Web Application Firewall

FAQs

Issue	05
Date	2024-03-22

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Security Declaration

Vulnerability

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

Contents

1 Most Frequently Asked Questions

Purchasing WAF

- Can I Use WAF Across Regions?
- Does WAF Support Custom Authorization Policies?
- Domain Name Expansion Package
- QPS Expansion Package

Modifying WAF Instance Specifications

- How Do I Change the WAF Instance Edition to a Lower One and Reduce Number of Packages?
- What Can I Do If the Website Traffic Exceeds the WAF Service Request Limit?
- Can I Change WAF Specifications During Renewal?

Connecting Website Domain Name to WAF

- What Data Is Required for Connecting a Domain Name/IP Address to WAF?
- Which Non-Standard Ports Does WAF Support?
- How Do I Add a Domain Name/IP Address to WAF?
- How Do I Configure the Client Protocol and Server Protocol?
- What Can I Do If the Message "Illegal server address" Is Displayed When I Add a Domain Name?
- Why Is My Domain Name or IP Address Inaccessible?
- Can I Configure the Origin Server Address to an IPv6 Address in WAF?

Troubleshooting Service Interruptions

- How Can I Upload Files After the Website Is Connected to WAF?
- How Do I Troubleshoot 404/502/504 Errors?
- What Is the Connection Timeout Duration of WAF? Can I Manually Set the Timeout Duration?
- Why Am I Seeing Error Code 523?

Protection Rules

2 About WAF

2.1 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. After purchasing WAF, you only need to connect your domain name to use WAF to protect your web applications.

For more details, see **Adding a Domain Name to WAF**.

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.

NOTICE

If you are using a cloud WAF instance, you only need to change the DNS resolution record of your website to let traffic pass through WAF. Modifying DNS resolution may affect website access services. You are advised to perform this operation during off-peak hours. For details, see **Connecting a Domain Name to WAF**.

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, purchase dedicated WAF instances in the same VPC as that for the origin servers.

Can WAF Protect Both Cloud or On-premises Servers?

Yes. A cloud WAF instance can protect servers on any cloud platforms. This means that a cloud WAF instance can protect both cloud and on-premises servers, provided the servers are connected to the Internet.

A cloud WAF instance protects your servers based on domain names regardless of whether your server is on the cloud or not, where your server resides, or to which project or account your server belongs.

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.

For details about the WAF protection process, see **Configuration Guidance**.

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.

If you want to cache all website contents, you can deploy CDN and deploy WAF between CDN and the origin server. For details, see **Domain Setup with Both CDN and WAF Deployed**.

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.

WAF does not cache website data. If you want to cache website content, use CDNor deploy both WAF and CDN.

For details about the combination of WAF and CDN, see **Combine WAF and CDN: Better Protection and Faster Access**

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.

You are advised to use an ELB load balancer and dedicated WAF instances and then configure two-way authentication on the load balancer. The procedure is as follows:

1. **Buy a Dedicated WAF Instance**.
2. Connect your website to WAF and configure ELB. For details, see **Connection Process (Dedicated Mode)**.
3. Configure two-way authentication on the ELB load balancer. For details, see **HTTPS Mutual Authentication**.

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.

For details, see **Configuring a CC Attack Protection Rule**.

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.

There are some restrictions on QPS. For details, see **Edition Differences**.

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.

The procedure varies depending on the WAF instance type you are using:

- Cloud mode: **Whitelisting WAF IP Addresses**
- Dedicated mode: **Whitelisting the Back-to-Source IP Addresses of Your Dedicated WAF Instances**

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. For more details, see **Switching the Load Balancing Algorithm**.

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.

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.

For details, see **Configuring Anti-Crawler Rules**.

Does WAF Support Protocols Used in MS Exchange?

WAF supports HTTP and HTTPS for logging in to Exchange on the web, but does not support mail-related protocols such as Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3), or Internet Message Access Protocol (IMAP) used by MS Exchange.

Can WAF Defend Against XOR Injection Attacks?

Yes. WAF can defend against XOR injection attacks.

What Is the bind_ip Parameter in WAF Logs?

After your website is connected to WAF, WAF functions as a reverse proxy between the client and the origin server. WAF examines traffic to your website, filters out malicious traffic, and forwards health traffic to your origin servers. **bind_ip** indicates the WAF IP addresses used by WAF to forward healthy traffic. WAF IP addresses must be whitelisted on your origin server. For more details about how to whitelist WAF IP addresses, see **How Do I Whitelist IP Address Ranges of Cloud WAF?**

Can WAF Protect All Domain Names Mapped to My Website IP Address If I Have Connected the IP Address to WAF?

No.

In dedicated mode, the origin server IP address can be connected to WAF, and the IP address can be a private or internal IP address. WAF protects only the traffic accessed through the IP address but cannot protect the traffic to the domain name mapped to the IP address. To protect a domain name, connect the domain name to WAF.

Why Are There A Large Number of Timeout Requests?

In cloud mode, WAF is shared by you and other customers. The service growth of other customers may cause a high WAF forwarding latency. If you expect a low latency, dedicated WAF instances are recommended. In dedicated mode, WAF instances are for your exclusive use so WAF forwarding latency cannot be affected by other customers.

Does WAF Support HTTP/3?

No. Currently, WAF supports HTTP/2 but does not support HTTP/3.

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.

Can WAF in Cloud Mode Protect Domain Names of Other Accounts?

Yes. Cloud WAF protects domain names. To protect a domain name of other accounts, you only need to add the domain name to the cloud WAF instance you are using in the current account.

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.

2.2 WAF Functions

2.2.1 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?**

2.2.2 What Objects Does WAF Protect?

WAF can protect websites through domain names or IP addresses.

