Web Application Firewall

User Guide

Issue 148

Date 2024-02-22

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Contents

1 WAF Operation Guide

After you enable the WAF service, you need to connect your website domain name to WAF so that all access requests are forwarded to WAF for protection.

Procedure for Using WAF

Figure 1-1 shows the procedure. **Table 1-1** describes the procedure.

Figure 1-1 Procedure for using WAF

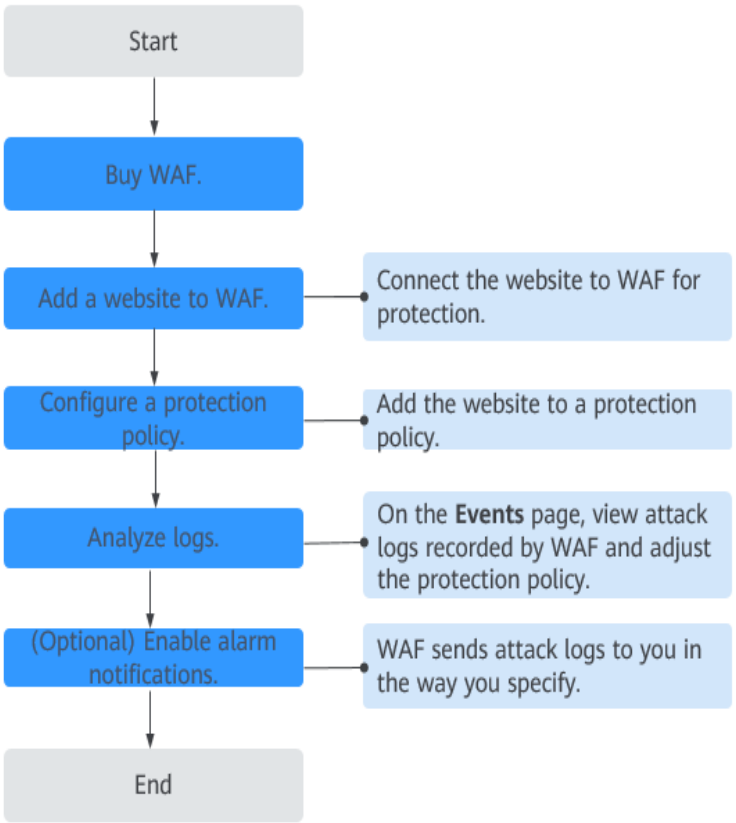


Table 1-1 Procedure for using WAF

Operation	Description
Buy WAF.	Buy a cloud WAF instance in the yearly/monthly or pay-per-use billing mode or buy dedicated WAF instances billed in the pay-per-use billing mode. **NOTICE** • To buy pay-per-use WAF instances, **submit a service ticket** to enable the service. • To use ELB-access WAF, you need to **submit a service ticket** to enable it for you first. If you have bought a cloud WAF, you can use ELB-access WAF and cloud WAF at the same time as long as the cloud WAF you are using is the standard edition or the above. • WAF APIs are free.
Add a website to WAF.	Add websites you want to protect to your WAF instance. • Cloud - CNAME Access: See **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**. • Cloud - ELB Access: See **Adding a Website to WAF (Cloud Mode - ELB Access)**. • Dedicated mode: See **Step 1: Add a Website to WAF (Dedicated Mode)**. **NOTE** • Using WAF does not affect your web server performance because the WAF engine is not running on your web server. • After your domain name is connected to WAF, there will be a latency of tens of milliseconds, which might be raised based on the size of the requested page or number of incoming requests.
Configure 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.
Analyze logs.	WAF displays blocked or logged-only attacks on the **Events** page. You can view and analyze protection logs to adjust your website protection policies or mask false alarms.
(Optional) Enable alarm notifications.	Enable this function to receive an alarm notification the instant 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.

Related Functions

Beyond functions in **Procedure for Using WAF**, WAF also provides the following functions for you to improve your website security performance.

Table 1-2 Related functions

Function	Description
Dashboard	You can view protection data of yesterday, today, last 3 days, last 7 days, or last 30 days.
Configuring a Security Report	WAF can generate daily, weekly, monthly, or custom reports based on the report templates you have created. Reports will be sent to you in the way and within the time range you configure.
Configuring PCI DSS/3DS Certification Check and Configuring the Minimum TLS Version and Cipher Suite	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.
Enabling WAF IPv6 Protection	If you enable IPv6 protection, WAF assigns an IPv6 address to your domain name. In this manner, your website can be reached using the IPv6 address.
Enabling the HTTP/2 Protocol	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**.
Configuring Connection Timeout	• The default 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 duration for the connection between WAF and an origin server is 60 seconds. You can manually set the timeout duration on the WAF console.
Configuring Connection Protection	If a large number of 502 Bad Gateway and 504 Gateway Timeout errors are detected, you can enable WAF breakdown protection and connection protection to let WAF suspend your website and protect your origin servers from being crashed. When the 502/504 error requests and pending URL requests reach the thresholds you configure, WAF enables corresponding protection for your website.
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**.
Editing Response Page for Blocked Requests	If a visitor is blocked by WAF, the **Default** block page of WAF is returned by default. You can also configure **Custom** or **Redirection** for the block page to be returned as required.

Function	Description
Forwarding Custom Header Fields	You can use WAF to add additional header information, for example, $request_id, to associate requests on the entire link. You can follow this topic to let WAF insert additional fields into a header and forward requests to origin servers. Note that the key value of a custom header field cannot be the same as any native Nginx fields.
Managing Certificates	If you upload a certificate to WAF, you can directly select the certificate when adding a website to WAF.
Managing IP Address Blacklist and Whitelist Groups	With IP address groups, you can quickly add IP addresses or IP address ranges to a blacklist or whitelist rule.
Managing Dedicated 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.
Viewing Product Details	On the **Product Details** page, you can view information about all your WAF instances, including the edition, domain quotas, and specifications.

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.

NOTE

- To buy pay-per-use WAF instances, **submit a service ticket** to enable the service.
- To use ELB-access cloud WAF, you need to **submit a service ticket** to enable it for you first. ELB-access cloud WAF is available in some regions. For details, see **Functions**.
- If you have purchased cloud WAF (standard, professional, or platinum edition), CNAME and ELB access methods share the domain name, bandwidth, and rule extension packages you have purchased.
- WAF APIs are free.

Before You Start

- Only one billing mode can be selected for your WAF instance in an account.
- In the yearly/monthly billing mode, only one WAF edition can be purchased under an account in the same great region such as CN East, including CN East-Shanghai1 and CN East-Shanghai2 regions.
- Switch between yearly/monthly and pay-per-use payments is supported. For details, see **Can I Switch Between Yearly/Monthly and Pay-per-Use Payments for WAF?**
- For a cloud WAF instance billed on a yearly/monthly basis, after it expires or you unsubscribe from it, you can enable another WAF instance billed on either yearly/monthly or pay-per-use basis. The WAF service can save the configuration data of the original WAF instance so that you can use the configuration data without having to configure the new WAF instance only when the following conditions are met:
  - If you choose the pay-per-use billing mode, the new and original WAF instances must be under the same project in the same region.

  - If you choose the yearly/monthly billing mode, the new and original WAF instances must be in the same region.
- For a cloud WAF instance billed on a pay-per-use basis, you can disable the yearly/monthly billing mode and then enable the instance in either yearly/monthly or pay-per-use billing mode.

NOTICE

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

Prerequisites

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

Constraints

- Only one WAF edition can be purchased under an account in the same geographic region (for example, CN East regions).

  NOTE

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

  Generally, a WAF instance purchased in any region can protect web services in all regions. To make a WAF instance forward your website traffic faster, select the region nearest to your services.
- The specifications of a WAF instance cannot be changed once you complete the purchase. To use a WAF instance with lower specifications, unsubscribe from the WAF instance you are using and buy another one.
- If you are using a professional or platinum WAF instance, you can configure any non-standard ports for your website. To do so, **submit a ticket** to enable custom non-standard ports.

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.)

NOTICE

- If you have purchased cloud WAF (standard, professional, or platinum edition), CNAME and ELB access methods share the domain name, bandwidth, and rule extension packages you have purchased.
- The bandwidth limit applies only to websites accessed in cloud mode. Websites accessed in ELB mode have no bandwidth limit but only QPS limit.

- 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.

Purchasing a WAF Instance Billed Yearly/Monthly (New Console)

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 & Compliance**.

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 Select a region and WAF edition.

NOTE

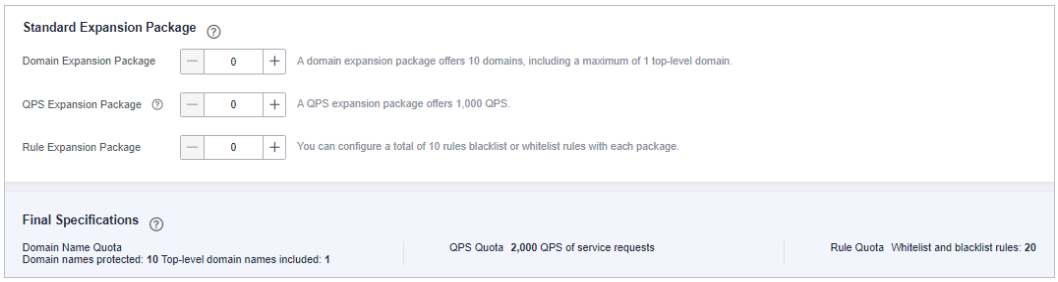
Generally, a WAF instance purchased in any region can protect web services in all regions. To make a WAF instance forward your website traffic faster, select the region nearest to your services.

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

Step 8 Specify the number of domain name, QPS, or rule expansion packages.

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

Figure 2-1 Selecting expansion packages



Step 9 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 10 Confirm the product details and click **Buy Now**.

Step 11 Check the order details and read the *Huawei Cloud WAF Disclaimer*. Then, select the box and click **Pay Now**.

Step 12 Confirm the order details and click **Pay Now**.

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

----End

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

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

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

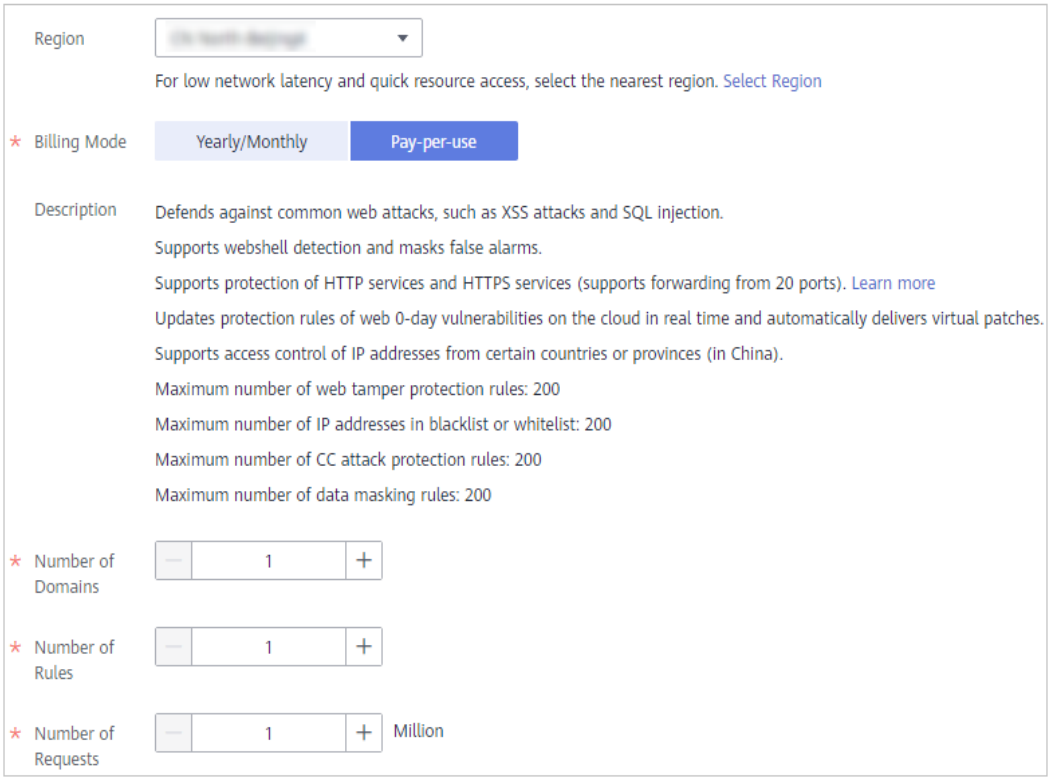
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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**, select an edition, and configure the number of domain names, rules, and requests. **Figure 2-2** shows an example.

Figure 2-2 Selecting **pay-per-use**



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 **Region** drop-down list.

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.

Other Operations

- **Changing the Edition and Specifications of a Cloud WAF Instance**

  In cloud mode, to protect more domain names or traffic, upgrade the instance edition or increase the number of expansion packages.
- **How Do I Unsubscribe from WAF?**
- **How Do I Renew My 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.

NOTE

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

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

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.

Procedure

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

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

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**.

Figure 2-3 Configuring a dedicated WAF instance

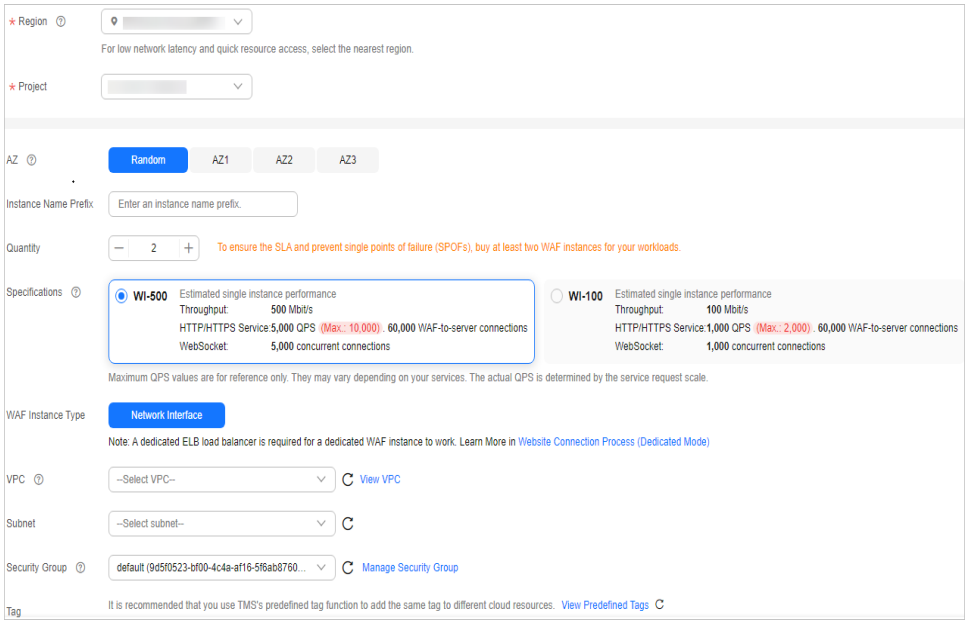


Table 2-1 Parameters of a dedicated WAF instance

Parameter	Description
Region	For details about supported regions, see **In Which Regions Is WAF Available?** Generally, a WAF instance purchased in any region can protect web services in all regions. To make a WAF instance forward your website traffic faster and reduce latency, select the region nearest to your services.
Project	Select a project in the target region.
AZ	Select an AZ in the selected region. **NOTE** After an AZ is selected, it cannot be changed after the purchase.
Instance Name Prefix	Set a prefix of the dedicated WAF instance name. If you purchase multiple instances, the prefix to each instance name is the same.
Quantity	Set the number of WAF instances you want to buy. 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.

Parameter	Description
Specifications	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
WAF Instance Type	Select a WAF instance type. Only **Network interface** is available now. The WAF instance will be connected to your network through a VPC network interface. Only dedicated load balancers can be used for this type of instance. For details, see **Website Connection Process (Dedicated Mode)**. **NOTE** If you want to select **ECS** for the instance type, you need to **submit a service ticket** to confirm that the region your services are deployed in supports this type of WAF instance.
VPC	Select the VPC to which the origin server belongs.
Subnet	Select a subnet configured in the VPC.

Parameter	Description
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. For more details, see **Adding a Security Group Rule**. • If your dedicated WAF instance and origin server are not in the same VPC, enable communications between the instance and the subnet of the origin server in the security group.
Tag	TMS's predefined tag function is recommended for adding the same tag to different cloud resources. If your organization has configured a tag policy for Web Application Firewall (WAF), you need to add tags to dedicated WAF instances based on the tag policy rules. If a tag does not comply with the policies, dedicated WAF instance may fail to be created. Contact your organization administrator to learn more about tag policies.
Authorization	This parameter is 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, 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.

Step 8 Confirm the order details 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.

Other 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

Protocol & Port	Type	Source Address	Description
TCP: 443	IPv4	100.125.0.0/16	WAF policy synchronization

2.3 Changing the Edition and Specifications of a Cloud WAF Instance

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.)

  NOTICE

  - If you have purchased cloud WAF (standard, professional, or platinum edition), CNAME and ELB access methods share the domain name, bandwidth, and rule extension packages you have purchased.
  - The bandwidth limit applies only to websites accessed in cloud mode. Websites accessed in ELB mode have no bandwidth limit but only QPS limit.
- 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, bandwidth, 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.

Procedure

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 & Compliance**.

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.

  By default, the number of extension packages cannot be reduced to 0. To do so, click **Unsubscribe**.
- 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 Confirm the order details 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

2.4 Expansion Packages Available in Cloud WAF

2.4.1 Domain Name 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.

In the upper right corner of the WAF management console, click **Change** to buy a domain expansion package.

NOTICE

You can reduce quantity of or unsubscribe from purchased domain name expansion packages. For details, see **Changing the Edition and Specifications of a Cloud WAF Instance**.

Domain Name Quota of Different Editions in Cloud Mode

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 upgrade your cloud WAF edition to increase the domain name quota. For details, see **Changing the Edition and Specifications of a Cloud WAF Instance**.

2.4.2 QPS Expansion Packages

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

NOTICE

You can reduce quantity of or unsubscribe from purchased QPS expansion packages. For details, see **Changing the Edition and Specifications of a Cloud WAF Instance**.

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 contains:
  - 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

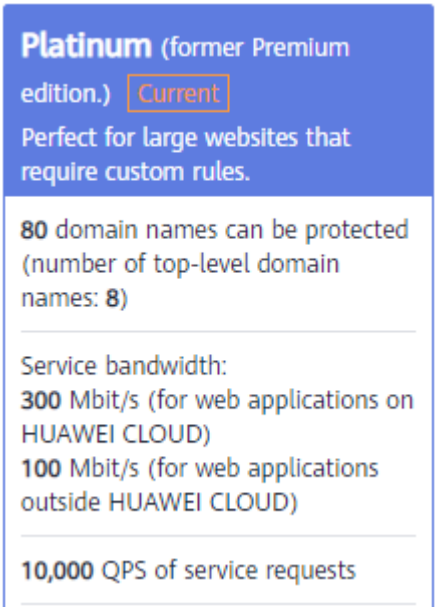
    Service bandwidth: 20 Mbit/s

    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.

Figure 2-4 Service bandwidth



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.

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.

QPS Expansion Package

If your website service traffic is much more than what your WAF instance can protect, you can buy more 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. For details, see **Changing the Edition and Specifications of a Cloud WAF Instance**.

2.4.3 Rule Expansion Packages

For cloud WAF instances, if the quota for IP address blacklist and whitelist rules of your current WAF instance is insufficient, you can buy rule expansion packages to configure more such kind of rules.

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

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

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

NOTICE

You can reduce quantity of or unsubscribe from purchased rule expansion packages. For details, see **Changing the Edition and Specifications of a Cloud WAF Instance**.

3 Dashboard

On the **Dashboard** page, you can view the protection logs of all protected websites or instances for a specified time range, including yesterday, today, past 3 days, past 7 days, or past 30 days. On this page, event logs are displayed by different dimensions, including the number of requests and attack types, QPS, bandwidth, response code, event distribution, top 10 attacked domain names, top 10 attack source IP addresses, top 10 attacked URLs, top 10 attack source locations, and top 10 error pages.

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

- A domain name has been added and connected to WAF.
- WAF protection is enabled.
- At least one protection rule has been configured for the domain name.

Specification Limitations

On the **Dashboard** page, protection data of a maximum of 30 days can be viewed.

How to Calculate QPS

The QPS calculation method varies depending on the time range. For details, see **Table 3-1**.

Table 3-1 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.

Procedure

Step 1 Log in to the management console.

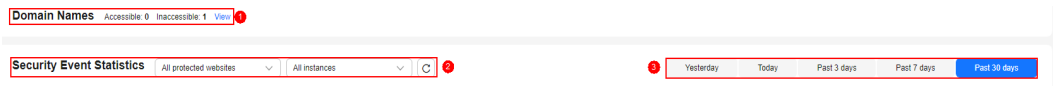
Step 2 Click in the upper left corner of the management console and select a region or project.

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

Step 4 In the upper part of the page, specify the website, instance, and time range for your query.

- By default, the information about all websites you add to WAF in all enterprise projects are displayed.
- **Domain Names**: shows information about websites added to the WAF instance. Click **View** to go to the **Website Settings** page and view details about domain names of protected websites.
- Query time: You can select **Yesterday**, **Today**, **Past 3 days**, **Past 7 days**, or **Past 30 days**.

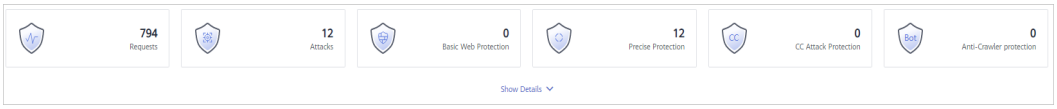
Figure 3-1 Setting search criteria



Step 5 View 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 of the 10 domain names with the most requests, attacks, and basic web protection, precise protection, CC attack protection, and anti-crawler protection actions.

Figure 3-2 Protection action statistics



Step 6 Query security data in the **Security Event Statistics** area.

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 3-3 Security Event Statistics

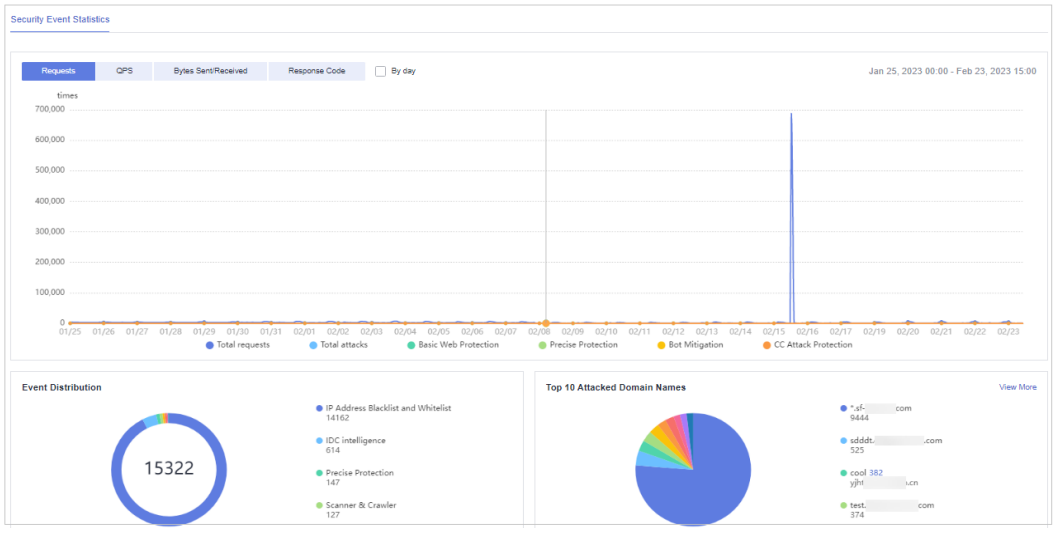


Table 3-2 Parameters in Security Event Statistics

Parameter	Description
Requests	You can view how many requests for your website as well as total attacks and attacks of each attack type.

Parameter	Description
QPS	Average number of requests per second for the domain name. For details about the values of 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	Bandwidth usage 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.
Event Distribution	Types of attack events Click an area in the **Event Distribution** area to view the type, number, and proportion of an attack.
Top 10 Attacked Domain Names	The ten most attacked domain names and the number of attacks on each domain name. Click **View More** to go to the **Events** page and view more protection data.
Top 10 Attack Source IP Addresses	The ten source IP addresses with the most attacks and the number of attacks from each source IP address. Click **View More** to go to the **Events** page and view more protection data.
Top 10 Attacked URLs	The ten most attacked URLs and the number of attacks on each URL. Click **View More** to go to the **Events** page and view more protection data.

----End

4 Security Reports

WAF can generate daily, weekly, monthly, or custom reports based on the report templates you have created. Reports will be sent to you in the way and within the time range you configure.

Prerequisites

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

Constraints

- WAF offers a quota for creating report templates.
  - Cloud mode - professional edition: 10
  - Cloud mode - platinum or dedicated edition: 20
  - Cloud mode - standard edition: 5
- WAF stores security reports for six months only. You are advised to regularly download reports to meet compliance and audit requirements.

Creating a Report Template

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

Step 2 Click in the upper left corner 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 & Compliance**.

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

Step 5 In the upper left corner of the list, click **Create Report Template**. **Table 4-1** describes the parameters.

Figure 4-1 Create Report Template

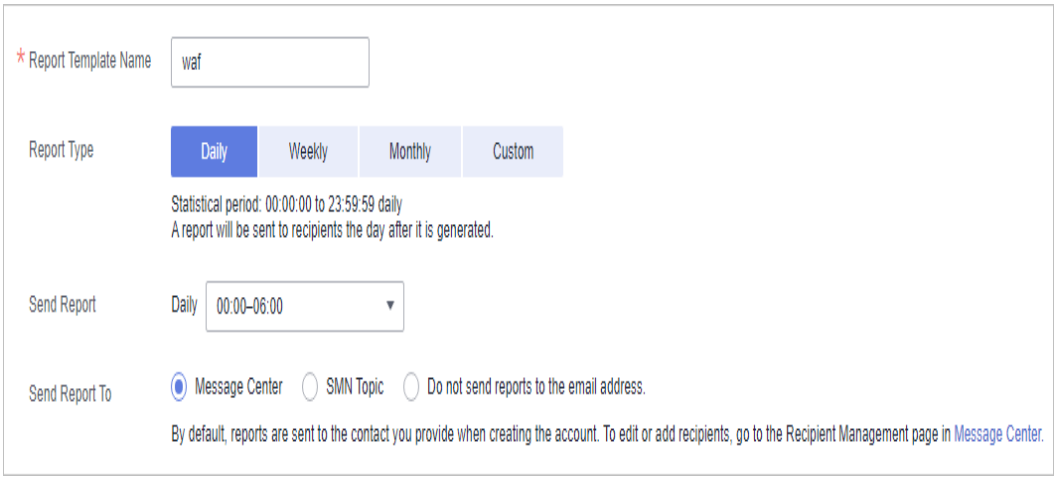


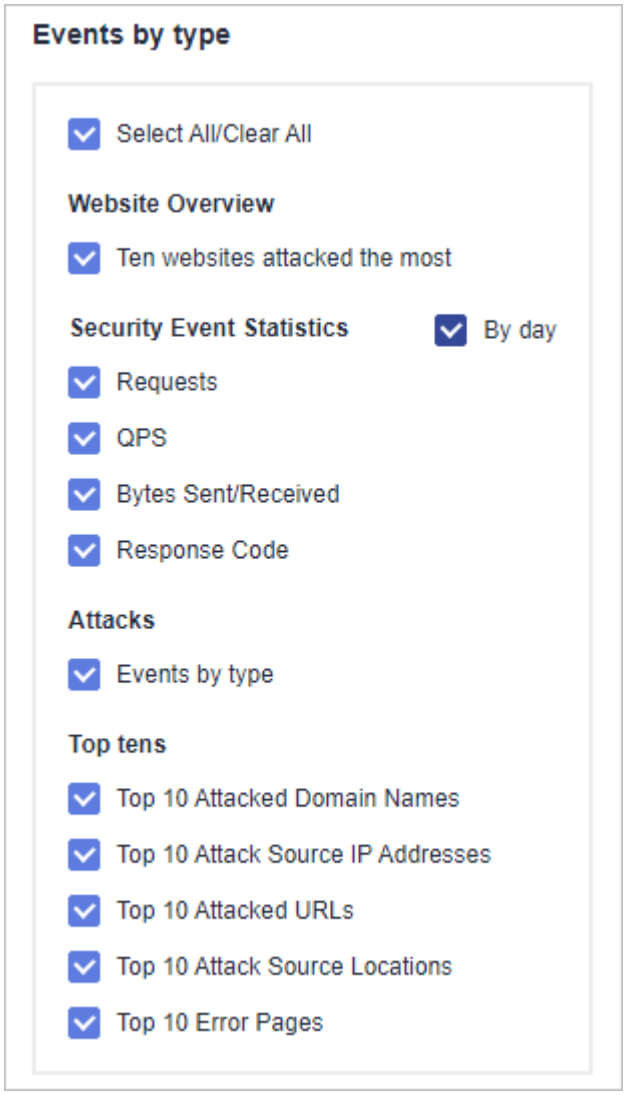
Table 4-1 Parameters for creating a report template

Parameter	Description
Report Template Name	Name of the custom security report template.
Report Type	• Daily Statistical period: 00:00:00 to 23:59:59 every day A report will be sent to the recipients the day after it is generated. • Weekly Statistical period: 00:00:00 on Monday to 23:59:59 on Sunday A report will be sent to the recipients the next Monday after it is generated. • Monthly Statistical period: 00:00:00 on the first day of each month to 23:59:59 on the last day of that month A report will be sent to the recipients on the first day of the month after it is generated. • Custom Customize the log statistics period.
Data Scope	If **Report Type** is set to **Custom**, you need to set **Statistical Period**.
Send Report	Set the time range for sending daily reports. • Daily, weekly, and monthly reports: WAF sends protection log reports to recipients every day, every Monday, and on the first day of each month, respectively. • **Custom**: The report will be sent after it is generated.

Parameter	Description
Send Report To	You can enable any of the following ways to receive security reports: • **Message Center**: Click in the upper right corner of the page to access the message center and add recipient information. • **SMN Topic**: Select a topic from the drop-down list or click **Create SMN Topic** to create one and configure recipients.

Step 6 Click **Next: Set Report Content** and select the content you want the report to include.

Figure 4-2 Select Report Content



Step 7 Click **Save Report**.

----End

Downloading a Report

WAF stores security reports for six months only. You are advised to regularly download reports to meet compliance and audit requirements.

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

Step 2 Click  in the upper left corner 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 & Compliance**.

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

Step 5 In the row containing the desired report template, click **Download New Report** in the **Operation** column.

----End

Other Operations

- By default, report templates are enabled once they are created. To disable a report template, locate the row containing the report template you want to disable and choose **More** > **Disable** in the **Operation** column.
- To delete a report template, locate the row containing the report template you want to delete and choose **More** > **Delete** in the **Operation** column.
- To copy a report template, locate the row containing the report template you want to copy and choose **More** > **Copy** in the **Operation** column.
- To edit a report template, locate the row containing the report template you want to edit and choose **More** > **Edit** in the **Operation** column.

5 Events

5.1 Viewing Protection Event Logs

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.

NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and view protection event logs in the project.

Prerequisites

The website to be protected has been connected to WAF.

Constraints

- If the security software installed on your server blocks the event file from being downloaded, close the software and download the file again.
- On the WAF console, you can view the event data for all protected domain names over the last 30 days. You can authorize LTS to log WAF activities so that you can view attack and access logs and store all logs for a long time. For more details, see. **Enabling LTS for WAF Logging**.
- 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.

Procedure

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.

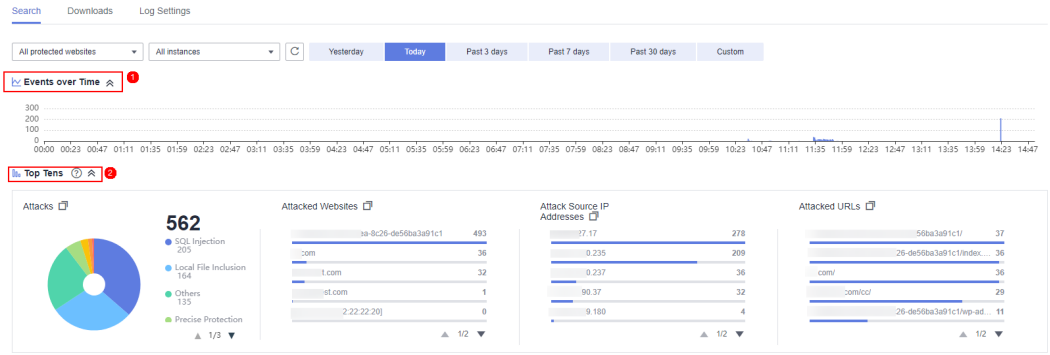
Step 3 Click ☰ in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.

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**: WAF 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 5-1 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 5-2** lists parameters for filter conditions.
- In the upper left corner of the event list, click **Export** to export events. If the number of events is less than 200, the events are exported to your local PC. If the number of events is greater than or equal to 200, the event record is displayed on the **Downloads** page. You can download the events on the **Downloads** page.
- 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 5-2 Events

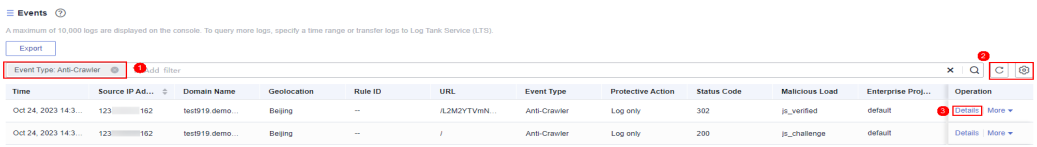


Table 5-1 Search condition fields

Parameter	Parameter
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
Protective Action	The options are **Block**, **Log only**, and **Verification code**. 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.
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
Status Code	HTTP status code returned on the block page.
Domain Name	Attacked domain name

Table 5-2 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	-

Parameter	Description	Example Value
URL	Attacked URL	/admin
Event Type	Type of attack	SQL injection
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	The location or part of the attack that causes damage or the number of times that the URL was accessed. **NOTE** • In a CC attack, the malicious load indicates the number of times that the URL was accessed. • For blacklist protection events, the malicious load is left blank.	id=1 and 1='1
Enterprise Project	Enterprise project your websites belong to.	default

----End

5.2 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 event.

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.
- The attack event will not be displayed on the **Events** page. You will no longer receive any alarm notifications about the event.
- 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.

Procedure

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 & Compliance**.

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 5-3 Handling a false alarm

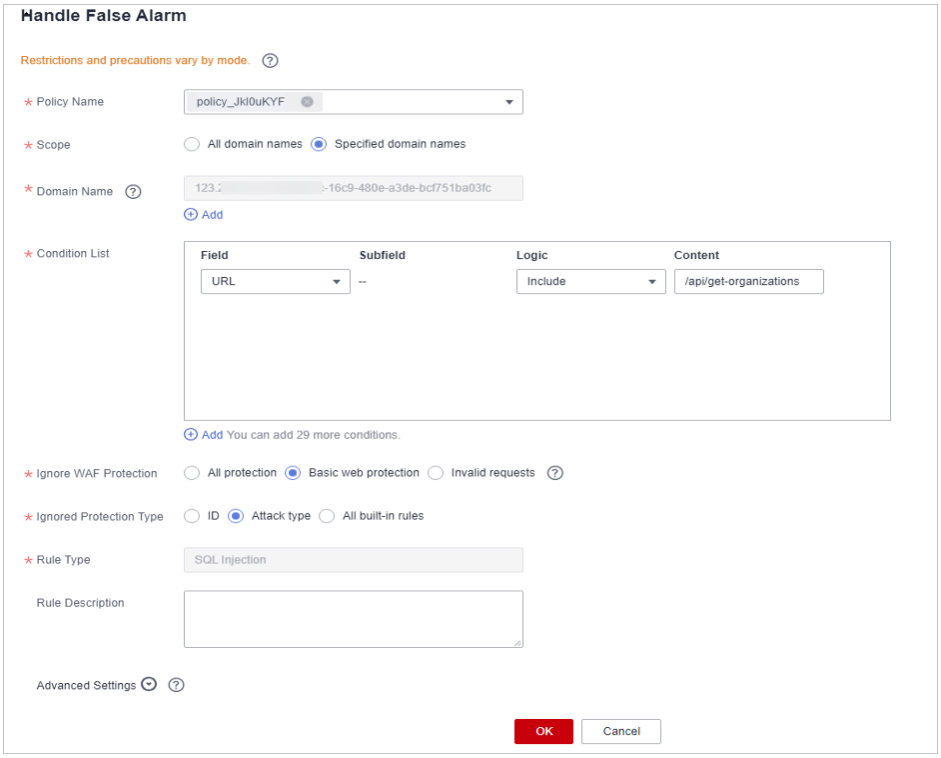


Table 5-3 Parameters

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. To add more domain names, click **Add** to add them one by one.	www.example.com

Parameter	Description	Example Value
Condition List	– Click **Add** in the condition box to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. – You can click **Add** outside the condition box to add a group of conditions. A maximum of three groups of conditions can be added. The relationship between multiple groups of conditions is **or**. So, the rule takes effect when one group of conditions is met. 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

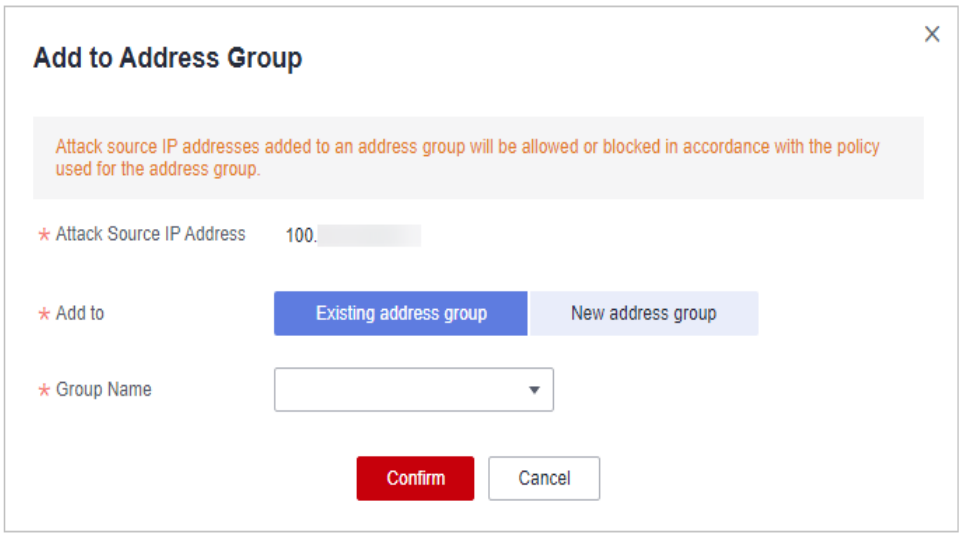
Parameter	Description	Example Value
Ignore WAF Protection	– **All protection**: All WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule. – **Basic web protection**: You can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, 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 URI 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.
Advanced Settings	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 5-4 Add to Address Group



- 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 5-5 Add to Blacklist/Whitelist

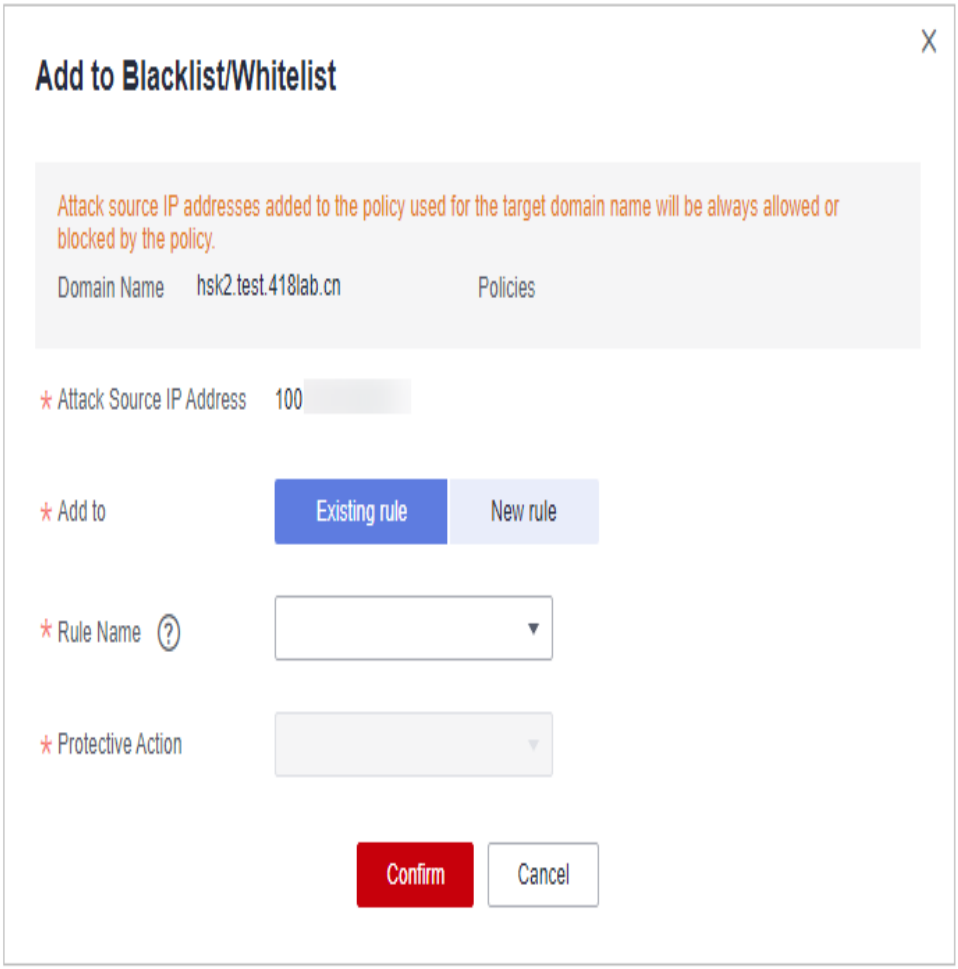


Table 5-4 Parameter

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.

Parameter	Description
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 request the page for which the global protection whitelist rule is configured to check whether the configuration takes effect.

Other 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 more details, see **Configuring a Global Protection Whitelist Rule to Ignore False Alarms**.

5.3 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 to be protected has been added 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.

Procedure

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 & Compliance**.

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

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

Table 5-5 Parameter description

Parameter	Description
File Name	The format is *file-name*.**csv**.
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
time	When the event occurred.	2020/11/21 0:20:44
url	URL of the protected domain name	N/A

Other Operations

Enable LTS in WAF for long-term log storage. In LTS, you can view attack and access log details. For more details, see **Enabling LTS for WAF Logging**.

5.4 Enabling LTS for WAF Logging

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

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

NOTICE

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

Prerequisites

- You have purchased a WAF instance.
- The website to be protected has been added to WAF.

Impact on the System

Enabling LTS for WAF does not affect WAF performance.

Enabling LTS for WAF Protection Event Logging

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

Step 2 Click  in the upper left corner 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 & Compliance**.

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

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

Figure 5-6 Log settings

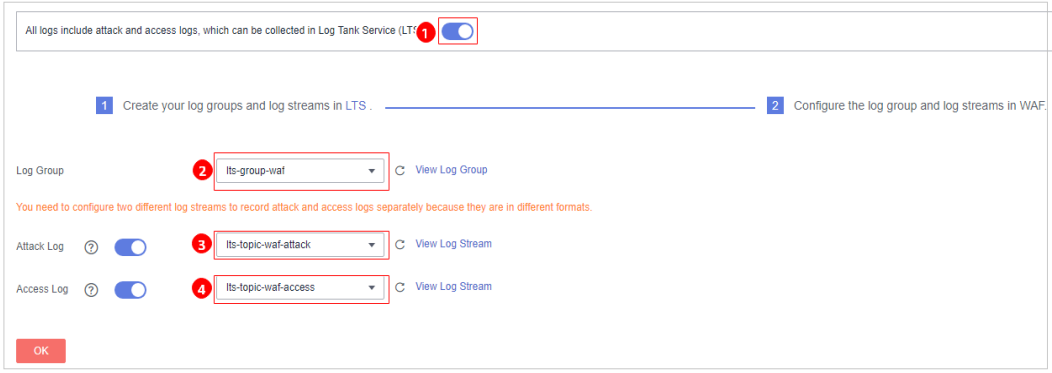


Table 5-6 Log configuration

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

Step 6 Click **OK**.

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

----End

Viewing WAF Protection Event Logs on LTS

After enabling LTS, perform the following steps to view and analyze WAF logs on the LTS console.

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.

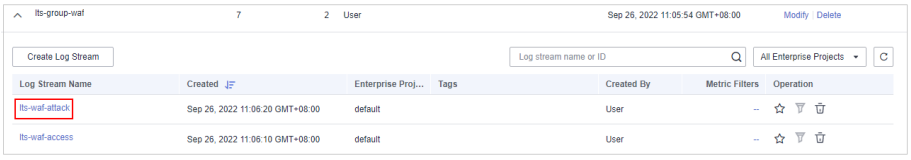
Step 3 Click in the upper left corner of the page and choose **Management & Deployment** > **Log Tank Service**.

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

Step 5 View protection event logs.

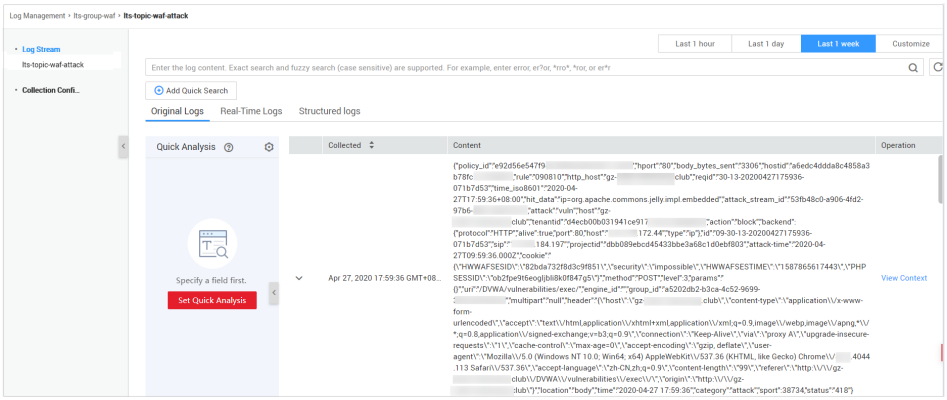
- View attack logs.
  a. In the log stream list, click the name of the configured attack log stream.

  Figure 5-7 Log stream name configured for attack logs

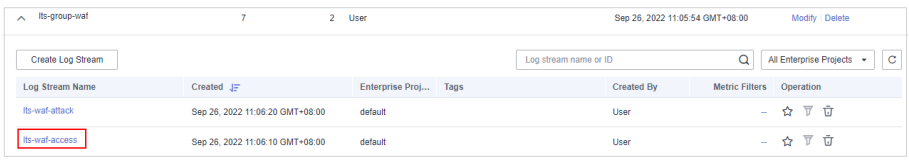
  b. View attack logs.

  Figure 5-8 Viewing attack logs

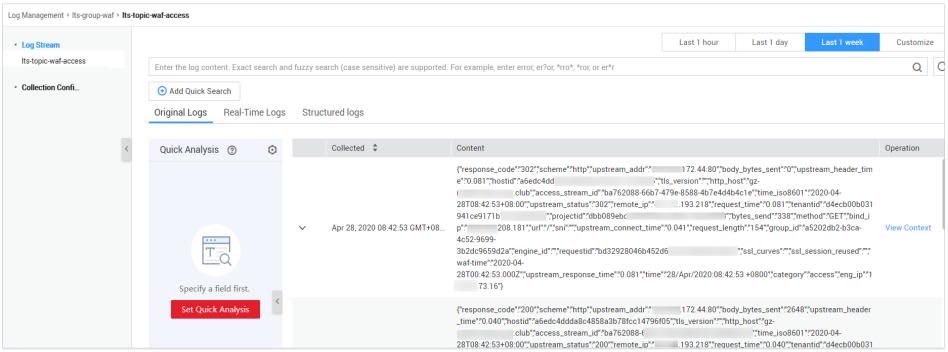
- View access logs.
  a. In the log stream list, click the name of the configured access log stream.

  Figure 5-9 Log stream name configured for access logs

  b. View access logs.

Figure 5-10 Viewing access logs



----End

WAF access_log Field

Field	Type	Field Description	Description
access_log.requestid	string	Random ID	The value is the same as the last eight characters of the **req_id** field in the attack log.
access_log.time	string	Access time	GMT time a log is generated.
access_log.connection_requests	string	Sequence number of the request over the connection	-
access_log.eng_ip	string	IP address of the WAF engine	-
access_log.pid	string	The engine that processes the request	Engine (worker PID).
access_log.hostid	string	Domain name identifier of the access request.	Protected domain name ID (upstream_id).
access_log.tenantid	string	Account ID	ID of your account.

Field	Type	Field Description	Description
access_log.projectid	string	ID of the project the protected domain name belongs to	Project ID of a user in a specific region.
access_log.remote_ip	string	Remote IP address of the request at layer 4	IP address from which a client request originates. **NOTICE** If a layer-7 proxy is deployed in front of WAF, this field indicates the IP address of the proxy node closest to WAF. The real IP address of the visitor is specified by the **x-forwarded-for** and **x_real_ip** fields.
access_log.remote_port	string	Remote port of the request at layer 4	Port used by the IP address from which a client request originates
access_log.sip	string	IP address of the client that sends the request	For example, XFF.
access_log.scheme	string	Request protocol	Protocols that can be used in the request: • HTTP • HTTPS
access_log.response_code	string	Response code	Response status code returned by the origin server to WAF.
access_log.method	string	Request method.	Request type in a request line. Generally, the value is **GET** or **POST**.
access_log.http_host	string	Domain name of the requested server.	Address, domain name, or IP address entered in the address bar of a browser.
access_log.url	string	Request URL.	Path in a URL (excluding the domain name).
access_log.request_length	string	Request length.	The request length includes the access request address, HTTP request header, and number of bytes in the request body.

Field	Type	Field Description	Description
access_log.bytes_send	string	Total number of bytes sent to the client.	Number of bytes sent by WAF to the client.
access_log.body_bytes_sent	string	Total number of bytes of the response body sent to the client	Number of bytes of the response body sent by WAF to the client
access_log.upstream_addr	string	Address of the backend server.	IP address of the origin server for which a request is destined. For example, if WAF forwards requests to an ECS, the IP address of the ECS is returned to this parameter.
access_log.request_time	string	Request processing time	Processing time starts when the first byte of the client is read (unit: s).
access_log.upstream_response_time	string	Backend server response time	Time the backend server responds to the WAF request (unit: s).
access_log.upstream_status	string	Backend server response code	Response status code returned by the backend server to WAF.
access_log.upstream_connect_time	string	Time for the origin server to establish a connection to its backend services. Unit: second.	When SSL is used, the time for the handshake process is also recorded. Time used for establishing a connection for a request. Use commas (,) to separate the time used for each request.
access_log.upstream_header_time	string	Time used by the backend server to receive the first byte of the response header. Unit: second	Response time for multiple requests. Use commas (,) to separate the time used for each response.

Field	Type	Field Description	Description
access_log.bind_ip	string	WAF engine back-to-source IP address.	Back-to-source IP address used by the WAF engine.
access_log.group_id	string	LTS log group ID	ID of the log group for interconnecting WAF with LTS.
access_log.access_stream_id	string	Log stream ID.	ID of **access_stream** of the user in the log group identified by the **group_id** field.
access_log.engine_id	string	WAF engine ID	Unique ID of the WAF engine.
access_log.time_iso8601	string	ISO 8601 time format of logs.	-
access_log.sni	string	Domain name requested through SNI.	-
access_log.tls_version	string	Protocol versioning an SSL connection.	TLS version used in the request.
access_log.ssl_curves	string	Curve group list supported by the client.	-
access_log.ssl_session_reused	string	SSL session reuse	Whether the SSL session can be reused **r**: Yes **.**: No
access_log.process_time	string	Engine attack detection duration (unit: ms)	-
access_log.args	string	The parameter data in the URL	-

Field	Type	Field Description	Description
access_log.x_forwarded_for	string	IP address chain for a proxy when the proxy is deployed in front of WAF.	The sting includes one or more IP addresses. The leftmost IP address is the originating IP address of the client. Each time the proxy server receives a request, it adds the source IP address of the request to the right of the originating IP address.
access_log.cdn_src_ip	string	Client IP address identified by CDN when CDN is deployed in front of WAF	This field specifies the real IP address of the client if CDN is deployed in front of WAF. **NOTICE** Some CDN vendors may use other fields. WAF records only the most common fields.
access_log.x_real_ip	string	Real IP address of the client when a proxy is deployed in front of WAF.	Real IP address of the client, which is identified by the proxy.
access_log.intel_crawler	string	Used for intelligence anti-crawler analysis.	-
access_log.ssl_ciphers_md5	string	MD5 value of the SSL cipher (ssl_ciphers).	-
access_log.ssl_cipher	string	SSL cipher used.	-
access_log.web_tag	string	Website name.	-
access_log.user_agent	string	User agent in the request header.	-
access_log.upstream_response_length	string	Backend server response size.	-

Field	Type	Field Description	Description
access_log.region_id	string	Region where the request is received.	-
access_log.enterprise_project_id	string	ID of the enterprise project that the requested domain name belongs to.	-
access_log.referer	string	Referer content in the request header.	The value can contain a maximum of 128 characters. Characters over 128 characters will be truncated.
access_log.rule	string	Protection rule that the request matched.	If multiple rules are matched, only one rule is displayed.

WAF attack_log field description

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

Field	Type	Field Description	Description
attack_log.attack	string	Type of attack	Attack type. This parameter is listed in attack logs only. • **default**: default attacks • **sqli**: SQL injections • **xss**: cross-site scripting (XSS) attacks • **webshell**: web shells • **robot**: malicious crawlers • **cmdi**: command injections • **rfi**: remote file inclusion attacks • **lfi**: local file inclusion attacks • **illegal**: unauthorized requests • **vuln**: exploits • **cc**: attacks that hit the CC protection rules • **custom_custom**: attacks that hit a precise protection rule • **custom_whiteblackip**: attacks that hit an IP address blacklist or whitelist rule • **custom_geoip**: attacks that hit a geolocation access control rule • **antitamper**: attacks that hit a web tamper protection rule • **anticrawler**: attacks that hit the JS challenge anti-crawler rule • **leakage**: vulnerabilities that hit an information leakage prevention rule • **antiscan_high_freq_scan**: Attacks that hit malicious scanning rules. • **followed_action**: The source is marked as a known attack source. For details, see **Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration**.
attack_log.action	string	Protective action	WAF defense action. • **block**: WAF blocks attacks. • **log**: WAF only logs detected attacks. • **captcha**: Verification code

Field	Type	Field Description	Description
attack_log.sub_type	string	Crawler types	When **attack** is set to **robot**, this parameter cannot be left blank. • **script_tool**: Script tools • **search_engine**: Search engines • **scanner:** Scanning tools • **uncategorized**: Other crawlers
attack_log.rule	string	ID of the triggered rule or the description of the custom policy type.	-
attack_log.rule_name	string	Description of a custom rule type.	This field is empty when a basic protection rule is matched.
attack_log.location	string	Location triggering the malicious load	-
attack_log.req_body	sting	Request body.	-
attack_log.resp_headers	string	Response header	-
attack_log.hit_data	string	String triggering the malicious load	-
attack_log.resp_body	string	Response body	-
attack_log.backend.protocol	string	Backend protocol.	-
attack_log.backend.alive	string	Backend server status.	-
attack_log.backend.port	string	Backend server port.	-
attack_log.backend.host	string	Backend server host value.	-
attack_log.backend.type	string	Backend server type.	IP address or domain name.

