Web Application Firewall

User Guide

Issue	06
Date	2023-10-30

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Introduction

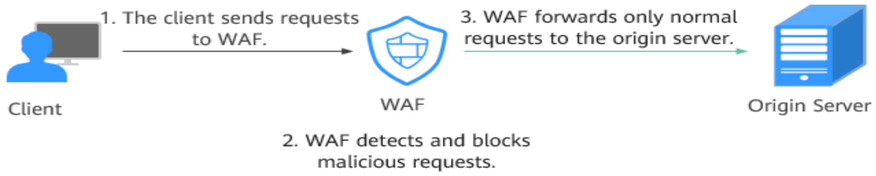
1.1 Web Application Firewall

Web Application Firewall (WAF) keeps web services stable and secure. It examines all HTTP and HTTPS requests to detect and block the following attacks: Structured Query Language (SQL) injection, cross-site scripting (XSS), web shells, command and code injections, file inclusion, sensitive file access, third-party vulnerability exploits, Challenge Collapsar (CC) attacks, malicious crawlers, and cross-site request forgery (CSRF).

How WAF Works

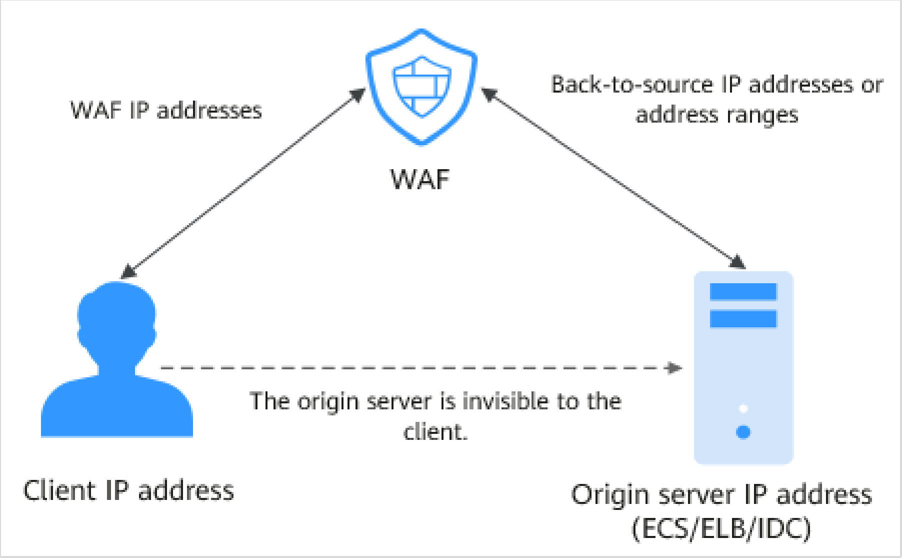
After enabling WAF, add the website to WAF on the WAF console. After a website is connected to WAF, all website access requests are forwarded to WAF first. WAF detects and filters out malicious attack traffic, and returns normal traffic to the origin server to ensure that the origin server is secure, stable, and available.

Figure 1-1 How WAF works for CNAME or dedicated access


1. The client sends requests to WAF.
3. WAF forwards only normal requests to the origin server.
Client
WAF
Origin Server
2. WAF detects and blocks malicious requests.

The process of forwarding traffic from WAF to origin servers is called back-to-source. WAF uses back-to-source IP addresses to send client requests to the origin server. When a website is connected to WAF, the destination IP addresses to the client are the IP addresses of WAF, so that the origin server IP address is invisible to the client.

Figure 1-2 Back-to-source IP address


WAF IP addresses
WAF
Back-to-source IP addresses or address ranges
The origin server is invisible to the client.
Client IP address
Origin server IP address (ECS/ELB/IDC)

Protection object

WAF offers the cloud and dedicated modes to protect websites. You can add either domain names or IP addresses to WAF. Before you start, get familiar with the following differences:

- Cloud mode: protects your cloud and on-premises web applications as long as they have domain names.
- Dedicated mode: protects your cloud web applications as long as they have domain names or IP addresses.

1.2 Functions

WAF makes it easier for you to handle web security risks.

Protection for IP Addresses and Domain Names (Wildcard, Top-level, and Second-Level Domain Names)

WAF offers the cloud and dedicated modes to protect websites. You can add either domain names or IP addresses to WAF. Before you start, get familiar with the following differences:

- Cloud mode: protects your cloud and on-premises web applications as long as they have domain names.
- Dedicated mode: protects your cloud web applications as long as they have domain names or IP addresses.

HTTP/HTTPS Service Protection

WAF keeps applications stable and secure. It examines HTTP and HTTPS requests to detect and block attacks, such as Structure Query Language (SQL) injections, cross-site scripting (XSS), web shells, command or code injections, file inclusion, sensitive file access, third-party vulnerability exploits, CC attacks, malicious crawlers, and cross-site request forgery (CSRF).

WebSocket/WebSockets

WAF supports the WebSocket/WebSockets protocol, which is enabled by default.

PCI DSS/PCI 3DS Compliance Certification and TLS Checks

- TLS has three versions (TLS v1.0, TLS v1.1, and TLS v1.2) and seven cipher suites. You can select the one best fits your business needs.
- WAF supports PCI DSS and PCI 3DS compliance certification check.

Basic Web Protection

With an extensive preset reputation database, WAF defends against Open Web Application Security Project (OWASP) top 10 threats, vulnerability exploits, web shells, and other threats.

- All-around protection

  WAF detects and blocks varied attacks, such as SQL injection, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, directory (path) traversal attacks, sensitive file access, command and code injections, web shells, backdoors, malicious HTTP requests, and third-party vulnerability exploits.
- Precise identification
  - WAF uses built-in semantic analysis engine and regex engine and supports configuring of blacklist/whitelist rules, which reduces false positives.
  - WAF supports anti-escape and automatic restoration of common codes, which improves the capability of recognizing deformation web attacks.

    WAF can decode the following types of code: url_encode, Unicode, XML, OCT, hexadecimal, HTML escape, and base64 code, case confusion, JavaScript, shell, and PHP concatenation confusion

CC Attack Prevention

A CC attack protection rule can limit access to a specific path (URL) of the protected website based on a specific IP address, cookie, or referer in access requests. So, WAF can accurately identify and mitigate CC attacks, such as brute-force attacks by exploiting weak passwords. Protective actions of CC attack protection rules include **Verification code**, **Block**, **Dynamically block**, and **Log only**.

- Flexible policy configuration

  WAF allows you to flexibly set rate limiting policies by IP address, cookie, or Referer field.
- Returned page customization

  You can customize returned content and page types to meet diverse service needs.

GUI-based Security Data

WAF provides a GUI-based interface for you to monitor attack information and event logs in real time.

- Centralized policy configuration

  On the WAF console, you can configure policies applicable to multiple protected domain names in a centralized manner so that the policies can be quickly delivered and take effect.

- Traffic and event statistics

  WAF displays the number of requests, the number and types of security events, and log information in real time.

Non-Standard Ports

WAF can protect standard ports, such as 80 and 443 and a wide range of non-standard ports.

Table 1-1 Ports supported by WAF

Deployment Mode	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
Cloud mode	Standard ports	80	443	Unlimited
	Non-standard ports (86 in total)	81, 82, 83, 84, 86, 87, 88, 89, 800, 808, 5000, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8999, 8011, 8012, 8013, 8014, 8015, 8016, 8017, and 8070	4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, and 8805	20
Dedicated mode	Standard ports	80	443	Unlimited

Deployment Mode	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
	Non-standard ports (182 in total)	9945, 9770, 81, 82, 83, 84, 88, 89, 800, 808, 1000, 1090, 3128, 3333, 3501, 3601, 4444, 5000, 5222, 5555, 5601, 6001, 6666, 6788, 6789, 6842, 6868, 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, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9802, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702, 8011, 8012, 8013, 8014,	8750, 8445, 18010, 4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, 8805, 9999	Unlimited

Deployment Mode	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
		8015, 8016, 8017, and 8070		

Precise Protection

Support precise logic- and parameter-based access control policies.

- A variety of parameter conditions

  Set conditions with combinations of common HTTP parameters, such as **IP**, **URL**, **Referer**, **User Agent**, **Params**, and **Header**.
- Abundant logical conditions

  WAF blocks or allows traffic based on logical conditions, such as "Include", "Exclude", "Equal to", "Not equal to", "Prefix is", and "Prefix is not."

Malicious Scanner and Crawler Prevention

Blocks web page crawling with user-defined scanner and crawler rules. This feature improves protection accuracy.

IP Address Blacklist and Whitelist

This function allows you to blacklist or whitelist IP addresses or an IP address range to improve defense accuracy.

Known Attack Source

- 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.
- Known attack source rules can be set based on attacks blocked against the basic web protection, precise access protection, and blacklist and whitelist rules.

Connection Protection

If a large number of 502 Bad Gateway or 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 starts corresponding protection for your website.

Configuring Connection Timeout

- The default timeout duration for connections between a browser and WAF is 120 seconds, which cannot be manually set.

- The default timeout duration for connections between WAF and your origin server is 60 seconds. If you use a dedicated WAF instance or cloud WAF instance in the professional edition (the formerly enterprise edition) or platinum edition (the formerly ultimate edition), you can customize a timeout duration.

  In the **Basic Information** area on the website information page, enable **Timeout Settings**. Then, click ✎ next to **WAF-to-Server Connection Timeout**, **Read Timeout**, and **Write Timeout**, modify settings one by one, and click ✓ to save.

Geolocation Access Control

You can allow some web requests and block others based on the geographical locations of IP addresses that the requests originate from.

Web Page Tampering Prevention

You can configure cache for static web pages. When a user accesses a web page, the system returns a cached page to the user and randomly checks whether the page is tampered with.

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.

- Feature library

  Blocks web page crawling with user-defined scanner and crawler rules. This feature improves protection accuracy.

- JavaScript

  Identifies and blocks JavaScript crawling with user-defined rules.

Global Protection Whitelist (formerly False Alarm Masking)

This function enables you to ignore certain attack detection rules for specific requests.

Data Masking

WAF masks sensitive information, such as usernames and passwords, in the event log.

Information Leakage Prevention

WAF prevents your sensitive information from being disclosed on web pages, such as ID numbers, phone numbers, and email addresses.

Reliable

WAF can be deployed on multiple clusters in multiple regions based on the load balancing principle. This can prevent single point of failures (SPOFs) and ensure online smooth capacity expansion, maximizing service stability.

Alarm Notification

You can enable notification for attack logs. Once this function is enabled, WAF sends attack logs to you by the method you configure.

Event Management

- WAF allows you to view and handle false alarms for blocked or logged events.
- You can download events data over the past five days.

1.3 Edition Differences

WAF provides cloud and dedicated modes for you to deploy WAF instances. For more details, see **Cloud and Dedicated WAF Modes**.

Cloud and Dedicated WAF Modes

You can select the cloud WAF and/or dedicated WAF instances to meet your business needs. For their differences, see **Table 1-2**. **Figure 1-3** shows deployment architectures.

Figure 1-3 Cloud and dedicated WAF deployment architectures

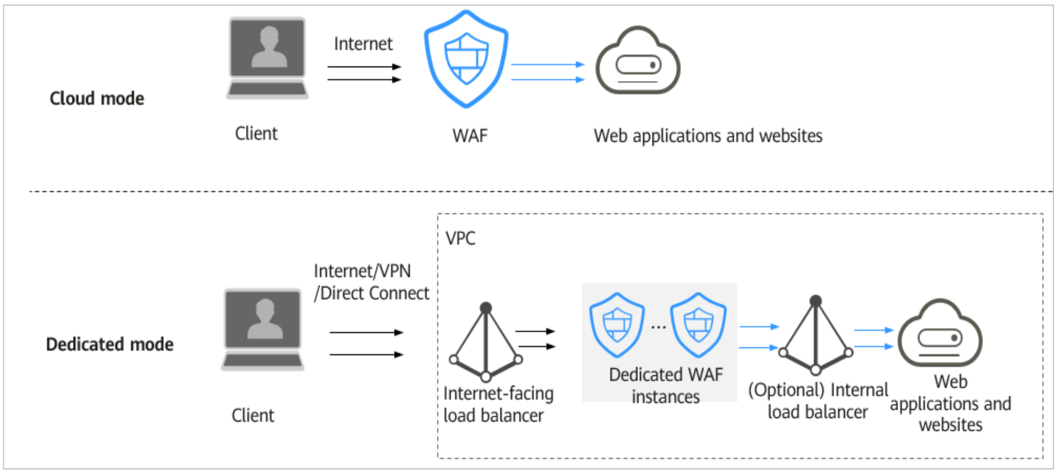

Cloud mode
Client
Internet
WAF
Web applications and websites
Dedicated mode
Client
Internet/VPN
/Direct Connect
VPC
Internet-facing load balancer
Dedicated WAF instances
(Optional) Internal load balancer
Web applications and websites

Table 1-2 Description of how to use different modes of WAF instances

Item	Cloud Mode	Dedicated mode
Billing mode	Pay-per-use	Pay-per-use

Item	Cloud Mode	Dedicated mode
Application scenarios	Service servers are deployed on a cloud or in on-premises data centers.	Service servers are deployed on a cloud. Dedicated WAF instances are suitable large enterprise websites that have a large service scale and have customized security requirements.
Protection objects	Domain names	● Domain names ● IP addresses
Advantages	● Protection capability scaling by upgrading specifications ● Protection for cloud and on-premises web services	● Flexible deployment ● Exclusive use of WAF instances ● Protection against large-scale traffic attacks ● Low network latency with dedicated WAF instances being deployed in a VPC

Specifications Supported by Each Edition

Table 1-3 lists the specifications of cloud WAF and a dedicated WAF instance.

Table 1-3 Applicable service scale

Service Scale	Cloud Mode	Dedicated Mode
Peak rate of normal service requests	-	The following lists the specifications of a single instance. ● 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 **NOTICE** Maximum QPS values are for reference only. They may vary depending on your businesses. The real-world QPS is related to the request size and the type and quantity of protection rules you customize.
Service bandwidth threshold (Origin servers are deployed on the cloud.)	-	● Specifications: WI-500. Referenced performance: Throughput: 500 Mbit/s ● Specifications: WI-100. Referenced performance: Throughput: 100 Mbit/s
Number of domain names	30 (Supports three top-level domain names.)	2,000 (Supports 2,000 top-level domain names)

Service Scale	Cloud Mode	Dedicated Mode
Back-to-source IP address quantity (the number of WAF IP addresses that can be allowed by a protected domain name)	20	N/A
Quantity of supported ports	N/A	● Standard ports: 80 and 443 ● Non-standard ports: Unlimited
Peak rate of CC attack protection	N/A	● Specifications: WI-500. Referenced performance: Maximum QPS: 20,000 ● Specifications: WI-100. Referenced performance: Maximum QPS: 4,000
CC attack protection rules	200	100
Precise protection rules	1,000	100
Reference table rules	1,000	100
IP address blacklist and whitelist rules	2,000	100
Geolocation access control rules	200	100
Web tamper protection rules	200	100
Information leakage prevention rules	200	100
Global protection whitelist rules	2,000	1,000
Data masking rules	200	100

1.4 Product Advantages

WAF examines web traffic from multiple dimensions to accurately identify malicious requests and filter attacks, reducing the risks of data being tampered with or stolen.

Precisely and Efficiently Identify Threats

- WAF uses rule and AI dual engines and integrates our latest security rules and best practices.
- You can configure enterprise-grade policies to protect your website more precisely, including custom alarm pages, combining multiple conditions in a CC attack protection rule, and blacklisting or whitelisting a large number of IP addresses.

Strong Protection for User Data Privacy

- Sensitive information, such as accounts and passwords, in attack logs can be anonymized.
- PCI-DSS checks for SSL encryption are available.
- The minimum TLS protocol version and cipher suite can be configured.

1.5 Application Scenarios

Common protection

WAF helps you defend against common web attacks, such as command injection and sensitive file access.

Protection for online shopping mall promotion activities

Countless malicious requests may be sent to service interfaces during online promotions. WAF allows configurable rate limiting policies to defend against CC attacks. This prevents services from breaking down due to many concurrent requests, ensuring response to legitimate requests.

Protection against zero-day vulnerabilities

Services cannot recover quickly from impact of zero-day vulnerabilities in third-party web frameworks and plug-ins. WAF updates the preset protection rules immediately to add an additional protection layer to such web frameworks and plug-ins, and this layer can react faster than fixing the vulnerabilities.

Data leakage prevention

WAF prevents malicious actors from using methods such as SQL injection and web shells to bypass application security and gain remote access to web databases. You can configure anti-data leakage rules on WAF to provide the following functions:

- Precise identification

  WAF uses semantic analysis & regex to examine traffic from different dimensions, precisely detecting malicious traffic.
- Distortion attack detection

  WAF detects a wide range of distortion attack patterns with 7 decoding methods to prevent bypass attempts.

Web page tampering prevention

WAF ensures that attackers cannot leave backdoors on your web servers or tamper with your web page content, preventing damage to your credibility. You can configure web tamper protection rules on WAF to provide the following functions:

- Website malicious code detection

  You can configure WAF to detect malicious code injected into web servers and ensure secure visits to web pages.

- Web page tampering prevention

  WAF prevents attackers from tampering with web page content or publishing inappropriate information that can damage your reputation.

1.6 About Billing

WAF instances can be billed monthly or on a pay-per-use basis, which is postpaid.

Billing Items

Figure 1-4 WAF billing modes

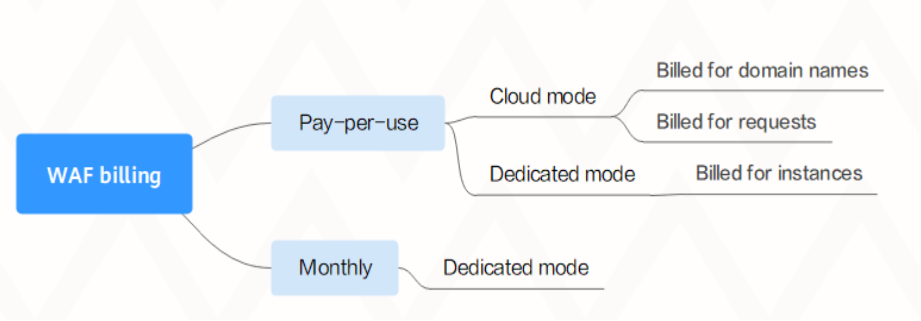


Table 1-4 Billing items

Mode	Billing Mode	Billing Item	Billing Description
Cloud mode	Pay-per-use	- Number of domains - Number of requests	- Number of domain names: Billed on an hourly basis. Once a domain name is added during the billing period, it will be billed no matter when it is deleted. - Number of requests: Billed on a monthly basis.
Dedicated mode	Pay-per-use	Number of instances	Billed for what you use
	Monthly	Number of instances	You will be billed based on how many instances you apply for and what instance specifications you select.

Billing Modes

- Monthly billing: The longer you use the service, the more money you save. You will be billed based on how many instances you apply for and what instance specifications you select.
- Pay-per-use billing: you can enable or disable an instance anytime you want.
  - For a pay-per-use cloud WAF instance, you are billed for the number of added domain names and number of handled requests.
  - For a pay-per-use dedicated WAF instance, you are billed for the required duration (accurate to second), which starts when the instance is created and ends when the instance is deleted.

FAQs

For more billing FAQs, see **WAF FAQs**.

1.7 Project and Enterprise Project

Project

Projects in IAM are used to group and isolate OpenStack resources (computing resources, storage resources, and network resources). Resources in your account must be mounted under projects. A project can be a department or a project team. Multiple projects can be created under one account.

Enterprise Project

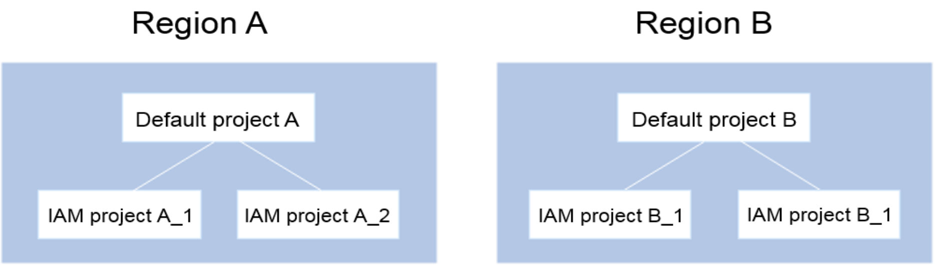
Enterprise projects are used to categorize and manage multiple resources. Resources of the same type can be put under an enterprise project. The use of enterprise projects does not affect the use of HSS.

You can classify resources by department or project group and put related resources into one enterprise project for management. Resources can be moved between enterprise projects.

Differences Between Projects and Enterprise Projects

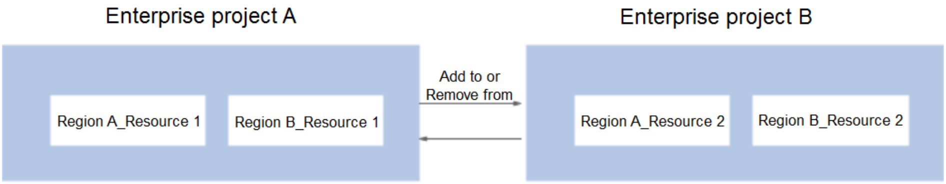
- IAM Project

  Projects are used to categorize and physically isolate resources in a region. Resources in an IAM project cannot be transferred. They can only be deleted and then rebuilt.



- Enterprise Project

  Enterprise projects are upgraded based on IAM projects and used to categorize and manage resources of different projects of an enterprise. An enterprise project can contain resources of multiple regions, and resources can be added to or removed from enterprise projects. If you have enabled enterprise management, you cannot create an IAM project and can only manage existing projects. In the future, IAM projects will be replaced by enterprise projects, which are more flexible.



Both projects and enterprise projects can be managed by one or more user groups. Users who manage enterprise projects belong to user groups. After a policy is granted to a user group, users in the group can obtain the permissions defined in the policy in the project or enterprise project.

1.8 Accessing and Using WAF

1.8.1 How to Access WAF

You can access WAF using the management console. If you have registered with the public cloud, you can directly log in to the management console.

- Cloud mode: On the homepage, choose **Security** > **Web Application Firewall**.
- Dedicated mode: On the homepage, choose **Security** > **Web Application Firewall (Dedicated)**.

1.8.2 How to Use WAF

The evolution of hacking techniques has caused frequent cybersecurity incidents against web servers. WAF provides comprehensive security protection for web services.

You can configure policies to detect attacks such as SQL injection, Cross-Site Scripting (XSS), web shells, command and code injections, file inclusion, sensitive file access, third-party vulnerability exploits, Challenge Collapsar (CC) attacks, malicious crawler scanning, and Cross-Site Request Forgery (CSRF).

WAF features an easy-to-use console and provides event logs and statistics reports, helping you stay up to date with the security of your website and allowing you to mask false alarms or add whitelist rules to ignore false alarms.

1.9 Related Services

This section describes the relationship between WAF and other cloud services.

CTS

Cloud Trace Service (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 1-5 WAF operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a WAF instance	instance	createInstance
Deleting a WAF instance	instance	deleteInstance
Modifying a WAF instance	instance	alterInstanceName
Modifying the protection status of a WAF instance	instance	modifyProtectStatus
Modifying the connection status of a WAF instance	instance	modifyAccessStatus
Creating a policy	policy	createPolicy
Applying a policy	policy	applyToHost
Modifying a policy	policy	modifyPolicy
Deleting a policy	policy	deletePolicy
Modifying alarm notification settings	alertNoticeConfig	modifyAlertNoticeConfig
Uploading a certificate	certificate	createCertificate
Changing the name of a certificate	certificate	modifyCertificate
Deleting a certificate	certificate	deleteCertificate
Adding a CC attack protection rule	policy	createCc
Modifying a CC attack protection rule	policy	modifyCc
Deleting a CC attack protection rule	policy	deleteCc
Adding a precise protection rule	policy	createCustom
Modifying a precise protection rule	policy	modifyCustom
Deleting a precise protection rule	policy	deleteCustom
Adding a blacklist or whitelist rule	policy	createWhiteblackip

Operation	Resource Type	Trace Name
Modifying a blacklist or whitelist rule	policy	modifyWhiteblackip
Deleting a blacklist or whitelist rule	policy	deleteWhiteblackip
Creating/updating a web tamper protection rule	policy	createAntitamper
Deleting a web tamper protection rule	policy	deleteAntitamper
Creating a global protection whitelist (formerly false alarm masking) rule	policy	createIgnore
Deleting a global protection whitelist (formerly false alarm masking) rule	policy	deleteIgnore
Adding a data masking rule	policy	createPrivacy
Modifying a data masking rule	policy	modifyPrivacy
Deleting a data masking rule	policy	deletePrivacy

Cloud Eye

Cloud Eye monitors the metrics of WAF, so that you can understand the protection status of WAF in a timely manner, and set protection policies accordingly. For details, see the *Cloud Eye User Guide*.

For details about monitoring metrics, see **Monitoring Metrics**.

TMS

Tag Management Service (TMS) is a visualized service for fast and unified tag management that enables you to label and manage WAF instances by tags.

Table 1-6 WAF operations supported by TMS

Operation	Resource Type	Event Name
Creating a WAF instance tag	Tag	createResourceTag
Deleting a WAF instance tag	Tag	deleteResourceTag

IAM

Identity and Access Management (IAM) provides the permission management function for WAF. Only users granted with the WAF Administrator permissions can use WAF. To obtain the permissions, contact users who have the Security Administrator permissions. For details, see the *Identity and Access Management User Guide*.

SMN

The Simple Message Notification (SMN) service provides the notification function. After the notification function is enabled in WAF, users will receive an SMS message or email when an attack on a protected domain is detected. For details about SMN, see the *Simple Message Notification User Guide*.

ELB

You can add your WAF instances to a load balancer so that your website traffic is distributed by the load balancer across WAF instances for detection and then forwarded by WAF to the origin servers. By this way, website traffic will be protected even if one of your WAF instances becomes faulty.

Enterprise Management

You can manage multiple projects in an enterprise, separately settle their costs, and assign different personnel for them. A project can be started or stopped independently without affecting others. You can easily manage your projects after creating an enterprise project for each of them.

WAF can be interconnected with Enterprise Management. You can manage WAF resources by enterprise project and grant different permissions to users.

1.10 Personal Data Protection Mechanism

To ensure that website visitors' personal data, such as the username, password, and mobile phone number, will not be obtained by unauthorized or unauthenticated entities or people and to prevent data leakage, WAF encrypts your personal data before storing it to control access to the data and records logs for operations performed on the data.

Personal Data to Be Collected

WAF records requests that trigger attack alarms in event logs. **Table 1-7** provides the personal data collected and generated by WAF.

Table 1-7 Personal data

Type	Collection Method	Can Be Modified	Mandatory
Request source IP address	Attacker IP address that is blocked or recorded by WAF when the domain name is attacked.	No	Yes
URL	Attacked URL of the protected domain name, or URL of the protected domain name that is blocked or recorded by WAF.	No	Yes
HTTP/HTTPS header information (including the cookie)	Cookie value and header value entered on the configuration page when you configure a CC attack or precise protection rule.	No	No If the configured cookie and header fields do not contain users' personal information, the requests recorded by WAF will not collect or generate such personal data.
Request parameters (Get and Post)	Request details recorded by WAF in protection logs.	No	No If request parameters do not contain users' personal information, the requests recorded by WAF will not collect or generate such personal data.

Storage Mode

The values of sensitive fields are saved after being anonymized, and the values of other fields are saved in plaintext in logs.

Access Control

Users can view only logs related to their own services.

1.11 Permissions Management

1.11.1 User Permissions (Cloud Mode)

The system provides two types of default permissions: user management and resource management. User management includes management of users, user groups, and user groups' rights. Users with resource management permissions can control the operations performed on cloud service resources.

1.11.2 WAF Permissions Management (Dedicated Mode)

If you need to assign different permissions to employees in your enterprise to access your WAF resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you secure access to your resources.

With IAM, you can use your account to create IAM users, and assign permissions to the users to control their access to specific resources. For example, some software developers in your enterprise need to use WAF resources but must not delete them or perform any high-risk operations. To achieve this result, you can create IAM users for the software developers and grant them only the permissions required for using WAF resources.

If your account does not need individual IAM users for permissions management, then you may skip over this chapter.

WAF Permissions

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles 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.

WAF is a project-level service deployed and accessed in specific physical regions. To assign WAF permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing WAF, the users need to switch to a region where they have been authorized to use the WAF service.

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to users responsibilities. Only a limited number of service-level roles for authorization are available. You need to also assign other dependent roles for the permission control to take effect. Roles are not ideal for fine-grained authorization and secure access control.
- Policies: A fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain

conditions. This mechanism allows for more flexible policy-based authorization and meets secure access control requirements. For example, you can grant WAF users only the permissions for managing a certain type of resources. Most policies define permissions based on APIs. For the API actions supported by WAF, see **WAF Permissions and Supported Actions**.

Table 1-8 lists all the system roles supported by WAF.

Table 1-8 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	

Helpful Links

- **WAF Custom Policies**
- **WAF Permissions and Supported Actions**

2 Monitoring Metrics

Function Description

This section describes monitoring metrics reported by WAF to Cloud Eye as well as their namespaces and dimensions. You can use the management console or APIs provided by Cloud Eye to query the monitoring metrics of the monitored object and alarms generated for WAF.

Namespace

SYS.WAF

NOTE

A namespace is an abstract collection of resources and objects. Multiple namespaces can be created in a single cluster, but they are isolated from each other. This enables namespaces to share the same cluster services without affecting each other.

Cloud WAF Monitoring Metrics

Table 2-1 Monitoring metrics

Metric ID	Metric Name	Meaning	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
attacks	attacks	Total number of attacks on a protected domain name in a given period	>= 0 count	Measurement object: protected domain name Dimension: waf_instance_id	5 minutes

Metric ID	Metric Name	Meaning	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
requests	requests	Total number of requests for a protected domain name in a given period	>= 0 count	Measurement object: protected domain name Dimension: waf_instance_id	5 minutes

Metrics for Dedicated WAF Instances

Table 2-2 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: % Collection method: 100% minus idle CPU usage percentage	0% to 100% Value type: Float	Dedicated WAF instances	1 minute
mem_util	Memory Usage	Memory usage of the monitored object Unit: % Collection method: 100% minus idle memory percentage	0% to 100% Value type: Float	Dedicated WAF instances	1 minute

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
disk_util	Disk Usage	Disk usage of the monitored object Unit: % Collection method: 100% minus idle disk space percentage	0% to 100% Value type: Float	Dedicated WAF instances	1 minute
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 byte Value type: Float	Dedicated WAF instances	1 minute
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 minute

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
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 minute
disk_read_requests_rate	Disk Read Requests	Number of bytes 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 minute

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
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 minute
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 minute
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 minute

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
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 minute
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 minute
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 minute

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
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 minute
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 minute

Dimensions

Table 2-3 Dimensions

Key	Value
waf_instance_id	Domain name ID
instance_id	ID of the dedicated WAF instance

3 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.

Table 3-1 lists the ports that can be protected by WAF.

Table 3-1 Ports supported by WAF

Deployment Mode	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
Cloud mode	Standard ports	80	443	Unlimited
	Non-standard ports (86 in total)	81, 82, 83, 84, 86, 87, 88, 89, 800, 808, 5000, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8999, 8011, 8012, 8013, 8014, 8015, 8016, 8017, and 8070	4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, and 8805	20

Deployment Mode	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
Dedicated mode	Standard ports	80	443	Unlimited

Deployment Mode	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
	Non-standard ports (182 in total)	9945, 9770, 81, 82, 83, 84, 88, 89, 800, 808, 1000, 1090, 3128, 3333, 3501, 3601, 4444, 5000, 5222, 5555, 5601, 6001, 6666, 6788, 6789, 6842, 6868, 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, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9802, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702, 8011, 8012, 8013, 8014,	8750, 8445, 18010, 4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, 8805, 9999	Unlimited

Deployment Mode	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
		8015, 8016, 8017, and 8070		

4 Cloud WAF

4.1 Getting Started

4.1.1 Overview

Before using WAF, you need to connect your domain name to it and enable it for protection to take effect.

Table 4-1 describes the procedure to use WAF.

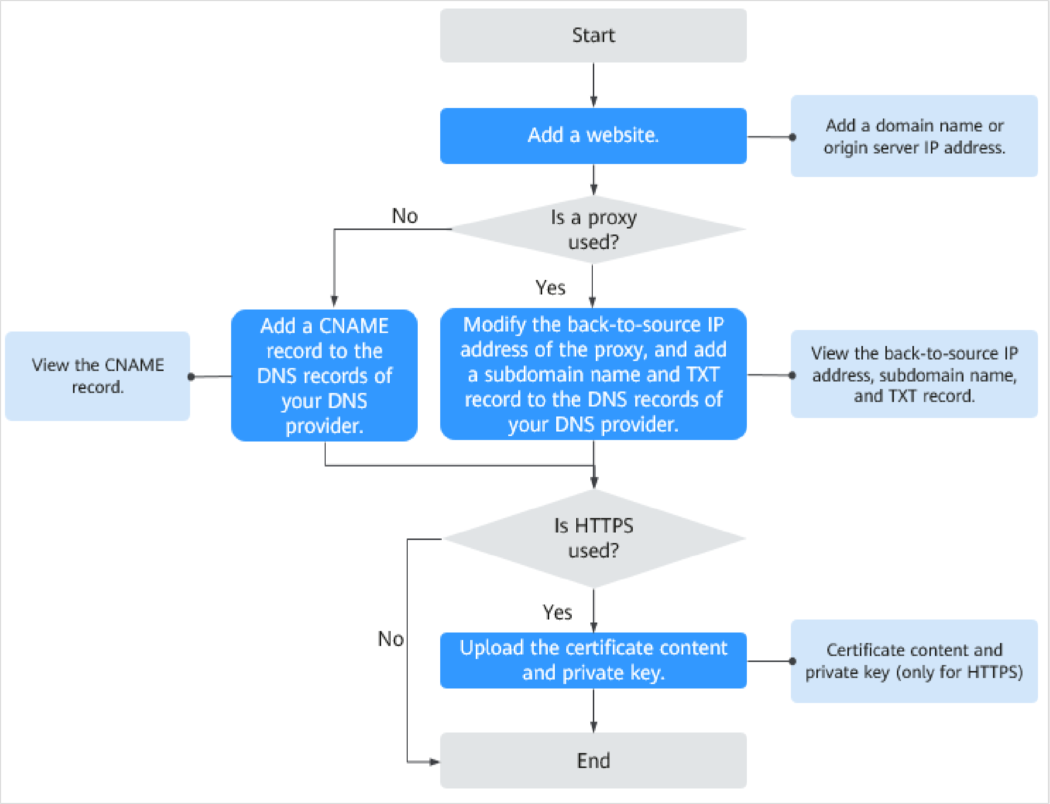
Table 4-1 Procedure to use WAF

Step	Description
Creating a domain name	Add a website to be protected. For details, see **Creating a Domain Name**.
Enabling WAF protection	Enable WAF protection to protect your web services. For details, see **Enabling WAF Protection**. **NOTE** ● The WAF engine does not run on your web server. Therefore, your web server performance will not be affected. ● After your domain name is connected to WAF, there will be a latency of tens of milliseconds, but might be raised based on the size of the requested page or number of incoming requests. ● You are billed for queries per second (QPS) or service bandwidth. One HTTP GET request is counted as a query, and the maximum QPS WAF can handle is 10,000. The total volume of normal traffic to a website or domain names protected by WAF is counted as the service bandwidth, and the maximum service bandwidth WAF can handle is 300 Mbit/s.

Step	Description
Configuring rules	In addition to the built-in protection rules, WAF provides a rich set of custom rules. For details, see **Rule Configurations**.
Enabling alarm notification	Once the function is enabled, users can receive attack logs at the earliest moment. For details, see **Enabling Alarm Notification**.
Handling false alarms	If the attack events blocked or logged are false positives, mask them. For details, see **Handling False Alarms**.
Viewing **Dashboard**	View the request and attack statistics, event distribution, and top 5 attack resource IP addresses of yesterday, today, past 3 days, past 7 days, or past 30 days. For details, see **Dashboard**.

For details about how to connect your website to WAF, see **Figure 4-1**.

Figure 4-1 Flowchart for connecting your website to WAF


Start
Add a website.
Add a domain name or origin server IP address.
Is a proxy used?
No
Yes
View the CNAME record.
Add a CNAME record to the DNS records of your DNS provider.
Modify the back-to-source IP address of the proxy, and add a subdomain name and TXT record to the DNS records of your DNS provider.
View the back-to-source IP address, subdomain name, and TXT record.
Is HTTPS used?
Yes
No
Upload the certificate content and private key.
Certificate content and private key (only for HTTPS)
End

4.1.2 Creating a Domain Name

This section describes how to create a domain name and connect it to WAF. After connecting a domain name, WAF works 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.

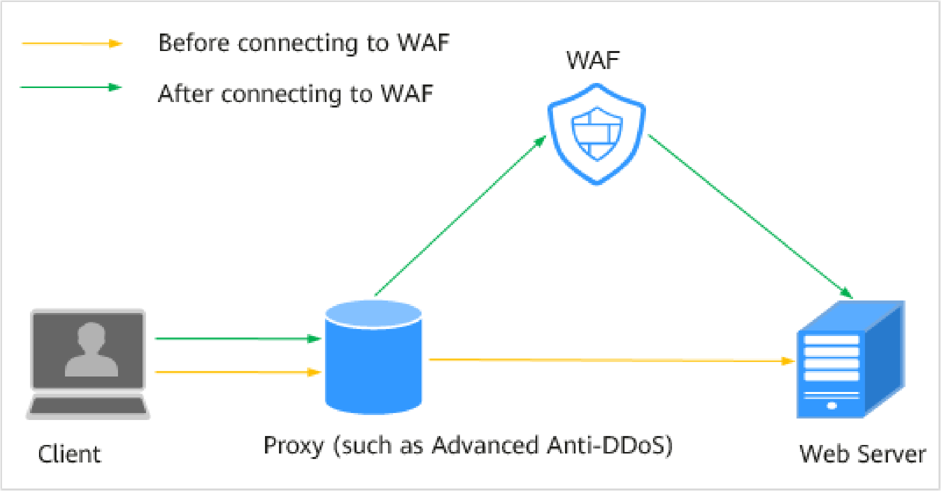
Prerequisites

Login credentials have been obtained.

Domain Configuration Principle

- Figure 4-2 shows how WAF works if the web server is using a proxy.

Figure 4-2 A proxy configured



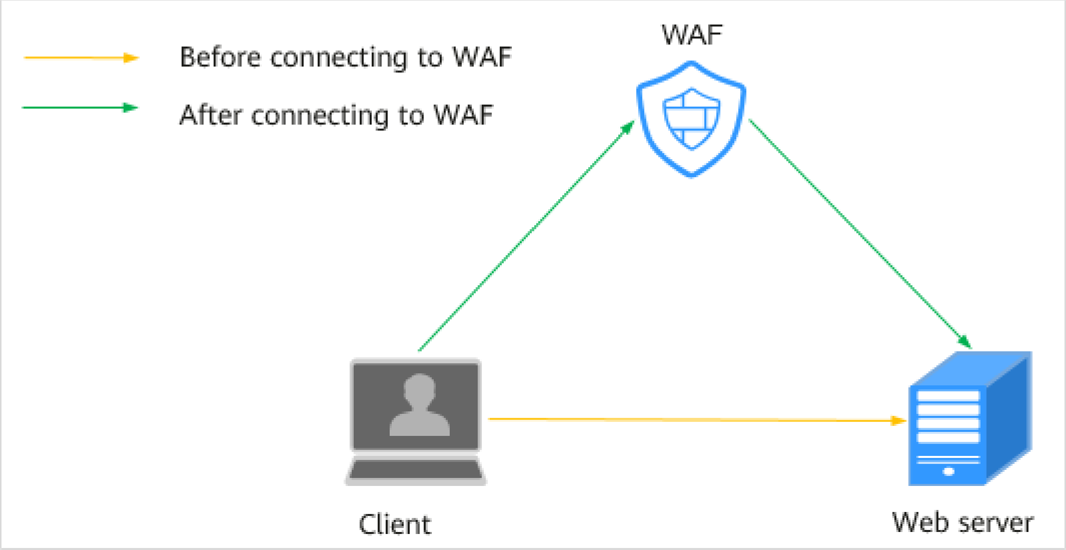
  - DNS resolves the domain name to the IP address of a proxy (such as AAD) before your site is moved to WAF. In this case, the traffic passes through the proxy and then the proxy routes the traffic back to the origin server.
  - After your site is moved to WAF, DNS resolves your domain name to the access address 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 access address of WAF.

    ii. Add a WAF subdomain name and TXT record to the DNS records of your DNS provider.

- Figure 4-3 shows how WAF works if the web server does not use a proxy.

Figure 4-3 No proxy configured



- DNS resolves your domain name to the origin server IP address before your site 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.

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 **Service List** at the top of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane, choose **Domains**.

Step 5 Click **Create Domain**.

Step 6 On the **Create Domain** page, specify required parameters by referring to **Table 4-2**.

Table 4-2 Parameter description

Parameter	Description	Example Value
Domain Name	A domain name to be protected, which can be a single domain name or a wildcard domain name. ● Single domain name: For example, *www.example.com* ● Wildcard domain name – If the server IP address of each subdomain name is the same, enter a wildcard domain name. For example, ***.example.com**. – 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**
Non-standard Port	Set this parameter only if **Non-standard Port** is selected. ● If **Client Protocol** is **HTTP**, WAF protects the standard port 80 by default. To protect a non-standard port, select **Non-standard Port** and then select a value from the **Port** drop-down list. ● If **Client Protocol** is **HTTPS**, WAF protects the standard port 443 by default. To protect a non-standard port, select **Non-standard Port** and then select a value from the **Port** drop-down list. For details about non-standard ports supported by WAF, see **Web Application Firewall**.	**4443**

Parameter	Description	Example Value
Server Configuration	Address configurations of the web server, including **Client Protocol**, **Server Protocol**, **Server Address**, and **Server Port**. ● **Client Protocol**: Type of client protocol. The options are **HTTP** and **HTTPS**. ● **Server Protocol**: Protocol used by WAF to forward requests to the server. The options are **HTTP** and **HTTPS**. **NOTE** For details about configuring **Client Protocol** and **Server Protocol**, see **Rules for Configuring Client Protocol and Server Protocol**. ● **Server Address**: IP address (generally the A record before the domain name is connected to WAF) or domain name (generally the CNAME before the domain name is connected to WAF) of the web server that a client accesses **NOTE** WAF cannot check server health. To check server health, use WAF along with Elastic Load Balance (ELB). After a load balancer is configured, use the EIP bound to the load balancer as your origin server IP address and point this IP address to your WAF instance. ● **Server Port**: Port number used by the web server	**Client Protocol**: **HTTPS** **Server Protocol**: **HTTP** **Server Address**: *XXX.XXX.1.1* **Server Port**: **80**
Certificate Name	If **Client Protocol** is **HTTPS**, select an existing certificate or upload a new certificate. For details about how to upload a new certificate, see **Step 7**.	None

Step 7 Upload a new certificate if **Client Protocol** is **HTTPS**.

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

   Currently, only .pem certificates are supported. If the certificate is not in .pem format, convert it into a .pem certificate by referring to **Table 4-3** before uploading.

Table 4-3 Certificate conversion commands

Format	Usage (Using OpenSSL)
CER/CRT	Rename the **cert.crt** certificate file to **cert.pem**.

Format	Usage (Using OpenSSL)
PFX	– Obtain a private key. For example, run the following command to convert **cert.pfx** into **cert.key**: **openssl pkcs12 -in cert.pfx -nocerts -out cert.key -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. As an example, run the following command to convert **cert.cer** into **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

2. Click **OK**.

Step 8 Set **Proxy Configured**. The default value is **No**.

NOTICE

If a proxy is deployed before WAF on your website, the WAF working mode cannot be switched to **Bypassed**.

- If your website is using a proxy such as Advanced Anti-DDoS (AAD), Content Delivery Network (CDN), or any other cloud acceleration service, select **Yes** so that the WAF security policies take effect on the origin server IP address. If this parameter is **No**, WAF cannot obtain the real IP address requested by a web visitor.

  NOTE

  If a proxy such as CDN is used, WAF obtains the real source IP address of a client from the HTTP Header **X-Forwarded-For** by default. If the proxy does not use **X-Forwarded-For** to identify the real source IP address of a client, click ✎ next to **X-Forwarded-For** in the row of **Source IP Header**. In the displayed dialog box, select an existing source IP header or select **Custom** and enter a source IP header.

- If your website does not use a proxy, select **No**.

Step 9 Click **Create Now**. In the upper right corner of the page, if **Domain created successfully** is displayed, the domain name is created.

NOTE

If you do not want to connect the domain name to WAF in this step, click **Next**. Then click **Finish**. **DNS** is displayed as **Unconfigured**. Later, you can refer to **Connecting a Domain Name** to finish domain connection.

- If a proxy such as CDN or AAD is used, you need to configure the back-to-source IP address, subdomain name, and TXT record.
  a. Configure the back-to-source IP address of the proxy on the website.

     For example, change the back-to-source IP address of CDN or AAD to the WAF IP address.

  b. Configure **Subdomain Name** and **TXT Record**.

     Add a subdomain name and TXT record to the DNS records of your DNS provider.

NOTICE

The high availability of our system, which is based on multi-AZ deployments to support both active-active and disaster recovery, relies on the WAF CNAME record. Do not use a fixed IP address to access services. Otherwise, service disaster recovery reliability will be affected.

- If no proxy is used, the CNAME record must be configured.
  a. Go to your DNS provider and configure the CNAME record. For details, contact your DNS provider.

NOTICE

The high availability of our system, which is based on multi-AZ deployments to support both active-active and disaster recovery, relies on the WAF CNAME record. Do not use a fixed IP address to access services. Otherwise, service disaster recovery reliability will be affected.

1. Do not modify the hosts file. Add the CNAME record directly to the DNS records of your DNS provider.
2. Do not use the A record to replace the CNAME record.

The CNAME binding method of some common DNS providers is listed for your reference. If the following configuration is inconsistent with the actual configuration, rely on information provided by the DNS providers.

i. Log in to the management console of the DNS provider.

ii. Go to the domain resolution record page.

iii. Set the CNAME resolution record.

  ○ Set the record type to **CNAME**.

  ○ Generally, enter the domain name prefix in the host record. For example, if the protected domain name is **admin.demo.com**, enter **admin** in the host record.

  ○ The record value is the CNAME generated by WAF.

- ○ Resolution line: keep the default value **TTL**.

iv. Click **Save**.

NOTICE

The preceding resolution methods are provided by third parties. This document does not control or assume responsibility for any third party content, including but not limited to its accuracy, compatibility, reliability, availability, legitimacy, appropriateness, performance, non-infringement, or status update, unless otherwise specified in this document.

b. Verify that the CNAME has been configured.

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

ii. Run the following command to query the CNAME. If the configured CNAME is displayed, the configuration is successful.

nslookup www.*domain*.com

Step 10 After the domain name is connected to WAF, click **Next**.

Step 11 Click **Finish**.

You can view the DNS status and mode of the domain name in the domain list.

NOTE

- If your web server is using other firewalls, disable the firewalls or whitelist the 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.
- If a domain name has been connected to WAF, **DNS** should be **Normal**. If **DNS** is **Unconfigured**, choose **More** > **Check DNS** in the **Operation** column of the target domain name to check the DNS status. If the problem persists, perform domain connection again by referring to **What Should I Do If the DNS Status Is Unconfigured?**
- After a domain name is created, WAF protection is enabled by default. The mode of Basic Web Protection is **Log only** (detected attacks are only logged but not blocked.). WAF creates a CC attack protection rule for the domain name by default. The rule can be modified but cannot be deleted. **Rate Limit** in the rule is 500 requests/5 seconds by default and it can be adjusted up to 10,000 requests/5 seconds. If you want a higher rate limit than the maximum value, contact the administrator.

----End

Rules for Configuring Client Protocol and Server Protocol

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

- HTTP mode.

  Client Protocol and **Server Protocol** are set to **HTTP**.

NOTICE

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

- HTTPS mode. This configuration allows web visitors to access your website over HTTPS only. If they access over HTTP, they are redirected to https://www.example.com.

NOTICE

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

- HTTP and HTTPS mode.

  Add two server configurations. One uses **HTTP** for **Client Protocol** and **Server Protocol**, and the other uses **HTTPS** for **Client Protocol** and **Server Protocol**.

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/HTTP mode.

  Client Protocol is set to **HTTPS** and **Server Protocol** is set to **HTTP**.

NOTICE

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

4.1.3 Allowing WAF Back-to-Source IP Addresses to Access Origin Servers

To let your cloud WAF instances 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 in cloud mode.

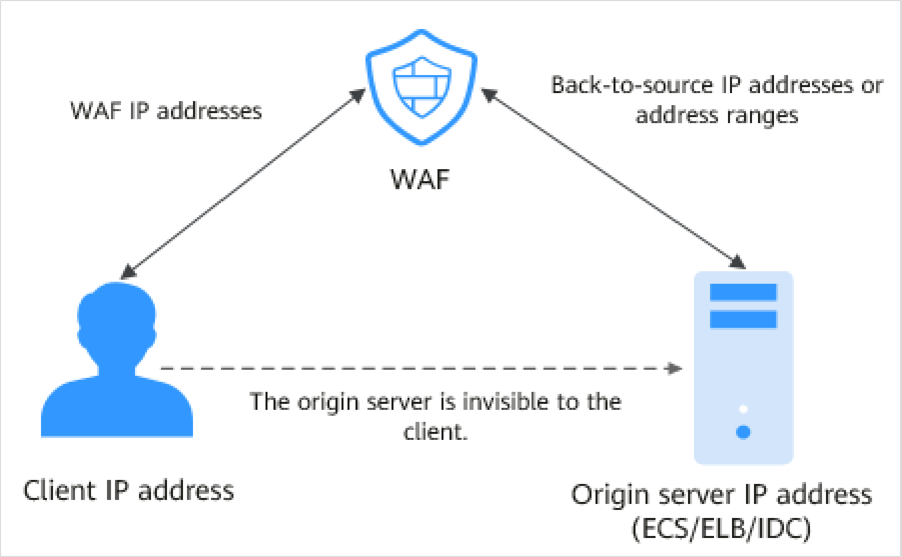
What Are Back-to-Source IP Addresses?

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 back-to-source IP addresses due to service 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 4-4 Back-to-source IP address


WAF IP addresses
WAF
Back-to-source IP addresses or address ranges
The origin server is invisible to the client.
Client IP address
Origin server IP address (ECS/ELB/IDC)

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.

NOTE

WAF back-to-source IP addresses are periodically updated. Whitelist the new IP addresses in time to prevent these IP addresses from being blocked by origin servers.

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 **Service List** at the top of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Domains** to go to the domain name settings page.

Step 5 Above the website list, click **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.

----End

4.1.4 Testing WAF

This section describes how to connect your domain to WAF on a local PC and then access the site to verify whether WAF works properly.

Before testing WAF, ensure that the protocol, address, and port number used by the origin server of the domain name (for example, **www.test.com**) are correct. If **Client Protocol** is **HTTPS**, ensure that uploaded certificate content and private key are correct.

Prerequisites

- Login credentials have been obtained.
- A domain name without using any other proxy has been created.

Connecting Your Domain to WAF Locally

Step 1 Obtain the CNAME value.

1. Log in to the management console.

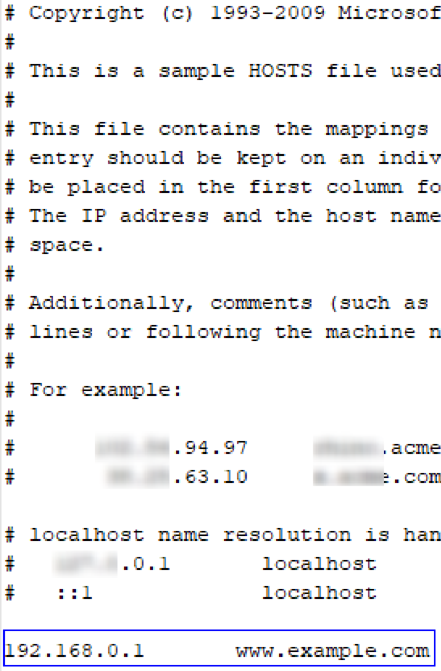
2. Click 📍 in the upper left corner of the management console and select a region or project.
3. Click **Service List** at the top of the page. Choose **Security** > **Web Application Firewall** On the displayed page, choose **Domains**.
4. In the row of the desired domain name, under the **Name** column, click the domain name you want to test.
5. In the **CNAME** row, click ⧉ to copy the CNAME value.

Step 2 Ping the CNAME value and record the corresponding IP address (for example, **192.168.0.1**).

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

1. Use a text editor, such as Notepad or Notepad++, to open the **hosts** file. Generally, the **hosts** file is stored in the **C:\Windows\System32\drivers\etc\** directory.
2. Add the back-to-source IP address of WAF obtained in **Step 2** and protected domain name to the **hosts** file. **Figure 4-5** shows an example.