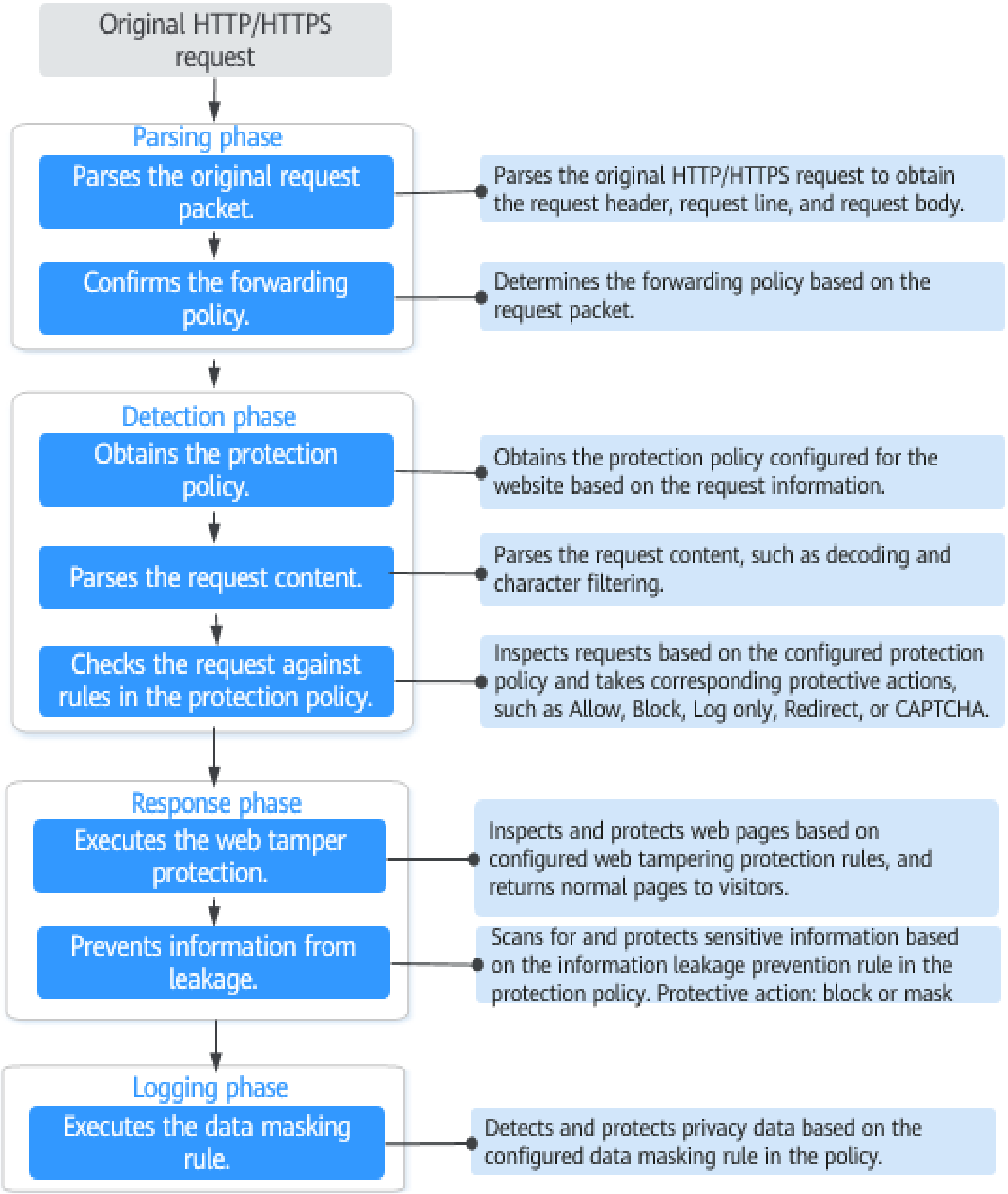
- In cloud CNAME access mode, only website domain names can be added to WAF.

  Your origin server IP address configured in WAF must a public IP address. For example, if an Elastic Load Balance (ELB) load balancer from Huawei Cloud 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.

2.2.3 Does WAF Block Customized POST Requests?

No. WAF does not block user-defined POST requests. **Figure 2-1** shows the detection process of the WAF built-in protection rules for original HTTP/HTTPS requests.

Figure 2-1 WAF engine work process


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

For details about the WAF protection process, see **Configuration Guidance**.

2.2.4 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 2-1 describes the differences

Table 2-1 Differences between the web tamper protection functions of HSS and WTP

Item	HSS	WAF
Static web page protection	Locks files in driver and web file directories to prevent attackers from tampering with them.	Caches static web pages on servers.
Dynamic web page protection	● Dynamic WTP Protects your data while Tomcat is running, detecting dynamic data tampering in databases. ● Privileged process management Allows privileged processes to modify web pages.	No
Backup and restoration	● Active backup and restoration If WTP detects that a file in the protection directory is tampered with, it immediately uses the backup file on the local host to restore the file. ● Remote backup and restoration If a file directory or backup directory on the local server becomes invalid, you can use the remote backup service to restore the tampered web page.	No
Suitable for	Websites that have high security requirements and difficult to be manually recovered	Websites that only require application-layer protection

Purchase Suggestion

Website	Service
Common websites	WAF web tamper protection + HSS enterprise edition
Websites that require strong protection and anti-tampering capabilities	WAF web tamper protection + HSS WTP

2.2.5 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

2.2.6 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.

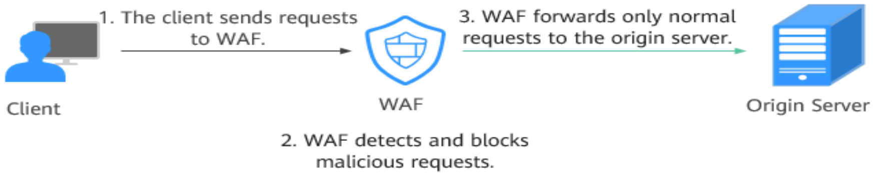
2.2.7 What Are the Differences Between WAF Forwarding and Nginx Forwarding?

