

Web Application Firewall

User Guide

Date 2024-03-30

Contents

1 Service Overview	1
1.1 What Is WAF?	1
1.2 Edition Differences	2
1.3 Basic Concepts	5
1.4 Functions	8
1.5 Product Advantages	13
1.6 Application Scenarios	14
1.7 Personal Data Protection Mechanism	15
1.8 WAF Permissions Management	16
1.9 WAF and Other Services	18
2 WAF Operation Guide	19
3 Enabling WAF	22
4 Dashboard	26
5 Events	30
5.1 Viewing Protection Event Logs	30
5.2 Handling False Alarms	33
5.3 Downloading Events Data	39
5.4 Enabling LTS for WAF Logging	40
6 Policies	56
6.1 How to Configure WAF Protection	56
6.2 Configuring Basic Protection Rules to Defend Against Common Web Attacks	60
6.3 Configuring a CC Attack Protection Rule	65
6.4 Configuring Custom Precise Protection Rules	72
6.5 Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses	81
6.6 Configuring Geolocation Access Control Rules to Block or Allow Requests from Specific Locations	89
6.7 Configuring Web Tamper Protection Rules to Prevent Static Web Pages from Being Tampered With	94
6.8 Configuring Anti-Crawler Rules	98
6.9 Configuring Information Leakage Prevention Rules to Protect Sensitive Information from Leakage	107
6.10 Configuring a Global Protection Whitelist Rule to Ignore False Alarms	111
6.11 Configuring Data Masking Rules to Prevent Privacy Information Leakage	116

6.12 Creating a Reference Table to Configure Protection Metrics In Batches.....	120
6.13 Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration.....	123
6.14 Condition Field Description.....	128
7 Managing Policies.....	132
7.1 Creating a Protection Policy.....	132
7.2 Adding a Domain Name to a Policy.....	133
7.3 Adding Rules to One or More Policies.....	134
8 Website Settings.....	136
8.1 Adding a Website to WAF (Cloud Mode).....	136
8.1.1 Process for Adding a Website to WAF (Cloud Mode).....	136
8.1.2 Step 1: Add a Domain Name to WAF (Cloud Mode).....	141
8.1.3 Step 2: Whitelist WAF IP Addresses.....	147
8.1.4 Step 3: Test WAF.....	149
8.1.5 Step 4: Modify the DNS Records of the Domain Name.....	152
8.1.6 Configuration Example: Adding a Domain Name to WAF.....	154
8.2 Connecting a Website to WAF.....	159
8.2.1 Connection Process (Dedicated Mode).....	159
8.2.2 Step 1: Add a Website to WAF (Dedicated Mode).....	162
8.2.3 Step 2: Configure a Load Balancer for WAF.....	168
8.2.4 Step 3: Bind an EIP to a Load Balancer.....	170
8.2.5 Step 4: Whitelist IP Addresses of Dedicated WAF Instances.....	171
8.2.6 Step 5: Test Dedicated WAF Instances.....	174
8.3 Advanced Settings.....	176
8.3.1 Configuring PCI DSS/3DS Certification Check and TLS Version.....	176
8.3.2 Configuring a Traffic Identifier for a Known Attack Source.....	184
8.3.3 Modifying the Alarm Page.....	187
8.4 Basic Information.....	189
8.4.1 Viewing Basic Information.....	189
8.4.2 Switching WAF Working Mode.....	191
8.4.3 Updating a Certificate.....	192
8.4.4 Editing Server Information.....	194
8.4.5 Viewing Protection Information About a Protected Website on Cloud Eye.....	195
8.4.6 Deleting a Protected Website from WAF.....	196
8.5 Ports Supported by WAF.....	198
9 Object Management.....	201
9.1 Certificate Management.....	201
9.1.1 Uploading a Certificate.....	201
9.1.2 Using a Certificate for a Protected Website in WAF.....	204
9.1.3 Viewing Certificate Information.....	205
9.1.4 Deleting a Certificate.....	206
9.2 Managing IP Address Blacklist and Whitelist Groups.....	207

9.2.1 Adding an IP Address Group.....	207
9.2.2 Modifying or Deleting a Blacklist or Whitelist IP Address Group.....	208
10 System Management.....	210
10.1 Managing Dedicated WAF Engines.....	210
10.2 Viewing Product Details.....	214
10.3 Enabling Alarm Notifications.....	214
11 Permissions Management.....	218
11.1 IAM Permissions Management.....	218
11.1.1 Creating a User Group and Granting Permissions.....	218
11.1.2 WAF Custom Policies.....	220
11.1.3 WAF Permissions and Supported Actions.....	221
12 Monitoring and Auditing.....	225
12.1 Monitoring.....	225
12.1.1 WAF Monitored Metrics.....	225
12.1.2 Configuring Alarm Monitoring Rules.....	248
12.1.3 Viewing Monitored Metrics.....	249
12.2 Auditing.....	249
12.2.1 WAF Operations Recorded by CTS.....	249
12.2.2 Querying Real-Time Traces.....	251
13 FAQs.....	254
13.1 About WAF.....	254
13.1.1 FAQs for Beginners.....	254
13.1.2 WAF Functions.....	259
13.1.2.1 Can WAF Protect an IP Address?.....	259
13.1.2.2 What Objects Does WAF Protect?.....	260
13.1.2.3 Does WAF Block Customized POST Requests?.....	260
13.1.2.4 What Are the Differences Between the Web Tamper Protection Functions of WAF and HSS?....	261
13.1.2.5 Which Web Service Framework Protocols Does WAF Support?.....	263
13.1.2.6 Can WAF Protect Websites Accessed Through HSTS or NTLM Authentication?.....	263
13.1.2.7 What Are the Differences Between WAF Forwarding and Nginx Forwarding?.....	263
13.1.2.8 Can I Configure Session Cookies in WAF?.....	264
13.1.2.9 How Does WAF Detect SQL Injection, XSS, and PHP Injection Attacks?.....	265
13.1.2.10 Can WAF Defend Against the Apache Struts2 Remote Code Execution Vulnerability (CVE-2021-31805)?.....	266
13.1.3 WAF Usage.....	266
13.1.3.1 Why Does the Vulnerability Scanning Tool Report Disabled Non-standard Ports for My WAF-Protected Website?.....	266
13.1.3.2 How Do I Obtain the Real IP Address of a Web Visitor?.....	267
13.1.3.3 Will Traffic Be Permitted After WAF Is Switched to the Bypassed Mode?.....	267
13.1.3.4 What Are Local File Inclusion and Remote File Inclusion?.....	268
13.1.3.5 What Is the Difference Between QPS and the Number of Requests?.....	268

13.1.3.6 Does WAF Support Custom Authorization Policies?.....	269
13.1.3.7 How Do I Configure My Server to Allow Only Requests from WAF?.....	269
13.1.3.8 Why Do Cookies Contain the HWWAFSESID or HWWAFSESTIME field?.....	269
13.1.3.9 Can I Switch Between the WAF Cloud Mode and Dedicated Mode?.....	270
13.1.3.10 How Do I Configure WAF If a Reverse Proxy Server Is Deployed for My Website?.....	270
13.1.3.11 How Does WAF Forward Access Requests When Both a Wildcard Domain Name and a Single Domain Name Are Connected to WAF?.....	270
13.2 Service Request/Specification.....	270
13.2.1 WAF Instance Specifications Change.....	271
13.2.1.1 What Are the Impacts When QPS Exceeds the Allowed Peak Rate?.....	271
13.2.2 About Service Requests.....	271
13.2.2.1 Where Can I View the Inbound and Outbound Bandwidths of a Protected Website?.....	271
13.3 Website Domain Name Access Configuration.....	272
13.3.1 Domain Name and Port Configuration.....	272
13.3.1.1 How Do I Add a Domain Name/IP Address to WAF?.....	272
13.3.1.2 Which Non-Standard Ports Does WAF Support?.....	274
13.3.1.3 How Do I Use a Dedicated WAF Instance to Protect Non-Standard Ports That Are Not Supported by the Dedicated Instance?.....	277
13.3.1.4 How Do I Configure Domain Names to Be Protected When Adding Domain Names?.....	278
13.3.1.5 Do I Have to Configure the Same Port as That of the Origin Server When Adding a Website to WAF?.....	279
13.3.1.6 How Do I Configure Non-standard Ports When Adding a Protected Domain Name?.....	280
13.3.1.7 What Can I Do If One of Ports on an Origin Server Does Not Require WAF Protection?.....	282
13.3.1.8 What Data Is Required for Connecting a Domain Name/IP Address to WAF?.....	282
13.3.1.9 How Do I Safely Delete a Protected Domain Name?.....	282
13.3.1.10 Can I Change the Domain Name That Has Been Added to WAF?.....	283
13.3.1.11 What Are the Precautions for Configuring Multiple Server Addresses for Backend Servers?.....	283
13.3.1.12 Does WAF Support Wildcard Domain Names?.....	283
13.3.1.13 How Do I Route Website Traffic to My Cloud WAF Instance?.....	284
13.3.1.14 Can I Configure Multiple Load Balancers for a Dedicated WAF Instance?.....	285
13.3.1.15 Why Am I Seeing the "Someone else has already added this domain name. Please confirm that the domain name belongs to you" Error Message?.....	285
13.3.2 Certificate Management.....	285
13.3.2.1 How Do I Select a Certificate When Configuring a Wildcard Domain Name?.....	285
13.3.2.2 How Do I Modify a Certificate?.....	285
13.3.2.3 Do I Need to Import the Certificates That Have Been Uploaded to ELB to WAF?.....	286
13.3.2.4 How Do I Convert a Certificate into PEM Format?.....	286
13.3.3 Server Configuration.....	287
13.3.3.1 How Do I Configure the Client Protocol and Server Protocol?.....	287
13.3.3.2 Why Cannot I Select a Client Protocol When Adding a Domain Name?.....	289
13.3.3.3 Can I Set the Origin Server Address to a CNAME Record If I Use Cloud WAF?.....	290
13.3.4 Operations After Connecting Websites to WAF.....	290
13.3.4.1 Can I Access a Website Using an IP Address After a Domain Name Is Connected to WAF?.....	290

13.3.4.2 How Do I Test WAF?.....	290
13.3.4.3 How Can I Forward Requests Directly to the Origin Server Without Passing Through WAF?.....	290
13.4 Service Interruption Check.....	291
13.4.1 How Do I Troubleshoot 404/502/504 Errors?.....	291
13.4.2 Why Is My Domain Name or IP Address Inaccessible?.....	300
13.4.3 How Do I Handle False Alarms as WAF Blocks Normal Requests to My Website?.....	305
13.4.4 Why Does WAF Block Normal Requests as Invalid Requests?.....	307
13.4.5 How Do I Whitelist IP Address Ranges of Cloud WAF?.....	307
13.4.6 What Is the Connection Timeout Duration of WAF? Can I Manually Set the Timeout Duration?..	309
13.4.7 How Do I Solve the Problem of Excessive Redirection Times?.....	310
13.4.8 Why Are HTTPS Requests Denied on Some Mobile Phones?.....	310
13.4.9 How Do I Fix an Incomplete Certificate Chain?.....	311
13.4.10 Why Does My Certificate Not Match the Key?.....	315
13.4.11 Why Am I Seeing Error Code 418?.....	316
13.4.12 Why Am I Seeing Error Code 523?.....	316
13.4.13 Why Does the Website Login Page Continuously Refreshed After a Domain Name Is Connected to WAF?.....	317
13.4.14 Why Does the Requested Page Respond Slowly After the HTTP Forwarding Policy Is Configured?	318
13.4.15 How Can I Upload Files After the Website Is Connected to WAF?.....	318
13.4.16 Why Am I Seeing Error Code 414 Request-URI Too Large?.....	318
13.4.17 What Do I Do If the Protocol Is Not Supported and the Client and Server Do Not Support Common SSL Protocol Versions or Cipher Suites?.....	320
13.4.18 Why Cannot I Access the Dedicated Engine Page?.....	320
13.4.19 Why Is the Bar Mitzvah Attack on SSL/TLS Detected?.....	320
13.5 Protection Rule Configuration.....	321
13.5.1 Basic Web Protection.....	321
13.5.1.1 How Do I Switch the Mode of Basic Web Protection from Log Only to Block?.....	321
13.5.1.2 Which Protection Levels Can Be Set for Basic Web Protection?.....	321
13.5.2 CC Attack Protection Rules.....	322
13.5.2.1 What Is the Peak Rate of CC Attack Protection?.....	322
13.5.2.2 How Do I Configure a CC Attack Protection Rule?.....	323
13.5.2.3 When Is Cookie Used to Identify Users?.....	323
13.5.2.4 What Are the Differences Between Rate Limit and Allowable Frequency in a CC Rule?.....	324
13.5.3 Precise Protection rules.....	324
13.5.3.1 Can a Precise Protection Rule Take Effect in a Specified Period?.....	324
13.5.3.2 Can a Path Containing # Be Matched in a Precise Protection Rule?.....	324
13.5.3.3 How Can I Allow Access from .js Files?.....	325
13.5.4 IP Address Blacklist and Whitelist.....	325
13.5.4.1 Can I Batch Add IP Addresses to a Blacklist or Whitelist Rule?.....	325
13.5.4.2 Can I Import or Export a Blacklist or Whitelist into or from WAF?.....	325
13.5.4.3 How Do I Block Abnormal IP Addresses?.....	325
13.5.5 Anti-Crawler Protection.....	327

13.5.5.1 Why Is the Requested Page Unable to Load After JavaScript Anti-Crawler Is Enabled?.....	327
13.5.5.2 Is There Any Impact on Website Loading Speed If Other Crawler Check in Anti-Crawler Is Enabled?.....	328
13.5.5.3 How Does JavaScript Anti-Crawler Detection Work?.....	328
13.5.6 Others.....	330
13.5.6.1 In Which Situations Will the WAF Policies Fail?.....	330
13.5.6.2 How Do I Allow Requests from Only IP Addresses in a Specified Geographical Region?.....	330
13.5.6.3 What Working Modes and Protection Mechanisms Does WAF Have?.....	332
13.5.6.4 What Types of Protection Rules Does WAF Support?.....	333
13.5.6.5 Which of the WAF Protection Rules Support the Log-Only Protective Action?.....	334
13.5.6.6 How Do I Allow Only Specified IP Addresses to Access Protected Websites?.....	334
13.5.6.7 Which Protection Rules Are Included in the System-Generated Policy?.....	338
13.5.6.8 Why Does the Page Fail to Be Refreshed After WTP Is Enabled?.....	339
13.5.6.9 What Are the Differences Between Blacklist/Whitelist Rules and Precise Protection Rules on Blocking Access Requests from Specified IP Addresses?.....	340
13.5.6.10 What Do I Do If a Scanner, such as AppScan, Detects that the Cookie Is Missing Secure or HttpOnly?.....	341
13.6 Protection Event Logs.....	341
13.6.1 Can WAF Log Protection Events?.....	341
13.6.2 How Do I Obtain Data about Block Actions?.....	342
13.6.3 What Does "Mismatch" for "Protective Action" Mean in the Event List?.....	342
13.6.4 How Long Can WAF Protection Logs Be Stored?.....	342
13.6.5 Can I Query Protection Events of a Batch of Specified IP Addresses at Once?.....	342
13.6.6 Will WAF Record Unblocked Events?.....	342
13.6.7 Why Is the Traffic Statistics on WAF Inconsistent with That on the Origin Server?.....	343
A Change History.....	344

1 Service Overview

1.1 What Is WAF?

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

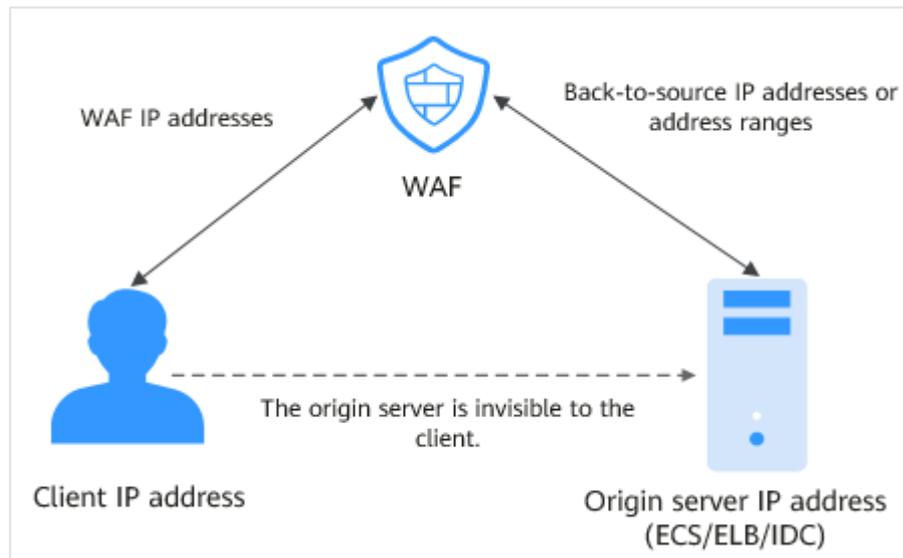
After applying for WAF, add the website to WAF on the WAF console. After a website is connected to WAF, all website access requests are forwarded to WAF first. WAF detects and filters out malicious attack traffic, and returns normal traffic to the origin server to ensure that the origin server is secure,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

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



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

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

- Cloud mode: protects your web applications on or off the cloud through domain names.
- Dedicated mode: protects your web applications on the cloud through domain names or IP addresses.

1.2 Edition Differences

WAF provides cloud and dedicated modes for you to deploy WAF instances. For more details, see [Cloud and Dedicated WAF Modes](#).

Cloud and Dedicated WAF Modes

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

Figure 1-3 Cloud and dedicated WAF deployment architectures

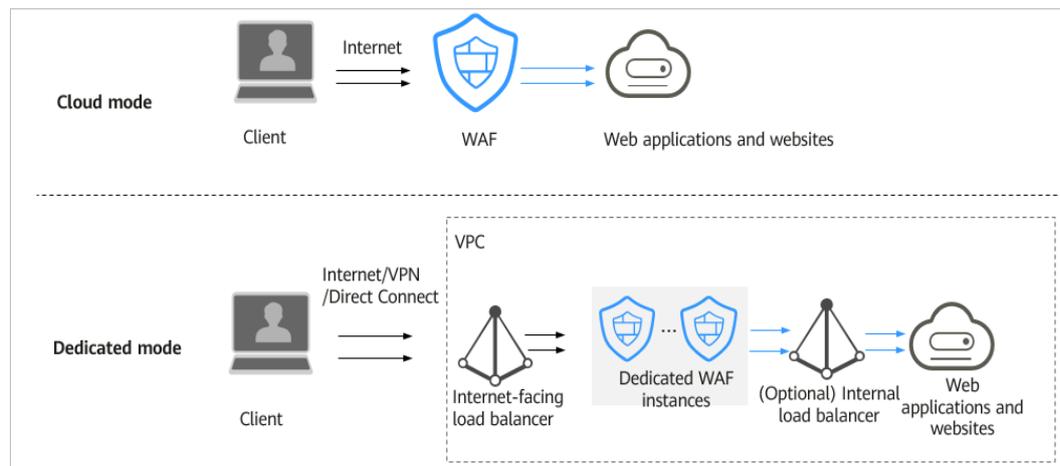


Table 1-1 Description of how to use different modes of WAF instances

Item	Cloud Mode	Dedicated mode
Billing mode	Pay-per-use	Pay-per-use
Application scenarios	Service servers are deployed on a cloud or in on-premises data centers.	Service servers are deployed on a cloud. Dedicated WAF instances are suitable large enterprise websites that have a large service scale and have customized security requirements.
Protection objects	Domain names	<ul style="list-style-type: none"> Domain names IP addresses
Advantages	<ul style="list-style-type: none"> Protection capability scaling by upgrading specifications Protection for cloud and on-premises web services 	<ul style="list-style-type: none"> Flexible deployment Exclusive use of WAF instances Protection against large-scale traffic attacks Low network latency with dedicated WAF instances being deployed in a VPC

Specifications Supported by Each Edition

Table 1-2 lists the specifications of cloud WAF and a dedicated WAF instance.

Table 1-2 Applicable service scale

Service Scale	Cloud Mode	Dedicated Mode
Peak rate of normal service requests	-	<p>The following lists the specifications of a single instance.</p> <ul style="list-style-type: none"> ● Specifications: WI-500. Referenced performance: <ul style="list-style-type: none"> - HTTP services - Recommended QPS: 5,000. Maximum QPS: 10,000. - HTTPS services - Recommended QPS: 4,000. Maximum QPS: 8,000. - WebSocket service - Maximum concurrent connections: 5,000 - Maximum WAF-to-server persistent connections: 60,000 ● Specifications: WI-100. Referenced performance: <ul style="list-style-type: none"> - HTTP services - Recommended QPS: 1,000. Maximum QPS: 2,000. - HTTPS services - Recommended QPS: 800. Maximum QPS: 1,600 - WebSocket service - Maximum concurrent connections: 1,000 - Maximum WAF-to-server persistent connections: 60,000 <p>NOTICE Maximum QPS values are for reference only. They may vary depending on your businesses. The real-world QPS is related to the request size and the type and quantity of protection rules you customize.</p>
Service bandwidth threshold (Origin servers are deployed on the cloud.)	-	<ul style="list-style-type: none"> ● Specifications: WI-500. Referenced performance: Throughput: 500 Mbit/s ● Specifications: WI-100. Referenced performance: Throughput: 100 Mbit/s
Number of domain names	30 (Supports three top-level domain names.)	2,000 (Supports 2,000 top-level domain names)

Service Scale	Cloud Mode	Dedicated Mode
Back-to-source IP address quantity (the number of WAF IP addresses that can be allowed by a protected domain name)	20	N/A
Quantity of supported ports	N/A	<ul style="list-style-type: none"> Standard ports: 80 and 443 Non-standard ports: Unlimited
Peak rate of CC attack protection	N/A	<ul style="list-style-type: none"> Specifications: WI-500. Referenced performance: Maximum QPS: 20,000 Specifications: WI-100. Referenced performance: Maximum QPS: 4,000
CC attack protection rules	200	100
Precise protection rules	1,000	100
Reference table rules	1,000	100
IP address blacklist and whitelist rules	2,000	100
Geolocation access control rules	200	100
Web tamper protection rules	200	100
Information leakage prevention rules	200	100
Global protection whitelist rules	2,000	1,000
Data masking rules	200	100

1.3 Basic Concepts

This document describes terms related to WAF.

CC Attack

Challenge Collapsar (CC) attacks are web attacks against web servers or applications. In CC attacks, attackers send a large amount of standard GET/POST requests to target system to exhaust web servers or applications. For example, attackers can send requests to URIs of databases or other resources to make the servers unable to respond to normal requests.

Cross-Site Request Forgery (CSRF)

CSRF, or XSRF is a common web attack. Attackers may trick the victim into submitting a malicious request that inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf. If the user is currently authenticated to the site, the site will have no way to distinguish between the forged request and a legitimate request sent by the victim, as browser requests always carry session cookies associated with the site.

Scanner

A scanner is a program that automatically detects security vulnerabilities on local or remote servers. It can quickly and accurately detect vulnerabilities of scanned targets and provide scanning results for users.

Web Tamper Protection

Web Tamper Protection (WTP) can protect your files, such as web pages, documents, mages, and databases, in specific directories against tampering and sabotage from hackers and viruses.

Cross-site Scripting (XSS) Attack

XSS is a type of attack that exploits security vulnerabilities in web applications. The attacker injects auto-executed malicious code into webpages to steal user information when they visit the pages.

SQL Injection

SQL injection is a common web attack whereby attackers inject malicious SQL commands into query strings of backend databases for the victim web application to deceive the server into executing them. By exploiting these commands, the attacker can obtain sensitive information, add users, export files, or even gain the highest permissions to the database or system.

Command Injection

Command injection is a cyber attack that executes fabricated OS commands and escape from a blacklist by calling web APIs to attack services.

Code Injection

Code injection is an attack that exploits logic defects of web applications in input validation or code execution vulnerabilities of some script functions.

Sensitive File Access

Sensitive files, such as configuration files and permission management files related to the operating system and application service framework, are mission-critical data. If sensitive files are accessible through Internet requests, the services will be at risk.

Server-Side Request Forgery

Server-side request forgery (SSRF) is a web security vulnerability constructed by an attacker to form a request initiated by the server. Generally, the target of an SSRF attack is the internal system that cannot be accessed from the external network. If a server supports obtaining data from other server applications but not filters or restricts destination addresses, an SSRF vulnerability may be made by attackers.

Web Shell

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

Hotlinking

Hotlinking is an act that a crafty website links to files hosted on your servers, instead of storing files on their own servers. Generally, the crafty website links to large files, such as images and videos, as large files use much more bandwidth than small ones. So you have to pay for access traffic of the bad actors. They steal your server bandwidth, making your website slow.

Multi-pattern Matching

Multi-pattern matching is a highly efficient multi-mode matching algorithm that is used for feature detection of request traffic, which greatly improves the performance of the detection engine.

Precise Protection

You can create a custom precise protection rule that combines multiple common HTTP fields, such as the URL, IP, Params, Cookie, Referer, User-Agent, and Header. You can also combine logic conditions to block or allow traffic precisely.

Blacklist and Whitelist

The IP address whitelist includes trusted IP addresses. Requests from the trusted IP addresses are forwarded without inspection. The IP address blacklist includes malicious IP addresses. The traffic from these IP addresses is handled based on inspection policies.

Intelligent Decoding

This is a method that intelligently identifies multiple codes in a request for infinite multi-layer obfuscation and performs in-depth decoding to obtain the original attack intent of the attacker.

Semantic Analysis-based Detection

A syntax tree is constructed based on the semantic context to analyze and determine whether the payload is an attack payload.

Rate Limit

Access control policies are used to limit the access over a specific interface.

Anti-Crawler

A powerful crawler feature library is used to detect varied types of crawlers, such as engine crawlers, script crawlers, and scanning tools.

A Record

An address (A) record maps a host name (or domain name) to the IP address of the server hosting the domain name.

SQL Injection Attack

SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution.

Non-standard Port

Non-standard ports are the ports other than ports 80 and 443.

1.4 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)	<p>WAF offers the cloud and dedicated modes to protect websites. You can add either domain names or IP addresses to WAF. Before you start, get familiar with the following differences:</p> <ul style="list-style-type: none"> • Cloud mode: protects your web applications on or off the cloud through domain names. • Dedicated mode: protects your web applications on the cloud through domain names or IP addresses.
	HTTP/HTTPS service protection	WAF can protect HTTP and HTTPS traffic for a website.
	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>NOTE If you set Protective Action to Block, 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 preset reputation database, WAF defends against Open Web Application Security Project (OWASP) top 10 threats, vulnerability exploits, web shells, and other threats.</p> <ul style="list-style-type: none"> ● General Check WAF defends against attacks such as SQL injections, XSS, file inclusions, Bash vulnerabilities, remote command execution, directory traversal, sensitive file access, and command/code injections. ● Web shell detection WAF protects against web shells from upload interface. ● Precise identification <ul style="list-style-type: none"> – WAF uses built-in semantic analysis engine and regex engine and supports configuring of blacklist/whitelist rules, which reduces false positives. – WAF supports anti-escape and automatic restoration of common codes, which improves the capability of recognizing deformation web attacks. WAF can decode the following types of code: url_encode, Unicode, XML, OCT, hexadecimal, HTML escape, and base64 code, case confusion, JavaScript, shell, and PHP concatenation confusion ● 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. ● Header detection WAF detects all header fields in the requests.
	CC attack protection rules	WAF can restrict access to a specific URL on your website based on a unique IP address, cookie, or referer field, mitigating CC attacks.

Function		Description
	<p>Precise protection rules</p> <p>NOTE If you set Protective Action to Block, 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>WAF enables you to combine common HTTP fields (such as IP, path, referer, user agent, and params) to configure powerful and precise access control policies. You can configure precision protection rules to protect workloads from hotlinking and block requests with empty fields.</p>
	<p>Blacklist and whitelist rules</p> <p>NOTE If you set Protective Action to Block, 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.</p>	<p>You can configure blacklist and whitelist rules to block, log only, or allow access requests from specified IP addresses.</p>
	<p>Geolocation access control rules</p>	<p>You can customize these rules to allow or block requests from a specific country or region.</p>
	<p>Web tamper protection rules</p>	<p>You can configure these rules to prevent a static web page from being tampered with.</p>
	<p>Website anti-crawler protection</p>	<p>WAF dynamically analyzes your website service models and accurately identifies crawler behavior based on data risk control and bot identification systems.</p>
	<p>Information leakage prevention rules</p>	<p>You can add two types of information leakage prevention rules.</p> <ul style="list-style-type: none"> • 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.

Function		Description
	Global protection whitelist rules	This function ignores certain attack detection rules for specific requests.
	Data masking rules	You can configure data masking rules to prevent sensitive data such as passwords from being displayed in event logs.
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 .	
PCI DSS/PCI 3DS compliance certification and TLS checks	<ul style="list-style-type: none"> • TLS has three versions (TLS v1.0, TLS v1.1, and TLS v1.2) and seven cipher suites. You can select the one best fits your business needs. • WAF supports PCI DSS and PCI 3DS compliance certification check. 	
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 .	
Advanced settings	PCI DSS/PCI 3DS compliance certification and TLS checks	<ul style="list-style-type: none"> • TLS has three versions (TLS v1.0, TLS v1.1, and TLS v1.2). You can select the one best fits your business needs. • WAF supports PCI DSS and PCI 3DS compliance certification check.

Function		Description
	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 .
Event management		<ul style="list-style-type: none"> • WAF allows you to view and handle false alarms for blocked or logged events. • You can download events data over the past five days. • You can use Log Tank Service (LTS) to record all WAF logs, including attack and access logs.
Notifications		You can enable notification for attack logs. If this function is enabled, WAF sends attack logs to you by the method you configure.
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"> • Centralized policy configuration On the WAF console, you can configure policies applicable to multiple protected domain names in a centralized manner so that the policies can be quickly delivered and take effect. • Traffic and event statistics WAF displays the number of requests, the number and types of security events, and log information in real time.
High flexibility and reliability		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.

1.5 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.

1.6 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.

1.7 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

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

Storage Mode

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

Access Control

Users can view only logs related to their own services.

1.8 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 Tenant Guest and Server Administrator roles. <ul style="list-style-type: none"> • Tenant Guest: A global role, which must be assigned in the global project. • Server Administrator: A project-level role, which must be assigned in the same project.
WAF FullAccess	All permissions for WAF	System-defined policy	None.

Role/Policy Name	Description	Category	Dependencies
WAF ReadOnlyAccess	Read-only permissions for WAF.	System-defined policy	

1.9 WAF and Other Services

This topic describes WAF and other cloud services.

CTS

Cloud Trace Service (CTS) records all WAF operations for you to query, audit, and backtrack.

Cloud Eye

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

For details about monitored WAF metrics, see [WAF Monitored Metrics](#).

ELB

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

IAM

Identity and Access Management (IAM) provides the permission management function for WAF. Only users granted WAF Administrator permissions can use WAF. To obtain this permission, contact the users who have the Security Administrator permissions.

LTS

Log Tank Service (LTS) collects log data from hosts and cloud services. WAF allows you to transfer WAF attack logs and access logs to LTS so that you can handle with logs in real time.

SMN

Simple Message Notification (SMN) service provides the notification function. After you enable the notification function in WAF, alarm information will be sent to you as configured once your domain name is attacked.

2 WAF Operation Guide

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

Procedure for Using WAF

[Figure 2-1](#) shows the procedure. [Table 2-1](#) describes the procedure.

Figure 2-1 Procedure for using WAF

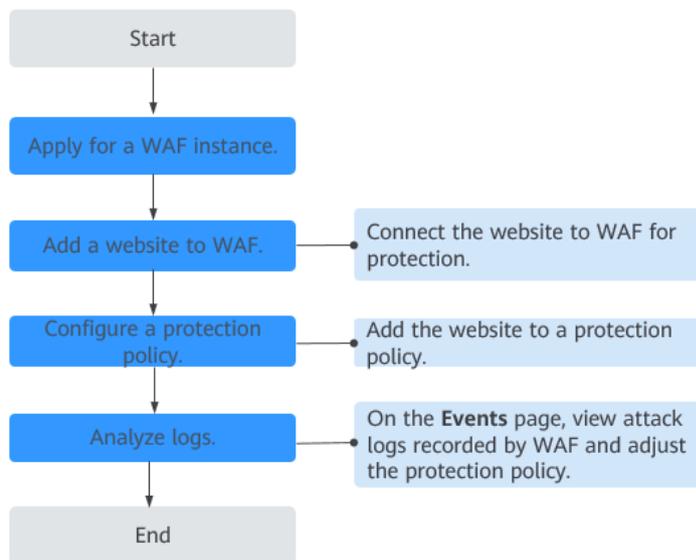


Table 2-1 Procedure for using WAF

Operation	Description
Apply for a WAF Instance	Apply for a WAF instance to enable WAF protection.

Operation	Description
Add a website to WAF.	<p>Add websites you want to protect to your WAF instance.</p> <ul style="list-style-type: none"> • Cloud mode: See Step 1: Add a Domain Name to WAF (Cloud Mode). • Dedicated mode: See Step 1: Add a Website to WAF (Dedicated Mode). <p>NOTE</p> <ul style="list-style-type: none"> • Using WAF does not affect your web server performance because the WAF engine is not running on your web server. • After your domain name is connected to WAF, there will be a latency of tens of milliseconds, which might be raised based on the size of the requested page or number of incoming requests.
Configure a protection policy.	<p>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.</p>
Analyze logs.	<p>WAF displays blocked or logged-only attacks on the Events page. You can view and analyze protection logs to adjust your website protection policies or mask false alarms.</p>
(Optional) Enable alarm notifications.	<p>Enable this function to receive an alarm notification the instant an attack is detected.</p> <p>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.</p>

Related Functions

Beyond functions in [Procedure for Using WAF](#), WAF also provides the following functions for you to improve your website security performance.

Table 2-2 Related functions

Function	Description
Dashboard	You can view protection data of yesterday, today, last 3 days, last 7 days, or last 30 days.
Configuring PCI DSS/3DS Certification Check and Configuring the Minimum TLS Version and Cipher Suite	TLS v1.0 and the cipher suite 1 are configured by default in WAF for general security. To protect your websites better, set the minimum TLS version to a later version and select a more secure cipher suite.

Function	Description
Configuring a Traffic Identifier for a Known Attack Source	WAF allows you to configure traffic identifiers by IP address, session, or user tag to block possibly malicious requests from known attack sources based on IP address , Cookie , or Params .
Editing Response Page for Blocked Requests	If a visitor is blocked by WAF, the Default block page of WAF is returned by default. You can also configure Custom or Redirection for the block page to be returned as required.
Managing Certificates	If you upload a certificate to WAF, you can directly select the certificate when adding a website to WAF.
Managing IP Address Blacklist and Whitelist Groups	With IP address groups, you can quickly add IP addresses or IP address ranges to a blacklist or whitelist rule.
Managing Dedicated Engines	This topic describes how to manage your dedicated WAF instances (or engines), including viewing instance information, viewing instance monitoring configurations, upgrading the instance edition, or deleting an instance.
Viewing Product Details	On the Product Details page, you can view information about all your WAF instances, including the edition, domain quotas, and specifications.

3 Enabling WAF

Before using WAF, enable a WAF instance.

This topic walks you through how to apply for a cloud WAF instance. A cloud WAF instance can protect your web servers either on the cloud or on premises.

If your service servers are deployed on the cloud, you can buy dedicated WAF instances (or dedicated WAF engines) to protect important web applications and services as long as they are accessible through domain names or IP addresses.

Prerequisites

- You have obtained management console login credentials for an account with the **WAF Administrator** and **WAF FullAccess** permissions.
- You have applied for a VPC before applying for a dedicated WAF instance.
- You have created resource sets.

Applying for a Cloud 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.

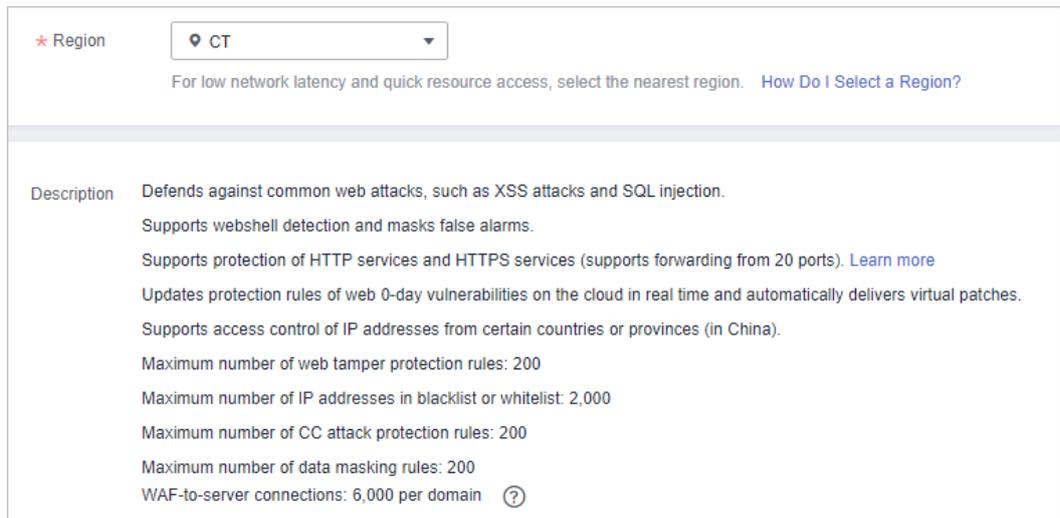
Step 3 Click  in the left upper corner and choose **Security > Web Application Firewall** to go to the **Dashboard** page.

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

Step 5 Select **Cloud Mode**.

Step 6 On the displayed page, select a region.

Figure 3-1 Enabling WAF



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

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

----End

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

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

Step 5 Select **Dedicated Mode**.

Step 6 On the **Apply for Web Application Firewall** page, set WAF instance parameters by referring to [Table 3-1](#).

Figure 3-2 Configuring a dedicated WAF instance

The screenshot shows the configuration interface for a dedicated WAF instance. The fields are as follows:

- Instance Name Prefix:** A text input field with the placeholder "Enter an instance name prefix."
- Quantity:** A numeric input field set to "2". A note below it states: "To ensure the SLA and prevent single points of failure (SPOFs), apply for at least two WAF instances for your workloads."
- Specifications:** Two buttons, "WAF-500" (selected) and "WAF-100". Below them, performance metrics are listed: "Single-instance performance (Reference only) Throughput: 500 Mbit/s; QPS: 5,000, Max. 10,000" and "WAF-to-Server connections supported: 60,000 per instance, 5,000 per domain".
- WAF Instance Type:** A button labeled "ECS". A note below it says: "Your WAF instance will be created on your ECS. You can view details of the ECS on the ECS console."
- CPU Architecture:** A button labeled "x86".
- ECS Specifications:** A section titled "Select any of the following ECSs to run your WAF instance." containing a table:

Flavor Name	vCPUs Memory	System Disk (High I/O)	Data Disk (Ultra-high I/O)
<input checked="" type="radio"/> c6.2xlarge.2	8 vCPUs 16 GB	40 GB	200 GB
- VPC:** A dropdown menu showing "--Select VPC--" and a "View VPC" link.
- Subnet:** A dropdown menu showing "--Select subnet--" and a refresh icon.
- Security Group:** A dropdown menu showing "default (5bcb2ed3-4d8a-4328-83bf-98..." and a "Manage Security Group" link.

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. To ensure the SLA and prevent single points of failure (SPOFs), apply for at least two WAF instances for your workloads.
Specifications	Select specifications for your instance. WAF offers two types of specifications, 500 Mbit/s and 100 Mbit/s.
WAF Instance Type	ECS Your WAF instance will be created on your ECS. You can view details of the ECS on the ECS console.
CPU Architecture	Select CPU architecture for your instance.
ECS Specifications	Select ECS specifications for your instance.

Parameter	Description
VPC	Select the VPC to which the origin server belongs.
Subnet	Select a subnet configured in the VPC.
Security Group	<p>Select a security group in the region or click Manage Security Group to go to the VPC console and create a security group. After you select a security group, the WAF instance will be protected by the access rules of the security group.</p> <p>NOTICE</p> <ul style="list-style-type: none"> • You can configure your security group as follows: <ul style="list-style-type: none"> - Inbound rules Add an inbound rule to allow incoming network traffic to pass through over a specified port based on your service requirements. For example, if you want to allow access from port 80, you can add a rule that allows TCP and port 80. - Outbound rules The value is Default. All outgoing network traffic is allowed by default. • If your dedicated WAF instance and origin server are not in the same VPC, enable communications between the instance and the subnet of the origin server in the security group.

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

Step 8 Confirm the configuration and click **Apply Now**.

Step 9 Click **Back to Dedicated Engine List**. On the **Dedicated Engine** page, view the instance status.

----End

4 Dashboard

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

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 4-1](#).

Table 4-1 QPS calculation

Time Range	Average QPS Description	Peak QPS Description
Yesterday or Today	The QPS curve is made with the average QPS in every minute.	The QPS curve is made with each peak QPS in every minute.
Past 3 days	The QPS curve is made with the average QPS in every five minutes.	The QPS curve is made with each peak QPS in every five minutes.

Time Range	Average QPS Description	Peak QPS Description
Past 7 days	The QPS curve is made with the maximum value among the average QPS in every five minutes at a 10-minute interval.	The QPS curve is made with each peak QPS in every 10 minutes.
Past 30 days	The QPS curve is made with the maximum value among the average QPS in every five minutes at a one-hour interval.	The QPS curve is made with the peak QPS in every hour.

 **NOTE**

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

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the left upper corner and choose **Security > Web Application Firewall** to go to the **Dashboard** page.
- Step 4** In the upper part of the page, specify the website, instance, and time range for your query.
 - By default, the information about all websites you add to WAF in all enterprise projects are displayed.
 - **Domain Names:** shows information about websites added to the WAF instance. Click **View** to go to the **Website Settings** page and view details about domain names of protected websites.
 - Query time: You can select **Yesterday**, **Today**, **Past 3 days**, **Past 7 days**, or **Past 30 days**.

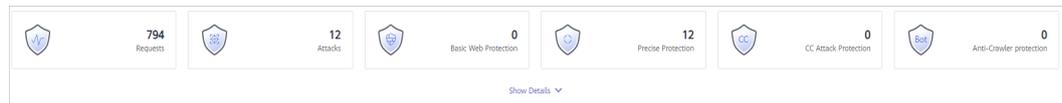
Figure 4-1 Setting search criteria



- Step 5** View how many requests, attacks, and attacked pages by attack type over the specified time range.
 - **Requests:** shows the page views of the website, making it easy for you to view the total number of pages accessed by visitors in a certain period of time.
 - **Attacks:** shows how many times the website are attacked.

- You can view how many pages are attacked by a certain type of attack within a certain period of time.
- You can click **Show Details** to view the details of the 10 domain names with the most requests, attacks, and basic web protection, precise protection, CC attack protection, and anti-crawler protection actions.

Figure 4-2 Protection action statistics



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

By day: You can select this option to view the data gathered by the day. If you leave this option unselected, you have the following options:

- **Yesterday** and **Today:** Security event data is gathered every minute.
- **Past 3 days:** Security event data is gathered every 5 minutes.
- **Past 7 days:** Security event data is gathered every 10 minutes.
- **Past 30 days:** Security event data is gathered every hour.

Figure 4-3 Security Event Statistics

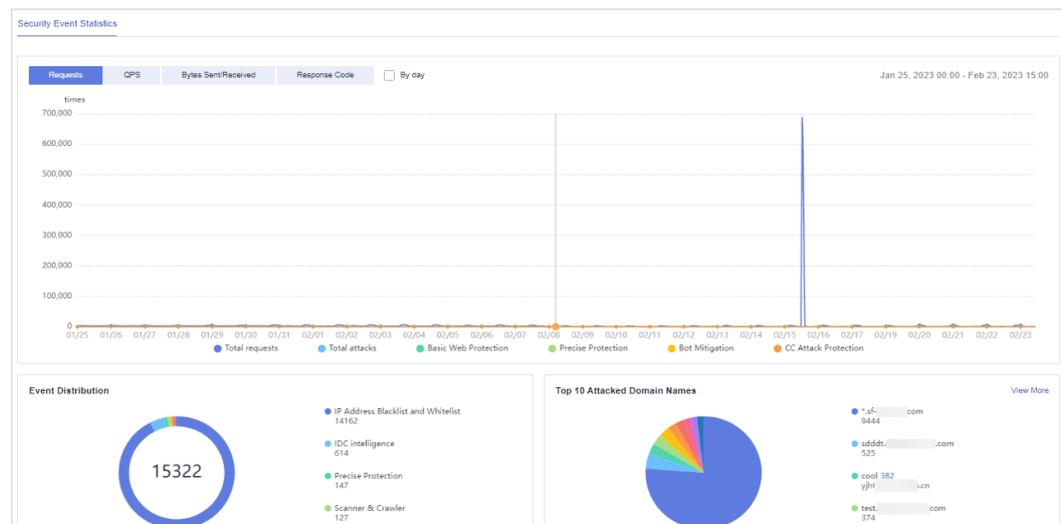


Table 4-2 Parameters in Security Event Statistics

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

Parameter	Description
QPS	<p>Average number of requests per second for the domain name. For details about the values of QPS, see How to Calculate QPS.</p> <p>Queries Per Second (QPS) indicates the number of requests per second. For example, an HTTP GET request is also called a query.</p>
Bytes Sent/Received	<p>Bandwidth usage</p> <p>The value of sent and received bytes is calculated by adding the values of request_length and upstream_bytes_received by time, so the value is different from the network bandwidth monitored on the EIP. This value is also affected by web page compression, connection reuse, and TCP retransmission.</p>
Response Code	<p>Response codes returned by WAF to the client or returned by the origin server to WAF along with the corresponding number of responses. You can click WAF to Client or Origin Server to WAF to view the corresponding information.</p> <p>The number of response codes is accumulated based on the sequence of response codes (from left to right) in the lower part of the chart. The number of response codes is the difference between two lines. If the value of a response code is 0, the line of the response code overlaps that of the previous response code.</p>
Event Distribution	<p>Types of attack events</p> <p>Click an area in the Event Distribution area to view the type, number, and proportion of an attack.</p>
Top 10 Attacked Domain Names	<p>The ten most attacked domain names and the number of attacks on each domain name.</p> <p>Click View More to go to the Events page and view more protection data.</p>
Top 10 Attack Source IP Addresses	<p>The ten source IP addresses with the most attacks and the number of attacks from each source IP address.</p> <p>Click View More to go to the Events page and view more protection data.</p>
Top 10 Attacked URLs	<p>The ten most attacked URLs and the number of attacks on each URL.</p> <p>Click View More to go to the Events page and view more protection data.</p>

----End

5 Events

5.1 Viewing Protection Event Logs

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

Prerequisites

The website to be protected has been connected to WAF.

Constraints

- If the security software installed on your server blocks the event file from being downloaded, close the software and download the file again.
- On the WAF console, you can view the event data for all protected domain names over the last 30 days. You can authorize LTS to log WAF activities so that you can view attack and access logs and store all logs for a long time. For more details, see. [Enabling LTS for WAF Logging](#).
- If you switch the WAF working mode for a website to **Suspended**, WAF only forwards all requests to the website without inspection. It does not log any attack events neither.

Procedure

Step 1 Log in to the management console.

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

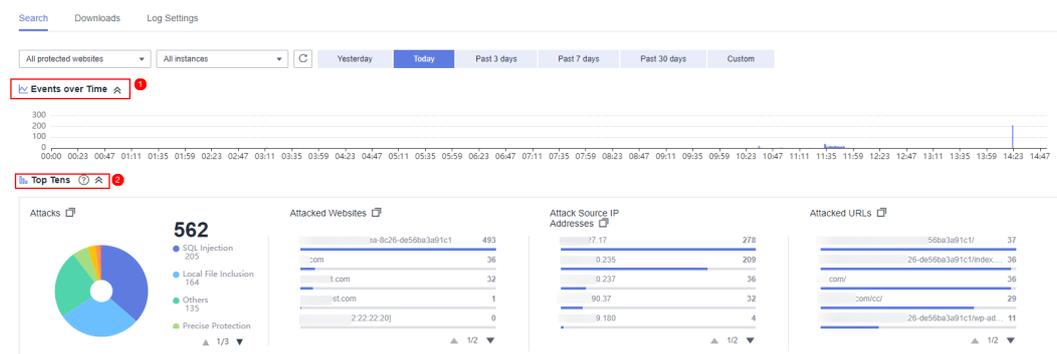
Step 3 Click  in the upper left corner and choose **Web Application Firewall** under **Security**.

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

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

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

Figure 5-1 Events



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

- Configure a filter by combining several conditions. Then, click **OK**. Conditions will be displayed above the event list. [Table 5-2](#) lists parameters for filter conditions.
- Click  to select fields you want to display in the event lists.
- To view event details, locate the row containing the event and click **Details** in the **Operation** column.

Figure 5-2 Events

The screenshot shows the 'Events' table with the following columns: Time, Source IP Address, Domain Name, Geolocation, Event Type, Protective Action, and Operation. Two event rows are displayed:

Time	Source IP Address	Domain Name	Geolocation	Event Type	Protective Action	Operation
Aug 01, 2022 18:24:09	100.100.100.100	hsk2.com	unknown	SQL Injection	Block	Details Handle
Aug 01, 2022 17:18:17	100.100.100.100	hsk2.com	unknown	SQL Injection	Block	Details Handle

Table 5-1 Search condition fields

Parameter	Parameter
Event ID	ID of the event.
Event Type	Type of the attack. By default, All is selected. You can view logs of all attack types or select an attack type to view corresponding attack logs.
Rule ID	ID of a built-in protection rule in WAF basic web protection

Parameter	Parameter
Protective Action	The options are Block , Log only , and Verification code . Verification code: In CC attack protection rules, you can set Protective Action to Verification code . If a visitor sends too many requests, with the request quantity exceeding the rate limit specified by the CC attack protection rule used, a message is displayed to ask the visitor to provide a verification code. Visitor's requests will be blocked unless they enter a valid verification code.
Source IP Address	Public IP address of the web visitor/attacker By default, All is selected. You can view logs of all attack source IP addresses, select an attack source IP address, or enter an attack source IP address to view corresponding attack logs.
URL	Attacked URL

Table 5-2 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
Rule ID	ID of a built-in protection rule in WAF basic web protection	-
URL	Attacked URL	/admin
Event Type	Type of attack	SQL injection
Protective Action	Protective actions configured in the rule. The options are Block , Log only , and Verification code . NOTE If an access request matches a web tamper protection rule, information leakage prevention rule, or data masking rule, the protective action is marked as Mismatch .	Block
Status Code	HTTP status code returned on the block page.	418

Parameter	Description	Example Value
Malicious Load	<p>The location or part of the attack that causes damage or the number of times that the URL was accessed.</p> <p>NOTE</p> <ul style="list-style-type: none"> In a CC attack, the malicious load indicates the number of times that the URL was accessed. For blacklist protection events, the malicious load is left blank. 	id=1 and 1='1

----End

5.2 Handling False Alarms

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

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

Prerequisites

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

Constraints

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

- Dedicated WAF instances earlier than June 2022 do not support **All protection** for **Ignore WAF Protection**. Only **Basic web protection** can be selected.

Application Scenarios

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

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.

Table 5-3 Parameters

Parameter	Description	Example Value
Scope	<ul style="list-style-type: none"> – All domain names: By default, this rule will be used to all domain names that are protected by the current policy. – Specified domain names: Specify a domain name range this rule applies to. 	Specified domain names

Parameter	Description	Example Value
Domain Name	<p>This parameter is mandatory when you select Specified domain names for Scope.</p> <p>Enter a single domain name that matches the wildcard domain name being protected by the current policy.</p>	www.example.com
Condition List	<p>Click Add to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. A condition includes the following parameters:</p> <p>Parameters for configuring a condition are described as follows:</p> <ul style="list-style-type: none"> - Field - Subfield: Configure this field only when Params, Cookie, or Header is selected for Field. <p>NOTICE 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"> - Logic: Select a logical relationship from the drop-down list. - Content: Enter or select the content that matches the condition. 	Path, Include, / product
Ignore WAF Protection	<ul style="list-style-type: none"> - All protection: All WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule. - Basic web protection: You can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, if XSS check is not required for a URL, you can whitelist XSS rule. 	Basic web protection

Parameter	Description	Example Value
Ignored Protection Type	<p>If you select Basic web protection for Ignored Protection Type, specify the following parameters:</p> <ul style="list-style-type: none"> - ID: Configure the rule by event ID. - Attack type: Configure the rule by attack type, such as XSS and SQL injection. One type contains one or more rule IDs. - All built-in rules: all checks enabled in Basic Web Protection. 	Attack type
Rule ID	<p>This parameter is mandatory when you select ID for Ignored Protection Type.</p> <p>Rule ID of a misreported event in Events whose type is not Custom. You are advised to handle false alarms on the Events page.</p>	041046
Rule Type	<p>This parameter is mandatory when you select Attack type for Ignored Protection Type.</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	<p>A brief description of the rule. This parameter is optional.</p>	SQL injection attacks are not intercepted.