Figure 4-5 Adding a record



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      [redacted].94.97     [redacted].acme.com          # source server
#       [redacted].63.10     [redacted].com              # x client host

# localhost name resolution is handled within DNS itself.
#    [redacted].0.1       localhost
#    ::1             localhost

192.168.0.1       www.example.com
```

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

   It is expected that the resolved IP address is the back-to-source IP address of WAF 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 refresh the DNS cache.

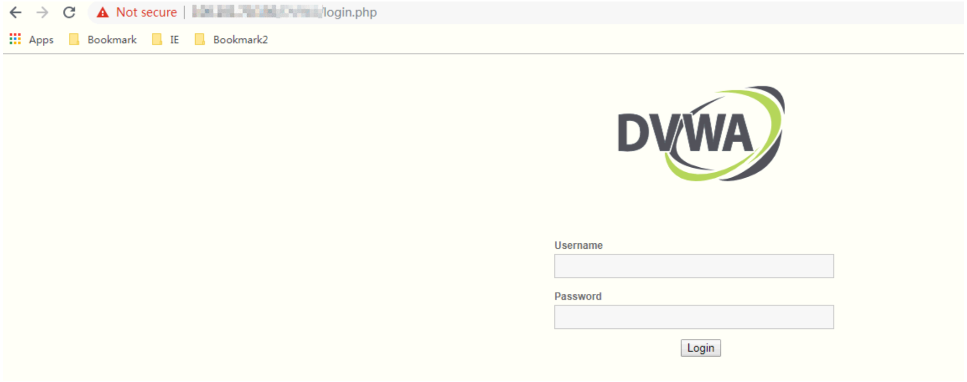
----End

Verifying Whether WAF Forwarding Is Normal

Step 1 Clear the browser cache and enter the domain name in the address box of a browser to check whether the website can be accessed.

If the domain name resolves to the back-to-source IP address of WAF and WAF configurations are correct, the website can be accessed.

Figure 4-6 Normal access

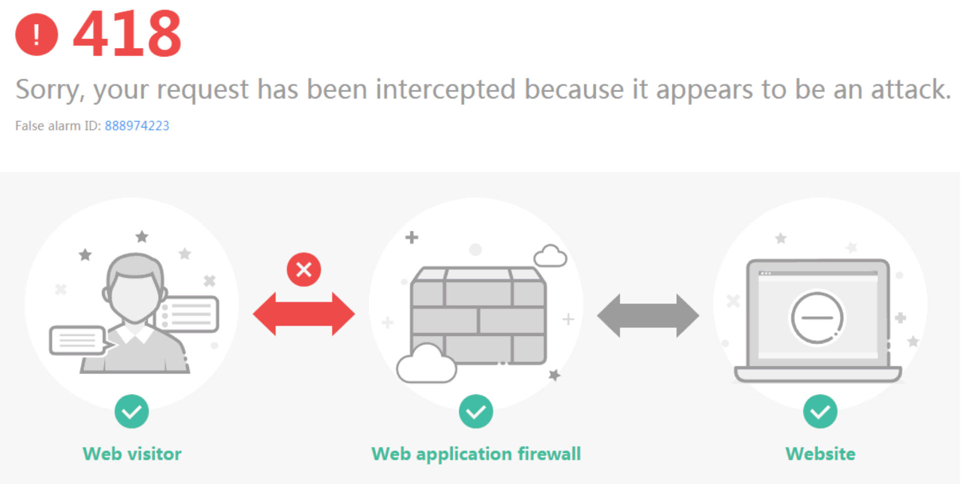


Not secure | [redacted]login.php

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 **http://www.test.com?id=1%20or%201%20=1** in the address box of the browser to simulate an SQL injection attack, and check whether WAF blocks the attack. See **Figure 4-7**.

Figure 4-7 Request blocked



418

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

False alarm ID: 888974223

3. In the navigation pane on the left, click **Events** and view test data on the displayed page.

----End

4.1.5 Connecting a Domain Name to WAF

This section describes how to connect a domain name to WAF so that website traffic passes through WAF.

To ensure that WAF works properly, you are advised to test WAF by following the instructions in **Testing WAF** before performing this operation.

How WAF Works

- No proxy used

  DNS resolves your domain name to the origin server IP address before the site is moved to WAF. DNS resolves your domain name to the CNAME of WAF after the site is connected to WAF. WAF then filters out illegitimate traffic and only routes legitimate traffic back to the origin server.

- A proxy (such as AAD) used

  DNS resolves the domain name to the AAD IP address before your site is moved to WAF. In this case, the traffic passes through AAD and then AAD routes the traffic back to the origin server. After your site is moved to WAF, change the AAD back-to-source IP address to the access address of WAF and add a subdomain name and TXT record to the DNS records of your DNS provider for WAF to take effect. In this way, AAD forwards the traffic to WAF. WAF then filters out illegitimate traffic and only routes legitimate traffic back to the origin server.

Prerequisites

- Login credentials have been obtained.
- A domain name has been created but not 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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Domains**.

Step 4 In the **Name** column, click the target domain name. Its information is displayed.

- Without a proxy

  a. In the CNAME row, click ⧉ to copy the CNAME value.

  b. Go to your DNS provider and configure the CNAME record. For details, contact your DNS provider.

NOTICE

The high availability of our system, which is based on multi-AZ deployments to support both active-active and disaster recovery, relies on the WAF CNAME record. Do not use a fixed IP address to access services. Otherwise, service disaster recovery reliability will be affected.

1. Do not modify the hosts file. Add the CNAME record directly to the DNS records of your DNS provider.
2. Do not use the A record to replace the CNAME record.

The CNAME binding method of some common DNS providers is listed for your reference. If the following configuration is inconsistent with the actual configuration, rely on information provided by the DNS providers.

i. Log in to the management console of the DNS provider.

ii. Go to the domain resolution record page.

iii. Set the CNAME resolution record.

  - Set the record type to **CNAME**.
  - Generally, enter the domain name prefix in the host record. For example, if the protected domain name is **admin.demo.com**, enter **admin** in the host record.
  - The record value is the CNAME generated by WAF.
  - Resolution line: keep the default value **TTL**.

iv. Click **Save**.

NOTICE

The preceding resolution methods are provided by third parties. This document does not control or assume responsibility for any third party content, including but not limited to its accuracy, compatibility, reliability, availability, legitimacy, appropriateness, performance, non-infringement, or status update, unless otherwise specified in this document.

c. Verify that the CNAME has been configured.

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

ii. Run the following command to query the CNAME. If the configured CNAME is displayed, the configuration is successful.

nslookup www.*domain*.com

- With a proxy

a. Click ⧉ in the **Access Address**, **Subdomain Name**, and **TXT Record** rows to copy the required values, respectively.

b. Change the back-to-source address of the proxy (such as AAD or CDN) to the copied access address. Add a subdomain name and TXT record to the DNS records of your DNS provider. Then, the domain name is connected to WAF and traffic passes through WAF.

NOTICE

The high availability of our system, which is based on multi-AZ deployments to support both active-active and disaster recovery, relies on the WAF CNAME record. Do not use a fixed IP address to access services. Otherwise, service disaster recovery reliability will be affected.

NOTE

By default, WAF detects the DNS resolution status of each domain name to be protected on an hourly basis. If you have performed domain connection and **DNS** is **Normal**, the domain name is connected to WAF.

----End

4.2 Certificate Management

4.2.1 Uploading a Certificate

This section describes how to upload a certificate.

Prerequisites

Login credentials have been obtained.

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 **Service List** at the top of the page and choose **Security** > **Web Application Firewall**.

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

Step 5 In the upper right corner of the displayed page, click **Upload Certificate**. In the displayed **Upload Certificate** dialog box, enter the certificate name and paste the certificate file and private key to the corresponding text boxes.

Currently, only .pem certificates are supported. If the certificate is not in .pem format, convert it into a .pem certificate by referring to **Table 4-4** before uploading.

Table 4-4 Certificate conversion commands

Format	Usage (Using OpenSSL)
CER/CRT	Rename the **cert.crt** certificate file to **cert.pem**.

Format	Usage (Using OpenSSL)
PFX	● Obtain a private key. For example, run the following command to convert **cert.pfx** into **cert.key**: **openssl pkcs12 -in cert.pfx -nocerts -out cert.key -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. As an example, run the following command to convert **cert.cer** into **cert.pem**: **openssl x509 -inform der -in cert.cer -out cert.pem**

Step 6 Click **OK**.

NOTE

- If the number of uploaded certificates reaches the upper limit, delete the certificates that are not associated with any domain names by referring to **Deleting a Certificate** and then upload a certificate again.
- To modify a certificate name, click ✎ next to the target certificate name in the **Certificate Name** column.

----End

4.2.2 Deleting a Certificate

This section describes how to delete an unused certificate.

Prerequisites

- Login credentials have been obtained.
- The certificate to be deleted is not associated with any 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 **Service List** at the top of the page and choose **Security** > **Web Application Firewall**.

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

Step 5 Locate the row that contains the certificate to be deleted, in the **Operation** column, click **Delete**.

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

----End

4.3 Domain Management

4.3.1 Viewing Basic Information

This section describes how to view domain information and edit server information.

Prerequisites

Login credentials have been obtained.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Domains**. **Table 4-5** describes parameters.

Table 4-5 Parameter description

Parameter	Description
Name	Protected domain name
Mode	WAF mode of the protected domain name ● **Enabled**: WAF is enabled. ● **Disabled**: WAF is disabled. ● **Bypassed**: In this mode, requests are directly sent to the backend server without passing through WAF.
DNS	DNS resolution status ● **Unconfigured**: The domain name is not connected to WAF or domain connection fails. To solve the problem, see **What Should I Do If the DNS Status Is Unconfigured?** ● **Normal**: The domain name is connected to WAF.

Parameter	Description
Protection Status over Past 3 Days	Protection status of the domain name over the past three days. In the **Operation** column, choose **More** > **View Attack** to view specific protection logs.
Policy	Policy configuration of the domain name. Click **Configure Policy** to configure rules by referring to **Rule Configurations**.

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

Step 5 View domain information.

1. View **Basic Information** and **WAF Information**.

   In the upper right corner of the domain information page, click ⟳ to refresh the page.

   NOTE

   - **Domain ID**: unique ID that is generated randomly for a domain name.
   - **Creation Time**: time when the domain name is created.
   - Click ⧉ in the **Access Address**, **Subdomain Name**, **TXT Record**, or **WAF IP Address Range** row to copy the required value.
   - If **Client Protocol** is set to **HTTPS**, updating the certificate is required. To do so, click ✎ next to **Certificate Name**. In the displayed dialog box, select an existing certificate.
   - If your web server stops using a proxy, click ✎ next to the value of **Proxy Configured**. In the dialog box displayed, select **No**.

   NOTE

   - **Domain ID**: unique ID that is generated randomly for a domain name.
   - **Creation Time**: time when the domain name is created.
   - Click ⧉ in the target row to copy the value of **CNAME** or **WAF IP Address Range**.
   - If **Client Protocol** is set to **HTTPS**, updating the certificate is required. To do so, click ✎ next to **Certificate Name**. In the displayed dialog box, select an existing certificate.
   - If your web server stops using a proxy, click ✎ next to the value of **Proxy Configured**. In the dialog box displayed, select **Yes**.

2. View the server information.

   Click **Edit Server Information**. On the displayed page, edit server configurations, such as the client protocol and associated certificate.

----End

Related Operations

In the **Operation** column of the domain list, you can:

- Click **Switch Mode** to switch the WAF working mode.
- Click **Configure Policy** to configure WAF protection rules.
- Choose **More** > **Check DNS** to check the DNS resolution status.
- Choose **More** > **View Attack** to view the WAF protection logs.
- Choose **More** > **View Metric** to view the WAF monitoring logs. For more details, see *Cloud Eye User Guide*.
- Choose **More** > **Delete** to delete the protected domain.

4.3.2 Enabling WAF Protection

This section describes how to enable WAF protection.

NOTE

- The WAF engine does not run on your web server. Therefore, your web server performance will not be affected.
- After your domain name is connected to WAF, there will be a latency of tens of milliseconds, but might be raised based on the size of the requested page or number of incoming requests.
- You are billed for queries per second (QPS) or service bandwidth. One HTTP GET request is counted as a query, and the maximum QPS WAF can handle is 10,000. The total volume of normal traffic to a website or domain names protected by WAF is counted as the service bandwidth, and the maximum service bandwidth WAF can handle is 300 Mbit/s.

Prerequisites

- Login credentials have been obtained.
- **Mode** for WAF to protect the domain name is **Disabled** or **Bypassed**.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Domains**.

Step 4 In the row containing the desired domain name, click **Switch Mode** in the **Operation** column.

Step 5 In the **Switch Mode** dialog box, select **Enabled** and then click **OK**.

----End

4.3.3 Disabling WAF Protection

This section describes how to disable WAF protection. In this mode, WAF only forwards requests, but does not detect them.

Prerequisites

- Login credentials have been obtained.
- **Mode** for WAF to protect the domain name is **Enabled** or **Bypassed**.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Domains**.

Step 4 In the row containing the desired domain name, click **Switch Mode** in the **Operation** column.

Step 5 In the **Switch Mode** dialog box, select **Enabled** and then click **OK**.

----End

4.3.4 Setting WAF Bypassed Mode

This section describes how to set the bypassed mode whereby requests are sent directly to the backend server without passing through WAF.

NOTE

In special scenarios such as testing, if services need to be restored to the state where the domain name is not connected to WAF, use the **Bypassed** mode.

Prerequisites

- Login credentials have been obtained.
- **Mode** for WAF to protect the domain name is **Enabled** or **Disabled**.
- Your web server does not use a proxy.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Domains**.

Step 4 In the row containing the desired domain name, click **Switch Mode** in the **Operation** column.

Step 5 In the dialog box displayed, select **Bypassed** and then click **OK**.

----End

4.3.5 Deleting a Protected Domain Name

This section describes how to delete a protected domain name from WAF.

NOTICE

- If the domain name to be deleted has been connected to WAF, re-resolve it with the DNS provider before you delete it to make it point to the origin server IP address. Otherwise, traffic intended to it will not be directed to the server, affecting access.
- Deletion takes effect within 1 minute and deleted domain names cannot be recovered. Therefore, exercise caution when deleting a domain name.

Prerequisites

- Login credentials have been obtained.
- The domain name to be deleted is resolved to the origin server address.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Domains**.

Step 4 Locate the row that contains the domain name to be deleted. In the **Operation** column, choose **More** > **Delete**.

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

Step 5 Click **Yes**. If **Domain deleted successfully** is displayed in the upper right corner, the domain name is deleted.

----End

4.4 Rule Configurations

This section describes how to configure protection rules.

4.4.1 Enabling Basic Web Protection

This section describes how to enable basic web protection.

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, and detects web shells, robots (search engine, scanner, and script tool), and other crawlers.

Prerequisites

- Login credentials have been obtained.
- The domain name to be protected has been created.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Domains**.

Step 4 Locate the row that contains the desired domain name. In the **Operation** column, click **Configure Policy**.

Step 5 In the **Basic Web Protection** area, specify **Status** and **Mode** by referring to **Table 4-6**. After the configuration completes, in the upper right corner of the **Protection Status** list, click **Save**. In the displayed dialog box, click **Yes** to save the settings. If you do not want to save the settings, click **Cancel**.

Table 4-6 Parameter description

Parameter	Description
Status	Status of Basic Web Protection
Mode	● **Block**: WAF blocks and logs detected attacks. ● **Log only**: WAF logs detected attacks only.

Step 6 In the **Basic Web Protection** configuration area, click **Advanced Settings**. Enable the protection type that best fits your needs.

NOTE

If you do not click **Save** after changing **Status** and **Mode** in **Step 5**, a **Warning** dialog box is displayed when you click **Advanced Settings**.

- Click **Yes** to cancel the previous settings.
- Click **No** and then **Save** to save the settings.

Table 4-7 Protection types

Type	Description
General Check	Defends against attacks, such as SQL injection, XSS, remote overflow vulnerability, file inclusion, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injection.
Webshell Detection	Defends against web shells from the upload interface.
Search Engine	Uses web crawlers such as Googlebot and Baiduspider to find pages for search engines.
Scanner	Scans for vulnerabilities, viruses, and performs other types of web scans, such as OpenVAS and Nmap.
Script Tool	Executes automatic tasks and program scripts, such as HttpClient, OkHttp, and Python programs. **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	Crawlers for other purposes, such as site monitoring, access proxy, and web page analysis.

1. Set the protection level.

   In the upper part of the page, select a protection level: **Low**, **Medium**, or **High**. The default value is **Medium**.

Table 4-8 Protection levels

Protection Level	Description
Low	WAF only blocks the requests with obvious attack signatures. If a large number of false alarms are reported, **Low** is recommended.
Medium	The default level is **Medium**, which meets a majority of web protection requirements.
High	WAF blocks the requests with no attack signature but have specific attack patterns. **High** is recommended if you want to block SQL injection, XSS, and command injection attacks.

2. Set the protection type.

   By default, **General Check** and **Scanner** are enabled. You can click to enable other protection types.

3. Click **Save** in the upper right of the page to save the settings. Otherwise, click **Cancel**.

----End

4.4.2 Configuring CC Attack Protection Rules

This section describes how to configure CC attack protection rules.

With these rules, rate limiting policies are set based on the IP addresses, cookies, or Referer field to accurately identify and mitigate CC attacks.

Prerequisites

- Login credentials have been obtained.
- The domain name to be protected has been created.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Domains**.

Step 4 Locate the row that contains the desired domain name. In the **Operation** column, click **Configure Policy**.

Step 5 In the **CC Attack Protection** area, specify **Status** and **Mode**. After the configuration completes, in the upper right corner of the **Protection Status** list, click **Save**. In the displayed dialog box, click **Yes** to save the settings. If you do not want to save the settings, click **Cancel**.

Step 6 Click **Customize Rule**. On the displayed **CC Attack Protection** page, click **Add Rule** in the upper left corner.

NOTE

If you do not click **Save** after changing **Status** in **Step 5**, a **Warning** dialog box is displayed when you click **Customize Rule**.

- Click **Yes** to cancel the previous settings.
- Click **No** and then **Save** to save the settings.

WAF creates a default CC attack protection rule. The rule can be modified but cannot be deleted. **Rate Limit** in the rule is 500 requests/5 seconds by default and it can be adjusted up to 10000 requests/5 seconds. If you want a higher rate limit than the maximum value, contact the administrator.

Step 7 In the displayed dialog box, specify the parameters by referring to **Table 4-9**.

Table 4-9 Rule parameters

Parameter	Description	Example Value
Path	Part of the URL without 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**, the WAF engine converts **///** to **/**.	**/admin***

Parameter	Description	Example Value
Rate Limit Mode	- **Per IP address**: A web visitor is identified by the IP address. - **Per user**: A web visitor is identified by the cookie key value. - **Other**: A web visitor is identified by the Referer field (user-defined request source). **NOTE** If **Rate Limit Mode** is **Other**, **Content** of **Referer** is set to a complete URL containing the domain name. The **Content** field supports prefix match and exact match only, and cannot contain two or more consecutive slashes, for example, **///admin**. If you enter **///admin**, the WAF engine converts it to **/admin**. For example, if **Path** is **/admin** and you do not want visitors to access the page from **www.test.com**, set **Content** to **http://www.test.com**.	Per user
User Identifier	A cookie field that you need to set if **Rate Limit Mode** is **Per user**. This value supports exact match only and does not support regular expressions. If a website uses the **name** field in the cookie to uniquely identify a web visitor, enter **name**. If you do not set this value, WAF will automatically assign one.	**name**
Rate Limit	Number of requests allowed from a web visitor in the rate limiting period. The visitor's access request is denied if the limit is reached.	**10** requests **60** seconds

Parameter	Description	Example Value
Protective Action	Action to perform if the maximum number of requests is reached. Options are **Verification code** and **Block**. ● **Verification code**: A verification code is displayed when the number of requests reaches the maximum limit within a specified period. Upon completing the verification, you are no longer restricted by the maximum number of requests allowed. ● **Block**: Requests are blocked if the maximum number of requests is reached. **NOTE** If **Rate Limit Mode** is **Other**, **Protective Action** can only be **Block**.	**Block**
Block Duration	Time required for the page to be restored to normal state after being blocked	**600** seconds
Block Page	Error page displayed when the maximum number of requests has been reached. This parameter is set only when **Protective Action** is **Block**. ● If you select **Default settings**, the default block page is displayed. ● If you select **Customize**, set a custom message.	**Customize**
Block Page Type	If you select **Customize** 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 **Customize** for **Block Page**, set the content to be returned.	**<html><body>Forbidden</body></html>**

Step 8 Click **OK**.

- To modify the added rule, click **Modify** in the row containing the target rule.
- The default CC attack protection rule created by WAF can be modified but cannot be deleted.
- To delete the added rule, click **Delete** in the row containing the target rule.

----End

4.4.3 Configuring Precise Protection Rules

This section describes how to configure precise protection rules.

With these rules, WAF allows you to customize combinations of HTTP headers, cookies, URLs, request parameters, and IP addresses, improving defense accuracy.

Prerequisites

- Login credentials have been obtained.
- The domain name to be protected has been created.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Domains**.

Step 4 Locate the row that contains the desired domain name. In the **Operation** column, click **Configure Policy**.

Step 5 In the **Precise Protection** area, specify **Status**. After the configuration completes, in the upper right corner of the **Protection Status** list, click **Save**. In the displayed dialog box, click **Yes** to save the settings. If you do not want to save the settings, click **Cancel**.

Step 6 Click **Customize Rule**. On the displayed page, specify **Detection Mode**.

> NOTE
>
> If you do not click **Save** after changing **Status** in **Step 4**, a **Warning** dialog box is displayed when you click **Customize Rule**.
>
> - Click **Yes** to cancel the previous settings.
> - Click **No** and then **Save** to save the settings.

Two detection modes are available:

- Instant Detection: WAF immediately ends threat detection and blocks the request that hits the configured precise protection rule.
- Full Detection: WAF blocks all requests that hit the configured precise protection rule when it finishes all threat detections.

The default detection mode is **Instant Detection**. After changing the detection mode, click **Save**.

Step 7 In the upper left corner of the **Precise Protection** page, click **Add Rule**.

Step 8 In the displayed dialog box, specify the parameters by referring to **Table 4-10**.

Table 4-10 Rule parameters

Parameter	Description	Example Value
Rule Name	Customizable rule name	waftest

Parameter	Description	Example Value
Protective Action	Its value is **Block** or **Allow**. The default value is **Block**.	**Block**
Effective Since	Select **Immediately** or select **Customize** to set a period. This period can only be a time segment in the future.	**Immediately**
Condition List	Click **Add** to add conditions. You must add one to thirty conditions to a protection rule. If more than one condition is added, all the conditions must be met simultaneously for the rule to take effect. ● **Field** ● **Subfield**: Configure this field only when **Params**, **Cookie**, or **Header** is selected. **NOTICE** The length of a subfield cannot exceed 2048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed. ● **Logic**: Select the desired logical relationship from the drop-down list. ● **Content**: Enter or select the content of condition matching. **NOTE** For detailed configurations, see **Table 4-11**.	● **Path Include /admin** ● **User Agent Prefix is not mozilla/5.0** ● **IP Equal to 192.168.2.3** ● **Cookie key1 Prefix is not Nessus**
Priority	Priority of a rule being executed Smaller values correspond to higher priorities. If two rules are assigned with the same priority, the rule added earlier has higher priority.	50

Table 4-11 Condition list configurations

Field	Example Subfield	Logic	Example Content
Path: URL excluding a domain name. This value supports exact match only. For example, if the path to be protected is **/admin**, set **Path** to **/admin**.	None	**Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, or **Suffix is not**	**/buy/phone/**
User Agent: A user agent of the scanner to be protected	None	**Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, or **Suffix is not**	**Mozilla/5.0 (Windows NT 6.1)**
IP: An IP address of the visitor to be protected	None	**Equal to** or **Not equal to**	**192.168.2.3**
Params: A request parameter to be protected	**sttl**	**Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, or **Suffix is not**	**201901150929**
Cookie: A small piece of data to identify web visitors	**name**	**Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, or **Suffix is not**	**Nessus**

Field	Example Subfield	Logic	Example Content
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**.	None	**Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, or **Suffix is not**	**http://www.test.com**
Header: A user-defined HTTP header	**Accept**	**Include**, **Exclude**, **Equal to**, **Not equal to**, **Prefix is**, **Prefix is not**, **Suffix is**, or **Suffix is not**	**text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8**

Step 9 Click **OK**.

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

----End

4.4.4 Configuring Blacklist or Whitelist Rules

This section describes how to configure blacklist or whitelist rules to block or allow specific IP addresses or address ranges.

Blacklist and Whitelist only takes effect for specified domain names.

Prerequisites

- Login credentials have been obtained.
- The domain name to be protected has been created.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Domains**.

Step 4 Locate the row that contains the desired domain name. In the **Operation** column, click **Configure Policy**.

Step 5 In the **Blacklist and Whitelist** area, specify **Status**. After the configuration completes, in the upper right corner of the **Protection Status** list, click **Save**. In the displayed dialog box, click **Yes** to save the settings. If you do not want to save the settings, click **Cancel**.

Step 6 Click **Customize Rule**. On the displayed **Blacklist and Whitelist** page, click **Add Rule** in the upper left corner.

NOTE

If you do not click **Save** after changing **Status** in **Step 5**, a **Warning** dialog box is displayed when you click **Customize Rule**.

- Click **Yes** to cancel the previous settings.
- Click **No** and then **Save** to save the settings.

Step 7 In the displayed dialog box, specify the parameters by referring to **Table 4-12**.

Table 4-12 Rule parameters

Parameter	Description	Example Value
IP Address or Range	● IP address: IP address to be added to the blacklist or whitelist ● IP address range: IP address and subnet mask defining a network segment	● XXX.XXX.1.1 ● XXX.XXX.1.0/24
Protective Action	If **IP Address or Range** is to be added to a whitelist, set this parameter to **Whitelist**. If **IP Address or Range** is to be added to a blacklist, set this parameter to **Blacklist**.	**Blacklist**

Step 8 Click **OK**.

- To modify the added rule, click **Modify** in the row containing the target rule.

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

----End

4.4.5 Configuring Web Tamper Protection Rules

This section describes how to configure web tamper protection (WTP) rules.

You can configure these rules to prevent a static web page from being tampered with.

WTP has the following advantages:

- Quicker response to requests

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

  If an attacker modifies a static web page on the server, WAF returns the cached original web page to web visitors, ensuring that visitors never access tampered-with pages.

  WAF can randomly extract a request from a web visitor to compare the requested page with the web page on the server. If WAF detects that the page has been tampered with, it notifies the user by SMS or email. For details about alarm notification settings, see **Enabling Alarm Notification**.

Prerequisites

- Login credentials have been obtained.
- The domain name to be protected has been created.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Domains**.

Step 4 Locate the row that contains the desired domain name. In the **Operation** column, click **Configure Policy**.

Step 5 In the **Web Tamper Protection** area, specify **Status**. After the configuration completes, in the upper right corner of the **Protection Status** list, click **Save**. In the displayed dialog box, click **Yes** to save the settings. If you do not want to save the settings, click **Cancel**.

Step 6 Click **Customize Rule**. On the displayed **Web Tamper Protection** page, click **Add Rule** in the upper left corner.

NOTE

If you do not click **Save** after changing **Status** in **Step 5**, a **Warning** dialog box is displayed when you click **Customize Rule**.

- Click **Yes** to cancel the previous settings.
- Click **No** and then **Save** to save the settings.

Step 7 In the displayed dialog box, specify the parameters by referring to **Table 4-13**.

Table 4-13 Rule parameters

Parameter	Description	Example Value
Domain Name	Domain name to be protected	**www.example.com**
Path	URL excluding a domain name **NOTE** • The path does not support regular expressions. • The path cannot contain two or more consecutive slashes. For example, **///admin**. If you enter **///admin**, the WAF engine converts **///** to **/**.	**/admin** For example, if the URL to be protected is **http://www.example.com/admin**, set **Path** to **/admin**.

Step 8 Click **OK**.

- In the event of changes on the protected web page, WAF needs to re-cache the web page content. In this case, click **Update Cache** in the row containing the target rule.
- To delete the added rule, click **Delete** in the row containing the target rule.

----End

4.4.6 Configuring False Alarm Masking Rules

This section describes how to configure false alarm masking rules.

You can add false alarms to the whitelist and ignore certain event IDs (for example, skip XSS check for a specified URL).

False alarm masking only applies to events logged by built-in basic web protection rules. If you want to mask events logged by custom rules, delete the rules.

Prerequisites

- Login credentials have been obtained.
- The domain name to be protected has been created.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Domains**.

Step 4 Locate the row that contains the desired domain name. In the **Operation** column, click **Configure Policy**.

Step 5 In the **False Alarm Masking** area, specify **Status**. After the configuration completes, in the upper right corner of the **Protection Status** list, click **Save**. In the displayed dialog box, click **Yes** to save the settings. If you do not want to save the settings, click **Cancel**.

Step 6 Click **Customize Rule**. On the displayed **False Alarm Masking** page, click **Add Rule** in the upper left corner.

NOTE

If you do not click **Save** after changing **Status** in **Step 5**, a **Warning** dialog box is displayed when you click **Customize Rule**.

- Click **Yes** to cancel the previous settings.
- Click **No** and then **Save** to save the settings.

Step 7 In the displayed dialog box, specify the parameters by referring to **Table 4-14**.

NOTE

False alarm masking only applies to events logged by built-in basic web protection rules. If you want to mask events logged by custom rules, delete the rules.

Table 4-14 Rule parameters

Parameter	Description	Example Value
Path	Misreported URL excluding a 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**, the WAF engine converts **///** to **/**.	**/admin** For example, if the URL to be protected is **http://www.example.com/admin**, set **Path** to **/admin**.
Event ID	ID of the built-in rule corresponding to the attack event for which the false alarm masking is to be performed **NOTE** To obtain the event ID, go to the **Events** page, select the **Search** tab, locate the row where the attack event resides, and click **Handle False Alarm** in the **Operation** column.	0000-0000-0000-14-6faa68ff067b246a555a3efbb9fb83dc

Step 8 Click **OK**. If **Rule added successfully** is displayed in the upper right corner, the rule is added.

To delete the added rule, click **Delete** in the row containing the target rule.

----End

4.4.7 Configuring Data Masking Rules

This section describes how to configure data masking rules. Data Masking prevents such data as usernames and passwords from being displayed in event logs.

Prerequisites

- Login credentials have been obtained.

- The domain name to be protected has been created.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Domains**.

Step 4 Locate the row that contains the desired domain name. In the **Operation** column, click **Configure Policy**.

Step 5 In the **Data Masking** area, specify **Status**. After the configuration completes, in the upper right corner of the **Protection Status** list, click **Save**. In the displayed dialog box, click **Yes** to save the settings. If you do not want to save the settings, click **Cancel**.

Step 6 Click **Customize Rule**. On the displayed **Data Masking** page, click **Add Rule** in the upper left corner.

NOTE

If you do not click **Save** after changing **Status** in **Step 5**, a **Warning** dialog box is displayed when you click **Customize Rule**.

- Click **Yes** to cancel the previous settings.
- Click **No** and then **Save** to save the settings.

Step 7 In the displayed dialog box, specify the parameters by referring to **Table 4-15**.

Table 4-15 Rule parameters

Parameter	Description	Example Value
Path	URL excluding a 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**, the WAF engine converts **///** to **/**.	**/admin/login.php** For example, if the URL to be protected is **http://www.example.com/admin/login.php**, set **Path** to **/admin/login.php**.
Masked Field	A field set to be masked ● **Params**: A request parameter ● **Header**: A user-defined HTTP header	● If **Masked Field** is set to **Params**, configure **Subfield** based on your needs. If it is set to **id**, the content that matches **id** will be masked. ● If **Masked Field** is set to **Header**, configure **Subfield** based on your needs. If it is set to **Accept**, the content that matches **Accept** will be masked.
Subfield	Set the parameter based on **Masked Field**. The masked field will not be displayed in the log. **NOTICE** The length of a subfield cannot exceed 2048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.	

Step 8 Click **OK**.

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

----End

4.5 Policy Management

4.5.1 Creating a Policy

A policy is a combination of multiple rules, such as basic web protection, blacklist or whitelist, and precise protection rules. A policy can be applied to multiple domain names. This section describes how to create a policy.

Prerequisites

Login credentials have been obtained.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane, choose **Policies**.

Step 4 In the upper right corner above the list, click **Create Protection Policy**.

Step 5 In the dialog box displayed, enter a policy name and click **OK**.

Step 6 In the **Policy Name** column, click the target policy name. On the displayed page, add rules to the policy by referring to Section **Rule Configurations**.

NOTE

- To modify a policy name, click next to the target policy name. In the dialog box displayed, enter a new policy name.
- After a domain name is created, WAF protection is enabled by default. The mode of Basic Web Protection is **Log only** (detected attacks are only logged but not blocked.). By default, WAF creates a CC attack protection rule to the policy. The rule can be modified but cannot be deleted.

----End

4.5.2 Applying a Policy to Your Domain Names

This section describes how to apply a policy to your domain names.

Prerequisites

- Login credentials have been obtained.
- The domain name to be protected has been created.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane, choose **Policies**.

Step 4 In the row containing the target policy, click **Bind Domain** in the **Operation** column.

Step 5 Select one or more domain names from the **Domain Name** drop-down list.

To view information about all domain names, click **View Domains**.

NOTICE

- A protected domain name can use only one policy, but one policy can be applied to multiple domain names.
- To delete a policy bound to domain names, bind these domain names to other policies, and click **Delete** in the **Operation** column of the target policy name.

Step 6 Click **OK**.

----End

4.6 Dashboard

This section describes how to view event logs in a specified time (for example, today), including attack and request statistics, the number of attacks from the top 5 source IP addresses, and event distribution.

Prerequisites

Login credentials have been obtained.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall** to go to the **Dashboard** page.

Step 4 In the domain name drop-down list, select a domain name to view its event logs. The query time can be **Yesterday**, **Today**, **Past 3 days**, **Past 7 days**, and **Past 30 days**.

NOTE

You can select **All domain names** or a specific domain name from the drop-down list.

Table 4-16 Parameter description of event logs

Parameter	Description	Remarks
Requests	Total number of requests to the specified domain name If **All domain names** is selected, the total number of requests to all domain names is displayed.	N/A
Peak Value	Maximum number of requests to the specified domain name per second	N/A
Attacks	Number of attacks on the specified domain name	N/A
Attack Sources	Number of sources that attack the specified domain name	N/A
Attacks	Trend of attacks	The trend of attacks is displayed by default.
Requests	Trend of requests	Click **Requests** to view the trend of requests.
Event Distribution	Types of attack events	● Click any colored area in the event distribution circle under **Event Distribution** to view the type, number, and proportion of an attack. ● To stop displaying information about a specific type of event, click the corresponding legend with the same color to the right of the circle.
Top 5 Source IP Addresses (Attacks)	Top 5 attack source IP addresses and their cumulative number of attacks	N/A

----End

4.7 Event Management

4.7.1 Handling False Alarms

This section describes how to mask false alarms and view event details if you find out that an event is misreported.

Prerequisites

- Login credentials have been obtained.
- The event list contains at least one misreported event.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Events**.

Step 4 Click the **Search** tab. In the domain name drop-down list, select a domain name or **All domain names** to view target event logs. The query time can be **Yesterday**, **Today**, **Past 3 days**, **Past 7 days**, **Past 30 days**, or a user-defined time. For details about parameters, see **Table 4-17** and **Table 4-18**.

In the upper right corner of the event list, click **Search by ID** to search a target event by ID.

Table 4-17 Event parameters

Parameter	Description
Event Type	Type of an attack By default, **All** is selected. You can view logs of all attack types or select an attack type to view target attack logs.
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 target attack logs.

Table 4-18 Log list parameters

Parameter	Description
Time	Time when an attack occurs
Source IP Address	Public IP address of the web visitor/attacker
Domain Name	Attacked domain name

Parameter	Description
URL	Attacked URL
Malicious load	Location of the malicious load
Event Type	Type of an attack
Protective Action	Protective actions.

NOTE

To view event details, click **Details** in the **Operation** column of the event list.

Step 5 If an event is misreported, add a false alarm masking rule by clicking **Handle False Alarm** in the row of the event. **Table 4-19** lists related parameters.

NOTE

- False alarm masking only applies to events logged by built-in basic web protection rules. If you want to mask events logged by custom rules, delete the rules.
- In the upper right corner of the **Handle False Alarm** dialog box, click **False Alarm Masking** to go to the **False Alarm Masking** page. On this page, you can add a false alarm masking rule.

Table 4-19 Parameter description

Parameter	Description	Example Value
Domain Name	Domain name where an attack occurs, which is obtained automatically by the system	--
Path	Misreported URL excluding a 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**, the WAF engine converts **///** to **/**.	**/admin***

Parameter	Description	Example Value
Event ID	ID of a built-in rule, which is automatically read.	0000-0000-0000-14-a77516b2df8a3324461edb9140d8c45b

Step 6 Click **OK**. The event is no longer displayed in the event list.

> NOTE
>
> You can switch to the **Domains** page, locate the row containing the target domain name, and click **Configure Policy** in the **Operation** column. In the **False Alarm Masking** area, click **Customize Rule** to view the added false alarm rule.

----End

4.7.2 Downloading Events Data

This section describes how to download events (logged and blocked events) data over the past five days. An event file is generated at 01:00:00 (UTC time) of the second day.

Prerequisites

- Login credentials have been obtained for logging in to the management console.
- An event file has been generated.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Events**. On the displayed page, click the **Download** tab. **Table 4-20** lists related parameters.

Table 4-20 Parameter description

Parameter	Description
Name	The format is *file name*.**csv**.
Number of Events	Total number of blocked and logged events **NOTE** The maximum number of events in a file is 10,000. If the number of events exceeds 10,000, another file is generated.

Step 4 In the **Operation** column, click **Download Data** to download data to the local PC.

----End

4.7.3 Enabling Alarm Notification

This section describes how to enable notification for attack logs. Once this function is enabled, WAF sends attack logs to users by email or SMS.

Prerequisites

- Login credentials have been obtained.
- The SMN service has been enabled.

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 **Service List** at the top of the page. Choose **Security** > **Web Application Firewall**. In the navigation pane on the left, choose **Events**.

Step 4 Click the **Notify** tab and configure alarm notification parameters by referring to **Table 4-21**.

Table 4-21 Notification setting parameters

Parameter	Description
Notification ID	Alarm event ID
Notification	Whether to enable notification
Notification Topic	Click the drop-down list to select an available topic or click **View Topic** to create a topic. For more information, see the *Simple Message Notification User Guide*.
Threshold	Alarm threshold **NOTE** Alarm notifications are sent when the number of attacks is greater than or equal to the threshold within the configured period.
Event Type	By default, **All** is selected. You can also click **Customize** to specify event types. For details about event types, see **Table 4-22**.

Table 4-22 List of event types

Event Type	Description
Challenge Collapsar	CC attack. When you find out that your website is experiencing slowed processing and high bandwidth usage, it may have been under CC attacks.
Command Injection	Command injection. It is a technique used by hackers to execute system commands on a server by chaining commands and bypassing blacklists to invoke web application interfaces.
Custom	Events logged by one or more precise protection rules
Illegal Request	Invalid requests. For example, more than 512 parameters are used.
SQL Injection	SQL injection. It is a common web attack whereby attackers inject malicious SQL commands into database query strings to deceive the server into executing them. By exploiting these commands, the attacker can obtain sensitive information, add users, export files, or even gain the highest permissions to the database or system.
Local File Inclusion	Local file inclusion (LFI) allows attackers to access files on a local server or download sensitive configurations. The vulnerability occurs due to the use of user-supplied input without proper validation.
Scanner & Crawler	Scanner and crawler attack events
AntiTamper	Events logged by one or more web tamper protection rules
Remote File Inclusion	Remote file inclusion
Miscellaneous	Other types of attacks, such as a combination of SQL injection and command injection attacks or certain CVE vulnerabilities
Cross Site Scripting	XSS. It is a type of attacks that exploits security vulnerabilities in web applications. XSS enables attackers to inject auto-executed malicious codes into web pages to steal users' information when they visit the pages.
Black/White IP	Events logged by one or more blacklist or whitelist rules

Event Type	Description
Webshell	A web shell is an attack script. After intruding into a website, an attacker adds an .asp, .php, .jsp, or .cgi script file with normal web page files. Then, the attacker accesses the file from a web browser and uses it as a backdoor to obtain a command execution environment for controlling the web server. For this reason, web shells are also called backdoor tools.

Step 5 Click **Save**.

----End

5 Dedicated WAF Mode

5.1 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 5-1 shows the procedure. **Table 5-1** describes the procedure.

Figure 5-1 Procedure for using WAF

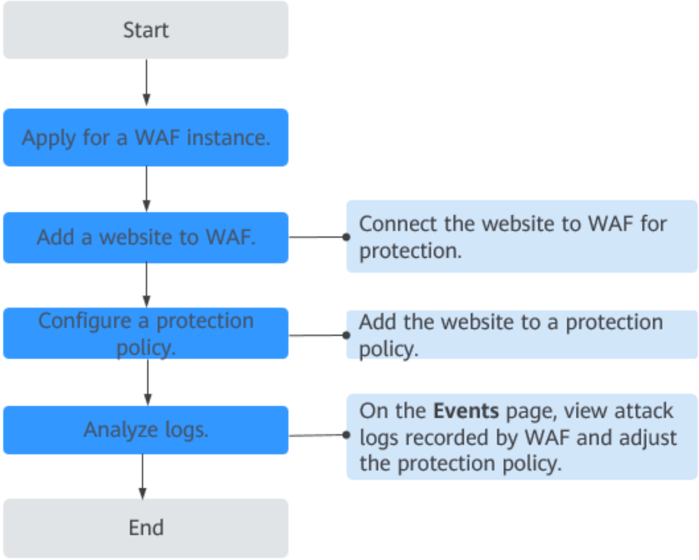

Start
Apply for a WAF instance.
Add a website to WAF.
Connect the website to WAF for protection.
Configure a protection policy.
Add the website to a protection policy.
Analyze logs.
On the **Events** page, view attack logs recorded by WAF and adjust the protection policy.
End

Table 5-1 Procedure for using WAF

Operation	Description
Apply for a WAF instance.	Apply for a dedicated WAF instance.
Add a website to WAF.	Add websites you want to protect to your WAF instance. **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.

Related Functions

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

Table 5-2 Related functions

Function	Description
Dashboard	You can view protection data of yesterday, today, last 3 days, last 7 days, or last 30 days.
Configuring 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.
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 for the connection between WAF and an origin server is 30 seconds. You can manually set the timeout on the WAF console.

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

5.2 Applying for a Dedicated WAF Instance

If your service servers are deployed on the cloud, you can buy dedicated WAF instances (or dedicated WAF engines) to protect important websites through domain names or to protect web applications with only IP addresses.

Prerequisites

- You have obtained management console login credentials for an account with the **WAF Administrator** and **WAF FullAccess** permissions.
- A VPC is available.
- Resource sets have been created.

Before You Start

After your application for a dedicated WAF instance succeeds, its specifications cannot be modified.

NOTICE

It takes about 10 minutes to create a dedicated WAF instance. If the instance is in the **Running** status, the instance has been created successfully.

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 (Dedicated)** under **Security**.

Step 4 Configure instance parameters by referring to **Table 5-3**.

Table 5-3 Parameters of a dedicated WAF instance

Parameter	Description
WAF Mode	Dedicated Mode
Region	Generally, a WAF instance you apply for 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.
AZ	Select an AZ in the selected region.
Instance Name Prefix	Set a prefix of the dedicated WAF instance name. If you apply for multiple instances at a time, the prefix to each instance name is the same.
Quantity	Set the number of WAF instances you want to apply for.
Specifications	Select specifications for your instance. WAF offers two types of specifications, 500 Mbit/s and 100 Mbit/s.
WAF Instance Type	Your WAF instance will be connected to your network through a VPC network interface. (If ELB is used, only dedicated load balancers can be used.)
CPU Architecture	Select CPU architecture for your instance.
ECS Specifications	Select ECS specifications for your 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 The value is **Default**. All outgoing network traffic is allowed by default. ● If your dedicated WAF instance and origin server are not in the same VPC, enable communications between the instance and the subnet of the origin server in the security group.
Tag	It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources.
Authorization	Select "I agree to assign permissions of the following roles to WAF: Tenant Guest, Server Administrator, VPC Administrator, and ELB Administrator." After you agree the authorization, WAF will create agencies in IAM for you.

Step 5 In the lower right corner of the page, click **Create Now**.

Step 6 Confirm the configuration and click **Create Now**.

Step 7 Click **Back to Dedicated Engine List**. On the **Dedicated Engine** page, view the instance status.

It takes about 10 minutes to create a dedicated WAF instance. If the instance is in the **Running** status, the instance has been created.

----End

5.3 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, event distribution, top 10 attacked domain names, top 10 attack source IP addresses, and top 10 attacked URLs.

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 5-4**.

Table 5-4 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.
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 upper left corner and choose **Web Application Firewall (Dedicated)** under **Security**.

Step 4 In the upper part of the page, select a project from the **Enterprise Project** drop-down list. Then, 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 in the selected enterprise project. 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**.

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.

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

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.

Table 5-5 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.
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.

Parameter	Description
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

5.4 Events

5.4.1 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 (Dedicated)** under **Security**.

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.

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 5-7** 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.

Table 5-6 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

Table 5-7 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
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

5.4.2 Handling False Alarms

If you confirm that an attack event on the **Events** page is a false alarm, you can handle the event as false alarm by ignoring the URL and rule ID in basic web protection, or by deleting or disabling the corresponding protection rule you configured. After an attack event is handled as a false alarm, the event will not be displayed on the **Events** page anymore.

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

NOTE

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

Prerequisites

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

Constraints

- Only attack events blocked or recorded by built-in basic web protection rules and features in anti-crawler protection can be handled as false alarms.
- For events generated based on custom rules (such as a CC attack protection rule, precise protection rule, blacklist rule, whitelist rule, or geolocation access control rule), they cannot be handled as false alarms. To ignore such an event, delete or disable the custom rule hit by the event.
- An attack event can only be handled as a false alarm once.
- After an attack event is handled as a false alarm, the attack event will not be displayed on the **Events** page.
- 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 (Dedicated)** under **Security**.

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 **More** > **Handle as False Alarm** and handle the hit rule.

Table 5-8 Parameters

Parameter	Description	Example Value
Scope	– **All domain names**: By default, this rule will be used to all domain names that are protected by the current policy. – **Specified domain names**: Specify a domain name range this rule applies to.	Specified domain names
Domain Name	This parameter is mandatory when you select **Specified domain names** for **Scope**. Enter a single domain name that matches the wildcard domain name being protected by the current policy.	www.example.com
Condition List	Click **Add** to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. A condition includes the following parameters: Parameters for configuring a condition are described as follows: – **Field** – **Subfield**: Configure this field only when **Params**, **Cookie**, or **Header** is selected for **Field**. **NOTICE** The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed. – **Logic**: Select a logical relationship from the drop-down list. – **Content**: Enter or select the content that matches the condition.	Path, Include, / product

Parameter	Description	Example Value
Ignore WAF Protection	– **All protection**: All WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule. – **Basic web protection**: You can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, if XSS check is not required for a URL, you can whitelist XSS rule.	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
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.

Parameter	Description	Example Value
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.

- 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.

Table 5-9 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.

Parameter	Description
IP Address/Range/Group	This parameter is mandatory when you select **New rule** for **Add to**. You can select **IP address/Range** or **Address Group** to add IP addresses a blacklist or whitelist rule.
Group Name	This parameter is mandatory when you select **Address group** for **IP Address/Range/Group**. Select an address group from the drop-down list.
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.

Related Operations

If an event is handled as a false alarm, the rule hit will be added to the global protection whitelist rule list. You can go to the **Policies** page and then switch to the **Global Protection Whitelist** page to manage the rule, including querying, disabling, deleting, and modifying the rule. For more details, see **Configuring a Global Protection Whitelist Rule to Ignore False Alarms**.

5.4.3 Downloading Events Data

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

NOTE

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

Prerequisites

- The website 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 (Dedicated)** under **Security**.

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

Step 5 Click the **Downloads** tab and download the desired protection data. **Table 5-10** describes the parameters.

Table 5-10 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

5.4.4 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.

Prerequisites

- 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 (Dedicated)** under **Security**.

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

Step 5 Click the **Configure Logs** tab, enable LTS (●), and select a log group and log stream. **Table 5-11** describes the parameters.

Table 5-11 Log configuration

Parameter	Description	Example Value
Log Group	Select a log group.	lts-group-waf
Attack Log	Select 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. 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.
  b. View attack logs.
- View access logs.
  a. In the log stream list, click the name of the configured access log stream.
  b. View 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	-

Field	Type	Field Description	Description
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.
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**.

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

Field	Type	Field Description	Description
access_log.upstream_connect_time	string	Time for the origin server to establish a connection to its backend services. Unit: second.	When SSL is used, the time for the handshake process is also recorded. Time used for establishing a connection for a request. Use commas (,) to separate the time used for each request.
access_log.upstream_header_time	string	Time used by the backend server to receive the first byte of the response header. Unit: second	Response time for multiple requests. Use commas (,) to separate the time used for each response.
access_log.bind_ip	string	WAF engine back-to-source IP address.	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.

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

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

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.
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.)	-

5.5 Policies

5.5.1 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 5-12 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**
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**

Protection Rule	Description	Reference
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**
Data masking rules	You can configure data masking rules to prevent sensitive data such as passwords from being displayed in event logs.	**Configuring Data Masking Rules to Prevent Privacy Information Leakage**

WAF Rule Priorities

The built-in protection rules of WAF help you defend against common web application attacks, including XSS attacks, SQL injection, crawlers, and web shells.

You can customize protection rules to let WAF better protect your website services using these custom rules. Figure 5-2 shows how WAF engine built-in protection rules work. Figure 5-3 shows the detection sequence of rules you configured.

Figure 5-2 WAF engine work process

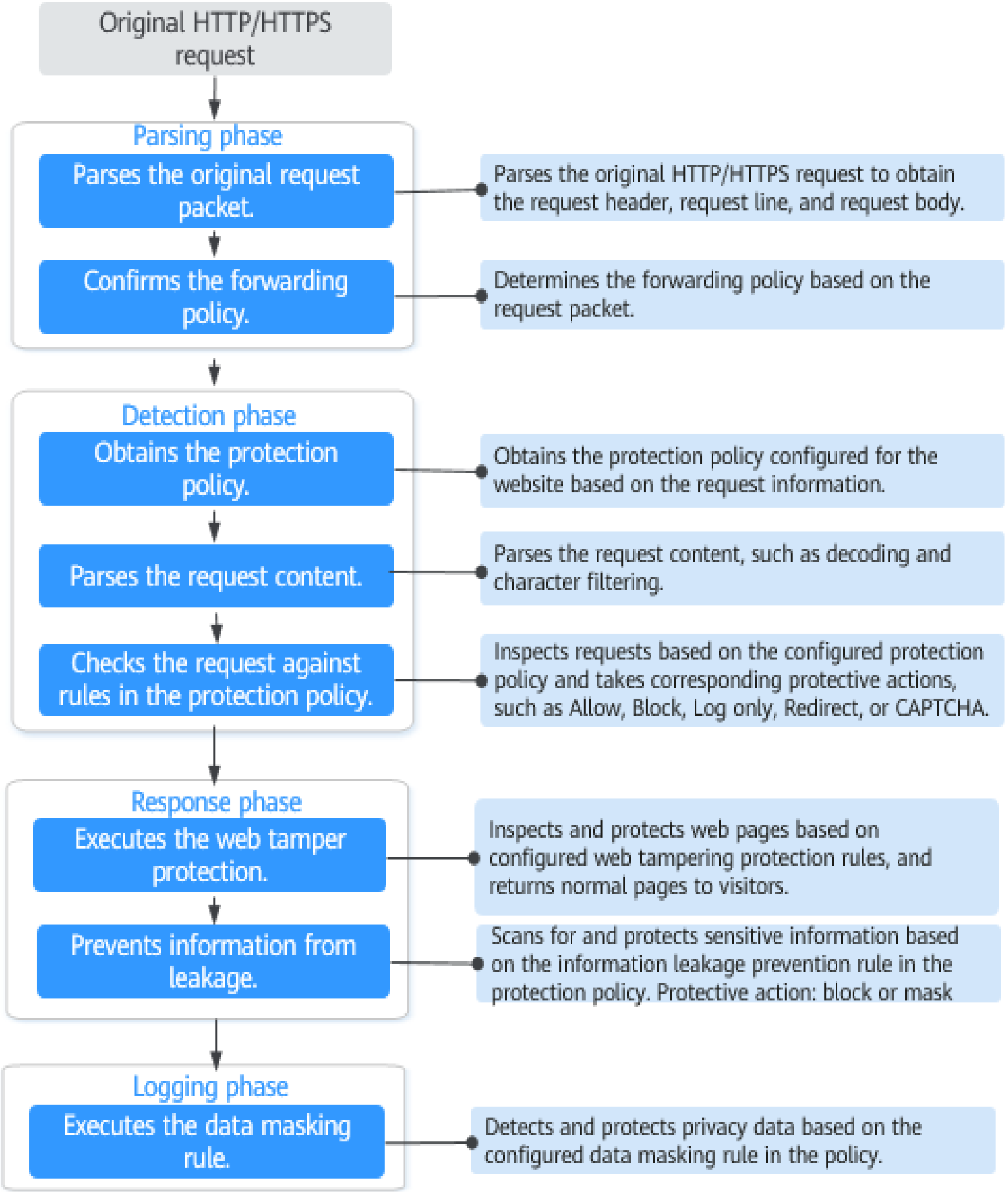
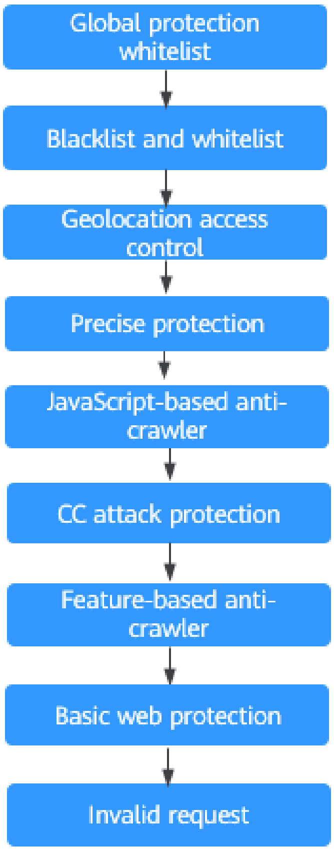

Original HTTP/HTTPS request
Parsing phase
Parses the original request packet.
Confirms the forwarding policy.
Parses the original HTTP/HTTPS request to obtain the request header, request line, and request body.
Determines the forwarding policy based on the request packet.
Detection phase
Obtains the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

Figure 5-3 Priorities of protection rules


Global protection whitelist
Blacklist and whitelist
Geolocation access control
Precise protection
JavaScript-based anti-crawler
CC attack protection
Feature-based anti-crawler
Basic web protection
Invalid request

Response actions

- Pass: The current request is unconditionally permitted after a protection rule is matched.
- Block: The current request is blocked after a rule is matched.
- CAPTCHA: The system will perform human-machine verification after a rule is matched.
- Redirect: The system will notify you to redirect the request after a rule is matched.
- Log: Only attack information is recorded after a rule is matched.
- Mask: The system will anonymize sensitive information after a rule is matched.

5.5.2 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.

NOTE

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

Prerequisites

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

Constraints

- 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.

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 (Dedicated)** under **Security**.

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 In the **Basic Web Protection** configuration area, change **Status** and **Mode** as needed by referring to **Table 5-13**.

Table 5-13 Parameter description

Parameter	Description
Status	Status of Basic Web Protection ● : enabled. ● : disabled
Mode	● **Block**: WAF blocks and logs detected attacks. ● **Log only**: WAF only logs detected attacks.

Step 7 In the **Basic Web Protection** configuration area, click **Advanced Settings**.

Step 8 Click the **Protection Status** tab, and enable protection types one by one by referring to **Table 5-15**.

1. Set the protective action.
   - **Block**: WAF blocks and logs detected attacks.

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

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

Table 5-14 Protection levels

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

3. Set the protection type.

NOTICE

By default, **General Check** is enabled. You can enable other protection types by referring to **Table 5-15**.

Table 5-15 Protection types

Type	Description
General Check	Defends against attacks such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections. SQL injection attacks are mainly detected based on semantics. **NOTE** If you enable **General Check**, WAF checks your websites based on the built-in rules.
Webshell Detection	Protects against web shells from upload interface. **NOTE** If you enable **Webshell Detection**, WAF detects web page Trojan horses inserted through the upload interface.
Deep Inspection	Identifies and blocks evasion attacks, such as the ones that use homomorphic character obfuscation, command injection with deformed wildcard characters, UTF7, data URI scheme, and other techniques. **NOTE** If you enable **Deep Inspection**, WAF detects and defends against evasion attacks in depth.
Header Inspection	This function is disabled by default. When it is disabled, General Check will check some of the header fields, such as User-Agent, Content-type, Accept-Language, and Cookie. **NOTE** If you enable this function, WAF checks all header fields in the requests.