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 2-2 How WAF works for CNAME or dedicated access

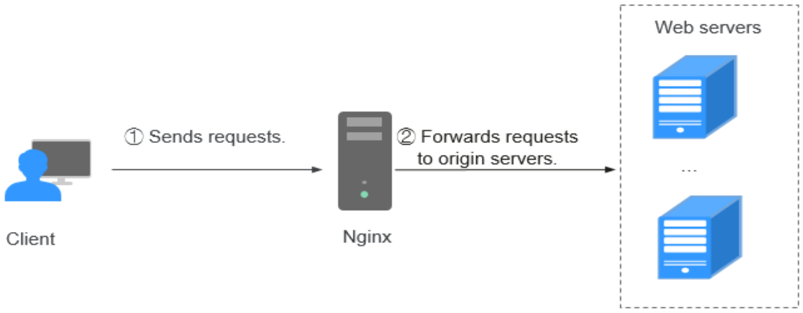

1. The client sends requests to WAF.
3. WAF forwards only normal requests to the origin server.
Client
WAF
Origin Server
2. WAF detects and blocks malicious requests.

- Nginx forwarding

  Nginx works as a reverse proxy server. After receiving the access request from the client, the reverse proxy server directly forwards the access request to the web server and returns the result obtained from the web server to the client. The reverse proxy server is installed in the website equipment room. It functions as a proxy for the web server to receive and forward access requests.

  The reverse proxy server prevents malicious attacks from the Internet to intranet servers, caches data to reduce workloads on the intranet servers, and implements access security control and load balancing.

Figure 2-3 How Nginx Works



2.2.8 What Are the Differences Between WAF and CFW?

Web Application Firewall (WAF) and Cloud Firewall (CFW) are different products we provided. WAF is used to protect your web services, while CFW is used to protect Internet border and VPC border traffic.

Table 2-2 lists differences between WAF and CFW.

Table 2-2 Differences between WAF and CFW

Category	WAF	CFW
Definition	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).	Cloud Firewall (CFW) is a next-generation cloud-native firewall. It protects Internet and VPC borders on the cloud by real-time intrusion detection and prevention, global unified access control, full traffic analysis, log audit, and tracing. It employs AI for intelligent defense, and can be elastically scaled to meet changing business needs, helping you easily handle security threats. CFW is a basic service that provides network security protection for user services on the cloud.
Protection mechanism	WAF works as a reverse proxy between the client and the origin server. 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.	CFW can implement refined control over all traffic, including Internet border protection, cross-VPC and cross-VM traffic, to prevent external intrusion, internal penetration attacks, and unauthorized access from the inside to the outside.

Category	WAF	CFW
Deployment mode	WAF can be deployed in cloud mode ,ELB mode, and dedicated mode. ● **Cloud - CNAME**: a good choice no matter where your web services are deployed, on Huawei Cloud, any other cloud, even in on-premises data centers, as long as they have domain names. The application scenarios for different editions are as follows: – Standard edition This edition is suitable for small- and medium-sized websites that do not have special security requirements. – Professional edition This edition is suitable for medium-sized enterprise websites or services that are open to the Internet, focus on data security, and have high security requirements. – Platinum edition This edition is suitable for large- and medium-sized enterprise websites that have large-scale services or have special security requirements. ● **Dedicated**: a good choice if your service servers are deployed on Huawei Cloud as long as they have domain names or IP addresses. Dedicated WAF instances are suitable large enterprise websites that have a large service scale and have customized security requirements.	Protection for Internet border and VPC border
Protection objects	Domain names or IP addresses	Elastic IP Address (EIP)

Category	WAF	CFW
Functions	WAF identifies and blocks a wide range of suspicious 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).	● Asset management and intrusion defense: CFW detects and defends against intrusions into cloud assets that are accessible over the Internet in real time. ● Access control: You can control access at Internet borders. ● Traffic Analysis and log audit: CFW controls, analyzes, and visualizes VPC traffic, audits logs, and traces traffic sources.

2.2.9 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.

For details, see **Configuring a CC Attack Protection Rule**.

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.

2.2.10 How Does WAF Detect SQL Injection, XSS, and PHP Injection Attacks?

A Structured Query Language (SQL) injection is a common web attack. The attacker injects malicious SQL commands into database query strings to deceive the server into executing commands. By exploiting these commands, the attacker can obtain sensitive information, add users, export files, or even gain the highest permissions to the database or system.

XSS attacks exploit vulnerabilities left during web page development to inject malicious instruction code into web pages so that attackers can trick visitors into loading and executing malicious web page programs attackers fabricated. These malicious web page programs are usually JavaScript, but they can also include Java, VBScript, ActiveX, Flash, or even common HTML. After an attack succeeds, the attacker may obtain various content, including but not limited to higher permissions (for example, permissions for certain operations), private content, sessions, and cookies.

How Does WAF Detect SQL Injection Attacks?

WAF detects and matches SQL keywords, special characters, operators, and comment symbols.

- SQL keywords: union, Select, from, as, asc, desc, order by, sort, and, or, load, delete, update, execute, count, top, between, declare, distinct, distinctrow, sleep, waitfor, delay, having, sysdate, when, dba_user, case, delay, and the like
- Special characters: ',; ()
- Mathematical operators: ±, *, /, %, and |
- Operators: =, >, <, >=, <=, !=, +=, and -=
- Comment symbols: – or /**/

How Does WAF Detect XSS Attacks?

WAF checks HTML script tags, event processors, script protocols, and styles to prevent malicious users from injecting malicious XSS statements through client requests.

- XSS keywords (such as **javascript**, **script**, **object**, **style**, **iframe**, **body**, **input**, **form**, **onerror**, and **alert**)
- Special characters (<, >, ', and ")
- External links (href="http://xxx/",src="http://xxx/attack.js")

NOTE

Rich text can be uploaded using multipart upload instead of body. In multipart upload, rich text is stored in forms and can be decoded even if it is encoded using Base64. Analyze your services and do not use quotation marks and angle brackets as far as possible.

