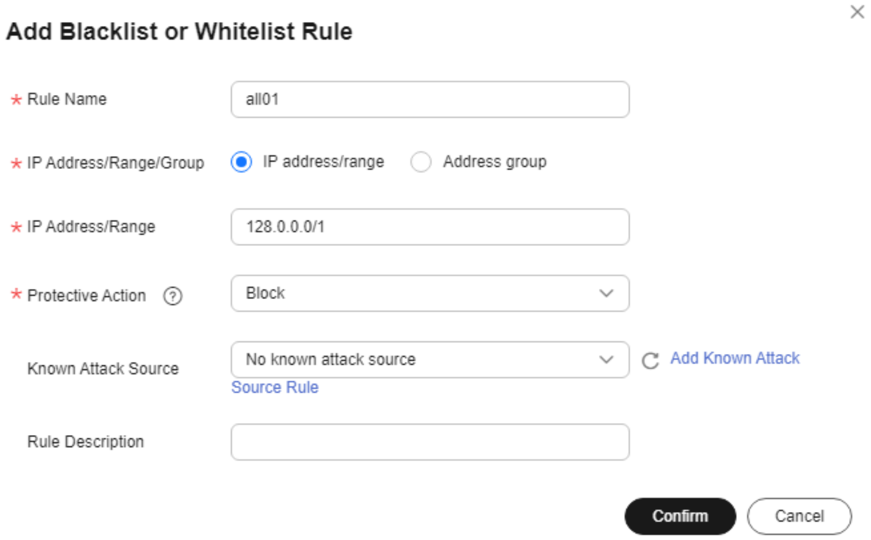
* IP Address/Range: 1.0.0.0/1

* Protective Action: Block

Known Attack Source: No known attack source

Rule Description:

Figure 5-23 Blocking IP address range 128.0.0.0/1



Add Blacklist or Whitelist Rule

* Rule Name: all01

* IP Address/Range/Group: ● IP address/range ○ Address group

* IP Address/Range: 128.0.0.0/1

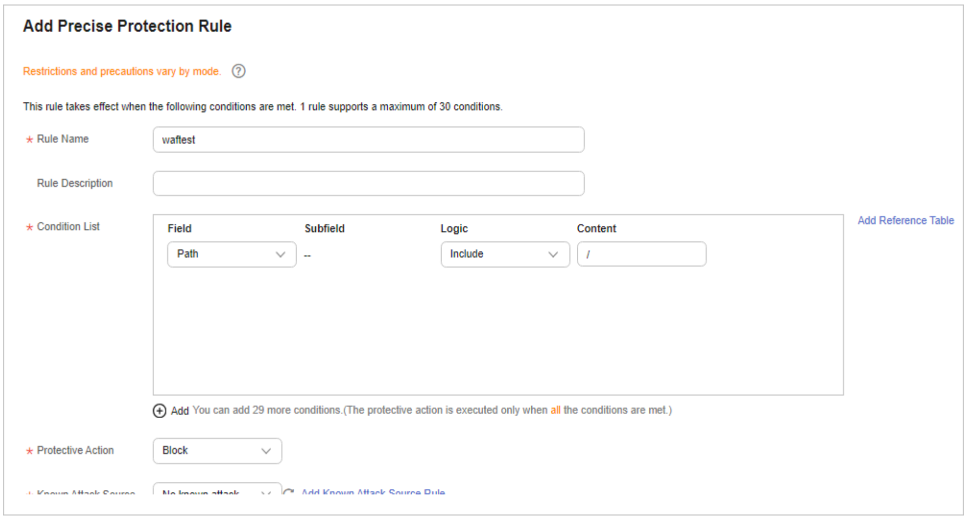
* Protective Action: Block

Known Attack Source: No known attack source

Rule Description:

- **Method 2**: Add a precise protection rule to block all access requests, as shown in **Figure 5-24**.

Figure 5-24 Blocking all access requests



Add Precise Protection Rule

Restrictions and precautions vary by mode. ?

This rule takes effect when the following conditions are met. 1 rule supports a maximum of 30 conditions.

* Rule Name: waftest

Rule Description:

* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/

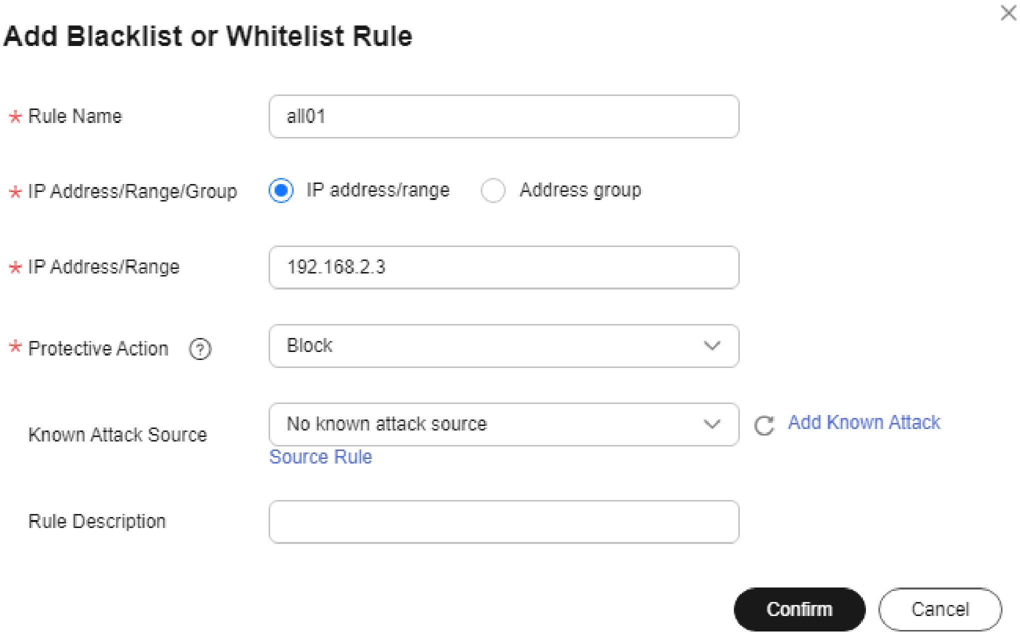
⊕ Add You can add 29 more conditions.(The protective action is executed only when all the conditions are met.)

* Protective Action: Block

* Known Attack Source: No known attack

Step 2 Refer to **Figure 5-25** and add a whitelist rule to allow a specified IP address, for example, *XXX.XXX.2.3*.

Figure 5-25 Allowing the access of a specified IP address



Add Blacklist or Whitelist Rule

* Rule Name: all01

* IP Address/Range/Group: ● IP address/range ○ Address group

* IP Address/Range: 192.168.2.3

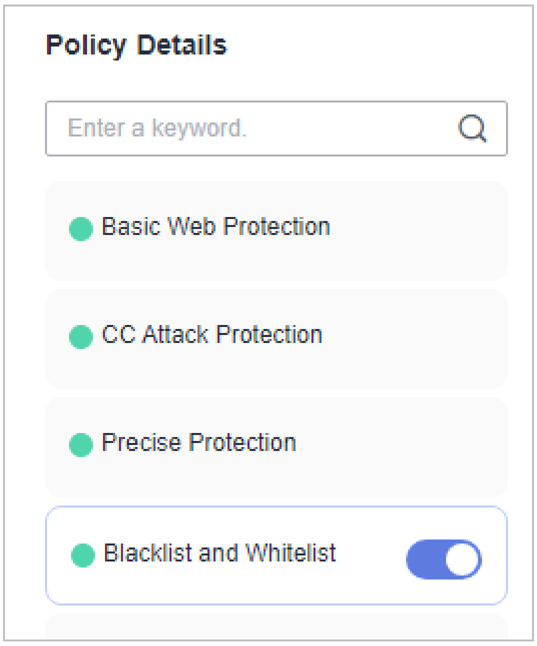
* Protective Action ?: Block

Known Attack Source: No known attack source

Rule Description:

Step 3 Enable the white and blacklist protection.

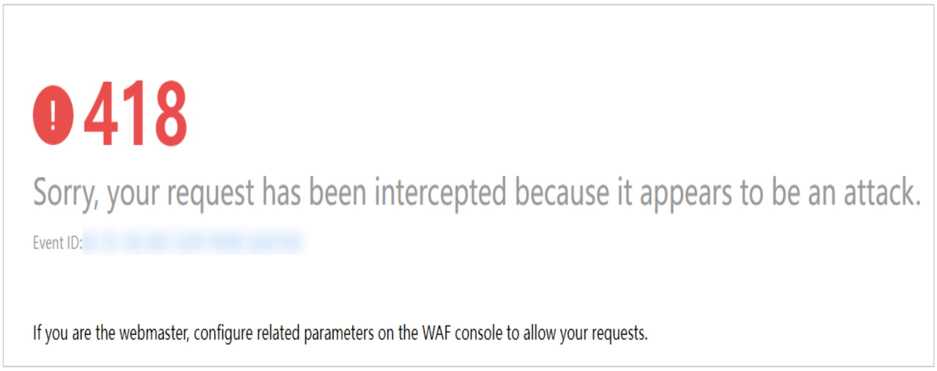
Figure 5-26 Blacklist and Whitelist configuration area



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 5-27** shows an example of the block page.

Figure 5-27 Block page



418

Sorry, your request has been intercepted because it appears to be an attack.

Event ID: [redacted]

If you are the webmaster, configure related parameters on the WAF console to allow your requests.

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 Access Requests from IP Addresses in a Specified Region**.

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 the project.

Prerequisites

A website has been added to WAF.

Constraints

- One region can be configured in only one geolocation access control 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.

Configuring a Geolocation Access Control Rule

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 **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 Click the name of the target policy to go to the protection configuration page.

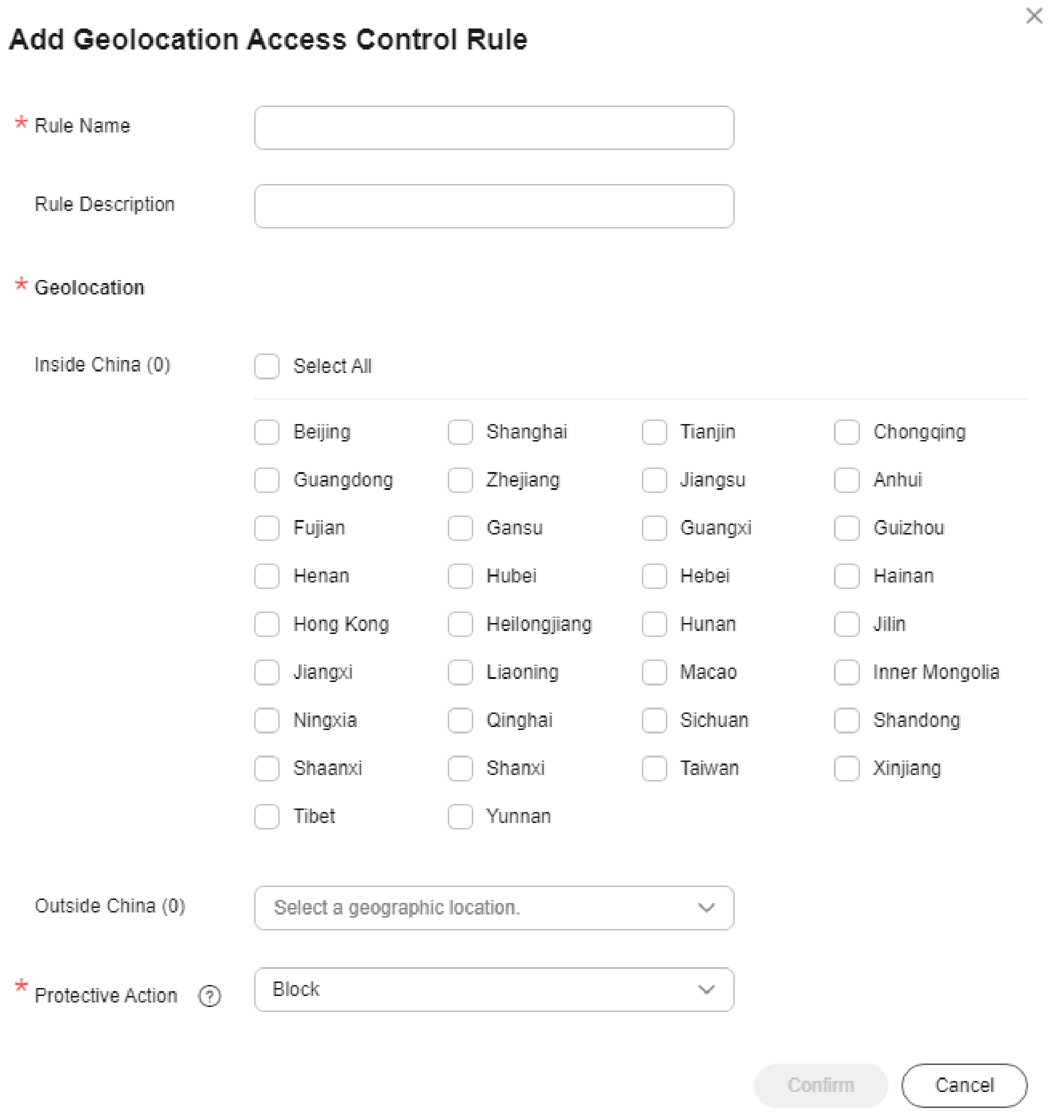
Step 6 Click the **Geolocation Access Control** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

Step 7 In the upper left corner above the **Geolocation Access Control** list, click **Add Rule**.

Step 8 In the displayed dialog box, add a geolocation access control rule by referring to **Table 5-7**.

Figure 5-28 Adding a geolocation access control rule



Add Geolocation Access Control Rule

* Rule Name

Rule Description

* Geolocation

Inside China (0) □ Select All

□ Beijing □ Shanghai □ Tianjin □ Chongqing
□ Guangdong □ Zhejiang □ Jiangsu □ Anhui
□ Fujian □ Gansu □ Guangxi □ Guizhou
□ Henan □ Hubei □ Hebei □ Hainan
□ Hong Kong □ Heilongjiang □ Hunan □ Jilin
□ Jiangxi □ Liaoning □ Macao □ Inner Mongolia
□ Ningxia □ Qinghai □ Sichuan □ Shandong
□ Shaanxi □ Shanxi □ Taiwan □ Xinjiang
□ Tibet □ Yunnan

Outside China (0) Select a geographic location.

* Protective Action Block

Table 5-7 Rule parameters

Parameter	Description	Example Value
Rule Name	Rule name you configured	dlfw
Rule Description	A brief description of the rule. This parameter is optional.	waf
Geolocation	Geographical scope of the IP address.	-
Protective Action	Action WAF will take if the rule is hit. You can select **Block**, **Allow**, or **Log only**.	**Block**

Step 9 Click **Confirm**. You can then view the added rule in the list of the geolocation access control rules.

- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

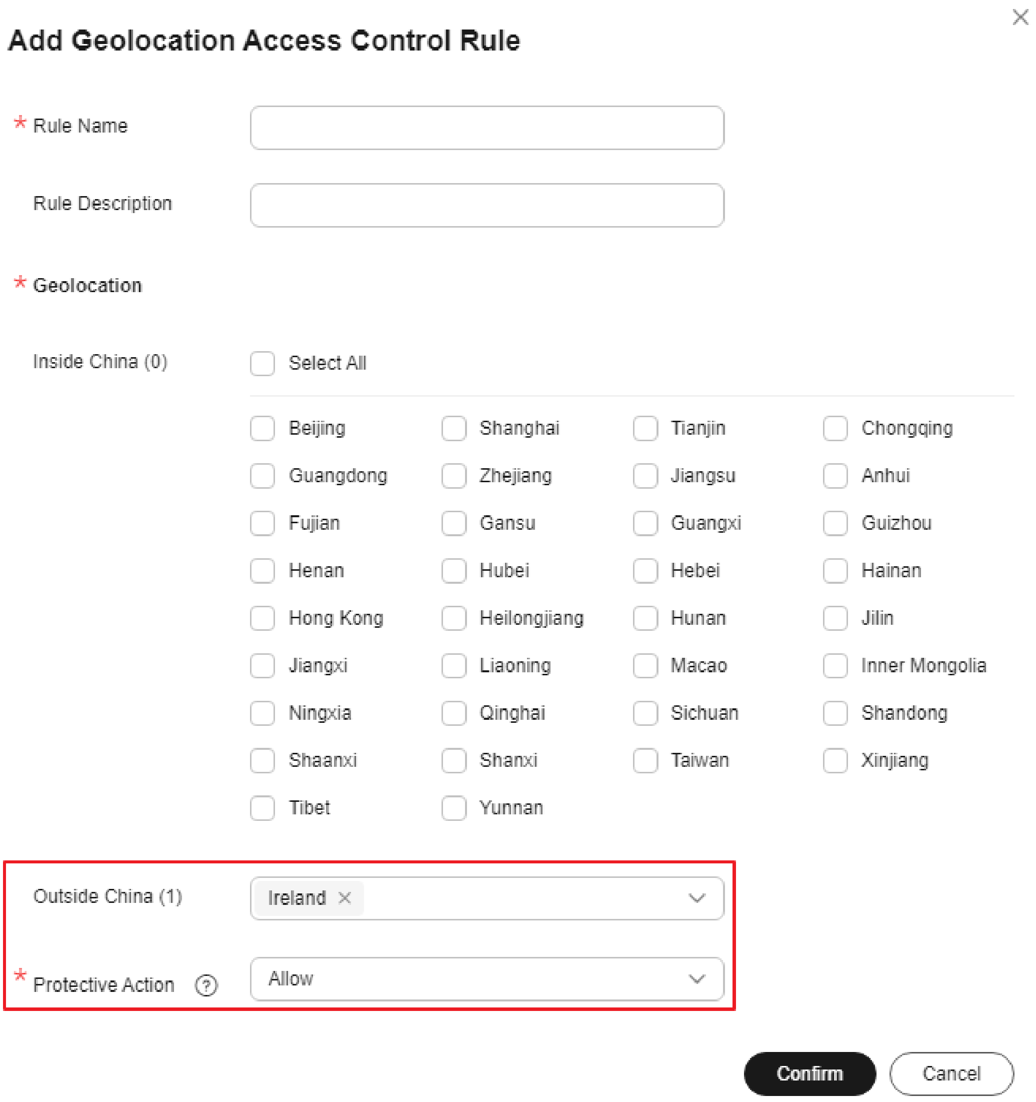
----End

Configuration Example - Allowing Access Requests from IP Addresses in a Specified Region

Assume that domain name *www.example.com* has been connected to WAF and you want to allow only IP addresses in **Ireland** to access the domain name. Perform the following steps:

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

Figure 5-29 Selecting Allow for Protective Action



Add Geolocation Access Control Rule

* Rule Name:

Rule Description:

* Geolocation

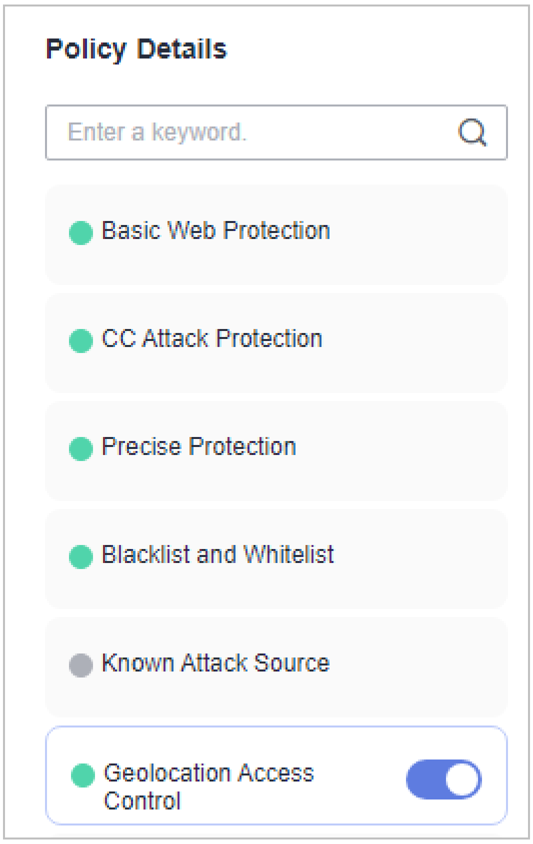
Inside China (0): □ Select All

Outside China (1): Ireland

* Protective Action: Allow

Step 2 Enable geolocation access control.

Figure 5-30 Geolocation Access Control configuration area



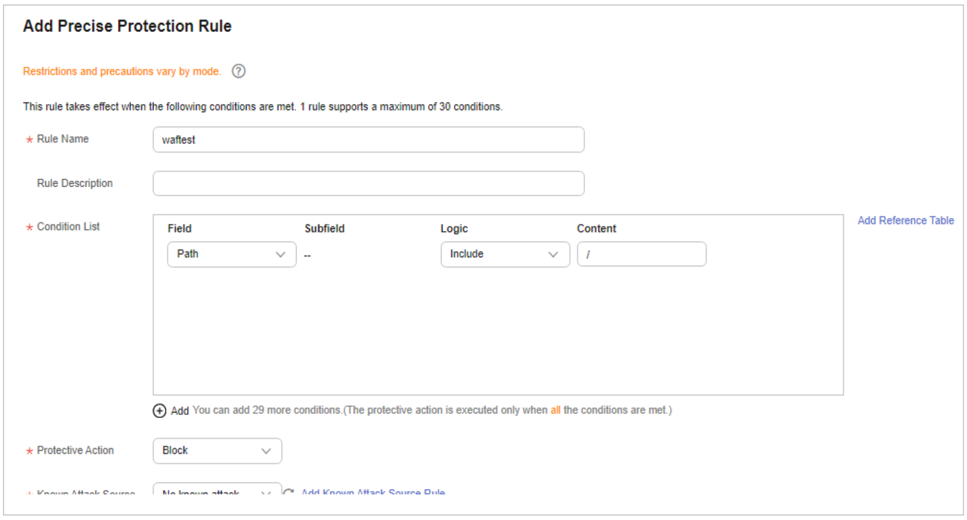
Policy Details

Enter a keyword.

- ● Basic Web Protection
- ● CC Attack Protection
- ● Precise Protection
- ● Blacklist and Whitelist
- ○ Known Attack Source
- ● Geolocation Access Control (enabled)

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

Figure 5-31 Blocking all access requests



Add Precise Protection Rule

Restrictions and precautions vary by mode.

This rule takes effect when the following conditions are met. 1 rule supports a maximum of 30 conditions.

* Rule Name: waftest

Rule Description:

* Condition List:

Field	Subfield	Logic	Content
Path	--	Include	/

Add Reference Table

⊕ Add You can add 29 more conditions.(The protective action is executed only when all the conditions are met.)

* Protective Action: Block

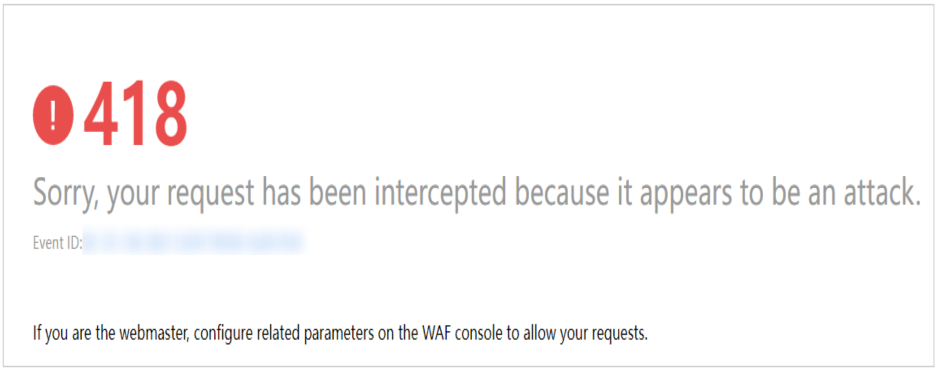
* Known Attack Source: No known attack   Add Known Attack Source Rule

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 **Ireland** accesses the page, WAF blocks the access request.

Figure 5-32 Block page



418

Sorry, your request has been intercepted because it appears to be an attack.

Event ID: [redacted]

If you are the webmaster, configure related parameters on the WAF console to allow your requests.

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 **Ireland** have been blocked.