----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 **Step 1: Add a Website to WAF (Dedicated Mode)**.
- 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.

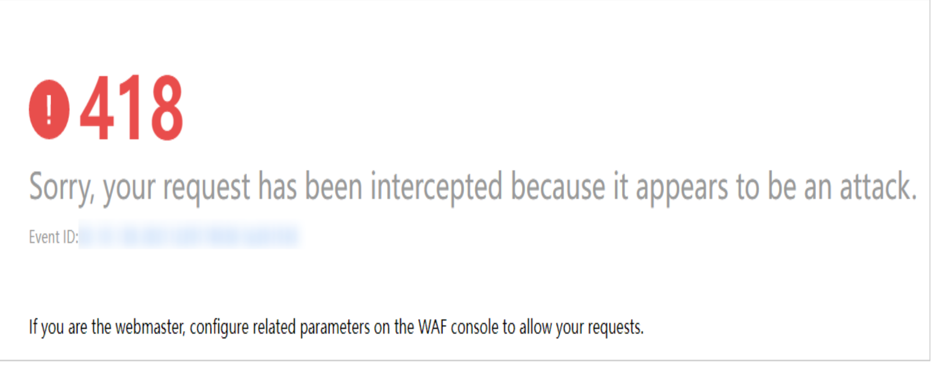
Step 1 Enable **General Check** in **Basic Web Protection** and set the protection mode to **Block**.

Step 2 Enable WAF basic web protection.

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

WAF blocks the access request. **Figure 5-4** shows an example block page.

Figure 5-4 Block page



418

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

Event ID: [redacted]

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

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

----End

5.5.3 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. To use this protection, ensure that you have toggled on **CC Attack Protection**).

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

Prerequisites

A website has been added to WAF.

Constraints

- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- 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**.

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 (Dedicated)** under **Security**.

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 In the **CC Attack Protection** configuration area, change **Status** if needed and click **Customize Rule** to go to the **CC Attack Protection** page.

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

Step 8 In the displayed dialog box, configure a CC attack protection rule by referring to **Table 5-16**.

Table 5-16 Rule parameters

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

Parameter	Description	Example Value
Rate Limit Mode	● **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**.	--
User Identifier	This parameter is mandatory when you select **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

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**, **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**
Rate Limit	The number of requests allowed from a website visitor in the rate limit period. If the number of requests exceeds the rate limit, WAF takes the action you configure for **Protective Action**.	**10** requests allowed in **60** seconds

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 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 **Step 1: Add a Website to WAF (Dedicated Mode)**.
- 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

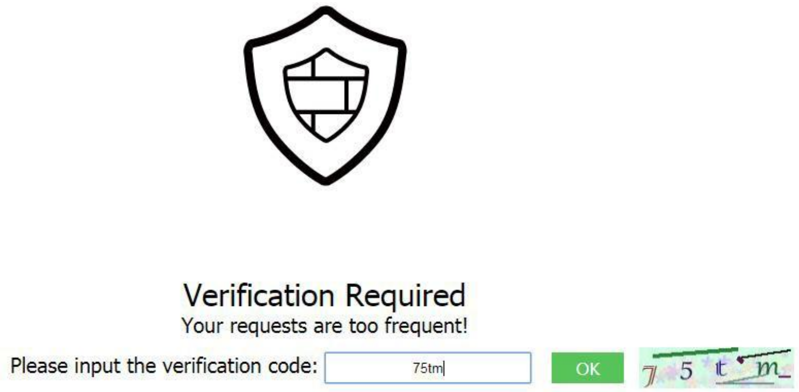
If domain name **www.example.com** has been connected to WAF, perform the following steps to verify that WAF CAPTCHA verification is enabled.

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

Step 2 Enable 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.



Verification Required

Your requests are too frequent!

Please input the verification code: 75tm

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

----End

5.5.4 Configuring Custom Precise Protection Rules

You can combine common HTTP fields, such as **IP**, **Path**, **Referer**, **User Agent**, and **Params** in a protection rule to let WAF allow, block, or only log the requests that match the combined conditions.

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

NOTE

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

Prerequisites

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

Constraints

- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- 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 (Dedicated)** under **Security**.

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 In the **Precise Protection** configuration area, change **Status** as needed and click **Customize Rule** to go to the **Precise Protection** page.

Step 7 On the **Precise Protection** page, set **Detection Mode**.

Two detection modes are available:

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

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

Step 9 In the displayed dialog box, add a rule by referring to **Table 5-17**.

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**.

Table 5-17 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 **Params**, **Cookie**, or **Header** is selected for **Field**. ● **Logic**: Select a logical relationship from the drop-down list. **NOTE** – If **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any of them**, **Suffix is any value**, or **Suffix is not any of them** is selected, select an existing reference table in the **Content** drop-down list. For details, see **Creating a Reference Table to Configure Protection Metrics In Batches**. – **Exclude any value**, **Not equal to any value**, **Prefix is not any of them**, and **Suffix is not any of them** indicates, respectively, that WAF performs the protection action (block, allow, or log only) when the field in the access request does not contain, is not equal to, or the prefix or suffix is not any value set in the reference table. For example, assume that **Path** field is set to **Exclude any value** and the **test** reference table is selected. If *test1*, *test2*, and *test3* are set in the **test** reference table, WAF performs the protection action when the path of the access request does not contain *test1*, *test2*, or *test3*. ● **Content**: Enter or select the content of condition matching. **NOTE** For more details about the configurations in general, see **Table 5-28**.	**Path Include /admin**

Parameter	Description	Example Value
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 there are requests that are blocked mistakenly.	**Block**
Known Attack Source	If you set **Protective Action** to **Block**, you can select a blocking type for a known attack source rule. Then, WAF blocks requests matching the configured **IP**, **Cookie**, or **Params** for a length of time that depends on the selected blocking type.	**Long-term IP address blocking**
Priority	Rule priority. If you have added multiple rules, rules are matched by priority. The smaller the value you set, the higher the priority. **NOTICE** If multiple precise access control rules have the same priority, WAF matches the rules in the sequence of time the rules are added.	**5**
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 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 **Step 1: Add a Website to WAF (Dedicated Mode)**.
- 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.

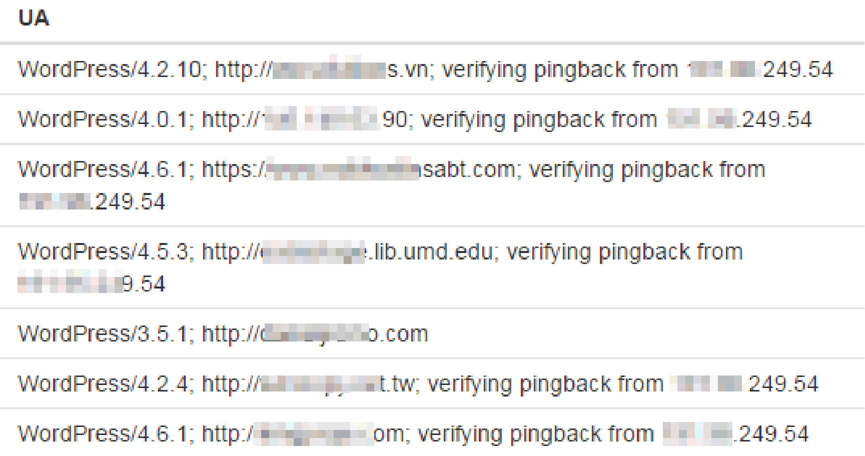
Step 3 Return to the WAF console. In the navigation pane, click **Events**. On the displayed page, view or **download events data**.

----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 5-5 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.

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

You can configure blacklist and whitelist rules to block, log only, or allow access requests from specific IP addresses or IP address ranges.

Prerequisites

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

Constraints

- WAF does not support batch import of blacklists or whitelists. To configure multiple IP address or IP address range rules, add blacklist and whitelist rules one by one to allow or block specified IP addresses or IP 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.
- 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.

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 (Dedicated)** under **Security**.

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 In the **Blacklist and Whitelist** configuration area, change **Status** as needed and click **Customize Rule**.

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

Step 8 In the displayed dialog box, specify the parameters by referring to **Table 5-18**.

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.

Table 5-18 Rule parameters

Parameter	Description	Example Value
Rule Name	Rule name you entered.	WAF
IP Address/ Range	IP addresses or IP address ranges are supported. ● IP address: IP address to be added to the blacklist or whitelist ● IP address range: IP address and subnet mask defining a network segment	XXX.XXX.2.3
Protective Action	● **Block**: Select **Block** if you want to blacklist an IP address or IP address range. ● **Allow**: Select **Allow** if you want to whitelist an IP address or IP address range. ● **Log only**: Select **Log only** if you want to observe an IP address or IP address range. Then, WAF determines whether the IP address or IP address range are blacklisted or whitelisted based on the **events data**.	Block
Known Attack Source	If you select **Block** for **Protective Action**, you can select a blocking type of a known attack source rule. WAF will block requests matching the configured 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 following the instructions in **Step 1: Add a Website to WAF (Dedicated Mode)**.
- 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

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

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

NOTE

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

Prerequisites

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

Constraints

- 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 (Dedicated)** under **Security**.

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 In the **Geolocation Access Control** configuration area, change **Status** if needed and click **Customize Rule**.

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

Step 8 In the displayed dialog box, add a geolocation access control rule by referring to **Table 5-19**.

Table 5-19 Rule parameters

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

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

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

----End

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 **Step 1: Add a Website to WAF (Dedicated Mode)**.
- 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

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

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

NOTE

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

How It Works

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

  So, if the URL in the **Referer** header field is the same as the configured anti-tamper path, for example, **/index.html**, all resources (resources ending with png, jpg, jpeg, gif, bmp, css or js) matching the request are also cached.

Prerequisites

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

Constraints

- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.

- Ensure that the origin server response contains the **Content-Type** response header, or WAF may fail to cache the origin server response.

Application Scenarios

- Quicker response to requests

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

- Web tamper protection

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

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 (Dedicated)** under **Security**.

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 In the **Web Tamper Protection** configuration area, change **Status** if needed and click **Customize Rule** to go to the **Web Tamper Protection** page.

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

Step 8 In the displayed dialog box, specify the parameters by referring to **Table 5-20**.

Table 5-20 Rule parameters

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

Parameter	Description	Example Value
Path	A part of the URL, not including the domain name A URL is used to define the address of a web page. The basic URL format is as follows: Protocol name://Domain name or IP address[:Port]/[Path/.../File name]. For example, if the URL is **http://www.example.com/admin**, set **Path** to **/admin**. **NOTE** ● The path does not support regular expressions. ● The path cannot contain two or more consecutive slashes. For example, **///admin**. If you enter **///admin**, WAF converts **///** to **/**.	**/admin**
Rule Description	A brief description of the rule. This parameter is optional.	None

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

----End

Related Operations

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

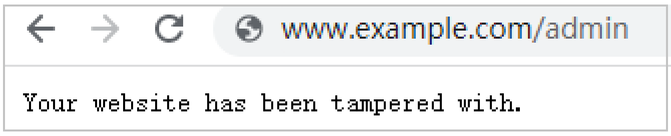
Configuration Example - Static Web Page Tamper Prevention

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

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

A tampered page is returned.

Figure 5-6 A static page that has been tampered with



Your website has been tampered with.

Step 2 Add a web tamper prevention rule to WAF.

Step 3 Enable WTP.

Step 4 Use a browser to access **http://www.example.com/admin**. WAF will cache the page.

Step 5 Access **http://www.example.com/admin** again.

The intact page is returned.

----End

5.5.8 Configuring Anti-Crawler Rules

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

NOTE

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

Prerequisites

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

Constraints

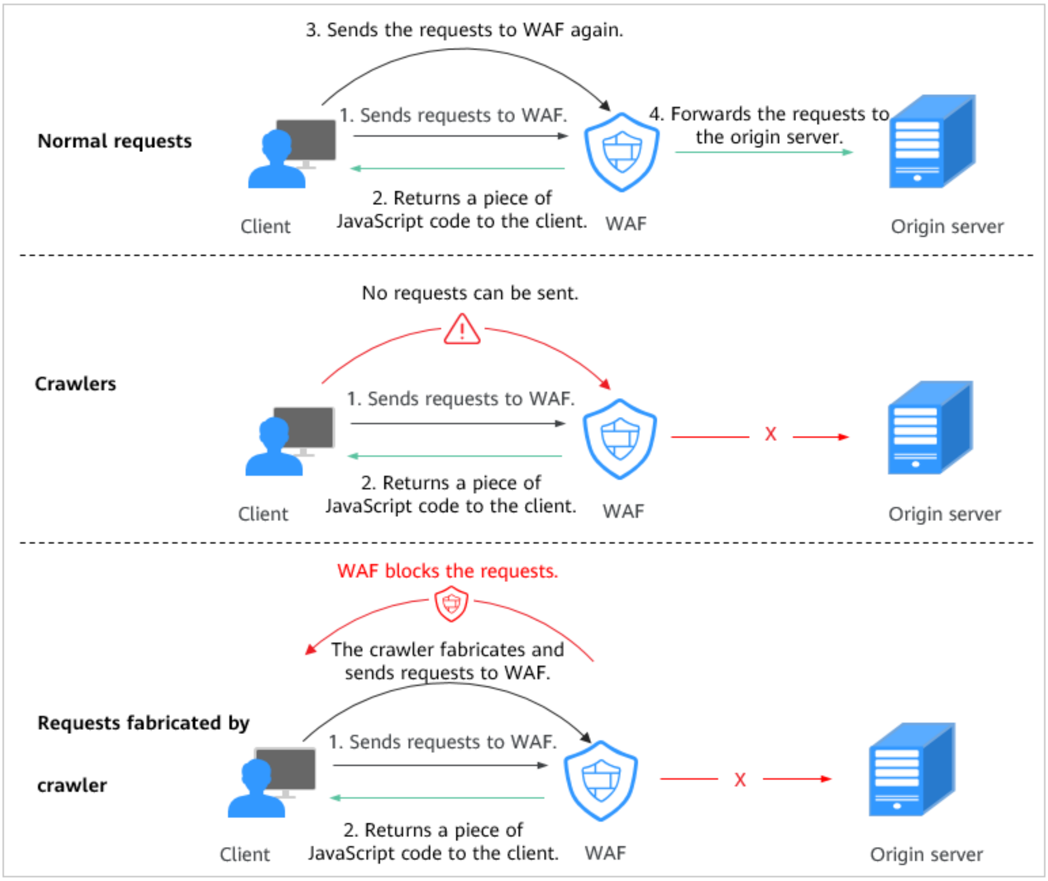
- Cookies must be enabled and JavaScript supported by any browser used to access a website protected by anti-crawler protection rules.
- If your service is connected to CDN, exercise caution when using the JS anti-crawler function.

  CDN caching may impact JS anti-crawler performance and page accessibility.
- WAF only logs JavaScript challenge and JavaScript authentication events. No other protective actions can be configured for JavaScript challenge and authentication.
- WAF JavaScript-based anti-crawler rules only check GET requests and do not check POST requests.

How JavaScript Anti-Crawler Protection Works

Figure 5-7 shows how JavaScript anti-crawler detection works, which includes JavaScript challenges (step 1 and step 2) and JavaScript authentication (step 3).

Figure 5-7 JavaScript Anti-Crawler protection process

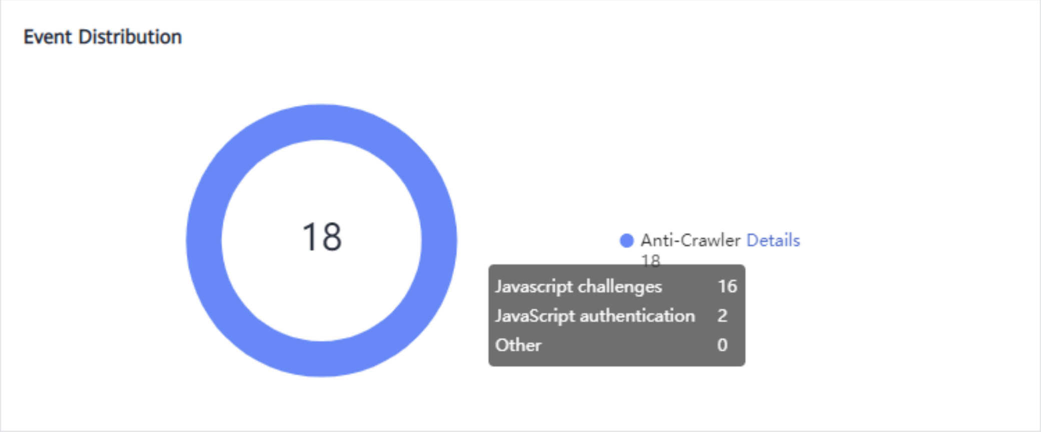

3. Sends the requests to WAF again.
Normal requests
1. Sends requests to WAF.
4. Forwards the requests to the origin server.
2. Returns a piece of JavaScript code to the client.
Client
WAF
Origin server
No requests can be sent.
Crawlers
1. Sends requests to WAF.
X
2. Returns a piece of JavaScript code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

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

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

By collecting statistics on the number of JavaScript challenges and authentication responses, the system calculates how many requests the JavaScript anti-crawler defends. In **Figure 5-8**, the JavaScript anti-crawler has logged 18 events, 16 of which are JavaScript challenge responses, and 2 of which are JavaScript authentication responses. **Others** indicates the number of WAF authentication requests fabricated by the crawler.

Figure 5-8 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 (Dedicated)** under **Security**.

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 In the **Anti-Crawler** configuration area, toggle on the function if needed. Then, click **Configure Anti-Crawler**.

Step 7 Select the **Feature Library** tab and enable the protection by referring to **Table 5-21**.

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.

Table 5-21 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.
Scanner	This rule is used to block scanners, such as OpenVAS and Nmap. A scanner scans for vulnerabilities, viruses, and other jobs.	After you enable this rule, WAF detects and blocks scanner crawlers.
Script Tool	This rule is used to block script tools. A script tool is often used to execute automatic tasks and program scripts, such as HttpClient, OkHttp, and Python programs.	If you enable this rule, WAF detects and blocks the execution of automatic tasks and program scripts. **NOTE** If your application uses scripts such as HttpClient, OkHttp, and Python, disable **Script Tool**. Otherwise, WAF will identify such script tools as crawlers and block the application.
Other	This rule is used to block crawlers used for other purposes, such as site monitoring, using access proxies, and web page analysis. **NOTE** To avoid being blocked by WAF, crawlers may use a large number of IP address proxies.	If you enable this rule, WAF detects and blocks crawlers that are used for various purposes.

Step 8 Select the **JavaScript** tab and change **Status** if needed.

JavaScript anti-crawler is disabled by default. To enable it, click ○ and then click **OK** in the displayed dialog box to toggle on ●.

NOTICE

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

  CDN caching may impact JS anti-crawler performance and page accessibility.

Step 9 Configure a JavaScript-based anti-crawler rule by referring to **Table 5-22**.

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

- To protect all paths except a specified path

  Set **Protection Mode** to **Protect all paths**. Then, click **Exclude Path**, configure protected paths, and click **Confirm**.
- To protect a specified path only

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

Table 5-22 Parameters of a JavaScript-based anti-crawler protection rule

Parameter	Description	Example Value
Rule Name	Name of the rule	wafjs

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
Logic	Select a logical relationship from the drop-down list.	Include
Rule Description	A brief description of the rule.	None
Effective Date	Immediate	Immediate

----End

Related Operations

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

Configuration Example - Logging Script Crawlers Only

To verify that WAF is protecting domain name **www.example.com** against an anti-crawler rule:

Step 1 Execute a JavaScript tool to crawl web page content.

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

Step 3 Enable anti-crawler protection.

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

----End

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

You can add two types of information leakage prevention rules.

- Sensitive information filtering: prevents disclosure of sensitive information (such as ID numbers, phone numbers, and email addresses).
- Response code interception: blocks the specified HTTP status codes.

NOTE

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

Prerequisites

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

Constraints

- 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 (Dedicated)** under **Security**.

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 In the **Information Leakage Prevention** configuration area, change **Status** if needed and click **Customize Rule**.

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

Step 8 In the dialog box displayed, add an information leakage prevention rule by referring to **Table 5-23**.

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:

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.

Table 5-23 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**

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

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

----End

Related Operations

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

Configuration Example — Masking Sensitive Information

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

Step 1 Add an information leakage prevention rule.

Step 2 Enable information leakage prevention.

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.

----End

5.5.10 Configuring a Global Protection Whitelist Rule to Ignore False Alarms

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

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

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

NOTE

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

Prerequisites

A website has been added to WAF.

Constraints

- If you select **All protection** for **Ignore WAF Protection**, all WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule.
- If you select **Basic web protection** for **Ignore WAF Protection**, global protection whitelist rules take effect only for events triggered against WAF built-in rules in **Basic Web Protection** and anti-crawler rules under **Feature Library**.
  - Basic web protection rules

    Basic web protection defends against common web attacks, such as SQL injection, XSS attacks, remote buffer overflow attacks, file inclusion, Bash vulnerability exploits, remote command execution, directory traversal, sensitive file access, and command and code injections. Basic web protection also detects web shells and evasion attacks.
  - Feature-based anti-crawler protection

    Feature-based anti-crawler identifies and blocks crawler behavior from search engines, scanners, script tools, and other crawlers.
- 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 (Dedicated)** under **Security**.

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 In the **Global Protection Whitelist** configuration area, click **Status** if needed. Then, click **Customize Rule**.

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 5-24**.

Table 5-24 Parameters

Parameter	Description	Example Value
Scope	● **All domain names**: By default, this rule will be used to all domain names that are protected by the current policy. ● **Specified domain names**: Specify a domain name range this rule applies to.	Specified domain names
Domain Name	This parameter is mandatory when you select **Specified domain names** for **Scope**. Enter a single domain name that matches the wildcard domain name being protected by the current policy.	www.example.com
Condition List	Click **Add** to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. A condition includes the following parameters: Parameters for configuring a condition are described as follows: ● **Field** ● **Subfield**: Configure this field only when **Params**, **Cookie**, or **Header** is selected for **Field**. **NOTICE** The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed. ● **Logic**: Select a logical relationship from the drop-down list. ● **Content**: Enter or select the content that matches the condition.	Path, Include, / product

Parameter	Description	Example Value
Ignore WAF Protection	● **All protection**: All WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule. ● **Basic web protection**: You can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, if XSS check is not required for a URL, you can whitelist XSS rule.	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
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.

Parameter	Description	Example Value
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

Related Operations

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

5.5.11 Configuring Data Masking Rules to Prevent Privacy Information Leakage

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

NOTE

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

Prerequisites

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

Constraints

It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.

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 (Dedicated)** under **Security**.

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 In the **Data Masking** configuration area, change **Status** if needed and click **Customize Rule**.

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

Step 8 In the displayed dialog box, specify the parameters described in **Table 5-25**.

Table 5-25 Rule parameters

Parameter	Description	Example Value
Path	Part of the URL that does not include the domain name. ● Prefix match: The path ending with * indicates that the path is used as a prefix. For example, if the path to be protected is **/admin/test.php** or **/adminabc**, set **Path** to **/admin***. ● Exact match: The path to be entered must match the path to be protected. If the path to be protected is **/admin**, set **Path** to **/admin**. **NOTE** ● The path supports prefix and exact matches only and does not support regular expressions. ● The path cannot contain two or more consecutive slashes. For example, **///admin**. If you enter **///admin**, WAF converts **///** to **/**.	**/admin/login.php** For example, if the URL to be protected is **http://www.example.com/admin/login.php**, set **Path** to **/admin/login.php**.
Masked Field	A field set to be masked ● **Params**: A request parameter ● **Cookie**: A small piece of data to identify web visitors ● **Header**: A user-defined HTTP header ● **Form**: A form parameter	● If **Masked Field** is **Params** and **Field Name** is **id**, content that matches **id** is masked. ● If **Masked Field** is **Cookie** and **Field Name** is **name**, content that matches **name** is masked.
Field Name	Set the parameter based on **Masked Field**. The masked field will not be displayed in logs. **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

Related Operations

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

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

5.5.12 Creating a Reference Table to Configure Protection Metrics In Batches

This topic describes how to create a reference table to batch configure protection metrics of a single type, such as **Path**, **User Agent**, **IP**, **Params**, **Cookie**, **Referer**, and **Header**. A reference table can be referenced by CC attack protection rules and precise protection rules.

When you configure a CC attack protection rule or precise protection rule, if the **Logic** field in the **Trigger** list is set to **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any value**, **Suffix is any value**, or **Suffix is not any value**, you can select an appropriate reference table from the **Content** drop-down list.

NOTE

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

Prerequisites

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

Application Scenarios

Reference tables can be used for configuring multiple protection fields in CC attack protection 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 (Dedicated)** under **Security**.

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 In the **CC Attack Protection** or **Precise Protection** area, click **Customize Rule**.

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

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

Step 9 In the **Add Reference Table** dialog box, specify the parameters by referring to **Table 5-26**.

Table 5-26 Parameter description

Parameter	Description	Example Value
Name	Table name you entered	test
Type	● **Path**: A URL to be protected, excluding a domain name ● **User Agent**: A user agent of the scanner to be protected ● **IP**: An IP address of the visitor to be protected. ● **Params**: A request parameter to be protected ● **Cookie**: A small piece of data to identify web visitors ● **Referer**: A user-defined request resource For example, if the protected path is **/admin/xxx** and you do not want visitors to be able to access it from *www.test.com*, set **Value** to **http://www.test.com**. ● **Header**: A user-defined HTTP header	**Path**
Value	Value of the corresponding **Type**. Wildcards are not allowed. **NOTE** Click **Add** to add more than one value.	**/buy/phone/**

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

----End

Related Operations

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

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

If WAF blocks a malicious request by IP address, Cookie, or Params, you can configure a known attack source rule to let WAF automatically block all requests from the attack source for a blocking duration set in the known attack source rule. For example, if a blocked malicious request originates from an IP address 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**.

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 (Dedicated)** under **Security**.

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 In the **Known Attack Source** configuration area, change **Status** if needed and click **Customize Rule** to go to the **Known Attack Source** page.

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

Step 8 In the displayed dialog box, specify the parameters by referring to **Table 5-27**.

Table 5-27 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

Related Operations

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

Configuration Example - Blocking Known Attack Source Identified by Cookie

Assume that domain name *www.example.com* has been connected to WAF and a visitor has sent one or more malicious requests through IP address

XXX.XXX.248.195. You want to block access requests from this IP address and whose cookie is **jsessionid** for 10 minutes. Refer to the following steps to configure a rule and verify its effect.

Step 1 On the **Website Settings** page, click *www.example.com* to go to its basic information page.

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

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

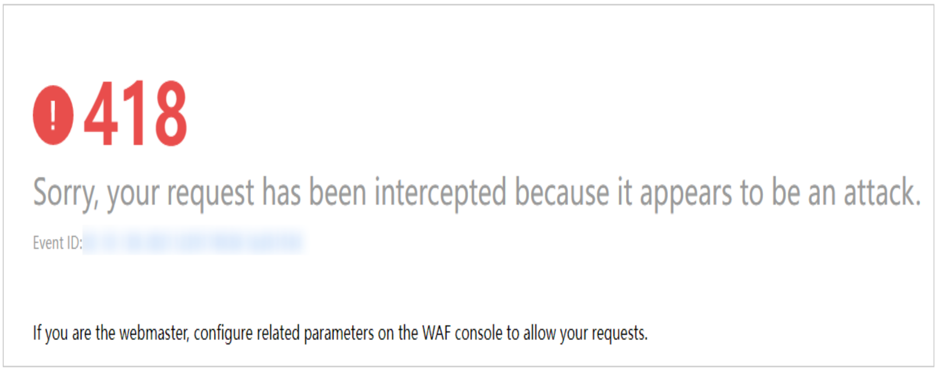
Step 4 Enable the known attack source protection.

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

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

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

Figure 5-9 Block page



418

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

Event ID: [redacted]

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

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

----End

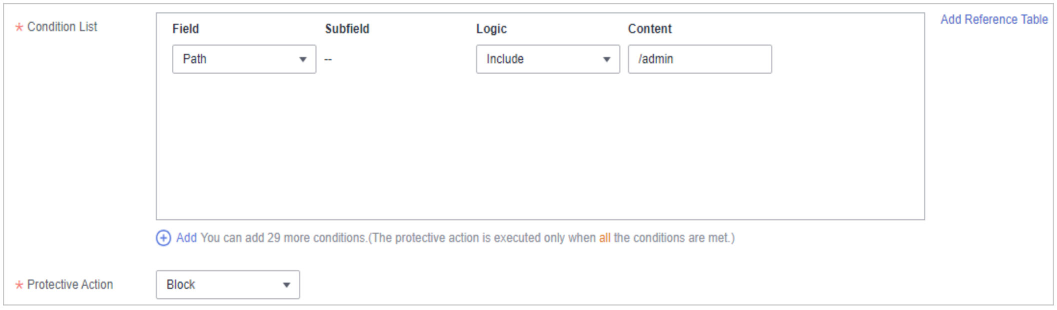
5.5.14 Condition Field Description

When setting a CC attack, precise access, or global whitelist protection rule, there are some fields in the **Condition List** or **Trigger** area. These fields together are used to define the request attributes to trigger the rule. This topic describes the fields that you can specify in conditions to trigger a rule.

What Is a Condition Field?

A condition field specifies the request attribute WAF checks against protection rules. When configuring a **CC attack protection rule**, **precise access protection rule**, or **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 5-10 Condition field



* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/admin

Add Reference Table

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

* Protective Action: Block

A condition field consists of the field, 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 5-28 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

Field	Subfield	Logic	Content (Example)
Params: A request parameter to be protected	- All fields - Any subfield - Custom		201901150929
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

5.6 Managing Policies

5.6.1 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

A protected website domain name can use only one policy.

Procedure

Step 1 Log in to the management console.

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

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

Step 4 In the upper left corner, click **Add Policy**.

Step 5 In the displayed dialog box, enter the policy name and click **Confirm**. The added policy will be displayed in the policy list.

Step 6 In the **Policy Name** column, click the policy name. On the displayed page, add rules to the policy by referring to **Rule Configurations**.

----End

Related Operations

- To modify a policy name, click ✎ next to the policy name. In the dialog box displayed, enter a new policy name.
- To delete a rule, locate the row containing the rule. In the **Operation** column, click **Delete**.

5.6.2 Adding a Domain Name to a Policy

You can add a domain name to a new policy you think applicable. Then, the original policy applied to the domain name stops working on this domain name.

NOTE

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

Prerequisites

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 (Dedicated)** under **Security**.

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.

Step 7 Click **Confirm**.

----End

5.6.3 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 (Dedicated)** under **Security**.

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

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

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

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

Step 8 Set other parameters.

- To add a CC attack protection rule, see **Table 5-16**.
- To add a precise protection rule, see **Table 5-17**.
- To add a blacklist or whitelist rule, see **Table 5-18**.
- To add a geolocation access control rule, see **Table 5-19**.
- To add a WTP rule, see **Table 5-20**.
- To add an information leakage prevention rule, see **Table 5-23**.
- To add a global protection whitelist rule, see **Table 5-24**.
- To add a data masking rule, see **Table 5-25**.

Step 9 Click **Confirm**.

----End

5.7 Website Settings

5.7.1 Connecting a Website to WAF (Dedicated Mode)

5.7.1.1 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.

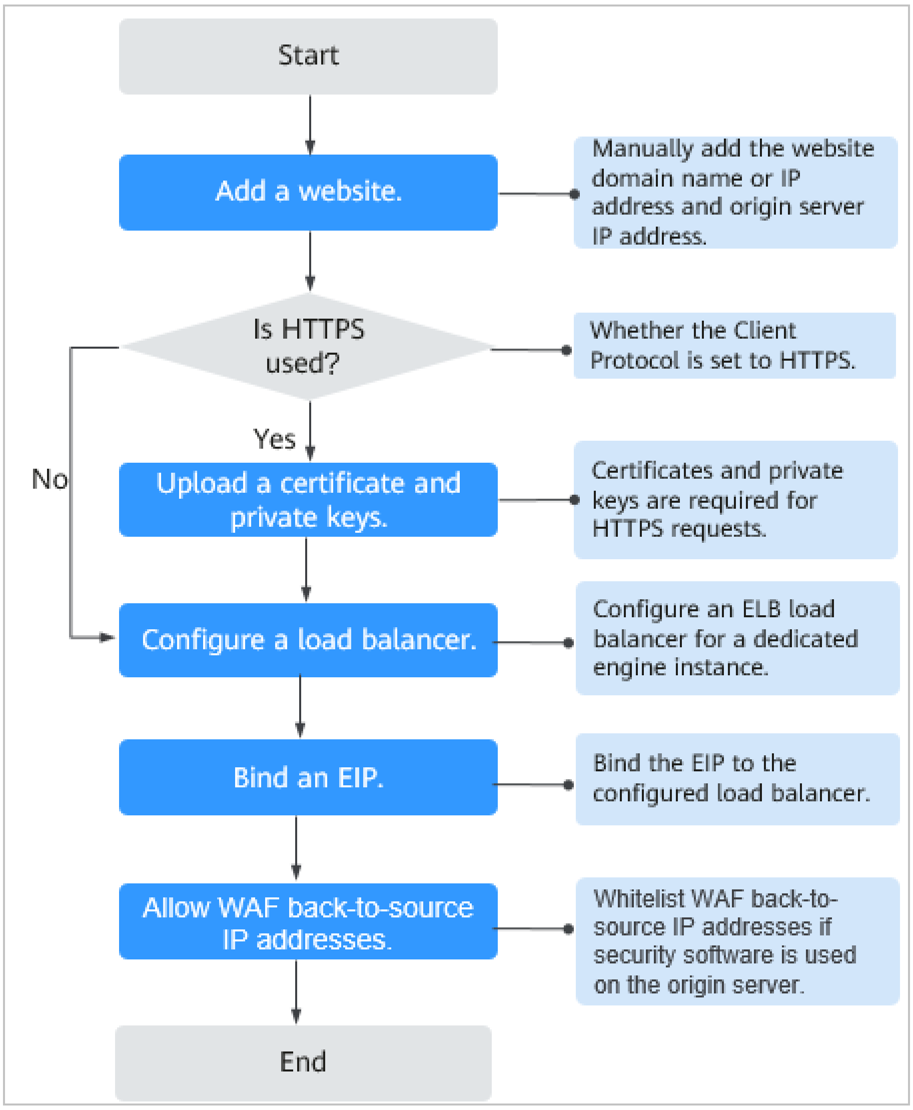
Constraints

- Dedicated WAF instances can protect only web applications and websites that are accessible through domain names or IP addresses.
- A dedicated Elastic Load Balance (ELB) load balancer has been used to distribute workloads for the website you want to add to WAF.

Processes of Connecting a Website to WAF

Before using a dedicated WAF instance, complete the required configurations by following the process shown in **Figure 5-11**.

Figure 5-11 Process of connecting a website to a dedicated WAF instance


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

Collecting Domain Name/IP Address Details

Before adding a domain name or IP address to WAF, obtain the information listed in **Table 5-29**.

Table 5-29 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	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
	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

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 a certificate is not in .pem, convert it 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 My Domain Name or IP Address Inaccessible?**

5.7.1.2 Step 1: Add a Website to WAF (Dedicated Mode)

If your service servers are deployed on the cloud, you can add the domain name or IP address of the website to WAF so that the website traffic is forwarded to WAF for inspection.

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 applied for 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.
- If your website has no layer-7 proxy server such as CDN and cloud acceleration service deployed in front of WAF and uses only layer-4 load balancers (or NAT), set **Proxy Configured** to **No**. Otherwise, **Proxy Configured** must be set to **Yes**. This ensures that WAF obtains real IP addresses of website visitors and takes protective actions configured in protection policies.

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 (Dedicated)** under **Security**.

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

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

Step 6 Configure basic information of the domain name referring to **Table 5-30**.

Table 5-30 Parameter description

Parameter	Description	Example Value
Website Name	Website name you specify.	WAF-OCB
Protected Object	A domain name or IP address of the website to be protected. The domain name 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 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.	Single domain name: **www.example.com** Wildcard domain name: ***.example.com** IP address format: *XXX.XXX.1.1*
Website Remarks	Brief description of the website	test
Protected Port	Select the port that needs to be protected from the drop-down list box. To protect port 80 or 443, select **Standard port** from the drop-down list.	Standard ports

Parameter	Description	Example Value
Server Configuration	Address of the web server. The configuration contains the **Client Protocol**, **Server protocol**, VPC, **Server Address,** and **Server Port**. ● **Client Protocol**: Protocol used for forwarding a client requests to the dedicated WAF instance. The options are **HTTP** and **HTTPS**. ● **Server Protocol**: Protocol used for forwarding a client request to the origin server through the dedicated WAF instance. The options are **HTTP** and **HTTPS**. **NOTE** WAF can check WebSocket and WebSockets requests, which is enabled by default. ● **VPC**: Select the VPC to which the dedicated WAF instance belongs. ● **Server Address**: Private IP address of the website server that a client (for example, a browser) accesses. ● **Server Port**: service port of the server to which the dedicated WAF instance forwards client requests.	**Client Protocol**: **HTTP** **Server Protocol**: **HTTP** **VPC**: vpc-default **Server Address**: *192.168.1.1* **Server Port**: **80**
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**. For details about how to create a certificate, see **Uploading a Certificate**. **NOTICE** ● Only .pem certificates can be used in WAF. If the certificate is not in .pem, convert it into a .pem certificate by referring to **Importing a New Certificate** before uploading the certificate. ● 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, you need to add domain names one by one in WAF.	None

Step 7 Configure **Proxy Configured**.

If your website has no layer-7 proxy server such as CDN and cloud acceleration service deployed in front of WAF and uses only layer-4 load balancers (or NAT), set **Proxy Configured** to **No**. Otherwise, **Proxy Configured** must be set to **Yes**.

This ensures that WAF obtains real IP addresses of website visitors and takes protective actions configured in protection policies.

Step 8 Select a policy. By default, **System-generated policy** is selected.

You can select a policy you configured. 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.

Step 9 Click **Confirm**.

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** and **Step 3: Bind an EIP to a Load Balancer**.

----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.

   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 5-31** before uploading it.

Table 5-31 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**.

5.7.1.3 Step 2: Configure a Load Balancer for WAF

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

Prerequisites

- You have added a website to a dedicated WAF instance.
- You have created a load balancer.
- 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.

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.
- 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 **Basic Information** page.

Step 5 Click the **Listeners** tab. 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.

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

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.

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.

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 upper left corner and choose **Web Application Firewall (Dedicated)** under **Security**.

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

Step 5 In the row 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**.

NOTICE

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

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)**.

----End

Verification

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

5.7.1.4 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**.

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

5.7.1.5 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 upper left corner and choose **Web Application Firewall (Dedicated)** under **Security**.

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

Step 5 In the **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 5-32**.

Table 5-32 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 ELB to distribute traffic, perform the following steps to configure an access control policy to allow only the IP addresses of the dedicated WAF instances to access the origin server:

Step 1 Log in to the management console.

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

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

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

Step 5 In the **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 On the displayed details page, click the **Listeners** tab and then click **Configure Access Control** in the **Access Control** column.

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

1. Click **Create IP Address Group** and add the IP addresses of the dedicated WAF instances into the IP address group. You can obtain these IP addresses from **Step 5**.
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

5.7.1.6 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.

- 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.

5.7.2 Advanced Settings

5.7.2.1 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 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.

NOTE

If you have enabled enterprise projects, ensure that you have all operation permissions for the project where your WAF instance locates. Then, you can select the enterprise project from the **Enterprise Project** drop-down list and configure PCI DSS or PCI 3DS and TLS for the domain names.

Prerequisites

- The website to be protected has been added to WAF.
- Your website uses HTTPS as the client protocol.

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 5-33** lists the recommended minimum TLS versions for different scenarios.

Table 5-33 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.
Websites with basic security requirements, for example, small- and medium-sized enterprise websites.	TLS v1.1	WAF automatically blocks website access requests that use TLS v1.0.
Client applications with no special security requirements	TLS v1.0	Requests using any TLS protocols can access the website.

NOTE

Before you configure TLS, **check the TLS version of your website**.

The recommended cipher suite in WAF is **Cipher suite 1**. Cipher suite 1 offers a good mix of browser compatibility and security. For details about each cipher suite, see **Table 5-34**.

NOTE

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

Table 5-34 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 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 Name	Cipher Suite Configuration Value	Description
Cipher suite 2	● EECDH+AESGCM ● EDH+AESGCM	● Compatibility: Average. Strict compliance with forward secrecy requirements of PCI DSS and excellent protection, but browsers of earlier versions may be unable to access the website. ● Security: Excellent
Cipher suite 3	● ECDHE-RSA-AES128-GCM-SHA256 ● ECDHE-RSA-AES256-GCM-SHA384 ● ECDHE-RSA-AES256-SHA384 ● RC4 ● HIGH ● !MD5 ● !aNULL ● !eNULL ● !NULL ● !DH ● !EDH	● Compatibility: Average. Earlier versions of browsers may be unable to access the website. ● Security: Excellent. Multiple algorithms, such as ECDHE, DHE-GCM, and RSA-AES-GCM, are supported.
Cipher suite 4	● ECDHE-RSA-AES256-GCM-SHA384 ● ECDHE-RSA-AES128-GCM-SHA256 ● ECDHE-RSA-AES256-SHA384 ● AES256-SHA256 ● RC4 ● HIGH ● !MD5 ● !aNULL ● !eNULL ● !NULL ● !EDH	● Compatibility: Good. A wide range of browsers are supported. ● Security: Average. The GCM algorithm is supported.

Cipher Suite Name	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 5-35** 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 5-35 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 (Dedicated)** under **Security**.

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.

- 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.

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.

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

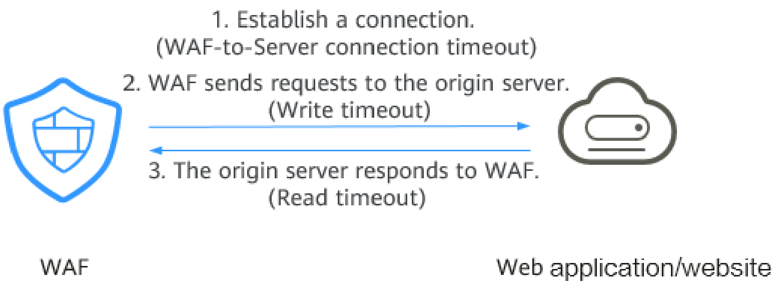
If you want to set a timeout duration for each request between your WAF instance and origin server, enable **Timeout Settings** and specify **WAF-to-Server connection timeout (s)**, **Read timeout (s)**, and **Write timeout (s)**. This function cannot be disabled once it is enabled.

- **WAF-to-Server Connection Timeout**: timeout for WAF and the origin server to establish a TCP connection.
- **Write Timeout**: Timeout set for WAF to send a request to the origin server. If the origin server does not receive a request within the specified write timeout, the connection times out.

- **Read Timeout**: Timeout set for WAF to read responses from the origin server. If WAF does not receive any response from the origin server within the specified read timeout, the connection times out.

Figure 5-12 shows the three steps for WAF to forward requests to an origin server.

Figure 5-12 WAF forwarding requests to origin servers.


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

NOTE

- The timeout for connections from a browser to WAF is 120 seconds. The value varies depending on your browser settings and cannot be changed on the WAF console.
- The default timeout duration for the connection between WAF and an origin server is 30 seconds. This topic walks you through how to customize the timeout duration.

Prerequisites

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

Constraints

- The timeout duration for connections between a browser and WAF cannot be modified. Only timeout duration for connections between WAF and your origin server can be modified.
- This function cannot be disabled once it is enabled.

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 (Dedicated)** under **Security**.

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

5.7.2.3 Enabling 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.

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 **Connection Protection**, make sure **you have updated dedicated WAF instances to the latest version,** or your services might be affected.

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 (Dedicated)** under **Security**.

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 **Connection Protection** area, click the status toggle to enable it.

Step 7 Click ✎ next to each parameter, edit **Breakdown Protection** and **Connection Protection** parameters to meet your requirements, and click ✓ to save settings. **Table 5-36** describes these parameters.

Table 5-36 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
	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

Parameter		Description	Example Value
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

----End

5.7.2.4 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

- 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 (Dedicated)** under **Security**.

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 5-37**.

Table 5-37 Traffic identifier parameters

Tag	Description	Example Value
IP Tag	HTTP request header field of the original client IP address. 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
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

5.7.2.5 Modifying the Alarm Page

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

NOTE

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

Prerequisites

A website has been added to WAF.

Constraints

- 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 (Dedicated)** under **Security**.

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.
- 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**.

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

  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

5.7.3 Basic Information

5.7.3.1 Viewing Basic Information

This topic describes how to view the basic information about a protected website, switch WAF working mode, and delete a domain name of a protected website from WAF.

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 (Dedicated)** under **Security**.

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 5-38**.

Table 5-38 Parameter description

Parameter	Description
Domain Name	Domain name or IP address of a website you want to protect.
Protection	How your WAF instance is deployed for your website. Only **Dedicated mode** is available.

Parameter	Description
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. Click ▾ and select one of the following working mode: ● **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. For details, see **Switching WAF Working Mode**.
Policy	The total number of protection policies configured in WAF. You can click a number to go to the rule configuration page.
Access Progress	The progress of connecting your website to WAF or the website access status.
Created	Time when the domain name was added to WAF.
Enterprise Project	Enterprise project to which the domain name belongs.

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.

----End

5.7.3.2 Switching WAF Working Mode

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

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.

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 (Dedicated)** under **Security**.

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

Step 5 In the **Mode** column of the row containing the target domain name, click ▾ and select a working mode.

----End

5.7.3.3 Updating a Certificate

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

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

- If you plan to update the certificate associated with the website, associate a new certificate with your website on the WAF console.

NOTE

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

Prerequisites

- The website to be protected has been added to WAF.
- Your website uses HTTPS as the client protocol.

Constraints

- Each domain name must have a certificate associated. A wildcard domain name can only use a wildcard domain certificate. If you only have single-domain certificates, add domain names one by one in WAF.
- Only .pem certificates can be used in WAF. If the certificate is not in .pem, before uploading it, convert it to .pem by referring to **Step 6**.

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.

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 (Dedicated)** under **Security**.

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.

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 5-39** before uploading it.

Table 5-39 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.

Step 7 Click **Confirm**.

----End

5.7.3.4 Editing Server Information

This topic describes how to edit or add server information for a website to be protected.

Applicable scenarios:

- Modify server information, including **Client Protocol**, **Server Protocol**, **VPC**, **Server Address**, 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 (Dedicated)** under **Security**.

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 ✎.

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**.

Step 8 Click **Confirm**.

----End

5.7.3.5 Deleting a Protected Website from WAF

This topic describes how to remove a website from WAF if you no longer need to protect it.

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

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 (Dedicated)** under **Security**.

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.

If you want to retain the policy applied 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

5.8 Certificate Management

5.8.1 Uploading a Certificate

If you select **HTTPS** for **Client Protocol** when you add a website to WAF, a certificate must be associated with the website.

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

NOTE

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

Prerequisites

You have obtained the certificate file and certificate private key.

Specification Limitations

You can create 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 WAF can protect 10 domain names, you can create 10 certificates in WAF.

Constraints

If you import a new certificate when adding a protected website or updating a certificate, the certificate is added to the certificate list on the **Certificates** page, and the imported certificates is counted in the number of created certificates.

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 (Dedicated)** under **Security**.

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

Step 5 Click **Upload 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.

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 5-40** before uploading it.

Table 5-40 Certificate conversion commands

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

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

NOTE

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

Step 7 Click **Confirm**.

----End

Verification

The certificate you created is displayed in the certificate list.

Related Operations

- To change the certificate name, move the cursor over the name of the certificate, click ✎, and enter a certificate name.

  NOTICE

  If the certificate is in use, unbind the certificate from the domain name first. Otherwise, the certificate name cannot be changed.

- To view details about a certificate, click **View** in the **Operation** column of the certificate.

- In the row containing the certificate you want, click **Use** in the **Operation** column to use the certificate to the corresponding domain name.
- To delete a certificate, locate the row of the certificate and click **Delete** in the **Operation** column.

5.8.2 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 (Dedicated)** under **Security**.

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

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

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

Step 7 Click **Confirm**.

----End

Verification

The protected website is listed in the **Domain Name** column of the certificate.

Related Operations

- To change the certificate name, move the cursor over the name of the certificate, click ✎, and enter a certificate name.

  NOTICE

  If the certificate is in use, unbind the certificate from the domain name first. Otherwise, the certificate name cannot be changed.

- To view details about a certificate, click **View** in the **Operation** column of the certificate.
- To delete a certificate, locate the row of the certificate and click **Delete** in the **Operation** column.

5.8.3 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 (Dedicated)** under **Security**.

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

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

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

----End

Related Operations

If a certificate to be deleted is bound to a website, unbind it from the website before deletion.

To unbind a certificate from a website domain name, perform the following steps:

Step 1 In the **Domain Name** column of the row containing the desired certificate, click the domain name to go to the basic information page.

Step 2 Click ✎ next to the certificate name. In the displayed dialog box, upload a new certificate or select an existing certificate.

----End

5.8.4 Viewing Certificate Information

This topic describes how to view certificate details, including the certificate name, domain name a certificate is used for, and expiration time.

NOTE

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

Prerequisites

You have created a certificate to WAF.

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 (Dedicated)** under **Security**.

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

Step 5 View the certificate information. **Table 5-41** describes the parameters.

Table 5-41 Certificate parameters

Parameter	Description
Name	Certificate name.

Parameter	Description
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.

----End

Related Operations

- To change the certificate name, move the cursor over the name of the certificate, click ✎, and enter a certificate name.

  NOTICE

  If the certificate is in use, unbind the certificate from the domain name first. Otherwise, the certificate name cannot be changed.

- To view details about a certificate, click **View** in the **Operation** column of the certificate.
- In the row containing the certificate you want, click **Use** in the **Operation** column to use the certificate to the corresponding domain name.
- To delete a certificate, locate the row of the certificate and click **Delete** in the **Operation** column.

5.9 System Management

5.9.1 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 applied for a dedicated WAF instance.
- Your login account has the **IAM ReadOnly** permission.

Viewing Information About a Dedicated WAF Instance

Step 1 Log in to the management console.

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

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

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

Step 5 View information about a dedicated WAF instance. **Table 5-42** describes parameters.

Table 5-42 Key parameters of dedicated WAF instances

Parameter	Description	Example Value
Instance Name	Name automatically generated when an instance is created.	None
Protected Website	Domain name of the website protected by the instance.	www.example.com
VPC	VPC where the instance resides	vpc-waf
Subnet	Subnet where an instance resides	subnet-62bb
IP Address	IP address of the subnet in the VPC where the WAF instance is deployed.	192.168.0.186
Access Status	Connection status of the instance.	Accessible
Running Status	Status of the instance.	Running
Version	Dedicated WAF	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 and choose **Web Application Firewall (Dedicated)** under **Security**.

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

Step 5 In the row of the instance, click **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 and choose **Web Application Firewall (Dedicated)** under **Security**.

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

Step 5 In the row 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 anytime. A deleted dedicated WAF instance will no longer protect the website added to it.

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 and choose **Web Application Firewall (Dedicated)** under **Security**.

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

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

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

----End

5.9.2 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 applied for a 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 and choose **Web Application Firewall (Dedicated)** under **Security**.

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**.

----End

5.10 Authorizing and Associating an Enterprise Project

Enterprise Management service provides unified cloud resource management based on enterprise projects, and resource and personnel management within enterprise projects. Enterprise projects can be managed by one or more user groups. You can create WAF enterprise projects on the Enterprise Management console to manage your WAF resources centrally.

Creating an Enterprise Project and Assigning Permissions

- Creating an enterprise project

  On the management console, click **Enterprise** in the upper right corner to go to the **Enterprise Management** page. Click **Create Enterprise Project** and enter a name.

  NOTE

  Enterprise is available on the management console only if you have enabled the enterprise project, or you have an enterprise account.

- Authorization

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

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

  b. In the navigation pane on the left, choose **Personnel Management** > **User Management**. Locate the row that contains the target user, click **Add to User Group** in the **Operation** column. In the available user groups on the left pane, select the target ones and move them to the right pane.

- Associating the resource with enterprise projects

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

  – Associate a WAF instance with an enterprise project when applying for WAF

- 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.

5.11 Auditing

5.11.1 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 5-43 WAF Operations Recorded by CTS

Operation	Resource Type	Trace Name
Creating a WAF instance	instance	createInstance
Deleting a WAF instance	instance	deleteInstance
Modifying a WAF instance	instance	alterInstanceName
Modifying the protection status of a WAF instance	instance	modifyProtectStatus
Modifying the connection status of a WAF instance	instance	modifyAccessStatus
Creating a WAF policy	policy	createPolicy
Applying a WAF policy	policy	applyToHost
Modifying a policy	policy	modifyPolicy
Deleting a WAF policy	policy	deletePolicy
Uploading a certificate	certificate	createCertificate
Changing the name of a certificate	certificate	modifyCertificate
Deleting a certificate	certificate	deleteCertificate
Adding a CC attack protection rule	policy	createCc
Modifying a CC attack protection rule	policy	modifyCc
Deleting a CC attack protection rule	policy	deleteCc

Operation	Resource Type	Trace Name
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
Deleting a web tamper protection rule	policy	deleteAntitamper
Creating a global protection whitelist rule	policy	createIgnore
Deleting a rule	policy	deleteIgnore
Adding a data masking rule	policy	createPrivacy
Modifying a data masking rule	policy	modifyPrivacy
Deleting a data masking rule	policy	deletePrivacy

5.11.2 Viewing an Audit Trace

After you enable CTS, the system starts recording operations on WAF. You can view the operation records for the last seven days on the CTS console.

Viewing WAF Logs on the CTS 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 management console and select **Cloud Trace Service** under **Management & Deployment**.

Step 4 Choose **Trace List** in the navigation pane.

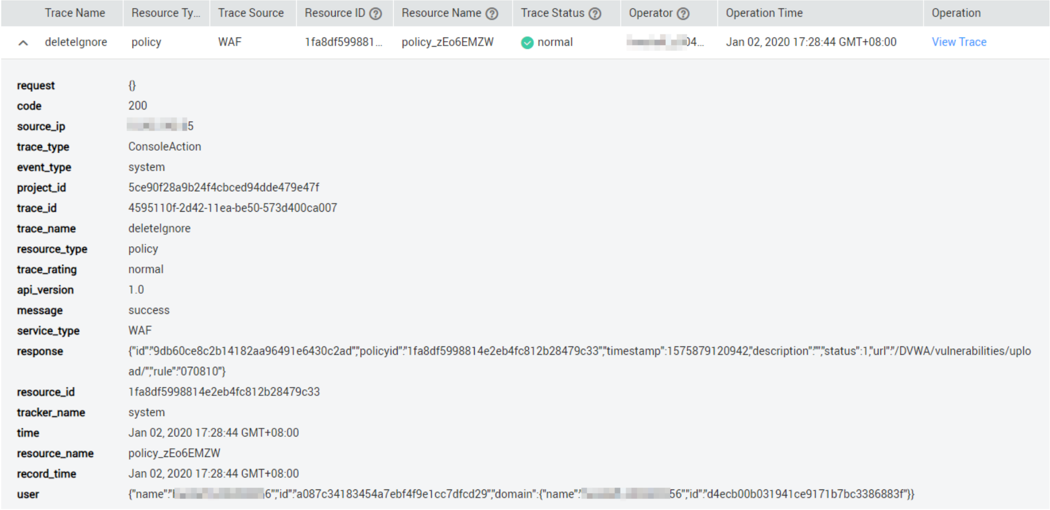
Step 5 Click **Filter** and specify filtering criteria as needed. The following four filters are available:

- **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**.
  - Set **Trace Type** to **Management**.
  - Set **Trace Source** to **WAF**.
  - When you select **Resource ID** for **Search By**, you also need to enter a resource ID.
- **Operator**: Select a specific operator (a user other than tenant).
- **Trace Status**: Available options include **All trace statuses**, **normal**, **warning**, and **incident**. You can only select one of them.
- **Time Range**: In the upper right corner of the page, you can query traces in the last 1 hour, last 1 day, last 1 week, or within a customized period.

Step 6 Click **Query**.

Step 7 Click ⌄ on the left of a trace to see its details.

Figure 5-13 Expanding trace details

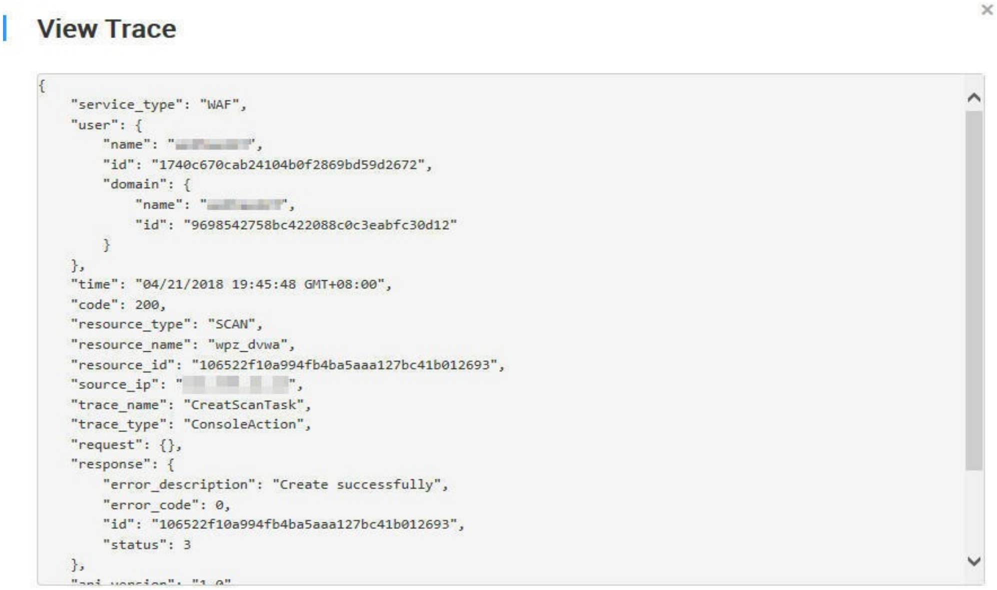


	Trace Name	Resource Ty...	Trace Source	Resource ID ⓘ	Resource Name ⓘ	Trace Status ⓘ	Operator ⓘ	Operation Time	Operation
⌃	deleteIgnore	policy	WAF	1fa8df599881...	policy_zEo6EMZW	✓ normal	[redacted]04...	Jan 02, 2020 17:28:44 GMT+08:00	View Trace

request	{}
code	200
source_ip	[redacted]5
trace_type	ConsoleAction
event_type	system
project_id	5ce90f28a9b24f4cbced94dde479e47f
trace_id	4595110f-2d42-11ea-be50-573d400ca007
trace_name	deleteIgnore
resource_type	policy
trace_rating	normal
api_version	1.0
message	success
service_type	WAF
response	{"id":"9db60ce8c2b14182aa96491e6430c2ad","policyid":"1fa8df5998814e2eb4fc812b28479c33","timestamp":1575879120942,"description":"","status":1,"url":"/DVWA/vulnerabilities/upload/","rule":"070810"}
resource_id	1fa8df5998814e2eb4fc812b28479c33
tracker_name	system
time	Jan 02, 2020 17:28:44 GMT+08:00
resource_name	policy_zEo6EMZW
record_time	Jan 02, 2020 17:28:44 GMT+08:00
user	{"name":"[redacted]6","id":"a087c34183454a7ebf4f9e1cc7dfcd29","domain":{"name":"[redacted]56","id":"d4ecb00b031941ce9171b7bc3386883f"}}

Step 8 Click **View Trace** in the **Operation** column. In the displayed **View Trace** dialog box, the trace structure details are displayed.

Figure 5-14 Viewing the trace



View Trace