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

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

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

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

6 Policies

6.1 How to Configure WAF Protection

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

Process of Configuring Policies

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

Table 6-1 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 Protection Rules 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 a CC Attack Protection Rule**
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 6-1** shows how WAF engine built-in protection rules work. **Figure 6-2** shows the detection sequence of rules you configured.

Figure 6-1 WAF engine work process

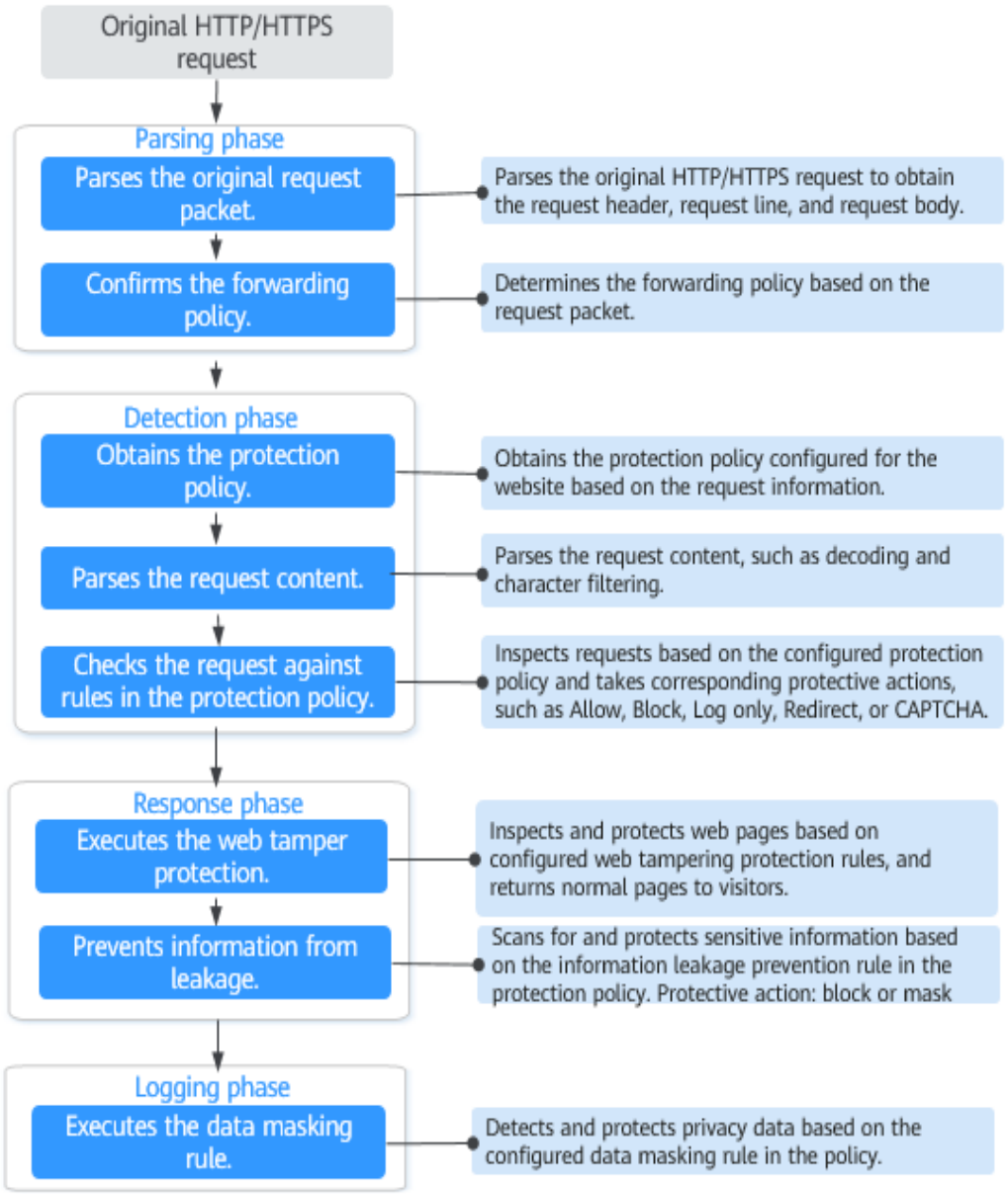
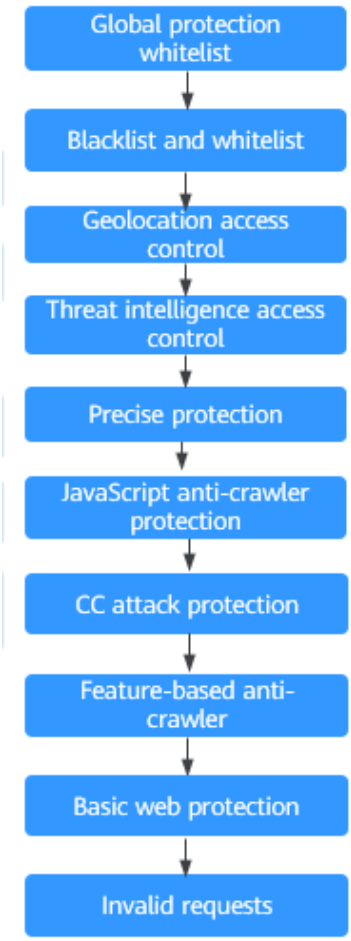


Figure 6-2 Priorities of protection rules



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.

6.2 Configuring Basic Protection Rules 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.

For details about how to configure basic web protection rules, see **Basic Web Protection**.

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**.

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

Constraints

- Basic web protection has two modes: **Block** and **Log only**.
- 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.
- If you select **Block** for **Basic Web Protection**, you can **configure access control criteria for a known attack source**. WAF will block requests matching the configured IP address, cookie, or params for a length of time configured as part of the rule.
- Currently, the deep inspection and header inspection are supported in CN-Hong Kong, CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN South-Guangzhou, CN South-Shenzhen, CN Southwest-Guiyang1, and AP-Bangkok.
- Currently, Shiro decryption check is supported in CN North-Beijing4 and CN-Hong Kong.

Procedure

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 & Compliance**.

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

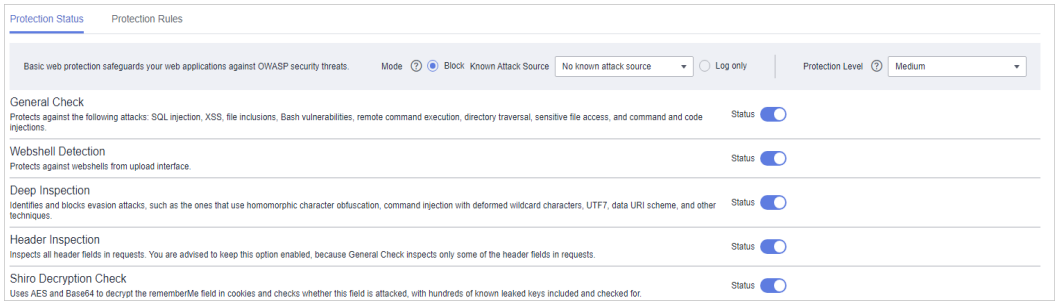
Step 5 Click the name of the target policy to go to the protection configuration page.

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 6-3**.

Figure 6-3 Basic web protection



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 6-2 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.

Protection Level	Description
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 6-3**.

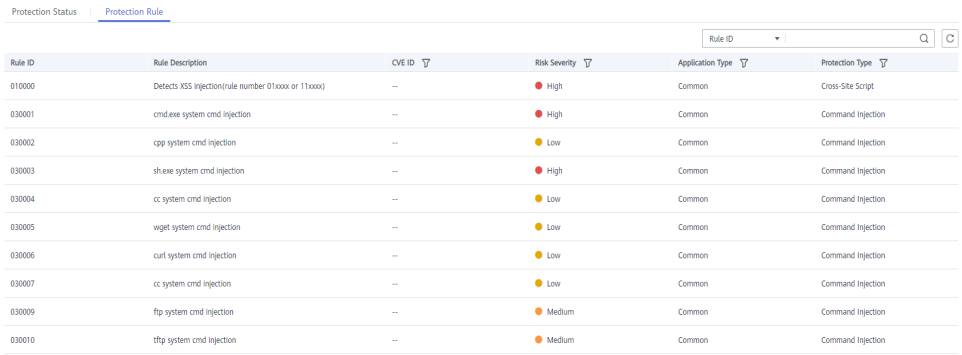
Table 6-3 Protection types

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.

Type	Description
Header Inspection	This function is disabled by default. When it is disabled, General Check will check some of the header fields, such as User-Agent, Content-type, Accept-Language, and Cookie. **NOTE** If you enable this function, WAF checks all header fields in the requests.
Shiro Decryption Check	This function is disabled by default. After this function is enabled, WAF uses AES and Base64 to decrypt the rememberMe field in cookies and checks whether this field is attacked. There are hundreds of known leaked keys included and checked for. **NOTE** If your website uses Shiro 1.2.4 or earlier, or your website uses Shiro 1.2.5 or later but AES is not configured, it is strongly recommended that you enable Shiro decryption detection to prevent attackers from using leaked keys to construct attacks.

Step 8 Click the **Protection Rules** tab to view details. **Figure 6-4** shows an example. For more details about the parameters, see **Table 6-4**.

Figure 6-4 Viewing protection rules



NOTE

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

Table 6-4 Protection rules

Parameter	Description
Rule ID	The protection rule ID, which is generated automatically.
Rule Description	Details of attacks the protection rule is configured for.

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

----End

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, choose **Events**. On the displayed page, view or **download events data**.

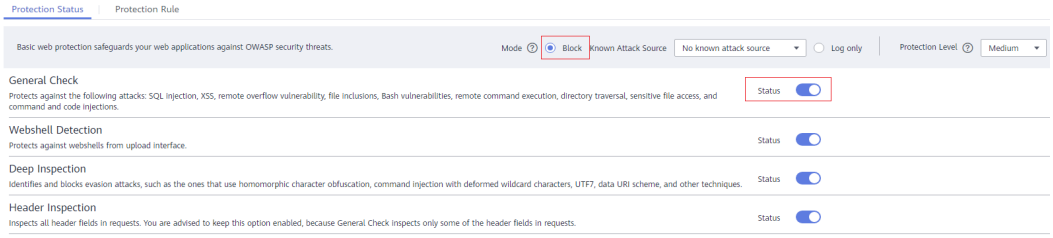
----End

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.

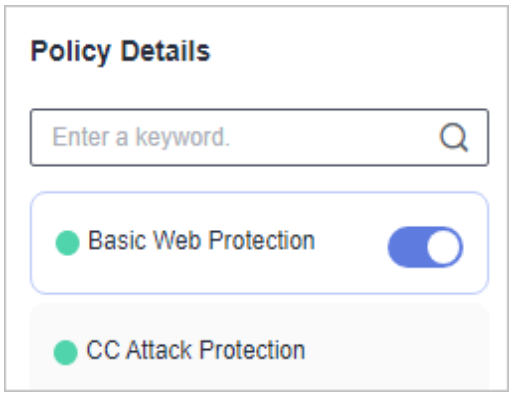
Step 1 Enable **General Check** in **Basic Web Protection** and set the protection mode to **Block**.

Figure 6-5 Enabling General Check



Step 2 Enable WAF basic web protection.

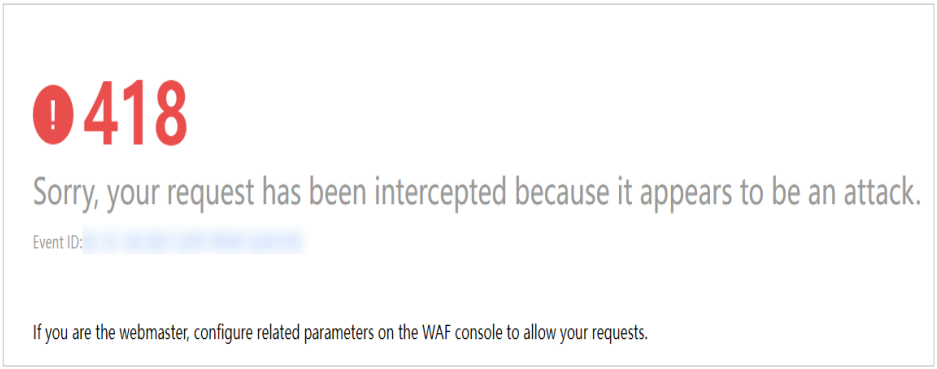
Figure 6-6 Basic Web Protection configuration area



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

WAF blocks the access request. **Figure 6-7** shows an example block page.

Figure 6-7 Block page



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

----End

6.3 Configuring Intelligent Access Control Rules to Accurately Defend Against CC Attacks

If you enable intelligent access control, WAF uses built-in AI-powered models to analyze traffic to your website, identify CC attacks and abnormal features in HTTP

requests on the origin server, and generate specific precise protection and access control rules for your website. In this way, WAF can then automatically protect your website from CC attacks.

NOTICE

The intelligent access control protection is now available for open beta test (OBT). To enable it, **submit a service ticket.**

Prerequisites

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

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

Constraints

- In cloud mode, only the standard, professional, and platinum editions support intelligent access control rules.
- Intelligent access control protection is available in North China regions only.

Procedure

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 & Compliance**.

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 **Intelligent Access Control** configuration area and toggle it on or off if needed.

- : enabled.
- : disabled.

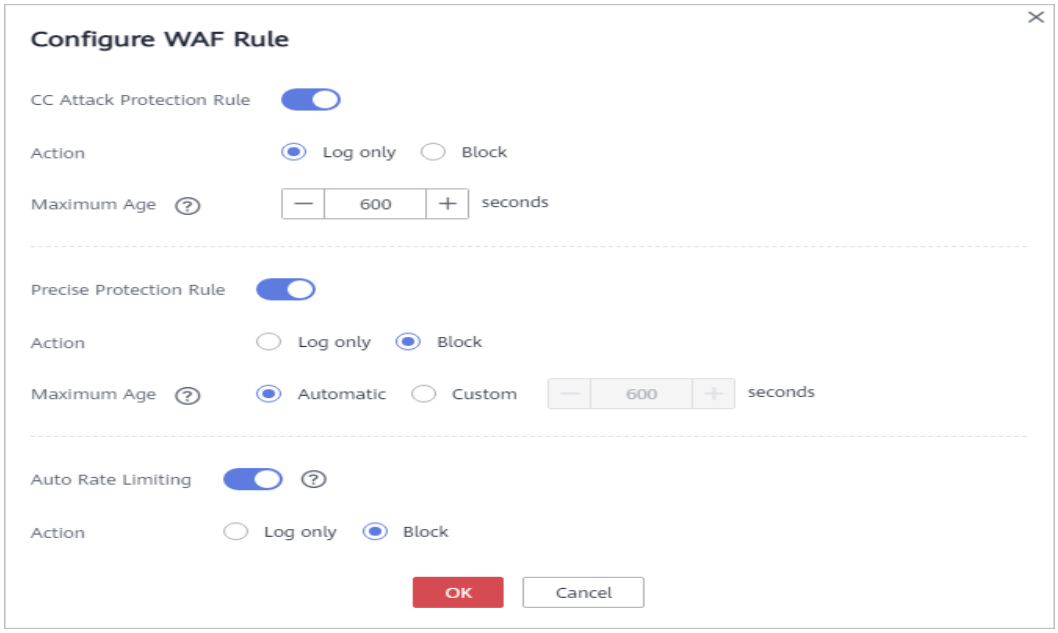
Step 7 Click **Intelligent Threat Access Control**.

CC Attack Protection Rule/**Precise Protection Rule**: Configure **Action** and **Maximum Age** for them after you enable them.

- **Action**: Select **Log only** or **Block**.

- **Maximum Age**: The rule becomes invalid if WAF does not detect any CC attack traffic within the maximum age you configure.

Figure 6-8 Configure WAF Rule



Step 8 Click **OK**.

Click **View WAF Rule** to view the protection policies automatically generated by WAF after it detects CC attacks.

----End

6.4 Configuring a CC Attack Protection Rule

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

- The website to be protected has been added to WAF.
  - For CNAME access in cloud mode, see **Adding a Website to WAF (Cloud Mode-CNAME Access)**.
  - For ELB access in cloud mode, see **Adding a Website to WAF (Cloud Mode - ELB Access)**.
  - For dedicated mode, see **Connecting a Website to WAF (Dedicated Mode)**.
- If you use a dedicated WAF instance, ensure that it has been upgraded to the latest version. For details, see **Managing Dedicated WAF Engines**.

Constraints

- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- 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**.
- Managing reference tables is not included in the standard edition.
- Global request counting for **all WAF instances** can be configured only in cloud WAF editions.
- If you are using a cloud WAF edition and your website uses proxies such as anti-DDoS, Content Delivery Network (CDN), and cloud acceleration services, select **Source** for **Rate Limit Mode** and then **Per user** and enable **All WAF instances**.

NOTE

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

- Cloud mode: This mode supports global request counting for all WAF instances. That means WAF aggregates requests to all WAF nodes for rate limiting. You can just enable this function during configuration.
- Dedicated mode: This mode does not support global counting for all WAF instances. The **Rate Limit** can be set to the maximum access requests allowed for a visit divided by the number of proxies in front of WAF or the number of WAF instances, whichever is smaller.

  Assume that you use three proxy services in front of WAF and use two dedicated WAF instances to protect your website. The smaller value is 2. If you want to limit the requests of a visitor within 1,000 times in a rate limiting period, you can set **Rate Limit** to 500, which is 1,000 divided by 2.

Procedure

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 & Compliance**.

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 6-5**.

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

Figure 6-9 Adding a CC attack protection rule

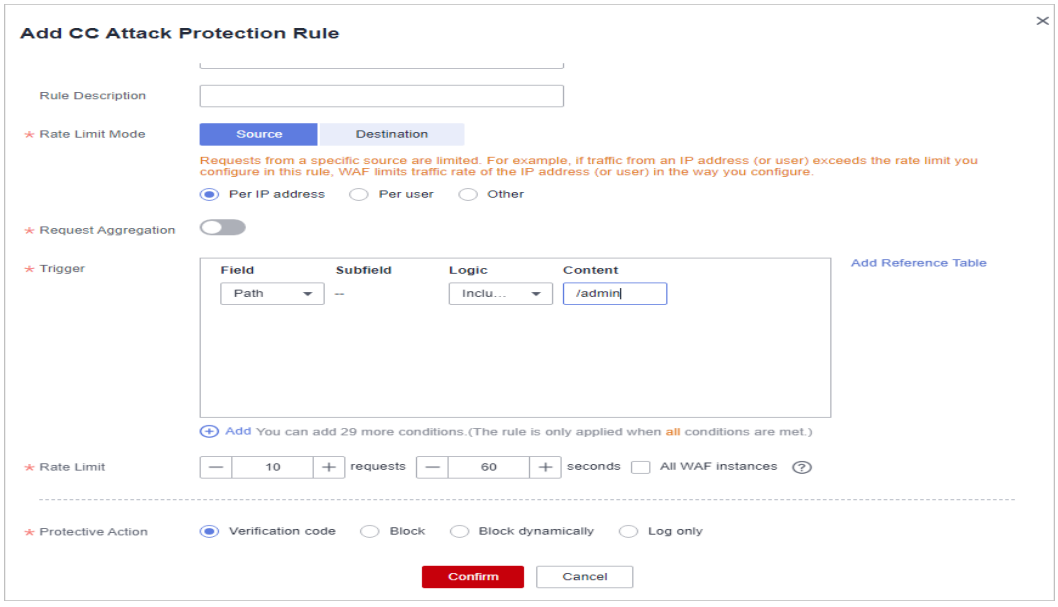


Table 6-5 Rule parameters

Parameter	Description	Example Value
Rule Name	Name of the rule	waftest

Parameter	Description	Example Value
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** to 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 if all of the conditions are met. • **Field** • **Subfield**: Configure this field only when **IPv4**, **IPv6**, **Cookie**, **Header**, or **Params** 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. **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**

Parameter	Description	Example Value
Rate Limit	The number of requests allowed from a website visitor in the rate limit period. If the number of requests exceeds the rate limit, WAF takes the action you configure for **Protective Action**. **All WAF instances**: Requests to on one or more WAF instances will be counted together according to the rate limit mode you select. By default, requests to each WAF instance are counted. If you enable this, WAF will count requests to all your WAF instances for triggering this rule. To enable user-based rate limiting, **Per user** or **Other** (**Referer** must be configured) instead of **Per IP address** must be selected for **Rate Limit Mode**. This is because IP address-based rate limiting cannot limit the access rate of a specific user. However, in user-based rate limiting, requests may be forwarded to one or more WAF instances. Therefore, **All WAF instances** must be enabled for triggering the rule precisely. **NOTE** If a website has used other proxy services, such as CDN and advanced anti-DDoS in front of WAF, the access requests to WAF will be distributed to each WAF instance for traffic forwarding. By default, WAF counts requests on each WAF instance separately. To set a proper rate limit frequency, follow the following principles: • Cloud mode: This mode supports global request counting for all WAF instances. That means WAF aggregates requests to all WAF nodes for rate limiting. You can just enable this function during configuration. • Dedicated mode: This mode does not support global counting for all WAF instances. The **Rate Limit** can be set to the maximum access requests allowed for a visit divided by the number of proxies in front of WAF or the number of WAF instances, whichever is smaller. Assume that you use three proxy services in front of WAF and use two dedicated WAF instances to protect your website. The smaller value is 2. If you want to limit the requests of a visitor within 1,000 times in a rate limiting period, you can set **Rate Limit** to 500, which is 1,000 divided by 2.	**10** requests allowed in **60** seconds

Parameter	Description	Example Value
Protective Action	The action that WAF will take if the number of requests exceeds **Rate Limit** you configured. The options are as follows: • **Verification code**: WAF allows requests that trigger the rule as long as your website visitors complete the required verification. • **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. You can **download events data** and view the protection logs of the domain name.	Block
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

Parameter	Description	Example Value
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

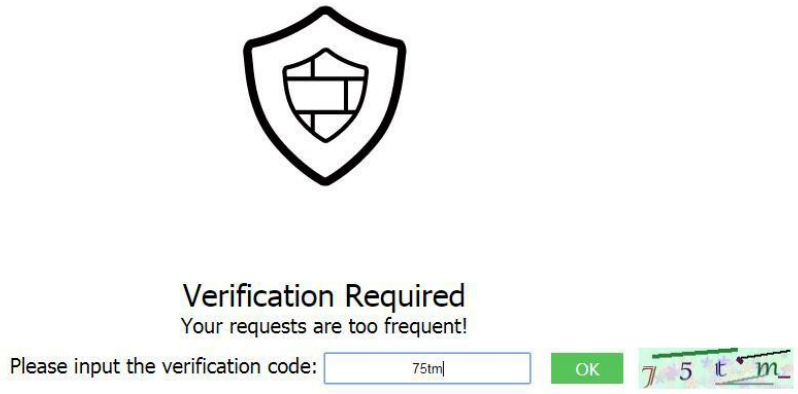
If you have configured a CC attack protection rule like **Figure 6-9** (with **Protective Action** set to **Block**) for your domain name **www.example.com**, take the following steps to verify the protection effect:

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.



Step 3 Return to the WAF console. In the navigation pane, choose **Events**. On the displayed page, view or **download events data**.

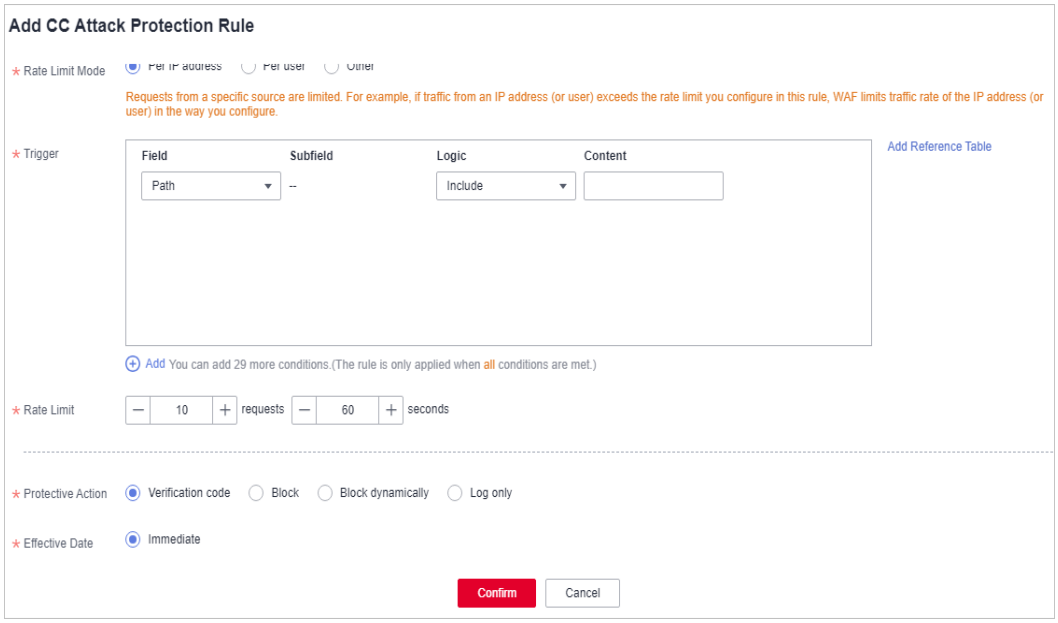
----End

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.

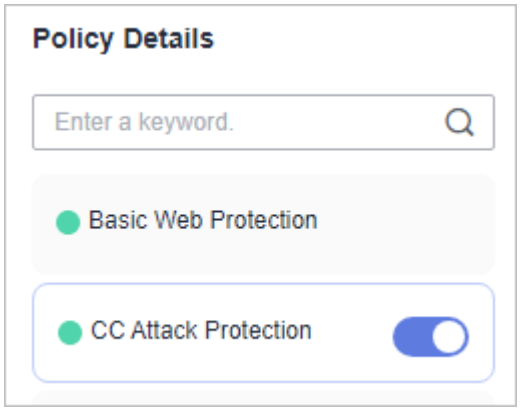
Step 1 Add a CC attack protection rule with **Protection Action** set to **Verification code**.

Figure 6-10 Verification code



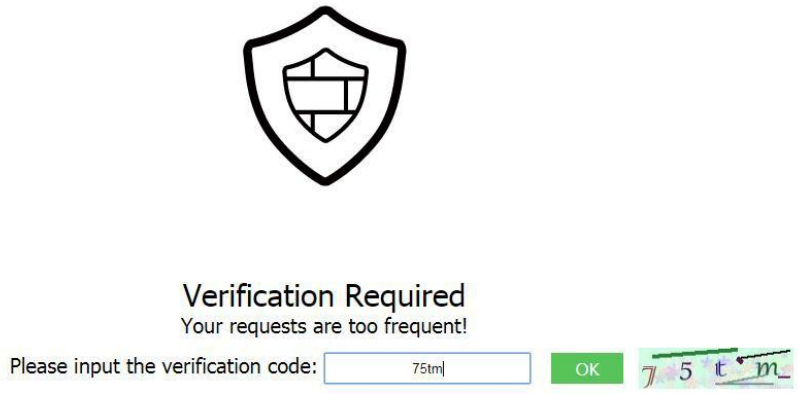
Step 2 Enable CC attack protection.

Figure 6-11 Enabling CC Attack Protection



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

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



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

----End

6.5 Configuring Custom Precise Protection Rules

You can combine common HTTP fields, such as **IP**, **Path**, **Referer**, **User Agent**, and **Params** in a protection rule to let WAF allow, block, or only log the requests that match the combined conditions. In addition, **JavaScript challenge** verification is supported. WAF returns a piece of JavaScript code that can be automatically executed by a normal browser to the client. If the client properly executes JavaScript code, WAF allows all requests from the client within a period of time (30 minutes by default). During this period, no verification is required. If the client fails to execute the code, WAF blocks the requests.

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

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**.

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

Constraints

- **Full Detection** is not included in the WAF standard edition or cloud WAF billed on a pay-per-use basis.
- The reference table function is not included in the WAF standard edition or cloud WAF billed on a pay-per-use basis.
- 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.
- 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: (' "<>&*#% \?)

Application Scenarios

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

Procedure

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 & Compliance**.

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.

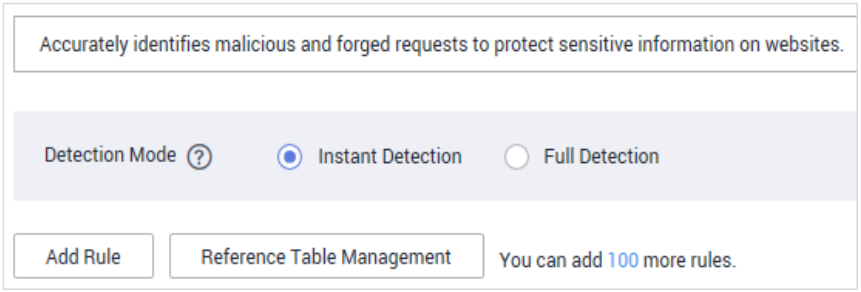
-  : enabled.
-  : disabled.

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.

Figure 6-12 Setting Detection Mode



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 6-6**.

The settings shown in **Figure 6-13** 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 6-13 Add Precise Protection Rule

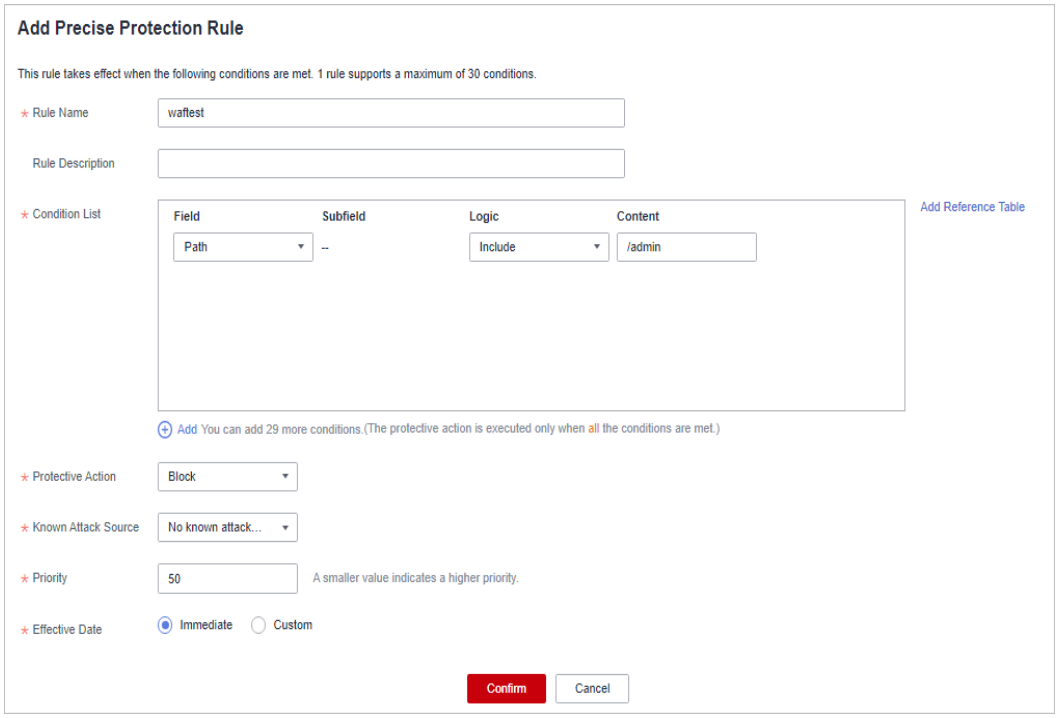


Table 6-6 Rule parameters

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

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 **IPv4**, **IPv6**, **Params**, **Cookie**, **Known feature crawler**, 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. **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*.	• **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
	• **Content**: Enter or select the content of condition matching. **NOTE** For more details about the configurations in general, see **Table 6-17**.	
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. For details, see **Modifying the Alarm 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 the there are requests that are blocked mistakenly. • **JS Challenge**: WAF returns a piece of JavaScript code that can be automatically executed by a normal browser to the client. If the client properly executes the JavaScript code, WAF allows all requests from the client within a period of time (30 minutes by default). During this period, no verification is required. If the client fails to execute the code, WAF blocks the requests.	**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**

Parameter	Description	Example Value
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**
Effective Date	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

If you have configured a precise protection rule as shown in **Figure 6-13** for your domain name, to verify WAF is protecting your website (**www.example.com**) against the 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 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, click **Events**. On the displayed page, view or **download events data**.

----End

Configuration Example - Blocking a Certain Type of Attack Requests

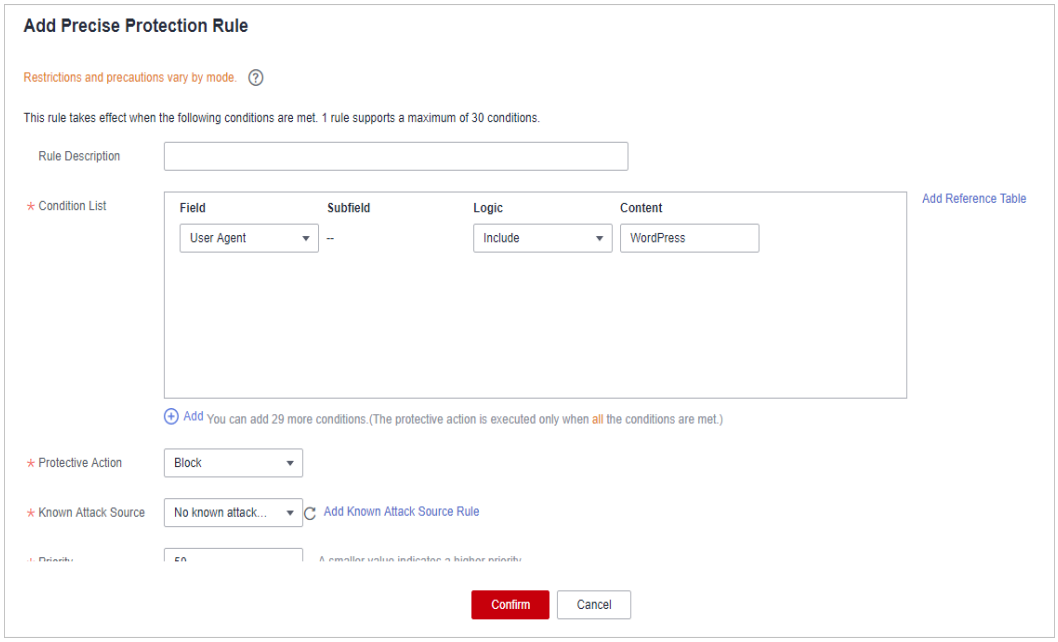
Analysis of a specific type of WordPress pingback attack shows that the **User Agent** field contains WordPress.

Figure 6-14 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.

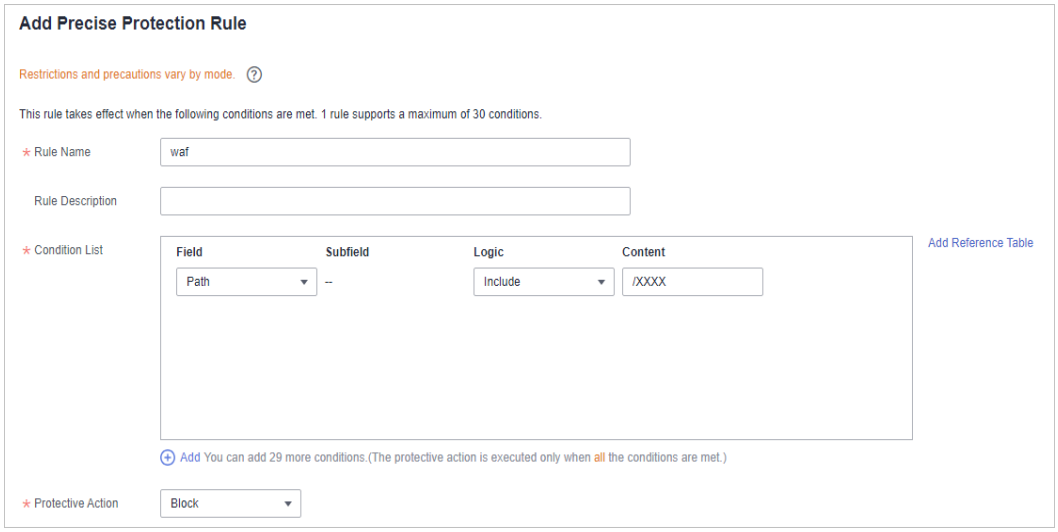
Figure 6-15 User Agent configuration



Configuration Example - Blocking Attack 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.

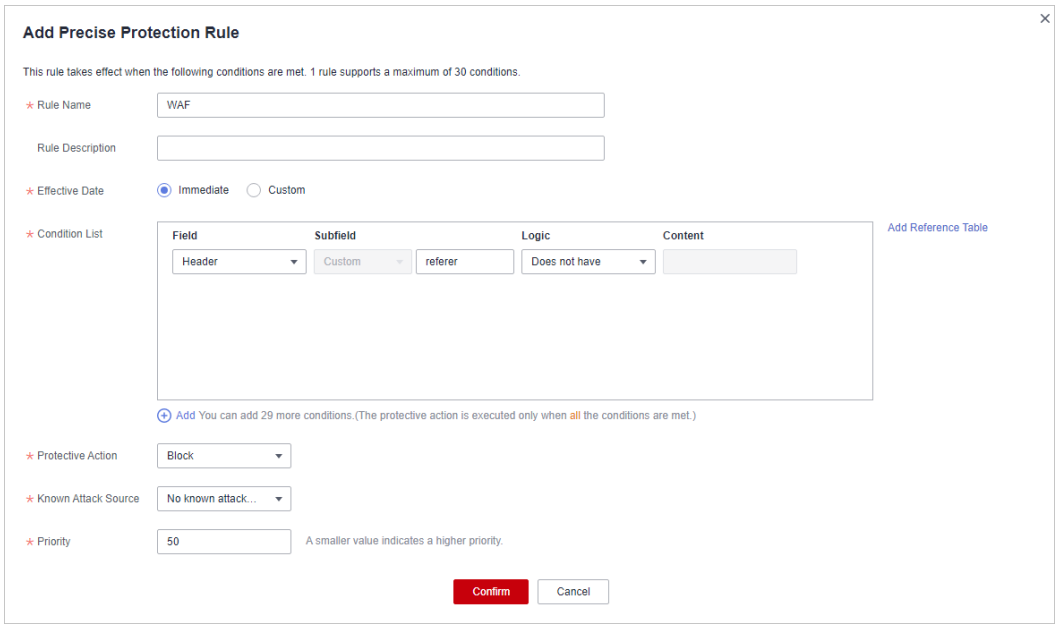
Figure 6-16 Blocking requests to a specific URL



Configuration Example - Blocking Requests with null Fields

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

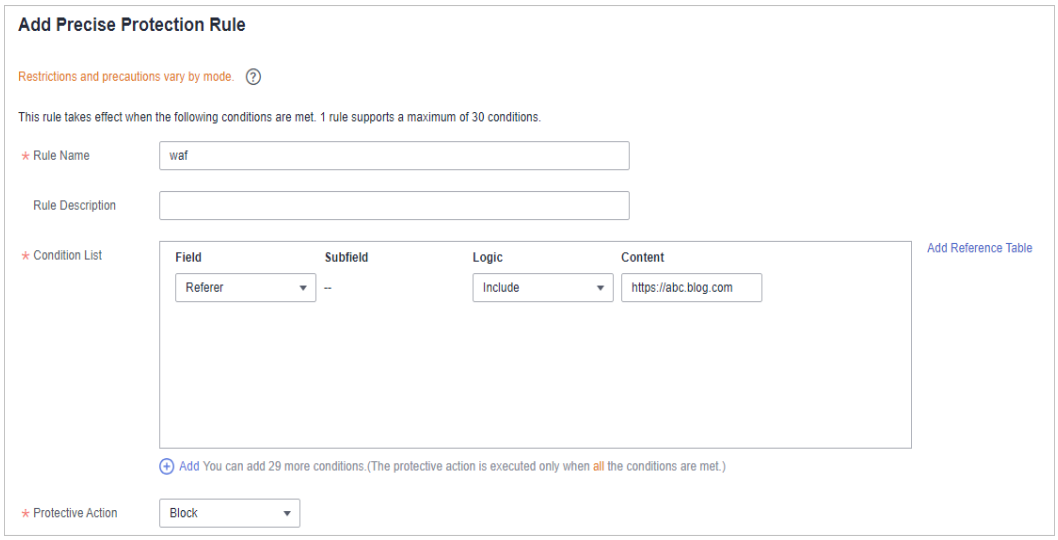
Figure 6-17 Blocking requests with empty Referer



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 6-18** to block access requests of .zip files.

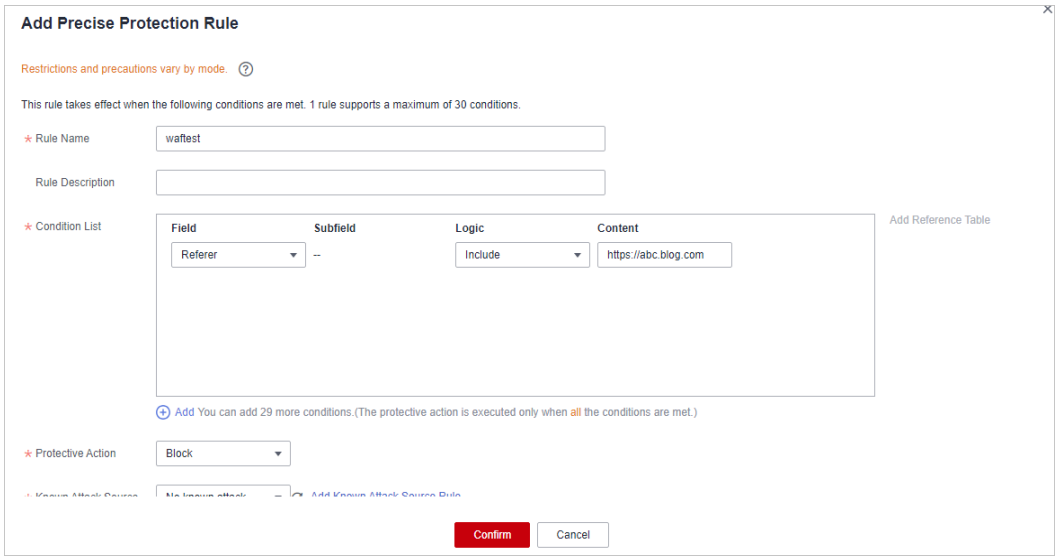
Figure 6-18 Blocking requests of specific file types



Configuration Example - Preventing Hotlinking

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

Figure 6-19 Preventing hotlinking



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

You can configure two precise protection rules, one to block all requests, as shown in **Figure 6-20**, but then another one to allow the access from a specific IP address, as shown in **Figure 6-21**.

Figure 6-20 Blocking all requests

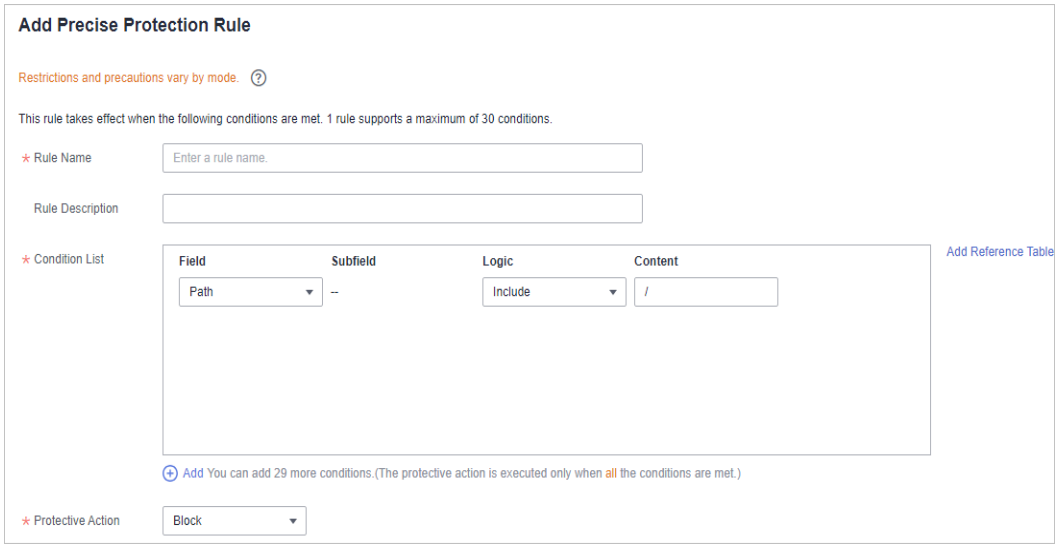
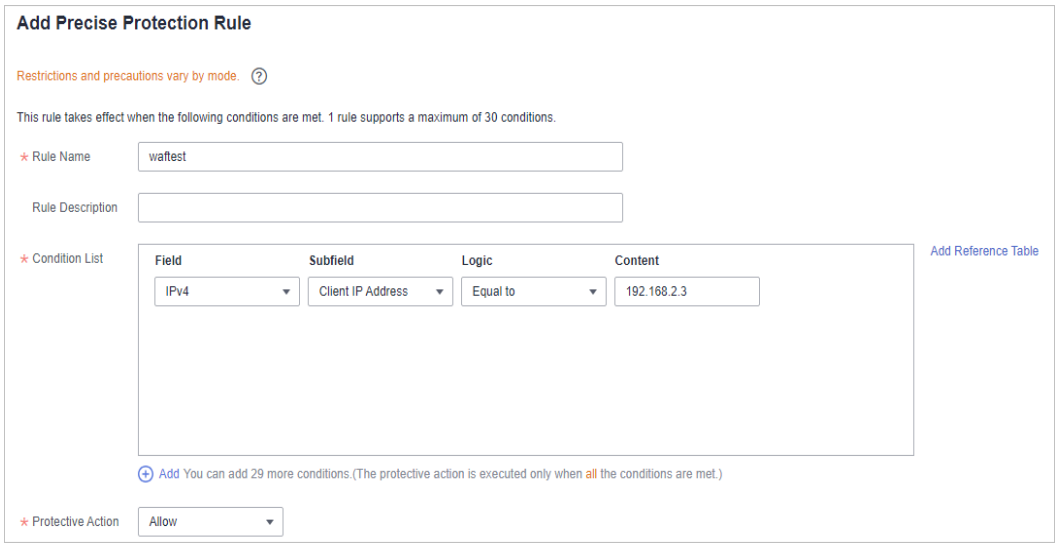


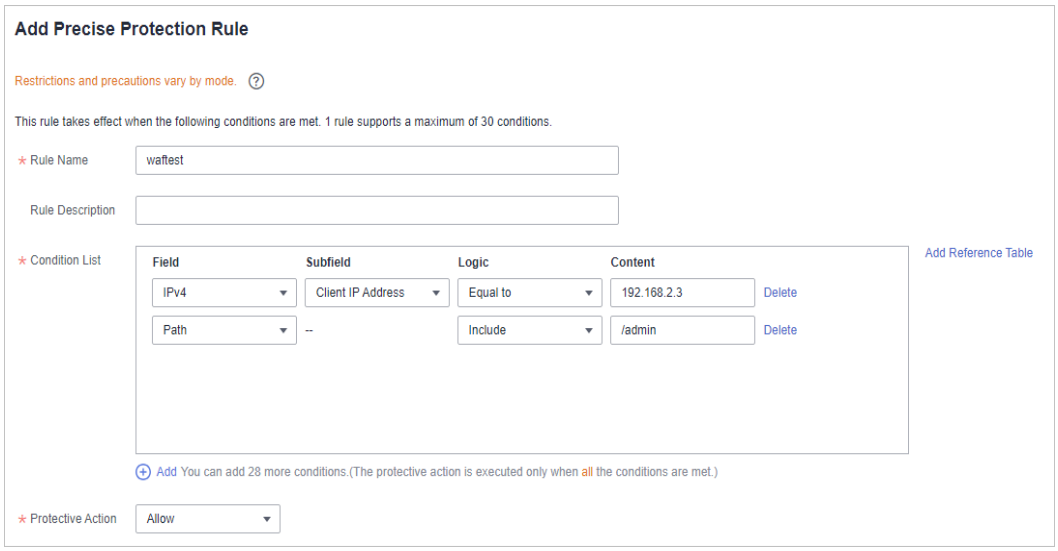
Figure 6-21 Allowing the access of a specified IP address



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

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

Figure 6-22 Allowing specific IP addresses to access specified URLs



6.6 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. 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

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

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

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**.
- For dedicated and ELB-accessed cloud WAF instances, if the load balancers they use support IPv6 addresses, those WAF instances also support IPv6 addresses or IPv6 address ranges.

- 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.
- 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.

  NOTICE

  If you want to allow only specified IP addresses to access the protected website, see **How Do I Allow Only Specified IP Addresses to Access the Protected Website?**

- If you set **Protective Action** of a blacklist or whitelist rule to **Block**, you can **configure known attack source rules to block the attack source IP address for a specified period of time**. WAF will block requests matching the configured IP address, Cookie, or Params for a block duration you specify.

Specification Limitations

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

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

Impact on the System

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

Procedure

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 & Compliance**.

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 6-7**. **Figure 6-23** and **Figure 6-24** 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 6-23 Adding an IP address/Range to a blacklist or whitelist rule

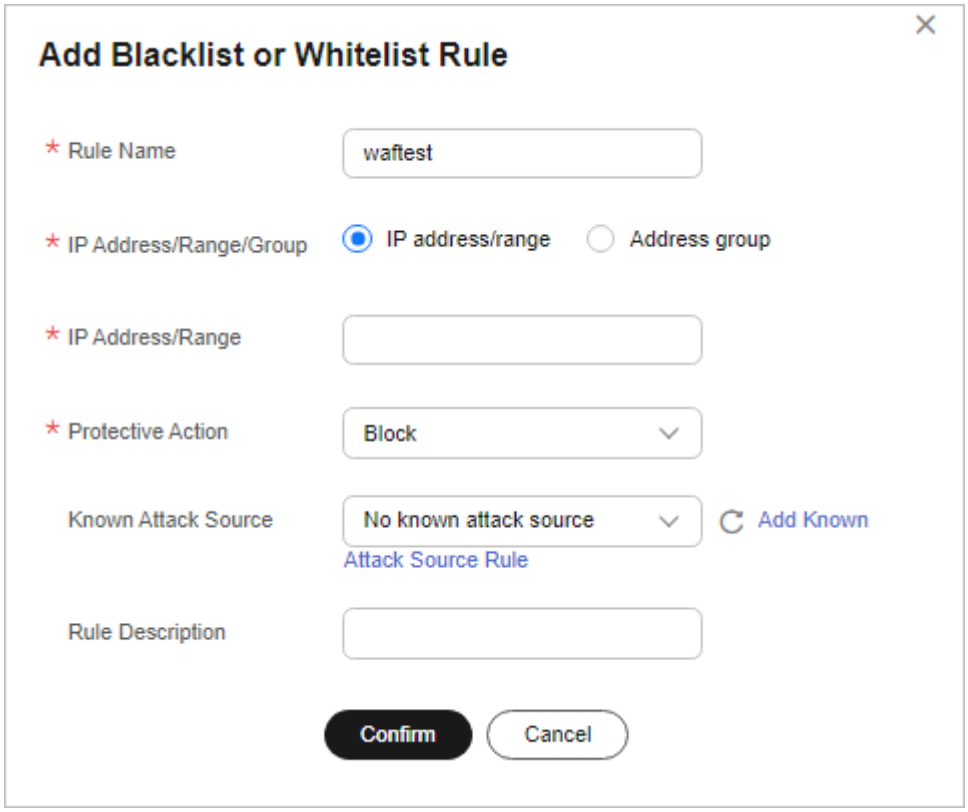


Figure 6-24 Batching adding IP addresses/Ranges to a blacklist or whitelist rule

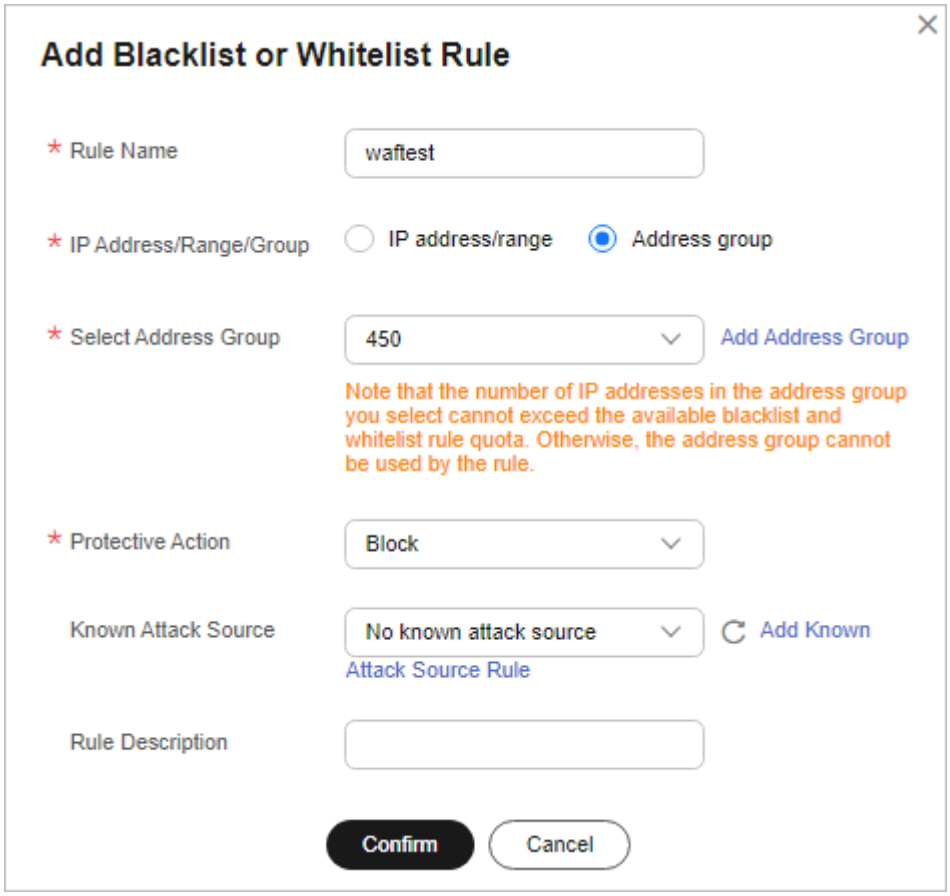


Table 6-7 Rule parameters

Parameter	Description	Example Value
Rule Name	Rule name you entered.	waftest
IP Address/ Range/Group	You can select **IP address/ Range** or **Address Group** to add IP addresses a blacklist or whitelist rule.	IP Address/Range

Parameter	Description	Example Value
IP Address/ Range	This parameter is mandatory if you select **IP address/range** for **IP Address/Range/Group**. IP addresses or IP address ranges are supported. • IP address: IP address to be added to the blacklist or whitelist • IP address range: IP address and subnet mask defining a network segment **NOTICE** Only the professional and platinum editions support IPv6 protection.	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 IP address, Cookie, or Params for a length of time configured as part of the rule.	Long-term IP address 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

If you have added domain name **www.example.com** to this rule, to verify WAF is protecting the corresponding website:

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 **Procedure**.

