

# Web Application Firewall

## User Guide

**Issue** 01  
**Date** 2024-04-13



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

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

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

## **Huawei Cloud Computing Technologies Co., Ltd.**

Address: Huawei Cloud Data Center Jiaoxinggong Road  
Qianzhong Avenue  
Gui'an New District  
Gui Zhou 550029  
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

---

# Contents

---

<b>1 Service Overview</b>	<b>1</b>
1.1 What Is Web Application Firewall?	1
1.2 Product Specifications	2
1.3 Functions	4
1.4 Product Advantages	9
1.5 Application Scenarios	10
1.6 Personal Data Protection Mechanism	11
1.7 WAF Permissions Management	12
<b>2 Overview</b>	<b>14</b>
<b>3 Applying for a Dedicated WAF Engine</b>	<b>18</b>
<b>4 Enabling WAF Protection</b>	<b>21</b>
4.1 Ports Supported by WAF	21
4.2 Connecting a Website to WAF	22
4.2.1 Connection Process (Dedicated Mode)	22
4.2.2 Step 1: Add a Website to WAF	24
4.2.3 Step 2: Configure a Load Balancer	29
4.2.4 Step 3: Bind an EIP to a Load Balancer	31
4.2.5 Step 4: Whitelist the Back-to-Source IP Addresses of Your Dedicated WAF Instances	32
<b>5 Website Domain Name Management</b>	<b>35</b>
5.1 Viewing Basic Information	35
5.2 Switching WAF Working Mode	37
5.3 Configuring the Minimum TLS Version and Cipher Suite	38
5.4 Configuring Connection Timeout	44
5.5 Configuring Connection Protection	45
5.6 Updating a Certificate	47
5.7 Configuring a Traffic Identifier for a Known Attack Source	49
5.8 Editing Server Information	51
5.9 Modifying the Alarm Page	52
5.10 Removing a Protected Website from WAF	53
<b>6 Certificate Management</b>	<b>55</b>
6.1 Uploading a Certificate	55

6.2 Deleting a Certificate.....	57
6.3 Viewing Certificate Information.....	58
<b>7 Managing IP Address Blacklist and Whitelist Groups.....</b>	<b>60</b>
7.1 Adding an IP Address Group.....	60
7.2 Modifying or Deleting a Blacklist or Whitelist IP Address Group.....	61
<b>8 Rule Configuration.....</b>	<b>63</b>
8.1 Configuration Guidance.....	63
8.2 Configuring Basic Web Protection Rules.....	68
8.3 Configuring a CC Attack Protection Rule.....	71
8.4 Configuring a Precise Protection Rule.....	78
8.5 Adding a Reference Table.....	84
8.6 Configuring an IP Address Blacklist or Whitelist Rule.....	85
8.7 Configuring a Known Attack Source Rule.....	89
8.8 Configuring a Geolocation Access Control Rule.....	92
8.9 Configuring a Web Tamper Protection Rule.....	93
8.10 Configuring Anti-Crawler Rules.....	96
8.11 Configuring an Information Leakage Prevention Rule.....	98
8.12 Configuring a Global Protection Whitelist (Formerly False Alarm Masking) Rule.....	101
8.13 Configuring a Data Masking Rule.....	105
<b>9 Dashboard.....</b>	<b>108</b>
<b>10 Event Management.....</b>	<b>111</b>
10.1 Viewing Protection Event Logs.....	111
10.2 Handling False Alarms.....	113
10.3 Downloading Events Data.....	116
<b>11 Enabling Alarm Notifications.....</b>	<b>119</b>
<b>12 Policy Management.....</b>	<b>122</b>
12.1 Creating a Protection Policy.....	122
12.2 Adding Rules to One or More Policies.....	123
12.3 Applying a Policy to Your Website.....	124
<b>13 Dedicated WAF Engine Management.....</b>	<b>125</b>
<b>14 Viewing Product Details.....</b>	<b>128</b>
<b>15 Permissions Management.....</b>	<b>129</b>
15.1 WAF Custom Policies.....	129
15.2 WAF Permissions and Supported Actions.....	130
<b>16 FAQs.....</b>	<b>135</b>
16.1 About WAF.....	135
16.1.1 WAF Functions.....	135
16.1.1.1 Can WAF Protect an IP Address?.....	135

16.1.1.2 What Objects Does WAF Protect?.....	135
16.1.1.3 Which OSs Does WAF Support?.....	135
16.1.1.4 Which Layers Does WAF Provide Protection At?.....	135
16.1.1.5 Does WAF Support File Caching?.....	135
16.1.1.6 About WAF Protection.....	136
16.1.1.7 Does WAF Support Two-Way SSL Authentication?.....	136
16.1.1.8 Does WAF Support Application Layer Protocol- and Content-Based Access Control?.....	137
16.1.1.9 Can WAF Check the Body I Add to a POST Request?.....	137
16.1.1.10 Can WAF Limit the Access Speed of a Domain Name?.....	137
16.1.1.11 Can WAF Block Data Packets in multipart/form-data Format?.....	137
16.1.1.12 Can a WAF Instance Be Deployed in the VPC?.....	137
16.1.1.13 Can WAF Block URL Requests That Contain Special Characters?.....	137
16.1.1.14 Can WAF Block Spam and Malicious User Registrations?.....	137
16.1.1.15 Can WAF Block Requests for Calling Other APIs from Web Pages?.....	138
16.1.1.16 Can I Configure Session Cookies in WAF?.....	138
16.1.1.17 Does WAF Block Customized POST Requests?.....	138
16.1.1.18 Can WAF Limit Access Through Domain Names?.....	139
16.1.1.19 Does WAF Have the IPS Module?.....	140
16.1.1.20 Which Web Service Framework Protocols Does WAF Support?.....	140
16.1.1.21 Can WAF Protect Websites Accessed Through HSTS or NTLM Authentication?.....	140
16.1.1.22 What Are the Differences Between WAF Forwarding and Nginx Forwarding?.....	140
16.1.1.23 Does WAF Cache Website Data?.....	141
16.1.1.24 Is WAF a Hardware Firewall or a Software Firewall?.....	141
16.1.1.25 Is There Any Impact on Origin Servers If I Enable HTTP/2 in WAF?.....	142
16.1.1.26 How Does WAF Detect SQL Injection and XSS Attacks?.....	142
16.1.1.27 Can WAF Defend Against the Apache Struts2 Remote Code Execution Vulnerability (CVE-2021-31805)?.....	143
16.1.1.28 Does a Dedicated WAF Instance Support Cross-VPC Protection?.....	143
16.1.2 WAF Usage.....	143
16.1.2.1 Why Does the Vulnerability Scanning Tool Report Disabled Non-standard Ports for My WAF-Protected Website?.....	143
16.1.2.2 Does WAF Affect Email Ports or Email Receiving and Sending?.....	143
16.1.2.3 How Do I Obtain the Real IP Address of a Web Visitor?.....	144
16.1.2.4 How Does WAF Block Requests?.....	144
16.1.2.5 What Are Local File Inclusion and Remote File Inclusion?.....	144
16.1.2.6 What Is the Difference Between QPS and the Number of Requests?.....	144
16.1.2.7 What Are Concurrent Requests?.....	145
16.1.2.8 Can WAF Block Requests When a Certificate Is Mounted on ELB?.....	145
16.1.2.9 Does WAF Affect My Existing Workloads and Server Running?.....	145
16.1.2.10 How Do I Configure My Server to Allow Only Requests from WAF?.....	145
16.1.2.11 Why Do Cookies Contain the <b>HWWAFSESID</b> or <b>HWWAFSESTIME</b> field?.....	146
16.1.2.12 How Do I Configure WAF If a Reverse Proxy Server Is Deployed for My Website?.....	146

16.1.2.13 How Does WAF Forward Access Requests When Both a Wildcard Domain Name and a Single Domain Name Are Connected to WAF?.....	146
16.1.2.14 Does WAF Affect Data Transmission from the Internal Network to an External Network?.....	146
16.1.2.15 Do I Need to Make Some Changes in WAF If the Security Group for Origin Server (Address) Is Changed?.....	147
16.2 Website Domain Name Access Configuration.....	147
16.2.1 Domain Name and Port Configuration.....	147
16.2.1.1 How Do I Add a Domain Name/IP Address to WAF?.....	147
16.2.1.2 Which Non-Standard Ports Does WAF Support?.....	148
16.2.1.3 Can WAF Protect Multiple Domain Names That Point to the Same Origin Server?.....	150
16.2.1.4 How Do I Configure Domain Names to Be Protected When Adding Domain Names?.....	150
16.2.1.5 Do I Have to Configure the Same Port as That of the Origin Server When Adding a Website to WAF?.....	151
16.2.1.6 What Can I Do If One of Ports on an Origin Server Does Not Require WAF Protection?.....	151
16.2.1.7 What Data Is Required for Connecting a Domain Name/IP Address to WAF?.....	151
16.2.1.8 How Do I Safely Delete a Protected Domain Name?.....	152
16.2.1.9 Can I Change the Domain Name That Has Been Added to WAF?.....	152
16.2.1.10 What Are the Precautions for Configuring Multiple Server Addresses for Backend Servers?.....	152
16.2.1.11 Does WAF Support Wildcard Domain Names?.....	152
16.2.1.12 Can I Configure Multiple Load Balancers for a Dedicated WAF Instance?.....	153
16.2.1.13 Why Am I Seeing the "Someone else has already added this domain name. Please confirm that the domain name belongs to you" Error Message?.....	153
16.2.2 Certificate Management.....	153
16.2.2.1 How Do I Select a Certificate When Configuring a Wildcard Domain Name?.....	153
16.2.2.2 Do I Need to Import the Certificates That Have Been Uploaded to ELB to WAF?.....	153
16.2.2.3 How Do I Convert a Certificate into PEM Format?.....	153
16.3 Service Interruption Check.....	154
16.3.1 How Do I Troubleshoot 404/502/504 Errors?.....	154
16.3.2 Why Is My Domain Name or IP Address Inaccessible?.....	158
16.3.3 How Do I Handle False Alarms as WAF Blocks Normal Requests to My Website?.....	160
16.3.4 Why Does WAF Block Normal Requests as Invalid Requests?.....	162
16.3.5 What Is the Connection Timeout Duration of WAF? Can I Manually Set the Timeout Duration?..	162
16.3.6 How Do I Solve the Problem of Excessive Redirection Times?.....	162
16.3.7 Why Are HTTPS Requests Denied on Some Mobile Phones?.....	163
16.3.8 How Do I Fix an Incomplete Certificate Chain?.....	163
16.3.9 Why Does My Certificate Not Match the Key?.....	167
16.3.10 Why Am I Seeing Error Code 418?.....	168
16.3.11 Why Am I Seeing Error Code 523?.....	168
16.3.12 Why Does the Website Login Page Continuously Refreshed After a Domain Name Is Connected to WAF?.....	168
16.3.13 Why Does the Requested Page Respond Slowly After the HTTP Forwarding Policy Is Configured?.....	168
16.3.14 How Can I Upload Files After the Website Is Connected to WAF?.....	169
16.3.15 Why Is the Bar Mitzvah Attack on SSL/TLS Detected?.....	169

16.4 Protection Rule Configuration.....	169
16.4.1 Basic Web Protection.....	169
16.4.1.1 How Do I Switch the Mode of Basic Web Protection from Log Only to Block?.....	169
16.4.1.2 Which Protection Levels Can Be Set for Basic Web Protection?.....	170
16.4.2 CC Attack Protection Rules.....	170
16.4.2.1 How Do I Configure a CC Attack Protection Rule?.....	170
16.4.2.2 When Is Cookie Used to Identify Users?.....	171
16.4.2.3 What Are the Differences Between <b>Rate Limit</b> and <b>Allowable Frequency</b> in a CC Rule?.....	171
16.4.3 Precise Protection rules.....	171
16.4.3.1 Can a Precise Protection Rule Take Effect in a Specified Period?.....	171
16.4.4 Anti-Crawler Protection.....	171
16.4.4.1 Why Are There No Protection Logs for Some Requests Blocked by WAF JavaScript Anti-Crawler Rules?.....	171
16.4.5 Others.....	172
16.4.5.1 In Which Situations Will the WAF Policies Fail?.....	172
16.4.5.2 Is the Path of a WAF Protection Rule Case-sensitive?.....	172
16.4.5.3 What Protection Rules Does WAF Support?.....	172
16.4.5.4 Which of the WAF Protection Rules Support the Log-Only Protective Action?.....	173
16.4.5.5 Why Does the Page Fail to Be Refreshed After WTP Is Enabled?.....	173
16.4.5.6 What Are the Differences Between Blacklist/Whitelist Rules and Precise Protection Rules on Blocking Access Requests from Specified IP Addresses?.....	174
16.4.5.7 What Do I Do If a Scanner, such as AppScan, Detects that the Cookie Is Missing Secure or HttpOnly?.....	175
<b>A Change History.....</b>	<b>176</b>

# 1 Service Overview

## 1.1 What Is 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).

After you enable a WAF instance, add your website domain to the WAF instance on the WAF console. All public network traffic for your website then goes to WAF first. WAF identifies and filters out the illegitimate traffic, and routes only the legitimate traffic to your origin server to ensure site security.

### How WAF Works

After applying for 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.

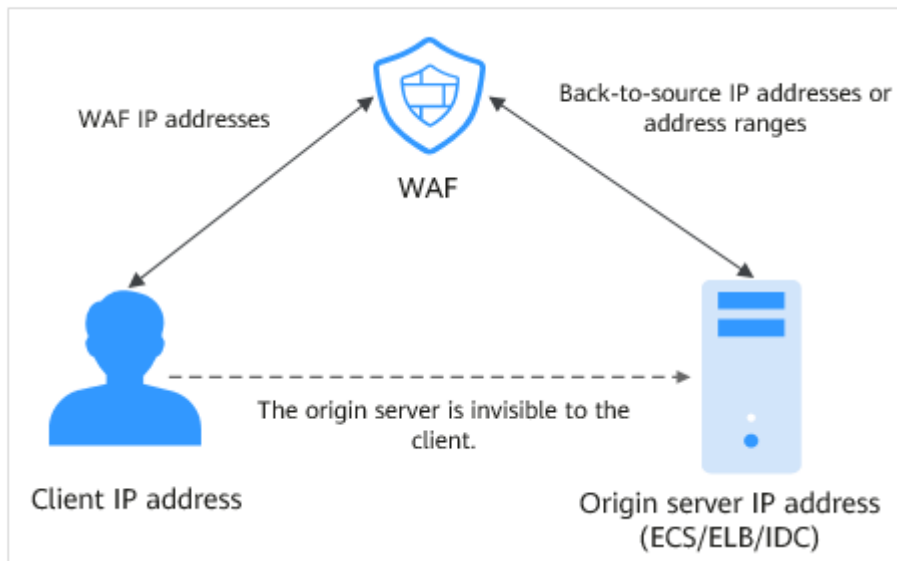
**Figure 1-1** How WAF protects a website



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



## What WAF Protects

Objects supported by WAF: domain names or IP addresses of web applications on the clouds or on-premises data centers

## 1.2 Product Specifications

WAF is deployed in dedicated mode. The following tables describe specifications and functions of the dedicated WAF instances.

### Dedicated Mode

**Table 1-1** describes dedicated WAF instances.

**Table 1-1** Dedicated mode description

Item	Description
Deployment mode	Dedicated WAF instances
Application scenarios	Service servers are deployed on the cloud. Suitable for large enterprise websites that have a large service scale and have customized security requirements.
Protection objects	Domain names or IP addresses

Item	Description
Advantages	<ul style="list-style-type: none"> <li>• Enable cloud and on-premises deployment.</li> <li>• Enable exclusive use of WAF instance.</li> <li>• Meet requirements for protection against large-scale traffic attacks.</li> <li>• Deploy dedicated WAF instances in a VPC to reduce network latency.</li> </ul>

## Service Scale

For more details, see [Table 1-2](#).

**Table 1-2** Applicable service scale

Service Metrics	Specifications
Peak rate of normal service requests	<p>The following lists the specifications of a single instance.</p> <ul style="list-style-type: none"> <li>• Specifications: WI-500. Referenced performance: <ul style="list-style-type: none"> <li>- HTTP services - Recommended QPS: 5,000. Maximum QPS: 10,000.</li> <li>- HTTPS services - Recommended QPS: 4,000. Maximum QPS: 8,000.</li> <li>- WebSocket service - Maximum concurrent connections: 5,000</li> <li>- Maximum WAF-to-server persistent connections: 60,000</li> </ul> </li> <li>• Specifications: WI-100. Referenced performance: <ul style="list-style-type: none"> <li>- HTTP services - Recommended QPS: 1,000. Maximum QPS: 2,000.</li> <li>- HTTPS services - Recommended QPS: 800. Maximum QPS: 1,600</li> <li>- WebSocket service - Maximum concurrent connections: 1,000</li> <li>- Maximum WAF-to-server persistent connections: 60,000</li> </ul> </li> </ul> <p><b>NOTICE</b> 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.</p>
Service bandwidth threshold	<ul style="list-style-type: none"> <li>• Specifications: WI-500. Referenced performance: Throughput: 500 Mbit/s</li> <li>• Specifications: WI-100. Referenced performance: Throughput: 100 Mbit/s</li> </ul>

Service Metrics	Specifications
Number of domain names	2,000 (Supports 2,000 top-level domain names)
Quantity of supported ports	<ul style="list-style-type: none"><li>• Standard ports: Unlimited</li><li>• Non-standard ports: Unlimited</li></ul>
Peak rate of CC attack protection	<ul style="list-style-type: none"><li>• Specifications: WI-500. Referenced performance: Maximum QPS: 20,000</li><li>• Specifications: WI-100. Referenced performance: Maximum QPS: 4,000</li></ul>
CC attack protection rules	100
Precise protection rules	100
Reference table rules	100
IP address blacklist and whitelist rules	1,000
Geolocation access control rules	100
Web tamper protection rules	100
Information leakage prevention rules	100
False Alarm Masking	1,000
Data masking rules	100

**NOTICE**

- The number of domains is the total number of top-level domain names (for example, example.com), single domain names/subdomain names (for example, www.example.com), and wildcard domain names (for example, \*.example.com).
- If a domain name maps to different ports, each port is considered to represent a different domain name. For example, **www.example.com:8080** and **www.example.com:8081** are counted towards your quota as two distinct domain names.



## 1.3 Functions

WAF helps you protect services from various web security risks. The following table lists the functions of WAF.

Function		Description
Service configuration	Protection for IP addresses and domain names (wildcard, top-level, and second-level domain names)	Objects supported by WAF: domain names or IP addresses of web applications on a cloud or on-premises data centers
	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 shell upload, 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 can check WebSocket and WebSockets requests, which is enabled by default.
	Non-standard port protection	In addition to standard ports 80 and 443, WAF also supports non-standard ports.

Function		Description
Web application security protection	<p>Basic Web Protection</p> <p><b>NOTE</b> If you set <b>Protective Action</b> to <b>Block</b>, you can use the known attack source function. It means that if WAF blocks malicious requests from a visitor, you can enable this function to let WAF block requests from the same visitor for a period of time.</p>	<p>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.</p> <ul style="list-style-type: none"> <li>● 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.</li> <li>● Web shell detection WAF protects against web shells from upload interface.</li> <li>● Precise identification <ul style="list-style-type: none"> <li>– WAF uses built-in semantic analysis engine and regex engine and supports configuring of blacklist/whitelist rules, which reduces false positives.</li> <li>– 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</li> </ul> </li> <li>● Deep inspection WAF 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.</li> <li>● Header detection WAF detects all header fields in the requests.</li> </ul>

Function		Description
	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 <b>NOTE</b> If you set <b>Protective Action to Block</b> , you can use the known attack source function. It means that if WAF blocks malicious requests from a visitor, you can enable this function to let WAF block requests from the same visitor for a period of time.	WAF allows you to customize protection rules by combining HTTP headers, cookies, URLs, request parameters, and client IP addresses.
	Blacklist and whitelist rules <b>NOTE</b> If you set <b>Protective Action to Block</b> , you can use the known attack source function. It means that if WAF blocks malicious requests from a visitor, WAF will proactively block requests from the same visitor for a period of time.	You can configure blacklist and whitelist rules to block, log only, or allow access requests from specified IP addresses.
	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	WAF dynamically analyzes your website service models and accurately identifies crawler behavior based on data risk control and bot identification systems.