```
{
    "service_type": "WAF",
    "user": {
        "name": "[redacted]",
        "id": "1740c670cab24104b0f2869bd59d2672",
        "domain": {
            "name": "[redacted]",
            "id": "9698542758bc422088c0c3eabfc30d12"
        }
    },
    "time": "04/21/2018 19:45:48 GMT+08:00",
    "code": 200,
    "resource_type": "SCAN",
    "resource_name": "wpz_dvwa",
    "resource_id": "106522f10a994fb4ba5aaa127bc41b012693",
    "source_ip": "[redacted]",
    "trace_name": "CreatScanTask",
    "trace_type": "ConsoleAction",
    "request": {},
    "response": {
        "error_description": "Create successfully",
        "error_code": 0,
        "id": "106522f10a994fb4ba5aaa127bc41b012693",
        "status": 3
    },
    "api_version": "1.0"
```

----End

6 Best Practices

6.1 Mitigating Web Security Vulnerabilities

6.1.1 Java Spring Framework Remote Code Execution Vulnerability

Spring Framework is a lightweight open-source application framework for developing enterprise Java applications. A remote code execution (RCE) vulnerability was disclosed in the Spring framework and classified as critical. This vulnerability can be exploited to attack Java applications running on JDK 9 or later versions.

Vulnerability Name

Zero-Day RCE Vulnerability in the Spring Framework

Affected Versions

- JDK 9 or later
- Applications developed using the Spring Framework or derived framework

Mitigation

Step 1 **Apply for Dedicated WAF Engine**.

Step 2 Add the website domain name to WAF and connect it to WAF.

- Cloud mode: **Creating a Domain Name**
- Dedicated mode: **Step 1: Add a Website to WAF (Dedicated Mode)**

Step 3 In the **Basic Web Protection** configuration area, set **Mode** to **Block**. For details, see **Configuring Basic Protection Rules to Defend Against Common Web Attacks**.

NOTICE

There are two types of malicious payload in this vulnerability. Whether to enable **Header Inspection** depends on the type of payloads in your services.

- Type 1: Malicious payloads are included in submitted parameters. In this situation, **Header Inspection** can be disabled.
- Type 2: Malicious payloads are included in a custom header field. In this situation, **Header Inspection** must be enabled to block attacks.

Type 2 malicious payloads depend on Type 1 malicious payloads so whether to enable **Header Inspection** is determined by your service requirements.

----End

6.1.2 Apache Dubbo Deserialization Vulnerability

On February 10, 2020, Apache Dubbo officially released the CVE-2019-17564 vulnerability notice, and the vulnerability severity is medium. Unsafe deserialization occurs within a Dubbo application which has HTTP remoting enabled. An attacker may submit a POST request with a Java object in it to completely compromise a Provider instance of Apache Dubbo, if this instance enables HTTP. Now, WAF provides protection against this vulnerability.

Affected Versions

This vulnerability affects Apache Dubbo 2.7.0 to 2.7.4, 2.6.0 to 2.6.7, and all 2.5.*x*. versions.

Mitigation Version

Apache Dubbo 2.7.5

Solutions

Upgrade Apache Dubbo to version 2.7.5.

If a quick upgrade is not possible or you want to defend against more vulnerabilities, use WAF. The procedure is as follows:

Step 1 **Apply for a dedicated WAF instance**.

Step 2 Add the website domain name to WAF and route website traffic to WAF.

- Cloud mode: **Creating a Domain Name**
- Dedicated mode: **Step 1: Add a Website to WAF (Dedicated Mode)**

Step 3 Set the mode of Basic Web Protection to **Block**. For details, see **Configuring Basic Protection Rules to Defend Against Common Web Attacks**.

----End

6.1.3 DoS Vulnerability in the Open-Source Component Fastjson

On September 3, 2019, the security team detected a DoS vulnerability in multiple versions of the widely used open-source component Fastjson. An attacker can exploit this vulnerability to construct malicious requests and send them to the server that uses Fastjson. As a result, the memory and CPU of the server are used up, and the server breaks down, causing service breakdown. WAF provides protection against this vulnerability.

Affected Versions

Versions earlier than Fastjson 1.2.60

Mitigation Version

Fastjson 1.2.60

Official Solution

Upgrade the open-source component Fastjson to 1.2.60.

Mitigation

WAF can detect and defend against this vulnerability. The procedure is as follows:

Step 1 **Apply for a dedicated WAF instance**.

Step 2 Add the website domain name to WAF and route website traffic to WAF.

- Cloud mode: **Creating a Domain Name**
- Dedicated mode: **Step 1: Add a Website to WAF (Dedicated Mode)**

Step 3 Set the mode of Basic Web Protection to **Block**. For details, see **Configuring Basic Protection Rules to Defend Against Common Web Attacks**.

----End

6.1.4 Remote Code Execution Vulnerability of Fastjson

On July 12, 2019, the Emergency Response Center detected that the open-source component Fastjson had a remote code execution vulnerability. This vulnerability is an extension of the deserialization vulnerability of Fastjson 1.2.24 detected in 2017 and can be directly used to obtain server permissions, causing serious damage.

Affected Versions

Versions earlier than Fastjson 1.2.51

Mitigation Version

Fastjson 1.2.51 or later

Official Solution

Upgrade Fastjson to 1.2.51 or the latest 1.2.58 version.

Mitigation

The built-in protection rules of WAF can defend against this vulnerability. The procedure is as follows:

Step 1 **Apply for a dedicated WAF instance**.

Step 2 Add the website domain name to WAF and route website traffic to WAF.

- Cloud mode: **Creating a Domain Name**
- Dedicated mode: **Step 1: Add a Website to WAF (Dedicated Mode)**

Step 3 Set the mode of Basic Web Protection to **Block**. For details, see **Configuring Basic Protection Rules to Defend Against Common Web Attacks**.

----End

6.1.5 Oracle WebLogic wls9-async Deserialization Remote Command Execution Vulnerability (CNVD-C-2019-48814)

It revealed that the Oracle WebLogic wls9-async component had a deserialization vulnerability. Unauthorized remote attackers can use this vulnerability to implement remote code execution and gain server permissions.

Vulnerability ID

CNVD-C-2019-48814

Vulnerability Name

Oracle WebLogic wls9-async Deserialization Remote Command Execution Vulnerability

Vulnerability Description

The WebLogic wls9-async component has a defect. The website built on the WebLogic Server has security risks. Attackers can construct HTTP requests to obtain the permission of the target server and execute arbitrary code remotely without authorization.

Affected Products

- Oracle WebLogic Server 10.X
- Oracle WebLogic Server 12.1.3

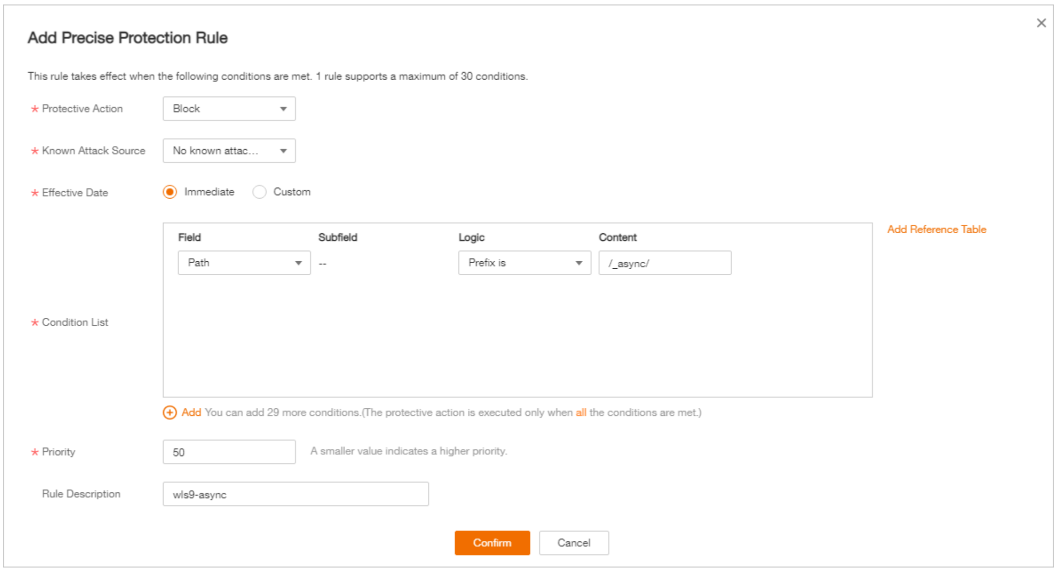
Official Solution

The patch for fixing this vulnerability has not been released.

Mitigation

Configure precise protection rules to restrict access from the URLs whose prefixes are **/_async/** or **/wls-wsat/** by referring to **Figure 6-1** and **Figure 6-2** and block remote code execution requests initiated by exploiting this vulnerability.

Figure 6-1 async configuration



Add Precise Protection Rule

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

* Protective Action: Block

* Known Attack Source: No known attac...

* Effective Date: ● Immediate ○ Custom

* Condition List

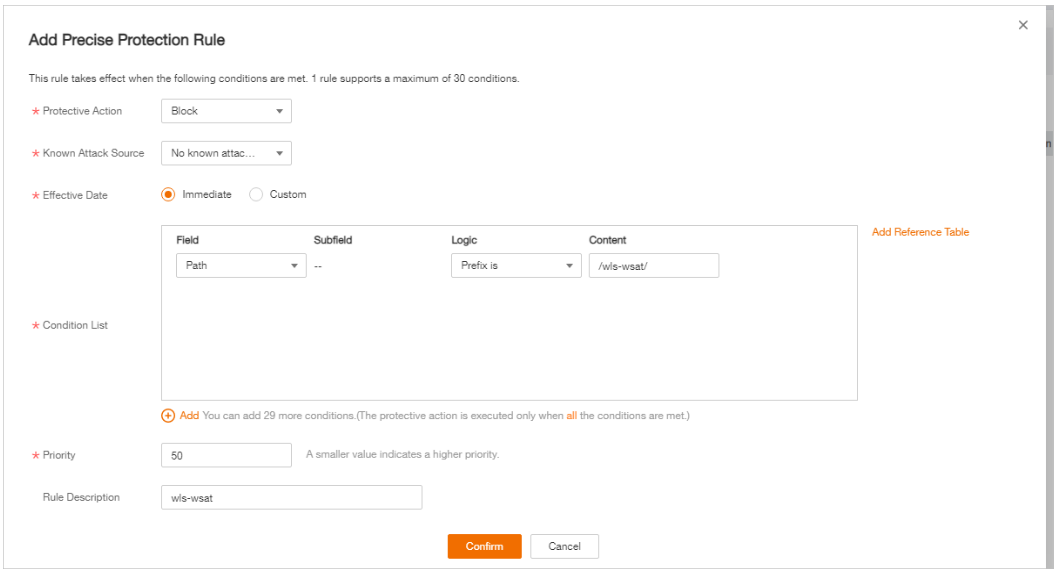
Field	Subfield	Logic	Content
Path	--	Prefix is	/_async/

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

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

Rule Description: wls9-async

Figure 6-2 wls-wsat configuration



Add Precise Protection Rule

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

* Protective Action: Block

* Known Attack Source: No known attac...

* Effective Date: ● Immediate ○ Custom

* Condition List

Field	Subfield	Logic	Content
Path	--	Prefix is	/wls-wsat/

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

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

Rule Description: wls-wsat

6.2 Configuring the Minimum TLS Version and Cipher Suite to Better Secure Connections

HTTPS is a network protocol constructed based on Transport Layer Security (TLS) and HTTP for encrypted transmission and identity authentication. When you add a domain name to WAF, set **Client Protocol** to **HTTPS**. Then, you can configure the minimum TLS version and cipher suite to harden website security. The details are as follows:

- Minimum TLS version

  The minimum TLS version that can be used by a client to access the website. After you configure the minimum TLS version, only the requests over the connections secured with the minimum TLS version or the later version can access your website. This helps you meet security requirements for industrial websites.

  NOTE

  - Up to now, three TLS versions (TLS v1.0, TLS v1.1, and TLS v1.2) have been released, among which TLS v1.0 and TLS v1.1 have been released for a long time. Some encryption algorithms (such as SHA1 and RC4) used by TLS v1.0 and TLS v1.1 are vulnerable to attacks. TLS v1.0 and TLS v1.1 cannot meet the geometric growth of data transmission encryption requirements, which might bring potential security risks. To secure the communication and meet the Payment Card Industry Data Security Standard (PCI DSS), PCI Security Standards Council (PCI SSC) stated that it no longer accepted TLS v1.0 as of June 30, 2018. Vendors of mainstream browsers, such as Mozilla Firefox, Apple Safari, Google Chrome, and Microsoft Edge, also declared that they would stop supporting TLS v1.0 and TLS v1.1 by 2020.
  - You can query the TLS version supported by the website through other tools.

- Cipher suites

  A cipher suite is a set of algorithms that help secure a network connection through TLS. A more secure cipher suite can better secure the confidentiality and data integrity of websites.

Recommended Minimum TLS Versions for Different Scenarios

To better secure your website, configure an appropriate TLS version. **Table 6-1** lists the recommended minimum TLS versions for different scenarios.

Table 6-1 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.
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.

Recommended Cipher Suites

The default 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 6-2**.

NOTE

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

Table 6-2 Description of cipher suites

Cipher Suite	Cryptographic Algorithm	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 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 earlier version browsers may be unable to access the website. • Security: Excellent
Cipher suite 3	ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH	• Compatibility: Average. Earlier versions of browsers may be unable to access the website. • Security: Excellent. Support for ECDHE, DHE-GCM, and RSA-AES-GCM algorithms but not CBC

Cipher Suite	Cryptographic Algorithm	Description
Cipher suite 4	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH	● Compatibility: Good. A wide range of browsers are supported. ● Security: Average. The GCM algorithm is supported.
Cipher suite 5	AES128-SHA:AES256-SHA:AES128-SHA256:AES256-SHA256:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4:!DHE:@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 cipher suites provided by WAF are compatible with the latest browsers and clients, but are incompatible with some browsers of earlier versions. Compatible browsers or clients of a certain cipher suite may vary depending on the TLS version configured. Using TLS v1.0 as an example, **Table 6-3** describes the browser and client compatibility.

NOTICE

It is recommended that compatibility tests should be carried out on the service environment to ensure service stability.

Table 6-3 Incompatible browsers and clients for cipher suites under TLS v1.0

Browser/Client	Default Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4
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

Configuring the Minimum TLS Version and Cipher Suite

The following describes how to configure TLS v1.2 and cipher suite 1 as the minimum TLS version and how to verify that the configuration takes effect for dedicated WAF instances.

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 (Dedicated)** under **Security**.

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 Click ✎ in the **TLS Configuration** row.

NOTE

WAF allows you to enable PCI DSS and PCI 3-Domain Secure (3DS) compliance certification checks with just a few clicks. After they are enabled, WAF will configure the minimum TLS version in accordance with the PCI DSS and PCI 3DS compliance certification requirements.

- 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.

Step 7 In the displayed **TLS Configuration** dialog box, select **TLS v1.2** as the minimum TLS version and **Cipher suite 1**.

Step 8 Click **Confirm**.

----End

Verification

If the **Minimum TLS Version** is set to **TLS v1.2**, verify that 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.

You can run commands on the local PC to check whether the TLS is configured successfully. Before the verification, ensure that **OpenSSL** has been installed on your local PC.

Step 1 Copy the CNAME record of the protected domain name and use the CNAME record to obtain WAF back-to-source IP addresses.

1. Log in to the management console.
2. Click 📍 in the upper left corner of the management console and select a region or project.
3. Click ☰ in the upper left corner and choose **Web Application Firewall (Dedicated)** under **Security**.
4. In the navigation pane on the left, choose **Website Settings**.
5. In the **Domain Name** column, click the domain name of the website to go to the basic information page.
6. In the **CNAME** row, click ⧉ to copy the CNAME record.

Step 2 Obtain the WAF back-to-source IP addresses.

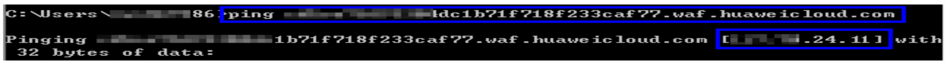
- Cloud mode

  In the command line interface (CLI) of the Windows OS, run the following command to obtain WAF back-to-source IP addresses:

  ping *CNAME record*

  The command output displays WAF back-to-source IP addresses. **Figure 6-3** shows an example.

Figure 6-3 ping cname



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

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

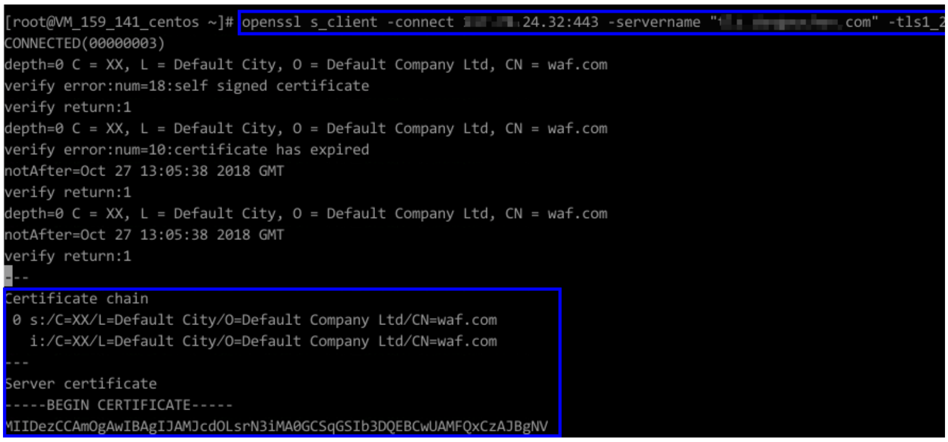
- Dedicated mode
  a. In the navigation pane on the left, choose **Instances Management** > **Dedicated Engine** to go to the dedicated WAF instance page.
  b. In the **IP Address** column, obtain the subnet IP addresses of all dedicated WAF instances. Those subnet IP addresses are back-to-source IP addresses of dedicated WAF instances.

Step 3 Run the following command to verify that the protected website can be accessed using TLS v1.2.

openssl s_client -connect *WAF back-to-source IP address* **-servername** "*Domain name of the protected website*" **-tls1_2**

If the certificate information similar to the one shown in **Figure 6-4** is displayed, the website can be accessed using TLS v1.2.

Figure 6-4 Verifying TLS v1.2



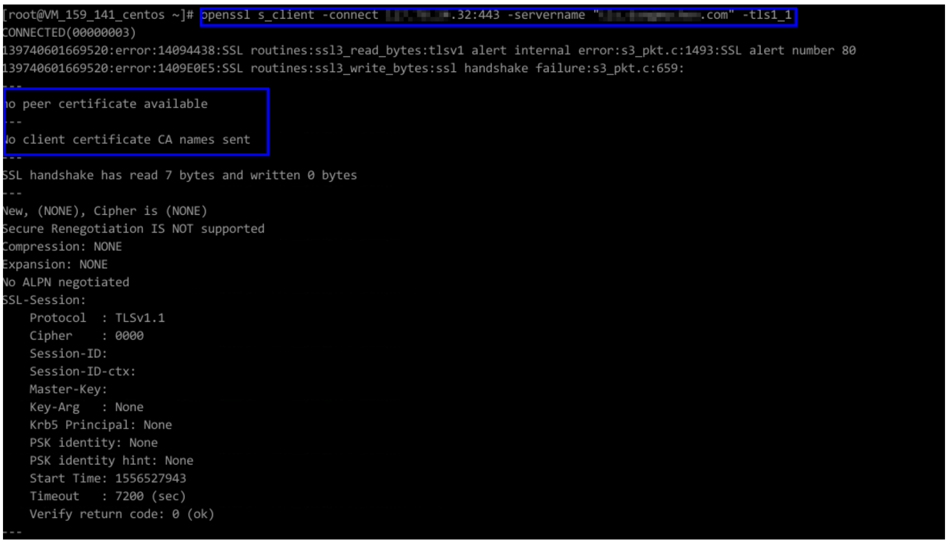
```
[root@VM_159_141_centos ~]# openssl s_client -connect [redacted]24.32:443 -servername "[redacted].com" -tls1_2
CONNECTED(00000003)
depth=0 C = XX, L = Default City, O = Default Company Ltd, CN = waf.com
verify error:num=18:self signed certificate
verify return:1
depth=0 C = XX, L = Default City, O = Default Company Ltd, CN = waf.com
verify error:num=10:certificate has expired
notAfter=Oct 27 13:05:38 2018 GMT
verify return:1
depth=0 C = XX, L = Default City, O = Default Company Ltd, CN = waf.com
notAfter=Oct 27 13:05:38 2018 GMT
verify return:1
---
Certificate chain
 0 s:/C=XX/L=Default City/O=Default Company Ltd/CN=waf.com
   i:/C=XX/L=Default City/O=Default Company Ltd/CN=waf.com
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDezCCAmOgAwIBAgIJAMJcdOLsrN3iMA0GCSqGSIb3DQEBCwUAMFQxCzAJBgNV
```

Step 4 Run the following command to verify that the protected website cannot be accessed using TLS v1.1.

openssl s_client -connect *WAF back-to-source IP address* **-servername** "*Protected domain name*" **-tls1_1**

If no certificate information is displayed, as shown in **Figure 6-5**, WAF has blocked the access that used TLS v1.1.

Figure 6-5 Verifying TLS v1.1



```
[root@VM_159_141_centos ~]# openssl s_client -connect [redacted].32:443 -servername "[redacted].com" -tls1_1
CONNECTED(00000003)
139740601669520:error:14094438:SSL routines:ssl3_read_bytes:tlsv1 alert internal error:s3_pkt.c:1493:SSL alert number 80
139740601669520:error:1409E0E5:SSL routines:ssl3_write_bytes:ssl handshake failure:s3_pkt.c:659:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 7 bytes and written 0 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.1
    Cipher    : 0000
    Session-ID:
    Session-ID-ctx:
    Master-Key:
    Key-Arg   : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
    Start Time: 1556527943
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
---
```

----End

6.3 Configuring CC Attack Protection

6.3.1 Overview

This section guides you through configuring IP address-based rate limiting and cookie-based protection rules against Challenge Collapsar (CC) attacks.

How Can We Know Whether a CC Attack Occurs?

If you find that the website processing speed decreases and the network bandwidth usage is high, your website may suffer from CC attacks. In this case, check whether the number of access logs or network connections increases significantly. If yes, your website is suffering from CC attacks. Then you can configure a protection rule to protect your website from CC attacks.

NOTE

- WAF protects application-layer traffic against DoS attacks, such as HTTP GET attacks.
- WAF does not protect your website at or below layer 4 against DDoS traffic, such as ACK Flood and UDP flood attacks. Anti-DDoS and Advanced Anti-DDoS (AAD) are recommended to defend against such attacks.

6.3.2 IP Address-based Rate Limiting

If no proxy is used between WAF and web visitors, limiting source IP addresses is an effective way to detect attacks. IP address-based rate limiting policies are recommended.

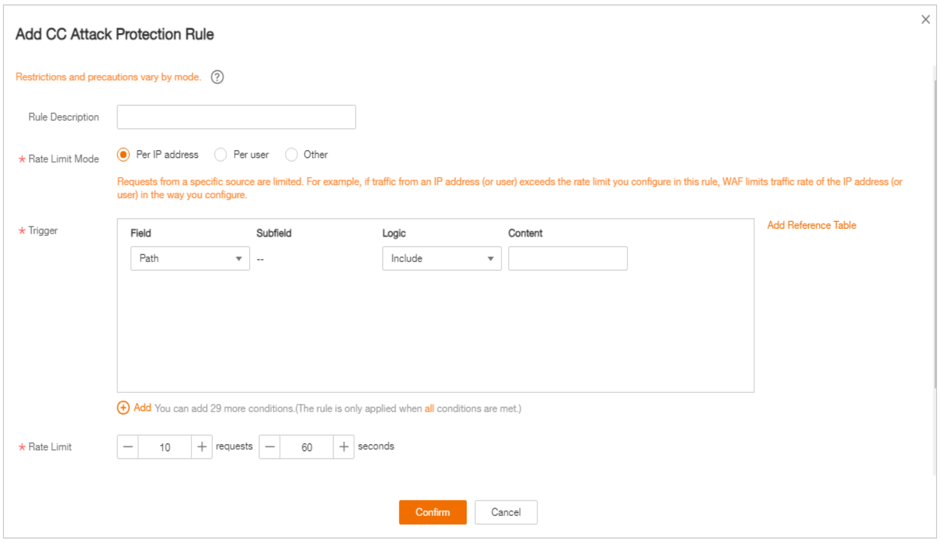
Use Cases

Attackers use several hosts to continuously send HTTP POST requests to website **www.example.com**. Those malicious requests will use up website resources, such as the website connections and bandwidth. As a result, the website fails to respond to normal requests and its competitiveness decreases sharply.

Protective Measures

1. Based on the access statistics, check whether a large number of requests were sent from a specific IP address. If yes, it is likely that the website was hit by CC attacks.
2. Log in to the management console and route website traffic to WAF.
   - Cloud mode: **Creating a Domain Name**
   - Dedicated mode: **Step 1: Add a Website to WAF (Dedicated Mode)**
3. In the **Policy** column of the row containing the target domain name, click the number of enabled protection rules. On the displayed **Policies** page, keep the **Status** toggle on (●) for **CC Attack Protection**.
4. Then, add a CC attack protection rule to limit the rate of request traffic destined for the domain name. Set **Rate Limit Mode** to **Per IP address**, **Rate Limit** based on your service features, and **Protective Action** to **Verification code** to prevent blocking legitimate users. **Figure 6-6** shows the settings.

Figure 6-6 Per IP address



Add CC Attack Protection Rule

Restrictions and precautions vary by mode.

Rule Description:

* Rate Limit Mode: ● Per IP address ○ Per user ○ Other

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.

* Trigger

Field	Subfield	Logic	Content
Path	--	Include	

Add Reference Table

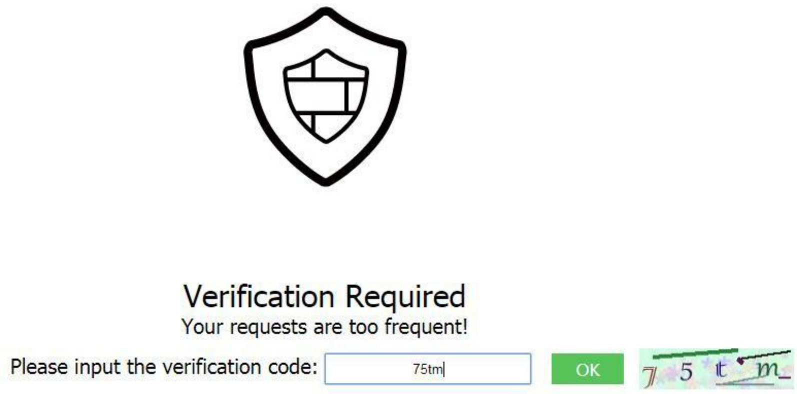
Add You can add 29 more conditions.(The rule is only applied when all conditions are met.)

* Rate Limit: 10 requests 60 seconds

   - **Rate Limit Mode**: Select **Per IP address** to distinguish a single web visitor based on IP addresses.
   - **Rate Limit**: Number of requests allowed from a website visitor in the rate limiting period. The visitor's access request is denied if the limit is reached.
   - **Protective Action**: To prevent legitimate requests from being blocked, select **Verification code**.
     - **Verification code**: A verification code is required if your website visitor's requests reaches **Rate Limit** you configured. WAF allows requests that trigger the rule as long as the website visitors complete the required verification.

- **Block**: Requests are blocked if the number of requests exceeds the configured rate limit.
- **Log only**: Requests are logged only but not blocked if the number of requests exceeds the configured rate limit.

If the number of access requests exceeds the configured rate limit, the visitors are required to enter a verification code to continue the access.



Verification Required

Your requests are too frequent!

Please input the verification code: 75tm

Go to the **Events** page and view details about attack events.

6.3.3 Cookie-based CC Attack Protection

In some cases, it may be difficult for WAF to obtain real IP addresses of website visitors. For example, if a website uses proxies that do not use the **X-Forwarded-For** HTTP header field, WAF is unable to obtain the real access IP addresses. In this situation, the cookie field should be configured to identify visitors and **All WAF instances** should be enabled for precise user-based rate limiting.

Use Cases

Attackers may control several hosts and disguise as normal visitors to continuously send HTTP POST requests to website **www.example.com** through the same IP address or many different IP addresses. As a result, the website may respond slowly or even fails to respond to normal requests as the attackers exhausted website resources like connections and bandwidth.

Protective Measures

1. Based on the access statistics, check whether a large number of requests are sent from a specific IP address. If yes, it is likely that the website is hit by CC attacks.
2. Log in to the management console and route website traffic to WAF.
   - Cloud mode: **Creating a Domain Name**
   - Dedicated mode: **Step 1: Add a Website to WAF (Dedicated Mode)**
3. In the **Policy** column of the row containing the target domain name, click the number of enabled protection rules. On the displayed **Policies** page, keep the **Status** toggle on (●) for **CC Attack Protection**.

4. Add a CC attack protection rule. Set **Rate Limit Mode** to **Per user** and enter the user identifier, which is the variable in the cookie field. To identify visitors more effectively, use **sessionid** or **token**.

   NOTE

   With a CC attack protection rule, you can configure **Protective Action** to **Block** and specify a block duration. Then, once an attack is blocked, the attacker will be blocked until the block duration expires. These settings are recommended if your applications have high security requirements.

   - **Rate Limit Mode**: Select **Per user** to distinguish a single web visitor based on cookies.
   - **User Identifier**: To identify visitors more effectively, use **sessionid** or **token**.
   - **Rate Limit**: Number of requests allowed from a web visitor in the rate limiting period. The visitor's access request is denied if the limit is reached.
   - **Protective Action**: Select **Block**. Then specify **Block Duration**. Once an attack is blocked, the attacker will be blocked until the block duration expires. These settings are recommended if your applications have high security requirements.
     - **Verification code**: A verification code is required if your website visitor's requests reaches **Rate Limit** you configured. WAF allows requests that trigger the rule as long as the website visitors complete the required verification.
     - **Block**: Requests are blocked if the number of requests exceeds the configured rate limit.
     - **Log only**: Requests are logged only but not blocked if the number of requests exceeds the configured rate limit.
   - **Block Page**: Select **Default settings** or **Custom**.

6.3.4 Restricting Malicious Requests in Promotions by Using Cookies and HWWAFSESID

This topic describes how to configure cookies and HWWAFSESID fields in CC attack protection rules to restrict malicious requests in promotions.

Application Scenarios

- **Scenario 1**: To steal extra bonus (such as goods in promotions or downloads), a malicious actor may use the same account to send requests to a website by changing IP addresses or terminals.

  Protective measures: **Using Cookies (or User IDs) to Configure a Path-based CC Attack Protection Rule**
- **Scenario 2**: To steal extra bonus (such as goods in promotions or downloads), a malicious actor may use multiple accounts to send requests to a website through the same PC by frequently changing its IP address.

  Protective measures: **Using HWWAFSESID to Configure a CC Attack Protection Rule**

Using Cookies (or User IDs) to Configure a Path-based CC Attack Protection Rule

Step 1 Log in to the management console and connect your website to WAF.

- Cloud mode: **Creating a Domain Name**
- Dedicated mode: **Step 1: Add a Website to WAF (Dedicated Mode)**

Step 2 In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.

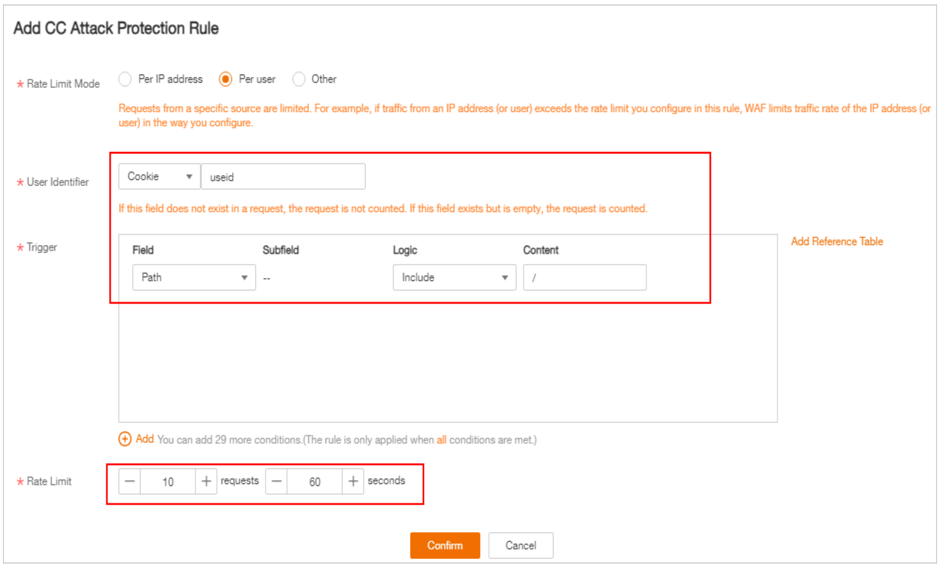
Step 3 In the **CC Attack Protection** configuration area, toggle **CC Attack Protection** on if needed. Then, click **Customize Rule**.

Step 4 In the upper left corner of the **CC Attack Protection** page, click **Add Rule**.

Step 5 Configure a CC attack protection rule using a cookie or user ID to limit traffic to the path. **Figure 6-7** shows an example.

Set the following parameters based on site requirements:

Figure 6-7 Configuring service cookies



Add CC Attack Protection Rule

* Rate Limit Mode ○ Per IP address ● Per user ○ Other

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.

* User Identifier: Cookie, useid

If this field does not exist in a request, the request is not counted. If this field exists but is empty, the request is counted.

* Trigger

Field	Subfield	Logic	Content
Path	--	Include	/

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

* Rate Limit: 10 requests 60 seconds

Step 6 Click **Confirm**.

----End

Using HWWAFSESID to Configure a CC Attack Protection Rule

Step 1 Log in to the management console and connect your website to WAF.

- Cloud mode: **Creating a Domain Name**
- Dedicated mode: **Step 1: Add a Website to WAF (Dedicated Mode)**

Step 2 In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.

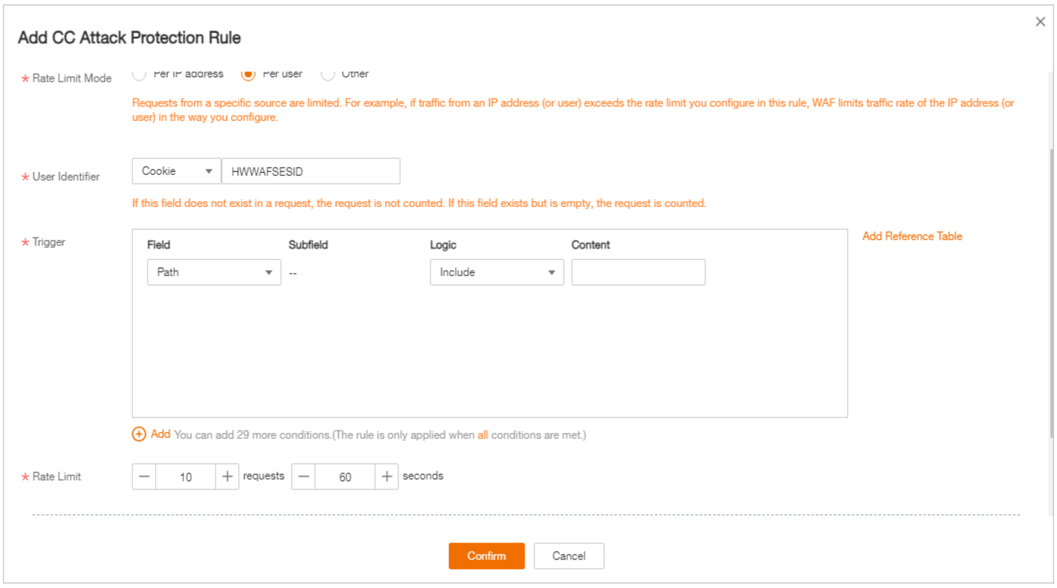
Step 3 In the **CC Attack Protection** configuration area, toggle **CC Attack Protection** on () if needed. Then, click **Customize Rule**.

Step 4 In the upper left corner of the **CC Attack Protection** page, click **Add Rule**.

Step 5 Configure a CC attack protection rule using HWWAFSESID to limit traffic to the path. For details, see **Figure 6-8**.

- **User Identifier**: Select **Cookie** and set it to **HWWAFSESID**.
- Other parameters: Set them to meet your service requirements.

Figure 6-8 HWWAFSESID-based rate limiting



Add CC Attack Protection Rule

* Rate Limit Mode: ○ Per IP address ● Per user ○ Other

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.

* User Identifier: Cookie HWWAFSESID

If this field does not exist in a request, the request is not counted. If this field exists but is empty, the request is counted.

* Trigger

Field	Subfield	Logic	Content
Path	--	Include	

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

* Rate Limit: 10 requests 60 seconds

Step 6 Click **Confirm**.

----End

6.4 Configuring Anti-Crawler Rules to Prevent Crawler Attacks

Web crawlers make network information collection and query easy, but they also introduce the following negative impacts:

- Web crawlers always consume too much server bandwidth and increase server load as they use specific policies to browser as much information of high value on a website as possible.
- Bad actors may use web crawlers to launch DoS attacks against websites. As a result, websites may fail to provide normal services due to resource exhaustion.
- Bad actors may use web crawlers to steal mission-critical data on your websites, which will damage your economic interests.

WAF provides three anti-crawler policies, bot detection by identifying User-Agent, website anti-crawler by checking browser validity, and CC attack protection by limiting the access frequency, to comprehensively mitigate crawler attacks against your websites.

Prerequisites

The domain name has been connected to WAF.

Enabling Robot Detection to Identify User-Agent

If you enable robot detection, WAF can detect and block threats such as malicious crawlers, scanners, and web shells.

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 (Dedicated)** under **Security**.

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

Step 5 In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.

Step 6 Ensure that **Basic Web Protection** is enabled (status: ●).

Step 7 Click **Advanced Settings**. On the **Protection Status** page, enable **General Check** and **Webshell Detection**.

Step 8 In the **Anti-Crawler** configuration area, toggle it on. Click **Configure Anti-Crawler**.

Step 9 On the **Feature Library** page, enable protection functions based on your business needs.

----End

If WAF detects that a malicious crawler or scanner is crawling your website, WAF immediately blocks it and logs the event. You can view the crawler protection logs on the **Events** page.

Enabling Anti-Crawler Protection to Verify Browser Validity

If you enable anti-crawler protection, WAF dynamically analyzes website service models and accurately identifies crawler behavior based on data risk control and bot identification approaches.

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 (Dedicated)** under **Security**.

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

Step 5 In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.

Step 6 In the **Anti-Crawler** configuration area, toggle on the function if needed. Then, click **Configure Anti-Crawler**.

Step 7 Configure a JavaScript-based anti-crawler rule by referring to **Table 6-4**.

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

- To protect all paths except a specified path

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

- To protect a specified path only

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

Table 6-4 Parameters of a JavaScript-based anti-crawler protection rule

Parameter	Description	Example Value
Rule Name	Name of the rule	wafjs
Path	A part of the URL, not including the domain name A URL is used to define the address of a web page. The basic URL format is as follows: Protocol name://Domain name or IP address[:Port]/[Path/.../File name]. For example, if the URL is **http://www.example.com/admin**, set **Path** to **/admin**. **NOTE** ● The path does not support regular expressions. ● The path cannot contain two or more consecutive slashes. For example, **///admin**. If you enter **///admin**, WAF converts **///** to **/**.	/admin

Parameter	Description	Example Value
Logic	Select a logical relationship from the drop-down list.	Include
Rule Description	A brief description of the rule.	None
Effective Date	Immediate	Immediate

----End

Configuring CC Attack Protection to Limit Access Frequency

A CC attack protection rule uses a specific IP address, cookie, or referer to limit the access to a specific path (URL), mitigating the impact of CC attacks on web services.

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.

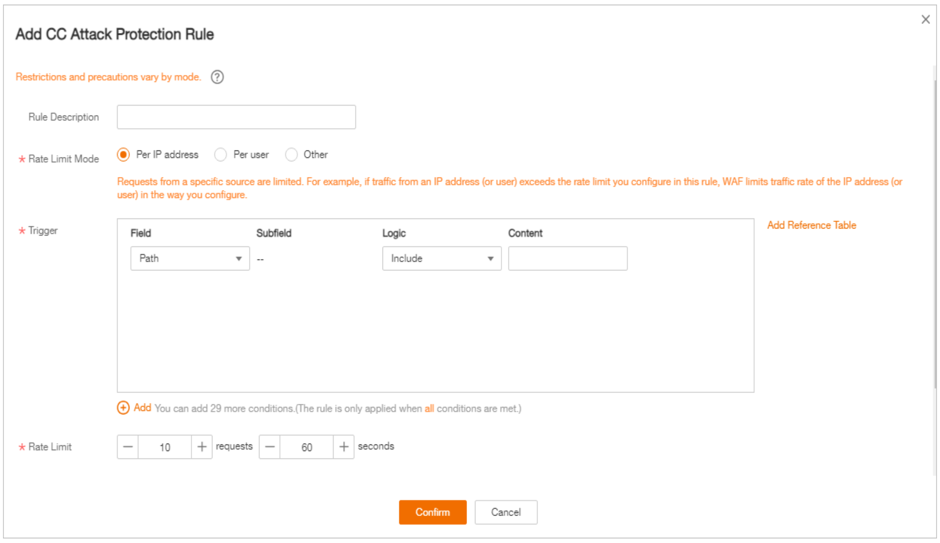
Step 3 Click ☰ in the upper left corner and choose **Web Application Firewall (Dedicated)** under **Security**.

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

Step 5 In the **Policy** column of the row containing the target domain name, click the number of enabled protection rules. On the displayed **Policies** page, keep the **Status** toggle on ( ) for **CC Attack Protection**.

Step 6 In the upper left corner above the **CC Attack Protection** rule list, click **Add Rule**. The following uses IP address-based rate limiting and human-machine verification as examples to describe how to add an IP address-based rate limiting rule, as shown in **Figure 6-9**.

Figure 6-9 Per IP address



Add CC Attack Protection Rule

Restrictions and precautions vary by mode.

Rule Description

* Rate Limit Mode: ● Per IP address ○ Per user ○ Other

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.

* Trigger

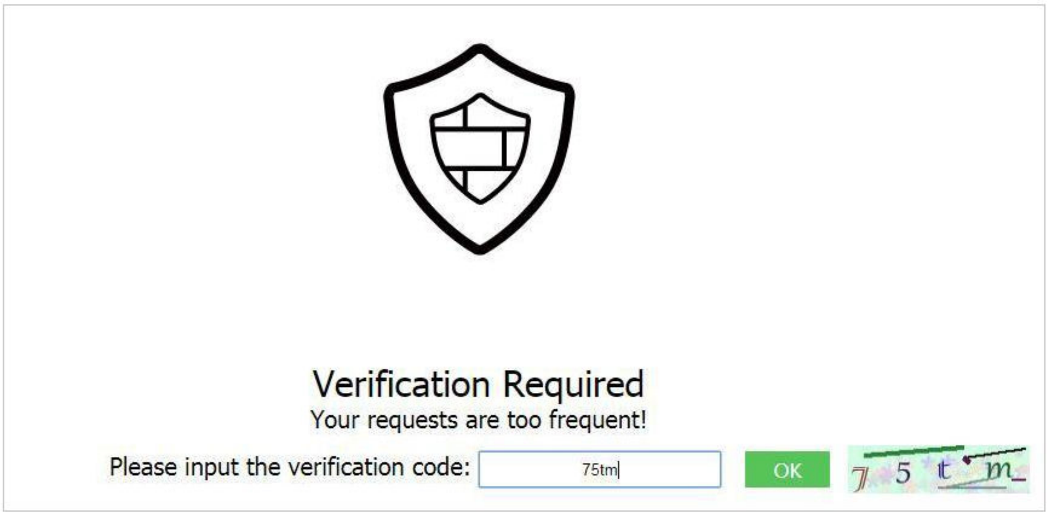
Field	Subfield	Logic	Content
Path	--	Include	

Add Reference Table

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

* Rate Limit: 10 requests 60 seconds

If the number of access requests exceeds the configured rate limit, the visitors are required to enter a verification code to continue the access.



Verification Required

Your requests are too frequent!

Please input the verification code: 75tm

----End

6.5 Configuring an Access Control Policy on an ECS or ELB to Protect Origin Servers

After you connect your website to Web Application Firewall (WAF), configure an access control policy on your origin server to allow only the WAF back-to-source IP addresses. This prevents hackers from obtaining your origin server IP addresses and then bypassing WAF to attack origin servers.

This topic walks you through how to check whether origin servers have exposure risks and how to configure access control policies. This topic applies to scenarios where your origin servers are deploying on ECSs or have been added to backend servers of an ELB load balancer.

NOTE

- WAF will forward incoming traffic destined for the origin servers no matter whether you configure access control rules on the origin servers. However, if you have no access control rules configured on origin servers, bad actors may bypass WAF and directly attack your origin servers once they obtain your origin server IP addresses.
- If you use an NAT gateway before an ECS for forwarding data, you also need to configure an inbound rule in the security group the ECS belongs to by referring to **Configuring an Inbound Rule for an ECS**. This rule allows only WAF IP addresses to access origin servers to keep them secure.

Precautions

- Before configuring an access control policy on an origin server, ensure that you have connected all domain names of websites hosted on Elastic Cloud Server (ECS) or having Elastic Load Balance (ELB) deployed to WAF.
- The following issued should be considered when you configure a security group:
  - If you enable the WAF bypassed mode for your website but do not disable security group and network ACL configurations, the origin server may become inaccessible from the Internet.
  - If new WAF back-to-source IP addresses are assigned to WAF after a security group is configured for your website, the website may respond 5xx errors frequently.

How Do I Check Whether the Origin Server IP Address Is Exposed?

You can use a Telnet tool to establish a connection over the service port of the public IP address of your origin server (or enter the IP address of your web application in the browser). Then, check whether the connection is established.

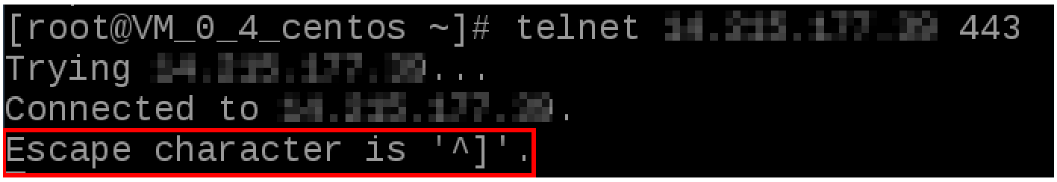
- Connection established

  The origin server has exposed to the public. Once a hacker obtains the public IP address of the origin server, the hacker can bypass WAF and directly attack the origin server.
- Connection not established

  The origin server is hidden from the public and there is no exposure risk.

For example, to check whether the origin server is exposed, check whether the origin server IP address that has been protected by WAF can be connected over port 443. If information similar to that shown in **Figure 6-10** is displayed, the connection is established and the origin server IP address is exposed.

Figure 6-10 Testing