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, choose **Events**. On the displayed page, view or **download events data**.

----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 the following two blacklist and whitelist rules to block all IP addresses:

Figure 6-25 Blocking IP address range 1.0.0.0/1

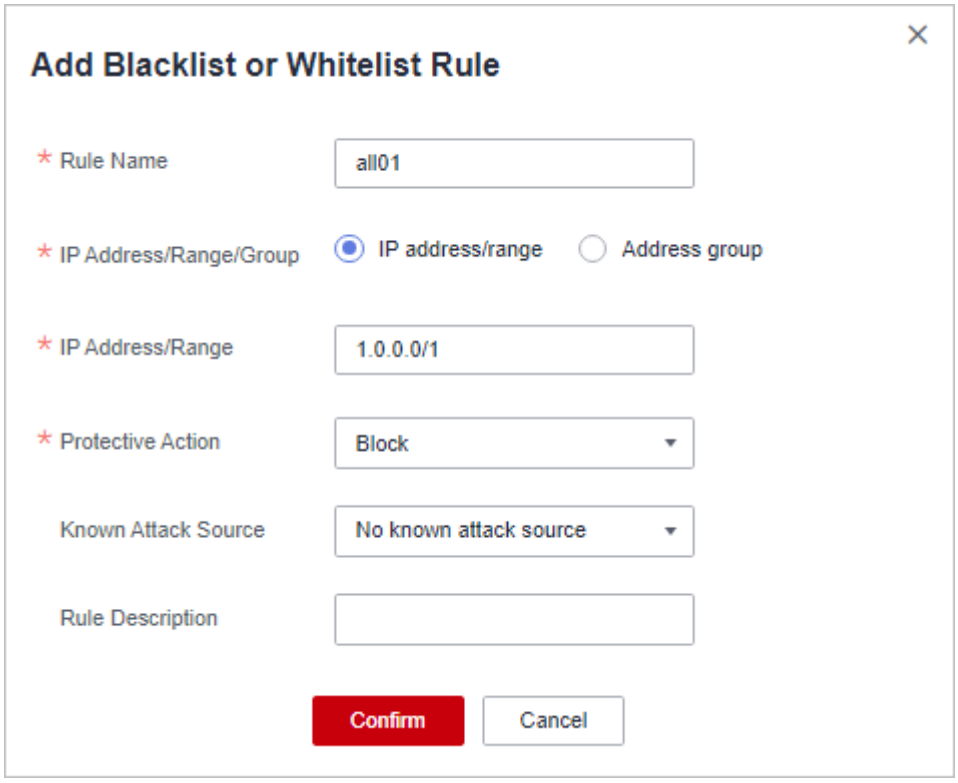
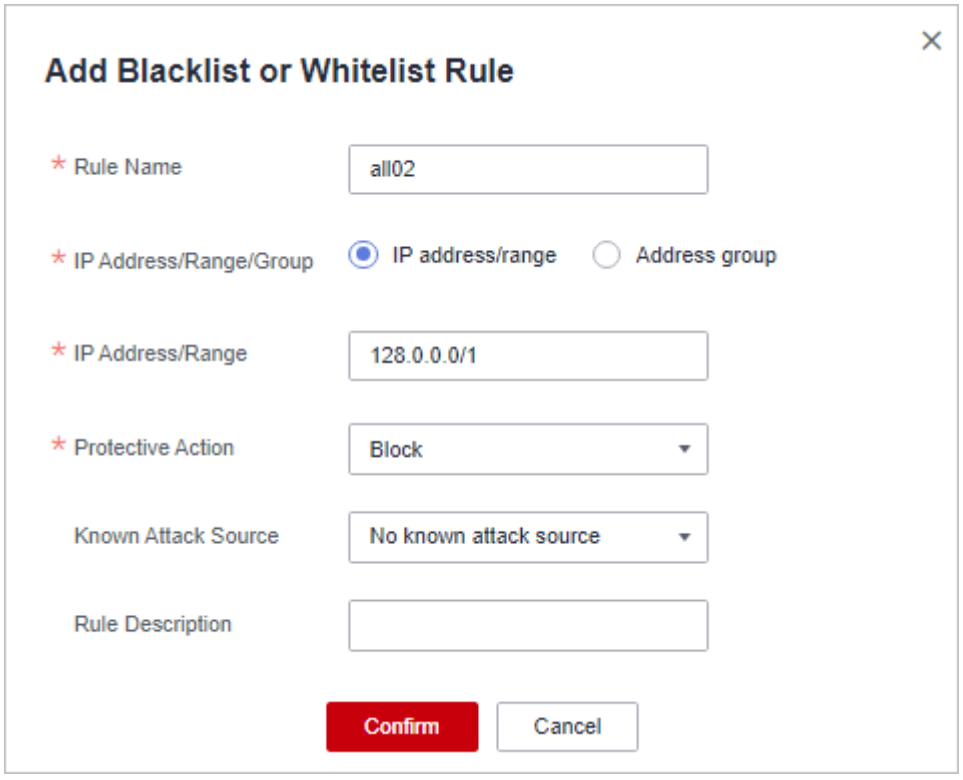
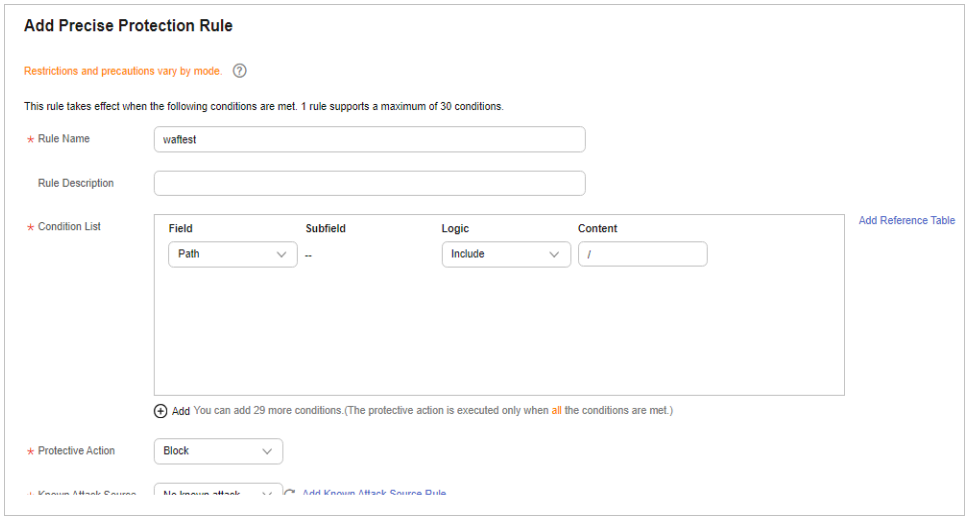


Figure 6-26 Blocking IP address range 128.0.0.0/1



You can also add a precise protection rule to block all access requests, as shown in **Figure 6-27**.

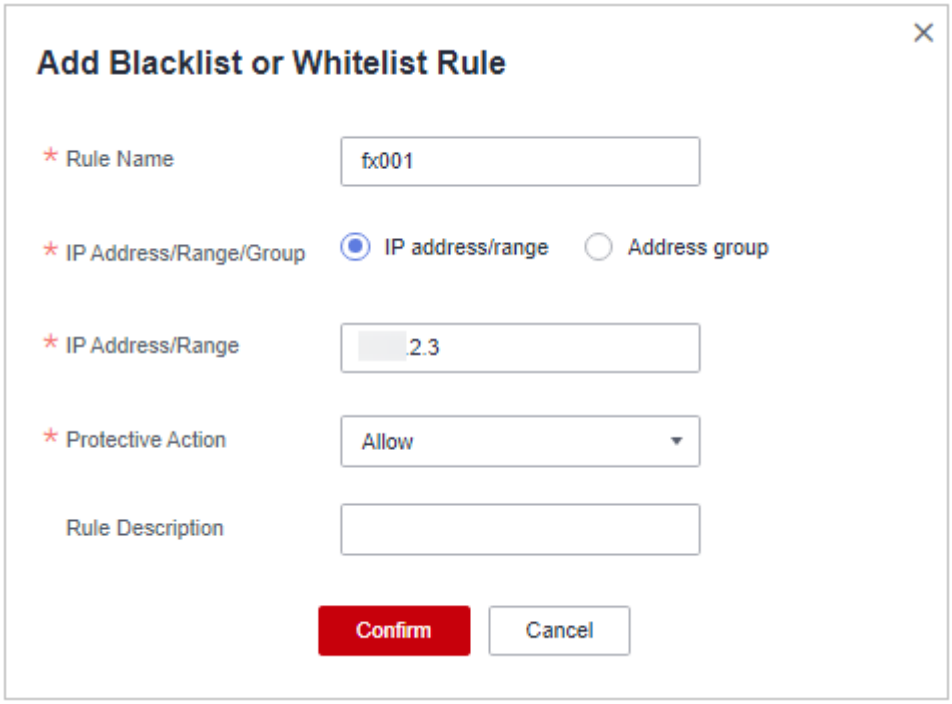
Figure 6-27 Blocking all access requests



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

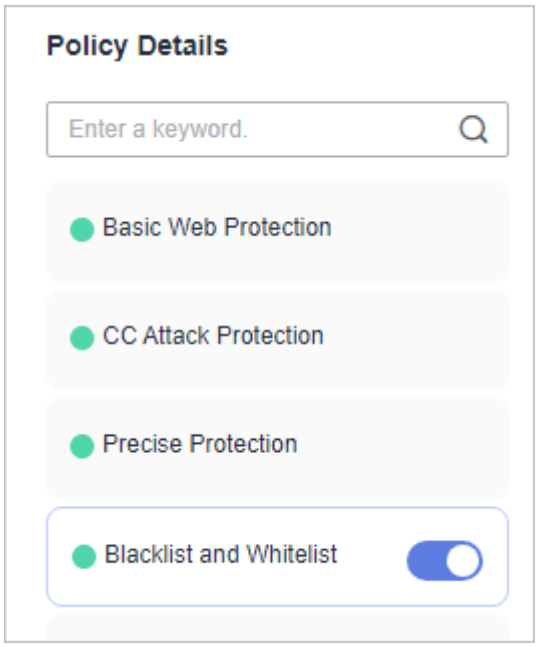
Step 2 Refer to **Figure 6-28** and add a whitelist rule to allow a specified IP address, for example, *XXX.XXX.2.3*.

Figure 6-28 Allowing the access of a specified IP address



Step 3 Enable the white and blacklist protection.

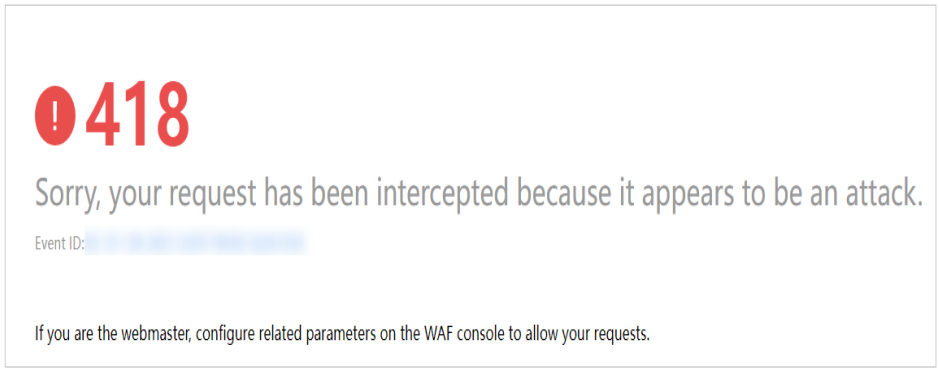
Figure 6-29 Blacklist and Whitelist configuration area



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 6-30** shows an example of the block page.

Figure 6-30 Block page



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

----End

6.7 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

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

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

Constraints

- This function is not supported in the standard edition.
- 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.

Procedure

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 & Compliance**.

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 6-8**.

Figure 6-31 Adding a geolocation access control rule

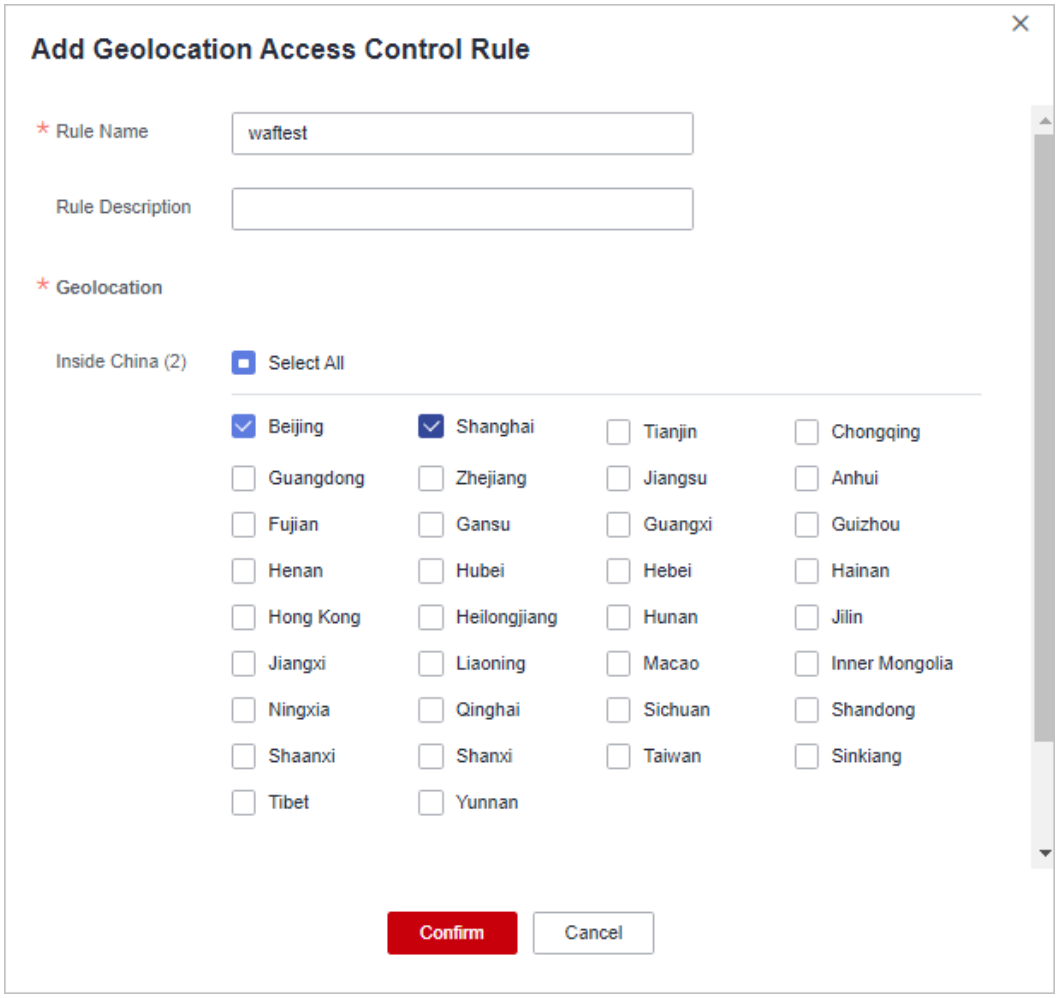


Table 6-8 Rule parameters

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. You can select a region inside China or outside China.	-
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.

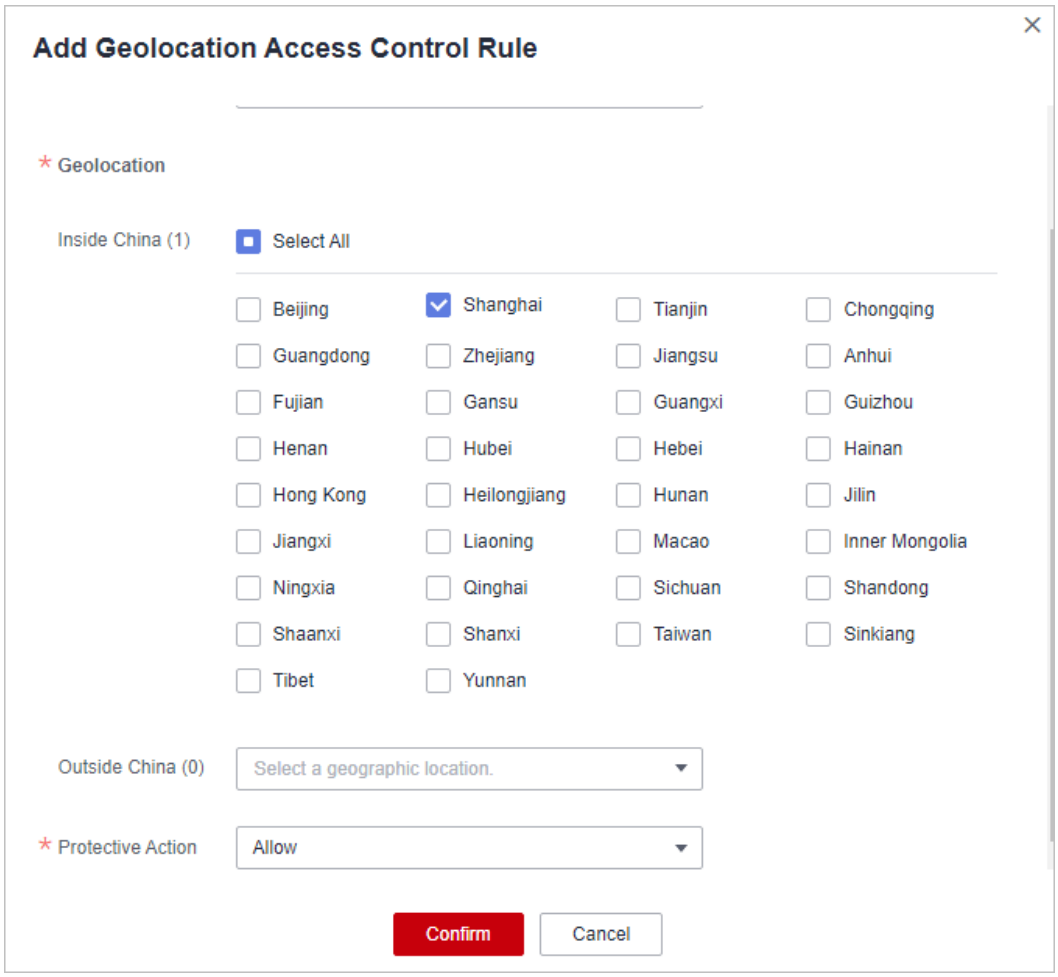
----End

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 **Shanghai, China** to access the domain name. Perform the following steps:

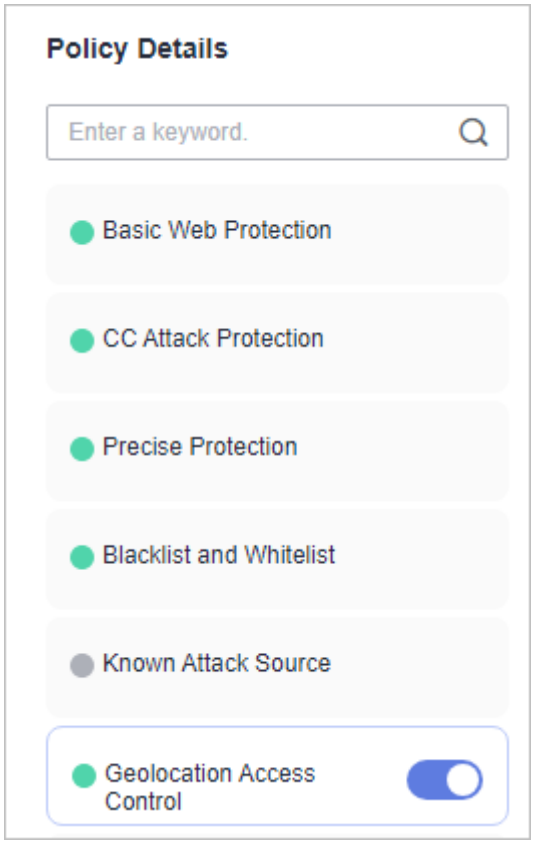
Step 1 Add a geolocation access control rule: Select **Shanghai** for **Geolocation** and select **Allow** for **Protective Action**.

Figure 6-32 Selecting Allow for Protective Action



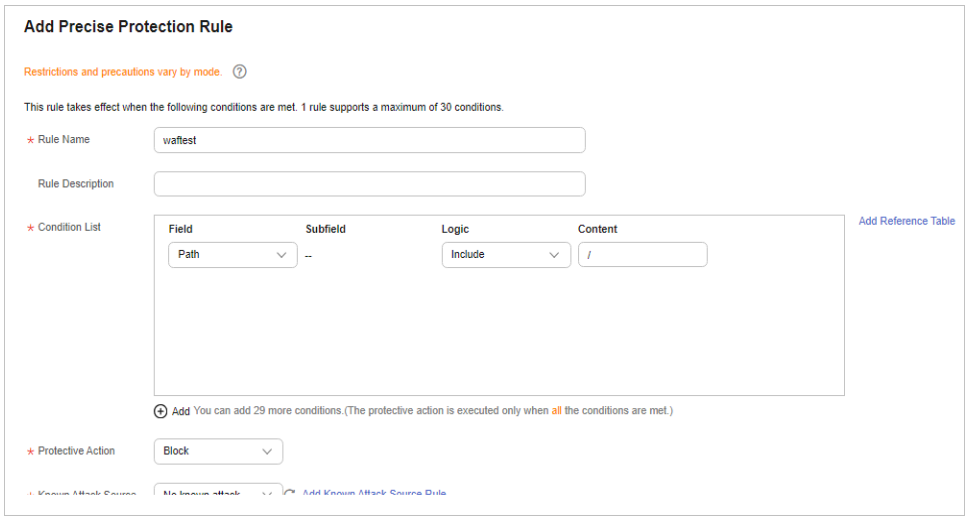
Step 2 Enable geolocation access control.

Figure 6-33 Geolocation Access Control configuration area



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

Figure 6-34 Blocking all access requests

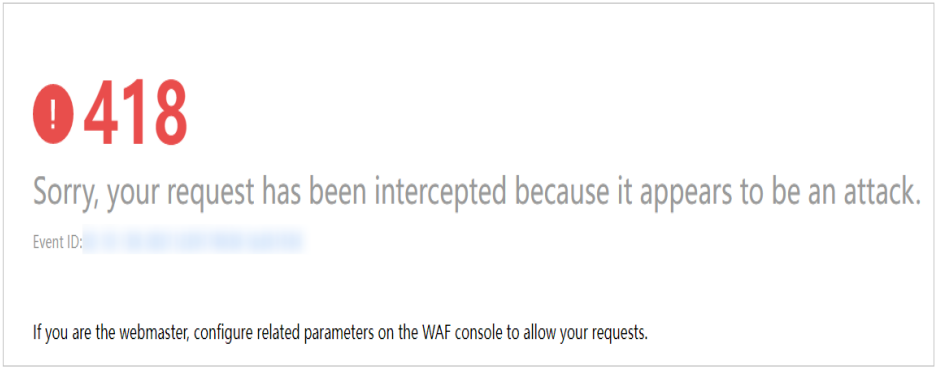


For details, see **Configuring Custom Precise Protection Rules**.

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

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

Figure 6-35 Block page



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

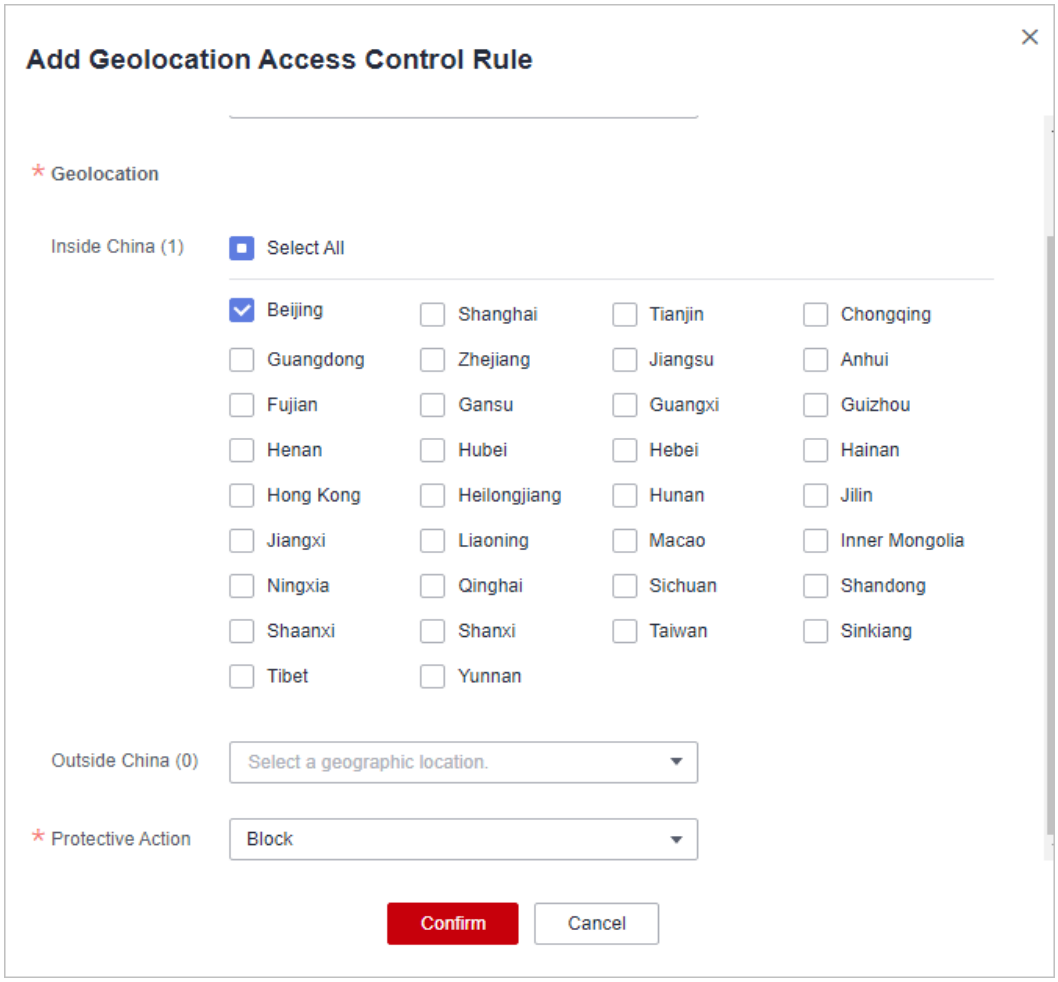
----End

Configuration Example - Blocking 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 **Beijing** to access the domain name. The following shows how to configure a rule to this end:

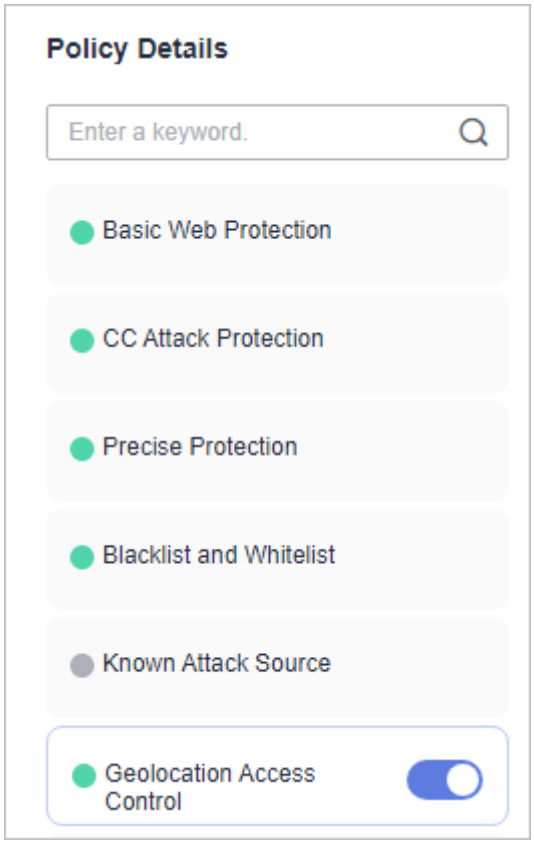
Step 1 Add a geolocation access control rule, select **Beijing** for **Geolocation** and **Block** for **Protective Action**.

Figure 6-36 Blocking access requests from a specific region



Step 2 Enable geolocation access control.

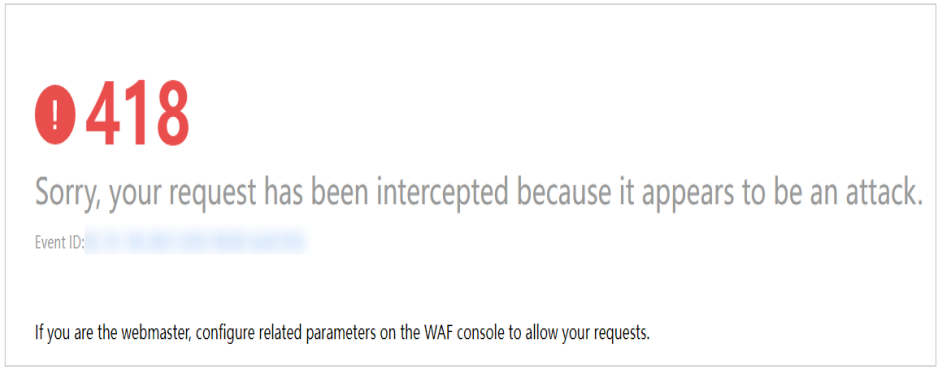
Figure 6-37 Geolocation Access Control configuration area



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

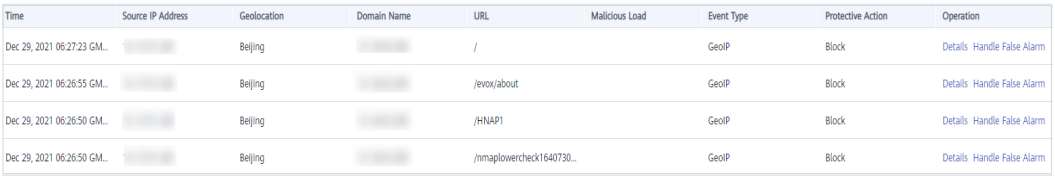
When an access request from IP addresses inside **Beijing** accesses the page, WAF blocks the access request.

Figure 6-38 Block page



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

Figure 6-39 Viewing events - blocking access requests from IP addresses in a region



----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 **Procedure**.

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

Step 4 Go to the WAF console. In the navigation pane on the left, choose **Events**. On the displayed page, view or **download events data**.

----End

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

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

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.
- WAF can cache user-defined header fields. In the upper part of the page, click **Modify Field** to configure the header fields you want WAF to cache.

Prerequisites

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

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

Constraints

- The ELB-access cloud WAF does not support this type of protection rule.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- Ensure that the origin server response contains the **Content-Type** response header, or WAF may fail to cache the origin server response.

Application Scenarios

- Quicker response to requests

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

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

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

Procedure

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 & Compliance**.

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 6-9**.

Figure 6-40 Adding a web tamper protection rule

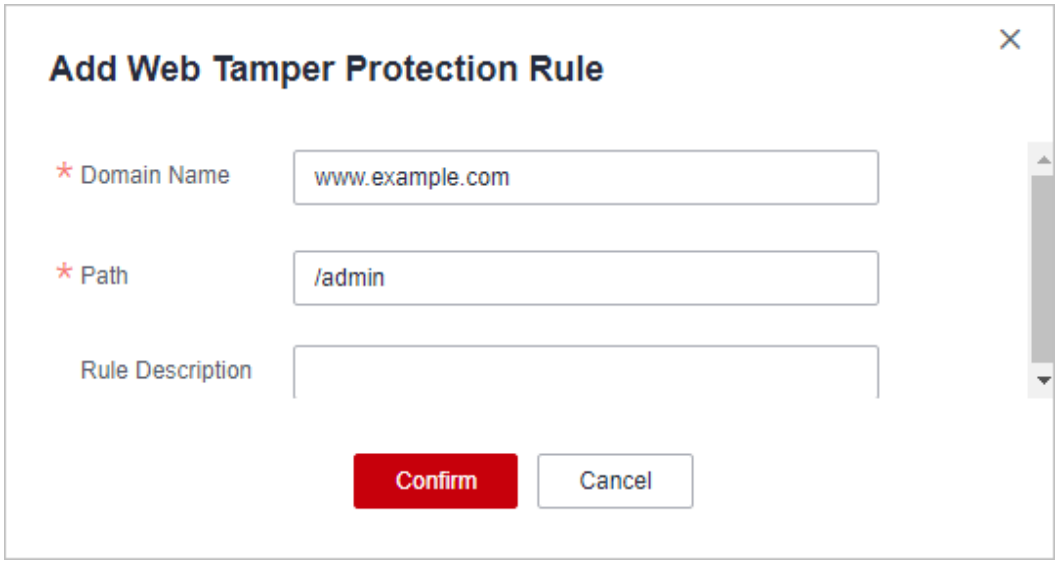


Table 6-9 Rule parameters

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

Other 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.

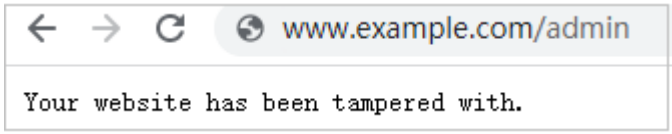
Configuration Example - Static Web Page Tamper Prevention

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

Step 1 Use a browser to access **http://www.example.com/admin**.

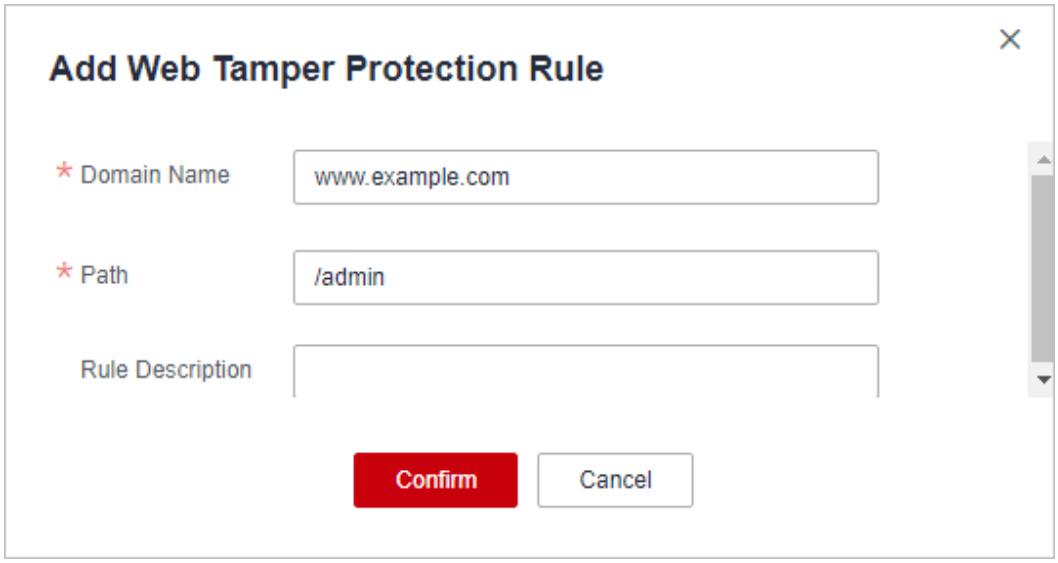
A tampered page is returned.

Figure 6-41 A static page that has been tampered with



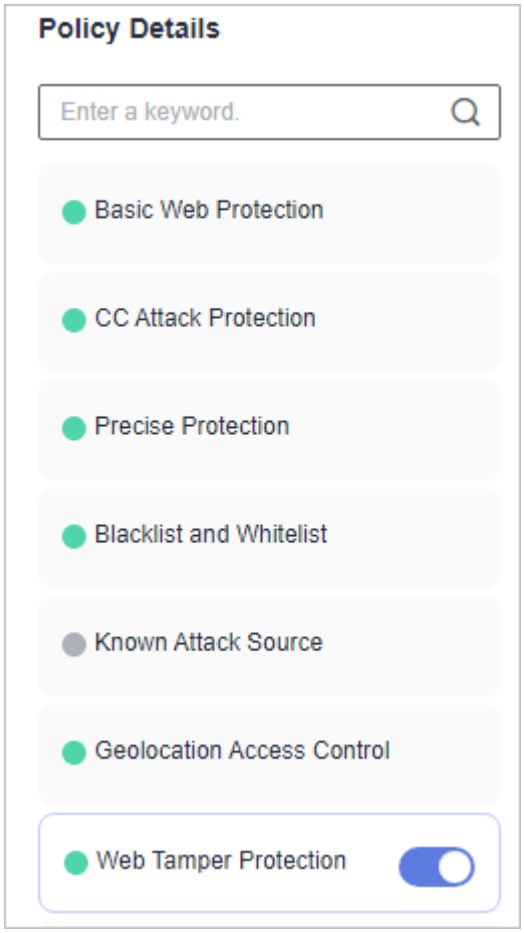
Step 2 Add a web tamper prevention rule to WAF.

Figure 6-42 Adding a web tamper protection rule



Step 3 Enable WTP.

Figure 6-43 Web Tamper Protection configuration area



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

6.9 Configuring Anti-Crawler Rules

You can configure website anti-crawler protection rules to protect against search engines, scanners, script tools, and other crawlers, and use JavaScript to create custom anti-crawler protection rules.

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**.

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

Constraints

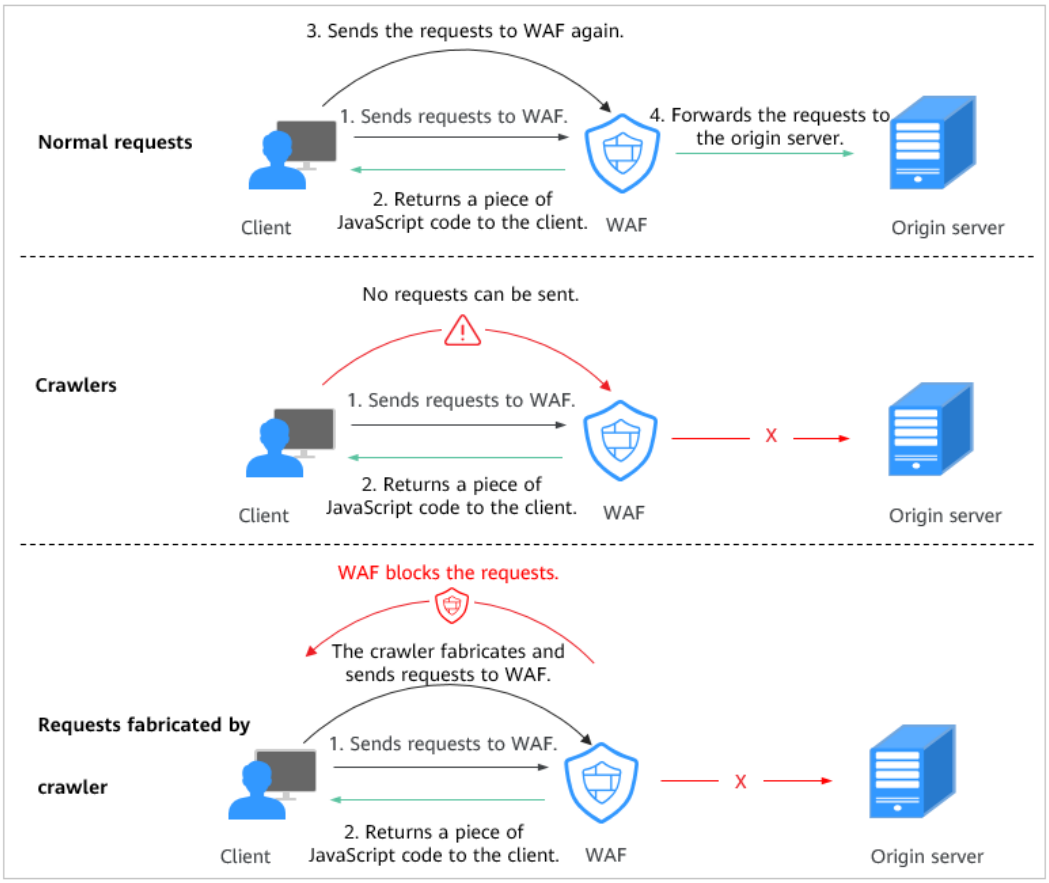
- Cookies must be enabled and JavaScript supported by any browser used to access a website protected by anti-crawler protection rules.
- If your service is connected to CDN, exercise caution when using the JS anti-crawler function.

  CDN caching may impact JS anti-crawler performance and page accessibility.
- The JavaScript anti-crawler function is unavailable for pay-per-use WAF instances.
- This function is not supported in the standard edition.
- JS anti-crawler protection is not supported in **ELB access** in **Cloud Mode** WAF.
- If JavaScript anti-crawler event logs cannot be viewed, see **Why Are There No Protection Logs for Some Requests Blocked by WAF JavaScript Anti-Crawler Rules?**
- The protective action for website anti-crawler JavaScript challenge is **Log only**, and that for JavaScript authentication is **Verification code**. If a visitor fails the JavaScript authentication, a verification code is required for access. Requests will be forwarded as long as the visitor enters a valid verification code.
- WAF JavaScript-based anti-crawler rules only check GET requests and do not check POST requests.

How JavaScript Anti-Crawler Protection Works

Figure 6-44 shows how JavaScript anti-crawler detection works, which includes JavaScript challenges (step 1 and step 2) and JavaScript authentication (step 3).

Figure 6-44 JavaScript Anti-Crawler protection process

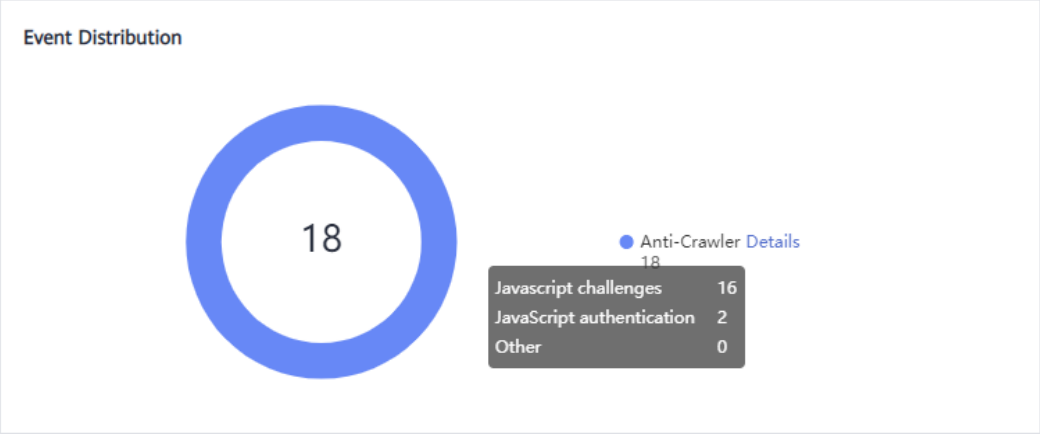


If JavaScript anti-crawler is enabled when a client sends a request, WAF returns a piece of JavaScript code to the client.

- If the client sends a normal request to the website, triggered by the received JavaScript code, the client will automatically send the request to WAF again. WAF then forwards the request to the origin server. This process is called JavaScript verification.
- If the client is a crawler, it cannot be triggered by the received JavaScript code and will not send a request to WAF again. The client fails JavaScript authentication.
- If a client crawler fabricates a WAF authentication request and sends the request to WAF, the WAF will block the request. The client fails JavaScript authentication.

By collecting statistics on the number of JavaScript challenges and authentication responses, the system calculates how many requests the JavaScript anti-crawler defends. In **Figure 6-45**, 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 6-45 Parameters of a JavaScript anti-crawler protection rule



NOTICE

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

Procedure

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 & Compliance**.

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 6-10**.

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 6-46 Feature Library

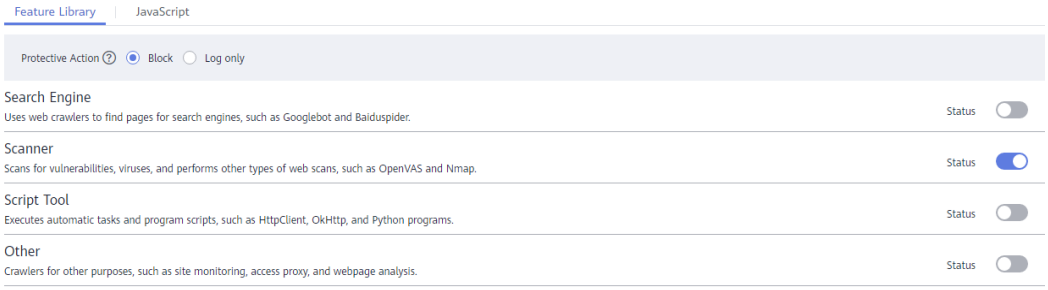


Table 6-10 Anti-crawler detection features

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 **Confirm** in the displayed dialog box to toggle on  .

Protective Action: **Block**, **Verification code**, and **Log only**.

NOTE

Verification code: If the JavaScript challenge fails, a verification code is required. Requests will be blocked unless the visitor enters a correct verification code.

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.

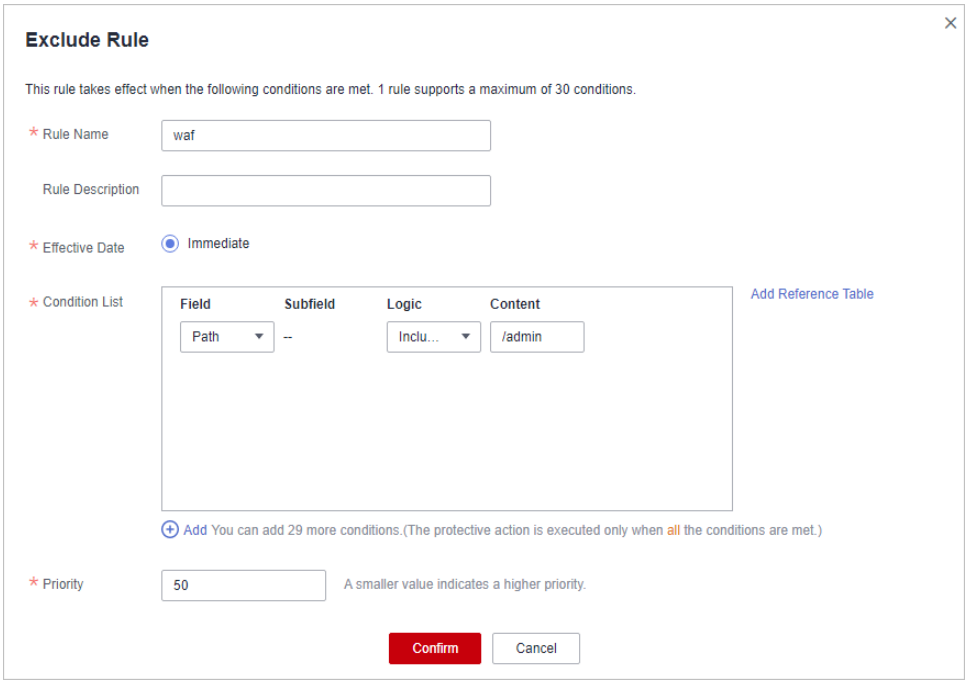
Step 9 Configure a JavaScript-based anti-crawler rule by referring to **Table 6-11**.

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

- To protect all requests except requests that hit a specified rule

Set **Protection Mode** to **Protect all requests**. Then, click **Exclude Rule**, configure the request exclusion rule, and click **Confirm**.

Figure 6-47 Exclude Rule



- To protect a specified request only

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

Table 6-11 Parameters of a JavaScript-based anti-crawler protection rule

Parameter	Description	Example Value
Rule Name	Name of the rule	waf
Rule Description	A brief description of the rule. This parameter is optional.	-
Effective Date	Time the rule takes effect.	Immediate

Parameter	Description	Example Value
Condition List	Parameters for configuring a condition are as follows: • **Field**: Select the field you want to protect from the drop-down list. Currently, only **Path** and **User Agent** are included. • **Subfield** • **Logic**: Select a logical relationship from the drop-down list. **NOTE** If you set **Logic** to **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any of them**, **Suffix is any value**, or **Suffix is not any of them**, you need to select a reference table. • **Content**: Enter or select the content that matches the condition.	**Path Include /admin**
Priority	Rule priority. If you have added multiple rules, rules are matched by priority. The smaller the value you set, the higher the priority.	5

----End

Other 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.

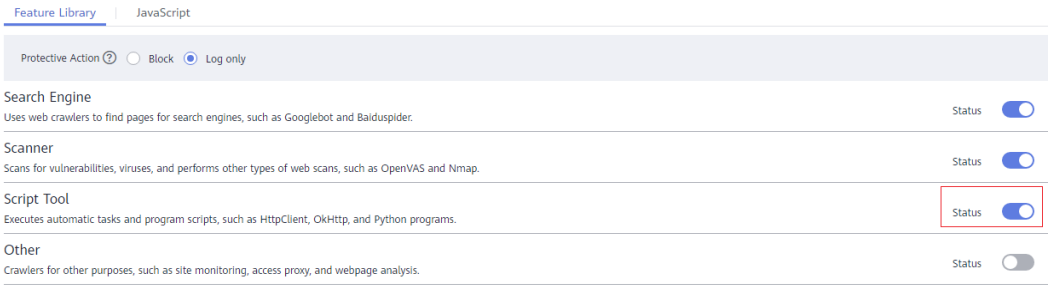
Configuration Example - Logging Script Crawlers Only

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.

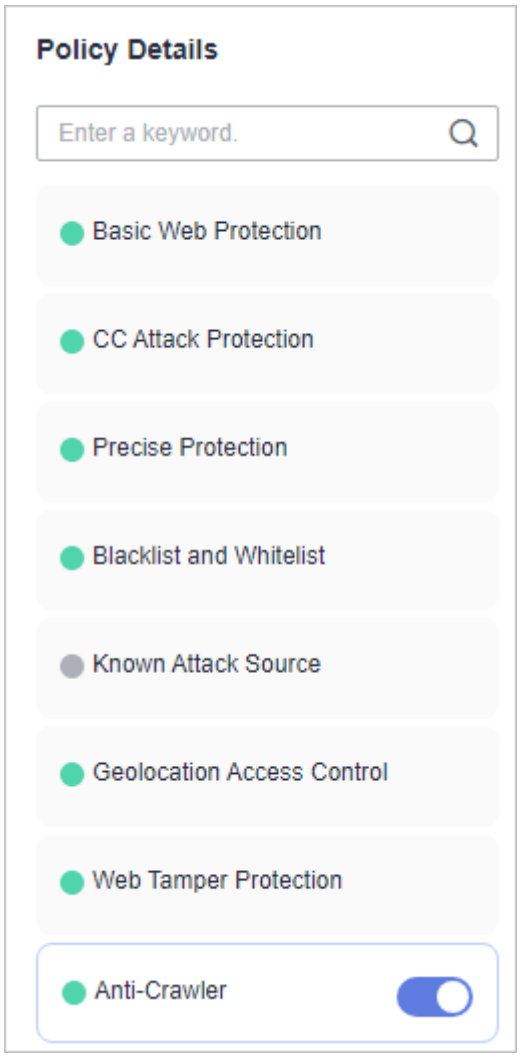
Step 2 On the **Feature Library** tab, enable **Script Tool** and select **Log only** for **Protective Action**. (If WAF detects an attack, it logs the attack only.)

Figure 6-48 Enabling Script Tool



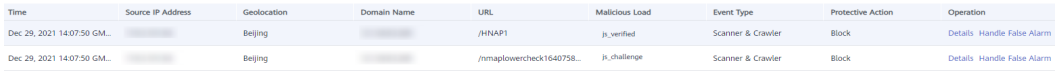
Step 3 Enable anti-crawler protection.

Figure 6-49 Anti-Crawler configuration area



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

Figure 6-50 Viewing Events - Script crawlers



----End

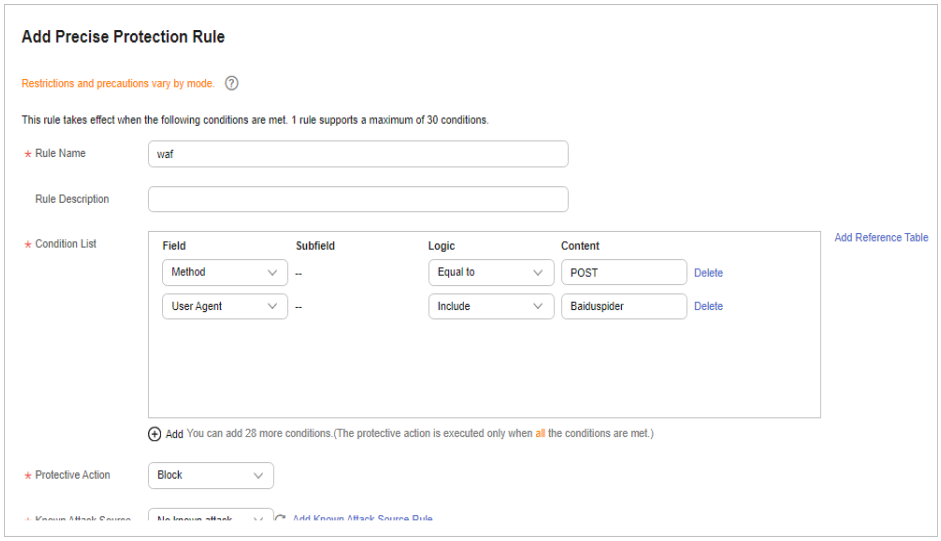
Configuration Example - Search Engine

The following shows how 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 6-51 Blocking POST requests



----End

6.10 Configuring Information Leakage Prevention Rules to Protect Sensitive Information from Leakage

You can add two types of information leakage prevention rules.

- Sensitive information filtering: prevents disclosure of sensitive information (such as ID numbers, phone numbers, 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**.

- For CNAME access in cloud mode, see **Adding a Website to WAF (Cloud Mode-CNAME Access)**.

- For ELB access in cloud mode, see **Adding a Website to WAF (Cloud Mode - ELB Access)**.
- For dedicated mode, see **Connecting a Website to WAF (Dedicated Mode)**.

Constraints

- The ELB-access cloud WAF does not support this type of protection rule.
- This function is not included in the standard 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.

Procedure

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 & Compliance**.

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.