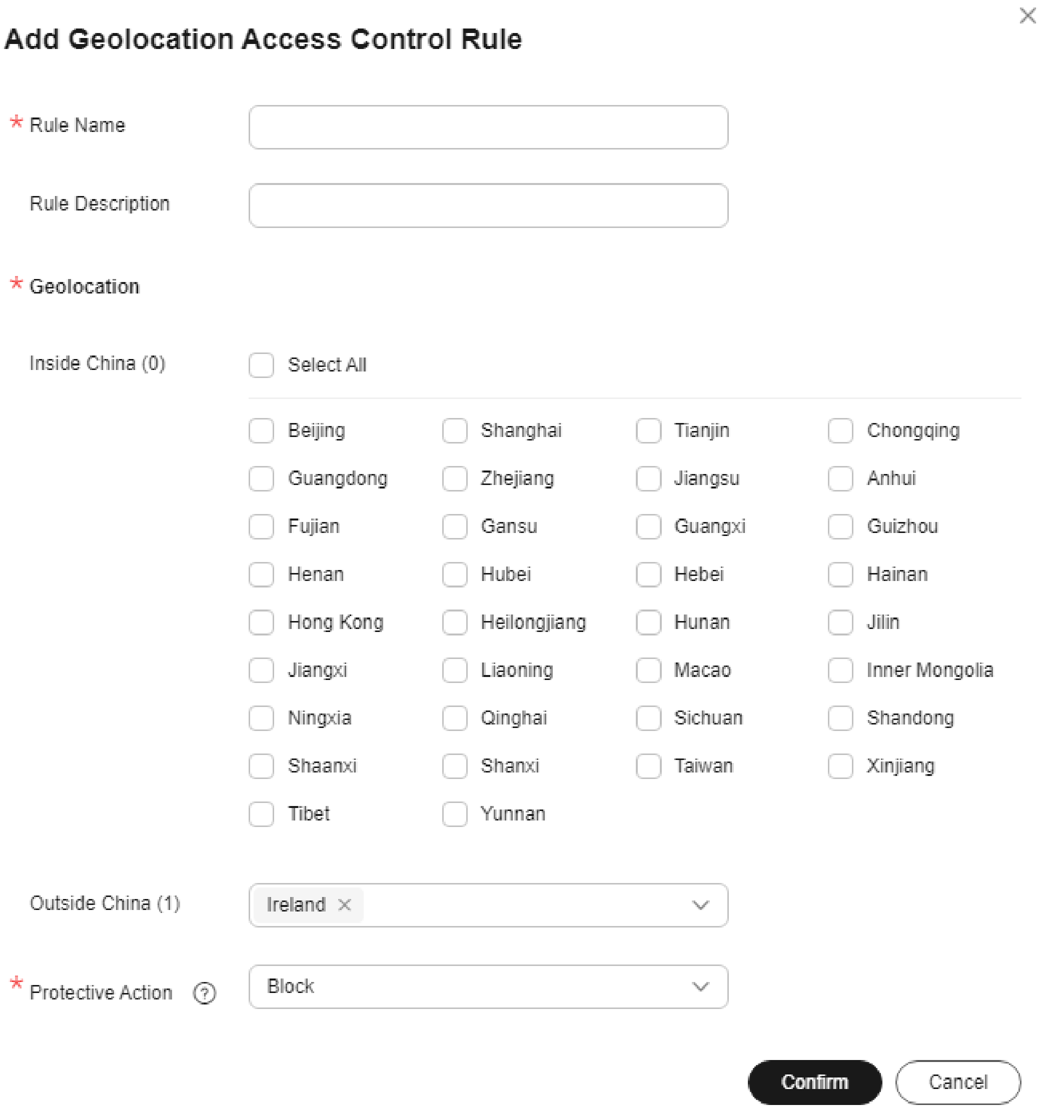
----End

Configuration Example - Blocking Access Requests from IP Addresses in a Specified Region

Assume that domain name *www.example.com* has been connected to WAF and you want to block all IP addresses from **Ireland** to access the domain name. The following shows how to configure a rule to this end:

Step 1 Add a geolocation access control rule, select **Ireland** for **Geolocation** and **Block** for **Protective Action**.

Figure 5-33 Blocking access requests from a specific region



Add Geolocation Access Control Rule

* Rule Name

Rule Description

* Geolocation

Inside China (0) □ Select All

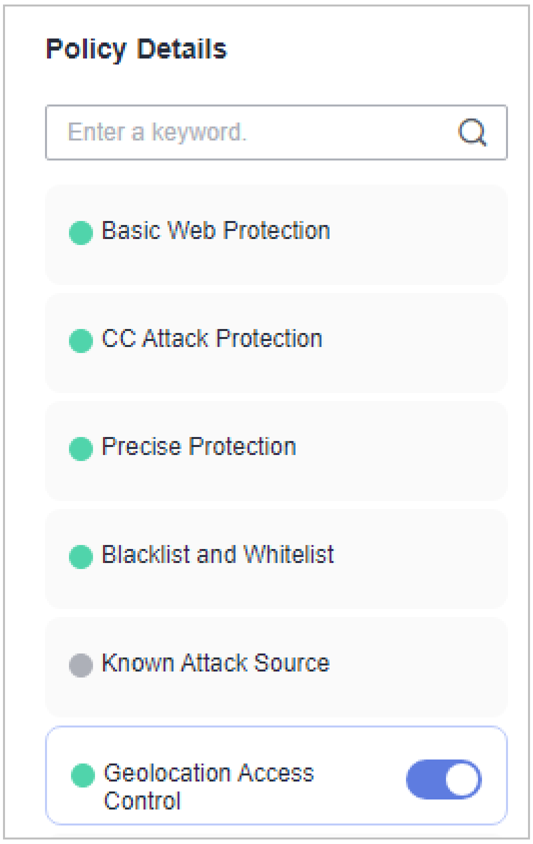
□ Beijing	□ Shanghai	□ Tianjin	□ Chongqing
□ Guangdong	□ Zhejiang	□ Jiangsu	□ Anhui
□ Fujian	□ Gansu	□ Guangxi	□ Guizhou
□ Henan	□ Hubei	□ Hebei	□ Hainan
□ Hong Kong	□ Heilongjiang	□ Hunan	□ Jilin
□ Jiangxi	□ Liaoning	□ Macao	□ Inner Mongolia
□ Ningxia	□ Qinghai	□ Sichuan	□ Shandong
□ Shaanxi	□ Shanxi	□ Taiwan	□ Xinjiang
□ Tibet	□ Yunnan		

Outside China (1) Ireland ×

* Protective Action Block

Step 2 Enable geolocation access control.

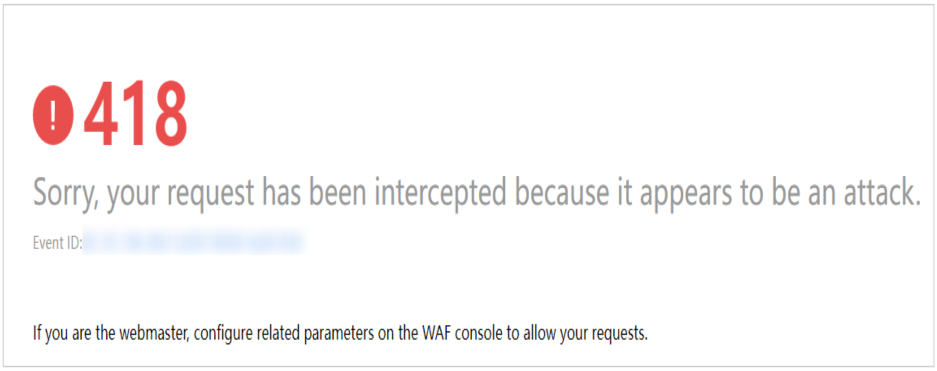
Figure 5-34 Geolocation Access Control configuration area



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

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

Figure 5-35 Block page



418

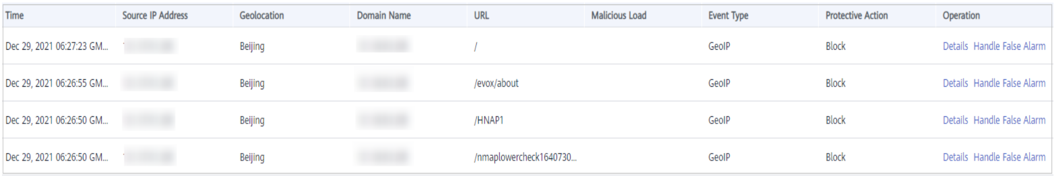
Sorry, your request has been intercepted because it appears to be an attack.

Event ID: [redacted]

If you are the webmaster, configure related parameters on the WAF console to allow your requests.

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

Figure 5-36 Viewing events - blocking access requests from IP addresses in a region



Time	Source IP Address	Geolocation	Domain Name	URL	Malicious Load	Event Type	Protective Action	Operation
Dec 29, 2021 06:27:23 GM...	[redacted]	Beijing	[redacted]	/		GeoIP	Block	Details Handle False Alarm
Dec 29, 2021 06:26:55 GM...	[redacted]	Beijing	[redacted]	/evox/about		GeoIP	Block	Details Handle False Alarm
Dec 29, 2021 06:26:50 GM...	[redacted]	Beijing	[redacted]	/HNAP1		GeoIP	Block	Details Handle False Alarm
Dec 29, 2021 06:26:50 GM...	[redacted]	Beijing	[redacted]	/nmaplowercheck1640730...		GeoIP	Block	Details Handle False Alarm

----End

Protection Effect

To verify WAF is protecting your website (**www.example.com**) against a rule:

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 referring to **Website Settings**.
- If the website is accessible, go to **2**.

Step 2 Add a geolocation access control rule by referring to **Configuring a Geolocation Access Control Rule**.

Step 3 Clear the browser cache and access **http://www.example.com**. Normally, WAF blocks such requests and returns the block page.

Step 4 Return to the WAF console. In the navigation pane, click **Events**. On the displayed page, view the event log.

----End

5.7 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.

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 the project.

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.

Prerequisites

You have **added your website to a policy**.

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.
- 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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 Click the name of the target policy to go to the protection configuration page.

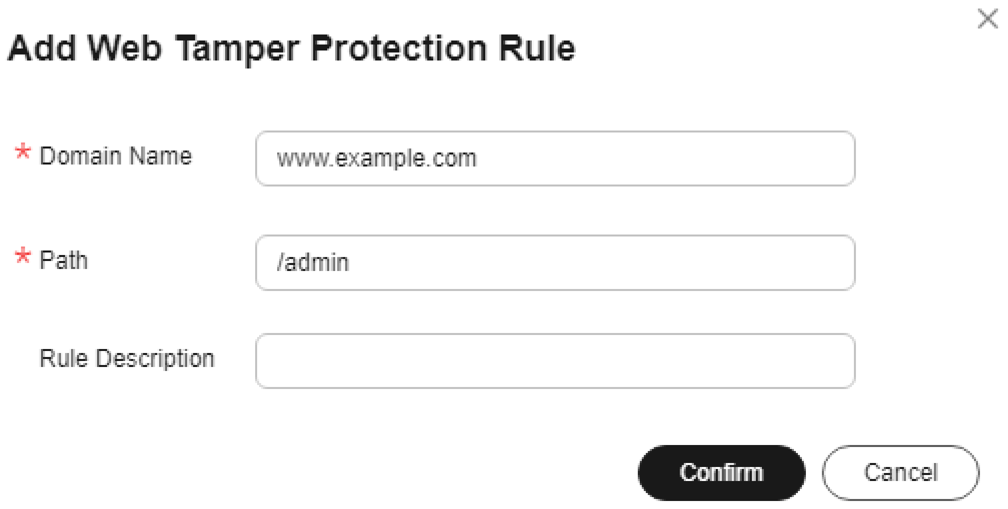
Step 6 Click the **Web Tamper Protection** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

Step 7 In the upper left corner above the **Web Tamper Protection** rule list, click **Add Rule**.

Step 8 In the displayed dialog box, specify the parameters by referring to **Table 5-8**.

Figure 5-37 Adding a web tamper protection rule



Add Web Tamper Protection Rule

* Domain Name: www.example.com

* Path: /admin

Rule Description:

Table 5-8 Rule parameters

Parameter	Description	Example Value
Domain Name	Domain name of the website to be protected	**www.example.com**

Parameter	Description	Example Value
Path	A part of the URL, not including the domain name A URL is used to define the address of a web page. The basic URL format is as follows: Protocol name://Domain name or IP address[:Port]/[Path/.../File name]. For example, if the URL is **http://www.example.com/admin**, set **Path** to **/admin**. **NOTE** ● The path 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**
Rule Description	A brief description of the rule. This parameter is optional.	None

Step 9 Click **Confirm**. You can view the rule in the list of web tamper protection rules.

----End

Related Operations

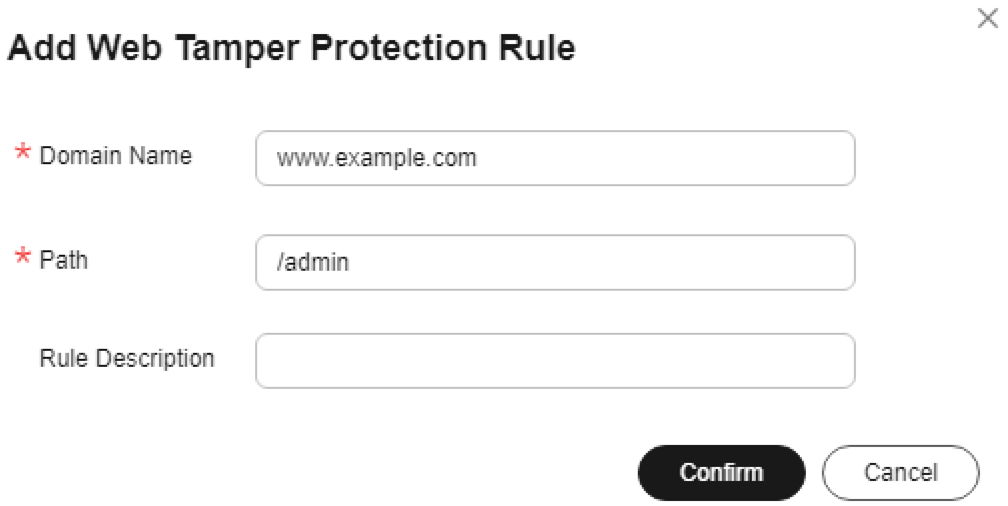
- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To update cache of a protected web page, click **Update Cache** in the row containing the corresponding web tamper protection rule. If the rule fails to be updated, WAF will return the recently cached page but not the latest page.
- To delete a rule, click **Delete** in the row containing the rule.

Configuration Example - Static Web Page Tamper Prevention

To verify WAF is protecting a static page **/admin** on your website **www.example.com** from being tampered with:

Step 1 Add a web tamper prevention rule to WAF.

Figure 5-38 Adding a web tamper protection rule



Add Web Tamper Protection Rule

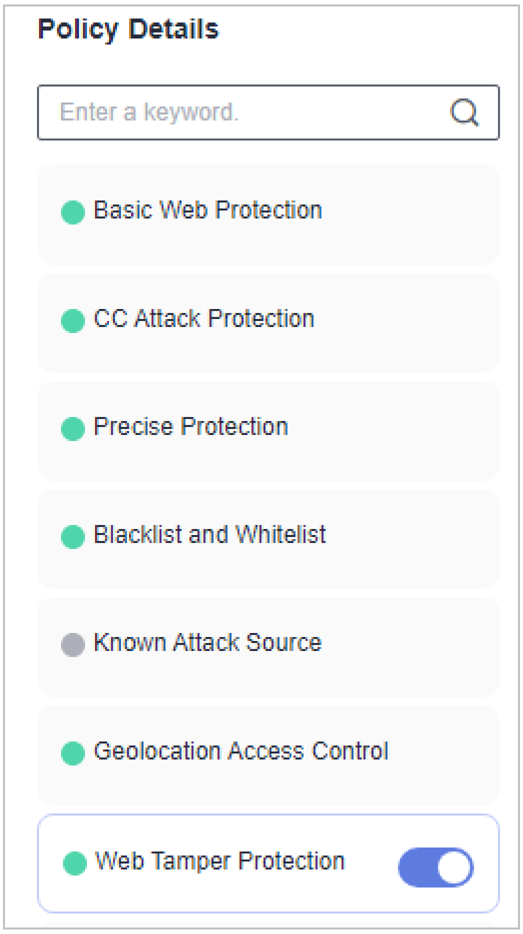
* Domain Name: www.example.com

* Path: /admin

Rule Description:

Step 2 Enable WTP.

Figure 5-39 Web Tamper Protection configuration area



Policy Details

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 **http://www.example.com/admin** again.

The intact page is returned.

----End

5.8 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.

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 the project.

Prerequisites

A website has been added to WAF.

Constraints

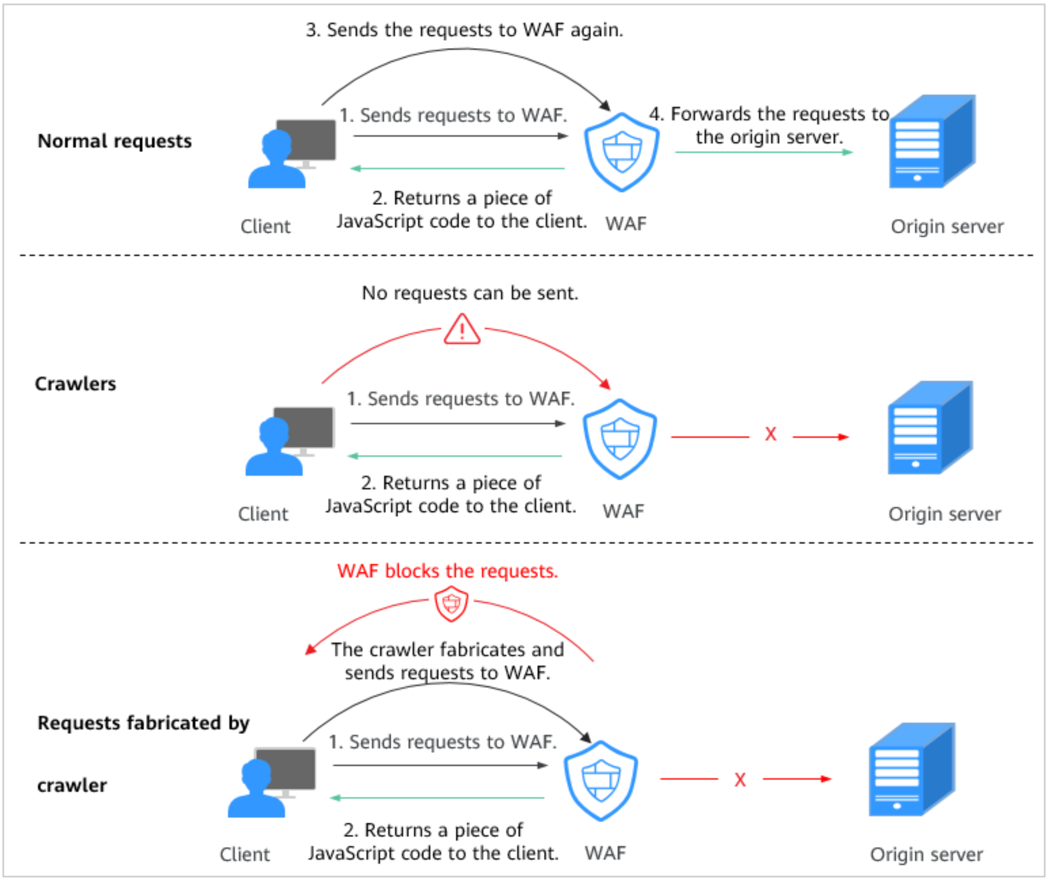
- Cookies must be enabled and JavaScript supported by any browser used to access a website protected by anti-crawler protection rules.
- If your service is connected to CDN, exercise caution when using the JS anti-crawler function.

  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.
- 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?**
- WAF only logs JavaScript challenge and JavaScript authentication events. No other protective actions can be configured for JavaScript challenge and authentication.
- WAF JavaScript-based anti-crawler rules only check GET requests and do not check POST requests.

How JavaScript Anti-Crawler Protection Works

Figure 5-40 shows how JavaScript anti-crawler detection works, which includes JavaScript challenges (step 1 and step 2) and JavaScript authentication (step 3).

Figure 5-40 JavaScript Anti-Crawler protection process

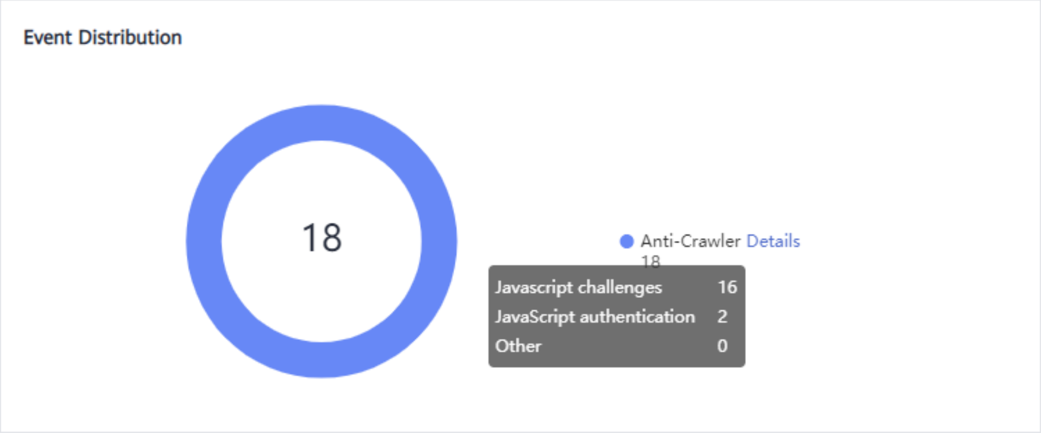

3. Sends the requests to WAF again.
Normal requests
1. Sends requests to WAF.
4. Forwards the requests to the origin server.
2. Returns a piece of JavaScript code to the client.
Client
WAF
Origin server
No requests can be sent.
Crawlers
1. Sends requests to WAF.
2. Returns a piece of JavaScript code to the client.
X
Client
WAF
Origin server
WAF blocks the requests.
The crawler fabricates and sends requests to WAF.
Requests fabricated by crawler
1. Sends requests to WAF.
2. Returns a piece of JavaScript code to the client.
X
Client
WAF
Origin server

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 5-41**, the JavaScript anti-crawler has logged 18 events, 16 of which are JavaScript challenge responses, and 2 of which are JavaScript authentication responses. **Others** indicates the number of WAF authentication requests fabricated by the crawler.

Figure 5-41 Parameters of a JavaScript anti-crawler protection rule



Javascript challenges	16
JavaScript authentication	2
Other	0

NOTICE

WAF only logs JavaScript challenge and JavaScript authentication events. No other protective actions can be configured for JavaScript challenge and authentication.

Configuring an Anti-Crawler Rule

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 **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 Click the name of the target policy to go to the protection configuration page.

Step 6 Click the **Anti-Crawler** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

Step 7 Select the **Feature Library** tab and enable the protection by referring to **Table 5-9**.

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:

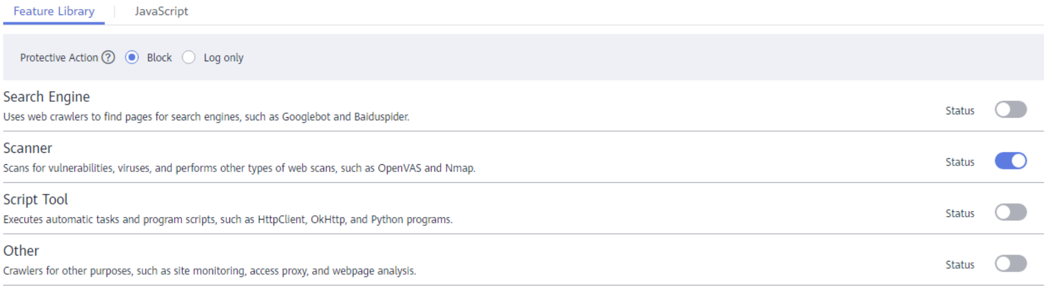
- Blocking requests of search engines may affect your website SEO.
- Blocking scripts may block some applications because those applications may trigger anti-crawler rules if their user-agent field is not modified.

- **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 5-42 Feature Library



Feature Library | JavaScript

Protective Action ● Block ○ Log only

Search Engine
Uses web crawlers to find pages for search engines, such as Googlebot and Baiduspider.
Status ○

Scanner
Scans for vulnerabilities, viruses, and performs other types of web scans, such as OpenVAS and Nmap.
Status ●

Script Tool
Executes automatic tasks and program scripts, such as HttpClient, OkHttp, and Python programs.
Status ○

Other
Crawlers for other purposes, such as site monitoring, access proxy, and webpage analysis.
Status ○

Table 5-9 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**.
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.

Type	Description	Remarks
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 8 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 ●.

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.