How Does WAF Detect PHP Injection Attacks?

If a request contains keywords similar to "system(xx)", the keywords may cause PHP injection attacks. WAF will then block such requests.

2.2.11 Can WAF Defend Against the Apache Struts2 Remote Code Execution Vulnerability (CVE-2021-31805)?

Yes. WAF basic web protection rules can defend against the Apache Struts2 remote code execution vulnerability (CVE-2021-31805).

Configuration Procedure

Step 1 But WAF.

Step 2 Add the website domain name to WAF and connect it to WAF. For details, see **Adding a Domain Name to WAF**.

Step 3 In the **Basic Web Protection** configuration area, set **Mode** to **Block**. For details, see **Configuring Basic Web Protection Rules**.

----End

2.3 WAF Usage

2.3.1 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.

2.3.2 What Are the Restrictions on Using WAF in Enterprise Projects?

Each enterprise project is independent from the others.

- The created policies can be used only by their own projects. For example, if you create policy A for a main project, the rules created for the sub-projects do not belong to policy A. You must create a policy for sub-projects separately.

- The created certificates can be used only by their own projects. A main project and sub-project can only use its own certificates.

2.3.3 How Do I Obtain the Real IP Address of a Web Visitor?

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

Generally, a proxy such as CDN, WAF, and anti-DDoS service is deployed between the client and server. Web visitors cannot directly access the server. For example, **web visitor** > **CDN/WAF/anti-DDoS** > **origin server**.

When forwarding requests to the downstream server, the transparent proxy server adds an **X-Forwarded-For** field to the HTTP header to identify the web visitor's real IP address in the format of **X-Forwarded-For: real IP address of the web visitor, proxy 1-IP address, proxy 2-IP address, proxy 3-IP address, ...->...**.

Therefore, you can obtain the web visitor's real IP address from the **X-Forwarded-For** field. The first IP address in this field is the web visitor's real IP address.

2.3.4 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.

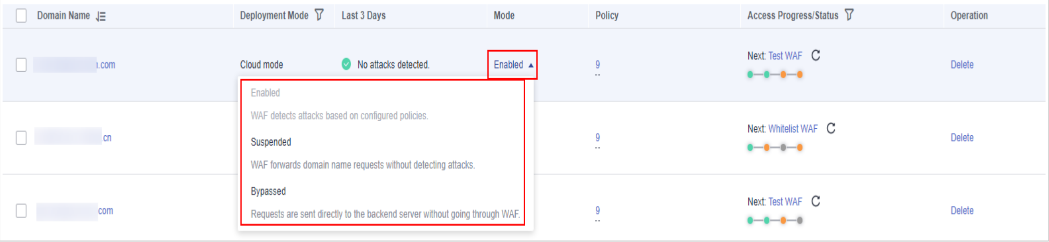
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

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 2-4 Switching WAF working mode



□	Domain Name	Deployment Mode	Last 3 Days	Mode	Policy	Access Progress/Status	Operation
□	[redacted].com	Cloud mode	No attacks detected.	Enabled ▲	9 --	Next: Test WAF	Delete
□	[redacted]cn				9 --	Next: Whitelist WAF	Delete
□	[redacted]com				9 --	Next: Test WAF	Delete

Enabled

WAF detects attacks based on configured policies.

Suspended

WAF forwards domain name requests without detecting attacks.

Bypassed

Requests are sent directly to the backend server without going through WAF.

----End

2.3.5 What Are Local File Inclusion and Remote File Inclusion?

You can view security events such as file inclusion in WAF protection events to quickly locate attack sources or analyze attack events.

Program developers write repeatedly used functions into a single file. When such functions need to be used, the file is directly invoked. The file invoking process is called file inclusion. File inclusion vulnerabilities are classified into two categories, based on whether the file is a remotely hosted file or a local file available on the web server:

- Local file inclusion
- Remote file inclusion

A file inclusion vulnerability allows an attacker to access unauthorized or sensitive files available on the web server or to execute malicious files on the web server by using such a file. This vulnerability is mainly due to a bad input validation mechanism, wherein the user's input that is passed to the file include commands without proper validation. The impact of this vulnerability can lead to malicious code execution on the server or reveal data present in sensitive files.

For details about protection event logs, see **Viewing Protection Event Logs**.

2.3.6 What Is the Difference Between QPS and the Number of Requests?

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

Queries Per Second (QPS) is the number of requests a server can handle per second.

NOTE

QPS is used to measure the number of queries, or requests, per second.

For details about QPS on the **Dashboard** page, see **Table 2-3**.

Table 2-3 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.

For details about QPS performance of different WAF editions, see **Edition Differences**.

2.3.7 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.

2.3.8 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.

For details, see the following topics:

- Configure an access control policy on the origin server to whitelist the WAF IP addresses. For details, see **How Do I Whitelist IP Address Ranges of Cloud WAF?**.
- Disable other firewalls and security software on origin servers.

2.3.9 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.

2.3.10 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.

NOTICE

2.3.11 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.

2.3.12 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.

2.4 Regions and AZs

2.4.1 What Are Regions and AZs?

Concepts

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

Selecting a Region

If you or your users are in Europe, select the **EU-Dublin** region.

Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.

2.4.2 Can I Use WAF Across Regions?

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

2.5 Configuring IPv6 Addresses

2.5.1 Which WAF Editions in Which Regions Support IPv6 Protection?

You can purchase professional or platinum WAF instances to protect your IPv6 addresses.

NOTICE

- WAF can inspect requests that use both IPv4 and IPv6 addresses for the same domain name.
- For web services that still use the IPv4 protocol stack, WAF supports the NAT64 mechanism. NAT64 is an IPv6 conversion mechanism that enables communication between the IPv6 and IPv4 hosts using network address translation (NAT). WAF can convert an IPv4 source site to an IPv6 website and converts external IPv6 access traffic to internal IPv4 traffic.