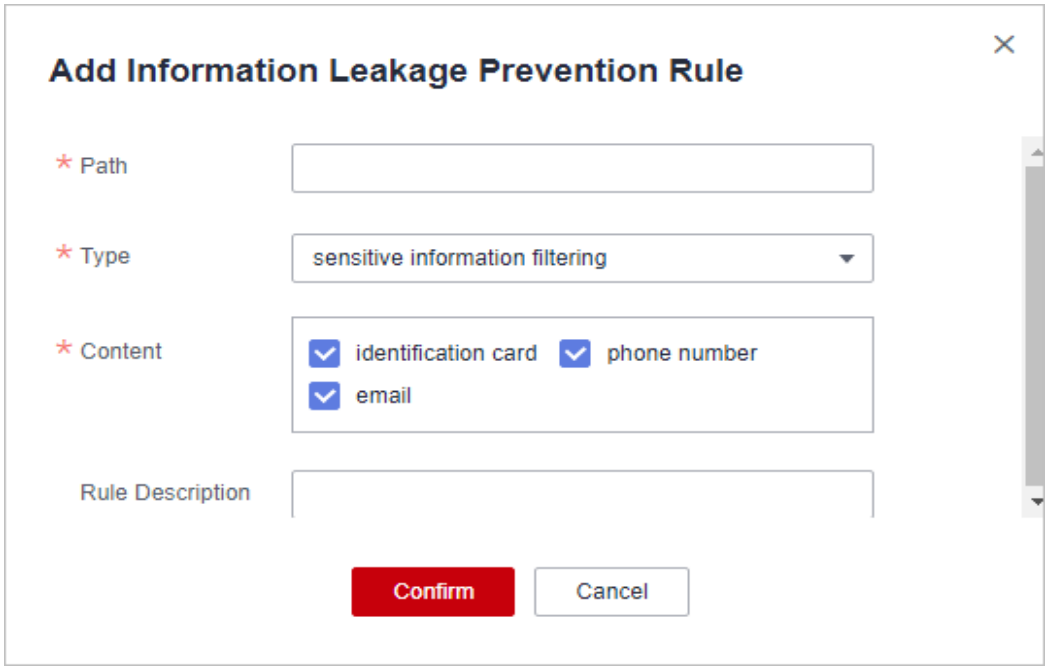
Step 7 In the upper left corner above the **Information Leakage Prevention** rule list, click **Add Rule**.

Step 8 In the dialog box displayed, add an information leakage prevention rule by referring to **Table 6-12**.

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 6-52 Sensitive information leakage



Response code interception: An error page of a specific HTTP response code may contain sensitive information. You can configure rules to block such error pages to prevent such information from being leaked out. For example, you can set the following rule to block error pages of specified HTTP response codes 404, 502, and 503.

Figure 6-53 Blocking response codes

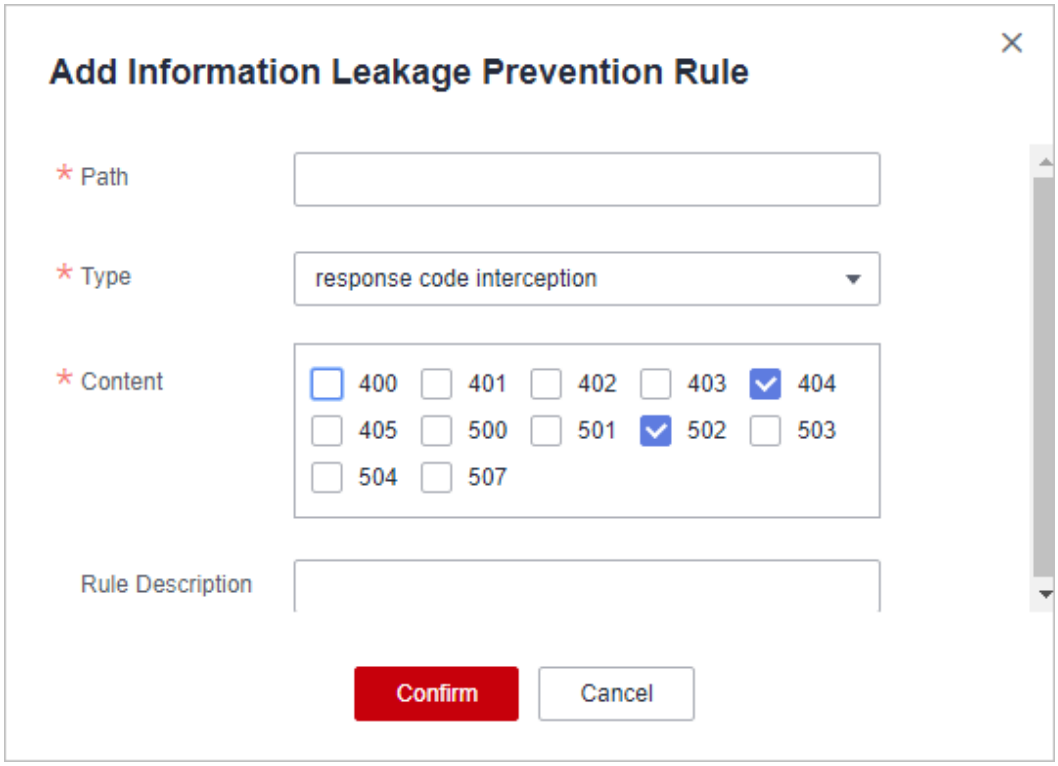


Table 6-12 Rule parameters

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**
Protective Action	Action the rule takes. You can select **Block** or **Log only**.	Block
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

Other Operations

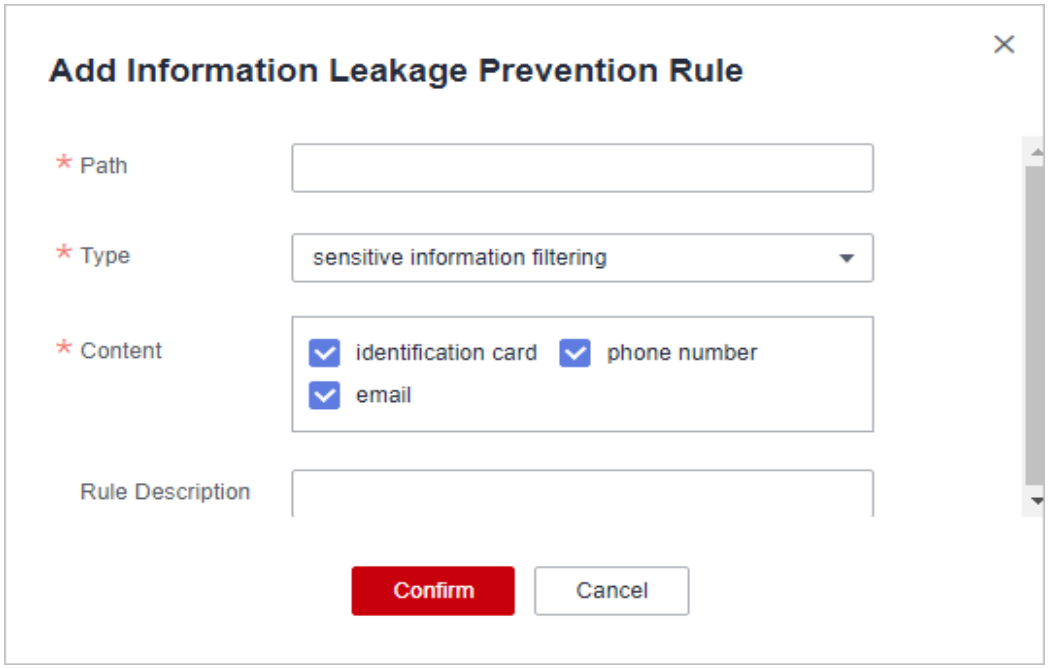
- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

Configuration Example — Masking Sensitive Information

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

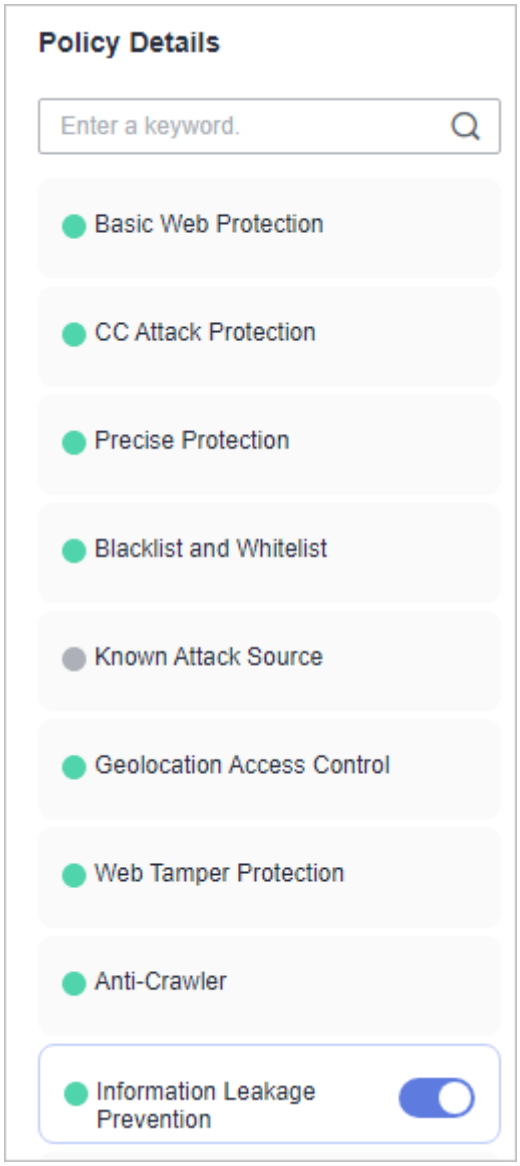
Step 1 Add an information leakage prevention rule.

Figure 6-54 Sensitive information leakage



Step 2 Enable information leakage prevention.

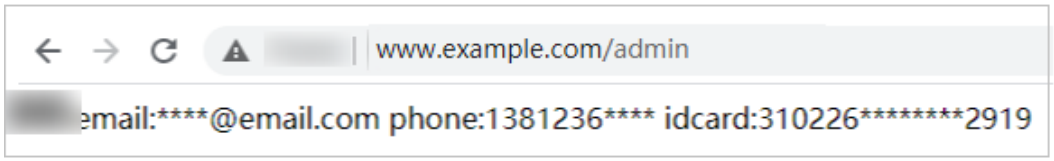
Figure 6-55 Information Leakage Prevention configuration area



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 6-56 Sensitive information masked



----End

6.11 Configuring a Global Protection Whitelist Rule to Ignore False Alarms

Once an attack hits a WAF basic web protection rule or a feature-library anti-crawler rule, WAF will respond to the attack immediately according to the protective action (**Log only** or **Block**) you configured for the rule and display an event on the **Events** page.

You can add false alarm masking rules to let WAF ignore certain rule IDs or event types (for example, skip XSS checks for a specific URL).

- If you select **All protection** for **Ignore WAF Protection**, all WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule.
- If you select **Basic Web Protection** for **Ignore WAF Protection**, you can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, if XSS check is not required for a URL, you can whitelist XSS rule.
- If you select **Invalid requests** for **Ignore WAF Protection**, WAF will whitelist invalid requests.

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.

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

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.

- 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.
- 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.

Procedure

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 & Compliance**.

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 protection whitelist rule by referring to **Table 6-13**.

Figure 6-57 Add Global Protection Whitelist Rule

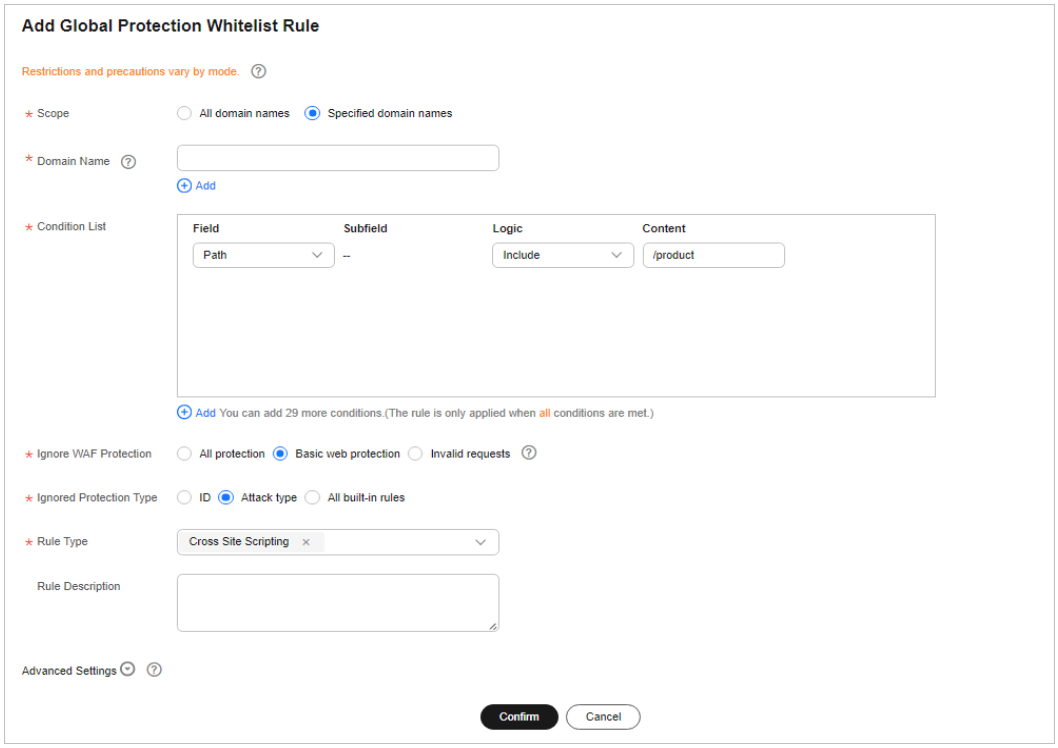


Table 6-13 Parameters

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. To add more domain names, click **Add** to add them one by one.	www.example.com

Parameter	Description	Example Value
Condition List	• Click **Add** in the condition box to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. • You can click **Add** outside the condition box to add a group of conditions. A maximum of three groups of conditions can be added. The relationship between multiple groups of conditions is **or**. So, the rule takes effect when one group of conditions is met. 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 URI 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.
Advanced Settings	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 **OK**.

----End

Other 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.

6.12 Configuring Data Masking Rules to Prevent Privacy Information Leakage

This topic describes how to configure data masking rules. You can configure data masking rules to prevent sensitive data such as passwords from being displayed in event logs.

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**.

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

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.

Procedure

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 & Compliance**.

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 6-14**.

Figure 6-58 Adding a data masking rule

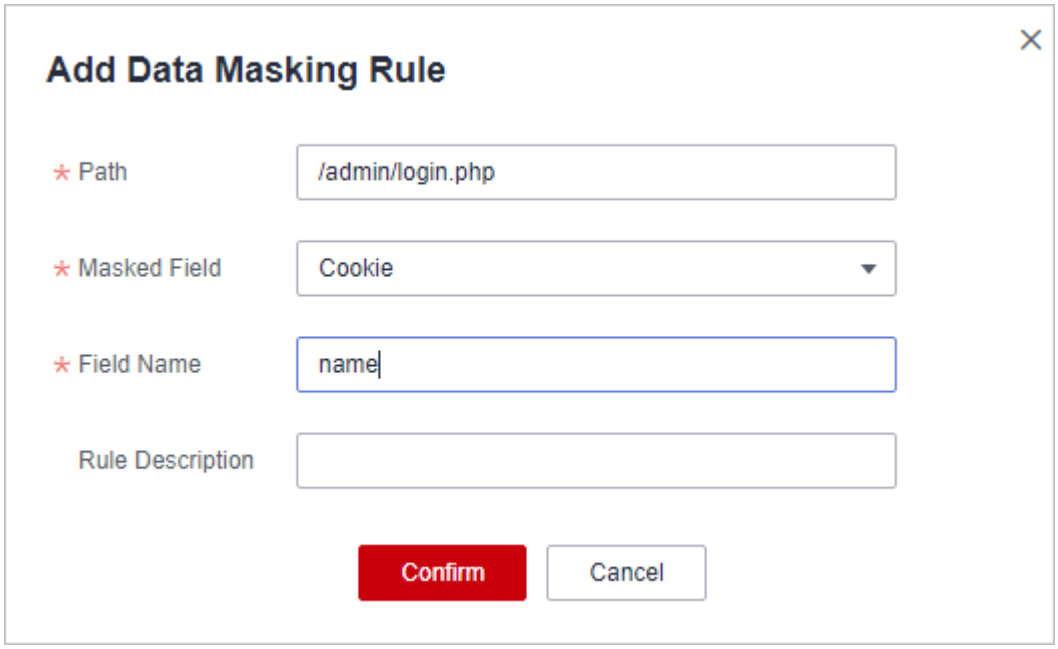


Table 6-14 Rule parameters

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. **NOTICE** The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.	
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

Other Operations

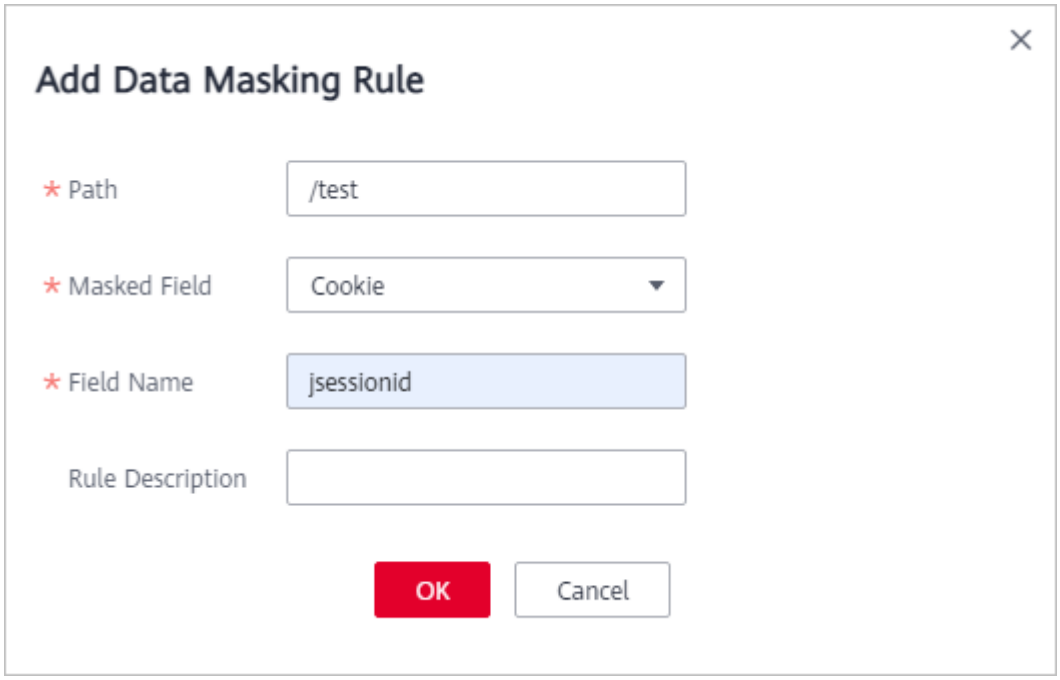
- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

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**):

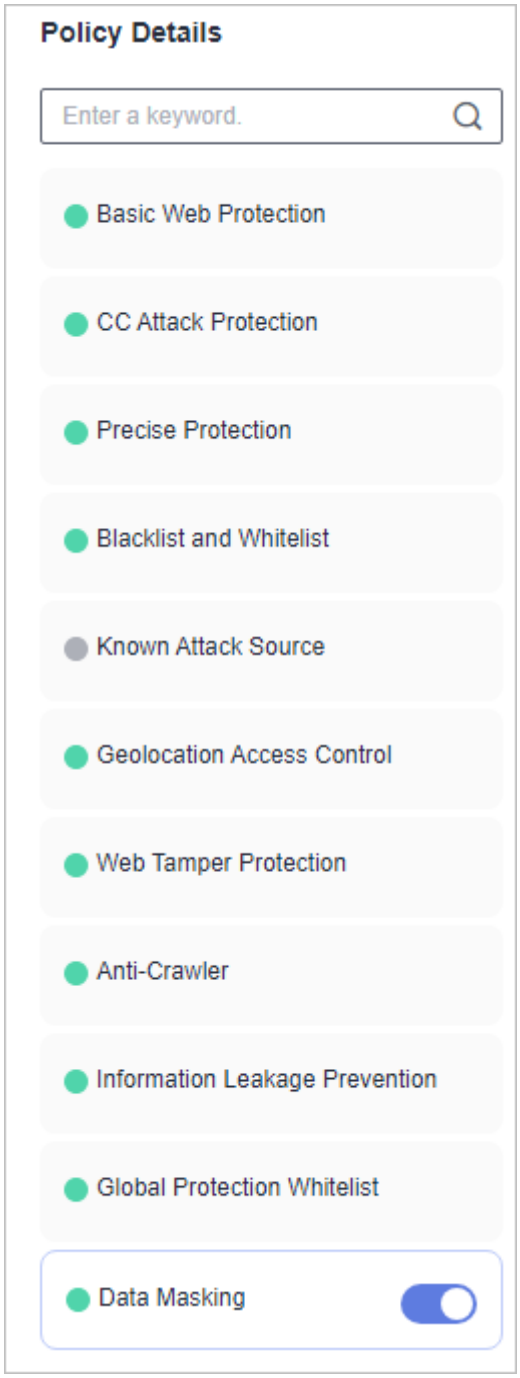
Step 1 Add a data masking rule.

Figure 6-59 Select **Cookie** for **Masked Field** and enter **jsessionid** in **Field Name**.



Step 2 Enable data masking.

Figure 6-60 Data Masking configuration area

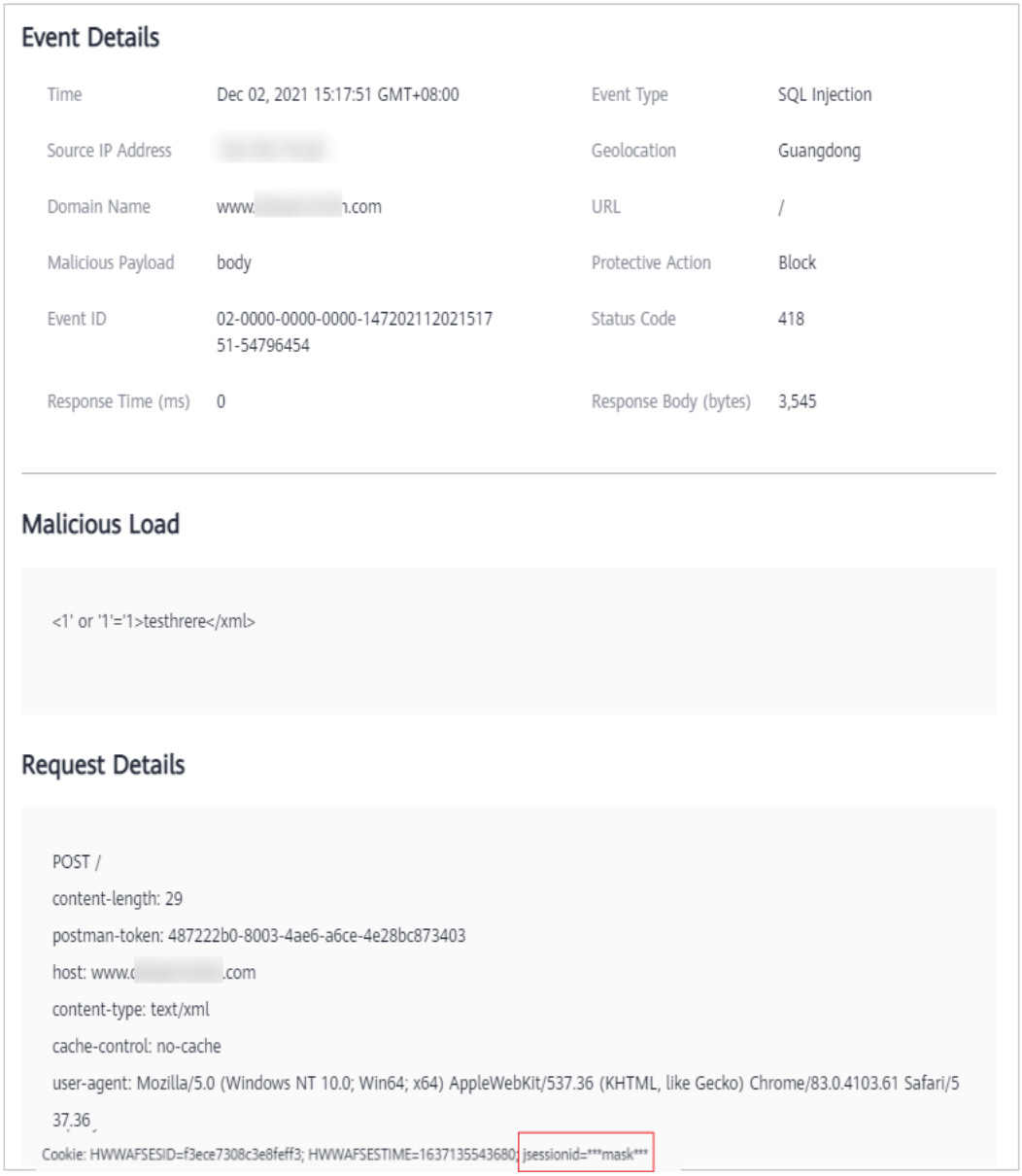


Step 3 In the navigation pane on the left, choose **Events**.

Step 4 In the row containing the event hit the rule, click **Details** in the **Operation** column and view the event details.

Data in the **jsessionid** cookie field is masked.

Figure 6-61 Viewing events - privacy data masking



----End

6.13 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, anti-crawler protection rules, and precise protection rules.

When you configure a CC attack protection rule, anti-crawler rule, or precise protection rule, if the **Logic** field in the **Trigger** list is set to **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any**

value, **Prefix is not any value**, **Suffix is any value**, or **Suffix is not any value**, you can select an appropriate reference table from the **Content** drop-down list.

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**.

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

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, anti-crawler, and precise protection rules.

Procedure

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 & Compliance**.

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 6-15**.

Figure 6-62 Adding a reference table

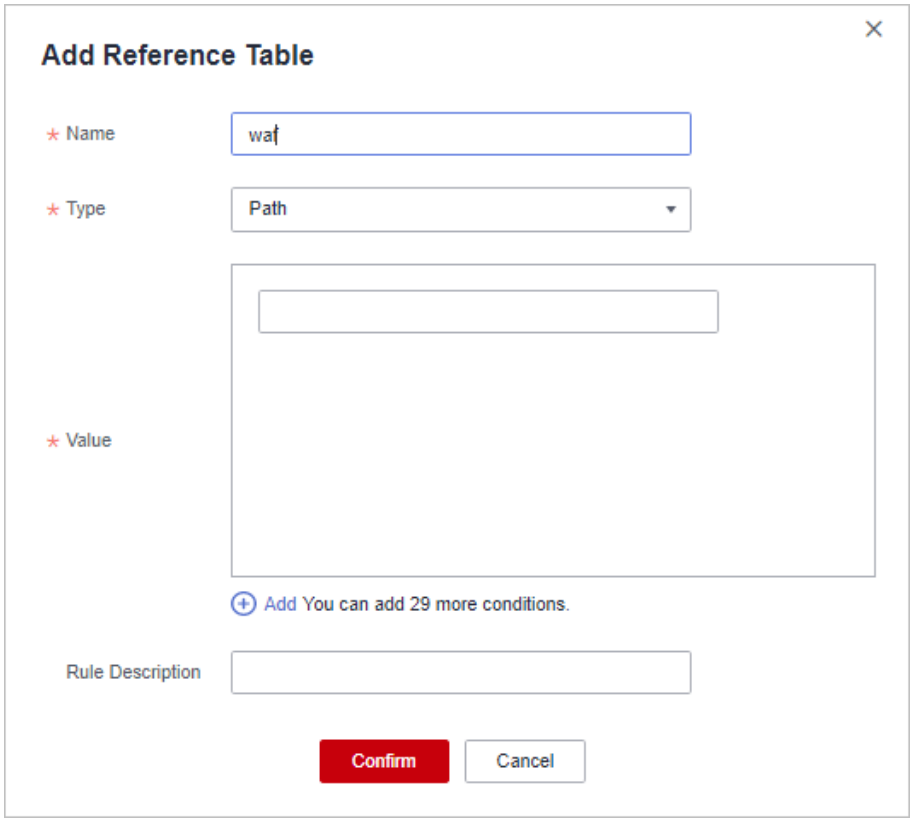


Table 6-15 Parameter description

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 • **Request Body**: data contained in an HTTP request.	**Path**
Value	Value of the corresponding **Type**. Wildcards are not allowed. **NOTE** Click **Add** to add more than one value.	**/buy/phone/**

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

----End

Other 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.

6.14 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, and IP address whitelist 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

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

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

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.
- 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.
- 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**.

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.

Procedure

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 & Compliance**.

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 6-16.

Figure 6-63 Add Known Attack Source Rule

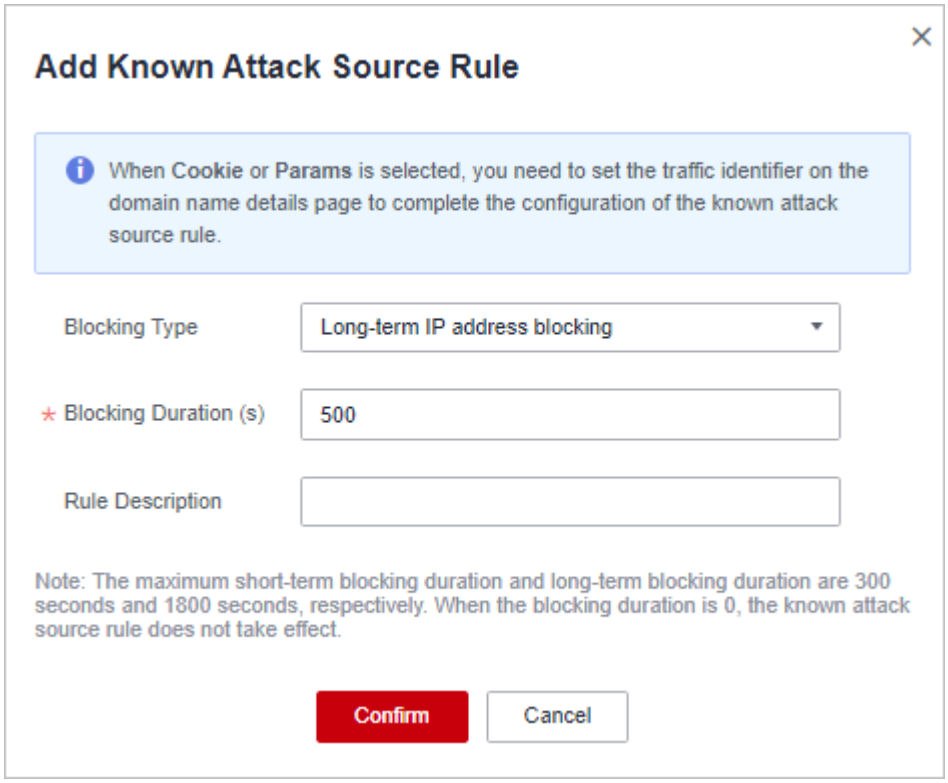


Table 6-16 Known attack source parameters

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**	**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

Other Operations

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

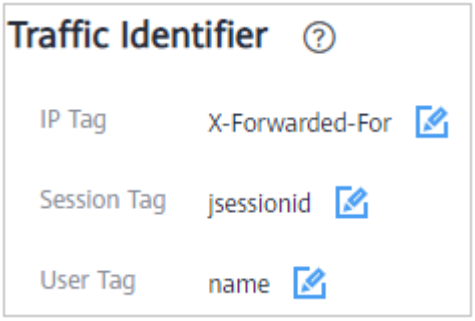
Configuration Example - Blocking Known Attack Source Identified by Cookie

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.

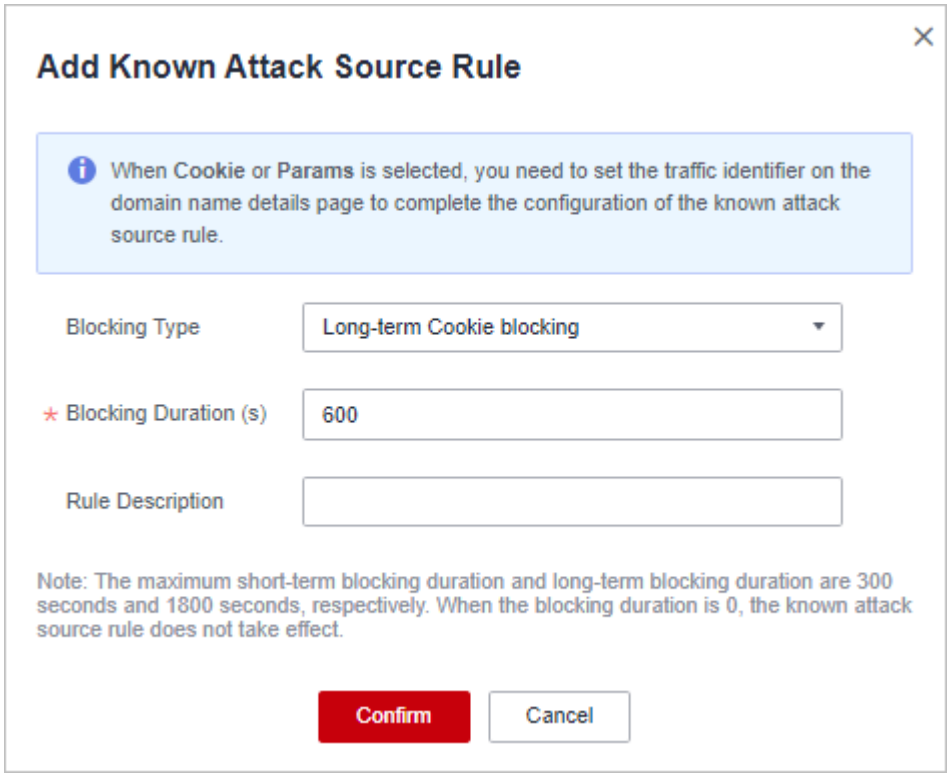
Step 2 In the **Traffic Identifier** area, configure the cookie in the **Session Tag** field.

Figure 6-64 Traffic Identifier



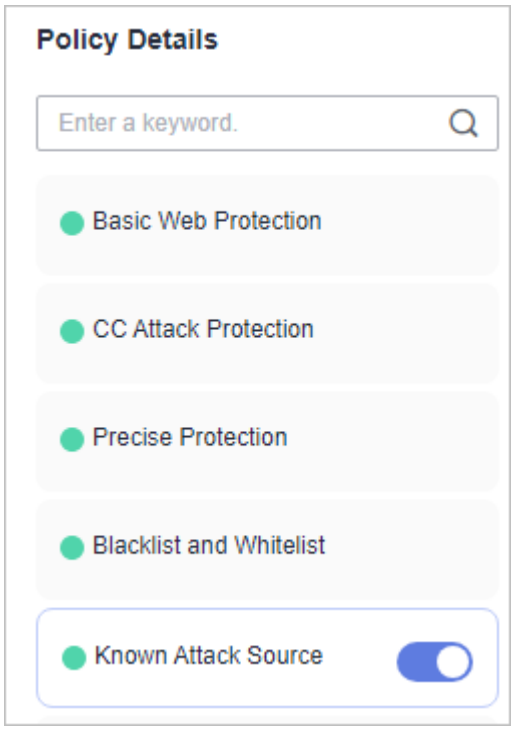
Step 3 Add a known attack source, select **Long-term Cookie blocking** for **Blocking Type**, and set block duration to 600 seconds.

Figure 6-65 Adding a Cookie-based known attack source rule



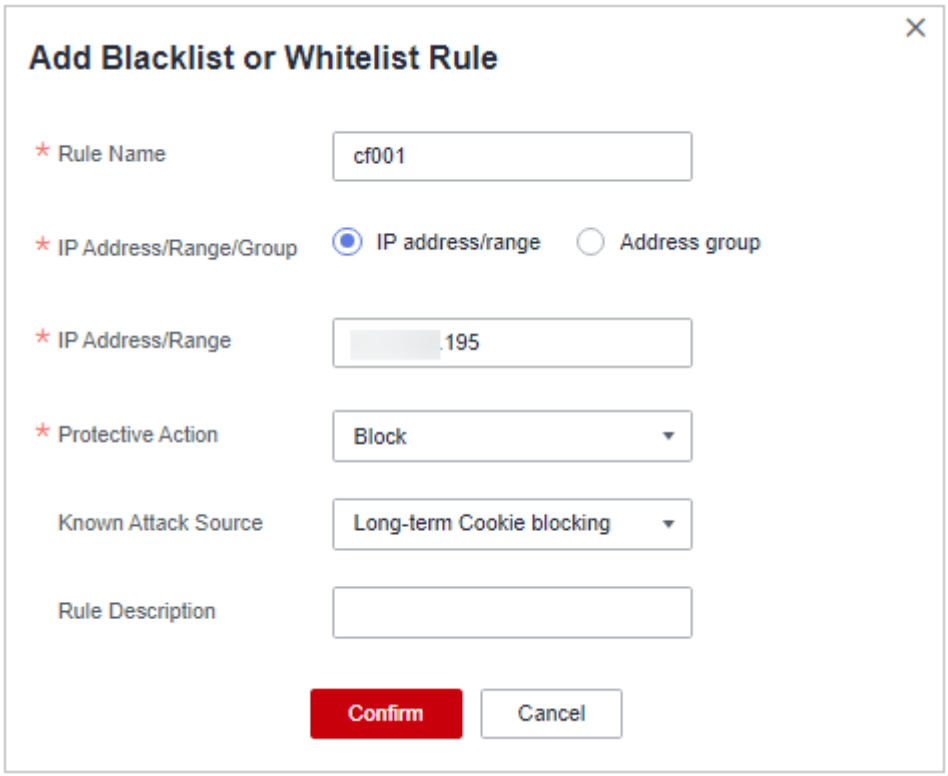
Step 4 Enable the known attack source protection.

Figure 6-66 Known Attack Source configuration area



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

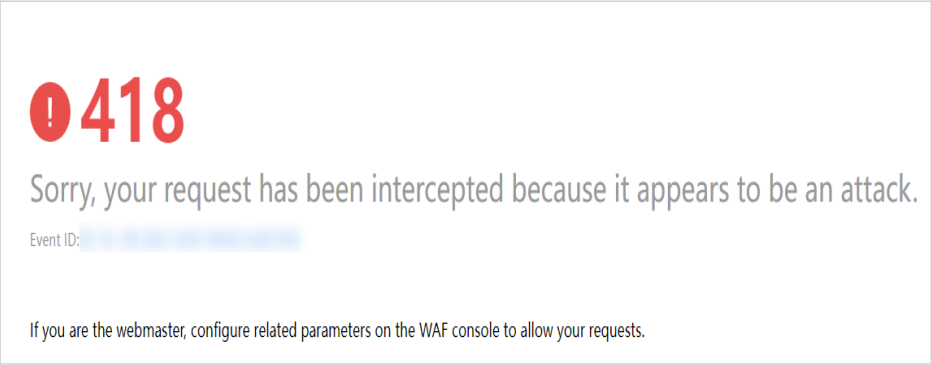
Figure 6-67 Specifying a known attack source rule



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 6-68 Block page



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

----End

6.15 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 **false alarm masking rule**, 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 6-69 Condition field

A condition field consists of the field, logic, and content. Example:

- Example 1: If **Field** is set to **Path**, **logic** to **Include**, and **Content** to **/admin**, a request matches the rule when the requested path contains /admin.
- Example 2: If **Field** is set to **IP**, **Logic** to **Equal to**, and **Content** to **192.XX.XX.3**, a request matches the rule when the client IP address is 192.XX.XX.3.

Supported Condition Fields

Table 6-17 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)*
IP: An IP address of the visitor to be protected.	• 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** 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
Location	--	• Included • Excluded	--

Field	Subfield	Logic	Content (Example)
Known feature crawler	--	• Match • Mismatch	• Search Engine • Scanner • Script Tool • Other

6.16 Application Types WAF Can Protect

Table 6-18 lists the application types that can be protected by basic web protection rules.

Table 6-18 Application types that WAF can protect

4images	Dragon-Fire IDS	Log4j2	ProjectButler
A1Stats	Drunken Golem GP	Loggix	Pulse Secure
Achievo	Drupal	Ipswitch 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 CVSearchServic e	HPInsightDiagnos tics	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	PHPAddressBoo k	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	-	-	-

7 Managing Policies

7.1 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.

Prerequisites

A website has been added to WAF.

Constraints

- This function is not included in the standard edition.
- A protected website domain name can use only one policy.
- You can copy policies in the same project.

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

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

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 & Compliance**.

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 **Copy**.

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

----End

Other 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.

7.2 Adding a Domain Name to a Policy

This topic describes how to apply a policy to your protected 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 project from the **Enterprise Project** drop-down list and configure protection policies for the domain names in batches.

Prerequisites

A website has been added to WAF.

Constraints

This function is not included in the standard edition.

Procedure

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 & Compliance**.

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

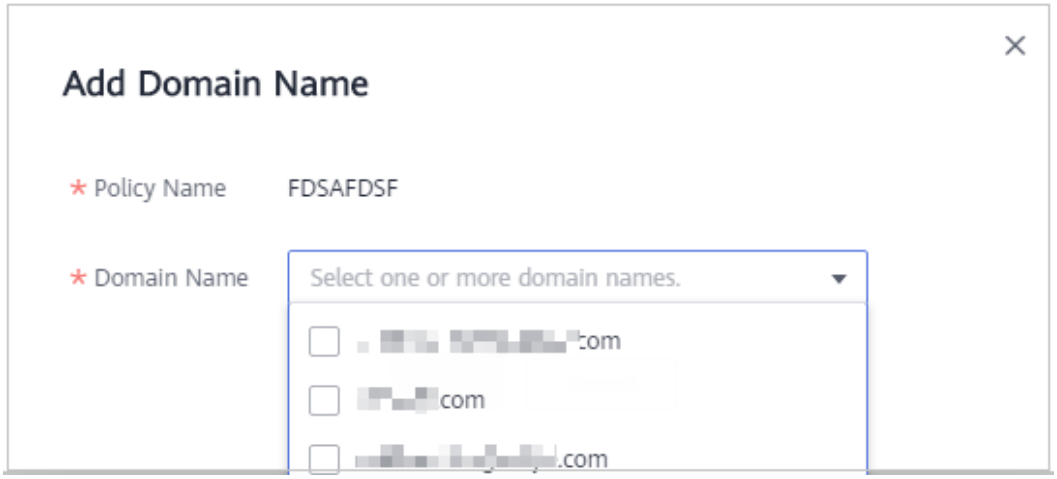
Step 5 In the row containing the policy you want to apply to a website, click **Add Domain Name** in the **Operation** column.

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 **Delete** in the **Operation** column of the policy you want to delete.

Figure 7-1 Selecting one or more domain names



Step 7 Click **Confirm**.

----End

7.3 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.

Prerequisites

A website has been added to WAF.

Procedure

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 & Compliance**.

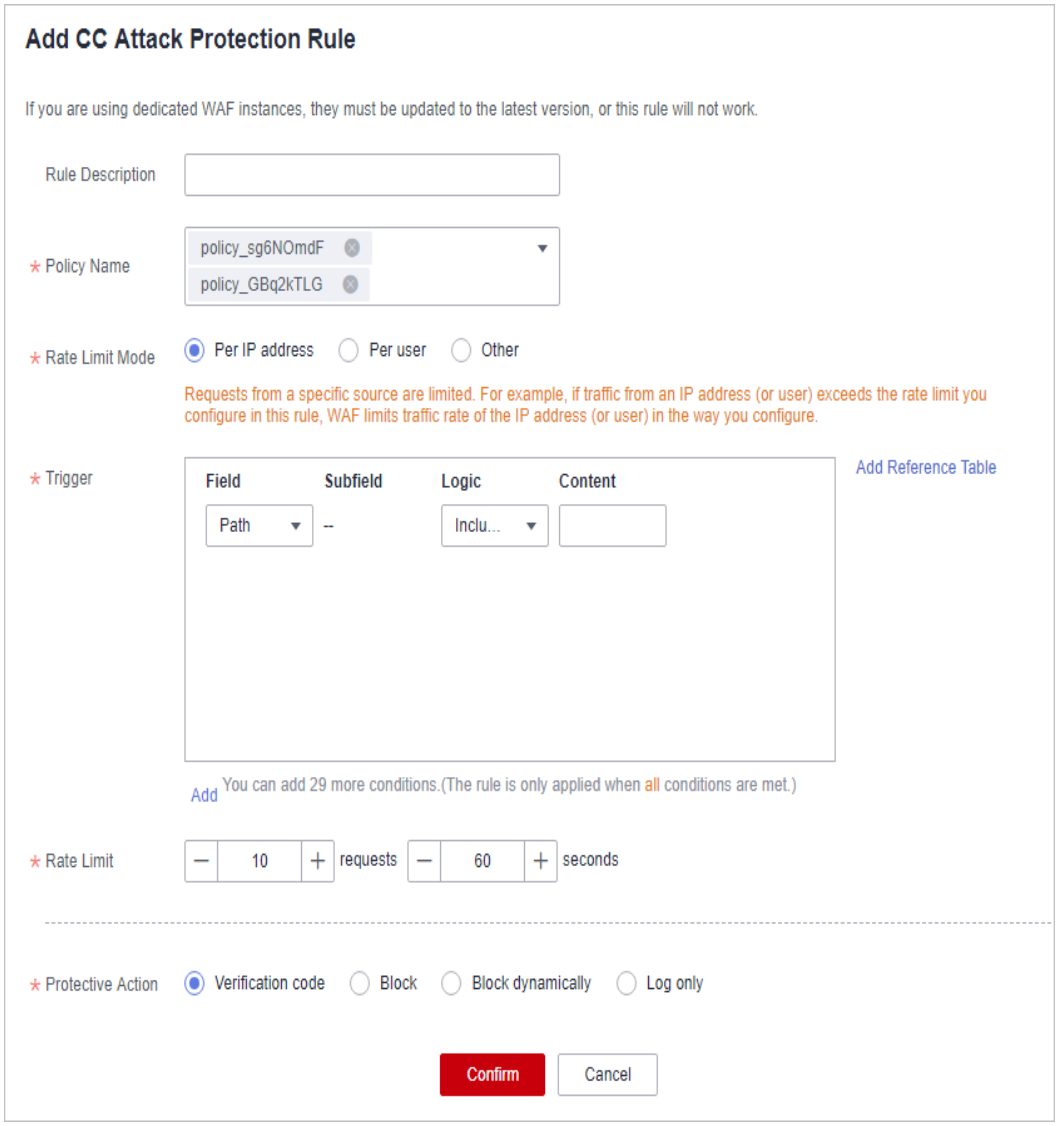
Step 4 In the navigation pane on the left, choose **Policies**.

Step 5 In the upper left corner above the policy list, click **View 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 7-2 Adding a rule to one or more policies



Step 8 Set other parameters.

- To add a CC attack protection rule, see **Table 6-5**.
- To add a precise protection rule, see **Table 6-6**.
- To add a blacklist or whitelist rule, see **Table 6-7**.
- To add a geolocation access control rule, see **Table 6-8**.
- To add a WTP rule, see **Table 6-9**.
- To add an information leakage prevention rule, see **Table 6-12**.
- To add a global protection whitelist rule, see **Table 6-13**.
- To add a data masking rule, see **Table 6-14**.

Step 9 Click **Confirm**.

----End

Other 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.

8 Website Settings

8.1 Adding a Website to WAF (Cloud Mode-CNAME Access)

8.1.1 Process for Adding a Website to WAF (Cloud Mode-CNAME Access)

This topic describes how to connect a domain name of a website to WAF in CNAME access mode so that the access traffic destined for the website can be forwarded to WAF for protection.

Constraints

- In CNAME access method, a cloud WAF instance can protect web applications and websites deployed on Huawei Cloud, other clouds, or even on-premises data centers as long as they are accessible through domain names. For details, see **Edition Differences**.
- After your website is connected to WAF, you can upload a file no larger than 10 GB each time.

Prerequisites

The following describes how WAF works when there is a proxy used or no proxy used in front of WAF:

- Proxy used

  If your website has used proxies, such as anti-DDoS, Content Delivery Network (CDN), or cloud acceleration, **Figure 8-1** shows how WAF works.

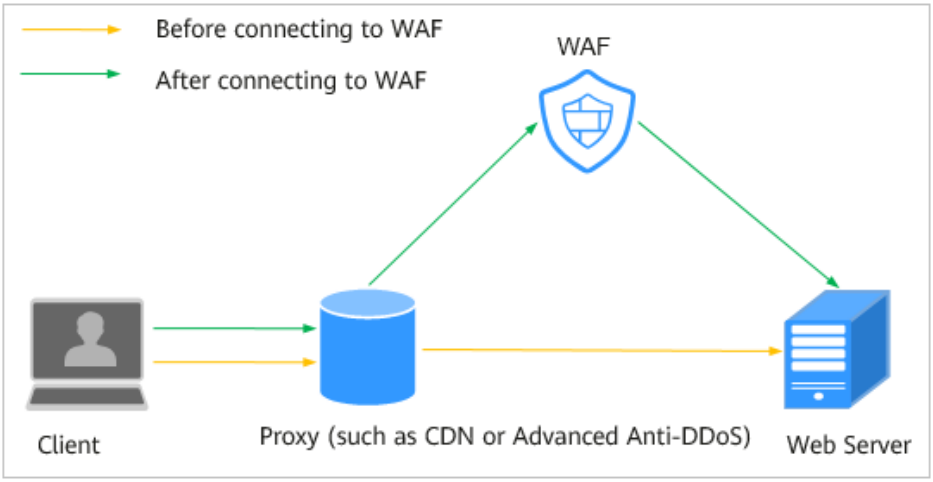
  - DNS resolves the domain name to the proxy IP address before your website is connected to WAF. In this case, the traffic passes through the proxy and then the proxy routes the traffic back to the origin server.
  - After you connect your website to WAF, change the back-to-source address of the proxy to the **CNAME** record of WAF. In this way, the proxy

forwards the traffic to WAF. WAF then filters out illegitimate traffic and only routes legitimate traffic back to the origin server.

i. Change the back-to-source IP address of the proxy to the CNAME record of WAF.

ii. (Optional) Add a WAF subdomain name and TXT record at your DNS provider.

Figure 8-1 WAF configuration when a proxy is used

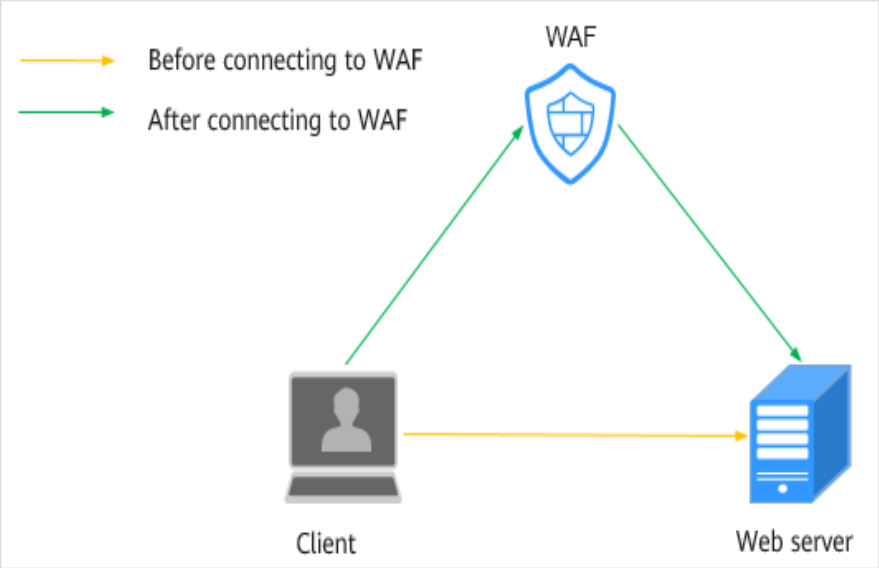


- No proxy used

  If no proxy is used before the website is connected to WAF, **Figure 8-2** shows how WAF works.

  - DNS resolves your domain name to the origin server IP address before your website is connected to WAF. Therefore, web visitors can directly access the server.
  - After your website is connected to WAF, DNS resolves your domain name to the CNAME record of WAF. In this way, the traffic passes through WAF. WAF then filters out illegitimate traffic and only routes legitimate traffic back to the origin server.

Figure 8-2 No proxy used



Processes of Connecting a Website to WAF

After purchasing a cloud WAF instance, complete the required configurations by following the process shown in **Figure 8-3**.

Figure 8-3 Process of connecting a website to WAF - Cloud Mode (CNAME Access)

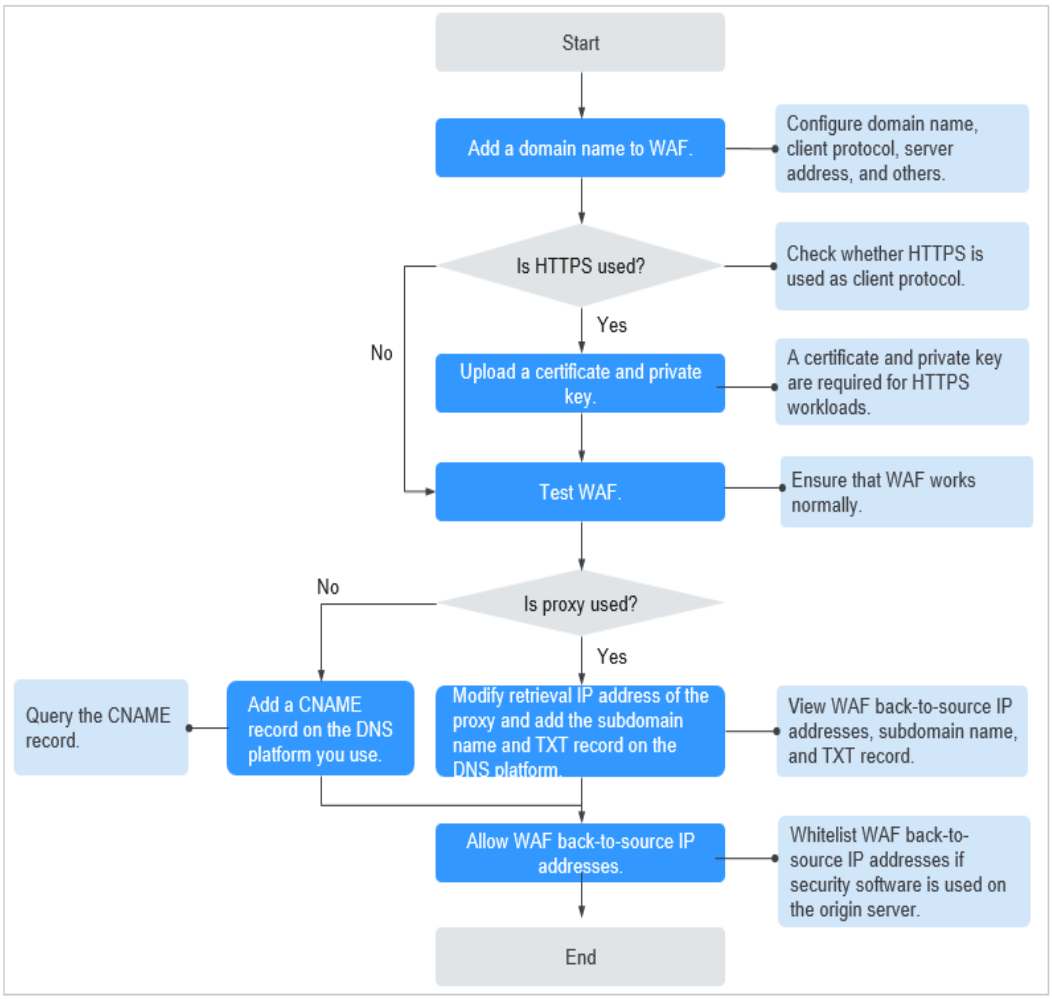


Table 8-1 Process of connecting your website domain name to WAF

Procedure	Description
Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)	Configure basic information, such as the domain name, protocol, and origin server.
Step 2: Whitelist WAF 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.
Step 3: Test 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
Step 4: Modify the DNS Records of the 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.