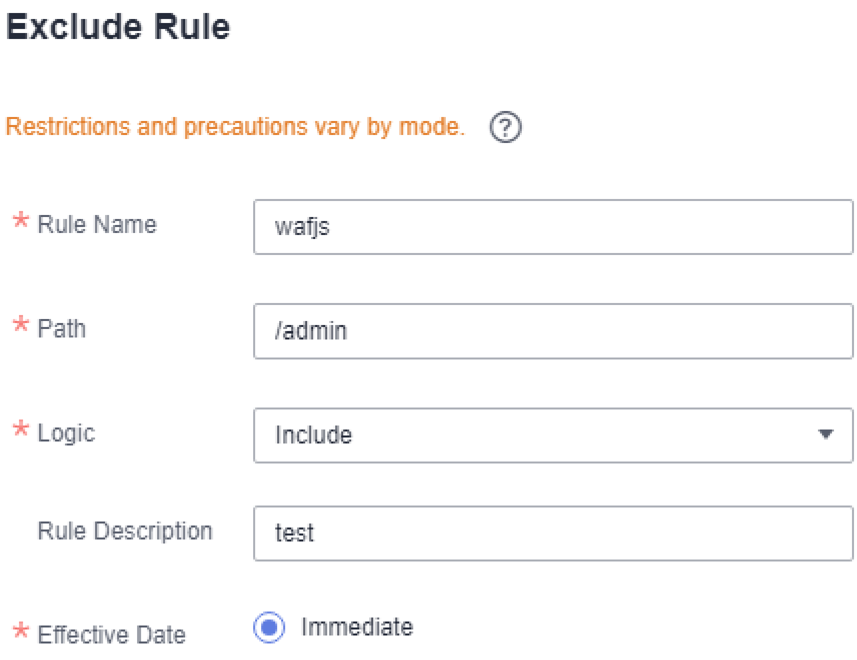
Step 9 Configure a JavaScript-based anti-crawler rule by referring to **Table 5-10**.

Two protective actions are provided: **Protect all requests** and **Protect specified requests**.

- To protect all paths except a specified path

  Set **Protection Mode** to **Protect all paths**. Then, click **Exclude Path**, configure protected paths, and click **Confirm**.

Figure 5-43 Exclude Rule



Exclude Rule

Restrictions and precautions vary by mode.

* Rule Name: wafjs

* Path: /admin

* Logic: Include

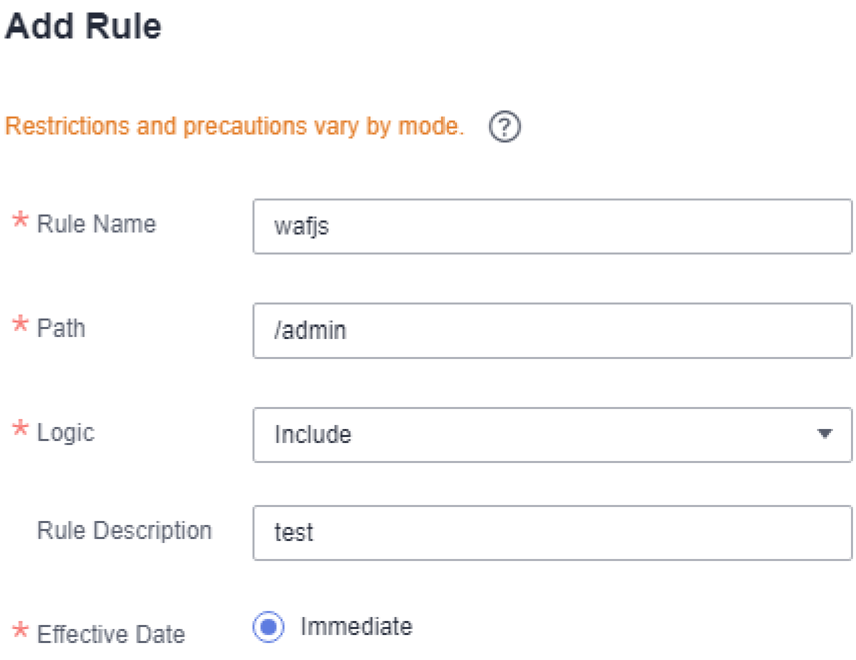
Rule Description: test

* Effective Date: ● Immediate

- To protect a specified path only

  Set **Protection Mode** to **Protect specified requests**, click **Add Rule**, configure the request rule, and click **Confirm**.

Figure 5-44 Add Rule



Add Rule

Restrictions and precautions vary by mode.

* Rule Name: wafjs

* Path: /admin

* Logic: Include

Rule Description: test

* Effective Date: ● Immediate

Table 5-10 Parameters of a JavaScript-based anti-crawler protection rule

Parameter	Description	Example Value
Rule Name	Name of the rule	wafjs
Path	A part of the URL, not including the domain name A URL is used to define the address of a web page. The basic URL format is as follows: Protocol name://Domain name or IP address[:Port]/[Path/.../File name]. For example, if the URL is **http://www.example.com/admin**, set **Path** to **/admin**. **NOTE** ● The path 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
Logic	Select a logical relationship from the drop-down list.	Include
Rule Description	A brief description of the rule.	None
Effective Date	Immediate	Immediate

----End

Related Operations

- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

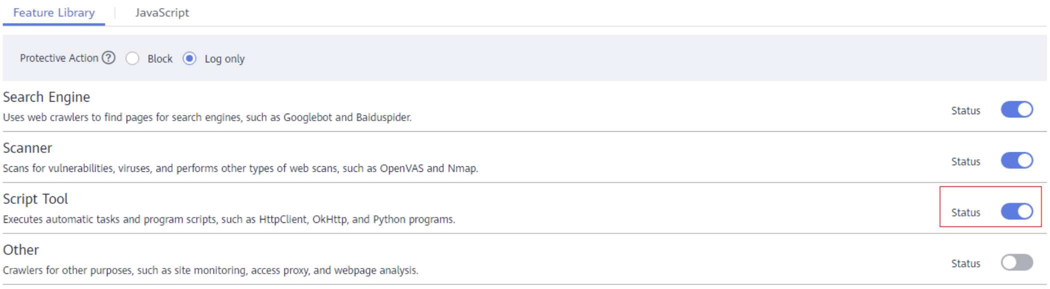
Configuration Example - Logging Script Crawlers Only

To verify that WAF is protecting 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 5-45 Enabling Script Tool



Feature Library | JavaScript

Protective Action ○ Block ● Log only

Search Engine
Uses web crawlers to find pages for search engines, such as Googlebot and Baiduspider.
Status: on

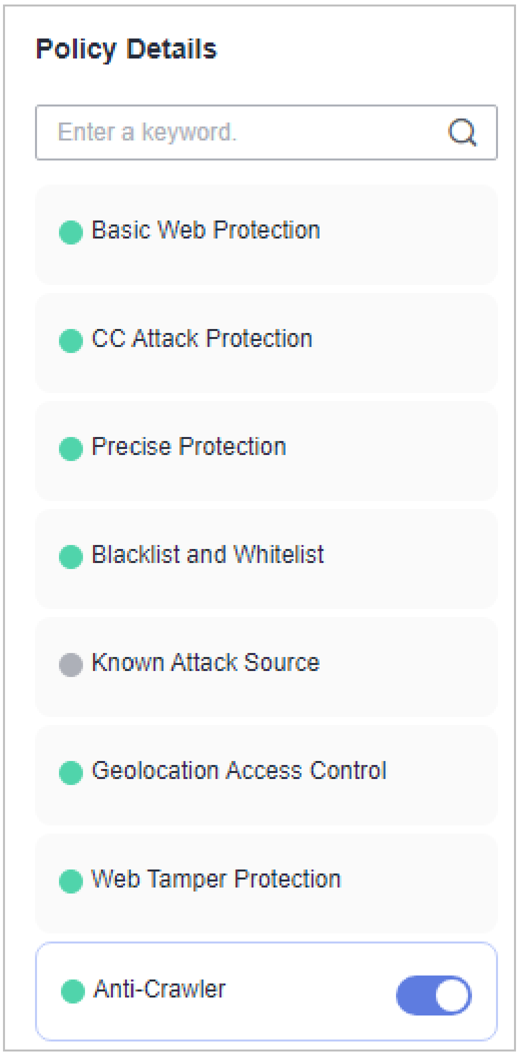
Scanner
Scans for vulnerabilities, viruses, and performs other types of web scans, such as OpenVAS and Nmap.
Status: on

Script Tool
Executes automatic tasks and program scripts, such as HttpClient, OkHttp, and Python programs.
Status: on

Other
Crawlers for other purposes, such as site monitoring, access proxy, and webpage analysis.
Status: off

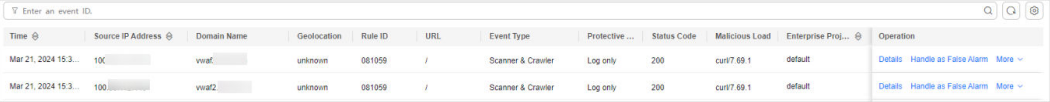
Step 3 Enable anti-crawler protection.

Figure 5-46 Anti-Crawler configuration area



Step 4 In the navigation pane on the left, choose **Events** to go to the **Events** page.

Figure 5-47 Viewing Events - Script crawlers



Time	Source IP Address	Domain Name	Geolocation	Rule ID	URL	Event Type	Protective ...	Status Code	Malicious Load	Enterprise Proj...	Operation
Mar 21, 2024 15:3...	10([redacted]	vwaf. [redacted]	unknown	081059	/	Scanner & Crawler	Log only	200	curl/7.69.1	default	Details Handle as False Alarm More
Mar 21, 2024 15:3...	100. [redacted]	vwaf2. [redacted]	unknown	081059	/	Scanner & Crawler	Log only	200	curl/7.69.1	default	Details Handle as False Alarm More

----End

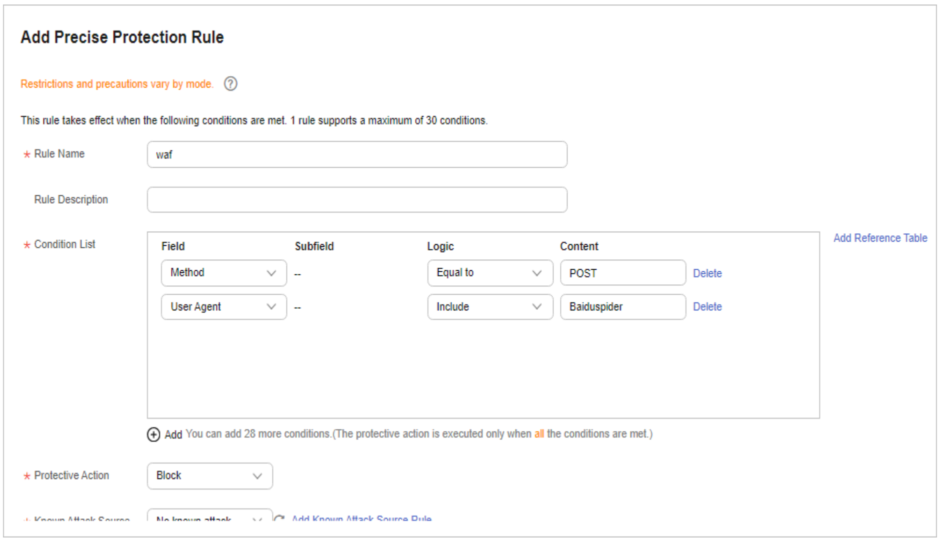
Configuration Example - Search Engine

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 6**.

Step 2 Configure a precise protection rule by referring to **Configuring Custom Precise Protection Rules**.

Figure 5-48 Blocking POST requests



Add Precise Protection Rule

Restrictions and precautions vary by mode.

This rule takes effect when the following conditions are met. 1 rule supports a maximum of 30 conditions.

* Rule Name: waf

Rule Description:

* Condition List

Field	Subfield	Logic	Content	
Method	--	Equal to	POST	Delete
User Agent	--	Include	Baiduspider	Delete

Add Reference Table

Add You can add 28 more conditions.(The protective action is executed only when all the conditions are met.)

* Protective Action: Block

* Known Attack Source: No known attack — Add Known Attack Source Rule

----End

5.9 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, and email addresses.
- Response code interception: blocks the specified HTTP status codes.

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 the project.

Prerequisites

You have **added your website to a policy**.

Constraints

- 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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 Click the name of the target policy to go to the protection configuration page.

Step 6 Click the **Information Leakage Prevention** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

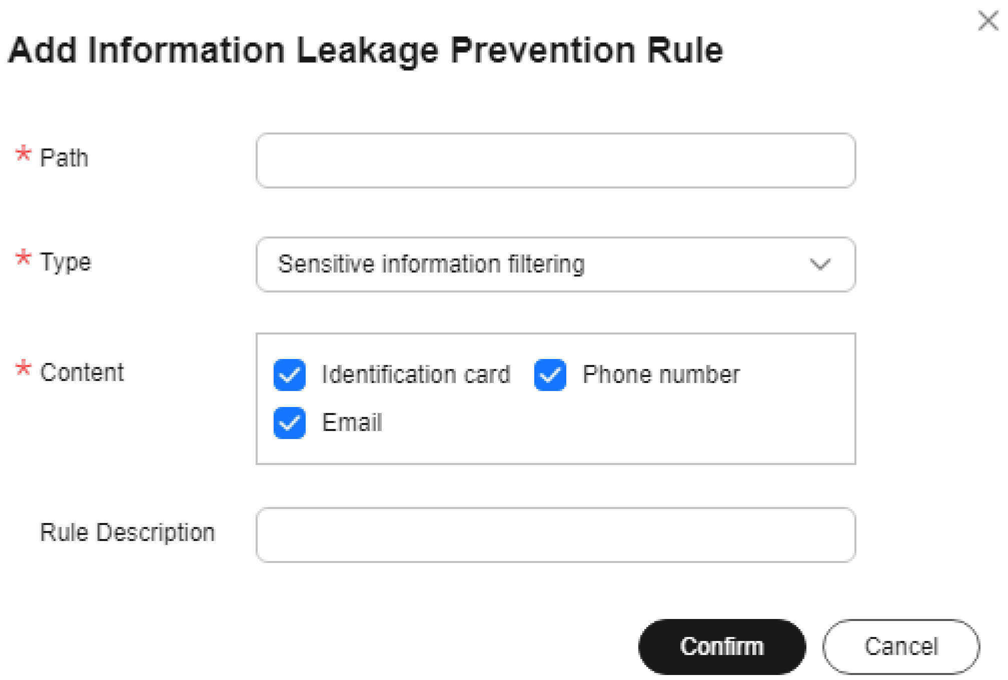
Step 7 In the upper left corner above the **Information Leakage Prevention** rule list, click **Add Rule**.

Step 8 In the dialog box displayed, add an information leakage prevention rule by referring to **Table 5-11**.

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 5-49 Sensitive information leakage



Add Information Leakage Prevention Rule

* Path

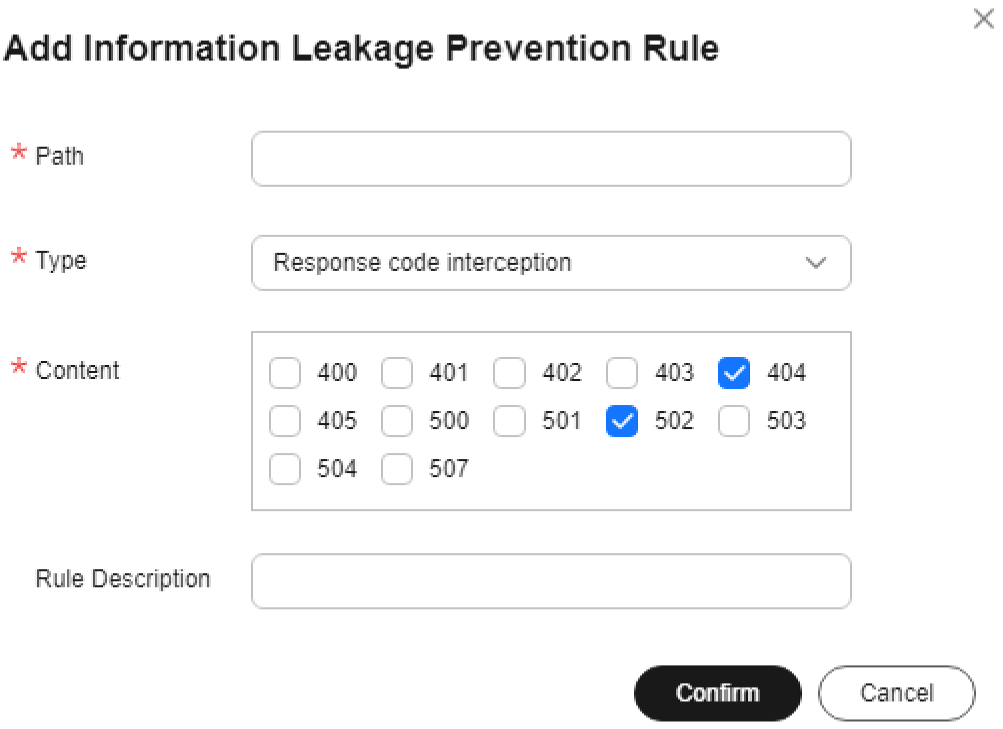
* Type: Sensitive information filtering

* Content: ☑ Identification card ☑ Phone number ☑ Email

Rule Description

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 5-50 Blocking response codes



Add Information Leakage Prevention Rule

* Path

* Type: Response code interception

* Content

☐ 400 ☐ 401 ☐ 402 ☐ 403 ☑ 404
☐ 405 ☐ 500 ☐ 501 ☑ 502 ☐ 503
☐ 504 ☐ 507

Rule Description

Table 5-11 Rule parameters

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***
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**
Rule Description	A brief description of the rule. This parameter is optional.	None

Step 9 Click **Confirm**. The added information leakage prevention rule is displayed in the list of information leakage prevention rules.

----End

Related Operations

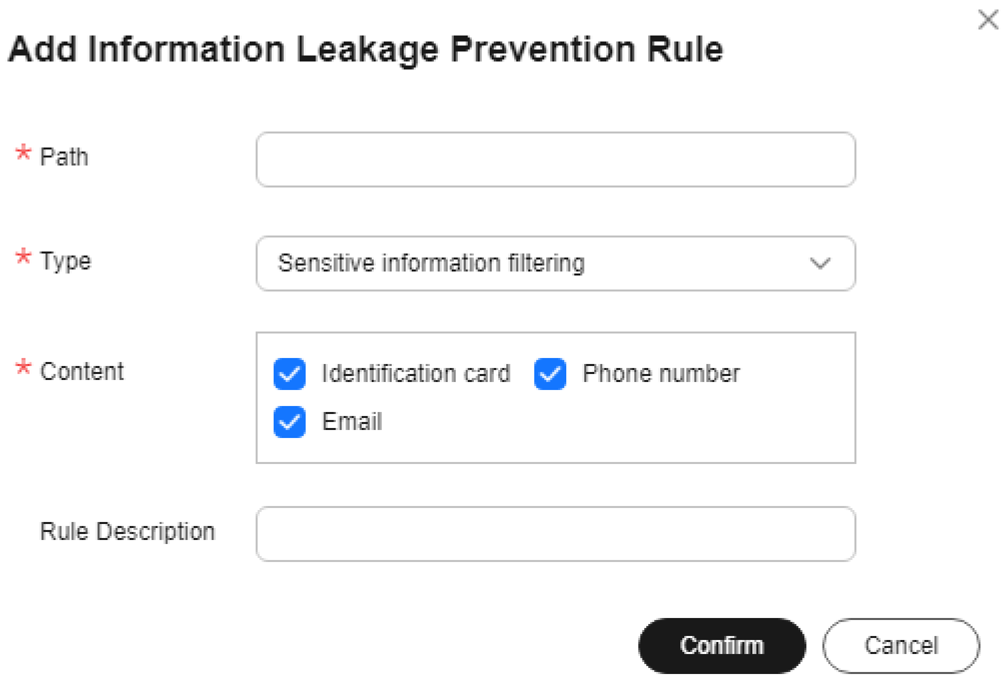
- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

Configuration Example — Masking Sensitive Information

To verify that WAF is protecting your domain name *www.example.com* against an information leakage prevention rule:

Step 1 Add an information leakage prevention rule.

Figure 5-51 Sensitive information leakage



Add Information Leakage Prevention Rule

* Path

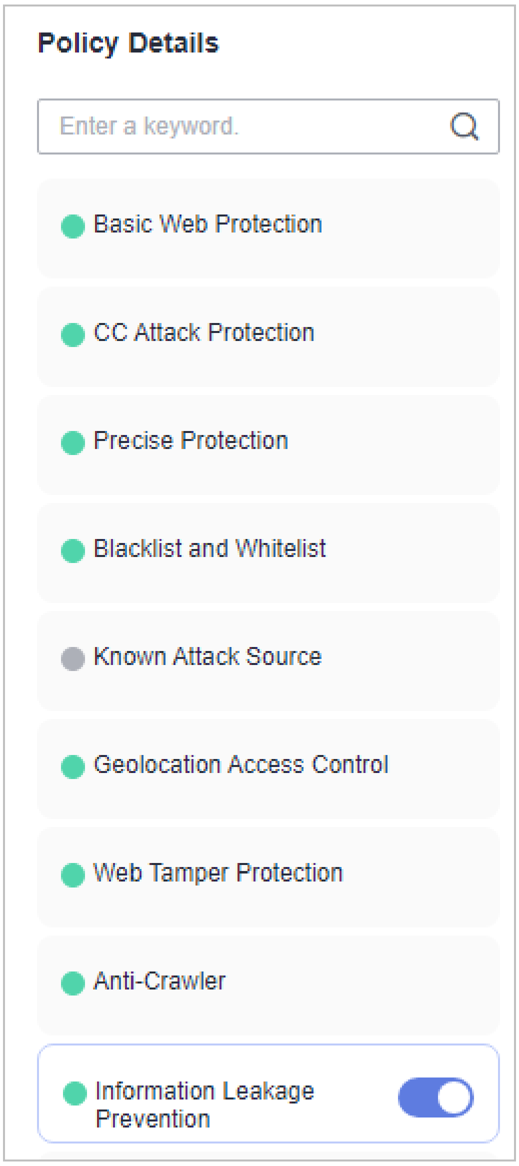
* Type: Sensitive information filtering

* Content: ☑ Identification card ☑ Phone number ☑ Email

Rule Description

Step 2 Enable information leakage prevention.

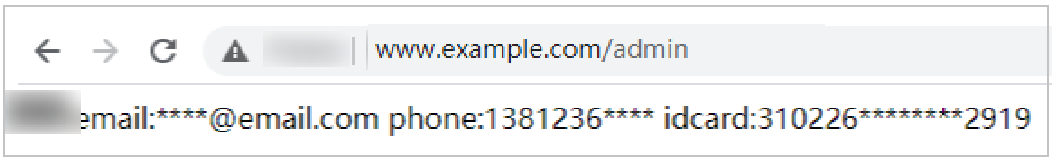
Figure 5-52 Information Leakage Prevention configuration area



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 5-53 Sensitive information masked



[redacted] email:****@email.com phone:1381236**** idcard:310226********2919

----End

5.10 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.

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 the project.

Prerequisites

A website has been added to WAF.

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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 Click the name of the target policy to go to the protection configuration page.

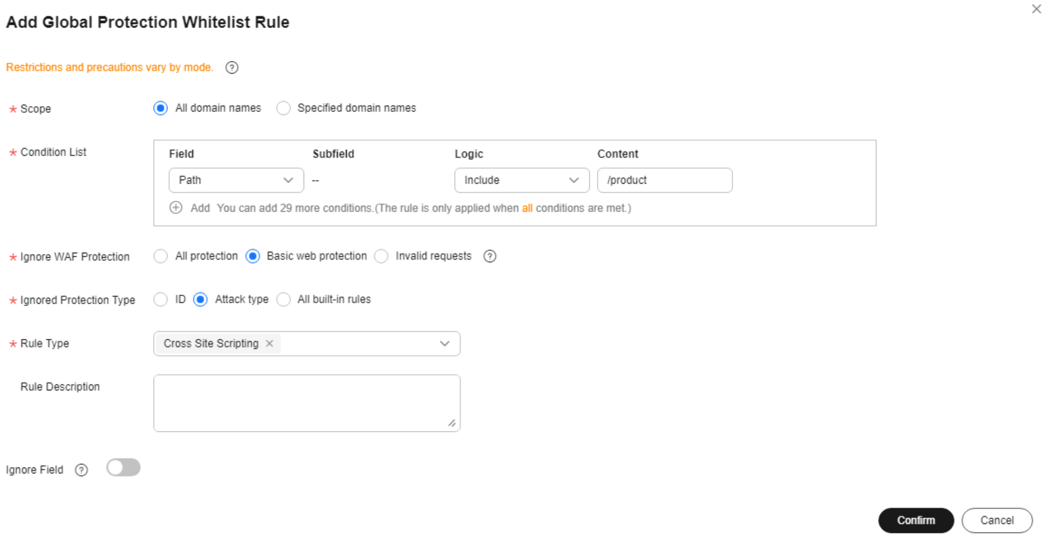
Step 6 Click the **Blacklist and Whitelist** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

Step 7 In the upper left corner above the **Global Protection Whitelist** rule list, click **Add Rule**.