Function		Description
	Information leakage prevention rules	<p>You can add two types of information leakage prevention rules.</p> <ul style="list-style-type: none"> <li>• Sensitive information filtering: prevents disclosure of sensitive information (such as ID numbers, phone numbers, and email addresses).</li> <li>• Response code interception: blocks the specified HTTP status codes.</li> </ul>
	Global protection whitelist (formerly false alarm masking) rules	This function ignores certain attack detection rules for specific requests.
	Data masking rules	Data masking prevents such data as passwords from being displayed in event logs.
Connection protection		<p>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.</p>
Configuring connection timeout		<ul style="list-style-type: none"> <li>• The default timeout period 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 page.</li> <li>• The default timeout duration for connections between WAF and your origin server is 60 seconds. You can customize a timeout duration on the WAF console.</li> </ul> <p>On the <b>Basic Information</b> page, enable <b>Timeout Settings</b> and click . Then, specify <b>WAF-to-Server connection timeout (s)</b>, <b>Read timeout (s)</b>, and <b>Write timeout (s)</b> and click  to save settings.</p>

Function	Description
Event management	<ul style="list-style-type: none"> <li>WAF allows you to view and handle false alarms for blocked or logged events.</li> <li>You can download events data over the past five days.</li> </ul>
GUI-based security data	<p>WAF provides a GUI-based interface for you to monitor attack information and event logs in real time.</p> <ul style="list-style-type: none"> <li><b>Centralized policy configuration</b> 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.</li> <li><b>Traffic and event statistics</b> WAF displays the number of requests, the number and types of security events, and log information in real time.</li> </ul>
High flexibility and reliability	<p>WAF can be deployed on multiple clusters in multiple regions based on the load balancing principle. This can prevent single points of failure (SPOFs) and ensure online smooth capacity expansion, maximizing service stability.</p>

## 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 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 1-3](#) provides the personal data collected and generated by WAF.

**Table 1-3** 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.

Type	Collection Method	Can Be Modified	Mandatory
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.

# 1.7 WAF Permissions Management

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 1-4** lists all the system roles supported by WAF.

**Table 1-4** System policies supported by WAF

Role/Policy Name	Description	Category	Dependencies
WAF Administrator	Administrator permissions for WAF	System-defined role	Dependent on the <b>Tenant Guest</b> and <b>Server Administrator</b> roles. <ul style="list-style-type: none"> <li>• <b>Tenant Guest:</b> A global role, which must be assigned in the global project.</li> <li>• <b>Server Administrator:</b> A project-level role, which must be assigned in the same project.</li> </ul>
WAF FullAccess	All permissions for WAF	System-defined policy	None.
WAF ReadOnlyAccess	Read-only permissions for WAF.	System-defined policy	

# 2 Overview

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.

## Website Service Review

Sort out all website services you want to protect with WAF. This helps you learn about your workloads and specific data of your workloads so that you can choose and configure appropriate protection policies.

**Table 2-1** Website services

Item	Description
<b>Website and Service Information</b>	
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. <b>NOTE</b> 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 locations where the requests originate from)	Determine the attack source and then set geolocation access control rules to block users from these locations.
Whether the service uses 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 you want to apply for the instance.
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 IP addresses.

Item	Description
Domain protocol	<p>Check whether WAF supports the communication protocol used by your site.</p> <p><b>NOTE</b> WAF can protect your website only when <b>Client Protocol</b> and <b>Server Protocol</b> are configured based on the real situation of your website.</p> <ul style="list-style-type: none"> <li>• <b>Client Protocol:</b> the protocol used by a client (for example, a browser) to access your website. You can select <b>HTTP</b> or <b>HTTPS</b>.</li> <li>• <b>Server Protocol:</b> the protocol used by WAF to forward requests from the client (such as a browser) to the origin server. You can select <b>HTTP</b> or <b>HTTPS</b>.</li> </ul>
Service port	<p>Check whether your service ports are within the port range supported by WAF.</p> <ul style="list-style-type: none"> <li>• Standard ports <ul style="list-style-type: none"> <li>– 80: default port when the client protocol is HTTP</li> <li>– 443: default port when the client protocol is HTTPS</li> </ul> </li> <li>• Non-standard ports Ports other than ports 80 and 443.</li> </ul>
Whether TLSv1.0 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.
<b>Services and Attacks</b>	
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.

Item	Description
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.

## How to Use WAF

[Table 2-2](#) describes the procedure to use WAF.

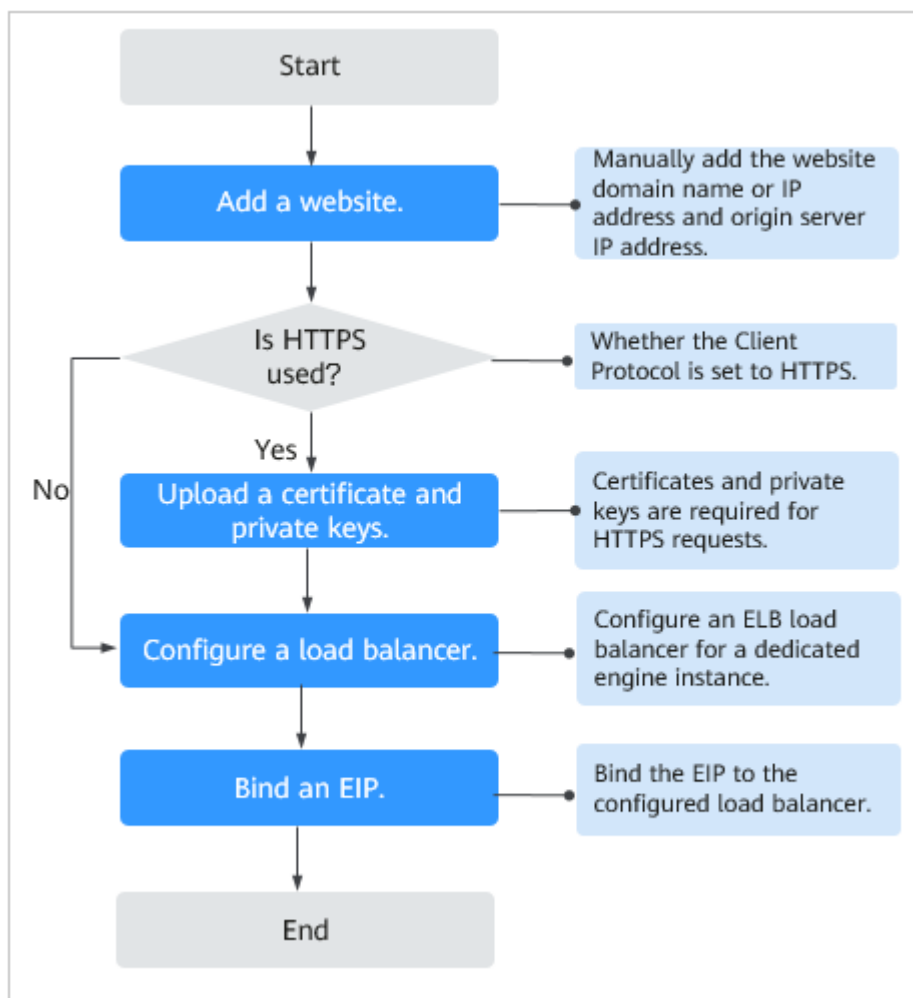
**Table 2-2** Procedure to use WAF

Step	Description
Applying for dedicated WAF instances	Apply for a dedicated WAF instance. For details, see <a href="#">Applying for a Dedicated WAF Engine</a> .
Adding a website to WAF	Add the website you want to protect to WAF. For details, see <a href="#">Step 1: Add a Website to WAF</a> .
Enabling WAF protection	Enable WAF protection to protect added website. <b>NOTE</b> <ul style="list-style-type: none"> <li>Using WAF does not affect your web server performance because the WAF engine is not running on your web server.</li> <li>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.</li> </ul>
Configuring protection rules	Use WAF built-in protection rules and configure custom rules to protect your website. For more details, see <a href="#">Rule Configuration</a> .
Handling false alarms	Mask blocked or logged events which are handled as false alarms. For more details, see <a href="#">Handling False Alarms</a> .

Step	Description
Viewing <b>Dashboard</b>	View protection data of yesterday, today, last 3 days, last 7 days, or last 30 days. For more details, see <a href="#">Dashboard</a> .

For details about how to connect your website to WAF, see [Figure 2-1](#).

**Figure 2-1** Flowchart of connecting a website to WAF





# 3 Applying for a Dedicated WAF Engine

---

If your service servers are deployed on the cloud, you can apply for dedicated WAF engines (or dedicated WAF instances) to protect important websites through domain names or 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.

## Precautions

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** under **Security**.
- Step 4** If you are a first-time user for dedicated WAF instances, click **Apply for Dedicated Engine Now** on the left of the page.

 **NOTE**

If you are not a first-time user for dedicated WAF instances, click **Create WAF** in the upper right corner of the page.

**Step 5** On the **Apply for Web Application Firewall** page, set WAF instance parameters by referring to [Table 3-1](#).

**Table 3-1** Parameters of a dedicated WAF instance

Parameter	Description
Billing Mode	Dedicated WAF instances are billed on a pay-per-use basis. You are billed for the required duration by the second, which starts when the instance is created and ends when the instance is deleted.
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	<b>ECS</b> Your WAF instance will be created on your ECS. You can view details of the ECS on the ECS console.
CPU Architecture	Select CPU specifications for your instance.
ECS Specifications	Select ECS specifications for your instance.
Estimated Final Specifications	Expected throughput for your reference.
VPC	Select the VPC to which the origin server belongs. <b>NOTICE</b> If you select a VPC that supports IPv6 and enable IPv6, the dedicated WAF instance supports IPv6 protection.
Subnet	Select a subnet configured in the VPC.

Parameter	Description
Security Group	<p>Select a security group in the region or click <b>Manage Security Group</b> 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.</p> <p><b>NOTICE</b></p> <ul style="list-style-type: none"> <li>• You can configure your security group as follows: <ul style="list-style-type: none"> <li>- 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 <b>TCP</b> and port <b>80</b>.</li> <li>- Outbound rules All outgoing network traffic is allowed by default.</li> </ul> </li> <li>• 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.</li> </ul>

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

**Step 7** Confirm the configuration and click **Apply Now**.

**Step 8** 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 successfully.

----End

# 4 Enabling WAF Protection

---

## 4.1 Ports Supported by WAF

**Table 4-1** lists the ports that can be protected by WAF.

**Table 4-1** Ports supported by WAF

Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
Standard ports	80	443	Unlimited

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, 8015, 8016, 8017, and 8070	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

## 4.2 Connecting a Website to WAF

### 4.2.1 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.

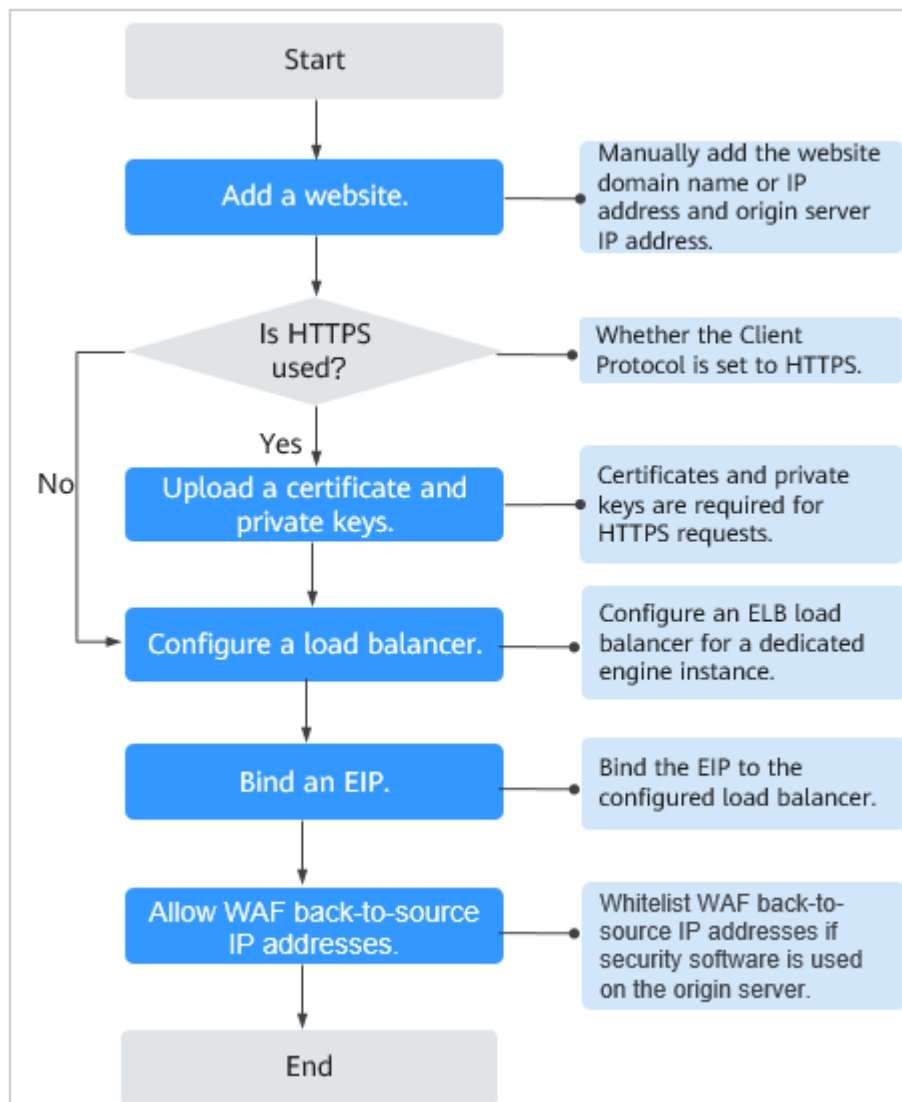
## Constraints

Dedicated WAF instances can only protect web applications and websites that are accessible through domain names or IP addresses.

## Processes of Connecting a Website to WAF

Before using a dedicated WAF instance, complete the required configurations by following the process shown in [Figure 4-1](#).

**Figure 4-1** Process of connecting a website to a dedicated WAF instance



## 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?](#)

## 4.2.2 Step 1: Add a Website to WAF

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.

### Prerequisites

You have applied for a dedicated WAF instance.

### Constraints

- An Internet-facing load balancer has been deployed on the website you want to protect with dedicated WAF instances.
- 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.

### Collecting Domain Name/IP Address Information

Before adding a domain name or IP address, obtain the information listed in [Table 4-2](#).


**Table 4-2** Domain name or IP address details required

Information	Parameter	Description	Example Value
Parameters	Domain Name	<ul style="list-style-type: none"><li>• 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.</li><li>• IP: IP address of the website.</li></ul>	www.example.com


Information	Parameter	Description	Example Value
	Protected Port	The service port corresponding to the domain name of the website you want to protect. <ul style="list-style-type: none"> <li>Standard ports <ul style="list-style-type: none"> <li>80: default port when the client protocol is set to HTTP</li> <li>443: default port when the client protocol is set to HTTPS</li> </ul> </li> <li>Non-standard ports Ports other than ports 80 and 443</li> </ul>	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 to the client (such as a browser). The options are <b>HTTP</b> and <b>HTTPS</b> .	HTTP
	VPC	Select the VPC that the dedicated WAF instance belongs to.	vpc-default
	Server Address	Private IP address of the website server that a client (for example, a browser) accesses.	192.168.1.1
(Optional) Certificate	Certificate Name	If you set <b>Client Protocol</b> to <b>HTTPS</b> , you are required to configure a certificate on WAF and associate the certificate with the domain name. <b>NOTICE</b> Only .pem certificates can be used in WAF. If a certificate is not in .pem, convert it by referring to <a href="#">How Do I Convert a Certificate into PEM Format?</a>	None

## Procedure

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

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



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

**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** Provide the domain name details.

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

 **NOTE**

- If the server IP address of each subdomain name is the same, enter a wildcard domain name to be protected. For example, if the subdomain names *a.example.com*, *b.example.com*, and *c.example.com* have the same server IP address, you can add the wildcard domain name *\*.example.com* to WAF to protect all three.
- If the server IP addresses of subdomain names are different, add subdomain names as single domain names one by one.
- **Website Remarks:** (Optional) You can provide remarks about your website if you want.

**Step 7** Configure the origin server. [Table 4-3](#) describes the parameters.

**Table 4-3** Parameter description

Parameter	Description	Example Value
Protected Port	Select the port type that you want WAF to protect from the drop-down list. To protect port 80 or 443, select <b>Standard port</b> from the drop-down list.	81

Parameter	Description	Example Value
Server Configuration	<p>Address of the web server. The configuration contains the <b>Client Protocol</b>, <b>Server protocol</b>, <b>VPC</b>, <b>Server Address</b>, and <b>Server Port</b>.</p> <ul style="list-style-type: none"> <li>• <b>Client Protocol</b>: protocol used by a client to access a server. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>• <b>Server Protocol</b>: protocol used by WAF to forward client requests. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>• <b>VPC</b>: Select the VPC to which the dedicated WAF instance belongs.</li> </ul> <p><b>NOTE</b> To implement active-active services and prevent single points of failure (SPOFs), it is recommended that at least two WAF instances be deployed in the same VPC.</p> <ul style="list-style-type: none"> <li>• <b>Server Address</b>: Private/internal IP address of the website server that a client (for example, a browser) accesses. The following IP address formats are supported: <ul style="list-style-type: none"> <li>- IPv4, for example, XX.XXX.1.1</li> <li>- IPv6, for example, fe80:0000:0000:0000:0000:0000:0000:0000</li> </ul> </li> <li>• <b>Server Port</b>: service port of the server to which the dedicated WAF instance forwards client requests.</li> </ul>	<p><b>Client Protocol:</b> <b>HTTP</b></p> <p><b>Server Protocol:</b> <b>HTTP</b></p> <p><b>Server Address:</b> XXX.XXX.1.1</p> <p><b>Server Port:</b> <b>80</b></p>
Certificate Name	<p>If you set <b>Client Protocol</b> to <b>HTTPS</b>, an SSL certificate is required.</p> <p>You can select an International certificate and/or Chinese certificate, or import a new certificate. For details about how to import a certificate, see <a href="#">Importing a New Certificate</a>.</p> <p><b>NOTICE</b></p> <ul style="list-style-type: none"> <li>• Only .pem certificates can be used in WAF. If the certificate is not in .pem format, convert it into .pem by referring to <a href="#">Importing a New Certificate</a> before uploading the certificate.</li> <li>• 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.</li> <li>• 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.</li> </ul>	--

**Step 8** Configure the advanced settings.

- **Proxy:** WAF security policies take effect for real client IP addresses where the requests initiate. To ensure that WAF obtains real client IP addresses, if your website has layer-7 proxy servers such as CDN and cloud acceleration products deployed in front of WAF, select **Yes** for **Proxy**.
- **Policy:** The **system-generated policy** is selected by default. You can select a policy you configured before. You can also customize rules after the domain name is connected to WAF.

System-generated policies include:

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

 **NOTE**

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

**Step 9** Click **OK**.

----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**.
  - If you select **Chinese** for **Type**, specify **Certificate Name**, and copy the signature certificate, signature private key, encryption certificate, and encryption private key to the corresponding text boxes.
  - If you select **International** for **Type**, specify **Certificate Name** and copy 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 4-4](#) before uploading it.

**Table 4-4** Certificate conversion commands

Format	Conversion Method
CER/CRT	Rename the <b>cert.crt</b> certificate file to <b>cert.pem</b> .
PFX	<ul style="list-style-type: none"> <li>Obtain a private key. For example, run the following command to convert <b>cert.pfx</b> into <b>key.pem</b>: <b>openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes</b></li> <li>Obtain a certificate. For example, run the following command to convert <b>cert.pfx</b> into <b>cert.pem</b>: <b>openssl pkcs12 -in cert.pfx -nokeys -out cert.pem</b></li> </ul>
P7B	<ol style="list-style-type: none"> <li>Convert a certificate. For example, run the following command to convert <b>cert.p7b</b> into <b>cert.cer</b>: <b>openssl pkcs7 -print_certs -in cert.p7b -out cert.cer</b></li> <li>Rename certificate file <b>cert.cer</b> to <b>cert.pem</b>.</li> </ol>
DER	<ul style="list-style-type: none"> <li>Obtain a private key. For example, run the following command to convert <b>privatekey.der</b> into <b>privatekey.pem</b>: <b>openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem</b></li> <li>Obtain a certificate. For example, run the following command to convert <b>cert.cer</b> into <b>cert.pem</b>: <b>openssl x509 -inform der -in cert.der -out cert.pem</b></li> </ul>

 **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**.

### 4.2.3 Step 2: Configure a Load Balancer

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.