Parameter	Description	Example Value
Advanced Settings	<p>To ignore attacks of a specific field, specify the field in the Advanced Settings area. After you add the rule, WAF will stop blocking attack events of the specified field.</p> <p>Select a target field from the first drop-down list box on the left. The following fields are supported: Params, Cookie, Header, Body, and Multipart.</p> <ul style="list-style-type: none"> - If you select Params, Cookie, or Header, you can select All or Field to configure a subfield. - If you select Body or Multipart, you can select All. - If you select Cookie, the Domain Name box for the rule can be empty. <p>NOTE If All is selected, WAF will not block all attack events of the selected field.</p>	Params All

- 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 triggering the event will be blocked or allowed based on the policy used for the address group.
Add to: You can select an existing address group or create an address group.
- Add the source IP address to a blacklist or whitelist rule of the corresponding protected domain name. Locate the row containing the desired event. In the **Operation** column, click **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 5-4 Parameter

Parameter	Description
Add to	<ul style="list-style-type: none"> - Existing rule - New rule
Rule Name	<ul style="list-style-type: none"> - If you select Existing rule for Add to, select a rule name from the drop-down list. - If you select New rule for Add to, customize a blacklist or whitelist rule.

Parameter	Description
IP Address/Range/Group	This parameter is mandatory when you select New rule for Add to . You can select IP address/Range or Address Group to add IP addresses a blacklist or whitelist rule.
Group Name	This parameter is mandatory when you select Address group for IP Address/Range/Group . Select an address group from the drop-down list. You can also click New address group to create an address group. For details, see Adding an IP Address Group .
Protective Action	<ul style="list-style-type: none"> - Block: Select Block if you want to blacklist an IP address or IP address range. - Allow: Select Allow if you want to whitelist an IP address or IP address range. - Log only: Select Log only if you want to observe an IP address or IP address range.
Known Attack Source	If you select Block for Protective Action , you can select a blocking type of a known attack source rule. WAF will block requests matching the configured IP address, Cookie, or Params for a length of time configured as part of the rule.
Rule Description	A brief description of the rule. This parameter is optional.

----End

Verification

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

Related Operations

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

5.3 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 **Downloads** tab and download the desired protection data. [Table 5-5](#) describes the parameters.

Table 5-5 Parameter description

Parameter	Description
File Name	The format is <i>file-name.csv</i> .
Number of Events	Total number of blocked and logged events NOTE Each file can include a maximum of 5,000 events. If there are more than 5,000 events, another file is generated.

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

----End

Fields in a Protection Event Data File

Field	Description	Example Value
action	Protective action taken in response to the event	block
attack	Attack type	SQL Injection
body	Request content of the attack	N/A
cookie	Cookie of the attacker	N/A
headers	Header of the attacker	N/A
host	Domain name or IP address of the protected website	www.example.com
id	ID of the event.	02-11-16-20201121060347-feb42002
payload	The part of the attack that causes damage to the protected website	python-requests/2.20.1
payload_location	The location of the attack that causes damage or the number of times that the URL is accessed by the attacker	user-agent
policyid	Policy ID.	d5580c8f6cd4403ebbf85892d4bb b8e4
request_line	Request line of the attack	GET /
rule	ID of the rule against which the event is generated.	81066
sip	Public IP address of the web visitor/attacker	N/A
time	When the event occurred.	2020/11/21 0:20:44
url	URL of the protected domain name	N/A

5.4 Enabling LTS for WAF Logging

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

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

Prerequisites

- You have applied for your WAF.
- The website to be protected has been added to WAF.

Impact on the System

Enabling LTS for WAF does not affect WAF performance.

Enabling LTS for WAF Protection Event Logging

Step 1 Log in to the management console.

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

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

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

Step 5 Click the tab, enable LTS (), and select a log group and log stream. [Table 5-6](#) describes the parameters.

Figure 5-3 Log settings

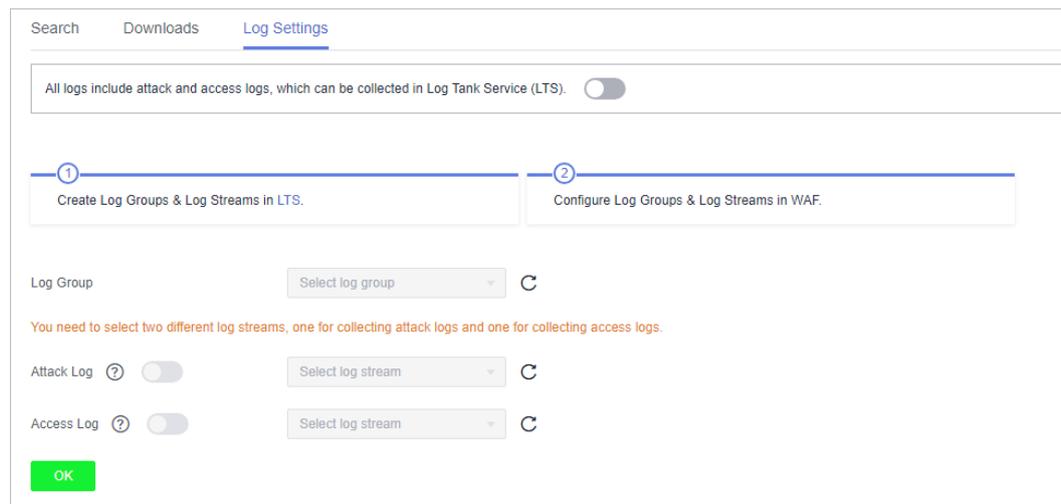


Table 5-6 Log configuration

Parameter	Description	Example Value
Log Group	Select a log group.	lts-group-waf
Attack Log	Select a log stream. An attack log includes information about event type, protective action, and attack source IP address of each attack.	lts-topic-waf-attack
Access Log	Select a log stream. An access log includes key information about access time, client IP address, and resource URL of each HTTP access requests.	lts-topic-waf-access

Step 6 Click **OK**.

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

----End

Viewing WAF Protection Event Logs on LTS

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

Step 1 Log in to the management console.

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

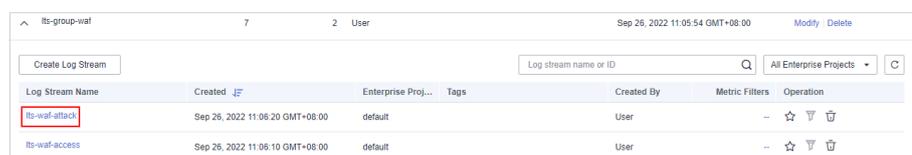
Step 3 Click  in the upper left corner of the page and choose **Management & Deployment > Log Tank Service**.

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

Step 5 View protection event logs.

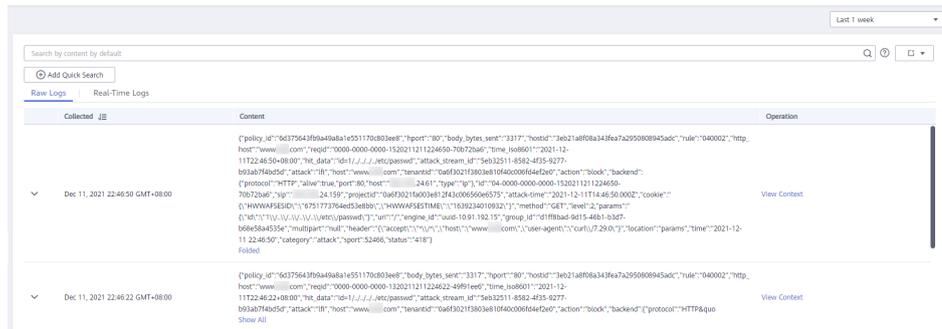
- View attack logs.
 - a. In the log stream list, click the name of the configured attack log stream.

Figure 5-4 Log stream name configured for attack logs



b. View attack logs.

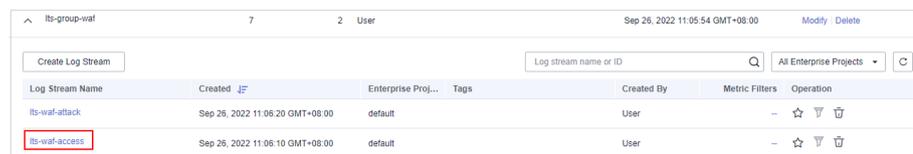
Figure 5-5 Viewing attack logs



- View access logs.

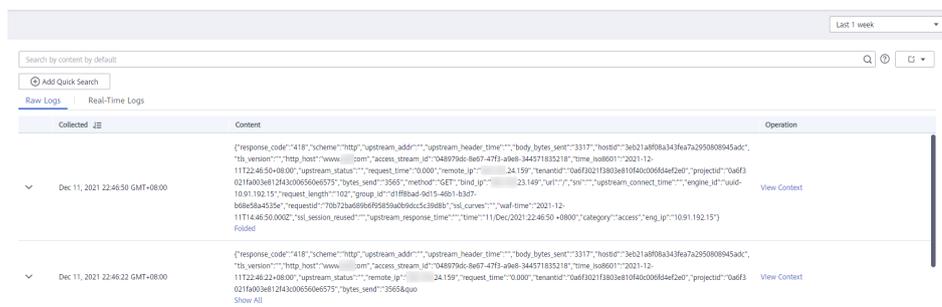
- a. In the log stream list, click the name of the configured access log stream.

Figure 5-6 Log stream name configured for access logs



b. View access logs.

Figure 5-7 Viewing access logs



----End

WAF access_log Field

Field	Type	Field Description	Description
access_log.requestid	string	Random ID	The value is the same as the last eight characters of the req_id field in the attack log.
access_log.time	string	Access time	GMT time a log is generated.

Field	Type	Field Description	Description
access_log.connection_requests	string	Sequence number of the request over the connection	-
access_log.eng_ip	string	IP address of the WAF engine	-
access_log.pid	string	The engine that processes the request	Engine (worker PID).
access_log.hostid	string	Domain name identifier of the access request.	Protected domain name ID (upstream_id).
access_log.tenantid	string	Account ID	ID of your account.
access_log.projectid	string	ID of the project the protected domain name belongs to	Project ID of a user in a specific region.
access_log.remote_ip	string	Remote IP address of the request at layer 4	IP address from which a client request originates. NOTICE If a layer-7 proxy is deployed in front of WAF, this field indicates the IP address of the proxy node closest to WAF. The real IP address of the visitor is specified by the x-forwarded-for and x_real_ip fields.
access_log.remote_port	string	Remote port of the request at layer 4	Port used by the IP address from which a client request originates
access_log.sip	string	IP address of the client that sends the request	For example, XFF.

Field	Type	Field Description	Description
access_log.scheme	string	Request protocol	Protocols that can be used in the request: <ul style="list-style-type: none"> • HTTP • HTTPS
access_log.response_code	string	Response code	Response status code returned by the origin server to WAF.
access_log.method	string	Request method.	Request type in a request line. Generally, the value is GET or POST .
access_log.http_host	string	Domain name of the requested server.	Address, domain name, or IP address entered in the address bar of a browser.
access_log.url	string	Request URL.	Path in a URL (excluding the domain name).
access_log.request_length	string	Request length.	The request length includes the access request address, HTTP request header, and number of bytes in the request body.
access_log.bytes_send	string	Total number of bytes sent to the client.	Number of bytes sent by WAF to the client.
access_log.body_bytes_sent	string	Total number of bytes of the response body sent to the client	Number of bytes of the response body sent by WAF to the client
access_log.upstream_addr	string	Address of the backend server.	IP address of the origin server for which a request is destined. For example, if WAF forwards requests to an ECS, the IP address of the ECS is returned to this parameter.
access_log.request_time	string	Request processing time	Processing time starts when the first byte of the client is read (unit: s).
access_log.upstream_response_time	string	Backend server response time	Time the backend server responds to the WAF request (unit: s).

Field	Type	Field Description	Description
access_log.upstream_status	string	Backend server response code	Response status code returned by the backend server to WAF.
access_log.upstream_connect_time	string	Time for the origin server to establish a connection to its backend services. Unit: second.	When SSL is used, the time for the handshake process is also recorded. Time used for establishing a connection for a request. Use commas (,) to separate the time used for each request.
access_log.upstream_header_time	string	Time used by the backend server to receive the first byte of the response header. Unit: second	Response time for multiple requests. Use commas (,) to separate the time used for each response.
access_log.bind_ip	string	WAF engine back-to-source IP address.	Back-to-source IP address used by the WAF engine.
access_log.group_id	string	LTS log group ID	ID of the log group for interconnecting WAF with LTS.
access_log.access_stream_id	string	Log stream ID.	ID of access_stream of the user in the log group identified by the group_id field.
access_log.engine_id	string	WAF engine ID	Unique ID of the WAF engine.
access_log.time_iso8601	string	ISO 8601 time format of logs.	-
access_log.sni	string	Domain name requested through SNI.	-

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

Field	Type	Field Description	Description
access_log.x_real_ip	string	Real IP address of the client when a proxy is deployed in front of WAF.	Real IP address of the client, which is identified by the proxy.
access_log.intel_crawler	string	Used for intelligence anti-crawler analysis.	-
access_log.ssl_ciphers_md5	string	MD5 value of the SSL cipher (ssl_ciphers).	-
access_log.ssl_cipher	string	SSL cipher used.	-
access_log.web_tag	string	Website name.	-
access_log.user_agent	string	User agent in the request header.	-
access_log.upstream_response_length	string	Backend server response size.	-
access_log.region_id	string	Region where the request is received.	-
access_log.enterprise_project_id	string	ID of the enterprise project that the requested domain name belongs to.	-

Field	Type	Field Description	Description
access_log.referrer	string	Referer content in the request header.	The value can contain a maximum of 128 characters. Characters over 128 characters will be truncated.
access_log.rule	string	Protection rule that the request matched.	If multiple rules are matched, only one rule is displayed.

WAF attack_log field description

Field	Type	Field Description	Description
attack_log.category	string	Log category	The value is attack .
attack_log.time	string	Log time	-
attack_log.time_iso8601	string	ISO 8601 time format of logs.	-
attack_log.policy_id	string	Policy ID	-
attack_log.level	string	Protection level	Protection level of a built-in rule in basic web protection <ul style="list-style-type: none"> ● 1: Low ● 2: Medium ● 3: High

Field	Type	Field Description	Description
attack_log.attack	string	Type of attack	<p>Attack type. This parameter is listed in attack logs only.</p> <ul style="list-style-type: none"> • default: default attacks • sqli: SQL injections • xss: cross-site scripting (XSS) attacks • webshell: web shells • robot: malicious crawlers • cmdi: command injections • rfi: remote file inclusion attacks • lfi: local file inclusion attacks • illegal: unauthorized requests • vuln: exploits • cc: attacks that hit the CC protection rules • custom_custom: attacks that hit a precise protection rule • custom_blackip: attacks that hit an IP address blacklist or whitelist rule • custom_geoip: attacks that hit a geolocation access control rule • antitamper: attacks that hit a web tamper protection rule • anticrawler: attacks that hit the JS challenge anti-crawler rule • leakage: vulnerabilities that hit an information leakage prevention rule • antiscan_high_freq_scan: Attacks that hit malicious scanning rules. • followed_action: The source is marked as a known attack source.
attack_log.action	string	Protective action	<p>WAF defense action.</p> <ul style="list-style-type: none"> • block: WAF blocks attacks. • log: WAF only logs detected attacks. • captcha: Verification code

Field	Type	Field Description	Description
attack_log.sub_type	string	Crawler types	When attack is set to robot , this parameter cannot be left blank. <ul style="list-style-type: none"> • script_tool: Script tools • search_engine: Search engines • scanner: Scanning tools • uncategorized: Other crawlers
attack_log.rule	string	ID of the triggered rule or the description of the custom policy type.	-
attack_log.rule_name	string	Description of a custom rule type.	This field is empty when a basic protection rule is matched.
attack_log.location	string	Location triggering the malicious load	-
attack_log.req_body	string	Request body.	-
attack_log.resp_headers	string	Response header	-
attack_log.hit_data	string	String triggering the malicious load	-
attack_log.resp_body	string	Response body	-
attack_log.backend.protocol	string	Backend protocol.	-
attack_log.backend.alive	string	Backend server status.	-
attack_log.backend.port	string	Backend server port.	-
attack_log.backend.host	string	Backend server host value.	-
attack_log.backend.type	string	Backend server type.	IP address or domain name.

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

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

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

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

6 Policies

6.1 How to Configure WAF Protection

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

Process of Configuring Policies

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

Table 6-1 Configurable protection rules

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

Protection Rule	Description	Reference
Blacklist and whitelist rules	You can configure blacklist and whitelist rules to block, log only, or allow access requests from specified IP addresses.	Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses
Known attack source rules	These rules can block the IP addresses from which blocked malicious requests originate. These rules are dependent on other rules.	Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration
Geolocation access control rules	You can customize these rules to allow or block requests from a specific country or region.	Configuring Geolocation Access Control Rules to Block or Allow Requests from Specific Locations
Web tamper protection rules	You can configure these rules to prevent a static web page from being tampered with.	Configuring Web Tamper Protection Rules to Prevent Static Web Pages from Being Tampered With
Website anti-crawler protection	This function dynamically analyzes website service models and accurately identifies crawler behavior based on data risk control and bot identification systems, such as JS Challenge.	Configuring Anti-Crawler Rules
Information leakage prevention rules	You can add two types of information leakage prevention rules. <ul style="list-style-type: none"> • Sensitive information filtering: prevents disclosure of sensitive information (such as ID numbers, phone numbers, and email addresses). • Response code interception: blocks the specified HTTP status codes. 	Configuring Information Leakage Prevention Rules to Protect Sensitive Information from Leakage
Global protection whitelist rules	You can configure these rules to let WAF ignore certain rules for specific requests.	Configuring a Global Protection Whitelist Rule to Ignore False Alarms

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

WAF Rule Priorities

The built-in protection rules of WAF help you defend against common web application attacks, including XSS attacks, SQL injection, crawlers, and web shells. You can customize protection rules to let WAF better protect your website services using these custom rules. [Figure 6-1](#) shows how WAF engine built-in protection rules work. [Figure 6-2](#) shows the detection sequence of rules you configured.

Figure 6-1 WAF engine work process

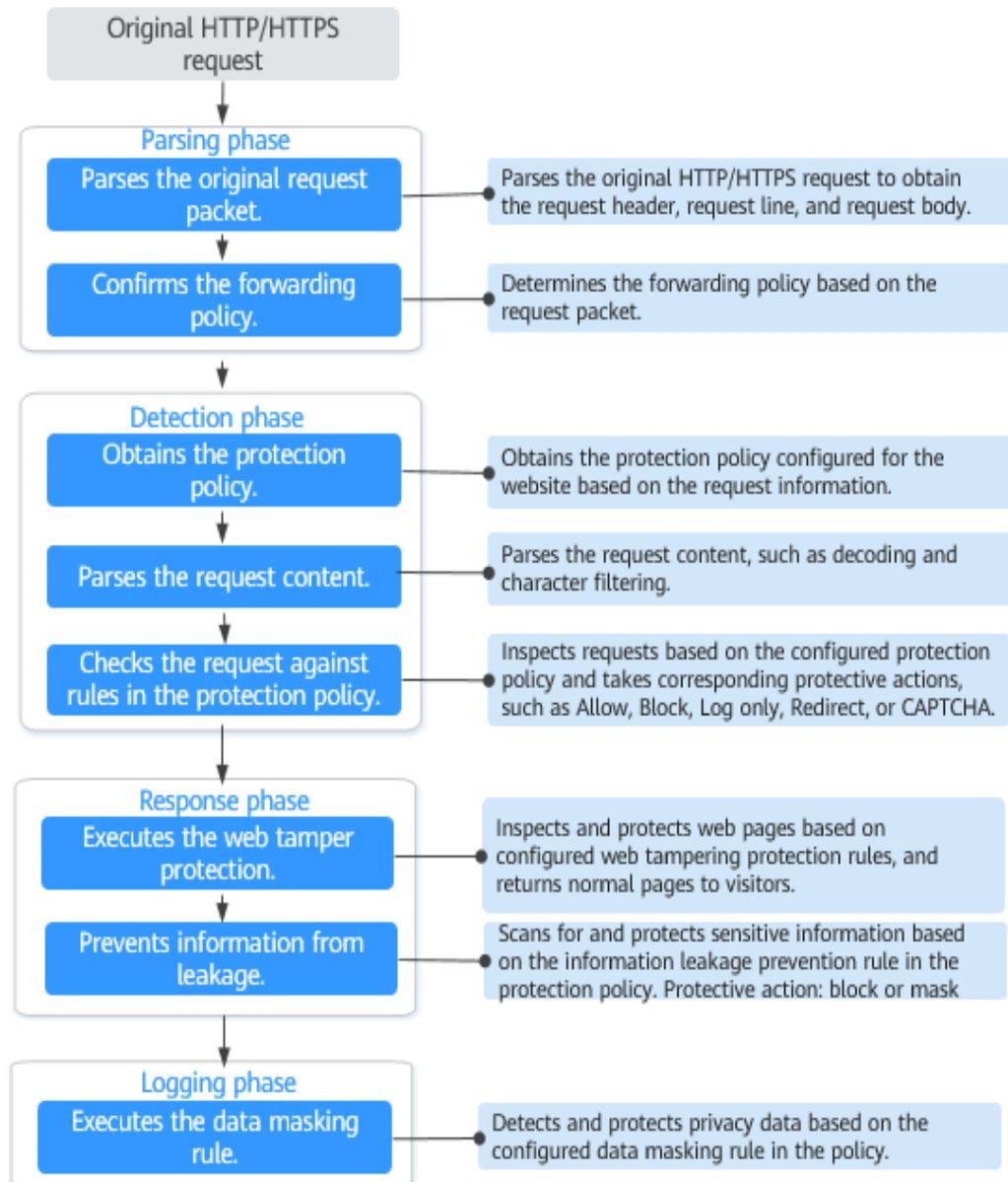
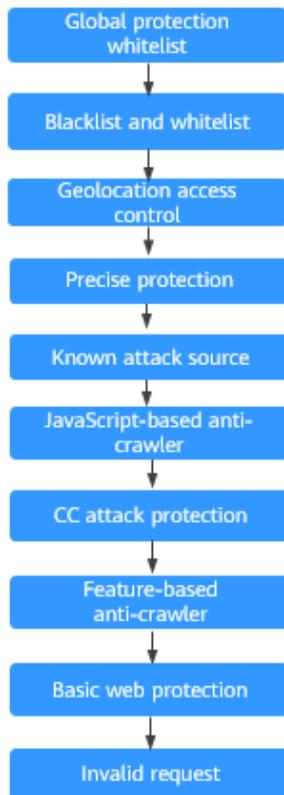


Figure 6-2 Priorities of protection rules



Response actions

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

6.2 Configuring Basic Protection Rules to Defend Against Common Web Attacks

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

Prerequisites

You have [added your website to a policy](#).

Constraints

- Basic web protection has two modes: **Block** and **Log only**.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- If you select **Block** for **Basic Web Protection**, you can [configure access control criteria for a known attack source](#). WAF will block requests matching the configured IP address, cookie, or params for a length of time configured as part of the rule.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** Click the name of the target policy to go to the protection configuration page.
- Step 6** In the **Basic Web Protection** configuration area, change **Status** and **Mode** as needed by referring to [Table 6-2](#).

Figure 6-3 Basic Web Protection configuration area



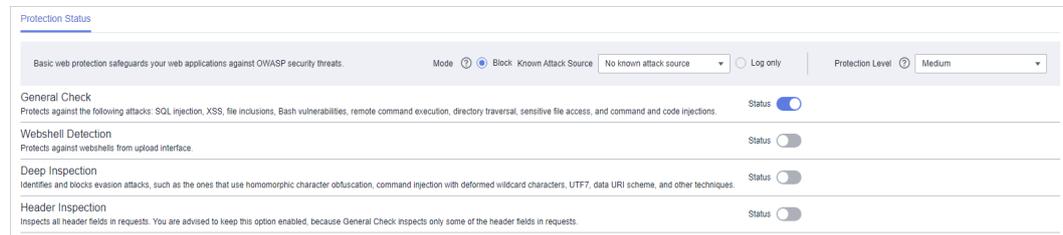
Table 6-2 Parameter description

Parameter	Description
Status	Status of Basic Web Protection <ul style="list-style-type: none"> •  : enabled. •  : disabled.
Mode	<ul style="list-style-type: none"> • Block: WAF blocks and logs detected attacks. • Log only: WAF only logs detected attacks.

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

Step 8 Click the **Protection Status** tab, and enable protection types one by one by referring to [Table 6-4](#).

Figure 6-4 Basic web protection



- Set the protective action.
 - Block:** WAF blocks and logs detected attacks.
If you select **Block**, you can select a known attack source rule to let WAF block requests accordingly. For details, see [Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration](#).
 - Log only:** WAF only logs detected attacks.
- Set the protection level.
In the upper part of the page, set **Protection Level** to **Low**, **Medium**, or **High**. The default value is **Medium**.

Table 6-3 Protection levels

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

- Set the protection type.

NOTICE

By default, **General Check** is enabled. You can enable other protection types by referring to [Table 6-4](#).

Table 6-4 Protection types

Type	Description
General Check	<p>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.</p> <p>NOTE If you enable General Check, WAF checks your websites based on the built-in rules.</p>
Webshell Detection	<p>Protects against web shells from upload interface.</p> <p>NOTE If you enable Webshell Detection, WAF detects web page Trojan horses inserted through the upload interface.</p>
Deep Inspection	<p>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.</p> <p>NOTE If you enable Deep Inspection, WAF detects and defends against evasion attacks in depth.</p>
Header Inspection	<p>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.</p> <p>NOTE If you enable this function, WAF checks all header fields in the requests.</p>

Step 9 Click the **Protection Rules** tab to view details. For more details about the parameters, see [Table 6-5](#).

 **NOTE**

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

Table 6-5 Protection rules

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

Parameter	Description
CVE ID	Common Vulnerabilities & Exposures (CVE) ID, which corresponds to the protection rule. For non-CVE vulnerabilities, a double dash (--) is displayed.
Risk Severity	The severity of the vulnerability, including: <ul style="list-style-type: none"> • High • Medium • Low
Application Type	The application type the protection rule is used for.
Protection Type	The type of the protection rule. WAF can discover SQL injection, command injection, XSS attacks, XML external entity (XXE) injection, Expression Language (EL) Injection, CSRF, SSRF, local file inclusion, remote file inclusion, website Trojans, malicious crawlers, session fixation attacks, deserialization vulnerabilities, remote command execution, information leakage, DoS attacks, source code/data leakage.

----End

Protection Effect

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

- Step 1** Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.
 - If the website is inaccessible, connect the website domain name to WAF by following the instructions in [Website Settings](#).
 - If the website is accessible, go to [Step 2](#).
- Step 2** Clear the browser cache and enter **http://www.example.com?id=1%27%20or%201=1** in the address box of the browser to simulate an SQL injection attack.
- Step 3** Return to the WAF console. In the navigation pane, choose **Events**. On the displayed page, view or [download events data](#).

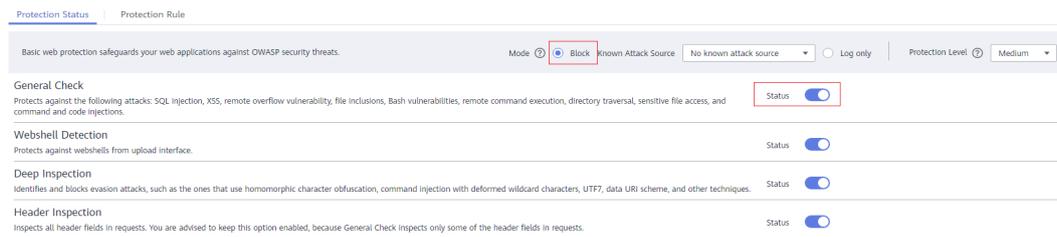
----End

Example - Blocking SQL Injection Attacks

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

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

Figure 6-5 Enabling General Check



Step 2 Enable WAF basic web protection.

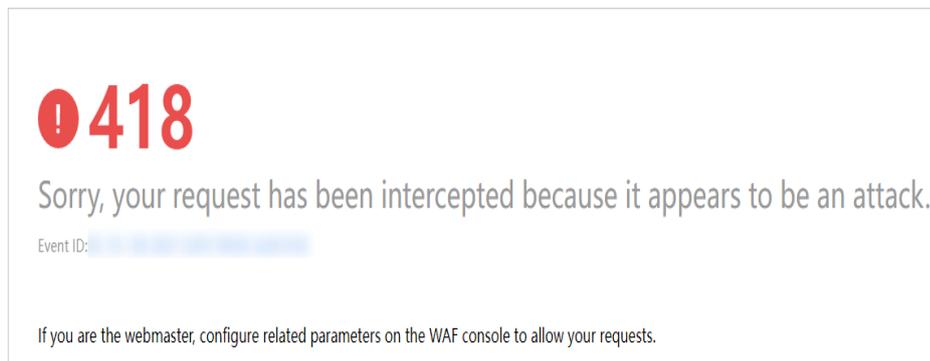
Figure 6-6 Basic Web Protection configuration area



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

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

Figure 6-7 Block page



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

----End

6.3 Configuring a CC Attack Protection Rule

CC attack protection can limit the access to a protected website based on a single IP address, cookie, or referer. To use this protection, ensure that you have toggled on **CC Attack Protection**).

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

Prerequisites

A website has been added to WAF.

Constraints

- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- If you set **Logic** to **Include any value**, **Exclude any value**, **Equal to any value**, **Not equal to any value**, **Prefix is any value**, **Prefix is not any of them**, **Suffix is any value**, or **Suffix is not any of them**, select an existing reference table. For details, see [Creating a Reference Table to Configure Protection Metrics In Batches](#).

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** Click the name of the target policy to go to the protection configuration page.
- Step 6** In the **CC Attack Protection** configuration area, change **Status** if needed and click **Customize Rule** to go to the **CC Attack Protection** page.

Figure 6-8 CC Attack Protection configuration area



- Step 7** In the upper left corner above the **CC Attack Protection** rule list, click **Add Rule**.
- Step 8** In the displayed dialog box, configure a CC attack protection rule by referring to [Table 6-6](#).

Figure 6-9 Adding a CC attack protection rule

Add CC Attack Protection Rule

Restrictions and precautions vary by mode. ⓘ

Rule Description

★ Rate Limit Mode Per IP address Per user Other

Requests from a specific source are limited. For example, if traffic from an IP address (or user) exceeds the rate limit you configure in this rule, WAF limits traffic rate of the IP address (or user) in the way you configure.

★ User Identifier

If this field does not exist in a request, the request is not counted. If this field exists but is empty, the request is counted.

★ Trigger

Field	Subfield	Logic	Content
<input type="text" value="Path"/>	--	<input type="text" value="Include"/>	<input type="text" value="/admin"/>

[Add Reference Table](#)

Table 6-6 Rule parameters

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

Parameter	Description	Example Value
User Identifier	<p>This parameter is mandatory when you select Per user for Rate Limit Mode.</p> <ul style="list-style-type: none"> ● Cookie: A cookie field name. You need to configure an attribute variable name in the cookie that can uniquely identify a web visitor based on your website requirements. This field does not support regular expressions. Only complete matches are supported. For example, if a website uses the name field in the cookie to uniquely identify a web visitor, enter name. ● Header: Set the user-defined HTTP header you want to protect. You need to configure the HTTP header that can identify web visitors based on your website requirements. 	name
Trigger	<p>Click Add to add conditions. At least one condition is required, but up to 30 conditions are allowed. If you add more than one condition, the rule will only take effect if all of the conditions are met.</p> <ul style="list-style-type: none"> ● Field ● Subfield: Configure this field only when IPv4, Cookie, Header, or Params is selected for Field. <p>NOTICE A subfield cannot exceed 2,048 bytes.</p> <ul style="list-style-type: none"> ● Logic: Select a logical relationship from the drop-down list. <p>NOTE If you set Logic to Include any value, Exclude any value, Equal to any value, Not equal to any value, Prefix is any value, Prefix is not any of them, Suffix is any value, or Suffix is not any of them, select an existing reference table. For details, see Creating a Reference Table to Configure Protection Metrics In Batches.</p> <ul style="list-style-type: none"> ● Content: Enter or select the content that matches the condition. 	Path Include / admin
Rate Limit	<p>The number of requests allowed from a website visitor in the rate limit period. If the number of requests exceeds the rate limit, WAF takes the action you configure for Protective Action.</p>	10 requests allowed in 60 seconds

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

Parameter	Description	Example Value
Block Page Type	If you select Custom for Block Page , select a type of the block page among options application/json , text/html , and text/xml .	text/html
Page Content	If you select Custom for Block Page , configure the content to be returned.	<p>Page content styles corresponding to different page types are as follows:</p> <ul style="list-style-type: none"> • text/html: <code><html><body>Forbidden</body></html></code> • application/json: <code>{"msg": "Forbidden"}</code> • text/xml: <code><?xml version="1.0" encoding="utf-8"?><error><msg>Forbidden</msg></error></code>

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

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

----End

Protection Effect

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

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

- If the website is inaccessible, connect the website domain name to WAF by referring to [Website Settings](#).
- If the website is accessible, go to **2**.

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

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

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

----End

Configuration Example - Verification Code

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

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

Figure 6-10 Verification code

Add CC Attack Protection Rule

* User Identifier: Cookie | name

If this field does not exist in a request, the request is not counted. If this field exists but is empty, the request is counted.

* Trigger:

Field	Subfield	Logic	Content
Path	--	Include	/admin

Add Reference Table

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

* Rate Limit: 10 requests | 60 seconds

* Protective Action: Verification code | Block | Block dynamically | Log only

* Effective Date: Immediate

Confirm | Cancel

Step 2 Enable CC attack protection.

Figure 6-11 CC Attack Protection configuration area

CC Attack Protection

Configures rate limiting policies based on IP addresses or cookies to mitigate CC attacks.

Status:

[Customize Rule](#)

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

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



Verification Required

Your requests are too frequent!

Please input the verification code:

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

----End

6.4 Configuring Custom Precise Protection Rules

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

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

Prerequisites

You have [added your website to a policy](#).

Constraints

- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- If you configure **Protective Action** to **Block** for a precise protection rule, you can configure a known attack source rule by referring to [Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration](#). WAF will block requests matching the configured IP address, Cookie, or Params for a length of time configured as part of the rule.
- The path content cannot contain the following special characters: (' "<>&*#% \?)

Application Scenarios

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

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** Click the name of the target policy to go to the protection configuration page.
- Step 6** In the **Precise Protection** configuration area, change **Status** as needed and click **Customize Rule** to go to the **Precise Protection** page.

Figure 6-12 Precise Protection configuration area



- Step 7** On the **Precise Protection** page, set **Detection Mode**.
Two detection modes are available:
 - **Instant Detection:** If a request matches a configured precise protection rule, WAF immediately ends threat detection and blocks the request.
 - **Full Detection:** If a request matches a configured precise protection rule, WAF finishes its scan first and then blocks all requests that match the configured precise protection rule.
- Step 8** In the upper left corner above the **Precise Protection** rule list, click **Add Rule**.
- Step 9** In the displayed dialog box, add a rule by referring to [Table 6-7](#).

The settings shown in [Figure 6-13](#) are used as an example. If a visitor tries to access a URL containing **/admin**, WAF will block the request.

NOTICE

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

Figure 6-13 Add Precise Protection Rule

Add Precise Protection Rule

Restrictions and precautions vary by mode. [?](#)

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

Rule Description

* Condition List

Field	Subfield	Logic	Content
<input type="text" value="Path"/>	--	<input type="text" value="Include"/>	<input type="text" value="/admin/"/>

[Add Reference Table](#)

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

* Protective Action

* Known Attack Source [Add Known Attack Source Rule](#)

Priority A smaller value indicates a higher priority.

Table 6-7 Rule parameters

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

Parameter	Description	Example Value
Condition List	<p>Click Add to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. A condition includes the following parameters:</p> <p>Parameters for configuring a condition are described as follows:</p> <ul style="list-style-type: none"> • Field • Subfield: Configure this field only when Params, Cookie, or Header is selected for Field. • Logic: Select a logical relationship from the drop-down list. <p>NOTE</p> <ul style="list-style-type: none"> - If Include any value, Exclude any value, Equal to any value, Not equal to any value, Prefix is any value, Prefix is not any of them, Suffix is any value, or Suffix is not any of them is selected, select an existing reference table in the Content drop-down list. For details, see Creating a Reference Table to Configure Protection Metrics In Batches. - Exclude any value, Not equal to any value, Prefix is not any of them, and Suffix is not any of them indicates, respectively, that WAF performs the protection action (block, allow, or log only) when the field in the access request does not contain, is not equal to, or the prefix or suffix is not any value set in the reference table. For example, assume that Path field is set to Exclude any value and the test reference table is selected. If <i>test1</i>, <i>test2</i>, and <i>test3</i> are set in the test 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>. <ul style="list-style-type: none"> • Content: Enter or select the content of condition matching. <p>NOTE For more details about the configurations in general, see Table 6-18.</p>	<ul style="list-style-type: none"> • Path Include /admin • User Agent Prefix is not mozilla/5.0 • IP Equal to 192.168.2.3 • Cookie key1 Prefix is not jsessionid

Parameter	Description	Example Value
Protective Action	<ul style="list-style-type: none"> • Block: The request that hit the rule will be blocked and a block response page is returned to the client that initiates the request. By default, WAF uses a unified block response page. You can also customize this page. For details, see Modifying the Alarm Page. • Allow: Requests that hit the rule are forwarded to backend servers. • Log only: Requests that hit the rule are not blocked, but will be logged. You can use WAF logs to query requests that hit the current rule and analyze the protection results of the rule. For example, check whether there are requests that are blocked mistakenly. 	Block
Known Attack Source	If you set Protective Action to Block , you can select a blocking type for a known attack source rule. Then, WAF blocks requests matching the configured IP , Cookie , or Params for a length of time that depends on the selected blocking type.	Long-term IP address blocking
Priority	<p>Rule priority. If you have added multiple rules, rules are matched by priority. The smaller the value you set, the higher the priority.</p> <p>NOTICE If multiple precise access control rules have the same priority, WAF matches the rules in the sequence of time the rules are added.</p>	5
Effective Date	Select Immediate to enable the rule immediately, or select Custom to configure when you wish the rule to be enabled.	Immediate

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

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

----End

Protection Effect

If you have configured a precise protection rule as shown in [Figure 6-13](#) for your domain name, to verify WAF is protecting your website ([www.example.com](#)) against the rule:

- Step 1** Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.
- If the website is inaccessible, connect the website domain name to WAF by following the instructions in [Website Settings](#).
 - If the website is accessible, go to [Step 2](#).
- Step 2** Clear the browser cache and enter [http://www.example.com/admin](#) (or any page containing [/admin](#)) in the address bar. Normally, WAF blocks the requests that meet the conditions and returns the block page.
- Step 3** Return to the WAF console. In the navigation pane, click **Events**. On the displayed page, view or [download events data](#).

----End

Configuration Example - Blocking a Certain Type of Attack Requests

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

Figure 6-14 WordPress pingback attack

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

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

Figure 6-15 User Agent configuration

The screenshot shows the 'Add Precise Protection Rule' configuration interface. At the top, it says 'Restrictions and precautions vary by mode.' Below that, a note states 'This rule takes effect when the following conditions are met. 1 rule supports a maximum of 30 conditions.' The 'Rule Description' field contains 'wafest'. The 'Condition List' section contains one condition: 'User Agent' (Field) with a subfield of '--', logic set to 'Include', and content 'WordPress'. Below the condition list, there is a note: 'Add You can add 29 more conditions.(The protective action is executed only when all the conditions are met.)'. The 'Protective Action' is set to 'Block'. The 'Known Attack Source' is set to 'No known attack...' with a link to 'Add Known Attack Source Rule'. At the bottom, there are 'Confirm' and 'Cancel' buttons.

Configuration Example - Blocking Attack Requests to a Certain URL

If a large number of IP addresses are accessing a URL that does not exist, configure the following protection rule to block such requests to reduce resource usage on the origin server.

Figure 6-16 Blocking requests to a specific URL

The screenshot shows the 'Add Precise Protection Rule' configuration interface. At the top, it says 'Restrictions and precautions vary by mode.' Below that, a note states 'This rule takes effect when the following conditions are met. 1 rule supports a maximum of 30 conditions.' The 'Rule Name' field contains 'waf'. The 'Rule Description' field is empty. The 'Condition List' section contains one condition: 'Path' (Field) with a subfield of '--', logic set to 'Include', and content '/XXXX'. Below the condition list, there is a note: 'Add You can add 29 more conditions.(The protective action is executed only when all the conditions are met.)'. The 'Protective Action' is set to 'Block'.

Configuration Example - Blocking Requests with null Fields

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

Figure 6-17 Blocking requests with empty Referer

Add Precise Protection Rule

Restrictions and precautions vary by mode. ?

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

Rule Description: wafest

Field	Subfield	Logic	Content
Header	referer	Does not have	

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

Protective Action: Block

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

Priority: 50 A smaller value indicates a higher priority.

Confirm Cancel

Configuration Example - Blocking Specified File Types (ZIP, TAR, and DOCX)

You can configure file types that match the path field to block specific files of certain types. For example, if you want to block .zip files, you can configure a precise protection rule as shown in [Figure 6-18](#) to block access requests of .zip files.

Figure 6-18 Blocking requests of specific file types

Add Precise Protection Rule

Restrictions and precautions vary by mode. ?

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

Rule Name: waf

Rule Description:

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

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

Protective Action: Block

Configuration Example - Preventing Hotlinking

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

Figure 6-19 Preventing hotlinking

Add Precise Protection Rule

Restrictions and precautions vary by mode. ?

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

* Rule Name: waftest

Rule Description:

* Condition List:

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

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

* Protective Action: Block

* Known Attack Sources: No known attacks. Add Known Attack Sources Rule

Confirm Cancel

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

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

Figure 6-20 Blocking all requests

Add Precise Protection Rule

Restrictions and precautions vary by mode. ?

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

* Rule Name: Enter a rule name.

Rule Description:

* Condition List:

Field	Subfield	Logic	Content
Path	--	Include	/

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

* Protective Action: Block

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

Add Precise Protection Rule

Restrictions and precautions vary by mode. ?

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

* Rule Name

Rule Description

* Condition List

Field	Subfield	Logic	Content
IPv4	Client IP Address	Equal to	192.168.2.3

[Add Reference Table](#)

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

* Protective Action

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

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

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

Add Precise Protection Rule

Restrictions and precautions vary by mode. ?

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

* Rule Name

Rule Description

* Condition List

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

[Add Reference Table](#)

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

* Protective Action

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

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

Prerequisites

You have [added your website to a policy](#).

Constraints

- WAF supports batch import of IP address blacklists and whitelists. You can use address groups to add multiple IP addresses/ranges quickly to a blacklist or whitelist rule. For details, see [Adding an IP Address Group](#).
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- The address 0.0.0.0/0 cannot be added to a WAF IP address blacklist or whitelist, and if a whitelist conflicts with a blacklist, the whitelist rule takes priority. If you want to allow only a specific IP address within a range of blocked addresses, add a blacklist rule to block the range and then add a whitelist rule to allow the individual address you wish to allow.
- If you set **Protective Action** of a blacklist or whitelist rule to **Block**, you can [configure known attack source rules to block the attack source IP address for a specified period of time](#). WAF will block requests matching the configured IP address, Cookie, or Params for a block duration you specify.

Impact on the System

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

Procedure

Step 1 Log in to the management console.

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

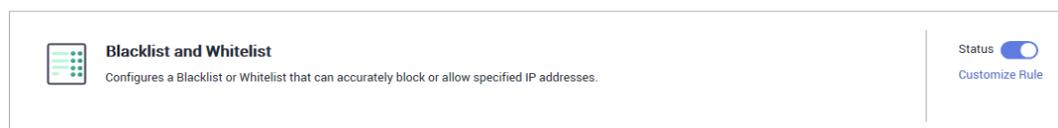
Step 3 Click  in the upper left corner and choose **Web Application Firewall** under **Security**.

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

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

Step 6 In the **Blacklist and Whitelist** configuration area, change **Status** as needed and click **Customize Rule**.

Figure 6-23 Blacklist and Whitelist configuration area



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

Step 8 In the displayed dialog box, specify the parameters by referring to [Table 6-8](#).

NOTE

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

Figure 6-24 Adding a blacklist or whitelist rule

Table 6-8 Rule parameters

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

Parameter	Description	Example Value
IP Address/ Range	<p>This parameter is mandatory if you select IP address/range for IP Address/Range/Group. IP addresses or IP address ranges are supported.</p> <ul style="list-style-type: none"> • IP address: IP address to be added to the blacklist or whitelist • IP address range: IP address and subnet mask defining a network segment 	XXX.XXX.2.3
Select Address Group	<p>This parameter is mandatory if you select Address group for IP Address/Range/Group. Select an IP address group from the drop-down list. You can also click Add Address Group to create an address group. For details, see Adding an IP Address Group.</p>	groupwaf
Protective Action	<ul style="list-style-type: none"> • Block: Select Block if you want to blacklist an IP address or IP address range. • Allow: Select Allow if you want to whitelist an IP address or IP address range. • Log only: Select Log only if you want to observe an IP address or IP address range. Then, WAF determines whether the IP address or IP address range are blacklisted or whitelisted based on the events data. 	Block

Parameter	Description	Example Value
Known Attack Source	If you select Block for Protective Action , you can select a blocking type of a known attack source rule. WAF will block requests matching the configured IP address, Cookie, or Params for a length of time configured as part of the rule.	Long-term IP address blocking
Rule Description	A brief description of the rule. This parameter is optional.	None

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

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

----End

Protection Effect

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

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

- If the website is inaccessible, connect the website domain name to WAF by referring to [Website Settings](#).
- If the website is accessible, go to [Step 2](#).

Step 2 Blacklist the IP address of a client according to the instructions in [Procedure](#).

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

Step 4 Return to the WAF console. In the navigation pane, choose **Events**. On the displayed page, view or [download events data](#).

----End

Example Configuration - Allowing a Specified IP Addresses

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

Step 1 Add the following two blacklist and whitelist rules to block all IP addresses:

Figure 6-25 Blocking IP address range 1.0.0.0/1

The screenshot shows a dialog box titled "Add Blacklist or Whitelist Rule" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Rule Name:** A text input field containing "all01".
- IP Address/Range/Group:** Radio buttons for "IP address/range" (selected) and "Address group".
- IP Address/Range:** A text input field containing "1.0.0.0/1".
- Protective Action:** A dropdown menu with "Block" selected.
- Known Attack Source:** A dropdown menu with "No known attack source" selected. To the right is a blue link "Add Known Attack Source Rule".
- Rule Description:** An empty text input field.
- Buttons:** A green "Confirm" button and a white "Cancel" button at the bottom.

Figure 6-26 Blocking IP address range 128.0.0.0/1

The screenshot shows a dialog box titled "Add Blacklist or Whitelist Rule" with a close button (X) in the top right corner. The form contains the following fields and options:

- Rule Name:** Text input field containing "all01".
- IP Address/Range/Group:** Radio button options. "IP address/range" is selected (indicated by a blue dot), and "Address group" is unselected.
- IP Address/Range:** Text input field containing "128.0.0.0/1".
- Protective Action:** Dropdown menu with "Block" selected.
- Known Attack Source:** Dropdown menu with "No known attack source" selected. To the right is a blue link "Add Known Attack Source Rule" with a refresh icon.
- Rule Description:** Empty text input field.
- Buttons:** A green "Confirm" button and a grey "Cancel" button at the bottom.

You can also add a precise protection rule to block all access requests, as shown in [Figure 6-27](#).

Figure 6-27 Blocking all access requests

The screenshot shows a dialog box titled "Add Precise Protection Rule" with a help icon (?) in the top right corner. The form contains the following fields and options:

- Rule Name:** Text input field containing "wafest".
- Rule Description:** Empty text input field.
- Condition List:** A table with columns "Field", "Subfield", "Logic", and "Content". One condition is listed: Field "Path", Subfield "-", Logic "Include", and Content "/". To the right is a blue link "Add Reference Table".
- Protective Action:** Dropdown menu with "Block" selected.
- Known Attack Source:** Dropdown menu with "No known attack source" selected. To the right is a blue link "Add Known Attack Source Rule" with a refresh icon.
- Footer:** A note: "Add You can add 29 more conditions. (The protective action is executed only when all the conditions are met.)"

For details, see [Configuring Custom Precise Protection Rules](#).

Step 2 Refer to [Figure 6-28](#) and add a whitelist rule to allow a specified IP address, for example, `XXX.XXX.2.3`.

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

Add Blacklist or Whitelist Rule

* Rule Name

* IP Address/Range/Group IP address/range Address group

* IP Address/Range

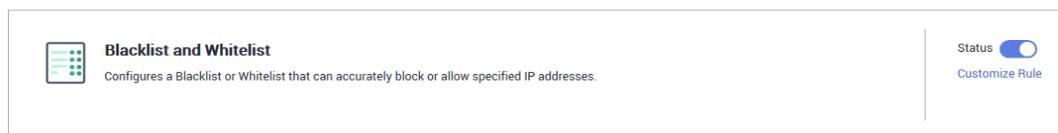
* Protective Action

Rule Description

Confirm

Step 3 Enable the white and blacklist protection.

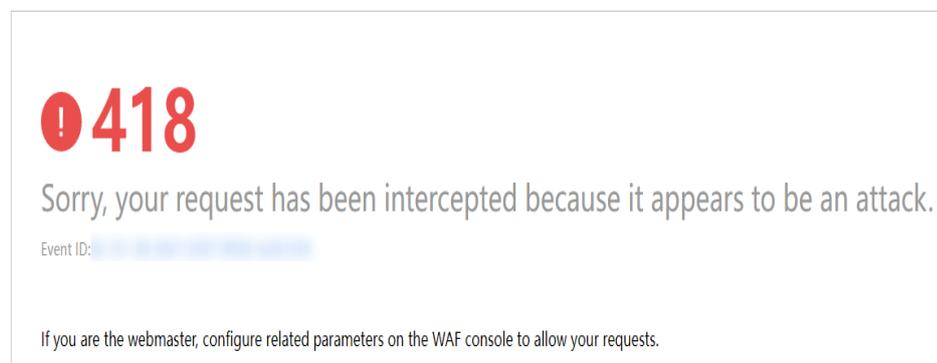
Figure 6-29 Blacklist and Whitelist configuration area



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

If the IP address of a visitor is not the one specified in [Step 2](#), WAF blocks the access request. [Figure 6-30](#) shows an example of the block page.

Figure 6-30 Block page



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

----End

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

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

Prerequisites

You have [added your website to a policy](#).

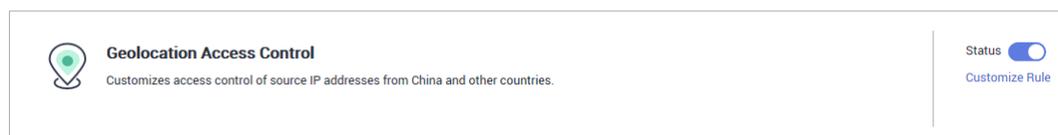
Constraints

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

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** Click the name of the target policy to go to the protection configuration page.
- Step 6** In the **Geolocation Access Control** configuration area, change **Status** if needed and click **Customize Rule**.

Figure 6-31 Geolocation Access Control configuration area



- Step 7** In the upper left corner above the **Geolocation Access Control** list, click **Add Rule**.
- Step 8** In the displayed dialog box, add a geolocation access control rule by referring to [Table 6-9](#).