Step 8 Add a global whitelist rule by referring to **Table 5-12**.

Figure 5-54 Add Global Protection Whitelist Rule



Add Global Protection Whitelist Rule

Restrictions and precautions vary by mode.

* Scope: ● All domain names ○ Specified domain names

* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/product

Add You can add 29 more conditions.(The rule is only applied when all conditions are met.)

* Ignore WAF Protection: ○ All protection ● Basic web protection ○ Invalid requests

* Ignored Protection Type: ○ ID ● Attack type ○ All built-in rules

* Rule Type: Cross Site Scripting

Rule Description:

Ignore Field

Table 5-12 Parameters

Parameter	Description	Example Value
Scope	● **All domain names**: By default, this rule will be used 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.	www.example.com
Condition List	Click **Add** 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. A condition includes the following parameters: Parameters for configuring a condition are described as follows: ● **Field** ● **Subfield**: Configure this field only when **Params**, **Cookie**, or **Header** is selected for **Field**. **NOTICE** The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed. ● **Logic**: Select a logical relationship from the drop-down list. ● **Content**: Enter or select the content that matches the condition.	Path, Include, / 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 Protection Type**, specify the following parameters: - **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 attack events of 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 9 Click **Confirm**.

----End

Related Operations

- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

5.11 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.

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 the project.

Prerequisites

A website has been added to WAF.

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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 Click the name of the target policy to go to the protection configuration page.

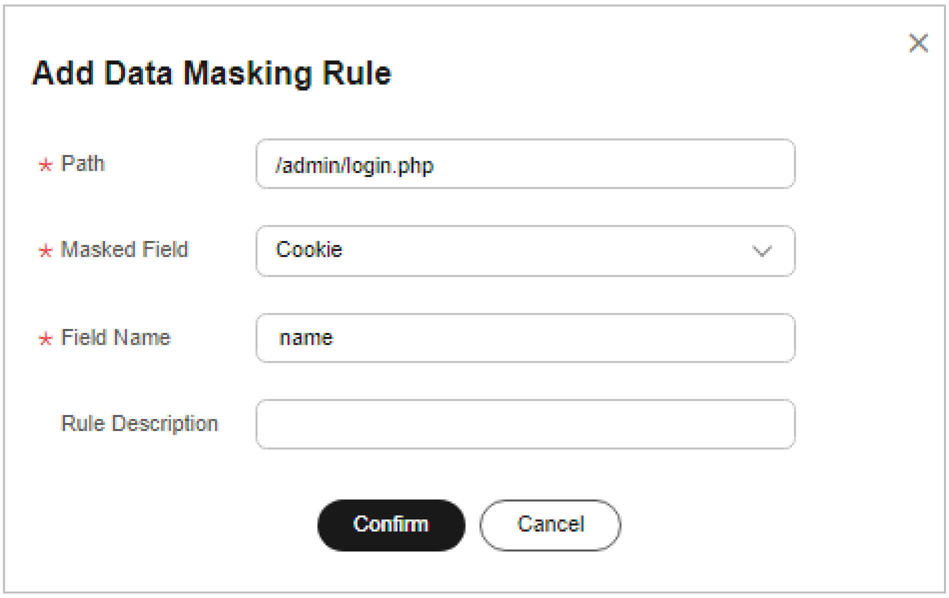
Step 6 Click the **Data Masking** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

Step 7 In the upper left corner above the **Data Masking** rule list, click **Add Rule**.

Step 8 In the displayed dialog box, specify the parameters described in **Table 5-13**.

Figure 5-55 Adding a data masking rule



Add Data Masking Rule

* Path: /admin/login.php
* Masked Field: Cookie
* Field Name: name
Rule Description:

Table 5-13 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**.

Parameter	Description	Example Value
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 9 Click **Confirm**. The added data masking rule is displayed in the list of data masking rules.

----End

Related Operations

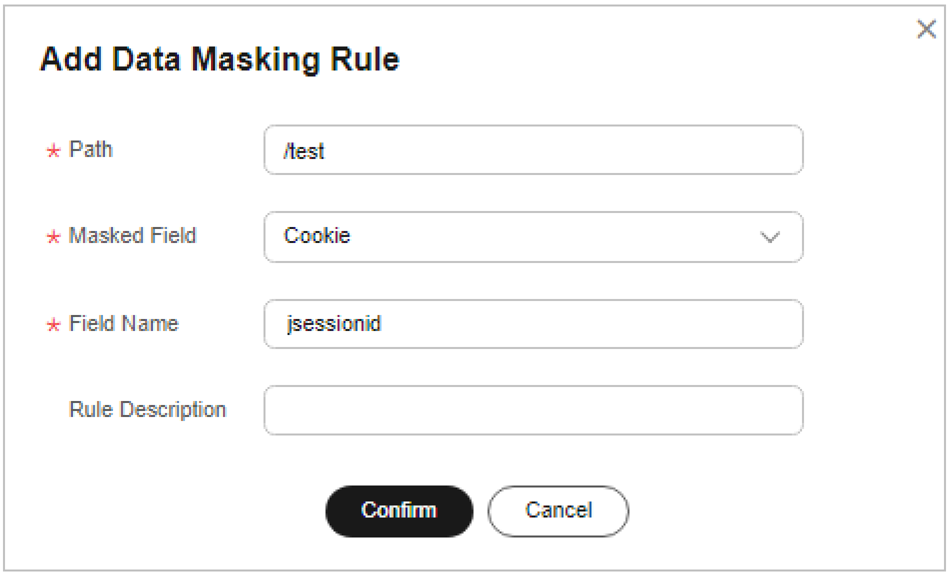
- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

Configuration Example - Masking the Cookie Field

To verify that WAF is protecting your domain name *www.example.com* against a data masking rule (with **Cookie** selected for **Masked Field** and **jsessionid** entered in **Field Name**):

Step 1 Add a data masking rule.

Figure 5-56 Select **Cookie** for **Masked Field** and enter **jsessionid** in **Field Name**.



Add Data Masking Rule

* Path: /test

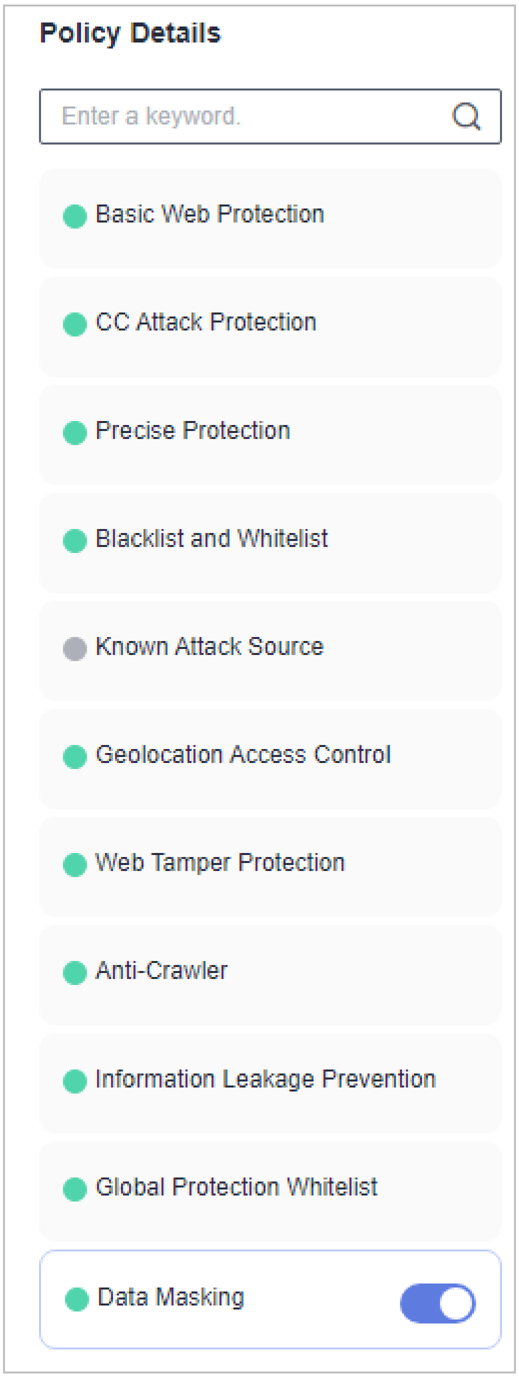
* Masked Field: Cookie

* Field Name: jsessionid

Rule Description:

Step 2 Enable data masking.

Figure 5-57 Data Masking configuration area



Policy Details

Enter a keyword.

● Basic Web Protection

● CC Attack Protection

● Precise Protection

● Blacklist and Whitelist

● Known Attack Source

● Geolocation Access Control

● Web Tamper Protection

● Anti-Crawler

● Information Leakage Prevention

● Global Protection Whitelist

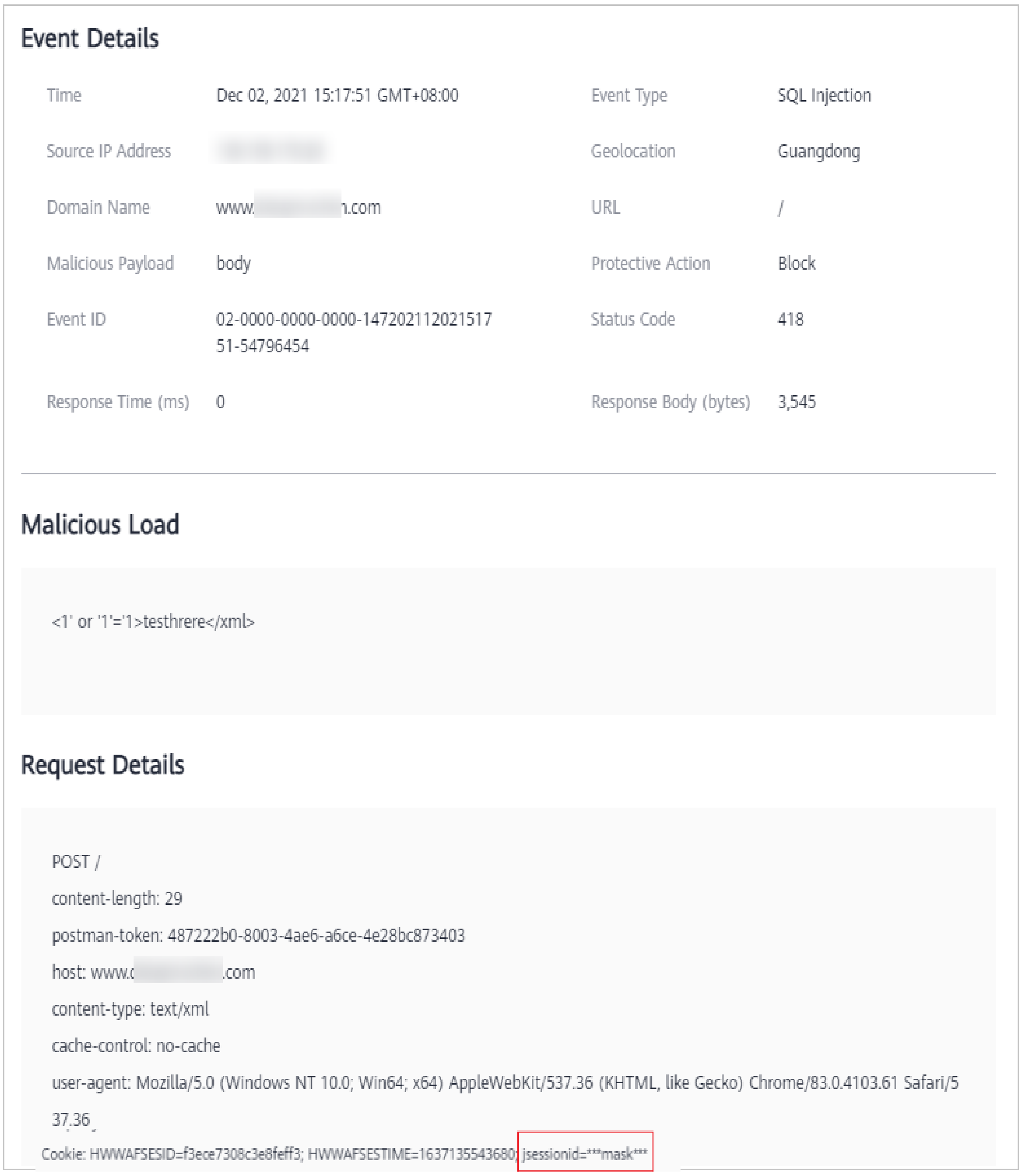
● Data Masking

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 5-58 Viewing events - privacy data masking



Event Details

Time	Dec 02, 2021 15:17:51 GMT+08:00	Event Type	SQL Injection
Source IP Address	[redacted]	Geolocation	Guangdong
Domain Name	www.[redacted]n.com	URL	/
Malicious Payload	body	Protective Action	Block
Event ID	02-0000-0000-0000-147202112021517 51-54796454	Status Code	418
Response Time (ms)	0	Response Body (bytes)	3,545

Malicious Load

```
<1' or '1'='1>testhrere</xml>
```

Request Details

```
POST /
content-length: 29
postman-token: 487222b0-8003-4ae6-a6ce-4e28bc873403
host: www.c[redacted].com
content-type: text/xml
cache-control: no-cache
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/5
37.36
Cookie: HWWAFSESID=f3ece7308c3e8feff3; HWWAFSESTIME=1637135543680; jsessionid=***mask***
```

----End

5.12 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 and precise protection rules.

When you configure a CC attack protection 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.

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 the project.

Prerequisites

A website has been added to WAF.

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 and precise protection rules.

Creating a Reference Table

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 **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 Click the name of the target policy to go to the protection configuration page.

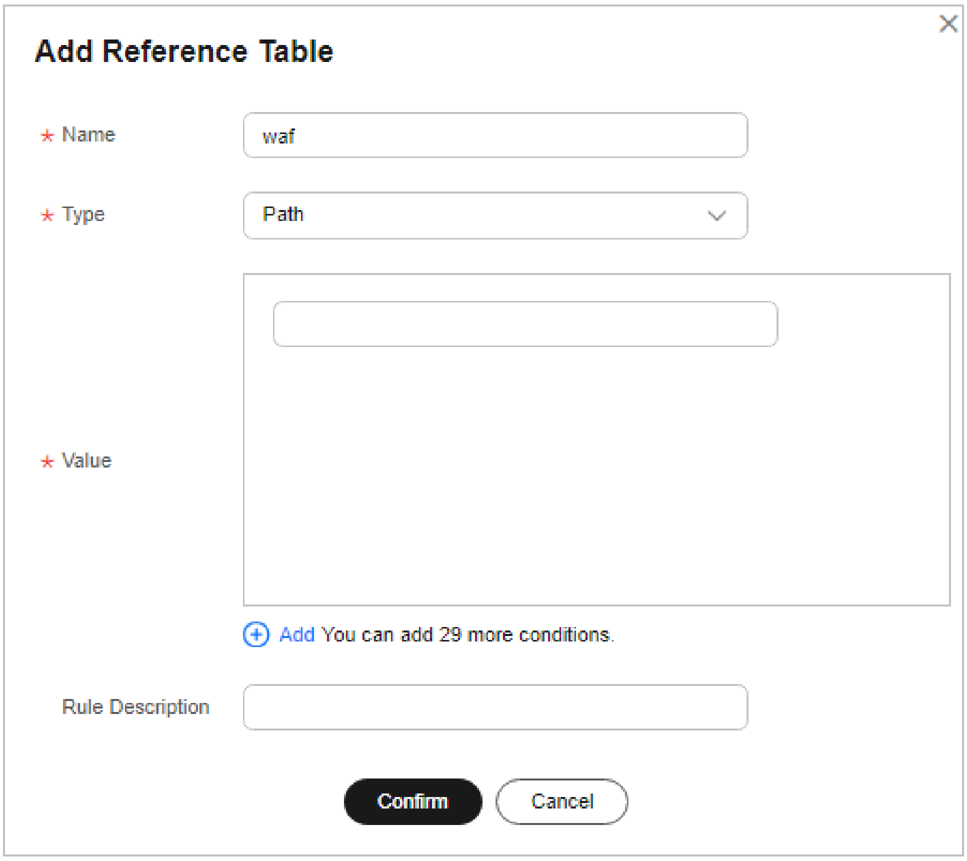
Step 6 Click the **CC Attack Protection** or **Precise Protection** configuration area.

Step 7 Click **Reference Table Management** in the upper left corner of the list.

Step 8 On the **Reference Table Management** page, click **Add Reference Table**.

Step 9 In the **Add Reference Table** dialog box, specify the parameters by referring to **Table 5-14**.

Figure 5-59 Adding a reference table



Add Reference Table

* Name: waf

* Type: Path

* Value

Add You can add 29 more conditions.

Rule Description

Table 5-14 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. ● **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	**Path**
Value	Value of the corresponding **Type**. Wildcards are not allowed. **NOTE** Click **Add** to add more than one value.	**/buy/phone/**
Rule Description	Description of the rule.	-

Step 10 Click **Confirm**. You can then view the added reference table in the reference table list.

----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.

5.13 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 an 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, precise protection, IP address blacklist, IP address whitelist, and other rules. You can use known attack source rules in basic web protection, precise protection, and IP blacklist or whitelist rules as long as you set **Protective Action** to **Block** for these rules.

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 the project.

Prerequisites

A website has been added to WAF.

Constraints

- For a known attack source rule to take effect, it must be enabled when you configure basic web protection, precise protection, blacklist, or 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 by 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**.
- 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.

- The maximum time an IP address can be blocked for is 30 minutes.

Configuring a Known Attack Source Rule

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 **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 Click the name of the target policy to go to the protection configuration page.

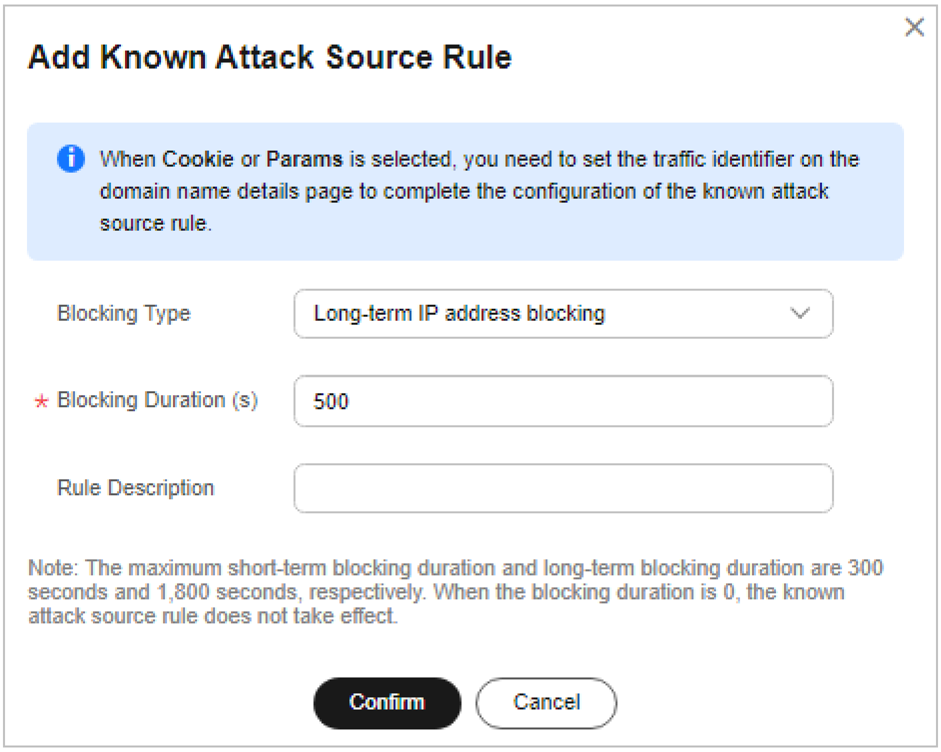
Step 6 Click the **Known Attack Source** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

Step 7 In the upper left corner above the known attack source rules, click **Add Known Attack Source Rule**.

Step 8 In the displayed dialog box, specify the parameters by referring to **Table 5-15**.

Figure 5-60 Add Known Attack Source Rule



Add Known Attack Source Rule

When Cookie or Params is selected, you need to set the traffic identifier on the domain name details page to complete the configuration of the known attack source rule.

Blocking Type: Long-term IP address blocking

* Blocking Duration (s): 500

Rule Description:

Note: The maximum short-term blocking duration and long-term blocking duration are 300 seconds and 1,800 seconds, respectively. When the blocking duration is 0, the known attack source rule does not take effect.

Table 5-15 Known attack source parameters

Parameter	Description	Example Value
Blocking Type	Specifies the blocking type. 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: ● (300, 1800] for long-term blocking ● (0, 300] for short-term blocking	500
Rule Description	A brief description of the rule. This parameter is optional.	None

Step 9 Click **Confirm**. You can then view the added known attack source rule in the list.

----End

Related Operations

- To modify a rule, click **Modify** in row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

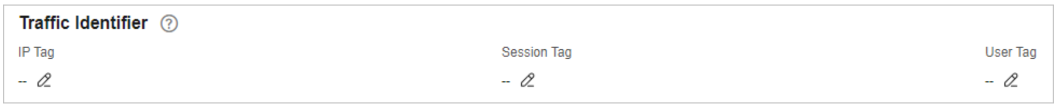
Configuration Example - Blocking Known Attack Source Identified by Cookie

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. Refer to the following steps to configure a rule and verify its effect.

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 5-61 Traffic Identifier

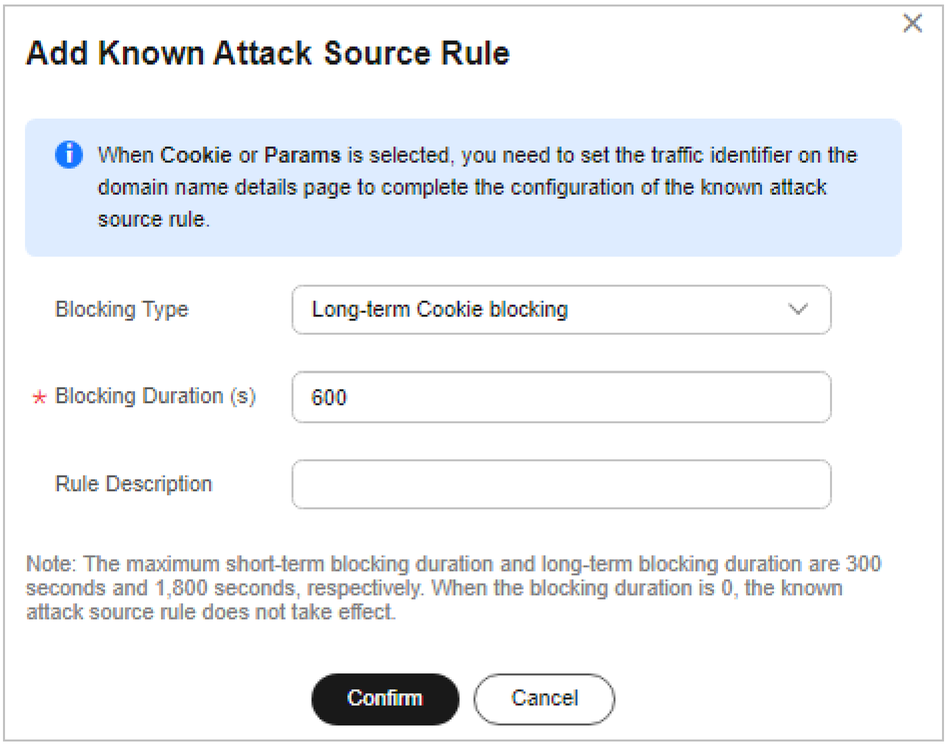


Traffic Identifier

IP Tag	Session Tag	User Tag
--	--	--

Step 3 Add a known attack source, select **Long-term Cookie blocking** for **Blocking Type**, and set block duration to 600 seconds.

Figure 5-62 Adding a Cookie-based known attack source rule



Add Known Attack Source Rule

When **Cookie** or **Params** is selected, you need to set the traffic identifier on the domain name details page to complete the configuration of the known attack source rule.