## 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.

## 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** 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, click **Add Listener**, and configure the listener information.
- Step 6** Click **Next: Configure Request Routing Policy**.

---

### NOTICE

If you select **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**, add an ECS, and configure the health check.
- Step 8** Click **Next: Confirm**.
- Step 9** Click **Submit**.
- Step 10** Go to the page of the added listener, select the **Backend Server Groups** tab, and click **Add**.
- Step 11** In the **Add Backend Server** dialog box, select the dedicated WAF instance you have created.
- Step 12** Click **Next** and configure a port for the dedicated engine.

**NOTICE**

The listening port of the dedicated WAF instance must be the same as that configured in [Step 1: Add a Website to WAF](#). If you configure a standard port for the website, set the HTTP listening port to **80** and HTTPS listening port to **443**.

**Step 13** Click **Finish**.

----End

## Verification

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

## 4.2.4 Step 3: Bind an EIP to a Load Balancer


After you configure a load balancer for your dedicated WAF instance, you need to 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.


## 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 **Elastic Load Balancers** page, locate the row that contains the load balancer configured for the origin server. Then, in the **Operation** column, click **More >Unbind IPv4/6 EIP**.

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

**Step 6** On the **Load Balancers** page, locate the row that contains the load balancer configured for the dedicated WAF instance, click **More** in the **Operation** column, and select **Bind IPv4/6 EIP**.

**Step 7** In the **Bind EIP** dialog box, select the EIP unbound in [Step 4](#) and click **OK**.

----End

## 4.2.5 Step 4: Whitelist the Back-to-Source IP Addresses of Your 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 from being attacked even if the server IP address is exposed to hackers accidentally. 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. As a result, your website may become unavailable or respond very slowly. Therefore, ACL rules must be configured on the origin server to trust only the subnet IP addresses of your dedicated WAF instances.


### Prerequisites


Your website has been connected to your dedicated WAF instances.


### 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** 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 4-5](#).

**Table 4-5** Inbound rule parameters

Parameter	Description
Protocol & Port	Protocol and port for which the security group rule takes effect. If you select <b>TCP (Custom ports)</b> , 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 <a href="#">Step 5</a> . Configure an inbound rule for each IP address.  <b>NOTE</b> An inbound rule can contain only one IP address. To configure an inbound rule for each IP address, click <b>Add Rule</b> 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 address443
----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** 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 Website Domain Name Management



## 5.1 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.

### Prerequisites

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

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- Step 4** In the navigation pane on the left, choose **Website Settings**.
- Step 5** View the protected website lists. For details about parameters, see [Table 5-1](#).




**Table 5-1** Parameters



Parameter	Parameter
Domain Name	Protected domain name or IP address.
Deployment Mode	How your WAF instance is deployed for your website. Only <b>Dedicated mode</b> is available.
Last 3 Days	Protection status of the domain name over the past three days.

Parameter	Parameter
Mode	<p>WAF mode of the protected domain name. You can click ▼ to select one of the following protection modes:</p> <ul style="list-style-type: none"> <li>● <b>Enabled:</b> WAF is enabled.</li> <li>● <b>Suspended:</b> 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 <b>Suspended</b>. 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 (formerly false alarm masking) rules to reduce false alarms.</li> </ul>
Policy	<p>Number of types of WAF protection enabled for the domain name. You can click the number to go to the rule configuration page and configure specific protection rules. For details, see <a href="#">Rule Configuration</a>.</p>
Access Progress	<p>The progress of connecting your website to WAF or the website access status.</p> <ul style="list-style-type: none"> <li>● <b>Inaccessible:</b> The website has not been connected to WAF yet or failed to connect to WAF.</li> <li>● <b>Accessible:</b> The website has been connected to WAF.</li> </ul> <p><b>NOTICE</b> The initial <b>Access Status</b> of a website deployed in <b>Dedicated mode</b> is <b>Inaccessible</b>. When a request reaches your WAF instance, the access status automatically changes to <b>Accessible</b>.</p>
Operation	<p>To remove a protected website from WAF, click <b>Delete</b>.</p>

**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.

- Update the certificate: If you select **HTTPS** for **Client Protocol**, an SSL certificate is required. To update the certificate, click  next to the certificate name in the **International Certificate** or **Chinese Certificate** row. Then, in the displayed dialog box, upload a new certificate or select an existing certificate. For more details, see [Updating a Certificate](#).
- Update the TLS version and TLS cipher suite for accessing the origin server: If you select **HTTPS** for **Client Protocol**, you can change TLS version to a more secure one. To do so, click  next to the TLS Configuration field. Then, in the displayed dialog box, select the desired TLS version and TLS cipher suite. For more details, see [Configuring the Minimum TLS Version and Cipher Suite](#).
- Modify the field of **Proxy Configured**: Click . In the displayed dialog box, select **Yes** if your web server is using a proxy.

- Customize the alarm page: Click . In the displayed dialog box, select **Custom** or **Redirection** and complete required configurations. By default, **Alarm Page** is **Default**.
- If you want to set a timeout duration for each request, enable **Timeout Settings** and click  to specify **WAF-to-Server Connection Timeout (s)**, **Read Timeout (s)**, and **Write Timeout (s)**. This function cannot be disabled after being enabled. For details, see [Configuring Connection Timeout](#).

----End

## 5.2 Switching WAF Working Mode

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

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

### Procedure

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

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

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

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

**Step 5** In the row containing the domain name of the target website, click ▼ in the **Mode** column.

----End

## 5.3 Configuring the Minimum TLS Version and Cipher Suite

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.

### Prerequisites

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

### Application Scenarios

By default, the minimum TLS version configured for WAF is **TLS v1.0**. To ensure website security, configure the right TLS version for your service requirements. [Table 5-2](#) lists the recommended minimum TLS versions for different scenarios.

**Table 5-2** 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.

Scenario	Minimum TLS Version (Recommended)	Protection Effect
Client applications with no special security requirements	TLS v1.0	Requests using any TLS protocols can access the website.

The recommended cipher suite in WAF is **Cipher suite 1**. Cipher suite 1 offers a good mix of browser compatibility and security. For details about each cipher suite, see [Table 5-3](#).

**Table 5-3** Description of cipher suites

Cipher Suite Name	Supported cryptographic algorithms	Description
Default cipher suite	<ul style="list-style-type: none"> <li>• ECDHE-RSA-AES256-SHA384</li> <li>• AES256-SHA256</li> <li>• HIGH</li> <li>• !MD5</li> <li>• !aNULL</li> <li>• !eNULL</li> <li>• !NULL</li> <li>• !DH</li> <li>• !EDH</li> <li>• !AESGCM</li> </ul>	<ul style="list-style-type: none"> <li>• Compatibility: Good. A wide range of browsers are supported.</li> <li>• Security: Average</li> </ul>

Cipher Suite Name	Supported cryptographic algorithms	Description
Cipher suite 1	<ul style="list-style-type: none"> <li>● ECDHE-ECDSA-AES256-GCM-SHA384</li> <li>● HIGH</li> <li>● !MEDIUM</li> <li>● !LOW</li> <li>● !aNULL</li> <li>● !eNULL</li> <li>● !DES</li> <li>● !MD5</li> <li>● !PSK</li> <li>● !kRSA</li> <li>● !SRP</li> <li>● !3DES</li> <li>● !DSS</li> <li>● !EXP</li> <li>● !CAMELLIA</li> <li>● @STRENGTH</li> </ul>	<p>Recommended configuration.</p> <ul style="list-style-type: none"> <li>● Compatibility: Good. A wide range of browsers are supported.</li> <li>● Security: Good</li> </ul>
Cipher suite 2	<ul style="list-style-type: none"> <li>● ECDH+AESGCM</li> <li>● EDH+AESGCM</li> </ul>	<ul style="list-style-type: none"> <li>● 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.</li> <li>● Security: Excellent</li> </ul>
Cipher suite 3	<ul style="list-style-type: none"> <li>● ECDHE-RSA-AES128-GCM-SHA256</li> <li>● ECDHE-RSA-AES256-GCM-SHA384</li> <li>● ECDHE-RSA-AES256-SHA384</li> <li>● HIGH</li> <li>● !MD5</li> <li>● !aNULL</li> <li>● !eNULL</li> <li>● !NULL</li> <li>● !DH</li> <li>● !EDH</li> </ul>	<ul style="list-style-type: none"> <li>● Compatibility: Average. Earlier versions of browsers may be unable to access the website.</li> <li>● Security: Excellent. Multiple algorithms, such as ECDHE, DHE-GCM, and RSA-AES-GCM, are supported.</li> </ul>

Cipher Suite Name	Supported cryptographic algorithms	Description
Cipher suite 4	<ul style="list-style-type: none"> <li>• ECDHE-RSA-AES256-GCM-SHA384</li> <li>• ECDHE-RSA-AES128-GCM-SHA256</li> <li>• ECDHE-RSA-AES256-SHA384</li> <li>• AES256-SHA256</li> <li>• HIGH</li> <li>• !MD5</li> <li>• !aNULL</li> <li>• !eNULL</li> <li>• !NULL</li> <li>• !EDH</li> </ul>	<ul style="list-style-type: none"> <li>• Compatibility: Good. A wide range of browsers are supported.</li> <li>• Security: Average. The GCM algorithm is supported.</li> </ul>

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 5-4](#) 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 5-4** 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



Browser/Client	Default Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4
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
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

Browser/Client	Default Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4
Safari 6.0.4/OS X 10.8.4	Compatible	Compatible	Not compatible	Compatible	Compatible

## Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- Step 4** In the navigation pane on the left, choose **Website Settings**.
- Step 5** In the **Domain Name** column, click the domain name of the website to go to the basic information page.
- Step 6** In the **Compliance Certification** row, you can select **PCI DSS** or **PCI 3DS** to enable compliance check.
- Step 7** Click  next to the configured cipher suite in the **International Certificate** or **Chinese Certificate** row.
- Step 8** In the displayed **TLS Configuration** dialog box, specify the TLS version and cipher suite.
- If you select **International** for **Type**, 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.
  - If you select **Chinese** for **Type**, only TLS version **gmtls** and default cipher suite can be used.
- Step 9** Click **OK**.
- 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.

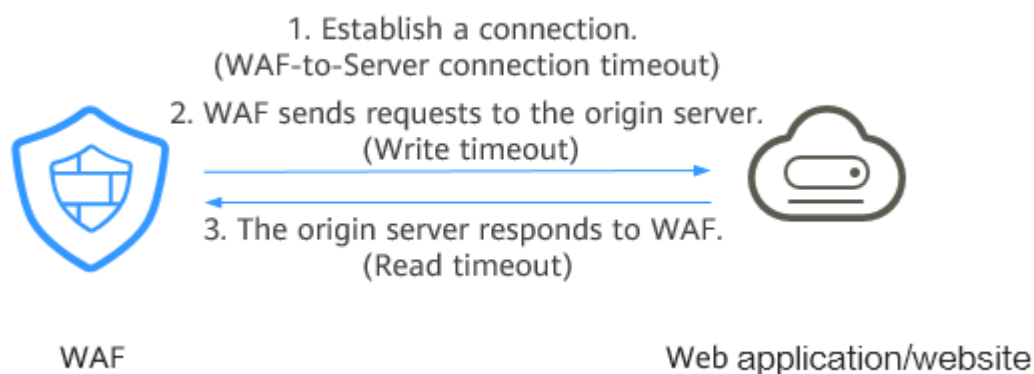
## 5.4 Configuring Connection Timeout

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 5-1** shows the three steps for WAF to forward requests to an origin server.

**Figure 5-1** WAF forwarding requests to origin servers.



### NOTE

- The timeout period 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 page.
- The default timeout duration for the connection between WAF and an origin server is 60 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 and choose **Web Application Firewall** under **Security**.

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

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

**Step 5** In the **Timeout Settings** row, click the **Status** toggle and enable it if needed.

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

----End

## 5.5 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.

### 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.
- The **dedicated WAF instance must be upgraded to the latest version** before you enable **Connection Protection**, or your website workloads may be interrupted.

### Procedure

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

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

- Step 3** In the navigation pane, choose **Website Settings**.
- Step 4** In the **Domain Name** column, click the domain name of the website to go to the basic information page.
- Step 5** In the **Connection Protection** area, click the status toggle to enable it.
- Step 6** Click  next to each parameter, edit **Breakdown Protection** and **Connection Protection** parameters to meet your requirements, and click  to save settings. [Table 5-5](#) describes these parameters.

**Table 5-5** Connection Protection parameters

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

Parameter		Description	Example Value
	Multiplier for Consecutive Breakdowns	<p>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.</p> <p>For example, assume that <b>Initial Downtime (s)</b> is set to 180s and <b>Multiplier for Consecutive Breakdowns</b> is set to 3.</p> <ul style="list-style-type: none"> <li>• If the breakdown is triggered for the second time, that is, less than 3, the protection duration is 360s (180s x 2).</li> <li>• 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).</li> <li>• When the accumulated downtime duration exceeds 1 hour (3,600s), the number of breakdowns are counted from 0.</li> </ul>	3
Connection Protection	Pending URL Request Threshold	Connection Protection is triggered when the number of read URL requests reaches the threshold you configure.	6,000
	Duration (s)	Protection duration. During this period, WAF stops forwarding client requests.	60

----End

## 5.6 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.

## 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** under **Security & Compliance**.

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

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

**Step 6** In the **International Certificate** or **Chinese Certificate** row, click  next to the certificate name. Then, in the displayed **Update Certificate** dialog box, import a new certificate or select an existing certificate.

- For international certificates, if **Import new certificate** is selected for **Update Method**, enter a certificate name and copy the certificate file and private key to the corresponding text boxes.
- For Chinese certificates, if **Import new certificate** is selected for **Update Method**, enter a certificate name and copy the signature certificate, signature

private key, encryption certificate, and encryption private key to the corresponding text boxes.

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

**Step 7** Click **Confirm**.

----End

## 5.7 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**.

### Prerequisites


The website to be protected has been added to WAF.


### Constraints

- If the IP address tag is configured, ensure that the protected website has a layer-7 proxy configured in front of WAF and that **Proxy Configured** is set to **Yes** for the protected website.  
If the IP address tag is not configured, WAF identifies the client IP address by default.
- Before enabling Cookie- or Params-based known attack source rules, configure a session or user tag for the corresponding website domain name.

### Procedure


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

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

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

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

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

**Step 6** In the **Traffic Identifier** area, click  next to **IP Tag**, **Session Tag**, or **User Tag** to configure a traffic identifier by referring to [Table 5-6](#).



**Table 5-6** Traffic identifier parameters

Tag	Description	Example Value
IP Tag	<p>HTTP request header field of the original client IP address.</p> <p>Ensure that the protected website has a layer-7 proxy configured in front of WAF and that <b>Proxy Configured</b> under the website basic information settings is set to <b>Yes</b> for this parameter to take effect.</p> <p>WAF obtains client IP addresses in the following sequence.</p> <ol style="list-style-type: none"><li>1. If an IP tag is configured, WAF firstly obtains the source IP header list configured in <b>upstream</b>. If no value is obtained, go to <a href="#">Step 6.2</a>.</li><li>2. WAF obtains the value of the <b>cdn-src-ip</b> field in the source IP header list configured in the config file. If no value is obtained, go to <a href="#">Step 6.3</a>.</li><li>3. WAF obtains the value of the <b>x-real-ip</b> field. If no value is obtained, go to <a href="#">Step 6.4</a>.</li><li>4. WAF obtains the first public IP address from the left of the <b>x-forwarded-for</b> field. If no public IP address is obtained, go to <a href="#">Step 6.5</a>.</li><li>5. WAF obtains the value of the <b>remote_addr</b> field, which includes the IP address used for establishing the TCP connection.</li></ol>	X-Forwarded-For

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

**Step 7** Click **Confirm**.

----End

## 5.8 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](#).

### Prerequisites


A website has been added to WAF.


### Impact on the System


Modifying the server configuration does not affect services.

### Procedure

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

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

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

- Step 4** In the navigation pane on the left, choose **Website Settings**.
- Step 5** In the **Domain Name** column, click the domain name of the website to go to the basic information page.
- Step 6** In the **Server Information** area, click .
- 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

## 5.9 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.



### 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** under **Security & Compliance**.
- Step 4** In the navigation pane on the left, choose **Website Settings**.
- Step 5** In the **Domain Name** column, click the domain name of the website to go to the basic information page.

- Step 6** Click  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

## 5.10 Removing a Protected Website from WAF

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

Before removing a website from WAF, go to your DNS provider and resolve your domain name to the IP address of the origin server, or the traffic to your domain name cannot be routed to the origin server.



### 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** under **Security & Compliance**.

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

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

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

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

# 6 Certificate Management

---

## 6.1 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.

You can upload a certificate to WAF. Then you can directly select the uploaded certificate for the protected website.

### Prerequisites

You have obtained the certificate file and certificate private key.

### Specification Limitations

You can upload as many certificates in WAF as the number of domain names that can be protected by your WAF instances in the same account.



### 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** under **Security**.

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

**Step 5** Click **Upload Certificate**.

- If you select **Chinese** for **Type**, specify **Certificate Name** and copy the signature certificate, signature private key, encryption certificate, and encryption private key to the corresponding text boxes.
- If you select **International** for **Type**, specify **Certificate Name** and copy 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 6-1](#) before uploading it.

**Table 6-1** Certificate conversion commands

Format	Conversion Method
CER/CRT	Rename the <b>cert.crt</b> certificate file to <b>cert.pem</b> .
PFX	<ul style="list-style-type: none"> <li>• Obtain a private key. For example, run the following command to convert <b>cert.pfx</b> into <b>key.pem</b>: <b>openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes</b></li> <li>• Obtain a certificate. For example, run the following command to convert <b>cert.pfx</b> into <b>cert.pem</b>: <b>openssl pkcs12 -in cert.pfx -nokeys -out cert.pem</b></li> </ul>
P7B	<ol style="list-style-type: none"> <li>1. Convert a certificate. For example, run the following command to convert <b>cert.p7b</b> into <b>cert.cer</b>: <b>openssl pkcs7 -print_certs -in cert.p7b -out cert.cer</b></li> <li>2. Rename certificate file <b>cert.cer</b> to <b>cert.pem</b>.</li> </ol>
DER	<ul style="list-style-type: none"> <li>• Obtain a private key. For example, run the following command to convert <b>privatekey.der</b> into <b>privatekey.pem</b>: <b>openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem</b></li> <li>• Obtain a certificate. For example, run the following command to convert <b>cert.cer</b> into <b>cert.pem</b>: <b>openssl x509 -inform der -in cert.der -out cert.pem</b></li> </ul>

 **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 6** Click **Confirm**.

----End

## Verification

The certificate you created is displayed in the certificate list.

## Other Operations

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

---

### NOTICE

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

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

## 6.2 Deleting a Certificate

This topic describes how to delete an expired or invalid certificate.

### Prerequisites

The certificate you want to delete is not bound to a protected website.

### Constraints


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


### Impact on the System

- Deleting certificates does not affect services.
- Deleted certificates cannot be recovered. Exercise caution when performing this operation.

### Procedure

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

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

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

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

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

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

----End




## Other Operations

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

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

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

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

----End

## 6.3 Viewing Certificate Information


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


### Prerequisites

You have created or pushed a certificate to WAF.

### Procedure

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

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

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

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

**Step 5** View the certificate information. [Table 6-2](#) describes the parameters.


**Table 6-2** Certificate parameters

Parameter	Description
Name	Certificate name.
Type	You can select <b>International</b> or <b>Chinese</b> certificates.

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 <a href="#">Updating a Certificate</a> .
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

## Other Operations

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

---

### NOTICE

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

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

# 7 Managing IP Address Blacklist and Whitelist Groups

---

## 7.1 Adding an IP Address Group

With IP address groups, you can quickly add IP addresses or IP address ranges to a blacklist or whitelist rule.



### Prerequisites

You have applied for a WAF instance.