```
[root@VM_0_4_centos ~]# telnet [redacted] 443
Trying [redacted]...
Connected to [redacted].
Escape character is '^]'.
```

Obtaining WAF Back-to-Source IP Addresses

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

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 (Dedicated)** under **Security**.

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

Step 5 In the upper right corner above the website list, click the **WAF Back-to-Source IP Addresses** link.

> NOTE
>
> WAF back-to-source IP addresses are periodically updated. Whitelist the new IP addresses in time to prevent those IP addresses from being blocked by origin servers.

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

----End

Configuring an Inbound Rule for an ECS

If your origin server is deployed on an 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.

> NOTICE
>
> Ensure that all WAF back-to-source IP addresses are whitelisted by an inbound rule of the security group configured for the ECS. Otherwise, website may become inaccessible.

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 you want. 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 ID and 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 6-5**.

Table 6-5 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 IP address is configured in a rule. Click **Add Rule** to add more rules. A maximum of 10 rules can be added.

Step 8 Click **OK**.

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

To check whether the security group rules take effect, refer to **How Do I Check Whether the Origin Server IP Address Is Exposed?** If a connection cannot be established over the service port but the website is still accessible, the configuration takes effect.

----End

Enabling ELB Access Control

If your origin server is deployed on backend servers of an 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 On the displayed details page, click the **Listeners** tab and then click **Configure Access Control** in the **Access Control** column.

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

1. Click **Create IP Address Group** and add the dedicated WAF instance IP addresses copied in **Step 6** into the IP address group.

2. Select the IP address group created in **Step 6.1** from the **IP Address Group** drop-down list.

Step 7 Click **OK**.

To check whether the security group rules take effect, refer to **How Do I Check Whether the Origin Server IP Address Is Exposed?** If a connection cannot be established over the service port but the website is still accessible, the configuration takes effect.

----End

6.6 Configuring Basic Web Protection

This topic describes best practices in basic web protection.

Application Scenarios

Web Application Firewall (WAF) keeps web services stable and secure. It examines all HTTP and HTTPS requests to detect and block the following attacks: Structured Query Language (SQL) injection, cross-site scripting (XSS), web shells, command and code injections, file inclusion, sensitive file access, third-party vulnerability exploits, Challenge Collapsar (CC) attacks, malicious crawlers, and cross-site request forgery (CSRF).

Protection Policy

Step 1 Log in to the management console.

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

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

Step 4 In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.

Step 5 In the **Basic Web Protection** configuration area, change its status if needed.

By default, **Basic Web Protection** is enabled and its mode is **Log only**.

- Protection status
  - ●: **Basic Web Protection** is enabled.
  - ○: **Basic Web Protection** is disabled.
- Protection mode: block or log only
  - **Block**: WAF blocks and logs the detected attacks.
  - **Log only**: WAF only logs the detected attacks.

Step 6 Click **Advanced Settings**. Go to the **Basic Web Protection** page.

- **Protection Level**: high, medium, and low. The default level is **Low**.

Table 6-6 Protection levels

Protection Level	Description
Low	WAF only blocks the requests with obvious attack signatures. If a large number of false alarms are reported, **Low** is recommended.
Medium	The default level is **Medium**, which meets a majority of web protection requirements.
High	WAF blocks the requests with no attack signature but have specific attack patterns. **High** is recommended if you want to block SQL injection, XSS, and command injection attacks.

- Specify the protection type.

  By default, **General Check** is enabled in WAF. You can enable other protection types to meet your business needs.

----End

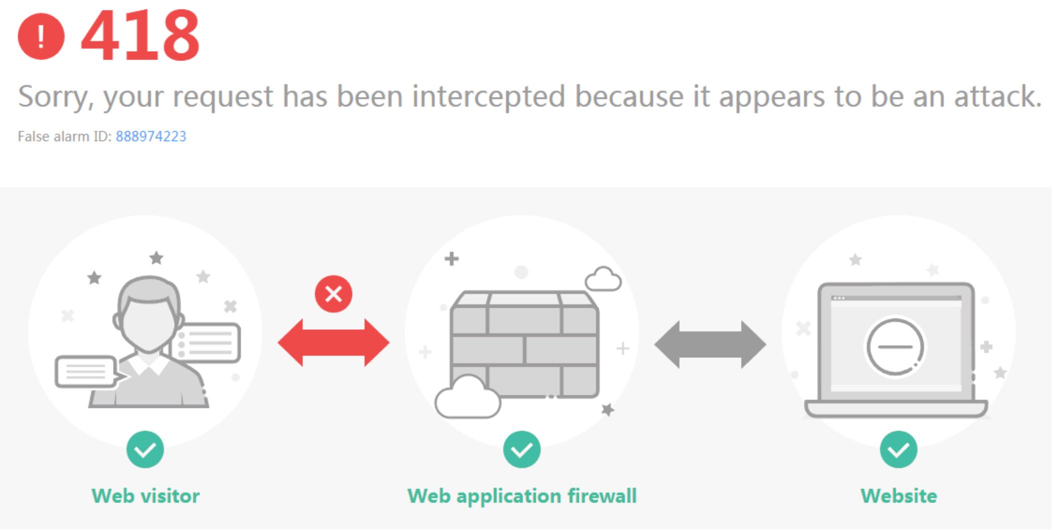
Usage Instructions

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

Protection Effect

To check whether basic web protection takes effect, enter a test domain name in the address bar of your browser and simulate an SQL injection attack. If WAF blocks the attack, the configuration works. You can view attack event logs on the **Dashboard** page.

Figure 6-11 Blocking SQL attacks



418

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

False alarm ID: 888974223

You can also view protection logs generated in yesterday, today, past 3 days, past 7 days, 30 days, or user-defined time range on the **Events** page.

6.7 Handling False Alarms to Get Improved Basic Web Protection

After you connect your website to Web Application Firewall (WAF) and enable basic web protection, WAF detects and blocks requests that match the rules you configured. If a normal request matches a basic web protection rule and is blocked by WAF, you can handle the event as false alarm. In this way, WAF will no longer block the same type of request.

Prerequisites

You can view false alarm events on the **Events** page.

Constraints

An event can only be handled as a false alarm once.

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.

Impact on the System

- The event will not be displayed on the **Events** page and you will not receive any alarm notifications about the event.
- If an event is handled as a false alarm, the rule hit will be added to the global protection whitelist (formerly false alarm masking) rule list. You can go to the **Policies** page and then switch to the **Global Protection Whitelist (Formerly False Alarm Masking)** page to manage the rule, including querying, disabling, deleting, and modifying the rule.

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.

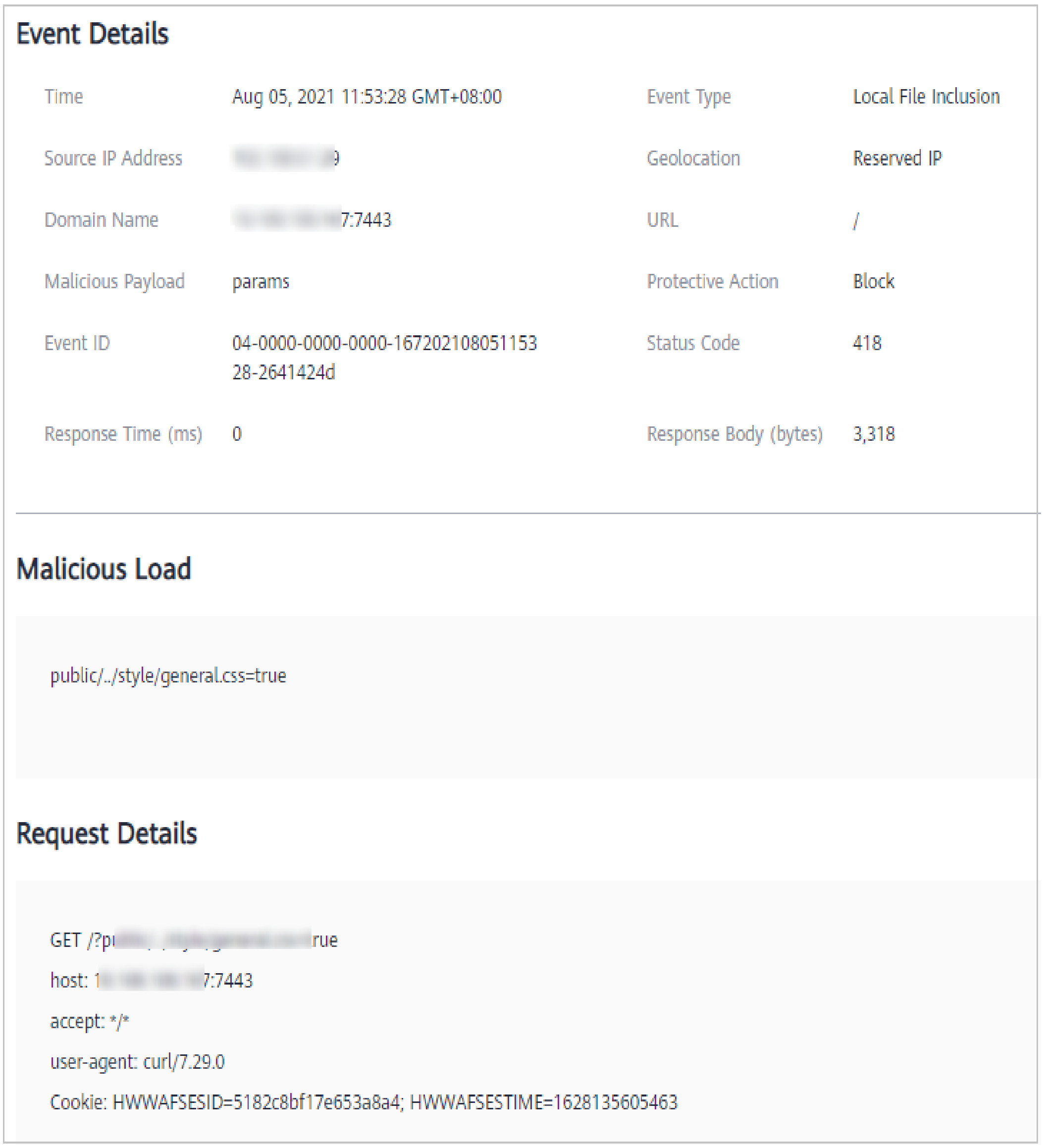
Step 3 Click ☰ in the upper left corner and choose **Web Application Firewall (Dedicated)** under **Security**.

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

Step 5 In the event list, search for false alarms by protected website, event type, source IP address, and URL.

Step 6 In the **Operation** column of an event you consider as a false alarm, click **Details**. On the displayed page, confirm that the event is a false alarm.

Figure 6-12 Event Details



Event Details

Time	Aug 05, 2021 11:53:28 GMT+08:00	Event Type	Local File Inclusion
Source IP Address	[redacted]9	Geolocation	Reserved IP
Domain Name	[redacted]7:7443	URL	/
Malicious Payload	params	Protective Action	Block
Event ID	04-0000-0000-0000-16720210805115328-2641424d	Status Code	418
Response Time (ms)	0	Response Body (bytes)	3,318

Malicious Load

```
public/../style/general.css=true
```

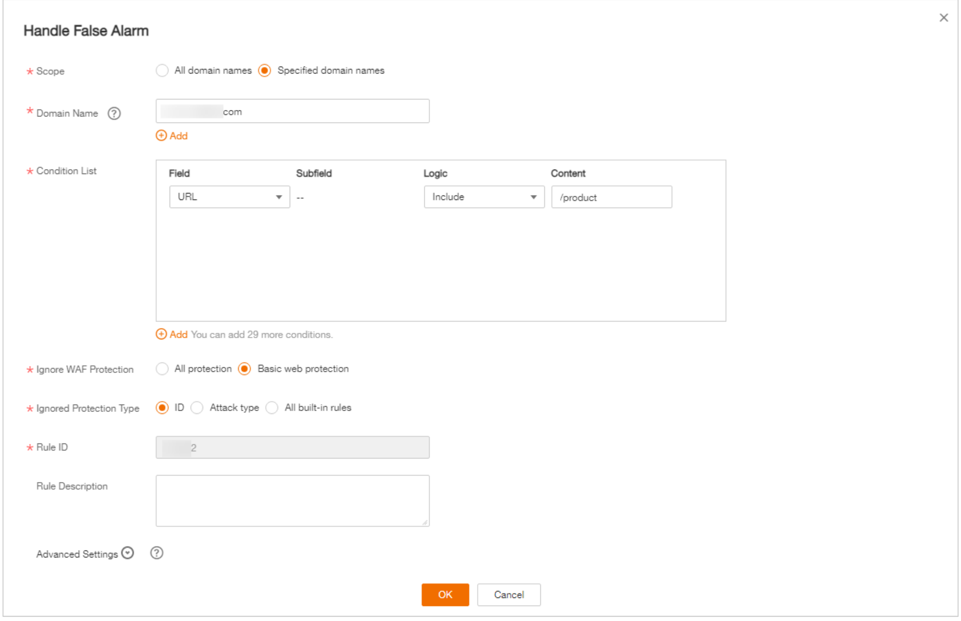
Request Details

```
GET /?p[redacted]rue
host: 1[redacted]7:7443
accept: */*
user-agent: curl/7.29.0
Cookie: HWWAFSESID=5182c8bf17e653a8a4; HWWAFSESTIME=1628135605463
```

Step 7 In the row containing the event, click **More** > **Handle as False Alarm**.

Step 8 In the displayed dialog box, add a false alarm handling policy. For details, see **Handling False Alarms**.

Figure 6-13 Add Global Protection Whitelist Rule



Handle False Alarm

* Scope ○ All domain names ● Specified domain names

* Domain Name [redacted]com

⊕ Add

* Condition List

Field	Subfield	Logic	Content
URL	--	Include	/product

⊕ Add You can add 29 more conditions.

* Ignore WAF Protection ○ All protection ● Basic web protection

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

* Rule ID [redacted]2

Rule Description

Advanced Settings

----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 event list. You can clear the cache, refresh the browser, and access the page again to verify whether the false alarm was successfully handled. If the requested page responds normally, the configuration takes effect.

Basic Web Protection Check Items

WAF basic web protection defends against common Open Web Application Security Project (OWASP) security threats. WAF uses built-in semantic analysis and regular expression engines for basic web protection to detect and block threats such as malicious scanners, IP addresses, and web shells. You can enable all protection rules in basic web protection or only the ones you want. For details, see **Table 6-7**.

Table 6-7 Protection types

Type	Description
General Check	Defends against attacks such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections. SQL injection attacks are mainly detected based on semantics. **NOTE** If you enable **General Check**, WAF checks your websites based on the built-in rules.
Webshell Detection	Protects against web shells from upload interface. **NOTE** If you enable **Webshell Detection**, WAF detects web page Trojan horses inserted through the upload interface.
Deep Inspection	Identifies and blocks evasion attacks, such as the ones that use homomorphic character obfuscation, command injection with deformed wildcard characters, UTF7, data URI scheme, and other techniques. **NOTE** If you enable **Deep Inspection**, WAF detects and defends against evasion attacks in depth.
Header Inspection	This function is disabled by default. When it is disabled, General Check will check some of the header fields, such as User-Agent, Content-type, Accept-Language, and Cookie. **NOTE** If you enable this function, WAF checks all header fields in the requests.

Basic Web Protection Levels

WAF provides three basic web protection levels, **Low**, **Medium**, and **High**. The default level is **Medium**. The lower the protection level, the higher the false negative rate and the lower the false positive rate. For details, see **Table 6-8**.

Table 6-8 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.

Protection Level	Description
Medium	The default level is **Medium**, which meets a majority of web protection requirements.
High	WAF blocks the requests with no attack signature but have specific attack patterns. **High** is recommended if you want to block SQL injection, XSS, and command injection attacks.

6.8 Verifying a Global Protection Whitelist (Formerly False Alarm Masking) Rule by Simulating Requests with Postman

After your website is connected to WAF, you can use an API test tool to send HTTP/HTTPS requests to the website and verify that WAF protection rules take effect. This topic uses Postman as an example to describe how to verify a global protection whitelist (formerly false alarm masking) rule.

Example

Assume that your workloads are deployed in the **/product** directory, and parameter ID contains scripts or rich text submitted by your customers. To ensure service running and improve WAF protection accuracy, you plan to mask false alarms generated for content submitted by the customers.

Prerequisites

- You have connected the website you want to protect to WAF.
- **Basic Web Protection** has been enabled and its **Mode** is **Block**. **General Check** has been enabled.

Procedure

Step 1 Download and install Postman.

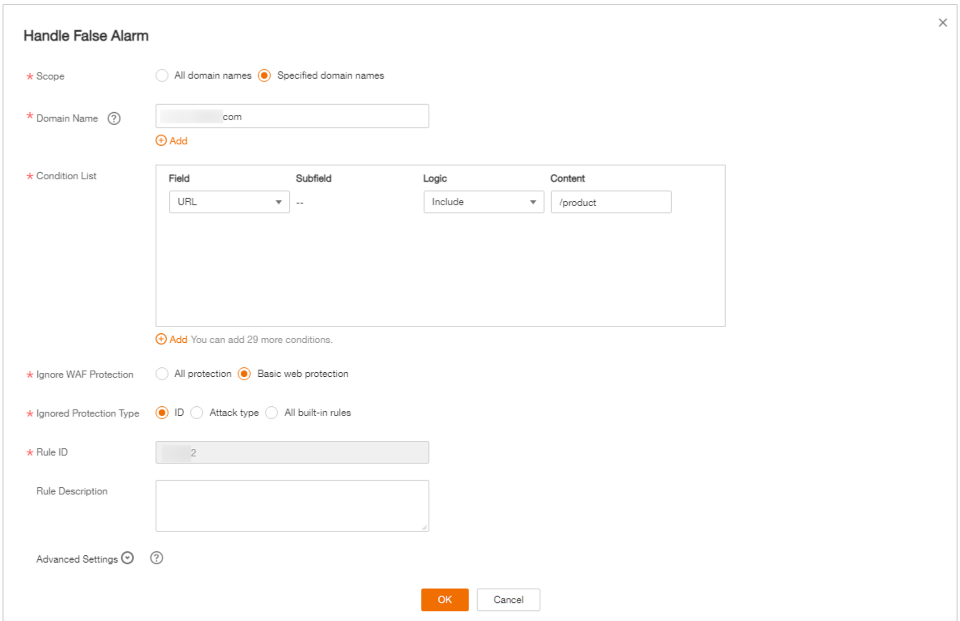
Step 2 On Postman, set the request path to **/product** and parameter ID to a common test script and send the request. The access request to the protected website is blocked.

Step 3 Handle the false alarm.

1. Log in to the management console.
2. Click 📍 in the upper left corner of the management console and select a region or project.
3. Click ☰ in the upper left corner and choose **Web Application Firewall (Dedicated)** under **Security**.

4. In the navigation pane on the left, choose **Events**.
5. On the **Events** page, WAF **010000** rule for **XSS Attack** is hit.
6. In the row containing the event, click **More** > **Handle as False Alarm**.
7. In the **Handle False Alarm** dialog box, add a global protection whitelist rule as shown in **Figure 6-14**.

Figure 6-14 Add Global Protection Whitelist Rule



Handle False Alarm

* Scope ○ All domain names ● Specified domain names

* Domain Name [redacted]com

* Condition List

Field	Subfield	Logic	Content
URL	--	Include	/product

You can add 29 more conditions.

* Ignore WAF Protection ○ All protection ● Basic web protection

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

* Rule ID [redacted]2

Rule Description

Advanced Settings

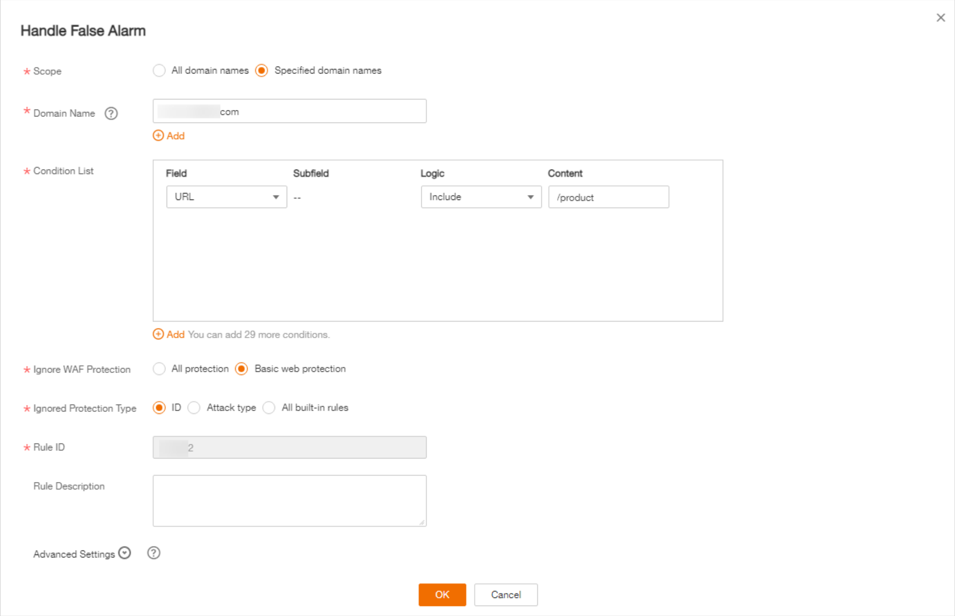
8. Click **OK**.

   It takes about 5 minutes for a protection rule to take effect.

Step 4 On Postman, set the request path to **/product** and parameter ID to a common test script and send the request again. The access request to the protected website is blocked again.

Step 5 Handle the false alarms that hit the **110053 XSS attack** rule by referring to **Step 3**.

Figure 6-15 Add Global Protection Whitelist Rule



Handle False Alarm

* Scope ○ All domain names ● Specified domain names

* Domain Name [redacted].com

Add

* Condition List

Field	Subfield	Logic	Content
URL	--	Include	/product

Add You can add 29 more conditions.

* Ignore WAF Protection ○ All protection ● Basic web protection

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

* Rule ID [redacted]2

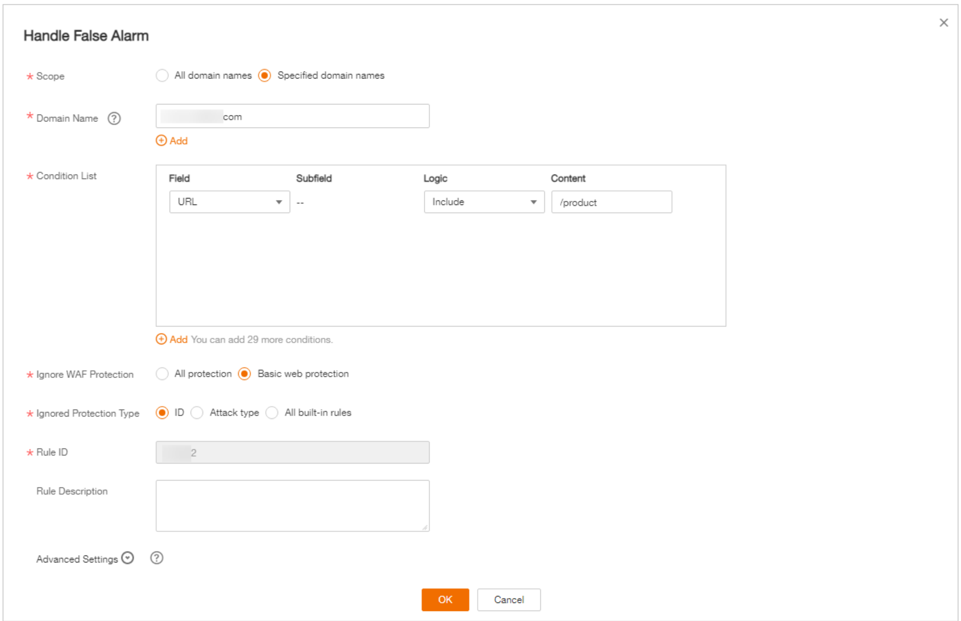
Rule Description

Advanced Settings

Step 6 On Postman, set the request path to **/product** and parameter ID to a common test script and send the request third time. The access request to the protected website is still blocked.

Step 7 Handle the false alarm that hits the **110060** rule for **XSS attack** by referring to **Step 3**.

Figure 6-16 Add Global Protection Whitelist Rule



Handle False Alarm

* Scope ○ All domain names ● Specified domain names

* Domain Name [redacted].com

Add

* Condition List

Field	Subfield	Logic	Content
URL	--	Include	/product

Add You can add 29 more conditions.

* Ignore WAF Protection ○ All protection ● Basic web protection

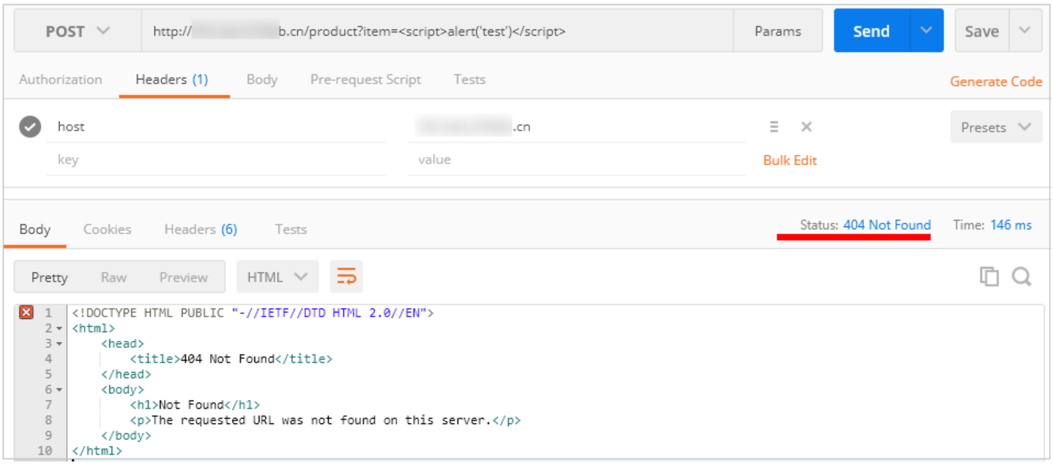
* Ignored Protection Type ● ID ○ Attack type ○ All built-in rules

* Rule ID [redacted]2

Rule Description

Advanced Settings

Step 8 On Postman, set the request path to **/product** and the parameter ID to a common test script and send the request forth time. In this case, the access request to the protected website is not blocked. All global protection whitelist rules have taken effect.



POST http://[redacted]b.cn/product?item=<script>alert('test')</script>

host: [redacted].cn

Status: 404 Not Found Time: 146 ms

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
    <head>
        <title>404 Not Found</title>
    </head>
    <body>
        <h1>Not Found</h1>
        <p>The requested URL was not found on this server.</p>
    </body>
</html>
```

Go to the **Event** page, no new XSS attack event is displayed.

Step 9 Simulate an attack on Postman to verify that the configured global protection whitelist (formerly false alarm masking) rules do not stop WAF from blocking XSS attacks against other parameters.

1. On Postman, set the request path to **/product** and parameter **item** to a common test script and send the request. The access request to the protected website is blocked.

2. On the **Events** page, view the XSS attack against parameter **item**.

Step 10 Simulate an attack on Postman to verify that the configured global protection whitelist (formerly false alarm masking) rules do not stop WAF from blocking XSS attacks against other paths.

1. On Postman, set the request path to **/order** and parameter ID to a common test script and send the request. The access request to the protected website is blocked.

2. On the **Events** page, view the event generated for blocked XSS attack against **/order** (**URL**) and parameter ID.

----End

6.9 WAF Cloud Mode Access Configuration

6.9.1 Preparations

To enable WAF protection, you need to add domain names of your web services to WAF and route website traffic to WAF. Before you start, get familiar with what you want to protect with WAF.

Website Service Review

Sort out all website services you want to protect with WAF. This helps you learn about status quo and specific data for making right decisions in configuring protection policies.

Table 6-9 Website services

Item	Description
Website and Service Information	
Daily peak traffic of website/web application services, including the bandwidth (in Mbit/s) and QPS	Use it as the basis for selecting the service bandwidth and QPS specifications. **NOTE** If your website traffic peak exceeds the maximum QPS specifications you are using, WAF will stop checking the traffic and directly forward it to the origin server. There is no protection for your website or applications.
Major user group (for example, major area that the requests originate from)	Determine the attack source and then set geolocation access control rules to block users from these areas.
Whether the service is a C/S architecture	If yes, check whether there is an app client, Windows client, Linux client, code callback, or any other client.
Location where the origin server is deployed	Decide which region to buy.
Operating system (Linux or Windows) and web service middleware (Apache, Nginx, or IIS) of the origin server	Check whether access control is enabled for the origin server. If yes, whitelist WAF back-to-source IP addresses.
Domain protocol	Check whether WAF supports the communication protocol used by your site. **NOTE** WAF can protect your website only when **Client Protocol** and **Server Protocol** are configured based on the real situation of your website. ● **Client Protocol**: the protocol used by a client (for example, a browser) to access your website. You can select **HTTP** or **HTTPS**. ● **Server Protocol**: the protocol used by WAF to forward requests from the client (such as a browser) to the origin server. You can select **HTTP** or **HTTPS**.
Service port	Check whether your service ports are within the port range supported by WAF. ● Standard ports – Port 80: default port when the client protocol is set to HTTP – Port 443: default port when the client protocol is set to HTTPS ● Non-standard ports Ports other than ports 80 and 443

Item	Description
Whether TLS v1.0 or weak encryption suite is supported	Check whether WAF supports the encryption suite used by your site.
Whether advanced anti-DDoS, CDN, or other proxy services are deployed in front of WAF.	Check whether a proxy is used and whether domain name is resolved to a correct address.
Whether the client supports Server Name Indication (for HTTPS services)	If your domain name supports HTTPS, the client and server must support Server Name Indication (SNI).
Service interaction	Understand the service interaction process and service processing logic to facilitate subsequent configuration of protection policies.
Active users	Determine the severity of an attack event to take a low-risk measure to respond it.
Services and Attacks	
Service types and features (such as games, cards, websites, or apps)	Help analyze the attack signatures.
Inbound traffic range and connection status of a single user or a single IP address	Help determine whether a rate limiting policy can be configured per IP address.
User group attribute	For example, individual users, Internet cafe users, or proxy users
Whether your website experienced large-volumetric attacks, the attack type, and maximum peak traffic	Determine whether a DDoS protection service is required and determine the DDoS protection specifications based on the peak attack traffic.
Whether your website experienced CC attacks and the maximum peak QPS in a CC attack	Configure the protection policies based on attack signatures.
Whether the pressure test has been performed	Evaluate the request processing performance of the origin server to determine whether service anomaly occurs due to attacks.

Prerequisites

- The domain name information, such as the IP address and port for the origin server, has been added to WAF in **Cloud** mode.
- An administrator account is available for you to change DNS records for WAF to take effect.

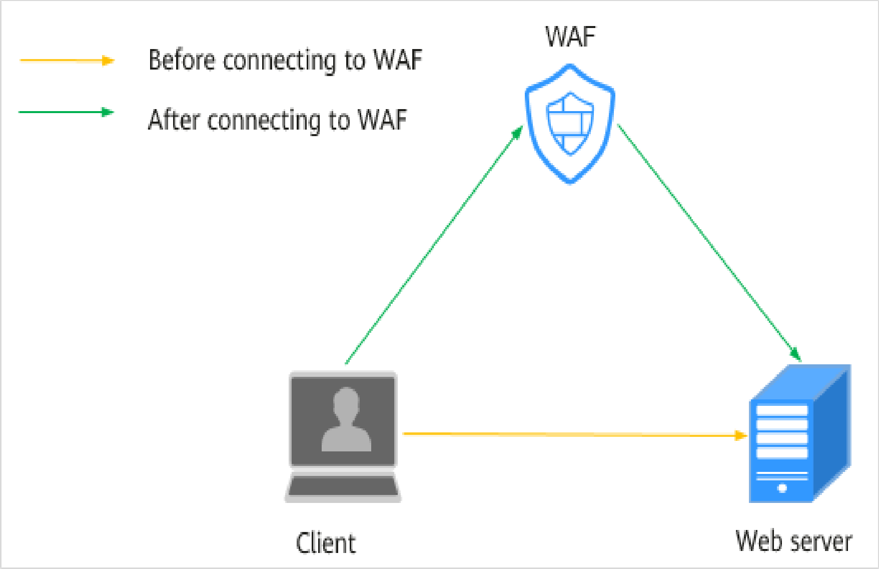
- The pressure test has been performed.
- The IP addresses of trusted clients have been whitelisted if your website has trusted clients (such as certain monitoring systems, APIs invoked by internal IP addresses or IP address ranges, and program clients).

6.9.2 Connecting a Domain Name to WAF for Websites with no Proxy Used

If your website is not added to WAF, DNS resolves your domain name to the IP address of the origin server. If your website is added to WAF, DNS resolves your domain name to the CNAME of WAF. In this way, the traffic passes through WAF. WAF inspects every traffic coming from the client and filters out malicious traffic. This section describes how to change DNS settings for WAF to take effect.

Schematic Diagram

Figure 6-17 No proxy used



Prerequisites

- Website domain names are available.
- The account to update the DNS configuration is available.
- (Optional) You have whitelisted WAF back-to-source IP addresses. If other security software is used on the origin server, whitelist the WAF back-to-source IP addresses to prevent normal traffic from being blocked. For details, see **Configuring an Access Control Policy on an ECS or ELB to Protect Origin Servers**.
- (Optional) You have tested WAF before changing DNS settings. This can prevent service interruption due to incorrect configurations. For details, see **Testing WAF**.

Scenario

- If the **Type** of the domain name host record added on DNS is **CNAME - Map one domain to another**, complete the configuration based on the instructions in **CNAME Access**.

CNAME Access

If the **Type** of the domain name host record added on DNS is **CNAME - Map one domain to another**, add the domain name to WAF by following the steps below.

The following describes how to configure CNAME records on some common DNS platforms. The following configuration is for reference only.

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 (Dedicated)** under **Security**.
3. In the navigation pane on the left, choose **Website Settings**.
4. In the **Domain Name** column, click the website domain name to go to the basic information page.
5. In the **CNAME** row, click ⧉ to copy the CNAME value.

Step 2 Change the DNS settings.

1. Log in to the management console of the DNS provider.
2. Go to the domain resolution record page.
3. In the displayed **Modify Record Set** dialog box, change the record.
   - **Name**: Domain name configured in WAF
   - **Type**: Select **CNAME - Map one domain to another**.
   - **Line**: **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 copied CNAME value from WAF.
   - Keep other settings unchanged.

NOTE

About modifying the resolution record:

- The CNAME record must be unique for the same host record. The existing CNAME record must be changed to the 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 another record, such as the A record, MX record, or TXT record. If the record type cannot be 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.

Step 3 (Optional) Ping the IP address of your domain name to check whether the new DNS settings take effect.

NOTE

It takes some time for the new DNS settings to take effect. If ping fails, wait for 5 minutes and ping again.

----End

6.10 Upgrading a Dedicated WAF Instance

You can upgrade your dedicated WAF instances on the WAF console to obtain the latest protection performance. To ensure business availability during the upgrade, upgrade your dedicated WAF instances by following the procedure below.

NOTICE

If your workloads have high reliability requirements, at least two dedicated WAF instances should be deployed in dual-active or multi-active architecture. A single dedicated WAF instance may cause single points of failure (SPOFs) once the ECS hosting it becomes faulty.

Prerequisites

You have connected the website to a dedicated WAF instance.

Upgrading a Single Dedicated WAF Instance

If you have deployed only one dedicated WAF instance for your workloads, perform the following operations:

Step 1 **Apply for a dedicated WAF instance**.

- The new dedicated WAF instance is of the latest version. So its **Upgrade** button is grayed out.
- The VPC, subnet, security group, and other settings of the new instance must be the same as those of the original one. In this way, the new instance automatically synchronizes all WAF protection configurations of the original instance.

Step 2 Run the curl command on any ECS in the VPC the original dedicated WAF instance locates to check whether the workloads are normal.

- HTTP workloads

  curl http://*IP-address-of-the-dedicated-WAF-instance* **:***Service-port* **-H "host:***Service-domain-name***" -H "User-Agent: Test"**

- HTTPS workloads

  curl https://*IP-address-of-the-dedicated-WAF-instance* **:***Service-port* **-H "host:***Service-domain-name***" -H "User-Agent: Test"**

Check whether the service is normal. If the service is normal, go to **Step 3**. If the service is abnormal, fix the issue by referring to **Why Is My Domain Name or IP**

Address Inaccessible? and **How Do I Troubleshoot 500/502/504 Errors?**. After the fault is rectified, go to **Step 3**.

NOTE

To run a curl command, your ECS must meet the following requirements:

- The network communication is normal.
- A curl command line tool has been installed. If you are using a Windows ECS, manually install a **curl** command line tool on it. If you are a using a non-Windows ECS, no such action is required as the curl tool is installed automatically along with the operating system.

Step 3 Add the new dedicated WAF instance to the backend server group of the ELB load balancer you are using.

The following uses a shared load balancer to show how to add an instance to a backend server group.

1. Click ☰ in the upper left corner and choose **Web Application Firewall (Dedicated)** under **Security**.
2. In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.
3. Locate the row containing the WAF instance. In the **Operation** column, click **More** > **Add to ELB**.
4. In the **Add to ELB** dialog box, specify **ELB (Load Balancer)**, **ELB Listener**, and **Backend Server Group** you configure for the original dedicated instance.
5. Click **Confirm**. Then, configure service port for the WAF instance. In this example, configure **Backend Port** to the one we configured for the original dedicated instance.

Step 4 On the ELB console, set the weight of the original dedicated instance to **0**.

Requests are not forwarded to a backend server if its weight is set to 0.

Step 5 Delete the original dedicated WAF instance during off-peak hours.

View the monitored metrics on Cloud Eye for the dedicated WAF instance, if there are less than five new connections, the traffic to the instance has decreased. For details, see **Viewing Metrics of a Dedicated WAF Instance**.

1. In the navigation pane on the left on the WAF console, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.
2. In the row of the instance, click **More** > **Delete** in the **Operation** column.
3. Click **Confirm**.

   Resources on deleted instance are released and cannot be restored.

----End

Upgrading Multiple Dedicated WAF Instances

If you have deployed multiple dedicated WAF instances for your workloads, perform the following steps to upgrade them:

Step 1 On the ELB console, obtain the weight of a dedicated instance and then change the weight to **0**.

Requests are not forwarded to a backend server if its weight is set to 0.

Step 2 Upgrade the dedicated WAF instance during off-peak hours.

View the monitored metrics on Cloud Eye for the dedicated WAF instance, if there are less than five new connections, the traffic to the instance has decreased. For details, see **Viewing Metrics of a Dedicated WAF Instance**.

1. In the navigation pane on the left on the WAF console, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.
2. In the row containing the desired instance, click **Upgrade** in the **Operation** column.
3. Confirm the upgrade conditions and click **Confirm**.

   It takes about 5 minutes for the upgrade to complete.

Step 3 Run the curl command on any ECS in the VPC the dedicated WAF instance locates to check whether the workloads are normal.

- HTTP workloads

  curl http://*IP-address-of-the-dedicated-WAF-instance* **:***Service-port* **-H "host:***Service-domain-name***" -H "User-Agent: Test"**
- HTTPS workloads

  curl https://*IP-address-of-the-dedicated-WAF-instance* **:***Service-port* **-H "host:***Service-domain-name***" -H "User-Agent: Test"**

Check whether the service is normal. If the service is normal, go to **Step 4**. If the service is abnormal, fix the issue by referring to **Why Is My Domain Name or IP Address Inaccessible?** and **How Do I Troubleshoot 500/502/504 Errors?**. After the fault is rectified, go to **Step 4**.

NOTE

To run a curl command, your ECS must meet the following requirements:

- The network communication is normal.
- A curl command line tool has been installed. If you are using a Windows ECS, manually install a **curl** command line tool on it. If you are a using a non-Windows ECS, no such action is required as the curl tool is installed automatically along with the operating system.

Step 4 On the ELB console, change the weight of the dedicated instance from **0** to the one you obtain in **Step 1**.

Step 5 Upgrade other dedicated WAF instances one by one by referring to **Step 1** to **Step 4**.

----End

6.11 Obtaining Real Client IP Addresses

A client IP address refers to an IP address of a visitor (or the device a visitor uses to initiate the request). Sometimes, a web application needs to require the client

IP address. For example, a voting system needs to obtain the client IP addresses to ensure that each client casts only once.

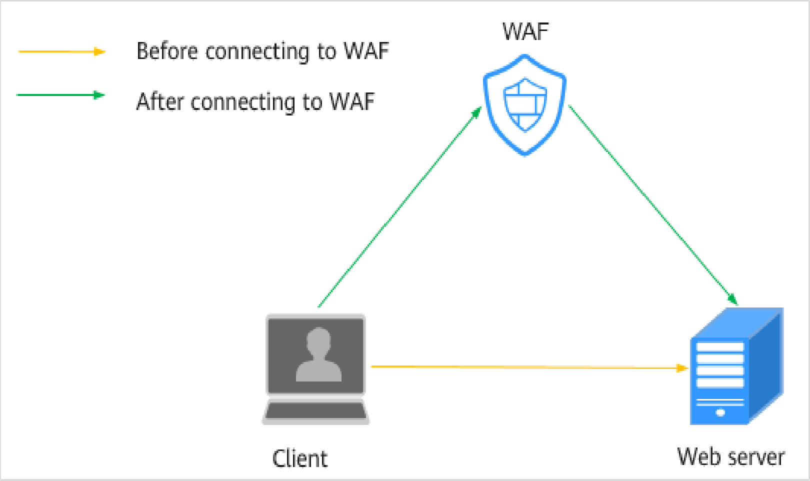
After your website is connected to WAF, WAF works as a reverse proxy between the client and the server. The real IP address of the server is hidden, and only the IP addresses of WAF are visible to web visitors. In this case, you can directly obtain the real IP address of the client through WAF or configure the website server to obtain the real IP address of the client.

The following describes how to obtain the client IP address from WAF and how to configure different types of web application servers, including Tomcat, Apache, Nginx, IIS 6, and IIS 7, to obtain the client IP address.

Background

Generally, a browser request does not directly reach the web server. Proxy servers, such as CDN, WAF, and advanced anti-DDoS, may be deployed between the browser and the origin server. Using WAF as an example, see **Figure 6-18**.

Figure 6-18 WAF deployment diagram



NOTE

- 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.

In this case, the access request may be forwarded by multiple layers of security or acceleration proxies before reaching the origin server. So, how does the server obtain the real IP address of the client that initiates the request?

When forwarding HTTP requests to the downstream server, the transparent proxy server adds an **X-Forwarded-For** field to the HTTP header to identify the client IP address in the format of **X-Forwarded-For: client IP address, proxy 1-IP address, proxy 2-IP address, proxy 3-IP address, ……..->….**

Then, you can obtain the client IP address from the **X-Forwarded-For** field, the first IP address in which is the client IP address.

Constraints

- Ensure that **Proxy Configured** is configured correctly when you add the website to the WAF instance, or WAF cannot obtain the real IP address of your website visitors.

  To ensure that WAF obtains real client IP addresses and takes protective actions configured in protection policies, if your website has layer-7 proxy server such as CDN and cloud acceleration products deployed in front of WAF, select **Yes** for **Proxy Configured**. In other cases, select **No** for **Proxy Configured**.
- In normal cases, the first IP address in the **X-Forwarded-For** field is the real IP address of the client. If the length of an IPv6 address exceeds the length limit of the **X-Forwarded-For** field, the IP address cannot be read. In NAT64, the load balancer uses IPv4 listeners, which cannot read IPv6 addresses.

Obtaining the Client IP Address from WAF

After a website is connected to WAF, WAF is deployed between the client and server as a reverse proxy to protect the website.

The following describes how WAF uses the X-Forwarded-For and X-Real-IP variables to obtain the real IP address of a client:

- Using the **X-Forwarded-For** field to obtain the client IP address

  The client IP address is placed in the **X-Forwarded-For** HTTP header field. The format is as follows:

  ```
  X-Forwarded-For: Client IP address,Proxy 1-IP address,Proxy 2-IP address,...
  ```

  NOTE

  The first IP address included in the **X-Forwarded-For** field is the client IP address.

  The methods to obtain the **X-Forwarded-For** field by invoking the SDK interface in different programming languages are as follows:

  - **ASP**
    ```
    Request.ServerVariables("HTTP_X_FORWARDED_FOR")
    ```
  - **ASP.NET(C#)**
    ```
    Request.ServerVariables["HTTP_X_FORWARDED_FOR"]
    ```
  - **PHP**
    ```
    $_SERVER["HTTP_X_FORWARDED_FOR"]
    ```
  - **JSP**
    ```
    request.getHeader("HTTP_X_FORWARDED_FOR")
    ```
- Using the **X-Real-IP** field to obtain the client IP address (modifications caused by reverse proxies is considered)

  The methods to obtain the **X-Real-IP** field by invoking the SDK interface in different programming languages are as follows:

  - **ASP**
    ```
    Request.ServerVariables("HTTP_X_REAL_IP")
    ```
  - **ASP.NET(C#)**
    ```
    Request.ServerVariables["HTTP_X_REAL_IP"]
    ```
  - **PHP**
    ```
    $_SERVER["HTTP_X_REAL_IP"]
    ```

- **JSP**

  ```
  request.getHeader("HTTP_X_REAL_IP")
  ```

How Does Tomcat Obtain the Client IP Address from Access Logs?

If Tomcat is deployed on your origin server, you can enable the X-Forwarded-For function of Tomcat to obtain the client IP address.

Step 1 Open the **server.xml** file in the **tomcat/conf/** directory. Partial information about the AccessLogValue logging function is as follows:

```
<Host name="localhost"  appBase="webapps" unpackWARs="true" autoDeploy="true">
       <Valve className="org.apache.catalina.values.AccessLogValue" directory="logs"
              prefix="localhost_access_log." suffix=".txt"
              pattern="%h %l %u %t "%r" %s %b" />
```

Step 2 Add **%{X-Forwarded-For}i** to **pattern**. Part of the modified **server.xml** file is as follows:

```
<Host name="localhost"  appBase="webapps" unpackWARs="true" autoDeploy="true">
       <Valve className="org.apache.catalina.valves.AccessLogValue" directory="logs"
              prefix="localhost_access_log." suffix=".txt"
              pattern="%{X-Forwarded-For}i %h %l %u %t "%r" %s %b" />
</Host>
```

Step 3 View the **localhost_access_log** file to obtain the client IP address from the **X-Forwarded-For** field.

----End

How Does Apache Obtain the Client IP Address from Access Logs?

If Apache HTTP Server 2.4 or later is deployed on your origin server, you can use the **mod_remoteip.so** file under **remoteip_module** in the Apache installation package to obtain the real client IP address.

- CentOS 7.6

  a. Add the following content to the **httpd.conf** file:

  ```
  LoadModule remoteip_module modules/mod_remoteip.so ##Load the mod_remoteip.so module.
  RemoteIPHeader X-Forwarded-For ## Set RemoteIPHeader.
  RemoteIPInternalProxy WAF IP address range##Set the WAF back-to-source IP address range.
  ```

  > **NOTE**
  >
  > - File **/etc/httpd/conf.modules.d/00-base.conf:46** has been added to the **mod_remoteip.so** module.
  > - Use spaces to separate multiple back-to-source IP address ranges.

  b. Replace **%h** with **%a** in the log format file.

  ```
  LogFormat "%a %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
  LogFormat "%a %l %u %t \"%r\" %>s %b" common
  ```

  c. Restart the Apache service to make the configuration take effect.

- Ubuntu 20.04.2

  a. Add the following content to the **apache2.conf** file:

  ```
  ln -s ../mods-available/remoteip.load /etc/apache2/mods-enabled/remoteip.load  ##Load the
  mod_remoteip.so module.
  RemoteIPHeader X-Forwarded-For   ## Set RemoteIPHeader.
  RemoteIPInternalProxy WAF IP address range##Set the WAF back-to-source IP address range.
  ```

NOTE

- You can also add the following content to load the **mod_remoteip.so** module:

  LoadModule remoteip_module /usr/lib/apache2/modules/mod_remoteip.so
- Use spaces to separate multiple back-to-source IP address ranges.

b. Replace **%h** with **%a** in the log format file.

```
LogFormat "%a %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%a %l %u %t \"%r\" %>s %b" common
```

c. Restart the Apache service to make the configuration take effect.

If Apache 2.2 or earlier is deployed on your origin server, to obtain the real client IP address, you can run commands to install third-party module **mod_rpaf** of Apache and modify the **http.conf** file

Step 1 Run the following commands to install third-party module **mod_rpaf** for Apache:

```
wget https://github.com/gnif/mod_rpaf/archive/v0.6.0.tar.gz
tar xvfz mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/usr/local/apache/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
```

Step 2 Open the **httpd.conf** configuration file and modify the file content as follows:

```
LoadModule rpaf_module   modules/mod_rpaf-2.0.so ##Load module mod_rpaf.
<IfModule mod_rpaf.c>
RPAFenable On
RPAFsethostname On
RPAFproxy_ips 127.0.0.1 <Reverse proxy IP address>
RPAFheader X-Forwarded-For
</IfModule>
```

Step 3 Define the log format.

```
LogFormat "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" common
```

Step 4 Enable customized logs.

```
CustomLog"[Apache server directory]/logs/$access.log"common
```

Step 5 Restart the Apache server for the configuration to take effect.

```
/[Apache server directory]/httpd/bin/apachectl restart
```

Step 6 View the **access.log** file to obtain the client IP address from the **X-Forwarded-For** field.