Figure 6-32 Adding a geolocation access control rule

Table 6-9 Rule parameters

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

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

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

----End

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

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

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

Figure 6-33 Selecting Allow for Protective Action

Add Geolocation Access Control Rule

* Geolocation

Inside China (0) Select All

<input type="checkbox"/> Beijing	<input type="checkbox"/> Shanghai	<input type="checkbox"/> Tianjin	<input type="checkbox"/> Chongqing
<input type="checkbox"/> Guangdong	<input type="checkbox"/> Zhejiang	<input type="checkbox"/> Jiangsu	<input type="checkbox"/> Anhui
<input type="checkbox"/> Fujian	<input type="checkbox"/> Gansu	<input type="checkbox"/> Guangxi	<input type="checkbox"/> Guizhou
<input type="checkbox"/> Henan	<input type="checkbox"/> Hubei	<input type="checkbox"/> Hebei	<input type="checkbox"/> Hainan
<input type="checkbox"/> Hong Kong	<input type="checkbox"/> Heilongjiang	<input type="checkbox"/> Hunan	<input type="checkbox"/> Jilin
<input type="checkbox"/> Jiangxi	<input type="checkbox"/> Liaoning	<input type="checkbox"/> Macao	<input type="checkbox"/> Inner Mongolia
<input type="checkbox"/> Ningxia	<input type="checkbox"/> Qinghai	<input type="checkbox"/> Sichuan	<input type="checkbox"/> Shandong
<input type="checkbox"/> Shaanxi	<input type="checkbox"/> Shanxi	<input type="checkbox"/> Taiwan	<input type="checkbox"/> Sinkiang
<input type="checkbox"/> Tibet	<input type="checkbox"/> Yunnan		

Outside China (1)

* Protective Action

- Step 2** Enable geolocation access control.

Figure 6-34 Geolocation Access Control configuration area

Geolocation Access Control
Customizes access control of source IP addresses from China and other countries.

Status [Customize Rule](#)

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

Figure 6-35 Blocking all access requests

Add Precise Protection Rule

Restrictions and precautions vary by mode. ?

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

* Rule Name:

Rule Description:

* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/

Add Reference Table

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

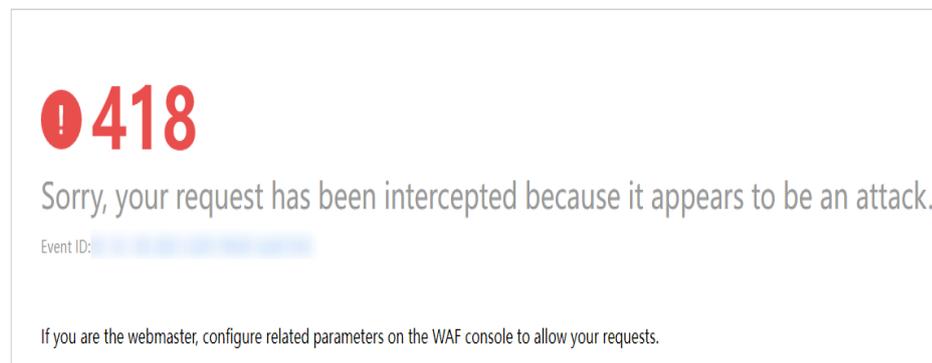
* Protective Action:

Known Attack Sources:

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

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

Figure 6-36 Block page



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

----End

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

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

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

Figure 6-37 Blocking access requests from a specific region

Add Geolocation Access Control Rule

* Geolocation

Inside China (0) Select All

<input type="checkbox"/> Beijing	<input type="checkbox"/> Shanghai	<input type="checkbox"/> Tianjin	<input type="checkbox"/> Chongqing
<input type="checkbox"/> Guangdong	<input type="checkbox"/> Zhejiang	<input type="checkbox"/> Jiangsu	<input type="checkbox"/> Anhui
<input type="checkbox"/> Fujian	<input type="checkbox"/> Gansu	<input type="checkbox"/> Guangxi	<input type="checkbox"/> Guizhou
<input type="checkbox"/> Henan	<input type="checkbox"/> Hubei	<input type="checkbox"/> Hebei	<input type="checkbox"/> Hainan
<input type="checkbox"/> Hong Kong	<input type="checkbox"/> Heilongjiang	<input type="checkbox"/> Hunan	<input type="checkbox"/> Jilin
<input type="checkbox"/> Jiangxi	<input type="checkbox"/> Liaoning	<input type="checkbox"/> Macao	<input type="checkbox"/> Inner Mongolia
<input type="checkbox"/> Ningxia	<input type="checkbox"/> Qinghai	<input type="checkbox"/> Sichuan	<input type="checkbox"/> Shandong
<input type="checkbox"/> Shaanxi	<input type="checkbox"/> Shanxi	<input type="checkbox"/> Taiwan	<input type="checkbox"/> Sinkiang
<input type="checkbox"/> Tibet	<input type="checkbox"/> Yunnan		

Outside China (1)

* Protective Action

Step 2 Enable geolocation access control.

Figure 6-38 Geolocation Access Control configuration area

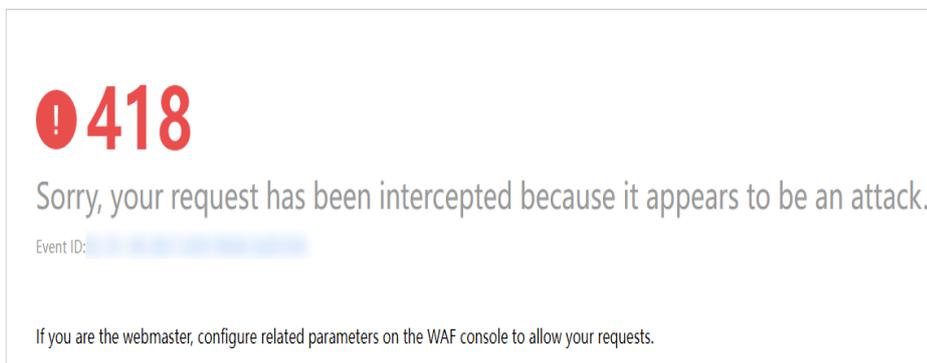
 **Geolocation Access Control**
Customizes access control of source IP addresses from China and other countries.

Status [Customize Rule](#)

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

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

Figure 6-39 Block page



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

Figure 6-40 Viewing events - blocking access requests from IP addresses in a region

Time	Source IP Address	Geolocation	Domain Name	URL	Malicious Load	Event Type	Protective Action	Operation
Dec 29, 2021 06:27:23 GM...	[blurred]	Beijing	[blurred]	/		GeoIP	Block	Details Handle False Alarm
Dec 29, 2021 06:26:55 GM...	[blurred]	Beijing	[blurred]	/evox/about		GeoIP	Block	Details Handle False Alarm
Dec 29, 2021 06:26:50 GM...	[blurred]	Beijing	[blurred]	/HNAP1		GeoIP	Block	Details Handle False Alarm
Dec 29, 2021 06:26:50 GM...	[blurred]	Beijing	[blurred]	/mmaglowercheck1640730...		GeoIP	Block	Details Handle False Alarm

----End

Protection Effect

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

- Step 1** Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.
- If the website is inaccessible, connect the website domain name to WAF by referring to [Website Settings](#).
 - If the website is accessible, go to [2](#).
- Step 2** Add a geolocation access control rule by referring to [Procedure](#).
- Step 3** Clear the browser cache and access <http://www.example.com>. Normally, WAF blocks such requests and returns the block page.
- Step 4** Go to the WAF console. In the navigation pane on the left, choose **Events**. On the displayed page, view or [download events data](#).

----End

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

You can set web tamper protection rules to protect specific website pages (such as the ones contain important content) from being tampered with. If a web page

protected with such a rule is requested, WAF returns the origin page it has cached based on the rule so that visitors always receive the authenticate web pages.

How It Works

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

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

Prerequisites

You have [added your website to a policy](#).

Constraints

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

Application Scenarios

- Quicker response to requests
After a web tamper protection rule is configured, WAF caches static web pages on the server. When receiving a request from a web visitor, WAF directly returns the cached web page to the web visitor.
- Web tamper protection
If an attacker modifies a static web page on the server, WAF still returns the cached original web page to visitors. Visitors never see the pages that were tampered with.
WAF randomly extracts requests from a visitor to compare the page they received with the page on the server. If WAF detects that the page has been tampered with, it notifies you by SMS or email, depending on what you configure. For more details, see [Enabling Alarm Notifications](#).

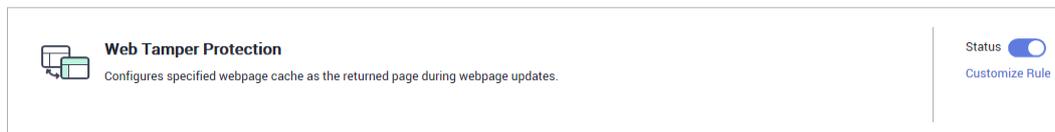
Procedure

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 **Policies**.
- Step 5** Click the name of the target policy to go to the protection configuration page.
- Step 6** In the **Web Tamper Protection** configuration area, change **Status** if needed and click **Customize Rule** to go to the **Web Tamper Protection** page.

Figure 6-41 Web Tamper Protection configuration area



- Step 7** In the upper left corner above the **Web Tamper Protection** rule list, click **Add Rule**.
- Step 8** In the displayed dialog box, specify the parameters by referring to [Table 6-10](#).

Figure 6-42 Adding a web tamper protection rule

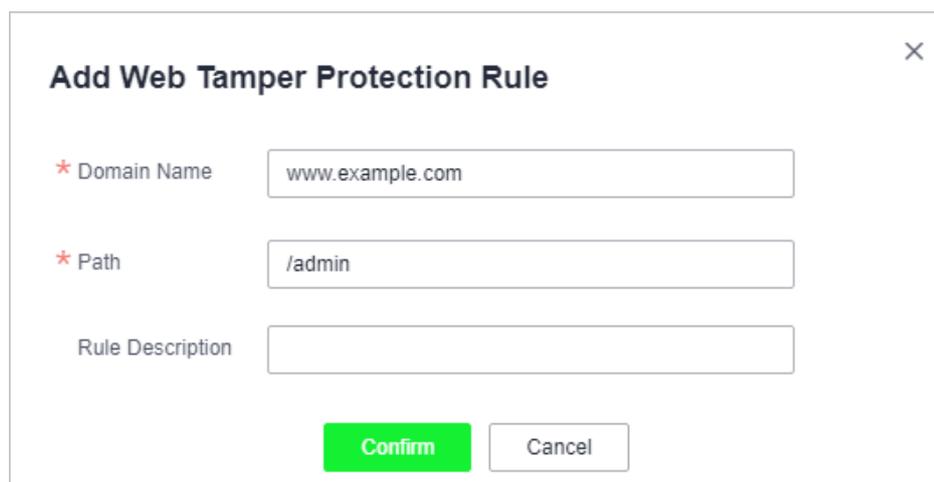


Table 6-10 Rule parameters

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

Parameter	Description	Example Value
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 http://www.example.com/admin, set Path to /admin.</p> <p>NOTE</p> <ul style="list-style-type: none"> • The path does not support regular expressions. • The path cannot contain two or more consecutive slashes. For example, ///admin. If you enter ///admin, WAF converts /// to /. 	/admin
Rule Description	A brief description of the rule. This parameter is optional.	None

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

----End

Related Operations

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

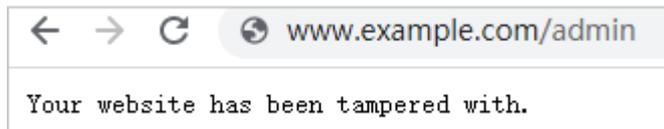
Configuration Example - Static Web Page Tamper Prevention

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

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

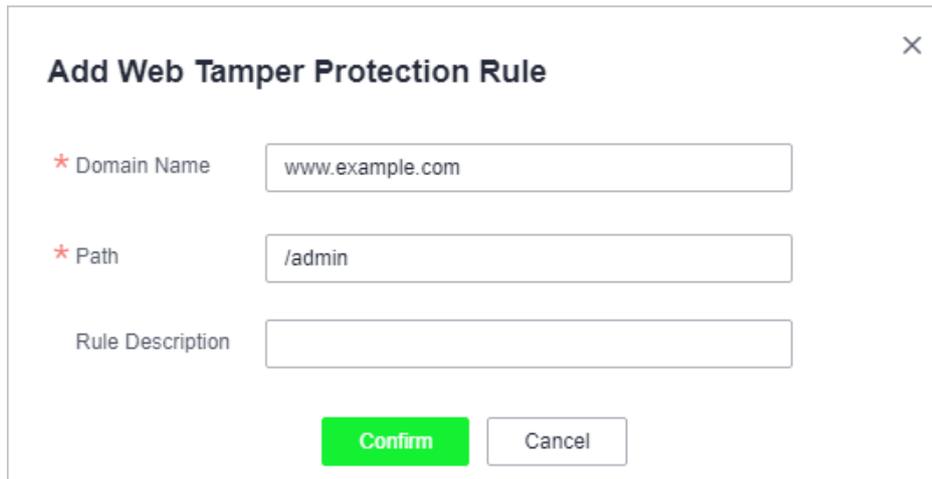
A tampered page is returned.

Figure 6-43 A static page that has been tampered with



Step 2 Add a web tamper prevention rule to WAF.

Figure 6-44 Adding a web tamper protection rule

A dialog box titled 'Add Web Tamper Protection Rule' with a close button (X) in the top right corner. It contains three input fields: 'Domain Name' with the value 'www.example.com', 'Path' with the value '/admin', and 'Rule Description' which is empty. At the bottom, there are two buttons: a green 'Confirm' button and a grey 'Cancel' button.

Step 3 Enable WTP.

Figure 6-45 Web Tamper Protection configuration area



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

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

The intact page is returned.

----End

6.8 Configuring Anti-Crawler Rules

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

Prerequisites

You have [added your website to a policy](#).

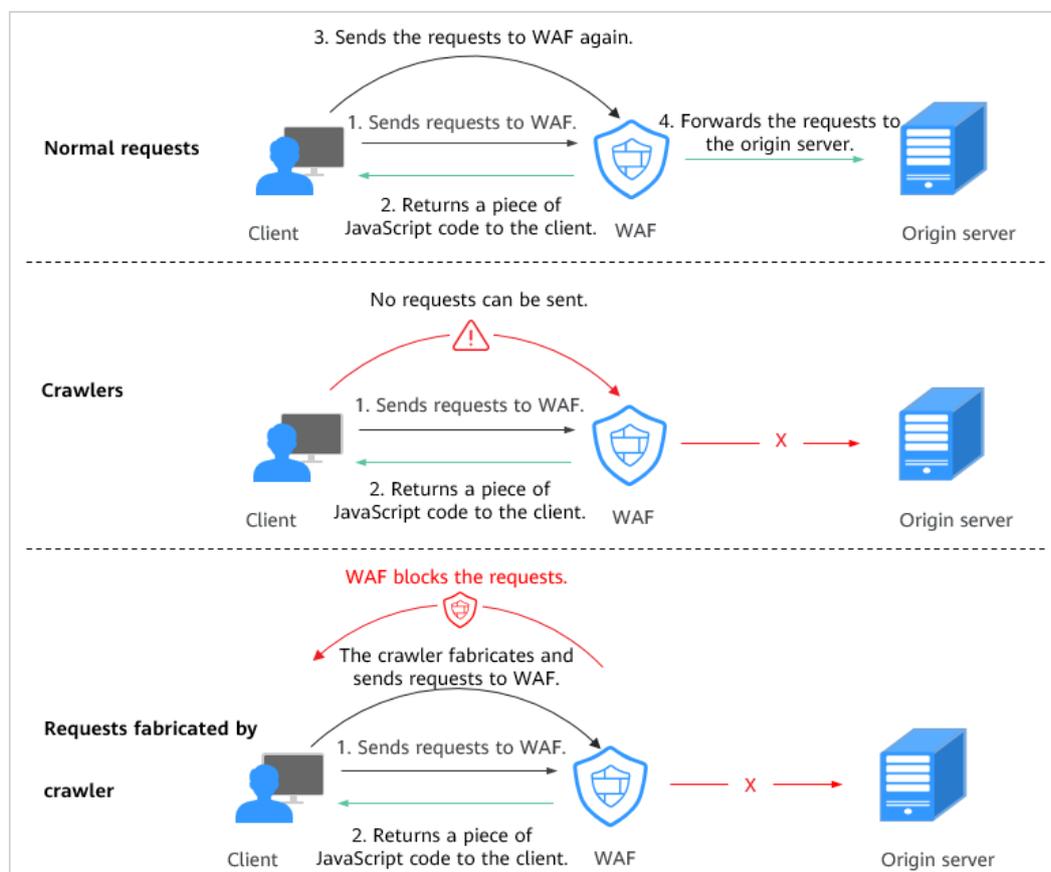
Constraints

- Cookies must be enabled and JavaScript supported by any browser used to access a website protected by anti-crawler protection rules.
- If your service is connected to CDN, exercise caution when using the JS anti-crawler function.
CDN caching may impact JS anti-crawler performance and page accessibility.
- WAF only logs JavaScript challenge and JavaScript authentication events. No other protective actions can be configured for JavaScript challenge and authentication.
- WAF JavaScript-based anti-crawler rules only check GET requests and do not check POST requests.

How JavaScript Anti-Crawler Protection Works

Figure 6-46 shows how JavaScript anti-crawler detection works, which includes JavaScript challenges (step 1 and step 2) and JavaScript authentication (step 3).

Figure 6-46 JavaScript Anti-Crawler protection process



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

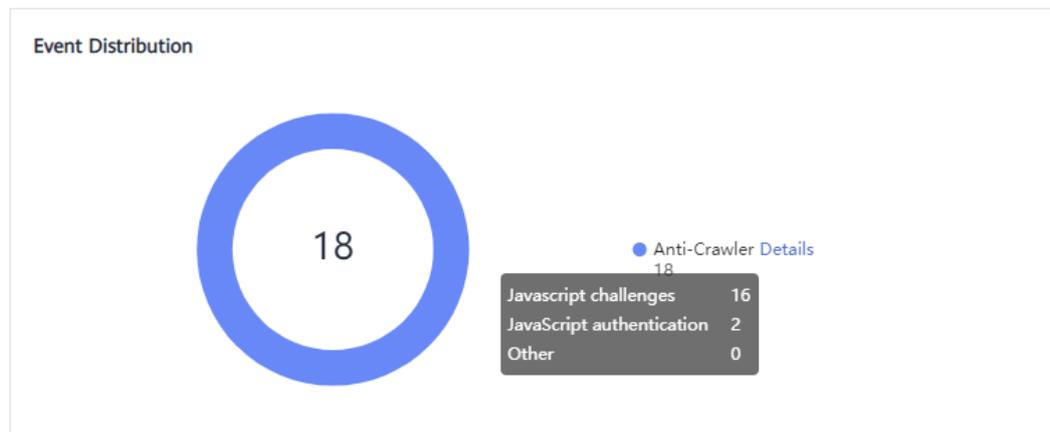
- If the client sends a normal request to the website, triggered by the received JavaScript code, the client will automatically send the request to WAF again.

WAF then forwards the request to the origin server. This process is called JavaScript verification.

- If the client is a crawler, it cannot be triggered by the received JavaScript code and will not send a request to WAF again. The client fails JavaScript authentication.
- If a client crawler fabricates a WAF authentication request and sends the request to WAF, the WAF will block the request. The client fails JavaScript authentication.

By collecting statistics on the number of JavaScript challenges and authentication responses, the system calculates how many requests the JavaScript anti-crawler defends. In [Figure 6-47](#), the JavaScript anti-crawler has logged 18 events, 16 of which are JavaScript challenge responses, and 2 of which are JavaScript authentication responses. **Others** indicates the number of WAF authentication requests fabricated by the crawler.

Figure 6-47 Parameters of a JavaScript anti-crawler protection rule



NOTICE

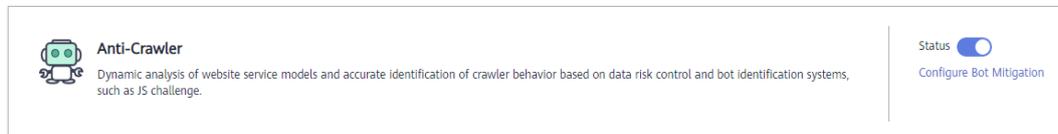
WAF only logs JavaScript challenge and JavaScript authentication events. No other protective actions can be configured for JavaScript challenge and authentication.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** Click the name of the target policy to go to the protection configuration page.

Step 6 In the **Anti-Crawler** configuration area, toggle on the function if needed. Then, click **Configure Bot Mitigation**.

Figure 6-48 Anti-Crawler configuration area



Step 7 Select the **Feature Library** tab and enable the protection by referring to [Table 6-11](#).

A feature-based anti-crawler rule has two protective actions:

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

CAUTION

Enabling this feature may have the following impacts:

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

- **Log only**
Detected attacks are logged only. This is the default protective action.

Scanner is enabled by default, but you can enable other protection types if needed.

Figure 6-49 Feature Library

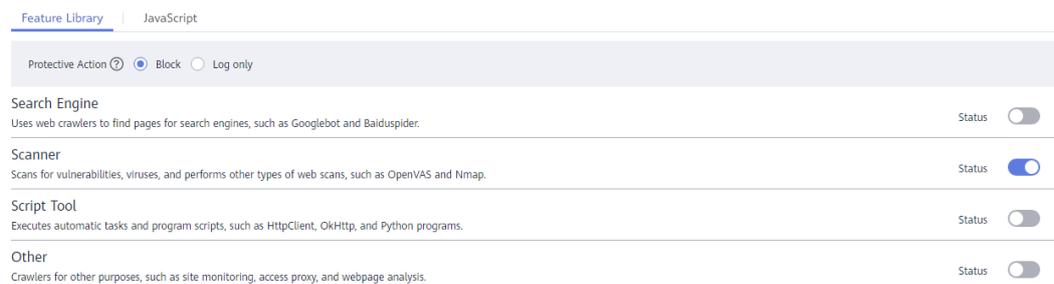


Table 6-11 Anti-crawler detection features

Type	Description	Remarks
Search Engine	This rule is used to block web crawlers, such as Googlebot and Baiduspider, from collecting content from your site.	If you enable this rule, WAF detects and blocks search engine crawlers. NOTE If Search Engine is not enabled, WAF does not block POST requests from Googlebot or Baiduspider. If you want to block POST requests from Baiduspider, use the configuration described in Configuration Example - Search Engine .
Scanner	This rule is used to block scanners, such as OpenVAS and Nmap. A scanner scans for vulnerabilities, viruses, and other jobs.	After you enable this rule, WAF detects and blocks scanner crawlers.
Script Tool	This rule is used to block script tools. A script tool is often used to execute automatic tasks and program scripts, such as HttpClient, OkHttp, and Python programs.	If you enable this rule, WAF detects and blocks the execution of automatic tasks and program scripts. NOTE If your application uses scripts such as HttpClient, OkHttp, and Python, disable Script Tool . Otherwise, WAF will identify such script tools as crawlers and block the application.
Other	This rule is used to block crawlers used for other purposes, such as site monitoring, using access proxies, and web page analysis. NOTE To avoid being blocked by WAF, crawlers may use a large number of IP address proxies.	If you enable this rule, WAF detects and blocks crawlers that are used for various purposes.

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

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

NOTICE

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

Step 9 Configure a JavaScript-based anti-crawler rule by referring to [Table 6-12](#).

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

- To protect all requests except requests that hit a specified rule
Set **Protection Mode** to **Protect all requests**. Then, click **Exclude Rule**, configure the request exclusion rule, and click **Confirm**.

Figure 6-50 Exclude Rule

- To protect a specified request only
Set **Protection Mode** to **Protect specified requests**, click **Add Rule**, configure the request rule, and click **Confirm**.

Figure 6-51 Add Rule

Add Rule

Restrictions and precautions vary by mode. [?](#)

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

* Rule Name

Rule Description

* Effective Date Immediate

* Condition List

Field	Subfield	Logic	Content
Path	--	Inclu...	/admin

[Add Reference Table](#)

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

* Priority A smaller value indicates a higher priority.

Table 6-12 Parameters of a JavaScript-based anti-crawler protection rule

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

Parameter	Description	Example Value
Condition List	<p>Parameters for configuring a condition are as follows:</p> <ul style="list-style-type: none"> • Field: Select the field you want to protect from the drop-down list. Currently, only Path and User Agent are included. • Subfield • Logic: Select a logical relationship from the drop-down list. <p>NOTE If you set Logic to Include any value, Exclude any value, Equal to any value, Not equal to any value, Prefix is any value, Prefix is not any of them, Suffix is any value, or Suffix is not any of them, you need to select a reference table.</p> <ul style="list-style-type: none"> • Content: Enter or select the content that matches the condition. 	Path Include /admin
Priority	Rule priority. If you have added multiple rules, rules are matched by priority. The smaller the value you set, the higher the priority.	5

----End

Related Operations

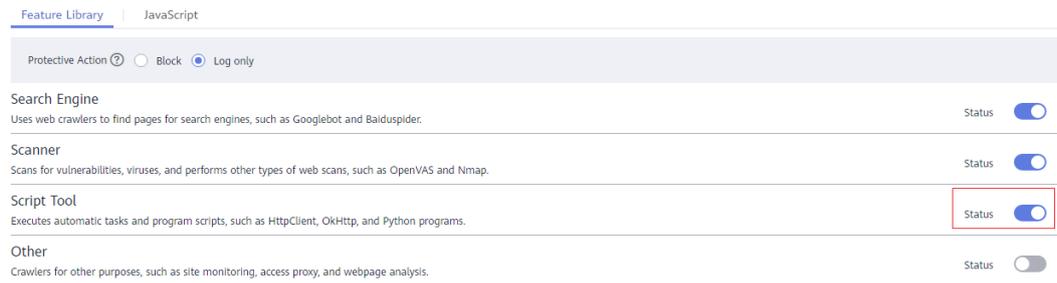
- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

Configuration Example - Logging Script Crawlers Only

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

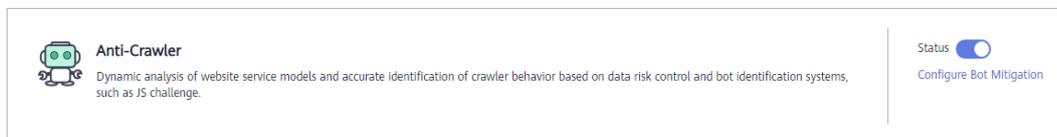
- Step 1** Execute a JavaScript tool to crawl web page content.
- Step 2** On the **Feature Library** tab, enable **Script Tool** and select **Log only** for **Protective Action**. (If WAF detects an attack, it logs the attack only.)

Figure 6-52 Enabling Script Tool



Step 3 Enable anti-crawler protection.

Figure 6-53 Anti-Crawler configuration area



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

----End

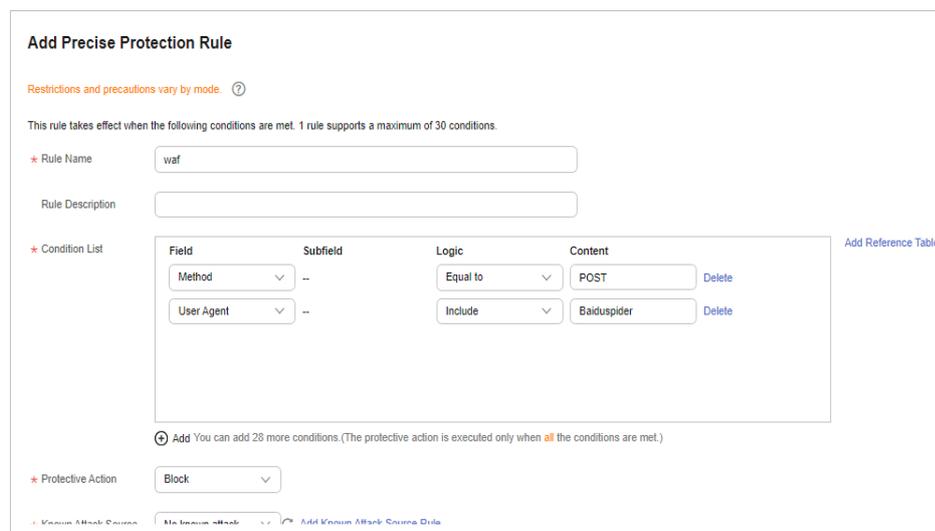
Configuration Example - Search Engine

The following shows how to allow the search engine of Baidu or Google and block the POST request of Baidu.

Step 1 Set **Status** of **Search Engine** to  by referring to the instructions in [Step 6](#).

Step 2 Configure a precise protection rule by referring to [Configuring Custom Precise Protection Rules](#).

Figure 6-54 Blocking POST requests



----End

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

You can add two types of information leakage prevention rules.

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

Prerequisites

You have [added your website to a policy](#).

Constraints

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

Procedure

Step 1 Log in to the management console.

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

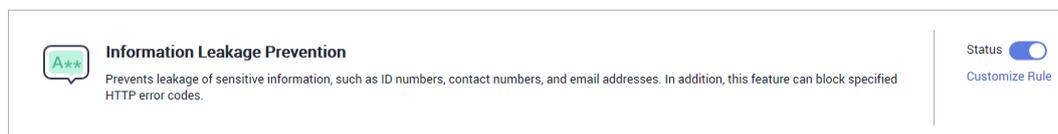
Step 3 Click  in the upper left corner and choose **Web Application Firewall** under **Security**.

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

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

Step 6 In the **Information Leakage Prevention** configuration area, change **Status** if needed and click **Customize Rule**.

Figure 6-55 Information Leakage Prevention configuration area



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

Step 8 In the dialog box displayed, add an information leakage prevention rule by referring to [Table 6-13](#).

Information leakage prevention rules prevent sensitive information (such as ID numbers, phone numbers, and email addresses) from being disclosed. This type of rule can also block specified HTTP status codes.

Sensitive information filtering: Configure rules to mask sensitive information, such as phone numbers and ID numbers, from web pages. For example, you can set the following protection rules to mask sensitive information, such as ID numbers, phone numbers, and email addresses:

Figure 6-56 Sensitive information leakage

Add Information Leakage Prevention Rule [X]

* Path: /admin*

* Type: Sensitive information filtering

* Content: Identification card Phone number Email

Rule Description: [Empty text box]

[Confirm] [Cancel]

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

Figure 6-57 Blocking response codes

Table 6-13 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"> • Prefix match: Only the prefix of the path to be entered must match that of the path to be protected. If the path to be protected is /admin, set Path to /admin*. • Exact match: The path to be entered must match the path to be protected. If the path to be protected is /admin, set Path to /admin. <p>NOTE</p> <ul style="list-style-type: none"> – The path supports prefix and exact matches only. Regular expressions are not supported. – The path cannot contain two or more consecutive slashes. For example, ///admin. If you enter ///admin, the WAF engine converts /// to /. 	/admin*

Parameter	Description	Example Value
Type	<ul style="list-style-type: none"> • Sensitive information filtering • Response code interception: Enable WAF to block the specified HTTP response code page. 	Sensitive information filtering
Content	Information to be protected. Options are Identification card, Phone number, and Email.	Identification card
Rule Description	A brief description of the rule. This parameter is optional.	None

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

----End

Related Operations

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

Configuration Example — Masking Sensitive Information

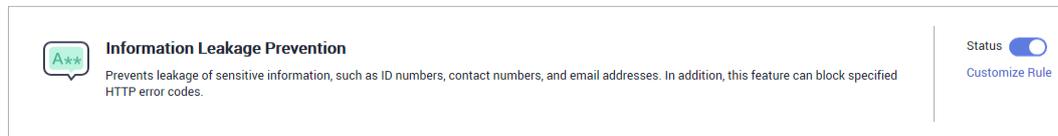
To verify that WAF is protecting your domain name *www.example.com* against an information leakage prevention rule:

Step 1 Add an information leakage prevention rule.

Figure 6-58 Sensitive information leakage

Step 2 Enable information leakage prevention.

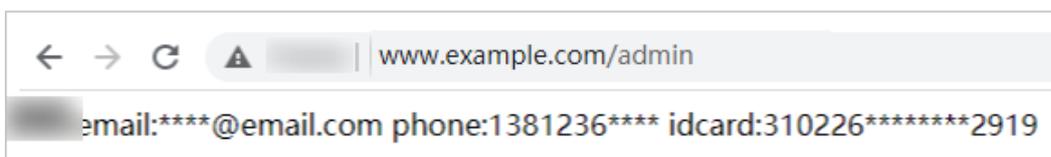
Figure 6-59 Information Leakage Prevention configuration area



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

The email address, phone number, and identity number on the returned page are masked.

Figure 6-60 Sensitive information masked



----End

6.10 Configuring a Global Protection Whitelist Rule to Ignore False Alarms

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

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

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

Prerequisites

A website has been added 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 rules take effect only for events triggered against WAF built-in rules in **Basic Web Protection** and anti-crawler rules under **Feature Library**.
 - Basic web protection rules
Basic web protection defends against common web attacks, such as SQL injection, XSS attacks, remote buffer overflow attacks, file inclusion, Bash vulnerability exploits, remote command execution, directory traversal, sensitive file access, and command and code injections. Basic web protection also detects web shells and evasion attacks.
 - Feature-based anti-crawler protection
Feature-based anti-crawler identifies and blocks crawler behavior from search engines, scanners, script tools, and other crawlers.
- It takes several minutes for a new rule to take effect. After the rule takes effect, protection events triggered by the rule will be displayed on the **Events** page.
- You can configure a global protection whitelist rule by referring to **Handling False Alarms**. After handling a false alarm, you can view the rule in the global protection whitelist rule list.

Procedure

Step 1 Log in to the management console.

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

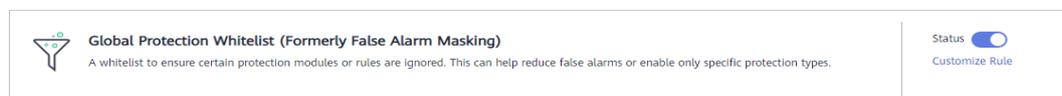
Step 3 Click  in the upper left corner and choose **Web Application Firewall** under **Security**.

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

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

Step 6 In the **Global Protection Whitelist** configuration area, click **Status** if needed. Then, click **Customize Rule**.

Figure 6-61 Global Protection Whitelist configuration area



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

Step 8 Add a global protection whitelist rule by referring to [Table 6-14](#).

Figure 6-62 Add Global Protection Whitelist Rule

Add Global Protection Whitelist Rule

Restrictions and precautions vary by mode. [?](#)

* Scope All domain names Specified domain names

* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/product

[+](#) Add You can add 29 more conditions.(The rule is only applied when **all** conditions are met.)

* Ignore WAF Protection All protection Basic web protection

Rule Description

Table 6-14 Parameters

Parameter	Description	Example Value
Scope	<ul style="list-style-type: none"> All domain names: By default, this rule will be used to all domain names that are protected by the current policy. Specified domain names: Specify a domain name range this rule applies to. 	Specified domain names
Domain Name	<p>This parameter is mandatory when you select Specified domain names for Scope.</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 Add to add conditions. At least one condition needs to be added. You can add up to 30 conditions to a protection rule. If more than one condition is added, all of the conditions must be met for the rule to be applied. A condition includes the following parameters:</p> <p>Parameters for configuring a condition are described as follows:</p> <ul style="list-style-type: none"> • Field • Subfield: Configure this field only when Params, Cookie, or Header is selected for Field. <p>NOTICE 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"> • Logic: Select a logical relationship from the drop-down list. • Content: Enter or select the content that matches the condition. 	Path, Include, / product
Ignore WAF Protection	<ul style="list-style-type: none"> • All protection: All WAF rules do not take effect, and WAF allows all request traffic to the domain names in the rule. • Basic web protection: You can ignore basic web protection by rule ID, attack type, or all built-in rules. For example, if XSS check is not required for a URL, you can whitelist XSS rule. 	Basic web protection
Ignored Protection Type	<p>If you select Basic web protection for Ignored Protection Type, specify the following parameters:</p> <ul style="list-style-type: none"> • ID: Configure the rule by event ID. • Attack type: Configure the rule by attack type, such as XSS and SQL injection. One type contains one or more rule IDs. • All built-in rules: all checks enabled in Basic Web Protection. 	Attack type

Parameter	Description	Example Value
Rule ID	<p>This parameter is mandatory when you select ID for Ignored Protection Type.</p> <p>Rule ID of a misreported event in Events whose type is not Custom. You are advised to handle false alarms on the Events page.</p>	041046
Rule Type	<p>This parameter is mandatory when you select Attack type for Ignored Protection Type.</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 Advanced Settings 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: Params, Cookie, Header, Body, and Multipart.</p> <ul style="list-style-type: none"> • If you select Params, Cookie, or Header, you can select All or Field to configure a subfield. • If you select Body or Multipart, you can select All. • If you select Cookie, the Domain Name box for the rule can be empty. <p>NOTE If All is selected, WAF will not block all attack events of the selected field.</p>	Params All

Step 9 Click **OK**.

----End

Related Operations

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

6.11 Configuring Data Masking Rules to Prevent Privacy Information Leakage

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

Prerequisites

You have [added your website to a policy](#).

Constraints

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

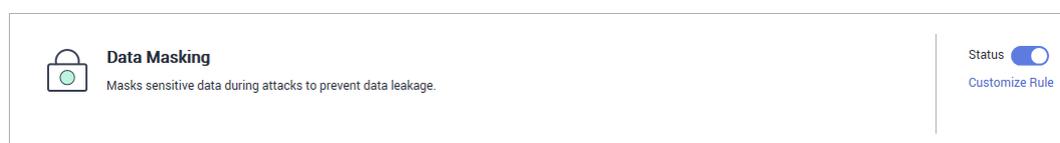
Impact on the System

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

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** Click the name of the target policy to go to the protection configuration page.
- Step 6** In the **Data Masking** configuration area, change **Status** if needed and click **Customize Rule**.

Figure 6-63 Data Masking configuration area



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

Step 8 In the displayed dialog box, specify the parameters described in [Table 6-15](#).

Figure 6-64 Adding a data masking rule

Table 6-15 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"> Prefix match: The path ending with * indicates that the path is used as a prefix. For example, if the path to be protected is <code>/admin/test.php</code> or <code>/adminabc</code>, set Path to <code>/admin*</code>. Exact match: The path to be entered must match the path to be protected. If the path to be protected is <code>/admin</code>, set Path to <code>/admin</code>. <p>NOTE</p> <ul style="list-style-type: none"> The path supports prefix and exact matches only and does not support regular expressions. The path cannot contain two or more consecutive slashes. For example, <code>///admin</code>. If you enter <code>///admin</code>, WAF converts <code>///</code> to <code>/</code>. 	<p><code>/admin/login.php</code></p> <p>For example, if the URL to be protected is <code>http://www.example.com/admin/login.php</code>, set Path to <code>/admin/login.php</code>.</p>

Parameter	Description	Example Value
Masked Field	<p>A field set to be masked</p> <ul style="list-style-type: none"> • Params: A request parameter • Cookie: A small piece of data to identify web visitors • Header: A user-defined HTTP header • Form: A form parameter 	<ul style="list-style-type: none"> • If Masked Field is Params and Field Name is id, content that matches id is masked. • If Masked Field is Cookie and Field Name is name, content that matches name is masked.
Field Name	<p>Set the parameter based on Masked Field. The masked field will not be displayed in logs.</p> <p>NOTICE The length of a subfield cannot exceed 2,048 bytes. Only digits, letters, underscores (_), and hyphens (-) are allowed.</p>	
Rule Description	A brief description of the rule. This parameter is optional.	None

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

----End

Related Operations

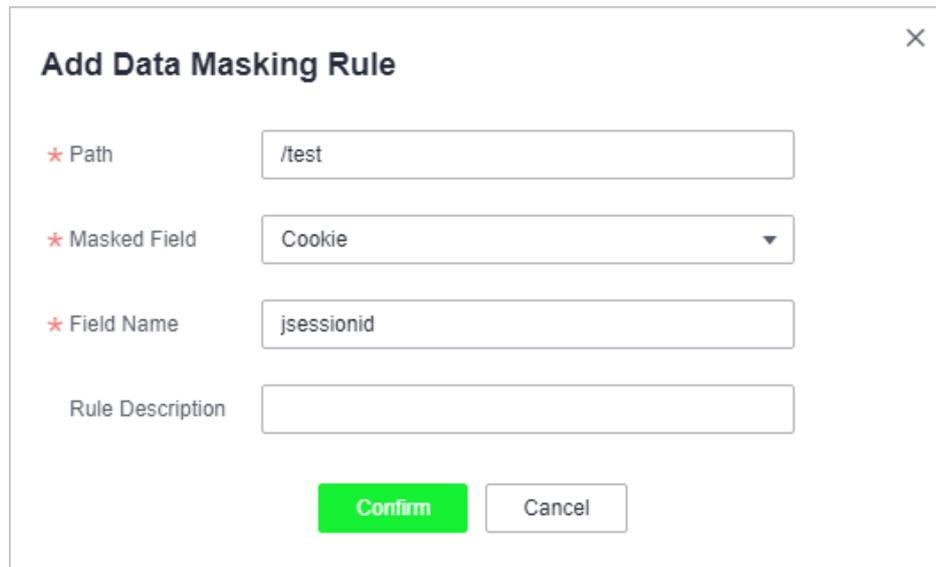
- To disable a rule, click **Disable** in the **Operation** column of the rule. The default **Rule Status** is **Enabled**.
- To modify a rule, click **Modify** in the row containing the rule.
- To delete a rule, click **Delete** in the row containing the rule.

Configuration Example - Masking the Cookie Field

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

Step 1 Add a data masking rule.

Figure 6-65 Select **Cookie** for **Masked Field** and enter **jsessionId** in **Field Name**.



Add Data Masking Rule [Close]

* Path: /test

* Masked Field: Cookie

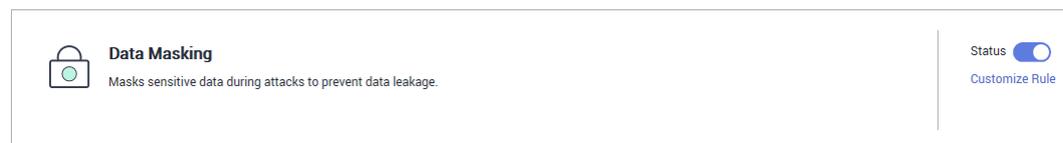
* Field Name: jsessionId

Rule Description: [Empty]

[Confirm] [Cancel]

Step 2 Enable data masking.

Figure 6-66 Data Masking configuration area



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

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

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

Figure 6-67 Viewing events - privacy data masking

Event Details

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

Malicious Load

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

Request Details

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

----End

6.12 Creating a Reference Table to Configure Protection Metrics In Batches

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

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

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

Prerequisites

You have [added your website to a policy](#).

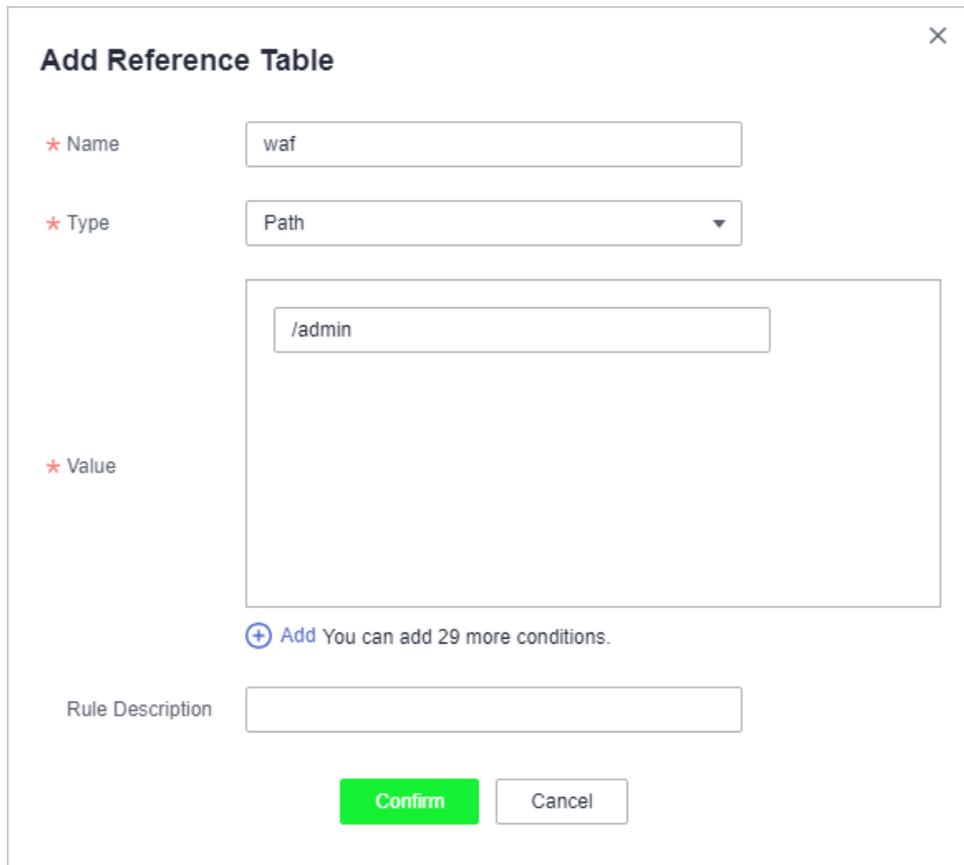
Application Scenarios

Reference tables can be used for configuring multiple protection fields in CC attack protection and precise protection rules.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** Click the name of the target policy to go to the protection configuration page.
- Step 6** In the **CC Attack Protection** or **Precise Protection** area, click **Customize Rule**.
- Step 7** Click **Reference Table Management** in the upper left corner of the list.
- Step 8** On the **Reference Table Management** page, click **Add Reference Table**.
- Step 9** In the **Add Reference Table** dialog box, specify the parameters by referring to [Table 6-16](#).

Figure 6-68 Adding a reference table



Add Reference Table [X]

* Name

* Type

* Value

[+ Add](#) You can add 29 more conditions.

Rule Description

Table 6-16 Parameter description

Parameter	Description	Example Value
Name	Table name you entered	test

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

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

----End

Related Operations

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

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

If WAF blocks a malicious request by IP address, Cookie, or Params, you can configure a known attack source rule to let WAF automatically block all requests

from the attack source for a blocking duration set in the known attack source rule. For example, if a blocked malicious request originates from an IP address and you set the blocking duration to 500 seconds, WAF will block the IP address for 500 seconds after the known attack source rule takes effect.

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

Prerequisites

You have [added your website to a policy](#).

Constraints

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

Specification Limitations

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

Procedure

Step 1 Log in to the management console.

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

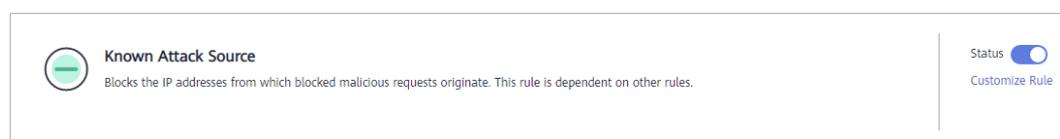
Step 3 Click  in the upper left corner and choose **Web Application Firewall** under **Security**.

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

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

Step 6 In the **Known Attack Source** configuration area, change **Status** if needed and click **Customize Rule** to go to the **Known Attack Source** page.

Figure 6-69 Known Attack Source configuration



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

Step 8 In the displayed dialog box, specify the parameters by referring to [Table 6-17](#).

Figure 6-70 Add Known Attack Source Rule

Table 6-17 Known attack source parameters

Parameter	Description	Example Value
Blocking Type	Specifies the blocking type. The options are: <ul style="list-style-type: none"> • Long-term IP address blocking • Short-term IP address blocking • Long-term Cookie blocking • Short-term Cookie blocking • Long-term Params blocking • Short-term Params blocking 	Long-term IP address blocking

Parameter	Description	Example Value
Blocking Duration (s)	The blocking duration must be an integer and range from: <ul style="list-style-type: none"> • (300, 1800] for long-term blocking • (0, 300] for short-term blocking 	500
Rule Description	A brief description of the rule. This parameter is optional.	None

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

----End

Related Operations

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

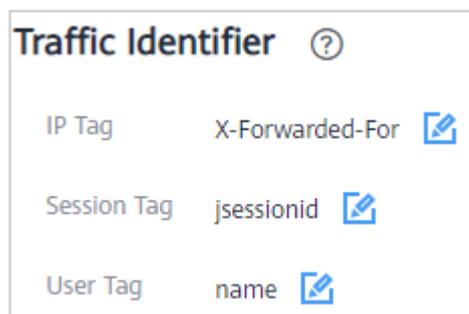
Configuration Example - Blocking Known Attack Source Identified by Cookie

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

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

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

Figure 6-71 Traffic Identifier



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

Figure 6-72 Adding a Cookie-based known attack source rule

Add Known Attack Source Rule

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

Blocking Type: Long-term IP address blocking

* Blocking Duration (s): 600

Rule Description:

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

Confirm Cancel

Step 4 Enable the known attack source protection.

Figure 6-73 Known Attack Source configuration

Known Attack Source
Blocks the IP addresses from which blocked malicious requests originate. This rule is dependent on other rules.

Status Customize Rule

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

Figure 6-74 Specifying a known attack source rule

Add Blacklist or Whitelist Rule

* Rule Name

* IP Address/Range/Group IP address/range Address group

* IP Address/Range

* Protective Action

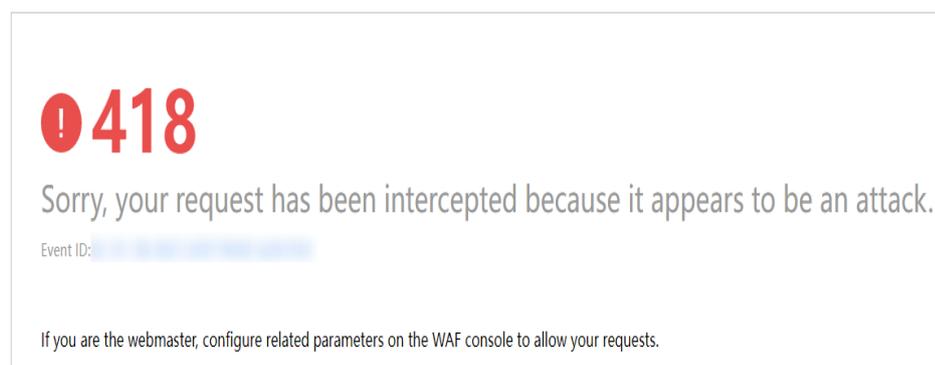
Known Attack Source [Add Known Attack Source Rule](#)

Rule Description

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

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

Figure 6-75 Block page



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

----End

6.14 Condition Field Description

When setting a CC attack, precise access, or global whitelist protection rule, there are some fields in the **Condition List** or **Trigger** area. These fields together are

used to define the request attributes to trigger the rule. This topic describes the fields that you can specify in conditions to trigger a rule.

What Is a Condition Field?

A condition field specifies the request attribute WAF checks against protection rules. When configuring a **CC attack protection rule**, **precise access protection rule**, or **false alarm masking rule**, you can define condition fields to specify request attributes to trigger the rule. If a request meets the conditions set in a rule, the request matches the rule. WAF handles the request based on the action (for example, allow, block, or log only) set in the rule.

Figure 6-76 Condition field

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

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

Supported Condition Fields

Table 6-18 Condition list configurations

Field	Subfield	Logic	Content (Example)
Path: Part of a URL that does not include a domain name. This value supports exact matches only. For example, if the path to be protected is / admin , Path must be set to / admin .	--	Select the desired logical relationship from the Logic drop-down list.	/buy/phone/ NOTICE <ul style="list-style-type: none"> • If Path is set to /, all paths of the website are protected. • The path content cannot contain the following special characters: (' "<>&*#%?\?)