### Constraints

Do not add the same IP address or IP address range to different IP address groups, or the IP address groups will fail to be 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  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Objects > Address Groups**.
- Step 5** Click the **My Address Groups** tab.
- Step 6** On the upper left of the address group list, click **Add Address Group**.
- Step 7** In the displayed **Add Address Group** dialog box, enter an address group name and provide IP address/IP ranges.

**Step 8** Click **OK**.

----End

## 7.2 Modifying or Deleting a Blacklist or Whitelist IP Address Group

This topic describes how to modify or delete an IP address group.

### Prerequisites


You have created an IP address group.


### Constraints

- Do not add an IP address or IP address range that has been added to a different IP address group to the existing address group, or the IP address group will fail to be modified.
- Only address groups not used by any rules can be deleted. Before you delete an address group that is being used by a blacklist or whitelist rule, remove the address group from the rule first.

### Procedure

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

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

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

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

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

**Table 7-1** Parameter description

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

**Step 6** Modify or delete an IP address group.

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

----End

# 8 Rule Configuration

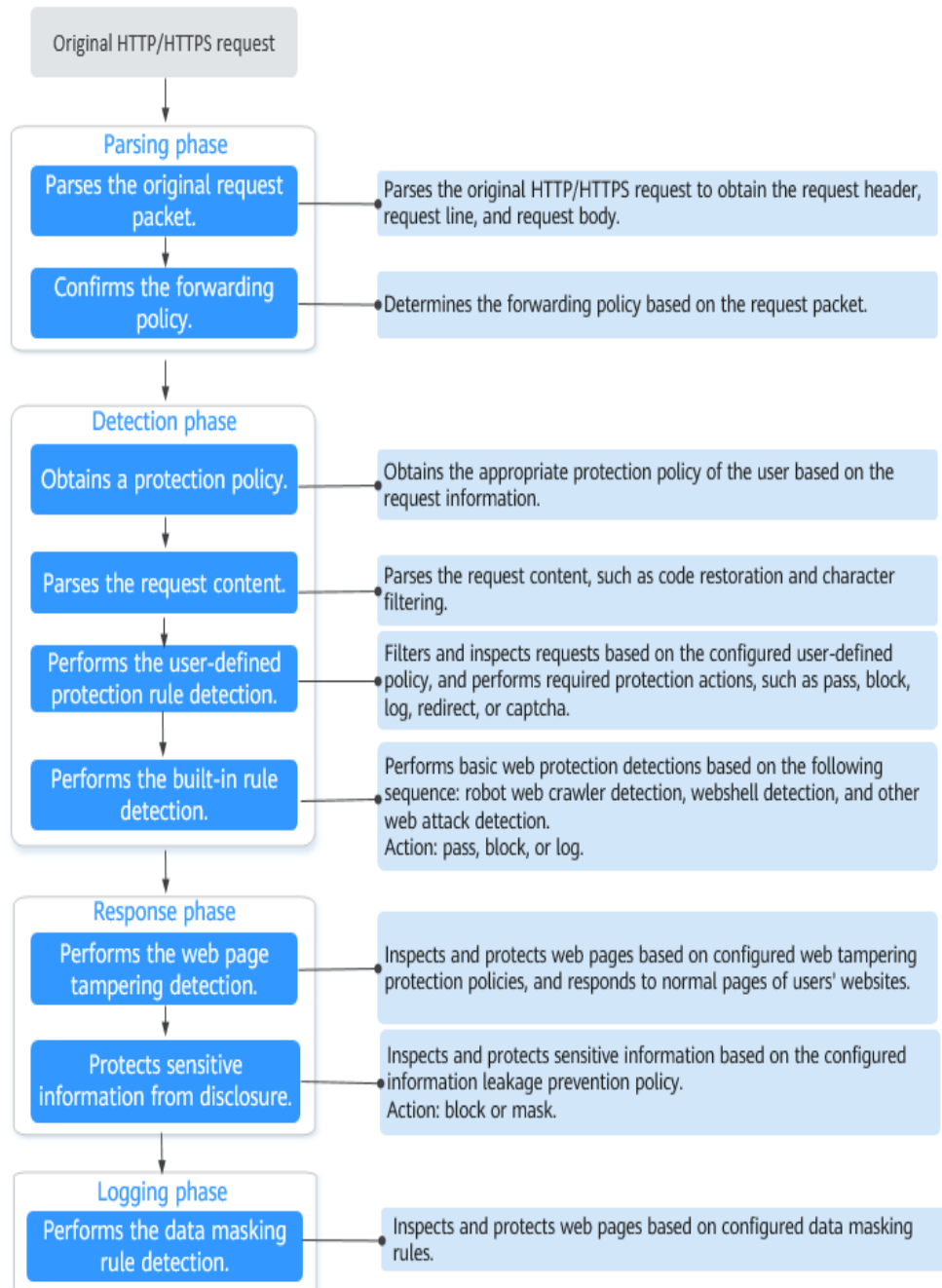
---

## 8.1 Configuration Guidance

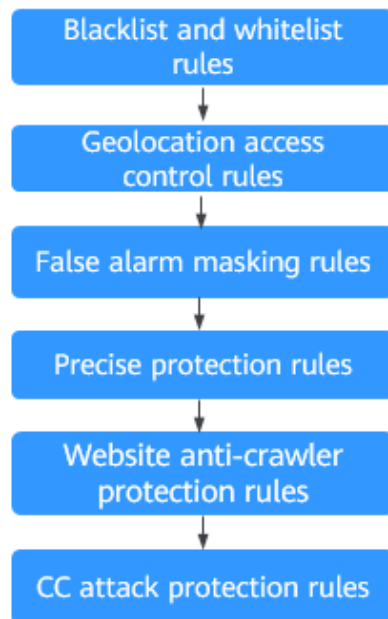
### How WAF Engine Works

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 8-1](#) shows how WAF engine built-in protection rules work. [Figure 8-2](#) shows the detection sequence of user-defined rules.

Figure 8-1 WAF engine detection process



**Figure 8-2** Priorities of custom protection rules



#### Response actions

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

## Protection Rule Configuration Methods

WAF provides the following customized configuration methods to simplify the configuration process. Select a proper configuration method to meet your service requirements.

### Method 1: Configuring protection rules for a single domain name

This method is recommended when you have few domain name services or have different configuration rules for domain name services.

#### NOTE

After a domain name is added to WAF, WAF automatically associates a protection policy with the domain name, and protection rules configured for the domain name are also added to the protection policy by default. If there are domain names applicable to the protection policy, you can directly add them to the policy. For details, see [Applying a Policy to Your Website](#).



- Where to configure
  - a. In the navigation pane, choose **Website Settings**.
  - b. In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.
- Protection rules you can configure on the rule configuration page

**Table 8-1** Configurable protection rules

Protection Rule	Description	Reference
Basic web protection rules	With an extensive reputation database, WAF defends against Open Web Application Security Project (OWASP) top 10 threats, and detects and blocks threats, such as malicious scanners, IP addresses, and web shells.	<a href="#">Configuring Basic Web Protection Rules</a>
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.	<a href="#">Configuring a CC Attack Protection Rule</a>
Precise protection rules	You can customize protection rules by combining HTTP headers, cookies, URLs, request parameters, and client IP addresses.	<a href="#">Configuring a Precise Protection Rule</a>
Blacklist and whitelist rules	You can configure blacklist and whitelist rules to block, log only, or allow access requests from specified IP addresses.	<a href="#">Configuring an IP Address Blacklist or Whitelist Rule</a>
Known attack source rules	These rules can block the IP addresses from which blocked malicious requests originate. These rules are dependent on other rules.	<a href="#">Configuring a Known Attack Source Rule</a>
Geolocation access control rules	You can customize these rules to allow or block requests from a specific country or region.	<a href="#">Configuring a Geolocation Access Control Rule</a>

Protection Rule	Description	Reference
Web tamper protection rules	You can configure these rules to prevent a static web page from being tampered with.	<a href="#">Configuring a Web Tamper Protection Rule</a>
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.	<a href="#">Configuring Anti-Crawler Rules</a>
Information leakage prevention rules	You can add two types of information leakage prevention rules. <ul style="list-style-type: none"> <li>• Sensitive information filtering: prevents disclosure of sensitive information (such as ID numbers, phone numbers, and email addresses).</li> <li>• Response code interception: blocks the specified HTTP status codes.</li> </ul>	<a href="#">Configuring an Information Leakage Prevention Rule</a>
Global protection whitelist (formerly false alarm masking) rules	You can configure these rules to let WAF ignore certain rules for specific requests.	<a href="#">Configuring a Global Protection Whitelist (Formerly False Alarm Masking) Rule</a>
Data masking rules	You can configure data masking rules to prevent sensitive data such as passwords from being displayed in event logs.	<a href="#">Configuring a Data Masking Rule</a>

### Method 2: Configuring protection rules for multiple domain names

This method is recommended if you have many domain name services and require the same protection policy for multiple domain names. This method greatly reduces repeated configuration workloads and improves the protection efficiency.

- Where to configure  
In the navigation pane on the left, choose **Policies**.
- Procedure
  - a. Add a policy. For details, see [Creating a Protection Policy](#).

- b. Configure protection rules. For details, see [Adding Rules to One or More Policies](#).
- c. Batch add multiple domain names to the policy. For details, see [Applying a Policy to Your Website](#).

## 8.2 Configuring Basic Web Protection Rules

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.



### NOTICE

Basic web protection has two modes: **Block** and **Log only**.



### Prerequisites

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

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- Step 4** In the navigation pane on the left, choose **Website Settings**.
- Step 5** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** page.
- Step 6** In the **Basic Web Protection** configuration area, change **Status** and **Mode** as needed by referring to [Table 8-2](#).

**Table 8-2** Parameter description

Parameter	Description
Status	Status of Basic Web Protection <ul style="list-style-type: none"> <li>•  : enabled.</li> <li>•  : disabled.</li> </ul>

Parameter	Description
Mode	<ul style="list-style-type: none"> <li>• <b>Block</b>: WAF blocks and logs detected attacks.</li> <li>• <b>Log only</b>: WAF only logs detected attacks.</li> </ul>

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

**Step 8** Enable protection types you need by referring to [Table 8-4](#).

1. 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 8-3** Protection levels

Protection Level	Description
Low	WAF only blocks the requests with obvious attack signatures. If a large number of false alarms are reported, <b>Low</b> is recommended.
Medium	The default level is <b>Medium</b> , 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 <b>High</b> .

2. Set the protection type.

---

**NOTICE**

By default, **General Check** is enabled. You can enable other protection types by referring to [Table 8-4](#).

---

**Table 8-4** 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. <b>NOTE</b> If you enable <b>General Check</b> , WAF checks your websites based on the built-in rules.
Webshell Detection	Protects against web shells from upload interface. <b>NOTE</b> If you enable <b>Webshell Detection</b> , 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. <b>NOTE</b> If you enable <b>Deep Inspection</b> , 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. <b>NOTE</b> 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 box of a browser 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](#).
  - 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.

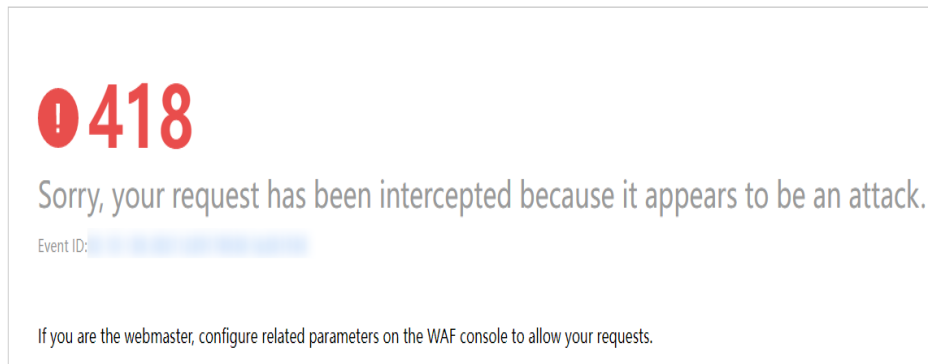
**Step 1** Enable **General Check** in **Basic Web Protection** and set the protection mode to **Block**.

**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 8-3](#) shows an example block page.

**Figure 8-3** Block page



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

----End

## 8.3 Configuring a CC Attack Protection Rule

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 Referrer, mitigating CC attacks. To make your custom CC attack protection rules take effect, ensure that you have enabled CC attack protection.

### Prerequisites



You have added the website you want to protect 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 your website is connected to both WAF and Content Delivery Network (CDN) and the **Protective Action** is set to **Verification code** in the CC attack protection rule, set **Path** to a dynamic page.

## Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- Step 4** In the navigation pane on the left, choose **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 **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 of the **CC Attack Protection** page, click **Add Rule**.
- Step 8** In the displayed dialog box, configure a CC attack protection rule by referring to [Table 8-5](#).

If a visitor whose cookie is **name** accesses a page on your website where the address includes **/admin** at the end (for example, <https://www.example.com/adminlogic>) more than 10 times within 60 seconds, WAF blocks the requests from visitors of the same cookie **name** for 600s and returns the page configured for **Page Content**.

**Table 8-5** Rule parameters

Parameter	Description	Example Value
Rate Limit Mode	<ul style="list-style-type: none"><li>● <b>Per IP address:</b> A website visitor is identified by the IP address.</li><li>● <b>Per user:</b> A website visitor is identified by the key value of <b>Cookie</b> or <b>Header</b>.</li><li>● <b>Other:</b> A website visitor is identified by the Referer field (user-defined request source).</li></ul> <p><b>NOTE</b></p> <p>If you set <b>Rate Limit Mode</b> to <b>Other</b>, set <b>Content</b> of <b>Referer</b> to a complete URL containing the domain name. The <b>Content</b> field supports prefix match and exact match only, but cannot contain two or more consecutive slashes, for example, <b>///admin</b>. If you enter <b>///admin</b>, WAF will convert it to <b>/admin</b>.</p> <p>For example, if <b>Path</b> is <b>/admin</b>, and you do not want visitors to access the page from <b>www.test.com</b>, set <b>Content</b> of <b>Referer</b> to <b>http://www.test.com</b>.</p>	<b>Per user</b>



Parameter	Description	Example Value
Trigger	<p>Click <b>Add</b> 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.</p> <ul style="list-style-type: none"> <li>• <b>Field:</b> The options are <b>Path, IP, Cookie, Header,</b> and <b>Params.</b></li> <li>• <b>Subfield:</b> Configure this field only when <b>Cookie, Header,</b> or <b>Params</b> is selected for <b>Field.</b></li> </ul> <p><b>NOTICE</b> The length of a subfield cannot exceed 2048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.</p> <ul style="list-style-type: none"> <li>• <b>Logic:</b> Select a logical relationship from the drop-down list.</li> </ul> <p><b>NOTE</b> If you set <b>Logic</b> to <b>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,</b> or <b>Suffix is not any of them,</b> select an existing reference table. For details, see <a href="#">Adding a Reference Table</a>.</p> <ul style="list-style-type: none"> <li>• <b>Content:</b> Enter or select the content that matches the condition.</li> </ul>	<p><b>Path Include /admin</b></p>
User Identifier	<p>This parameter is mandatory when you select <b>Per user</b> for <b>Rate Limit Mode.</b></p> <ul style="list-style-type: none"> <li>• <b>Cookie:</b> 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 <b>name</b> field in the cookie to uniquely identify a website visitor, select <b>name.</b></li> <li>• <b>Header:</b> 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.</li> </ul>	<p>name</p>

Parameter	Description	Example Value
Rate Limit	The number of requests allowed from a website visitor in the rate limit period. If the number of requests exceeds the rate limit, WAF takes the action you configure for <b>Protective Action</b> .	<b>10</b> requests allowed in <b>60</b> seconds
Protective Action	The action that WAF will take if the number of requests exceeds <b>Rate Limit</b> you configured. The options are as follows: <ul style="list-style-type: none"> <li>• <b>Verification code:</b> WAF allows requests that trigger the rule as long as your website visitors complete the required verification.</li> <li>• <b>Block:</b> WAF blocks requests that trigger the rule.</li> <li>• <b>Block dynamically:</b> WAF blocks requests that trigger the rule based on <b>Allowable Frequency</b>, which you configure after the first rate limit period is over.</li> <li>• <b>Log only:</b> WAF only logs requests that trigger the rule. You can <a href="#">download event data</a> and view the protection logs of a specific domain name.</li> </ul>	<b>Block</b>
Allowable Frequency	This parameter can be set if you select <b>Block dynamically</b> for <b>Protective Action</b> . WAF blocks requests that trigger the rule based on <b>Rate Limit</b> first. Then, in the following rate limit period, WAF blocks requests that trigger the rule based on <b>Allowable Frequency</b> you configure. <b>Allowable Frequency</b> cannot be larger than <b>Rate Limit</b> . <b>NOTE</b> If you set <b>Allowable Frequency</b> to <b>0</b> , WAF blocks all requests that trigger the rule in the next rate limit period.	<b>8</b> requests allowed in <b>60</b> seconds
Block Duration	Period of time for which to block the item when you set <b>Protective Action</b> to <b>Block</b> .	<b>600</b> seconds

Parameter	Description	Example Value
Block Page	The page displayed if the maximum number of requests has been reached. This parameter is configured only when <b>Protective Action</b> is set to <b>Block</b> . <ul style="list-style-type: none"> <li>If you select <b>Default settings</b>, the default block page is displayed.</li> <li>If you select <b>Custom</b>, a custom error message is displayed.</li> </ul>	<b>Custom</b>
Block Page Type	If you select <b>Custom</b> for <b>Block Page</b> , select a type of block page. The options are: <ul style="list-style-type: none"> <li><b>application/json</b></li> <li><b>text/html</b></li> <li><b>text/xml</b></li> </ul>	<b>text/html</b>
Page Content	If you select <b>Custom</b> for <b>Block Page</b> , configure the content to be returned.	Page content styles corresponding to different page types are as follows: <ul style="list-style-type: none"> <li><b>text/html:</b> &lt;html&gt;&lt;body&gt;Forbidden&lt;/body&gt;&lt;/html&gt;</li> <li><b>application/json:</b> {"msg": "Forbidden"}</li> <li><b>text/xml:</b> &lt;?xml version="1.0" encoding="utf-8"?&gt;&lt;error&gt;&lt;msg&gt;Forbidden&lt;/msg&gt;&lt;/error&gt;</li> </ul>
Rule Description	A description of the rule. This parameter is optional.	None

**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, to verify WAF is protecting your website (**www.example.com**) against the configured CC attack protection rule:

- Step 1** Clear the browser cache and enter the domain name in the address box of a browser 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](#).
  - If the website is accessible, go to [Step 2](#).
- Step 2** Clear the browser cache, enter **http://www.example.com/admin** in the address bar, and refresh the page 10 times within 60 seconds. In normal cases, the custom block page will be displayed the eleventh time you refresh the page, and the requested page will be accessible when you refresh the page 600 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 for 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|

OK



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

----End

## 8.4 Configuring a Precise Protection Rule

WAF allows you to customize protection rules by combining HTTP headers, cookies, URLs, request parameters, and client IP addresses.

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.

### Prerequisites

You have added the website you want to protect 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 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](#). WAF will block requests matching the configured IP address, Cookie, or Params for a length of time configured as part of the rule.


### Application Scenarios

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

### Procedure

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

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

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

**Step 4** In the navigation pane on the left, choose **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 **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** Click **Add Rule**.

**Step 9** In the displayed dialog box, add a rule by referring to [Table 8-6](#).

**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**.

If a visitor tries to access a URL containing **/admin**, WAF will block the request.