----End

How Does Nginx Obtain the Client IP Address from Access Logs?

If an Nginx reverse proxy is deployed on your origin server, you can configure location information on the Nginx reverse proxy so that the backend web server can use similar functions to obtain the client IP address

Step 1 Configure the following information in the corresponding location of the Nginx reverse proxy to obtain the information about the client IP address:

```
Location ^ /<uri> {
    proxy_pass  ....;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
}
```

Step 2 The backend web server obtains the real IP address of your website visitors by defining the Nginx log parameter **$http_x_forwarded_for**.

Example

```
log_format main ' "<$http_Cdn_Src_IP>" "{$http_x_real_ip}" "[$http_x_forwarded_for]" "$remote_addr"
' '$http_user_agent - $remote_user [$time_local] "$request" '   ' $status $body_bytes_sent "$http_referer" ';
```

----End

How Does IIS 6 Obtain the Client IP Address from Access Logs?

If you have deployed an IIS 6 server on your origin server, you can install the **F5XForwardedFor.dll** plug-in and obtain the client IP address from the access logs recorded by the IIS 6 server.

Step 1 Download the F5XForwardedFor module.

Step 2 Copy the **F5XForwardedFor.dll** file in the **x86\Release** or **x64\Release** directory to a specified directory (for example, **C:\ISAPIFilters**) based on the operating system version of your server. Ensure that the IIS process has the read permission for the directory.

Step 3 Open the IIS manager, right-click the website that is currently open, and choose **Attribute** from the shortcut menu. The **Attribute** page is displayed.

Step 4 On the **Attribute** page, switch to **ISAPI filter** and click **Add**. In the dialog box that is displayed, configure the following information:

- **Filter Name**: Set this parameter to **F5XForwardedFor**.
- **Executable file**: Set this parameter to the full path of **F5XForwardedFor.dll**, for example, **C:\ISAPIFilters\F5XForwardedFor.dll**.

Step 5 Click **OK** to restart the IIS 6 server.

Step 6 View the access logs recorded by the IIS 6 server (the default log path is **C:\WINDOWS\system32\LogFiles\**, and the IIS log file name extension is **.log**). You can obtain client IP address from the **X-Forwarded-For** field.

----End

How Does IIS 7 Obtain the Client IP Address from Access Logs?

If you have deployed an IIS 7 server on your origin server, you can install the **F5XForwardedFor.dll** module and obtain the client IP address from the access logs recorded by the IIS 7 server.

Step 1 Download the F5XForwardedFor module.

Step 2 Copy the **F5XFFHttpModule.dll** and **F5XFFHttpModule.ini** files in the **x86\Release** or **x64\Release** directory to a specified directory (for example, **C:\x_forwarded_for\x86** or **C:\x_forwarded_for\x64**) based on the operating system version of your server. Ensure that the IIS process has the read permission for the directory.

Step 3 On the server home page, double-click **Modules** to go to the **Modules** page.

Step 4 Click **Configure Native Module**. In the dialog box displayed, click **Register**.

Step 5 In the displayed dialog box, register the downloaded DLL file according to the operating system, and then click **OK**.

- x86 operating system: registration module **x_forwarded_for_x86**

  - **Name**: **x_forwarded_for_x86**
  - **Path**: **C:\x_forwarded_for\x86\F5XFFHttpModule.dll**
- x64: Register the module **x_forwarded_for_x64**.
  - **Name**: **x_forwarded_for_x64**
  - **Path**: **C:\x_forwarded_for\x64\F5XFFHttpModule.dll**

Step 6 After the registration is complete, select the newly registered module (**x_forwarded_for_x86** or **x_forwarded_for_x64**) and click **OK**.

Step 7 In **ISAPI and CGI restriction**, add the registered DLL files by operating system and change **Restriction** to **Permitting**.

- x86 operating system:
  - **ISAPI or CGI path**: **C:\x_forwarded_for\x86\F5XFFHttpModule.dll**
  - **Description**: **x86**
- x64 operating system:
  - **ISAPI or CGI path**: **C:\x_forwarded_for\x64\F5XFFHttpModule.dll**
  - **Description**: **x64**

Step 8 Restart the IIS 7 server and wait for the configuration to take effect.

Step 9 View the access logs recorded by the IIS 7 server (the default log path is **C:\WINDOWS\system32\LogFiles\**, and the IIS log file name extension is **.log**). You can obtain the client IP address from the **X-Forwarded-For** field.

----End

6.12 Using LTS to Quickly Query and Analyze WAF Access Logs

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.

This practice uses the access log stream **lts-waf-access** of log group **lts-waf** as an example to describe how to use LTS to quickly query and analyze logs.

Prerequisites

- You have connected the website you want to protect to WAF.
- You have **Enabling LTS for WAF Logging**.

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** > **Log Tank Service**.

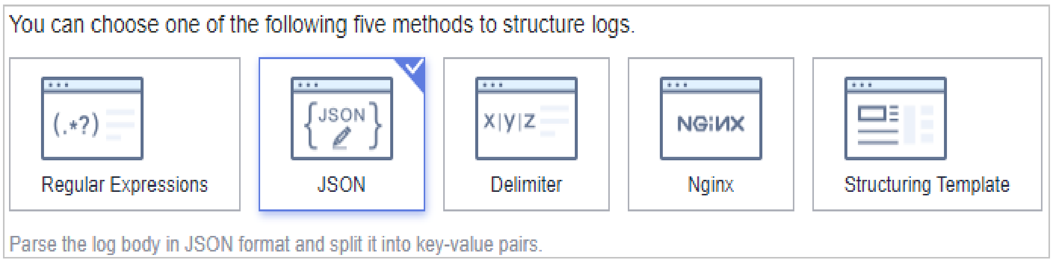
Step 4 In the **Log Group Name** column, click the name of the target log group (for example, **lts-waf**) to go the log stream page.

Step 5 In the **Log Stream Name** column, click the name of the log stream used for WAF access logs (for example, **lts-waf-access**). Then, select the **Log Stream** tab.

Step 6 On the log stream details page, click ⚙ in the upper right corner. On the page displayed, click the **Cloud Structured Parsing** tab.

Step 7 Select **JSON** as the log structure, as shown in **Figure 6-19**.

Figure 6-19 JSON



You can choose one of the following five methods to structure logs.

Parse the log body in JSON format and split it into key-value pairs.

Step 8 In the **Step 1 Select a sample log event.** area, click **Select from existing log events**. In the displayed **Select Log Event** dialog box, select a log and click **OK**.

Step 9 In the **Step 2 Extract fields** area, click **Intelligent Extraction** and enable quick analysis for the log field you want to analyze (for example, **remote_ip**).

remote_ip: IP address of a client from which the request originates.

Step 10 Click **Save**. Then, LTS will start a quick analysis and do statistics for logs collected in a certain period.

Step 11 In the navigation pane, choose **Visualization**. On the right pane, select a log query time range, enter an SQL statement in the search box, and click **Query** to query the specified log.

You can enter either of the following SQL statements in the search box to query logs of a specified IP address:

select * where remote_ip = 'xx.xx.xx.xx' or **select * where remote_ip like 'xx.xx.xx%'**

----End

6.13 Using LTS to Analyze How WAF Blocks Spring Core RCE Vulnerability in Real Time

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

This topic walks you through on how to enable the LTS quick analysis for WAF attack logs and use the Spring rule ID to quickly query and analyze the logs of the blocked Spring Core RCE vulnerabilities.

Prerequisites

- You have connected the website you want to protect to WAF.
- You have **Enabling LTS for WAF Logging**.
- You have obtained the Spring rule ID.

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** > **Log Tank Service**.

Step 4 In the log group list, expand the WAF log group and choose log stream **attack**.

Step 5 On the log stream details page, click ⚙ in the upper right corner. On the page displayed, click the **Cloud Structured Parsing** tab.

Step 6 Select **JSON** for log structuring. Then, click **Select from existing events** and select a log in the dialog box displayed on the right.

Step 7 Click **Intelligent Extraction** to find the fields you want to analyze quickly. Enable these fields in the **Quick Analysis** column. After this, you can collect and analyze periodic logs.

Step 8 Find the **category** field, click ✎ in the **Alias** column, change the field name, and click ✓ to save the settings.

NOTE

There is already a built-in **category** field in the system so you need to change the alias name of the **category** field, or your settings cannot be saved.

Step 9 In the lower right corner of the list, click **Save**. LTS quickly analyzes and collects statistics on logs in the specified period.

Step 10 In the navigation pane on the left, choose **Visualization**. Enter the following command and click **Query** to view the logs of the blocked Spring core RCE vulnerability.

select rule, hit_data where rule IN('XX','XX','XX','XX',)

----End

6.14 Using LTS to Configure Block Alarms for WAF Rules

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

This topic walks you through how to enable LTS quick analysis for WAF attack logs and configure alarm rules to analyze WAF attack logs and generate alarms. In this way, you can gain insight into the protection status of your workloads in WAF in real time and make informed decisions.

Prerequisites

- You have connected the website you want to protect to WAF.
- You have enabled WAF attack log stream in LTS.
- You have enabled Simple Message Notification (SMN).

Quickly Analyzing Rule Block Logs

Step 1 Log in to the management console.

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

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

Step 4 In the log group list, expand the WAF log group and choose log stream **attack**.

Step 5 On the log stream details page, click ⚙ in the upper right corner. On the page displayed, click the **Cloud Structured Parsing** tab.

Step 6 Select **JSON** for log structuring. Then, click **Select from existing events** and select a log in the dialog box displayed on the right.

Step 7 Click **Intelligent Extraction** to find the fields you want to analyze quickly. Enable these fields in the **Quick Analysis** column. After this, you can collect and analyze periodic logs.

Step 8 Find the **category** field, click ✎ in the **Alias** column, change the field name, and click ✓ to save the settings.

NOTE

There is already a built-in **category** field in the system so you need to change the alias name of the **category** field, or your settings cannot be saved.

Step 9 In the lower right corner of the list, click **Save**. LTS quickly analyzes and collects statistics on logs in the specified period.

Step 10 In the navigation pane, choose **Visualization**. On the right pane, select a log query time range, enter an SQL statement in the search box, and click **Query**.

You can group logs by rule and URI. Enter the following SQL statement in the search box to query logs of a specified rule:

select rule, uri, count(*) as cnt where action = 'block' group by rule, uri order by cnt desc

----End

Creating an Alarm Rule

Step 1 Click ☰ in the upper left corner of the page and choose **Management & Governance** > **Log Tank Service**.

Step 2 In the navigation pane on the left, choose **Alarms** > **Alarm Rules**.

Step 3 Click **Create**. In the dialog box displayed on the right, specify related parameters. **Table 6-10** describes the parameters.

Table 6-10 Parameter description

Parameter	Description	Example Value
Rule Name	Name of the custom rule	WAF alarms
Statistics	Select **By SQL**.	By SQL
Charts	Click **Configure from Scratch**. ● Specify **Log Group Name** and **Log Stream Name**. ● **Query Time Range**: Time range for log statistics ● **Query Statement**: Enter the SQL statement configured in **Step 10**, for example, **select rule,uri,count(*) as cnt where action='block' group by rule,uri order by cnt desc**.	None
Query Frequency	Frequency which triggers alarms Generally, a fixed custom interval of 5 minutes is selected.	Custom interval 5 minutes
Conditional Expression	Alarm threshold	cnt>5
Alarm Severity	Select an alarm severity based on the blocking emergency of the rule. The options are **critical**, **major**, **minor**, and **info**.	Major
Send Notification	Select **Yes**.	Yes
SMN Topic	Select a topic from the drop-down list or create a topic. For details about topics and subscriptions, see the *Simple Message Notification User Guide*.	None
Time Zone/ Language	You can modify the language and time zone for receiving messages.	None

Parameter	Description	Example Value
Message Templates	Select an existing template from the drop-down list box or click **Create Message Template** and create a template.	sql_template

Step 4 Confirm all parameters and click **OK**. The alarm rule is configured. When the alarm rule is triggered, you will receive an alarm email or SMS message.

----End

6.15 Combining WAF and Layer-7 Load Balancers to Protect Services over Any Ports

This topic walks you through how to combine dedicated WAF instances and layer-7 load balancers to protect your services over non-standard ports that cannot be protected with WAF alone. For ports supported by WAF, see **Ports Supported by WAF**.

Protection Scenarios

The following procedure describes how WAF and ELB together protect **www.example.com:9876**. Port 9876 is a non-standard port WAF alone cannot protect.

Prerequisites

- A proper load balancer type is available.
- 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.

Procedure

Step 1 **Apply for a dedicated WAF instance**.

Step 2 Connect www.example.com to WAF by referring to **Step 1: Add a Website to WAF (Dedicated Mode)**. Select any non-standard port as the protected port, for example, port 86, set **Server Port** to **9876**, and set **Proxy Configured** to .

Step 3 Add listeners and backend server groups to the load balancer.

1. Log in to the management console.
2. Click 📍 in the upper left corner of the management console and select a region or project.
3. Click ☰ in the upper left corner of the page and choose **Elastic Load Balance** under **Networking** to go to the **Load Balancers** page.
4. Click the name of the load balancer in the **Name** column to go to the **Basic Information** page.
5. Click the **Listeners** tab and then click **Add Listener**. On the displayed page, configure the listener. In the **Frontend Port** text box, enter the port you want to protect. In this case, enter **9876**.
6. Click **Next: Configure Request Routing Policy**.

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.

7. Click **Next: Add Backend Server** and click **Next: Confirm**.

Step 4 Add the WAF instance to the load balancer.

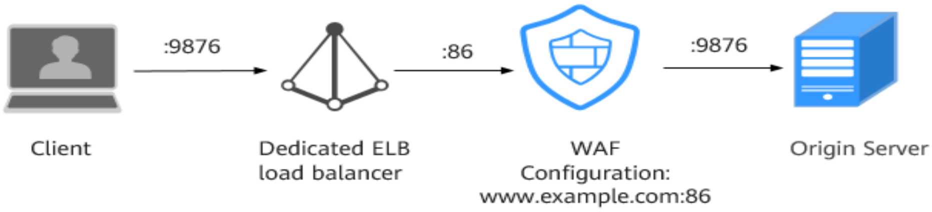
1. Log in to the management console.
2. Click 📍 in the upper left corner of the management console and select a region or project.
3. Click ☰ in the upper left corner and choose **Web Application Firewall (Dedicated)** under **Security**.
4. In the navigation pane on the left, choose **Instance Management** > **Dedicated Engine** to go to the dedicated WAF instance page.
5. Locate the row containing the WAF instance. In the **Operation** column, click **More** > **Add to ELB**.
6. In the **Add to ELB** dialog box, specify **ELB (Load Balancer)**, **ELB Listener**, and **Backend Server Group** based on **Step 3**.
7. Click **Confirm**. Then, configure service port for the WAF instance. In this example, configure **Backend Port** to **86**, which is the one we configured in **Step 2**.
8. Click **Confirm**.

Step 5 **Bind an EIP to a Load Balancer**.

Step 6 **Whitelist IP addresses of your dedicated WAF instances**.

----End

How the Combination Protects Traffic


:9876
:86
:9876
Client
Dedicated ELB load balancer
WAF Configuration: www.example.com:86
Origin Server

6.16 Combining WAF and HSS to Get Improved Web Tamper Protection

WAF examines HTTP/HTTPS requests. If an attacker attempts to tamper with web pages using attacks like SQL injection, WAF can identify and block the attacks in a timely manner, so they cannot sneak into or change anything in the OSs of your web servers.

Even if attacks bypass the first layer of protection, HSS WTP provides multi-level defenses. HSS WTP protects files in the web file directories from any unauthorized access. Only your website administrator can update the website content through the privileged process. Apart from that, HSS WTP also backs up web file directories locally and remotely. Once a file is tampered with, it can be quickly restored with backups. For dynamic web pages such as applications on web servers, HSS WTP uses Runtime Application Self-Protection (RASP) to monitor application access. It can detect tampering on dynamic data such as databases and prevent attackers from using applications to tamper with web pages in real time.

With HSS and WAF in place, you can stop worrying about web page tampering.

What Web Tampering Is and Impacts of Web Tampering

Web tampering is a type of cyberattack that exploits vulnerabilities in web applications to tamper with web application content or to insert hidden links. Web tampering attacks are often used to spread malicious information, incite unrest, and steal money.

Links to pornographic or otherwise illegal content may be inserted into normal web pages. Tampered web pages can permanently damage the brand image of your organization.

Differences Between The Web Tamper Protection Functions of HSS and WAF

Table 6-11 Differences between the web tamper protection functions of HSS and WAF

Type	HSS	WAF
Static web pages	Locks files in driver and web file directories to prevent attackers from tampering with them.	Caches static web pages on servers.

Type	HSS	WAF
Dynamic web pages	● Dynamic WTP Protects your data while Tomcat is running, detecting dynamic data tampering in databases. ● Privileged process management Allows only privileged processes to modify web pages.	Not supported
Backup and restoration	● Proactive backup and restoration If WTP detects that a file in the protection directory is tampered with, it immediately uses the backup file on the local server to restore the file. ● Remote backup and restoration If a file directory or backup directory on the local server becomes invalid, you can use the remote backup service to restore the tampered web page.	Not supported
Protection object	Web tamper prevention. This function is suitable for websites that have high protection requirements.	Websites that only require application-layer protection

Configuring a Web Tamper Protection Rule in WAF

Step 1 Log in to the management console.

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

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

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 In the **Web Tamper Protection** configuration area, change **Status** if needed and click **Customize Rule** to go to the **Web Tamper Protection** page.

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 6-12**.

Table 6-12 Rule parameters

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

Enabling HSS Web Tamper Protection

Step 1 .

Step 2 In the navigation pane, choose **Prevention** > **Web Tamper Protection**. On the **Web Tamper Protection** page, click **Add Server**.

Step 3 On the **Add Server** page, click the **Available servers** tab. Select the target server, select a quota from the drop-down list or retain the default value, and click **Add and Enable Protection**.

Step 4 View the server status on the **Web Tamper Protection** page.

The premium edition will be enabled when you enable WTP.

- Choose **Prevention** > **Web Tamper Protection**. If the **Protection Status** of the server is **Protected**, WTP has been enabled.

----End

NOTICE

- Before disabling WTP, perform a comprehensive detection on the server, handle known risks, and record operation information to prevent O&M errors and attacks on the server.
- If WTP is disabled, web applications are more likely to be tampered with. Therefore, you need to delete important data on the server, stop important services on the server, and disconnect the server from the external network in a timely manner to avoid unnecessary losses caused by attacks on the server.
- After you or disable WTP, files in the protected directory are no longer protected. You are advised to process files in the protected directory before performing these operations.
- If you find some files missing after disabling WTP, search for them in the local or remote backup path.
- The premium edition will be disabled when you disable WTP.

7 IAM Permissions Management

7.1 Creating a User Group and Granting Permissions

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 7-1**).

Prerequisites

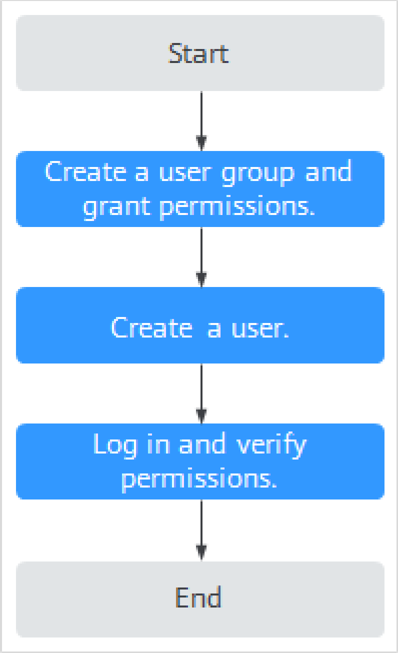
Table 7-1 System policies supported by WAF

Role/Policy Name	Description	Category	Dependencies
WAF Administrator	Administrator permissions for WAF	System-defined role	Dependent on the **Tenant Guest** and **Server Administrator** roles. ● **Tenant Guest**: A global role, which must be assigned in the global project. ● **Server Administrator**: A project-level role, which must be assigned in the same project.

Role/Policy Name	Description	Category	Dependencies
WAF FullAccess	All permissions for WAF	System-defined policy	None.
WAF ReadOnlyAccess	Read-only permissions for WAF.	System-defined policy	