Blocking Type: Long-term Cookie blocking

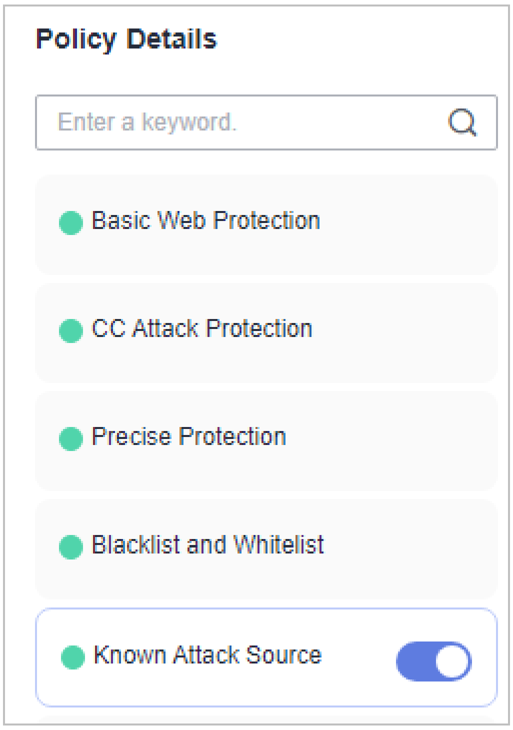
* Blocking Duration (s): 600

Rule Description:

Note: The maximum short-term blocking duration and long-term blocking duration are 300 seconds and 1,800 seconds, respectively. When the blocking duration is 0, the known attack source rule does not take effect.

Step 4 Enable the known attack source protection.

Figure 5-63 Known Attack Source configuration area



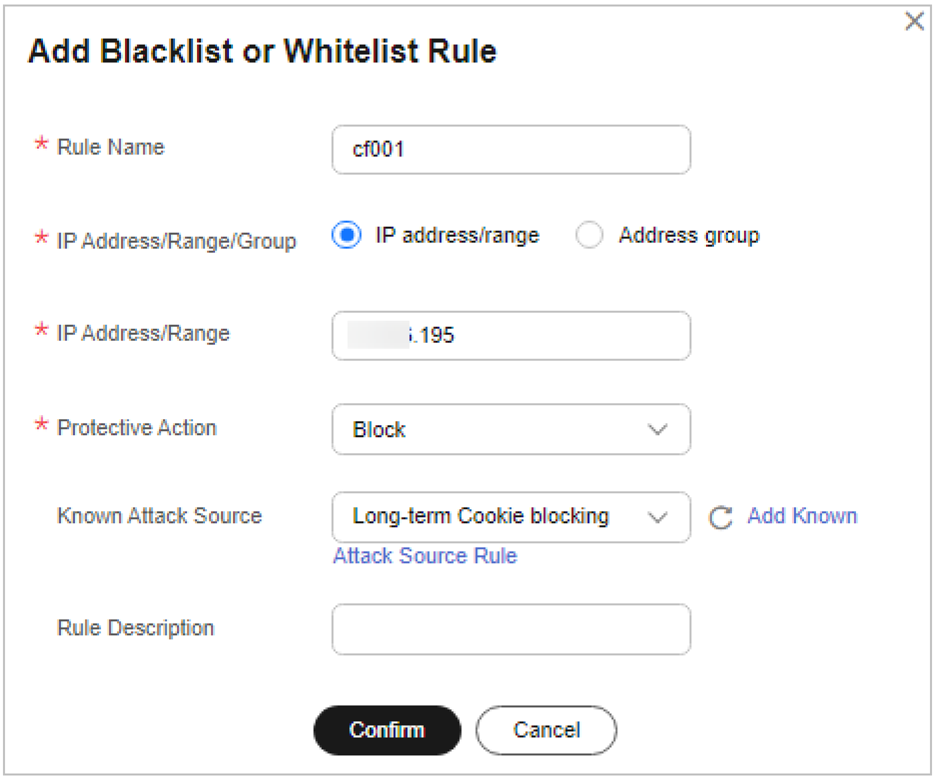
Policy Details

Enter a keyword.

- ● Basic Web Protection
- ● CC Attack Protection
- ● Precise Protection
- ● Blacklist and Whitelist
- ● Known Attack Source (enabled)

Step 5 Add a blacklist and whitelist rule to block *XXX.XXX.248.195*. Select **Long-term Cookie blocking** for **Known Attack Source**.

Figure 5-64 Specifying a known attack source rule



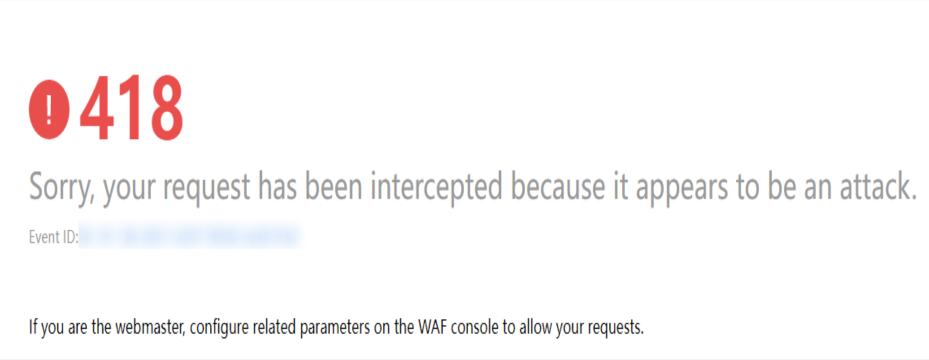
Add Blacklist or Whitelist Rule

* Rule Name	cf001
* IP Address/Range/Group	● IP address/range ○ Address group
* IP Address/Range	[redacted].195
* Protective Action	Block
Known Attack Source	Long-term Cookie blocking
Rule Description	

Step 6 Clear the browser cache and access http://www.example.com.

When a request from IP address *XXX.XXX.248.195*, WAF blocks the access. When WAF detects that the cookie of the access request from the IP address is **jsessionid**, WAF blocks the access request for 10 minutes.

Figure 5-65 Block page



418

Sorry, your request has been intercepted because it appears to be an attack.

Event ID: [redacted]

If you are the webmaster, configure related parameters on the WAF console to allow your requests.

Step 7 Go to the WAF console. In the navigation pane on the left, choose **Events**. View the event on the **Events** page.

----End

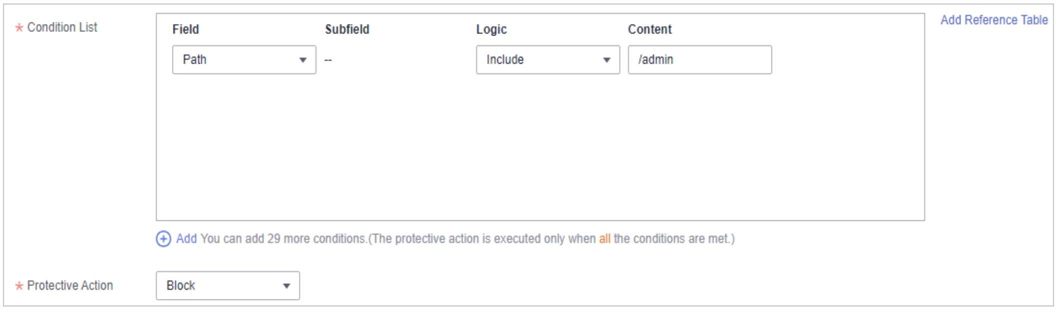
5.14 Condition Field Description

When setting a CC attack, precise access, or global whitelist protection rule, there are some fields in the **Condition List** or **Trigger** 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 against 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 matches the rule. WAF handles the request based on the action (for example, allow, block, or log only) set in the rule.

Figure 5-66 Condition field



* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/admin

Add Reference Table

Add You can add 29 more conditions.(The protective action is executed only when all the conditions are met.)

* Protective Action: Block

A condition field consists of the 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: Set **Field** 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 5-16 Condition list configurations

Field	Subfield	Logic	Content (Example)
Path: Part of a URL that does not include a domain name. This value supports exact matches only. For example, if the path to be protected is **/admin**, **Path** must be set to **/admin**.	--	Select the desired logical relationship from the **Logic** drop-down list.	*/buy/phone/* **NOTICE** ● If **Path** is set to **/**, all paths of the website are protected. ● The path content cannot contain the following special characters: (<>*)
User Agent: A user agent of the scanner to be protected	--		*Mozilla/5.0 (Windows NT 6.1)*
IPv4: An IP address of the visitor.	● Client IP Address ● X-Forwarded-For ● TCP connection IP address		XXX.XXX.1.1
Params: A request parameter to be protected	● All fields ● Any subfield ● Custom		201901150929

Field	Subfield	Logic	Content (Example)
Referer: A user-defined request resource For example, if the protected path is **/admin/xxx** and you do not want visitors to access the page from **www.test.com**, set **Content** for **Referer** to **http://www.test.com**.	--		http://www.test.com
Cookie: A small piece of data to identify web visitors	- All fields - Any subfield - Custom		jsessionid
Header: A user-defined HTTP header	- All fields - Any subfield - Custom		*text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8*
Method: the user-defined request method.	--		**GET**, **POST**, **PUT**, **DELETE**, and **PATCH**
Request Line: Length of a user-defined request line.	--		50
Request: Length of a user-defined request. It includes the request header, request line, and request body.	--		--
Protocol: the protocol of the request.	--		http

Field	Subfield	Logic	Content (Example)
Request message body.	--	● Include ● Exclude ● Include any value ● Exclude any value ● Regex matching	--

5.15 Application Types WAF Can Protect

Table 5-17 lists the application types that can be protected by basic web protection rules.

Table 5-17 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 Page

On the **Dashboard** page, 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.

Statistics on the **Dashboard** page are updated every two minutes.

NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and view security statistics data of the project.

Prerequisites

- You have **connected a website to WAF**.
- At least one protection rule has been configured for the domain name.

Specification Limitations

On the **Dashboard** page, protection data of up to 30 days can be viewed.

How to Calculate QPS

The QPS calculation method varies depending on the time range. For details, see **Table 6-1**.

Table 6-1 QPS calculation

Time Range	Average QPS Description	Peak QPS Description
Yesterday or **Today**	The QPS curve is made with the average QPS in every minute.	The QPS curve is made with each peak QPS in every minute.

Time Range	Average QPS Description	Peak QPS Description
Past 3 days	The QPS curve is made with the average QPS in every five minutes.	The QPS curve is made with each peak 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.	The QPS curve is made with each peak QPS in every 10 minutes.
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.	The QPS curve is made with the peak QPS in every hour.

NOTE

Queries Per Second (QPS) indicates the number of requests per second. For example, an HTTP GET request is also called a query. The number of requests is the total number of requests in a specific time range.

Viewing the Dashboard

Step 1 Log in to the management console.

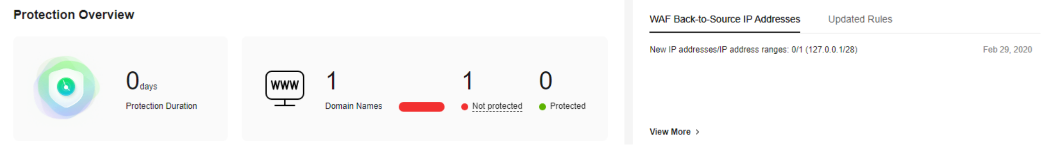
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner and choose **Security** > **Web Application Firewall** to go to the **Dashboard** page.

Step 4 View the protection status in the **Protection Overview** area.

- **Protection Duration**: You can learn of how long the cloud WAF or dedicated WAF you purchase the earliest protects websites in the current enterprise project.
- **Domain Names**: You can learn of how many domain names you add to WAF in the current enterprise project, as well as how many of them are accessible and how many of them are inaccessible.
- **WAF Back-to-Source IP Addresses**: In this area, you will learn of 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.
- **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.

Figure 6-1 Protection Overview



Step 5 Query security data in the **Security Event Statistics** area.

- By default, protection details about all websites add to all WAF instances in all enterprise projects for the logged-in account are displayed. You can query details by website, instance, and time range. The time range can be yesterday, today, past 3 days, past 7 days, or past 30 days. You can also specify a custom time range that is no longer than 30 days.
- You can select **Compare** or **Tile** to view data.
- **By day**: You can select this option to view the data gathered by the day. If you leave this option unselected, you have the following options:
  - **Yesterday** and **Today**: Security event data is gathered every minute.
  - **Past 3 days**: Security event data is gathered every 5 minutes.
  - **Past 7 days**: Security event data is gathered every 10 minutes.
  - **Past 30 days**: Security event data is gathered every hour.

Figure 6-2 Security Event Statistics

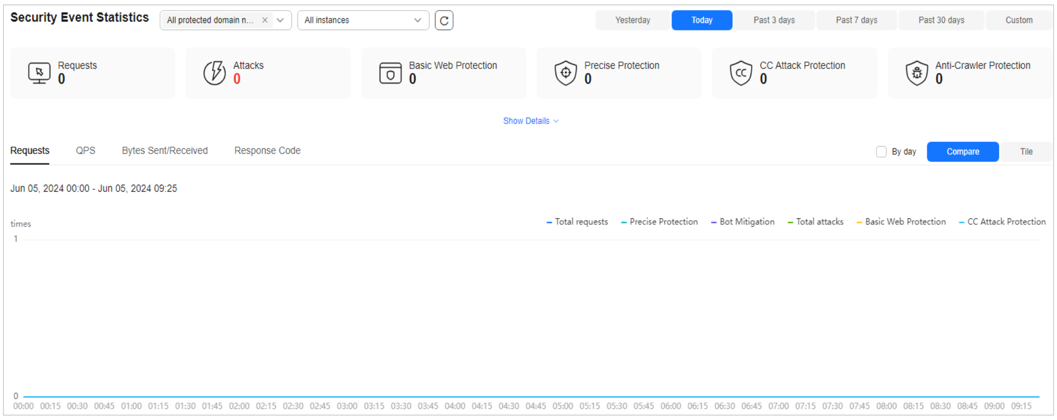


Table 6-2 Security Event Statistics

Section	Description
Section 1 shows how many requests, attacks, and attacked pages by attack type over the specified time range.	● **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. ● **Attacks**: shows how many times the website are attacked. ● You can view how many pages are attacked by a certain type of attack within 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, and anti-crawler protection actions.

Section	Description
Section 2 shows more security metrics about requests, QPS, response code, and sent and received bytes.	● **Requests**: You can view how many requests for your website as well as total attacks and attacks of each attack type. ● **QPS**: You can learn of the average number of requests per second for the domain name. For details about QPS, see **How to Calculate QPS**. Queries Per Second (QPS) indicates the number of requests per second. For example, an HTTP GET request is also called a query. ● **Bytes Sent/Received**: You can learn how much bandwidth is used for requests to the domain name. 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, and TCP retransmission. ● **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.

Step 6 View the **Event Source Statistics** area.

Table 6-3 Parameters in Event Source Statistics

Parameter	Description
Event Distribution	Types of attack events Click an area in the **Event Distribution** area to view the type, number, and proportion of an attack.

Parameter	Description
Attacked Domain Names	The five most attacked domain names and the number of attacks on each domain name. You can click **View More** to go to the **Events** page and view more protection details.
Attack Source IP Addresses	The five source IP addresses with the most attacks and the number of attacks from each source IP address. You can click **View More** to go to the **Events** page and view more protection details.
Attacked URLs	The five most attacked URLs and the number of attacks on each URL. You can click **View More** to go to the **Events** page and view more protection details.

----End

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 set **Client Protocol** to **HTTPS**, set the minimum TLS version and cipher suite (a set of multiple cryptographic algorithms) for your domain name to block requests that use a TLS version earlier than the configured one.

TLS v1.0 and the cipher suite 1 are configured by default in WAF for general security. To protect your websites better, set the minimum TLS version to a later version and select a more secure cipher suite.

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

- The website to be protected has been added to WAF.

- Your website uses HTTPS as the client protocol.

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 v1.0 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 **Cipher suite 1**. Cipher suite 1 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
Default cipher suite **NOTE** By default, **Cipher suite 1** is configured for websites. However, if the request does not carry the server name indication (SNI), WAF uses the **Default 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 Name	Cryptographic Algorithm Supported	Cryptographic Algorithm Not Supported	Description
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 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 Name	Cryptographic Algorithm Supported	Cryptographic Algorithm Not Supported	Description
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 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

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	Default Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4	Cipher suite 5	Cipher suite 6
Google Chrome 63 /macOS High Sierra 10.13.2	Not compatible	Compatible	Compatible	Compatible	Not compatible	Compatible	√
Google Chrome 49/ Windows XP SP3	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible	Compatible	Compatible
Internet Explorer 6 /Windows XP	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
Safari 6/iOS 6.0.1	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	Compatible
Safari 7/iOS 7.1	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	Compatible
Safari 7/OS X 10.9	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	Compatible
Safari 8/iOS 8.4	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	Compatible
Safari 8/OS X 10.10	Compatible	Compatible	Not compatible	Compatible	Compatible	Compatible	Compatible
Internet Explorer 7/Windows Vista	Compatible	Compatible	Not compatible	Compatible	Compatible	Not compatible	√
Internet Explorer 8, 9, or 10 /Windows 7	Compatible	Compatible	Not compatible	Compatible	Compatible	Not compatible	√
Internet Explorer 10 /Windows Phone 8.0	Compatible	Compatible	Not compatible	Compatible	Compatible	Not compatible	√

Browser/Client	Default Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4	Cipher suite 5	Cipher suite 6
Java 7u25	Compatible	Compatible	Not compatible	Compatible	Compatible	Not compatible	√
OpenSSL 0.9.8y	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	√
Safari 6.0.4/OS X 10.8.4	Compatible	Compatible	Not compatible	Compatible	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 of the management console and select a region or project.

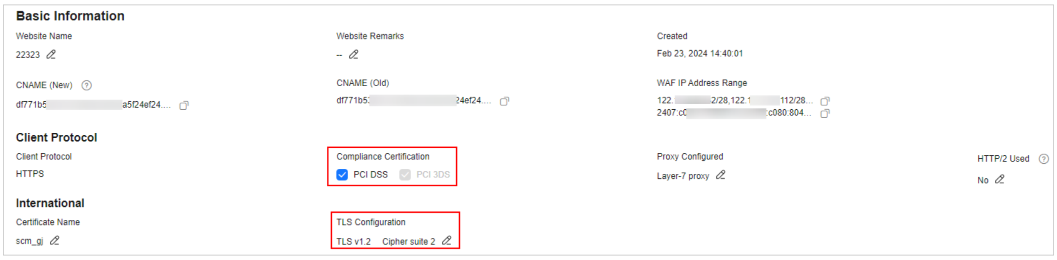
Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Website Settings**.

Step 5 In the **Domain Name** column, click the domain name of the website to go to the basic information page.

Step 6 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



Basic Information

Website Name
22323 ✎

Website Remarks
-- ✎

Created
Feb 23, 2024 14:40:01

CNAME (New) ?
df771b5[redacted]a5f24ef24.... ❐

CNAME (Old)
df771b5[redacted]24ef24.... ❐

WAF IP Address Range
122.[redacted]2/28,122.1[redacted]112/28... ❐
2407:c0[redacted]c080:804... ❐

Client Protocol

Client Protocol
HTTPS

Compliance Certification
☑ PCI DSS ☐ PCI 3DS

Proxy Configured
Layer-7 proxy ✎

HTTP/2 Used ?
No ✎

International

Certificate Name
scm_gj ✎

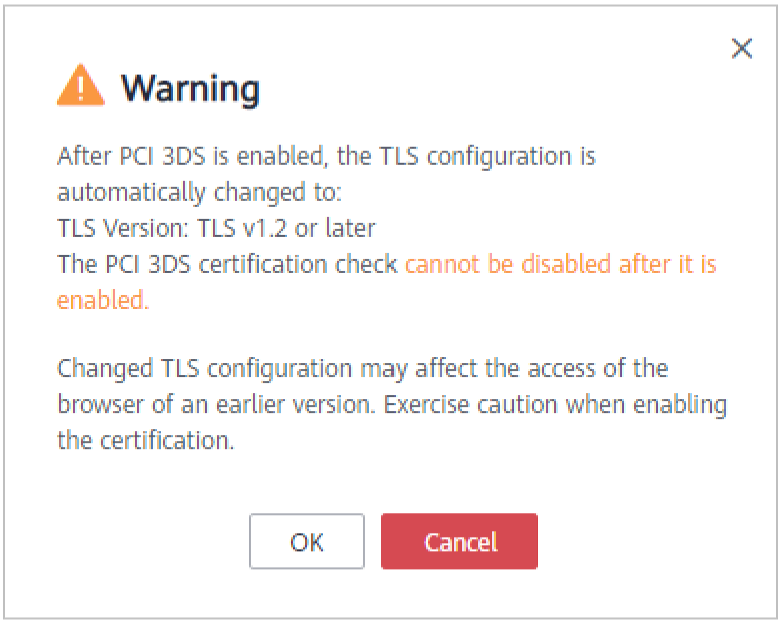
TLS Configuration
TLS v1.2 Cipher suite 2 ✎

- 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.



Warning

After PCI 3DS is enabled, the TLS configuration is automatically changed to:
TLS Version: TLS v1.2 or later
The PCI 3DS certification check cannot be disabled after it is enabled.

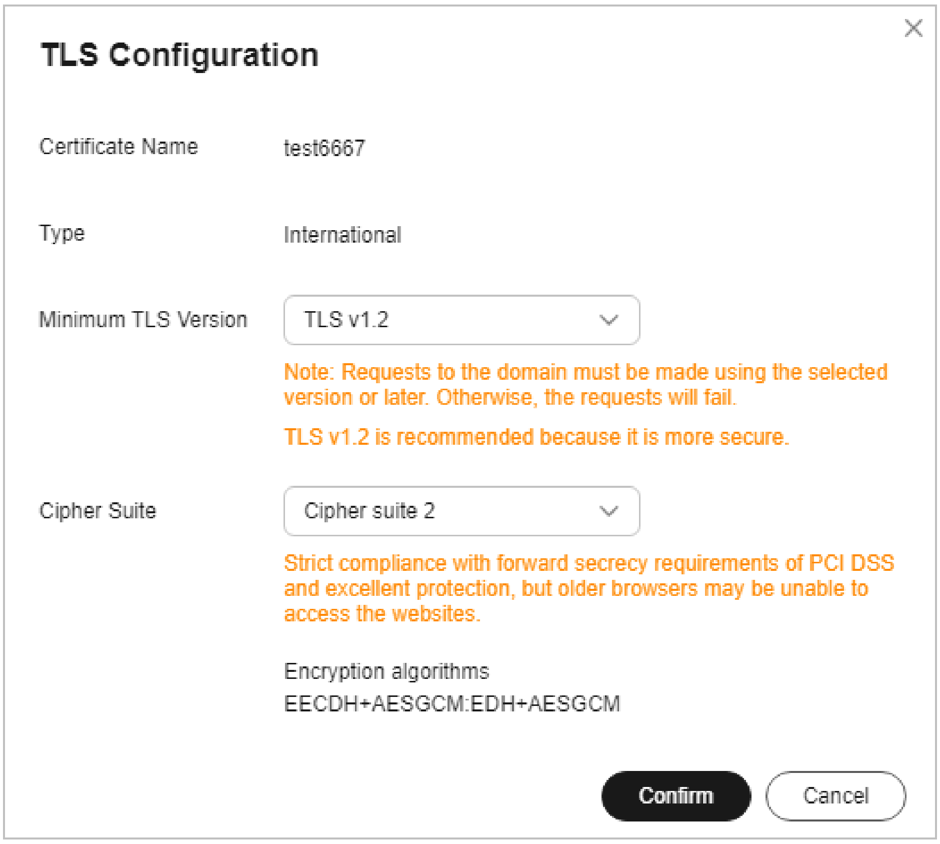
Changed TLS configuration may affect the access of the browser of an earlier version. Exercise caution when enabling the certification.

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 7 In the displayed **TLS Configuration** dialog box, select the minimum TLS version and cipher suite.

Figure 7-2 TLS Configuration



TLS Configuration

Certificate Name: test6667

Type: International

Minimum TLS Version: TLS v1.2

Note: Requests to the domain must be made using the selected version or later. Otherwise, the requests will fail.

TLS v1.2 is recommended because it is more secure.

Cipher Suite: Cipher suite 2

Strict compliance with forward secrecy requirements of PCI DSS and excellent protection, but older browsers may be unable to access the websites.

Encryption algorithms
EECDH+AESGCM:EDH+AESGCM

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 8 Click **Confirm**.

----End

Verification

If the **Minimum TLS Version** is set to **TLS v1.2**, the website can be accessed over connections secured by TLS v1.2 or later, but cannot be accessed over connections secured by TLS v1.1 or earlier.