**Table 8-6** Rule parameters

Parameter	Description	Example Value
Protective Action	You can select <b>Block</b> , <b>Allow</b> , or <b>Log only</b> . Default value: <b>Block</b>	<b>Block</b>
Known Attack Source	If you set <b>Protective Action</b> to <b>Block</b> , you can select a blocking type for a known attack source rule. Then, WAF blocks requests matching the configured <b>IP</b> , <b>Cookie</b> , or <b>Params</b> for a length of time that depends on the selected blocking type.	<b>Long-term IP address blocking</b>
Effective Date	Select <b>Immediate</b> to enable the rule immediately, or select <b>Custom</b> to configure when you wish the rule to be enabled.	<b>Immediate</b>

Parameter	Description	Example Value
Condition List	<p>Click <b>Add</b> 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:</p> <p>Parameters for configuring a condition are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>Field</b></li> <li>• <b>Subfield:</b> Configure this field only when <b>IP</b>, <b>Params</b>, <b>Cookie</b>, or <b>Header</b> is selected for <b>Field</b>.</li> </ul> <p><b>NOTICE</b> The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.</p> <ul style="list-style-type: none"> <li>• <b>Logic:</b> Select a logical relationship from the drop-down list.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- If <b>Include any value</b>, <b>Exclude any value</b>, <b>Equal to any value</b>, <b>Not equal to any value</b>, <b>Prefix is any value</b>, <b>Prefix is not any of them</b>, <b>Suffix is any value</b>, or <b>Suffix is not any of them</b> is selected, select an existing reference table in the <b>Content</b> drop-down list. For details, see <a href="#">Adding a Reference Table</a>.</li> <li>- <b>Exclude any value</b>, <b>Not equal to any value</b>, <b>Prefix is not any of them</b>, and <b>Suffix is not any of them</b> 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 <b>Path</b> field is set to <b>Exclude any value</b> and the <b>test</b> reference table is selected. If <i>test1</i>, <i>test2</i>, and <i>test3</i> are set in the <b>test</b> reference table, WAF performs the protection action when the path of the access request does not contain <i>test1</i>, <i>test2</i>, or <i>test3</i>.</li> </ul> <ul style="list-style-type: none"> <li>• <b>Content:</b> Enter or select the content of condition matching.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Path Include /admin</b></li> <li>• <b>User Agent Prefix is not mozilla/5.0</b></li> <li>• <b>IP Equal to 192.168.2.3</b></li> <li>• <b>Cookie key1 Prefix is not jsessionid</b></li> </ul>

Parameter	Description	Example Value
	<b>NOTE</b> For more details about the configurations in general, see <a href="#">Table 8-7</a> .	
Priority	Rule priority. If you have added multiple rules, rules are matched by priority. The smaller the value you set, the higher the priority.	5
Rule Description	A brief description of the rule. This parameter is optional.	None

**Table 8-7** Condition list configurations

Field	Subfield	Logic	Example Content
<b>Path:</b> 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 / <b>admin</b> , <b>Path</b> must be set to / <b>admin</b> .	None	Select a logical relationship from the drop-down list.	<b>/buy/phone/</b> <b>NOTICE</b> If <b>Path</b> is set to /, all paths of the website are protected.
<b>User Agent:</b> A user agent of the scanner to be checked.	None		<b>Mozilla/5.0 (Windows NT 6.1)</b>
<b>IP:</b> An IP address of the visitor for the protection.	--		XXX.XXX.1.1
<b>Params:</b> A request parameter.	<ul style="list-style-type: none"> <li>● All fields</li> <li>● Any subfield</li> <li>● Custom</li> </ul>		<b>201901150929</b>



Field	Subfield	Logic	Example Content
<p><b>Referer:</b> A user-defined request resource.</p> <p>For example, if the protected path is / <b>admin/xxx</b> and you do not want visitors to access the page from <b>www.test.com</b>, set <b>Content</b> to <b>http://www.test.com</b>.</p>	--		http:// www.test.com
<p><b>Cookie:</b> A small piece of data to identify web visitors.</p>	<ul style="list-style-type: none"> <li>• All fields</li> <li>• Any subfield</li> <li>• Custom</li> </ul>		jsessionId
<p><b>Header:</b> A user-defined HTTP header.</p>	<ul style="list-style-type: none"> <li>• All fields</li> <li>• Any subfield</li> <li>• Custom</li> </ul>		text/ html,application/ xhtml +xml,application / xml;q=0.9,image/ webp,image/ png,*/*;q=0.8
<p><b>Method:</b> the user-defined request method.</p>	None		GET, POST, PUT, DELETE, and PATCH
<p><b>Request Line:</b> Length of a user-defined request line.</p>	None		50

Field	Subfield	Logic	Example Content
<b>Request:</b> Length of a user-defined request. It includes the request header, request line, and request body.	None		None
<b>Protocol:</b> the protocol of the request.	None		http

**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](#).
- 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 - Allowing a Specified IP Address to Access Your Website

You can configure two precise protection rules, one to block all requests, but then another one to allow the access from a specific IP address.

## 8.5 Adding a Reference Table



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.

Reference tables can be used by CC attack protection 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.

### Prerequisites

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

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- Step 4** In the navigation pane on the left, choose **Website Settings**.
- Step 5** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** 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 8-8](#).

**Table 8-8** Parameter description

Parameter	Description	Example Value
Name	Table name you entered	test

Parameter	Description	Example Value
Type	<ul style="list-style-type: none"> <li>• <b>Path:</b> A URL to be protected, excluding a domain name</li> <li>• <b>User Agent:</b> A user agent of the scanner to be protected</li> <li>• <b>IP:</b> An IP address of the visitor to be protected.</li> <li>• <b>Params:</b> A request parameter to be protected</li> <li>• <b>Cookie:</b> A small piece of data to identify web visitors</li> <li>• <b>Referer:</b> A user-defined request resource For example, if the protected path is /<b>admin/xxx</b> and you do not want visitors to be able to access it from <i>www.test.com</i>, set <b>Value</b> to <b>http://www.test.com</b>.</li> <li>• <b>Header:</b> A user-defined HTTP header</li> </ul>	Path
Value	Value of the corresponding <b>Type</b> . Wildcards are not allowed.  <b>NOTE</b> Click <b>Add</b> to add more than one value.	/buy/phone/

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

----End

### Other Operations

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

## 8.6 Configuring an IP Address Blacklist or Whitelist Rule

You can configure blacklist and whitelist rules to block, log only, or allow access requests from specific IP addresses or IP address ranges. You can add a single IP address or import an IP address group to the blacklist or whitelist.

## Prerequisites

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

## 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.
- If you configure **Protective Action** to **Block** for a blacklist or whitelist rule, you can configure a known attack source rule by referring to [Configuring 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.


## Impact on the System

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

## Procedure

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

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

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

**Step 4** In the navigation pane on the left, choose **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 **Blacklist and Whitelist** configuration area, change **Status** as needed and click **Customize Rule**.

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

**Step 8** In the displayed dialog box, specify the parameters by referring to [Table 8-9](#).

### 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 8-9** Rule parameters

Parameter	Description	Example Value
Rule Name	Rule name you entered.	WAF
IP Address/ Range/Group	You can select <b>IP address/Range</b> or <b>Address Group</b> to add IP addresses a blacklist or whitelist rule.	IP Address/Range
IP Address/ Range	This parameter is mandatory if you select <b>IP address/range</b> for <b>IP Address/Range/Group</b> . IP addresses or IP address ranges are supported. <ul style="list-style-type: none"> <li>• IP address: IP address to be added to the blacklist or whitelist</li> <li>• IP address range: IP address and subnet mask defining a network segment</li> </ul>	XXX.XXX.2.3
Select Address Group	This parameter is mandatory if you select <b>Address group</b> for <b>IP Address/Range/Group</b> . Select an IP address group from the drop-down list. You can also click <b>Add Address Group</b> to create an address group. For details, see <a href="#">Adding an IP Address Group</a> .	groupwaf

Parameter	Description	Example Value
Protective Action	<ul style="list-style-type: none"> <li>• <b>Block:</b> Select <b>Block</b> if you want to blacklist an IP address or IP address range.</li> <li>• <b>Allow:</b> Select <b>Allow</b> if you want to whitelist an IP address or IP address range.</li> <li>• <b>Log only:</b> Select <b>Log only</b> 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 <b>events data</b>.</li> </ul>	Block
Known Attack Source	If you select <b>Block</b> for <b>Protective Action</b> , 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

## Example Configuration - Allowing a Specified IP Addresses

To allow three IP addresses but block others:

**Configure a block rule** to block all requests, and then whitelist the three IP addresses.

## 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](#).
  - 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

## 8.7 Configuring a Known Attack Source Rule

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.

### Prerequisites

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

### Constraints



- For a known attack source rule to take effect, it must be enabled when you configure basic web protection, precise protection, blacklist, or whitelist protection rules.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- Before adding a known attack source rule for malicious requests blocked by Cookie or Params, a traffic identifier must be configured for the corresponding domain name. For more details, see [Configuring a Traffic Identifier for a Known Attack Source](#).



## Specification Limitations

- You can configure up to six blocking types. Each type can have one known attack source rule configured.
- The maximum time an IP address can be blocked for is 30 minutes.

## Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- Step 4** In the navigation pane on the left, choose **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 **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 of 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 8-10](#).

**Table 8-10** Known attack source parameters

Parameter	Description	Example Value
Blocking Type	Specifies the blocking type. The options are: <ul style="list-style-type: none"> <li>• <b>Long-term IP address blocking</b></li> <li>• <b>Short-term IP address blocking</b></li> <li>• <b>Long-term Cookie blocking</b></li> <li>• <b>Short-term Cookie blocking</b></li> <li>• <b>Long-term Params blocking</b></li> <li>• <b>Short-term Params blocking</b></li> </ul>	<b>Long-term IP address blocking</b>
Blocking Duration (s)	The blocking duration must be an integer and range from: <ul style="list-style-type: none"> <li>• (300, 1800] for long-term blocking</li> <li>• (0, 300] for short-term blocking</li> </ul>	500

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

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

----End

## Other Operations

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

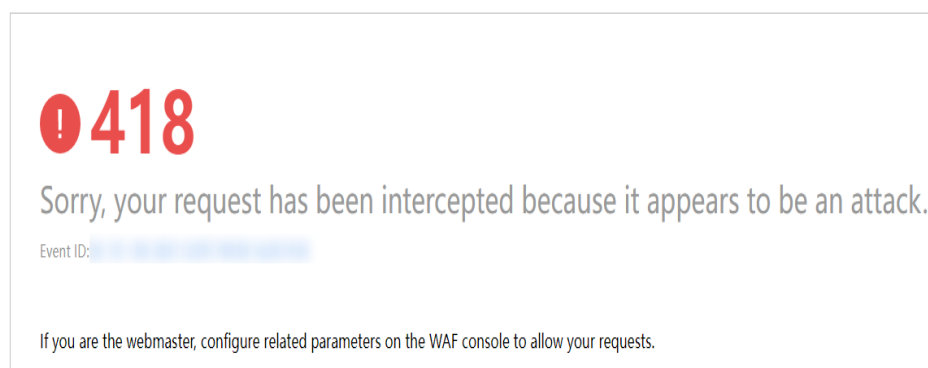
## Configuration Example - Blocking Known Attack Source Identified by Cookie

Assume that domain name *www.example.com* has been connected to WAF and a visitor has sent one or more malicious requests through IP address *XXX.XXX.248.195*. You want to block access requests from this IP address and whose cookie is **jsessionid** for 10 minutes. Refer to the following steps to configure a rule and verify its effect.

- Step 1** On the **Website Settings** page, click *www.example.com* to go to its basic information page.
- Step 2** In the **Traffic Identifier** area, configure the cookie in the **Session Tag** field.
- 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 8-4** Block page



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

----End

## 8.8 Configuring a Geolocation Access Control Rule

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.

### Prerequisites


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


### Constraints

- One region can be configured in only one geolocation access control rule.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.

### Procedure

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

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

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

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

**Step 5** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** 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 of the **Geolocation Access Control** page, click **Add Rule**.

**Step 8** In the displayed dialog box, add a geolocation access control rule by referring to [Table 8-11](#).

**Table 8-11** Rule parameters

Parameter	Description	Example Value
Rule Name	Rule name you configured	dlfw

Parameter	Description	Example Value
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 <b>Block</b> , <b>Allow</b> , or <b>Log only</b> .	<b>Block</b>

**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 box of a browser 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](#).
- 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

## 8.9 Configuring a Web Tamper Protection Rule

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

### How It Works

- Return directly the cached web page to the normal web visitor to accelerate request response.

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

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

## Prerequisites

You have added the website you want to protect 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.
- 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** under **Security & Compliance**.

**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 **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 of the **Web Tamper Protection** page, click **Add Rule**.

**Step 8** In the displayed dialog box, specify the parameters by referring to [Table 8-12](#).

**Table 8-12** Rule parameters

Parameter	Description	Example Value
Domain Name	Domain name of the website to be protected	<b>www.example.com</b>
Path	<p>A part of the URL, not including the domain name</p> <p>A URL is used to define the address of a web page. The basic URL format is as follows:</p> <p>Protocol name://Domain name or IP address[:Port]/[Path/.../File name].</p> <p>For example, if the URL is <b>http://www.example.com/admin</b>, set <b>Path</b> to <b>/admin</b>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>The path does not support regular expressions.</li> <li>The path cannot contain two or more consecutive slashes. For example, <b>///admin</b>. If you enter <b>///admin</b>, WAF converts <b>///</b> to <b>/</b>.</li> </ul>	<b>/admin</b>
Rule Description	A brief description of the rule. This parameter is optional.	None

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

----End

## Other Operations

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

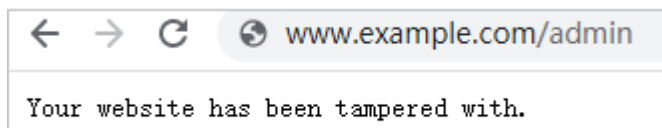
## Configuration Example - Static Web Page Tamper Prevention

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

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

A tampered page is returned.

**Figure 8-5** A static page that has been tampered with



**Step 2** Add a web tamper prevention rule to WAF.

**Step 3** Enabling 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

## 8.10 Configuring Anti-Crawler Rules

You can configure website anti-crawler protection rules to defend against crawlers such as search engines, scanners, script tools, and other crawlers.

### Prerequisites


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


### Constraints

- Cookies must be enabled and JavaScript supported by any browser used to access a website protected by anti-crawler 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.
- If your service is connected to CDN, exercise caution when using this function. CDN caching may impact Anti-Crawler performance and page accessibility.

### Procedure

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

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

- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- Step 4** In the navigation pane on the left, choose **Website Settings**.
- Step 5** In the **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, enable anti-crawler using the toggle on the right. If you enable this function, click **Configure Bot Mitigation**.
- Step 7** Select the **Feature Library** tab and enable the protection by referring to [Table 8-13](#).

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 8-13** 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.  <b>NOTE</b> If <b>Search Engine</b> 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.



Type	Description	Remarks
Script Tool	This rule is used to block script tools. A script tool is often used to execute automatic tasks and program scripts, such as HttpClient, OkHttp, and Python programs.	If you enable this rule, WAF detects and blocks the execution of automatic tasks and program scripts. <b>NOTE</b> If your application uses scripts such as HttpClient, OkHttp, and Python, disable <b>Script Tool</b> . 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. <b>NOTE</b> 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.

----End

## 8.11 Configuring an Information Leakage Prevention Rule

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.

### Prerequisites



You have added the website you want to protect 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.

### Procedure

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

- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- Step 4** In the navigation pane on the left, choose **Website Settings**.
- Step 5** In the **Policy** column of the row containing the domain name, click the number to go to the **Policies** 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 of the **Information Leakage Prevention** page, click **Add Rule**.
- Step 8** In the dialog box displayed, add an information leakage prevention rule by referring to [Table 8-14](#).

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 8-14** Rule parameters

Parameter	Description	Example Value
Path	<p>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.</p> <ul style="list-style-type: none"> <li>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 <b>/admin</b>, set <b>Path</b> to <b>/admin*</b>.</li> <li>Exact match: The path to be entered must match the path to be protected. If the path to be protected is <b>/admin</b>, set <b>Path</b> to <b>/admin</b>.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>The path supports prefix and exact matches only. Regular expressions are not supported.</li> <li>The path cannot contain two or more consecutive slashes. For example, <b>///admin</b>. If you enter <b>///admin</b>, the WAF engine converts <b>///</b> to <b>/</b>.</li> </ul>	<b>/admin*</b>
Type	<ul style="list-style-type: none"> <li><b>Sensitive information filtering</b></li> <li><b>Response code interception:</b> Enable WAF to block the specified HTTP response code page.</li> </ul>	<b>Sensitive information filtering</b>
Content	Information to be protected. Options are <b>Identification card</b> , <b>Phone number</b> , and <b>Email</b> .	<b>Identification card</b>
Rule Description	A brief description of the rule. This parameter is optional.	None

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

----End

## Other Operations

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

## 8.12 Configuring a Global Protection Whitelist (Formerly False Alarm Masking) Rule

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.

### Prerequisites



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

### Constraints

- You can configure false alarm masking rules only for attack events blocked or recorded by basic web protection rules preset in WAF.
- 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 (formerly false alarm masking) 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 (formerly false alarm masking) rule by referring to [Handling False Alarms](#). After handling a false alarm, you can view the rule in the global protection whitelist (formerly false alarm masking) rule list.

### Procedure

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

- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- Step 4** In the navigation pane on the left, choose **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 **Global Protection Whitelist (Formerly False Alarm Masking)** configuration area, click **Status** if needed. Then, click **Customize Rule**.
- Step 7** In the upper left corner of the **Global Protection Whitelist** page, click **Add Rule**.
- Step 8** Add a global protection whitelist rule by referring to [Table 8-15](#).

**Table 8-15** Parameters

Parameter	Description	Example Value
Scope	<ul style="list-style-type: none"> <li>• <b>All domain names:</b> By default, this rule will be used to all domain names that are protected by the current policy.</li> <li>• <b>Scope:</b> Specify a domain name range this rule applies to.</li> </ul>	Specified domain names
Domain Name	<p>This parameter is mandatory when you select <b>Specified domain names</b> for <b>Scope</b>.</p> <p>Enter a single domain name that matches the wildcard domain name being protected by the current policy.</p>	www.example.com

Parameter	Description	Example Value
Condition List	<p>Click <b>Add</b> 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:</p> <p>Parameters for configuring a condition are described as follows:</p> <ul style="list-style-type: none"> <li>• <b>Field</b></li> <li>• <b>Subfield:</b> Configure this field only when <b>Params</b>, <b>Cookie</b>, or <b>Header</b> is selected for <b>Field</b>.</li> </ul> <p><b>NOTICE</b> The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.</p> <ul style="list-style-type: none"> <li>• <b>Logic:</b> Select a logical relationship from the drop-down list.</li> <li>• <b>Content:</b> Enter or select the content that matches the condition.</li> </ul>	Path, Include, / product
Ignore WAF Protection	<ul style="list-style-type: none"> <li>• <b>All protection:</b> All WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule.</li> <li>• <b>Basic Web Protection:</b> 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.</li> </ul>	Basic Web Protection
Ignored Protection Type	<p>If you select <b>Basic web protection</b> for <b>Ignored Protection Type</b>, specify the following parameters:</p> <ul style="list-style-type: none"> <li>• <b>ID:</b> Configure the rule by event ID.</li> <li>• <b>Attack type:</b> Configure the rule by attack type, such as XSS and SQL injection. One type contains one or more rule IDs.</li> <li>• <b>All built-in rules:</b> all checks enabled in <b>Basic Web Protection</b>.</li> </ul>	Attack type

Parameter	Description	Example Value
ID	<p>This parameter is mandatory when you select <b>ID</b> for <b>Ignored Protection Type</b>.</p> <p>ID of an attack event on the <b>Events</b> page. If the event type is <b>Custom</b>, it has no event ID. Click <b>Handle False Alarm</b> in the row containing the attack event to obtain the ID. You are advised to configure global protection whitelist (formerly false alarm masking) rules on the <b>Events</b> page by referring to <a href="#">Handling False Alarms</a>.</p>	041046
Attack type	<p>This parameter is mandatory when you select <b>Attack type</b> for <b>Ignored Protection Type</b>.</p> <p>Select an attack type from the drop-down list box.</p> <p>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.</p>	SQL injection
Rule Description	A brief description of the rule. This parameter is optional.	SQL injection attacks are not intercepted.
Advanced Settings	<p>To ignore attacks of a specific field, specify the field in the <b>Advanced Settings</b> area. After you add the rule, WAF will stop blocking attack events of the specified field.</p> <p>Select a target field from the first drop-down list box on the left. The following fields are supported: <b>Params</b>, <b>Cookie</b>, <b>Header</b>, <b>Body</b>, and <b>Multipart</b>.</p> <ul style="list-style-type: none"> <li>• If you select <b>Params</b>, <b>Cookie</b>, or <b>Header</b>, you can select <b>All</b> or <b>Specified field</b> to configure a subfield.</li> <li>• If you select <b>Body</b> or <b>Multipart</b>, you can select <b>All</b>.</li> <li>• If you select <b>Cookie</b>, the <b>Domain Name</b> can be empty.</li> </ul> <p><b>NOTE</b> If <b>All</b> is selected, WAF will not block all attack events of the selected field.</p>	Params All

**Step 9** Click **OK**.

----**End**

## Other Operations

- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a global protection whitelist (formerly false alarm masking) rule, click **Modify** in the row containing the rule.
- To delete a global protection whitelist (formerly false alarm masking) rule, click **Delete** in the row containing the rule.