After you connect a domain name to WAF, WAF works as a reverse proxy between the client and the server. The real IP address of the origin server is hidden and only the IP address of WAF is visible to web visitors.

Collecting Domain Name Information

Before adding a domain name, obtain the information listed in **Table 8-2**.

Table 8-2 Domain name information required

Information	Parameter	Description	Example
Whether a proxy is used for the domain name	Proxy Configured	• **Layer-7 proxy**: Web proxy products, such as layer-7 anti-DDoS, CDN, and other cloud acceleration services, that will change the source and destination IP addresses are deployed in front of WAF. • **Layer-4 proxy**: Web proxy products, such as layer-4 anti-DDoS, that will not change the source or destination IP addresses are deployed in front of WAF. • **No proxy**: No proxy products are deployed in front of WAF. **NOTE** If you select **layer-7 proxy**, WAF obtains the real access IP address of the visit from the configured header field. For details, see **Configuring Header Field Forwarding**.	-

Information	Parameter	Description	Example
Parameters	Domain Name	The domain name is used by visitors to access your website. A domain name consists of letters separated by dots (.). It is a human readable address that maps to the machine readable IP address of your server.	www.example.com
	Protected Port	The service port corresponding to the domain name of the website you want to protect. • Standard Ports – 80: default port when the client protocol is HTTP – 443: default port when the client protocol is HTTPS • Non-standard ports Ports other than ports 80 and 443 **NOTICE** If your website uses a non-standard port, check whether the WAF edition you plan to buy can protect the non-standard port before you make a purchase. For details, see **Ports Supported by WAF**.	80
	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**.	-
	Client Protocol	Protocol used by a client (for example, a browser) to access the website. WAF supports HTTP and HTTPS.	HTTP
	Server Protocol	Protocol used by WAF to forward requests from the client (such as a browser). The options are **HTTP** and **HTTPS**.	HTTP
	Server Address	Public IP address or domain name of the origin server for a client (such as a browser) to access. Generally, a public IP address maps to the A record of the domain name configured on the DNS, and a domain name to the CNAME record.	XXX.XXX.1.1

Information	Parameter	Description	Example
(Optional) Certificate	Certificate Name	If you set **Client Protocol** to **HTTPS**, you are required to configure a certificate on WAF and associate the certificate with the domain name. **NOTICE** Only .pem certificates can be used in WAF. If the certificate is not in PEM format, convert it into pem format by referring to **How Do I Convert a Certificate into PEM Format?**	-

Fixing Inaccessible Websites

If a domain name fails to be connected to WAF, its access status is **Inaccessible**. To fix this issue, see **Why Is the Access Status of a Domain Name or IP Address Inaccessible?**

8.1.2 Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)

This topic describes how to add a domain name to WAF in CNAME access mode so that the website traffic can pass through WAF. After you connect a website domain name to your WAF instance, WAF works as a reverse proxy between the client and the server. The real IP address of the server is hidden and only the IP address of WAF is visible to web visitors.

NOTE

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

Prerequisites

You have **purchased a cloud WAF instance**.

Constraints

Constraint	Description
Domain name	• You can enter a multi-level single domain name (for example, top-level domain name example.com and level-2 domain name www.example.com) or a wildcard domain name (*.example.com). **NOTICE** 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. 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 to be protected. For example, if the subdomain names a.example.com, b.example.com, and c.example.com have the same server IP address, you can add the wildcard domain name *.example.com to WAF to protect all three. • If the server IP addresses of subdomain names are different, add subdomain names as single domain names one by one. • A 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.
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**.

Constraint	Description
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.
Account	Domain names added by an IAM user can be viewed by the account that creates the IAM user, but domain names added by an account cannot be viewed by IAM users created under the account.
Other	• WAF does not support user-defined HTTP headers for protected domain names. • After your website is connected to WAF, you can upload a file no larger than 10 GB each time.

Specification Limitations

After your website is connected to WAF, you can upload a file no larger than 10 GB each time.

Impact on the System

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?**

Procedure

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 & Compliance**.

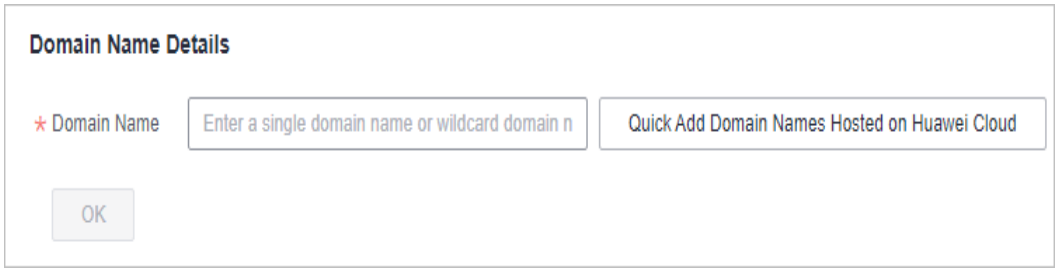
Step 4 In the navigation pane, choose **Website Settings**.

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

Step 6 Select **Cloud - CNAME** and click **OK**.

Step 7 Enter the domain name in the **Domain Name** text box and click **OK**.

Figure 8-4 Domain Name



You can enter a multi-level single domain name (for example, top-level domain name example.com and level-2 domain name www.example.com) or a wildcard domain name (*.example.com).

NOTICE

- The following are the rules for adding wildcards to 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 to be protected. 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.

If your domain name is hosted on Huawei Cloud, you can click **Quick Add Domain Names Hosted on Huawei Cloud**. In the **Select Domain Name** dialog box displayed, select the domain name you want to protect and click **OK**. The hosted domain name is automatically added to WAF.

Step 8 Provide the domain name details. **Figure 8-5** shows an example.

- **Website Name**: (Optional) You can customize the website name.
- **Domain Name**: Enter 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.
- **Website Remarks**: (Optional) You can provide remarks about your website if you want.

Figure 8-5 Configuring domain name details

Step 9 Configure the origin server. **Table 8-3** describes the parameters. **Figure 8-6** shows an example.

Figure 8-6 Origin Server Settings

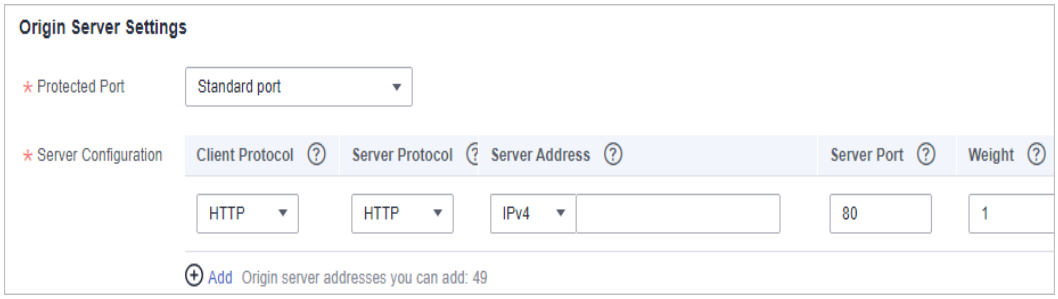


Table 8-3 Parameter description

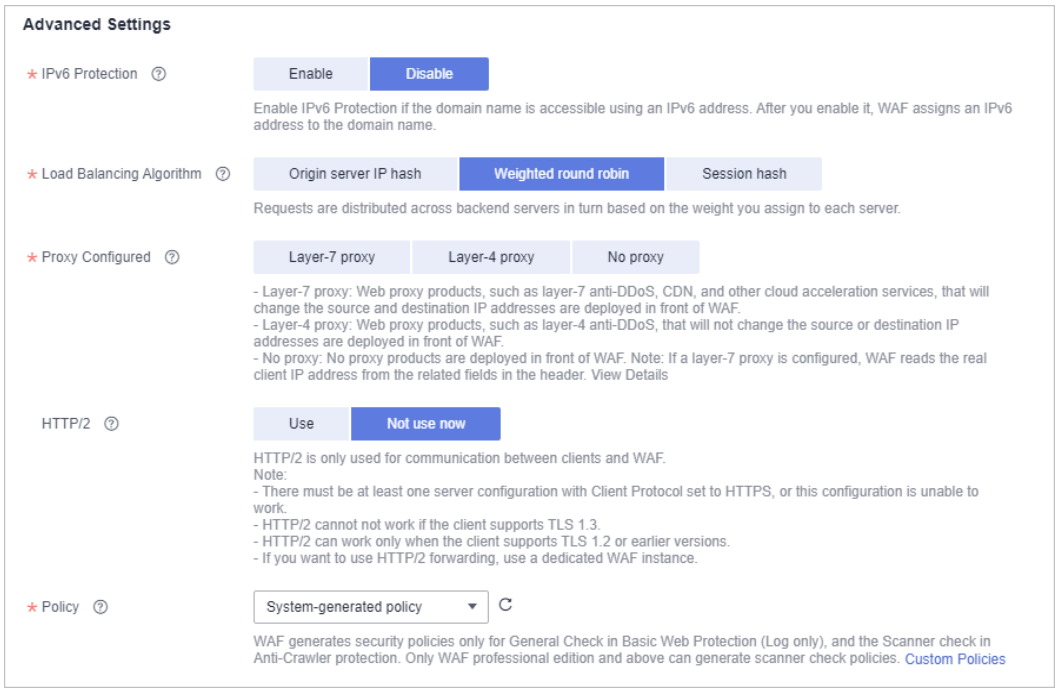
Parameter	Description	Example Value
Protected Port	Select the port type that you want WAF to protect from the drop-down list. To protect port 80 or 443, select **Standard port** from the drop-down list. For details about ports supported by WAF, see **Ports Supported by WAF**. **NOTE** If a port other 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	Configurations of your web server address. You need to configure the client protocol, server protocol, server weights, server address, and server port. • **Client Protocol**: protocol used by a client to access a server. The options are **HTTP** and **HTTPS**. If you set **Client Protocol** to **HTTPS**, **HTTP/2** can be enabled. For details, see **Enabling HTTP/2**. • **Server Protocol**: protocol used by WAF to forward client requests. The options are **HTTP** and **HTTPS**. **NOTE** – For details about configuring **Client Protocol** and **Server Protocol**, see **Example 4: Configuring Protocols for Different Access Methods**. – WAF can check WebSocket and WebSockets request, which is enabled by default. • **Server Address**: public IP address (generally corresponding to the A record of the domain name configured on the DNS) or domain name (generally corresponding to the CNAME of the domain name configured on the DNS) of the web server that a client accesses. The following IP address formats are supported: – IPv4 address, for example, XX.XXX.1.1 – IPv6 address, for example, fe80:0000:0000:0000:0000:0000:0000:0000 **NOTICE** Only the professional and platinum editions support IPv6 protection. • **Server Port**: service port over which the WAF instance forwards client requests to the origin server. • **Weight**: Requests are distributed across backend origin servers based on the load balancing algorithm you select and the weight you assign to each server.	**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. You can select a created certificate or import a certificate. For details about how to import a certificate, see **Importing a New Certificate**. The imported certificates are listed on the **Certificates** page. For more details, see **Uploading a Certificate**. Alternatively, you can buy a certificate on the CCM console and push it to WAF. For details about how to push an SSL certificate in CCM to WAF, see **Pushing an SSL Certificate to Other Cloud Services**. **NOTICE** • Only .pem certificates can be used in WAF. If the certificate is not in .pem format, convert it into .pem by referring to **Table 8-5** before uploading the certificate. • Currently, certificates purchased in Huawei Cloud SCM can be pushed only to the **default** enterprise project. For other enterprise projects, SSL certificates pushed by SCM cannot be used. • If your website certificate is about to expire, purchase a new certificate before the expiration date and update the certificate associated with the website in WAF. • 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.	--

Step 10 Complete advanced settings.

Figure 8-7 Advanced Settings



- **IPv6 Protection**: Enable IPv6 Protection if the domain name is accessible using an IPv6 address. After you enable it, WAF assigns an IPv6 address to the domain name.
  - If you select **IPv6** for **Server Address**, **IPv6 Protection** is enabled by default.
  - If you select **IPv4** for **Server Address** and enable **IPv6 Protection**, WAF will assign an IPv6 address to the domain name so that the website is accessible over the IPv6 address. In this way, requests to the IPv6 address are routed by WAF to the IPv4 address of the origin server.

  NOTE

  If the origin server uses IPv6 addresses, IPv6 protection is enabled by default. To prevent IPv6 service from interruption, keep the IPv6 protection enabled. If IPv6 protection is not needed, edit the server configuration and delete IPv6 configuration from the origin server first. For details, see **Editing Server Information**.
- **Load Balancing Algorithm**: Select an algorithm.
  - **Origin server IP hash**: Requests from the same IP address are routed to the same backend server.
  - Weighted round robin: All requests are distributed across origin servers in turn based on weights set to each origin server. The origin server with a larger weight receives more requests than others.
  - **Session hash**: Requests with the same session tag are routed to the same origin server. To enable this algorithm, **configure traffic identifiers for known attack sources**, or Session hash algorithm cannot take effect.

  For details, see **Switching the Load Balancing Algorithm**.
- Configure **Proxy Configured**.

  - **Layer-7 proxy**: Web proxy products, such as layer-7 anti-DDoS, CDN, and other cloud acceleration services, that will change the source and destination IP addresses are deployed in front of WAF.
  - **Layer-4 proxy**: Web proxy products, such as layer-4 anti-DDoS, that will not change the source or destination IP addresses are deployed in front of WAF.
  - **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 more details, see **Switching WAF Working Mode**.
  - If there is no proxy used for the protected website but you select **Layer-7 proxy** or **Layer-4 proxy** for **Proxy Configured**, WAF trusts the **X-Forwarded-For** field in the HTTP request header when obtaining the real source IP address. So there is no impact on your services.
  - If you select **layer-7 proxy**, WAF obtains the real access IP address of the visit from the configured header field. For details, see **Configuring Header Field Forwarding**.

- **HTTP/2**: If your website is accessible over HTTP and HTTPS, use HTTP/2.

  HTTP/2 can be used only for access between the client and WAF on the condition that at least one origin server has **HTTPS** used for **Client Protocol**.

  NOTICE

  - 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.

- Specify **Policy**. By default, **system-generated policy** is selected. You can select custom rules. For details, see **Table 8-4**.

  NOTICE

  If you are using WAF standard edition, only **System-generated policy** is available.

  You can select a policy you configured. You can also customize rules after the domain name is connected to WAF.

Table 8-4 System-generated policies

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

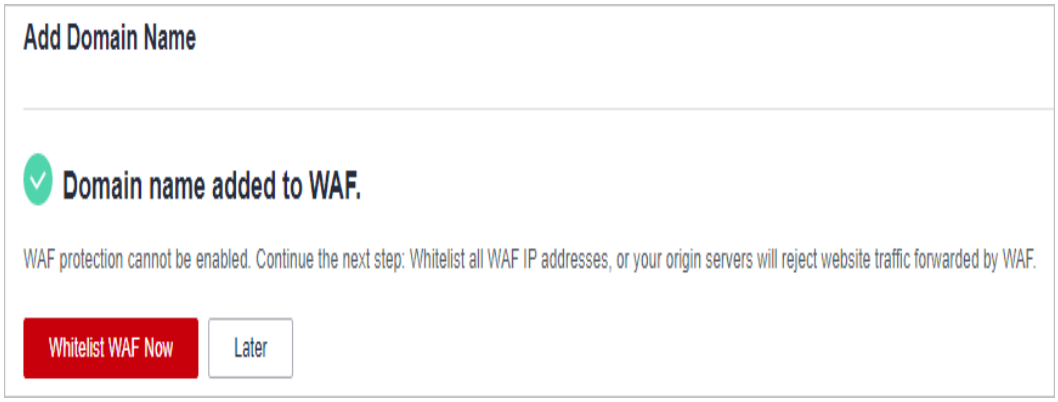
NOTE

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

Step 11 Click **OK**.

To enable WAF protection, there are three more steps, whitelisting WAF IP addresses, testing WAF, and routing your website traffic to WAF. You can click **Later** in this step. Then, finish those steps by referring to **Step 2: Whitelist WAF IP Addresses**, **Step 3: Test WAF**, and **Step 4: Modify the DNS Records of the Domain Name**.

Figure 8-8 Domain name added to WAF.



----End

Verification

- By default, WAF detects the **Access Status** of each protected domain name on an hourly basis.
- Generally, if you have performed domain connection and **Access Status** is **Accessible**, the domain name is connected to WAF.

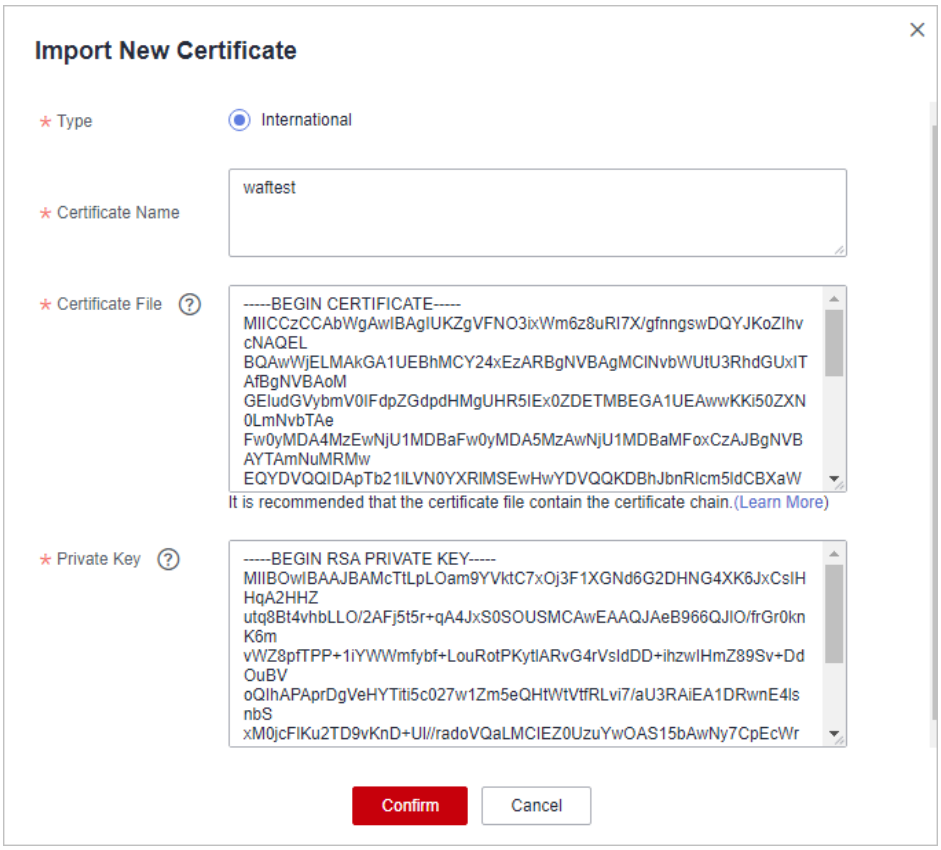
  If a domain name has been connected to WAF but **Access Status** is **Inaccessible**, click to refresh. If **Access Status** is still **Inaccessible**, connect the domain name to WAF again by referring to **Step 4: Modify the DNS Records of the Domain Name**.

Importing a New Certificate

If you set **Client Protocol** to **HTTPS**, an SSL certificate is required. You can perform the following steps to import a new certificate.

1. Click **Import New Certificate**. In the displayed **Import New Certificate** dialog box, enter the certificate name and paste the certificate file and private key to the corresponding text boxes.

Figure 8-9 Import New Certificate



NOTE

WAF encrypts and saves the private key to keep it safe.

Only .pem certificates can be used in WAF. If the certificate is not in .pem format, convert it into .pem locally by referring to **Table 8-5** before uploading it.

Table 8-5 Certificate conversion commands

Format	Conversion Method
CER/CRT	Rename the **cert.crt** certificate file to **cert.pem**.
PFX	• Obtain a private key. For example, run the following command to convert **cert.pfx** into **key.pem**: **openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes** • Obtain a certificate. For example, run the following command to convert **cert.pfx** into **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. Convert a certificate. For example, run the following command to convert **cert.p7b** into **cert.cer**: **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. Rename certificate file **cert.cer** to **cert.pem**.

Format	Conversion Method
DER	• Obtain a private key. For example, run the following command to convert **privatekey.der** into **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** • Obtain a certificate. For example, run the following command to convert **cert.cer** into **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTE

- Before running an OpenSSL command, ensure that the **OpenSSL** tool has been installed on the local host.
- If your local PC runs a Windows operating system, go to the command line interface (CLI) and then run the certificate conversion command.

2. Click **Confirm**.

Example Configuration

There are some configuration examples provided for your reference in **Configuration Example: Adding a Domain Name to WAF**.

8.1.3 Step 2: Whitelist WAF IP Addresses

In cloud CNAME access mode, to let WAF take effect, configure ACL rules on the origin server to trust only the back-to-source IP addresses of all your cloud WAF instances. This prevents hackers from attacking the origin server through the server IP addresses.

NOTICE

ACL rules must be configured on the origin server to whitelist WAF back-to-source IP addresses. Otherwise, your website visitors will frequently receive 502 or 504 error code when your website is connected to WAF.

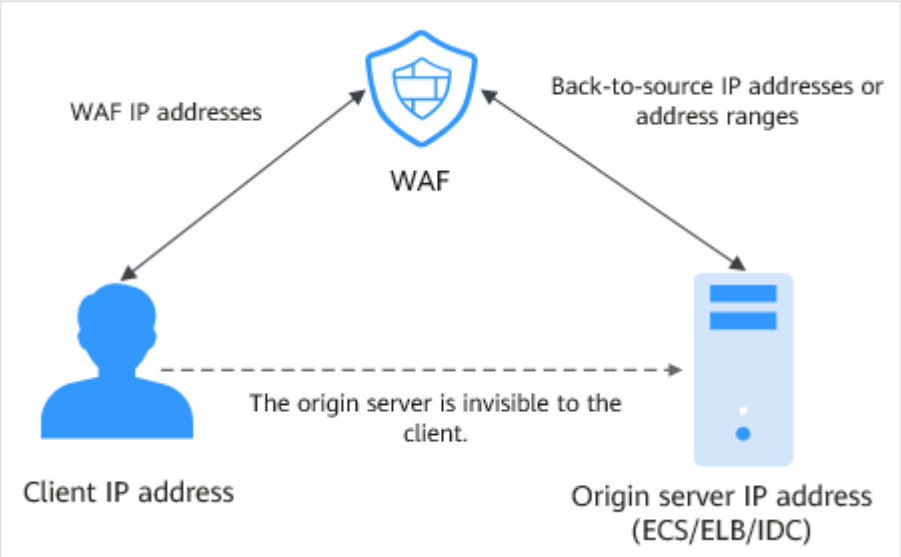
What Are Back-to-Source IP Addresses?

From the perspective of a server, all web requests originate from WAF. The IP addresses used by WAF forwarding are back-to-source IP addresses of WAF. The real client IP address is written into the X-Forwarded-For (XFF) HTTP header field.

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.

Figure 8-10 Back-to-source IP address



WAF Back-to-Source IP Address Check Mechanism

A back-to-source IP address, or WAF IP address, is randomly allocated from the back-to-source IP address range. When WAF forwards requests to the origin server, WAF will check the IP address status. If the IP address is abnormal, WAF will remove it and randomly allocate a normal one to receive or send requests.

Why Do I Need to Whitelist the WAF IP Address Ranges?

All web requests originate from a limited quantity of WAF IP addresses. The security software on the origin server may most likely regard these IP addresses as malicious and block them. Once WAF IP addresses are blocked, the website may fail to be accessed or it opens extremely slowly. To fix this, add the WAF IP addresses to the whitelist of the security software.

NOTE

After you connect your website to WAF, uninstall other security software from the origin server or allow only the requests from WAF to access your origin server. This ensures normal access and protects the origin server from hacking.

Procedure

Step 1 Log in to the management console.

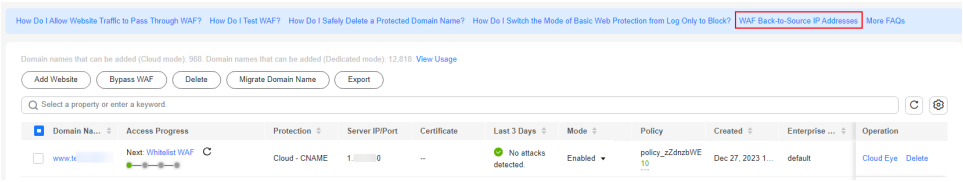
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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

Step 5 Above the website list, click **WAF Back-to-Source IP Addresses**.

Figure 8-11 WAF Back-to-Source IP Addresses



Step 6 In the displayed dialog box, click **Copy** to copy all the addresses.

Step 7 Open the security software on the origin server and add the copied IP addresses to the whitelist.

- If your origin servers are deployed on the Huawei Cloud ECSs, see **Whitelisting WAF IP Addresses on Origin Servers That Are Deployed on Huawei Cloud ECSs**.
- If your origin servers use Huawei Cloud ELB, see **Whitelisting WAF IP Addresses on Origin Servers That Use Huawei Cloud ELB**.
- If you also use Cloud Firewall (CFW) on Huawei Cloud, refer to **Adding a Protection Rule**.
- If your website is deployed on servers on other cloud vendors, whitelist the WAF 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.

----End

Whitelisting WAF IP Addresses on Origin Servers That Are Deployed on Huawei Cloud ECSs

If your origin server is deployed on a Huawei Cloud ECS, perform the following steps to configure a security group rule to allow only the WAF back-to-source IP addresses 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 of the page and choose **Compute** > **Elastic Cloud Server**.

Step 4 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 5 Click the **Security Groups** tab. Then, click **Change Security Group**.

Step 6 Click the security group name to view the details.

Step 7 Click the **Inbound Rules** tab and click **Add Rule**. Then, specify parameters in the **Add Inbound Rule** dialog box. For details, see **Table 8-6**. **Figure 8-12** shows an example.

Figure 8-12 Add Inbound Rule

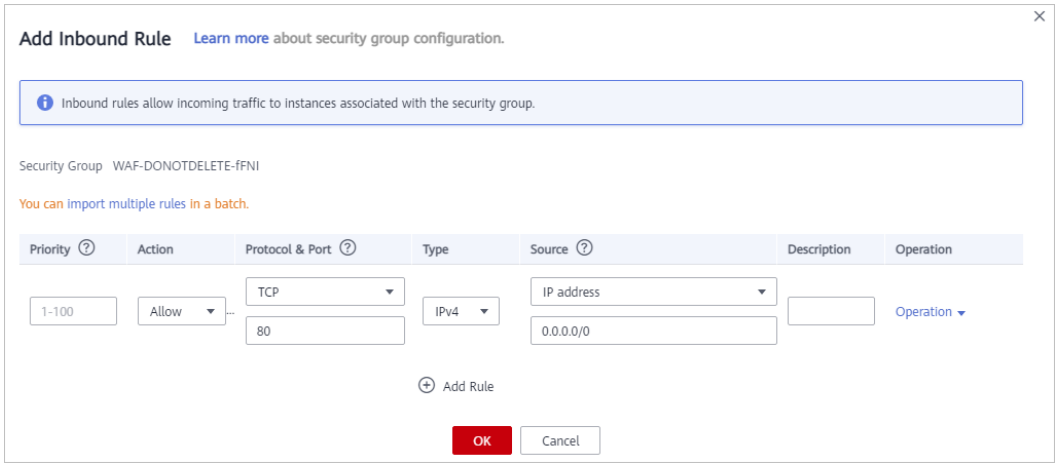


Table 8-6 Inbound rule parameters

Parameter	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.
Source	Add all WAF back-to-source IP addresses copied in **Step 6** one by one. **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 8 Click **OK**.

Then, the security group rules allow all inbound traffic from the WAF back-to-source IP addresses.

----End

Whitelisting WAF IP Addresses on Origin Servers That Use Huawei Cloud ELB

If your origin server is deployed on backend servers of a Huawei Cloud ELB load balancer, perform the following steps to configure an access control list to allow only the WAF back-to-source IP addresses to access the origin server.

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

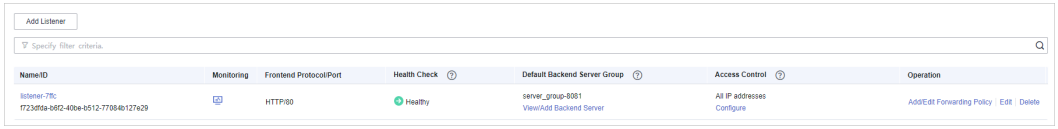
Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Networking** > **Elastic Load Balance**.

Step 4 Locate the load balancer you want. In the **Listener** column, click the listener name to go to the details page.

Step 5 In the **Access Control** row of the target listener, click **Configure**.

Figure 8-13 Listener list



Step 6 In the displayed dialog box, select **Whitelist** for **Access Control**.

1. Click **Create IP Address Group** and add the dedicated WAF instance IP addresses obtained in **Step 6** to the group being created.
2. Select the IP address group created in **Step 6.1** from the **IP Address Group** drop-down list.

Step 7 Click **OK**.

----End

8.1.4 Step 3: Test WAF

To ensure that WAF can forward your website requests normally, test WAF locally after you add the domain to WAF.

Before testing WAF, ensure that the protocol, address, and port used by the origin server (for example, **www.example5.com**) are correct. If **Client Protocol** is set to **HTTPS**, ensure that the uploaded certificate and private key are correct.

Background

You can configure local DNS records for domain name resolution by modifying local hosts file. To test connection between WAF and your website locally, you need to resolve the website domain name to WAF IP addresses on a 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.

Prerequisites

You have **added your domain name to WAF**.

Constraints

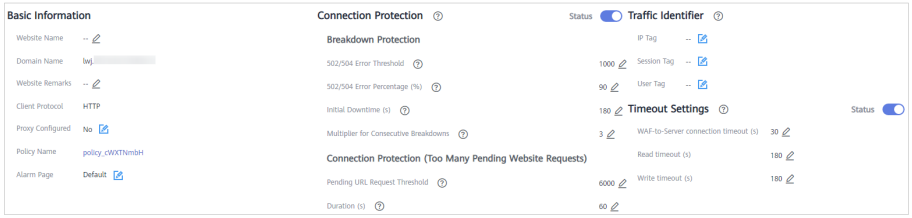
A CNAME record is generated based on the domain name. For the same domain name, the CNAME records are the same.

Connecting a Domain Name to WAF Locally

Step 1 Obtain the CNAME record.

1. Click in the upper left corner of the management console and select a region or project.
2. Click in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
3. In the navigation pane, choose **Website Settings**.
4. In the **Domain Name** column, click the target domain name to go to the **Basic Information** page.

Figure 8-14 Basic Information



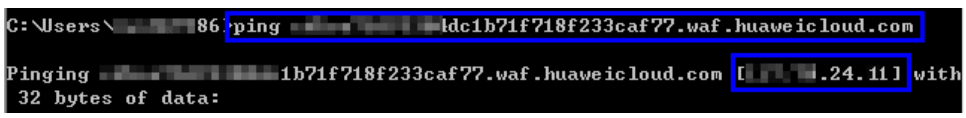
5. In the **CNAME** row, click to copy the CNAME record.

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 the CLI and run the **ping xxxxxxxdc1b71f718f233caf77.waf.huaweicloud.com** command to obtain the WAF back-to-source IP address. As shown in **Figure 8-15**, the WAF back-to-source IP address is displayed.

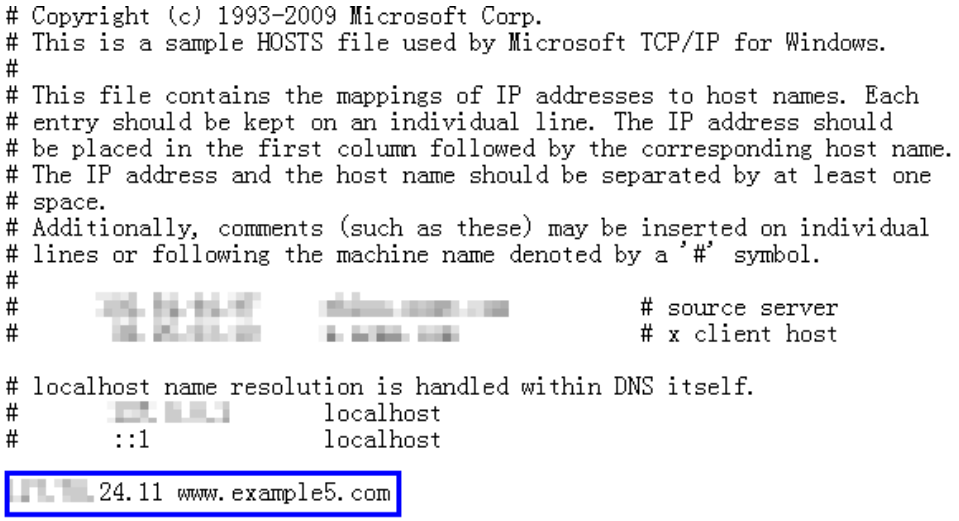
Figure 8-15 Ping CNAME



Step 3 Add the domain name and WAF back-to-source IP address to the **hosts** file.

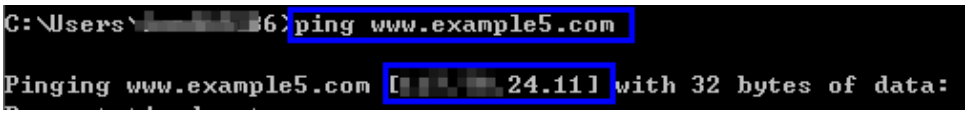
1. Use a text editor to open the **hosts** file. Generally, the **hosts** file is stored in the **C:\Windows\System32\drivers\etc** directory.
2. Add the WAF IP address obtained in **Step 2** and protected domain name to the **hosts** file.

Figure 8-16 Adding a record



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

Figure 8-17 Pinging the domain name



It is expected that the resolved IP address is the WAF back-to-source IP address obtained in **Step 2**. If the resolved IP address is the origin server address, run the **ipconfig/flushdns** command in the Windows operating system to flush the DNS cache.

----End

Checking Whether WAF Forwarding Is Normal

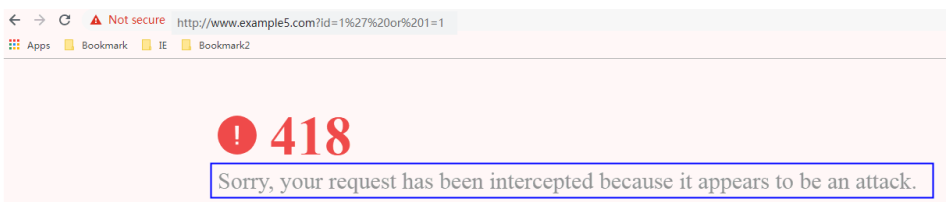
Step 1 Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

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

Step 2 Simulate simple web attack commands.

1. Set the mode of **Basic Web Protection** to **Block**. For details, see **Enabling Basic Web Protection**.
2. 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 8-18** shows an example.

Figure 8-18 Request blocked



3. In the navigation pane, choose **Events** to view test data.

----End

8.1.5 Step 4: Modify the DNS Records of the Domain Name

After a domain name is connected 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.

To ensure that your WAF instance works properly, test it according to the instructions in **Step 3: Test WAF** before routing your business traffic to WAF.

Prerequisites

- You have added the domain name you want to protect to the cloud WAF instance you have in CNAME access mode. For details, see **Step 1: Add a Domain Name to WAF (Cloud Mode)**.
- You have the permission to modify domain name resolution settings on the DNS platform hosting your domain name.
- You have **whitelisted WAF IP addresses** on your origin servers.
- (Optional) You have **tested your website connectivity** to ensure that WAF can forward requests.

Constraints

WAF protection takes effect only for real client IP addresses where requests originate. To ensure that WAF obtains real client IP addresses, if your website has layer-7 proxies such as CDN and cloud acceleration products deployed in front of WAF, **Layer-7 proxy** must be selected for **Proxy Configured**.

Specification Limitations

After your website is connected to WAF, you can upload a file no larger than 10 GB each time.

How WAF Works

- No proxy used

  DNS resolves your domain name to the origin server IP address before the site is connected to WAF. DNS resolves your domain name to the CNAME of WAF after the site is connected to WAF. Then WAF inspects the incoming traffic and filters out malicious traffic.

- A proxy (such as anti-DDoS service) used

  If a proxy such as anti-DDoS service is used on your site before it is connected to WAF, DNS resolves the domain name of your site to the anti-DDoS IP address. The traffic goes to the anti-DDoS service and the anti-DDoS service then routes the traffic back to the origin server. After you connect your website to WAF, change the back-to-source address of the proxy (such as anti-DDoS service) to the CNAME of WAF. In this way, the proxy forwards the

traffic to WAF. WAF then filters out illegitimate traffic and only routes legitimate traffic back to the origin server.

NOTE

- To ensure that WAF can properly forward requests, perform local verification by referring to **Testing WAF** before modifying the DNS configuration.
- 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. WAF can determine which user owns the domain name based on the subdomain name and TXT record. For details about the configuration method, see **What Are Impacts If No Subdomain Name and TXT Record Are Configured?**

Operation Guide

After a domain name is added, WAF generates a CNAME record, or CNAME, subdomain name, and TXT record for DNS to resolve the domain name to WAF so that website traffic can pass through WAF for detection. For details, see **Table 8-7**.

Table 8-7 Operation guide

Scenario	Generated Parameter Value	Operation Related to Domain Name Resolution
No proxy used	CNAME	The DNS obtains the CNAME of WAF.
Proxy used	CNAME, subdomain name, and TXT record	• Change the back-to-source IP address of the proxy, such as anti-DDoS service, to the CNAME of WAF. • (Optional) Add a WAF subdomain name and TXT record at your DNS provider.

Procedure

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.

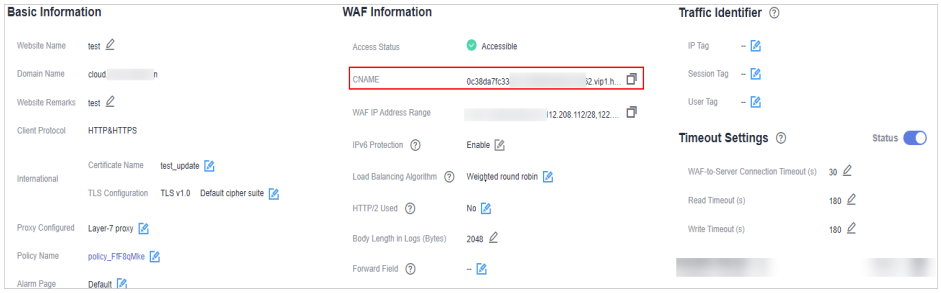
Step 3 Click in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.

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

Step 5 In the row containing the desired domain name, click the domain name to go to the **Basic Information** page.

Step 6 In the **CNAME** row, click to copy the CNAME record.

Figure 8-19 Copying the CNAME record



If the message "CNAME copied successfully" is displayed in the upper right corner of the page, the CNAME record is copied successfully.

Step 7 Connect the domain name to WAF.

- No proxy used

  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.

  a. Click in the upper left corner of the page and choose **Networking** > **Domain Name Service**.
  b. In the navigation pane on the left, choose **Public Zones**.
  c. In the **Operation** column of the target domain name, click **Manage Record Set**. The **Record Sets** tab page is displayed.
  d. In the row containing the desired record set, click **Modify** in the **Operation** column.
  e. 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 CNAME record copied from WAF.
     - Keep other settings unchanged.

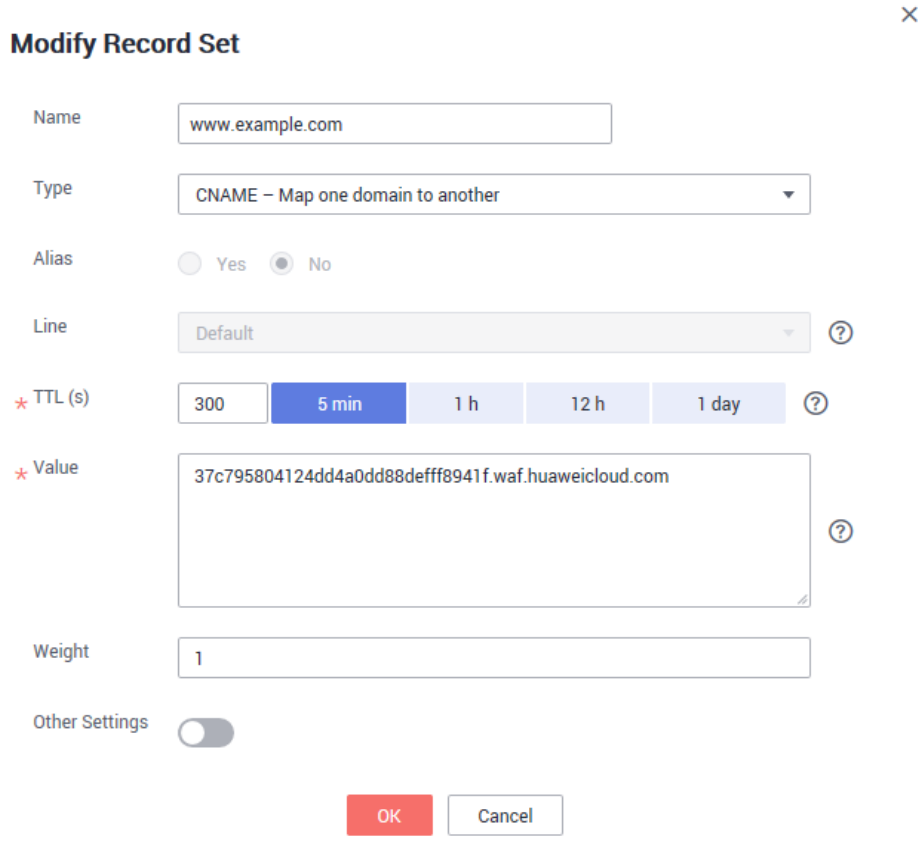
NOTE

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?**

Figure 8-20 Modify Record Set



f. Click **OK**.

- Proxy used

  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 **Subdomain Name** and **TXT Record**: In the row of **Access Status**, click **How to Access**. In the **Access Guide** dialog box, copy **Subdomain Name** and **TXT Record**.
2. Add **Subdomain Name** at the DNS provider and configure **TXT Record** for the subdomain name. For details about the configuration method, see **What Are Impacts If No Subdomain Name and TXT Record Are Configured?**

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

Step 8 Verify that the CNAME of the domain name has been configured.

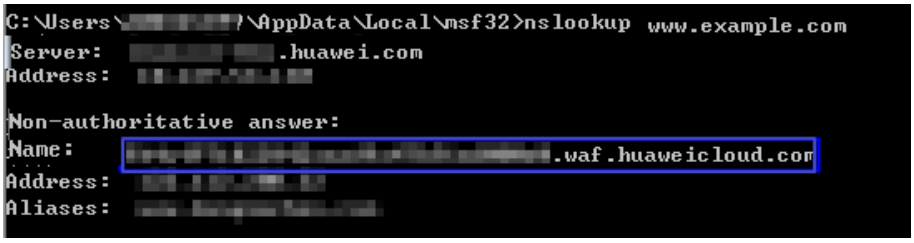
1. In Windows, choose **Start** > **Run**. Then enter **cmd** and press **Enter**.
2. Run a **nslookup** command to query the CNAME record.

   If the configured CNAME is returned, the configuration is successful. An example command response is displayed in **Figure 8-21**.

   Example command:

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

Figure 8-21 Querying the CNAME



----End

Follow-up Procedure

- If your server uses other network firewalls, disable these network firewalls or add the WAF IP address range to the IP address whitelist of these network firewalls. Otherwise, these firewalls may regard the WAF IP address as a malicious IP address. For details, see **How Do I Whitelist WAF IP Address Ranges?**
- If your web server is using personal security software, replace it with enterprise security software and whitelist the WAF IP address ranges.

Verification

- By default, WAF detects the **Access Status** of each protected domain name on an hourly basis.
- Generally, if you have performed domain connection and **Access Status** is **Accessible**, the domain name is connected to WAF.

Other Operations

- Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?
- What Are Impacts If No Subdomain Names or TXT Records Are Configured?

8.1.6 Configuration Example: Adding a Domain Name to WAF

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

- Example 1: Protecting Traffic to the Same Standard Port with Different Origin Server IP Addresses Assigned
- Example 2: Protecting Traffic to a Non-Standard Port with Different Origin Server IP Addresses Assigned
- Example 3: Protecting Different Service Ports
- Example 4: Configuring Protocols for Different Access Methods

Example 1: Protecting Traffic to the Same Standard Port with Different Origin Server IP Addresses Assigned

1. Select **Standard port** from the **Protected Port** drop-down list.
2. Select **HTTP** or **HTTPS** for **Client Protocol**. Figure 8-22 and Figure 8-23 show standard port configurations when the client protocol is HTTP or HTTPS.

Figure 8-22 Port 80

Figure 8-23 Port 443

NOTE

If **Client Protocol** is set to **HTTPS**, a certificate is required.

3. Your website visitors can access the website without adding a port to the end of the domain name. For example, enter **http://www.example.com** in the address box of the browser to access the website.

Example 2: Protecting Traffic to a Non-Standard Port with Different Origin Server IP Addresses Assigned

1. In the **Protected Port** drop-down list, select a non-standard port you want to protect.
2. Select **HTTP** or **HTTPS** for **Client Protocol** for all server ports. **Figure 8-24** and **Figure 8-25** show the configuration of non-standard HTTP or HTTPS port, respectively.

Figure 8-24 Other HTTP port besides port 80

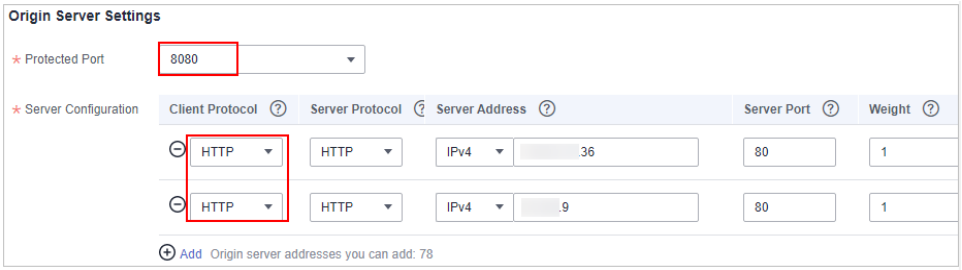
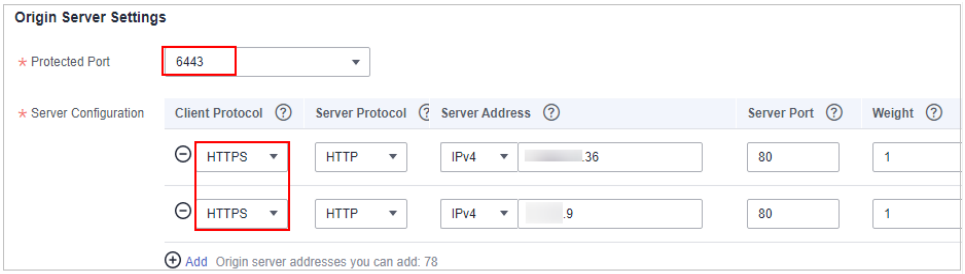


Figure 8-25 Other HTTPS port besides port 443



NOTE

If **Client Protocol** is set to **HTTPS**, a certificate is required.

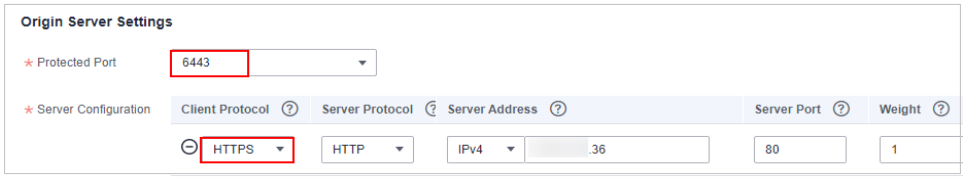
3. Visitors must add the configured non-standard port to the domain name when they access your website. Otherwise, error 404 is returned. If the non-standard port is 8080, enter *http://www.example.com:8080* in the address box of the browser.

Example 3: Protecting Different Service Ports

If the service ports to be protected are different, configure the ports separately. For example, to protect ports 8080 and 6443 for your site **www.example.com**, add the domain separately for each port, as shown in **Figure 8-26** and **Figure 8-27**.

Figure 8-26 Protecting port 8080

Figure 8-27 Protecting port 6443

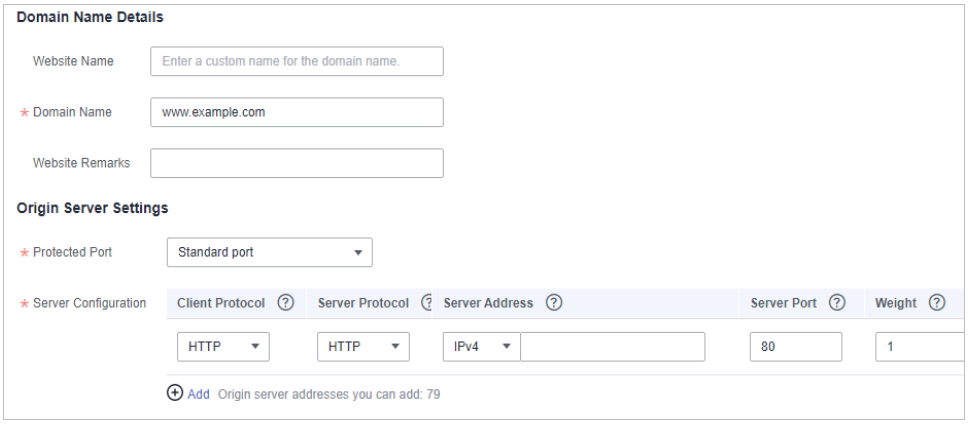


Example 4: Configuring Protocols for Different Access Methods

WAF provides various protocol types. If your website is www.example.com, WAF provides the following four access modes:

- HTTP mode

  Figure 8-28 HTTP mode

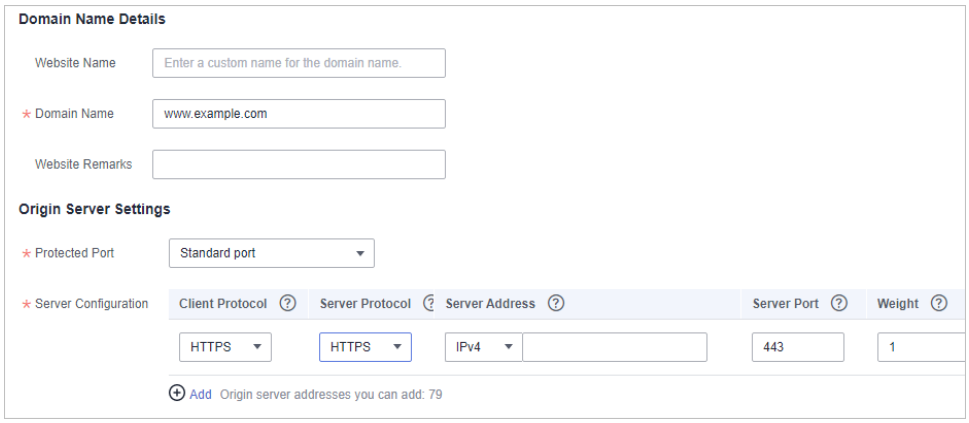


  NOTICE

  This configuration allows web visitors to access http://www.example.com over HTTP only. If they access it over HTTPS, they will receive the 302 Found code and be redirected to http://www.example.com.

- HTTPS method. This configuration allows web visitors to access your website over HTTPS only. If they access it over HTTP, they are redirected to the HTTPS URL.

Figure 8-29 HTTPS redirection

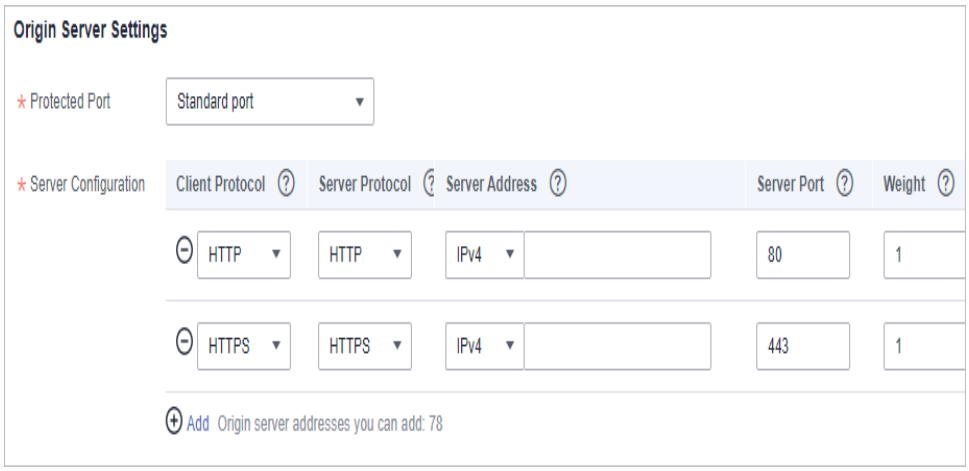


NOTICE

- If web visitors access your website over HTTPS, the website returns a successful response.
- If web visitors access http://www.example.com over HTTP, they will receive the 302 Found code and are directed to https://www.example.com.

- HTTP/HTTPS forwarding method

Figure 8-30 HTTP and HTTPS forwarding

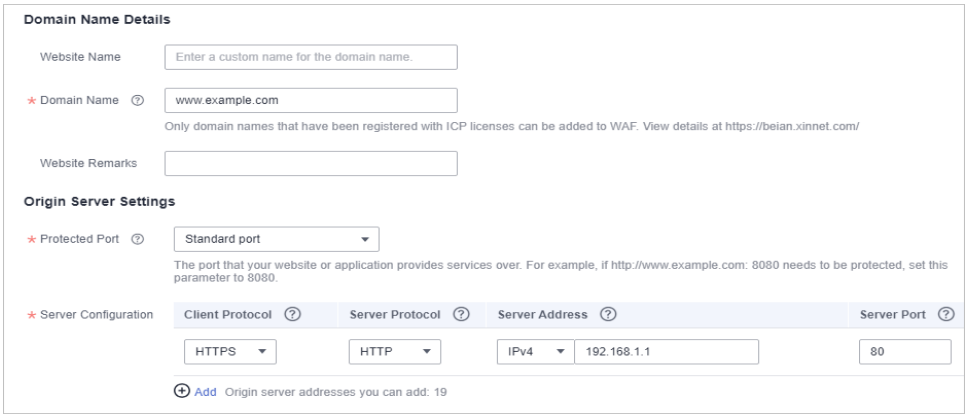


NOTICE

- If web visitors access your website over HTTP, the website returns a successful response but no communication between the browser and website is encrypted.
- If web visitors access your website over HTTPS, the website returns a successful response and all communications between the browser and website are encrypted.