7.1.2 Configuring a Timeout for Connections Between WAF and a Website Server

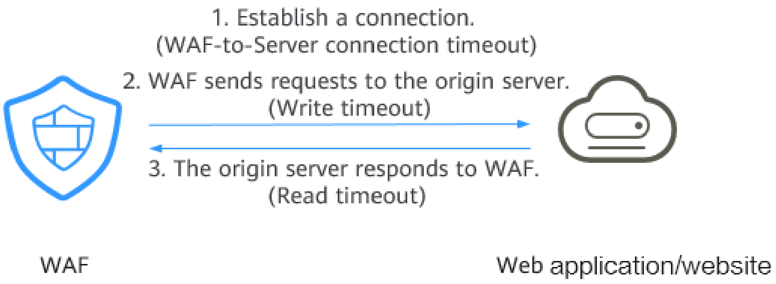
If you want to set a timeout duration for each request between your WAF instance and origin server, enable **Timeout Settings** and specify **WAF-to-Server**

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 7-3 shows the three steps for WAF to forward requests to an origin server.

Figure 7-3 WAF forwarding requests to origin servers.


1. Establish a connection.
(WAF-to-Server connection timeout)
2. WAF sends requests to the origin server.
(Write timeout)
3. The origin server responds to WAF.
(Read timeout)
WAF
Web application/website

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.

Prerequisites

The website you want to protect has been connected to WAF.

Constraints

- 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.

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 of the management console and select a region or project.

Step 3 In the navigation pane, choose **Website Settings**.

Step 4 In the **Domain Name** column, click the website domain name to go to the basic information page.

Step 5 In the **Timeout Settings** row, toggle on if needed.

Step 6 Click ✎, specify **WAF-to-Server connection timeout (s)**, **Read timeout (s)**, and **Write timeout (s)**, and click ✓ to save settings.

----End

7.1.3 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

The website you want to protect has been connected 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 **Proxy Configured** is set to **Layer-7 proxy** 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.

Traffic identifier for a known attack source

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.

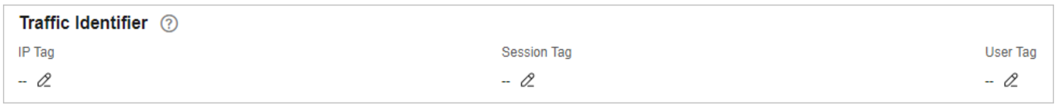
Step 3 Click ≡ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Website Settings**.

Step 5 In the **Domain Name** column, click the domain name of the target website to go to the basic information page.

Step 6 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 7-4 Traffic Identifier



Traffic Identifier

IP Tag	Session Tag	User Tag
-- ✎	-- ✎	-- ✎

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 **Proxy Configured** under the website basic information settings is set to **Layer-7 proxy** 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 **$remote_addr**. ● If the TCP Option Address (TOA) kernel module is configured for packets, but you do not want to identify TOA as the client IP address, set the IP address identifier to **$remote_sockaddr** and upgrade the dedicated engine version to the one later than May 2024. After doing this, layer-3 source IP addresses of packets will be identified as client IP addresses. ● 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

Tag	Description	Example Value
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.	jssessionid
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.	name

Step 7 Click **Confirm**.

----End

Related Operations

Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration

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

The website you want to protect has been connected to WAF.

Viewing Basic Information of a Website

Step 1 Log in to the management console.

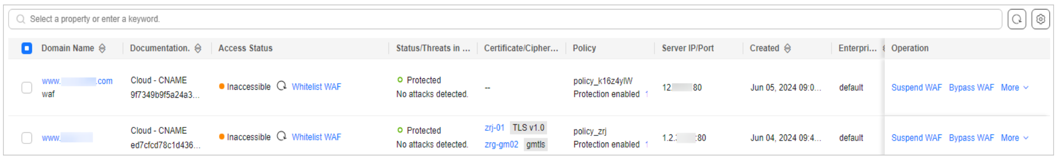
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Website Settings**.

Step 5 View the protected website list. For details about parameters, see **Table 7-5**.

Figure 7-5 Website list



Select a property or enter a keyword.

☐	Domain Name	Documentation.	Access Status	Status/Threats in ...	Certificate/Cipher...	Policy	Server IP/Port	Created	Enterpri...	Operation
☐	www.[redacted].com waf	Cloud - CNAME 9f7349b9f5a24a3...	● Inaccessible Whitelist WAF	○ Protected No attacks detected.	--	policy_k16z4ylW Protection enabled 1	12[redacted]80	Jun 05, 2024 09:0...	default	Suspend WAF Bypass WAF More
☐	www.[redacted]	Cloud - CNAME ed7cfcd78c1d436...	● Inaccessible Whitelist WAF	○ Protected No attacks detected.	zrj-01 TLS v1.0 zrg-gm02 gmtls	policy_zrj Protection enabled 1	1.2.[redacted]:80	Jun 04, 2024 09:4...	default	Suspend WAF Bypass WAF More

Table 7-5 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** 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.
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. ● **Bypassed**: In this mode, requests are directly sent to the backend servers without passing through WAF. **NOTE** The protection mode can be switched to **Bypassed** only when **Cloud Mode - CNAME** is selected for the website and the following conditions are met: – Website services need to be restored to the status when the domain is not connected to WAF. – You need to investigate website errors, such as 502, 504, or other incompatibility issues. – No proxies are configured between the client and WAF.
Certificate/Cipher Suite	Certificate and cipher suite used for the domain name. You can click the certificate name to go to the **Certificates** page.

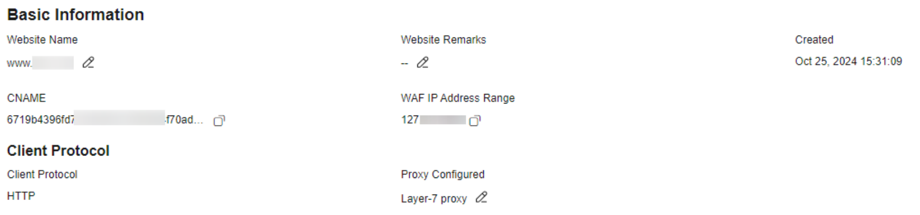
Parameter	Description
Policy	Number of types of WAF protection enabled for the domain name. Policy applied to the domain name. You can click the number to go to the rule configuration page and configure specific protection rules. For details, see **Configuring Protection Policies**.
Server IP/Port	Public 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.
Enterprise Project	Enterprise project the domain name belongs to.

Step 6 In the **Domain Name** column, click the domain name of the website to go to the basic information page.

Step 7 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 7-6 Basic Information



Basic Information

Website Name
www.[redacted]

Website Remarks
--

Created
Oct 25, 2024 15:31:09

CNAME
6719b4396fd7[redacted]f70ad...

WAF IP Address Range
127[redacted]

Client Protocol

Client Protocol
HTTP

Proxy Configured
Layer-7 proxy

----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

The website you want to protect has been connected to WAF.

Exporting Website Settings

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 and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Website Settings**.

Step 5 In the upper right corner above the website list, click **Export** to export the website information list.

----End

7.2.3 Switching WAF Working Mode

You can change the working mode of WAF. WAF can work in **Enabled**, **Suspended**, or **Bypassed** mode.

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

The website you want to protect has been connected to WAF.

Constraints

- The **Bypassed** mode is available only when **Protection** is set to **Cloud**.
- Before switching to the bypass mode, ensure that the service port of the origin server has been enabled.
- If you connect a domain name to WAF with different protection ports configured, WAF cannot be switched to the **Bypassed** for the domain name.
- In **Bypassed** mode, requests for the domain name are sent to the backend server directly and do not pass through WAF. Your domain name may become inaccessible if any of the following happens:
  - In the website server configuration, settings for **Client Protocol** and **Server Protocol** are inconsistent.
  - Different ports are set for **Protected Port** and **Server Port**.

Application Scenarios

- **Enabled**: In this mode, WAF defends your website against attacks based on configured policies.
- **Suspended**: 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 or log attacks. This mode is risky. You are advised to use the global protection whitelist rules to reduce false alarms.
- **Bypassed**: Requests are directly sent to backend origin servers without passing through WAF. Before enabling this mode, enable the service port of origin servers to let requests go to origin servers. The **Bypassed** mode can be enabled only when one of the following conditions is met:
  - Website services need to be restored to the status when the website is not connected to WAF.

- – You need to investigate website errors, such as 502, 504, or other incompatibility issues.
- – No proxies are configured between the client and WAF.

Impact on the System

In **Suspended** mode, your website is not protected because WAF only forwards requests. It does not scan for attacks. To avoid normal requests from being blocked, configure global protection whitelist rules, instead of using the **Suspended** mode.

Switching WAF Working Mode

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 **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Website Settings**.

Step 5 In the **Operation** column of the row containing the target domain name, select a protection mode. In the dialog box displayed, click **Confirm**.

- After you select **Enabled**, the **Status** of the domain name is **Protected**.
- After you select **Suspended**, the **Status** of the domain name is **Unprotected**.
- After you select **Bypassed**, the **Status** of the domain name is **Bypassed**.

----End

Related Operations

- **Handling False Alarms**
- **How Do I Troubleshoot 404/502/504 Errors?**

7.2.4 Updating the Certificate Used for a Website

If you set **Client Protocol** to **HTTPS** when you add a website to WAF, upload a certificate and use it 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

- The website to be protected has been added to WAF.
- Your website uses HTTPS as the 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 6**.
- 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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Website Settings**.

Step 5 In the **Domain Name** column, click the domain name of the website to go to the basic information page.

Step 6 Click the edit icon next to the certificate name. In the **Update Certificate** dialog box, import a new certificate or select an existing certificate.

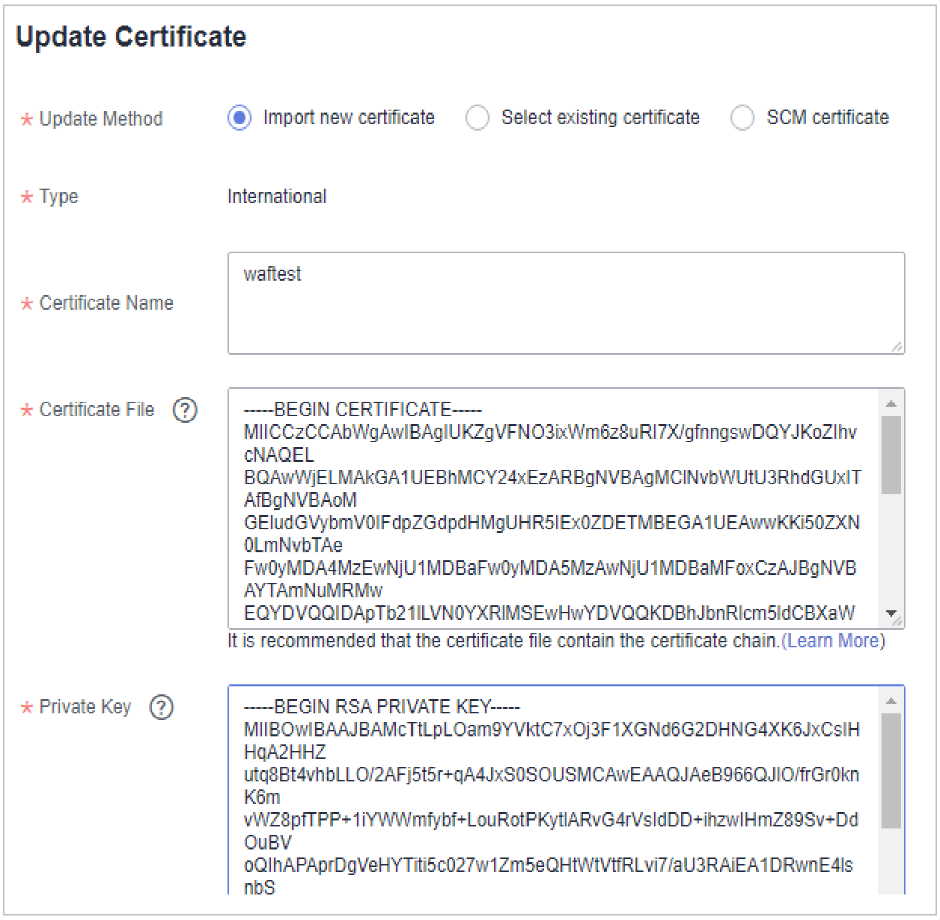
- If you select **Import new certificate** for **Update Method**, enter a certificate name, and copy and paste the certificate file and private key into the corresponding text boxes.

  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.

Figure 7-7 Update Certificate



Update Certificate

* Update Method ● Import new certificate ○ Select existing certificate ○ SCM certificate

* Type International

* Certificate Name waftest

* Certificate File

```
-----BEGIN CERTIFICATE-----
MIICCzCCAbWgAwIBAgIUKZgVFNO3ixWm6z8uRI7X/gfnngswDQYJKoZIhv
cNAQEL
BQAwWjELMAkGA1UEBhMCY24xEzARBgNVBAgMClNvbWUtU3RhdGUxIT
AfBgNVBAoM
GEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDETMBEGA1UEAwwKKi50ZXN
0LmNvbTAe
Fw0yMDA4MzEwNjU1MDBaFw0yMDA5MzAwNjU1MDBaMFoxCzAJBgNVB
AYTAmNuMRMw
EQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBXaW
```

It is recommended that the certificate file contain the certificate chain.(Learn More)

* Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAMcTtLpLOam9YVktC7xOj3F1XGNd6G2DHNG4XK6JxCsIH
HqA2HHZ
utq8Bt4vhbLLO/2AFj5t5r+qA4JxS0SOUSMCAwEAAQJAeB966QJIO/frGr0kn
K6m
vWZ8pfTPP+1iYWWmfybf+LouRotPKytlARvG4rVsldDD+ihzwIHmZ89Sv+Dd
OuBV
oQIhAPAprDgVeHYTiti5c027w1Zm5eQHtWtVtfRLvi7/aU3RAiEA1DRwnE4ls
nbS
```

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 7-6** before uploading it.

Table 7-6 Certificate conversion commands

Format	Conversion Method
CER/CRT	Rename the **cert.crt** certificate file to **cert.pem**.

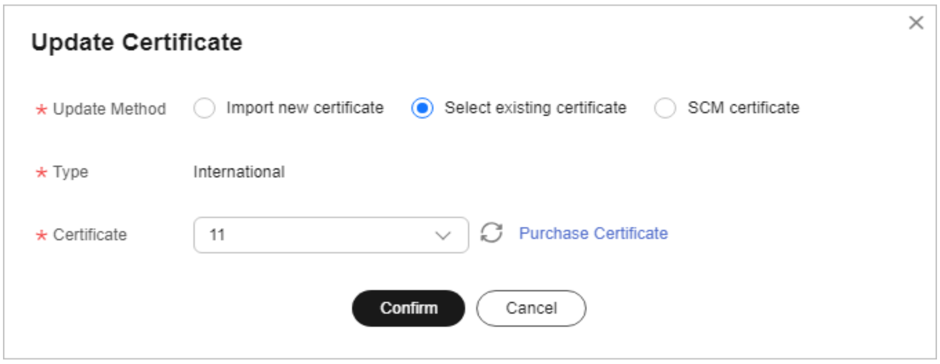
Format	Conversion Method
PFX	– Obtain a private key. For example, run the following command to convert **cert.pfx** into **key.pem**: **openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes** – Obtain a certificate. For example, run the following command to convert **cert.pfx** into **cert.pem**: **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.

Figure 7-8 Selecting an existing certificate



Update Certificate

* Update Method ○ Import new certificate ● Select existing certificate ○ SCM certificate

* Type International

* Certificate 11

NOTE

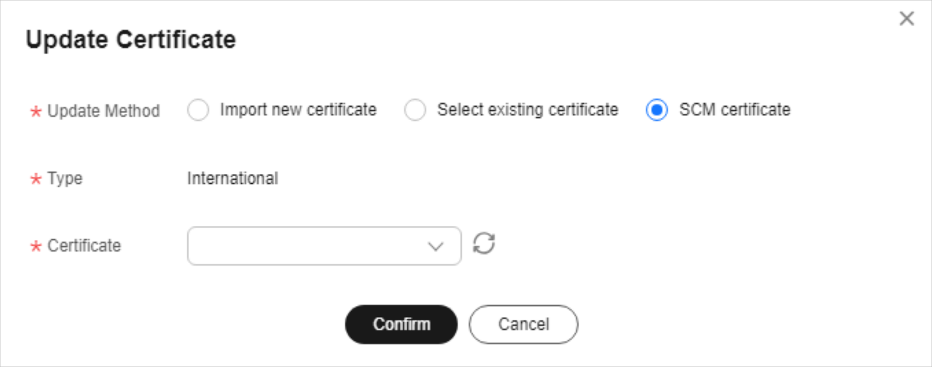
If there are no certificates available, click **Purchase Certificate** and purchase a certificate and push it to WAF.

- 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.

Figure 7-9 Selecting an SCM certificate


Update Certificate

* Update Method ○ Import new certificate ○ Select existing certificate ● SCM certificate

* Type International

* Certificate

Step 7 Click **Confirm**.

----End

Related Operations

Uploading a Certificate to WAF

7.2.5 Editing Server Information

If you select **Cloud** or **Dedicated** when adding a website to WAF, you can edit the server information of your website.

Applicable scenarios:

- Edit server information.
  - Cloud mode: You can modify configurations for **Client Protocol**, **Server Protocol**, **Server Address**, and **Server Port**.
  - Dedicated mode: You can modify configurations for **Client Protocol**, **Server Protocol**, **Server Address**, **VPC**, 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

The website you want to protect has been connected 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.

Impact on the System

Modifying the server configuration does not affect services.

Editing Server Information

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 **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Website Settings**.

Step 5 In the **Domain Name** column, click the domain name of the website to go to the basic information page.

Step 6 In the **Origin Servers** area, click **Edit**.

Step 7 On the **Edit Server Information** page, edit the server configurations (such as client protocols and associated certificates).

- 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 8 Click **Confirm**.

----End

Verification

After the server information is modified, it takes about two minutes for the modification to take effect.

7.2.6 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

The website you want to protect has been connected to WAF.

Viewing Protection Details About a Protected Website on Cloud Eye

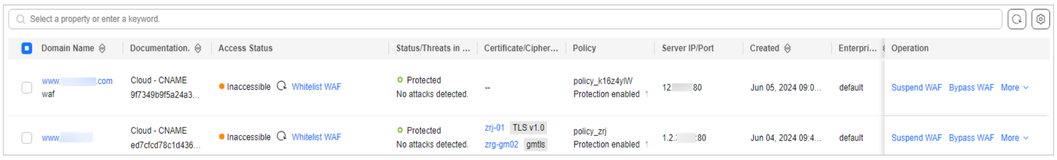
Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Website Settings**.

Figure 7-10 Website list



Select a property or enter a keyword.

Domain Name	Documentation.	Access Status	Status/Threats in ...	Certificate/Cipher...	Policy	Server IP/Port	Created	Enterpri...	Operation
www.[redacted].com waf	Cloud - CNAME 9f7349b9f5a24a3...	Inaccessible Whitelist WAF	Protected No attacks detected.	--	policy_k16z4yIW Protection enabled 1	12[redacted]80	Jun 05, 2024 09:0...	default	Suspend WAF Bypass WAF More
www.[redacted]	Cloud - CNAME ed7cfcd78c1d436...	Inaccessible Whitelist WAF	Protected No attacks detected.	zrj-01 TLS v1.0 zrg-gm02 gmtls	policy_zrj Protection enabled 1	1.2.[redacted]:80	Jun 04, 2024 09:4...	default	Suspend WAF Bypass WAF More

Step 5 In the row containing the protected domain name, click **Cloud Eye** in the **Operation** column to go to the Cloud Eye console and view the monitoring information.

----End

7.2.7 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

The website you want to protect has been connected to WAF.

Impact on the System

- In cloud 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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner and choose **Web Application Firewall** under **Security**.

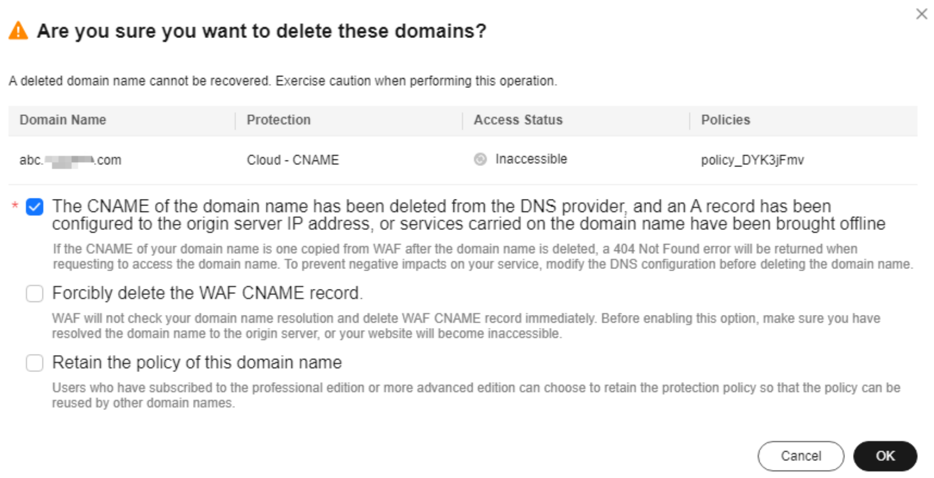
Step 4 In the navigation pane on the left, choose **Website Settings**.

Step 5 Locate the row of the target domain name. In the **Operation**, click **More** > **Delete**.

Step 6 In the displayed confirmation dialog box, confirm the deletion.

- Cloud mode
  - No proxy used

Figure 7-11 Deleting a protected domain name (no proxy used)



Are you sure you want to delete these domains?

A deleted domain name cannot be recovered. Exercise caution when performing this operation.

Domain Name	Protection	Access Status	Policies
abc.[redacted].com	Cloud - CNAME	Inaccessible	policy_DYK3jFmv

* ☑ 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 the CNAME of your domain name is one copied from WAF after the domain name is deleted, a 404 Not Found error will be returned when requesting to access the domain name. To prevent negative impacts on your service, modify the DNS configuration before deleting the domain name.

☐ Forcibly 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.

☐ Retain the policy of this domain name

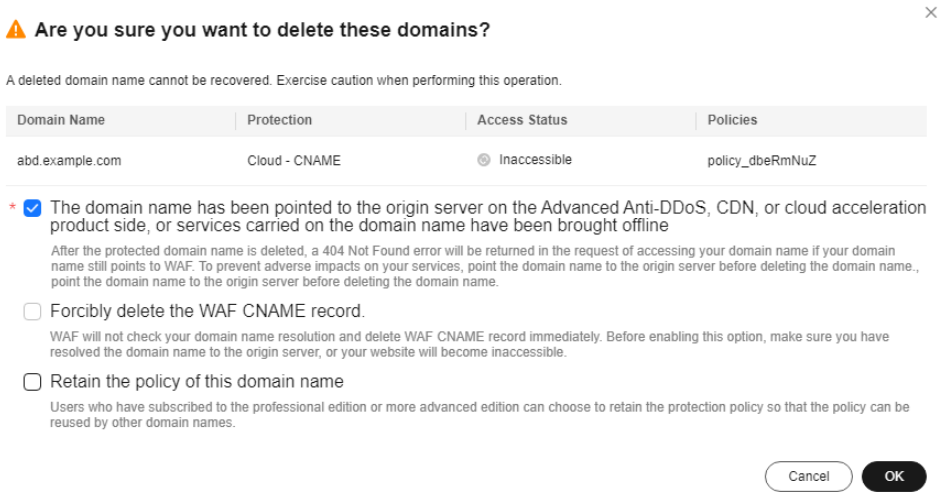
Users who have subscribed to the professional edition or more advanced edition can choose to retain the protection policy so that the policy can be reused by other domain names.

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 bound to the domain name, select **Retain the policy of this domain name**.

– Proxy used

Figure 7-12 Deleting a protected domain name (proxy used)



Are you sure you want to delete these domains?

A deleted domain name cannot be recovered. Exercise caution when performing this operation.

Domain Name	Protection	Access Status	Policies
abd.example.com	Cloud - CNAME	Inaccessible	policy_dbeRmNuZ

* ☑ 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

After the protected domain name is deleted, a 404 Not Found error will be returned in the request of accessing your domain name if your domain name still points to WAF. To prevent adverse impacts on your services, point the domain name to the origin server before deleting the domain name., point the domain name to the origin server before deleting the domain name.

☐ Forcibly 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.

☐ Retain the policy of this domain name

Users who have subscribed to the professional edition or more advanced edition can choose to retain the protection policy so that the policy can be reused by other domain names.

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 bound to the domain name, select **Retain the policy of this domain name**.

- Dedicated mode

  If you want to retain the policy bound to the domain name, select **Retain the policy of this domain name**.

Step 7 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

A protected website domain name can use only one policy.

Adding a Protection Policy

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 **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 In the upper left corner, click **Add Policy**.

Step 6 In the displayed dialog box, enter the policy name and click **Confirm**. The added policy will be displayed in the policy list.

Step 7 In the **Policy Name** column, click the policy name. On the displayed page, add rules to the policy by referring to **Rule Configurations**.

----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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner and choose **Web Application Firewall** under **Security**.

Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 Locate the row containing the policy you want to copy. In the **Operation** column, click **More** > **Copy**.

Step 6 In the dialog box displayed, enter a policy name and then click **Confirm**.

----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

The website you want to protect has been connected to WAF.

Adding a Domain Name to a Policy

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 **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.

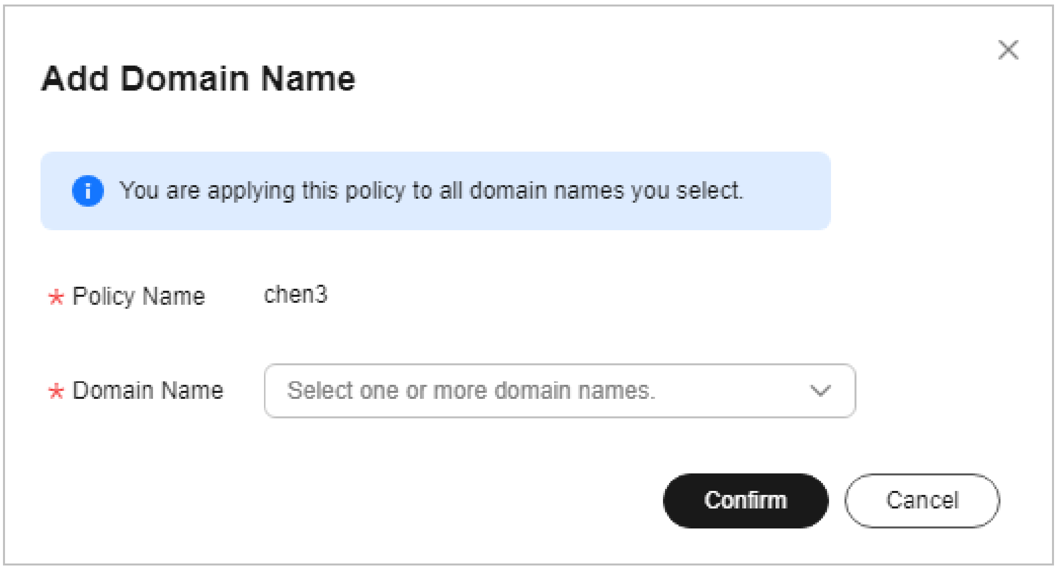
Step 5 In the row containing the policy you want to apply to a website, click **Add Domain Name** in the **Operation** column.

Step 6 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



Add Domain Name

You are applying this policy to all domain names you select.

* Policy Name chen3

* Domain Name Select one or more domain names.

Step 7 Click **Confirm**.

----End

8.3 Adding Rules to One or More Policies

This topic describes how to add rules to one or more policies.

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.

Adding Rules to One or More Policies

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 **Security** > **Web Application Firewall**.

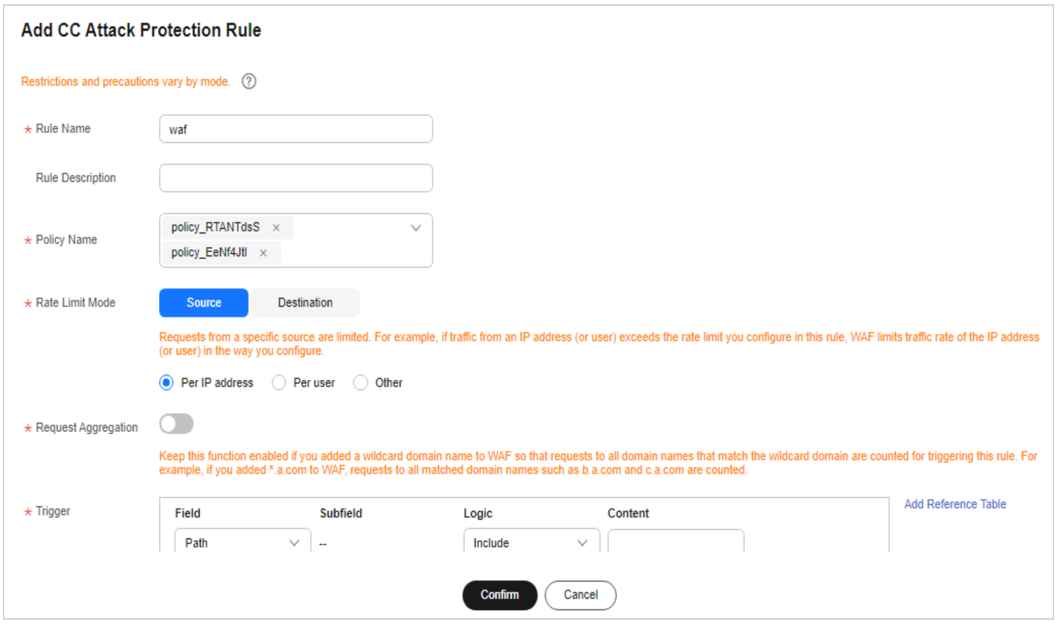
Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 In the upper left corner of the policy list, click **View All My Rules**.

Step 6 In the upper left corner above a list of a type of rule, click **Add Rule**.

Step 7 Select one or more policies from the **Policy Name** drop-down list.

Figure 8-2 Adding a rule to one or more policies



Add CC Attack Protection Rule

Restrictions and precautions vary by mode.

* Rule Name: waf

Rule Description:

* Policy Name: policy_RTANTdsS ×, policy_EeNf4Jtl ×

* Rate Limit Mode: Source | Destination

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 ○ Per user ○ Other

* Request Aggregation

Keep this function enabled if you added a wildcard domain name to WAF so that requests to all domain names that match the 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.

* Trigger

Field	Subfield	Logic	Content
Path	--	Include	

Step 8 Set other parameters.

- To add a CC attack protection rule, see **Table 5-4**.
- To add a precise protection rule, see **Table 5-5**.
- To add a blacklist or whitelist rule, see **Table 5-6**.
- To add a geolocation access control rule, see **Table 5-7**.
- To add a WTP rule, see **Table 5-8**.

- To add an information leakage prevention rule, see **Table 5-11**.
- To add a global protection whitelist rule, see **Table 5-12**.
- To add a data masking rule, see **Table 5-13**.

Step 9 Click **Confirm**.

----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 Object Management

9.1 Certificate Management

9.1.1 Uploading a Certificate to WAF

If you select **HTTPS** for **Client Protocol** when you add a website to WAF, a certificate must be associated with the 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 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 of the management console and select a region or project.

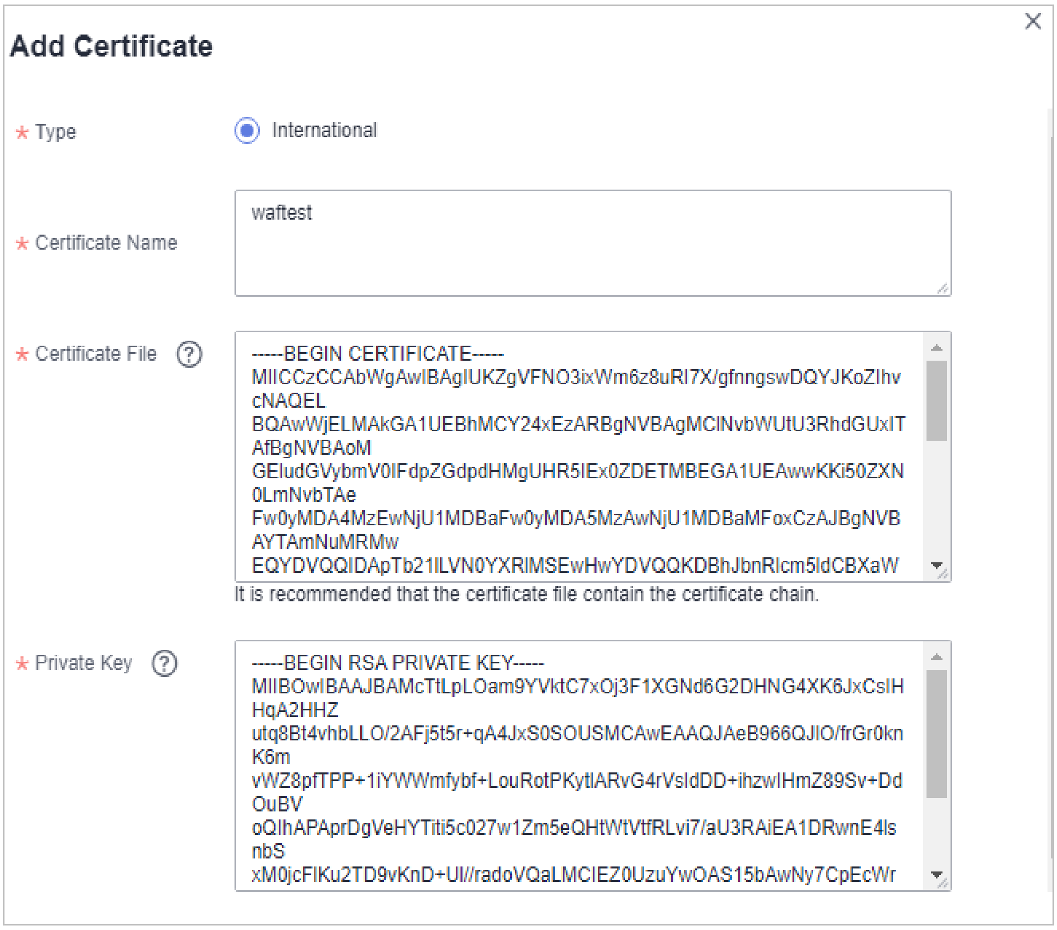
Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane, choose **Objects** > **Certificates**.

Step 5 Click **Add Certificate**.

Step 6 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 9-1 Upload Certificate



Add Certificate

* Type ● International

* Certificate Name: waftest

* Certificate File ⓘ