Field	Subfield	Logic	Content (Example)
User Agent: A user agent of the scanner to be protected	--		<i>Mozilla/5.0 (Windows NT 6.1)</i>
IP: An IP address of the visitor to be protected.	--		XXX.XXX.1.1
Params: A request parameter to be protected	<ul style="list-style-type: none"> ● All fields ● Any subfield ● Custom 		201901150929
Referer: A user-defined request resource For example, if the protected path is / admin/xxx and you do not want visitors to access the page from www.test.com , set Content to http://www.test.com .	--		http://www.test.com
Cookie: A small piece of data to identify web visitors	<ul style="list-style-type: none"> ● All fields ● Any subfield ● Custom 		jsessionId
Header: A user-defined HTTP header	<ul style="list-style-type: none"> ● All fields ● Any subfield ● Custom 		<i>text/ html,application/ xhtml +xml,application/ xml;q=0.9,image/ webp,image/apng,*/ *;q=0.8</i>
Method: the user-defined request method.	--		GET, POST, PUT, DELETE, and PATCH
Request Line: Length of a user-defined request line.	--		50

Field	Subfield	Logic	Content (Example)
Request: Length of a user-defined request. It includes the request header, request line, and request body.	--		--
Protocol: the protocol of the request.	--		http

7 Managing Policies

7.1 Creating a Protection Policy

A policy is a combination of rules, such as basic web protection, blacklist, whitelist, and precise protection rules. A policy can be applied to multiple domain names, but only one policy can be used for a domain name. This topic describes how to add a policy for your WAF instance.

Prerequisites

A website has been added to WAF.

Constraints

A protected website domain name can use only one policy.

Adding a Protection Policy

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** In the upper left corner, click **Add Policy**.
- Step 6** In the displayed dialog box, enter the policy name and click **Confirm**. The added policy will be displayed in the policy list.
- Step 7** In the **Policy Name** column, click the policy name. On the displayed page, add rules to the policy by referring to [Rule Configurations](#).

----End

Copying a Protection Policy

NOTE

If your policy has a known attack source rule configured, configure it again after you copy the policy as known attack source rules configured in dependent rules will become invalid in the new policy.

Step 1 Log in to the management console.

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

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

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

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

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

----End

Related Operations

- To modify a policy name, click  next to the policy name. In the dialog box displayed, enter a new policy name.
- To delete a rule, locate the row containing the rule. In the **Operation** column, click **Delete**.
- To delete protection policies in batches, select all policies you want to delete and click **Delete** above the policy list.

7.2 Adding a Domain Name to a Policy

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

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**.

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

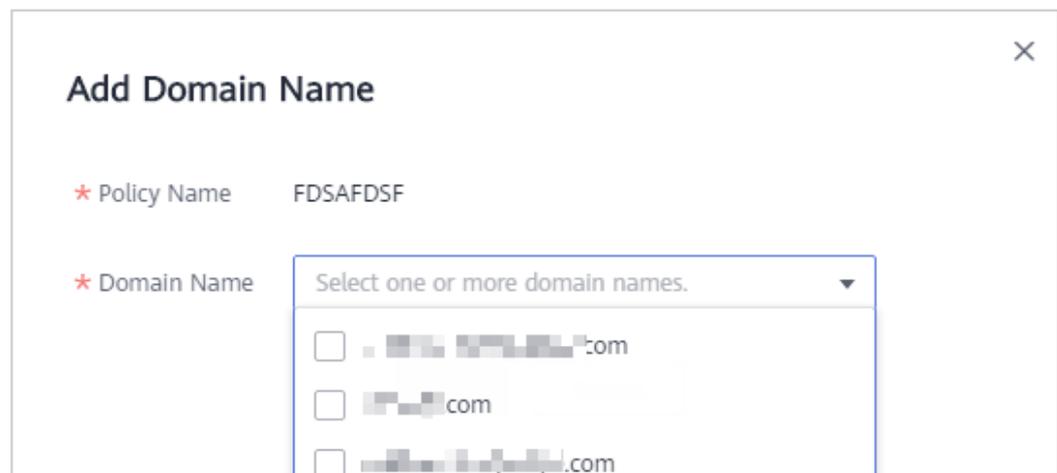
Step 5 In the row containing the policy you want to apply to a website, click **Add Domain Name** in the **Operation** column.

Step 6 Select one or more domain names from the **Domain Name** drop-down list.

NOTICE

- A protected domain name can use only one policy, but one policy can be applied to multiple domain names.
- To delete a policy that has been applied to domain names, add these domain names to other policies first. Then, click **Delete** in the **Operation** column of the policy you want to delete.

Figure 7-1 Selecting one or more domain names



Step 7 Click **Confirm**.

----End

7.3 Adding Rules to One or More Policies

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

Prerequisites

A website has been added to WAF.

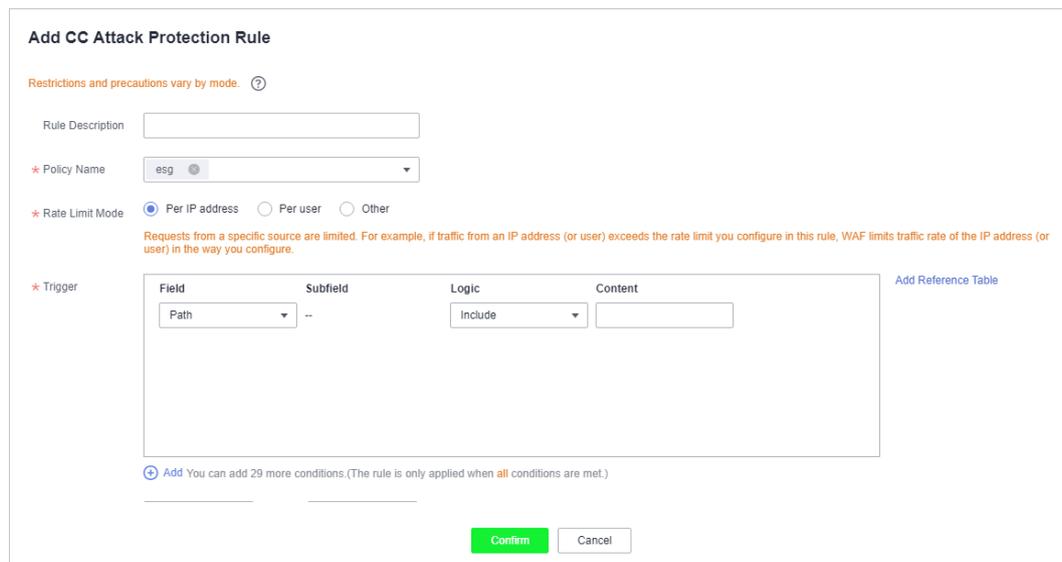
Procedure

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**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** In the upper left corner of the policy list, click **View All My Rules**.
- Step 6** In the upper left corner above a list of a type of rule, click **Add Rule**.
- Step 7** Select one or more policies from the **Policy Name** drop-down list.

Figure 7-2 Adding a rule to one or more policies



The screenshot shows the 'Add CC Attack Protection Rule' configuration interface. It includes a 'Rule Description' text field, a 'Policy Name' dropdown menu set to 'esg', and 'Rate Limit Mode' radio buttons for 'Per IP address' (selected), 'Per user', and 'Other'. A note explains that requests from a specific source are limited. The 'Trigger' section contains a table with columns for Field, Subfield, Logic, and Content. The first row shows 'Path' in the Field column, '--' in the Subfield column, 'Include' in the Logic column, and an empty Content field. A link 'Add Reference Table' is visible to the right. At the bottom, there is a green 'Confirm' button and a grey 'Cancel' button.

- Step 8** Set other parameters.
 - To add a CC attack protection rule, see [Table 6-6](#).
 - To add a precise protection rule, see [Table 6-7](#).
 - To add a blacklist or whitelist rule, see [Table 6-8](#).
 - To add a geolocation access control rule, see [Table 6-9](#).
 - To add a WTP rule, see [Table 6-10](#).
 - To add an information leakage prevention rule, see [Table 6-13](#).
 - To add a global protection whitelist rule, see [Table 6-14](#).
 - To add a data masking rule, see [Table 6-15](#).
 - Step 9** Click **Confirm**.
- End

8 Website Settings

8.1 Adding a Website to WAF (Cloud Mode)

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

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

Constraints

- In CNAME access method, a cloud WAF instance can protect web applications and websites deployed on a cloud or on-premises data center as long as they are accessible through domain names.
- After your website is connected to WAF, you can upload a file no larger than 10 GB each time.

Prerequisites

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

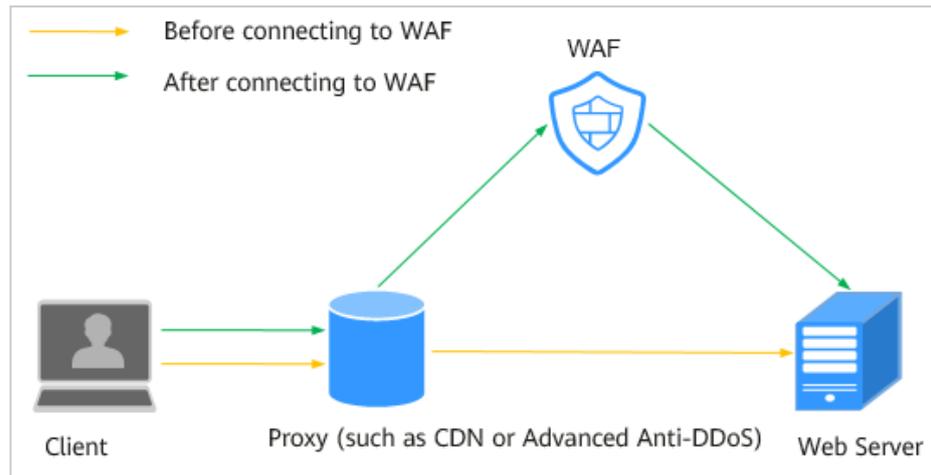
- Proxy used

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

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

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

Figure 8-1 WAF configuration when a proxy is used

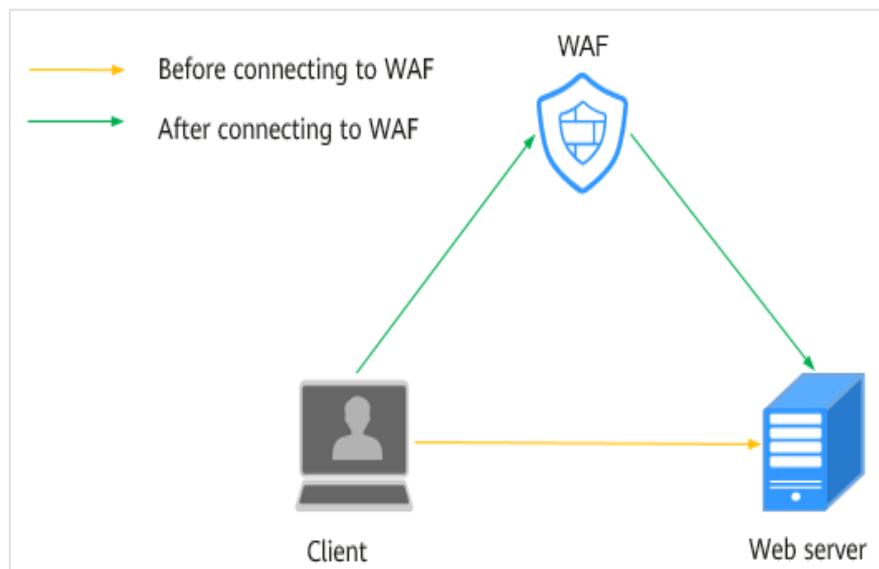


- No proxy used

If no proxy is used before the website is connected to WAF, [Figure 8-2](#) shows how WAF works.

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

Figure 8-2 No proxy used



Processes of Connecting a Website to WAF

After purchasing a cloud WAF instance, complete the required configurations by following the process shown in [Figure 8-3](#).

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

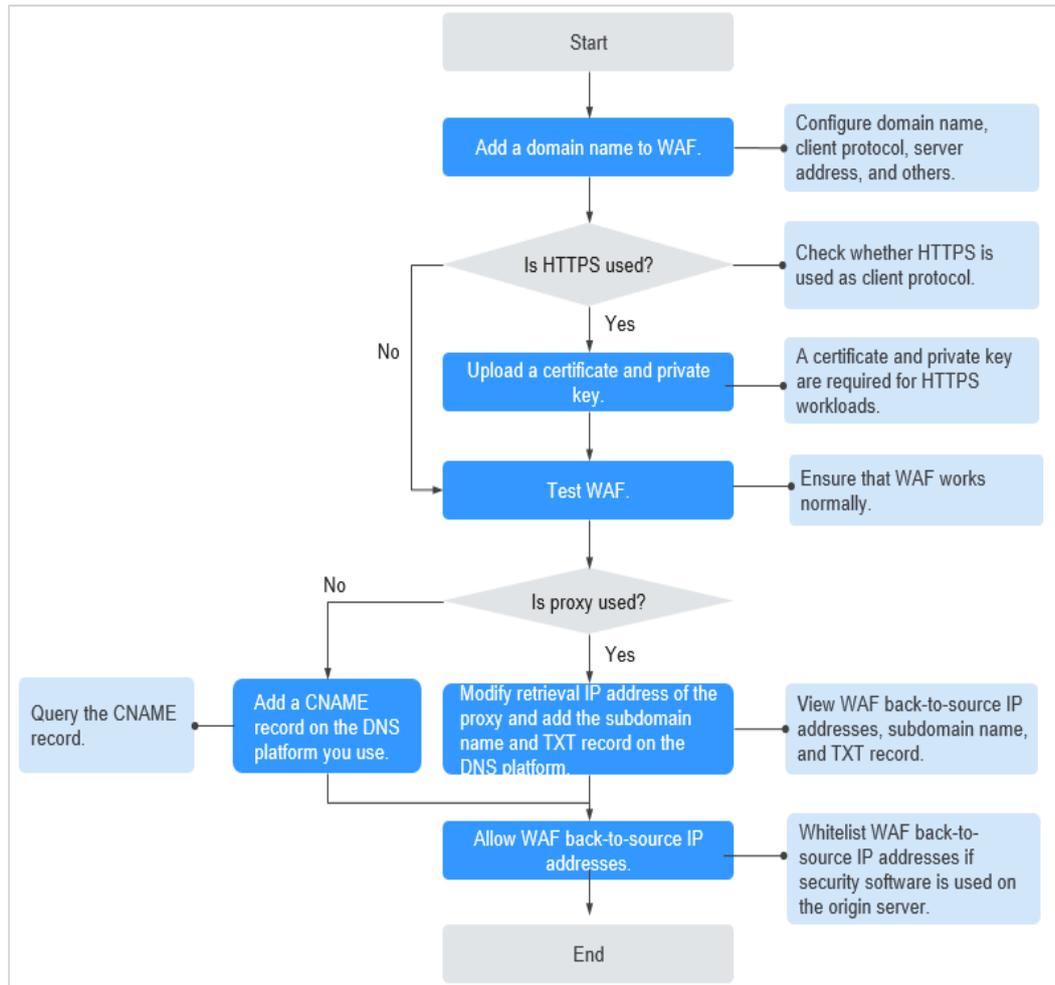


Table 8-1 Process of connecting your website domain name to WAF

Procedure	Description
Step 1: Add a Domain Name to WAF (Cloud Mode)	Configure basic information, such as the domain name, protocol, and origin server.
Step 2: Whitelist WAF IP Addresses	If other security software or firewalls are installed on your origin server, whitelist only requests from WAF. This ensures normal access and protects the origin server from hacking.

Procedure	Description
Step 3: Test WAF	To ensure that your WAF instance forwards website traffic normally, test the WAF instance locally and then route traffic destined for the website domain name to WAF by modifying DNS record.
Step 4: Modify the DNS Records of the Domain Name	<ul style="list-style-type: none"> No proxy used Configure a CNAME record for the protected domain name on the DNS platform you use. Proxy (such as advanced anti-DDoS and CDN) used Change the back-to-source IP address of the used proxy, such as advanced anti-DDoS and CDN, to the copied CNAME record.

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

Collecting Domain Name Details

Before adding a domain name, obtain the information listed in [Table 8-2](#).

Table 8-2 Domain name information required

Information	Parameter	Description	Example
Whether a proxy is used for the domain name	Proxy Configured	If your website has used proxies, such as anti-DDoS, Content Delivery Network (CDN), or cloud acceleration, this parameter must be set to Yes .	-
Parameters	Domain Name	The domain name is used by visitors to access your website. A domain name consists of letters separated by dots (.). It is a human readable address that maps to the machine readable IP address of your server.	www.example.com

Information	Parameter	Description	Example
	Protected Port	<p>The service port corresponding to the domain name of the website you want to protect.</p> <ul style="list-style-type: none"> • Standard Ports <ul style="list-style-type: none"> - 80: default port when the client protocol is HTTP - 443: default port when the client protocol is HTTPS • Non-standard ports Ports other than ports 80 and 443 <p>NOTICE If your website uses a non-standard port, check whether the WAF edition you plan to buy can protect the non-standard port before you make a purchase. For details, see Ports Supported by WAF.</p>	80
	Client Protocol	Protocol used by a client (for example, a browser) to access the website. WAF supports HTTP and HTTPS.	HTTP
	Server Protocol	Protocol used by WAF to forward requests from the client (such as a browser). The options are HTTP and HTTPS .	HTTP
	Server Address	Public IP address or domain name of the origin server for a client (such as a browser) to access. Generally, a public IP address maps to the A record of the domain name configured on the DNS, and a domain name to the CNAME record.	XXX.XXX.1.1
(Optional) Certificate	Certificate Name	<p>If you set Client Protocol to HTTPS, you are required to configure a certificate on WAF and associate the certificate with the domain name.</p> <p>NOTICE Only .pem certificates can be used in WAF. If a certificate is not in .pem, convert it by referring to How Do I Convert a Certificate into PEM Format?</p>	-

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?](#)

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

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

Prerequisites

You have applied for a cloud WAF instance.

Constraints

- Domain names added by an IAM user can be viewed by the account that creates the IAM user, but domain names added by an account cannot be viewed by IAM users created under the account.
- A protected domain name can only be added to WAF once in cloud mode. Each combination of a domain name and a non-standard port is counted towards the domain name quota of the WAF edition you are using. For example, `www.example.com:8080` and `www.example.com:8081` use two domain names of the quota. If you want to protect web services over multiple ports with the same domain name, add the domain name and each port to WAF.
- You can enter a multi-level single domain name (for example, top-level domain name `example.com` and level-2 domain name `www.example.com`) or a wildcard domain name (`*.example.com`).

NOTICE

- WAF does not support wildcard domain names containing underscores (`_`).
 - The following are the rules for adding wildcards to domain names:
 - If the server IP address of each subdomain name is the same, enter a wildcard domain name to be protected. For example, if the subdomain names `a.example.com`, `b.example.com`, and `c.example.com` have the same server IP address, you can add the wildcard domain name `*.example.com` to WAF to protect all three.
 - If the server IP addresses of subdomain names are different, add subdomain names as single domain names one by one.
-
- WAF does not support user-defined HTTP headers for protected domain names.
 - A CNAME record is generated based on the domain name. For the same domain name, the CNAME records are the same.
 - Only `.pem` certificates can be used in WAF.

- WAF supports the WebSocket protocol, which is enabled by default.
 - WebSocket request inspection is enabled by default if **Client Protocol** is set to **HTTP**.
 - WebSockets request inspection is enabled by default if **Client Protocol** is set to **HTTPS**.

Specification Limitations

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

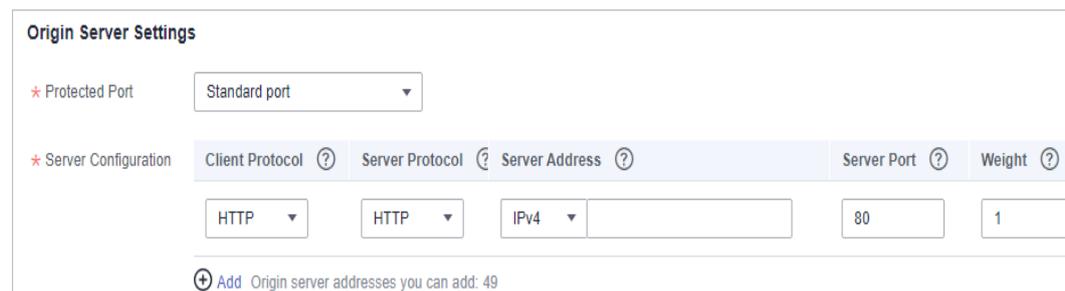
Impact on the System

If a non-standard port is configured, the visitors need to add the non-standard port to the end of the website address when they access the website.

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** Select **Cloud** and click **OK**.
- Step 7** Provide the domain name details.
 - **Website Name:** (Optional) You can customize the website name.
 - **Domain Name:** Enter the domain name you want WAF to protect. You can enter a top-level single domain name, like example.com, a second-level domain name, like www.example.com, or a wildcard domain name, like *.example.com.
 - **Website Remarks:** (Optional) You can provide remarks about your website if you want.
- Step 8** Configure the origin server. [Table 8-3](#) describes the parameters. [Figure 8-4](#) shows an example.

Figure 8-4 Origin Server Settings



Origin Server Settings					
* Protected Port	Standard port				
* Server Configuration	Client Protocol ?	Server Protocol ?	Server Address ?	Server Port ?	Weight ?
	HTTP	HTTP	IPv4	80	1
Add Origin server addresses you can add: 49					

Table 8-3 Parameter description

Parameter	Description	Example Value
Protected Port	<p>Select the port type that you want WAF to protect from the drop-down list.</p> <p>To protect port 80 or 443, select Standard port from the drop-down list.</p>	81
Server Configuration	<p>Configurations of your web server address. You need to configure the client protocol, server protocol, server address, and server port.</p> <ul style="list-style-type: none"> ● Client Protocol: protocol used by a client to access a server. The options are HTTP and HTTPS. ● Server Protocol: protocol used by WAF to forward client requests. The options are HTTP and HTTPS. <p>NOTE</p> <ul style="list-style-type: none"> - For details about configuring Client Protocol and Server Protocol, see Example 4: Configuring Protocols for Different Access Methods. - WAF can check WebSocket and WebSockets request, which is enabled by default. <ul style="list-style-type: none"> ● Server Address: public IP address (generally corresponding to the A record of the domain name configured on the DNS) or domain name (generally corresponding to the CNAME of the domain name configured on the DNS) of the web server that a client accesses. ● Server Port: service port over which the WAF instance forwards client requests to the origin server. 	<p>Client Protocol: HTTP</p> <p>Server Protocol: HTTP</p> <p>Server Address: XXX.XXX.1.1</p> <p>Server Port: 80</p>

Parameter	Description	Example Value
Certificate Name	<p>If you set Client Protocol to HTTPS, an SSL certificate is required. You can select a created certificate or import a certificate. For details about how to import a certificate, see Importing a New Certificate.</p> <p>The imported certificates are listed on the Certificates page. For more details, see Uploading a Certificate.</p> <p>NOTICE</p> <ul style="list-style-type: none"> • Only .pem certificates can be used in WAF. If the certificate is not in .pem format, convert it into .pem by referring to Table 8-5 before uploading the certificate. • If your website certificate is about to expire, purchase a new certificate before the expiration date and update the certificate associated with the website in WAF. • Each domain name must have a certificate associated. A wildcard domain name can only use a wildcard domain certificate. If you only have single-domain certificates, add domain names one by one in WAF. 	--

Step 9 Complete advanced settings.

- **Proxy Configured:** Select **Yes** if your website is using a web proxy, such as anti-DDoS, CDN, or cloud acceleration products.

If your website uses a layer-4 web proxy, such as advanced Anti-DDoS, set **Proxy Configured** to **Yes**. To ensure that WAF protection policies works on real source IP addresses, after [Step 4: Modify the DNS Records of the Domain Name](#) is complete, change **Proxy Configured** to **No** on the **Basic Information** page of the domain name.

Cut

NOTICE

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

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

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

Table 8-4 System-generated policies

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

 **NOTE**

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

Step 10 Click **OK**.

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

----End

Verification

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

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

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

 **NOTE**

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

Example Configuration

There are some configuration examples provided for your reference in [Configuration Example: Adding a Domain Name to WAF](#).

8.1.3 Step 2: Whitelist WAF IP Addresses

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

NOTICE

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

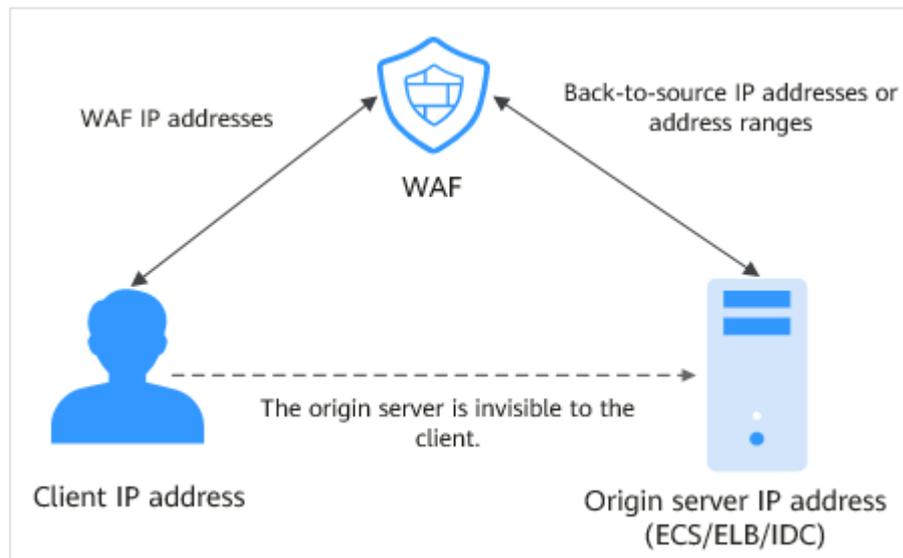
What Are Back-to-Source IP Addresses?

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

NOTE

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

Figure 8-6 Back-to-source IP address



WAF Back-to-Source IP Address Check Mechanism

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

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

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

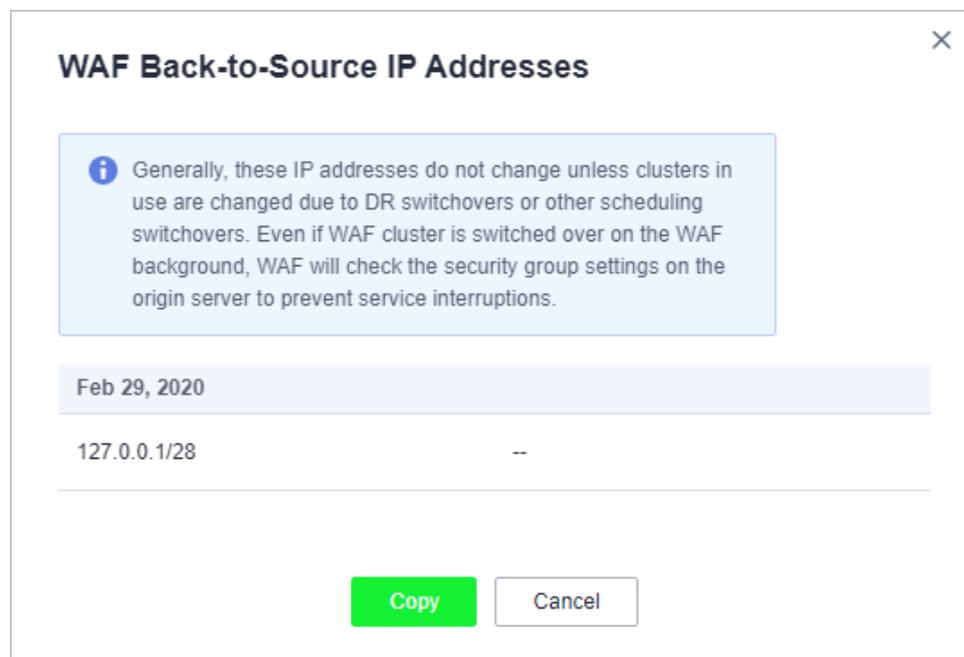
NOTE

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

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane, choose **Website Settings**.
- Step 5** Above the website list, click **WAF Back-to-Source IP Addresses**.
- Step 6** In the displayed dialog box, click **Copy** to copy all the addresses.

Figure 8-7 WAF Back-to-Source IP Addresses dialog box



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

----End

8.1.4 Step 3: Test WAF

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

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

Background

You can configure local DNS records for domain name resolution by modifying local hosts file. To test connection between WAF and your website locally, you

need to resolve the website domain name to WAF IP addresses on a local computer. In this way, you can access the protected domain name from the local computer to verify whether the domain name is accessible after it has been added to WAF, preventing website access exceptions caused by abnormal domain name configurations.

Prerequisites

You have [added your domain name to WAF](#).

Constraints

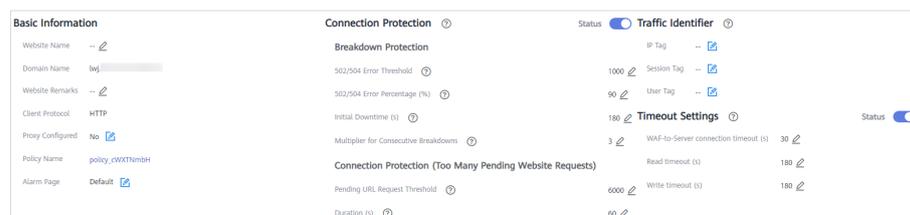
A CNAME record is generated based on the domain name. For the same domain name, the CNAME records are the same.

Connecting a Domain Name to WAF Locally

Step 1 Obtain the CNAME record.

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

Figure 8-8 Basic Information



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

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

Open the CLI and run the **ping CNAME** command to obtain the WAF back-to-source IP address. The WAF access IP address is returned.

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

1. Use a text editor to edit the hosts file. In Windows, the location of the hosts file is as follows:
 - Windows: **C:\Windows\System32\drivers\etc**
 - Linux: **/etc/hosts**
2. Add the WAF IP address obtained in [Step 2](#) and protected domain name to the **hosts** file.

Figure 8-9 Adding a record

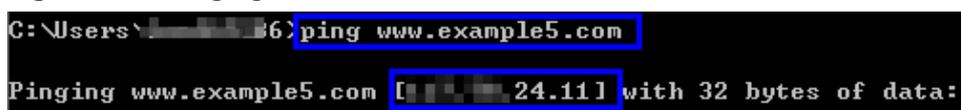
```
# Copyright (c) 1993-2009 Microsoft Corp.
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the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

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

24.11 www.example5.com
```

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

Figure 8-10 Pinging the domain name



```
C:\Users\... #6> ping www.example5.com
Pinging www.example5.com [24.11] with 32 bytes of data:
```

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

----End

Checking Whether WAF Forwarding Is Normal

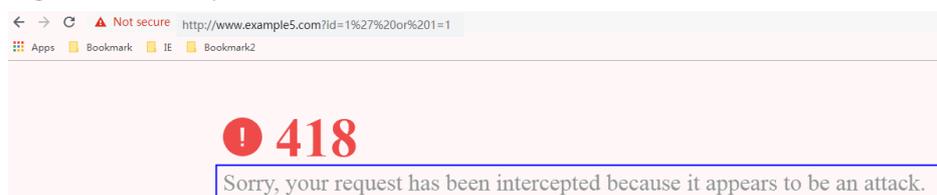
- Step 1** Clear the browser cache and enter the domain name in the address bar to check whether the website is accessible.

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

- Step 2** Simulate simple web attack commands.

1. Set the mode of **Basic Web Protection** to **Block**. For details, see [Enabling Basic Web Protection](#).
2. Clear the browser cache, enter the test domain name in the address bar, and check whether WAF blocks the simulated SQL injection attack against the domain name. [Figure 8-11](#) shows an example.

Figure 8-11 Request blocked



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

----End

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

After a domain name is connected to WAF, WAF functions as a reverse proxy between the client and server. The real IP address of the server is hidden, and only the IP address of WAF is visible to web visitors. You must point the DNS resolution of the domain name to the CNAME record provided by WAF. In this way, access requests can be resolved to WAF.

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

Prerequisites

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

Constraints

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

Specification Limitations

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

How WAF Works

- No proxy used
DNS resolves your domain name to the origin server IP address before the site is connected to WAF. DNS resolves your domain name to the CNAME of WAF after the site is connected to WAF. Then WAF inspects the incoming traffic and filters out malicious traffic.
- A proxy (such as anti-DDoS service) used
If a proxy such as anti-DDoS service is used on your site before it is connected to WAF, DNS resolves the domain name of your site to the anti-DDoS IP address. The traffic goes to the anti-DDoS service and the anti-DDoS service then routes the traffic back to the origin server. After you connect your website to WAF, change the back-to-source address of the proxy (such as anti-DDoS service) to the CNAME of WAF. In this way, the proxy forwards the

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

 **NOTE**

- To ensure that WAF can properly forward requests, test WAF by referring to [Testing WAF](#) before modifying the DNS configuration.
- To prevent other users from configuring your domain names on WAF in advance (this will cause interference on your domain name protection), add the subdomain name and TXT record on your DNS management platform. WAF can determine which user owns the domain name based on the subdomain name and TXT record.

Operation Guide

After a domain name is added, WAF generates a CNAME record, or CNAME, subdomain name, and TXT record for DNS to resolve the domain name to WAF so that website traffic can pass through WAF for detection. For details, see [Table 8-6](#).

Table 8-6 Operation guide

Scenario	Generated Parameter Value	Operation Related to Domain Name Resolution
No proxy used	CNAME	The DNS obtains the CNAME of WAF.
Proxy used	CNAME, subdomain name, and TXT record	<ul style="list-style-type: none"> • Change the back-to-source IP address of the proxy, such as anti-DDoS service, to the CNAME of WAF. • (Optional) Add a WAF subdomain name and TXT record at your DNS provider.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Website Settings**.
- Step 5** In the row containing the desired domain name, click the domain name to go to the **Basic Information** page.
- Step 6** In the **CNAME** row, click  to copy the CNAME record.

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

Step 7 Connect the domain name to WAF.

- No proxy used
Configure the CNAME record at your DNS provider. For details, contact your DNS provider.
- Proxy used
Change the back-to-source IP address of the used proxy, such as anti-DDoS and CDN services, to the copied CNAME record.

 **NOTE**

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

1. Obtain **Subdomain Name** and **TXT Record**: In the row of **Access Status**, click **How to Access**. In the **Access Guide** dialog box, copy **Subdomain Name** and **TXT Record**.
2. Add **Subdomain Name** at the DNS provider and configure **TXT Record** for the subdomain name.

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

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

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

Example command:

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

----End

Follow-up Procedure

- If your server uses other network firewalls, disable these network firewalls or add the WAF IP address range to the IP address whitelist of these network firewalls. Otherwise, these firewalls may regard the WAF IP address as a malicious IP address.
- If your web server is using personal security software, replace it with enterprise security software and whitelist the WAF IP address ranges.

Verification

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

8.1.6 Configuration Example: Adding a Domain Name to WAF

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

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

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

1. Select **Standard port** from the **Protected Port** drop-down list.
2. Select **HTTP** or **HTTPS** for **Client Protocol**. [Figure 8-12](#) and [Figure 8-13](#) show standard port configurations when the client protocol is HTTP or HTTPS.

Figure 8-12 Port 80

Origin Server Settings					
* Protected Port	Standard port				
* Server Configuration	Client Protocol ?	Server Protocol ?	Server Address ?	Server Port ?	Weight ?
⊖	HTTP	HTTP	IPv4 36	80	1
⊖	HTTP	HTTP	IPv4 .9	80	1

Figure 8-13 Port 443

Origin Server Settings					
* Protected Port	Standard port				
* Server Configuration	Client Protocol ?	Server Protocol ?	Server Address ?	Server Port ?	Weight ?
⊖	HTTP	HTTP	IPv4 36	80	1
⊖	HTTP	HTTP	IPv4 .9	80	1

NOTE

- If **Client Protocol** is set to **HTTPS**, a certificate is required.
3. Your website visitors can access the website without adding a port to the end of the domain name. For example, enter **http://www.example.com** in the address box of the browser to access the website.

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

1. In the **Protected Port** drop-down list, select a non-standard port you want to protect.
2. Select **HTTP** or **HTTPS** for **Client Protocol** for all server ports. [Figure 8-14](#) and [Figure 8-15](#) show the configuration of non-standard HTTP or HTTPS port, respectively.

Figure 8-14 Other HTTP port besides port 80

The screenshot shows the 'Origin Server Settings' interface. The 'Protected Port' is set to 8080. Under 'Server Configuration', there are two entries. The first entry has 'Client Protocol' set to HTTP, 'Server Protocol' set to HTTP, 'Server Address' set to .36, and 'Server Port' set to 80. The second entry has 'Client Protocol' set to HTTP, 'Server Protocol' set to HTTP, 'Server Address' set to .9, and 'Server Port' set to 80. A red box highlights the 'Protected Port' field and the 'Client Protocol' dropdowns for both server configurations.

Figure 8-15 Other HTTPS port besides port 443

The screenshot shows the 'Origin Server Settings' interface. The 'Protected Port' is set to 6443. Under 'Server Configuration', there are two entries. The first entry has 'Client Protocol' set to HTTPS, 'Server Protocol' set to HTTP, 'Server Address' set to .36, and 'Server Port' set to 80. The second entry has 'Client Protocol' set to HTTPS, 'Server Protocol' set to HTTP, 'Server Address' set to .9, and 'Server Port' set to 80. A red box highlights the 'Protected Port' field and the 'Client Protocol' dropdowns for both server configurations.

NOTE

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

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

Example 3: Protecting Different Service Ports

If the service ports to be protected are different, configure the ports separately. For example, to protect ports 8080 and 6443 for your site **www.example.com**, add the domain separately for each port, as shown in [Figure 8-16](#) and [Figure 8-17](#).

Figure 8-16 Protecting port 8080

The screenshot shows the 'Origin Server Settings' interface. The 'Protected Port' is set to 8080. Under 'Server Configuration', there is one entry with 'Client Protocol' set to HTTP, 'Server Protocol' set to HTTP, 'Server Address' set to .36, and 'Server Port' set to 80. A red box highlights the 'Protected Port' field and the 'Client Protocol' dropdown.

Figure 8-17 Protecting port 6443

The screenshot shows the 'Origin Server Settings' interface. The 'Protected Port' is set to 6443. Under 'Server Configuration', there is one entry with 'Client Protocol' set to HTTPS, 'Server Protocol' set to HTTP, 'Server Address' set to .36, and 'Server Port' set to 80. A red box highlights the 'Protected Port' field and the 'Client Protocol' dropdown.

Example 4: Configuring Protocols for Different Access Methods

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

- HTTP mode

Figure 8-18 HTTP mode

The screenshot shows the 'Domain Name Details' and 'Origin Server Settings' sections. In 'Domain Name Details', 'Website Name' is a placeholder, 'Domain Name' is 'www.example.com', and 'Website Remarks' is empty. In 'Origin Server Settings', 'Protected Port' is 'Standard port'. The 'Server Configuration' table has the following data:

Client Protocol	Server Protocol	Server Address	Server Port	Weight
HTTP	HTTP	IPv4	80	1

Below the table is a link: '+ Add Origin server addresses you can add: 79'.

NOTICE

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

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

Figure 8-19 HTTPS redirection

The screenshot shows the 'Domain Name Details' and 'Origin Server Settings' sections. In 'Domain Name Details', 'Website Name' is a placeholder, 'Domain Name' is 'www.example.com', and 'Website Remarks' is empty. In 'Origin Server Settings', 'Protected Port' is 'Standard port'. The 'Server Configuration' table has the following data:

Client Protocol	Server Protocol	Server Address	Server Port	Weight
HTTPS	HTTPS	IPv4	443	1

Below the table is a link: '+ Add Origin server addresses you can add: 79'.

NOTICE

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

Figure 8-20 HTTP and HTTPS forwarding

The screenshot shows the 'Origin Server Settings' configuration page. At the top, there is a 'Protected Port' dropdown menu set to 'Standard port'. Below this is a 'Server Configuration' table with columns for Client Protocol, Server Protocol, Server Address, Server Port, and Weight. Two rows are visible: one for HTTP forwarding (Client Protocol: HTTP, Server Protocol: HTTP, Server Address: IPv4, Server Port: 80, Weight: 1) and one for HTTPS forwarding (Client Protocol: HTTPS, Server Protocol: HTTPS, Server Address: IPv4, Server Port: 443, Weight: 1). At the bottom, there is an 'Add' button and a note: 'Origin server addresses you can add: 78'.

NOTICE

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

Figure 8-21 HTTPS offloading

The screenshot shows the 'Domain Name Details' configuration page. It includes fields for 'Website Name' (with a placeholder 'Enter a custom name for the domain name.'), 'Domain Name' (set to 'www.example.com'), and 'Website Remarks'. Below this is the 'Origin Server Settings' section. It features a 'Protected Port' dropdown set to 'Standard port' with a note: 'The port that your website or application provides services over. For example, if `http://www.example.com:8080` needs to be protected, set this parameter to 8080.' The 'Server Configuration' table has columns for Client Protocol, Server Protocol, Server Address, and Server Port. One row is visible for HTTPS offloading (Client Protocol: HTTPS, Server Protocol: HTTP, Server Address: IPv4, Server Port: 80). At the bottom, there is an 'Add' button and a note: 'Origin server addresses you can add: 19'.

NOTICE

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

8.2 Connecting a Website to WAF

8.2.1 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.

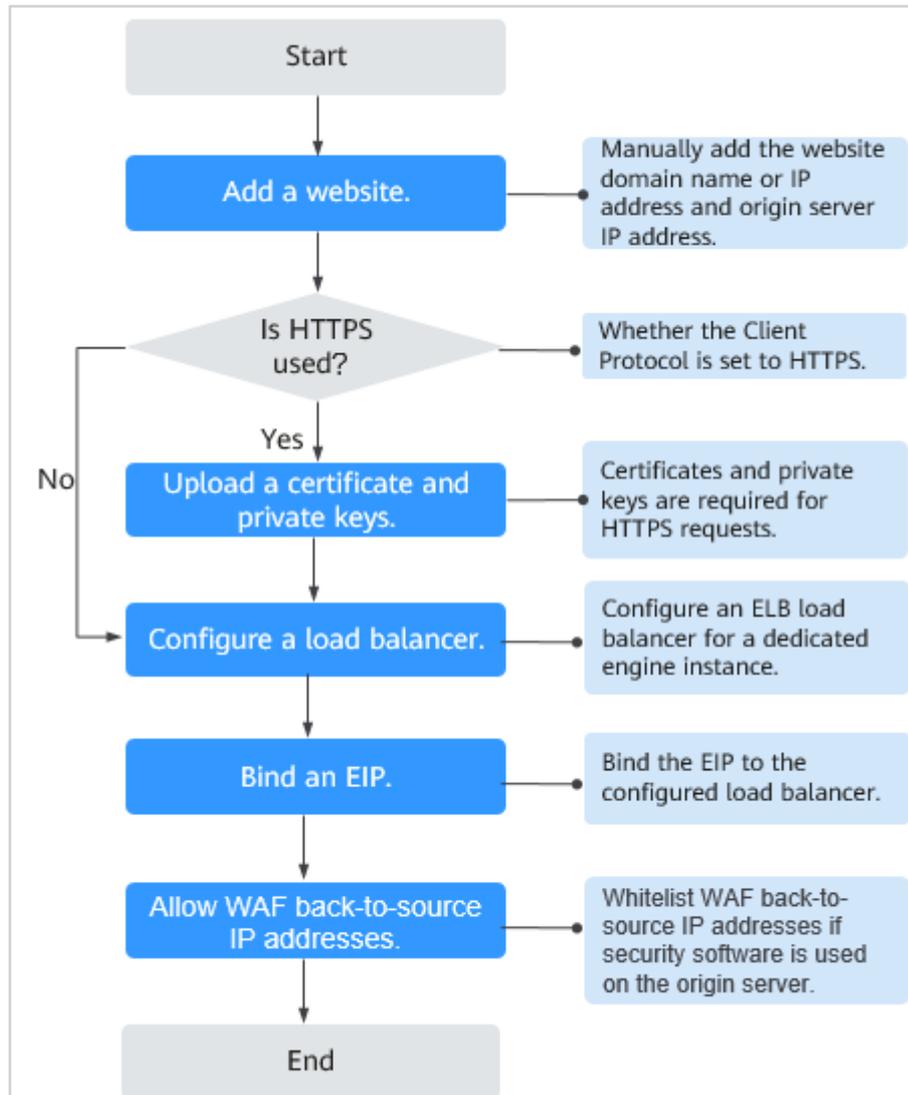
Constraints

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

Processes of Connecting a Website to WAF

Before using a dedicated WAF instance, complete the required configurations by following the process shown in [Figure 8-22](#).

Figure 8-22 Process of connecting a website to a dedicated WAF instance



Collecting Domain Name/IP Address Details

Before adding a domain name or IP address to WAF, obtain the information listed in [Table 8-7](#).

Table 8-7 Domain name or IP address details required

Information	Parameter	Description	Example
Parameters	Protected Object	<ul style="list-style-type: none"> Domain name: used by visitors to access your website. A domain name consists of letters separated by dots (.). It is a human readable address that maps to the machine readable IP address of your server. IP: IP address of the website. 	www.example.com
	Protected Port	<p>The service port corresponding to the domain name of the website you want to protect.</p> <ul style="list-style-type: none"> Standard ports <ul style="list-style-type: none"> 80: default port when the client protocol is HTTP 443: default port when the client protocol is HTTPS Non-standard ports Ports other than ports 80 and 443 	80
	Client Protocol	Protocol used by a client (for example, a browser) to access the website. WAF supports HTTP and HTTPS.	HTTP
	Server Protocol	Protocol used by WAF to forward requests from the client (such as a browser). The options are HTTP and HTTPS .	HTTP
	VPC	Select the VPC that the dedicated WAF instance belongs to.	vpc-default
	Server Address	<p>Private IP address of the website server.</p> <p>Log in to the ECS or ELB console and view the private IP address of the server in the instance list.</p> <p>NOTE The origin server address cannot be the same as that of the protected object.</p>	192.168.1.1

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

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?](#)

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

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

Prerequisites

You have applied for a dedicated WAF instance.

Constraints

- A dedicated Elastic Load Balance (ELB) load balancer has been used to distribute workloads for the website you want to add to WAF.
- If your website has no layer-7 proxy server such as CDN and cloud acceleration service deployed in front of WAF and uses only layer-4 load balancers (or NAT), set **Proxy Configured** to **No**. Otherwise, **Proxy Configured** must be set to **Yes**. This ensures that WAF obtains real IP addresses of website visitors and takes protective actions configured in protection policies.

Procedure

Step 1 Log in to the management console.

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

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

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

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

Step 6 Select **Dedicated** and click **OK**.

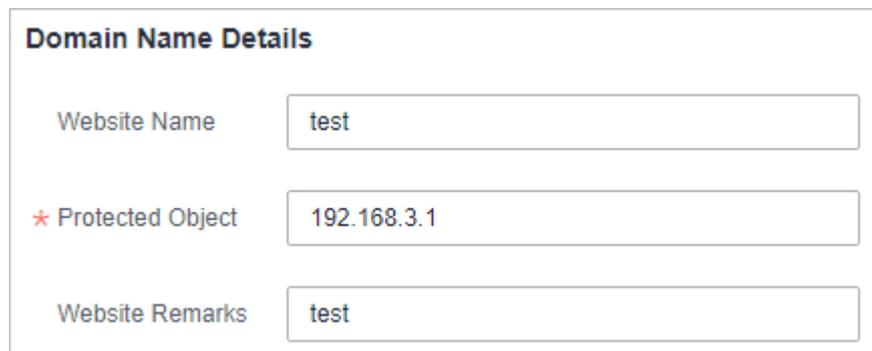
Step 7 Provide the domain name details.

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

 **NOTE**

- The wildcard * can be added to WAF to let WAF protect any domain names. If wildcard (*) is added to WAF, only non-standard ports other than 80 and 443 can be protected.
 - If the server IP address of each subdomain name is the same, enter a wildcard domain name to be protected. For example, if the subdomain names *a.example.com*, *b.example.com*, and *c.example.com* have the same server IP address, you can add the wildcard domain name **.example.com* to WAF to protect all three.
 - If the server IP addresses of subdomain names are different, add subdomain names as single domain names one by one.
- **Website Remarks:** (Optional) You can provide remarks about your website if you want.

Figure 8-23 Configuring domain name details



Domain Name Details

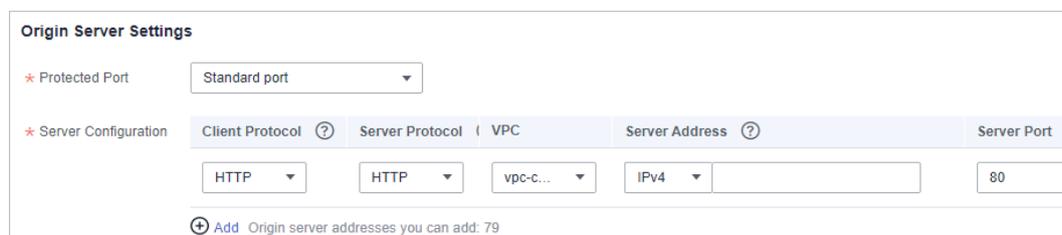
Website Name: test

* Protected Object: 192.168.3.1

Website Remarks: test

Step 8 Configure the origin server by referring to [Table 8-8](#).

Figure 8-24 Origin Server Settings



Origin Server Settings

* Protected Port: Standard port

* Server Configuration

Client Protocol	Server Protocol	VPC	Server Address	Server Port
HTTP	HTTP	vpc-c...	IPv4	80

+ Add Origin server addresses you can add: 79

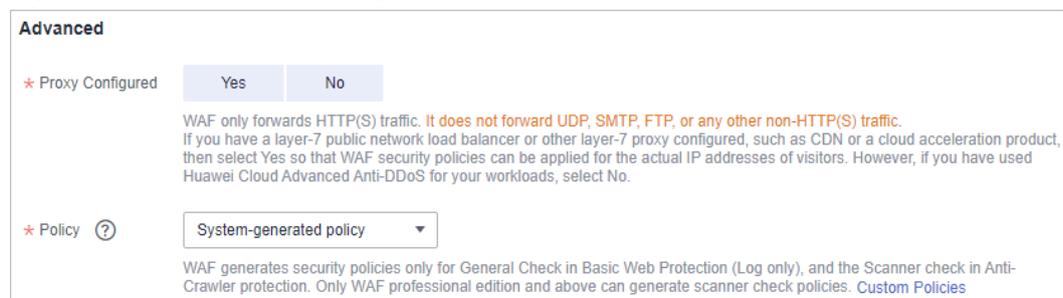
Table 8-8 Parameter description

Parameter	Description	Example Value
Protected Port	<p>Select the port type that you want WAF to protect from the drop-down list.</p> <p>To protect port 80 or 443, select Standard port from the drop-down list.</p>	81
Server Configuration	<p>Address of the web server. The configuration contains the Client Protocol, Server protocol, VPC, Server Address, and Server Port.</p> <ul style="list-style-type: none"> • Client Protocol: protocol used by a client to access a server. The options are HTTP and HTTPS. • Server Protocol: protocol used by WAF to forward client requests. The options are HTTP and HTTPS. • VPC: Select the VPC to which the dedicated WAF instance belongs. <p>NOTE To implement active-active services and prevent single points of failure (SPOFs), it is recommended that at least two WAF instances be configured in the same VPC.</p> <ul style="list-style-type: none"> • Server Address: private IP address of the website server. Log in to the ECS or ELB console and view the private IP address of the server in the instance list. <p>NOTE The origin server address cannot be the same as that of the protected object.</p> <ul style="list-style-type: none"> • Server Port: service port of the server to which the dedicated WAF instance forwards client requests. 	<p>Client Protocol: HTTP</p> <p>Server Protocol: HTTP</p> <p>Server Address: XXX.XXX.1.1</p> <p>Server Port: 80</p>

Parameter	Description	Example Value
Certificate Name	<p>If you set Client Protocol to HTTPS, an SSL certificate is required. You can select an existing certificate or import an external certificate. For details about how to import a certificate, see Importing a New Certificate.</p> <p>The newly imported certificates will be listed on the Certificates page. For more details, see Uploading a Certificate.</p> <p>NOTICE</p> <ul style="list-style-type: none"> • Only .pem certificates can be used in WAF. If the certificate is not in .pem format, convert it into .pem by referring to Importing a New Certificate before uploading the certificate. • If your website certificate is about to expire, purchase a new certificate before the expiration date and update the certificate associated with the website in WAF. • Each domain name must have a certificate associated. A wildcard domain name can only use a wildcard domain certificate. If you only have single-domain certificates, add domain names one by one in WAF. 	--

Step 9 Configure the advanced settings.