## 8.13 Configuring a Data Masking Rule

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

### Prerequisites

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

### Constraints


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


### Impact on the System

Sensitive data in the events will be masked to protect your website visitor's privacy.

### Procedure

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

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

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

**Step 4** In the navigation pane on the left, choose **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 **Data Masking** configuration area, change **Status** if needed and click **Customize Rule**.



**Step 7** In the upper left corner of the **Data Masking** page, click **Add Rule**.

**Step 8** In the displayed dialog box, specify the parameters described in [Table 8-16](#).

**Table 8-16** Rule parameters

Parameter	Description	Example Value
Path	<p>Part of the URL that does not include the domain name.</p> <ul style="list-style-type: none"> <li>Prefix match: The path ending with * indicates that the path is used as a prefix. For example, if the path to be protected is <b>/admin/test.php</b> or <b>/adminabc</b>, set <b>Path</b> to <b>/admin*</b>.</li> <li>Exact match: The path to be entered must match the path to be protected. If the path to be protected is <b>/admin</b>, set <b>Path</b> to <b>/admin</b>.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>The path supports prefix and exact matches only and does not support regular expressions.</li> <li>The path cannot contain two or more consecutive slashes. For example, <b>///admin</b>. If you enter <b>///admin</b>, WAF converts <b>///</b> to <b>.</b></li> </ul>	<p><b>/admin/login.php</b></p> <p>For example, if the URL to be protected is <b>http://www.example.com/admin/login.php</b>, set <b>Path</b> to <b>/admin/login.php</b>.</p>
Masked Field	<p>A field set to be masked</p> <ul style="list-style-type: none"> <li><b>Params</b>: A request parameter</li> <li><b>Cookie</b>: A small piece of data to identify web visitors</li> <li><b>Header</b>: A user-defined HTTP header</li> <li><b>Form</b>: A form parameter</li> </ul>	<ul style="list-style-type: none"> <li>If <b>Masked Field</b> is <b>Params</b> and <b>Field Name</b> is <b>id</b>, content that matches <b>id</b> is masked.</li> <li>If <b>Masked Field</b> is <b>Cookie</b> and <b>Field Name</b> is <b>name</b>, content that matches <b>name</b> is masked.</li> </ul>
Field Name	<p>Set the parameter based on <b>Masked Field</b>. The masked field will not be displayed in logs.</p> <p><b>NOTICE</b></p> <p>The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.</p>	
Rule Description	<p>A brief description of the rule. This parameter is optional.</p>	None

**Step 9** Click **Confirm**. The added data masking rule is displayed in the list of data masking rules.

----End

## Other Operations

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

# 9 Dashboard

This topic describes how to view event logs, including attack and request statistics, event distribution, top 10 attacked domain names, top 10 attack source IP addresses, and top 10 attacked URLs in a specified time range, such as yesterday, today, past 3 days, past 7 days, or past 30 days.

## 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 9-1](#).

**Table 9-1** QPS calculation

Time Range	Average QPS Description	Peak QPS Description
<b>Yesterday or Today</b>	The QPS curve is made with the average QPS in every minute.	The QPS curve is made with each peak QPS in every minute.
<b>Past 3 days</b>	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.
<b>Past 7 days</b>	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.


Time Range	Average QPS Description	Peak QPS Description
Past 30 days	The QPS curve is made with the maximum value among the average QPSs in every five minutes at a one-hour interval.	The QPS curve is made with the peak QPS in every hour.


 **NOTE**

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

## Procedure

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

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

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

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

- By default, the information about all websites you add to WAF in all enterprise projects are displayed.
- **Domain Names:** shows information about website domain names 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 pages under each type of attacks.

- **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 attacks 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 2 minutes.
- **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 9-2** Parameters in Security Event Statistics

Parameter	Description
Requests	You can view how many requests for your website as well as total attacks and attacks of each attack type.
QPS	Average number of requests per second for the domain name. For details about the values of QPS, see <a href="#">How to Calculate QPS</a> .  Queries Per Second (QPS) indicates the number of requests per second. For example, an HTTP GET request is also called a query.
Bandwidth	Bandwidth usage  The value of sent and received bytes is calculated by adding the values of <b>request_length</b> and <b>upstream_bytes_received</b> 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.
Event Distribution	Types of attack events  Click an area in the <b>Event Distribution</b> 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 <b>View More</b> to go to the <b>Events</b> 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 <b>View More</b> to go to the <b>Events</b> page and view more protection data.
Top 10 Attacked URLs	The ten most attacked URLs and the number of attacks on each URL.  Click <b>View More</b> to go to the <b>Events</b> page and view more protection data.

----End

# 10 Event Management

---

## 10.1 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.

---

### NOTICE

On the WAF console, you can view the event data for all protected domain names over the last 30 days.

---

### 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.
- If you switch the WAF working mode for a website to **Suspended**, WAF only forwards all requests to the website without inspection. It does not log any attack events neither.

### Procedure

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

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

- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Events**.
- Step 5** Click the **Search** tab. In the website or instance drop-down list, select a website to view corresponding event logs. The query time can be **Yesterday, Today, Past 3 days, Past 7 days, Past 30 days**, or a time range you configure.
- **Events over Time:** displays the WAF protection status of the selected website within the selected time range.
  - **Top Tens:** Displays a summary of top tens about protected domain names you select for a time range.
- Step 6** In the **Events** area, view the event details.
- Configure a filter by combining several conditions. Click **Add** and select filter conditions displayed. Then, click **OK**. [Table 10-1](#) lists parameters for filter conditions.
  - In the upper right corner of the event list, click  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 **Download Events** page. You can download the events on the **Download Events** 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.
  - Click  next to the source IP address to sort the event list in ascending or descending order of the origin server IP address.

**Table 10-1** Description of the conditions

Parameter	Parameter
Event ID	ID of the event.
Event Type	Type of the attack. By default, <b>All</b> 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 <b>Block, Log only, and Verification code</b> .
Source IP Address	Public IP address of the web visitor/attacker By default, <b>All</b> 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.

Parameter	Parameter
URL	Attacked URL

**Table 10-2** Parameters in the event list

Parameter	Description	Example Value
Time	When the attack occurred	2021/02/04 13:20:04
Source IP Address	Public IP address of the web visitor/attacker	-
Domain Name	Attacked domain name	www.example.com
Geolocation	Location where the IP address of the attack originates from	-
URL	Attacked URL	/admin
Event Type	Type of attack	SQL injection
Protective Action	Protective actions configured in the rule. The options are <b>Block</b> , <b>Log only</b> , and <b>Verification code</b> . <b>NOTE</b> If an access request matches a web tamper protection rule, information leakage prevention rule, or data masking rule, the protective action is marked as <b>Mismatch</b> .	Block

----End

## 10.2 Handling False Alarms

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

WAF detects attacks by using built-in basic web protection rules 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.

### 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 can be handled as false alarms.
- For events generated based on custom rules (such as a CC attack protection rule, precise protection rule, blacklist rule, whitelist rule, or geolocation access control rule), they cannot be handled as false alarms. To ignore such an event, delete or disable the custom rule hit by the event.
- An attack event can only be handled as a false alarm once.
- The attack event will not be displayed on the **Events** page.


## Application Scenarios

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

## Procedure

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

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

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

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

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

**Step 6** In the event list, handle events.

- If you confirm that an event is a false alarm, locate the row containing the event. In the **Operation** column, click **Handle** > **Handle as False Alarm** and handle the hit rule.
- Add the source IP address to an address group. Locate the row containing the desired event, in the **Operation** column, click **Handle** > **Add to Address Group**. The source IP address of 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 **Handle** > **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 10-3** Parameter

Parameter	Description
Add to	<ul style="list-style-type: none"> <li>- Existing rule</li> <li>- New rule</li> </ul>
Rule Name	<ul style="list-style-type: none"> <li>- If you select <b>Existing rule</b> for <b>Add to</b>, select a rule name from the drop-down list.</li> <li>- If you select <b>New rule</b> for <b>Add to</b>, customize a blacklist or whitelist rule.</li> </ul>
IP Address/Range/Group	<p>This parameter is mandatory when you select <b>New rule</b> for <b>Add to</b>.</p> <p>You can select <b>IP address/Range</b> or <b>Address Group</b> to add IP addresses a blacklist or whitelist rule.</p>
Group Name	<p>This parameter is mandatory when you select <b>Address group</b> for <b>IP Address/Range/Group</b>.</p> <p>Select an address group from the drop-down list. You can also click <b>New address group</b> to create an address group. For details, see <a href="#">Adding an IP Address Group</a>.</p>
Protective Action	<ul style="list-style-type: none"> <li>- <b>Block</b>: Select <b>Block</b> if you want to blacklist an IP address or IP address range.</li> <li>- <b>Allow</b>: Select <b>Allow</b> if you want to whitelist an IP address or IP address range.</li> <li>- <b>Log only</b>: Select <b>Log only</b> if you want to observe an IP address or IP address range.</li> </ul>
Known Attack Source	<p>If you select <b>Block</b> for <b>Protective Action</b>, 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.</p>
Rule Description	<p>A brief description of the rule. This parameter is optional.</p>

----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 (formerly false alarm masking) rule is configured to check whether the configuration takes effect.

## Other Operations

If an event is handled as a false alarm, the rule hit will be added to the global protection whitelist (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. For more details, see [Configuring a Global Protection Whitelist \(Formerly False Alarm Masking\) Rule](#).

## 10.3 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.



### Prerequisites

- The website to be protected has been added to WAF.
- An event file has been generated.

### Specification Limitations

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

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Events**.
- Step 5** Click the **Download Events** tab and download the desired protection data. [Table 10-4](#) describes the parameters.

**Table 10-4** Parameter description

Parameter	Description
File Name	The format is <i>file-name.csv</i> .

Parameter	Description
Number of Events	Total number of blocked and logged events <b>NOTE</b> 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.	d5580c8f6cd4403ebbf85892d4bb8e4
request_line	Request line of the attack	GET /
rule	ID of the rule against which the event is generated.	81066
sip	Public IP address of the web visitor/attacker	N/A

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

# 11 Enabling Alarm Notifications

---

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

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

## NOTE

- Before you set alarm notification, create a message topic in the SMN service.



## Prerequisites

SMN has been enabled.

## Constraints

Alarm notifications are sent if the number of attacks is at least equal to the threshold configured for a certain period.

## Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane, choose **Instance Management** > **Notifications**.
- Step 5** Click **Create** and configure alarm notification parameters. [Table 11-1](#) lists the parameters.

**Table 11-1** Description of notification setting parameters

Parameter	Description
Notification Type	<p>Select a notification type.</p> <ul style="list-style-type: none"> <li>• <b>Events:</b> WAF sends attack logs to you in the way you configure (such as SMS or email) once it detects log-only or blocked events.</li> <li>• <b>Certificate expiration:</b> When a certificate is about to expire, WAF notifies you by the way you configure, such as email or SMS.</li> </ul>
Notification Name	Name of the alarm notification.
Description	(Optional) A description of the purposes of the alarm.
Notification Topic	<p>Select a topic from the drop-down list.</p> <p>For details about topics and subscriptions, see the <i>Simple Message Notification User Guide</i>.</p>
Interval	<p>If you select <b>Events</b> for <b>Notification Type</b>, <b>Interval</b> must be configured.</p> <p><b>NOTE</b> Alarm notifications are sent if the number of attacks is at least equal to the threshold configured for a certain period.</p>
Event Type	<p>If you select <b>Events</b> for <b>Notification Type</b>, <b>Event Type</b> must be configured.</p> <p>By default, <b>All</b> is selected. To specify event types, click <b>Custom</b>.</p>
Notification Before Expiration	<p>This parameter must be configured if you select <b>Certificate expiration</b> for <b>Notification Type</b>.</p> <p>Select how long before a certificate expire WAF can send notifications. You can select <b>1 week</b>, <b>1 month</b>, or <b>2 months</b>.</p> <p>For example, if you select <b>1 week</b>, WAF will send you an SMS message or email one week before the certificate expires.</p>
Interval	<p>This parameter must be configured if you select <b>Certificate expiration</b> for <b>Notification Type</b>.</p> <p>How often WAF sends certificate expiration notifications to you. You can select <b>Weekly</b> or <b>Daily</b>.</p>

**Step 6** Click **OK**.

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

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

----End



# 12 Policy Management

---

## 12.1 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 to your WAF instance.



### 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 of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** In the upper left corner, click **Add Policy**.
- Step 6** In the displayed dialog box, enter the policy name and click **Confirm**. The added policy will be displayed in the policy list.
- Step 7** In the **Policy Name** column, click the policy name. On the displayed page, add rules to the policy by referring to [Rule Configurations](#).

----End

## Other Operations

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



## 12.2 Adding Rules to One or More Policies

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

### Prerequisites

A website has been added to WAF.

### Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** In the upper left corner of the page, click **All Rules**.
- Step 6** In the upper left corner above a rule to be added, 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 8-5](#).
  - To add a precise protection rule, see [Table 8-6](#).
  - To add a blacklist or whitelist rule, see [Table 8-9](#).
  - To add a geolocation access control rule, see [Table 8-11](#).
  - To add a WTP rule, see [Table 8-12](#).
  - To add an information leakage prevention rule, see [Table 8-14](#).
  - To add a global protection whitelist rule, see [Table 8-15](#).
  - To add a data masking rule, see [Table 8-16](#).
- Step 9** Click **OK**.  
----End

### Other Operations

- After a rule is added, the rule is **Enabled** by default. To disable it, click **Disable** in the **Operation** column of the target rule. You can also select

multiple rules and click **Disable** above the rule list to disable them all together.

- To modify a rule, locate the row that contains the rule and click **Modify** in the **Operation** column. You can also select multiple rules and click **Modify** above the list to modify them all together.
- To delete a rule, locate the row that contains the rule and click **Delete** in the **Operation** column. You can also select multiple rules and click **Delete** above the list to delete them all together.

## 12.3 Applying a Policy to Your Website


This topic describes how to apply a policy to your protected website.


### Prerequisites

A website has been added to WAF.

### Procedure

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

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

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

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

**Step 5** In the 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



# 13 Dedicated WAF Engine Management

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

## 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** under **Security & Compliance**.
- 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 13-1](#) describes parameters.

**Table 13-1** Parameters of a dedicated instance



Parameter	Description	Example Value
Instance Name	Name automatically generated when an instance is created.	None
Protected Website	Domain name of the website protected by the instance.	www.example.com
VPC	VPC where the instance resides	vpc-waf
Subnet	Subnet where an instance resides	subnet-62bb

Parameter	Description	Example Value
IP Addresses	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
Deployment	How the instance is deployed.	Standard mode (reverse proxy)
Specifications	Specifications of resources hosting the instance.	8 vCPUs   16 GB

----End

## Upgrading a Dedicated WAF Instance

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

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- 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 **Upgrade** in the **Operation** column.
- Step 6** Confirm the upgrade conditions and click **Confirm**.

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

----End

## 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** under **Security & Compliance**.
- 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 **Delete** in the **Operation** column.
- Step 6** Click **Confirm**.

----End

# 14 Viewing Product Details



---

On the **Product Details** page, you can view information about all your WAF instances, including the edition, domain quotas, and specifications.