```
-----BEGIN CERTIFICATE-----
MIICCzCCAbWgAwIBAgIUKZgVFNO3ixWm6z8uRI7X/gfnngswDQYJKoZIhv
cNAQEL
BQAwWjELMAkGA1UEBhMCY24xEzARBgNVBAgMClNvbWUtU3RhdGUxIT
AfBgNVBAoM
GEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDETMBEGA1UEAwwKKi50ZXN
0LmNvbTAe
Fw0yMDA4MzEwNjU1MDBaFw0yMDA5MzAwNjU1MDBaMFoxCzAJBgNVB
AYTAmNuMRMw
EQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJbnRlcm5ldCBXaW
```

It is recommended that the certificate file contain the certificate chain.

* Private Key ⓘ

```
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAMcTtLpLOam9YVktC7xOj3F1XGNd6G2DHNG4XK6JxCsIH
HqA2HHZ
utq8Bt4vhbLLO/2AFj5t5r+qA4JxS0SOUSMCAwEAAQJAeB966QJIO/frGr0kn
K6m
vWZ8pfTPP+1iYWWmfybf+LouRotPKytlARvG4rVsldDD+ihzwlHmZ89Sv+Dd
OuBV
oQIhAPAprDgVeHYTiti5c027w1Zm5eQHtWtVtfRLvi7/aU3RAiEA1DRwnE4ls
nbS
xM0jcFlKu2TD9vKnD+Ul//radoVQaLMClEZ0UzuYwOAS15bAwNy7CpEcWr
```

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 9-1** before uploading it.

Table 9-1 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**.
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 7 Click **Confirm**.

----End

Verification

The certificate you created is displayed in the certificate list.

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.

9.1.2 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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane, choose **Objects** > **Certificates**.

Step 5 In the row containing the certificate you want to use, click **Use** in the **Operation** column.

Step 6 In the displayed **Domain Name** dialog box, select the website you want to use the certificate to.

Step 7 Click **Confirm**.

----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.

9.1.3 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 created a certificate to WAF.

Checking Certificate Details

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 **Security** > **Web Application Firewall**.

Step 4 In the navigation pane, choose **Objects** > **Certificates**.

Step 5 View the certificate information. For details about related parameters, see **Table 9-2**.

Table 9-2 Certificate parameters

Parameter	Description
Name	Certificate name.
Type	Only **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.

----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.

9.1.4 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 **added 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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner and choose **Web Application Firewall** under **Security**.

Step 4 In the navigation pane, choose **Objects** > **Certificates**.

Step 5 In the row containing the certificate you want to share, click **More** > **Share** in the **Operation** column.

Step 6 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.

9.1.5 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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane, choose **Objects** > **Certificates**.

Step 5 In the row of the certificate, click **More** > **Delete** in the **Operation** column.

Step 6 In the displayed dialog box, click **Confirm**.

----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

9.2 Managing IP Address Blacklist and Whitelist Groups

9.2.1 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.

Adding a Blacklist or Whitelist IP Address Group

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 and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Objects** > **Address Groups**.

Step 5 On the upper left of the address group list, click **Add Address Group**.

Step 6 In the displayed **Add Address Group** dialog box, enter an address group name and provide IP addresses/IP address ranges.

Step 7 Click **Confirm**.

----End

9.2.2 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.

Prerequisites

You have created 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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Objects** > **Address Groups**.

Step 5 In the address group list, view the address group information.

Table 9-3 Parameter description

Parameter	Description
Group Name	Address group name you configured.
IP Address/ Range	IP addresses or IP address ranges added to the address group.
Rule	Rules that are using the address group.
Remarks	Supplementary information about the address group.

Step 6 Modify or delete an IP address group.

- Modify an address group.

  In the row containing the address group you want to modify, click **Modify** in the **Operation** column. In the **Modify Address Group** dialog box, change the group name or IP address/IP address range, and click **Confirm**.

- 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

10 System Management

10.1 Managing Dedicated WAF Engines

This topic describes how to manage your dedicated WAF instances (or engines), including viewing instance information, viewing instance monitoring configurations, upgrading the instance edition, or deleting 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.

Viewing Information About a Dedicated WAF Instance

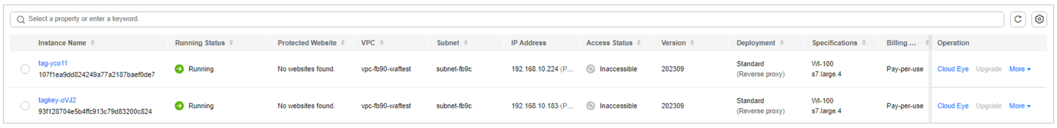
Step 1 Log in to the management console.

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 **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.

Figure 10-1 Dedicated engine list



Select a property or enter a keyword.

	Instance Name	Running Status	Protected Website	VPC	Subnet	IP Address	Access Status	Version	Deployment	Specifications	Billing ...	Operation
○	tag-yco11 107f1ea9dd824249a77a2187baef0de7	Running	No websites found.	vpc-fb90-waftest	subnet-fb9c	192.168.10.224 (P...	Inaccessible	202309	Standard (Reverse proxy)	WI-100 s7.large.4	Pay-per-use	Cloud Eye Upgrade More ▾
○	tagkey-oVJ2 93f128704e5b4ffc913c79d83200c824	Running	No websites found.	vpc-fb90-waftest	subnet-fb9c	192.168.10.183 (P...	Inaccessible	202309	Standard (Reverse proxy)	WI-100 s7.large.4	Pay-per-use	Cloud Eye Upgrade More ▾

Step 5 View information about a dedicated WAF instance. Table 10-1 describes parameters.

Table 10-1 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
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.	8 vCPUs | 16 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.

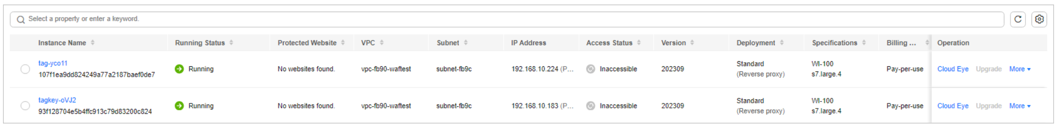
Step 1 Log in to the management console.

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

Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.

Figure 10-2 Dedicated engine list



Select a property or enter a keyword.

	Instance Name	Running Status	Protected Website	VPC	Subnet	IP Address	Access Status	Version	Deployment	Specifications	Billing ...	Operation
○	tag-yco11 107f1ea9dd824249a77a2187baef0de7	Running	No websites found.	vpc-fb90-waftest	subnet-fb9c	192.168.10.224 (P...	Inaccessible	202309	Standard (Reverse proxy)	WI-100 s7.large.4	Pay-per-use	Cloud Eye Upgrade More ▾
○	tagkey-oVJ2 93f128704e5b4ffc913c79d83200c824	Running	No websites found.	vpc-fb90-waftest	subnet-fb9c	192.168.10.183 (P...	Inaccessible	202309	Standard (Reverse proxy)	WI-100 s7.large.4	Pay-per-use	Cloud Eye Upgrade More ▾

Step 5 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

Upgrading a Dedicated WAF Instance

Only dedicated WAF instances in the **Running** status can be upgraded to the latest version.

NOTICE

- It takes about 20 minutes for upgrading an instance. During the upgrade, the instance is not available and cannot protect your domain names connected to it. To prevent service interruptions, use either of the following solutions:
  - **Solution 1**: Deploy multiple dedicated WAF instances for your domain name, add them to a backend server group of your load balancer, and enable the health check policy for the load balancer. In this way, if one dedicated WAF instance is not available, WAF automatically distributes the traffic to other healthy instances. There is almost no impact on your services except that website requests might be intermittently interrupted for few seconds.
  - **Solution 2**: If you deploy only one dedicated WAF instance, configure a load balancer before you start to let website traffic bypass WAF during the upgrade. After the upgrade is complete, configure the load balancer to distribute traffic to WAF.
- If you are using the latest version of WAF, the **Upgrade** button is grayed out.

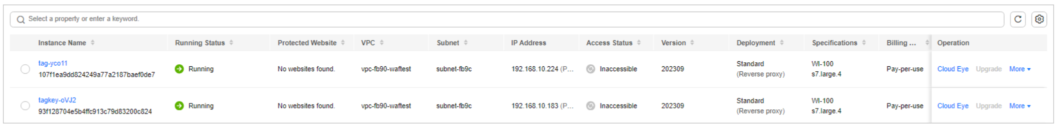
Step 1 Log in to the management console.

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 **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.

Figure 10-3 Dedicated engine list



Select a property or enter a keyword.

	Instance Name	Running Status	Protected Website	VPC	Subnet	IP Address	Access Status	Version	Deployment	Specifications	Billing ...	Operation
○	tag-yco11 107f1ea9dd824249a77a2187baef0de7	Running	No websites found.	vpc-fb90-waftest	subnet-fb9c	192.168.10.224 (P...	Inaccessible	202309	Standard (Reverse proxy)	WI-100 s7.large.4	Pay-per-use	Cloud Eye Upgrade More ▾
○	tagkey-oVJ2 93f128704e5b4ffc913c79d83200c824	Running	No websites found.	vpc-fb90-waftest	subnet-fb9c	192.168.10.183 (P...	Inaccessible	202309	Standard (Reverse proxy)	WI-100 s7.large.4	Pay-per-use	Cloud Eye Upgrade More ▾

Step 5 In the row containing the instance you want to upgrade, click **Upgrade** in the **Operation** column.

Step 6 Confirm the upgrade conditions and click **Confirm**.

Click **View Details** to view details of all dedicated WAF instance versions.

----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 of the management console and select a region or project.

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

Step 4 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.

Step 5 In the row of the instance, click **More** > **Roll Back** in the **Operation** column.

Step 6 In the dialog box displayed, confirm that the following conditions are met and select the following three conditions. Then, click **Confirm**.

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.

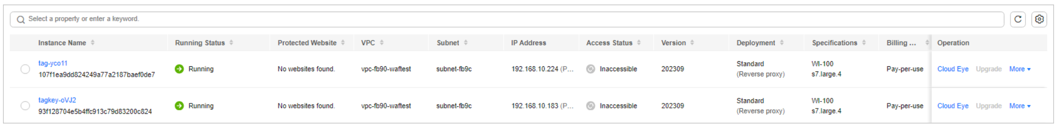
Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.

Figure 10-4 Dedicated engine list



Select a property or enter a keyword.

	Instance Name	Running Status	Protected Website	VPC	Subnet	IP Address	Access Status	Version	Deployment	Specifications	Billing ...	Operation
○	tag-yco11 107f1ea9dd824249a77a2187baef0de7	Running	No websites found.	vpc-fb90-waftest	subnet-fb9c	192.168.10.224 (P...	Inaccessible	202309	Standard (Reverse proxy)	WI-100 s7.large.4	Pay-per-use	Cloud Eye Upgrade More ▾
○	tagkey-oVJ2 93f128704e5b4ffc913c79d83200c824	Running	No websites found.	vpc-fb90-waftest	subnet-fb9c	192.168.10.183 (P...	Inaccessible	202309	Standard (Reverse proxy)	WI-100 s7.large.4	Pay-per-use	Cloud Eye Upgrade More ▾

Step 5 In the row containing the instance, choose **More** > **Change Security Group** in the **Operation** column.

Step 6 In the dialog box displayed, select the new security group and click **Confirm**.

----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.

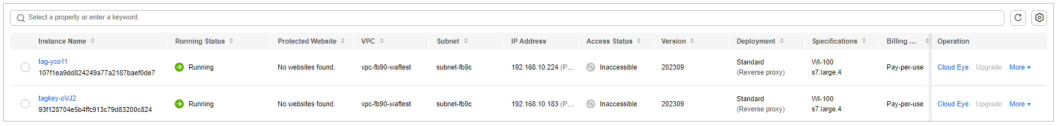
Step 1 Log in to the management console.

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

Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.

Figure 10-5 Dedicated engine list



Select a property or enter a keyword.

	Instance Name	Running Status	Protected Website	VPC	Subnet	IP Address	Access Status	Version	Deployment	Specifications	Billing ...	Operation
○	tag-yco11 107f1ea9dd824249a77a2187baef0de7	Running	No websites found.	vpc-fb90-waftest	subnet-fb9c	192.168.10.224 (P...	Inaccessible	202309	Standard (Reverse proxy)	WI-100 s7.large.4	Pay-per-use	Cloud Eye Upgrade More ▾
○	tagkey-oVJ2 93f128704e5b4ffc913c79d83200c824	Running	No websites found.	vpc-fb90-waftest	subnet-fb9c	192.168.10.183 (P...	Inaccessible	202309	Standard (Reverse proxy)	WI-100 s7.large.4	Pay-per-use	Cloud Eye Upgrade More ▾

Step 5 In the row of the instance, click **More** > **Delete** in the **Operation** column.

Step 6 In the displayed dialog box, enter **DELETE** and click **Confirm**.

----End

10.2 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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Instance Management** > **Product Details**.

Step 5 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.

----End

10.3 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 package allows you to add 10 domain names to WAF, including one top-level domain and nine subdomains or wildcard domains related to the top-level domain.
- 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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner and choose **Web Application Firewall** under **Security**.

Step 4 In the navigation pane on the left, choose **Instance Management** > **Product Details**.

Step 5 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.
- Billing information: Changing specifications does not change the billing mode or expiration date.

Step 6 In the lower right corner of the page, click **Next**.

Step 7 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 8 On the payment page, select a payment method and pay for your order or select a refund method to get your money refunded.

----End

10.4 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

- Before setting alarm notifications, create a message topic in SMN.
- 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 enable alarm notifications.

Prerequisites

SMN has been enabled.

Constraints

- Alarm notifications are sent if the number of attacks reaches the threshold you configure.

Enabling Alarm Notifications

Step 1 Log in to the management console.

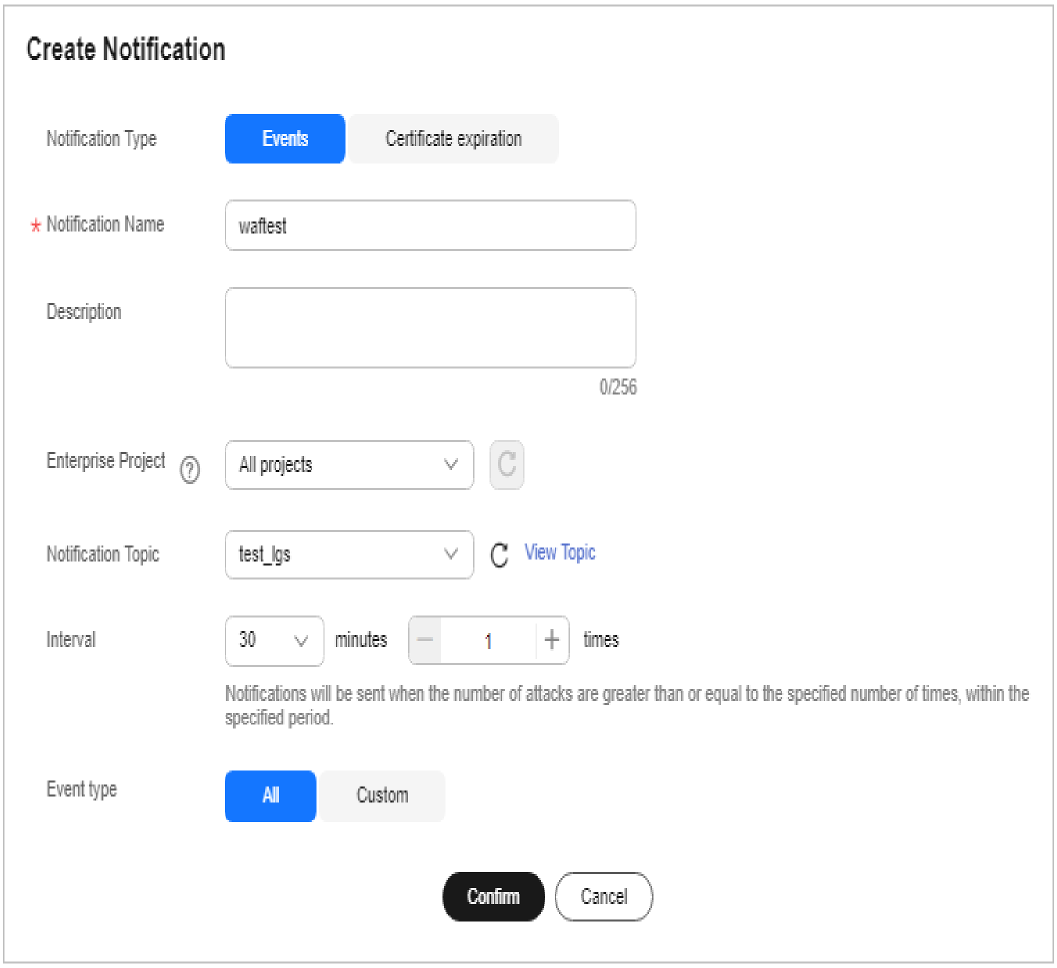
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane, choose **Instance Management** > **Notifications**.

Step 5 Click **Create** and configure alarm notification parameters. **Table 10-2** lists the parameters.

Figure 10-6 Create Notification



Create Notification

Notification Type: Events | Certificate expiration

* Notification Name: waftest

Description: 0/256

Enterprise Project: All projects

Notification Topic: test_lgs View Topic

Interval: 30 minutes 1 times

Notifications will be sent when the number of attacks are greater than or equal to the specified number of times, within the specified period.

Event type: All | Custom

Table 10-2 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.
Notification Name	Name of the alarm notification.
Description	(Optional) A description of the purposes of the alarm.
Enterprise Project	Select an enterprise project from the drop-down list. The notification takes effect in the selected enterprise project.

Parameter	Description
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*.
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** 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.
Interval	This parameter must be configured if you select **Certificate expiration** for **Notification Type**. How often WAF sends certificate expiration notifications to you. You can select **Weekly** or **Daily**.

Step 6 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.

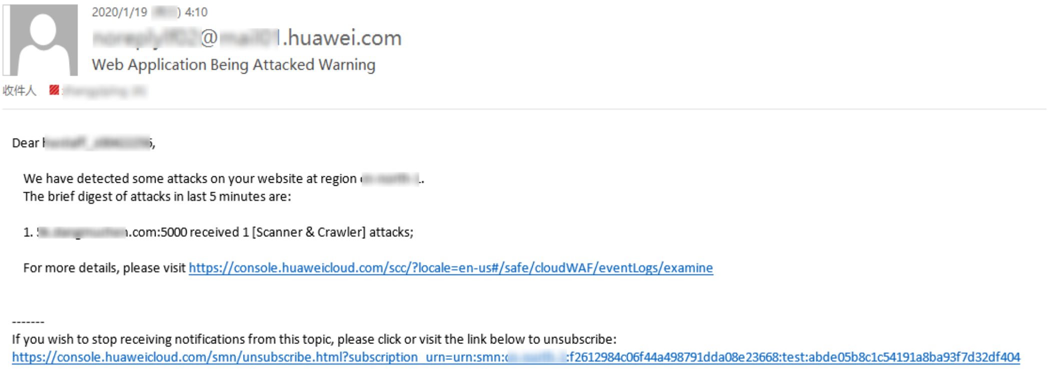
- To modify a notification, locate the row containing the notification and click **Modify** in the **Operation** column.

----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 10-7** shows an example of an alarm notification email.

Figure 10-7 Alarm notification email



2020/1/19 [redacted]) 4:10

[redacted]@[redacted].huawei.com

Web Application Being Attacked Warning

收件人 [redacted]

Dear [redacted],

We have detected some attacks on your website at region [redacted].
The brief digest of attacks in last 5 minutes are:

1. [redacted].com:5000 received 1 [Scanner & Crawler] attacks;

For more details, please visit https://console.huaweicloud.com/scc/?locale=en-us#/safe/cloudWAF/eventLogs/examine

----
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://console.huaweicloud.com/smn/unsubscribe.html?subscription_urn=urn:smn:[redacted]:f2612984c06f44a498791dda08e23668:test:abde05b8c1c54191a8ba93f7d32df404

11 Permissions Management

11.1 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.

- 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. Locate the row that contains the target enterprise project, click **View User Group** in the **Operation** column. Then, click **Add Authorization**, select the user groups you want to add and move them to the right pane. Click **Next** and select the policies.

  b. In the available user groups on the left pane, select the target ones and move them to the right pane.

- 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 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.

11.2 IAM Permissions Management

11.2.1 WAF Custom Policies

If the system-defined policies of WAF cannot meet your needs, you can create custom policies. For details about the actions supported by custom policies, see **WAF Permissions and Supported Actions**.

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**. The following section contains examples of common WAF custom policies.

WAF Example Custom Policies

- 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 policy

  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"
                        ]
                }
        ]
}
```