- HTTPS offloading by WAF

Figure 8-31 HTTPS offloading



NOTICE

If web visitors access your website over HTTPS, WAF forwards the requests to your origin server over HTTP.

8.2 Adding a Website to WAF (Cloud Mode - ELB Access)

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

- In this method, WAF is integrated into the gateway of an ELB load balancer through an SDK module. WAF extracts traffic through the SDK module embedded in the gateway for inspection.
- WAF synchronizes the inspection result to the load balancer, and the load balancer determines whether to forward client requests to the origin server based on the inspection result.
- In this method, WAF does not forward traffic. This reduces compatibility and stability problems.

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.

Prerequisites

- You have purchased a cloud WAF instance.

  NOTE

  - To use ELB-access cloud WAF, you need to **submit a service ticket** to enable it for you first. ELB-access cloud WAF is available in some regions. For details, see **Functions**.
  - If you have purchased cloud WAF (standard, professional, or platinum edition), CNAME and ELB access methods share the domain name, bandwidth, and rule extension packages you have purchased.

- You have purchased a dedicated load balancer with **Specifications** set to **Application load balancing (HTTP/HTTPS)**. For more details, see **Creating a Dedicated Load Balancer**.

Constraints

Only dedicated load balancers with **Specifications** set to **Application load balancing (HTTP/HTTPS)** can be used. Dedicated load balancers with **Specifications** set to **Network load balancing (TCP/UDP)** are not supported.

Collecting Domain Name/IP Address Details

Before adding a domain name or IP address, obtain the information listed in **Table 8-8**.

Table 8-8 Domain name or IP address details required

Parameter	Description	Example Value
Domain Name/IP Address	• Domain name: used by visitors to access your website. A domain name consists of letters separated by dots (.). It is a human readable address that maps to the machine readable IP address of your server. • IP: IP address of the website.	www.example.com

Procedure

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 & Compliance**.

Step 4 In the upper left corner of the website list, click **Add Website**.

Step 5 Select **Cloud - Load balancer** and configure basic domain name information by referring to **Table 8-9**.

Figure 8-32 Configuring basic settings of a website

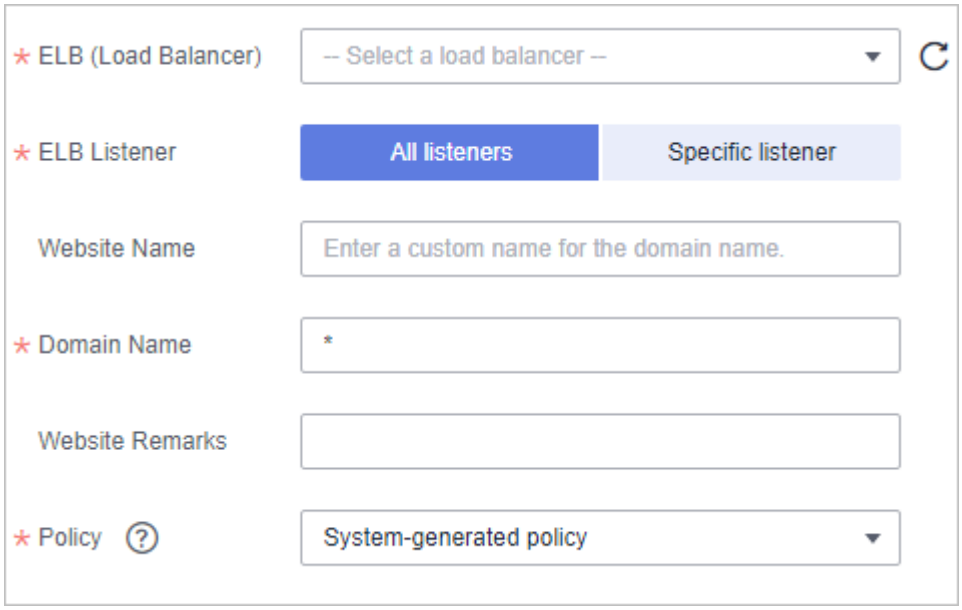


Table 8-9 Parameter description

Parameter	Description	Example Value
ELB (Load Balancer)	Select **ELB** in the drop-down list.	elb-waf-test
ELB Listener	• **All listeners** • **Specific listener**: Select a listener from the drop-down list.	All listeners
Website Name	Name of the website you want to protect	None

Parameter	Description	Example Value
Domain Name	The domain name of a website to be protected. It can be a single domain name or a wildcard domain name. ● Single domain name: Enter a single domain name, for example, www.example.com. ● Wildcard domain name **NOTE** WAF does not support wildcard domain names containing underscores (_). – 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.	Single domain name: **www.example.com** Wildcard domain name: ***.example.com** IP Address: XXX.XXX.1.1
Website Remarks	Brief description of the website	-
Policy	The **system-generated policy** is selected by default. You can select a policy you configured before. You can also customize rules after the domain name is connected to WAF. System-generated policies ● Basic web protection (**Log only** mode and common checks) The basic web protection defends against attacks such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections. ● Anti-crawler (**Log only** mode and **Scanner** feature) WAF only logs web scanning tasks, such as vulnerability scanning and virus scanning, such as crawling behavior of OpenVAS and Nmap. **NOTE** **Log only**: WAF only logs detected attack events instead of blocking them.	System-generated policy

Step 6 Click **OK**.

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

----End

Verification

The initial **Access Status** of a website is **Inaccessible**. If the access status of the website changes to **Accessible**, then the website is connected to WAF. When a request reaches the WAF instance for the website, the access status automatically changes to **Accessible**.

8.3 Connecting a Website to WAF (Dedicated Mode)

8.3.1 Connection Process (Dedicated Mode)

To let a dedicated WAF instance protect your website, the domain name of the website must be connected to the dedicated WAF instance so that the website incoming traffic can go to WAF first.

Constraints

- Dedicated WAF instances can protect only web applications and websites with servers deployed on Huawei Cloud and accessible through domain names or IP addresses. For details about WAF dedicated instances, see **Edition Differences**.
- A dedicated Elastic Load Balance (ELB) load balancer has been used to distribute workloads for the website you want to add to WAF. For details about load balancer types, see **Differences Between Dedicated and Shared Load Balancers**.

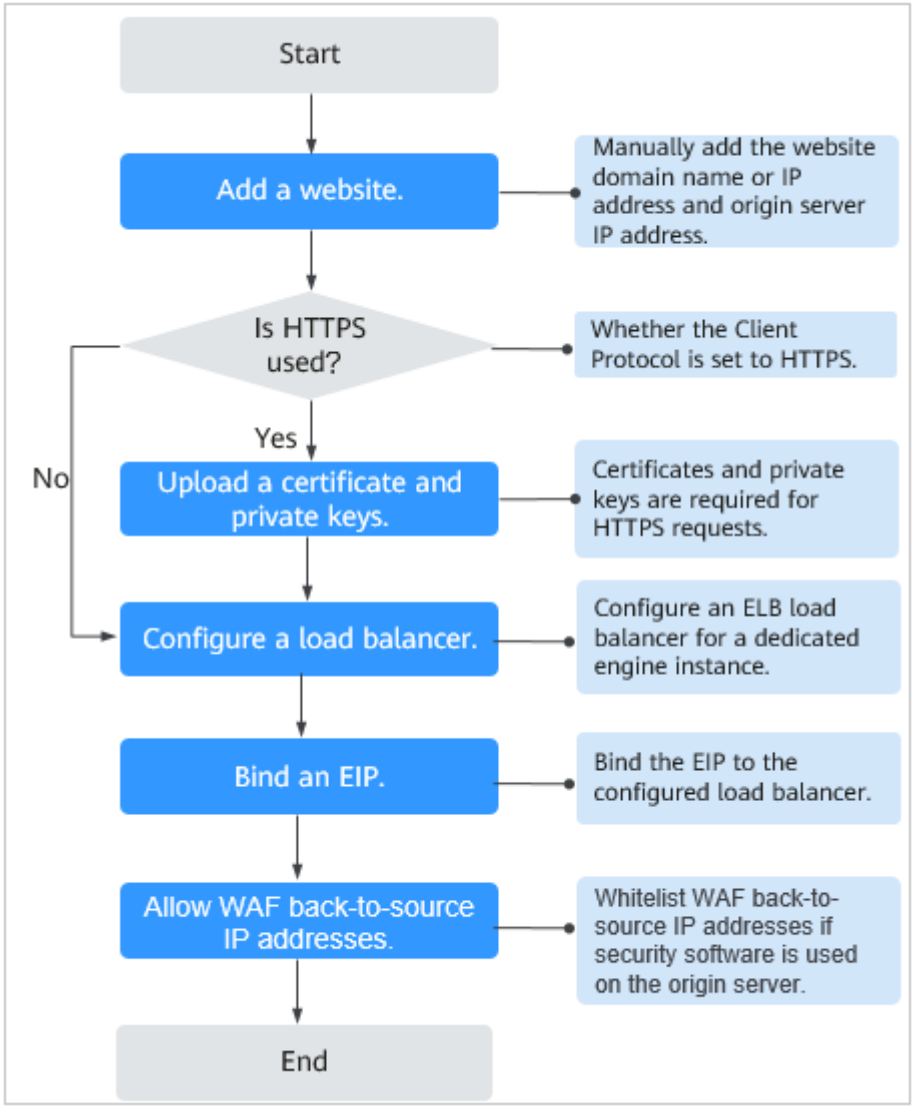
  NOTE

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

Processes of Connecting a Website to WAF

Before using a dedicated WAF instance, complete the required configurations by following the process shown in **Figure 8-33**.

Figure 8-33 Process of connecting a website to a dedicated WAF instance



Collecting Domain Name/IP Address Details

Before adding a domain name or IP address to WAF, obtain the information listed in **Table 8-10**.

Table 8-10 Domain name or IP address details required

Information	Parameter	Description	Example
Parameters	Protected Object	• Domain name: used by visitors to access your website. A domain name consists of letters separated by dots (.). It is a human readable address that maps to the machine readable IP address of your server. • IP: IP address of the website.	www.example.com
	Protected Port	The service port corresponding to the domain name of the website you want to protect. • Standard ports – 80: default port when the client protocol is HTTP – 443: default port when the client protocol is HTTPS • Non-standard ports Ports other than ports 80 and 443 **NOTICE** If your website uses a non-standard port, check whether the WAF edition you plan to buy can protect the non-standard port before you make a purchase. For details, see **Ports Supported by WAF**.	80
	Client Protocol	Protocol used by a client (for example, a browser) to access the website. WAF supports HTTP and HTTPS.	HTTP
	Server Protocol	Protocol used by WAF to forward requests from the client (such as a browser). The options are **HTTP** and **HTTPS**.	HTTP
	VPC	Select the VPC that the dedicated WAF instance belongs to.	vpc-default

Information	Parameter	Description	Example
	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.	192.168.1.1
(Optional) Certificate	Certificate Name	If you set **Client Protocol** to **HTTPS**, you are required to configure a certificate on WAF and associate the certificate with the domain name. **NOTICE** • Only .pem certificates can be used in WAF. If the certificate is not in PEM format, convert it into pem format by referring to **How Do I Convert a Certificate into PEM Format?** • Currently, certificates purchased in Huawei Cloud SCM can be pushed only to the **default** enterprise project. For other enterprise projects, SSL certificates pushed by SCM cannot be used.	-

Fixing Inaccessible Websites

If a domain name fails to be connected to WAF, its access status is **Inaccessible**. To fix this issue, see **Why Is the Access Status of a Domain Name or IP Address Inaccessible?**

8.3.2 Step 1: Add a 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.

Prerequisites

You have purchased a dedicated WAF instance.

Constraints

- A dedicated Elastic Load Balance (ELB) load balancer has been used to distribute workloads for the website you want to add to WAF. For details about load balancer types, see **Differences Between Dedicated and Shared Load Balancers**.

  NOTE

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

- 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. For details, see **Configuring Header Field Forwarding**.
- Certificate restrictions:
  - 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.
- If wildcard (*) is added to WAF, only non-standard ports other than 80 and 443 can be protected.

Procedure

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 & Compliance**.

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** and click **OK**.

Step 7 Provide the domain name details.

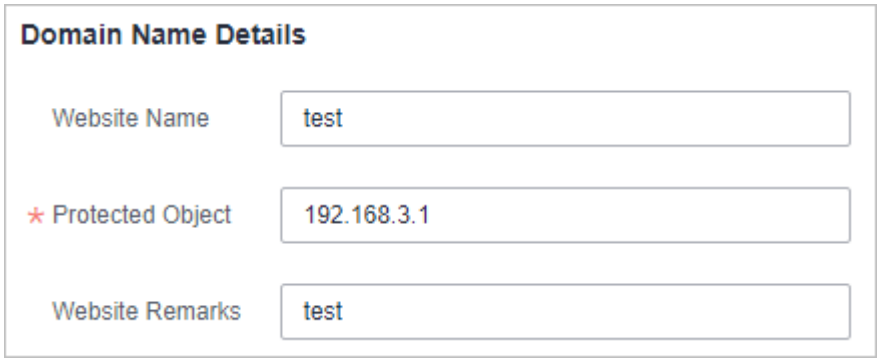
- **Website Name**: (Optional) You can customize the website name.
- **Protected Object**: Enter the domain name of a website you want WAF to protect. You can enter a single domain name or a wildcard domain name.

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 to be protected. 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.

- **Website Remarks**: (Optional) You can provide remarks about your website if you want.

Figure 8-34 Configuring domain name details



Step 8 Configure the origin server by referring to **Table 8-11**.

Figure 8-35 Origin Server Settings

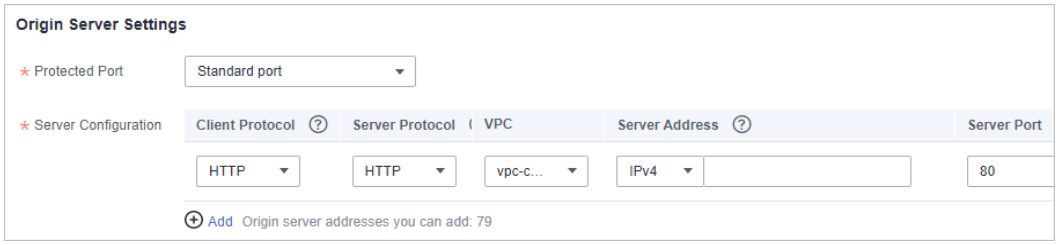


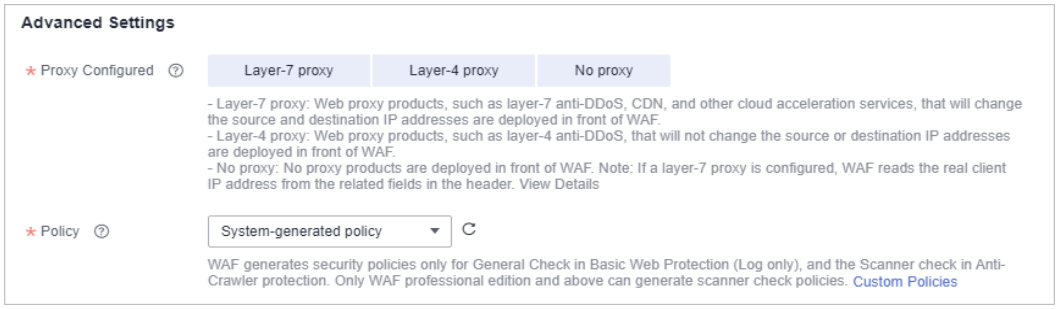
Table 8-11 Parameter description

Parameter	Description	Example Value
Protected Port	Select the port type that you want WAF to protect from the drop-down list. To protect port 80 or 443, select **Standard port** from the drop-down list. For details about ports supported by WAF, 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
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 used by WAF to forward client requests. The options are **HTTP** and **HTTPS**. • **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 purchased in the same VPC. • **Server Address**: private IP address of the website server. Log in to the ECS or ELB console and view the private IP address of the server in the instance list. **NOTE** The origin server address cannot be the same as that of the protected object. The following IP address formats are supported: – IPv4, for example, XX.XXX.1.1 – IPv6, for example, fe80:0000:0000:0000:0000:0000:0000:0000 • **Server Port**: service port of the server to which the dedicated WAF instance forwards client requests.	**Client Protocol**: **HTTP** **Server Protocol**: **HTTP** **Server Address**: XXX.XXX.1.1 **Server Port**: **80**

Parameter	Description	Example Value
Certificate Name	If you set **Client Protocol** to **HTTPS**, an SSL certificate is required. You can select an existing certificate or import an external certificate. For details about how to import a certificate, see **Importing a New Certificate**. The newly imported certificates will be listed on the **Certificates** page. For more details, see **Uploading a Certificate**. Alternatively, you can buy a certificate on the CCM console and push it to WAF. For details about how to push an SSL certificate in CCM to WAF, see **Pushing an SSL Certificate to Other Cloud Services**. **NOTICE** • Only .pem certificates can be used in WAF. If the certificate is not in .pem format, convert it into .pem by referring to **Importing a New Certificate** before uploading the certificate. • Currently, certificates purchased in Huawei Cloud SCM can be pushed only to the **default** enterprise project. For other enterprise projects, SSL certificates pushed by SCM cannot be used. • If your website certificate is about to expire, purchase a new certificate before the expiration date and update the certificate associated with the website in WAF. • 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.	--

Step 9 Configure the advanced settings.

Figure 8-36 Advanced settings



- Configure **Proxy Configured**.

- **Layer-7 proxy**: Web proxy products, such as layer-7 anti-DDoS, CDN, and other cloud acceleration services, that will change the source and destination IP addresses are deployed in front of WAF.
- **Layer-4 proxy**: Web proxy products, such as layer-4 anti-DDoS, that will not change the source or destination IP addresses are deployed in front of WAF.
- **No proxy**: No proxy products are deployed in front of WAF.

NOTICE

If you select **layer-7 proxy**, WAF obtains the real access IP address of the visit from the configured header field. For details, see **Configuring Header Field Forwarding**.

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

  System-generated policies include:

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

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

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

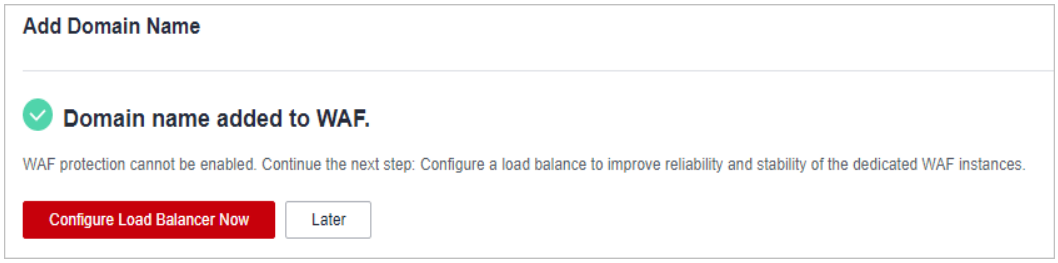
  NOTE

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

Step 10 Click **OK**.

To enable WAF protection, there are still several steps, including configuring a load balancer, binding an EIP to the load balancer, and whitelisting WAF IP addresses. 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 WAF**, **Step 3: Bind an EIP to a Load Balancer**, and **Step 4: Whitelist IP Addresses of Dedicated WAF Instances**.

Figure 8-37 Domain name added to WAF.



----End

Verification

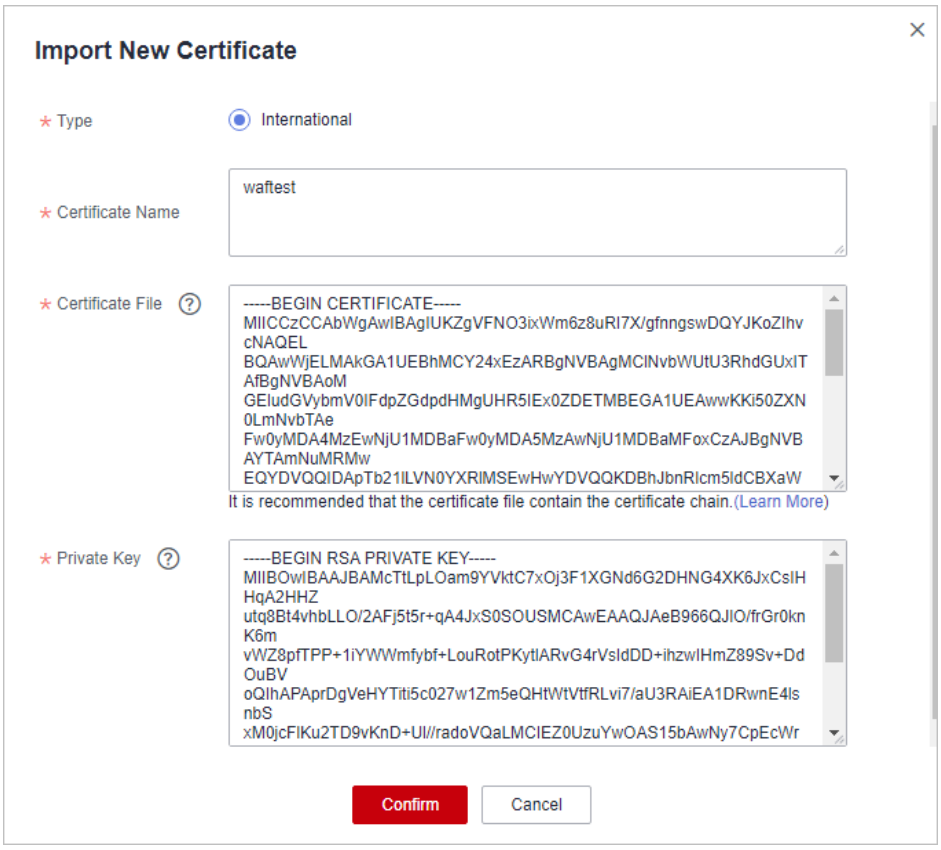
The initial **Access Status** of a website is **Inaccessible**. After you configure a load balancer and bind an EIP to the load balancer for your website, when a request reaches the WAF dedicated instance, the access status automatically changes to **Accessible**.

Importing a New Certificate

If you set **Client Protocol** to **HTTPS**, an SSL certificate is required. You can perform the following steps to import a new certificate.

1. Click **Import New Certificate**. 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 8-38 Import New Certificate



NOTE

WAF encrypts and saves the private key to keep it safe.

Only .pem certificates can be used in WAF. If the certificate is not in .pem format, convert it into .pem locally by referring to **Table 8-12** before uploading it.

Table 8-12 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.

2. Click **Confirm**.

8.3.3 Step 2: Configure a Load Balancer for WAF

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**.

Prerequisites

- You have added a website to 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). For details, see **Dedicated Engine Version Iteration**.

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

  You can configure your security group as follows:

  – Inbound rules

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

  – Outbound rules

    Retain the default settings. All outgoing network traffic is allowed by default.

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

Constraints

- If **Health Check** is configured, the health check result of the dedicated instance must be **Normal**, or the website requests cannot be pointed to WAF. For details about health check, see **How Do I Troubleshoot an Unhealthy Backend Server?**
- The backend port for the listener must be the same as the service port protected by the dedicated WAF instance, which is the protection port set in **Step 1: Add a Website to WAF (Dedicated Mode)**.
- WAF works as a layer-7 proxy. When configuring a listener, you can only select HTTP or HTTPS as the frontend protocol.

Impact on the System

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.

Adding a Listener

If **Health Check** is configured, the health check result of the dedicated instance must be **Healthy**, or the website requests cannot be pointed 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.

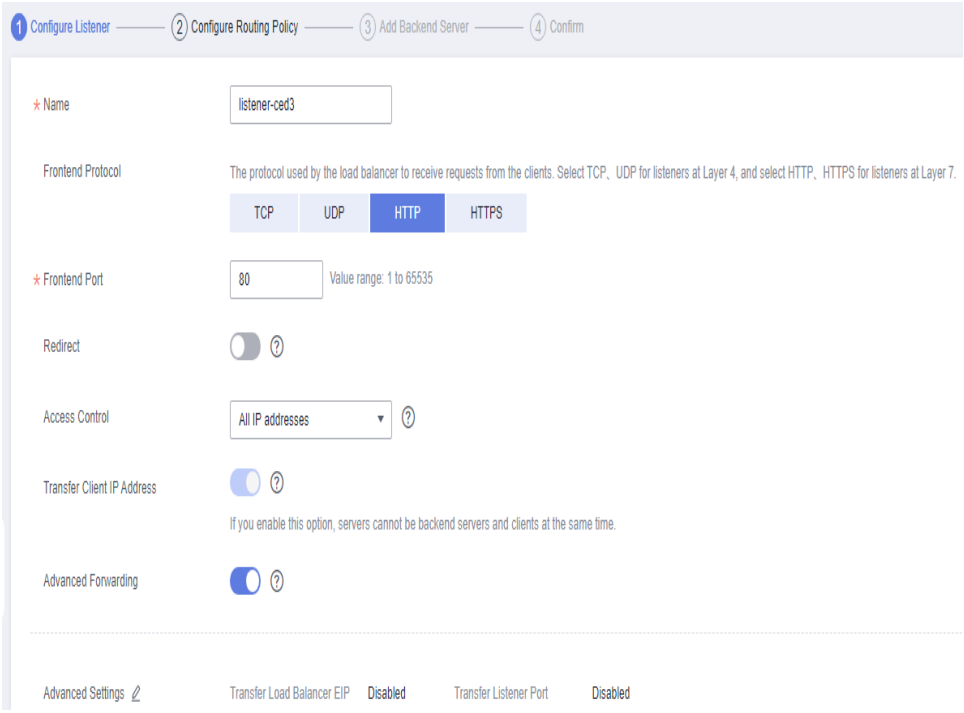
Step 3 Click ☰ in the upper left corner of the page and choose **Elastic Load Balance** under **Network** to go to the **Load Balancers** page.

Step 4 Click the name of the load balancer you want in the **Name** column to go to the **Listeners** page.

Step 5 Then, click **Add Listener** and configure the listener information.

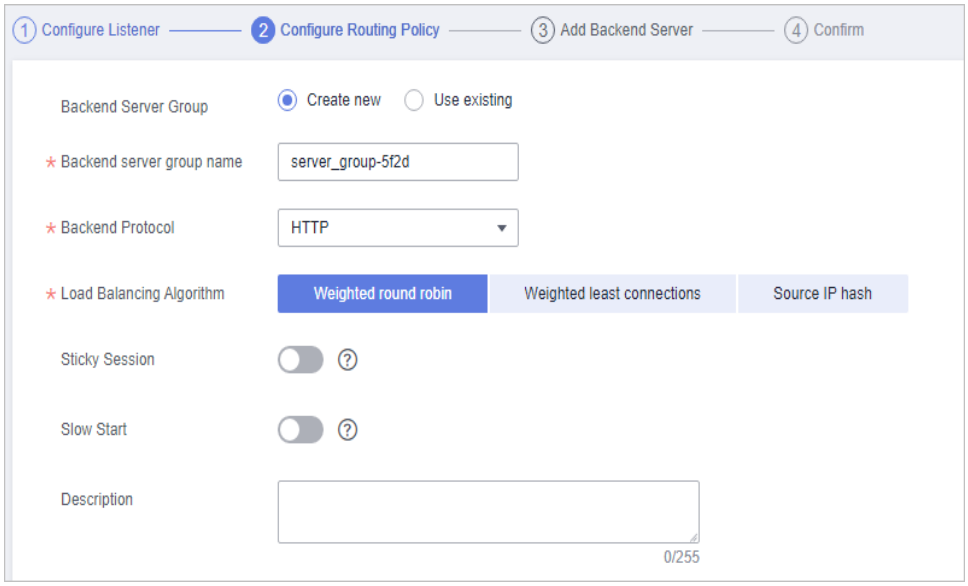
- **Frontend Port**: Set it to the origin server port configured in WAF.
- **Frontend Protocol**: Select HTTP or HTTPS.

Figure 8-39 Configuring a listener



Step 6 Click **Next: Configure Request Routing Policy**.

Figure 8-40 Configuring a backend server group



NOTICE

- 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.
- For details about ELB traffic distribution policies, see **Load Balancing Algorithms**.

Step 7 Click **Next: Add Backend Server** and configure a health check.

NOTICE

- 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 8 Click **Next: Confirm**.

Step 9 Click **Submit**.

----End

Adding WAF Instances to an ELB Load Balancer

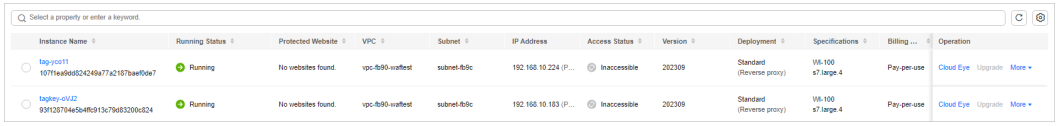
Step 1 **Log in to the management console**.

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

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

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

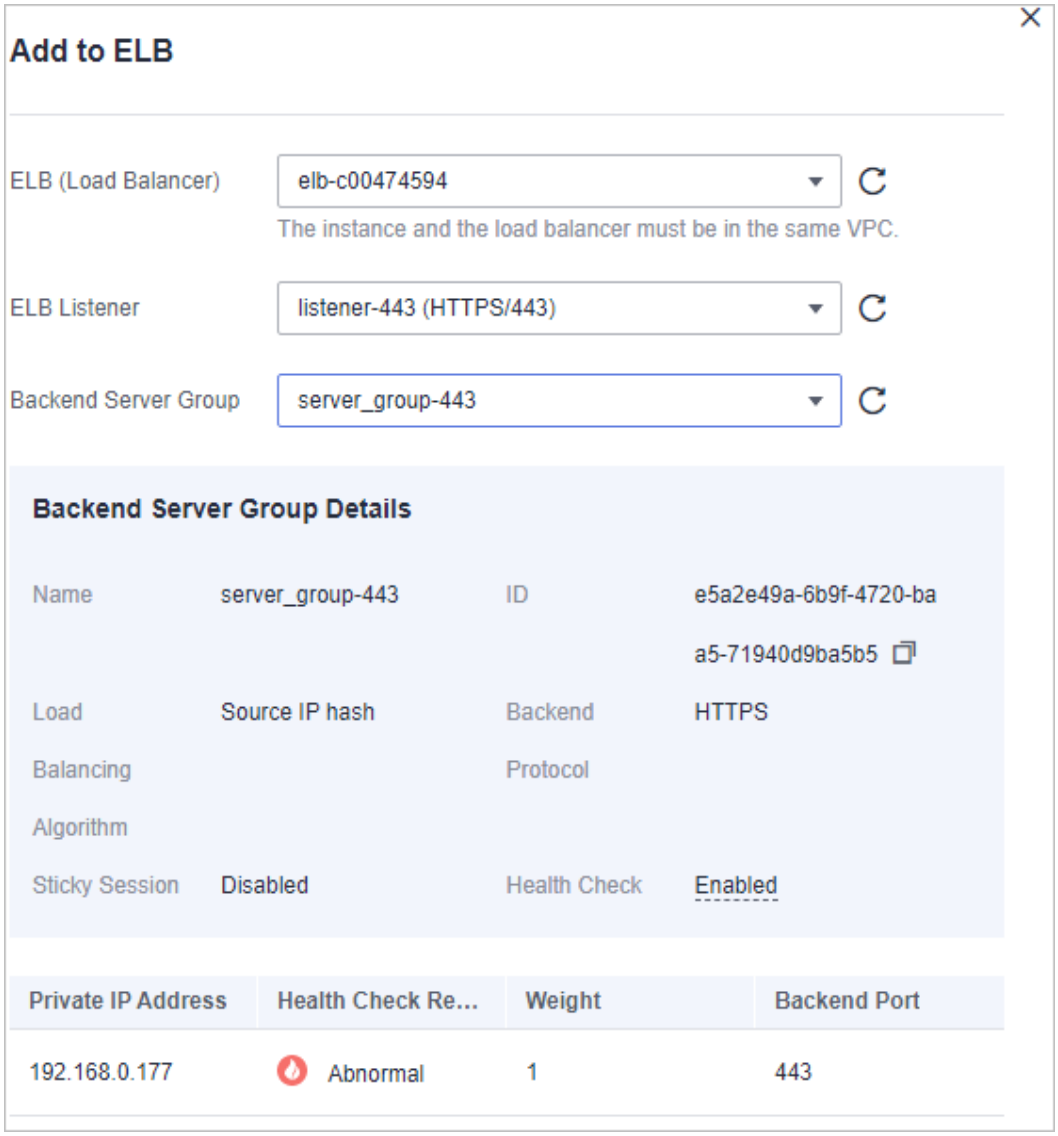
Figure 8-41 Dedicated engine list



Step 5 In the row containing the instance you want to upgrade, click **More** > **Add to ELB** in the **Operation** column.

Step 6 In the **Add to ELB** dialog box, specify **ELB (Load Balancer)**, **ELB Listener**, and **Backend Server Group** based on **Adding a Listener**.

Figure 8-42 Add to ELB

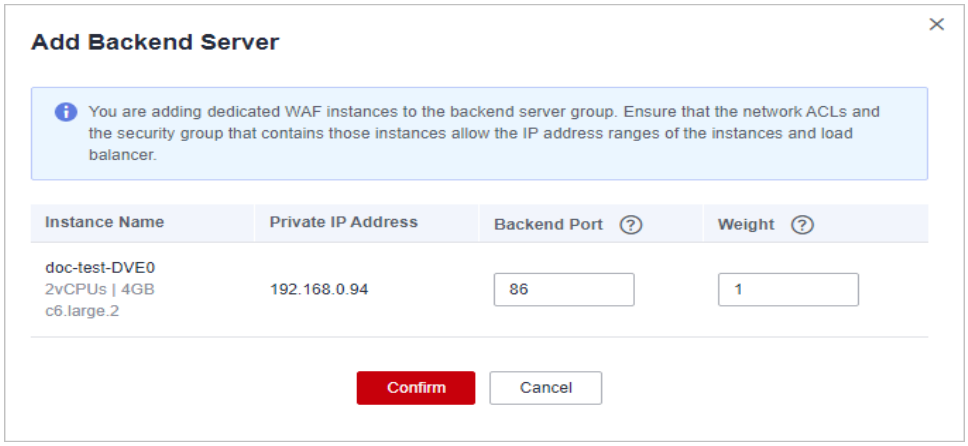


NOTICE

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

Step 7 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 (Dedicated Mode)**.

Figure 8-43 Configuring Backend Port



----End

Verification

If the **Health Check Result** is **Healthy**, the load balancer is configured.

8.3.4 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.

Prerequisites

You have configured **a load balancer** for a dedicated WAF instance.

Procedure

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 **Elastic Load Balance** under **Network** to go to the ELB console.

Step 4 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 8-44 Unbinding an EIP

Step 5 In the displayed dialog box, click **Yes**.

Step 6 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 7 In the displayed dialog box, select the EIP unbound in **Step 4** and click **OK**.

----End

8.3.5 Step 4: Whitelist IP Addresses of Dedicated WAF Instances

To let your dedicated WAF instances take effect, configure ACL rules on the origin server to trust only the back-to-source IP addresses of all your dedicated WAF instances. This prevents hackers from attacking the origin server through the server IP addresses.

NOTICE

ACL rules must be configured on the origin server to whitelist WAF back-to-source IP addresses. Otherwise, your website visitors will frequently receive 502 or 504 error code after your website is connected to WAF.

Why Do I Need to Whitelist the WAF Back-to-Source IP Addresses?

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.

Prerequisites

Your website has been connected to your dedicated WAF instances.

NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and whitelist back-to-source IP addresses of your dedicated WAF instances in the project.

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 **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 left upper corner and choose **Security & Compliance** > **Web Application Firewall** to go to the **Dashboard** page.

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

Figure 8-45 Dedicated engine list

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 **Compute** > **Elastic Cloud Server**.

Step 7 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 8 Click the **Security Groups** tab. Then, click **Change Security Group**.

Step 9 In the **Change Security Group** dialog box displayed, select a security group or create a security group and click **OK**.

Step 10 Click the security group ID and view the details.

Step 11 Click the **Inbound Rules** tab and click **Add Rule**. Then, specify parameters in the **Add Inbound Rule** dialog box. For details, see **Table 8-13**.

Figure 8-46 Add Inbound Rule

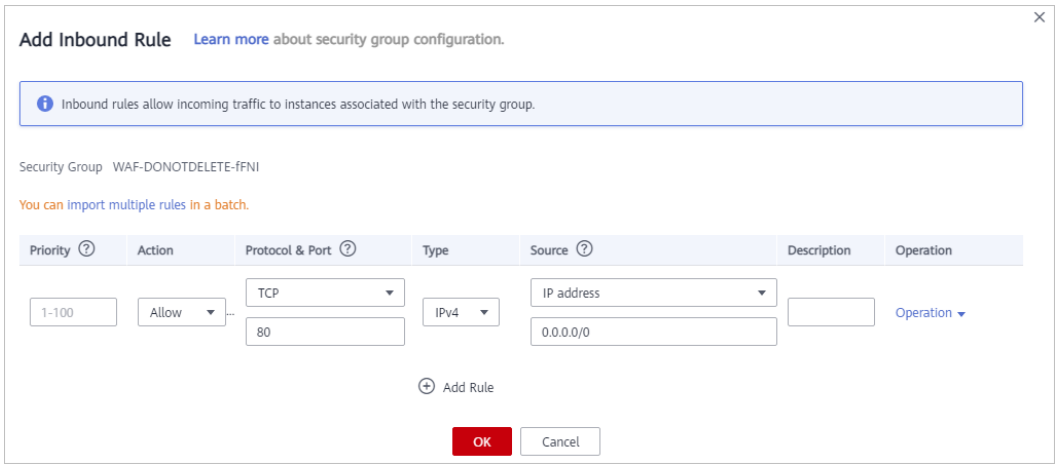


Table 8-13 Inbound rule parameters

Parameter	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.
Source	Subnet IP address of each dedicated WAF instance you obtain in **Step 5**. Configure an inbound rule for each IP address. **NOTE** An 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 12 Click **OK**.

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

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

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

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

----End

Pointing Traffic to a Load Balancer

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

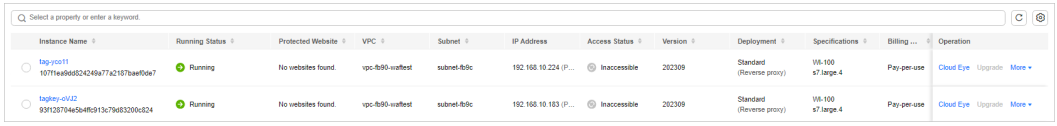
Step 1 Log in to the management console.

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

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

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

Figure 8-47 Dedicated engine list



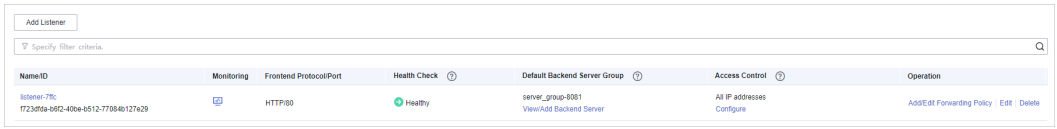
Step 5 In the **IP Address** column, obtain the IP address of each dedicated WAF instance under your account.

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 8-48 Listener list



Step 9 In the displayed dialog box, select **Whitelist** for **Access Control**.

1. Click **Create IP Address Group** and add the dedicated WAF instance 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

8.3.6 Step 5: Test Dedicated WAF Instances

To ensure that WAF can forward your website requests normally, test WAF locally after you add a website to WAF.

Prerequisites

You have performed operations in **Step 1: Add a Website to WAF (Dedicated Mode)** to **Step 4: Whitelist IP Addresses of Dedicated WAF Instances**.

(Optional) Testing a Dedicated WAF Instance

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

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

- Forwarding test

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

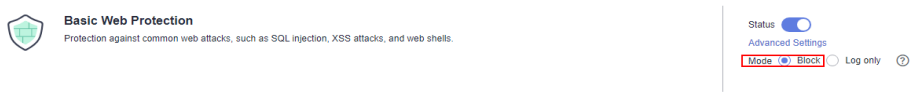
  For example:

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

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

- Attack blocking test

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

  b. Run the following command:

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

  Example:

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

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

----End

Testing the Dedicated WAF Instance and Dedicated ELB Load Balancer

- Forwarding test

  ```
  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:

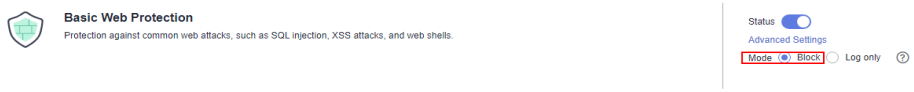
  ```
  curl -kv -H "Host: a.example.com" http://192.168.X.Y
  curl -kv -H "Host: a.example.com" http://100.10.X.X
  ```

  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.

  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.

8.4 Advanced Settings

8.4.1 Configuring PCI DSS/3DS Certification Check and TLS Version

Transport Layer Security (TLS) provides confidentiality and ensures data integrity for data sent between applications over the Internet. HTTPS is a network protocol constructed based on TLS and HTTP and can be used for encrypted transmission and identity authentication. If you select **Cloud** or **Dedicated** for **Protection** and set **Client Protocol** to **HTTPS**, set the minimum TLS version and cipher suite (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

- You have selected **Cloud - CNAME** or **Dedicated** for protection when adding the website to WAF.
- Your website uses HTTPS as the client protocol.

Constraints

- If **Client Protocol** for the website you want to protect is set to **HTTP**, TLS is not required, and you can skip this topic.
- If you configure multiple combinations of server information, PCI DSS and PCI 3DS compliance certification checks can be set only when **Client Protocol** is set to **HTTPS** in all of those combinations.

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 8-14** lists the recommended minimum TLS versions for different scenarios.

Table 8-14 Recommended minimum TLS versions

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.

Scenario	Minimum TLS Version (Recommended)	Protection Effect
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.

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 8-15**.

NOTE

The cipher suites whose configuration value starts with **!** are not supported. For example, !MD5 indicates that the MD5 algorithm is not supported.

Table 8-15 Description of cipher suites

Cipher Suite Name	Cipher Suite Configuration Value	Description
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 Name	Cipher Suite Configuration Value	Description
Cipher suite 1	• ECDHE-ECDSA-AES256-GCM-SHA384 • HIGH • !MEDIUM • !LOW • !aNULL • !eNULL • !DES • !MD5 • !PSK • !RC4 • !kRSA • !SRP • !3DES • !DSS • !EXP • !CAMELLIA • @STRENGTH	Recommended configuration. • Compatibility: Good. A wide range of browsers are supported. • Security: Good
Cipher suite 2	• EECDH+AESGCM • EDH+AESGCM	• Compatibility: Average. Strict compliance with forward secrecy requirements of PCI DSS and excellent protection, but browsers of earlier versions may be unable to access the website. • Security: Excellent

Cipher Suite Name	Cipher Suite Configuration Value	Description
Cipher suite 3	• ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-SHA384 • RC4 • HIGH • !MD5 • !aNULL • !eNULL • !NULL • !DH • !EDH	• Compatibility: Average. Earlier versions of browsers may be unable to access the website. • Security: Excellent. Multiple algorithms, such as ECDHE, DHE-GCM, and RSA-AES-GCM, are supported.
Cipher suite 4	• ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • AES256-SHA256 • RC4 • HIGH • !MD5 • !aNULL • !eNULL • !NULL • !EDH	• Compatibility: Good. A wide range of browsers are supported. • Security: Average. The GCM algorithm is supported.

Cipher Suite Name	Cipher Suite Configuration Value	Description
Cipher suite 5	• AES128-SHA:AES256-SHA • AES128-SHA256:AES256-SHA256 • HIGH • !MEDIUM • !LOW • !aNULL • !eNULL • !EXPORT • !DES • !MD5 • !PSK • !RC4 • !DHE • @STRENGTH	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 8-16** 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 8-16 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
Google Chrome 63 /macOS High Sierra 10.13.2	Not compatible	Compatible	Compatible	Compatible	Not compatible
Google Chrome 49/ Windows XP SP3	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
Internet Explorer 6 /Windows XP	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
Safari 6/iOS 6.0.1	Compatible	Compatible	Not compatible	Compatible	Compatible
Safari 7/iOS 7.1	Compatible	Compatible	Not compatible	Compatible	Compatible
Safari 7/OS X 10.9	Compatible	Compatible	Not compatible	Compatible	Compatible
Safari 8/iOS 8.4	Compatible	Compatible	Not compatible	Compatible	Compatible
Safari 8/OS X 10.10	Compatible	Compatible	Not compatible	Compatible	Compatible
Internet Explorer 7/Windows Vista	Compatible	Compatible	Not compatible	Compatible	Compatible
Internet Explorer 8, 9, or 10 /Windows 7	Compatible	Compatible	Not compatible	Compatible	Compatible
Internet Explorer 10 /Windows Phone 8.0	Compatible	Compatible	Not compatible	Compatible	Compatible

Browser/Client	Default Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4
Java 7u25	Compatible	Compatible	Not compatible	Compatible	Compatible
OpenSSL 0.9.8y	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
Safari 6.0.4/OS X 10.8.4	Compatible	Compatible	Not compatible	Compatible	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.

Procedure

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.

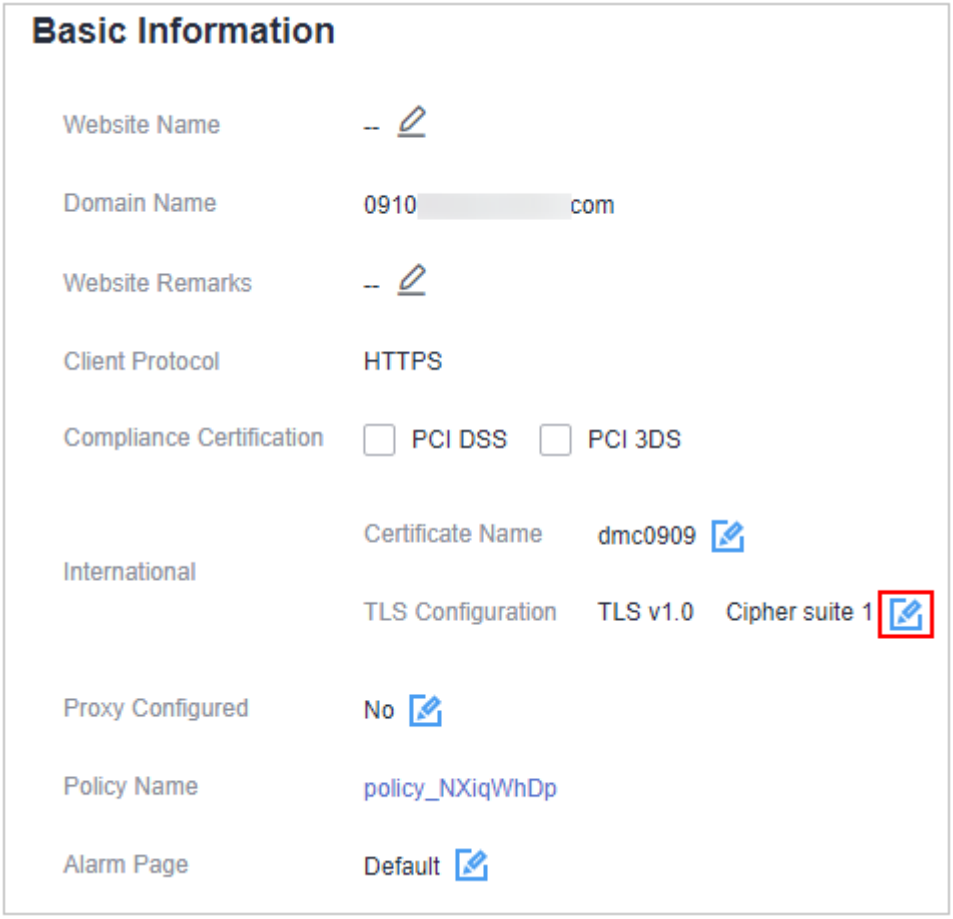
Step 3 Click in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.

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

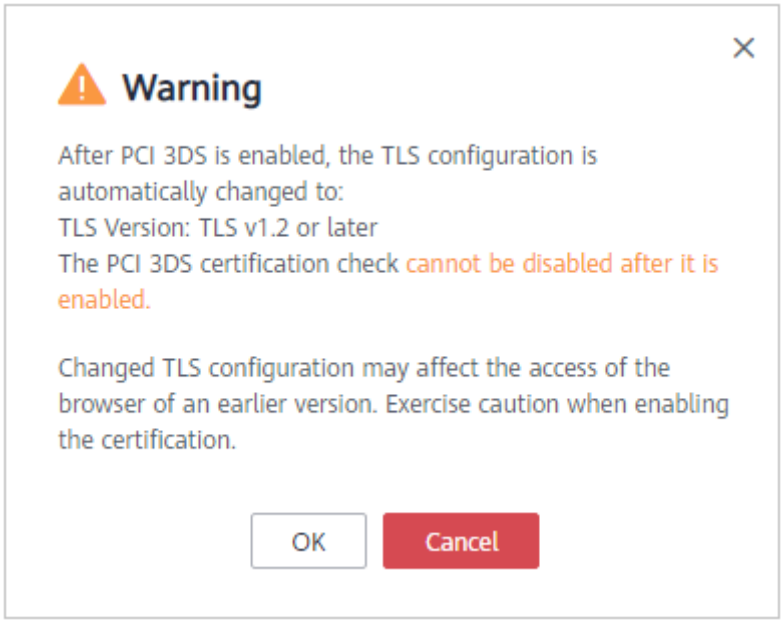
Step 5 In the **Domain Name** column, click the domain name of the website to go to the basic information page.

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 8-49 TLS configuration modification



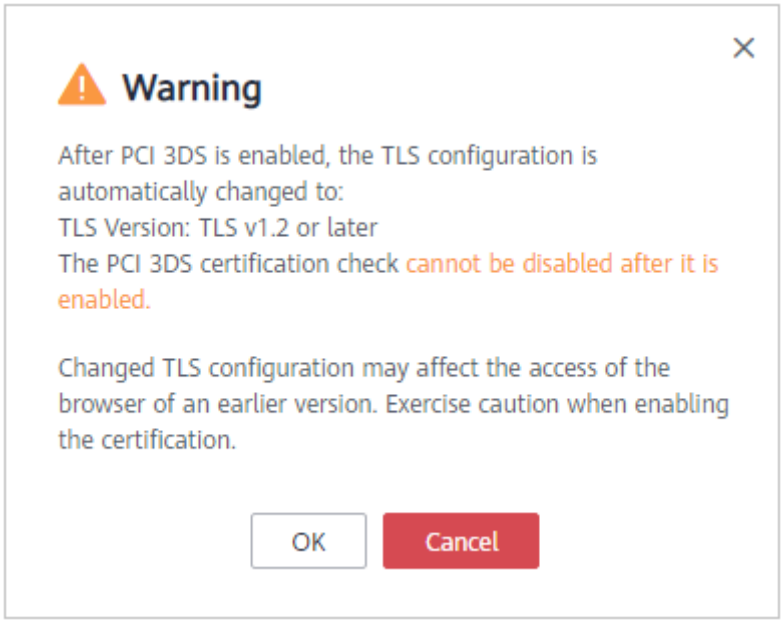
- Select **PCI DSS**. In the displayed **Warning** dialog box, click **OK** to enable the PCI DSS certification check.



NOTICE

If PCI DSS certification check is enabled, the minimum TLS version and cypher suite cannot be changed.

- Select **PCI 3DS**. In the displayed **Warning** dialog box, click **OK** to enable the PCI 3DS certification check.

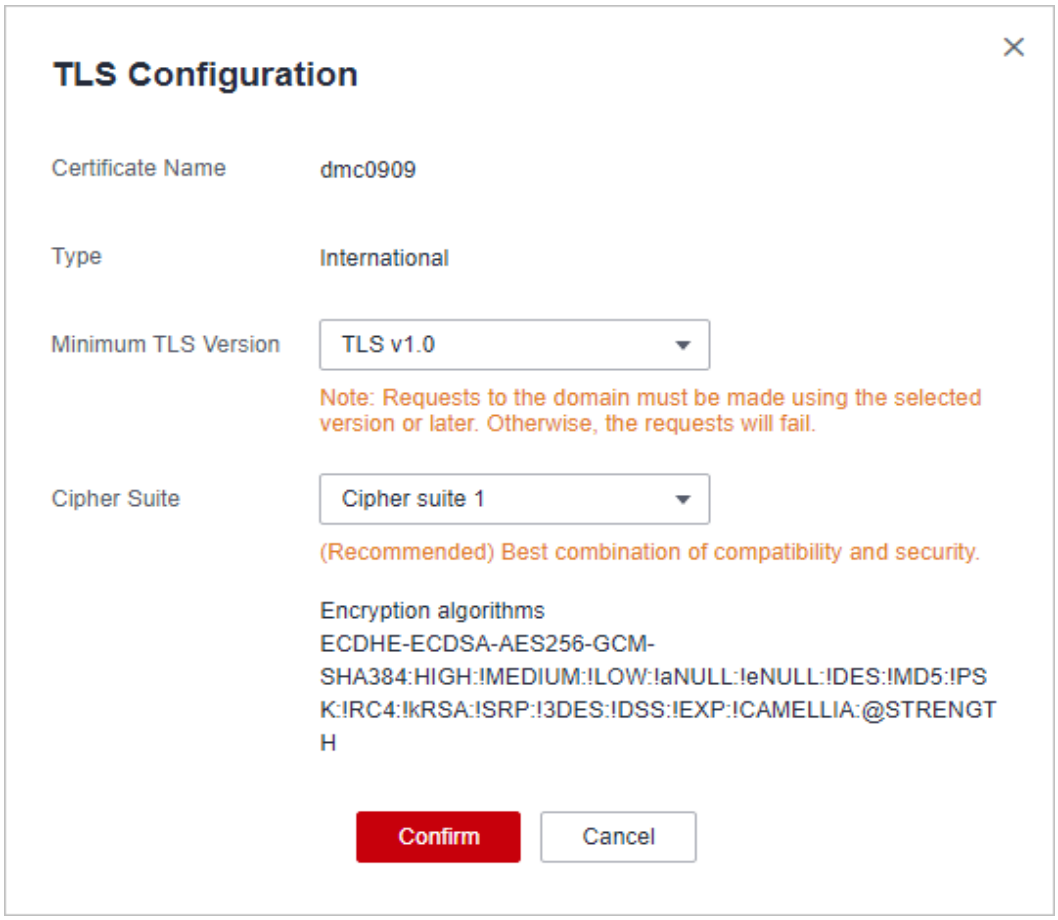


NOTICE

- If PCI 3DS certification check is enabled, the minimum TLS version cannot be changed.
- Once enabled, the PCI 3DS certification check cannot be disabled.

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

Figure 8-50 TLS Configuration



Select the minimum TLS version you need. The options are as follows:

- **TLS v1.0**: the default version. Requests using TLS v1.0 or later can access the domain name.
- **TLS v1.1**: Only requests using TLS v1.1 or later can access the domain name.
- **TLS v1.2**: Only requests using TLS v1.2 or later can access the domain name.

Step 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.

8.4.2 Enabling WAF IPv6 Protection

If your website requires IPv6 protection, you can enable IPv6 protection. After IPv6 protection is enabled, WAF assigns an IPv6 address to the domain name and uses the IPv6 address to access the origin server. WAF adds IPv6 address resolution in CNAME record sets by default. IPv6 access requests are forwarded to WAF first. WAF detects and filters out malicious attack traffic, and returns normal traffic to the origin server to ensure that the origin server is secure, stable, and available.

- If the origin server address of the protected website is an IPv6 address, IPv6 protection is enabled by default.
- If the origin server address of the protected website is set to an IPv4 address, after you manually enable IPv6 protection, WAF uses the NAT64 mechanism to translate the IPv4 website into an IPv6 website. In this way, requests to the IPv6 address are checked and routed by WAF to the origin server. NAT64 is a network address translation (NAT) mechanism that enables communications between IPv6 and IPv4 servers.

Prerequisites

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

Constraints

- You have selected **Cloud - CNAME** for your website deployment.
- Only the professional and platinum editions support IPv6 protection.
- For details about the regions that support IPv6 protection, see **Features**.
- If the origin server uses IPv6 addresses, IPv6 protection is enabled by default. To prevent IPv6 service from interruption, keep the IPv6 protection enabled. If IPv6 protection is not needed, edit the server configuration and delete IPv6 configuration from the origin server first. For details, see **Editing Server Information**.

Procedure

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 & Compliance**.

Step 4 In the navigation pane, 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 **IPv6 Protection** row, click  . In the dialog box displayed, select **Enable** and click **OK**.

----End

8.4.3 Enabling the HTTP/2 Protocol

If your website is accessible over the HTTP/2 protocol, enable HTTP/2 in WAF. The HTTP/2 protocol can be used only for access between the client and WAF on the condition that at least one origin server has **HTTPS** used for **Client Protocol**.

Prerequisites

- The website you want to protect has been added to WAF.
- You have selected **HTTPS** for **Client Protocol** for at least one piece of server configuration.

Constraints

- You have selected **Cloud - CNAME** for your website deployment.
- Only the professional and platinum editions support HTTP/2.
- For details about the regions that support HTTP/2, see **Functions**.

Procedure

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 & Compliance**.

Step 4 In the navigation pane, 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 **HTTP/2 Used** row, click . Then, select **Yes** and click **OK**.

----End

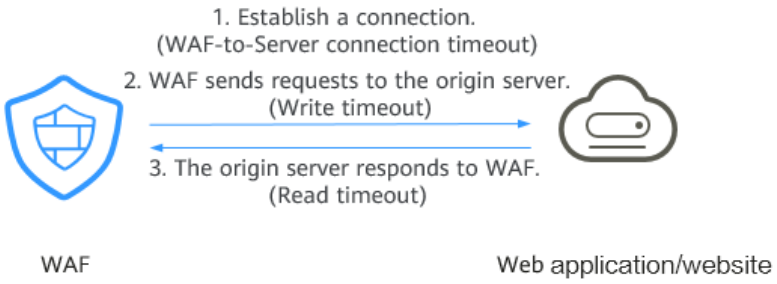
8.4.4 Configuring a Timeout for Connections Between WAF and a Website Server

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 8-51 shows the three steps for WAF to forward requests to an origin server.

Figure 8-51 WAF forwarding requests to origin servers.



NOTE

- The timeout for connections from a browser to WAF is 120 seconds. The value varies depending on your browser settings and cannot be changed on the WAF console.
- The default timeout for connections between WAF and your origin server is 30 seconds. You can customize this timeout. If you are using a dedicated WAF instance or professional or platinum edition cloud WAF instance, you can configure connection timeout, read timeout, and write timeout.
- For more constraints, see **Constraints**.

Prerequisites

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

Constraints

- You have selected **Cloud - CNAME** or **Dedicated** for protection when adding the website to WAF.
- In cloud mode, only the professional and platinum editions support custom connection timeouts.
- The timeout duration for connections between a browser and WAF cannot be modified. Only timeout duration for connections between WAF and your origin server can be modified.
- This function cannot be disabled once it is enabled.
- For details about regions where you can configure a connection timeout, see **Functions**.

Procedure

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 & Compliance**.

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

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

Step 6 In the **Timeout Settings** row, click the **Status** toggle and enable it if needed.

Step 7 Click , specify **WAF-to-Server connection timeout (s)**, **Read timeout (s)**, and **Write timeout (s)**, and click to save settings.

----End

8.4.5 Enabling Break Protection

If a large number of 502 Bad Gateway and 504 Gateway Timeout errors are detected, you can enable WAF breakdown protection and connection protection to let WAF suspend your website and protect your origin servers from being crashed. When the 502/504 error requests and pending URL requests reach the thresholds you configure, WAF enables corresponding protection for your website.

Prerequisites

- The website you want to protect has been added to WAF.
- You have upgraded the dedicated WAF instance to the latest version. For details, see **Upgrading a Dedicated WAF Instance**.

Constraints

- You have selected **Dedicated mode** for your website deployment.
- Before enabling **Break Protection**, make sure **you have updated dedicated WAF instances to the latest version,**, or your services might be affected.
- Connection Protection is available in some regions. For details, see **Functions**.

Procedure

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 & Compliance**.

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

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

Step 6 In the **Break Protection** area, click the status icon to toggle it on.

Figure 8-52 Break Protection

Step 7 Click next to each parameter, edit **Breakdown Protection** and **Connection Protection** parameters to meet your requirements, and click to save settings. Table 8-17 describes these parameters.

Table 8-17 Connection Protection parameters

Parameter		Description	Example Value
Breakdown Protection	502/504 Error Threshold	30s 502/504 Error Threshold	1000
	502/504 Error Percentage (%)	A breakdown is triggered when the 502/504 error threshold and percentage threshold have been reached.	90
	Initial Downtime (s)	Protection period upon the first breakdown. During this period, WAF stops forwarding client requests.	180

Parameter		Description	Example Value
	Multiplier for Consecutive Breakdowns	The maximum multiplier you can use for consecutive breakdowns. The number of breakdowns are counted from 0 every time the accumulated breakdown protection duration reaches 3,600s. For example, assume that **Initial Downtime (s)** is set to 180s and **Multiplier for Consecutive Breakdowns** is set to 3. ● If the breakdown is triggered for the second time, that is, less than 3, the protection duration is 360s (180s x 2). ● If the breakdown is triggered for the third or fourth time, that is, equal to or greater than 3, the protection duration is 540s (180s x 3). ● When the accumulated downtime duration exceeds 1 hour (3,600s), the number of breakdowns are counted from 0.	3
Connection Protection	Pending URL Request Threshold	Connection Protection is triggered when the number of read URL requests reaches the threshold you configure.	6,000
	Duration (s)	Protection duration. During this period, WAF stops forwarding client requests.	60

NOTE

The following uses **Connection Protection** settings in **Figure 8-52** as an example to describe how the protection works.

- **Breakdown Protection**: When the number of 502/504 errors returned by the protected website exceeds 1,000 and accounts for 90% or more of the total access requests of the website for the first time, the first breakdown protection is triggered. During the first breakdown protection, WAF stops forwarding client requests for 180s (that is, blocks visitors access to the website for 180s). If a second consecutive breakdown protection is triggered, WAF stops forwarding client requests for 360s (180 x 2). If a third or more consecutive breakdowns are triggered, WAF stops forwarding client requests for 540s (180s x 3). The breakdowns are counted from 0 when the total downtime duration exceeds one hour (3,600s).
- **Connection Protection**: When the number of read URL requests in the waiting queue exceeds 6,000, WAF stops forwarding client requests for 60 seconds and returns the maintenance page of the website to visitors.

----End

8.4.6 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 to be protected has been added 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.

Procedure

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 & Compliance**.

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** to configure a traffic identifier by referring to **Table 8-18**.

Figure 8-53 Traffic Identifier

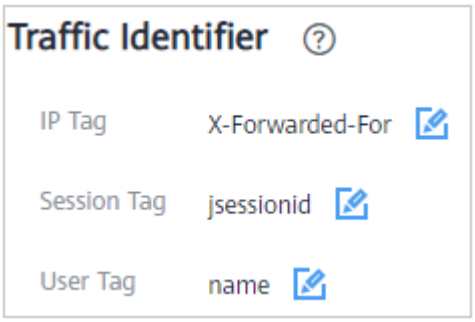


Table 8-18 Traffic identifier parameters

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. WAF obtains client IP addresses in the following sequence. For more details, see **How Does WAF Obtain the Real Client IP Address for a Request?** This field is used to store the real IP address of the client. You can customize the field name and configure multiple fields (separated by commas). After the configuration, WAF preferentially reads the configured field to obtain the real IP address of the client. If multiple fields are configured, WAF reads the IP address from left to right. **NOTICE** • If you want to use a TCP connection IP address as the client IP address, set **IP Tag** to **$remote_addr**. • If WAF does not obtain the real IP address of a client from fields you configure, WAF reads the **cdn-src-ip**, **x-real-ip**, **x-forwarded-for**, and **$remote_addr** fields in sequence to read the client IP address.	X-Forwarded-For
Session Tag	This tag is used to block possibly malicious requests based on the cookie attributes of an attack source. Configure this parameter to block requests based on cookie attributes.	jssessionid

Tag	Description	Example Value
User Tag	This tag is used to block possibly malicious requests based on the Params attribute of an attack source. Configure this parameter to block requests based on the Params attributes.	name

Step 7 Click **Confirm**.

----End

Other Operations

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

8.4.7 Forwarding Custom Header Fields

You can use WAF to add additional header information, for example, $request_id, to associate requests on the entire link. You can follow this topic to let WAF insert additional fields into a header and forward requests to origin servers. Note that the key value of a custom header field cannot be the same as any native Nginx fields.

Prerequisites

You have selected **Cloud - CNAME** or **Dedicated** for **Protection** when adding the website to WAF.

Constraints

- Header field forwarding can be configured only when you select **Cloud - CNAME** and **Dedicated** for **Protection**.
- Forwarding custom header fields is supported in some regions. For details, see **Functions**.
- You can configure up to eight key/value pairs.
- The key value can be set to any value other than keys in native Nginx fields.
- The value can be set to a custom string or a variable starting with $. Variables starting with $support only the following fields:

```
$time_local
$request_id
$connection_requests
$tenant_id
$project_id
$remote_addr
$remote_port
$scheme
$request_method
$http_host
$origin_uri
$request_length
```



```
$ssl_server_name
$ssl_protocol
$ssl_curves
$ssl_session_reused
```

Procedure

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.

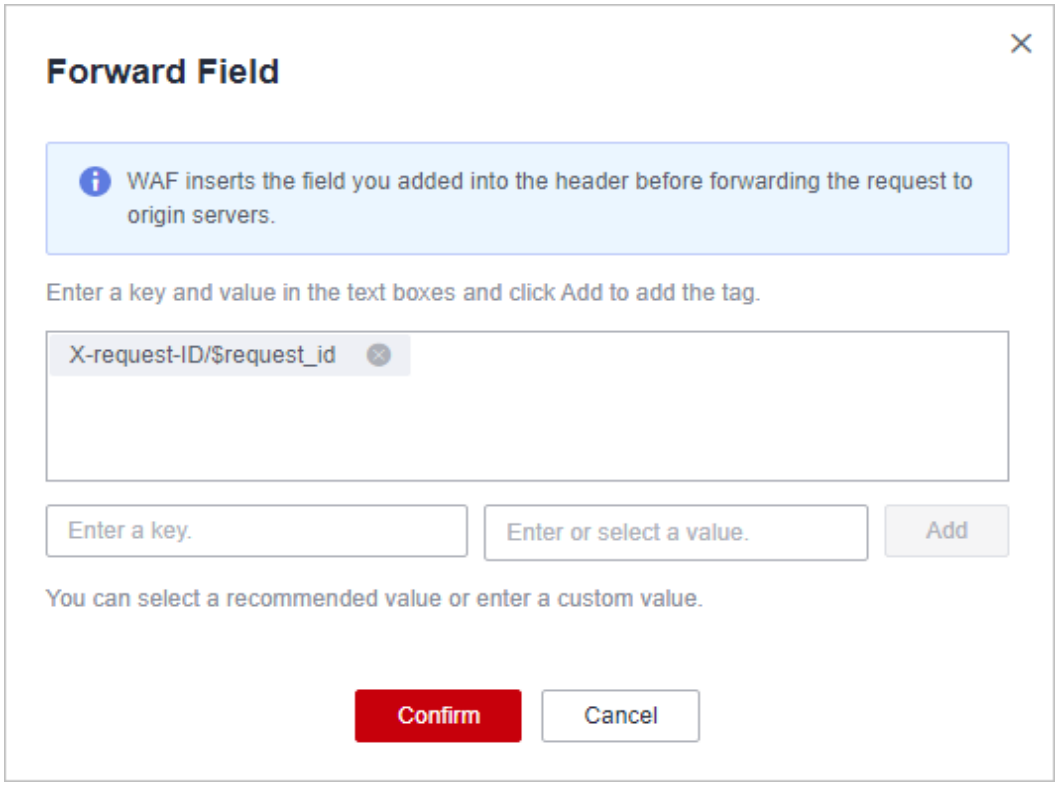
Step 3 Click in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.

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

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

Step 6 In the **Forward Field** column, click . In the displayed **Forward Field** dialog box, enter a key/value pair. To add more fields, click **Add**.

Figure 8-54 Forward Field



Step 7 After the fields are added, click **Confirm**.

----End

8.4.8 Modifying the Alarm Page

If a visitor is blocked by WAF, the **Default** block page of WAF is returned by default. You can also configure **Custom** or **Redirection** for the block page to be returned as required.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select the enterprise project from the **Enterprise Project** drop-down list and customize alarm pages for the domain names.

Prerequisites

A website has been added to WAF.

Constraints

- The **Redirection** mode is not supported if you select **Cloud - Load balancer** for the protected website.
- The content of the text/html, text/xml, and application/json pages can be configured on the **Custom** block page to be returned.
- The root domain name of the redirection address must be the same as the currently protected domain name (including a wildcard domain name). For example, if the protected domain name is **www.example.com** and the port is 8080, the redirection URL can be set to **http://www.example.com:8080/error.html**.

Procedure

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 & Compliance**.

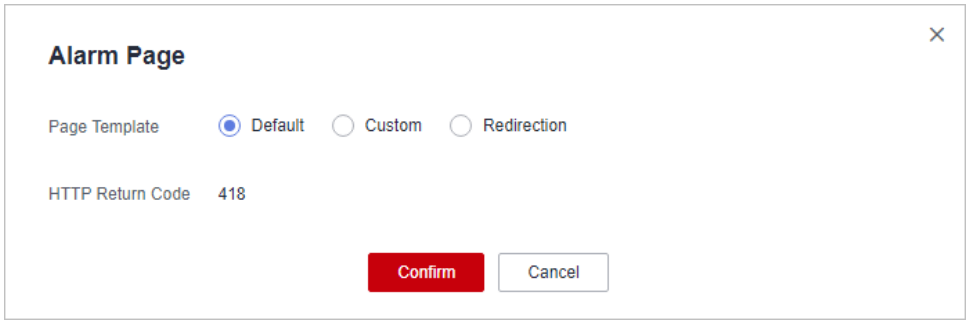
Step 4 In the navigation pane on the left, choose **Website Settings**.

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 page template name in the row where **Alarm Page** is located. In the displayed **Alarm Page** dialog box, specify **Page Template**.

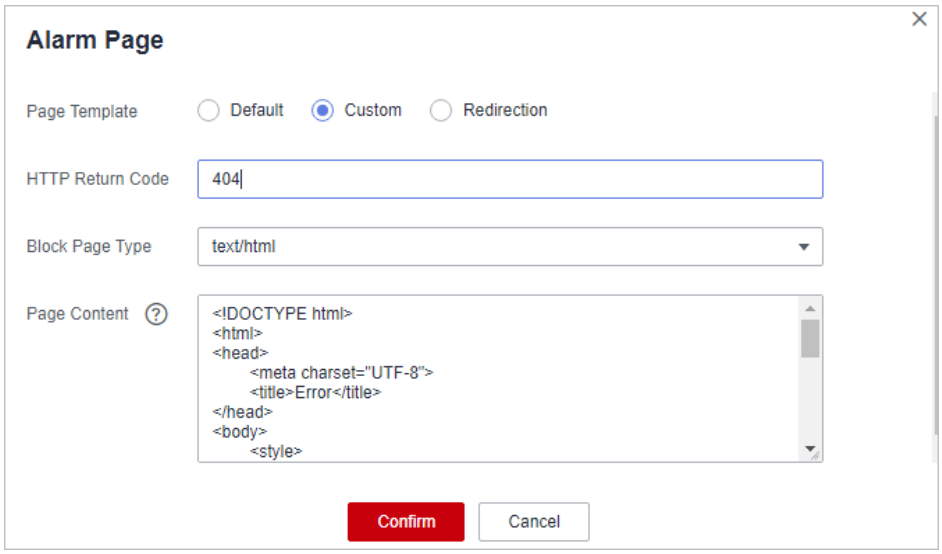
- To use the built-in page, select **Default**. An HTTP code 418 is returned.

Figure 8-55 Default alarm page



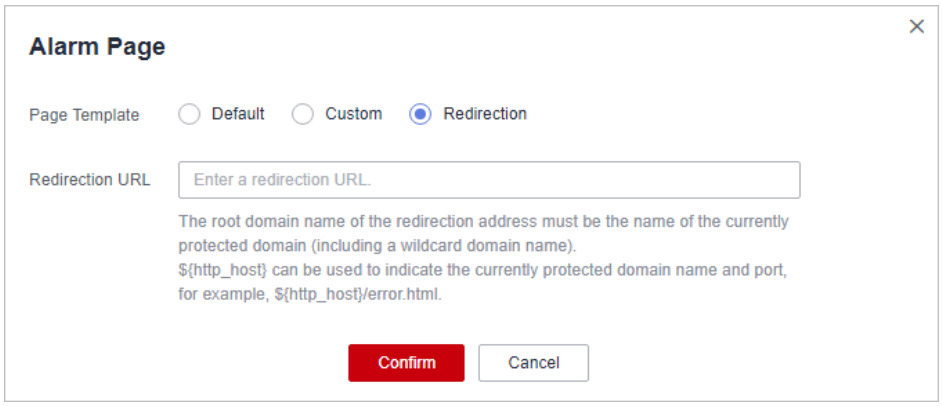
- To customize the alarm page, select **Custom** and configure following parameters.
  - **HTTP Return Code**: return code configured on a custom page.
  - **Block Page Type**: The options are **text/html**, **text/xml**, and **application/json**.
  - **Page Content**: Configure the page content based on the selected value for **Block Page Type**.

Figure 8-56 Custom alarm page



- To configure a redirection URL, select **Redirection**.

Figure 8-57 Redirection alarm page



The root domain name of the redirection URL must be the same as the currently protected domain name (including a wildcard domain name). For example, if the protected domain name is **www.example.com** and the port is 8080, the redirection URL can be set to **http://www.example.com:8080/error.html**.

Step 7 Click **Confirm**.

----End

8.5 Basic Information

8.5.1 Viewing Basic Information

This topic describes how to view client protocol, policy name, alarm page, CNAME record, and CNAME IP address configured for a protected domain name.

NOTE

If you have enabled enterprise projects, you can select your enterprise project from the **Enterprise Project** drop-down list and view domain names in the project.

Prerequisites

A website has been connected to WAF.

Procedure

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 & Compliance**.

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

Step 5 View the protected website lists. For details about parameters, see **Table 8-19**.

Figure 8-58 Website list

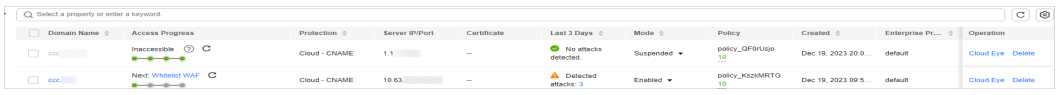


Table 8-19 Parameters

Parameter	Parameter
Domain Name	Protected domain name or IP address.

Parameter	Parameter
Protection	WAF protection configured for your website. The options can be **Cloud - CNAME**, **Cloud - Load balancer**, or **Dedicated**.
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.
Certificate	Certificate associated with the domain name. You can click the certificate name to go to the **Certificates** page.
Last 3 Days	Protection status of the domain name over the past three days.
Mode	WAF mode of the protected domain name. You can click ▼ to select one of the following protection modes: • **Enabled**: WAF is enabled. • **Suspended**: WAF 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 working mode can be switched to **Bypassed** only when **Cloud - 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 proxy is configured between the client and WAF. For details, see **Switching WAF Working Mode**.
Policy	Number of types of WAF protection enabled for the domain name. You can click the number to go to the rule configuration page and configure specific protection rules. For details, see **Policies**.

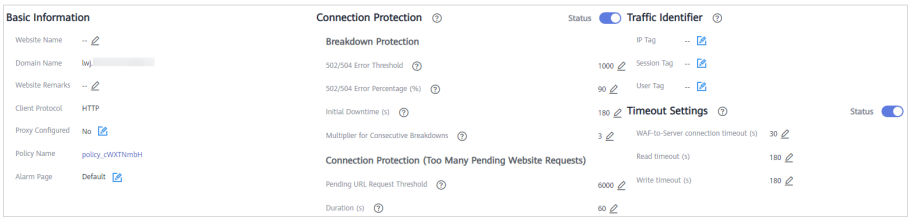
Parameter	Parameter
Access Progress	The progress of connecting your website to WAF or the website access status. • **Inaccessible**: The website has not been connected to WAF yet or failed to connect to WAF. • **Accessible**: The website has been connected to WAF. **NOTICE** The initial **Access Status** of a website protected in **Dedicated** or **Cloud - Load balancer** mode is **Inaccessible**. When a request reaches your WAF instance, the access status automatically changes to **Accessible**.
Created	Time the website was added to WAF.

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 8-59 Basic Information



----End

8.5.2 Exporting Website Settings

You can export settings of all websites protected by WAF in your account on the **Website Settings** page.

Prerequisites

There are websites that have been added to WAF.

Procedure

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 & Compliance**.

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

8.5.3 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 domain name of the website to be protected has been connected to WAF.

Constraints

- The **Bypassed** mode is available only when **Protection** is set to **Cloud - CNAME**.
- Before switching to the bypass mode, ensure that the service port of the origin server has been enabled.

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 (formerly false alarm masking) 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. Switch the mode to **Bypassed** only if 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 proxy is 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.

Procedure

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 & Compliance**.

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

Step 5 In the row containing the target domain name, click in the **Mode** column and select a mode you want.

----End

Other Operations

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

8.5.4 Switching the Load Balancing Algorithm

If you configure one or more origin server addresses, you can use a load balancing algorithm to distribute traffic across these origin servers. WAF supports the following algorithms:

- **Origin server IP hash**: Requests from the same IP address are routed to the same backend server.
- Weighted round robin: All requests are distributed across origin servers in turn based on weights set to each origin server. The origin server with a larger weight receives more requests than others.
- **Session hash**: Requests with the same session tag are routed to the same origin server. To enable this algorithm, **configure traffic identifiers for known attack sources**, or Session hash algorithm cannot take effect.

Prerequisites

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

Constraints

- You have selected **Cloud - CNAME** for **Protection** when adding the website to WAF.
- Only the professional and platinum editions support configuring load balancing algorithms.
- Configuring load balancing algorithms is supported in some regions. For details, see **Functions**.

Procedure

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 & Compliance**.

Step 4 In the navigation pane, 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 **Load Balancing Algorithm** field, click . In the dialog box displayed, select a load balancing algorithm and click **Confirm**.

----End

8.5.5 Change Policy for a Domain Name

This topic walks you through how to change the protection policy used for a website.

Prerequisites

You have used a **protection policy.** for a website.

Procedure

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 & Compliance**.

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

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

Step 6 In **Policy Name** row, click . In the dialog box displayed, select another protection policy and click **Confirm**.

----End

8.5.6 Updating a Certificate

If you select **Cloud - CNAME** or **Dedicated** for **Protection** and set **Client Protocol** to **HTTPS**, a certificate is required for your website.

- If your website certificate is about to expire, purchase a new certificate before the expiration date and update the certificate associated with the website in WAF.
- If you plan to update the certificate associated with the website, associate a new certificate with your website on the WAF console.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select the enterprise project from the **Enterprise Project** drop-down list and update certificates.

Prerequisites

- You have selected **Cloud - CNAME** or **Dedicated** for protection when adding the website 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**.
- Only accounts with the **SCM Administrator** and **SCM FullAccess** permissions can select SCM certificates.
- Before updating the certificate, ensure that your WAF instance and the certificate you want to upload belong to the same account.
- WAF can send notifications if a certificate expires. You can configure such notifications on the **Certificates** page.

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.

Procedure

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 & Compliance**.

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.

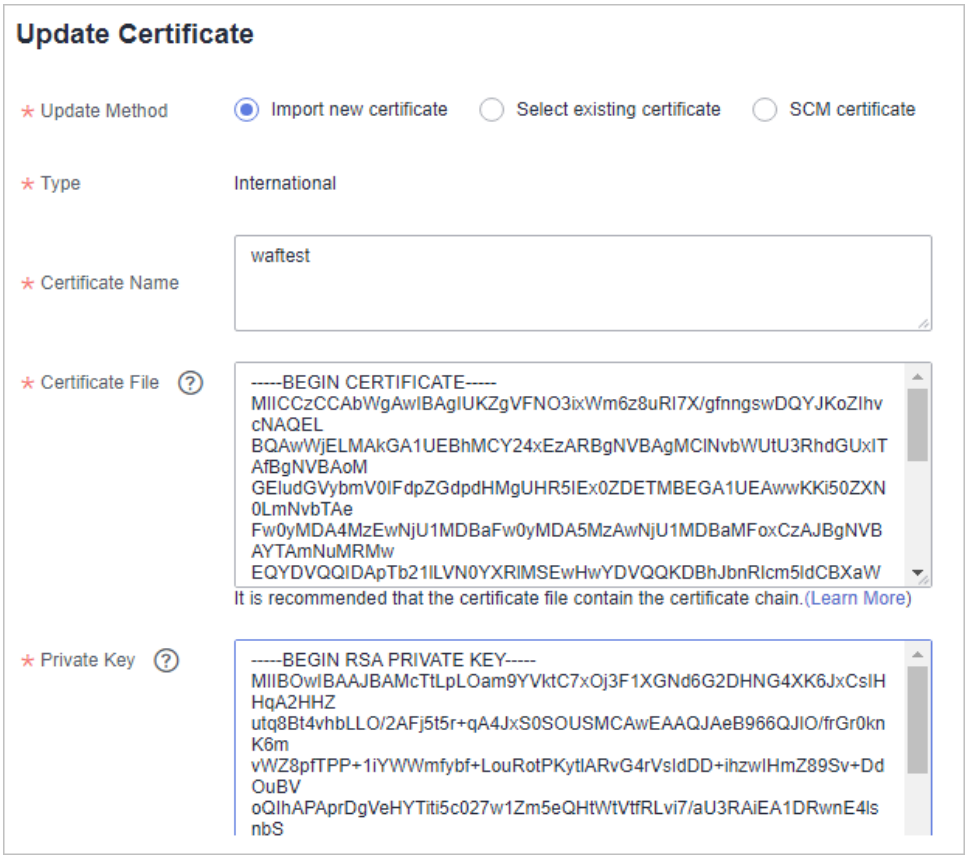
- If you select **Import new certificate** for **Update Method**, enter a certificate name, and copy and paste the certificate file and private key into the corresponding text boxes.

  The newly imported certificates will be listed on the **Certificates** page. For more details, see **Uploading a Certificate**.

  NOTE

  WAF encrypts and saves the private key to keep it safe.

Figure 8-60 Update Certificate



Only .pem certificates can be used in WAF. If the certificate is not in .pem format, convert it into .pem locally by referring to **Table 8-20** before uploading it.

Table 8-20 Certificate conversion commands

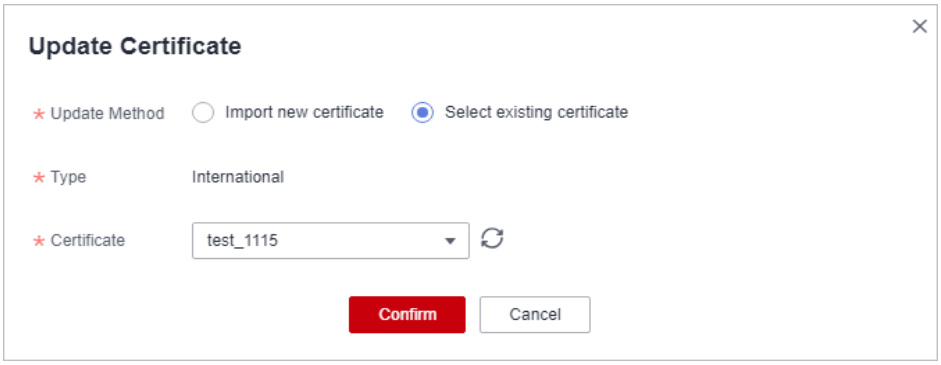
Format	Conversion Method
CER/CRT	Rename the **cert.crt** certificate file to **cert.pem**.
PFX	– Obtain a private key. For example, run the following command to convert **cert.pfx** into **key.pem**: **openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes** – Obtain a certificate. For example, run the following command to convert **cert.pfx** into **cert.pem**: **openssl pkcs12 -in cert.pfx -nokeys -out cert.pem**
P7B	1. Convert a certificate. For example, run the following command to convert **cert.p7b** into **cert.cer**: **openssl pkcs7 -print_certs -in cert.p7b -out cert.cer** 2. Rename certificate file **cert.cer** to **cert.pem**.
DER	– Obtain a private key. For example, run the following command to convert **privatekey.der** into **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** – Obtain a certificate. For example, run the following command to convert **cert.cer** into **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTE

- Before running an OpenSSL command, ensure that the **OpenSSL** tool has been installed on the local host.
- If your local PC runs a Windows operating system, go to the command line interface (CLI) and then run the certificate conversion command.

- If you select **Select existing certificate** for **Update Method**, select an existing certificate from the **Certificate** drop-down list.

Figure 8-61 Selecting an existing certificate



NOTE

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

- If you select **SCM certificate** for **Update Method**, select a certificate managed in CCM. It can be a certificate you purchased through CCM or an external certificate you uploaded to CCM.

CAUTION

The SCM certificate domain name must be the same as the one you added to WAF.

Step 7 Click **Confirm**.

----End

Other Operations

Uploading a Certificate

8.5.7 Editing Server Information

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

Applicable scenarios:

- Edit server information.
  - Cloud - CNAME access: 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 a 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 enterprise project from the **Enterprise Project** drop-down list and configure server information for the domain names.

Prerequisites

A website has been added to WAF.

Impact on the System

Modifying the server configuration does not affect services.

Procedure

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 & Compliance**.

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 **Server Information** area, click . **Figure 8-62** shows an example.

Figure 8-62 Server Information

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 a Certificate**.
- 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.

8.5.8 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 protected website details on Cloud Eye.

Prerequisites

The website to be protected has been added to WAF.

Procedure

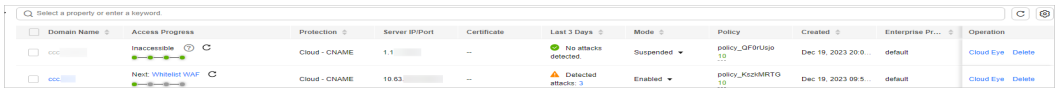
Step 1 Log in to the management console.

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 & Compliance**.

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

Figure 8-63 Website list



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

8.5.9 Migrating Domain Names to Other Enterprise Projects

WAF allows you to migrate domain names from an enterprise project to another one. Note that the migrated domain names will not be listed in the original enterprise project.

Certificates and policies are not migrated along with domain names. You need to configure them during the migration.

Prerequisites

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

Constraints

- In cloud mode, only the professional and platinum edition support migrating domain names to other enterprise projects.
- Certificates and policies are not migrated along with domain names. You need to configure them during the migration.

Procedure

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.

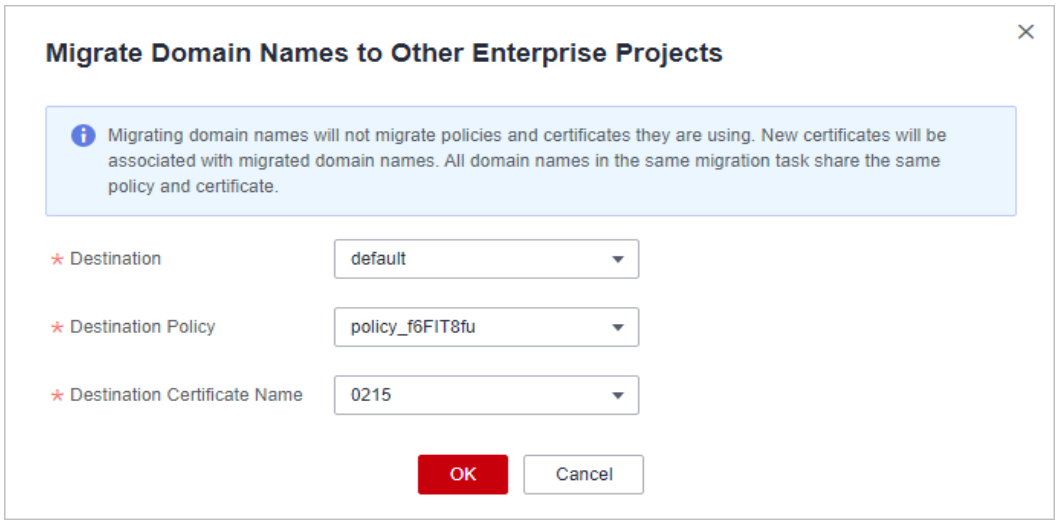
Step 3 Click in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.

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

Step 5 Select the domain names you want to migrate. In the upper right corner of the website list, click **Migrate Domain Name**.

- **Destination**: Select the enterprise project you want to migrate domain names to.
- **Destination Policy**: Select a policy for domain names you are migrating. This is because policies are not migrated along with domain names.
- **Destination Certificate Name**: Select a certificate for domain names you are migrating. This is because certificates are not migrated along with domain names.

Figure 8-64 Migrate Domain Names to Other Enterprise Projects



----End

8.5.10 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 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 **Website Settings**.

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

A website domain name has been added to WAF.

Impact on the System

- In cloud CNAME 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.
- 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.

Procedure

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 & Compliance**.

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

Step 5 In the row containing the website domain name you want to delete, click **Delete** in the **Operation** column.

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

- Cloud mode
  - No proxy used

    NOTE

    - Ensure that related configurations are completed and select **The CNAME of the domain name has been deleted from the DNS provider, and an A record has been configured to the origin server IP address, or services carried on the domain name have been brought offline**.
    - If you select **Forcible delete the WAF CNAME record.**, WAF will not check your domain name resolution and delete WAF CNAME record immediately. Before enabling this option, make sure you have resolved the domain name to the origin server, or your website will become inaccessible.
    - If you want to retain the policy bound to the domain name, select **Retain the policy of this domain name**.
  - Proxy used

NOTE

- Ensure that related configurations are completed and select **The domain name has been pointed to the origin server on the Advanced Anti-DDoS, CDN, or cloud acceleration product side, or services carried on the domain name have been brought offline**.
- If you select **Forcible delete the WAF CNAME record.**, WAF will not check your domain name resolution and delete WAF CNAME record immediately. Before enabling this option, make sure you have resolved the domain name to the origin server, or your website will become inaccessible.
- If you want to retain the policy bound to the domain name, select **Retain the policy of this domain name**.

- Cloud - ELB Access/Dedicated

  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

Other Operations

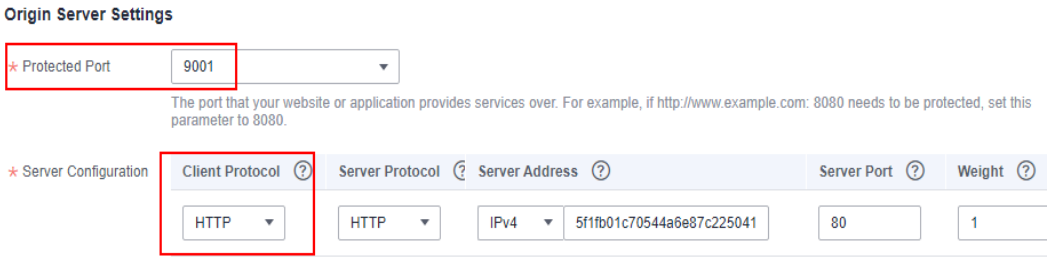
To delete domain names in batches, select the domain names and click **Delete** above the website list.

8.6 Ports Supported by WAF

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

For example, as shown in **Ports Supported by WAF**, a cloud WAF instance from the stand edition or later and dedicated WAF instances can protect port 9001 over HTTP. If you want to protect port 9001, you can use either a cloud WAF instance from the standard edition or later or a dedicated WAF instance. Then, configure the instance in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)** by referring to **Ports Supported by WAF**.

Figure 8-65 Port configuration



NOTICE

Note that the supported ports may differ depending on regions.

Standard Ports

WAF can protect the following standard ports.

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

Non-standard Ports That Can Be Protected by Cloud WAF

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 8-21 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

Non-standard Ports That Can Be Protected by Dedicated WAF Instances

If you use dedicated WAF instances, you can select any non-standard ports listed in **Table 8-22**.

Table 8-22 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

9 Object Management

9.1 Certificate Management

9.1.1 Uploading a Certificate

If you select **Cloud - CNAME** or **Dedicated** for **Protection** and set **Client Protocol** to **HTTPS**, a certificate is required for your website.

If you upload a certificate to WAF, you can directly select the certificate when adding a website to WAF.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select your enterprise project from the **Enterprise Project** drop-down list and upload certificates in the project.

Prerequisites

You have obtained the certificate file and certificate private key.

Specification Limitations

You can upload as many certificates in WAF as the number of domain names that can be protected by your WAF instances in the same account. For example, if you purchase a standard edition WAF instance, which can protect 10 domain names, and a domain name expansion package, which can protect 20 domain names, your WAF instance can protect 30 domain names total. In this case, you can upload 30 certificates.

Constraints

- If you purchase a certificate on the SCM console and push it to WAF, the certificate is added to the certificate list on the **Certificates** page on the WAF console. This certificate is also counted towards your total certificate quota. For details about how to push an SSL certificate in SCM to WAF, see **Pushing an SSL Certificate to Other Cloud Services**.

NOTICE

Currently, certificates purchased in Huawei Cloud SCM can be pushed only to the **default** enterprise project. For other enterprise projects, SSL certificates pushed by SCM cannot be used.

- If you import a new certificate when adding a protected website or updating a certificate, the certificate is added to the certificate list on the **Certificates** page, and the imported certificate is also counted towards your total certificate quota.

Application Scenario

If you select **HTTPS** for **Client Protocol**, a certificate is required.

Procedure

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.

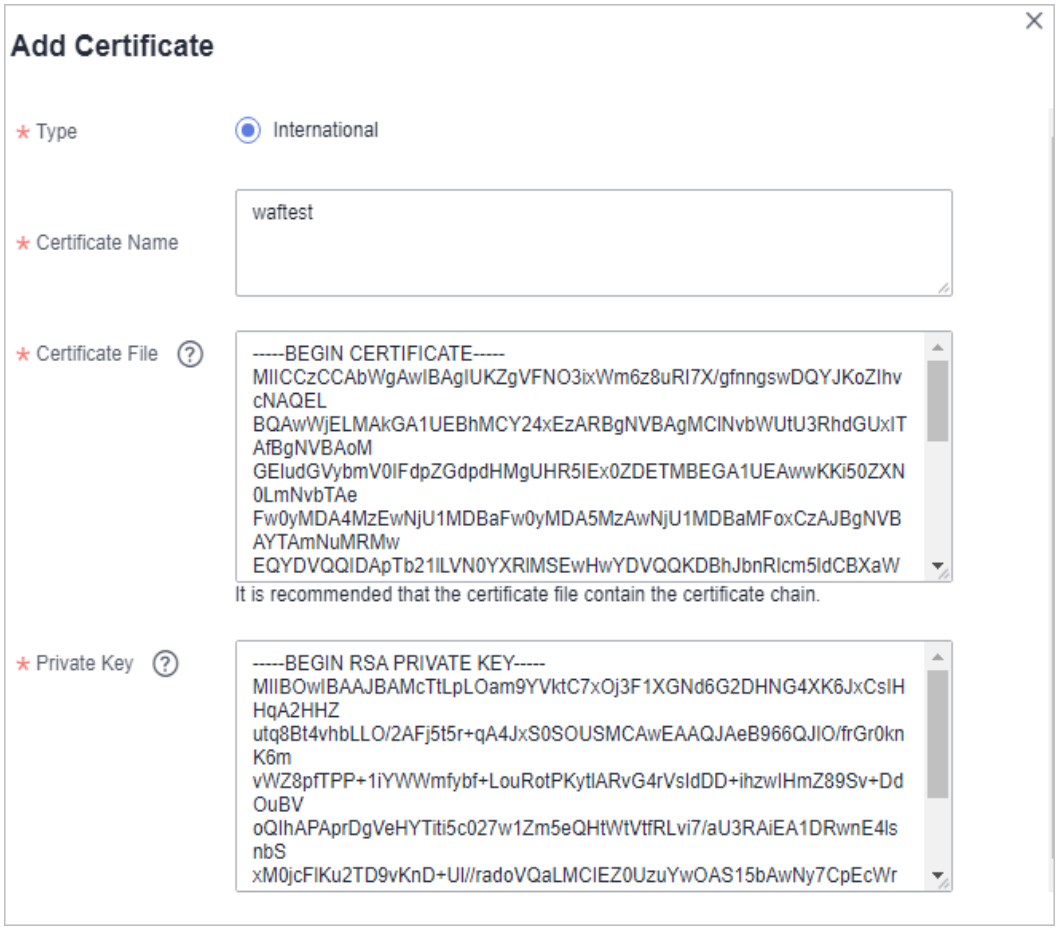
Step 3 Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.

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



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**.

Format	Conversion Method
DER	• Obtain a private key. For example, run the following command to convert **privatekey.der** into **privatekey.pem**: **openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem** • Obtain a certificate. For example, run the following command to convert **cert.cer** into **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

NOTE

- Before running an OpenSSL command, ensure that the **OpenSSL** tool has been installed on the local host.
- If your local PC runs a Windows operating system, go to the command line interface (CLI) and then run the certificate conversion command.

Step 7 Click **Confirm**.

----End

Verification

The certificate you created is displayed in the certificate list.

Other 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 **Share** 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.

Procedure

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 & Compliance**.

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.

Other 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 **Share** 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 or pushed a certificate to WAF.

Constraints

- For **certificates you upload to WAF**, WAF does not send expiration notifications to you.
- For certificates you push from CCM to WAF, the certificate validity period can be viewed in WAF only when you enable certificate expiration notifications in CCM.

Procedure

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 & Compliance**.

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

Step 5 View the certificate information. **Table 9-2** describes the parameters.

Figure 9-2 Certificate list

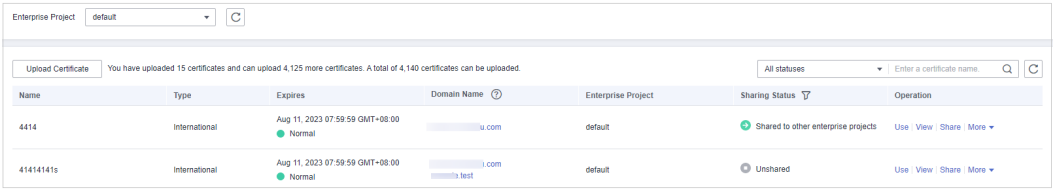


Table 9-2 Certificate parameters

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 a Certificate**.
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.
Enterprise Project	The enterprise project that the certificate belongs to.
Sharing Status	Whether the certificate is shared with other enterprise projects. • Shared • Unshared

----End

Other 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 **Share** 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 created or pushed a certificate to WAF.

Procedure

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 & Compliance**.

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

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

Step 6 In the displayed dialog box, select the target enterprise project and click **Confirm**.

----End

Other 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

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.

Procedure

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 & Compliance**.

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

Other 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.

Constraints

- For dedicated and ELB-accessed cloud WAF instances, if the load balancers they use support IPv6 addresses, those WAF instances also support IPv6 addresses or IPv6 address ranges.

Specification Limitations

- A maximum of 50 address groups can be created. You can add multiple IP addresses or IP address ranges to an address group. Use commas (,) to separate multiple IP addresses or IP address ranges. No line breaks are allowed.
- Before adding an address group to a blacklist or whitelist rule, ensure that your IP address blacklist and whitelist rule quota has not been used up.

NOTE

- For details, see **Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses**.

  For details about specifications, see **Edition Differences**.
- If the quota for IP address whitelist and blacklist rules of your cloud WAF cannot meet your requirements, you can purchase rule expansion packages under the current WAF instance edition or upgrade your WAF instance edition to increase such quota. A rule expansion package allows you to configure up to 10 IP address blacklist and whitelist rules.

  For details, see **Upgrading Cloud WAF Edition and Specifications**

Procedure

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 & Compliance**.

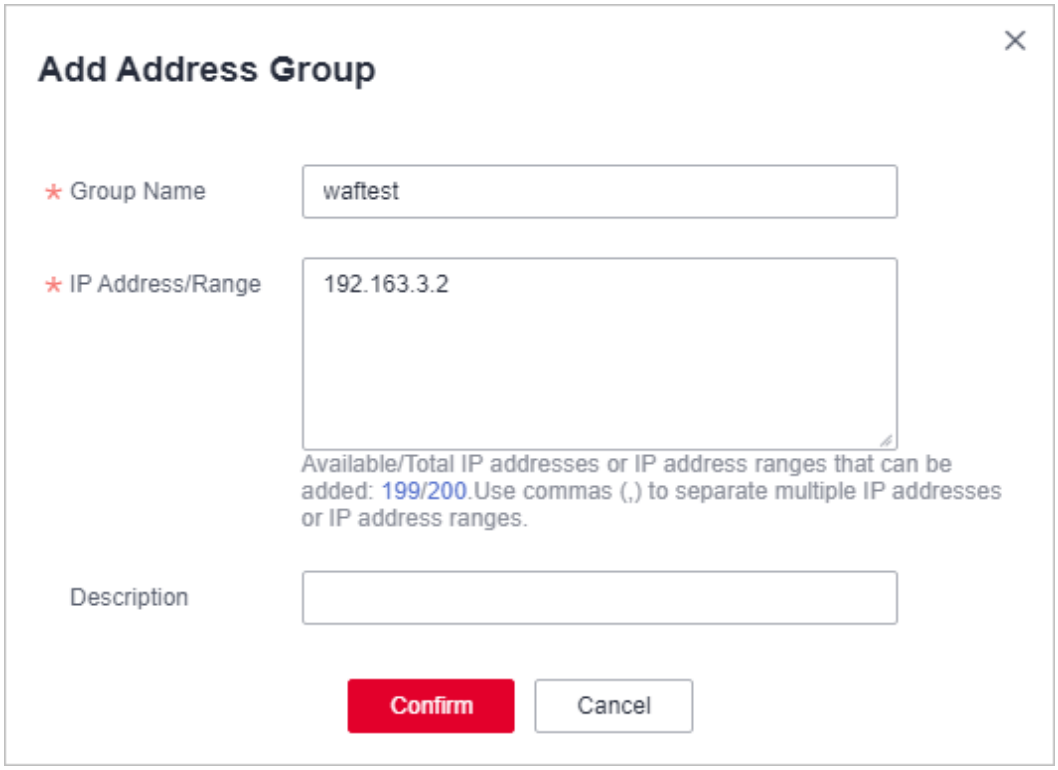
Step 4 In the navigation pane on the left, choose **Objects** > **Address Groups**.

Step 5 Click the **My Address Groups** tab.

Step 6 On the upper left of the address group list, click **Add Address Group**.

Step 7 In the displayed **Add Address Group** dialog box, enter an address group name and provide IP addresses/IP address ranges.

Figure 9-3 Add Address Group



Step 8 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

- Do not add an IP address or IP address range that has been added to a different IP address group to the existing address group, or the IP address group will fail to be modified.
- 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.

Procedure

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 & Compliance**.

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

Step 5 Click the **My Address Groups** tab.

Step 6 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.

Parameter	Description
Remarks	Supplementary information about the address group.

Step 7 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.

Dedicated Engine Version Iteration

Engine Version	Feature
December 2023	• You can configure a global protection whitelist rule to **ignore invalid requests**. • JavaScript-based anti-crawler rules support more protective actions, including **Block**, **Log only**, and **Verification code**.
August 2023	• The **$remote_addr** field is added to the IP identifier, which can be directly set to the IP address of the TCP connection. • IP addresses used in TCP connections can be identified by CC, precise protection, blacklist, and whitelist rules. • A block duration can be set if **Protective Action** is set to **Verification code** in a CC attack protection rule.

Engine Version	Feature
April 2023	• HTTP2 is enabled globally by default. There is no need to enable it manually. • By default, a request can pass through WAF four times before it goes to the origin server. Error code 523 will be returned if the request exceeds this limit. • Strict multipart format verification is supported. • Dedicated ELB network load balancers are supported. (In earlier versions, only shared load balancers and dedicated application load balancers are supported.)
November 2022	• Built-in tags can be added to attack logs (hit_data) when built-in rules are hit. • Destination rate limiting and response code conditions can be configured in CC attack protection rules.
September 2022	• TLS v1.3 is supported. • Protection for on-premises web servers is supported. • More types of statistics are added to heartbeat logs for attacks. • HTTPS ports 60700 to 60999 (300 ports) are added to the protection port list.
July 2022	• The wildcard domain name matching logic is supported. • The global protection whitelist is supported.
May 2022	Configuring the earliest TLS version based on instances is supported.
March 2022	• Rules can be updated and delivered from the management plane. • False alarm masking rules can work for all domain names and specified domain names. • All conditions can be configured for false alarm masking.
February 2022	The request logging methods are optimized.
January 2022	Some regular expression matching rules are optimized.
November 2021	• The log only mode is supported for information leakage rules. • Attack logs of invalid requests are added. • Precise protection rules can work to each IP address (only for IPv4 format) in the XFF request header. • Timeout duration can be set for specified domain names. • Some functions are optimized.

Engine Version	Feature
October 2021	The performance of some functions is improved.
September 2021	• Precise protection rules can work to the **request body** field. • Precise protection rules support regular expression matching and all subfields. • Some logs can be interconnected with LTS.
June 2021	• The HTTPS port supports HTTP/2. • The **region ID** field is added to access logs. • The **region ID** field and engine IP address are added to attack logs.

Viewing Information About a Dedicated WAF Instance

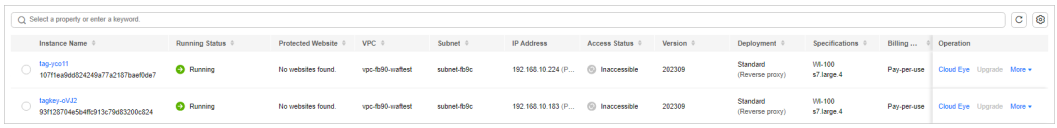
Step 1 Log in to the management console.

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

Step 3 Click in the upper left corner, select a region, and choose **Security & Compliance** > **Web Application Firewall** to go to the **Dashboard** page.

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



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

Parameter	Description	Example Value
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	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.

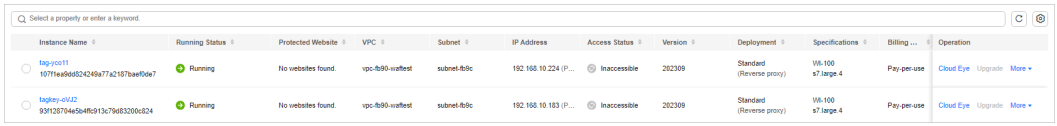
Step 1 Log in to the management console.

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, select a region, and choose **Security & Compliance** > **Web Application Firewall** to go to the **Dashboard** page.

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



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. Select an upgrade method based on the number of dedicated WAF instances you have.

- Upgrading a Single Dedicated WAF Instance
- Upgrading Multiple Dedicated WAF Instances

NOTE

If you are using the latest version of dedicated WAF instances, the **Upgrade** button is grayed out.

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.

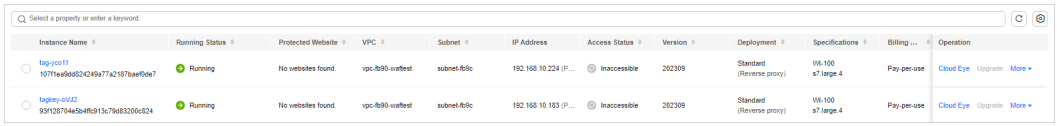
Step 1 Log in to the management console.

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, select a region, and choose **Security & Compliance** > **Web Application Firewall** to go to the **Dashboard** page.

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



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.

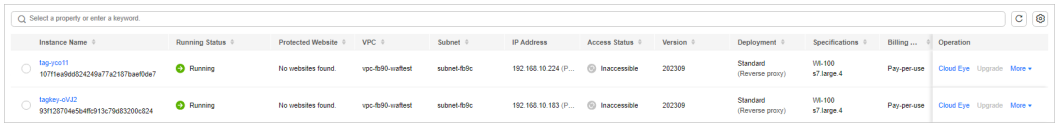
Step 1 Log in to the management console.

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, select a region, and choose **Security & Compliance** > **Web Application Firewall** to go to the **Dashboard** page.

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



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 **OK**.

----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.

Procedure

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 & Compliance**.

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.
- To renew a WAF instance, click **Renew** next to the instance.

- In the cloud mode configuration area, click **Change Specifications**. On the displayed page, you can change the edition and purchase an expansion package.

----End

10.3 Enabling Alarm Notifications

This topic describes how to enable notifications for attack logs. Once this function is enabled, WAF sends you SMS or email notifications if an attack is detected.

You can configure certificate expiration reminders. When a certificate is about to expire, WAF notifies you by the way you configure, such as email or SMS.

NOTE

- Simple Message Notification (SMN) is a paid service. For details, see **Product Pricing Details**.
- Before you set alarm notification, create a message topic in the SMN service. For details, see **Before You Publish a Message**.
- 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 or exceeds the threshold configured for a certain period.
- Only one alarm notification of the same type can be configured in an enterprise project.

Procedure

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 & Compliance**.

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 10-5 Create Notification

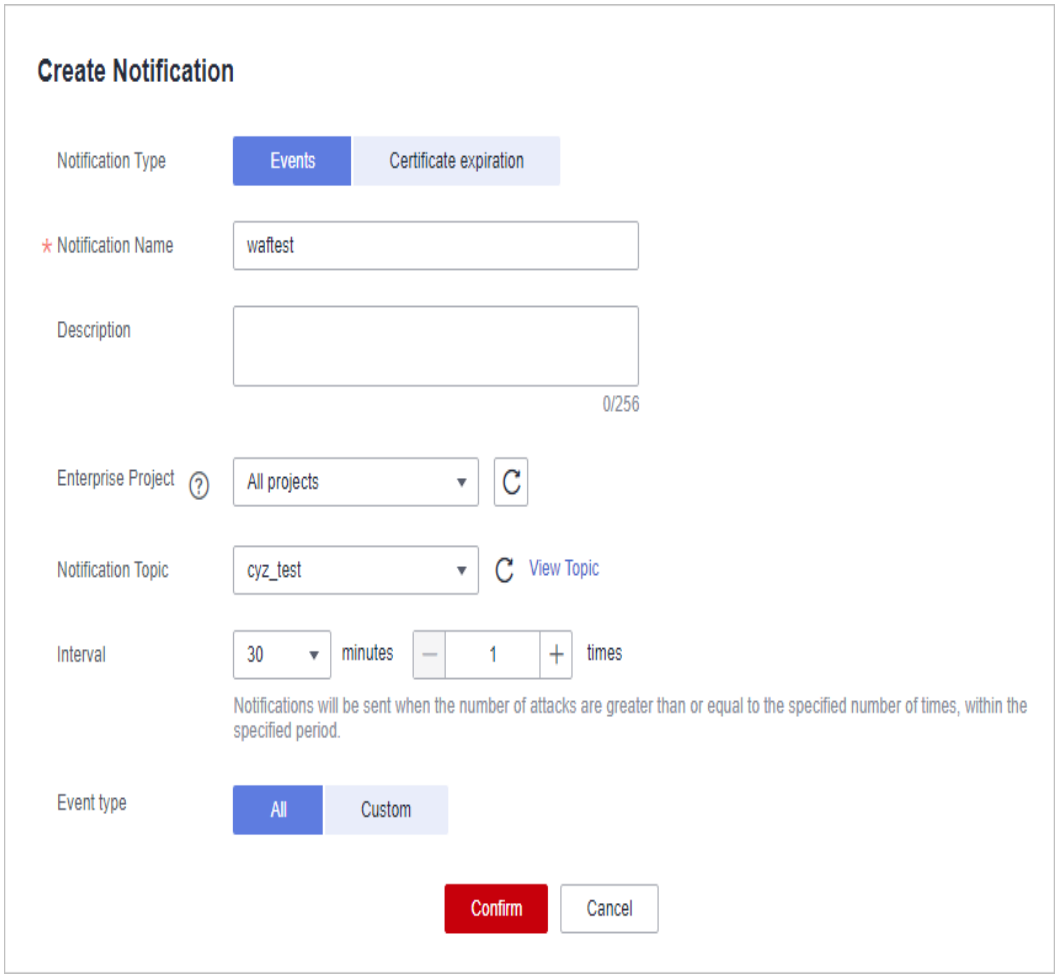


Table 10-2 Description of notification setting parameters

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 is at least equal to 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.

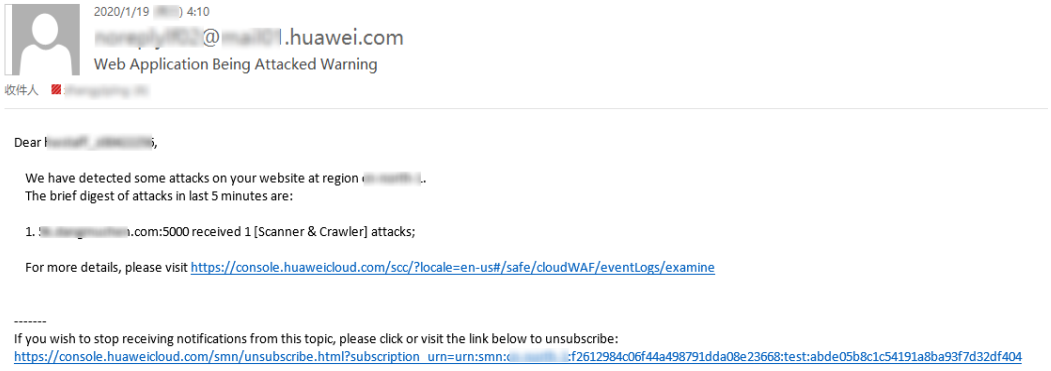
- To modify a notification, locate the row containing the notification and click **Modify** in the **Operation** column.

----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 10-6** shows an example of an alarm notification email.

Figure 10-6 Alarm notification email



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. To use this function, enable it by referring to **Enabling the Enterprise Center**.

- Authorization

  You can add a user group to an enterprise project and configure a policy to associate the enterprise project with the user group. You can add users to a user group to control which projects they can access and what resources they can perform operations on. To do so, perform the following operations:

  a. On the **Enterprise Management** console, click the name of an enterprise project to go to the enterprise project details page.

  b. On the **Permissions** tab, click **Authorize User Group** to go to the **User Groups** page on the IAM console. Associate the enterprise project with a user group and assign permissions to the group. For details, see **Creating a User Group and Granting Permissions**.

- Associating the resource with enterprise projects

  To use an enterprise project to manage cloud resources, associate resources with the enterprise project.

- Associate a WAF instance with an enterprise project when purchasing WAF

  On the page for buying WAF, select an enterprise project from the **Enterprise Project** drop-down list.
- Add WAF instances to an enterprise project after a WAF instance is purchased.

  On the **Enterprise Project Management** page, add existing 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.

For more information about enterprise project, see **Enterprise Management User Guide**.

11.2 IAM Permissions Management

11.2.1 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 11-1**).

Prerequisites

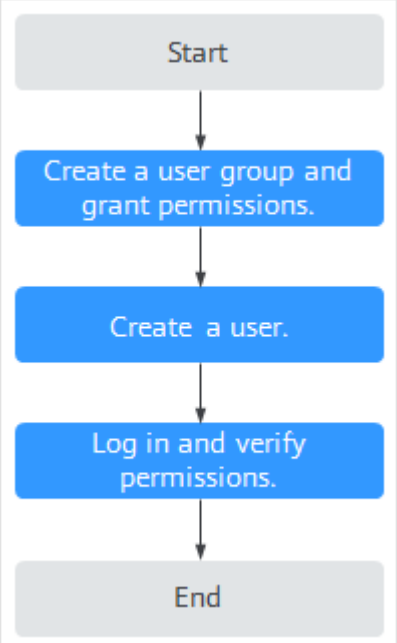
Learn about the permissions supported by WAF in **Table 11-1** and choose policies or roles based on your requirements. For the system policies of other services, see **System Permissions**.

Table 11-1 System policies supported by WAF

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

Process Flow

Figure 11-1 Process for granting permissions



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

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

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

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

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

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

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

11.2.2 WAF Custom Policies

Custom policies can be created to supplement the system-defined policies of WAF. 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.

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"
            ]
        }
    ]
}
```

11.2.3 WAF Permissions and Supported Actions

This topic describes fine-grained permissions management for your WAF instances. If your Huawei ID does not need individual IAM users, then you may skip over this section.