Figure 8-25 Advanced settings



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

System-generated policies include:

- Basic web protection (**Log only** mode and common checks)
The basic web protection defends against attacks such as SQL injections, XSS, remote overflow vulnerabilities, file inclusions, Bash vulnerabilities,

remote command execution, directory traversal, sensitive file access, and command/code injections.

- Anti-crawler (**Log only** mode and **Scanner** feature)

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

 **NOTE**

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

Step 10 Click **OK**.

To enable WAF protection, there are still several steps, including configuring a load balancer, binding an EIP to the load balancer, and whitelisting WAF IP addresses. You can click **Later** in this step. Then, follow the instructions and finish those steps by referring to [Step 2: Configure a Load Balancer for WAF](#), [Step 3: Bind an EIP to a Load Balancer](#), and [Step 4: Whitelist IP Addresses of Dedicated WAF Instances](#).

----End

Verification

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

Importing a New Certificate

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

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

Figure 8-26 Import New Certificate

Import New Certificate ✕

★ Type International

★ Certificate Name

★ Certificate File ?

```
-----BEGIN CERTIFICATE-----
MIICCCzCCAbWgAwIBAgIUkZgVFNO3ixWm6z8uRI7X/gfngswDQYJKoZIhvcNAQEL
BQAwWjELMAkGA1UEBhMCY24xEzARBgNVBAGMCINvbWU3RhdGUxIT
AfBgNVBAoM
GEludGVybmV0IFdpZGdpdHMgUHR5IEIx0ZDEtMDEyLWU3RhdGUxIT
QlMNVbTAE
Fw0yMDA4MzEwNjU1MDBaFw0yMDA5MzAwNjU1MDBaMFoxCzAJBgNVB
AYTAmNuMRMw
EQYDVQIDApTb21lLVN0YXRIMSEwHwYDVQQKDBhJbnRlcm5ldCBXaW
it is recommended that the certificate file contain the certificate chain.
```

★ Private Key ?

```
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAMcTlLpLOam9YVktC7xOj3F1XGNd6G2DHNG4XK6JxCSiH
HqA2HHZ
utq8Bt4vhhLLO/2AFj5t5r+qA4JxS0SOU5MCAwEAAQJAE9B66QJIO/frGr0kn
K6m
vWZ8pTPP+1iYWWmfybf+LouRotPKytlARvG4rVslDD+ihzwHmZ89Sv+Dd
OuBV
oQlhAPAprDgVeHYTiti5c027w1Zm5eQHTWtVtRlvi7/aU3RAIEA1DRwnE4ls
nbS
xM0jcFIKu2TD9vKnD+Ull/radoVQaLMCIEZ0UzuYwOAS15bAwNy7CpEcWr
```

NOTE

WAF encrypts and saves the private key to keep it safe. Only .pem certificates can be used in WAF. If the certificate is not in .pem format, convert it into .pem locally by referring to [Table 8-9](#) before uploading it.

Table 8-9 Certificate conversion commands

Format	Conversion Method
CER/CRT	Rename the cert.crt certificate file to cert.pem .
PFX	<ul style="list-style-type: none"> Obtain a private key. For example, run the following command to convert cert.pfx into key.pem: openssl pkcs12 -in cert.pfx -nocerts -out key.pem -nodes Obtain a certificate. For example, run the following command to convert cert.pfx into cert.pem: openssl pkcs12 -in cert.pfx -nokeys -out cert.pem

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

 **NOTE**

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

8.2.3 Step 2: Configure a Load Balancer for WAF

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

Prerequisites

- You have added a website to a dedicated WAF instance.
- You have created a load balancer.
- Related ports have been enabled in the security group to which the dedicated WAF instance belongs.

You can configure your security group as follows:

– Inbound rules

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

– Outbound rules

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

Constraints

- If **Health Check** is configured, the health check result of the dedicated instance must be **Normal**, or the website requests cannot be pointed to WAF.
- The backend port for the listener must be the same as the service port protected by the dedicated WAF instance, which is the protection port set in [Step 1: Add a Website to WAF \(Dedicated Mode\)](#).
- WAF works as a layer-7 proxy. When configuring a listener, you can only select HTTP or HTTPS as the frontend protocol.

Impact on the System

If you select **Weighted round robin** for **Load Balancing Algorithm**, disable **Sticky Session**. If you enable **Sticky Session**, the same requests will be forwarded to the same dedicated WAF instance. If this instance becomes faulty, an error will occur when the requests come to it next time.

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 **Load Balancers** page.
- Step 4** Click the name of the load balancer in the **Name** column to go to the **Basic Information** page.
- Step 5** Locate the **IP as a Backend** row, enable the function. In the displayed dialog box, click **OK**.
- Step 6** Click the **Listeners** tab, click **Add Listener**, and configure the listener name, front-end protocol, and port.
- Step 7** 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 8** Click **Next: Add Backend Server**. Then, select the **IP as Backend Servers** tab.

NOTICE

In the health check configuration, **Protocol** can only be set to **TCP**, or the health check will fail and ELB will not forward traffic to the backend WAF.

- Step 9** Click **Add IP as Backend Server**. In the displayed dialog box, configure **Backend Server IP Address** and **Backend Port**.
- **Backend Server IP Address:** Enter the IP address of the dedicated WAF engine, which you can obtain from the dedicated engine list.
 - **Backend Port:** Use the same one you configured in [Step 1: Add a Website to WAF \(Dedicated Mode\)](#). If you configure a standard port for the website, set the HTTP listening port to **80** and HTTPS listening port to **443**.
- Step 10** Click **OK**.
- Step 11** Click **Next: Confirm**, confirm the information, and click **Submit**.
- End

Verification

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

8.2.4 Step 3: Bind an EIP to a Load Balancer

If you configure a load balancer for your dedicated WAF instance, unbind the EIP from the origin server and then bind this EIP to the load balancer you configured. For details, see [Configuring a Load Balancer](#). The request traffic then goes to the dedicated WAF instance for attack detection first and then go to the origin server, ensuring the security, stability, and availability of the origin server.

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

Prerequisites

You have configured [a load balancer](#) for a dedicated WAF instance.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner of the page and choose **Elastic Load Balance** under **Network** to go to the ELB console.
- Step 4** On the **Load Balancers** page, unbind the EIP from the origin server.
- Unbinding an IPv4 EIP: Locate the row that contains the load balancer configured for the origin server. Then, in the **Operation** column, click **More > Unbind IPv4 EIP**.
 - Unbinding an IPv6 EIP: Locate the row that contains the load balancer configured for the origin server. Then, in the **Operation** column, click **More > Unbind IPv6 Address**.
- Step 5** In the displayed dialog box, click **Yes**.

Step 6 On the **Load Balancers** page, locate the load balancer configured for the dedicated WAF instance and bind the EIP unbound from the origin server to the load balancer.

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

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

----End

8.2.5 Step 4: Whitelist IP Addresses of Dedicated WAF Instances

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

NOTICE

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

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

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

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

Prerequisites

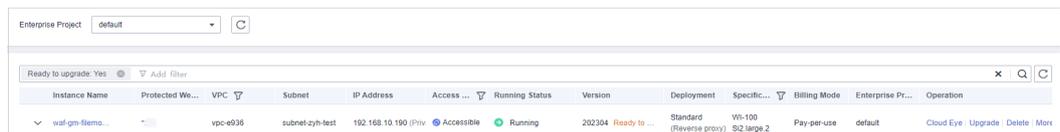
Your website has been connected to your dedicated WAF instances.

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.

Figure 8-27 Dedicated engine list



Instance Name	Protected We...	VPC	Subnet	IP Address	Access ...	Running Status	Version	Deployment	Specific...	Billing Mode	Enterprise Pr...	Operation
waf-gn-filem...		vpc-e936	subnet-zyh-test	192.168.10.190 (Priv)	Accessible	Running	202304	Standard (Reverse proxy) W-100 92-large.2		Pay-per-use	default	Cloud Eye Upgrade Delete More

- Step 5** In the **IP Address** column, obtain the IP address of each dedicated WAF instance under your account.
- Step 6** Click  in the upper left corner of the page and choose **Compute > Elastic Cloud Server**.
- Step 7** Locate the row containing the ECS hosting your website. In the **Name/ID** column, click the ECS name to go to the ECS details page.
- Step 8** Click the **Security Groups** tab. Then, click **Change Security Group**.
- Step 9** In the **Change Security Group** dialog box displayed, select a security group or create a security group and click **OK**.
- Step 10** Click the security group ID and view the details.
- Step 11** Click the **Inbound Rules** tab and click **Add Rule**. Then, specify parameters in the **Add Inbound Rule** dialog box. For details, see [Table 8-10](#).

Table 8-10 Inbound rule parameters

Parameter	Description
Protocol & Port	Protocol and port for which the security group rule takes effect. If you select TCP (Custom ports) , enter the origin server port number in the text box below the TCP box.

Parameter	Description
Source	Subnet IP address of each dedicated WAF instance you obtain in Step 5 . Configure an inbound rule for each IP address. NOTE An inbound rule can contain only one IP address. To configure an inbound rule for each IP address, click Add Rule to add more rules. A maximum of 10 rules can be configured.

Step 12 Click **OK**.

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

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

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

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

----End

Pointing Traffic to a Load Balancer

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

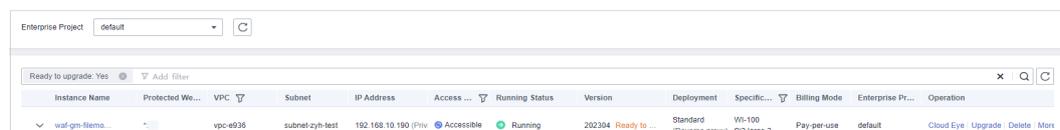
Step 1 Log in to the management console.

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

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

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

Figure 8-28 Dedicated engine list



Instance Name	Protected We...	VPC	Subnet	IP Address	Access...	Running Status	Version	Deployment	Specific...	Billing Mode	Enterprise Pr...	Operation
waf-gm-fitemo...		vpc-e936	subnet-zyh-test	192.168.10.190 (Priv)	Accessible	Running	202304	Standard (Reverse proxy)	W1-100 Siz:large.2	Pay-per-use	default	Cloud Eye Upgrade Delete More

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

- Step 6** Click  in the upper left corner of the page and choose **Networking > Elastic Load Balance**.
- Step 7** Locate the row containing the load balancer configured for your dedicated WAF instance and click the load balancer name in the **Name** column.
- Step 8** In the **Access Control** row of the target listener, click **Configure**.

Figure 8-29 Listener list



Name/ID	Monitoring	Frontend Protocol/Port	Health Check	Default Backend Server Group	Access Control	Operation
listener-76c-172395a-0402-40be-0512-77094b1271e29		HTTP/80	 Healthy	server_group-8081 View/Add Backend Server	All IP addresses Configure	Add/Edit Forwarding Policy Edit Delete

- Step 9** In the displayed dialog box, select **Whitelist** for **Access Control**.
1. Click **Create IP Address Group** and add the dedicated WAF instance IP addresses obtained in **Step 5** to the group being created.
 2. Select the IP address group created in **Step 9.1** from the **IP Address Group** drop-down list.
- Step 10** Click **OK**.

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

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

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

```
Telnet Origin server IP address443
----End
```

8.2.6 Step 5: Test Dedicated WAF Instances

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

Prerequisites

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

(Optional) Testing a Dedicated WAF Instance

- Step 1** Create an ECS that is in the same VPC as the dedicated WAF instance for sending requests.
- Step 2** Send requests to the dedicated WAF through the ECS created in **Step 1**.

- **Forwarding test**

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

For example:

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

 If the response code is 200, the request has been forwarded.
- **Attack blocking test**
 - a. Ensure that the block mode for basic web protection has been enabled in the policy used for the protected website.
 - b. Run the following command:

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

Example:

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

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

----End

Testing the Dedicated WAF Instance and Dedicated ELB Load Balancer

- **Forwarding test**

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

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

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

 Example:

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

 If the response code is 200, the request has been forwarded.
 If the dedicated WAF instance works but the request fails to be forwarded, check the load balancer settings first. If the load balancer health check result is unhealthy, disable health check and perform the preceding operations again.
- **Attack blocking test**
 - a. Ensure that the block mode for basic web protection has been enabled in the policy used for the protected website.
 - b. Run the following command:

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

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

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

 Example:

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

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

8.3 Advanced Settings

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

Transport Layer Security (TLS) provides confidentiality and ensures data integrity for data sent between applications over the Internet. HTTPS is a network protocol constructed based on TLS and HTTP and can be used for encrypted transmission and identity authentication. If you set **Client Protocol** to **HTTPS**, set the minimum TLS version and cipher suite (a set of multiple cryptographic algorithms) for your domain name to block requests that use a TLS version earlier than the configured one.

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

Prerequisites

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

Constraints

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

Application Scenarios

By default, the minimum TLS version configured for WAF is **TLS v1.0**. To ensure website security, configure the right TLS version for your service requirements. [Table 8-11](#) lists the recommended minimum TLS versions for different scenarios.

Table 8-11 Recommended minimum TLS versions

Scenario	Minimum TLS Version (Recommended)	Protection Effect
Websites that handle critical business data, such as sites used in banking, finance, securities, and e-commerce.	TLS v1.2	WAF automatically blocks website access requests that use TLS v1.0 or TLS v1.1.

Scenario	Minimum TLS Version (Recommended)	Protection Effect
Websites with basic security requirements, for example, small- and medium-sized enterprise websites.	TLS v1.1	WAF automatically blocks website access requests that use TLS v1.0.
Client applications with no special security requirements	TLS v1.0	Requests using any TLS protocols can access the website.

 **NOTE**

Before you configure TLS, [check the TLS version of your website](#).

The recommended cipher suite in WAF is **Cipher suite 1**. Cipher suite 1 offers a good mix of browser compatibility and security. For details about each cipher suite, see [Table 8-12](#).

Table 8-12 Description of cipher suites

Cipher Suite Name	Cryptographic Algorithm Supported	Cryptographic Algorithm Not Supported	Description
Default cipher suite NOTE By default, Cipher suite 1 is configured for websites. However, if the request does not carry the server name indication (SNI), WAF uses the Default cipher suite .	<ul style="list-style-type: none"> • ECDHE-RSA-AES256-SHA384 • AES256-SHA256 • RC4 • HIGH 	<ul style="list-style-type: none"> • MD5 • aNULL • eNULL • NULL • DH • EDH • AESGCM 	<ul style="list-style-type: none"> • Compatibility: Good. A wide range of browsers are supported. • Security: Average

Cipher Suite Name	Cryptographic Algorithm Supported	Cryptographic Algorithm Not Supported	Description
Cipher suite 1	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES256-GCM-SHA384 • HIGH 	<ul style="list-style-type: none"> • MEDIUM • LOW • aNULL • eNULL • DES • MD5 • PSK • RC4 • kRSA • 3DES • DSS • EXP • CAMELLIA 	<p>Recommended configuration.</p> <ul style="list-style-type: none"> • Compatibility: Good. A wide range of browsers are supported. • Security: Good
Cipher suite 2	<ul style="list-style-type: none"> • ECDH+AESGCM • EDH+AESGCM 	-	<ul style="list-style-type: none"> • Compatibility: Average. Strict compliance with forward secrecy requirements of PCI DSS and excellent protection, but browsers of earlier versions may be unable to access the website. • Security: Excellent

Cipher Suite Name	Cryptographic Algorithm Supported	Cryptographic Algorithm Not Supported	Description
Cipher suite 3	<ul style="list-style-type: none"> • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-SHA384 • RC4 • HIGH 	<ul style="list-style-type: none"> • MD5 • aNULL • eNULL • NULL • DH • EDH 	<ul style="list-style-type: none"> • Compatibility: Average. Earlier versions of browsers may be unable to access the website. • Security: Excellent. Multiple algorithms, such as ECDHE, DHE-GCM, and RSA-AES-GCM, are supported.
Cipher suite 4	<ul style="list-style-type: none"> • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-RSA-AES256-SHA384 • AES256-SHA256 • RC4 • HIGH 	<ul style="list-style-type: none"> • MD5 • aNULL • eNULL • NULL • EDH 	<ul style="list-style-type: none"> • Compatibility: Good. A wide range of browsers are supported. • Security: Average. The GCM algorithm is supported.
Cipher suite 5	<ul style="list-style-type: none"> • AES128-SHA:AES256-SHA • AES128-SHA256:AES256-SHA256 • HIGH 	<ul style="list-style-type: none"> • MEDIUM • LOW • aNULL • eNULL • EXPORT • DES • MD5 • PSK • RC4 • DHE 	Supported algorithms: RSA-AES-CBC only

Cipher Suite Name	Cryptographic Algorithm Supported	Cryptographic Algorithm Not Supported	Description
Cipher suite 6	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 	-	<ul style="list-style-type: none"> • Compatibility: Average • Security: Good

The TLS cipher suites in WAF are compatible with all browsers and clients of later versions but are incompatible with some browsers of earlier versions. [Table 8-13](#) lists the incompatible browsers and clients if the TLS v1.0 protocol is used.

NOTICE

It is recommended that compatibility tests should be carried out on the service environment to ensure service stability.

Table 8-13 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

Browser/Client	Default Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4
Google Chrome 49/ Windows XP SP3	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
Internet Explorer 6 /Windows XP	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
Internet Explorer 8 /Windows XP	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
Safari 6/iOS 6.0.1	Compatible	Compatible	Not compatible	Compatible	Compatible
Safari 7/iOS 7.1	Compatible	Compatible	Not compatible	Compatible	Compatible
Safari 7/OS X 10.9	Compatible	Compatible	Not compatible	Compatible	Compatible
Safari 8/iOS 8.4	Compatible	Compatible	Not compatible	Compatible	Compatible
Safari 8/OS X 10.10	Compatible	Compatible	Not compatible	Compatible	Compatible
Internet Explorer 7/Windows Vista	Compatible	Compatible	Not compatible	Compatible	Compatible
Internet Explorer 8, 9, or 10 /Windows 7	Compatible	Compatible	Not compatible	Compatible	Compatible
Internet Explorer 10 /Windows Phone 8.0	Compatible	Compatible	Not compatible	Compatible	Compatible
Java 7u25	Compatible	Compatible	Not compatible	Compatible	Compatible

Browser/Client	Default Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4
OpenSSL 0.9.8y	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
Safari 5.1.9/OS X 10.6.8	Compatible	Compatible	Not compatible	Compatible	Compatible
Safari 6.0.4/OS X 10.8.4	Compatible	Compatible	Not compatible	Compatible	Compatible

Impact on the System

- If you enable the PCI DSS certification check:
 - The minimum TLS version and cypher suite are automatically set to **TLS v1.2** and **EECDH+AESGCM:EDH+AESGCM**, respectively, and cannot be changed.
 - To change the minimum TLS version and cipher suite, disable the check.
- If you enable the PCI 3DS certification check:
 - The minimum TLS version is automatically set to **TLS v1.2** and cannot be changed.
 - The check cannot be disabled.

Procedure

Step 1 Log in to the management console.

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

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

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

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

Step 6 In the **Compliance Certification** row, you can select **PCI DSS** and/or **PCI 3DS** to allow WAF to check your website for the corresponding PCI certification compliance. In the **TLS Configuration** row, click  to complete TLS configuration.

Figure 8-30 TLS configuration modification

Basic Information	
Website Name	--
Domain Name	0910 <input type="text"/> com
Website Remarks	--
Client Protocol	HTTPS
Compliance Certification	<input type="checkbox"/> PCI DSS <input type="checkbox"/> PCI 3DS
International	Certificate Name dmc0909
	TLS Configuration TLS v1.0 Ciphersuite 1
Proxy Configured	No
Policy Name	policy_NXiqWhDp
Alarm Page	Default

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

NOTICE

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

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

NOTICE

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

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

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

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

Step 8 Click **Confirm**.

----End

Verification

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

8.3.2 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**.

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

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

Step 6 In the **Traffic Identifier** area, click  next to **IP Tag**, **Session Tag**, or **User Tag** to configure a traffic identifier by referring to [Table 8-14](#).

Figure 8-31 Traffic Identifier

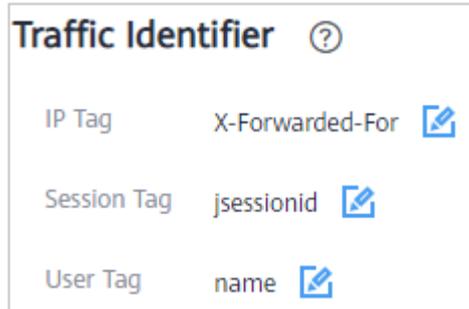


Table 8-14 Traffic identifier parameters

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 Proxy Configured under the website basic information settings is set to Yes for this parameter to take effect.</p> <p>This field is used to store the real IP address of the client. You can customize the field name and configure multiple fields (separated by commas). After the configuration, WAF preferentially reads the configured field to obtain the real IP address of the client. If multiple fields are configured, WAF reads the IP address from left to right.</p> <p>NOTICE</p> <ul style="list-style-type: none"> • If you want to use a TCP connection IP address as the client IP address, set IP Tag to \$remote_addr. • If WAF does not obtain the real IP address of a client from fields you configure, WAF reads the cdn-src-ip, x-real-ip, x-forwarded-for, and \$remote_addr fields in sequence to read the client IP address. 	X-Forwarded-For
Session Tag	<p>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.</p>	jsessionid

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

Step 7 Click **Confirm**.

----End

8.3.3 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**.

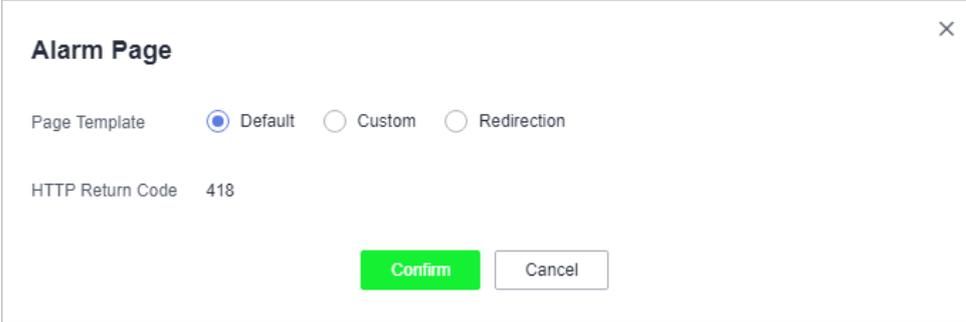
Step 4 In the navigation pane on the left, choose **Website Settings**.

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

Step 6 Click the edit icon next to the page template name in the row where **Alarm Page** is located. In the displayed **Alarm Page** dialog box, specify **Page Template**.

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

Figure 8-32 Default alarm page



Alarm Page [X]

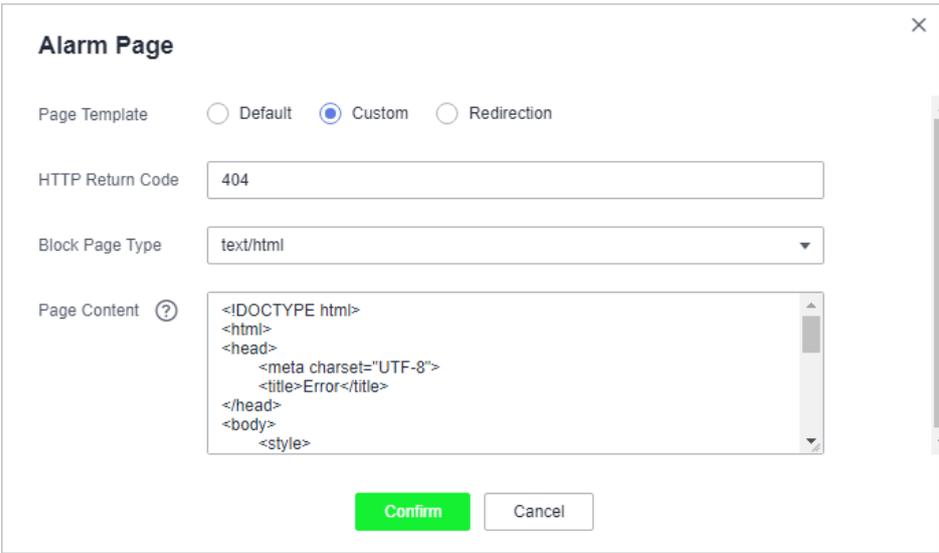
Page Template Default Custom Redirection

HTTP Return Code 418

Confirm Cancel

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

Figure 8-33 Custom alarm page



Alarm Page [X]

Page Template Default Custom Redirection

HTTP Return Code

Block Page Type

Page Content ?

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="UTF-8">
  <title>Error</title>
</head>
<body>
  <style>
```

Confirm Cancel

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

Figure 8-34 Redirection alarm page



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

Step 7 Click **Confirm**.

----End

8.4 Basic Information

8.4.1 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

A website has been connected to WAF.

Procedure

Step 1 Log in to the management console.

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

- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Website Settings**.
- Step 5** View the protected website lists. For details about parameters, see [Table 8-15](#).

Figure 8-35 Website list



Table 8-15 Parameters

Parameter	Parameter
Domain Name	Protected domain name or IP address.
Protection	WAF instance protection configured for your website. The options are Cloud and Dedicated .
Server IP/Port	Public IP address of the website server accessed by the client and the service port used by WAF to forward client requests to the server.
Certificate	Certificate associated with the domain name. You can click the certificate name to go to the Certificates page.
Last 3 Days	Protection status of the domain name over the past three days.
Mode	<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"> ● Enabled: WAF is enabled. ● Suspended: WAF is disabled. If a large number of normal requests are blocked, for example, status code 418 is frequently returned, then you can switch the mode to Suspended. In this mode, your website is not protected because WAF only forwards requests. It does not scan for attacks. This mode is risky. You are advised to use the global protection whitelist rules to reduce false alarms. ● Bypassed: In this mode, requests are directly sent to the backend servers without passing through WAF. <p>NOTE The working mode can be switched to Bypassed only if the website is protected in Cloud mode and the following conditions are met:</p> <ul style="list-style-type: none"> - Website services need to be restored to the status when the domain is not connected to WAF. - You need to investigate website errors, such as 502, 504, or other incompatibility issues. - No proxy is configured between the client and WAF. <p>For details, see Switching WAF Working Mode.</p>

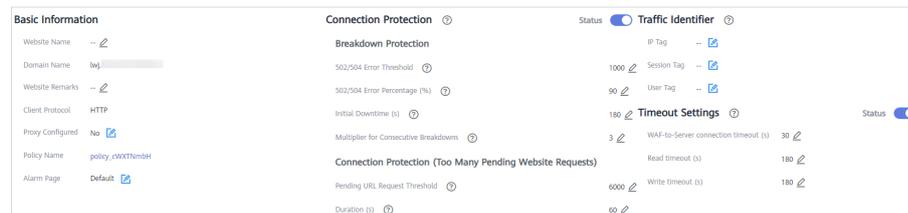
Parameter	Parameter
Policy	Number of types of WAF protection enabled for the domain name. You can click the number to go to the rule configuration page and configure specific protection rules. For details, see Policies .
Access Progress	The progress of connecting your website to WAF or the website access status. <ul style="list-style-type: none"> ● Inaccessible: The website has not been connected to WAF yet or failed to connect to WAF. ● Accessible: The website has been connected to WAF.
Created	Time the website was added to WAF.

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

Step 7 View the basic information about the domain name of the protected website.

To modify a parameter, locate the row that contains the target parameter and click the edit icon.

Figure 8-36 Basic Information



----End

8.4.2 Switching WAF Working Mode

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

Prerequisites

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

Constraints

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

Application Scenarios

- **Enabled:** In this mode, WAF defends your website against attacks based on configured policies.

- **Suspended:** If a large number of normal requests are blocked, for example, status code 418 is frequently returned, then you can switch the mode to **Suspended**. In this mode, your website is not protected because WAF only forwards requests. It does not scan for or log attacks. This mode is risky. You are advised to use the global protection whitelist (formerly false alarm masking) rules to reduce false alarms.
- **Bypassed:** Requests are directly sent to backend origin servers without passing through WAF. Before enabling this mode, enable the service port of origin servers to let requests go to origin servers. Switch the mode to **Bypassed** only if one of the following conditions is met:
 - Website services need to be restored to the status when the website is not connected to WAF.
 - You need to investigate website errors, such as 502, 504, or other incompatibility issues.
 - No proxy is configured between the client and WAF.

Impact on the System

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

----End

8.4.3 Updating a Certificate

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

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

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**.

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

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

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

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

NOTE

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

Only .pem certificates can be used in WAF. If the certificate is not in .pem format, convert it into .pem locally by referring to [Table 8-16](#) before uploading it.

Table 8-16 Certificate conversion commands

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

 **NOTE**

- Before running an OpenSSL command, ensure that the **OpenSSL** tool has been installed on the local host.
- If your local PC runs a Windows operating system, go to the command line interface (CLI) and then run the certificate conversion command.
- If you select **Select existing certificate** for **Update Method**, select an existing certificate from the **Certificate** drop-down list.

Step 7 Click **Confirm**.

----End

8.4.4 Editing Server Information

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

Applicable scenarios:

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

- Add server configurations.
- Update a certificate by referring to [Updating 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**.

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

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

Step 6 In the **Server Information** area, click . [Figure 8-37](#) shows an example.

Figure 8-37 Server Information



Client Protocol	Server Protocol	Server Address	Server Port
HTTP/HTTPS	HTTP	122	80

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

8.4.5 Viewing Protection Information About a Protected Website on Cloud Eye

You can go to Cloud Eye to view protection details about your websites protected with WAF.

Prerequisites

The website to be protected has been added to WAF.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Website Settings**.

Figure 8-38 Website list

Domain Name	Deployment M...	Server IP/Port	Certificate	Last 3 Days	Mode	Policy	Access Progress/Status	Created	Operation
1111.com	Cloud mode	30	--	▲ Attacks blocked: 9	Enabled	policy_LtZ3gBa9	Accessible	Nov 11, 2022 19:1...	Cloud Eye Delete

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

----End

8.4.6 Deleting a Protected Website from WAF

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

In cloud CNAME mode, before removing a website from WAF, you need to resolve your domain name to the IP address of the origin server, or the traffic to your domain name cannot be routed to the origin server.

Prerequisites

A website domain name has been added to WAF.

Impact on the System

- In cloud mode, before removing a website from WAF, you need to resolve the domain name to the origin server IP address on the DNS platform, or the traffic to your domain name cannot be routed to the origin server.
- If you select **Forcible delete the WAF CNAME record.**, WAF will not check your domain name resolution and delete WAF CNAME record immediately. Before enabling this option, make sure you have resolved the domain name to the origin server, or your website will become inaccessible.
- 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**.

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

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

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

- Cloud mode
 - No proxy used

 **NOTE**

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

- Proxy used

 **NOTE**

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

- Dedicated

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

Step 7 Click **OK**. If **Domain name deleted successfully** is displayed in the upper right corner, the domain name of the website was deleted.

----End

Related Operations

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

8.5 Ports Supported by WAF

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

[Table 8-17](#) lists the ports that can be protected by WAF.

Table 8-17 Ports supported by WAF

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

Deploy ment Mode	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
	Non-standard ports (182 in total)	9945, 9770, 81, 82, 83, 84, 88, 89, 800, 808, 1000, 1090, 3128, 3333, 3501, 3601, 4444, 5000, 5222, 5555, 5601, 6001, 6666, 6788, 6789, 6842, 6868, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9802, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702, 8011, 8012, 8013, 8014,	8750, 8445, 18010, 4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, 8805, 9999	Unlimited

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

9 Object Management

9.1 Certificate Management

9.1.1 Uploading a Certificate

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

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

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.

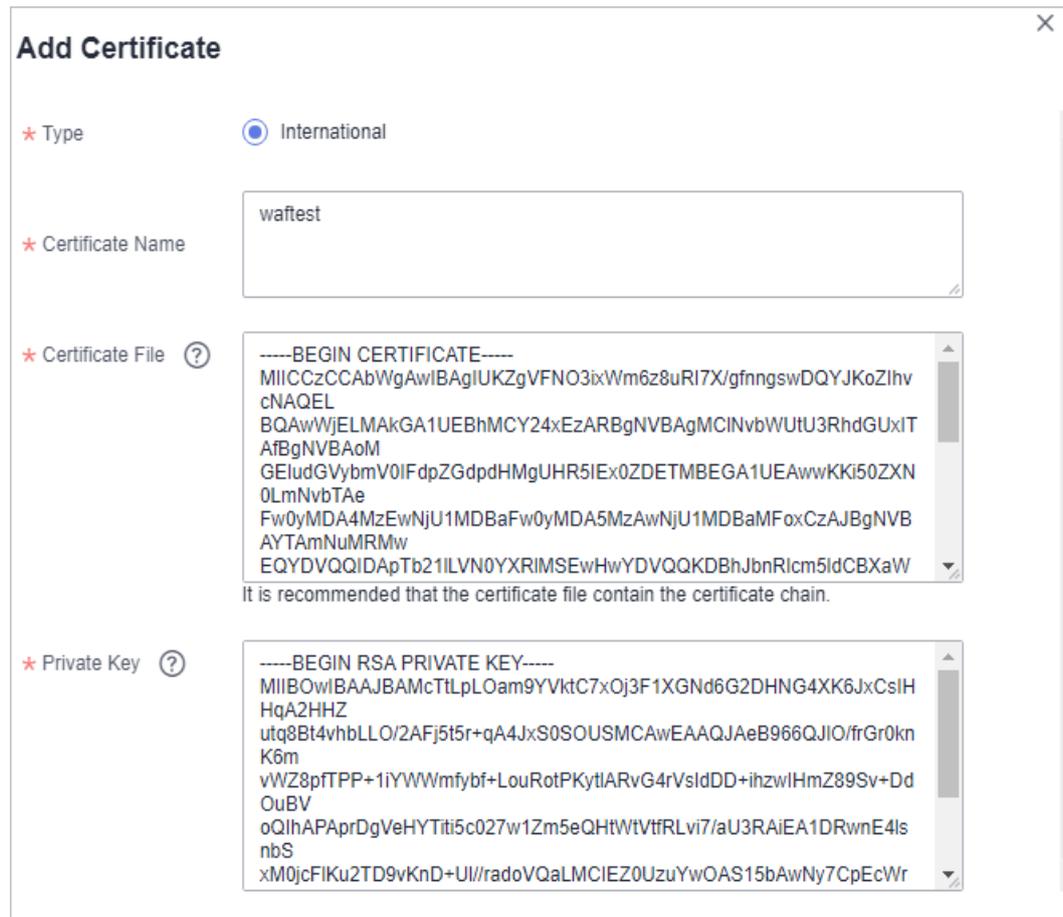
Procedure

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 **Add Certificate**.
- Step 6** In the displayed dialog box, enter a certificate name, and copy and paste the certificate file and private key to the corresponding text boxes.

Figure 9-1 Upload Certificate



Only .pem certificates can be used in WAF. If the certificate is not in .pem format, convert it into .pem locally by referring to [Table 9-1](#) before uploading it.

Table 9-1 Certificate conversion commands

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

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

 **NOTE**

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

Step 7 Click **Confirm**.

----End

Verification

The certificate you created is displayed in the certificate list.

Related Operations

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

NOTICE

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

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

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

9.1.2 Using a Certificate for a Protected Website in WAF

If you configure **Client Protocol** to **HTTPS** for your website, the website needs an SSL certificate. This topic describes how to bind an SSL certificate that you have uploaded to WAF to a website.

Prerequisites

- Your certificate is still valid.
- Your website uses HTTPS as the client protocol.

Constraints

- An SSL certificate can be used for multiple protected websites.
- A protected website can use only one SSL certificate.

Application Scenario

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

Procedure

Step 1 Log in to the management console.

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

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

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

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

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

Step 7 Click **Confirm**.

----End

Verification

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

Related Operations

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

NOTICE

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

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

9.1.3 Viewing Certificate Information

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

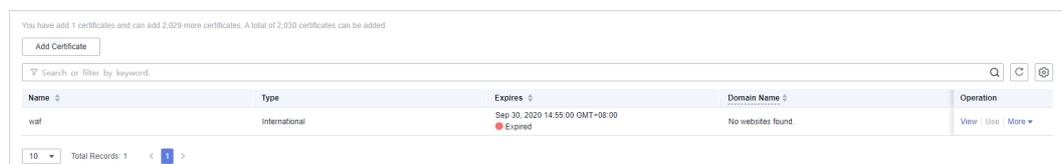
Prerequisites

You have created a certificate to WAF.

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane, choose **Objects > Certificates**.
- Step 5** View the certificate information. [Table 9-2](#) describes the parameters.

Figure 9-2 Certificate list



Name	Type	Expires	Domain Name	Operation
waf	International	Sep 30, 2020 14:55:00 GMT+08:00 Expired	No websites found	View Use More

Table 9-2 Certificate parameters

Parameter	Description
Name	Certificate name.
Type	Only International certificates are supported.
Expires	Certificate expiration time. It is recommended that you update the certificate before it expires. Otherwise, all WAF protection rules will be unable to take effect, and there can be massive impacts on the origin server, even more severe than a crashed host or website access failures. For more details, see Updating a Certificate .
Domain Name	The domain names protected by the certificate. Each domain name must be bound to a certificate. One certificate can be used for multiple domain names.

----End

Related Operations

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

NOTICE

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

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

9.1.4 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**.

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

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

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

----End

Related Operations

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

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

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

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

----End

9.2 Managing IP Address Blacklist and Whitelist Groups

9.2.1 Adding an IP Address Group

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

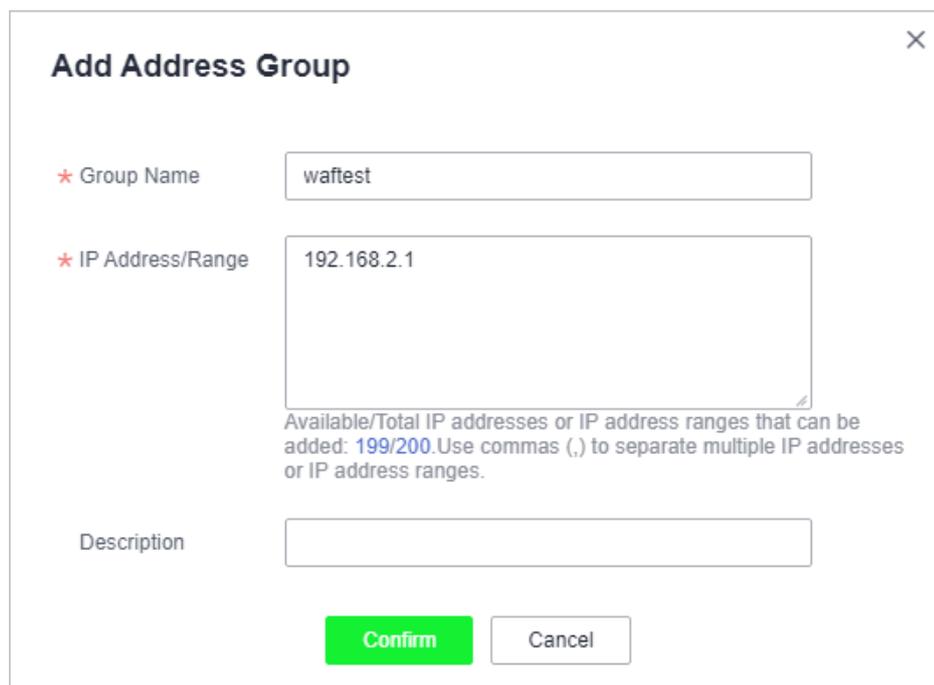
Prerequisites

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 **Objects > Address Groups**.
- Step 5** On the upper left of the address group list, click **Add Address Group**.
- Step 6** In the displayed **Add Address Group** dialog box, enter an address group name and provide IP addresses/IP address ranges.

Figure 9-3 Add Address Group



Add Address Group ✕

* Group Name

* IP Address/Range

Available/Total IP addresses or IP address ranges that can be added: 199/200. Use commas (,) to separate multiple IP addresses or IP address ranges.

Description

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

----End

9.2.2 Modifying or Deleting a Blacklist or Whitelist IP Address Group

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

Prerequisites

You have created an IP address group.

Constraints

Only address groups not used by any rules can be deleted. Before you delete an address group that is being used by a blacklist or whitelist rule, remove the address group from the rule first.

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 9-3 Parameter description

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

- Step 6** Modify or delete an IP address group.
 - Modify an address group.
In the row containing the address group you want to modify, click **Modify** in the **Operation** column. In the **Modify Address Group** dialog box, change the group name or IP address/IP address range, and click **Confirm**.
 - Delete an address group.
In the row containing the address group you want to delete, click **Delete** in the **Operation** column. In the displayed dialog box, click **OK**.

----End

10 System Management

10.1 Managing Dedicated WAF Engines

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

Prerequisites

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

Viewing Information About a Dedicated WAF Instance

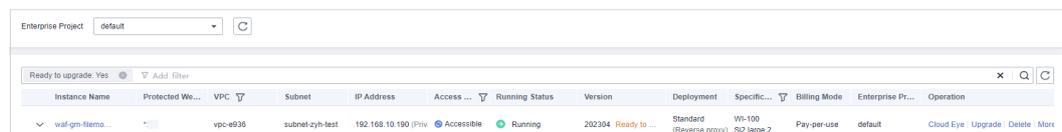
Step 1 Log in to the management console.

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**.

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

Figure 10-1 Dedicated engine list



Instance Name	Protected We...	VPC	Subnet	IP Address	Access ...	Running Status	Version	Deployment	Specific...	Billing Mode	Enterprise Pr...	Operation	
waf-gm-items...		vpc-e036	subnet-zyh-test	192.168.10.190 (Priv)	Accessible	Running	202304	Ready to ...	Standard (Reverse proxy)	W1-100 (Reverse proxy)	Pay-per-use	default	Cloud Eye Upgrade Delete More

Step 5 View information about a dedicated WAF instance. [Table 10-1](#) describes parameters.

Table 10-1 Key parameters of dedicated WAF instances

Parameter	Description	Example Value
Instance Name	Name automatically generated when an instance is created.	None
Protected Website	Domain name of the website protected by the instance.	www.example.com
VPC	VPC where the instance resides	vpc-waf
Subnet	Subnet where an instance resides	subnet-62bb
IP Address	IP address of the subnet in the VPC where the WAF instance is deployed.	192.168.0.186
Access Status	Connection status of the instance.	Accessible
Running Status	Status of the instance.	Running
Version	Dedicated WAF	202304
Deployment	How the instance is deployed.	Standard mode (reverse proxy)
Specifications	Specifications of resources hosting the instance.	8 vCPUs 16 GB

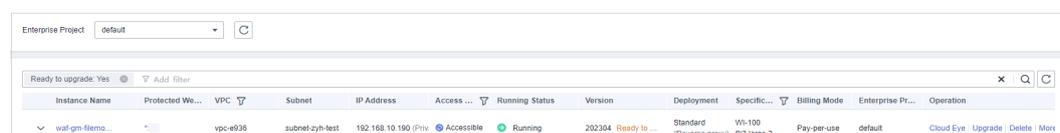
----End

Viewing Metrics of a Dedicated WAF Instance

When a WAF instance is in the **Running** status, you can view the monitored metrics about the instance.

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Instance Management > Dedicated Engine** to go to the dedicated WAF instance page.

Figure 10-2 Dedicated engine list



Instance Name	Protected We...	VPC	Subnet	IP Address	Access ...	Running Status	Version	Deployment	Specific...	Billing Mode	Enterprise Pr...	Operation	
waf-gn-filem...		vpc-e936	subnet-zyh-test	192.168.10.190 (Priv)	Accessible	Running	202304	Ready to ...	Standard (Reverse proxy)	W1-100	Pay-per-use	default	Cloud Eye Upgrade Delete More

Step 5 In the row of the instance, click **Cloud Eye** in the **Operation** column to go to the Cloud Eye console and view the monitoring information, such as CPU, memory, and bandwidth.

----End

Upgrading a Dedicated WAF Instance

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

NOTICE

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

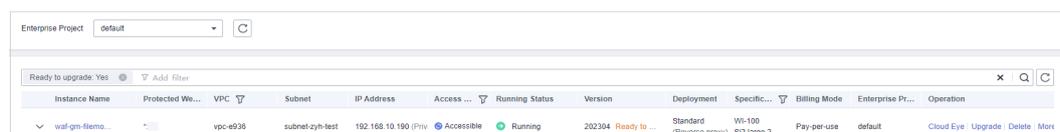
Step 1 Log in to the management console.

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

Step 3 Click  in the upper left corner 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.

Figure 10-3 Dedicated engine list



Instance Name	Protected We...	VPC	Subnet	IP Address	Access ...	Running Status	Version	Deployment	Specific...	Billing Mode	Enterprise Pr...	Operation	
waf-gm-Itemo...		vpc-e936	subnet-zyh-test	192.168.10.190 (Priv)	Accessible	Running	202304	Ready to ...	Standard (Reverse proxy)	W1-100 S2.large.2	Pay-per-use	default	Cloud Eye Upgrade Delete More

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

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

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

----End

Change Security Group for a Dedicated WAF Instance

If you select **Network Interface** for **Instance Type**, you can change the security group to which your dedicated instance belongs. After you select a security group, the WAF instance will be protected by the access rules of the security group.

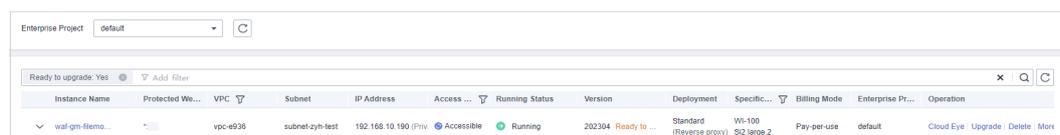
Step 1 Log in to the management console.

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

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

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

Figure 10-4 Dedicated engine list



Instance Name	Protected We...	VPC	Subnet	IP Address	Access ...	Running Status	Version	Deployment	Specific...	Billing Mode	Enterprise Pr...	Operation	
waf-gm-8tma...		vpc-e936	subnet-zyh-test	192.168.10.190 (Priv)	Accessible	Running	202304	Ready to ...	Standard (Reverse proxy)	W1-100 (Size large 2)	Pay-per-use	default	Cloud Eye Upgrade Delete More

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

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

----End

Deleting a Dedicated WAF Instance

You can delete a dedicated WAF instance 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.

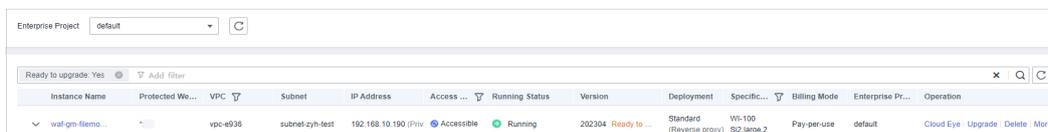
Step 1 Log in to the management console.

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**.

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

Figure 10-5 Dedicated engine list



Instance Name	Protected We...	VPC	Subnet	IP Address	Access ...	Running Status	Version	Deployment	Specific...	Billing Mode	Enterprise Pr...	Operation	
waf-gm-Itemo...		vpc-e936	subnet-zyh-test	192.168.10.190 (Priv)	Accessible	Running	202304	Ready to ...	Standard (Reverse proxy)	¥10-100 \$2 large.2	Pay-per-use	default	Cloud Eye Upgrade Delete More

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

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

----End

10.2 Viewing Product Details

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

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 disable a cloud WAF instance billed on a pay-per-use basis, click **Disable Pay-Per-Use Billing** for it and finish operations as prompted.

----End

10.3 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.

Prerequisites

SMN has been enabled.

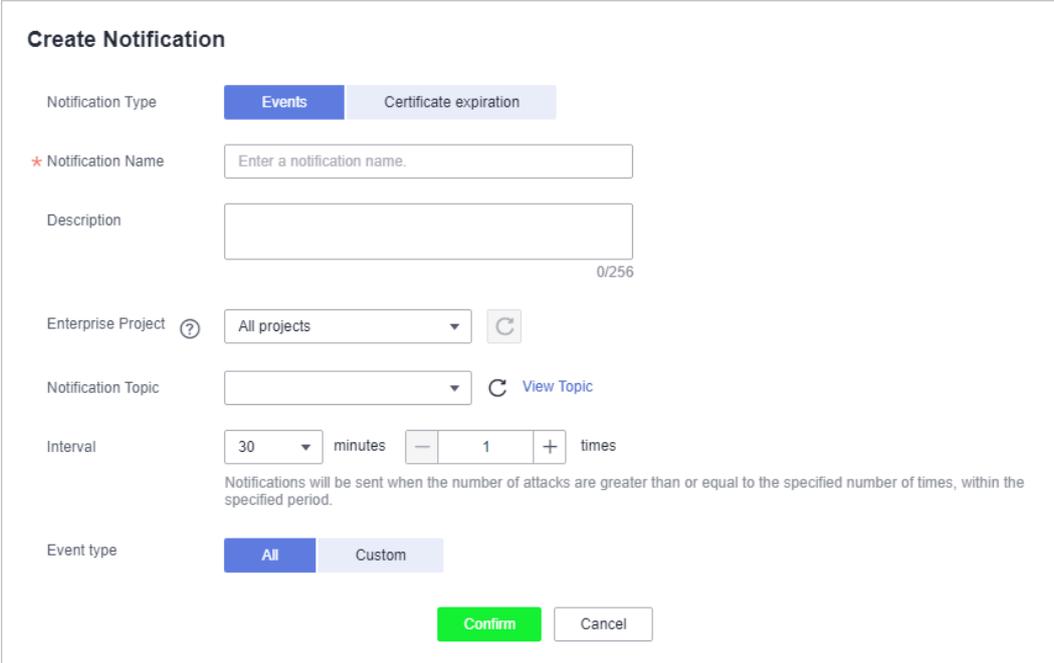
Constraints

- Alarm notifications are sent if the number of attacks reaches or exceeds the threshold configured for a certain period.

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 10-2](#) lists the parameters.

Figure 10-6 Create Notification



Create Notification

Notification Type: **Events** | Certificate expiration

* Notification Name:

Description:
0/256

Enterprise Project: 

Notification Topic:  [View Topic](#)

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

Event type: **All** | Custom

Confirm | Cancel

Table 10-2 Description of notification setting parameters

Parameter	Description
Notification Type	<p>Select a notification type.</p> <ul style="list-style-type: none"> • Events: WAF sends attack logs to you in the way you configure (such as SMS or email) once it detects log-only or blocked events. • Certificate expiration: When a certificate is about to expire, WAF notifies you by the way you configure, such as email or SMS.
Notification Name	Name of the alarm notification.
Description	(Optional) A description of the purposes of the alarm.
Enterprise Project	Select an enterprise project from the drop-down list. The notification takes effect in the selected enterprise project.
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 Events for Notification Type, Interval must be configured.</p> <p>NOTE 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 Events for Notification Type, Event Type must be configured.</p> <p>By default, All is selected. To specify event types, click Custom.</p>
Notification Before Expiration	<p>This parameter must be configured if you select Certificate expiration for Notification Type.</p> <p>Select how long before a certificate expire WAF can send notifications. You can select 1 week, 1 month, or 2 months.</p> <p>For example, if you select 1 week, 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 Certificate expiration for Notification Type.</p> <p>How often WAF sends certificate expiration notifications to you. You can select Weekly or Daily.</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

11 Permissions Management

11.1 IAM Permissions Management

11.1.1 Creating a User Group and Granting Permissions

With [IAM](#), you can:

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

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

This topic describes the procedure for granting permissions (see [Figure 11-1](#)).

Prerequisites

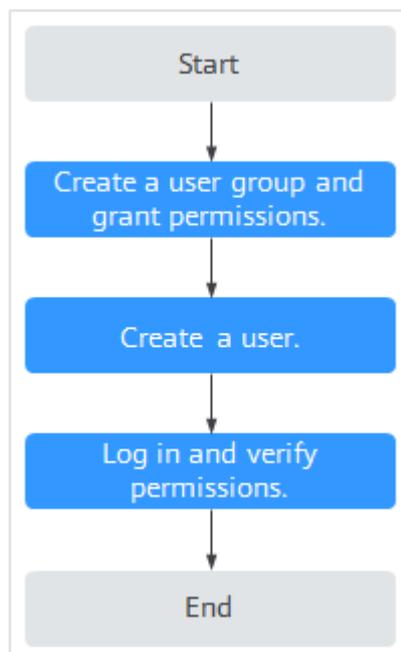
Learn about the permissions supported by WAF in [Table 11-1](#) and choose policies or roles based on your requirements. For the system policies of other services, see [System Permissions](#).

Table 11-1 System policies supported by WAF

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

Process Flow

Figure 11-1 Process for granting permissions



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

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

2. [Create a user and add the user to the user group.](#)

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

3. [Log in to the management console as the created user](#) and verify the permissions.

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

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

11.1.2 WAF Custom Policies

Custom policies can be created to supplement the system-defined policies of WAF. For details about the actions supported by custom policies, see [WAF Permissions and Supported Actions](#).

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see [Creating a Custom Policy](#). The following section contains examples of common WAF custom policies.

Example Custom Policies

- Example 1: Allowing users to query the protected domain list

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "waf:instance:list"
      ]
    }
  ]
}
```