2.5.2 How Do I Check Whether the Origin Server IP Address Configured in WAF Is an IPv6 Address?

Before performing this operation, ensure that a domain name has been added to WAF and the domain name has been connected to WAF.

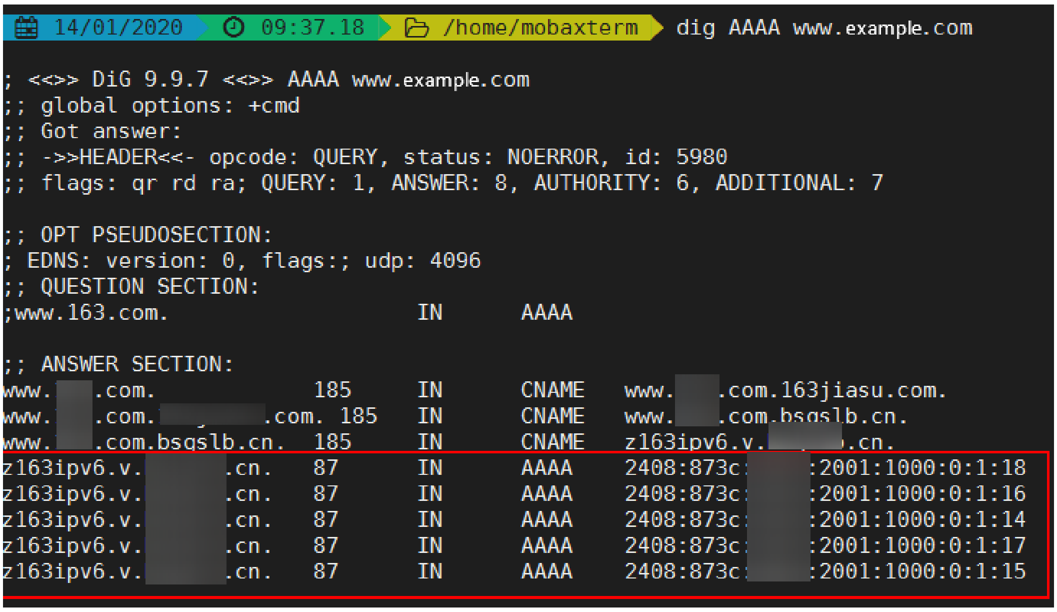
If a domain name *www.example.com* has been added, you can use the following method to check whether the configured origin server IP address is an IPv6 address:

Step 1 Open the cmd command line tool in the Windows operating system.

Step 2 Run the **dig AAAA www.example.com** command.

If the command output contains an IPv6 address, the configured origin server IP address is an IPv6 address.

Figure 2-5 Test result



```
 14/01/2020   09:37.18   /home/mobaxterm  dig AAAA www.example.com

; <<>> DiG 9.9.7 <<>> AAAA www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5980
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 6, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.163.com.                   IN      AAAA

;; ANSWER SECTION:
www.[redacted].com.             185     IN      CNAME   www.[redacted].com.163jiasu.com.
www.[redacted].com.[redacted].com. 185  IN      CNAME   www.[redacted].com.bsgslb.cn.
www.[redacted].com.bsgslb.cn.   185     IN      CNAME   z163ipv6.v.[redacted].cn.
z163ipv6.v.[redacted].cn.       87      IN      AAAA    2408:873c[redacted]:2001:1000:0:1:18
z163ipv6.v.[redacted].cn.       87      IN      AAAA    2408:873c[redacted]:2001:1000:0:1:16
z163ipv6.v.[redacted].cn.       87      IN      AAAA    2408:873c[redacted]:2001:1000:0:1:14
z163ipv6.v.[redacted].cn.       87      IN      AAAA    2408:873c[redacted]:2001:1000:0:1:17
z163ipv6.v.[redacted].cn.       87      IN      AAAA    2408:873c[redacted]:2001:1000:0:1:15
```

----End

2.5.3 Can I Configure the Origin Server Address to an IPv6 Address in WAF?

Yes. The origin server address configured in WAF can be an IPv4 or IPv6 address. If you have configured an IPv4 address, change it to an IPv6 address of the origin server at any time you want.

WAF supports the IPv6/IPv4 dual stack mode and NAT64 mechanism. The details are as follows:

- WAF can inspect requests that use both IPv4 and IPv6 addresses for the same domain name.
- For web services that still use the IPv4 protocol stack, WAF supports the NAT64 mechanism. NAT64 is an IPv6 conversion mechanism that enables communication between the IPv6 and IPv4 hosts using network address translation (NAT). WAF can convert an IPv4 source site to an IPv6 website and converts external IPv6 access traffic to internal IPv4 traffic.

2.5.4 How Does WAF Forward Traffic to an IPv6 Origin Server?

If the origin server address is an IPv6 address, WAF accesses the origin server over the IPv6 address. WAF adds IPv6 address resolution in CNAME record sets by default. IPv6 access requests are forwarded to WAF first. WAF detects and filters out malicious attack traffic, and returns normal traffic to the origin server to ensure that the origin server is secure, stable, and available.

WAF supports the IPv6/IPv4 dual stack mode and NAT64 mechanism. The details are as follows:

- WAF can inspect requests that use both IPv4 and IPv6 addresses for the same domain name.

- For web services that still use the IPv4 protocol stack, WAF supports the NAT64 mechanism. NAT64 is an IPv6 conversion mechanism that enables communication between the IPv6 and IPv4 hosts using network address translation (NAT). WAF can convert an IPv4 source site to an IPv6 website and converts external IPv6 access traffic to internal IPv4 traffic.

3 Purchasing WAF

3.1 What Are the Differences Between the Permissions of an Account and Those of IAM Users?

If you need many accounts within your organization, you can create IAM users and manage them effectively.

An account can allocate funds to IAM users so that IAM users can manage resources independently.

Both an account and its IAM user can create IAM users. An account can only manage its own IAM users but cannot manage the IAM users of other accounts.

An account and its IAM users are equally used. Their differences lie in what permissions you assign to them.