## 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** 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

# 15 Permissions Management

## 15.1 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.

### 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"
      ]
    }
  ]
}
```

## 15.2 WAF Permissions and Supported Actions

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

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

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

### Supported Actions

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

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

Permission	Action
Querying an information leakage prevention rule	waf:antiLeakageRule:get
Querying a web tamper protection rule	waf:antiTamperRule:get
Querying a CC attack protection rule	waf:ccRule:get
Querying a precise protection rule	waf:preciseProtectionRule:get
Querying a global protection whitelist (formerly false alarm masking) 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:geolpRule: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

Permission	Action
Updating a precise protection rule	waf:preciseProtectionRule:put
Updating a global protection whitelist (formerly false alarm masking) 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:geolpRule:put
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 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:geolpRule: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

Permission	Action
Creating a global protection whitelist (formerly false alarm masking) 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:geolpRule:create
Adding a certificate	waf:certificate:create
Adding a domain	waf:instance:create
Adding a policy	waf:policy:create
Querying information leakage prevention rules	waf:antiLeakageRule:list
Querying web tamper protection rules	waf:antiTamperRule:list
Querying CC attack protection rules	waf:ccRuleRule:list
Querying precise protection rules	waf:preciseProtectionRule:list
Querying the global protection whitelist (formerly false alarm masking) 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:geolpRule:list
Querying the protection domains	waf:instance:list
Querying protection policies	waf:policy:list
Querying the WAF dedicated instances	waf:premiumInstance:list
Querying a WAF dedicated instance	waf:premiumInstance:get
Creating a WAF dedicated instance	waf:premiumInstance:create

Permission	Action
Deleting a WAF dedicated instance	waf:premiumInstance:delete
Updating a WAF dedicated engine	waf:premiumInstance:put

# 16 FAQs

---

## 16.1 About WAF

### 16.1.1 WAF Functions

#### 16.1.1.1 Can WAF Protect an IP Address?

A WAF instance can protect 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?](#)

#### 16.1.1.2 What Objects Does WAF Protect?

WAF can protect domain names or IP addresses.

#### 16.1.1.3 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.

#### 16.1.1.4 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.

#### 16.1.1.5 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.

### 16.1.1.6 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 WAF Support Vulnerability Detection?

The basic web protection function of WAF can detect and block threats such as third-party security tool vulnerability attacks. If you enable the scanner item when configuring basic web protection 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.

#### 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.

### 16.1.1.7 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.

### **16.1.1.8 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.

### **16.1.1.9 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.

### **16.1.1.10 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.

### **16.1.1.11 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.

### **16.1.1.12 Can a WAF Instance Be Deployed in the VPC?**

Yes. You can deploy dedicated engine WAF instances in a VPC.

### **16.1.1.13 Can WAF Block URL Requests That Contain Special Characters?**

No. WAF can only detect and restrict source IP addresses.

### **16.1.1.14 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).



### 16.1.1.15 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.

### 16.1.1.16 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 of 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.

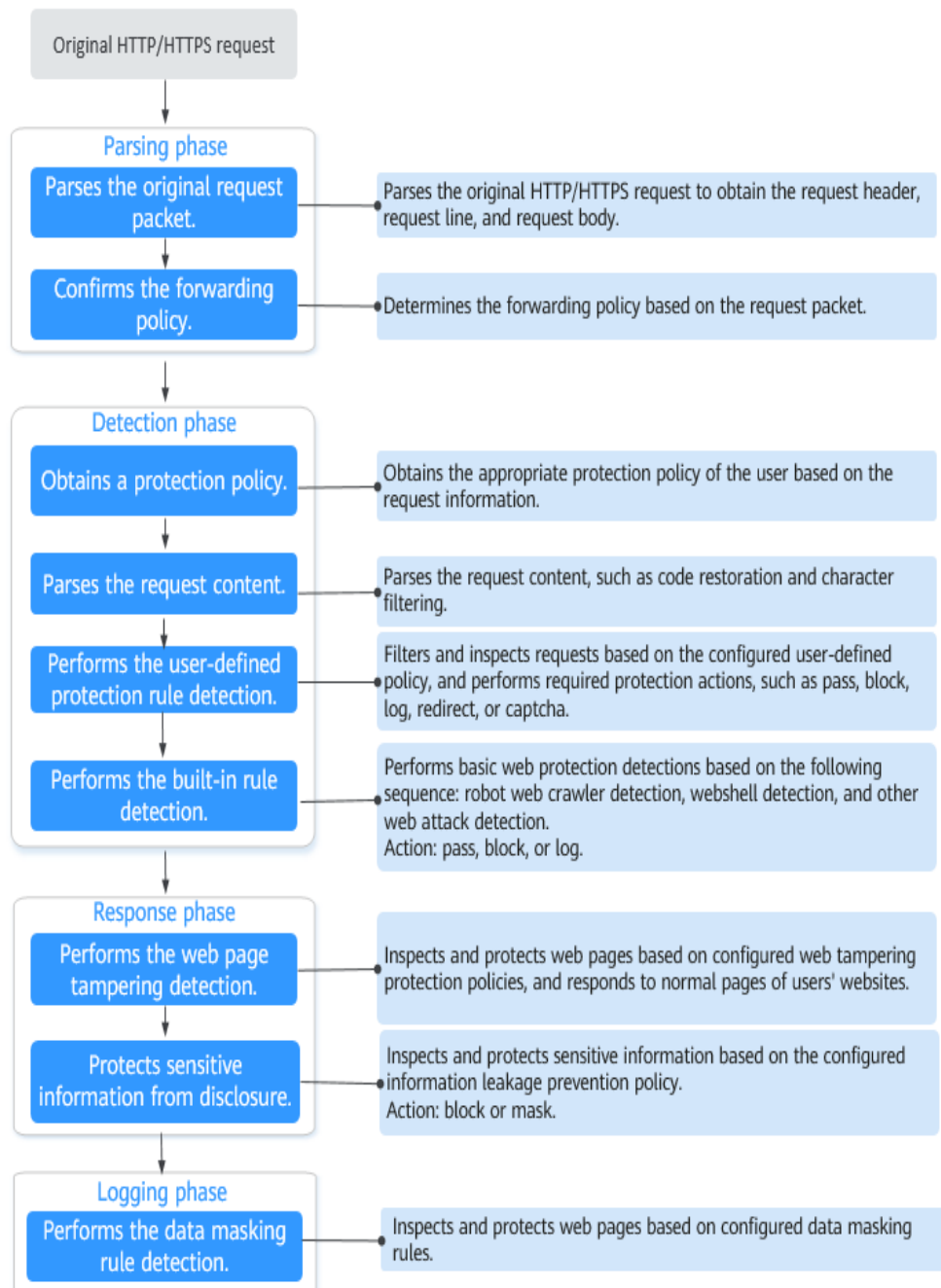
A cookie consists of a name, a value, and several optional attributes that control the cookie validity period, security, and usage scope. Cookies are classified into session cookies and persistent cookies. The details are as follows:

- 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.

### 16.1.1.17 Does WAF Block Customized POST Requests?

No. WAF does not block user-defined POST requests. [Figure 16-1](#) shows the detection process of the WAF built-in protection rules for original HTTP/HTTPS requests.

Figure 16-1 WAF engine detection process



### 16.1.1.18 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.

### 16.1.1.19 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.

### 16.1.1.20 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

### 16.1.1.21 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.

### 16.1.1.22 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 16-2** How WAF protects a website

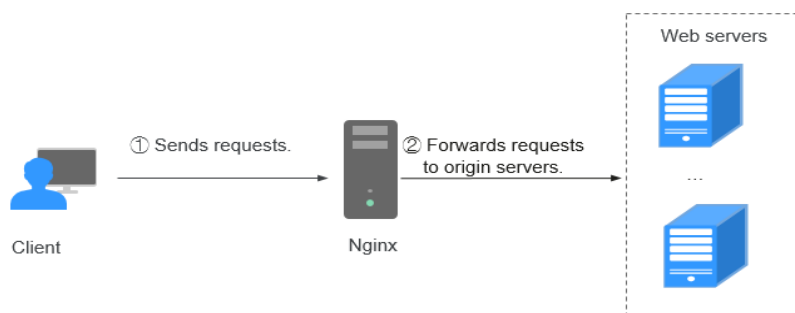


- Nginx forwarding

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 16-3** How Nginx Works



### 16.1.1.23 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.

### 16.1.1.24 Is WAF a Hardware Firewall or a Software Firewall?

WAF is a software firewall.

### 16.1.1.25 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. Therefore, service bandwidth of origin servers may rise as multiplexing in HTTP/2 may become invalid for origin servers.

### 16.1.1.26 How Does WAF Detect SQL Injection and XSS 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.

### 16.1.1.27 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).

### 16.1.1.28 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.

## 16.1.2 WAF Usage

### 16.1.2.1 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.

### 16.1.2.2 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.

### 16.1.2.3 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.

### 16.1.2.4 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.

### 16.1.2.5 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.

### 16.1.2.6 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 16-1](#).

**Table 16-1** QPS calculation

Time Range	Average QPS Description	Peak QPS Description
<b>Yesterday or Today</b>	The QPS curve is made with the average QPS in every minute.	The QPS curve is made with each peak QPS in every minute.
<b>Past 3 days</b>	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.
<b>Past 7 days</b>	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.
<b>Past 30 days</b>	The QPS curve is made with the maximum value among the average QPSs in every five minutes at a one-hour interval.	The QPS curve is made with the peak QPS in every hour.

### 16.1.2.7 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.

### 16.1.2.8 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.

### 16.1.2.9 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.

### 16.1.2.10 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.



### 16.1.2.11 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.

### 16.1.2.12 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. 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.

### 16.1.2.13 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.

### 16.1.2.14 Does WAF Affect Data Transmission from the Internal Network to an External Network?

No. 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 keep your origin server is secure, stable, and available.

### 16.1.2.15 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.

## 16.2 Website Domain Name Access Configuration

### 16.2.1 Domain Name and Port Configuration

#### 16.2.1.1 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.

---

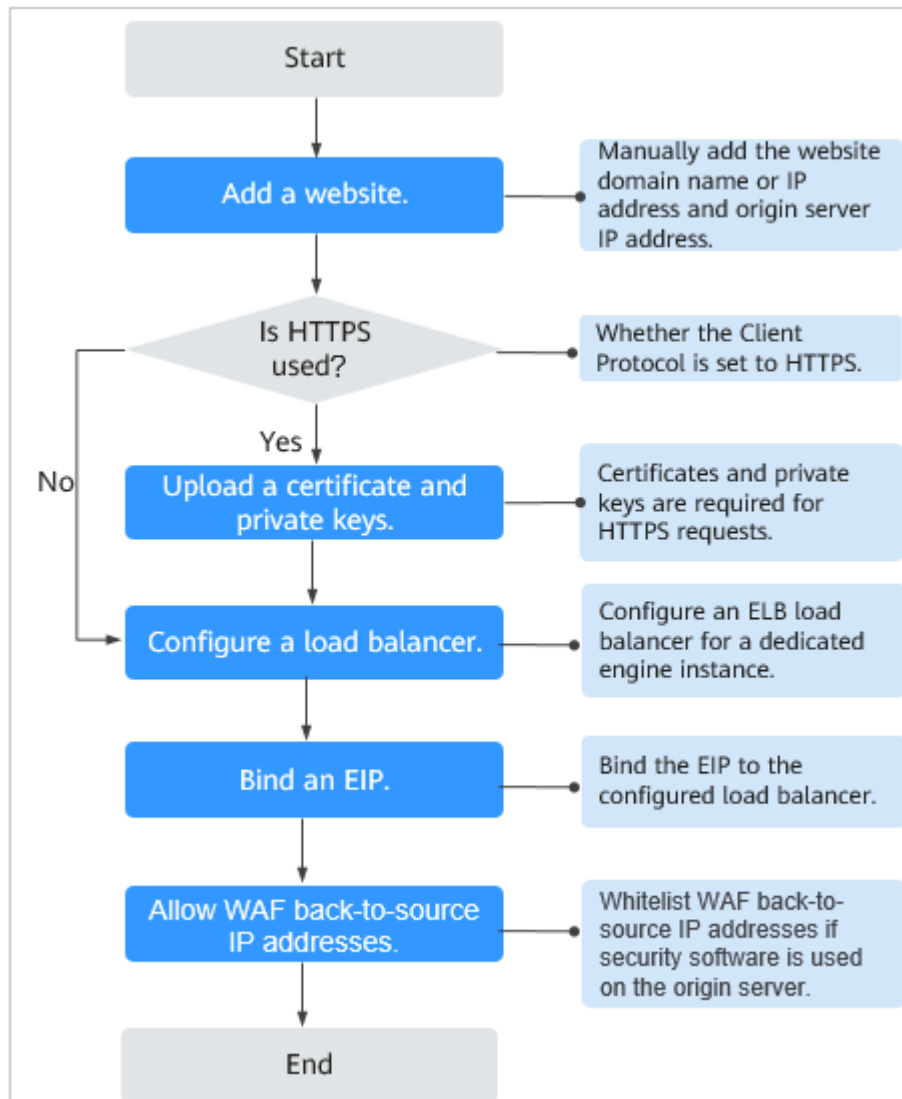
#### NOTICE

- 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 16-4** Process of connecting a website to a dedicated WAF instance



- 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 404/502/504 Errors?](#)

### 16.2.1.2 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 16-2** lists the ports that can be protected by WAF.

**Table 16-2** Ports supported by WAF

Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
Standard ports	80	443	Unlimited
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, 8015, 8016, 8017, and 8070	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

### 16.2.1.3 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.

### 16.2.1.4 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.

### 16.2.1.5 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.

### 16.2.1.6 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.

### 16.2.1.7 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:** IP address or domain name of the web server for client-side access.
  - **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.

### 16.2.1.8 How Do I Safely Delete a Protected Domain Name?

To delete a website from WAF, see [Removing a Protected Website from WAF](#). Before you start, get yourself familiar with the following precautions:

- 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.

### 16.2.1.9 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.

### 16.2.1.10 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.

### 16.2.1.11 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.

### 16.2.1.12 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.

### 16.2.1.13 Why Am I Seeing the "Someone else has already added this domain name. Please confirm that the domain name belongs to you" Error Message?

Someone else has already added this domain name. You need to confirm that the domain name belongs to you. If the domain name belongs to you, contact technical support. Your domain name might have been added to WAF under another account. If you want to add it to WAF under the current account, delete it from another account first.

## 16.2.2 Certificate Management

### 16.2.2.1 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.

### 16.2.2.2 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.

### 16.2.2.3 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 16-3](#) before uploading it.

**Table 16-3** Certificate conversion commands

Format	Conversion Method
CER/CRT	Rename the <b>cert.crt</b> certificate file to <b>cert.pem</b> .



Format	Conversion Method
PFX	<ul style="list-style-type: none"> <li>Obtain a private key. For example, run the following command to convert <b>cert.pfx</b> into <b>key.pem</b>: <b>openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes</b></li> <li>Obtain a certificate. For example, run the following command to convert <b>cert.pfx</b> into <b>cert.pem</b>: <b>openssl pkcs12 -in cert.pfx -nokeys -out cert.pem</b></li> </ul>
P7B	<ol style="list-style-type: none"> <li>Convert a certificate. For example, run the following command to convert <b>cert.p7b</b> into <b>cert.cer</b>: <b>openssl pkcs7 -print_certs -in cert.p7b -out cert.cer</b></li> <li>Rename certificate file <b>cert.cer</b> to <b>cert.pem</b>.</li> </ol>
DER	<ul style="list-style-type: none"> <li>Obtain a private key. For example, run the following command to convert <b>privatekey.der</b> into <b>privatekey.pem</b>: <b>openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem</b></li> <li>Obtain a certificate. For example, run the following command to convert <b>cert.cer</b> into <b>cert.pem</b>: <b>openssl x509 -inform der -in cert.der -out cert.pem</b></li> </ul>

 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.

## 16.3 Service Interruption Check

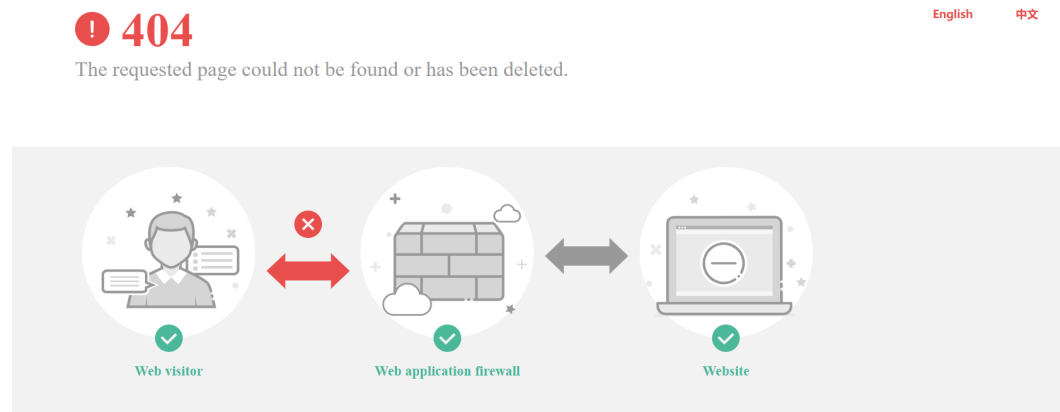
### 16.3.1 How Do I Troubleshoot 404/502/504 Errors?

If an error, such as 404 Not Found, 502 Bad Gateway, or 504 Gateway Timeout, occurs after a domain name is connected to WAF, use the following methods to locate the cause and remove the error:

#### 404 Not Found

**Scenario 1:** When a visitor accesses your website, the page shown in [Figure 16-5](#) is displayed.

Figure 16-5 404 page



**Cause:** The port added to a URL is incorrect.

- A non-standard port is configured when a domain name is connected to WAF. No port is added or the origin server port instead of the non-standard port is used to access the website. For example, use **https://www.example.com** or **https://www.example.com:80** to access the website.

**Solution:** Add the non-standard port to the URL and access the origin server again, for example, **https://www.example.com:8080**.

- No non-standard port is configured when a domain name is added to WAF. A non-standard port or the origin server port is used to access the website. For example, use **https://www.example.com:8080** to access the website.

**NOTE**

If no non-standard port is configured, WAF protects services on port 80/443 by default. To protect services on other ports, re-configure domain settings.

**Solution:** The domain name needs to be accessed directly. For example, **https://www.example.com**.

**Scenario 2:** When a visitor accesses your website, another 404 error page is displayed instead of the page shown in **Figure 16-5**.

**Cause:** The website does not exist or has been deleted.

**Solution:** Check your website.

## 502 Bad Gateway

**Scenario:** Website access is normal after the WAF configuration is complete. However, after a certain period of time, a 502 Bad Gateway error is reported frequently.

**NOTE**

If your web server is not deployed on the cloud, consult your server provider about whether the server has default block settings. If there are default block settings, ask the service provider to remove them.


Possible causes are as follows:

- **Cause 1:** Your website is using another security protection software. The software considers back-to-source IP addresses of WAF as malicious and blocks the requests forwarded by WAF. As a result, the site becomes inaccessible.

**Solution:** Add the WAF IP address ranges to the whitelist of the firewall (hardware or software), security protection software, and rate limiting module.

- **Cause 2:** Multiple backend servers are configured. However, one backend server is unreachable.

Perform the following steps to check whether the origin server configuration is correct:

- a. Log in to the management console, click **Service List** in the upper part of the page, and choose **Security > Web Application Firewall**.
- b. In the navigation pane, choose **Website Settings**.
- c. In the **Protected Website** column, click the domain name to go to the **Basic Information** page.
- d. In the **Server Information** area, click . On the displayed page, check whether the client protocol, server protocol, origin server address, and port used by the origin server are correct.
- e. Run the **curl** command on the host to check whether each origin server can be properly accessed.