- Example 2: Denying the user request of deleting web tamper protection rules
A deny policy must be used together with other policies. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

The following method can be used if you need to assign permissions of the **WAF FullAccess** policy to a user but also forbid the user from deleting web tamper protection rules (**waf:antiTamperRule:delete**). Create a custom policy with the action to delete web tamper protection rules, set its **Effect** to **Deny**, and assign both this policy and the **WAF FullAccess** policy to the group the user belongs to. Then the user can perform all operations on WAF except deleting web tamper protection rules. The following is a policy for denying web tamper protection rule deletion.

```
{
  "Version": "1.1",
```

```
"Statement": [
  {
    "Effect": "Deny",
    "Action": [
      "waf:antiTamperRule:delete"
    ]
  },
]
```

- **Multi-action policy**

A custom policy can contain the actions of multiple services that are of the project-level type. The following is an example policy containing actions of multiple services:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "waf:instance:get",
        "waf:certificate:get"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "hss:hosts:switchVersion",
        "hss:hosts:manualDetect",
        "hss:manualDetectStatus:get"
      ]
    }
  ]
}
```

11.1.3 WAF Permissions and Supported Actions

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

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

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

Supported Actions

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

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

Permission	Action
Querying an information leakage prevention rule	waf:antiLeakageRule:get
Querying a web tamper protection rule	waf:antiTamperRule:get
Querying a CC attack protection rule	waf:ccRule:get
Querying a precise protection rule	waf:preciseProtectionRule:get
Querying a 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:sourcelp:get
Updating an information leakage prevention rule	waf:antiLeakageRule:put
Updating a web tamper protection rule	waf:antiTamperRule:put
Updating a CC attack protection rule	waf:ccRuleRule:put
Updating a precise protection rule	waf:preciseProtectionRule:put

Permission	Action
Updating a global protection whitelist rule	waf:falseAlarmMaskRule:put
Updating a data masking rule	waf:privacyRule:put
Updating an IP address blacklist or whitelist rule	waf:whiteBlackIpRule:put
Updating a geolocation access control rule	waf: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 global protection whitelist rule	waf:falseAlarmMaskRule:delete
Deleting a data masking rule	waf:privacyRule:delete
Deleting a blacklist or whitelist rule	waf:whiteBlackIpRule:delete
Deleting a geolocation access control rule	waf: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
Creating a global protection whitelist rule	waf:falseAlarmMaskRule:create

Permission	Action
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 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

12 Monitoring and Auditing

12.1 Monitoring

12.1.1 WAF Monitored Metrics

Function Description

This topic describes metrics reported by WAF to Cloud Eye as well as their namespaces and dimensions. You can use APIs provided by Cloud Eye to query the metrics of the monitored object and alarms generated for WAF. You can also query them on the Cloud Eye console.

namespaces

SYS.WAF

NOTE

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

Monitored Metrics for Protected Domain Names

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

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
requests	Number of Requests	Number of requests returned by WAF in the last 5 minutes Unit: Count Collection method: The total number of requests for the domain name are collected.	≥ 0 Value type: Float	Protected domain name	5 minutes
waf_http_2xx	WAF Status Code (2XX)	Number of 2XX status codes returned by WAF in the last 5 minutes Unit: Count Collection method: Number of 2XX status codes returned	≥ 0 Value type: Float	Protected domain name	5
waf_http_3xx	WAF Status Code (3XX)	Number of 3XX status codes returned by WAF in the last 5 minutes Unit: Count Collection method: Number of 3XX status codes returned	≥ 0 Value type: Float	Protected domain name	5

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

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

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
waf_process_time_0	WAF Latency [0-10) ms	<p>This metric is used to collect how many requests are processed by WAF at latencies from 0 ms (included) to 10 ms (excluded) in the last 5 minutes.</p> <p>Unit: Count Collection method: The number of requests processed by WAF at latencies from 0 ms (included) to 10 ms (excluded) in the last 5 minutes are collected.</p>	<p>≥ 0 Value type: Float</p>	Protected domain name	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
waf_process_time_10	WAF Latency [10-20) ms	<p>This metric is used to collect how many requests are processed by WAF at latencies in the 10 ms to less than 20 ms range in the last 5 minutes.</p> <p>Unit: Count</p> <p>Collection method: The number of requests processed by WAF at latencies in the 10 ms to less than 20 ms range in the last 5 minutes are collected.</p>	<p>≥ 0</p> <p>Value type: Float</p>	Protected domain name	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
waf_process_time_20	WAF Latency [20-50) ms	<p>This metric is used to collect how many requests are processed by WAF at latencies from 20 ms (included) to 50 ms (excluded) in the last 5 minutes.</p> <p>Unit: Count Collection method: The number of requests processed by WAF at latencies from 20 ms (included) to 50 ms (excluded) in the last 5 minutes are collected.</p>	<p>≥ 0 Value type: Float</p>	Protected domain name	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
waf_process_time_50	WAF Latency [50-100) ms	<p>This metric is used to collect how many requests are processed by WAF at latencies from 50 ms (included) to 100 ms (excluded) in the last 5 minutes.</p> <p>Unit: Count Collection method: The number of requests processed by WAF at latencies from 50 ms (included) to 100 ms (excluded) in the last 5 minutes are collected.</p>	<p>≥ 0 Value type: Float</p>	Protected domain name	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
waf_process_time_100	WAF Latency [100, 1,000) ms	This metric is used to collect how many requests are processed by WAF at latencies in the 100 ms to less than 1,000 ms range in the last 5 minutes. Unit: Count Collection method: The number of requests processed by WAF at latencies in the 100 ms to less than 1000 ms range in the last 5 minutes are collected.	≥ 0 Value type: Float	Protected domain name	5 minutes
waf_process_time_1000	WAF Latency [1,000, above) ms	This metric is used to collect how many requests are processed by WAF at latencies above 1000 ms in the last 5 minutes. Unit: Count Collection method: The number of requests processed by WAF at latencies above 1000 ms in the last 5 minutes are collected.	≥ 0 Value type: Float	Protected domain name	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
qps_peak	Peak QPS	<p>This metric is used to collect the peak QPS of the domain name in the last 5 minutes.</p> <p>Unit: Count</p> <p>Collection method: The peak QPS of the domain name in the last 5 minutes is collected.</p>	<p>≥ 0</p> <p>Value type: Float</p>	Protected domain name	5 minutes
qps_mean	Average QPS	<p>This metric is used to collect the average QPS of the domain name in the last 5 minutes.</p> <p>Unit: Count</p> <p>Collection method: The average QPS of the domain name in the last 5 minutes is collected.</p>	<p>≥ 0</p> <p>Value type: Float</p>	Protected domain name	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
waf_http_0	No WAF Status Code	<p>This metric is used to collect how many requests with no status code returned by WAF in the last 5 minutes.</p> <p>Unit: Count</p> <p>Collection method: The number of requests with no WAF status code returned in the last 5 minutes is collected.</p>	<p>≥ 0</p> <p>Value type: Float</p>	Protected domain name	5 minutes
upstream_code_2xx	Status Code Returned to the Client (2XX)	<p>This metric is used to collect how many requests with 2XX status code are returned by the origin server in the last 5 minutes.</p> <p>Unit: Count</p> <p>Collection method: The number of requests with 2XX status code returned by the origin server in the last 5 minutes is collected.</p>	<p>≥ 0</p> <p>Value type: Float</p>	Protected domain name	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
upstream_code_3xx	Status Code Returned by the Origin Server (3XX)	<p>This metric is used to collect how many requests with 3XX status code are returned by the origin server in the last 5 minutes.</p> <p>Unit: Count</p> <p>Collection method: The number of requests with 3XX status code returned by the origin server in the last 5 minutes is collected.</p>	<p>≥ 0</p> <p>Value type: Float</p>	Protected domain name	5 minutes
upstream_code_4xx	Status Code Returned by the Origin Server (4XX)	<p>This metric is used to collect how many requests with 4XX status code are returned by the origin server in the last 5 minutes.</p> <p>Unit: Count</p> <p>Collection method: The number of requests with 4XX status code returned by the origin server in the last 5 minutes is collected.</p>	<p>≥ 0</p> <p>Value type: Float</p>	Protected domain name	5 minutes

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
upstream_code_5xx	Status Code Returned by the Origin Server (5XX)	This metric is used to collect how many requests with 5XX status code are returned by the origin server in the last 5 minutes. Unit: Count Collection method: The number of requests with 5XX status code returned by the origin server in the last 5 minutes is collected.	≥ 0 Value type: Float	Protected domain name	5 minutes
upstream_code_0	No Origin Server Status Code	This metric is used to collect how many requests with no status code returned by the origin server in the last 5 minutes. Unit: Count Collection method: The number of requests with no status code returned by the origin server in the last 5 minutes is collected.	≥ 0 Value type: Float	Protected domain name	5 minutes

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

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

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

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

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

Metrics for Dedicated WAF Instances

Table 12-2 Metrics for dedicated waf instances

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

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

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

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

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

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

Dimensions

Key	Value
instance_id	ID of the dedicated WAF instance
waf_instance_id	ID of the website protected with WAF

Example of Raw Data Format of Monitored Metrics

```
[
  {
    "metric": {
      // Namespace
      "namespace": "SYS.WAF",
      "dimensions": [
        {
          // Dimension name, for example, protected website
          "name": "waf_instance_id",
          // ID of the monitored object in this dimension, for example, ID of the protected website
          "value": "082db2f542e0438aa520035b3e99cd99"
        }
      ],
      //Metric ID
      "metric_name": "waf_http_2xx"
    },
    // Time to live, which is predefined for the metric
    "ttl": 172800,
    // Metric value
    "value": 0.0,
    // Metric unit
    "unit": "Count",
    // Metric value type
    "type": "float",
    // Collection time for the metric
    "collect_time": 1637677359778
  }
]
```

12.1.2 Configuring Alarm Monitoring Rules

You can set WAF alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, metric, threshold, monitoring scope, and whether to send notifications. This helps you learn the WAF protection status in a timely manner.

Prerequisites

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

Procedure

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner of the page and choose **Management & Deployment > Cloud Eye**.
- Step 4** In the navigation pane on the left, choose **Alarm Management > Alarm Rules**.
- Step 5** In the upper right corner of the page, click **Create Alarm Rule**.
- Step 6** Set the alarm rule name.

Step 7 Select **Web Application Firewall** from the **Resource Type** drop-down list, and select a dimension, monitoring scope, alarm template, and whether to send a notification.

Step 8 Click **Create**. In the displayed dialog box, click **OK**.

----End

12.1.3 Viewing Monitored Metrics

You can view WAF metrics on the management console to learn about the WAF protection status in a timely manner and set protection policies based on the metrics.

Prerequisites

WAF alarm rules have been configured in Cloud Eye. For more details, see [Configuring Alarm Monitoring Rules](#).

Procedure

Step 1 Log in to the management console.

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

Step 3 Click  in the upper left corner of the page and choose **Management & Deployment > Cloud Eye**.

Step 4 In the navigation pane on the left, choose **Cloud Service Monitoring > Web Application Firewall**.

Step 5 In the row containing the dedicated instance or protected domain name, click **View Metric** in the **Operation** column.

NOTE

To view the monitoring information about a specific website, you can go to the **Website Settings** page, locate the row containing the target domain name and click **Cloud Eye** in the **Operation** column.

----End

12.2 Auditing

12.2.1 WAF Operations Recorded by CTS

CTS provides records of operations on WAF. With CTS, you can query, audit, and backtrack these operations. For details, see the *Cloud Trace Service User Guide*.

Table 12-3 WAF Operations Recorded by CTS

Operation	Resource Type	Trace Name
Creating a WAF instance	instance	createInstance
Deleting a WAF instance	instance	deleteInstance
Modifying a WAF instance	instance	alterInstanceName
Modifying the protection status of a WAF instance	instance	modifyProtectStatus
Modifying the connection status of a WAF instance	instance	modifyAccessStatus
Creating a WAF policy	policy	createPolicy
Applying a WAF policy	policy	applyToHost
Modifying a policy	policy	modifyPolicy
Deleting a WAF policy	policy	deletePolicy
Uploading a certificate	certificate	createCertificate
Changing the name of a certificate	certificate	modifyCertificate
Deleting a certificate	certificate	deleteCertificate
Adding a CC attack protection rule	policy	createCc
Modifying a CC attack protection rule	policy	modifyCc
Deleting a CC attack protection rule	policy	deleteCc
Adding a precise protection rule	policy	createCustom
Modifying a precise protection rule	policy	modifyCustom
Deleting a precise protection rule	policy	deleteCustom
Adding an IP address blacklist or whitelist rule	policy	createWhiteblackip
Modifying an IP address blacklist or whitelist rule	policy	modifyWhiteblackip
Deleting an IP address blacklist or whitelist rule	policy	deleteWhiteblackip
Creating/updating a web tamper protection rule	policy	createAntitamper

Operation	Resource Type	Trace Name
Deleting a web tamper protection rule	policy	deleteAntitamper
Creating a global protection whitelist rule	policy	createIgnore
Deleting a global protection whitelist rule	policy	deleteIgnore
Adding a data masking rule	policy	createPrivacy
Modifying a data masking rule	policy	modifyPrivacy
Deleting a data masking rule	policy	deletePrivacy

12.2.2 Querying Real-Time Traces

Scenarios

After you enable CTS and the management tracker is created, CTS starts recording operations on cloud resources. After a data tracker is created, the system starts recording operations on data in OBS buckets. CTS stores operation records generated in the last seven days.

This section describes how to query and export operation records of the last seven days on the CTS console.

- [Viewing Real-Time Traces in the Trace List of the New Edition](#)
- [Viewing Real-Time Traces in the Trace List of the Old Edition](#)

Viewing Real-Time Traces in the Trace List of the New Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. On the **Trace List** page, use advanced search to query traces. You can combine one or more filters.
 - **Trace Name:** Enter a trace name.
 - **Trace ID:** Enter a trace ID.
 - **Resource Name:** Enter a resource name. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty.
 - **Resource ID:** Enter a resource ID. Leave this field empty if the resource has no resource ID or if resource creation failed.
 - **Trace Source:** Select a cloud service name from the drop-down list.

- **Resource Type:** Select a resource type from the drop-down list.
 - **Operator:** Select one or more operators from the drop-down list.
 - **Trace Status:** Select **normal**, **warning**, or **incident**.
 - **normal:** The operation succeeded.
 - **warning:** The operation failed.
 - **incident:** The operation caused a fault that is more serious than the operation failure, for example, causing other faults.
 - Time range: Select **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.
5. On the **Trace List** page, you can also export and refresh the trace list, and customize the list display settings.
- Enter any keyword in the search box and click  to filter desired traces.
 - Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5000 records.
 - Click  to view the latest information about traces.
 - Click  to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled () , excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.
6. For details about key fields in the trace structure, see section "Trace References" > "Trace Structure" and section "Trace References" > "Example Traces".
7. (Optional) On the **Trace List** page of the new edition, click **Go to Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

Viewing Real-Time Traces in the Trace List of the Old Edition

1. Log in to the management console.
2. Click  in the upper left corner and choose **Management & Deployment** > **Cloud Trace Service**. The CTS console is displayed.
3. Choose **Trace List** in the navigation pane on the left.
4. Each time you log in to the CTS console, the new edition is displayed by default. Click **Go to Old Edition** in the upper right corner to switch to the trace list of the old edition.
5. Set filters to search for your desired traces. The following filters are available:
 - **Trace Type, Trace Source, Resource Type, and Search By:** Select a filter from the drop-down list.
 - If you select **Resource ID** for **Search By**, specify a resource ID.
 - If you select **Trace name** for **Search By**, specify a trace name.
 - If you select **Resource name** for **Search By**, specify a resource name.

- **Operator:** Select a user.
 - **Trace Status:** Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
 - Time range: You can query traces generated during any time range in the last seven days.
 - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
6. Click **Query**.
 7. On the **Trace List** page, you can also export and refresh the trace list.
 - Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5000 records.
 - Click  to view the latest information about traces.
 8. Click  on the left of a trace to expand its details.

Trace Name	Resource Type	Trace Source	Resource ID	Resource Name	Trace Status	Operator	Operation Time	Operation
createDockerConfig	dockerlogincmd	SWR	-	dockerlogincmd	normal		Nov 16, 2023 10:54:04 GMT+08:00	View Trace

```

request
trace_id: [redacted]
code: 200
trace_name: createDockerConfig
resource_type: dockerlogincmd
trace_rating: normal
api_version: ""
message: createDockerConfig, Method: POST Url=/v2/management/secret, Reason:
source_ip: [redacted]
domain_id: [redacted]
trace_type: ApiCall
            
```

9. Click **View Trace** in the **Operation** column. The trace details are displayed.

View Trace ×

```

{
  "request": "",
  "trace_id": "[redacted]",
  "code": "200",
  "trace_name": "createDockerConfig",
  "resource_type": "dockerlogincmd",
  "trace_rating": "normal",
  "api_version": "",
  "message": "createDockerConfig, Method: POST Url=/v2/management/secret, Reason:",
  "source_ip": "[redacted]",
  "domain_id": "[redacted]",
  "trace_type": "ApiCall",
  "service_type": "SWR",
  "event_type": "system",
  "project_id": "[redacted]",
  "response": "",
  "resource_id": "",
  "tracker_name": "system",
  "time": "Nov 16, 2023 10:54:04 GMT+08:00",
  "resource_name": "dockerlogincmd",
  "user": {
    "domain": {
      "name": "[redacted]",
      "id": "[redacted]"
    }
  }
}
            