For details about WAF account permissions, see **Permissions Management**.

3.2 Can I Share My WAF with Other Accounts?

WAF cannot be shared by multiple accounts. Each account needs to individually purchase a WAF instance. However, a WAF instance can be shared with IAM users created with the current account.

Sharing WAF Among Multiple IAM Users

Assume that you have created an account, *domain1*, by registering with Huawei Cloud, and used *domain1* to create two IAM users, *sub-user1a* and *sub-user1b*, in IAM. If you have granted WAF permissions to *sub-user1b*, *sub-user1b* can then use the WAF service of *sub-user1a*.

For details about granting permissions, see **Creating a User Group and Granting Permissions**.

3.3 How Does WAF Calculate Domain Name Quota Usage?

The number of domain names protected by WAF is calculated as follows:

- The number of domains is the total number of top-level domain names (for example, example.com), single domain names/second-level domains (for example, www.example.com), and wildcard domain names (for example, *.example.com). For example, the standard edition WAF can protect up to 10 domain names. You can add one top-level domain name and nine subdomain names or wildcard domain names related to the top-level domain name.
- If a domain name maps to different ports, each port is considered to represent a different domain name. For example, **www.example.com:8080** and **www.example.com:8081** are counted towards your quota as two distinct domain names.
- You can upload as many certificates in WAF as the number of domain names that can be protected by your WAF instances in the same account. For example, if you purchase a standard edition WAF instance, which can protect 10 domain names, a dedicated WAF instance, which can protect 2,000 domain names, and a domain name expansion package (20 domain names), your WAF instances can protect 2,030 domain names total (2,000 + 20 +10). In this case, you can upload 2,030 certificates.

For details, see **Edition Differences**.

4 Service Request/Specification

4.1 WAF Instance Specifications Change

4.1.1 How Do I Change the WAF Instance Edition to a Lower One and Reduce Number of Packages?

- To change WAF edition: In the **Edition** row, click **Change Edition** in the **Details** column. In the displayed **Change Edition** pane, select an edition and click **OK**.
- To change expansion packages: In the **Details** column of the **Domain Name Quota**, **QPS Quota**, and **Rule Quota** rows, increase or decrease the number of expansion packages, respectively.

  By default, the number of extension packages cannot be reduced to 0. To do so, click **Unsubscribe**.
- Billing information: Changing specifications does not change the billing mode or expiration date.

WAF provides standard, professional, and platinum editions. To use a WAF instance with lower specifications, unsubscribe from the WAF instance you are using and buy another one.

NOTE

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

4.1.2 Can I Add More Protection Rules?

In cloud mode, WAF provides standard, professional, and platinum editions for you. For details, see **Edition Differences**. If the edition you are using cannot meet your service requirements, you can upgrade it.

4.1.3 What Can I Do If the Website Traffic Exceeds the WAF Service Request Limit?

If your website normal traffic exceeds the service request limit offered by the edition you select, website traffic forwarding may be adversely affected.

For example, your website traffic may be limited, packets may be discarded randomly, and WAF may be bypassed automatically. Your website services may be unavailable, frozen, or respond very slowly.

NOTE

If website traffic exceeded the WAF service request limit, WAF does not send alarm notifications. If the QPS limit supported by the WAF edition you are using is exceeded, WAF will send alarm notifications once it detects attacks on your website. For details, see **Enabling Alarm Notification**

In this case, upgrade your edition or buy extra QPS expansion packages.

4.1.4 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.

Table 4-1 lists the QPS specifications supported by each WAF edition.

Table 4-1 QPS specifications supported by WAF

Edition	Peak Rate of Normal Service Requests	Peak Rate of CC Attack Defense
Standard	2,000 QPS	100,000 QPS
Professional	5,000 QPS	200,000QPS
Platinum	10,000 QPS	1,000,000 QPS

Edition	Peak Rate of Normal Service Requests	Peak Rate of CC Attack Defense
Dedicated mode	The following lists the specifications of a single instance. ● Specifications: WI-500. Referenced performance: – HTTP services - Recommended QPS: 5,000. Maximum QPS: 10,000. – HTTPS services - Recommended QPS: 4,000. Maximum QPS: 8,000. – WebSocket service - Maximum concurrent connections: 5,000 – Maximum WAF-to-server persistent connections: 60,000 ● Specifications: WI-100. Referenced performance: – HTTP services - Recommended QPS: 1,000. Maximum QPS: 2,000. – HTTPS services - Recommended QPS: 800. Maximum QPS: 1,600 – WebSocket service - Maximum concurrent connections: 1,000 – Maximum WAF-to-server persistent connections: 60,000	● Specifications: WI-500. Referenced performance: Maximum QPS: 20,000 ● Specifications: WI-100. Referenced performance: Maximum QPS: 4,000

4.1.5 Can I Change WAF Specifications During Renewal?

No. You can renew your cloud WAF instance, but you cannot change its specifications during renewal. You can renew your subscriptions to the current WAF edition, purchased domain, QPS, and/or rule expansion packages. If you need to change the WAF specifications during the renewal, **Changing the Edition and Specifications of a Cloud WAF Instance** and complete a renewal.

NOTICE

To reuse the configurations of a WAF instance, ensure that the original WAF instance you unsubscribed from and the new WAF instance you are purchasing are in the same region. If you buy a WAF instance again after an unsubscription, you still need to add the domain name to the new WAF instance and configure protection rules for the domain name based on protection requirements.

4.1.6 How Many Rules Can I Add to a WAF Instance?

The number of rules that you can add varies depending on the protection types in the WAF edition you are using. **Table 4-2** lists the specifications included in different editions.