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign permissions policies to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

You can grant users permissions by using **roles** and **policies**. Roles are provided by IAM to define service-based permissions depending on user's job responsibilities. Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions.

Supported Actions

WAF provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control.

- Permission: A statement in a policy that allows or denies certain operations.
- Action: Specific operations that are allowed or denied.

Permission	Action	IAM Project	Enterprise Project
Querying an information leakage prevention rule	waf:antiLeakageRule:get	√	√
Querying a web tamper protection rule	waf:antiTamperRule:get	√	√
Querying a CC attack protection rule	waf:ccRule:get	√	√
Querying a precise protection rule	waf:preciseProtection-Rule:get	√	√
Querying a global protection whitelist rule	waf:falseAlarmMaskRule:get	√	√
Querying a data masking rule	waf:privacyRule:get	√	√
Querying a blacklist or whitelist rule	waf:whiteBlackIpRule:get	√	√
Querying a geolocation access control rule	waf:geoIpRule:get	√	√
Querying a certificate	waf:certificate:get	√	√
Modifying WAF certificates	waf:certificate:put	√	√
Applying a certificate to a domain name	waf:certificate:apply	√	√
Querying a protection event	waf:event:get	√	√
Querying a protected domain	waf:instance:get	√	√
Querying a protection policy	waf:policy:get	√	√

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

Permission	Action	IAM Project	Enterprise Project
Deleting an information leakage prevention rule	waf:antiLeakageRule:delete	√	√
Deleting a web tamper protection rule	waf:antiTamperRule:delete	√	√
Deleting a CC attack protection rule	waf:ccRule:delete	√	√
Configuring a precise protection rule	waf:preciseProtection-Rule:delete	√	√
Deleting a global protection whitelist rule	waf:falseAlarmMaskRule:delete	√	√
Deleting a data masking rule	waf:privacyRule:delete	√	√
Deleting a blacklist or whitelist rule	waf:whiteBlackIpRule:delete	√	√
Deleting a geolocation access control rule	waf:geoIpRule:delete	√	√
Deleting a protected domain	waf:instance:delete	√	√
Deleting a protection policy	waf:policy:delete	√	√
Adding an information leakage prevention rule	waf:antiLeakageRule:create	√	√
Adding a web tamper protection rule	waf:antiTamperRule:create	√	√
Adding a CC attack protection rules	waf:ccRule:create	√	√

Permission	Action	IAM Project	Enterprise Project
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	√	√
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	√	√
Querying data masking rules	waf:privacyRule:list	√	√
Querying blacklist and whitelist rules	waf:whiteBlackIpRule:list	√	√

Permission	Action	IAM Project	Enterprise Project
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	√	√
Disable the pay-per-use billing for a WAF cloud-mode instance	waf:postpaid:delete	√	√
Viewing details of a WAF instance group	waf:pool:get	√	√
Modifying WAF instance group configuration	waf:pool:put	√	√

Permission	Action	IAM Project	Enterprise Project
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	√	√
Deleting health check configuration for a WAF instance group	waf:poolHealthMonitor:delete	√	√
Querying health check configurations for WAF instance groups	waf:poolHealthMonitor:list	√	√

11.3 Permission Dependency of the WAF Console

When using WAF, you may need to view resources of or use other cloud services. So you need to obtain required permissions for dependent services so that you can view resources or use WAF functions on WAF Console. To that end, make sure you have the WAF FullAccess or WAF ReadOnlyAccess assigned first. For details, see **Creating a User Group and Granting Permissions**.

Dependency Policy Configuration

To grant an IAM user the permissions to view or use resources of other cloud services on the WAF console, you must first grant the WAF Administrator, WAF FullAccess, or WAF ReadOnlyAccess policy to the user group to which the user belongs and then grant the dependency policies listed in **Table 11-2** to the user. These dependency policies will allow the IAM user to access resources of other cloud services.

Table 11-2 WAF console dependency policies and roles

Console Function	Dependent Services	Policy/Role Required
Dashboard	Enterprise Project Management Service (EPS)	You can view the data on the Dashboard page of an enterprise project only after obtaining the EPS ReadOnlyAccess system policy.
Buying a dedicated waf instance	Identity and Access Management (IAM) Network Console VPC Elastic Cloud Server (ECS) Tag Management Service (TMS)	• 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. The IAM system role **Security Administrator** is required for first-time buyers. For non-first-time buyers, you need to assign IAM system policy **IAM ReadOnlyAccess** or custom permissions to them. • The VPC ReadOnlyAccess system policy is required to select a VPC, subnet, and security group. • The ECS ReadOnlyAccess system policy is required to select **ECS** for WAF instance type. • The TMS ReadOnlyAccess system policy is required to view predefined tags.
Buying a WAF instance (for Dedicated Cloud)	Elastic Volume Service (EVS)	The EVS ReadOnlyAccess system policy is required to query EVS disks you have.

Console Function	Dependent Services	Policy/Role Required
Dedicated WAF engine management	Network Console VPC Elastic IP (EIP) Elastic Load Balance (ELB)	• The VPC ReadOnlyAccess system policy is required to query VPCs you have. • The EIP ReadOnlyAccess system policy is required to query EIPs bound to dedicated WAF instance. • The ELB ReadOnlyAccess system policy is required to query information about ELB load balancers bound to dedicated WAF instance.
Adding a website to WAF (ELB mode)	Elastic Load Balance (ELB)	The ELB Administrator system role is required along with the ELB FullAccess and ELB ReadOnlyAccess permissions to query load balancers bound to dedicated WAF instances.
Instance group management	Elastic Load Balance (ELB)	The ELB ReadOnlyAccess system policy is required to query load balancers used for a WAF instance group.
Adding a website to WAF (cloud and dedicated modes)	Cloud Certificate Manager (CCM)	The SCM ReadOnlyAccess system policy is required to query certificate details.
Editing server information	Cloud Certificate Manager (CCM)	
Website settings	Cloud Certificate Manager (CCM)	
Notifications	Simple Message Notification (SMN)	The SMN ReadOnlyAccess system policy is required to obtain SMN topic groups.
Enabling LTS for WAF logging	Log Tank Service (LTS)	The LTS ReadOnlyAccess system policy is required to select log group and log stream names created in LTS.

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.

Procedure

Step 1 Log in to the management console.

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

Step 3 Click  in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.

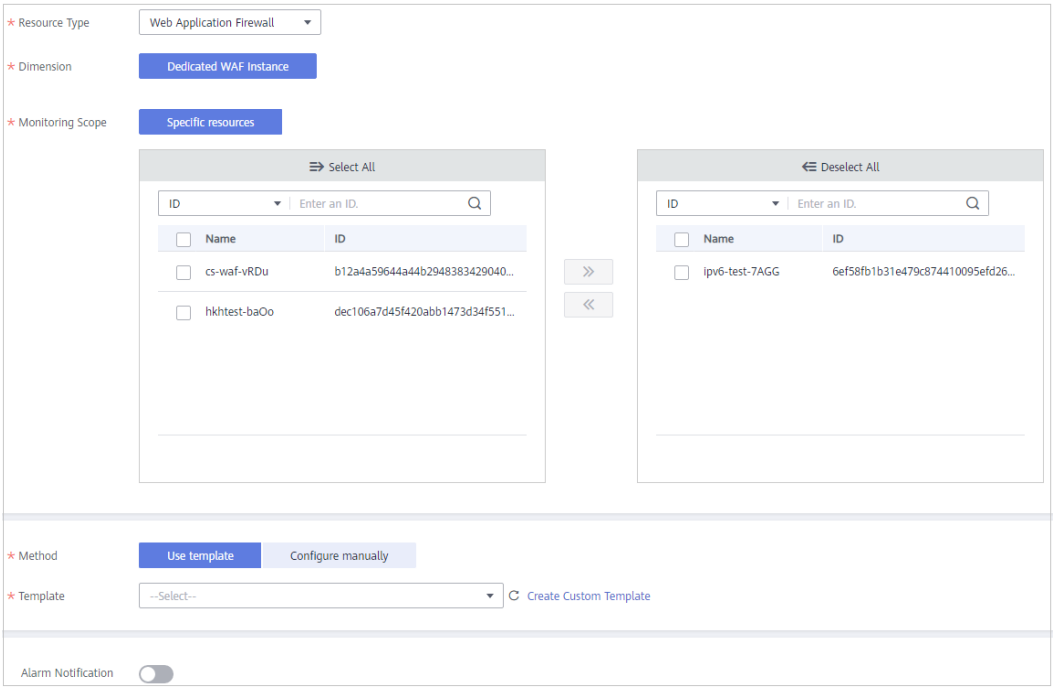
Step 5 In the upper right corner of the page, click **Create Alarm Rule**.

Step 6 Set the alarm rule name and select an enterprise project to which the alarm rule belongs.

Figure 12-1 Configuring alarms

Step 7 Select **Web Application Firewall** from the **Resource Type** drop-down list, and select a dimension, monitoring scope, alarm template, and whether to send a notification.

Figure 12-2 Configuring WAF alarm monitoring rules



Step 8 Click **Create**. In the displayed dialog box, click **OK**.

----End

12.1.3 Viewing Monitored Metrics

You can view WAF metrics on the management console to 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**.

Procedure

Step 1 Log in to the management console.

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

Step 3 Click in the upper left corner of the page and choose **Management & Governance** > **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
Adding a domain name to cloud WAF	instance	createInstance
Deleting a domain name from the cloud WAF	instance	deleteInstance
Modifying the protection status of a domain name in cloud mode	instance	modifyProtectStatus
Modifying the access status of a domain name in cloud mode	instance	modifyAccessStatus

Operation	Resource Type	Trace Name
Changing a domain name in cloud mode	instance	modifyInstance
Modifying DNS records for quick access to WAF	instance	quickAccessInstance
Adding a domain name to WAF (dedicated/ELB mode)	host	createHost
Changing a domain name added to WAF (dedicated/ELB mode)	host	modifyHost
Deleting a domain name from WAF (dedicated/ELB mode)	host	deleteHost
Changing WAF protection status (dedicated/ELB mode)	host	modifyProtectStatus
Changing domain name access status (dedicated/ELB mode)	host	modifyAccessStatus
Changing domain name access settings (dedicated/ELB mode)	host	modifyAccessProgress
Migrating domain names	migrate-host	migrateHosts
Uploading a certificate	certificate	createCertificate
Modifying a certificate	certificate	updateCertificate
Deleting a certificate	certificate	deleteCertificate
Applying a certificate to a domain name	certificate	applyCertificate

Operation	Resource Type	Trace Name
Sharing a certificate	certificate-sharing	createCertificateSharing
Disabling certificate sharing	certificate-sharing	deleteCertificateSharing
Creating a WAF policy	policy	createPolicy
Applying a WAF policy	policy	applyToHost
Modifying a policy	policy	modifyPolicy
Deleting a WAF policy	policy	deletePolicy
Adding a CC attack protection rule	policy	createCc
Modifying a CC attack protection rule	policy	modifyCc
Deleting a CC attack protection rule	policy	deleteCc
Adding a precise protection rule	policy	createCustom
Modifying a precise protection rule	policy	modifyCustom
Deleting a precise protection rule	policy	deleteCustom
Adding an IP address blacklist or whitelist rule	policy	createWhiteblackip
Modifying an IP address blacklist or whitelist rule	policy	modifyWhiteblackip
Deleting an IP address blacklist or whitelist rule	policy	deleteWhiteblackip
Creating/updating a web tamper protection rule	policy	createAntitamper
Enabling or disabling a web tamper protection rule	policy	modifyAntitamper

Operation	Resource Type	Trace Name
Deleting a web tamper protection rule	policy	deleteAntitamper
Creating a global whitelist rule	policy	createIgnore
Modifying a global protection whitelist rule	policy	modifyIgnore
Deleting a global protection whitelist rule	policy	deleteIgnore
Adding a data masking rule	policy	createPrivacy
Modifying a data masking rule	policy	modifyPrivacy
Deleting a data masking rule	policy	deletePrivacy
Creating a known attack source rule	policy	createPunishment
Modifying a known attack source rule	policy	modifyPunishment
Deleting a known attack source rule	policy	deletePunishment
Adding a geolocation access control rule	policy	createGeoip
Modifying a geolocation access control rule	policy	modifyGeoip
Deleting a geolocation access control rule	policy	deleteGeoip
Creating an anti-crawler rule	policy	createAnticrawler
Modifying an anti-crawler rule	policy	modifyAnticrawler
Deleting an anti-crawler rule	policy	deleteAnticrawler

Operation	Resource Type	Trace Name
Creating an information leakage prevention rule	policy	createAntileakage
Modifying an information leakage prevention rule	policy	modifyAntileakage
Deleting an information leakage prevention rule	policy	deleteAntileakage
Batch creating CC attack protection rules	policy	batchCreateCc
Batch modifying CC attack protection rules	policy	batchUpdateCc
Batch deleting CC attack protection rules	policy	batchDeleteCc
Batch creating precise protection rules	policy	batchCreateCustom
Batch modifying precise protection rules	policy	batchUpdateCustom
Batch deleting precise protection rules	policy	batchDeleteCustom
Batch creating IP address blacklist and whitelist rules	policy	batchCreateWhiteblackip
Batch modifying IP address blacklist or whitelist rules	policy	batchUpdateWhiteblackip
Batch deleting IP address blacklist or whitelist rules	policy	batchDeleteWhiteblackip
Batch creating geolocation access control rules	policy	batchCreateGeoip

Operation	Resource Type	Trace Name
Batch modifying geolocation access control rules	policy	batchUpdateGeoip
Batch deleting geolocation access control rules	policy	batchDeleteGeoip
Batch creating/ updating web tamper protection rules	policy	batchCreateAntitamper
Batch enabling or disabling web tamper protection rules	policy	batchUpdateAntitamper
Batch deleting web tamper protection rules	policy	batchDeleteAntitamper
Batch creating information leakage prevention rules	policy	batchCreateAntileakage
Batch modifying information leakage prevention rules	policy	batchUpdateAntileakage
Batch deleting information leakage prevention rules	policy	batchDeleteAntileakage
Batch creating global protection whitelist rules	policy	batchCreateIgnore
Batch modifying global protection whitelist rules	policy	batchUpdateIgnore
Batch deleting global protection whitelist rules	policy	batchDeleteIgnore
Batch creating data masking rules	policy	batchCreatePrivacy
Batch modifying data masking rules	policy	batchUpdatePrivacy
Batch deleting data masking rules	policy	batchDeletePrivacy

Operation	Resource Type	Trace Name
Creating alarm notifications	alertNoticeConfig	createAlertNoticeConfig
Modifying alarm notifications	alertNoticeConfig	modifyAlertNoticeConfig
Deleting alarm notifications	alertNoticeConfig	deleteAlertNoticeConfig
Batch deleting alarm notifications	alertNoticeConfig	batchDeleteAlertNoticeConfig
Deleting a dedicated WAF instance	instance	deleteInstance
Creating a dedicated WAF instance	instance	createInstance
Updating a dedicated WAF instance	instance	upgradeInstance
Changing the instance name	instance	alterInstanceName
Adding an address group	ip-group	createIPGroup
Modifying an address group	ip-group	modifyIPGroup
Deleting an address group	ip-group	deleteIPGroup
Creating a reference table	valueList	createValueList
Modifying a reference table	valueList	modifyValueList
Deleting a reference table	valueList	deleteValueList
Creating a Report Template	SecurityReport	createSecurityReportSubscription
Modifying a security report template	SecurityReport	updateSecurityReportSubscription
Deleting a security report template	SecurityReport	deleteSecurityReportSubscription

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 of the New Edition**
- **Viewing Real-Time Traces in the Trace List of the Old Edition**

Constraints

- Traces of a single account can be viewed on the CTS console. Multi-account traces can be viewed only on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. To store operation records for more than seven days, you must configure an OBS bucket to transfer records to it. Otherwise, you cannot query the operation records generated seven days ago.
- After performing operations on the cloud, you can query management traces on the CTS console 1 minute later and query data traces on the CTS console 5 minutes later.

Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
   - **Trace Name**: Enter a trace name.
   - **Trace ID**: Enter a trace ID.
   - **Resource Name**: Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
   - **Resource ID**: Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
   - **Trace Source**: Select a cloud service name from the drop-down list.
   - **Resource Type**: Select a resource type from the drop-down list.
   - **Operator**: Select one or more operators from the drop-down list.

- **Trace Status**: Select **normal**, **warning**, or **incident**.
  - **normal**: The operation succeeded.
  - **warning**: The operation failed.
  - **incident**: The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
- Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.

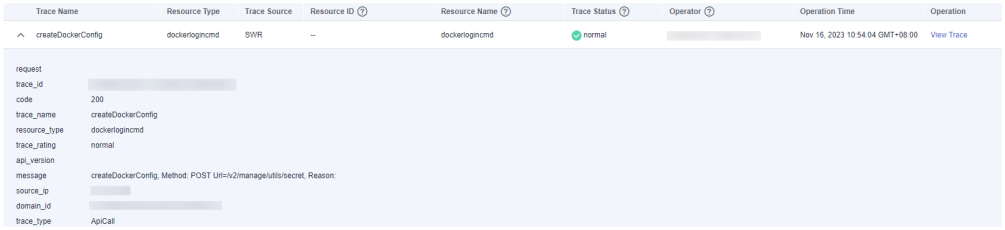
5. On the **Trace List** page, you can also export and refresh the trace list, and customize the list display settings.
   - Enter any keyword in the search box and click to filter desired traces.
   - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5000 records.
   - Click to view the latest information about traces.
   - Click to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled ( ), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

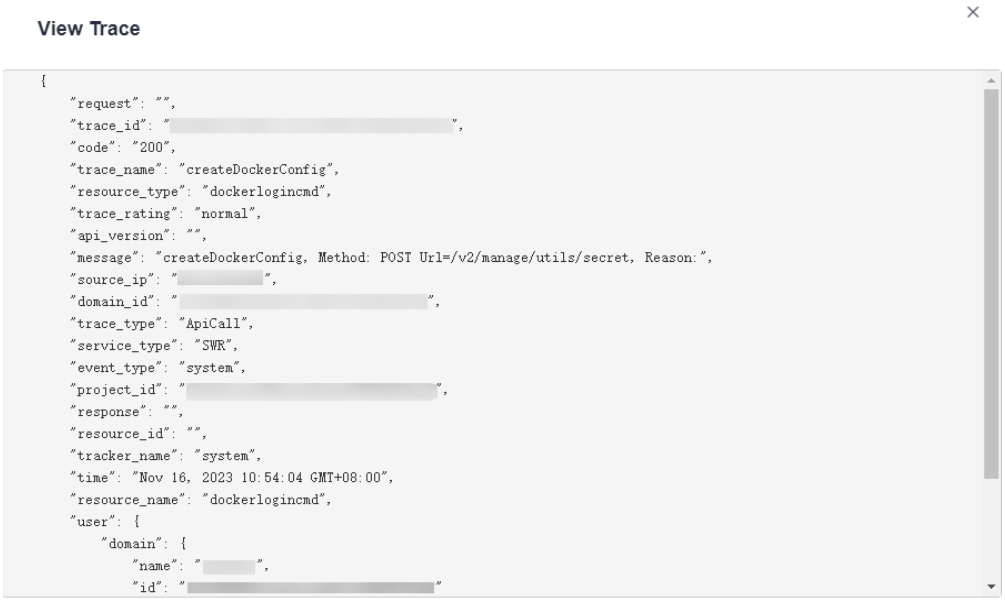
1. Log in to the management console.
2. Click in the upper left corner and choose **Management & Governance** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available:
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**: Select a filter from the drop-down list.
     - If you select **Resource ID** for **Search By**, specify a resource ID.
     - If you select **Trace name** for **Search By**, specify a trace name.
     - If you select **Resource name** for **Search By**, specify a resource name.
   - **Operator**: Select a user.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: 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.

6. Click **Query**.
7. On the **Trace List** page, you can also export and refresh the trace list.
   - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
   - Click to view the latest information about traces.
8. Click on the left of a trace to expand its details.



9. Click **View Trace** in the **Operation** column. The trace details are displayed.



10. For details about key fields in the trace structure, see **Trace Structure** and **Example Traces**.
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

A Change History

Released On	Description
2024-02-22	This issue is the 148th official release. Modified the following content: • **Configuring Custom Precise Protection Rules** • **Configuring a Global Protection Whitelist Rule to Ignore False Alarms**
2024-01-31	This issue is the 147th official release. Modified the following content: • **Buying a Cloud WAF Instance** • **Changing the Edition and Specifications of a Cloud WAF Instance** • **Dashboard** • **Viewing Protection Event Logs** • **Handling False Alarms** • **Policies** • **Process for Adding a Website to WAF (Cloud Mode-CNAME Access)** • **Advanced Settings** • **Basic Information** • **Enabling Alarm Notifications**
2023-11-30	This issue is the 146th official release. • Added the following content: – **Switching the Load Balancing Algorithm** • Modified the following content: – **Buying a Dedicated WAF Instance** – **Handling False Alarms** – **Policies**

Released On	Description
2023-11-15	This issue is the 145th official release. **Configuring PCI DSS/3DS Certification Check and TLS Version**: Modified some descriptions.
2023-11-10	This issue is the 144th official release. • Added the following content: **Adding a Website to WAF (Cloud Mode - ELB Access)** • Modified the following content: – **Buying a Cloud WAF Instance** – **WAF Operation Guide**
2023-11-03	This issue is the 143rd official release. Added the following content: **Permission Dependency of the WAF Console**
2023-10-10	This issue is the 142nd official release. Adjusted the document structure. • Added the following content: **Configuration Example: Adding a Domain Name to WAF** • Modified the following content: – **WAF Operation Guide** – **Managing Policies** – **Website Settings** – **How to Configure WAF Protection**
2023-09-13	This issue is the 141st official release. Modified the following content: • **Enabling WAF IPv6 Protection** • **Enabling the HTTP/2 Protocol** • **Configuring a Timeout for Connections Between WAF and a Website Server** • **Forwarding Custom Header Fields**
2023-09-08	This issue is the 140th official release. Modified the following content: **Authorizing and Associating an Enterprise Project**
2023-08-28	This issue is the 139th official release. Modified the following content: **Step 2: Configure a Load Balancer for WAF**
2023-08-09	This issue is the 138th official release. Modified the following content: **Ports Supported by WAF**

Released On	Description
2023-07-10	This issue is the 137th official release. • Added the following content: **Step 5: Test Dedicated WAF Instances** • Modified the following content: – **Enabling LTS for WAF Logging** – **WAF Operations Recorded by CTS**
2023-06-30	This issue is the 136th official release. • Added the following content: – **Security Reports** • Modified the following content: – **Configuring a Traffic Identifier for a Known Attack Source** – **Configuring Custom Precise Protection Rules** – **Configuring a CC Attack Protection Rule** – **Configuring a Global Protection Whitelist Rule to Ignore False Alarms** – **Buying a Cloud WAF Instance** – **Changing the Edition and Specifications of a Cloud WAF Instance** – **QPS Expansion Packages** – **Viewing Protection Event Logs**
2023-06-09	This issue is the 135th official release. Modified the following content: • **Upgrading a Dedicated WAF Instance**
2023-06-01	This issue is the 134th official release. Modified the following content: • **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)** • **Step 4: Modify the DNS Records of the Domain Name** • **Updating a Certificate** • **Viewing Information About a Dedicated WAF Instance**

Released On	Description
2023-04-30	This issue is the 133rd official release. • Added the following content: – **Migrating Domain Names to Other Enterprise Projects** – **Forwarding Custom Header Fields** • Modified the following content: – **Buying a Cloud WAF Instance** – **Buying a Dedicated WAF Instance** – **Changing the Edition and Specifications of a Cloud WAF Instance** – **Ports Supported by WAF** – **Step 1: Add a Website to WAF (Dedicated Mode)** – **Configuring PCI DSS/3DS Certification Check and TLS Version** – **Configuring Basic Protection Rules to Defend Against Common Web Attacks** – **Configuring Anti-Crawler Rules** – **Configuring Information Leakage Prevention Rules to Protect Sensitive Information from Leakage** – **Configuring Web Tamper Protection Rules to Prevent Static Web Pages from Being Tampered With** – **Managing Dedicated WAF Engines**
2023-04-20	This issue is the 132nd official release. Modified the following content: • **Step 2: Configure a Load Balancer for WAF** • **Step 1: Add a Website to WAF (Dedicated Mode)**
2023-04-14	This issue is the 131st official release. Modified the following content: • **Configuring a Timeout for Connections Between WAF and a Website Server**
2023-04-07	This issue is the 130th official release. **Configuring a Traffic Identifier for a Known Attack Source**: Modified some descriptions.
2023-03-16	This issue is the 129th official release. Modified the following content: • **Configuring Anti-Crawler Rules** • **Managing Dedicated WAF Engines**

Released On	Description
2023-03-13	This issue is the 128th official release. **Managing Dedicated WAF Engines**: Added the version iteration details for dedicated WAF.
2023-03-09	This issue is the 127th official release. **WAF Monitored Metrics**: Modified some descriptions.
2023-03-07	This issue is the 126th official release. **Step 2: Whitelist WAF IP Addresses**: Modified some descriptions.
2023-03-03	This issue is the 125th official release. Added the following content: • **Sharing a Certificate with Other Enterprise Projects** • **Changing the Edition and Specifications of a Cloud WAF Instance** • **Configuring a CC Attack Protection Rule** Updated the following content according to the new console: • **Buying a Cloud WAF Instance** • **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)** • **Viewing Basic Information** • **Viewing Certificate Information** • **Managing Dedicated WAF Engines** • **Dashboard** • **Events**
2023-02-22	This issue is the 124th official release. Modified the following content: • **QPS Expansion Packages** • **Buying a Cloud WAF Instance** • **Dashboard**
2023-01-17	This issue is the 123rd official release. **Configuration Example - Blocking Requests with null Fields**: Modified some descriptions.
2023-01-12	This issue is the 122nd official release. Added **Exporting Website Settings**.
2022-12-07	This issue is the one hundred and twenty-first official release. **Creating a Protection Policy**: Added descriptions of **Copy Policy**.

Released On	Description
2022-11-22	This issue is the one hundred and twentieth official release. **Configuring Custom Precise Protection Rules**: Modified some content.
2022-11-18	This issue is the one hundred and nineteenth official release. **Configuring Basic Protection Rules to Defend Against Common Web Attacks**: Added some descriptions.
2022-10-25	This issue is the 118th official release. Modified the following content: • **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)** • **Step 2: Whitelist WAF IP Addresses**
2022-10-08	This issue is the 117th official release. **Buying a Dedicated WAF Instance**: Modified constraints.
2022-09-07	This issue is the 116th official release. **Ports Supported by WAF**: Modified content.
2022-09-05	This issue is the 115th official release. Modified the following content: • **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**: Modified certain descriptions as some strings on the console were changed. • **Step 1: Add a Website to WAF (Dedicated Mode)**: Modified certain descriptions as some strings on the console were changed.
2022-08-26	This issue is the 114th official release. **Enabling Alarm Notifications**: Modified the alarm notification page.
2022-08-19	This issue is the 113th official release. Modified the following content: **Buying a Dedicated WAF Instance**
2022-08-16	This issue is the 112th official release. Modified the following content: • **WAF Operations Recorded by CTS**: Optimized parameter descriptions. • **Step 2: Configure a Load Balancer for WAF**: Added the procedure for adding WAF instances to an ELB load balancer.

Released On	Description
2022-08-03	This issue is the 111th official release. Modified the following content: • **Managing Dedicated WAF Engines**: Added the procedure for adding WAF instances to an ELB load balancer. • **WAF Monitored Metrics**: Modified descriptions of some parameters.
2022-07-21	This issue is the 110th official release. **Configuring Basic Protection Rules to Defend Against Common Web Attacks**: Added the descriptions of application type and protection type.
2022-07-18	This issue is the 109th official release. Optimized parameter descriptions in **Configuring a Global Protection Whitelist Rule to Ignore False Alarms**.
2022-07-06	This issue is the 108th official release. Modified the following content: • **Configuring a CC Attack Protection Rule**: Requests to **All WAF instances** are counted in a CC attack protection rule. • **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)** • **Enabling WAF IPv6 Protection**
2022-07-04	This issue is the 107th official release. Released the global protection whitelist function. Modified the following content: • **Configuring a Global Protection Whitelist Rule to Ignore False Alarms** • **Handling False Alarms** • **Adding Rules to One or More Policies** • **Configuring Basic Protection Rules to Defend Against Common Web Attacks** • **Viewing Basic Information** • **Switching WAF Working Mode**
2022-06-27	This issue is the 106th official release. Modified the following content: • **Buying a Cloud WAF Instance**: Updated screenshots of the purchase page. • **Configuring Basic Protection Rules to Defend Against Common Web Attacks**: Added **Shiro Decryption Check**.

Released On	Description
2022-06-22	This issue is the 105th official release. Modified the following content: • **Configuring a CC Attack Protection Rule**: Updated the document based on GUI changes. • **Configuring Geolocation Access Control Rules to Block or Allow Requests from Specific Locations**: Modified the descriptions.
2022-06-09	This issue is the 104th official release. Modified the following content: • **Configuring a Timeout for Connections Between WAF and a Website Server**: Modified the descriptions. • **Ports Supported by WAF**: Add new ports.
2022-06-06	This issue is the 103rd official release. Modified the following content: • **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**: Added constraints on whether to use a proxy. • **Step 4: Modify the DNS Records of the Domain Name**: Modified the descriptions.
2022-05-30	This issue is the 102nd official release. • Added the following topic: **Ports Supported by WAF** • Modified the following topic: **Configuring Geolocation Access Control Rules to Block or Allow Requests from Specific Locations**
2022-05-26	This issue is the 101st official release. Modified the following content: • **Configuring a Global Protection Whitelist Rule to Ignore False Alarms**: Supported the modifying of false alarm masking rules. • **Adding Rules to One or More Policies**: Added batch modification, deletion, and closing operations to the **Other Operations** section. • **Dashboard**: Changed parameter descriptions. • **Configuring a Timeout for Connections Between WAF and a Website Server**: Added region constraints. • **Enabling Break Protection**: Added region constraints. • **Switching the Load Balancing Algorithm**: Added region constraints.

Released On	Description
2022-05-13	This issue is the 100th official release. Modified the following content: • **Buying WAF**: Adjusted the document structure. • **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**: Add a new topic to describe how to import a certificate.
2022-05-06	This issue is the ninety-ninth official release. Modified **Configuring a Global Protection Whitelist Rule to Ignore False Alarms**.
2022-05-05	This issue is the ninety-eighth official release. Added constraints in **Viewing Certificate Information**.
2022-04-27	This issue is the ninety-seventh official release. Added **Configuring Intelligent Access Control Rules to Accurately Defend Against CC Attacks**.
2022-04-24	This issue is the ninety-sixth official release. • Added the following content: – **Enabling Break Protection** – **Switching the Load Balancing Algorithm** • Modified the following content: – **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)** – **Switching the Load Balancing Algorithm**
2022-04-19	This issue is the ninety-fifth official release. • Added the following content: – **Enabling WAF IPv6 Protection** – **Enabling the HTTP/2 Protocol** – **Configuring a Timeout for Connections Between WAF and a Website Server** • Modified the following content: – **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)** – **Viewing Basic Information** – **WAF Monitored Metrics**
2022-04-12	This issue is the ninety-fourth official release. Modified related descriptions in **WAF Monitored Metrics**.

Released On	Description
2022-04-07	This issue is the ninety-third official release. • **Configuring Anti-Crawler Rules**: Added constraints. • **Step 2: Configure a Load Balancer for WAF**: Added some prerequisites.
2022-03-29	This issue is the ninety-second official release. Optimized the following content: • **WAF Operation Guide**: Added the website service descriptions. • **WAF Monitored Metrics**: Changed the packet rate unit. • **Switching WAF Working Mode**: Added the description of WAF bypass.
2022-03-22	This issue is the ninety-first official release. Optimized **Step 1: Add a Website to WAF (Dedicated Mode)**.
2022-03-17	This issue is the ninetieth official release. **How to Configure WAF Protection**: Modified content.
2022-03-07	This issue is the eighty-ninth official release. Modified the following content as dedicated WAF instances are provided: • **Buying a Dedicated WAF Instance** • **Connecting a Website to WAF (Dedicated Mode)** • **Basic Information** • **Uploading a Certificate** • **Adding an IP Address Group** • **Configuring Custom Precise Protection Rules** • **Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses** • **Managing Policies**
2022-02-11	This issue is the eighty-eighth official release. Modified related descriptions in **Configuring Web Tamper Protection Rules to Prevent Static Web Pages from Being Tampered With**.
2022-01-30	This issue is the eighty-seventh official release. • **How to Configure WAF Protection**: Optimized descriptions. • **Configuring Basic Protection Rules to Defend Against Common Web Attacks**: Optimized descriptions.

Released On	Description
2022-01-06	This issue is the eighty-sixth official release. **Configuring a Global Protection Whitelist Rule to Ignore False Alarms**: Optimized descriptions.
2021-12-30	This issue is the eighty-fifth official release. Added "Monitoring."
2021-12-20	This issue is the eighty-fourth official release. • Optimized descriptions in **Adding an IP Address Group**. • Optimized descriptions in **Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses**.
2021-12-10	This issue is the eighty-third official release. Added the descriptions of the new configuration rule in **Configuring Geolocation Access Control Rules to Block or Allow Requests from Specific Locations**.
2021-11-24	This issue is the eighty-second official release. Added configuration examples in "Rule Configuration."
2021-10-25	This issue is the eighty-first official release. • Added "Managing IP Address Group Blacklist and Whitelist." • Updated some screenshots and description in "Certificate Management." • Updated screenshots and descriptions in **Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses**.
2021-09-27	This issue is the eightieth official release. Updated some screenshots in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**.
2021-08-12	This issue is the seventy-ninth official release. Optimized descriptions in **Buying a Cloud WAF Instance**.
2021-08-06	This issue is the seventy-eighth official release. Renamed WAF editions: Rename professional edition standard edition, enterprise edition professional edition, and premium edition platinum edition.
2021-07-19	This issue is the seventy-seventh official release. Updated the description about how to access the management console.
2021-07-14	This issue is the seventy-sixth official release. Added restrictions on pushing SCM certificate to WAF in **Uploading a Certificate**.

Released On	Description
2021-07-08	This issue is the seventy-fifth official release. • **Changing the Edition and Specifications of a Cloud WAF Instance**: Optimized some descriptions. • Added constraints in **Configuring Custom Precise Protection Rules**.
2021-05-27	This issue is the seventy-fourth official release. Optimized descriptions in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**.
2021-05-18	This issue is the seventy-third official release. Optimized descriptions in **Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses**.
2021-05-12	This issue is the seventy-second official release. Added **Process for Adding a Website to WAF (Cloud Mode-CNAME Access)**.
2021-04-30	This issue is the seventy-first official release. • Added **Rule Expansion Packages**. • Updated some screenshots in **Dashboard**. • Updated some screenshots and descriptions in **Buying a Cloud WAF Instance**.
2021-04-15	This issue is the seventieth official release. • Optimized descriptions in **Step 3: Test WAF**. • Optimized the description of check items in **Configuring Anti-Crawler Rules**.
2021-03-11	This issue is the sixty-ninth official release. Added **Viewing Product Details**.
2021-02-25	This issue is the sixty-eighth official release. • Added **Authorizing and Associating an Enterprise Project**. • Added the description of header detection in **Configuring Basic Protection Rules to Defend Against Common Web Attacks**. • Updated the supported actions in **WAF Permissions and Supported Actions**.
2021-02-09	This issue is the sixty-seventh official release. Added the description of the JavaScript anti-crawler detection in **Configuring Anti-Crawler Rules**.

Released On	Description
2021-02-05	This issue is the sixty-sixth official release. • Added the procedure for buying WAF instances billed on a pay-per-use basis in **Buying a Cloud WAF Instance**. • Added the description of the pay-per-use billing mode for cloud instances in "Configuring a Protection Rule."
2021-01-25	This issue is the sixty-fifth official release. **Changing the Edition and Specifications of a Cloud WAF Instance**: Optimized some descriptions.
2020-12-31	This issue is the sixty-fourth official release. • Updated screenshots and descriptions in **Configuring Basic Protection Rules to Defend Against Common Web Attacks**. • Updated screenshots and descriptions in **Configuring Anti-Crawler Rules**. • Updated screenshots and descriptions in **Dashboard**.
2020-12-11	This issue is the sixty-third official release. Deleted the description of the pay-per-use billing mode for the cloud mode.
2020-11-18	This issue is the sixty-second official release. • **Configuring a CC Attack Protection Rule**: Optimized some descriptions. • Optimized descriptions in **Configuring Custom Precise Protection Rules**. • Optimized descriptions in **Handling False Alarms**.
2020-10-22	This issue is the sixty-first official release. • Optimized descriptions in **Configuring PCI DSS/3DS Certification Check and TLS Version**. • Updated some screenshots in **Updating a Certificate**. • **Configuring a CC Attack Protection Rule**: Optimized some descriptions. • Optimized descriptions in **Creating a Reference Table to Configure Protection Metrics In Batches**.
2020-09-23	This issue is the sixtieth official release. **Configuring a CC Attack Protection Rule**: Optimized the usage restrictions of the advanced mode.

Released On	Description
2020-09-11	This issue is the fifty-ninth official release. • Added the procedure for how to buy cloud WAF instances billed on a pay-per-use basis in **Buying a Cloud WAF Instance**. • Added the description of the pay-per-use billing mode in "Configuring a Protection Rule."
2020-08-27	This issue is the fifty-eighth official release. Added the description of enabling compliance certification checks in **Configuring PCI DSS/3DS Certification Check and TLS Version**.
2020-08-25	This issue is the fifty-seventh official release. • Added **Configuring a Traffic Identifier for a Known Attack Source** • Added **Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration**. • Added the description of known attack source protection in **Configuring Basic Protection Rules to Defend Against Common Web Attacks**, **Configuring Custom Precise Protection Rules**, and **Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses**.
2020-08-19	This issue is the fifty-sixth official release. Added log field description in **Enabling LTS for WAF Logging**.
2020-08-12	This issue is the fifty-fifth official release. • Added section "Certificate Management" • Updated the certificate description in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**.
2020-08-06	This issue is the fifty-fourth official release. Added the description of protection rules in **Configuring Basic Protection Rules to Defend Against Common Web Attacks**.
2020-07-20	This issue is the fifty-third official release. • **Configuring a CC Attack Protection Rule**: Added operation restrictions. • Added operation restrictions in **Handling False Alarms**.
2020-07-08	This issue is the fifty-second official release. • Updated screenshots in "Event Management." • Added descriptions of cipher suite 4 in **Configuring PCI DSS/3DS Certification Check and TLS Version**.

Released On	Description
2020-06-22	This issue is the fifty-first official release. Added **WAF Custom Policies** and **WAF Permissions and Supported Actions**.
2020-06-16	This issue is the fiftieth official release. • Updated the screenshots in **Configuring Anti-Crawler Rules**. • Optimized descriptions in **Updating a Certificate**.
2020-05-26	This issue is the forty-ninth official release. • **Buying a Cloud WAF Instance** and **Changing the Edition and Specifications of a Cloud WAF Instance**: Added some descriptions. • Added compatibility description of cipher suites in **Configuring PCI DSS/3DS Certification Check and TLS Version**. • Optimized the description of path parameters in **Configuring Web Tamper Protection Rules to Prevent Static Web Pages from Being Tampered With**.
2020-04-28	This issue is the forty-eighth official release. • Added **Enabling LTS for WAF Logging**. • Optimized descriptions in **Configuring PCI DSS/3DS Certification Check and TLS Version**. • Updated screenshots in section "Event Management."
2020-03-31	This issue is the forty-seventh official release. Updated some screenshots.
2020-03-12	This issue is the forty-sixth official release. Modified reference links in **Creating a User Group and Granting Permissions**.
2020-02-27	This issue is the forty-fifth official release. • Added **Configuring PCI DSS/3DS Certification Check and TLS Version**. • Updated screenshots and parameter descriptions in **Dashboard**. • Updated screenshots and descriptions in **Configuring a Global Protection Whitelist Rule to Ignore False Alarms**. • Updated screenshots and descriptions in **Handling False Alarms**.
2020-02-18	This issue is the forty-fourth official release. Modified descriptions and added alarm notification email examples in **Enabling Alarm Notifications**.

Released On	Description
2020-02-10	This issue is the forty-third official release. • **Changing the Edition and Specifications of a Cloud WAF Instance**: Added. • Optimized descriptions in **Buying a Cloud WAF Instance**. • Optimized descriptions in **Domain Name Expansion Package**. • Optimized descriptions in **QPS Expansion Packages**.
2019-12-26	This issue is the forty-second official release. Optimized descriptions in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**.
2019-12-24	This issue is the forty-first official release. • Optimized descriptions in **Buying a Cloud WAF Instance**. • Optimized descriptions in **Domain Name Expansion Package**. • Optimized descriptions in **Enabling Alarm Notifications**.
2019-12-16	This issue is the fortieth official release. • Updated the navigation path illustration. • Domain name switchover
2019-12-09	This issue is the thirty-ninth official release. • Optimized descriptions in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**. • Optimized descriptions in **Domain Name Expansion Package**. • Optimized descriptions in **Creating a Reference Table to Configure Protection Metrics In Batches**. • Optimized descriptions in **Creating a Protection Policy**. • Optimized descriptions in **Adding a Domain Name to a Policy**.
2019-11-28	This issue is the thirty-eighth official release. Optimized descriptions in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**.
2019-11-26	This issue is the thirty-seventh official release. • Optimized descriptions in **Domain Name Expansion Package**. • Optimized descriptions in **QPS Expansion Packages**.
2019-11-12	This issue is the thirty-sixth official release. Added **Viewing Protection Event Logs**.

Released On	Description
2019-11-07	This issue is the thirty-fifth official release. • Added **Modifying the Alarm Page**. • Optimized descriptions in **Viewing Basic Information**. • **Configuring a CC Attack Protection Rule**: Optimized some descriptions. • Optimized descriptions in **Creating a Reference Table to Configure Protection Metrics In Batches**.
2019-11-05	This issue is the thirty-fourth official release. • Optimized descriptions in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**. • Optimized descriptions in **Editing Server Information**. • Optimized descriptions in **Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses**.
2019-10-17	This issue is the thirty-third official release. • Optimized descriptions in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**. • Optimized descriptions in **Step 4: Modify the DNS Records of the Domain Name**. • Optimized descriptions in **Editing Server Information**. • Optimized descriptions in **Updating a Certificate**. • Optimized descriptions in **Configuring Basic Protection Rules to Defend Against Common Web Attacks**.
2019-10-14	This issue is the thirty-second official release. • Optimized descriptions in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**. • Optimized descriptions in **Viewing Basic Information**. • Optimized descriptions in **Updating a Certificate**. • Optimized descriptions in **Configuring Basic Protection Rules to Defend Against Common Web Attacks**. • **Configuring a CC Attack Protection Rule**: Optimized some descriptions. • Optimized descriptions in **Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses**.
2019-10-11	This issue is the thirty-first official release. • Modified section "Rule Configurations": **Rule Status** and **Log only** are added. • Modified section "Policy Management": **Rule Status** is added.

Released On	Description
2019-09-25	This issue is the thirtieth official release. • Added the description of QPS in **Buying a Cloud WAF Instance**. • Added remarks in **Handling False Alarms**.
2019-09-06	This issue is the twenty-ninth official release. • Optimized descriptions in **Updating a Certificate**. • Optimized descriptions in **Configuring Basic Protection Rules to Defend Against Common Web Attacks**. • **Configuring a CC Attack Protection Rule**: Optimized some descriptions.
2019-09-04	This issue is the twenty-eighth official release. Optimized descriptions in **Step 4: Modify the DNS Records of the Domain Name**.
2019-08-28	This issue is the twenty-seventh official release. • **Configuring a CC Attack Protection Rule**: Modified descriptions due to protection optimization. • Modified descriptions in **Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses** due to protection effect optimization.
2019-08-20	This issue is the twenty-sixth official release. Optimized some illustrations in the document.
2019-08-15	This issue is the twenty-fifth official release. • Added the configuration description of TXT records in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**. • Added the configuration description of TXT records in **Step 4: Modify the DNS Records of the Domain Name**. • Added descriptions of some parameters in **Downloading Events Data**.
2019-08-08	This issue is the twenty-fourth official release. • Optimized descriptions in **Buying a Cloud WAF Instance**. • Modified section "Rule Configurations" and added parameter **Rule Description** to the user-defined rule.
2019-07-02	This issue is the twenty-third official release. Optimized descriptions in **Step 4: Modify the DNS Records of the Domain Name**.

Released On	Description
2019-06-18	This issue is the twenty-second official release. • Optimized descriptions in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**. • Optimized descriptions in **Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses**.
2019-06-06	This issue is the twenty-first official release. • Added configuration examples in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**. • Optimized descriptions in **Configuring Basic Protection Rules to Defend Against Common Web Attacks**. • Optimized descriptions in **Handling False Alarms**.
2019-05-30	This issue is the twentieth official release. • Optimized descriptions in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**. • Optimized descriptions in **Step 4: Modify the DNS Records of the Domain Name**.
2019-05-14	This issue is the nineteenth official release. • Optimized descriptions in **Updating a Certificate**. • Modified "Rule Configurations."
2019-05-05	This issue is the eighteenth official release. Optimized descriptions in **Editing Server Information**.
2019-04-25	This issue is the seventeenth official release. • Added the description of the **Minimum TLS Version** in **Viewing Basic Information**. • Added the description of local authentication in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**. • Added the description of local authentication in **Step 4: Modify the DNS Records of the Domain Name**. • Added descriptions of three new fields in **Configuring Custom Precise Protection Rules**.
2019-03-30	This issue is the sixteenth official release. Added the description of the domain name list parameter in **Viewing Basic Information**.
2019-02-14	This issue is the fifteenth official release. • Optimized descriptions in **Deleting a Protected Website from WAF**. • Updated the screenshots based on the GUI changes.

Released On	Description
2019-01-03	This issue is the fourteenth official release. Adjusted the document layout.
2018-12-05	This issue is the thirteenth official release. Optimized descriptions in **Enabling Alarm Notifications**.
2018-11-15	This issue is the twelfth official release. • Modified screenshots and related descriptions in "Rule Configurations." • Optimized descriptions in **Step 4: Modify the DNS Records of the Domain Name**. • Optimized descriptions in **Enabling Alarm Notifications**.
2018-10-29	This issue is the eleventh official release. Optimized descriptions in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**.
2018-10-16	This issue is the tenth official release. • Optimized descriptions in **Creating a Protection Policy**. • Optimized descriptions in **Adding Rules to One or More Policies**. • Optimized descriptions in **Adding a Domain Name to a Policy**.
2018-08-09	This issue is the ninth official release. • Added **Creating a Reference Table to Configure Protection Metrics In Batches**. • Optimized descriptions in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**. • Optimized descriptions in **Configuring Custom Precise Protection Rules**. • Optimized descriptions in **Handling False Alarms**.
2018-08-02	This issue is the eighth official release. • Added **Downloading Events Data**. • Optimized descriptions in **Viewing Basic Information**. • Optimized descriptions in **Handling False Alarms**. • Optimized descriptions in **Viewing Protection Event Logs**. • Optimized descriptions in **Enabling Alarm Notifications**.
2018-07-19	This issue is the seventh official release. • Optimized descriptions in **Viewing Basic Information**. • Optimized descriptions in **Handling False Alarms**. • Updated the screenshots based on the GUI changes.

Released On	Description
2018-07-05	This issue is the sixth official release. • Optimized descriptions in **Configuring Basic Protection Rules to Defend Against Common Web Attacks**. • **Configuring a CC Attack Protection Rule**: Optimized some descriptions. • Optimized descriptions in **Configuring Custom Precise Protection Rules**. • Optimized descriptions in **Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses**. • Optimized descriptions in **Configuring Geolocation Access Control Rules to Block or Allow Requests from Specific Locations**. • Optimized descriptions in **Configuring Web Tamper Protection Rules to Prevent Static Web Pages from Being Tampered With**. • Optimized descriptions in **Configuring Anti-Crawler Rules**. • Optimized descriptions in **Configuring Information Leakage Prevention Rules to Protect Sensitive Information from Leakage**. • Optimized descriptions in **Configuring a Global Protection Whitelist Rule to Ignore False Alarms**. • Optimized descriptions in **Configuring Data Masking Rules to Prevent Privacy Information Leakage**. • Optimized descriptions in **Adding Rules to One or More Policies**.
2018-06-14	This issue is the fifth official release. • Optimized descriptions in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**. • Optimized descriptions in **Deleting a Protected Website from WAF**. • Updated the screenshots based on the GUI changes.
2018-06-07	This issue is the fourth official release. **Configuring a CC Attack Protection Rule**: Optimized some descriptions.
2018-05-31	This issue is the third official release. • Optimized descriptions in **Configuring Basic Protection Rules to Defend Against Common Web Attacks**. • Optimized descriptions in **Configuring Custom Precise Protection Rules**.

Released On	Description
2018-05-17	This issue is the second official release. Optimized descriptions in **Step 1: Add a Domain Name to WAF (Cloud Mode - CNAME Access)**.
2018-05-10	This issue is the first official release.