```

10. For details about key fields in the trace structure, see section "Trace References" > "Trace Structure" and section "Trace References" > "Example Traces".
11. (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

13 FAQs

13.1 About WAF

13.1.1 FAQs for Beginners

If you are a beginner for WAF, here are some useful FAQs.

Is WAF a Hardware Firewall or a Software Firewall?

WAF is a software firewall.

For more details, see [Website Settings](#).

Does WAF Affect My Existing Workloads and Server Running?

Enabling WAF does not interrupt your existing workloads or affect the running status of your origin servers. No additional operation (such as shutdown or restart) on the origin servers is required.

Can a WAF Instance Be Deployed in the VPC?

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

Does a Dedicated WAF Instance Support Cross-VPC Protection?

Dedicated WAF instances cannot protect origin servers in the VPCs that are different from where those WAF instances locate. To protect such origin servers, apply for dedicated WAF instances in the same VPC as that for the origin servers.

Which OSs Does WAF Support?

WAF is deployed on the cloud, which is irrelevant to an OS. Therefore, WAF supports any OS. A domain name server on any OS can be connected to WAF for protection.

Which Layers Does WAF Provide Protection At?

WAF provides protection at seven layers, namely, the physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer.

How Does WAF Block Requests?

WAF checks both the request header and body. For example, WAF detects the request body, such as form, XML, and JSON data, and blocks requests that do not comply with protection rules.

Does WAF Support File Caching?

WAF caches only static web pages that are configured with web tamper protection and sends the cached web pages that are not tampered with to web visitors.

Does WAF Cache Website Data?

WAF protects user data on the application layer. It supports cache configuration on static web pages. When a user accesses a web page, the system returns a cached page to the user and randomly checks whether the page has been tampered with.

Can I Use WAF to Check Health Status of Servers?

No. If you want to check health status of servers, the combination of ELB and WAF is recommended for your workloads. After you configure a load balancer in ELB, you can enable health checks for servers and use the EIP of the load balancer as the server IP address to establish connections between servers and WAF.

Does WAF Support Two-Way SSL Authentication?

No. You can configure a one-way SSL certificate on WAF.

NOTE

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

Does WAF Support Application Layer Protocol- and Content-Based Access Control?

WAF supports access control over content at the application layer. HTTP and HTTPS are both application layer protocols.

Can WAF Check the Body I Add to a POST Request?

The built-in detection of WAF checks POST data, and web shells are the files submitted in POST requests. WAF checks all data, such as forms and JSON files in POST requests based on the default protection policies.

You can configure a precise protection rule to check the body added to POST requests.

Can WAF Limit the Access Speed of a Domain Name?

No. However, you can customize a CC attack protection rule to restrict access to a specific URL on your website based on an IP address, cookie, or Referer, mitigating CC attacks.

Can WAF Block URL Requests That Contain Special Characters?

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

Can WAF Block Spam and Malicious User Registrations?

WAF cannot block business-related attacks, such as spam and malicious user registrations. To prevent these attacks, configure the registration verification mechanism on your website.

WAF is designed to keep web applications stable and secure. It examines all HTTP and HTTPS requests to detect for and block suspicious network attacks, such as Structure Query Language (SQL) injections, cross-site scripting (XSS) attacks, web shell upload, command or code injections, file inclusion, unauthorized sensitive file access, third-party vulnerability exploits, Challenge Collapsar (CC) attacks, malicious crawlers, and cross-site request forgery (CSRF).

Can WAF Block Requests for Calling Other APIs from Web Pages?

If the request data for calling other APIs on the web page is included in the domain names protected by WAF, the request data passes through WAF. WAF checks the request data and blocks it if it is an attack.

If the request data for calling other APIs on the web page is not included in the domain names protected by WAF, the request data does not pass through WAF. WAF cannot block the request data.

Can WAF Limit Access Through Domain Names?

No. WAF supports the blacklist and whitelist rules to block, log only, or permit access requests from specified IP addresses or IP address segments.

You can configure blacklist and whitelist rules to block, log only, or permit access requests from the IP addresses or IP address segments corresponding to the domain names.

Does WAF Have the IPS Module?

Unlike the traditional firewalls, WAF does not have an Intrusion Prevention System (IPS). WAF supports intrusion detection of only HTTP/HTTPS requests.

Can My WAF Instances Be Automatically Scalable?

No.

Is There Any Impact on Origin Servers If I Enable HTTP/2 in WAF?

Yes. HTTP/2 is not supported between WAF and the origin server. This means if you enable HTTP/2 in WAF, WAF can process HTTP/2 requests from clients, but

WAF can only forward the requests to origin server using HTTP 1.0/1.1. In this situation, the origin server request traffic may rise as multiplexing in HTTP/2 may become invalid for origin servers.

Does WAF Affect Email Ports or Email Receiving and Sending?

WAF protects web application pages. After your website is connected to WAF, there is no impact on your email port or email sending or receiving.

What Are Concurrent Requests?

The number of concurrent requests refers to the number of requests that the system can process simultaneously. When it comes to a website, concurrent requests refer to the requests from the visitors at the same time.

Can WAF Block Requests When a Certificate Is Mounted on ELB?

If the certificate is mounted on ELB, all requests sent through WAF are encrypted. For HTTPS services, you must upload the certificate to WAF so that WAF can detect the decrypted request and determine whether to block the request.

Do I Need to Make Some Changes in WAF If the Security Group for Origin Server (Address) Is Changed?

No modifications are required in WAF, but you are required to whitelist WAF IP addresses on the origin servers.

How Is the Load Balanced When Multiple Origin Servers Are Configured in WAF?

If you have configured multiple origin server IP addresses, WAF uses the weighted round robin algorithm to distribute access requests by default. You can also customize a load balancing algorithm as required.

Does gzip on the Origin Server Affect WAF?

If gzip is enabled on the origin server, WAF may incorrectly block normal access requests from the origin server. If the blocked request is a normal access request, you can handle the event as a false alarm by referring to [Handling False Alarms](#). After an event is handled as a false alarm, WAF stops blocking corresponding type of event. No such type of event will be displayed on the **Events** page and you will no longer receive alarm notifications accordingly.

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

No. After a website is connected to cloud WAF in CNAME access mode or to dedicated WAF instances, all website access requests are forwarded to WAF first. WAF detects and filters out malicious attack traffic, and returns normal traffic to the origin server to keep origin servers secure, stable, and available.

Can WAF Protect Multiple Domain Names That Point to the Same Origin Server?

Yes. If there are multiple domain names pointing to the same origin server, you can connect these domain names to WAF for protection.

WAF protects domain names or IP addresses. If multiple domain names use the same EIP to provide services, all these domain names must be connected to WAF.

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

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

What Is a Protection IP Address?

A protection IP address in WAF is the IP address of a website you use WAF to protect.

Does Cloud WAF Use Fixed IP Addresses for Domain Resolution?

After a domain name is added to WAF in cloud mode, WAF randomly assigns a CNAME record to the domain name for domain name resolution. This CNAME record is randomly assigned from the WAF IP address pool and is not fixed.

Will the CNAME Record Be Changed If the IP Address of the Origin Server Has Been Changed?

If you are using a cloud WAF instance, the CNAME record will not be changed when origin server IP addresses have been changed.

Do I Need to Add the Domain Name to WAF Again If the Domain Name IP Address Has Been Changed?

If the IP address of the website does not change, you do not need to reconfigure it in WAF. If the website resolves a new IP address, you need to add it in WAF again.

Do I Need to Bind an EIP to WAF?

No EIPs are required for cloud WAF instances. Dedicated WAF instances need to work with layer-7 dedicated load balancers. These load balancers need to use EIPs as service addresses.

Does WAF Support Vulnerability Detection?

WAF enables customizable anti-crawler rules to detect and block threats such as third-party security tool vulnerability attacks. If you enable the scanner item when configuring anti-crawler rules, WAF detects scanners and crawlers, such as OpenVAS and Nmap.

Does WAF Support Protocols Used in MS Exchange?

WAF supports HTTP and HTTPS for logging in to Exchange on the web, but does not support mail-related protocols such as Simple Mail Transfer Protocol (SMTP),

Post Office Protocol version 3 (POP3), or Internet Message Access Protocol (IMAP) used by MS Exchange.

Can WAF Defend Against XOR Injection Attacks?

Yes. WAF can defend against XOR injection attacks.

What Is the `bind_ip` Parameter in WAF Logs?

After your website is connected to WAF, WAF functions as a reverse proxy between the client and the origin server. WAF examines traffic to your website, filters out malicious traffic, and forwards healthy 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.

Can WAF Protect Websites in the C/S Architecture?

In the C/S architecture, WAF can protect only websites that use the layer-7 HTTP/HTTPS protocol.

Where Can I Query the Service QPS of the Current WAF Service?

You can query the inbound bandwidth or QPS quota usage of the origin server IP address on the origin server.

Can WAF Block Data Packets in multipart/form-data Format?

Yes.

The multipart/form-data indicates that the browser uses a form to upload files. For example, if an attachment is added to an email, the attachment is usually uploaded to the server in multipart/form-data format.

13.1.2 WAF Functions

13.1.2.1 Can WAF Protect an IP Address?

A WAF instance can protect IP addresses.

Cloud Mode

In this mode, only website domain names can be added to WAF for protection.

The origin server IP address configured in WAF can only be a public IP address.

To reduce the number of public IP addresses, you can use an Elastic Load Balance (ELB) load balancer to work as a proxy of backend private IP addresses. Then, you need to set the EIP (public IP address) bound to the load balancer as the origin server IP address.

Dedicated Mode

A dedicated or load balancing WAF instance can protect websites through either domain names or IP addresses.

The origin server IP address configured in WAF can be a public IP address or internal IP address.

For details about how to add a domain name to WAF, see [How Do I Add a Domain Name/IP Address to WAF?](#)

13.1.2.2 What Objects Does WAF Protect?

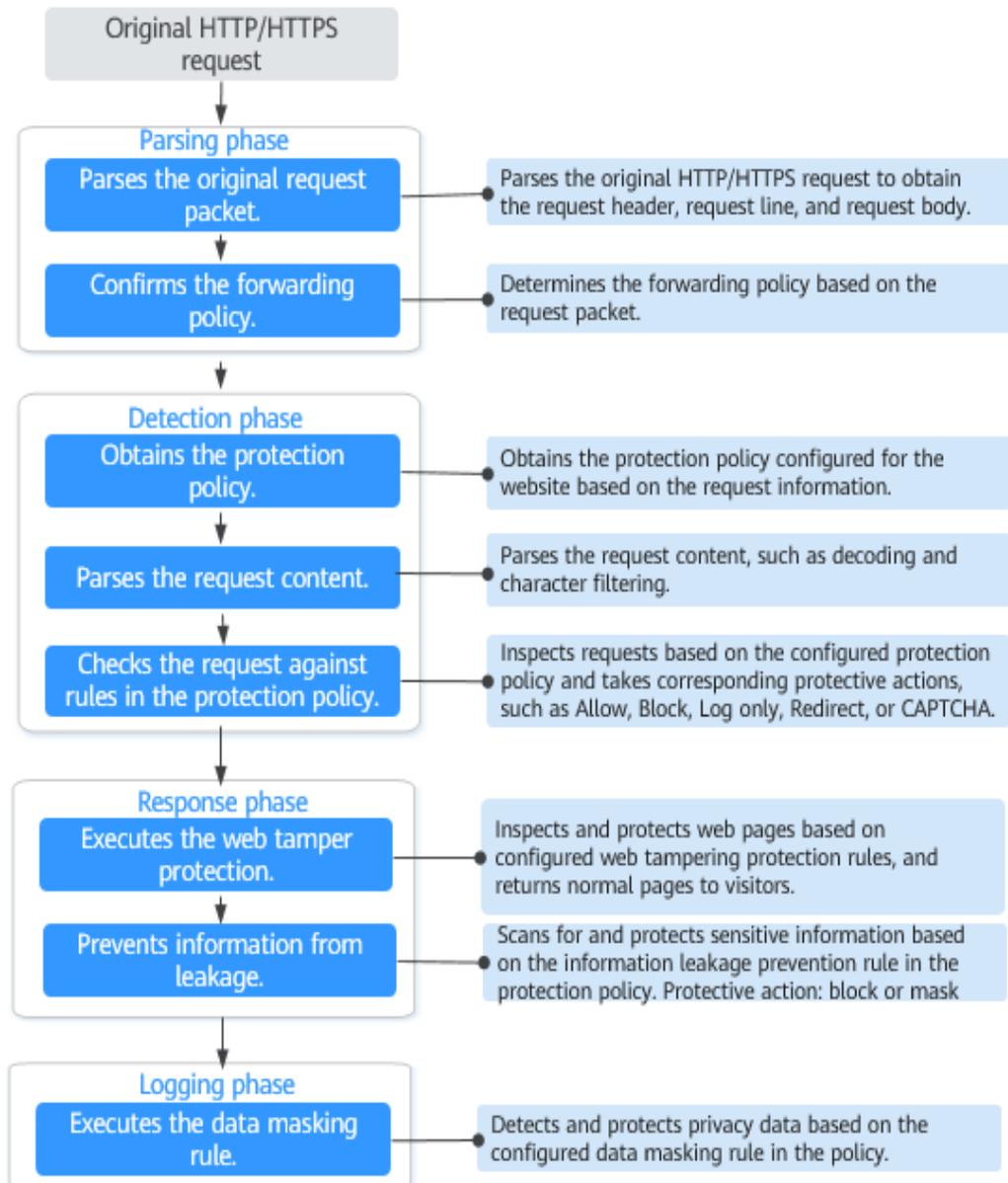
WAF can protect websites through domain names or IP addresses.

- In cloud CNAME access mode, only website domain names can be added to WAF.
Your origin server IP address configured in WAF must be a public IP address. For example, if an Elastic Load Balance (ELB) load balancer is configured for origin servers, a cloud WAF instance can protect origin servers as long as the load balancer has a public IP address bound.
- In dedicated mode, you can add website domain names or IP addresses to WAF.

13.1.2.3 Does WAF Block Customized POST Requests?

No. WAF does not block user-defined POST requests. [Figure 13-1](#) shows the detection process of the WAF built-in protection rules for original HTTP/HTTPS requests.

Figure 13-1 WAF engine work process



13.1.2.4 What Are the Differences Between the Web Tamper Protection Functions of WAF and HSS?

The web tamper protection function of HSS monitors website directories in real time, backs up files, and restores tampered files using the backup, protecting websites from tampering. This function is helpful for governments, educational institutions, and enterprises.

WAF protects user data on the application layer. It supports cache configuration on static web pages. When a user accesses a web page, the system returns a cached page to the user and randomly checks whether the page has been tampered with.

Differences Between the Web Tamper Protection Functions of HSS and WTP

Table 13-1 describes the differences

Table 13-1 Differences between the web tamper protection functions of HSS and WTP

Item	HSS	WAF
Static web page protection	Locks files in driver and web file directories to prevent attackers from tampering with them.	Caches static web pages on servers.
Dynamic web page protection	<ul style="list-style-type: none"> Dynamic WTP Protects your data while Tomcat is running, detecting dynamic data tampering in databases. Privileged process management Allows privileged processes to modify web pages. 	No
Backup and restoration	<ul style="list-style-type: none"> Active backup and restoration If WTP detects that a file in the protection directory is tampered with, it immediately uses the backup file on the local host to restore the file. Remote backup and restoration If a file directory or backup directory on the local server becomes invalid, you can use the remote backup service to restore the tampered web page. 	No
Suitable for	Websites that have high security requirements and difficult to be manually recovered	Websites that only require application-layer protection

Purchase Suggestion

Website	Service
Common websites	WAF web tamper protection + HSS enterprise edition
Websites that require strong protection and anti-tampering capabilities	WAF web tamper protection + HSS WTP

13.1.2.5 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

13.1.2.6 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.

13.1.2.7 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 13-2 How WAF works for CNAME or dedicated access

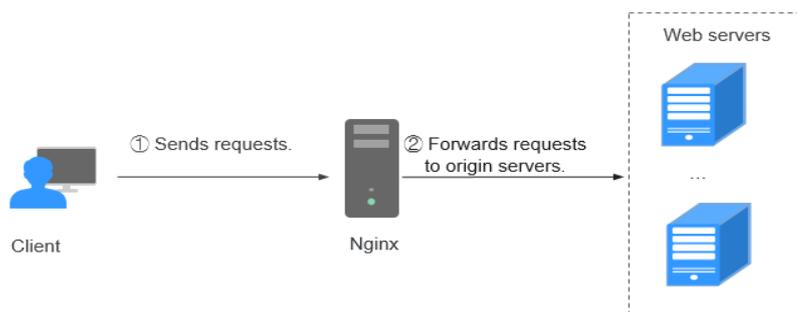


- Nginx forwarding

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 13-3 How Nginx Works



13.1.2.8 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.

13.1.2.9 How Does WAF Detect SQL Injection, XSS, and PHP Injection Attacks?

A Structured Query Language (SQL) injection is a common web attack. The attacker injects malicious SQL commands into database query strings to deceive the server into executing commands. By exploiting these commands, the attacker can obtain sensitive information, add users, export files, or even gain the highest permissions to the database or system.

XSS attacks exploit vulnerabilities left during web page development to inject malicious instruction code into web pages so that attackers can trick visitors into loading and executing malicious web page programs attackers fabricated. These malicious web page programs are usually JavaScript, but they can also include Java, VBScript, ActiveX, Flash, or even common HTML. After an attack succeeds, the attacker may obtain various content, including but not limited to higher permissions (for example, permissions for certain operations), private content, sessions, and cookies.

How Does WAF Detect SQL Injection Attacks?

WAF detects and matches SQL keywords, special characters, operators, and comment symbols.

- SQL keywords: union, Select, from, as, asc, desc, order by, sort, and, or, load, delete, update, execute, count, top, between, declare, distinct, distinctrow, sleep, waitfor, delay, having, sysdate, when, dba_user, case, delay, and the like
- Special characters: ', ;, ()
- Mathematical operators: ±, *, /, %, and |
- Operators: =, >, <, >=, <=, !=, +=, and -=
- Comment symbols: - or /**/

How Does WAF Detect XSS Attacks?

WAF checks HTML script tags, event processors, script protocols, and styles to prevent malicious users from injecting malicious XSS statements through client requests.

- XSS keywords (such as **javascript**, **script**, **object**, **style**, **iframe**, **body**, **input**, **form**, **onerror**, and **alert**)

- Special characters (<, >, ', and ")
- External links (href="http://xxx/",src="http://xxx/attack.js")

 **NOTE**

Rich text can be uploaded using multipart upload instead of body. In multipart upload, rich text is stored in forms and can be decoded even if it is encoded using Base64. Analyze your services and do not use quotation marks and angle brackets as far as possible.

How Does WAF Detect PHP Injection Attacks?

If a request contains keywords similar to "system(xx)", the keywords may cause PHP injection attacks. WAF will then block such requests.

13.1.2.10 Can WAF Defend Against the Apache Struts2 Remote Code Execution Vulnerability (CVE-2021-31805)?

Yes. WAF basic web protection rules can defend against the Apache Struts2 remote code execution vulnerability (CVE-2021-31805).

Configuration Procedure

Step 1 [Enable WAF](#).

Step 2 Add the website domain name to WAF and connect it to WAF. For details, see [Connecting a Website to WAF](#).

Step 3 In the **Basic Web Protection** configuration area, set **Mode** to **Block**. For details, see [Configuring Basic Protection Rules to Defend Against Common Web Attacks](#).

----End

13.1.3 WAF Usage

13.1.3.1 Why Does the Vulnerability Scanning Tool Report Disabled Non-standard Ports for My WAF-Protected Website?

Symptom

When a third-party vulnerability scanning tool scans the website whose domain name has been connected to WAF, the scan result shows that some standard ports (for example, 443) and non-standard ports (for example, 8000 and 8443) are vulnerable.

Possible Cause

WAF uses the same non-standard port engine for all WAF users. So, if a third-party vulnerability scanning tool performs a scan for your website, the enabled non-standard ports in WAF are reported. This means such port vulnerabilities in scan results do not affect your origin server security. WAF will safeguard your website after you point origin server IP address to WAF engine IP address through the CNAME record.

Handling Suggestions

No action is required.

13.1.3.2 How Do I Obtain the Real IP Address of a Web Visitor?

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

Generally, a proxy such as CDN, WAF, and anti-DDoS service is deployed between the client and server. Web visitors cannot directly access the server. For example, **web visitor > CDN/WAF/anti-DDoS > origin server**.

When forwarding requests to the downstream server, the transparent proxy server adds an **X-Forwarded-For** field to the HTTP header to identify the web visitor's real IP address in the format of **X-Forwarded-For: real IP address of the web visitor, proxy 1-IP address, proxy 2-IP address, proxy 3-IP address,->....**

Therefore, you can obtain the web visitor's real IP address from the **X-Forwarded-For** field. The first IP address in this field is the web visitor's real IP address.

13.1.3.3 Will Traffic Be Permitted After WAF Is Switched to the Bypassed Mode?

For cloud WAF instances, if you switch the instance working **Mode** to **Bypassed**, requests are directly sent to the original backend server without passing through WAF.

Switch the WAF mode to **Bypassed** only if one of the following conditions is met:

- Website services need to be restored to the status when the website is not connected to WAF.
- You need to investigate website errors, such as 502, 504, or other incompatibility issues.
- No proxy is configured between the client and WAF.

Effective Time of WAF Bypassed Working Mode

After you switch the WAF work **Mode** to **Bypassed**, it takes effect within 3 to 5 minutes.

Procedure for WAF Working Mechanism Switchover

Step 1 Log in to the management console.

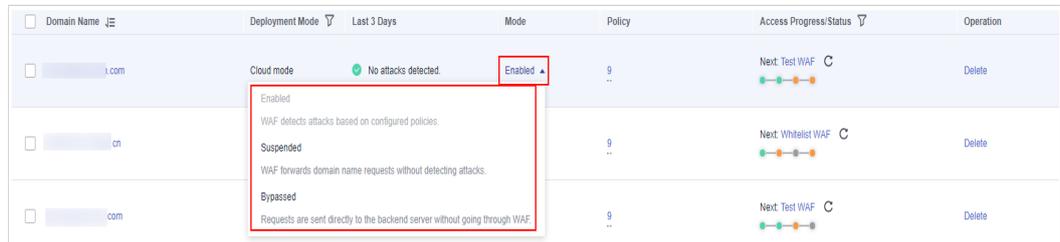
Step 2 Click  in the upper left corner of the management console and select a region or project.

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 row containing the target domain name, click ▼ in the **Mode** column and select **Bypassed**.

Figure 13-4 Switching WAF working mode



----End

13.1.3.4 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.

13.1.3.5 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 13-2](#).

Table 13-2 QPS calculation

Time Range	Average QPS Description	Peak QPS Description
Yesterday or Today	The QPS curve is made with the average QPS in every minute.	The QPS curve is made with each peak QPS in every minute.
Past 3 days	The QPS curve is made with the average QPS in every five minutes.	The QPS curve is made with each peak QPS in every five minutes.
Past 7 days	The QPS curve is made with the maximum value among the average QPS in every five minutes at a 10-minute interval.	The QPS curve is made with each peak QPS in every 10 minutes.
Past 30 days	The QPS curve is made with the maximum value among the average QPS in every five minutes at a one-hour interval.	The QPS curve is made with the peak QPS in every hour.

13.1.3.6 Does WAF Support Custom Authorization Policies?

WAF supports custom authorization policies. With IAM, you can:

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

13.1.3.7 How Do I Configure My Server to Allow Only Requests from WAF?

You can configure an access control rule on the origin server to allow only WAF back-to-source IP addresses to access the origin server. This prevents hackers from bypassing WAF to attack the origin server through origin server IP addresses, ensuring the security, stability, and availability of the origin server.

13.1.3.8 Why Do Cookies Contain the HWWAFSESID or HWWAFSESTIME field?

HWWAFSESID indicates the session ID, and **HWWAFSESTIME** indicates the session timestamp. These two fields are used to mark the request, for example, they can be used to count the requests for a CC protection rule.

After a domain name or IP address is connected to WAF, WAF inserts fields such as **HWWAFSESID** (session ID) and **HWWAFSESTIME** (session timestamp) into the cookie of your customer request. These fields are used by WAF to implement some functions, such as counting requests and monitoring request duration. If these fields are not inserted, some rules may be unable to work, such as CC attack

protection rules with verification code configured, known attack source rules, and dynamic anti-crawler rules.

13.1.3.9 Can I Switch Between the WAF Cloud Mode and Dedicated Mode?

Direct switchover is not supported, but you can complete required configurations then use the WAF mode you want. When adding a domain name or IP address to WAF, WAF offers cloud mode and dedicated mode to meet different needs. Once you select a WAF mode and connect the domain name to WAF, the WAF mode cannot be changed directly.

If you want to use another WAF mode for the domain name, deploy your services in the WAF mode you want first. Then, remove the domain name or IP address from the current WAF instance. After that, you can add the website in the mode you want to the WAF instance. For example, you are using a cloud WAF instance to protect domain name `www.example.com`. If you want to use a dedicated WAF instance to protect `www.example.com`, ensure that your current services are supported by WAF dedicated mode. Then, you can apply for a dedicated WAF instance and remove protected domain name `www.example.com` from the cloud WAF instance. Then, add `www.example.com` to the dedicated WAF instance.

13.1.3.10 How Do I Configure WAF If a Reverse Proxy Server Is Deployed for My Website?

In this case, the reverse proxy server will not be affected after the website is connected to WAF. In cloud CNAME access mode, WAF works as a reverse proxy between the client and your website server. The real IP addresses of your website server are hidden from the visitors, and only the IP addresses of WAF are visible to them.

13.1.3.11 How Does WAF Forward Access Requests When Both a Wildcard Domain Name and a Single Domain Name Are Connected to WAF?

WAF preferentially forwards access requests to the single domain name. If the single domain name cannot be identified, access requests will be forwarded to the wildcard domain name.

For example, if you connect single domain name `a.example.com` and wildcard domain name `*.example.com` to WAF, WAF preferentially forwards access requests to single domain name `a.example.com`.

If you are configuring a wildcard domain name, pay attention to the following:

- If the server IP address of each subdomain name is the same, enter a wildcard domain name. For example, if the subdomain names ***a.example.com***, ***b.example.com***, and ***c.example.com*** have the same server IP address, you can add the wildcard domain name ****.example.com*** to WAF to protect all three.
- If the server IP addresses of subdomain names are different, add subdomain names as single domain names one by one.

13.2 Service Request/Specification

13.2.1 WAF Instance Specifications Change

13.2.1.1 What Are the Impacts When QPS Exceeds the Allowed Peak Rate?

If the QPS specifications you select cannot handle the daily peak traffic of protected website or application services, WAF stops protecting your website. This will cause traffic limiting, random packet loss, automatic bypassing of WAF. As a result, your services may become unavailable, frozen, or respond very slowly for a certain period of time.

The following describes the QPS specifications supported by dedicated WAF instances in different deployments.

- Normal peak requests for a single instance:
 - Specifications: WI-500. Referenced performance:
 - HTTP services - Recommended QPS: 5,000. Maximum QPS: 10,000.
 - HTTPS services - Recommended QPS: 4,000. Maximum QPS: 8,000.
 - WebSocket service - Maximum concurrent connections: 5,000
 - Maximum WAF-to-server persistent connections: 60,000
 - Specifications: WI-100. Referenced performance:
 - HTTP services - Recommended QPS: 1,000. Maximum QPS: 2,000.
 - HTTPS services - Recommended QPS: 800. Maximum QPS: 1,600
 - WebSocket service - Maximum concurrent connections: 1,000
 - Maximum WAF-to-server persistent connections: 60,000
- Peak rate of CC attack protection
 - Specifications: WI-500. Referenced performance:
Maximum QPS: 20,000
 - Specifications: WI-100. Referenced performance:
Maximum QPS: 4,000

13.2.2 About Service Requests

13.2.2.1 Where Can I View the Inbound and Outbound Bandwidths of a Protected Website?

On the **Dashboard** page, you can view the bandwidth usage about the protected website or instance. The procedure is as follows:

Step 1 Log in to the management console.

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

- Step 3** Click  in the left upper corner and choose **Security > Web Application Firewall** to go to the **Dashboard** page.
- Step 4** In the website or instance drop-down list, select the website or instance you want to check and select a time range (yesterday, today, past 3 days, past 7 days, or past 30 days).
- Step 5** In the **Security Event Statistics** area, select the **Bytes Sent/Received** tab and view the inbound and outbound bandwidths.
- End

13.3 Website Domain Name Access Configuration

13.3.1 Domain Name and Port Configuration

13.3.1.1 How Do I Add a Domain Name/IP Address to WAF?

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

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

- Cloud mode: protects your web applications on or off the cloud through domain names.
- Dedicated mode: protects your web applications on the cloud through domain names or IP addresses.

NOTICE

- You can enter a multi-level single domain name (for example, top-level domain name `example.com` or second-level domain name `www.example.com`) or a wildcard domain name (`*.example.com`). The processes of connecting domain names to different WAF instance types are the same.
 - If the server IP address of each subdomain name is the same, enter a wildcard domain name. For example, if the subdomain names `a.example.com`, `b.example.com`, and `c.example.com` have the same server IP address, you can add the wildcard domain name `*.example.com` to WAF to protect all three.
 - If the server IP addresses of subdomain names are different, add subdomain names as single domain names one by one.

The following figure shows the process of connecting a website to WAF in each mode.

Figure 13-5 Process of connecting a website to WAF - Cloud Mode (CNAME Access)

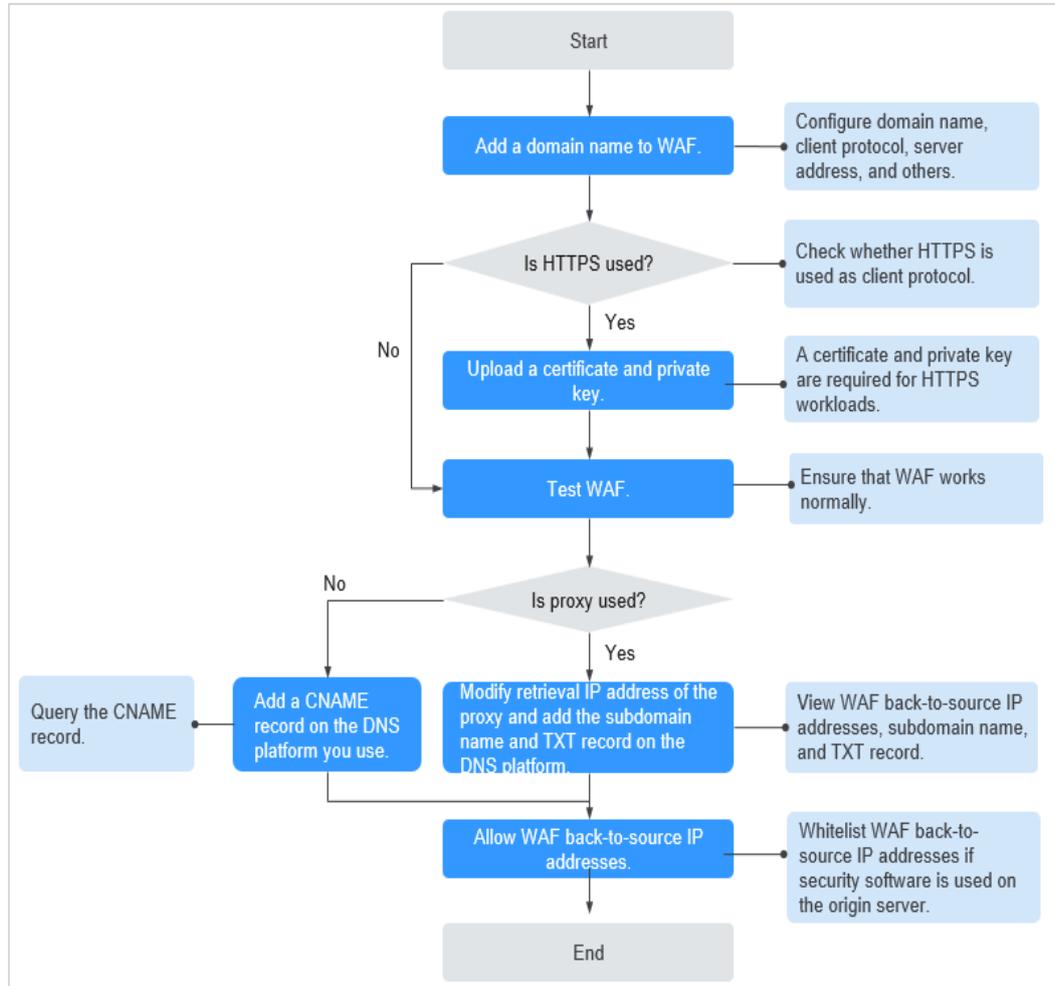
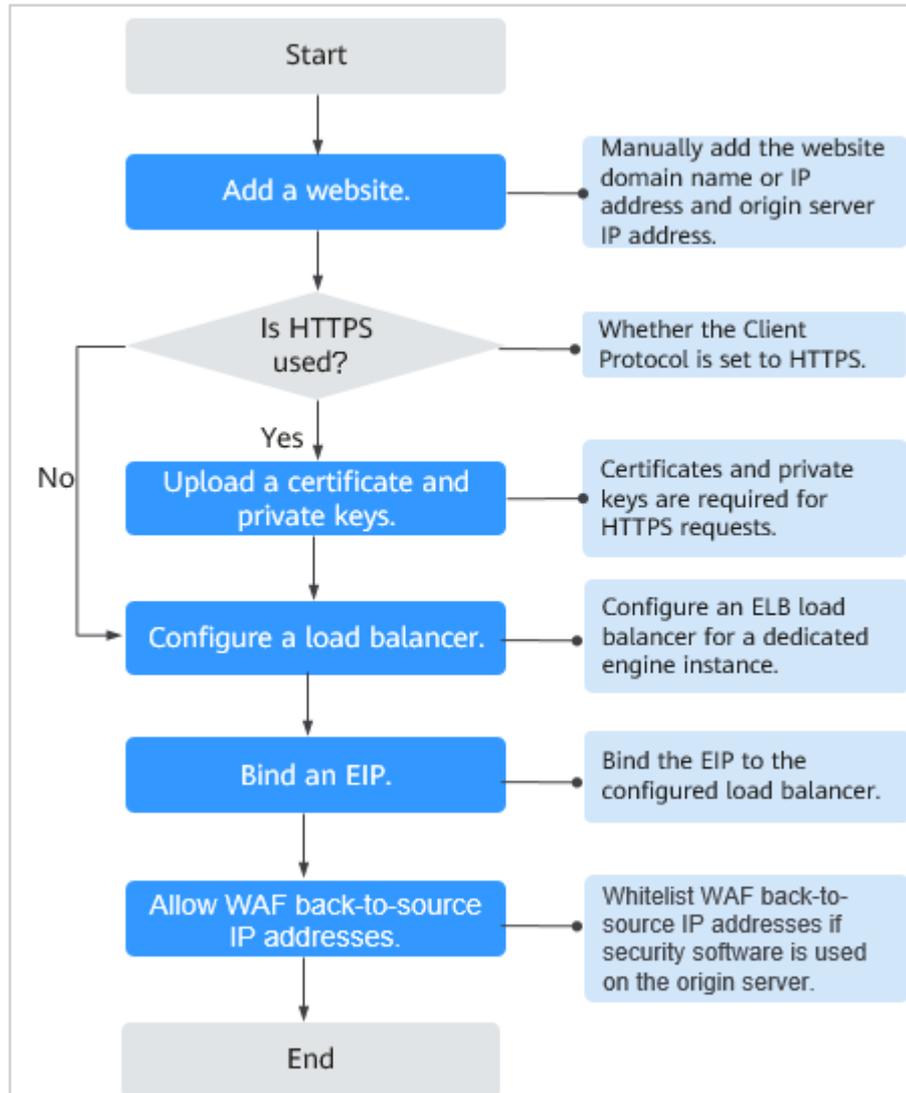


Figure 13-6 Process of connecting a website to a dedicated WAF instance



- 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

13.3.1.2 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 13-3 lists the ports that can be protected by WAF.

Table 13-3 Ports supported by WAF

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

Deploy ment Mode	Port Category	HTTP Protocol	HTTPS Protocol	Port Limit
	Non-standard ports (182 in total)	9945, 9770, 81, 82, 83, 84, 88, 89, 800, 808, 1000, 1090, 3128, 3333, 3501, 3601, 4444, 5000, 5222, 5555, 5601, 6001, 6666, 6788, 6789, 6842, 6868, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8800, 8686, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9802, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702, 8011, 8012, 8013, 8014,	8750, 8445, 18010, 4443, 5443, 6443, 7443, 8081, 8082, 8083, 8084, 8443, 8843, 9443, 8553, 8663, 9553, 9663, 18110, 18381, 18980, 28443, 18443, 8033, 18000, 19000, 7072, 7073, 8803, 8804, 8805, 9999	Unlimited

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

13.3.1.3 How Do I Use a Dedicated WAF Instance to Protect Non-Standard Ports That Are Not Supported by the Dedicated Instance?

To use a dedicated WAF instance to protect a non-standard port that is not supported by dedicated instance, configure an ELB load balancer to distribute traffic to any non-standard port that is supported by the dedicated instance. For supported non-standard ports, see [Which Non-Standard Ports Does WAF Support?](#)

For example, a client sends requests over HTTP to the dedicated WAF instance, and you protect the website whose domain name is `www.example.com:1234`. The dedicated instance cannot protect non-standard port 1234. In this case, you can configure a load balancer to distribute traffic to any other non-standard port (for example, port 81) that can be protected by the dedicated instance. In this way, traffic designated to non-standard port 1234 will be checked by WAF.

NOTICE

To ensure that the configuration takes effect, a wildcard domain name corresponding to the protected domain name is recommended for the **Domain Name** field. For example, if you want to protect `www.example.com:1234`, set **Domain Name** to `*.example.com`.

Perform the following steps:

Step 1 Log in to the management console.

Step 2 Add the domain name of the website you want to protect on the WAF console.

1. Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
2. In the navigation pane on the left, choose **Website Settings**.
3. In the upper left corner of the website list, click **Add Website**. On the displayed page, select **Dedicated mode**, enter the wildcard domain name `*.example.com` corresponding to `www.example.com:1234` in the **Domain Name** text box, and select a port (for example, 81) from the **Protected Port** drop-down list.
4. Select **Yes** for **Proxy Configured** and click **Confirm**.
5. Close the dialog box displayed.

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

Step 3 Configure a load balancer on the ELB console.

1. Click  in the upper left corner of the page and choose **Elastic Load Balance** under **Network** to go to the **Load Balancers** page.
2. Click the name of the load balancer you want in the **Name** column to go to the **Basic Information** page.
3. Locate the **IP as a Backend** row, enable the function. In the displayed dialog box, click **OK**.
4. Select the **Listeners** tab, click **Add Listener**, and configure the listener port to **1234**.
5. Click **Next: Configure Request Routing Policy**.
6. Click **Next: Add Backend Server**. Then, select the **IP as Backend Servers** tab.
7. Click **Add IP as Backend Server**. In the displayed dialog box, configure **Backend Server IP Address** and **Backend Port**.
 - **Backend Server IP Address:** Enter the IP address of the dedicated WAF engine, which you can obtain from the dedicated engine list.
 - **Backend Port:** 81, which is the same as the port you configured in [Step 2.3](#).
8. Click **OK**.
9. Click **Next: Confirm**, confirm the information, and click **Submit**.

Step 4 Unbind an elastic IP address (EIP) from the origin server and bind the EIP to the load balancer configured for the dedicated WAF instance.

----End

13.3.1.4 How Do I Configure Domain Names to Be Protected When Adding Domain Names?

Before using WAF, you need to add domain names to be protected to WAF based on your web service protection requirements. WAF supports addition of single domain names and wildcard domain names. This section describes how to configure domain names to be protected.

Basic Concepts

- Wildcard domain name

A wildcard domain name is a domain name that contains the wildcard * and starts with *..

For example, ***.example.com** is a correct wildcard domain name, but ***.*.example.com** is not.

NOTE

A wildcard domain name counts as one domain name.

- Single domain name

A single domain name is also called a common domain name and is a specific domain name (a non-wildcard domain name).

For example, **www.example.com** or **example.com** is a single domain name.

 NOTE

For example, **www.example.com** counts as a domain name and so does **a.www.example.com**.

Selecting a Domain Name Type

WAF supports single domain names and wildcard domain names.

The domain name purchased from the DNS service provider is a single domain name (example.com). The domain name added to WAF can be example.com, a subdomain name (for example, a.example.com), or wildcard domain name (*.example.com). You can select a domain name type based on the following scenarios:

- If services of a domain name to be protected are the same, enter a single domain name. For example, if all the services of www.example.com to be protected are services on port 8080, set **Domain Name** to a single domain name **www.example.com**.
- If the server IP address of each subdomain name is the same, enter a wildcard domain name to be protected. For example, if the server IP addresses corresponding to a.example.com, b.example.com, and c.example.com are the same, **Domain Name** can be set to a wildcard domain name ***.example.com**.
- If the server IP addresses of subdomain names are different, add subdomain names as single domain names one by one.

 NOTE

You are advised to set the added domain name to be protected to be the same as the domain name that is set at the DNS provider.

If A Single Domain Name and A Wildcard Domain Name Are Added To WAF at The Same Time, Which Domain Name Will WAF Check First?

WAF first checks the domain name that points to a specific page. For example, if www.example.com, *.a.example.com, and *.example.com are added to WAF, WAF checks them in the following sequence: www.example.com > *.a.example.com > *.example.com.

13.3.1.5 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.

13.3.1.6 How Do I Configure Non-standard Ports When Adding a Protected Domain Name?

When you add a domain name to WAF, **Port** must be configured to the service port of your website. You can configure it by referring to the following instructions:

- If **Client Protocol** is **HTTP**, WAF protects services on the standard port 80 by default. If **Client Protocol** is **HTTPS**, WAF protects services on the standard port 443 by default.
- To configure a port other than ports 80 and 443, select a non-standard port from the **Protected Port** drop-down list.

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

1. Select **Standard port** from the **Protected Port** drop-down list.
2. Select **HTTP** or **HTTPS** for **Client Protocol**. [Figure 13-7](#) and [Figure 13-8](#) show standard port configurations when the client protocol is HTTP or HTTPS.

Figure 13-7 Port 80

Origin Server Settings						
* Protected Port	Standard port					
* Server Configuration	Client Protocol	Server Protocol	Server Address	Server Port	Weight	
	HTTP	HTTP	IPv4 36	80	1	
	HTTP	HTTP	IPv4 .9	80	1	

Figure 13-8 Port 443

Origin Server Settings						
* Protected Port	Standard port					
* Server Configuration	Client Protocol	Server Protocol	Server Address	Server Port	Weight	
	HTTP	HTTP	IPv4 36	80	1	
	HTTP	HTTP	IPv4 .9	80	1	

NOTE

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

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

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

1. In the **Protected Port** drop-down list, select a non-standard port you want to protect.
2. Select **HTTP** or **HTTPS** for **Client Protocol** for all server ports. [Figure 13-9](#) and [Figure 13-10](#) show the configuration of non-standard HTTP or HTTPS port, respectively.

Figure 13-9 Other HTTP port besides port 80

The screenshot shows the 'Origin Server Settings' interface. The 'Protected Port' is set to 8080. Below, the 'Server Configuration' table has two rows, both with 'Client Protocol' set to HTTP. The first row has 'Server Protocol' as HTTP, 'Server Address' as IPv4 .36, and 'Server Port' as 80. The second row has 'Server Protocol' as HTTP, 'Server Address' as IPv4 .9, and 'Server Port' as 80. A red box highlights the 'Protected Port' field and the 'Client Protocol' dropdowns.

Client Protocol	Server Protocol	Server Address	Server Port	Weight
HTTP	HTTP	IPv4 .36	80	1
HTTP	HTTP	IPv4 .9	80	1

Figure 13-10 Other HTTPS port besides port 443

The screenshot shows the 'Origin Server Settings' interface. The 'Protected Port' is set to 6443. Below, the 'Server Configuration' table has two rows, both with 'Client Protocol' set to HTTPS. The first row has 'Server Protocol' as HTTP, 'Server Address' as IPv4 .36, and 'Server Port' as 80. The second row has 'Server Protocol' as HTTP, 'Server Address' as IPv4 .9, and 'Server Port' as 80. A red box highlights the 'Protected Port' field and the 'Client Protocol' dropdowns.

Client Protocol	Server Protocol	Server Address	Server Port	Weight
HTTPS	HTTP	IPv4 .36	80	1
HTTPS	HTTP	IPv4 .9	80	1

NOTE

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

Example 3: Protecting Different Service Ports

If the service ports to be protected are different, configure the ports separately. For example, to protect ports 8080 and 6443 for your site **www.example.com**, add the domain separately for each port, as shown in [Figure 13-11](#) and [Figure 13-12](#).

Figure 13-11 Protecting port 8080

The screenshot shows the 'Origin Server Settings' interface. The 'Protected Port' is set to 8080. Below, the 'Server Configuration' table has one row with 'Client Protocol' set to HTTP. The 'Server Protocol' is HTTP, 'Server Address' is IPv4 .36, and 'Server Port' is 80. A red box highlights the 'Protected Port' field and the 'Client Protocol' dropdown.

Client Protocol	Server Protocol	Server Address	Server Port	Weight
HTTP	HTTP	IPv4 .36	80	1

Figure 13-12 Protecting port 6443

The screenshot shows the 'Origin Server Settings' interface. The 'Protected Port' is set to 6443. Under 'Server Configuration', the 'Client Protocol' is set to HTTPS, the 'Server Protocol' is HTTP, the 'Server Address' is IPv4 .36, the 'Server Port' is 80, and the 'Weight' is 1.

13.3.1.7 What Can I Do If One of Ports on an Origin Server Does Not Require WAF Protection?

WAF protects your web application through its domain name and the corresponding service port. When you add a domain name to WAF, you specify the domain name and the port to be protected. After the website is connected to WAF, traffic will not be forwarded to WAF through other ports.

13.3.1.8 What Data Is Required for Connecting a Domain Name/IP Address to WAF?

Prepare information required for connecting a domain name 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:** public IP address (generally corresponding to the A record of the domain name configured on the DNS) or domain name (generally corresponding to the CNAME of the domain name configured on the DNS) of the web server that a client accesses.
 - **Server Port:** service port over which the WAF instance forwards client requests to the origin server.
- Certificate: If HTTPS is set for **Client Protocol**, associate the certificate to WAF.

13.3.1.9 How Do I Safely Delete a Protected Domain Name?

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

- In cloud mode, if you want to remove a protected website from WAF, go to the DNS platform and translate the domain name to the origin server IP address before you remove it. Otherwise, traffic intended to the domain name will not be directed to the origin server.
- If you select **Forcible delete the WAF CNAME record.**, WAF will not check your domain name resolution and delete WAF CNAME record immediately.

Before enabling this option, make sure you have resolved the domain name to the origin server, or your website will become inaccessible.

- It takes 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.

13.3.1.10 Can I Change the Domain Name That Has Been Added to WAF?

After a domain name is added to WAF, you cannot change its name. If you want to change the protected domain name, you are advised to delete the original one and add the domain name you want to protect.

13.3.1.11 What Are the Precautions for Configuring Multiple Server Addresses for Backend Servers?

- When configuring multiple server addresses for the same domain name, pay attention to the following:
 - For domain names mapping to non-standard ports
The client protocol, server protocol, and server for each piece of server configuration must be the same.
 - For domain names mapping to standard ports
The client protocol, server protocol, and server for each piece of server configuration can be different.
- When a domain name is added, WAF supports addition of multiple server IP addresses. WAF routes legitimate requests back to origin servers in polling mode, reducing the pressure on the servers and protecting the origin servers. For example, two backend server IP addresses (IP-A and IP-B) are added. When there are 10 requests for accessing the domain name, five requests are forwarded by WAF to the server identified by IP-A, and the other five requests are forwarded by WAF to the server identified by IP-B.

13.3.1.12 Does WAF Support Wildcard Domain Names?

Yes. When adding a domain name to WAF, you can configure a single domain name or a wildcard domain name based on your service requirements. The details are as follows:

- Single domain name
Configure a single domain name to be protected. For example, `www.example.com`
- Wildcard domain name
You can configure a wildcard domain name to let WAF protect multi-level domain names under the wildcard domain name.
 - If the server IP address of each subdomain name is the same, enter a wildcard domain name to be protected. For example, if the subdomain names *a.example.com*, *b.example.com*, and *c.example.com* have the same server IP address, you can directly add the wildcard domain name **.example.com* to WAF for protection.
 - If each subdomain name points to different server IP addresses, add subdomain names as single domain names one by one.

13.3.1.13 How Do I Route Website Traffic to My Cloud WAF Instance?

In cloud CNAME access mode, after you add your website to WAF, resolve the website domain name to WAF so that the traffic can pass through WAF. Then, WAF will filter out malicious requests and forward only legitimate requests to the origin server.

How WAF Works

- No proxy used
DNS resolves your domain name to the origin server IP address before the site is connected to WAF. DNS resolves your domain name to the CNAME of WAF after the site is connected to WAF. Then WAF inspects the incoming traffic and filters out malicious traffic.
- A proxy (such as anti-DDoS service) used
If a proxy such as anti-DDoS service is used on your site before it is connected to WAF, DNS resolves the domain name of your site to the anti-DDoS IP address. The traffic goes to the anti-DDoS service and the anti-DDoS service then routes the traffic back to the origin server. After you connect your website to WAF, change the back-to-source address of the proxy (such as anti-DDoS service) to the CNAME of WAF. In this way, the proxy forwards the traffic to WAF. WAF then filters out illegitimate traffic and only routes legitimate traffic back to the origin server.

NOTE

- To ensure that WAF can properly forward requests, test WAF by referring to [Testing WAF](#) before modifying the DNS configuration.
- To prevent other users from configuring your domain names on WAF in advance (this will cause interference on your domain name protection), add the subdomain name and TXT record on your DNS management platform. WAF can determine which user owns the domain name based on the subdomain name and TXT record.

Operation Guide

After a domain name is added, WAF generates a CNAME record, or CNAME, subdomain name, and TXT record for DNS to resolve the domain name to WAF so that website traffic can pass through WAF for detection. For details, see [Table 13-4](#).

Table 13-4 Operation guide

Scenario	Generated Parameter Value	Operation Related to Domain Name Resolution
No proxy used	CNAME	The DNS obtains the CNAME of WAF.

Scenario	Generated Parameter Value	Operation Related to Domain Name Resolution
Proxy used	CNAME, subdomain name, and TXT record	<ul style="list-style-type: none"> • Change the back-to-source IP address of the proxy, such as anti-DDoS service, to the CNAME of WAF. • (Optional) Add a WAF subdomain name and TXT record at your DNS provider.

Procedure

For details, see [Step 4: Modify the DNS Records of the Domain Name](#).

13.3.1.14 Can I Configure Multiple Load Balancers for a Dedicated WAF Instance?

Yes. You can add a dedicated WAF instance to backend server groups of more than one load balancers.

13.3.1.15 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.

13.3.2 Certificate Management

13.3.2.1 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.

13.3.2.2 How Do I Modify a Certificate?

If the purchased certificate is about to expire, you are advised to purchase a new certificate before the expiration date and update the certificate associated with the domain name in WAF.

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**.
 - Step 4** In the navigation pane on the left, choose **Website Settings**.
 - Step 5** In the **Domain Name** column, click the website domain name to go to the basic information page.
 - Step 6** Click the edit icon next to **Server Information**. If **Client Protocol** is **HTTPS**, select a new certificate from the certificate drop-down list or import a new certificate.
- End

13.3.2.3 Do I Need to Import the Certificates That Have Been Uploaded to ELB to WAF?

You can select a created certificate or import a new certificate. You need to import the certificate that has been uploaded to ELB to WAF.

13.3.2.4 How Do I Convert a Certificate into PEM Format?

Only .pem certificates can be used in WAF. If the certificate is not in .pem format, convert it into .pem locally by referring to [Table 13-5](#) before uploading it.

Table 13-5 Certificate conversion commands

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

Format	Conversion Method
DER	<ul style="list-style-type: none"> Obtain a private key. For example, run the following command to convert privatekey.der into privatekey.pem: openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem Obtain a certificate. For example, run the following command to convert cert.der into cert.pem: openssl x509 -inform der -in cert.der -out cert.pem

 NOTE

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

13.3.3 Server Configuration

13.3.3.1 How Do I Configure the Client Protocol and Server Protocol?

This FAQ describes how to configure the client and server protocol.

WAF provides various protocol types. Use [www.example.com](#) as an example. You can configure your WAF instance using any of the following methods:

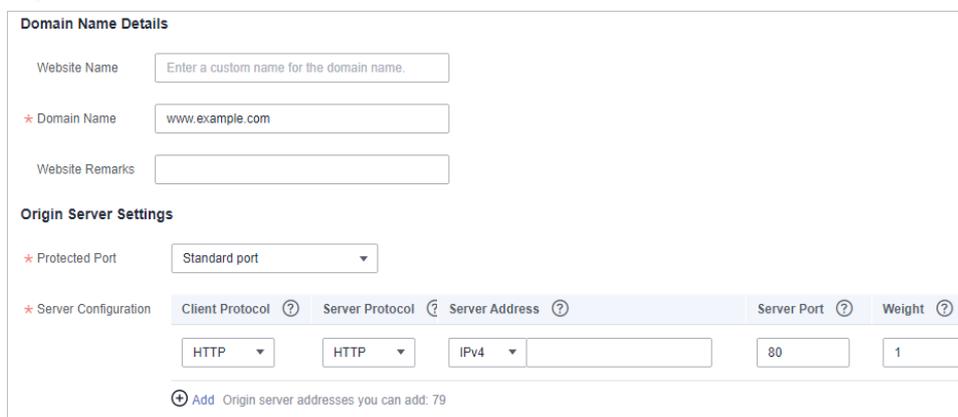
HTTP Access - 302 Redirection Response

Set **Client Protocol** and **Server Protocol** to HTTP. [Figure 13-13](#) shows an example.

NOTICE

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

Figure 13-13 HTTP mode



Domain Name Details

Website Name:

* Domain Name:

Website Remarks:

Origin Server Settings

* Protected Port:

* Server Configuration	Client Protocol ?	Server Protocol ?	Server Address ?	Server Port ?	Weight ?
	<input type="text" value="HTTP"/>	<input type="text" value="HTTP"/>	<input type="text" value="IPv4"/>	<input type="text" value="80"/>	<input type="text" value="1"/>

+ Add Origin server addresses you can add: 79

HTTPS Forcible Conversion

Set **Client Protocol** and **Server Protocol** to **HTTPS**. [Figure 13-14](#) shows an example. When the HTTP protocol is used to access the server, all initial client requests are forcibly converted from HTTP to HTTPS.

NOTICE

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

Figure 13-14 HTTPS redirection

The screenshot shows a configuration interface for domain name details. It includes fields for Website Name, Domain Name (www.example.com), and Website Remarks. Under Origin Server Settings, the Protected Port is set to Standard port. The Server Configuration table is as follows:

Client Protocol	Server Protocol	Server Address	Server Port	Weight
HTTPS	HTTPS	IPv4	443	1

At the bottom, there is a link to add more origin server addresses.

HTTP and HTTPS

Set **Client Protocol** and **Server Protocol**. [Figure 13-15](#) shows an example.

NOTICE

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

Figure 13-15 HTTP and HTTPS forwarding

The screenshot shows the 'Origin Server Settings' interface. At the top, there is a 'Protected Port' dropdown menu set to 'Standard port'. Below this is a 'Server Configuration' section with a table of settings. The table has five columns: Client Protocol, Server Protocol, Server Address, Server Port, and Weight. There are two rows of configuration: one for HTTP (Client Protocol: HTTP, Server Protocol: HTTP, Server Address: IPv4, Server Port: 80, Weight: 1) and one for HTTPS (Client Protocol: HTTPS, Server Protocol: HTTPS, Server Address: IPv4, Server Port: 443, Weight: 1). At the bottom, there is an 'Add' button and a note: 'Origin server addresses you can add: 78'.

HTTPS Offloading

Set **Client Protocol** to **HTTPS** and **Server Protocol** to **HTTP**.

NOTICE

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

Figure 13-16 HTTPS offloading

The screenshot shows the 'Domain Name Details' and 'Origin Server Settings' sections. In 'Domain Name Details', there is a 'Website Name' field with a placeholder 'Enter a custom name for the domain name.', a 'Domain Name' field with 'www.example.com', and a 'Website Remarks' field. Below this is the 'Origin Server Settings' section. It has a 'Protected Port' dropdown set to 'Standard port'. Below this is a note: 'The port that your website or application provides services over. For example, if http://www.example.com: 8080 needs to be protected, set this parameter to 8080.' The 'Server Configuration' table has five columns: Client Protocol, Server Protocol, Server Address, Server Port, and Weight. The configuration is: Client Protocol: HTTPS, Server Protocol: HTTP, Server Address: IPv4, Server Port: 80, Weight: 1. At the bottom, there is an 'Add' button and a note: 'Origin server addresses you can add: 19'.

13.3.3.2 Why Cannot I Select a Client Protocol When Adding a Domain Name?

The non-standard port you configured is not supported by the client protocol (HTTP/HTTPS). The non-standard port you will configure must be supported by the client protocol (HTTP/HTTPS).

For more details, see [Which Non-Standard Ports Does WAF Support?](#)

13.3.3.3 Can I Set the Origin Server Address to a CNAME Record If I Use Cloud WAF?

Yes. If the IP address of the origin server is set to a CNAME record, additional DNS resolution is performed after a domain name is added. That is, the CNAME is resolved to an IP address first. DNS resolution increases the delay. Therefore, a public network IP address is recommended for the origin server.

13.3.4 Operations After Connecting Websites to WAF

13.3.4.1 Can I Access a Website Using an IP Address After a Domain Name Is Connected to WAF?

After a domain name is connected to WAF, you can enter the origin server IP address in the address bar of the browser to access the website. However, your origin server IP address is easily exposed. As a result, attackers can bypass WAF and attack your origin server.

13.3.4.2 How Do I Test WAF?

Before you direct the traffic to WAF, perform local verification to ensure that all configurations are correct.

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

For details, see [Step 3: Test WAF](#).

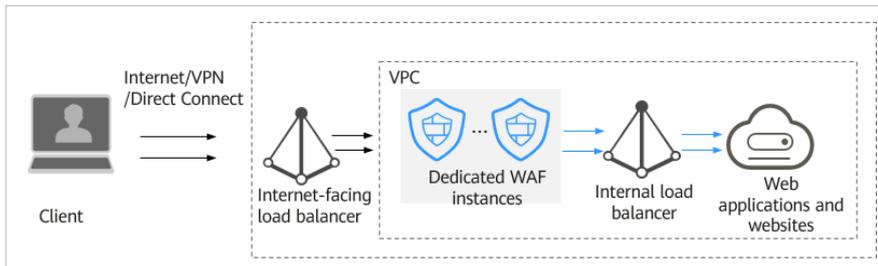
13.3.4.3 How Can I Forward Requests Directly to the Origin Server Without Passing Through WAF?

If you select **Cloud** for **Protection**, take the following steps to route your website traffic to origin servers.

If you select **Cloud - CNAME** or **Dedicated** for **Protection**, take the following steps to route your website traffic to origin servers.

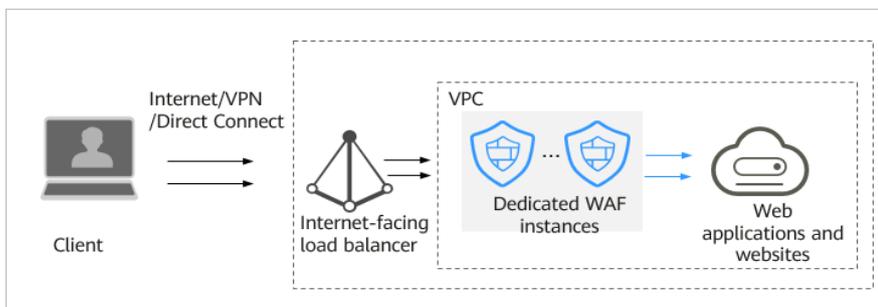
- Cloud
Switch the WAF working **Mode** to **Bypassed**. Then, your website requests directly go to the origin servers without passing through WAF. It takes about 3 to 5 minutes for WAF bypass to take effect.
- Dedicated mode
 - If your website has a private network load balancer deployed behind the dedicated WAF instance, as shown in [Figure 13-17](#), unbind the EIP from the internet-facing load balancer and then bind the EIP to the private load balancer. In doing so, your website traffic will bypass WAF and directly go to the origin server.

Figure 13-17 Dedicated WAF instance deployment architecture (private network load balancers deployed behind dedicated WAF instances)



- If your website has no private network load balancer deployed behind the dedicated WAF instance, as shown in **Figure 13-18**, unbind the EIP from the dedicated WAF instance and then bind the EIP to the origin server. In doing so, your website traffic will bypass WAF and directly go to the origin server.

Figure 13-18 Dedicated WAF instance deployment architecture (no private network load balancer deployed behind dedicated WAF instances)



13.4 Service Interruption Check

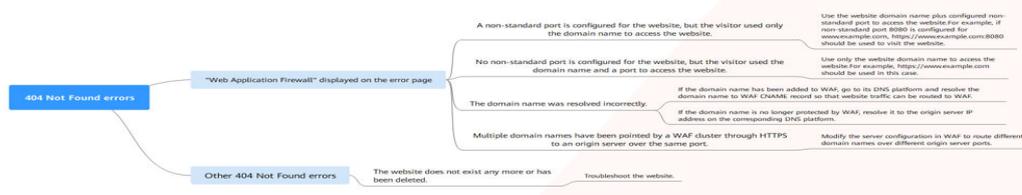
13.4.1 How Do I Troubleshoot 404/502/504 Errors?

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

404 Not Found Troubleshooting Process and Suggestions

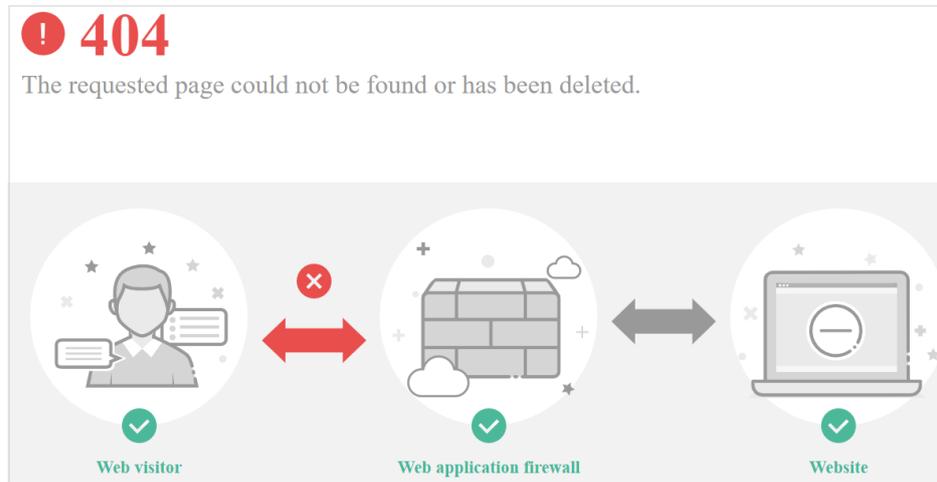
Refer to **Figure 13-19** to fix the 404 Not Found error occurred after your website is connected to WAF.

Figure 13-19 Troubleshooting for 404 Not Found error



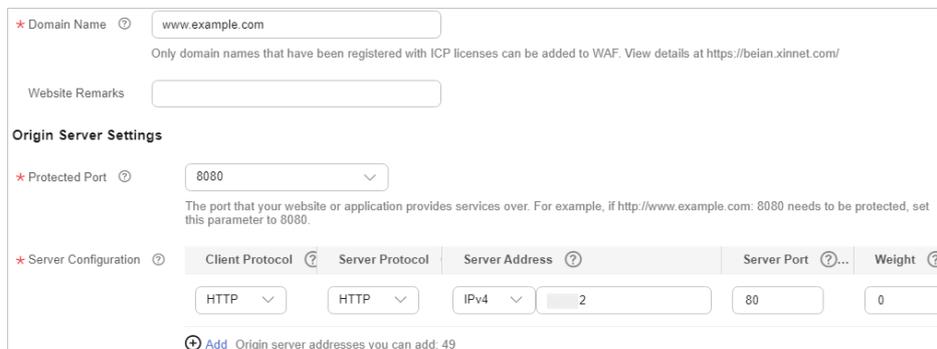
- If the page shown in **Figure 13-20** is displayed, the possible causes and solutions are as follows:

Figure 13-20 404 page



Cause 1: A non-standard port is configured when you add the domain name to WAF, but the visitors use the domain name and standard port or use only the domain name to access the website. For example, a non-standard port is configured as shown in **Figure 13-21**. A visitor uses `https://www.example.com` or `https://www.example.com:80` to access the website. As a result, 404 error page is displayed.

Figure 13-21 Configuration of a non-standard port



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

Cause 2: No non-standard port is configured when the domain name is added to WAF. The visitors use the domain name and a non-standard port or the non-standard port configured for origin server port to access the website. For example, access **`https://www.example.com:8080`** when the protection service shown in **Figure 13-22** is configured.

Figure 13-22 Non-standard port not configured

The screenshot shows a configuration page for a domain named 'www.example.com'. Under 'Origin Server Settings', the 'Protected Port' is set to 'Standard port'. Below this, there is a table for 'Server Configuration' with columns for Client Protocol, Server Protocol, Server Address, Server Port, and Weight. The current configuration shows HTTP for both protocols, IPv4 for the address, port 80, and a weight of 0. A note at the bottom indicates that 49 origin server addresses can be added.

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: Use only the domain name to access the website. For example, <https://www.example.com>.

Cause 3: The domain name is incorrectly resolved.

Solution:

- If the domain name has been added to WAF, resolve the domain name to WAF by referring to [Step 4: Modify the DNS Records of the Domain Name](#).
- If the domain name is no longer protected by WAF, resolve it to the origin server IP address on the DNS hosting platform.

Cause 4: If a WAF cluster pointed multiple domain names through HTTPS to an origin server over the same port, origin servers cannot tell which domain name a request originated from. This is because WAF uses persistent connections to forward requests to origin servers and Nginx identifies domain names based on Host and SNI. So, there might be a probability that requests destined for domain name A was mistakenly forwarded to domain name B, which causes 404 not found errors.

Solution: Modify the server configuration in WAF to route different domain names over different origin server ports.

- If the response page is not similar the one shown in [Figure 13-20](#), the possible causes and solutions are as follows:

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

Solution: Check the website.

502 Bad Gateway Troubleshooting Process and Solutions

Your website can be accessed normally after it is connected to WAF. However, after a period of time, the error code 502 is reported frequently. Refer to [Figure 13-23](#) to fix the issue.

Figure 13-23 Troubleshooting process for 502 Bad Gateway error

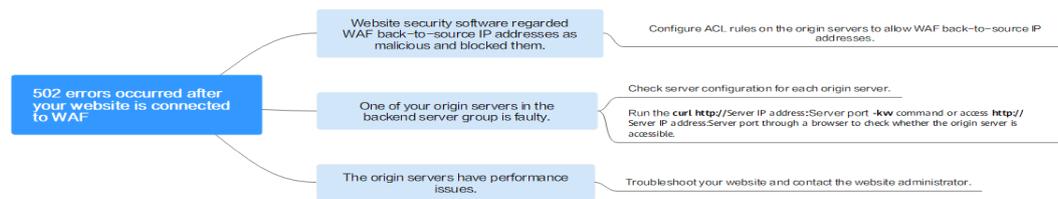


Table 13-6 Troubleshooting 502 Bad Gateway error

Possible Cause	Solution
Cause 1: Your website is using another security protection software. Such software considers WAF back-to-source IP addresses as malicious and blocks the requests forwarded by WAF.	Configure an access control policy on the origin server to whitelist the WAF IP addresses. <ul style="list-style-type: none"> • Cloud mode: See How Do I Whitelist IP Address Ranges of Cloud WAF? • Dedicated mode: See Whitelisting IP Addresses of Dedicated WAF Instances.
Cause 2: Multiple backend servers are configured for the website. However, one backend server is inaccessible.	Repeat Step 1 to Step 8 to ensure that all origin servers can be accessed.
Cause 3: Your website server may have performance issues.	Contact your website administrator to rectify the fault.

If one of your backend website servers is unreachable, perform the following steps to ensure that the website server configuration is correct.

NOTICE

It takes about two minutes for server information modification to take effect.

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Website Settings**.
- Step 5** In the **Protected Website** column, click the target domain name to go to the **Basic Information** page.

- Step 6** 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.

Figure 13-24 Server Configuration



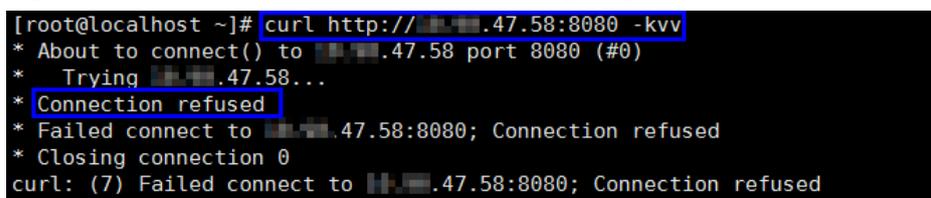
- Step 7** Check whether each origin server can be accessed properly.

- Run the following command on the server:
`curl http://xx.xx.xx.xx:yy -kvv`

 **NOTE**

- `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.
- 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 a Windows operating system. **curl** is installed along with other operating systems.

Figure 13-25 Command output for checking origin server



- If the command output indicates that the connection is normal, the website can be accessed.
- If the command output returns **connection refused**, the origin server is unreachable and website cannot be accessed. Go to **Step 8**.
- Enter `http://origin server address: origin server port` in the address box of the browser and press **Enter**.
 - If the website can be accessed, the website access is normal.
 - If the website cannot be accessed, the origin server is unreachable and the website cannot be accessed. Go to **Step 8**.

- Step 8** Check whether the origin server runs properly.

If not, restart it.

----End

504 Gateway Timeout Troubleshooting Process and Solutions

After you connect your website to WAF, the possibility of 504 gateway timeout errors rises as your website traffic increases. In some other cases, there might be a possibility of 504 gateway timeout error if the visitors access your website through origin server IP addresses. Refer to [Figure 13-26](#) to fix 504 gateway timeout errors.

Figure 13-26 Troubleshooting process for 504 Gateway Timeout errors



Table 13-7 Troubleshooting 504 Gateway Timeout errors

Possible Cause	Troubleshooting	Solution
<p>Cause 1: Backend server performance issues (such as too many connections or high CPU usage)</p>	<p>If the origin server performance is insufficient, check the origin server access logs and access traffic to analyze issues.</p>	<ul style="list-style-type: none"> ● Optimize the server configurations, including TCP network parameters and ulimit parameters. ● You are advised to add backend server groups or create new load balancers to support the increasing service workloads, if your website is connected to WAF in cloud mode. ● If you configure Client Protocol to HTTPS, to relieve burden on backend servers, configure HTTP for Server Protocol for WAF forwarding traffic to backend servers. For details, see Editing Server Information. ● Use CC attack protection rules to block malicious traffic.
<p>Cause 2</p> <ul style="list-style-type: none"> ● The WAF back-to-source IP addresses are not whitelisted or service port is not enabled in the security group. ● WAF back-to-source IP addresses are blocked by the firewall on the origin server. 	<p>Follow the solutions below for troubleshooting:</p> <ul style="list-style-type: none"> ● Check whether your origin server has security groups, firewalls, and security software deployed. ● Capture packets on the client and WAF, respectively, at the same time to check whether the origin server firewall proactively discards packets of the persistent connection to WAF. 	<ul style="list-style-type: none"> ● Configure an access control policy on the origin server to whitelist WAF IP addresses. ● Disable other firewalls and security software on origin servers.

Possible Cause	Troubleshooting	Solution
<p>Cause 3: Connection timeout and read timeout</p> <p>NOTE</p> <ul style="list-style-type: none"> • A 504 error occurs if the origin server is too slow to respond, for example, a slow response to database queries, a long upload time for a large file, or a faulty origin server. • The timeout for WAF to forward traffic to an origin server is 60s or 180s. A 504 error occurs if WAF fails to forward traffic within the configured timeout. 	<p>Troubleshooting methods:</p> <ul style="list-style-type: none"> • Bypass WAF and directly access the origin server and then check the response time. • View the origin server response time in access logs stored in Log Tank Service (LTS). • Bypass WAF, test the file upload function, and check the file size. 	<ul style="list-style-type: none"> • Database queries are slow. <ul style="list-style-type: none"> – 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. <ul style="list-style-type: none"> – 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 origin server is faulty. Check whether the origin server works properly.

Possible Cause	Troubleshooting	Solution
Cause 4: The bandwidth of the origin server is insufficient. When the access traffic is heavy, the origin server cannot handle all the traffic with its current bandwidth.	<p>Troubleshooting methods:</p> <ul style="list-style-type: none"> If you have a layer-7 load balancer deployed in the rear of WAF, you can query 504 logs on the load balancer. If you have a layer-4 load balancer deployed in the rear of WAF, you can query logs in the Traffic exceeded the bandwidth threshold field on the load balancer. If you have an EIP bound to the backend WAF instances, check the EIP traffic monitoring when 504 errors rise to the peak volume. 	Increase the bandwidth of the origin server.

Create a load balancer. Use the EIP of the load balancer as the IP address of the origin server and connect the EIP to WAF.

NOTICE

It takes about two minutes for server information modification to take effect.

Step 1 Create a shared load balancer.

Step 2 Log in to the management console.

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

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

Step 5 In the **Domain Name** column, click the domain name. Its information is displayed.

Step 6 In the **Server Information** area, click . On the displayed page, click **Add**.

Figure 13-27 Server Configuration



Step 7 Set the **Server Address** to the EIP bound to the load balancer.

Step 8 Click **OK**.

----End

13.4.2 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.

Troubleshooting and Solutions for Cloud WAF Instances

Refer to [Figure 13-28](#) and [Table 13-8](#) to fix connection failures for websites protected in cloud mode.

Figure 13-28 Troubleshooting for Cloud WAF

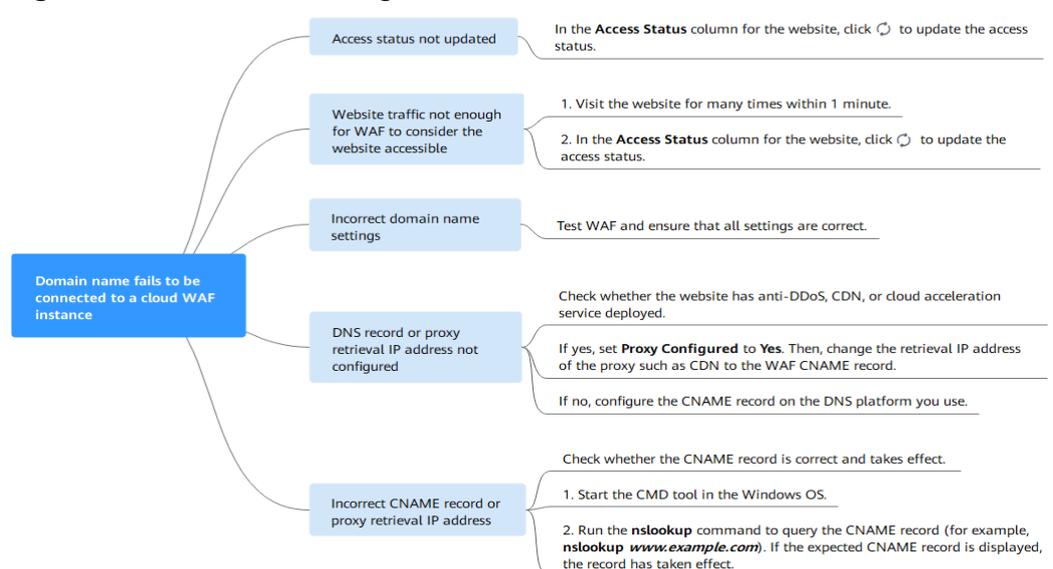


Table 13-8 Solutions for failures of WAF instances

Possible Cause	Solution
Cause 1: Access Status of Protected Website not updated	In the Access Status column for the protected website, click  to update the status.
Cause 2: Website access traffic not enough for WAF to consider the website accessible NOTICE After you connect a website to WAF, the website is considered accessible only when WAF detects at least 20 requests to the website within 5 minutes.	<ol style="list-style-type: none">1. Access the protected website for many times within 1 minute.2. In the Access Status column for the website, click  to update the status.

Possible Cause	Solution
<p>Cause 3: Incorrect domain name settings</p>	<p>NOTICE WAF can protect the website using the following types of domain names:</p> <ul style="list-style-type: none"> • Top-level domain names, for example, example.com • Single domain names/Second-level domains, for example, www.example.com • Wildcard domain names, for example, *.example.com <p>Domain names example.com and www.example.com are different. Ensure that correct domain names are added to WAF.</p> <p>Perform the following steps to ensure that the domain name settings are correct.</p> <ol style="list-style-type: none"> 1. In Windows OSs, choose Start > Run. Then enter cmd and press Enter. 2. Ping the CNAME record of the domain name to obtain the WAF back-to-source IP address. 3. Use a text editor to open the hosts file. Generally, the hosts file is stored in the C:\Windows\System32\drivers\etc\ directory. 4. Add a record into the hosts file in the format of DomainName WAF back-to-source IP address. 5. Save the hosts file after the record is added. In the CLI, run the ping Domain name added to WAF command, for example, ping www.example.com. If the WAF back-to-source IP address in 2 is displayed in the command output, the domain name settings are correct. <p>If there are incorrect domain name settings, remove the</p>

Possible Cause	Solution
	domain name from WAF and add it to WAF again.
Cause 4: DNS record or the back-to-source IP addresses of proxies not configured	<p>Check whether the website connected to WAF uses proxies such as advanced anti-DDoS, CDN, and cloud acceleration service.</p> <ul style="list-style-type: none"> ● Yes. <ul style="list-style-type: none"> - Change the back-to-source IP address of the proxy such as CDN to the CNAME record of WAF. - (Optional) Add a WAF subdomain name and TXT record at your DNS provider. ● If no, contact your DNS service provider to configure a CNAME record for the domain name.
Cause 5: Incorrect DNS record or proxy back-to-source address	<p>Perform the following steps to check whether the domain name CNAME record takes effect:</p> <ol style="list-style-type: none"> 1. In Windows OSs, choose Start > Run. Then enter cmd and press Enter. 2. Run a nslookup command to query the CNAME record. If the command output displays the CNAME record of WAF, the record takes effect. <p>Using <code>www.example.com</code> as an example, the output is as follows:</p> <pre>nslookup www.example.com</pre>

Troubleshooting and Solutions for Dedicated WAF

Refer to [Figure 13-29](#) and [Table 13-9](#) to fix connection failures.

Figure 13-29 Troubleshooting for dedicated mode

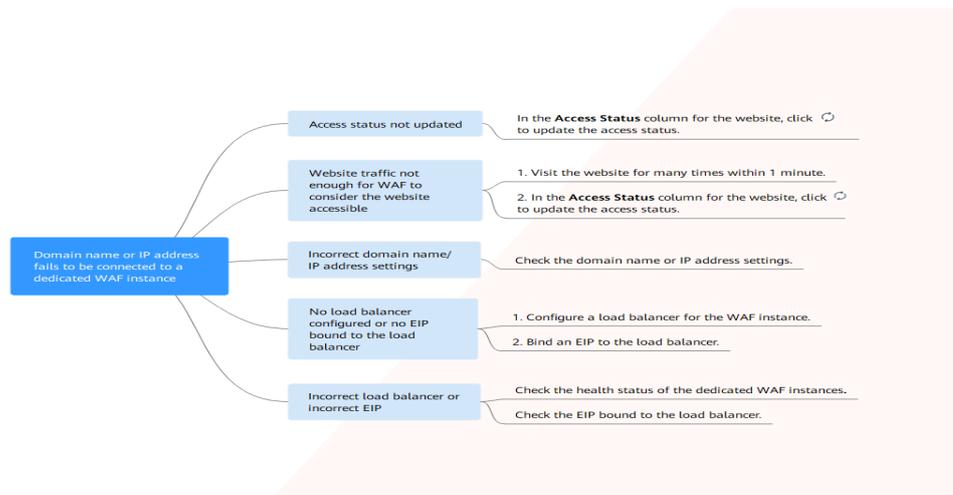


Table 13-9 Solutions for dedicated mode

Possible Cause	Solution
Cause 1: Access Status for Domain Name/IP Address not updated	In the Access Status column for the website, click  to update the status.
Cause 2: Website access traffic not enough for WAF to consider the website accessible NOTICE After you connect a website to WAF, the website is considered accessible only when WAF detects at least 20 requests to the website within 5 minutes.	<ol style="list-style-type: none"> 1. Access the protected website many times within 1 minute. 2. In the Access Status column for the website, click  to update the status.
Cause 3: Incorrect domain name or IP address settings	<p>Check domain name or IP address settings.</p> <p>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.</p>
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	<ol style="list-style-type: none"> 1. Configure a load balancer for dedicated WAF instances by referring to Configuring a Load Balancer. 2. Bind an EIP to a Load Balancer.

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

13.4.3 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.

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 13-10](#). 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.

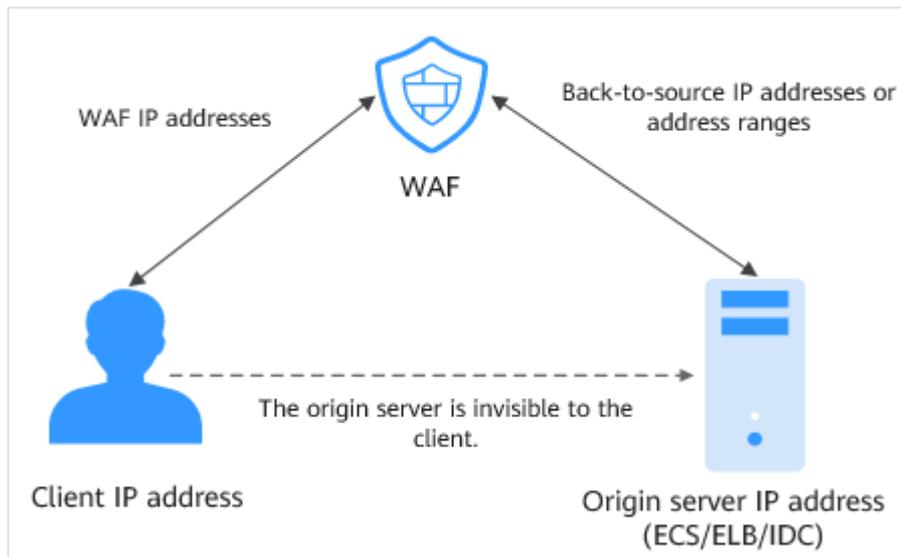
Table 13-10 Handling false alarms

Type of Hit Rule	Hit Rule	Handling Method
WAF built-in protection rules	<ul style="list-style-type: none"> • Basic web protection rules Basic web protection defends against common web attacks, such as SQL injection, XSS attacks, remote buffer overflow attacks, file inclusion, Bash vulnerability exploits, remote command execution, directory traversal, sensitive file access, and command and code injections. Basic web protection also detects web shells and evasion attacks. • Feature-based anti-crawler protection Feature-based anti-crawler identifies and blocks crawler behavior from search engines, scanners, script tools, and other crawlers. 	In the row containing the attack event, click Handle as False Alarm in the Operation column. For details, see Handling False Alarms .
Custom protection rules	<ul style="list-style-type: none"> • CC attack protection rules • Precise protection rules • Blacklist and whitelist rules • Geolocation access control rules • Web tamper protection rules • JavaScript anti-crawler protection • Information leakage prevention rules • Data masking rules 	Go to the page displaying the hit rule and delete it.
Other	<p>Invalid access requests</p> <p>NOTE If either of the following cases, WAF blocks the access request as an invalid request:</p> <ul style="list-style-type: none"> • When form-data is used for POST or PUT requests, the number of parameters in a form exceeds 8,192. • The URI contains more than 2,048 parameters. • The number of headers exceeds 512. 	Allow the blocked requests by referring to Configuring Custom Precise Protection Rules . The Handle as False Alarm button is grayed out for events that are generated against a precise protection rule.

NOTE

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

Figure 13-31 Back-to-source IP address



WAF Back-to-Source IP Address Check Mechanism

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

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

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

NOTE

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

Procedure

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

- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane, choose **Website Settings**.
- Step 5** Above the website list, click **WAF Back-to-Source IP Addresses**.
- Step 6** In the displayed dialog box, click **Copy** to copy all the addresses.

Figure 13-32 WAF Back-to-Source IP Addresses dialog box



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

----End

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

- The default timeout for connections from a browser to WAF is 120 seconds. The value varies depending on your browser settings and cannot be changed on the WAF console.
- The default timeout duration for connections between WAF and your origin server is 30 seconds. You can customize a timeout duration on the WAF console.

On the **Basic Information** page, enable **Timeout Settings** and click  . Then, specify **WAF-to-Server connection timeout (s)**, **Read timeout (s)**, and **Write timeout (s)** and click  to save settings.

13.4.7 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). [Figure 13-33](#) shows the finished server settings.

Figure 13-33 Example configuration

Client Protocol	Server Protocol	Server Address	Server Port	Weight
HTTP	HTTP	IPv4 9	80	1
HTTPS	HTTPS	IPv4 3	443	1

⊕ Add Origin server addresses you can add: 18

Your domain name supports the client protocol HTTPS using the certificate

International Existing certificates

[Import New Certificate](#)

You have modified server configurations. To apply the modifications, click OK. Otherwise, click Cancel.

Confirm Cancel

13.4.8 Why Are HTTPS Requests Denied on Some Mobile Phones?

If your visitors receive a page similar to the one in [Figure 13-34](#) 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 13-34 Access failed



13.4.9 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.

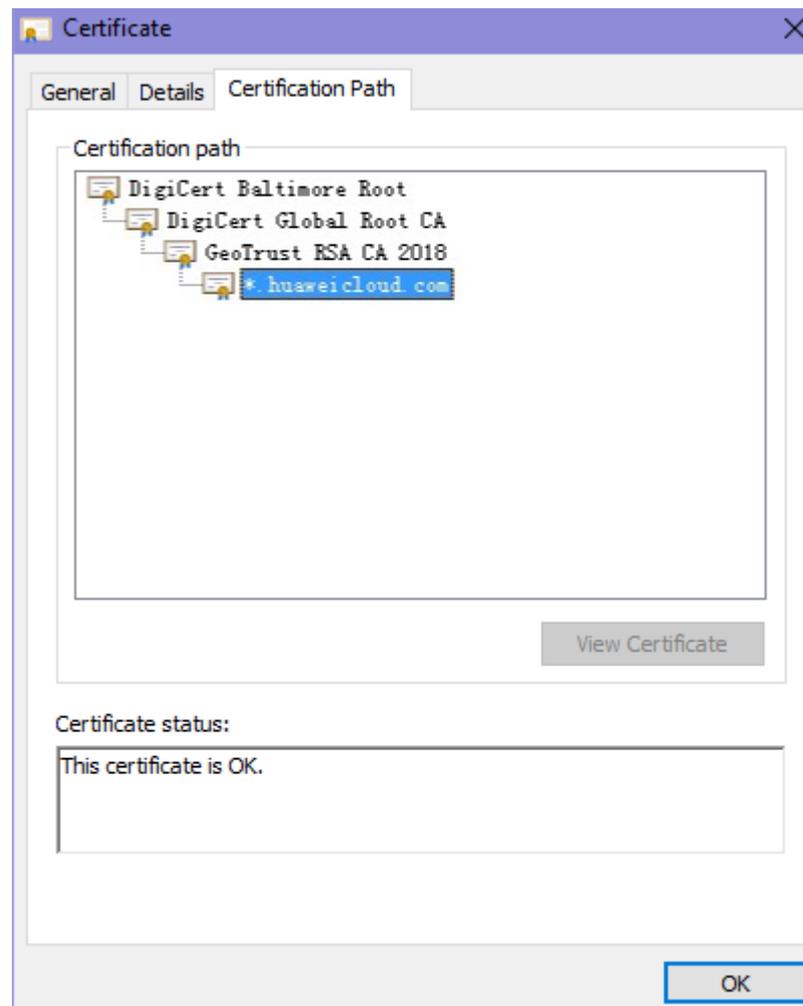
Use either of the following methods to fix it:

- 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 13-35** shows an example.

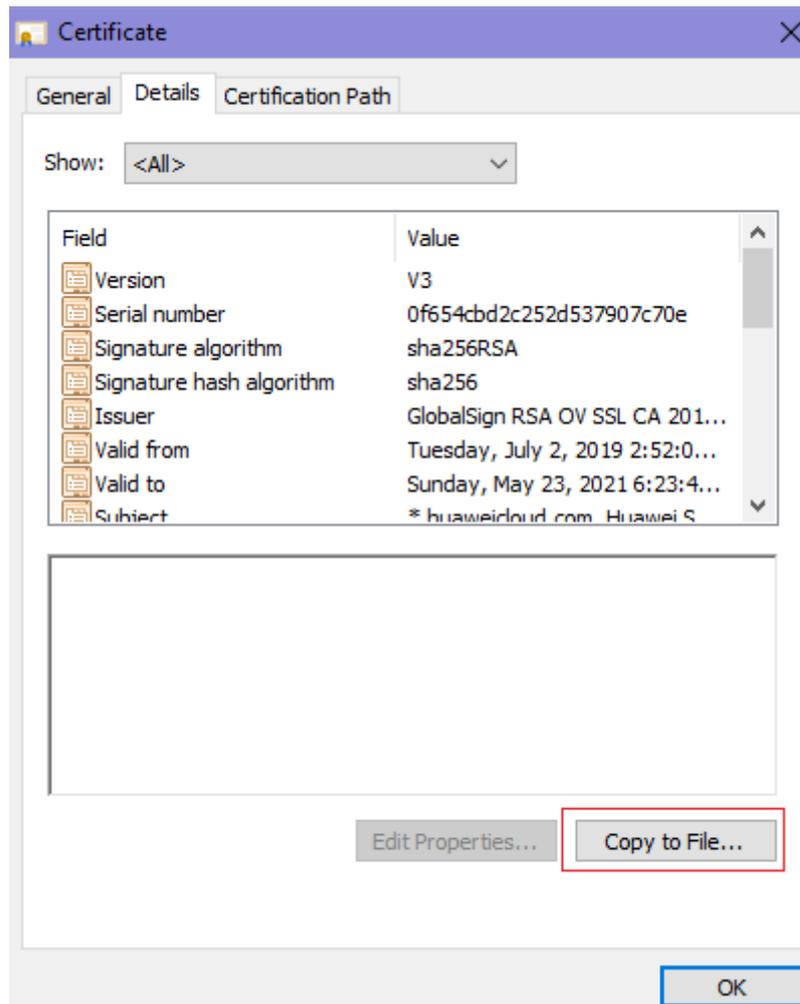
Figure 13-35 Viewing the certificate chain



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

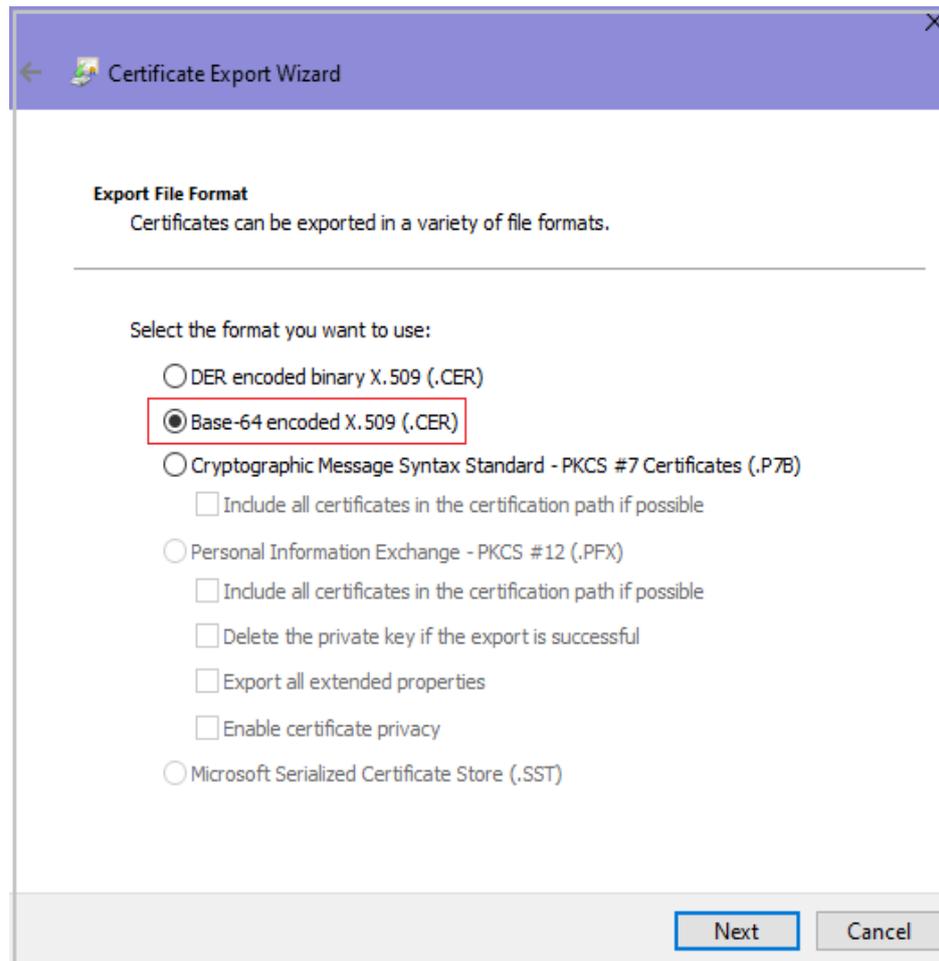
1. Select the certificate name and click the **Details** tab. [Figure 13-36](#) shows an example.

Figure 13-36 Details



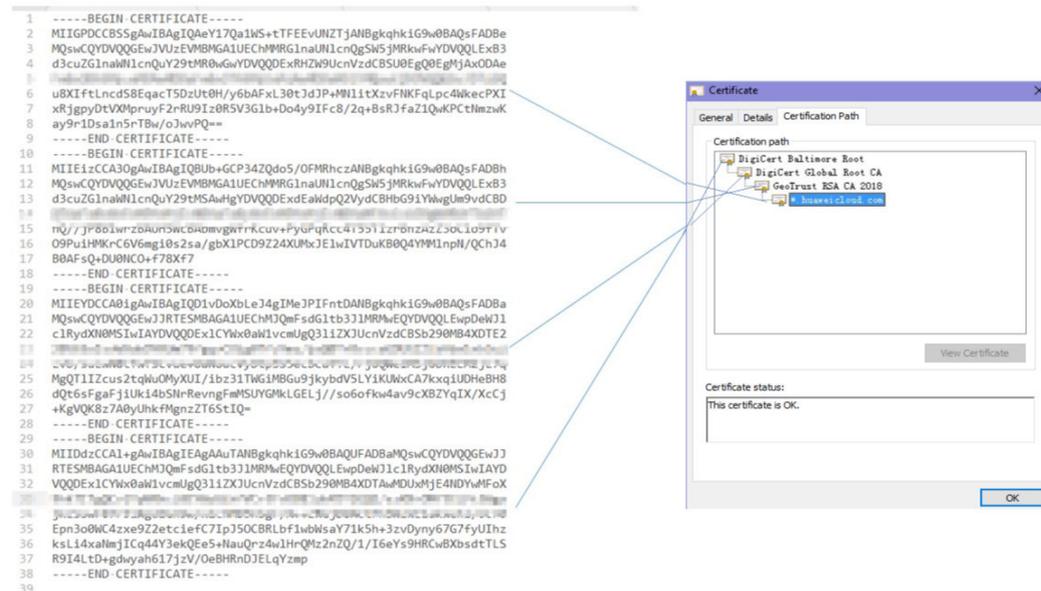
2. Click **Copy to File**, and then click **Next** as prompted.
3. Select **Base-64 encoded X.509 (.CER)** and click **Next**. [Figure 13-37](#) shows an example.

Figure 13-37 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 13-38](#).

Figure 13-38 Certificate rebuilding



Step 5 Upload the certificate again.

----End

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

Related Operations

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

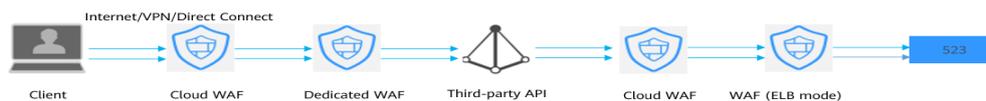
13.4.11 Why Am I Seeing Error Code 418?

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.

13.4.12 Why Am I Seeing Error Code 523?

If a request goes through WAF over four times, WAF will block the request and return error code 523 to avoid endless loops. If error code 523 is returned for your website requests, check how many WAF instances you are using.



Cause 1: A website is connected to more than four WAF instances.

Error code 523 will return if a website has been connected to different types of WAF instances more than 4 times.

Solution

Route website traffic to bypass redundant WAF instances.

- Step 1** Log in to the WAF management console.
- Step 2** In the navigation pane on the left, choose **Website Settings**.
- Step 3** Locate the website for which 523 error code is returned, retain one configuration, and delete the website from redundant WAF instances. For details, see [Deleting a Protected Website from WAF](#).

To prevent service interruptions due to such deletions, perform the following operations before removing a website from WAF:

Cloud mode: Go to your DNS provider and resolve your domain name to the IP address of the origin server. Otherwise, the traffic to your domain name cannot be routed to the origin server.

Dedicated mode: Remove redundant WAF instances from the backend server group of the load balancer so that no requests are forwarding to those WAF instances. .

----End

Cause 2: A Third-party Interface That Uses WAF Was Called

When a request is forwarded to the third-party API, header and cookie are forwarded without being changed. Only the host is modified. This makes WAF count the requests without clearing historical records.

Solution

Modify the header field in the reverse proxy request. The operations are as follows:

NOTICE

This method can be used only when Nginx is deployed after WAF on the user traffic link.

Step 1 Use **proxy_set_header** to redefine the request header sent to the proxy server. Run the following command to open the Nginx configuration file:

(The following command is used when Nginx is installed in the **/opt/nginx/** directory. Change the directory based on your situation.)