Table 4-2 WAF editions and applicable service scales

Service Scale	Standard	Professional	Platinum	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
Peak rate of normal service requests	● Service requests: 2,000 QPS ● WAF-to-Server connections: 6,000 per domain name	● Service requests: 5,000 QPS ● WAF-to-Server connections: 6,000 per domain name	● Service requests: 10,000 QPS ● WAF-to-Server connections: 6,000 per domain name	N/A	The following lists the specifications of a single instance. ● Specifications: WI-500. Referenced performance: – HTTP services - Recommended QPS: 5,000. Maximum QPS: 10,000. – HTTPS services - Recommended QPS: 4,000. Maximum QPS: 8,000. – WebSocket service - Maximum concurrent connections: 5,000 – Maximum WAF-to-server persistent connections: 60,000 ● Specifications: WI-100. Referenced performance:

Service Scale	Standard	Professional	Platinum	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
					– HTTP services - Recommended QPS: 1,000. Maximum QPS: 2,000. – HTTPS services - Recommended QPS: 800. Maximum QPS: 1,600 – WebSocket service - Maximum concurrent connections: 1,000 – Maximum WAF-to-server persistent connections: 60,000 **NOTICE** Maximum QPS values are for your reference only. They may vary depending on your businesses. The real-world QPS is related to the request size and the type and quantity of protection rules you customize.

Service Scale	Standard	Professional	Platinum	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
Service bandwidth threshold (The origin server is deployed on the cloud.)	100 Mbit/s	200 Mbit/s	300 Mbit/s	N/A	● Specifications: WI-500. Performance: Throughput: 500 Mbit/s ● Specifications: WI-100. Referenced performance: Throughput: 100 Mbit/s
Service bandwidth threshold (The origin server is not deployed on Huawei Cloud.)	30 Mbit/s	50 Mbit/s	100 Mbit/s	N/A	N/A
Number of domains	10 (Supports one top-level domain name.)	50 (Supports five top-level domain names.)	80 (Supports eight top-level domain names.)	30 (Supports three top-level domain names.)	2,000 (Supports 2,000 top-level domain names)
Back-to-source IP address quantity (the number of WAF back-to-source IP addresses that can be allowed by a protected domain name)	20	50	80	20	N/A

Service Scale	Standard	Professional	Platinum	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
Peak rate of CC attack defense	100,000 QPS	200,000 QPS	1,000,000 QPS	N/A	● Specifications: WI-500. Referenced performance: Maximum QPS: 20,000 ● Specifications: WI-100. Referenced performance: Maximum QPS: 4,000
Number of CC attack defense rules	20	50	100	200	100
Number of precise protection rules	20	50	100	200	100
Number of reference table rules	N/A	50	100	200	100
Number of IP address blacklist or whitelist rules	1,000	2,000	5,000	200	1,000
Number of geolocation access control rules	N/A	50	100	200	100
Number of web tamper protection rules	20	50	100	200	100

Service Scale	Standard	Professional	Platinum	Cloud Mode (Pay-Per-Use Billing)	Dedicated Mode
Number of information leakage prevention rules	N/A	50	100	200	100
Global protection whitelist rules	1,000	1,000	1,000	2,000	1,000
Number of data masking rules	20	50	100	200	100

4.1.7 Where and When Can I Buy a Domain, QPS, or Rule Expansion Package?

You can buy domain, QPS, and rule expansion packages when you purchase or upgrade a cloud WAF instance in standard, professional, or platinum edition.

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

Purchasing Expansion Packages While Purchasing Cloud WAF

Step 1 Log in to the management console.

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

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

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

Step 5 On the **Buy Web Application Firewall** page, specify **Region** and select an edition.

Step 6 Specify the number of domain name, QPS, and rule expansion packages.

Step 7 Set **Required Duration** and pay for the order.

NOTE

A WAF instance and its expansion packages have the same required duration.

----End

Purchasing Expansion Packages During the Upgrade

Step 1 Log in to the management console.

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

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

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

Step 5 On the purchase page, select any edition higher than the current one. By default, the current edition is selected.

Step 6 Specify the number of domain, QPS, and rule expansion packages you want to buy.

Step 7 In the lower right corner of the page, click **Next** and pay for the order.

NOTE

A WAF instance and its expansion packages have the same required duration.

----End

4.2 About Service Requests

4.2.1 How Do I Select Service QPS When Purchasing WAF?

WAF does not limit the protection bandwidth or shared bandwidth. It limits the service bandwidth and QPS. For details about service QPS, see **Edition Differences**.

What Is QPS?

The service QPS in WAF refers to the amount of normal traffic (unit: QPS) over all domain names and websites a WAF instance can protect. The QPS limit and bandwidth limit of a QPS expansion package:

- For web applications deployed on Huawei Cloud

  Service bandwidth: 50 Mbit/s

  QPS: 1,000 (Each HTTP GET request is a query.)

- For web applications not deployed on Huawei Cloud

  Service bandwidth: 20 Mbit/s

  QPS: 1,000 (Each HTTP GET request is a query.)

For details, see **QPS Expansion Packages**.

Before buying WAF, confirm the total inbound and outbound peak traffic of the websites to be protected by WAF. Ensure that the bandwidth of the WAF edition you select is greater than the total inbound peak traffic or the total outbound peak traffic, whichever is larger.

What Is Traffic?

Attack traffic must be removed in your estimations. For example, if your website is being accessed normally, WAF routes the traffic back to the origin ECS, but if your website is under attack, WAF blocks and filters out the illegitimate traffic, and routes only the legitimate traffic back to the origin ECS. The inbound and outbound traffic of the origin ECS you view on the ECS console is the normal traffic. If there are multiple ECSs, collect statistics on the normal traffic of all ECSs. For example, if you have six sites and the peak outbound traffic of each site does not exceed 2,000 QPS, then the total peak traffic volume does not exceed 12,000 QPS. In this case, you can buy the WAF platinum edition.

NOTE

Generally, the outbound traffic is larger than the inbound traffic.

What Happens If Website Traffic Exceeds the Service Bandwidth or Request Limit?

If your website normal traffic exceeds the service bandwidth or request limit offered by the edition you select, forwarding website traffic may be affected.