```
curl http://xx.xx.xx.xx:yy -kv
```

*xx.xx.xx.xx* indicates the IP address of the origin server. *yy* indicates the port of the origin server. *xx.xx.xx.xx* and *yy* must belong to the same origin server.

#### NOTE

- The host where the **curl** command can be run must meet the following requirements:
  - The network communication is normal.
  - The **curl** command has been installed. **curl** must be manually installed on the host running the Windows operating system. **curl** is installed along with other operating systems.
- You can also enter **http://origin server address.origin server port** in the address bar of the browser to check whether the origin server can be properly accessed.

If **connection refused** is displayed, the origin server is unreachable and website cannot be accessed. Perform the following operations:

- Check whether the server is running properly. If it is not, restart the server.
  - Add the WAF IP address ranges to the whitelist of the firewall (hardware or software), security protection software, and rate limiting module.
- **Cause 3:** Origin server performance

**Solution:** Contact your website owner to rectify the fault.

## 504 Gateway Timeout

**Scenario:** After the configuration of connecting a domain name to WAF is complete, your website works properly. However, with the increasing traffic volume, the number of 504 errors also increases. If you directly access the IP address of the origin server, the 504 error code is returned sometimes.

The possible causes are as follows:


- **Cause 1:** Backend server performance issues (such as too many connections or high CPU usage)

**Solution:**

- a. Optimize the server configuration, including TCP network parameters and ulimit parameters.
- b. To handle large-scale service increase, use method 1 or method 2 to perform the processing.

**Method 1:** Add a backend server group to the ELB load balancer.

**Method 2:** Create an ELB. Use the EIP of ELB as the IP address of the server to connect to WAF.

- i. Log in to the management console, click **Service List** in the upper part of the page, and choose **Security > Web Application Firewall**.
  - ii. In the navigation pane, choose **Website Settings**.
  - iii. In the **Protected Website** column, click the domain name to go to the **Basic Information** page.
  - iv. In the **Server Information** area, click . On the displayed page, click **Add**.
- c. If the **Client Protocol** is **HTTPS**, you can use HTTPS on the WAF side. However, it is recommended that **HTTP (Server Protocol)** to forward the requests to your web server, lowering the computational demands on backend servers.

- **Cause 2:** The WAF back-to-source IP addresses are not whitelisted or your origin server port is not enabled.

**Solution:** Whitelist the WAF back-to-source IP addresses in the corresponding ECS security groups.

- **Cause 3:** The origin server has a firewall and the firewall blocks the WAF IP addresses.

**Solution:** Whitelist the WAF back-to-source IP addresses in the corresponding ECS security groups or uninstall the firewall software except WAF.

- **Cause 4:** Connection timeout and read timeout

**Solution**

- Database queries are slow.
  - Tune services to shorten the query duration and improve user experience.
  - Modify the request interaction mode so that the persistent connection can have some data transmitted within 60 seconds, such

- as ACK packets, heartbeat packets, keep-alive packets, and other packets that can keep the session alive.
- It takes a long time to upload large files.
  - Tune services to shorten the file upload time.
  - An FTP server is recommended for file upload.
  - Upload the file through an IP address or a domain name that is not protected by WAF.
  - The default timeout period for a dedicated WAF instance to respond origin servers is 180s.
- The origin server is faulty.  
Check whether the origin server works properly.
- **Cause 5:** The bandwidth of the origin server exceeds the upper limit.  
**Solution:** Increase the bandwidth of the origin server.

## 16.3.2 Why Is My Domain Name or IP Address Inaccessible?

### Symptoms

If **Access Progress** for a website you have added to WAF is **Accessible**, the connection between WAF and the website domain name or IP address has been established.

---

#### NOTICE

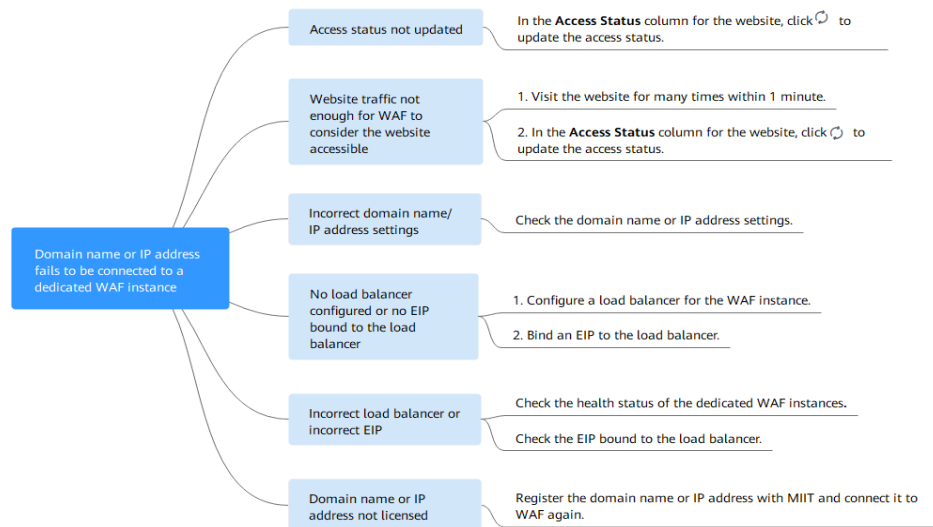
WAF automatically checks the access status of protected websites every hour. If WAF detects that a protected website has received 20 access requests within 5 minutes, it considers that the website has been successfully connected to WAF.

---

### Troubleshooting and Solutions for WAF Instances

Refer to [Figure 16-6](#) and [Table 16-4](#) to fix connection failures.

**Figure 16-6** Troubleshooting for dedicated mode



**Table 16-4** Solutions for dedicated mode

Possible Cause	Solution
Cause 1: <b>Access Status</b> for <b>Domain Name/IP Address</b> not updated	In the <b>Access Status</b> column for the website, click ↻ to update the status.
Cause 2: Website access traffic not enough for WAF to consider the website accessible <b>NOTICE</b> 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 <b>Access Status</b> 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 <a href="#">Configuring a Load Balancer</a> . 2. <a href="#">Bind an EIP to a Load Balancer</a> .

Possible Cause	Solution
Cause 5: Incorrect load balancer configured or incorrect EIP bound to the load balancer	<ul style="list-style-type: none"> <li>• After you <a href="#">configure a load balancer</a>, ensure that <b>Health Check Result</b> for the dedicated WAF instances added to the load balancer is <b>Healthy</b>.</li> <li>• After you <a href="#">bind an EIP to the load balancer</a>, check the EIP status.</li> </ul>

### 16.3.3 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.

If a large number of false alarms are reported for a specific service, handle them on the **Events** page. To do so, you can ignore the specific URL and rule ID. Then, WAF will no longer block the same type of request to the URL.

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 16-5](#). 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 16-5** Handling false alarms

Type of Hit Rule	Hit Rule	Handling Method
WAF built-in protection rules	<ul style="list-style-type: none"> <li>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.</li> <li>Feature-based anti-crawler protection Feature-based anti-crawler identifies and blocks crawler behavior from search engines, scanners, script tools, and other crawlers.</li> </ul>	In the row containing the attack event, click <b>Handle False Alarm</b> in the <b>Operation</b> column. For details, see <a href="#">Handling False Alarms</a> .
Custom protection rules	<ul style="list-style-type: none"> <li>CC attack protection rules</li> <li>Precise protection rules</li> <li>Blacklist and whitelist rules</li> <li>Geolocation access control rules</li> <li>Web tamper protection rules</li> <li>JavaScript anti-crawler protection</li> <li>Information leakage prevention rules</li> <li>Data masking rules</li> </ul>	Go to the page displaying the hit rule and delete it.
Other	<p>Invalid access requests</p> <p><b>NOTE</b> If either of the following cases, WAF blocks the access request as an invalid request:</p> <ul style="list-style-type: none"> <li>When <b>form-data</b> is used for POST or PUT requests, the number of parameters in a form exceeds 8,192.</li> <li>The URI contains more than 2,048 parameters.</li> <li>The number of headers exceeds 512.</li> </ul>	Allow the blocked requests by referring to <a href="#">Configuring a Precise Protection Rule</a> . The <b>Handle False Alarm</b> button for invalid access events are grayed out as such events are generated against a precise protection rule.



## 16.3.4 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.

### 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 referring to [Configuring a Precise Protection Rule](#).

## 16.3.5 What Is the Connection Timeout Duration of WAF? Can I Manually Set the Timeout Duration?

- The default timeout period 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 page.
- The default timeout duration for connections between WAF and your origin server is 60 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.

## 16.3.6 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).

## 16.3.7 Why Are HTTPS Requests Denied on Some Mobile Phones?

If your visitors receive a page similar to the one in [Figure 16-7](#) 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 16-7 Access failed



## 16.3.8 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.

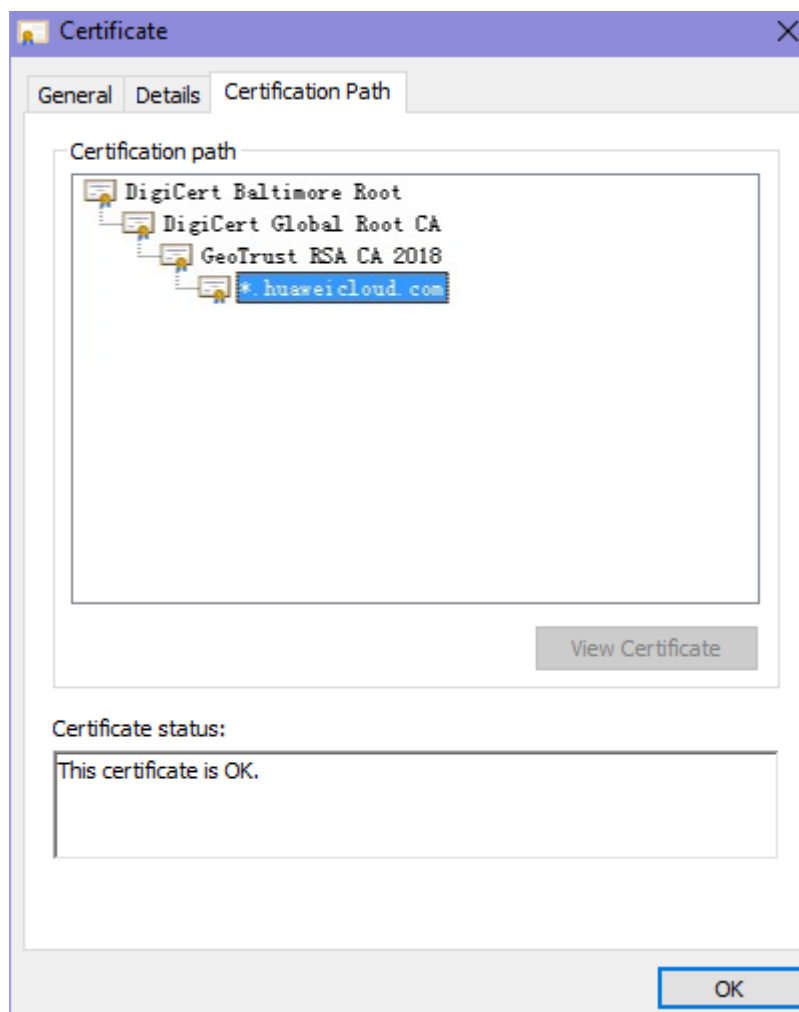
Use either of the following methods to fix it:

- 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 16-8](#) shows an example.

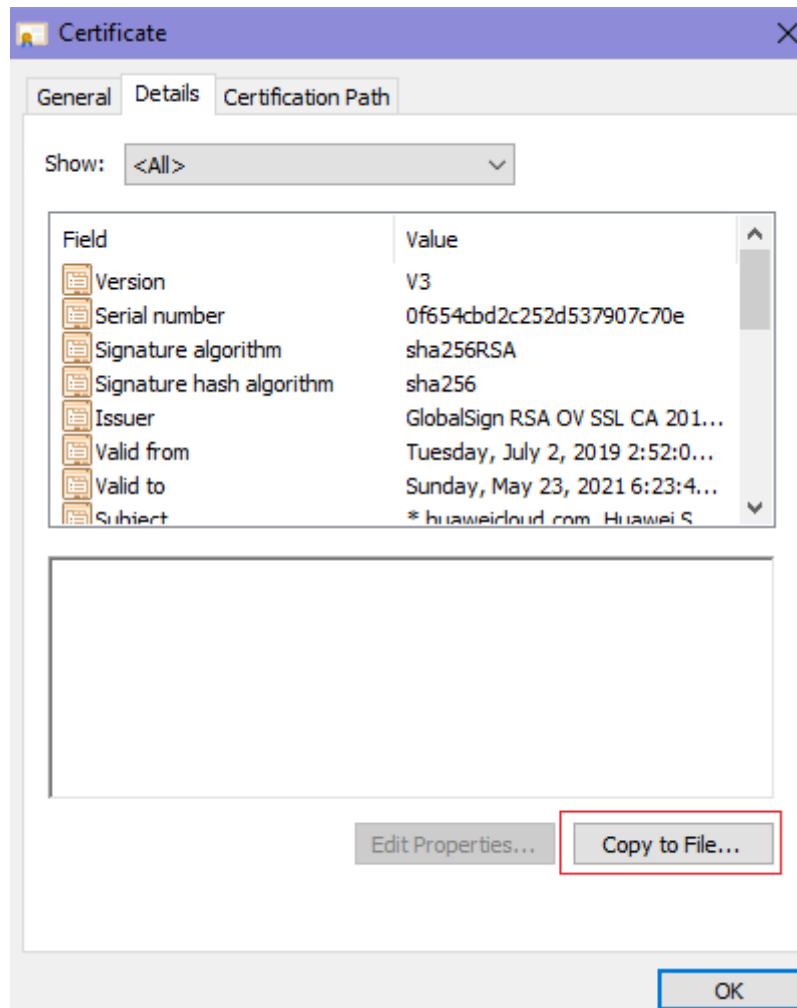
**Figure 16-8** Viewing the certificate chain



**Step 3** Save the certificates to the local PC one by one.

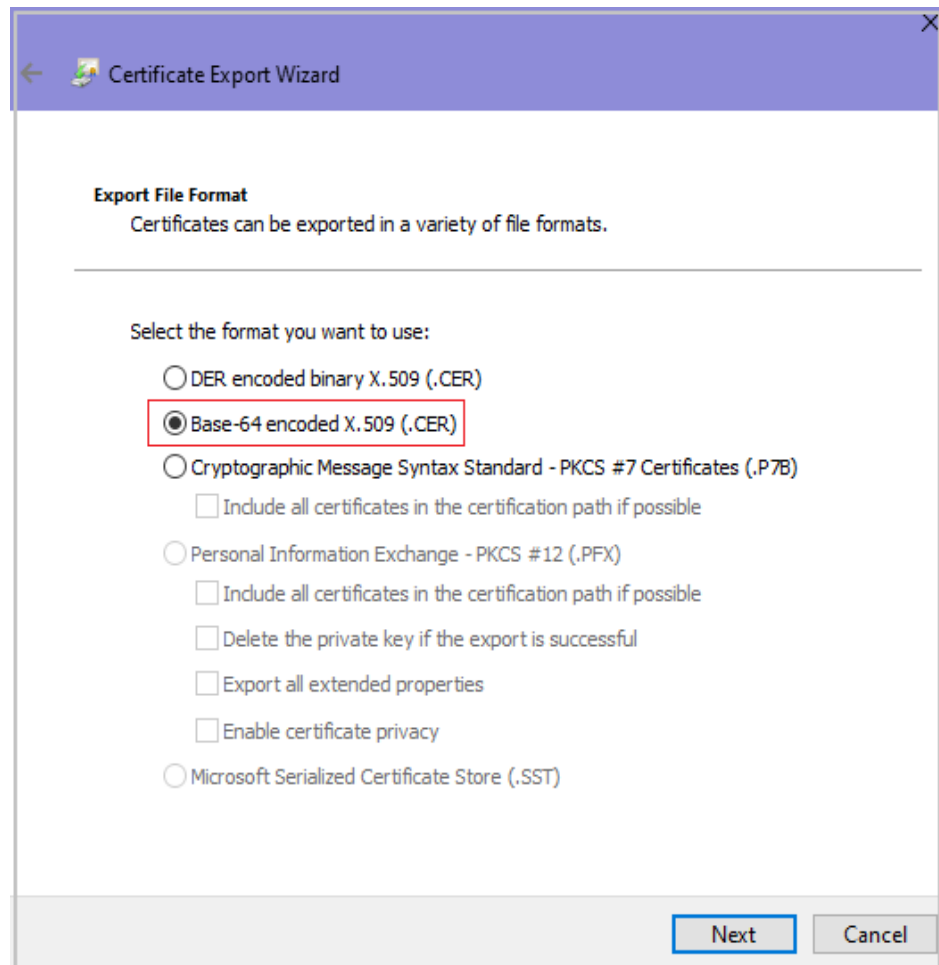
1. Select the certificate name and click the **Details** tab. [Figure 16-9](#) shows an example.

**Figure 16-9** Details



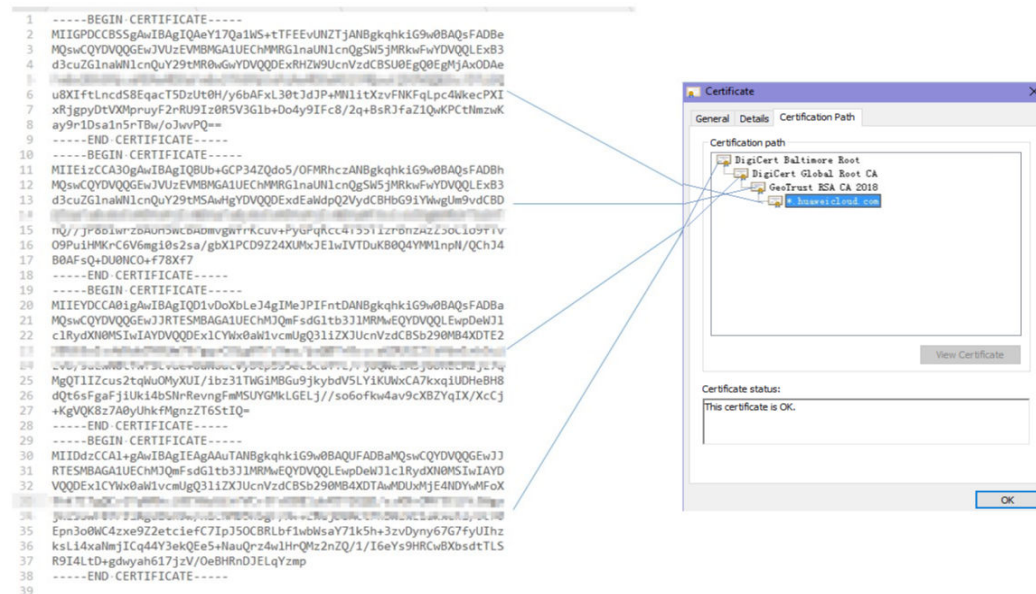
2. Click **Copy to File**, and then click **Next** as prompted.
3. Select **Base-64 encoded X.509 (.CER)** and click **Next**. [Figure 16-10](#) shows an example.

**Figure 16-10** Certificate Export Wizard



**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 16-11](#).

Figure 16-11 Certificate rebuilding



Step 5 Upload the certificate again.

----End

### 16.3.9 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.	<ol style="list-style-type: none"> <li>Run the following commands to check the MD5 hash values of the certificate and private key file:  <code>openssl x509 -noout -modulus -in &lt;certificate file&gt; openssl md5</code>  <code>openssl rsa -noout -modulus -in &lt;private key file&gt; openssl md5</code> </li> <li>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.</li> <li>If the certificate does not match the private key file, upload the correct certificate and private key file.</li> </ol>
Incorrect RSA private key format	<ol style="list-style-type: none"> <li>Run the following command to generate a new private key:  <code>openssl rsa -in &lt;private key file&gt; -out &lt;New private key file&gt;</code> </li> <li>Upload the private key again.</li> </ol>

## Other Operations

- [How Do I Fix an Incomplete Certificate Chain?](#)
- [Why Are HTTPS Requests Denied on Some Mobile Phones?](#)

### 16.3.10 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.

### 16.3.11 Why Am I Seeing Error Code 523?

If a request has passed through WAF four times, WAF blocks the request to prevent an infinite loop. In this case, error code 523 is returned.

Use the following methods to resolve the issue:

- Direct the request to the internal DNS server so that the request can bypass the public network.
- Configure the hosts file of the origin server.

The following uses the Windows operating system as an example.

- a. Use a text editor to open the **hosts** file. Generally, the **hosts** file is stored in the **C:\Windows\System32\drivers\etc\** directory.
- b. Add a record about the IP address of the origin server to the hosts file.
- c. Save the modification and exit.

### 16.3.12 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.

### 16.3.13 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?](#)

## 16.3.14 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

## 16.3.15 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 address this problem, you can set the minimum TLS version to TLS v1.2 and cipher suite to cipher suite 2.

## 16.4 Protection Rule Configuration


### 16.4.1 Basic Web Protection


#### 16.4.1.1 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** under **Security & Compliance**.

**Step 4** In the navigation pane, 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 **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

### 16.4.1.2 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 16-6](#).

**Table 16-6** Protection levels

Protection Level	Description
Low	WAF only blocks the requests with obvious attack signatures. If a large number of false alarms are reported, <b>Low</b> is recommended.
Medium	The default level is <b>Medium</b> , 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 <b>High</b> .

## 16.4.2 CC Attack Protection Rules

### 16.4.2.1 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**

For details, see [Configuring a CC Attack Protection Rule](#).

### 16.4.2.2 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.

### 16.4.2.3 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**.

## 16.4.3 Precise Protection rules

### 16.4.3.1 Can a Precise Protection Rule Take Effect in a Specified Period?

WAF does not allow precise protection access rules to 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.

## 16.4.4 Anti-Crawler Protection

### 16.4.4.1 Why Are There No Protection Logs for Some Requests Blocked by WAF JavaScript Anti-Crawler Rules?

After you enable the website anti-crawler protection, WAF returns a JavaScript code for the first access request to the domain name to the client browser, and

then checks whether the request is from a valid browser or crawler based on the data resolved and returned by the client browser.

The normal detection process of the Website anti-crawler protection is as follows:

1. An initial client request to the website is sent to WAF first.
2. WAF returns JavaScript code to the client.
3. The client resolves the JavaScript code and returns the execution result to WAF.
4. WAF checks whether the client of the request is a valid browser based on the result returned by the client.
  - If it is valid, WAF sends the request to the origin server.
  - If it is invalid, WAF generates an alarm log.

---

#### NOTICE

- To enable the anti-crawler protection, the browser on the client must have JavaScript and cookies enabled.
- If JavaScript and cookies are not supported by the client browser, only **1** and **2** can be performed. As a result, the following problems occur:
  - The client fails to get the requested pages.
  - No logs are recorded in WAF because the client does not send the execution result of parsing the JavaScript code.

Check your services. If your website can be accessed by other means except for a browser, disable anti-crawler protection.

---

## 16.4.5 Others

### 16.4.5.1 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.

### 16.4.5.2 Is the Path of a WAF Protection Rule Case-sensitive?

All paths configured for protection rules of WAF are case-sensitive.

### 16.4.5.3 What Protection Rules Does WAF Support?

The protection rules supported by WAF are described below.

- Basic Web Protection  
WAF can defend against common web attacks, such as SQL injection, XSS, web shells, and Trojans in HTTP upload channels. Once these functions are enabled, protection takes effect immediately.

- **CC Attack Protection**  
Flexible rate limiting policies can be set based on the IP addresses, cookies, or Referer field, mitigating CC attacks.
- **Precise Protection**  
Common HTTP fields can be combined to customize protection policies, such as CSRF protection. With user-defined rules, WAF can accurately detect malicious requests and protect sensitive information in websites.
- **Blacklist and Whitelist**  
Blacklist or whitelist rules allow you to block or allow specific IP addresses or address ranges, improving defense accuracy.
- **Geolocation Access Control**  
Geolocation access control rules allow you to customize access control based on the source IP addresses.
- **Web Tamper Protection**  
Cache configuration is performed 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 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.
- **Global Protection Whitelist (Formerly False Alarm Masking)**  
This function ignores certain attack detection rules for specific requests.
- **Data Masking**  
Data masking prevents such data as passwords from being displayed in event logs.
- **Information Leakage Prevention**  
WAF prevents user's sensitive information on web pages from being disclosed, such as ID numbers, phone numbers, and email addresses.

#### 16.4.5.4 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.

#### 16.4.5.5 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** under **Security & Compliance**.
- 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 **Configure Policy**.
- 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

#### 16.4.5.6 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 16-7](#) describes the differences between the two types of rules.

**Table 16-7** Differences between blacklist and whitelist rules and precise protection rules

Protection Rules	Protection	WAF Inspection Sequence
Blacklist and whitelist rules	This type of 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 filters access requests based on the protection rules and the triggering sequence. For details, see <a href="#">Configuration Guidance</a> .
Precise protection rules	You can combine common HTTP fields, such as <b>IP</b> , <b>Path</b> , <b>Referer</b> , <b>User Agent</b> , and <b>Params</b> 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.

### 16.4.5.7 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 after scanning the website, it records them as security threats.

# A Change History

---

Release On	Description
2024-04-13	This issue is the first official release.