```
vi /opt/nginx/conf/nginx.conf
```

Step 2 Add **proxy_set_header X-CloudWAF-Traffic-Tag 0** to the Nginx configuration file. The following is an example:

```
location ^~/test/ {  
    .....  
    proxy_set_header Host      $proxy_host;  
    proxy_set_header X-CloudWAF-Traffic-Tag 0;  
    .....  
    proxy_pass http://x.x.x.x;  
}
```

----End

Cause 3: Origin Server IP address Was Mistakenly Set to an IP Address of WAF or A Proxy in Front of WAF

If the origin server address is mistakenly set to the back-to-source IP address of WAF or an IP address of the proxy in front of WAF, the website requests go to an endless loop and error code 523 is returned.

Solution

Check the origin server configurations and enter a correct origin server address.

13.4.13 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.

13.4.14 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?](#)

13.4.15 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

13.4.16 Why Am I Seeing Error Code 414 Request-URI Too Large?

Symptoms

After a protected website is connected to WAF, the website is inaccessible and the error message "414 Request-URI Too Large" is displayed, as shown in [Figure 13-39](#).

Figure 13-39 Error Code 414 Request-URI Too Large



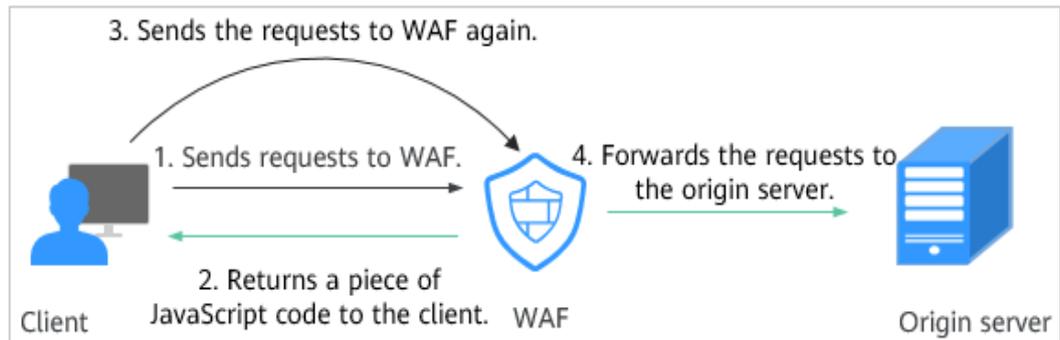
Possible Causes

The client browser cannot parse JavaScript. In this situation, the client browser caches the page that contains the JavaScript code returned by WAF. Each time the protected website is requested, the cached page is accessed. WAF then verifies that the access request is from an invalid browser or crawler. The access request verification fails. As a result, an infinite loop occurs, the URI length exceeds the browser limit, and the website becomes inaccessible.

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

the website, triggered by the received JavaScript code, the client will automatically send the request to WAF again. WAF then forwards the request to the origin server. This process is called JavaScript verification. **Figure 13-40** shows how JavaScript verification works.

Figure 13-40 JavaScript anti-crawler detection process

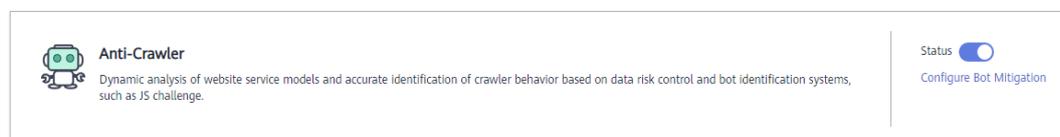


Handling Suggestions

Disable the JavaScript anti-crawler protection by performing the following steps:

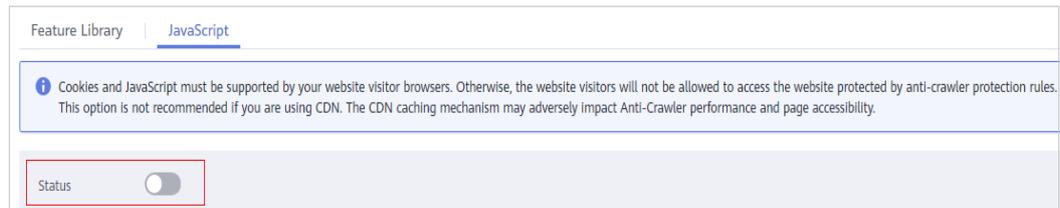
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** Click the name of the target policy to go to the protection configuration page.
- Step 6** In the **Anti-Crawler** configuration area, click **Configure Bot Mitigation**.

Figure 13-41 Anti-Crawler configuration area



- Step 7** Click the **JavaScript** tab and disable the JavaScript anti-crawler protection. Its status changes to .

Figure 13-42 Disabling JavaScript anti-crawler protection



----End

13.4.17 What Do I Do If the Protocol Is Not Supported and the Client and Server Do Not Support Common SSL Protocol Versions or Cipher Suites?

Symptom

After a domain name is connected to WAF, the website cannot be accessed. A message is displayed, indicating that the protocol is not supported. The client and server do not support common SSL protocol versions or cipher suites.

Solution

Select the default cipher suite for **Cipher Suite** in the **TLS Configuration** dialog box. For details, see [Configuring PCI DSS/3DS Certification Check and TLS Version](#).

13.4.18 Why Cannot I Access the Dedicated Engine Page?

Symptom

Error message "Failed to request IAM. Please check the current user's IAM permissions." is displayed when a user attempted to access the **Dedicate Engine** page under **Instance Management**.

Possible Cause

The **IAM ReadOnly** permission is not granted to the login account.

Solution

Assign the **IAM ReadOnly** permission to your account.

13.4.19 Why Is the Bar Mitzvah Attack on SSL/TLS Detected?

The bar mitzvah attack is an attack on SSL/TLS protocols that exploits a vulnerability in the RC4 cryptographic algorithm. This vulnerability can disclose ciphertext in SSL/TLS encrypted traffic in some cases, such as passwords, credit card data, or other privacy data, to hackers.

Solution

To solve this problem, you can set the minimum TLS version to TLS v1.2 and cipher suite to cipher suite 2.

13.5 Protection Rule Configuration

13.5.1 Basic Web Protection

13.5.1.1 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**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** Click the name of the target policy to go to the protection configuration page.
- Step 6** In the **Basic Web Protection** configuration area, set **Mode** to **Block**.

NOTICE

Log only and **Block** are merely modes of basic web protection. CC attack protection and precise protection have their own protective actions.

----End

13.5.1.2 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 13-11](#).

Table 13-11 Protection levels

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

13.5.2 CC Attack Protection Rules

13.5.2.1 What Is the Peak Rate of CC Attack Protection?

It depends on the WAF edition you are using. For details, see [Table 13-12](#).

Table 13-12 Applicable service scales

Service Scale	Dedicated Mode
Peak rate of normal service requests	<p>The following lists the specifications of a single instance.</p> <ul style="list-style-type: none"> ● Specifications: WI-500. Referenced performance: <ul style="list-style-type: none"> - HTTP services - Recommended QPS: 5,000. Maximum QPS: 10,000. - HTTPS services - Recommended QPS: 4,000. Maximum QPS: 8,000. - WebSocket service - Maximum concurrent connections: 5,000 - Maximum WAF-to-server persistent connections: 60,000 ● Specifications: WI-100. Referenced performance: <ul style="list-style-type: none"> - HTTP services - Recommended QPS: 1,000. Maximum QPS: 2,000. - HTTPS services - Recommended QPS: 800. Maximum QPS: 1,600 - WebSocket service - Maximum concurrent connections: 1,000 - Maximum WAF-to-server persistent connections: 60,000 <p>NOTICE Maximum QPS values are for reference only. They may vary depending on your businesses. The real-world QPS is related to the request size and the type and quantity of protection rules you customize.</p>
Peak rate of CC attack protection	<ul style="list-style-type: none"> ● Specifications: WI-500. Referenced performance: Maximum QPS: 20,000 ● Specifications: WI-100. Referenced performance: Maximum QPS: 4,000

13.5.2.2 How Do I Configure a CC Attack Protection Rule?

When a service interface is under an HTTP flood attack, you can set a CC attack protection rule on the WAF console to relieve service pressure.

WAF provides the following settings for a CC attack protection rule:

- Number of requests allowed from a web visitor in a specified period
- Identification of web visitors based on the IP address, cookie, or referer field.
- Action when the maximum limit is reached, such as **Block** or **Verification code**

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

13.5.2.3 When Is Cookie Used to Identify Users?

During the configuration of a CC attack protection rule, if IP addresses cannot identify users precisely, for example, when many users share an egress IP address, use Cookie to identify users.

If the cookie contains key values, such as the session value, of users, the key value can be used as the basis for identifying users.

13.5.2.4 What Are the Differences Between Rate Limit and Allowable Frequency in a CC Rule?

In a CC attack protection rule, **Rate Limit** specifies the maximum requests that a website visitor can initiate within the configured period. If the configured rate limit has been reached, WAF will respond according to the protective action configured. For example, if you configure **Rate Limit** to **10 requests** within **60 seconds** and **Protective Action** to **Block**, a maximum of 10 requests are allowed within 60 seconds. Once the website visitor initiates more than 10 requests within 60 seconds, WAF directly blocks the visitor from accessing the requested URL.

If you select **Advanced** for **Mode** and **Block dynamically** for **Protective Action**, configure **Rate Limit** and **Allowable Frequency**.

WAF blocks requests that trigger the rule based on **Rate Limit** first. Then, in the following rate limit period, WAF blocks requests that trigger the rule based on **Allowable Frequency** you configured. If blocking is triggered and **Allowable Frequency** is **0**, all requests that meet the rule conditions in the next period are blocked.

Differences

- The rate limit period of **Allowable Frequency** is the same as that of **Rate Limit**.
- **Allowable Frequency** is lower than or equal to **Rate Limit**, and **Allowable Frequency** can be **0**.

13.5.3 Precise Protection rules

13.5.3.1 Can a Precise Protection Rule Take Effect in a Specified Period?

Precise access protection rules can take effect in a specified period.

You can set precise protection rules to filter access requests based on a combination of common HTTP fields (such as IP address, path, referer, user agent, and params) to allow or block the requests that match the conditions.

13.5.3.2 Can a Path Containing # Be Matched in a Precise Protection Rule?

The path added to a precise protection rule cannot contain special characters ("<>*&# %\?").

The number sign (#) is a client parameter. Parameters following the number sign (#) are not transferred to the server for web page location. WAF and browsers do not consider the content following the number sign (#) as URL parameters. Therefore, the parameters cannot be obtained.

Add Precise Protection Rule

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

* Rule Name

Rule Description

* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/#/user/login

Warning: The value contains a maximum of 2,048 characters and cannot contain the following special characters: "<>&*#%?"

13.5.3.3 How Can I Allow Access from .js Files?

You can configure a precise protection rule in WAF to allow access from paths with the suffix .js. The configuration is as follows:

Add Precise Protection Rule

* Rule Name

Rule Description

* Condition List

Field	Subfield	Logic	Content
Path	--	Suffix is	.js

[Add Reference Table](#)

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

* Protective Action

13.5.4 IP Address Blacklist and Whitelist

13.5.4.1 Can I Batch Add IP Addresses to a Blacklist or Whitelist Rule?

Yes. You can select an address group when configuring a whitelist or blacklist rule. In this way, requests from those IP addresses included in the address group will be blocked, allowed, or logged only. You can also configure a blacklist or whitelist rule for each IP address or IP address range.

13.5.4.2 Can I Import or Export a Blacklist or Whitelist into or from WAF?

WAF supports importing of IP address blacklist or whitelist. To do so, select **Address group** for **IP Address/Range/Group** when you are adding a blacklist or whitelist rule. WAF does not support exporting of IP address blacklists and whitelists.

13.5.4.3 How Do I Block Abnormal IP Addresses?

You can blacklist an abnormal IP address. WAF directly blocks all the requests from the blacklisted IP address.

To blacklist an IP address, perform the following steps:

Step 1 Log in to the management console.

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

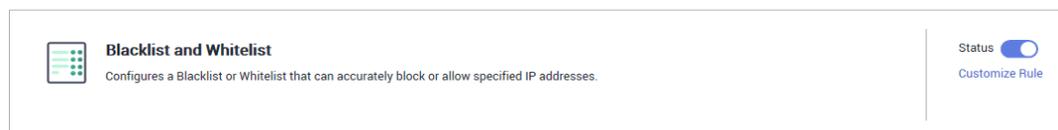
Step 3 Click  in the upper left corner and choose **Web Application Firewall** under **Security**.

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

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

Step 6 In the **Blacklist and Whitelist** configuration area, change **Status** as needed and click **Customize Rule**.

Figure 13-43 Blacklist and Whitelist configuration area



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

Step 8 In the displayed dialog box, add a blacklist or whitelist rule.

 **NOTE**

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

Figure 13-44 Adding a blacklist or whitelist rule

Add Blacklist or Whitelist Rule [X]

* Rule Name

* IP Address/Range/Group IP address/range Address group

* IP Address/Range

* Protective Action

Known Attack Source [Add Known Attack Source Rule](#)

Rule Description

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.

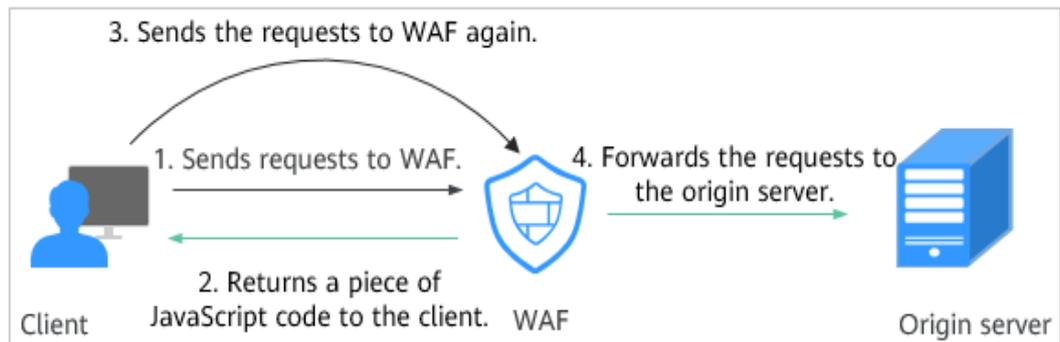
----End

13.5.5 Anti-Crawler Protection

13.5.5.1 Why Is the Requested Page Unable to Load After JavaScript Anti-Crawler Is Enabled?

After JavaScript anti-crawler is enabled, WAF returns a piece of JavaScript code to the client when the client sends a request. If the client sends a normal request to the website, triggered by the received JavaScript code, the client will automatically send the request to WAF again. WAF then forwards the request to the origin server. This process is called JavaScript verification. [Figure 13-45](#) shows how JavaScript verification works.

Figure 13-45 JavaScript anti-crawler detection process



NOTICE

- To enable the JavaScript anti-crawler protection, the browser on the client must have JavaScript and cookies enabled.
- If the client does not meet the preceding requirements, only steps 1 and 2 can be performed. In this case, the client request fails to obtain the page.

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

13.5.5.2 Is There Any Impact on Website Loading Speed If Other Crawler Check in Anti-Crawler Is Enabled?

If you have enabled **Other** when you configure **Feature Library** of anti-crawler protection, WAF detects crawlers for various purposes, such as website monitoring, access proxy, and web page analysis. Enabling this option does not affect web page visits or the web page browsing speed.

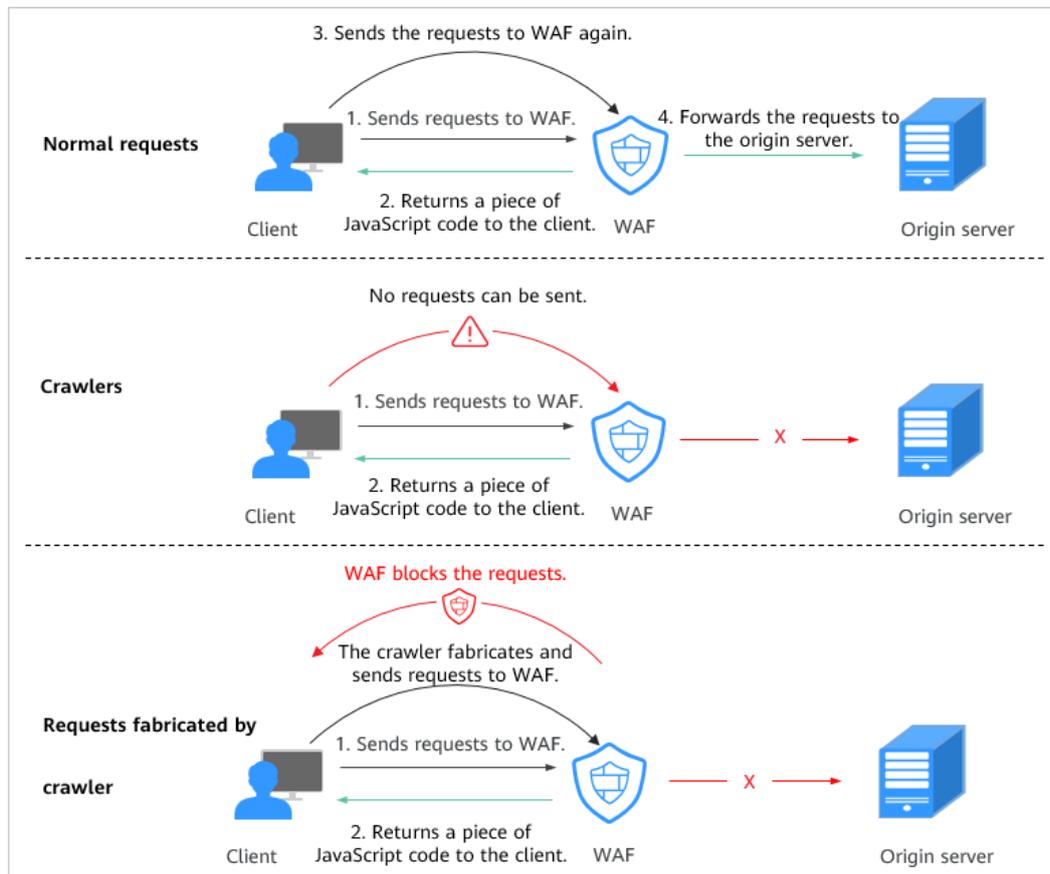
Figure 13-46 Enabling Other



13.5.5.3 How Does JavaScript Anti-Crawler Detection Work?

Figure 13-47 shows how JavaScript anti-crawler detection works, which includes JavaScript challenges (step 1 and step 2) and JavaScript authentication (step 3).

Figure 13-47 JavaScript Anti-Crawler protection process

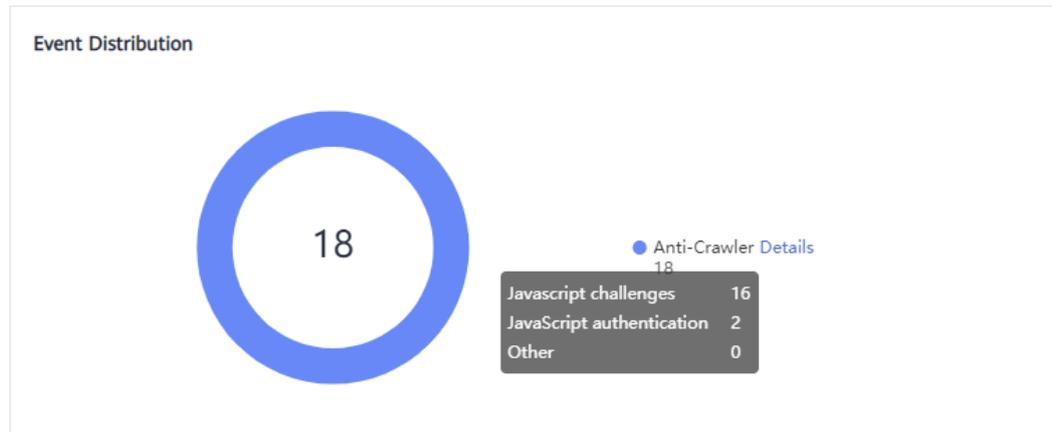


After JavaScript anti-crawler is enabled, WAF returns a piece of JavaScript code to the client when the client sends a request.

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

By collecting statistics on the number of JavaScript challenge and authentication responses, the system calculates how many requests the JavaScript anti-crawler defends. As shown in [Figure 13-48](#), the JavaScript anti-crawler logs 18 events, 16 of which are JavaScript challenge responses, 2 of which are JavaScript authentication responses. The number of **Other** is the WAF authentication requests fabricated by the crawler.

Figure 13-48 Parameters of a JavaScript anti-crawler protection rule



NOTICE

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

13.5.6 Others

13.5.6.1 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.

13.5.6.2 How Do I Allow Requests from Only IP Addresses in a Specified Geographical Region?

If you allow only IP addresses in a region to access the protected domain name, for example, only IP addresses from **Australia** can access the protected domain name, take the following steps:

 **NOTE**

Geolocation access control rules have higher priority than built-in WAF rules. If you configure a geolocation access control rule to allow IP addresses from a certain location, WAF then forwards traffic from those IP addresses without performing basic web protection checks.

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

Figure 13-49 Selecting Allow for Protective Action

Add Geolocation Access Control Rule

*** Geolocation**

Inside China (0) Select All

<input type="checkbox"/> Beijing	<input type="checkbox"/> Shanghai	<input type="checkbox"/> Tianjin	<input type="checkbox"/> Chongqing
<input type="checkbox"/> Guangdong	<input type="checkbox"/> Zhejiang	<input type="checkbox"/> Jiangsu	<input type="checkbox"/> Anhui
<input type="checkbox"/> Fujian	<input type="checkbox"/> Gansu	<input type="checkbox"/> Guangxi	<input type="checkbox"/> Guizhou
<input type="checkbox"/> Henan	<input type="checkbox"/> Hubei	<input type="checkbox"/> Hebei	<input type="checkbox"/> Hainan
<input type="checkbox"/> Hong Kong	<input type="checkbox"/> Heilongjiang	<input type="checkbox"/> Hunan	<input type="checkbox"/> Jilin
<input type="checkbox"/> Jiangxi	<input type="checkbox"/> Liaoning	<input type="checkbox"/> Macao	<input type="checkbox"/> Inner Mongolia
<input type="checkbox"/> Ningxia	<input type="checkbox"/> Qinghai	<input type="checkbox"/> Sichuan	<input type="checkbox"/> Shandong
<input type="checkbox"/> Shaanxi	<input type="checkbox"/> Shanxi	<input type="checkbox"/> Taiwan	<input type="checkbox"/> Sinkiang
<input type="checkbox"/> Tibet	<input type="checkbox"/> Yunnan		

Outside China (1)

*** Protective Action**

Step 2 Configure a precise protection rule to block all requests.

Figure 13-50 Blocking all access requests

Add Precise Protection Rule

Restrictions and precautions vary by mode. ?

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

*** Rule Name**

Rule Description

*** Condition List**

Field	Subfield	Logic	Content
Path	-	Include	/

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

*** Protective Action**

----End

13.5.6.3 What Working Modes and Protection Mechanisms Does WAF Have?

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

WAF supports the following working modes:

- Enabled
- Suspended
- Bypassed

NOTICE

- If a proxy is used for the website that is deployed in **Cloud mode** before it is connected to WAF, the WAF instance cannot be switched to the **Bypassed** mode.
 - The **Bypassed** mode is unavailable for websites deployed in **Dedicated mode**.
-

[Table 13-13](#) describes the protection mechanism.

Table 13-13 Supported protection mechanism

Protection Rule	Protective Action
Basic web protection rules	<ul style="list-style-type: none"> • Block • Log only
CC attack protection rules	<ul style="list-style-type: none"> • Verification code • Block • Block dynamically • Log only
Precise protection rules	<ul style="list-style-type: none"> • Block • Allow • Log only
Blacklist and whitelist rules	<ul style="list-style-type: none"> • Block • Allow • Log only
Geolocation access control rules	<ul style="list-style-type: none"> • Block • Allow • Log only

Protection Rule	Protective Action
Website anti-crawler protection	Protective actions for feature-based anti-crawler rules: <ul style="list-style-type: none"> • Block • Log only

13.5.6.4 What Types of Protection Rules Does WAF Support?

Table 13-14 lists all protection rules you can use in WAF.

Table 13-14 Configurable protection rules

Protection Rule	Description
Basic web protection rules	With an extensive reputation database, WAF defends against Open Web Application Security Project (OWASP) top 10 threats, and detects and blocks threats, such as malicious scanners, IP addresses, and web shells.
CC attack protection rules	CC attack protection rules can be customized to restrict access to a specific URL on your website based on a unique IP address, cookie, or referer field, mitigating CC attacks.
Precise protection rules	WAF allows you to customize protection rules by combining HTTP headers, cookies, URLs, request parameters, and client IP addresses.
Blacklist and whitelist rules	You can configure blacklist and whitelist rules to block, log only, or allow access requests from specified IP addresses.
Known attack source rules	These rules can block the IP addresses from which blocked malicious requests originate. These rules are dependent on other rules.
Geolocation access control rules	You can customize these rules to allow or block requests from a specific country or region.
Web tamper protection rules	You can configure these rules to prevent a static web page from being tampered with.
Website anti-crawler protection	This function dynamically analyzes website service models and accurately identifies crawler behavior based on data risk control and bot identification systems, such as JS Challenge.

Protection Rule	Description
Information leakage prevention rules	<p>You can add two types of information leakage prevention rules.</p> <ul style="list-style-type: none"> • Sensitive information filtering: prevents disclosure of sensitive information (such as ID numbers, phone numbers, and email addresses). • Response code interception: blocks the specified HTTP status codes.
Global protection whitelist rules	This function ignores certain attack detection rules for specific requests.
Data masking rules	You can configure data masking rules to prevent sensitive data such as passwords from being displayed in event logs.

13.5.6.5 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.

13.5.6.6 How Do I Allow Only Specified IP Addresses to Access Protected Websites?

After you add the website to WAF, configure blacklist and whitelist rules or precise protection rules to allow only specified IP addresses to access the website. WAF then blocks all source IP addresses except the specified ones.

Configuring IP Address Blacklist and Whitelist Rules to Block All Source IP Addresses Except the Specified Ones

Step 1 Log in to the management console.

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

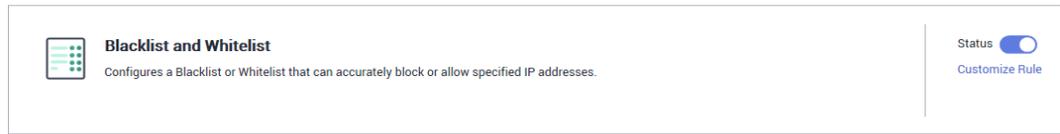
Step 3 Click  in the upper left corner and choose **Web Application Firewall** under **Security**.

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

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

Step 6 In the **Blacklist and Whitelist** configuration area, enable the protection.

Figure 13-51 Blacklist and Whitelist configuration area



Step 7 Click **Customize Rule**. On the displayed page, click **Add Rule** in the upper left corner.

Step 8 In the **Add Blacklist or Whitelist Rule** dialog box, add two blacklist rules to block all source IP addresses.

Figure 13-52 Blocking IP address range 1.0.0.0/1

Add Blacklist or Whitelist Rule

* Rule Name

* IP Address/Range/Group IP address/range Address group

* IP Address/Range

* Protective Action

Known Attack Source [Add Known Attack Source Rule](#)

Rule Description

Figure 13-53 Blocking IP address range 128.0.0.0/1

Add Blacklist or Whitelist Rule

* Rule Name

* IP Address/Range/Group IP address/range Address group

* IP Address/Range

* Protective Action

Known Attack Source [Add Known Attack Source Rule](#)

Rule Description

Step 9 Click **Add Rule**. In the displayed **Add Blacklist or Whitelist Rule** dialog box, add a rule for the specified IP address or IP address range.

For example, if you want to allow *XXX.XX.2.3* to access your website, add a protection rule as shown in [Figure 13-54](#).

Figure 13-54 Allowing the access of a specified IP address

Add Blacklist or Whitelist Rule

* Rule Name

* IP Address/Range/Group IP address/range Address group

* IP Address/Range

* Protective Action

Rule Description

----End

Configuring a Precise Protection Rule to Block All Source IP Addresses Except the Specified Ones

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** Click  in the upper left corner and choose **Web Application Firewall** under **Security**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** Click the name of the target policy to go to the protection configuration page.
- Step 6** In the **Precise Protection** configuration area, enable the protection.

Figure 13-55 Precise Protection configuration area

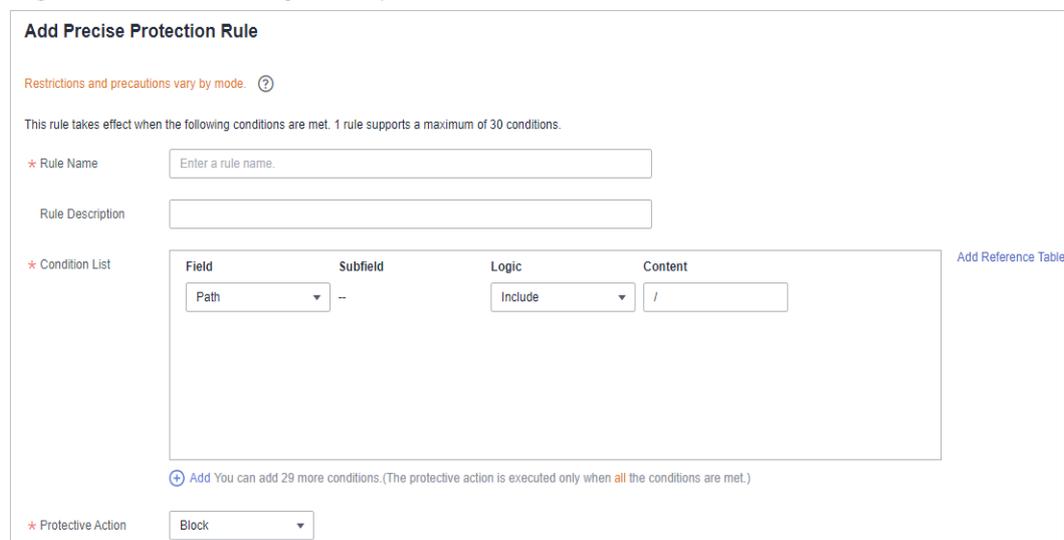


- Step 7** Click **Customize Rule**. In the upper left corner of the displayed page, click **Add Rule**.
- Step 8** In the displayed **Add Precise Protection Rule** dialog box, add a protection rule as shown in [Figure 13-56](#) to block all requests.

 **CAUTION**

The priority value here must be greater than that configured in [Step 9](#) because allowing access has a higher priority than blocking access and a smaller priority value indicates a higher priority.

Figure 13-56 Blocking all requests



Field	Subfield	Logic	Content
Path	--	Include	/

Step 9 Click **Add Rule**. In the displayed **Add Precise Protection Rule** dialog box, add a rule for the specified IP address.

For example, if you want to allow 192.168.2.3 to access the website, add a protection rule as shown in [Figure 13-57](#).

CAUTION

The priority value here must be smaller than that configured in [Step 8](#) because allowing access has a higher priority than blocking access and a smaller priority value indicates a higher priority.

Figure 13-57 Allowing the access of a specified IP address

Add Precise Protection Rule

Restrictions and precautions vary by mode. ?

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

* Rule Name

Rule Description

* Condition List

Field	Subfield	Logic	Content
IPv4	Client IP Address	Equal to	192.168.2.3

[Add Reference Table](#)

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

* Protective Action

----End

13.5.6.7 Which Protection Rules Are Included in the System-Generated Policy?

When you add a website to WAF, you can select an existing policy you have created or the system-generated policy. For details, see [Table 13-15](#).

NOTICE

If you are using WAF standard edition, only **System-generated policy** can be selected.

You can also tailor your protection rules after the domain name is connected to WAF.

Table 13-15 System-generated policies

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

 **NOTE**

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

13.5.6.8 Why Does the Page Fail to Be Refreshed After WTP Is Enabled?

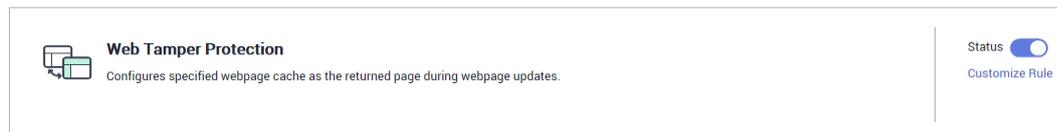
Web Tamper Protection (WTP) supports only caching of static web pages. Perform the following steps to fix this issue:

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**.
- Step 4** In the navigation pane on the left, choose **Policies**.
- Step 5** Click the name of the target policy to go to the protection configuration page.
- Step 6** In the **Web Tamper Protection** configuration area, check whether this function is enabled.

Figure 13-58 Web Tamper Protection configuration area



- 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

13.5.6.9 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 13-16](#) describes the differences between the two types of rules.

Table 13-16 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 checks access requests based on the protection rules and the triggering sequence.
Precise protection rules	You can combine common HTTP fields, such as IP , Path , Referer , User Agent , and Params in a protection rule to let WAF allow or block the requests that match the combined conditions.	Precise protection rules have lower priority compared with blacklist and whitelist rules.

13.5.6.10 What Do I Do If a Scanner, such as AppScan, Detects that the Cookie Is Missing Secure or HttpOnly?

Cookies are inserted by back-end web servers and can be implemented through framework configuration or set-cookie. Secure and HttpOnly in cookies help defend against attacks, such as XSS attacks to obtain cookies, and help defend against cookie hijacking.

If the AppScan scanner detects that the customer site does not insert security configuration fields, such as HttpOnly and Secure, into the cookie of the scan request, it records them as security threats.

13.6 Protection Event Logs

13.6.1 Can WAF Log Protection Events?

On the WAF console, you can view logs for the last 30 days and download logs for all protected websites for the last five days for free.

If you want to store WAF protection logs for a long time, enable Log Tank Service (LTS) at additional costs and authorize it for WAF logging. Logs can be stored in LTS for seven days by default but you can configure LTS for up to 30 days if needed. Logs earlier than 30 days are automatically deleted. However, you can configure LTS to dump those logs to an Object Storage Service (OBS) bucket or enable Data Ingestion Service (DIS) for long-term storage.

For details about how to configure LTS for WAF, see [Enabling LTS for WAF Logging](#).

13.6.2 How Do I Obtain Data about Block Actions?

WAF allows you to download the attack events (log-only and block events) data of all protected domain names over the past five days. A CSV file of the protection event data for the current day will be generated at the beginning of the next day.

For details about how to obtain event data, see .

13.6.3 What Does "Mismatch" for "Protective Action" Mean in the Event List?

If an access request matches a web tamper protection rule, information leakage prevention rule, or data masking rule, the protective action is marked as **Mismatch**.

13.6.4 How Long Can WAF Protection Logs Be Stored?

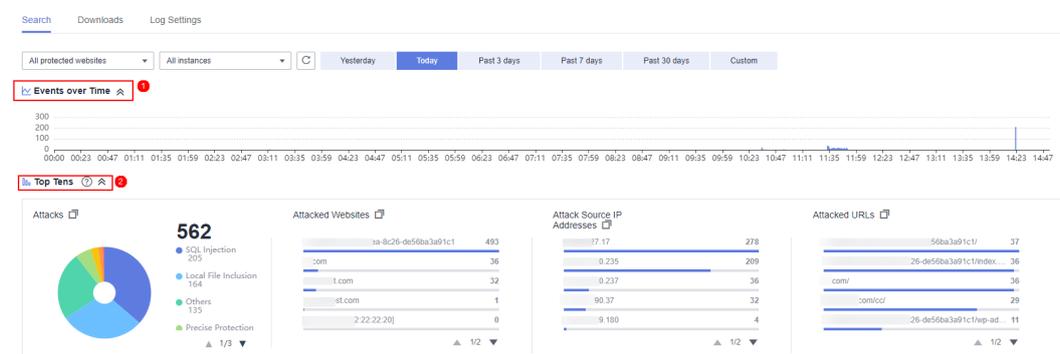
On the WAF console, you can view logs for the last 30 days and download logs for all protected websites for the last five days for free.

The storage duration depends on your choices. You can store WAF logs in Log Tank Service (LTS) for seven days by default and up to 30 days by additional custom configuration. Logs earlier than 30 days will be deleted automatically by LTS. LTS is additionally billed. If you seek for long-term storage, enable the log transfer function in LTS to dump those logs to Object Storage Service (OBS) buckets or enable Data Ingestion Service (DIS).

13.6.5 Can I Query Protection Events of a Batch of Specified IP Addresses at Once?

WAF does not support batch query of protection events of a batch of specified IP addresses at once. On the **Events** page, you can view events by a certain combination of **Event Type**, **Protective Action**, **Source IP Address**, **URL**, and **Event ID**.

Figure 13-59 Events



13.6.6 Will WAF Record Unblocked Events?

No. WAF blocks attack events based on the configured protection rules and records only blocked attack events in protection event logs.

13.6.7 Why Is the Traffic Statistics on WAF Inconsistent with That on the Origin Server?

In any of the following scenarios, the traffic statistics displayed on the WAF **Dashboard** page may be inconsistent with that displayed on the origin server:

- **Web page compression**
WAF enables compression by default. The web pages between the client (such as a browser) and WAF may be compressed (depending on the compression option of the browser), but the origin server may not support compression.
- **Connection reuse**
WAF reuses socket connections with the origin server, which reduces the bandwidth usage between the origin server and WAF.
- **Attack requests**
Attack requests blocked by WAF do not consume the bandwidth of the origin server.
- **Other abnormal requests**
If the origin server times out or cannot be connected, the bandwidth of the origin server is not consumed.
- **TCP retransmission**
WAF collects bandwidth statistics at layer 7, but the network adapter of the origin server collects bandwidth statistics at layer 4. If the network connection is poor, TCP retransmission occurs. The bandwidth measured by the network adapter is calculated repeatedly, but the data transmitted at layer 7 is not calculated repeatedly. In this case, the bandwidth displayed on WAF is lower than that displayed on the origin server.

A Change History

Release Date	Description
2024-03-30	<p>This issue is the sixth official release.</p> <ul style="list-style-type: none"> • Adjusted the document structure. • Added the following content: <ul style="list-style-type: none"> - Configuring a Known Attack Source Rule to Block Specific Visitors for a Specified Duration - Configuring a Traffic Identifier for a Known Attack Source - Modifying the Alarm Page - Viewing Protection Information About a Protected Website on Cloud Eye - Certificate Management - Managing IP Address Blacklist and Whitelist Groups - Viewing Product Details - Monitoring - FAQs for Beginners - How Do I Modify a Certificate? - Do I Need to Import the Certificates That Have Been Uploaded to ELB to WAF? - Why Am I Seeing Error Code 414 Request-URI Too Large? - What Do I Do If the Protocol Is Not Supported and the Client and Server Do Not Support Common SSL Protocol Versions or Cipher Suites? - Can I Batch Add IP Addresses to a Blacklist or Whitelist Rule? - Can I Import or Export a Blacklist or Whitelist into or from WAF? - How Do I Block Abnormal IP Addresses?

Release Date	Description
	<ul style="list-style-type: none"> - Is There Any Impact on Website Loading Speed If Other Crawler Check in Anti-Crawler Is Enabled? - How Does JavaScript Anti-Crawler Detection Work? - How Do I Allow Only Specified IP Addresses to Access Protected Websites? - Can I Query Protection Events of a Batch of Specified IP Addresses at Once? • Modified the following content: <ul style="list-style-type: none"> - Enabling WAF - WAF Operation Guide - Dashboard - Viewing Protection Event Logs - Policies - Configuring PCI DSS/3DS Certification Check and TLS Version - Managing Dedicated WAF Engines - Enabling Alarm Notifications
2023-11-15	<p>This issue is the fifth official release.</p> <ul style="list-style-type: none"> • Added Enabling LTS for WAF Logging. • Modified the following topic: Viewing Protection Event Logs.
2023-05-25	<p>This issue is the fourth official release.</p> <p>Added the following content:</p> <ul style="list-style-type: none"> • CTS • WAF Operations Recorded by CTS
2021-09-30	<p>This issue is the third official release.</p> <p>Added the description of the WAF cloud mode.</p>
2021-08-31	<p>This issue is the second official release.</p> <p>Optimized descriptions in "Permissions Management".</p>
2021-01-31	<p>This issue is the first official release.</p>