Process Flow

Figure 7-1 Process for granting permissions


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

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

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

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

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

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

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

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

7.2 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"
                        ]
                }
        ]
}
```

7.3 WAF Permissions and Supported Actions

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

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
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

Permission	Action
Querying a precise protection rule	waf:preciseProtectionRule: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
Querying a protection event	waf:event:get
Querying a protected domain	waf:instance:get
Querying a protection policy	waf:policy:get
Querying quota package information	waf:bundle:get
Querying the protection event download link	waf:dumpEventLink:get
Querying configurations	waf:consoleConfig:get
Querying the back-to-source IP address segment	waf:sourceIp:get
Updating an information leakage prevention rule	waf:antiLeakageRule:put
Updating a web tamper protection rule	waf:antiTamperRule:put
Updating a CC attack protection rule	waf:ccRuleRule:put
Updating a precise protection rule	waf:preciseProtectionRule:put
Updating a global protection whitelist rule	waf:falseAlarmMaskRule:put
Updating a data masking rule	waf:privacyRule:put
Updating an IP address blacklist or whitelist rule	waf:whiteBlackIpRule:put
Updating a geolocation access control rule	waf:geoIpRule:put

Permission	Action
Updating a protected domain	waf:instance:put
Updating a protection policy	waf:policy:put
Deleting an information leakage prevention rule	waf:antiLeakageRule:delete
Deleting a web tamper protection rule	waf:antiTamperRule:delete
Deleting a CC attack protection rule	waf:ccRule:delete
Configuring a precise protection rule	waf:preciseProtectionRule:delete
Deleting a global protection whitelist rule	waf:falseAlarmMaskRule:delete
Deleting a data masking rule	waf:privacyRule:delete
Deleting a blacklist or whitelist rule	waf:whiteBlackIpRule:delete
Deleting a geolocation access control rule	waf:geoIpRule:delete
Deleting a protected domain	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
Adding a precise protection rule	waf:preciseProtectionRule: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

Permission	Action
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:preciseProtectionRule: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
Querying geolocation access control rules	waf:geoIpRule:list
Querying the protection domains	waf:instance:list
Querying protection policies	waf:policy:list

8 FAQs

8.1 About the Product

8.1.1 FAQs for Beginners

If you are a beginner for WAF, here are some useful FAQs.

Is WAF a Hardware Firewall or a Software Firewall?

WAF is a software firewall.

Does WAF Affect My Existing Workloads and Server Running?

Enabling WAF does not interrupt your existing workloads or affect the running status of your origin servers. No additional operation (such as shutdown or restart) on the origin servers is required.

Can a WAF Instance Be Deployed in the VPC?

Yes. You can deploy dedicated engine WAF instances in a VPC.

Does a Dedicated WAF Instance Support Cross-VPC Protection?

Dedicated WAF instances cannot protect origin servers in the VPCs that are different from where those WAF instances locate. To protect such origin servers, apply for dedicated WAF instances in the same VPC as that for the origin servers.

Which OSs Does WAF Support?

WAF is deployed on the cloud, which is irrelevant to an OS. Therefore, WAF supports any OS. A domain name server on any OS can be connected to WAF for protection.

Which Layers Does WAF Provide Protection At?

WAF provides protection at seven layers, namely, the physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer.

How Does WAF Block Requests?

WAF checks both the request header and body. For example, WAF detects the request body, such as form, XML, and JSON data, and blocks requests that do not comply with protection rules.

Does WAF Support File Caching?

WAF caches only static web pages that are configured with web tamper protection and sends the cached web pages that are not tampered with to web visitors.

Does WAF Cache Website Data?

WAF protects user data on the application layer. It supports cache configuration on static web pages. When a user accesses a web page, the system returns a cached page to the user and randomly checks whether the page has been tampered with.

Can I Use WAF to Check Health Status of Servers?

No. If you want to check health status of servers, the combination of ELB and WAF is recommended for your workloads. After you configure a load balancer in ELB, you can enable health checks for servers and use the EIP of the load balancer as the server IP address to establish connections between servers and WAF.

Does WAF Support Two-Way SSL Authentication?

No. You can configure a one-way SSL certificate on WAF.

NOTE

If you set **Client Protocol** to **HTTPS** when adding a website to WAF, you will be required to upload a certificate and use it for your website.

Does WAF Support Application Layer Protocol- and Content-Based Access Control?

WAF supports access control over content at the application layer. HTTP and HTTPS are both application layer protocols.

Can WAF Check the Body I Add to a POST Request?

The built-in detection of WAF checks POST data, and web shells are the files submitted in POST requests. WAF checks all data, such as forms and JSON files in POST requests based on the default protection policies.

You can configure a precise protection rule to check the body added to POST requests.

Can WAF Limit the Access Speed of a Domain Name?

No. However, you can customize a CC attack protection rule to restrict access to a specific URL on your website based on an IP address, cookie, or Referer, mitigating CC attacks.

Can WAF Block URL Requests That Contain Special Characters?

No. WAF can only detect and restrict source IP addresses.

Can WAF Block Spam and Malicious User Registrations?

WAF cannot block business-related attacks, such as spam and malicious user registrations. To prevent these attacks, configure the registration verification mechanism on your website.

WAF is designed to keep web applications stable and secure. It examines all HTTP and HTTPS requests to detect for and block suspicious network attacks, such as Structure Query Language (SQL) injections, cross-site scripting (XSS) attacks, web shell upload, command or code injections, file inclusion, unauthorized sensitive file access, third-party vulnerability exploits, Challenge Collapsar (CC) attacks, malicious crawlers, and cross-site request forgery (CSRF).

Can WAF Block Requests for Calling Other APIs from Web Pages?

If the request data for calling other APIs on the web page is included in the domain names protected by WAF, the request data passes through WAF. WAF checks the request data and blocks it if it is an attack.

If the request data for calling other APIs on the web page is not included in the domain names protected by WAF, the request data does not pass through WAF. WAF cannot block the request data.

Can WAF Limit Access Through Domain Names?

No. WAF supports the blacklist and whitelist rules to block, log only, or permit access requests from specified IP addresses or IP address segments.

You can configure blacklist and whitelist rules to block, log only, or permit access requests from the IP addresses or IP address segments corresponding to the domain names.

Does WAF Have the IPS Module?

Unlike the traditional firewalls, WAF does not have an Intrusion Prevention System (IPS). WAF supports intrusion detection of only HTTP/HTTPS requests.

Can My WAF Instances Be Automatically Scalable?

No.

Is There Any Impact on Origin Servers If I Enable HTTP/2 in WAF?

Yes. HTTP/2 is not supported between WAF and the origin server. This means if you enable HTTP/2 in WAF, WAF can process HTTP/2 requests from clients, but

WAF can only forward the requests to origin server using HTTP 1.0/1.1. In this situation, the origin server request traffic may rise as multiplexing in HTTP/2 may become invalid for origin servers.

Does WAF Affect Email Ports or Email Receiving and Sending?

WAF protects web application pages. After your website is connected to WAF, there is no impact on your email port or email sending or receiving.

What Are Concurrent Requests?

The number of concurrent requests refers to the number of requests that the system can process simultaneously. When it comes to a website, concurrent requests refer to the requests from the visitors at the same time.

Can WAF Block Requests When a Certificate Is Mounted on ELB?

If the certificate is mounted on ELB, all requests sent through WAF are encrypted. For HTTPS services, you must upload the certificate to WAF so that WAF can detect the decrypted request and determine whether to block the request.

Do I Need to Make Some Changes in WAF If the Security Group for Origin Server (Address) Is Changed?

No modifications are required in WAF, but you are required to whitelist WAF IP addresses on the origin servers.

How Is the Load Balanced When Multiple Origin Servers Are Configured in WAF?

If you have configured multiple origin server IP addresses, WAF uses the weighted round robin algorithm to distribute access requests by default. You can also customize a load balancing algorithm as required.

Does gzip on the Origin Server Affect WAF?

If gzip is enabled on the origin server, WAF may incorrectly block normal access requests from the origin server. If the blocked request is a normal access request, you can handle the event as a false alarm by referring to **Handling False Alarms**. After an event is handled as a false alarm, WAF stops blocking corresponding type of event. No such type of event will be displayed on the **Events** page and you will no longer receive alarm notifications accordingly.

Does WAF Affect Data Transmission from the Internal Network to an External Network?

No. After a website is connected to cloud WAF in CNAME access mode or to dedicated WAF instances, all website access requests are forwarded to WAF first. WAF detects and filters out malicious attack traffic, and returns normal traffic to the origin server to keep origin servers secure, stable, and available.

Can WAF Protect Multiple Domain Names That Point to the Same Origin Server?

Yes. If there are multiple domain names pointing to the same origin server, you can connect these domain names to WAF for protection.

WAF protects domain names or IP addresses. If multiple domain names use the same EIP to provide services, all these domain names must be connected to WAF.

Is the Path of a WAF Protection Rule Case-sensitive?

All paths configured for protection rules of WAF are case-sensitive.

What Is a Protection IP Address?

A protection IP address in WAF is the IP address of a website you use WAF to protect.

Does Cloud WAF Use Fixed IP Addresses for Domain Resolution?

After a domain name is added to WAF in cloud mode, WAF randomly assigns a CNAME record to the domain name for domain name resolution. This CNAME record is randomly assigned from the WAF IP address pool and is not fixed.

Will the CNAME Record Be Changed If the IP Address of the Origin Server Has Been Changed?

If you are using a cloud WAF instance, the CNAME record will not be changed when origin server IP addresses have been changed.

Do I Need to Add the Domain Name to WAF Again If the Domain Name IP Address Has Been Changed?

If the IP address of the website does not change, you do not need to reconfigure it in WAF. If the website resolves a new IP address, you need to add it in WAF again.

Do I Need to Bind an EIP to WAF?

No EIPs are required for cloud WAF instances. Dedicated WAF instances need to work with layer-7 dedicated load balancers. These load balancers need to use EIPs as service addresses.

Does WAF Support Vulnerability Detection?

WAF enables customizable anti-crawler rules to detect and block threats such as third-party security tool vulnerability attacks. If you enable the scanner item when configuring anti-crawler rules, WAF detects scanners and crawlers, such as OpenVAS and Nmap.

Does WAF Support Protocols Used in MS Exchange?

WAF supports HTTP and HTTPS for logging in to Exchange on the web, but does not support mail-related protocols such as Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3), or Internet Message Access Protocol (IMAP) used by MS Exchange.

Can WAF Defend Against XOR Injection Attacks?

Yes. WAF can defend against XOR injection attacks.

What Is the bind_ip Parameter in WAF Logs?

After your website is connected to WAF, WAF functions as a reverse proxy between the client and the origin server. WAF examines traffic to your website, filters out malicious traffic, and forwards health traffic to your origin servers. **bind_ip** indicates the WAF IP addresses used by WAF to forward healthy traffic. WAF IP addresses must be whitelisted on your origin server. For more details about how to whitelist WAF IP addresses, see **How Do I Whitelist IP Address Ranges of Cloud WAF?**

Can WAF Protect All Domain Names Mapped to My Website IP Address If I Have Connected the IP Address to WAF?

No.

In dedicated mode, the origin server IP address can be connected to WAF, and the IP address can be a private or internal IP address. WAF protects only the traffic accessed through the IP address but cannot protect the traffic to the domain name mapped to the IP address. To protect a domain name, connect the domain name to WAF.

Can WAF Protect Websites in the C/S Architecture?

In the C/S architecture, WAF can protect only websites that use the layer-7 HTTP/HTTPS protocol.

Where Can I Query the Service QPS of the Current WAF Service?

You can query the inbound bandwidth or QPS quota usage of the origin server IP address on the origin server.

Can WAF Block Data Packets in multipart/form-data Format?

Yes.

The multipart/form-data indicates that the browser uses a form to upload files. For example, if an attachment is added to an email, the attachment is usually uploaded to the server in multipart/form-data format.

8.1.2 WAF Functions

8.1.2.1 Can WAF Protect an IP Address?

A WAF instance can protect IP addresses.

Cloud Mode

In this mode, only website domain names can be added to WAF for protection.

The origin server IP address configured in WAF can only be a public IP address.

To reduce the number of public IP addresses, you can use an Elastic Load Balance (ELB) load balancer to work as a proxy of backend private IP addresses. Then, you need to set the EIP (public IP address) bound to the load balancer as the origin server IP address.

Dedicated Mode

A dedicated or load balancing WAF instance can protect websites through either domain names or IP addresses.

The origin server IP address configured in WAF can be a public IP address or internal IP address.

For details about how to add a domain name to WAF, see **How Do I Add a Domain Name/IP Address to WAF?**

8.1.2.2 What Objects Does WAF Protect?

WAF can protect websites through domain names or IP addresses.

- In cloud CNAME access mode, only website domain names can be added to WAF.

  Your origin server IP address configured in WAF must a public IP address. For example, if an Elastic Load Balance (ELB) load balancer is configured for origin servers, a cloud WAF instance can protect origin servers as long as the load balancer has a public IP address bound.
- In dedicated mode, you can add website domain names or IP addresses to WAF.

8.1.2.3 About WAF Protection

What Is a Protection IP Address?

A protection IP address in WAF is the IP address of a website you use WAF to protect.

Does Cloud WAF Use Fixed IP Addresses for Domain Resolution?

After a domain name is added to WAF in cloud mode, WAF randomly assigns a CNAME record to the domain name for domain name resolution. This CNAME record is randomly assigned from the WAF IP address pool and is not fixed.

Will the CNAME Record Be Changed If the IP Address of the Origin Server Has Been Changed?

If you are using a cloud WAF instance, the CNAME record will not be changed when origin server IP addresses have been changed.

Do I Need to Add the Domain Name to WAF Again If the Domain Name IP Address Has Been Changed?

If the IP address of the website does not change, you do not need to reconfigure it in WAF. If the website resolves a new IP address, you need to add it in WAF again.

Do I Need to Bind an EIP to WAF?

No EIPs are required for cloud WAF instances. Dedicated WAF instances need to work with layer-7 dedicated load balancers. These load balancers need to use EIPs as service addresses.

Does WAF Support Vulnerability Detection?

WAF enables customizable anti-crawler rules to detect and block threats such as third-party security tool vulnerability attacks. If you enable the scanner item when configuring anti-crawler rules, WAF detects scanners and crawlers, such as OpenVAS and Nmap.

Does WAF Support Protocols Used in MS Exchange?

WAF supports HTTP and HTTPS for logging in to Exchange on the web, but does not support mail-related protocols such as Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3), or Internet Message Access Protocol (IMAP) used by MS Exchange.

Can WAF Defend Against XOR Injection Attacks?

Yes. WAF can defend against XOR injection attacks.

What Is the bind_ip Parameter in WAF Logs?

After your website is connected to WAF, WAF functions as a reverse proxy between the client and the origin server. WAF examines traffic to your website, filters out malicious traffic, and forwards health traffic to your origin servers. **bind_ip** indicates the WAF IP addresses used by WAF to forward healthy traffic. WAF IP addresses must be whitelisted on your origin server. For more details about how to whitelist WAF IP addresses, see **How Do I Whitelist IP Address Ranges of Cloud WAF?**

Can WAF Protect All Domain Names Mapped to My Website IP Address If I Have Connected the IP Address to WAF?

No.

In dedicated mode, the origin server IP address can be connected to WAF, and the IP address can be a private or internal IP address. WAF protects only the traffic accessed through the IP address but cannot protect the traffic to the domain name mapped to the IP address. To protect a domain name, connect the domain name to WAF.

Can WAF Protect Websites in the C/S Architecture?

In the C/S architecture, WAF can protect only websites that use the layer-7 HTTP/ HTTPS protocol.

Where Can I Query the Service QPS of the Current WAF Service?

You can query the inbound bandwidth or QPS usage of the origin server IP address on the origin server.

Can WAF Block Data Packets in multipart/form-data Format?

Yes.

The multipart/form-data indicates that the browser uses a form to upload files. For example, if an attachment is added to an email, the attachment is usually uploaded to the server in multipart/form-data format.

8.1.2.4 Can I Configure Session Cookies in WAF?

No. WAF does not support session cookies.

WAF allows you to configure CC attack protection rules to limit the access frequency to a specific path (URL) in a single cookie field, accurately identify CC attacks, and effectively mitigate CC attacks. For example, if a user whose cookie ID is **name** accesses the **/admin*** page under the protected domain name for more than 10 times within 60 seconds, you can configure a CC attack protection rule to forbid the user from accessing the domain name for 600 seconds.

What Are Cookies?

Cookies are data (usually encrypted) stored on the local terminal of a user by a website to identify the user and trace sessions. Cookies are sent by a web server to a browser to record personal information of the user.

A cookie consists of a name, a value, and several optional attributes that control the cookie validity period, security, and usage scope. Cookies are classified into session cookies and persistent cookies. The details are as follows:

- Session cookie

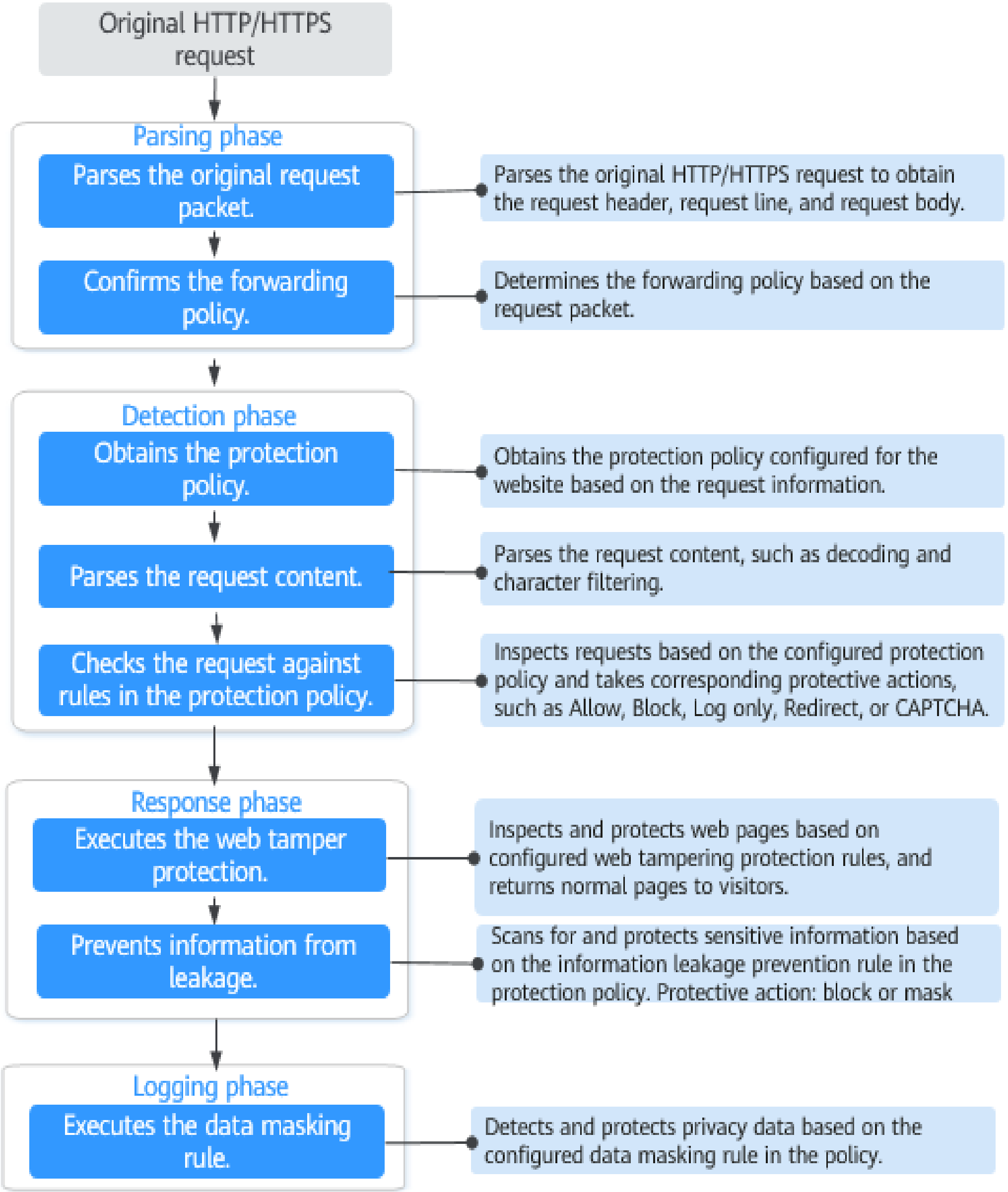
  A session cookie exists only in temporary memory while the user navigates the website. It does not have an expiration date. When the browser is closed, session cookies are deleted.
- Persistent cookie

  A persistent cookie has an expiration date and is stored in disks. Persistent cookies will be deleted after a specific length of time.

8.1.2.5 Does WAF Block Customized POST Requests?

No. WAF does not block user-defined POST requests. **Figure 8-1** shows the detection process of the WAF built-in protection rules for original HTTP/HTTPS requests.

Figure 8-1 WAF engine work process


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

8.1.2.6 What Are the Differences Between the Web Tamper Protection Functions of WAF and HSS?

The web tamper protection function of HSS monitors website directories in real time, backs up files, and restores tampered files using the backup, protecting websites from tampering. This function is helpful for governments, educational institutions, and enterprises.

WAF protects user data on the application layer. It supports cache configuration on static web pages. When a user accesses a web page, the system returns a cached page to the user and randomly checks whether the page has been tampered with.

Differences Between the Web Tamper Protection Functions of HSS and WTP

Table 8-1 describes the differences

Table 8-1 Differences between the web tamper protection functions of HSS and WTP

Item	HSS	WAF
Static web page protection	Locks files in driver and web file directories to prevent attackers from tampering with them.	Caches static web pages on servers.
Dynamic web page protection	● Dynamic WTP Protects your data while Tomcat is running, detecting dynamic data tampering in databases. ● Privileged process management Allows privileged processes to modify web pages.	No
Backup and restoration	● Active backup and restoration If WTP detects that a file in the protection directory is tampered with, it immediately uses the backup file on the local host to restore the file. ● Remote backup and restoration If a file directory or backup directory on the local server becomes invalid, you can use the remote backup service to restore the tampered web page.	No
Suitable for	Websites that have high security requirements and difficult to be manually recovered	Websites that only require application-layer protection

Purchase Suggestion

Website	Service
Common websites	WAF web tamper protection + HSS enterprise edition
Websites that require strong protection and anti-tampering capabilities	WAF web tamper protection + HSS WTP

8.1.2.7 Which Web Service Framework Protocols Does WAF Support?

WAF is deployed on the cloud.

Web Application Firewall (WAF) keeps web services stable and secure. It examines all HTTP and HTTPS requests to detect and block the following attacks: Structured Query Language (SQL) injection, cross-site scripting (XSS), web shells, command and code injections, file inclusion, sensitive file access, third-party vulnerability exploits, Challenge Collapsar (CC) attacks, malicious crawlers, and cross-site request forgery (CSRF).

WAF can examine the following requests:

- WebSocket and WebSockets (enabled by default)
  - WebSocket request inspection is enabled by default if **Client Protocol** is set to **HTTP**.
  - WebSockets request inspection is enabled by default if **Client Protocol** is set to **HTTPS**.
- HTTP/HTTPS

8.1.2.8 Can WAF Protect Websites Accessed Through HSTS or NTLM Authentication?

Yes. WAF can protect HTTP and HTTPS applications.

- If a website uses the HTTP Strict Transport Security (HSTS) policy, the client (such as a browser) is forced to use HTTPS to communicate with the website. This reduces the risk of session hijacking. Websites configured with HSTS policy use the HTTPS protocol. So, WAF can protect these websites.
- Windows New Technology LAN Manager (NTLM) is an authentication method over HTTP. NTLM uses a three-way handshake to authenticate a connection. NTLM authenticates a client (such as a browser) the same way the Windows remote login authentication does.

  WAF can protect applications that use NTLM to authenticate connection between a server and client, such as a browser.

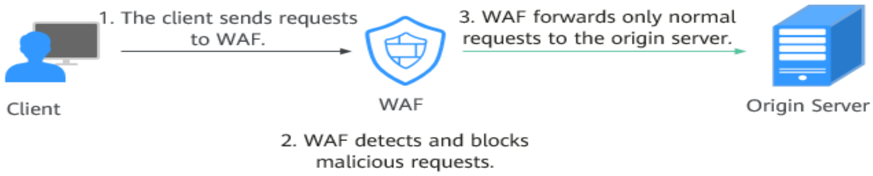
8.1.2.9 What Are the Differences Between WAF Forwarding and Nginx Forwarding?

Nginx directly forwards access requests to the origin server, while WAF detects and filters out malicious traffic and then forwards only the normal access requests to the origin server. The details are as follows:

- WAF forwarding

  After a website is connected to WAF, all access requests pass through WAF. WAF detects HTTP(S) requests to identify and block a wide range of attacks, such as SQL injection, cross-site scripting attacks, web shell uploads, command/code injection, file inclusion, sensitive file access, third-party application vulnerability attacks, CC attacks, malicious crawlers, cross-site request forgery (CSRF) attacks. Then, WAF sends normal traffic to the origin server. In this way, security, stability, and availability of your web applications are assured.

Figure 8-2 How WAF works for CNAME or dedicated access

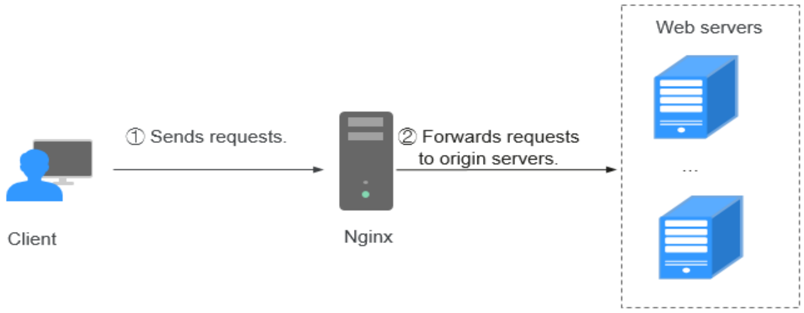

1. The client sends requests to WAF.
3. WAF forwards only normal requests to the origin server.
Client
WAF
Origin Server
2. WAF detects and blocks malicious requests.

- Nginx forwarding

  Nginx works as a reverse proxy server. After receiving the access request from the client, the reverse proxy server directly forwards the access request to the web server and returns the result obtained from the web server to the client. The reverse proxy server is installed in the website equipment room. It functions as a proxy for the web server to receive and forward access requests.

  The reverse proxy server prevents malicious attacks from the Internet to intranet servers, caches data to reduce workloads on the intranet servers, and implements access security control and load balancing.

Figure 8-3 How Nginx Works



8.1.2.10 How Does WAF Detect SQL Injection, XSS, and PHP Injection Attacks?

A Structured Query Language (SQL) injection is a common web attack. The attacker injects malicious SQL commands into database query strings to deceive the server into executing commands. By exploiting these commands, the attacker can obtain sensitive information, add users, export files, or even gain the highest permissions to the database or system.

XSS attacks exploit vulnerabilities left during web page development to inject malicious instruction code into web pages so that attackers can trick visitors into loading and executing malicious web page programs attackers fabricated. These malicious web page programs are usually JavaScript, but they can also include Java, VBScript, ActiveX, Flash, or even common HTML. After an attack succeeds, the attacker may obtain various content, including but not limited to higher permissions (for example, permissions for certain operations), private content, sessions, and cookies.

How Does WAF Detect SQL Injection Attacks?

WAF detects and matches SQL keywords, special characters, operators, and comment symbols.

- SQL keywords: union, Select, from, as, asc, desc, order by, sort, and, or, load, delete, update, execute, count, top, between, declare, distinct, distinctrow, sleep, waitfor, delay, having, sysdate, when, dba_user, case, delay, and the like
- Special characters: ',; ()
- Mathematical operators: **±**, *, **/**, **%**, and **|**
- Operators: **=**, **>**, **<**, **>=**, **<=**, **!=**, **+=**, and **-=**
- Comment symbols: – or /**/

How Does WAF Detect XSS Attacks?

WAF checks HTML script tags, event processors, script protocols, and styles to prevent malicious users from injecting malicious XSS statements through client requests.

- XSS keywords (such as **javascript**, **script**, **object**, **style**, **iframe**, **body**, **input**, **form**, **onerror**, and **alert**)
- Special characters (<, >, ', and ")
- External links (href="http://xxx/",src="http://xxx/attack.js")

NOTE

Rich text can be uploaded using multipart upload instead of body. In multipart upload, rich text is stored in forms and can be decoded even if it is encoded using Base64. Analyze your services and do not use quotation marks and angle brackets as far as possible.

How Does WAF Detect PHP Injection Attacks?

If a request contains keywords similar to "system(xx)", the keywords may cause PHP injection attacks. WAF will then block such requests.

8.1.2.11 Can WAF Defend Against the Apache Struts2 Remote Code Execution Vulnerability (CVE-2021-31805)?

Yes. WAF basic web protection rules can defend against the Apache Struts2 remote code execution vulnerability (CVE-2021-31805).

Configuration Procedure

Step 1 **Apply for a dedicated WAF instance**.

Step 2 Add the website domain name to WAF and route website traffic to WAF.

- Cloud mode: **Creating a Domain Name**
- Dedicated mode: **Step 1: Add a Website to WAF (Dedicated Mode)**

Step 3 Set the mode of Basic Web Protection to **Block**. For details, see **Configuring Basic Protection Rules to Defend Against Common Web Attacks**.

----End

8.1.3 WAF Usage

8.1.3.1 Why Does the Vulnerability Scanning Tool Report Disabled Non-standard Ports for My WAF-Protected Website?

Symptom

When a third-party vulnerability scanning tool scans the website whose domain name has been connected to WAF, the scan result shows that some standard ports (for example, 443) and non-standard ports (for example, 8000 and 8443) are vulnerable.

Possible Cause

WAF uses the same non-standard port engine for all WAF users. So, if a third-party vulnerability scanning tool performs a scan for your website, the enabled non-standard ports in WAF are reported. This means such port vulnerabilities in scan results do not affect your origin server security. WAF will safeguard your website after you point origin server IP address to WAF engine IP address through the CNAME record.

Handling Suggestions

No action is required.

8.1.3.2 How Do I Obtain the Real IP Address of a Web Visitor?

After you connect a website 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.

Generally, a proxy such as CDN, WAF, and anti-DDoS service is deployed between the client and server. Web visitors cannot directly access the server. For example, **web visitor** > **CDN/WAF/anti-DDoS** > **origin server**.

When forwarding requests to the downstream server, the transparent proxy server adds an **X-Forwarded-For** field to the HTTP header to identify the web visitor's real IP address in the format of **X-Forwarded-For: real IP address of the web visitor, proxy 1-IP address, proxy 2-IP address, proxy 3-IP address, ...->....**

Therefore, you can obtain the web visitor's real IP address from the **X-Forwarded-For** field. The first IP address in this field is the web visitor's real IP address.

8.1.3.3 What Are Local File Inclusion and Remote File Inclusion?

You can view security events such as file inclusion in WAF protection events to quickly locate attack sources or analyze attack events.

Program developers write repeatedly used functions into a single file. When such functions need to be used, the file is directly invoked. The file invoking process is called file inclusion. File inclusion vulnerabilities are classified into two categories, based on whether the file is a remotely hosted file or a local file available on the web server:

- Local file inclusion
- Remote file inclusion

A file inclusion vulnerability allows an attacker to access unauthorized or sensitive files available on the web server or to execute malicious files on the web server by using such a file. This vulnerability is mainly due to a bad input validation mechanism, wherein the user's input that is passed to the file include commands without proper validation. The impact of this vulnerability can lead to malicious code execution on the server or reveal data present in sensitive files.

8.1.3.4 What Is the Difference Between QPS and the Number of Requests?

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.

Queries Per Second (QPS) is the number of requests a server can handle per second.

NOTE

QPS is used to measure the number of queries, or requests, per second.

For details about QPS on the **Dashboard** page, see **Table 8-2**.

Table 8-2 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.
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.

8.1.3.5 Does WAF Support Custom Authorization Policies?

WAF supports custom authorization policies. 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.

8.1.3.6 Can I Add a Domain Name or IP Address to WAF Under Different Accounts?

If your domain name has been added to WAF in cloud mode, it cannot be added again. Therefore, a domain name cannot be added to WAF under different accounts.

However, in dedicated mode, you can add domain names or IP addresses to WAF under different accounts.

NOTICE

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

8.1.3.7 How Do I Configure My Server to Allow Only Requests from WAF?

You can configure an access control rule on the origin server to allow only WAF back-to-source IP addresses to access the origin server. This prevents hackers from bypassing WAF to attack the origin server through origin server IP addresses, ensuring the security, stability, and availability of the origin server.

8.1.3.8 Why Do Cookies Contain the HWWAFSESID or HWWAFSESTIME field?

HWWAFSESID indicates the session ID, and **HWWAFSESTIME** indicates the session timestamp. These two fields are used to mark the request, for example, they can be used to count the requests for a CC protection rule.

After a domain name or IP address is connected to WAF, WAF inserts fields such as **HWWAFSESID** (session ID) and **HWWAFSESTIME** (session timestamp) into the cookie of your customer request. These fields are used by WAF to implement some functions, such as counting requests and monitoring request duration. If these fields are not inserted, some rules may be unable to work, such as CC attack protection rules with verification code configured, known attack source rules, and dynamic anti-crawler rules.

8.1.3.9 Can I Switch Between the WAF Cloud Mode and Dedicated Mode?

Direct switchover is not supported, but you can complete required configurations then use the WAF mode you want. When adding a domain name or IP address to WAF, WAF offers cloud mode and dedicated mode to meet different needs. Once you select a WAF mode and connect the domain name to WAF, the WAF mode cannot be changed directly.

If you want to use another WAF mode for the domain name, deploy your services in the WAF mode you want first. Then, remove the domain name or IP address from the current WAF instance. After that, you can add the website in the mode you want to the WAF instance. For example, you are using a cloud WAF instance to protect domain name www.example.com. If you want to use a dedicated WAF instance to protect www.example.com, ensure that your current services are supported by WAF dedicated mode. Then, you can apply for a dedicated WAF instance and remove protected domain name www.example.com from the cloud WAF instance. Then, add www.example.com to the dedicated WAF instance.

8.1.3.10 How Do I Configure WAF If a Reverse Proxy Server Is Deployed for My Website?

In this case, the reverse proxy server will not be affected after the website is connected to WAF. In cloud CNAME access mode, WAF works as a reverse proxy between the client and your website server. The real IP addresses of your website server are hidden from the visitors, and only the IP addresses of WAF are visible to them.

8.1.3.11 How Does WAF Forward Access Requests When Both a Wildcard Domain Name and a Single Domain Name Are Connected to WAF?

WAF preferentially forwards access requests to the single domain name. If the single domain name cannot be identified, access requests will be forwarded to the wildcard domain name.

For example, if you connect single domain name a.example.com and wildcard domain name *.example.com to WAF, WAF preferentially forwards access requests to single domain name a.example.com.

If you are configuring a wildcard domain name, pay attention to the following:

- 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.

8.1.4 Enterprise Project

8.1.4.1 Can I Use WAF Across Enterprise Projects?

That depends on which mode your WAF instance is deployed. The details are as follows:

- Cloud mode

  You can use your cloud WAF for different enterprise projects.
- Dedicated mode

  If you dedicated WAF instance can communicate with the VPC where your origin servers belong, the instance can be used across enterprise projects.

Otherwise, the WAF dedicated you apply for in a certain enterprise project cannot be used for other enterprise projects.

NOTE

For the dedicated WAF instance that cannot communicate with the VPC where your origin servers belong, if you still want to use it for other enterprise projects, go to the **Enterprise Project Management** page and move the WAF instance to the target enterprise project. Then, you can use or upgrade the dedicated WAF instance in the enterprise project.

8.2 Service Request/Specification

8.2.1 WAF Instance Specifications Change

8.2.1.1 What Are the Impacts When QPS Exceeds the Allowed Peak Rate?

If the QPS specifications you select cannot handle the daily peak traffic of protected website or application services, WAF stops protecting your website. This will cause traffic limiting, random packet loss, automatic bypassing of WAF. As a result, your services may become unavailable, frozen, or respond very slowly for a certain period of time.

The following describes the QPS specifications supported by dedicated WAF instances in different deployments.

- Normal peak requests for a single instance:
  - 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
- Peak rate of CC attack protection
  - Specifications: WI-500. Referenced performance:

    Maximum QPS: 20,000
  - Specifications: WI-100. Referenced performance:

    Maximum QPS: 4,000

8.2.2 About Service Requests

8.2.2.1 Where Can I Query the Service QPS of the Current WAF Service?

You can query the inbound bandwidth or QPS usage of the origin server IP address on the origin server.

8.2.2.2 Where Can I View the Inbound and Outbound Bandwidths of a Protected Website?

On the **Dashboard** page, you can view the bandwidth usage about the protected website or instance. The procedure is as follows:

Step 1 Log in to the management console.

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

Step 3 In the website or instance drop-down list, select the website or instance you want to check and select a time range (yesterday, today, past 3 days, past 7 days, or past 30 days).

Step 4 In the **Security Event Statistics** area, select the **Bytes Sent/Received** tab and view the inbound and outbound bandwidths.

----End

8.3 About Billing

8.3.1 How Is WAF Billed?

The WAF cloud mode supports pay-per-use billing. You are billed for domain names you added to WAF and requests handled by WAF.

Dedicated WAF instances can be billed on a monthly or pay-per-use basis.

- Pay-per-use billing: You are billed for the required duration by the second, which starts when the instance is created and ends when the instance is deleted.
- Monthly billing: You will be billed based on how many instances you apply for and what instance specifications you select.

For more details, see **About Billing**.

8.3.2 Can I Use WAF for Free?

No. WAF is a paid service. Cloud WAF is billed on a pay-per-use (postpaid) basis. In this method, the billing starts when WAF is enabled and used and ends when the pay-per-use billing is disabled. You are billed based on the number of added domain names and the number of handled requests. Dedicated WAF instances are billed on a pay-per-use or monthly basis.

For more details, see **About Billing**.

8.4 Website Access Configuration

8.4.1 Domain Name and Port Configuration

8.4.1.1 How Do I Add a Domain Name/IP Address to WAF?

After you connect a domain name or IP address of the website you want to protect to WAF, 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.

WAF offers the cloud and dedicated modes to protect websites. You can add either domain names or IP addresses to WAF. Before you start, get familiar with the following differences:

- Cloud mode: protects your web applications on or off the cloud through domain names.
- Dedicated mode: protects your web applications on the cloud through domain names or IP addresses.

NOTICE

- You can enter a multi-level single domain name (for example, top-level domain name example.com or second-level domain name www.example.com) or a wildcard domain name (*.example.com). The processes of connecting domain names to different WAF instance types are the same.
  - If the server IP address of each subdomain name is the same, enter a wildcard domain name. For example, if the subdomain names ***a.example.com***, ***b.example.com***, and ***c.example.com*** have the same server IP address, you can add the wildcard domain name ****.example.com*** to WAF to protect all three.
  - If the server IP addresses of subdomain names are different, add subdomain names as single domain names one by one.
- Each combination of a domain name and a 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.

The following figure shows the process of connecting a website to WAF in each mode.

Figure 8-4 Process of connecting a website to WAF - Cloud Mode (CNAME Access)

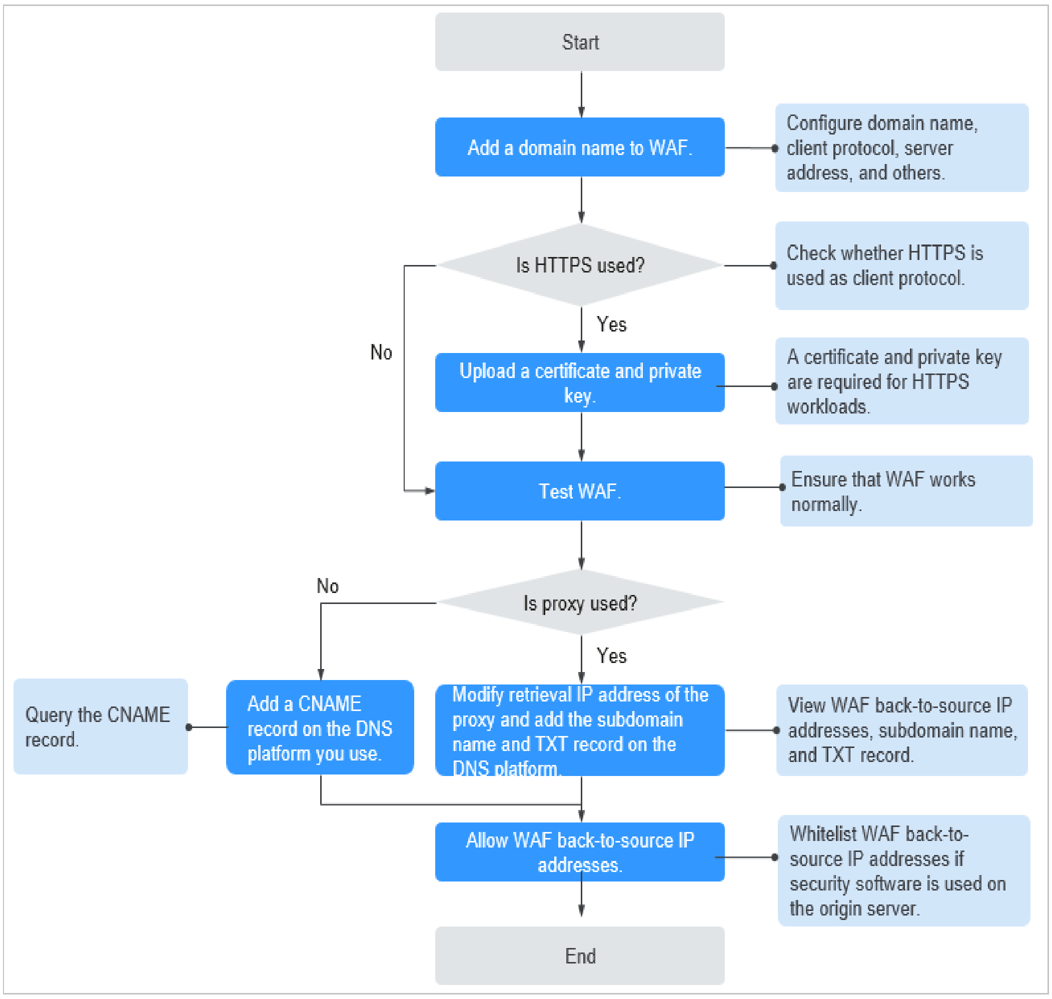
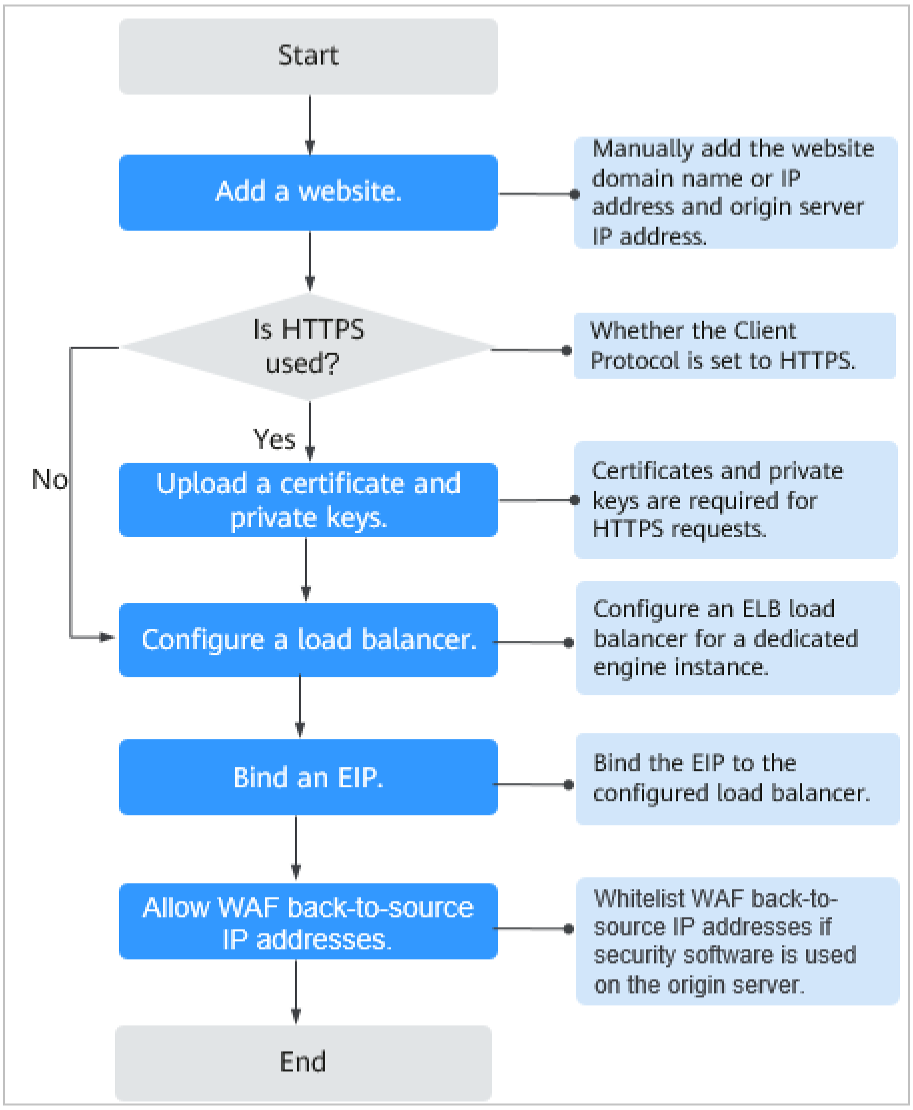

Start
Add a domain name to WAF.
Configure domain name, client protocol, server address, and others.
Is HTTPS used?
Check whether HTTPS is used as client protocol.
No
Yes
Upload a certificate and private key.
A certificate and private key are required for HTTPS workloads.
Test WAF.
Ensure that WAF works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

Figure 8-5 Process of connecting a website to a dedicated WAF instance


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

- If **Access Status** for protected website is **Inaccessible**, rectify the fault by referring to **Why Is My Domain Name or IP Address Inaccessible?**
- If your website becomes inaccessible after it is connected to WAF, rectify the issue by referring to **How Do I Troubleshoot 500/502/504 Errors?**

8.4.1.2 Which Non-Standard Ports Does WAF Support?

In addition to standard ports 80 and 443, WAF supports lots of non-standard ports. Supported non-standard ports vary depending on the edition and billing mode you select.

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.

Ports Supported by WAF

Table 8-3 lists the ports that can be protected by WAF.

Table 8-3 Ports supported by WAF

Deployment Mode	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
Cloud mode	Standard ports	80	443	Unlimited
	Non-standard ports (86 in total)	81, 82, 83, 84, 86, 87, 88, 89, 800, 808, 5000, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8999, 8011, 8012, 8013, 8014, 8015, 8016, 8017, and 8070	4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, and 8805	20
Dedicated mode	Standard ports	80	443	Unlimited

Deployment Mode	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
	Non-standard ports (182 in total)	9945, 9770, 81, 82, 83, 84, 88, 89, 800, 808, 1000, 1090, 3128, 3333, 3501, 3601, 4444, 5000, 5222, 5555, 5601, 6001, 6666, 6788, 6789, 6842, 6868, 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, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9802, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702, 8011, 8012, 8013, 8014,	8750, 8445, 18010, 4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, 8805, 9999	Unlimited

Deployment Mode	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
		8015, 8016, 8017, and 8070		

8.4.1.3 How Do I Use a Dedicated WAF Instance to Protect Non-Standard Ports That Are Not Supported by the Dedicated Instance?

To use a dedicated WAF instance to protect a non-standard port that is not supported by dedicated instance, configure an ELB load balancer to distribute traffic to any non-standard port that is supported by the dedicated instance. For supported non-standard ports, see **Which Non-Standard Ports Does WAF Support?**

For example, a client sends requests over HTTP to the dedicated WAF instance, and you protect the website whose domain name is www.example.com:1234. The dedicated instance cannot protect non-standard port 1234. In this case, you can configure a load balancer to distribute traffic to any other non-standard port (for example, port 81) that can be protected by the dedicated instance. In this way, traffic designated to non-standard port 1234 will be checked by WAF.

NOTICE

To ensure that the configuration takes effect, a wildcard domain name corresponding to the protected domain name is recommended for the **Domain Name** field. For example, if you want to protect www.example.com:1234, set **Domain Name** to ***.example.com**.

Perform the following steps:

Step 1 Log in to the management console.

Step 2 Add the domain name of the website you want to protect on the WAF console.

1. Click ☰ in the upper left corner and choose **Web Application Firewall (Dedicated)** under **Security**.
2. In the navigation pane on the left, choose **Website Settings**.
3. In the upper left corner of the website list, click **Add Website**. On the displayed page, select **Dedicated mode**, enter the wildcard domain name ***.example.com** corresponding to **www.example.com:1234** in the **Domain Name** text box, and select a port (for example, 81) from the **Protected Port** drop-down list.
4. Select **Yes** for **Proxy Configured** and click **Confirm**.
5. Close the dialog box displayed.

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

Step 3 Configure a load balancer on the ELB console.

1. Click ☰ in the upper left corner of the page and choose **Elastic Load Balance** under **Network** to go to the **Load Balancers** page.
2. Click the name of the load balancer you want in the **Name** column to go to the **Basic Information** page.
3. Locate the **IP as a Backend** row, enable the function. In the displayed dialog box, click **OK**.
4. Select the **Listeners** tab, click **Add Listener**, and configure the listener port to **1234**.
5. Click **Next: Configure Request Routing Policy**.
6. Click **Next: Add Backend Server**. Then, select the **IP as Backend Servers** tab.
7. Click **Add IP as Backend Server**. In the displayed dialog box, configure **Backend Server IP Address** and **Backend Port**.
   - **Backend Server IP Address**: Enter the IP address of the dedicated WAF engine, which you can obtain from the dedicated engine list.
   - **Backend Port**: 81, which is the same as the port you configured in **Step 2.3**.
8. Click **OK**.
9. Click **Next: Confirm**, confirm the information, and click **Submit**.

Step 4 Unbind an elastic IP address (EIP) from the origin server and bind the EIP to the load balancer configured for the dedicated WAF instance.

----End

8.4.1.4 How Do I Configure Domain Names to Be Protected When Adding Domain Names?

Before using WAF, you need to add domain names to be protected to WAF based on your web service protection requirements. WAF supports addition of single domain names and wildcard domain names. This section describes how to configure domain names to be protected.

Basic Concepts

- Wildcard domain name

  A wildcard domain name is a domain name that contains the wildcard * and starts with ***.**.

  For example, ***.example.com** is a correct wildcard domain name, but ***.*.example.com** is not.

  NOTE

  A wildcard domain name counts as one domain name.

- Single domain name

  A single domain name is also called a common domain name and is a specific domain name (a non-wildcard domain name).

  For example, **www.example.com** or **example.com** is a single domain name.

NOTE

For example, **www.example.com** counts as a domain name and so does **a.www.example.com**.

Selecting a Domain Name Type

WAF supports single domain names and wildcard domain names.

The domain name purchased from the DNS service provider is a single domain name (example.com). The domain name added to WAF can be example.com, a subdomain name (for example, a.example.com), or wildcard domain name (*.example.com). You can select a domain name type based on the following scenarios:

- If services of a domain name to be protected are the same, enter a single domain name. For example, if all the services of www.example.com to be protected are services on port 8080, set **Domain Name** to a single domain name **www.example.com**.
- If the server IP address of each subdomain name is the same, enter a wildcard domain name to be protected. For example, if the server IP addresses corresponding to a.example.com, b.example.com, and c.example.com are the same, **Domain Name** can be set to a wildcard domain name ***.example.com**.
- If the server IP addresses of subdomain names are different, add subdomain names as single domain names one by one.

NOTE

You are advised to set the added domain name to be protected to be the same as the domain name that is set at the DNS provider.

If A Single Domain Name and A Wildcard Domain Name Are Added To WAF at The Same Time, Which Domain Name Will WAF Check First?

WAF first checks the domain name that points to a specific page. For example, if www.example.com, *.a.example.com, and *.example.com are added to WAF, WAF checks them in the following sequence: www.example.com > *.a.example.com > *.example.com.

8.4.1.5 Do I Have to Configure the Same Port as That of the Origin Server When Adding a Website to WAF?

No. When you add a domain name to WAF, configure the server port to the port of the protected website. The origin server port is the service port used by WAF to forward your website requests. More details about port configuration are described as follows:

- If **Client Protocol** is **HTTP**, WAF protects services on the standard port 80 by default. If **Client Protocol** is **HTTPS**, WAF protects services on the standard port 443 by default.
- To configure a port other than ports 80 and 443, select a non-standard port from the **Protected Port** drop-down list.

8.4.1.6 How Do I Configure Non-standard Ports When Adding a Protected Domain Name?

When you add a domain name to WAF, **Port** must be configured to the service port of your website. You can configure it by referring to the following instructions:

- If **Client Protocol** is **HTTP**, WAF protects services on the standard port 80 by default. If **Client Protocol** is **HTTPS**, WAF protects services on the standard port 443 by default.
- To configure a port other than ports 80 and 443, select a non-standard port from the **Protected Port** drop-down list.

8.4.1.7 What Can I Do If One of Ports on an Origin Server Does Not Require WAF Protection?

WAF protects your web application through its domain name and the corresponding service port. When you add a domain name to WAF, you specify the domain name and the port to be protected. After the website is connected to WAF, traffic will not be forwarded to WAF through other ports.

8.4.1.8 What Data Is Required for Connecting a Domain Name/IP Address to WAF?

Prepare information required for connecting a domain name or IP address to WAF based on the mode of WAF instance you plan to apply for.

The following data is required:

- Domain name/IP address
- Port: the service port corresponding to the domain name to be protected. WAF supports non-standard ports.
- Server information
  - **Client Protocol**: protocol used by a client to access a server.
  - **Server Protocol**: protocol over which WAF forwards client requests to the server.
  - **Server Address**: private IP address of the website server.
  - **Server Port**: service port over which the WAF instance forwards client requests to the origin server.
- Certificate: If HTTPS is set for **Client Protocol**, associate the certificate to WAF.

8.4.1.9 How Do I Safely Delete a Protected Domain Name?

To delete a website from WAF, see **Deleting a Protected Website from WAF**. Before you start, get yourself familiar with the following precautions:

- In cloud mode, if you want to remove a protected website from WAF, go to the DNS platform and translate the domain name to the origin server IP address before you remove it. Otherwise, traffic intended to the domain name will not be directed to the origin server.

- It takes a while to remove a website from WAF, but once this action is started, it cannot be cancelled. Exercise caution when removing a website from WAF.

8.4.1.10 Can I Change the Domain Name That Has Been Added to WAF?

After a domain name is added to WAF, you cannot change its name. If you want to change the protected domain name, you are advised to delete the original one and add the domain name you want to protect.

8.4.1.11 What Are the Precautions for Configuring Multiple Server Addresses for Backend Servers?

- When configuring multiple server addresses for the same domain name, pay attention to the following:
  - For domain names mapping to non-standard ports

    The client protocol, server protocol, and server for each piece of server configuration must be the same.
  - For domain names mapping to standard ports

    The client protocol, server protocol, and server for each piece of server configuration can be different.
- When a domain name is added, WAF supports addition of multiple server IP addresses. WAF routes legitimate requests back to origin servers in polling mode, reducing the pressure on the servers and protecting the origin servers. For example, two backend server IP addresses (IP-A and IP-B) are added. When there are 10 requests for accessing the domain name, five requests are forwarded by WAF to the server identified by IP-A, and the other five requests are forwarded by WAF to the server identified by IP-B.

8.4.1.12 Does WAF Support Wildcard Domain Names?

Yes. When adding a domain name to WAF, you can configure a single domain name or a wildcard domain name based on your service requirements. The details are as follows:

- Single domain name

  Configure a single domain name to be protected. For example, www.example.com
- Wildcard domain name

  You can configure a wildcard domain name to let WAF protect multi-level domain names under the wildcard domain name.
  - 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 directly add the wildcard domain name ****.example.com*** to WAF for protection.
  - If each subdomain name points to different server IP addresses, add subdomain names as single domain names one by one.

8.4.1.13 How Do I Route Website Traffic to My Cloud WAF Instance?

In cloud CNAME access mode, after you add your website to WAF, resolve the website domain name to WAF so that the traffic can pass through WAF. Then, WAF will filter out malicious requests and forward only legitimate requests to the origin server.

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, test WAF 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.

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 8-4**.

Table 8-4 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

For details, see **Connecting a Domain Name to WAF**.

8.4.1.14 Can I Configure Multiple Load Balancers for a Dedicated WAF Instance?

Yes. You can add a dedicated WAF instance to backend server groups of more than one load balancers.

8.4.2 Certificate Management

8.4.2.1 How Do I Select a Certificate When Configuring a Wildcard Domain Name?

Each domain name must correspond to a certificate. A wildcard domain name can only be used for a wildcard domain certificate. If you only have single-domain certificates, you need to add domain names one by one in WAF.

8.4.2.2 How Do I Modify a Certificate?

If the purchased certificate is about to expire, you are advised to purchase a new certificate before the expiration date and update the certificate associated with the domain name in WAF.

Procedure (for dedicated WAF)

Step 1 Log in to the management console.

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

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

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

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

Step 6 Click ✎ next to **Server Information**. If **Client Protocol** is **HTTPS**, select a new certificate from the certificate drop-down list or import a new certificate.

----End

8.4.2.3 Do I Need to Import the Certificates That Have Been Uploaded to ELB to WAF?

You can select a created certificate or import a new certificate. You need to import the certificate that has been uploaded to ELB to WAF.

8.4.2.4 How Do I Convert a Certificate into PEM Format?

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**.
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.

8.4.3 Server Configuration

8.4.3.1 How Do I Configure the Client Protocol and Server Protocol?

This FAQ describes how to configure the client and server protocol.

WAF provides various protocol types. Use www.example.com as an example. You can configure your WAF instance using any of the following methods:

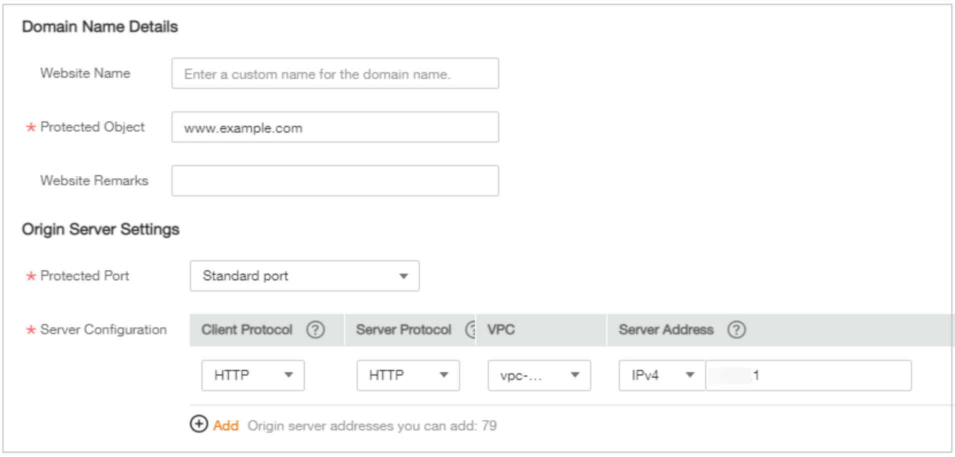
HTTP Access - 302 Redirection Response

Set **Client Protocol** and **Server Protocol** to **HTTP**. **Figure 8-6** shows an example.

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.

Figure 8-6 HTTP forwarding



Domain Name Details

Website Name	Enter a custom name for the domain name.
* Protected Object	www.example.com
Website Remarks	

Origin Server Settings

* Protected Port	Standard port

* Server Configuration

Client Protocol	Server Protocol	VPC	Server Address
HTTP	HTTP	vpc-...	IPv4 [redacted]1

Add Origin server addresses you can add: 79

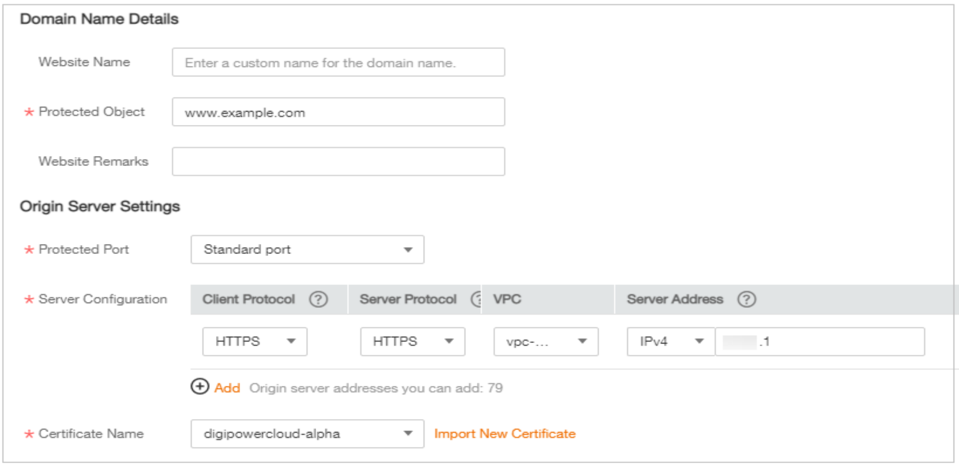
HTTPS Forcible Conversion

Set **Client Protocol** and **Server Protocol** to **HTTPS**. **Figure 8-7** shows an example. When the HTTP protocol is used to access the server, all initial client requests are forcibly converted from HTTP to HTTPS.

NOTICE

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

Figure 8-7 HTTPS redirection



Domain Name Details

Website Name	Enter a custom name for the domain name.
* Protected Object	www.example.com
Website Remarks	

Origin Server Settings

* Protected Port	Standard port

* Server Configuration

Client Protocol	Server Protocol	VPC	Server Address
HTTPS	HTTPS	vpc-...	IPv4 [redacted].1

Add Origin server addresses you can add: 79

* Certificate Name	digipowercloud-alpha Import New Certificate

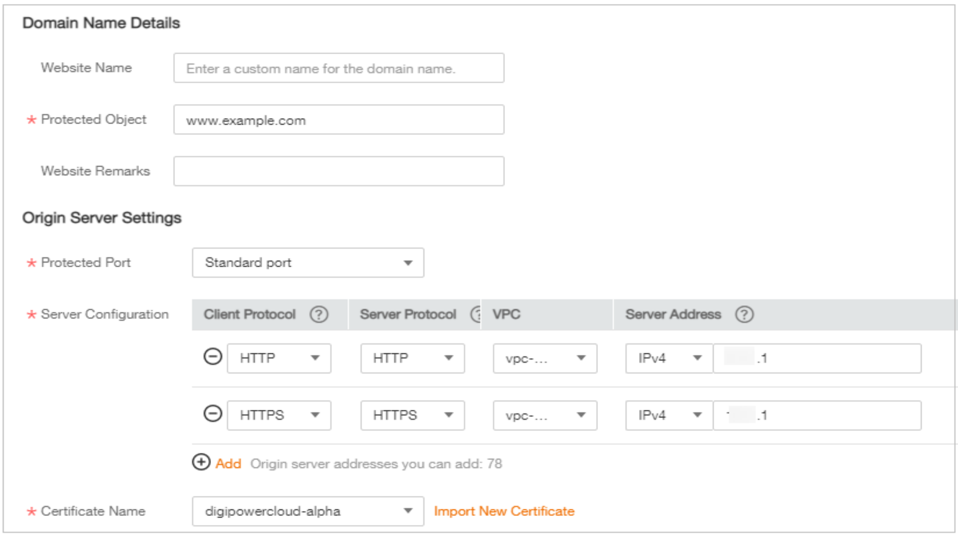
HTTP and HTTPS forwarding

Set **Client Protocol** and **Server Protocol**. **Figure 8-8** shows an example.

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.

Figure 8-8 HTTP and HTTPS forwarding



Domain Name Details

Website Name: Enter a custom name for the domain name.

* Protected Object: www.example.com

Website Remarks:

Origin Server Settings

* Protected Port: Standard port

* Server Configuration

Client Protocol	Server Protocol	VPC	Server Address	
HTTP	HTTP	vpc-...	IPv4	.1
HTTPS	HTTPS	vpc-...	IPv4	.1

Origin server addresses you can add: 78

* Certificate Name: digipowercloud-alpha

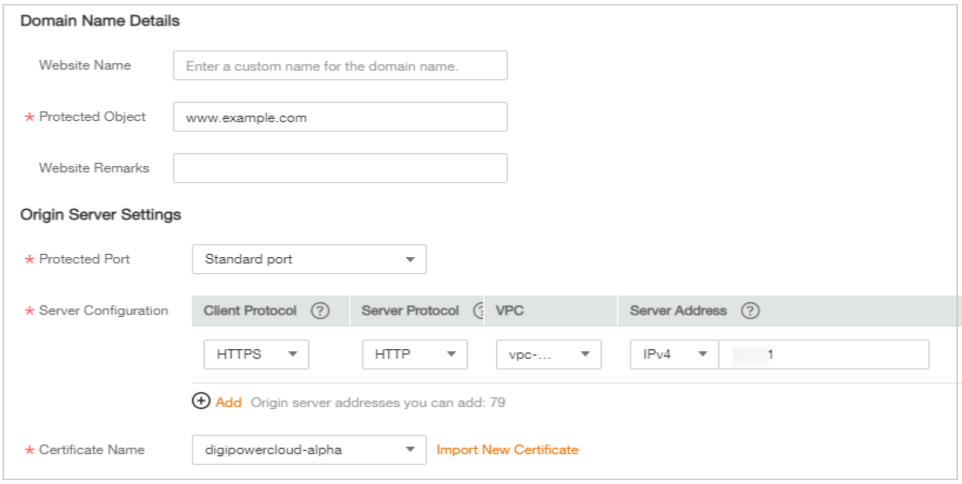
HTTPS Offloading

Set **Client Protocol** to **HTTPS** and **Server Protocol** to **HTTP**. **Figure 8-9** shows an example.

NOTICE

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

Figure 8-9 HTTPS offloading



Domain Name Details

Website Name: Enter a custom name for the domain name.

* Protected Object: www.example.com

Website Remarks:

Origin Server Settings

* Protected Port: Standard port

* Server Configuration:

Client Protocol	Server Protocol	VPC	Server Address
HTTPS	HTTP	vpc-...	IPv4 1

Add Origin server addresses you can add: 79

* Certificate Name: digipowercloud-alpha Import New Certificate

8.4.3.2 Why Cannot I Select a Client Protocol When Adding a Domain Name?

The non-standard port you configured is not supported by the client protocol (HTTP/HTTPS). The non-standard port you will configure must be supported by the client protocol (HTTP/HTTPS).

For more details, see **Which Non-Standard Ports Does WAF Support?**

8.4.3.3 Can I Set the Origin Server Address to a CNAME Record If I Use Cloud WAF?

Yes. If the IP address of the origin server is set to a CNAME record, additional DNS resolution is performed after a domain name is added. That is, the CNAME is resolved to an IP address first. DNS resolution increases the delay. Therefore, a public network IP address is recommended for the origin server.

8.4.4 Domain Name Resolution

8.4.4.1 What Should I Do If the DNS Status Is Unconfigured?

If **DNS** is **Unconfigured**, domain name resolution fails, that is, the domain name is not connected to WAF. In this case, perform the following steps to connect the domain name again:

- If a proxy such as CDN or AAD is used, you need to configure the back-to-source IP address, subdomain name, and TXT record.

  a. Configure the back-to-source IP address of the proxy on the website.

     For example, change the back-to-source IP address of CDN or AAD to the WAF IP address.

  b. Configure **Subdomain Name** and **TXT Record**.

     Add a subdomain name and TXT record to the DNS records of your DNS provider.

NOTICE

The high availability of our system, which is based on multi-AZ deployments to support both active-active and disaster recovery, relies on the WAF CNAME record. Do not use a fixed IP address to access services. Otherwise, service disaster recovery reliability will be affected.

- If no proxy is used, the CNAME record must be configured.

  a. Go to your DNS provider and configure the CNAME record. For details, contact your DNS provider.

  NOTICE

  The high availability of our system, which is based on multi-AZ deployments to support both active-active and disaster recovery, relies on the WAF CNAME record. Do not use a fixed IP address to access services. Otherwise, service disaster recovery reliability will be affected.

  1. Do not modify the hosts file. Add the CNAME record directly to the DNS records of your DNS provider.
  2. Do not use the A record to replace the CNAME record.

  The CNAME binding method of some common DNS providers is listed for your reference. If the following configuration is inconsistent with the actual configuration, rely on information provided by the DNS providers.

  i. Log in to the management console of the DNS provider.

  ii. Go to the domain resolution record page.

  iii. Set the CNAME resolution record.

     ○ Set the record type to **CNAME**.

     ○ Generally, enter the domain name prefix in the host record. For example, if the protected domain name is **admin.demo.com**, enter **admin** in the host record.

     ○ The record value is the CNAME generated by WAF.

     ○ Resolution line: keep the default value **TTL**.

  iv. Click **Save**.

  NOTICE

  The preceding resolution methods are provided by third parties. This document does not control or assume responsibility for any third party content, including but not limited to its accuracy, compatibility, reliability, availability, legitimacy, appropriateness, performance, non-infringement, or status update, unless otherwise specified in this document.

  b. Verify that the CNAME has been configured.

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

ii. Run the following command to query the CNAME. If the configured CNAME is displayed, the configuration is successful.

nslookup www.*domain***.com**

8.4.5 Operations After Connecting Websites to WAF

8.4.5.1 Can I Access a Website Using an IP Address After a Domain Name Is Connected to WAF?

After a domain name is connected to WAF, you can enter the origin server IP address in the address bar of the browser to access the website. However, your origin server IP address is easily exposed. As a result, attackers can bypass WAF and attack your origin server.

8.4.5.2 How Do I Test WAF?

Before you direct the traffic to WAF, perform local verification to ensure that all configurations are correct.

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

For details, see **Testing WAF**.

8.4.5.3 Why Cannot the Protection Mode Be Enabled After a Domain Name Is Connected to WAF?

Another tenant has configured the same domain name in WAF. As a result, the domain name ownership is occupied by another tenant. In this case, add a subdomain name and configure a TXT record for the subdomain name at your DNS provider.

8.5 Service Interruption Check

8.5.1 How Do I Troubleshoot 500/502/504 Errors?

If an error such as 500 Internal Server Error, 502 Bad Gateway, or 504 Gateway Timeout occurs after your web server connects to WAF, use the following methods to locate the cause and remove the error:

Symptom 1

After WAF is configured, your web server works properly. However, a few minutes later, a 502 Bad Gateway error is reported frequently.

- Possible Causes

  Interception by a firewall, security protection software installed on the backend server, or the rate limiting policy

- Solution

Add the WAF IP address ranges to the whitelist of the firewall (hardware or software), security protection software, and rate limiting module.

Symptom 2

After WAF is configured, the accessed page returns a 502/500 error frequently (when multiple backend servers are configured).

- Possible Cause

  Origin server configuration error

- Solution

  Locate the target domain name record in the domain name list and click the domain name. On the displayed page, in the **Server Information** area, check whether the protocol, IP address, and port number used by the origin server are correct.

  You can access the IP address of the origin server to check whether the backend service port is enabled.

Symptom 3

After WAF is configured, a 502 Bad Gateway error is reported frequently when web visitors request access to your server over HTTPS. However, web visitors can directly access the server.

- Possible Cause

  Outdated HTTPS version

- Solution

  A lower Secure Sockets Layer (SSL) version has serious security risks. WAF supports TLSv1.2 or later. If your server has a lower SSL version, a 502 Bad Gateway error is reported after your server connects to WAF. In this case, you need to upgrade the SSL version of your server. You can visit **https://www.ssllabs.com/ssltest/index.html** to check your SSL version.

  – If the OS of your web server is earlier than Windows Server 2008, the SSL protocol does not support TLSv1.2 or later. In this case, you need to upgrade the server OS to Windows Server 2008 or later (or a new version of Linux), and enable TLSv1.2 in services such as IIS.

  – If your web server does not run Windows, check whether the SSL protocol is TLSv1.2 or later.

Symptom 4

After WAF is configured, your web server works properly. However, when the number of requests increases, 502/504 errors increase as well. If web visitors directly access your web server, there is a possibility that the 502/504 error code is returned.

- Possible Cause

  Backend server performance issue

- Solution

  a. Optimize the server configuration, including TCP network parameters and ulimit parameters.

b. Increase the number of backend ECSs to support rising service volumes. WAF supports configuration of multiple backend servers.

c. If web visitors request access to your web server over HTTPS, you can use HTTPS forwarding on the WAF side. However, it is recommended that HTTP be used to forward the requests to your web server, lowering the computational pressure on backend servers.

8.5.2 Why Is My Domain Name or IP Address Inaccessible?

Symptoms

If **Access Progress/Status** for a website you have added to WAF is **Inaccessible**, the connection between WAF and the website domain name or IP address fails to be established.

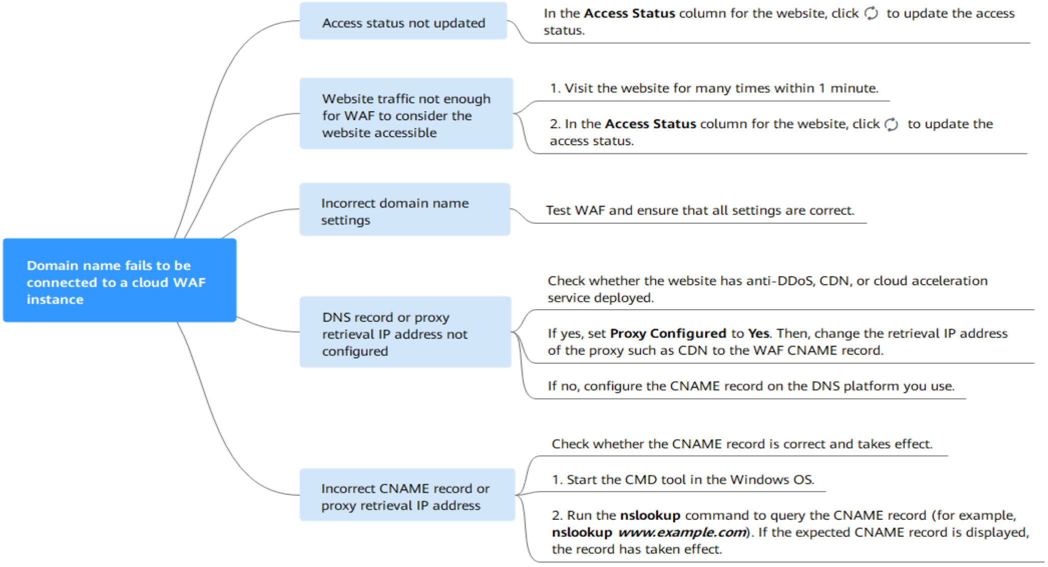
NOTICE

- WAF automatically checks the access status of protected websites every hour. If WAF detects that a protected website has received 20 access requests within 5 minutes, it considers that the website has been successfully connected to WAF.
- By default, WAF checks only the **Access Status** of domain names added or updated over the last two weeks. If a domain name was added to WAF two weeks ago and has not been modified in the last two weeks, you can click ⟳ in the **Access Progress** column to refresh the progress.

Troubleshooting and Solutions for Cloud WAF Instances

Refer to **Figure 8-10** and **Table 8-6** to fix connection failures for websites protected in cloud mode.

Figure 8-10 Troubleshooting for Cloud WAF



Domain name fails to be connected to a cloud WAF instance

Access status not updated

In the **Access Status** column for the website, click ⟳ to update the access status.

Website traffic not enough for WAF to consider the website accessible

1. Visit the website for many times within 1 minute.

2. In the **Access Status** column for the website, click ⟳ to update the access status.

Incorrect domain name settings

Test WAF and ensure that all settings are correct.

DNS record or proxy retrieval IP address not configured

Check whether the website has anti-DDoS, CDN, or cloud acceleration service deployed.

If yes, set **Proxy Configured** to **Yes**. Then, change the retrieval IP address of the proxy such as CDN to the WAF CNAME record.

If no, configure the CNAME record on the DNS platform you use.

Incorrect CNAME record or proxy retrieval IP address

Check whether the CNAME record is correct and takes effect.

1. Start the CMD tool in the Windows OS.

2. Run the **nslookup** command to query the CNAME record (for example, **nslookup** ***www.example.com***). If the expected CNAME record is displayed, the record has taken effect.

Table 8-6 Solutions for failures of WAF instances

Possible Cause	Solution
Cause 1: **Access Status** of **Protected Website** not updated	In the **Access Status** column for the protected website, click ↻ to update the status.
Cause 2: Website access traffic not enough for WAF to consider the website accessible **NOTICE** After you connect a website to WAF, the website is considered accessible only when WAF detects at least 20 requests to the website within 5 minutes.	1. Access the protected website for many times within 1 minute. 2. In the **Access Status** column for the website, click ↻ to update the status.

Possible Cause	Solution
Cause 3: Incorrect domain name settings	**NOTICE** WAF can protect the website using the following types of domain names: ● Top-level domain names, for example, example.com ● Single domain names/Second-level domains, for example, www.example.com ● Wildcard domain names, for example, *.example.com Domain names example.com and www.example.com are different. Ensure that correct domain names are added to WAF. Perform the following steps to ensure that the domain name settings are correct. 1. In Windows OSs, choose **Start** > **Run**. Then enter **cmd** and press **Enter**. 2. Ping the CNAME record of the domain name to obtain the WAF back-to-source IP address. 3. Use a text editor to open the **hosts** file. Generally, the **hosts** file is stored in the **C:\Windows\System32\drivers\etc\** directory. 4. Add a record into the **hosts** file in the format of ***DomainName WAF back-to-source IP address***. 5. Save the **hosts** file after the record is added. In the CLI, run the **ping** *Domain name added to WAF* command, for example, ping www.example.com. If the WAF back-to-source IP address in 2 is displayed in the command output, the domain name settings are correct. If there are incorrect domain name settings, remove the

Possible Cause	Solution
	domain name from WAF and add it to WAF again.
Cause 4: DNS record or the back-to-source IP addresses of proxies not configured	Check whether the website connected to WAF uses proxies such as advanced anti-DDoS, CDN, and cloud acceleration service. ● Yes. – Change the back-to-source IP address of the proxy such as CDN to the CNAME record of WAF. – (Optional) Add a WAF subdomain name and TXT record at your DNS provider. ● If no, contact your DNS service provider to configure a CNAME record for the domain name.
Cause 5: Incorrect DNS record or proxy back-to-source address	Perform the following steps to check whether the domain name CNAME record takes effect: 1. In Windows OSs, choose **Start** > **Run**. Then enter **cmd** and press **Enter**. 2. Run a **nslookup** command to query the CNAME record. If the command output displays the CNAME record of WAF, the record takes effect. Using www.example.com as an example, the output is as follows: `nslookup www.example.com`

Troubleshooting and Solutions for Dedicated WAF

Refer to **Figure 8-11** and **Table 8-7** to fix connection failures.

Figure 8-11 Troubleshooting for dedicated mode

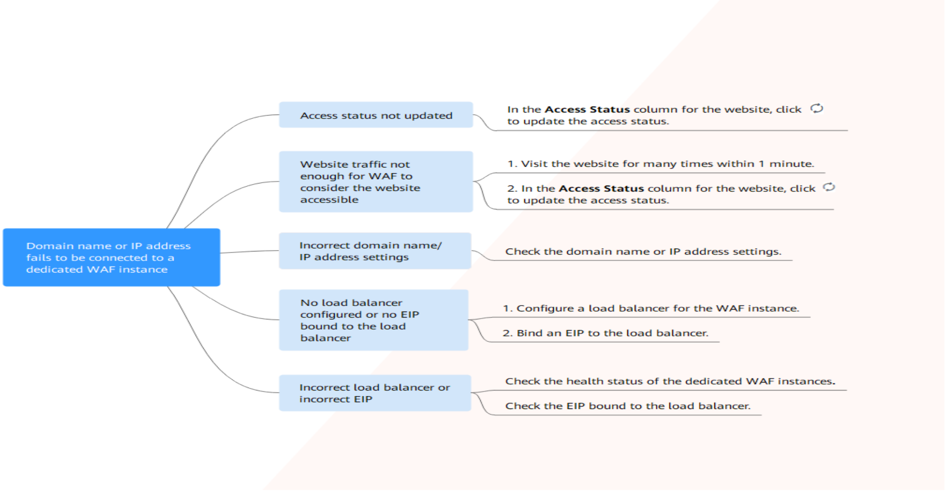

Domain name or IP address fails to be connected to a dedicated WAF instance
Access status not updated
In the **Access Status** column for the website, click ↻ to update the access status.
Website traffic not enough for WAF to consider the website accessible
1. Visit the website for many times within 1 minute.
2. In the **Access Status** column for the website, click ↻ to update the access status.
Incorrect domain name/ IP address settings
Check the domain name or IP address settings.
No load balancer configured or no EIP bound to the load balancer
1. Configure a load balancer for the WAF instance.
2. Bind an EIP to the load balancer.
Incorrect load balancer or incorrect EIP
Check the health status of the dedicated WAF instances.
Check the EIP bound to the load balancer.

Table 8-7 Solutions for dedicated mode

Possible Cause	Solution
Cause 1: **Access Status** for **Domain Name/IP Address** not updated	In the **Access Status** column for the website, click ↻ to update the status.
Cause 2: Website access traffic not enough for WAF to consider the website accessible **NOTICE** After you connect a website to WAF, the website is considered accessible only when WAF detects at least 20 requests to the website within 5 minutes.	1. Access the protected website many times within 1 minute. 2. In the **Access Status** column for the website, click ↻ to update the status.
Cause 3: Incorrect domain name or IP address settings	Check domain name or IP address settings. If there are incorrect settings for the domain name or IP address, remove this domain name or IP address from WAF and add it to WAF again.
Cause 4: No load balancer configured for the dedicated WAF instance or no EIP bound to the load balancer configured for the dedicated WAF instance	1. Configure a load balancer for dedicated WAF instances by referring to **Configuring a Load Balancer**. 2. **Bind an EIP to a Load Balancer**.

Possible Cause	Solution
Cause 5: Incorrect load balancer configured or incorrect EIP bound to the load balancer	- After you **configure a load balancer**, ensure that **Health Check Result** for the dedicated WAF instances added to the load balancer is **Healthy**. - After you **bind an EIP to the load balancer**, check the EIP status.

8.5.3 How Do I Handle False Alarms as WAF Blocks Normal Requests to My Website?

Once an attack hits a WAF 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.

NOTICE

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.

In the row containing the false alarm event, click **Details** in the **Operation** column and view the event details. If you are sure that the event is a false positive, handle it as a false alarm by referring to **Table 8-8**. After an event is handled as a false alarm, WAF stops blocking corresponding type of event. No such type of event will be displayed on the **Events** page and you will no longer receive alarm notifications accordingly.

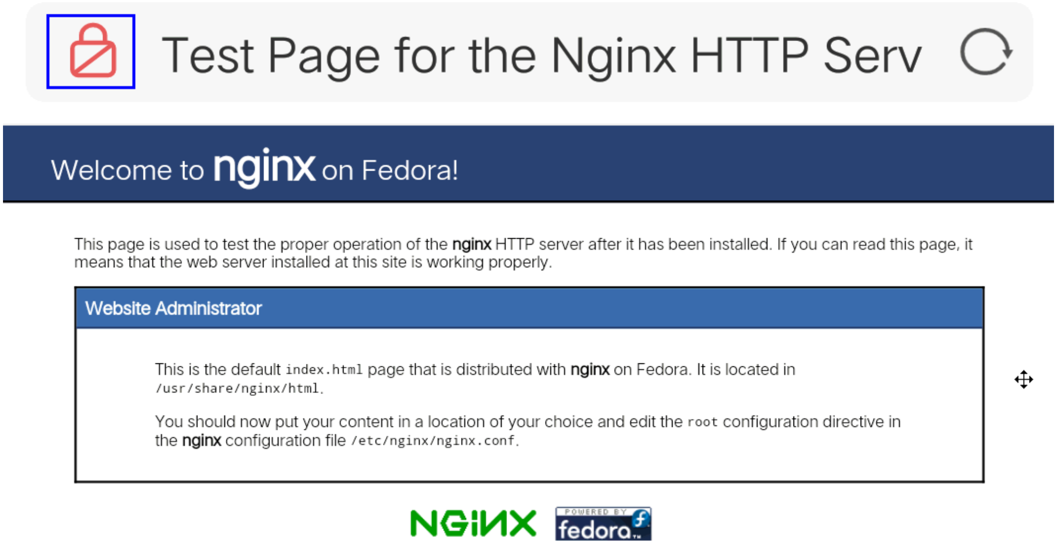
Table 8-8 Handling false alarms

Type of Hit Rule	Hit Rule	Handling Method
WAF built-in protection rules	● 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.	In the row containing the attack event, click **Handle as False Alarm** in the **Operation** column. For details, see **Handling False Alarms**.
Custom protection rules	● CC attack protection rules ● Precise protection rules ● Blacklist and whitelist rules ● Geolocation access control rules ● Web tamper protection rules ● JavaScript anti-crawler protection ● Information leakage prevention rules ● Data masking rules	Go to the page displaying the hit rule and delete it.
Other	Invalid access requests **NOTE** If either of the following cases, WAF blocks the access request as an invalid request: ● When **form-data** is used for POST or PUT requests, the number of parameters in a form exceeds 8,192. ● The URI contains more than 2,048 parameters. ● The number of headers exceeds 512.	Allow the blocked requests by referring to **Configuring Custom Precise Protection Rules**. The **Handle as False Alarm** button is grayed out for events that are generated against a precise protection rule.

8.5.4 Why Are HTTPS Requests Denied on Some Mobile Phones?

If your visitors receive a page similar to the one in **Figure 8-12** when they try to access your website through a mobile phone, an incomplete certificate chain is uploaded when you connect the website to WAF. Rectify the fault by referring to **How Do I Fix an Incomplete Certificate Chain?**

Figure 8-12 Access failed



Test Page for the Nginx HTTP Serv

Welcome to nginx on Fedora!

This page is used to test the proper operation of the **nginx** HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working properly.

Website Administrator

This is the default `index.html` page that is distributed with **nginx** on Fedora. It is located in `/usr/share/nginx/html`.

You should now put your content in a location of your choice and edit the `root` configuration directive in the **nginx** configuration file `/etc/nginx/nginx.conf`.

8.5.5 How Do I Fix an Incomplete Certificate Chain?

If the certificate provided by the certificate authority is not found in the built-in trust store on your platform and the certificate chain does not have a certificate authority, the certificate is incomplete. If you use the incomplete certificate to access the website corresponding to the protected domain name, the access will fail.

Use either of the following methods to fix it:

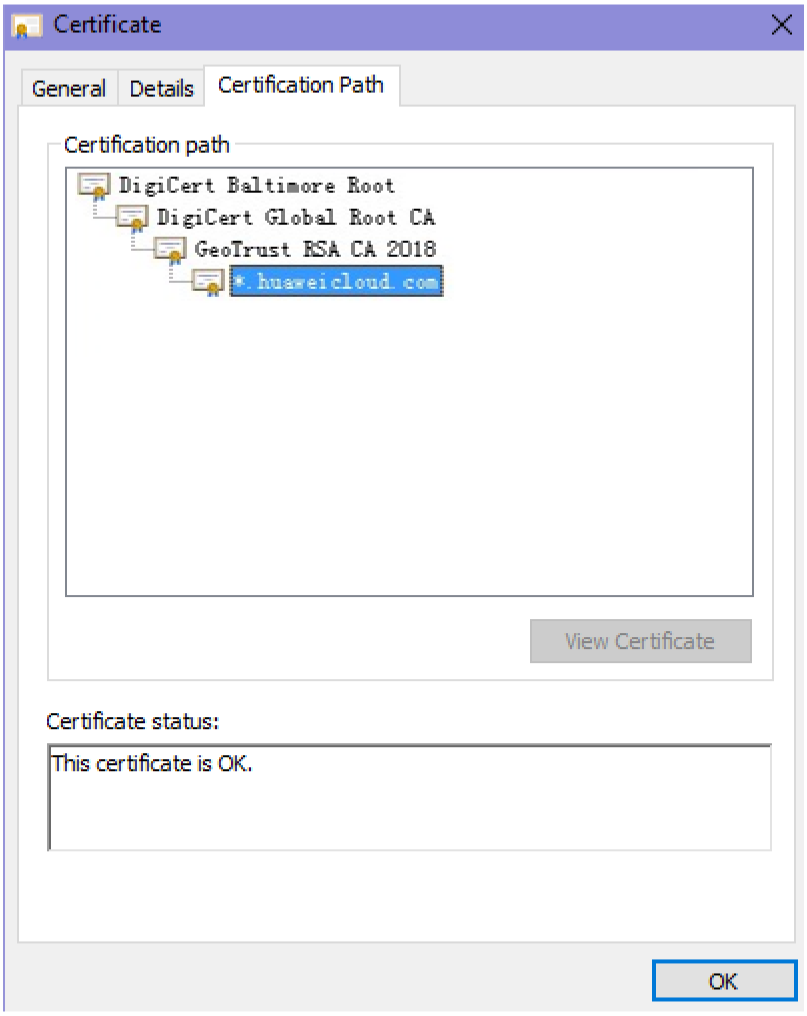
- Manually build up a complete certificate chain and upload the certificate. (This function is available soon.)
- Upload the correct certificate.

The latest Google Chrome version supports automatic verification of the trust chain. The following describes how to manually create a complete certificate chain:

Step 1 Check the certificate. Click the padlock in the address bar to view the certificate status.

Step 2 Check the certificate chain. Click **Certificate**. Select the **Certificate Path** tab and then click the certificate name to view the certificate status. **Figure 8-13** shows an example.

Figure 8-13 Viewing the certificate chain



DigiCert Baltimore Root
DigiCert Global Root CA
GeoTrust RSA CA 2018
*.huaweicloud.com

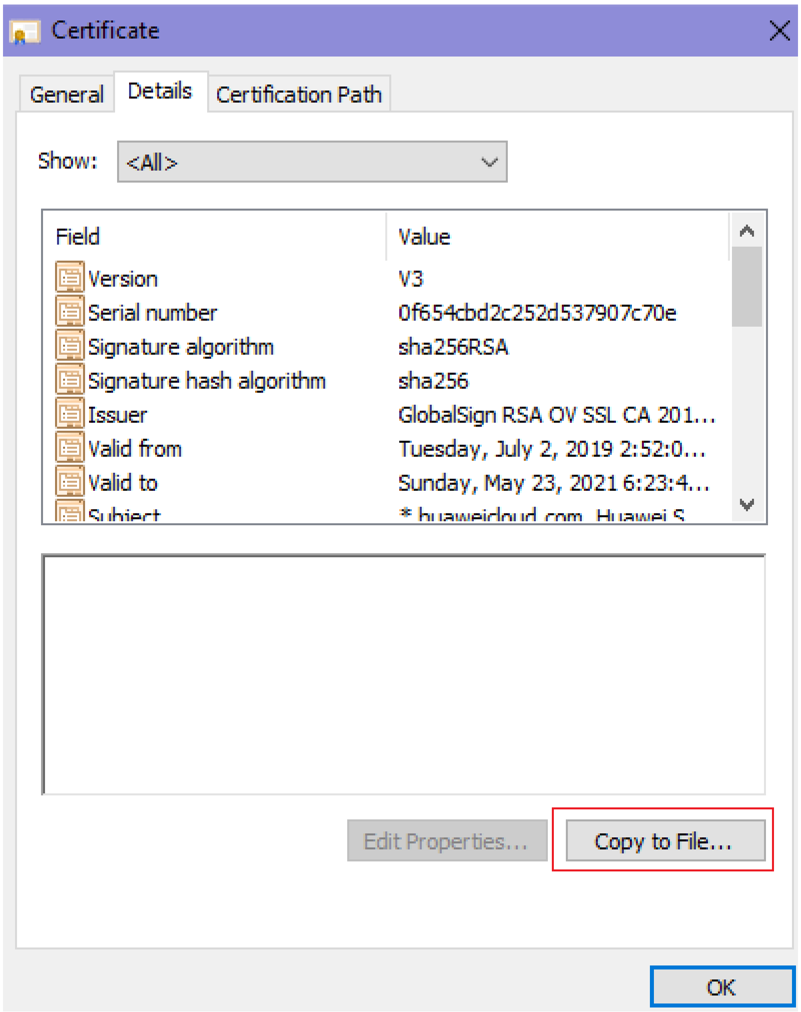
Certificate status:

This certificate is OK.

Step 3 Save the certificates to the local PC one by one.

1. Select the certificate name and click the **Details** tab. **Figure 8-14** shows an example.

Figure 8-14 Details

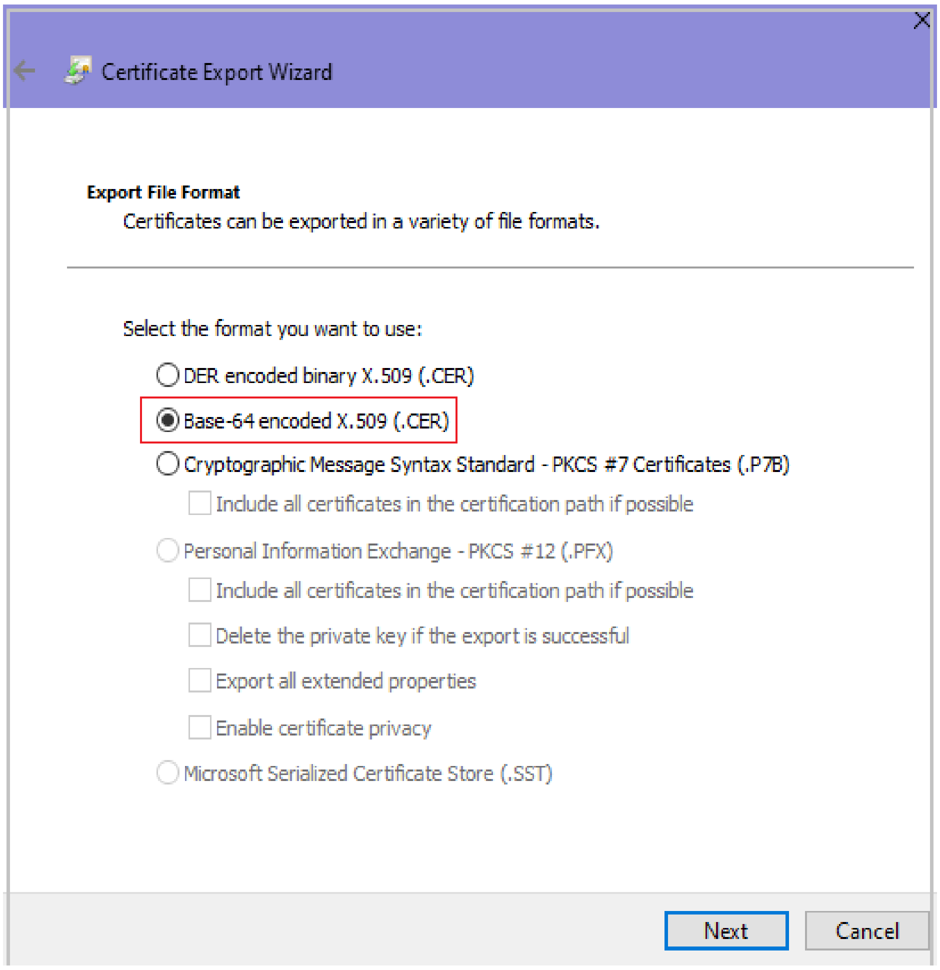


Show: <All>

Field	Value
Version	V3
Serial number	0f654cbd2c252d537907c70e
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	GlobalSign RSA OV SSL CA 201...
Valid from	Tuesday, July 2, 2019 2:52:0...
Valid to	Sunday, May 23, 2021 6:23:4...
Subject	* huaweicloud.com, Huawei S

2. Click **Copy to File**, and then click **Next** as prompted.
3. Select **Base-64 encoded X.509 (.CER)** and click **Next**. **Figure 8-15** shows an example.

Figure 8-15 Certificate Export Wizard



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

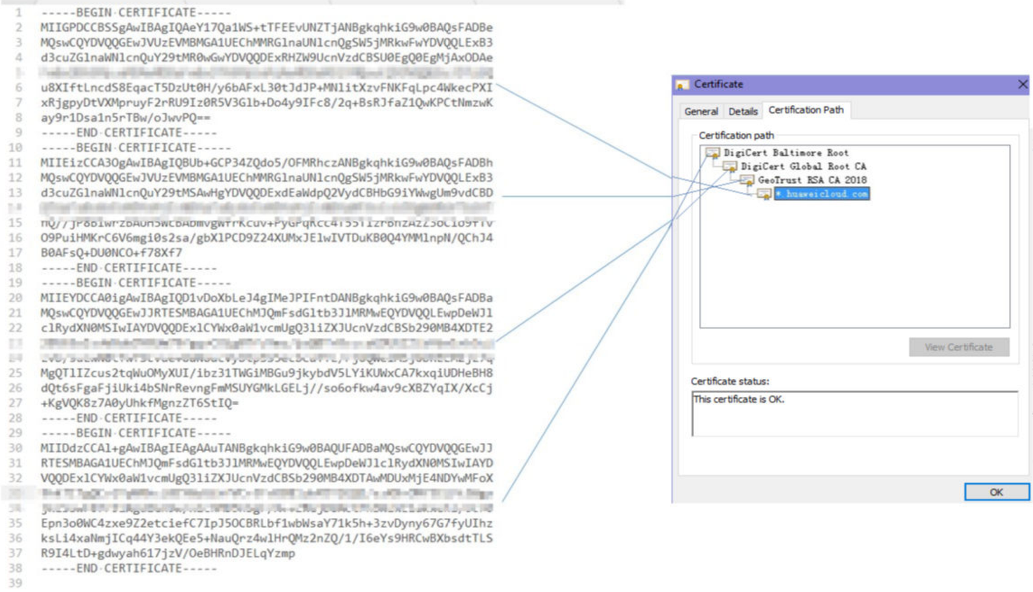
□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

Step 4 Rebuild the certificate. After all certificates are exported to the local PC, open the certificate file in Notepad and rebuild the certificate according to the sequence shown in **Figure 8-16**.

Figure 8-16 Certificate rebuilding