11.2.2 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.

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 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	√	√

Permission	Action	IAM Project	Enterprise Project
Querying a protected domain	waf:instance:get	√	√
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 segment	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	√	√

Permission	Action	IAM Project	Enterprise Project
Updating a protected domain	waf:instance:put	√	√
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:preciseProtectionRule: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	√	√

Permission	Action	IAM Project	Enterprise Project
Adding a web tamper protection rule	waf:antiTamperRule:create	√	√
Adding a CC attack protection rules	waf:ccRule:create	√	√
Adding a precise protection rule	waf:preciseProtection-Rule:create	√	√
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	√	√
Querying the global protection whitelist rule list	waf:falseAlarmMaskRule:list	√	√

Permission	Action	IAM Project	Enterprise Project
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	√	√
Disabling the pay-per-use billing for a WAF cloud-mode instance	waf:postpaid:delete	√	√

Permission	Action	IAM Project	Enterprise Project
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	√	√
Configuring health check for a WAF instance group	waf:poolHealthMonitor:create	√	√

Permission	Action	IAM Project	Enterprise Project
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 Monitoring and Auditing

12.1 Monitoring

12.1.1 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 12-1 Monitored metrics for domain names protected with WAF

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
requests	Number of Requests	Number of requests returned by WAF in the last 5 minutes Unit: Count Collection method: The total number of requests for the domain name are collected.	≥ 0 Value type: Float	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 Unit: Count Collection method: Number of 2XX status codes returned	≥ 0 Value type: Float	Protected domain dame	5
waf_http_3xx	WAF Status Code (3XX)	Number of 3XX status codes returned by WAF in the last 5 minutes Unit: Count Collection method: Number of 3XX status codes returned	≥ 0 Value type: Float	Protected domain dame	5

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
waf_http_4xx	WAF Status Code (4XX)	Number of 4XX status codes returned by WAF in the last 5 minutes Unit: Count Collection method: Number of 4XX status codes returned	≥ 0 Value type: Float	Protected domain dame	5
waf_http_5xx	WAF Status Code (5XX)	Number of 5XX status codes returned by WAF in the last 5 minutes Unit: Count Collection method: Number of 5XX status codes returned	≥ 0 Value type: Float	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 Unit: Count Collection method: Number of requests to the protected domain name while the website was down	≥ 0 Value type: Float	Protected domain dame	5

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
inbound_traffic	Total Inbound Traffic	Total inbound traffic in the last 5 minutes Unit: Mbit/s Collection method: Total inbound traffic in the last 5 minutes	≥0 Mbit Value type: Float	Protected domain dame	5
outbound_traffic	Total Outbound Traffic	Total outbound traffic in the last 5 minutes Unit: Mbit/s Collection method: Total outbound traffic in the last 5 minutes	≥0 Mbit Value type: Float	Protected domain dame	5

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
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. Unit: Count 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	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	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. Unit: Count 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	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	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. Unit: Count 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	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	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. Unit: Count 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	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	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. Unit: Count Collection method: The number of requests processed by WAF at latencies in the 100 ms to less than 1000 ms range in the last 5 minutes are collected.	≥ 0 Value type: Float	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. Unit: Count 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	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	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. Unit: Count Collection method: The peak QPS of the domain name in the last 5 minutes is collected.	≥ 0 Value type: Float	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. Unit: Count Collection method: The average QPS of the domain name in the last 5 minutes is collected.	≥ 0 Value type: Float	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	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. Unit: Count Collection method: The number of requests with no WAF status code returned in the last 5 minutes is collected.	≥ 0 Value type: Float	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. Unit: Count 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	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	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. Unit: Count 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	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. Unit: Count 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	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	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. Unit: Count 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	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. Unit: Count 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	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
inbound_traffic_peak	Peak Inbound Traffic	This metric is used to collect the peak inbound traffic to the domain name in the last 5 minutes. Unit: Mbit/s Collection method: The peak inbound traffic to the domain name in the last 5 minutes is collected.	≥0 Mbit/s Value type: Float	Protected domain dame	5 minutes
inbound_traffic_mean	Average Inbound Traffic	This metric is used to collect the average inbound traffic to the domain name in the last 5 minutes. Unit: Mbit/s Collection method: The average inbound traffic to the domain name in the last 5 minutes is collected.	≥0 Mbit/s Value type: Float	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
outbound_traffic_peak	Peak Outbound Traffic	This metric is used to collect the peak outbound traffic from the domain name in the last 5 minutes. Unit: Mbit/s Collection method: The peak outbound traffic from the domain name in the last 5 minutes is collected.	≥0 Mbit/s Value type: Float	Protected domain dame	5 minutes
outbound_traffic_mean	Average Outbound Traffic	This metric is used to collect the average outbound traffic from the domain name in the last 5 minutes. Unit: Mbit/s Collection method: The average outbound traffic from the domain name in the last 5 minutes is collected.	≥0 Mbit/s Value type: Float	Protected domain dame	5

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
attacks	Total number of attacks	This metric is used to collect the total number of attacks against the domain name in the last 5 minutes. Unit: Count Collection method: The system collects the number of attacks against the domain name over the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes
crawlers	Number of crawler attacks	This metric is used to collect the crawler attacks against the domain name in the last 5 minutes. Unit: Count Collection method: The system collects the number of crawler attacks against the domain name in the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
base_protection_counts	Number of attacks blocked by basic web protection	This metric is used to collect the number of attacks defended by basic web protection rules over the last 5 minutes. Unit: Count Collection method: The system collects the number of attacks hit basic web protection rules over the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes
precise_protection_counts	Precise protection times	This metric is used to collect the number of attacks defended by precise protection rules over the last 5 minutes. Unit: Count Collection method: The system collects the number of attacks hit precise protection rules over the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
cc_protection_counts	Number of CC attacks detected by WAF	This metric is used to collect the number of attacks defended by CC attack protection rules over the last 5 minutes. Unit: Count Collection method: The system collects the number of attacks hit CC attack protection rules over the last 5 minutes.	≥ 0 Value type: Float	Protected domain dame	5 minutes

Metrics for Dedicated WAF Instances

Table 12-2 Metrics for dedicated waf instances

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
cpu_util	CPU Usage	CPU consumed by the monitored object Unit: percentage (%) Collection method: 100% minus idle CPU usage percentage	0% to 100% Value type: Float	Dedicated WAF instances	1

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
mem_util	Memory Usage	Memory usage of the monitored object Unit: percentage (%) Collection method: 100% minus idle memory percentage	0% to 100% Value type: Float	Dedicated WAF instances	1
disk_util	Disk Usage	Disk usage of the monitored object Unit: percentage (%) Collection method: 100% minus idle disk space percentage	0% to 100% Value type: Float	Dedicated WAF instances	1
disk_avail_size	Available Disk Space	Available disk space of the monitored object Unit: byte, KB, MB, GB, TB or PB Collection mode: size of free disk space	≥ 0 bytes Value type: Float	Dedicated WAF instances	1

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
disk_read_bytes_rate	Disk Read Rate	Number of bytes the monitored object reads from the disk per second Unit: byte/s, KB/s, MB/s, or GB/s Collection mode: number of bytes read from the disk per second	≥0 byte/s Value type: Float	Dedicated WAF instances	1
disk_write_bytes_rate	Disk Write Rate	Number of bytes the monitored object writes into the disk per second Unit: byte/s, KB/s, MB/s, or GB/s Collection mode: number of bytes written into the disk per second	≥0 byte/s Value type: Float	Dedicated WAF instances	1

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
disk_read_requests_rate	Disk Read Requests	Number of requests the monitored object reads from the disk per second Unit: Requests/s Collection mode: number of read requests processed by the disk per second	≥0 request/s Value type: Float	Dedicated WAF instances	1
disk_write_requests_rate	Disk Write Requests	Number of requests the monitored object writes into the disk per second Unit: Requests/s Collection method: Number of write requests processed by the disk per second	≥0 request/s Value type: Float	Dedicated WAF instances	1
network_incoming_bytes_rate	Incoming Traffic	Incoming traffic per second on the monitored object Unit: byte/s, KB/s, MB/s, or GB/s Collection method: Incoming traffic over the NIC per second	≥0 byte/s Value type: Float	Dedicated WAF instances	1

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
network_outgoing_bytes_rate	Outgoing Traffic	Outgoing traffic per second on the monitored object Unit: byte/s, KB/s, MB/s, or GB/s Collection method: Outgoing traffic over the NIC per second	≥0 byte/s Value type: Float	Dedicated WAF instances	1
network_incoming_packets_rate	Incoming Packet Rate	Incoming packets per second on the monitored object Unit: packet/s Collection method: Incoming packets over the NIC per second	≥0 packet/s Value type: Int	Dedicated WAF instances	1
network_outgoing_packets_rate	Outgoing Packet Rate	Outgoing packets per second on the monitored object Unit: packet/s Collection method: Outgoing packets over the NIC per second	≥0 packet/s Value type: Int	Dedicated WAF instances	1

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
concurrent_connections	Concurrent Connections	Number of concurrent connections being processed Unit: count Collection method: Number of concurrent connections in the system	≥0 count Value type: Int	Dedicated WAF instances	1
active_connections	Active Connections	Number of active connections Unit: count Collection method: Number of active connections in the system	≥0 count Value type: Int	Dedicated WAF instances	1
latest_policy_sync_time	Latest Rule Synchronization	Time elapsed for the WAF to synchronize the latest custom rules Unit: ms Collection method: Time elapsed for synchronizing to the last policies	≥0 ms Value type: Int	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
   }
]
```

12.1.2 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

The website you want to protect has been connected to WAF.

Configuring Alarm Monitoring Rules

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 & Deployment** > **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

12.1.3 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 of the management console and select a region or project.

Step 3 Click ☰ in the upper left corner of the page and choose **Management & Deployment** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Cloud Service Monitoring** > **Web Application Firewall**.

Step 5 In the row containing the dedicated instance or protected domain name, click **View Metric** in the **Operation** column.

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

12.2 Auditing

12.2.1 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 12-3 WAF Operations Recorded by CTS

Operation	Resource Type	Trace Name
Creating a WAF instance	instance	createInstance
Deleting a WAF instance	instance	deleteInstance
Modifying a WAF instance	instance	alterInstanceName
Modifying the protection status of a WAF instance	instance	modifyProtectStatus
Modifying the connection status of a WAF instance	instance	modifyAccessStatus
Creating a WAF policy	policy	createPolicy
Applying a WAF policy	policy	applyToHost
Modifying a policy	policy	modifyPolicy
Deleting a WAF policy	policy	deletePolicy
Modifying alarm notification settings	alertNoticeConfig	modifyAlertNoticeConfig
Uploading a certificate	certificate	createCertificate
Changing the name of a certificate	certificate	modifyCertificate
Deleting a certificate from WAF	certificate	deleteCertificate
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

Operation	Resource Type	Trace Name
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
Deleting a web tamper protection rule	policy	deleteAntitamper
Creating a global protection whitelist rule	policy	createIgnore
Deleting a global protection whitelist rule	policy	deleteIgnore
Adding a data masking rule	policy	createPrivacy
Modifying a data masking rule	policy	modifyPrivacy
Deleting a data masking rule	policy	deletePrivacy

12.2.2 Querying Real-Time Traces

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in OBS buckets. CTS stores operation records generated in the last seven days.

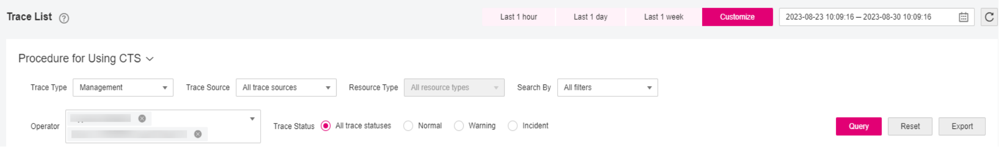
This section describes how to query and export operation records of the last seven days on the CTS console.

- **Viewing Real-Time Traces in the Trace List**

Viewing Real-Time Traces in the Trace List

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Management & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Set filters to search for your desired traces, as shown in **Figure 12-1**. The following filters are available:

Figure 12-1 Filters



Trace List ?

Last 1 hour | Last 1 day | Last 1 week | Customize | 2023-08-23 10:09:16 – 2023-08-30 10:09:16

Procedure for Using CTS

Trace Type: Management | Trace Source: All trace sources | Resource Type: All resource types | Search By: All filters

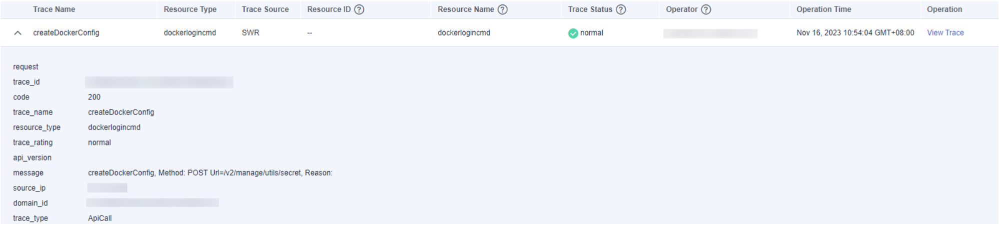
Operator: [redacted] [redacted]

Trace Status: ● All trace statuses ○ Normal ○ Warning ○ Incident

Query | Reset | Export

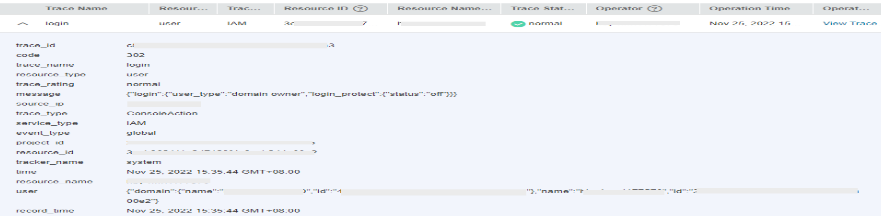
- **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
  - If you select **Resource ID** for **Search By**, specify a resource ID.
  - If you select **Trace name** for **Search By**, specify a trace name.
  - If you select **Resource name** for **Search By**, specify a resource name.
- **Operator**: Select a user.
- **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
- Time range: You can query traces generated during any time range in the last seven days.
- Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.

5. Click **Query**.
6. 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 5000 records.
   - Click ↻ to view the latest information about traces.
7. Click ⌄ on the left of a trace to expand its details.



Trace Name	Resource Type	Trace Source	Resource ID ?	Resource Name ?	Trace Status ?	Operator ?	Operation Time	Operation
createDockerConfig	dockerlogincmd	SWR	--	dockerlogincmd	normal	[redacted]	Nov 16, 2023 10:54:04 GMT+08:00	View Trace

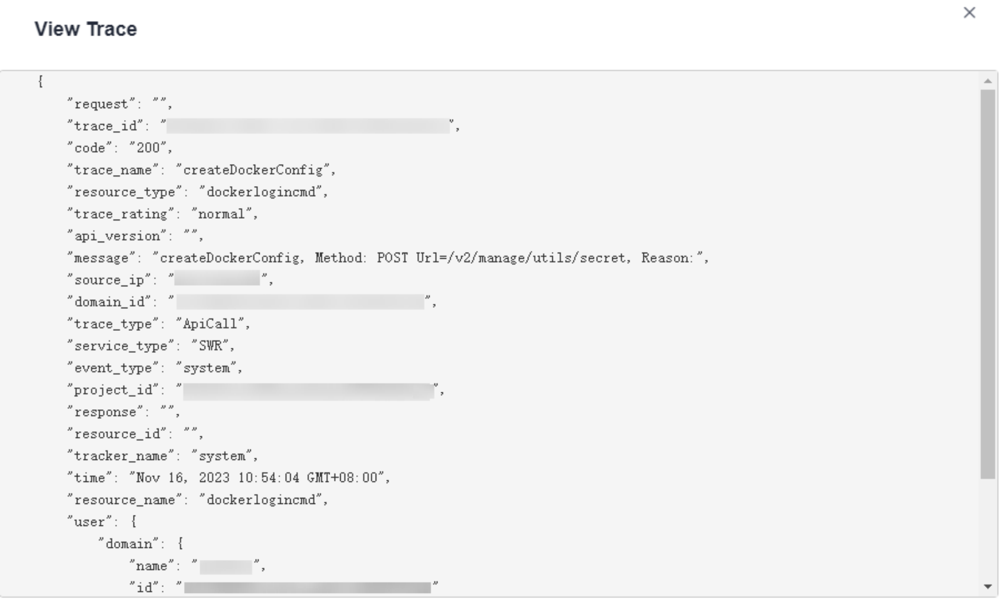
request	
trace_id	[redacted]
code	200
trace_name	createDockerConfig
resource_type	dockerlogincmd
trace_rating	normal
api_version	
message	createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:
source_ip	[redacted]
domain_id	[redacted]
trace_type	ApiCall



Trace Name	Resour...	Trac...	Resource ID ?	Resource Name...	Trace Stat...	Operator ?	Operation Time	Operat...
login	user	IAM	3c[redacted]7...	r[redacted]	normal	[redacted]	Nov 25, 2022 15...	View Trace.

trace_id	c[redacted]3
code	302
trace_name	login
resource_type	user
trace_rating	normal
message	{"login":{"user_type":"domain owner","login_protect":{"status":"off"}}}
source_ip	[redacted]
trace_type	ConsoleAction
service_type	IAM
event_type	global
project_id	[redacted]
resource_id	3[redacted]2
tracker_name	system
time	Nov 25, 2022 15:35:44 GMT+08:00
resource_name	[redacted]
user	{"domain":{"name":"[redacted])","id":"4[redacted]"},"name":"r[redacted]","id":"3[redacted] 00e2"}
record_time	Nov 25, 2022 15:35:44 GMT+08:00

8. Click **View Trace** in the **Operation** column. The trace details are displayed.



```
{
    "request": "",
    "trace_id": "[redacted]",
    "code": "200",
    "trace_name": "createDockerConfig",
    "resource_type": "dockerlogincmd",
    "trace_rating": "normal",
    "api_version": "",
    "message": "createDockerConfig, Method: POST Url=/v2/manage/utils/secret, Reason:",
    "source_ip": "[redacted]",
    "domain_id": "[redacted]",
    "trace_type": "ApiCall",
    "service_type": "SWR",
    "event_type": "system",
    "project_id": "[redacted]",
    "response": "",
    "resource_id": "",
    "tracker_name": "system",
    "time": "Nov 16, 2023 10:54:04 GMT+08:00",
    "resource_name": "dockerlogincmd",
    "user": {
        "domain": {
            "name": "[redacted]",
            "id": "[redacted]"
```

9. For details about key fields in the trace structure, see section "Trace References" > "Trace Structure" and section "Trace References" > "Example Traces" in the *CTS User Guide*.