```
-----BEGIN CERTIFICATE-----
MIIGPDCCBSSgAwIBAgIQAeY17Qa1WS+tTFEEvUNZTjANBgkqhkiG9w0BAQsFADBe
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMR0wGwYDVQQDExRHZW9UcnVzdCBSU0EgQ0EgMjAxODAe
[redacted]
u8XIftLncdS8EqacT5DzUt0H/y6bAFxL30tJdJP+MNlitXzvFNKFqLpc4WkecPXI
xRjgpyDtVXMpruyF2rRU9Iz0R5V3Glb+Do4y9IFc8/2q+BsRJfaZ1QwKPCtNmzwK
ay9r1Dsa1n5rTBw/oJwvPQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEizCCA3OgAwIBAgIQBUb+GCP34ZQdo5/OFMRhczANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
[redacted]
O9PuiHMKrC6V6mgi0s2sa/gbXlPCD9Z24XUMxJElwIVTDuKB0Q4YMMlnpN/QChJ4
B0AFsQ+DU0NCO+f78Xf7
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEYDCCA0igAwIBAgIQD1vDoXbLeJ4gIMeJPIFntDANBgkqhkiG9w0BAQsFADBa
MQswCQYDVQQGEwJJRTESMBAGA1UEChMJQmFsdGltb3JlMRMwEQYDVQQLEwpDeWJl
clRydXN0MSIwIAYDVQQDExlCYWx0aW1vcmUgQ3liZXJUcnVzdCBSb290MB4XDTE2
[redacted]
MgQTlIZcus2tqWuOMyXUI/ibz31TWGiMBGu9jkybdV5LYiKUWxCA7kxqiUDHeBH8
dQt6sFgaFjiUki4bSNrRevngFmMSUYGMkLGELj//so6ofkw4av9cXBZYqIX/XcCj
+KgVQK8z7A0yUhkfMgnzZT6StIQ=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIEAgAAuTANBgkqhkiG9w0BAQUFADBaMQswCQYDVQQGEwJJ
RTESMBAGA1UEChMJQmFsdGltb3JlMRMwEQYDVQQLEwpDeWJlclRydXN0MSIwIAYD
VQQDExlCYWx0aW1vcmUgQ3liZXJUcnVzdCBSb290MB4XDTAwMDUxMjE4NDYwMFoX
[redacted]
Epn3o0WC4zxe9Z2etciefC7IpJ5OCBRLbf1wbWsaY71k5h+3zvDyny67G7fyUIhz
ksLi4xaNmjICq44Y3ekQEe5+NauQrz4wlHrQMz2nZQ/1/I6eYs9HRCwBXbsdtTLS
R9I4LtD+gdwyah617jzV/OeBHRnDJELqYzmp
-----END CERTIFICATE-----
```

Certificate

Certification path

DigiCert Baltimore Root
DigiCert Global Root CA
GeoTrust RSA CA 2018
*.huaweicloud.com

Certificate status:

This certificate is OK.

Step 5 Upload the certificate again.

----End

8.5.6 Why Does My Certificate Not Match the Key?

After an HTTPS certificate is uploaded to the AAD or WAF console, a message is displayed indicating that the certificate and key do not match.

Solution

Possible Cause	How to Fix
The uploaded certificate does not match the uploaded private key.	1. Run the following commands to check the MD5 hash values of the certificate and private key file: **openssl x509 -noout -modulus -in** *<certificate file>***|openssl md5** **openssl rsa -noout -modulus -in** *<private key file>***|openssl md5** 2. Check whether the MD5 values of the certificate and private key file are the same. If they are different, the certificate file and private key file are associated with different domain names, and the content of the certificate does not match that of the private key file. 3. If the certificate does not match the private key file, upload the correct certificate and private key file.
Incorrect RSA private key format	1. Run the following command to generate a new private key: **openssl rsa -in <***private key file***> -out <***New private key file***>** 2. Upload the private key again.

Related Operations

- **How Do I Fix an Incomplete Certificate Chain?**
- **Why Are HTTPS Requests Denied on Some Mobile Phones?**

8.5.7 Why Am I Seeing Error Code 418?

If the request contains malicious load and is intercepted by WAF, error 418 is reported when you access the domain name protected by WAF. You can view WAF protection logs to view the cause.

- If you confirm that the request is a normal service request, you can handle the false alarm to prevent the recurrence of the protection event.
- If you confirm that the protection event is not a false alarm, your website is attacked and the malicious request is blocked by WAF.

8.5.8 How Can I Upload Files After the Website Is Connected to WAF?

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

To upload a file larger than 10 GB, upload the file through any of the following:

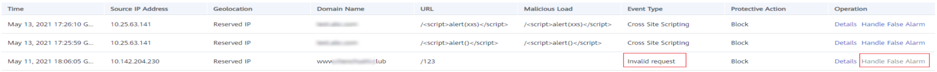
- IP address
- Separate web server that is not protected by WAF
- FTP server

8.5.9 Why Does WAF Block Normal Requests as Invalid Requests?

Symptom

After a website is connected to WAF, a normal access request is blocked by WAF. On the **Events** page, the corresponding **Event Type** reads **Invalid request**, and the **Handle False Alarm** button is grayed out, as shown in **Figure 8-17**.

Figure 8-17 Normal requests blocked by WAF as invalid requests



Time	Source IP Address	Geolocation	Domain Name	URL	Malicious Load	Event Type	Protective Action	Operation
May 13, 2021 17:26:10 G...	10.25.63.141	Reserved IP	[redacted]	/<script>alert(xxs)</script>	/<script>alert(xxs)</script>	Cross Site Scripting	Block	Details Handle False Alarm
May 13, 2021 17:25:59 G...	10.25.63.141	Reserved IP	[redacted]	/<script>alert()</script>	/<script>alert()</script>	Cross Site Scripting	Block	Details Handle False Alarm
May 11, 2021 18:06:05 G...	10.142.204.230	Reserved IP	www[redacted]lub	/123		Invalid request	Block	Details Handle False Alarm

Possible Cause

If either of the following cases, WAF blocks the access request as an invalid request:

- When **form-data** is used for POST or PUT requests, the number of parameters in a form exceeds 8,192.
- The URI contains more than 2,048 parameters.
- The number of headers exceeds 512.

Solution

If you confirm that the blocked request is a normal request, allow it by **Configuring Custom Precise Protection Rules**.

8.5.10 How Do I Whitelist IP Address Ranges of Cloud WAF?

To let WAF take effect in cloud mode, configure ACL rules on the origin server to trust only the back-to-source IP addresses of WAF. 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.

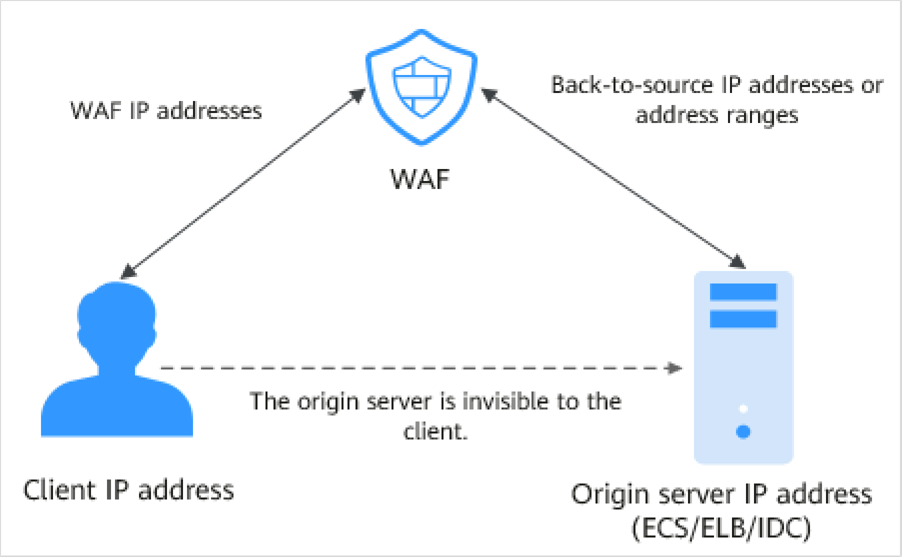
What Are Back-to-Source IP Addresses?

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 8-18 Back-to-source IP address


WAF IP addresses
Back-to-source IP addresses or address ranges
WAF
The origin server is invisible to the client.
Client IP address
Origin server IP address (ECS/ELB/IDC)

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 (Dedicated)** under **Security**.

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

Step 5 Above the website list, click **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.

----End

8.5.11 What Is the Connection Timeout Duration of WAF? Can I Manually Set the Timeout Duration?

- 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 connections between WAF and your origin server is 30 seconds. You can customize a timeout duration on the WAF console.

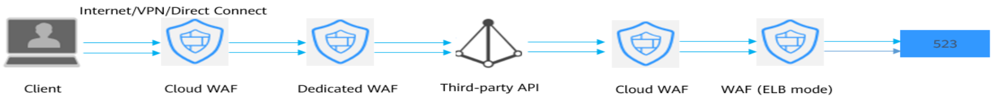
  On the **Basic Information** page, enable **Timeout Settings** and click ✓ . Then, specify **WAF-to-Server connection timeout (s)**, **Read timeout (s)**, and **Write timeout (s)** and click ✓ to save settings.

8.5.12 How Do I Solve the Problem of Excessive Redirection Times?

After a domain name is connected to WAF, if the system displays a message indicating that there are excessive redirection times when a user requests to access the target domain name, the possible cause is that you have configured forcible redirection from HTTP to HTTPS on the backend server and forwarding from HTTPS (client protocol) to HTTP (server protocol) is configured on WAF, WAF is forced to redirect user requests, causing an infinite loop. You can configure two pieces of server information about HTTP (client protocol) to HTTP (server protocol) and HTTPS (client protocol) to HTTPS (server protocol).

8.5.13 Why Am I Seeing Error Code 523?

If a request goes through WAF over four times, WAF will block the request and return error code 523 to avoid endless loops. If error code 523 is returned for your website requests, check how many WAF instances you are using.



Cause 1: A website is connected to more than four WAF instances.

Error code 523 will return if a website has been connected to different types of WAF instances more than 4 times.

Solution

Route website traffic to bypass redundant WAF instances.

Step 1 Log in to the WAF management console.

Step 2 In the navigation pane on the left, choose **Website Settings**.

Step 3 Locate the website for which 523 error code is returned, retain one configuration, and delete the website from redundant WAF instances. For details, see **Deleting a Protected Website from WAF**.

To prevent service interruptions due to such deletions, perform the following operations before removing a website from WAF:

Cloud mode: Go to your DNS provider and resolve your domain name to the IP address of the origin server. Otherwise, the traffic to your domain name cannot be routed to the origin server.

----End

Cause 2: A Third-party Interface That Uses WAF Was Called

When a request is forwarded to the third-party API, header and cookie are forwarded without being changed. Only the host is modified. This makes WAF count the requests without clearing historical records.

Solution

Modify the header field in the reverse proxy request. The operations are as follows:

NOTICE

This method can be used only when Nginx is deployed after WAF on the user traffic link.

Step 1 Use **proxy_set_header** to redefine the request header sent to the proxy server. Run the following command to open the Nginx configuration file:

(The following command is used when Nginx is installed in the **/opt/nginx/** directory. Change the directory based on your situation.)

vi /opt/nginx/conf/nginx.conf

Step 2 Add **proxy_set_header X-CloudWAF-Traffic-Tag 0** to the Nginx configuration file. The following is an example:

```
location  ^~/test/ {
   ......
   proxy_set_header Host       $proxy_host;
   proxy_set_header X-CloudWAF-Traffic-Tag 0;
   ......
   proxy_pass http://x.x.x.x;
}
```

----End

Cause 3: Origin Server IP address Was Mistakenly Set to an IP Address of WAF or A Proxy in Front of WAF

If the origin server address is mistakenly set to the back-to-source IP address of WAF or an IP address of the proxy in front of WAF, the website requests go to an endless loop and error code 523 is returned.

Solution

Check the origin server configurations and enter a correct origin server address.

8.5.14 Why Does the Website Login Page Continuously Refreshed After a Domain Name Is Connected to WAF?

After you connect the domain name of your website to WAF, all website requests are forwarded to WAF first. Then, WAF forwards only the normal traffic to the origin server. For each request from the client, WAF generates an identifier based on the access IP address and user agent. WAF has multiple back-to-source IP addresses that will be randomly allocated. When the back-to-source-IP address changes, the identifier of the request changes accordingly. As a result, the session is directly deleted by WAF, and the login page keeps refreshing. To avoid this problem, you are advised to use session cookies to keep session persistent.

8.5.15 Why Does the Requested Page Respond Slowly After the HTTP Forwarding Policy Is Configured?

In this case, add two forwarding policies. One is HTTP to HTTP forwarding, and the other is HTTPS to HTTPS forwarding.

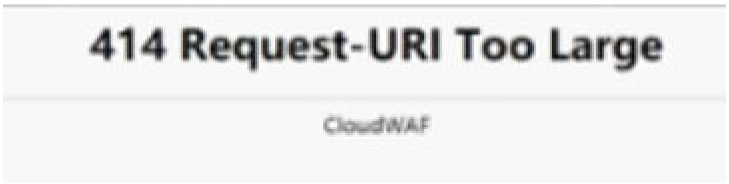
For details about how to configure a forwarding rule, see **How Do I Solve the Problem of Excessive Redirection Times?**

8.5.16 Why Am I Seeing Error Code 414 Request-URI Too Large?

Symptoms

After a protected website is connected to WAF, the website is inaccessible and the error message "414 Request-URI Too Large" is displayed, as shown in **Figure 8-19**.

Figure 8-19 Error Code 414 Request-URI Too Large



414 Request-URI Too Large

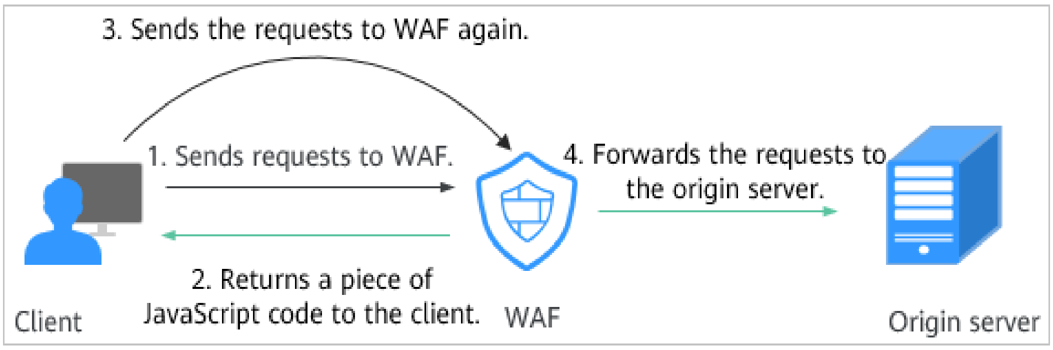
CloudWAF

Possible Causes

The client browser cannot parse JavaScript. In this situation, the client browser caches the page that contains the JavaScript code returned by WAF. Each time the protected website is requested, the cached page is accessed. WAF then verifies that the access request is from an invalid browser or crawler. The access request verification fails. As a result, an infinite loop occurs, the URI length exceeds the browser limit, and the website becomes inaccessible.

After JavaScript anti-crawler is enabled, WAF returns a piece of JavaScript code to the client when the client sends a request. 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. **Figure 8-20** shows how JavaScript verification works.

Figure 8-20 JavaScript anti-crawler detection process



3. Sends the requests to WAF again.
1. Sends requests to WAF.
4. Forwards the requests to the origin server.
2. Returns a piece of JavaScript code to the client.
Client
WAF
Origin server

Handling Suggestions

Disable the JavaScript anti-crawler protection by performing the following steps:

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 (Dedicated)** under **Security**.

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 In the **Anti-Crawler** configuration area, click **Configure Anti-Crawler**.

Step 7 Click the **JavaScript** tab and disable the JavaScript anti-crawler protection. Its status changes to ○.

----End

8.5.17 What Do I Do If the Protocol Is Not Supported and the Client and Server Do Not Support Common SSL Protocol Versions or Cipher Suites?

Symptom

After a domain name is connected to WAF, the website cannot be accessed. A message is displayed, indicating that the protocol is not supported. The client and server do not support common SSL protocol versions or cipher suites.

Solution

Select the default cipher suite for **Cipher Suite** in the **TLS Configuration** dialog box. For details, see .

8.5.18 Why Cannot I Access the Dedicated Engine Page?

Symptom

Error message "Failed to request IAM. Please check the current user's IAM permissions." is displayed when a user attempted to access the **Dedicate Engine** page under **Instance Management**.

Possible Cause

The **IAM ReadOnly** permission is not granted to the login account.

Solution

Assign the **IAM ReadOnly** permission to your account.

8.5.19 Why Is the Bar Mitzvah Attack on SSL/TLS Detected?

The bar mitzvah attack is an attack on SSL/TLS protocols that exploits a vulnerability in the RC4 cryptographic algorithm. This vulnerability can disclose ciphertext in SSL/TLS encrypted traffic in some cases, such as passwords, credit card data, or other privacy data, to hackers.

Solution

To solve this problem, you can set the minimum TLS version to TLS v1.2 and cipher suite to cipher suite 2.

8.6 Protection Rule Configuration

8.6.1 Basic Web Protection

8.6.1.1 How Do I Switch the Mode of Basic Web Protection from Log Only to Block?

This FAQ guides you to switch the mode of basic web protection to **Block**.

Perform the following operations:

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 (Dedicated)** under **Security**.

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 In the **Basic Web Protection** configuration area, set **Mode** to **Block**.

NOTICE

Log only and **Block** are merely modes of basic web protection. CC attack protection and precise protection have their own protective actions.

----End

8.6.1.2 Which Protection Levels Can Be Set for Basic Web Protection?

WAF provides three basic web protection levels: **Low**, **Medium**, and **High**. The default option is **Medium**. For details, see **Table 8-9**.

Table 8-9 Protection levels

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

8.6.2 CC Attack Protection Rules

8.6.2.1 What Is the Peak Rate of CC Attack Protection?

It depends on the WAF edition you are using. For details, see **Table 8-10**.

Table 8-10 Applicable service scales

Service Scale	Dedicated Mode
Peak rate of normal service requests	The following lists the specifications of a single instance. ● 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 **NOTICE** Maximum QPS values are for reference only. They may vary depending on your businesses. The real-world QPS is related to the request size and the type and quantity of protection rules you customize.
Peak rate of CC attack protection	● Specifications: WI-500. Referenced performance: Maximum QPS: 20,000 ● Specifications: WI-100. Referenced performance: Maximum QPS: 4,000

8.6.2.2 How Do I Configure a CC Attack Protection Rule?

When a service interface is under an HTTP flood attack, you can set a CC attack protection rule on the WAF console to relieve service pressure.

WAF provides the following settings for a CC attack protection rule:

- Number of requests allowed from a web visitor in a specified period
- Identification of web visitors based on the IP address, cookie, or referer field.
- Action when the maximum limit is reached, such as **Block** or **Verification code**

8.6.2.3 When Is Cookie Used to Identify Users?

During the configuration of a CC attack protection rule, if IP addresses cannot identify users precisely, for example, when many users share an egress IP address, use Cookie to identify users.

If the cookie contains key values, such as the session value, of users, the key value can be used as the basis for identifying users.

8.6.2.4 What Are the Differences Between Rate Limit and Allowable Frequency in a CC Rule?

In a CC attack protection rule, **Rate Limit** specifies the maximum requests that a website visitor can initiate within the configured period. If the configured rate limit has been reached, WAF will respond according to the protective action configured. For example, if you configure **Rate Limit** to **10 requests** within **60 seconds** and **Protective Action** to **Block**, a maximum of 10 requests are allowed within 60 seconds. Once the website visitor initiates more than 10 requests within 60 seconds, WAF directly blocks the visitor from accessing the requested URL.

If you select **Advanced** for **Mode** and **Block dynamically** for **Protective Action**, configure **Rate Limit** and **Allowable Frequency**.

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 configured. If blocking is triggered and **Allowable Frequency** is **0**, all requests that meet the rule conditions in the next period are blocked.

Differences

- The rate limit period of **Allowable Frequency** is the same as that of **Rate Limit**.
- **Allowable Frequency** is lower than or equal to **Rate Limit**, and **Allowable Frequency** can be **0**.

8.6.3 Precise Protection rules

8.6.3.1 Can a Precise Protection Rule Take Effect in a Specified Period?

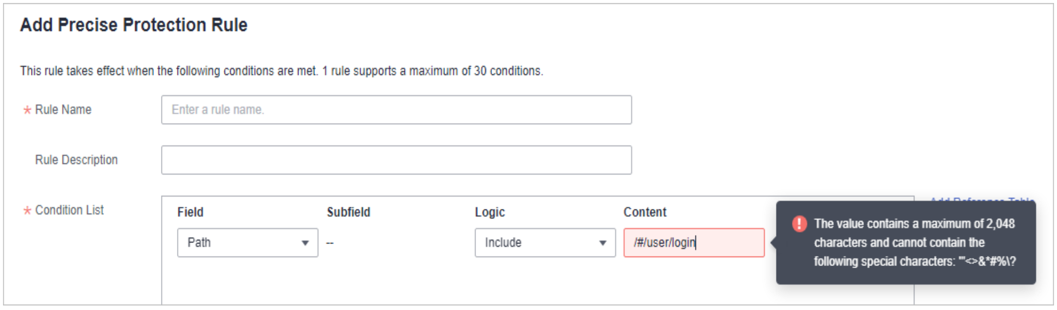
Precise access protection rules can take effect in a specified period.

You can set precise protection rules to filter access requests based on a combination of common HTTP fields (such as IP address, path, referer, user agent, and params) to allow or block the requests that match the conditions.

8.6.3.2 Can a Path Containing # Be Matched in a Precise Protection Rule?

The path added to a precise protection rule cannot contain special characters ('"<>&*# %\?).

The number sign (#) is a client parameter. Parameters following the number sign (#) are not transferred to the server for web page location. WAF and browsers do not consider the content following the number sign (#) as URL parameters. Therefore, the parameters cannot be obtained.



Add Precise Protection Rule

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

* Rule Name: Enter a rule name.

Rule Description:

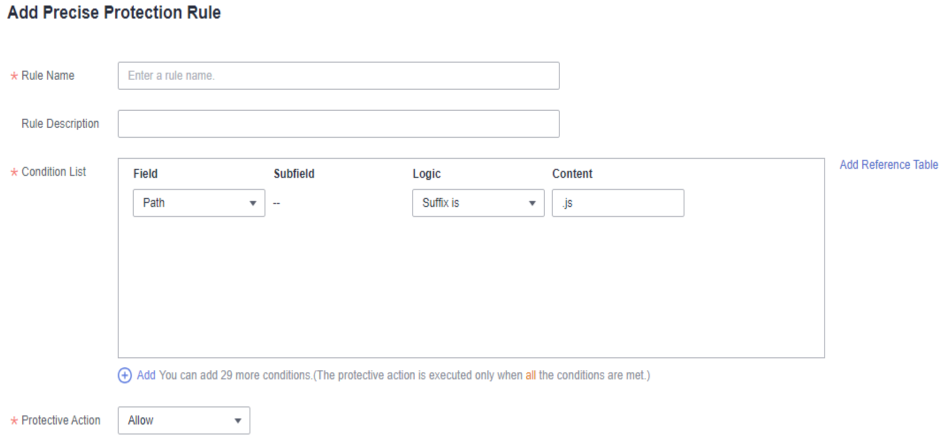
* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/#/user/login

The value contains a maximum of 2,048 characters and cannot contain the following special characters: "'<>&*#%\?

8.6.3.3 How Can I Allow Access from .js Files?

You can configure a precise protection rule in WAF to allow access from paths with the suffix .js. The configuration is as follows:



Add Precise Protection Rule

* Rule Name: Enter a rule name.

Rule Description:

* Condition List

Field	Subfield	Logic	Content
Path	--	Suffix is	.js

Add Reference Table

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

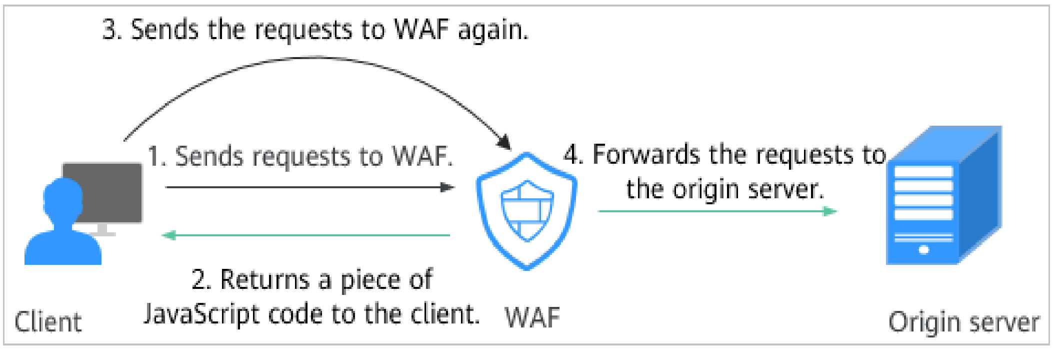
* Protective Action: Allow

8.6.4 Anti-Crawler Protection

8.6.4.1 Why Is the Requested Page Unable to Load After JavaScript Anti-Crawler Is Enabled?

After JavaScript anti-crawler is enabled, WAF returns a piece of JavaScript code to the client when the client sends a request. 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. **Figure 8-21** shows how JavaScript verification works.

Figure 8-21 JavaScript anti-crawler detection process


3. Sends the requests to WAF again.
1. Sends requests to WAF.
4. Forwards the requests to the origin server.
2. Returns a piece of JavaScript code to the client.
Client
WAF
Origin server

NOTICE

- To enable the JavaScript anti-crawler protection, the browser on the client must have JavaScript and cookies enabled.
- If the client does not meet the preceding requirements, only steps 1 and 2 can be performed. In this case, the client request fails to obtain the page.

Check your services. If your website can be accessed by other means except for a browser, disable JavaScript anti-crawler protection.

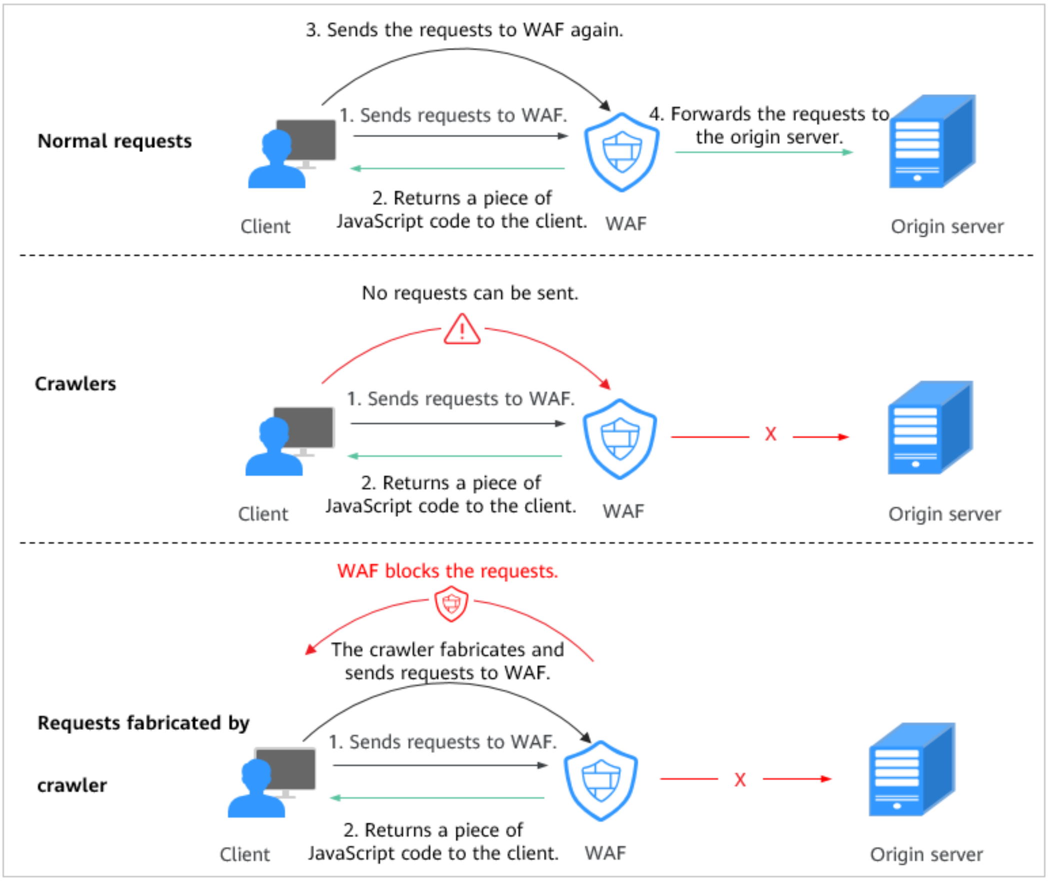
8.6.4.2 Is There Any Impact on Website Loading Speed If Other Crawler Check in Anti-Crawler Is Enabled?

If you have enabled **Other** when you configure **Feature Library** of anti-crawler protection, WAF detects crawlers for various purposes, such as website monitoring, access proxy, and web page analysis. Enabling this option does not affect web page visits or the web page browsing speed.

8.6.4.3 How Does JavaScript Anti-Crawler Detection Work?

Figure 8-22 shows how JavaScript anti-crawler detection works, which includes JavaScript challenges (step 1 and step 2) and JavaScript authentication (step 3).

Figure 8-22 JavaScript Anti-Crawler protection process

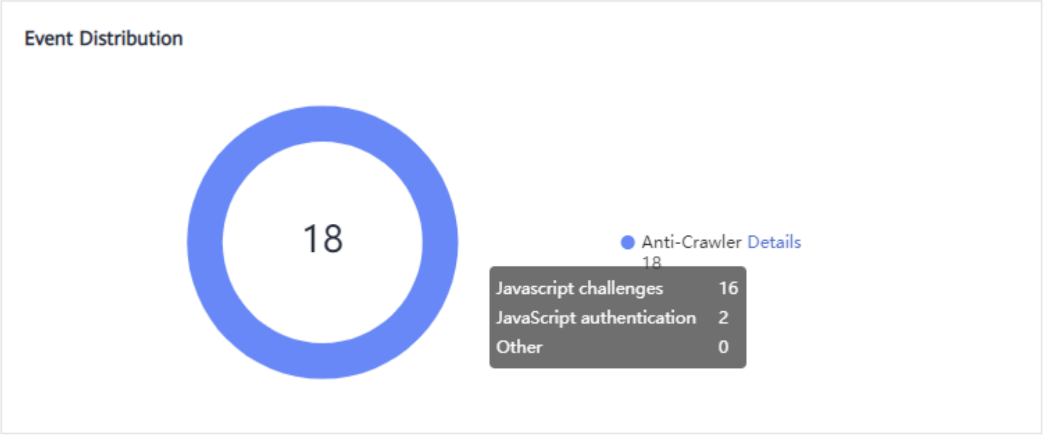

3. Sends the requests to WAF again.
Normal requests
1. Sends requests to WAF.
4. Forwards the requests to the origin server.
2. Returns a piece of JavaScript code to the client.
Client
WAF
Origin server
No requests can be sent.
Crawlers
1. Sends requests to WAF.
2. Returns a piece of JavaScript code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

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

- 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 challenge and authentication responses, the system calculates how many requests the JavaScript anti-crawler defends. As shown in **Figure 8-23**, the JavaScript anti-crawler logs 18 events, 16 of which are JavaScript challenge responses, 2 of which are JavaScript authentication responses. The number of **Other** is the WAF authentication requests fabricated by the crawler.

Figure 8-23 Parameters of a JavaScript anti-crawler protection rule



Javascript challenges	16
JavaScript authentication	2
Other	0

NOTICE

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

8.6.5 Others

8.6.5.1 In Which Situations Will the WAF Policies Fail?

Normally, all requests destined for your site will pass through WAF. However, if your site is using CDN and WAF, the WAF policy targeted at the requests for caching static content will not take effect because CDN directly returns these requests to the client.

8.6.5.2 Can I Export or Back Up the WAF Configuration?

The current WAF configuration cannot be exported or backed up.

8.6.5.3 What Working Modes and Protection Mechanisms Does WAF Have?

After you connect a domain name to your WAF instance, WAF works 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.

WAF supports the following working modes:

- Enabled
- Suspended

Table 8-11 describes the protection mechanism.

Table 8-11 Supported protection mechanism

Protection Rule	Protective Action
Basic web protection rules	● Block ● Log only
CC attack protection rules	● Verification code ● Block ● Block dynamically ● Log only
Precise protection rules	● Block ● Allow ● Log only
Blacklist and whitelist rules	● Block ● Allow ● Log only
Geolocation access control rules	● Block ● Allow ● Log only
Website anti-crawler protection	Protective actions for feature-based anti-crawler rules: ● Block ● Log only

8.6.5.4 Which Protection Rules Are Included in the System-Generated Policy?

When you add a website to WAF, you can select an existing policy you have created or the system-generated policy. For details, see **Table 8-12**.

NOTICE

If you are using WAF standard edition, only **System-generated policy** can be selected.

You can also tailor your protection rules after the domain name is connected to WAF.

Table 8-12 System-generated policies

Edition	Policy	Description
Cloud mode	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.
Dedicated mode	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.

8.6.5.5 What Types of Protection Rules Does WAF Support?

Table 8-13 lists all protection rules you can use in WAF.

Table 8-13 Configurable protection rules

Protection Rule	Description
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.
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.
Precise protection rules	WAF allows you to customize protection rules by combining HTTP headers, cookies, URLs, request parameters, and client IP addresses.
Blacklist and whitelist rules	You can configure blacklist and whitelist rules to block, log only, or allow access requests from 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.
Geolocation access control rules	You can customize these rules to allow or block requests from a specific country or region.
Web tamper protection rules	You can configure these rules to prevent a static web page 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.
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.
Global protection whitelist rules	This function ignores certain attack detection rules for specific requests.
Data masking rules	You can configure data masking rules to prevent sensitive data such as passwords from being displayed in event logs.

8.6.5.6 Which of the WAF Protection Rules Support the Log-Only Protective Action?

In WAF, **Log only** is available for **Protective Action** in basic web protection rules.

Log only is available for **Protective Action** in CC attack protection rules, precise protection rules, blacklist and whitelist rules, geolocation access control rules, and anti-crawler rules.

8.6.5.7 Why Does the Page Fail to Be Refreshed After WTP Is Enabled?

Web Tamper Protection (WTP) supports only caching of static web pages. Perform the following steps to fix this issue:

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 (Dedicated)** under **Security**.

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 In the **Web Tamper Protection** configuration area, check whether this function is enabled.

- If this function is enabled (●), go to **Step 7**.
- If this function is disabled (○), click ○ to enable the function. Refresh the page several minutes later.

Step 7 Click **Customize Rule**. On the displayed page, check whether the domain name and path are correct.

- If they are correct, go to **Step 8**.
- If they are incorrect, click **Delete** in the **Operation** column to delete the rule. Then, click **Add Rule** above the rule list and configure another rule.

  After the rule is added successfully, refresh the page several minutes later. Then, access the page again.

Step 8 In the row containing the web tamper protection rule, click **Update Cache** in the **Operation** column.

If the content of a protected page is modified, you must update the cache. Otherwise, WAF always returns the most recently cached content.

After updating the cache, refresh the page and access the page again. If the page is still not updated, contact technical support.

----End

8.6.5.8 What Are the Differences Between Blacklist/Whitelist Rules and Precise Protection Rules on Blocking Access Requests from Specified IP Addresses?

Both of them can block access requests from specified IP addresses. **Table 8-14** describes the differences between the two types of rules.

Table 8-14 Differences between blacklist and whitelist rules and precise protection rules

Protection Rules	Protection	WAF Inspection Sequence
Blacklist and whitelist rules	This type or rules can block, log only, or allow access requests from a specified IP address or IP address range.	Blacklist and whitelist rules have the highest priority. WAF checks access requests based on the protection rules and the triggering sequence.
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 or block the requests that match the combined conditions.	Precise protection rules have lower priority compared with blacklist and whitelist rules.

8.6.5.9 What Do I Do If a Scanner, such as AppScan, Detects that the Cookie Is Missing Secure or HttpOnly?

Cookies are inserted by back-end web servers and can be implemented through framework configuration or set-cookie. Secure and HttpOnly in cookies help defend against attacks, such as XSS attacks to obtain cookies, and help defend against cookie hijacking.

If the AppScan scanner detects that the customer site does not insert security configuration fields, such as HttpOnly and Secure, into the cookie of the scan request, it records them as security threats.

A Change History

Released On	Description
2023-10-30	This issue is the sixth official release. ● Adjusted the document structure. ● Added the following content: – Enabling LTS for WAF Logging – Using LTS to Quickly Query and Analyze WAF Access Logs – Using LTS to Analyze How WAF Blocks Spring Core RCE Vulnerability in Real Time – Using LTS to Configure Block Alarms for WAF Rules – Does Cloud WAF Use Fixed IP Addresses for Domain Resolution? – Will the CNAME Record Be Changed If the IP Address of the Origin Server Has Been Changed? – Do I Need to Add the Domain Name to WAF Again If the Domain Name IP Address Has Been Changed? – How Can I Allow Access from .js Files? ● Modified the following content: – Step 2: Configure a Load Balancer for WAF – Configuring PCI DSS/3DS Certification Check and Configuring the Minimum TLS Version and Cipher Suite – Configuring a CC Attack Protection Rule – Enabling Anti-Crawler Protection – Dashboard – Viewing event logs – Dedicated WAF Engine Management

Released On	Description
	– Configuring CC Attack Protection – Upgrading Dedicated WAF Instances
2023-06-15	This issue is the fifth official release. ● Modified "Edition Differences": Updated some screenshots. ● Added some screenshots.

Released On	Description
2023-03-30	This issue is the fourth official release. ● Added "Best Practices." ● "What Is Web Application Firewall": Added the cloud service principle diagram. ● Added "Edition Differences." ● Added "Ports Supported by WAF." ● Added "Key Operations Recorded by CTS." ● Added "Personal Data Protection Mechanism." ● Added the following FAQs: – About WAF Protection – Can WAF Block Data Packets in multipart/form-data Format? – Does a Dedicated WAF Instance Support Cross-VPC Protection? – What Are the Differences Between WAF Forwarding and Nginx Forwarding? – Does WAF Block Customized POST Requests? – Does WAF Have the IPS Module? – Is There Any Impact on Origin Servers If I Enable HTTP/2 in WAF? – Can WAF Defend Against the Apache Struts2 Remote Code Execution Vulnerability (CVE-2021-31805)? – Why Does the Vulnerability Scanning Tool Report Disabled Non-standard Ports for My WAF-Protected Website? – How Does WAF Block Requests? – Can WAF Block Requests When a Certificate Is Mounted on ELB? – Does WAF Affect My Existing Workloads and Server Running? – How Do I Configure My Server to Allow Only Requests from WAF? – Why Do Cookies Contain the **HWWAFSESID** or **HWWAFSESTIME** field? – How Do I Configure WAF If a Reverse Proxy Server Is Deployed for My Website? – Do I Need to Make Some Changes in WAF If the Security Group for Origin Server (Address) Is Changed? – Which Non-Standard Ports Does WAF Support?

Released On	Description
	– How Do I Use a Dedicated WAF Instance to Protect Non-Standard Ports That Are Not Supported by the Dedicated Instance? – Can WAF Protect Multiple Domain Names That Point to the Same Origin Server? – Do I Have to Configure the Same Port as That of the Origin Server When Adding a Domain Name to WAF? – What Can I Do If One of Ports on an Origin Server Does Not Require WAF Protection? – How Do I Safely Delete a Protected Domain Name? – Do I Need to Import the Certificates That Have Been Uploaded to ELB to WAF? – How Do I Configure the Client Protocol and Server Protocol? – Why Cannot I Select a Client Protocol When Adding a Domain Name? – Can I Set the Origin Server Address to a CNAME Record If I Am Using a Cloud WAF? – Can I Access a Website Using an IP Address After a Domain Name Is Connected to WAF? – Why Is My Domain Name or IP Address Inaccessible? – Why Does WAF Block Normal Requests as Invalid Requests? – What Is the Connection Timeout Duration of WAF? Can I Manually Set the Timeout Duration? – How Do I Solve the Problem of Excessive Redirection Times? – Why Does the Website Login Page Continuously Refreshed After a Domain Name Is Connected to WAF? – Why Does the Requested Page Respond Slowly After the HTTP Forwarding Policy Is Configured? – Why Am I Seeing Error Code 523? – FAQs About Protection Rule Configuration
2022-12-28	This issue is the third official release. ● Added "Dedicated WAF Mode." ● Added "Metrics." ● Added "Permissions Management." ● Adjusted the structure of "FAQs" and added some FAQs.

Released On	Description
2022-05-06	This issue is the second official issue. Modified "Overview": added descriptions about WAF billing mode and service bandwidth.
2021-07-14	This issue is the first official release.