For example, traffic limiting and random packet loss may occur. Your website services may be unavailable, frozen, or respond very slowly.

In this case, upgrade your edition or buy additional QPS expansion packages.

4.2.2 Is Service QPS Calculated Based on Incoming Traffic or Outgoing Traffic?

The service QPS in WAF refers to the amount of normal traffic (unit: QPS) over all domain names and websites a WAF instance can protect.

Before buying WAF, confirm the total inbound and outbound peak traffic of the websites to be protected by WAF. Ensure that the bandwidth of the WAF edition you select is greater than the total inbound peak traffic or the total outbound peak traffic, whichever is larger.

Attack traffic must be removed in your estimations. For example, if your website is being accessed normally, WAF routes the traffic back to the origin ECS, but if your website is under attack, WAF blocks and filters out the illegitimate traffic, and routes only the legitimate traffic back to the origin ECS. The inbound and outbound traffic of the origin ECS you view on the ECS console is the normal traffic. If there are multiple ECSs, collect statistics on the normal traffic of all ECSs. For example, if you have six sites and the peak outbound traffic of each site does not exceed 2,000 QPS, then the total peak traffic volume does not exceed 12,000 QPS. In this case, you can buy the WAF platinum edition.

NOTE

Generally, the outbound traffic is larger than the inbound traffic.

For details about bandwidth, see **QPS Expansion Package**.

4.2.3 Does WAF Have a Limit on the Protection Bandwidth or Shared Bandwidth?

WAF does not limit the protection bandwidth or shared bandwidth. WAF limits the service bandwidth and QPS.

The service QPS in WAF refers to the amount of normal traffic (unit: QPS) over all domain names and websites a WAF instance can protect.

Before buying WAF, confirm the total inbound and outbound peak traffic of the websites to be protected by WAF. Ensure that the bandwidth of the WAF edition you select is greater than the total inbound peak traffic or the total outbound peak traffic, whichever is larger.

For details, see **Edition Differences**.

4.2.4 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

5 Website Domain Name Access Configuration

5.1 Domain Name and Port Configuration

5.1.1 How Do I Add a Domain Name/IP Address to WAF?

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 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.
- A domain name cannot be added to WAF repeatedly.

  Each combination of a domain name and a non-standard port is counted towards the domain name quota of the WAF edition you are using. For example, www.example.com:8080 and www.example.com:8081 use two domain names of the quota. If you want to protect web services over multiple ports with the same domain name, add the domain name and each port to WAF.

The following figure shows the process of connecting a website to WAF in each mode.

Figure 5-1 Process of connecting a website to WAF

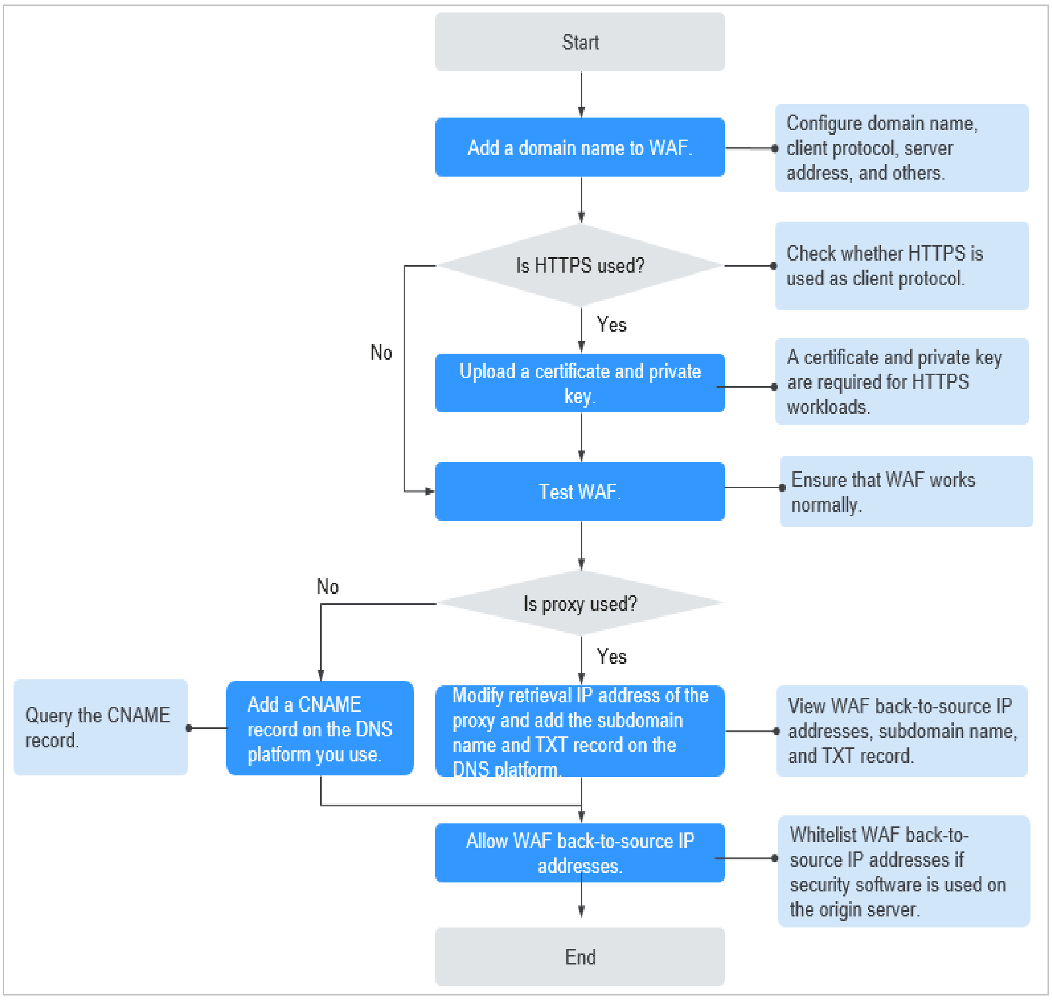
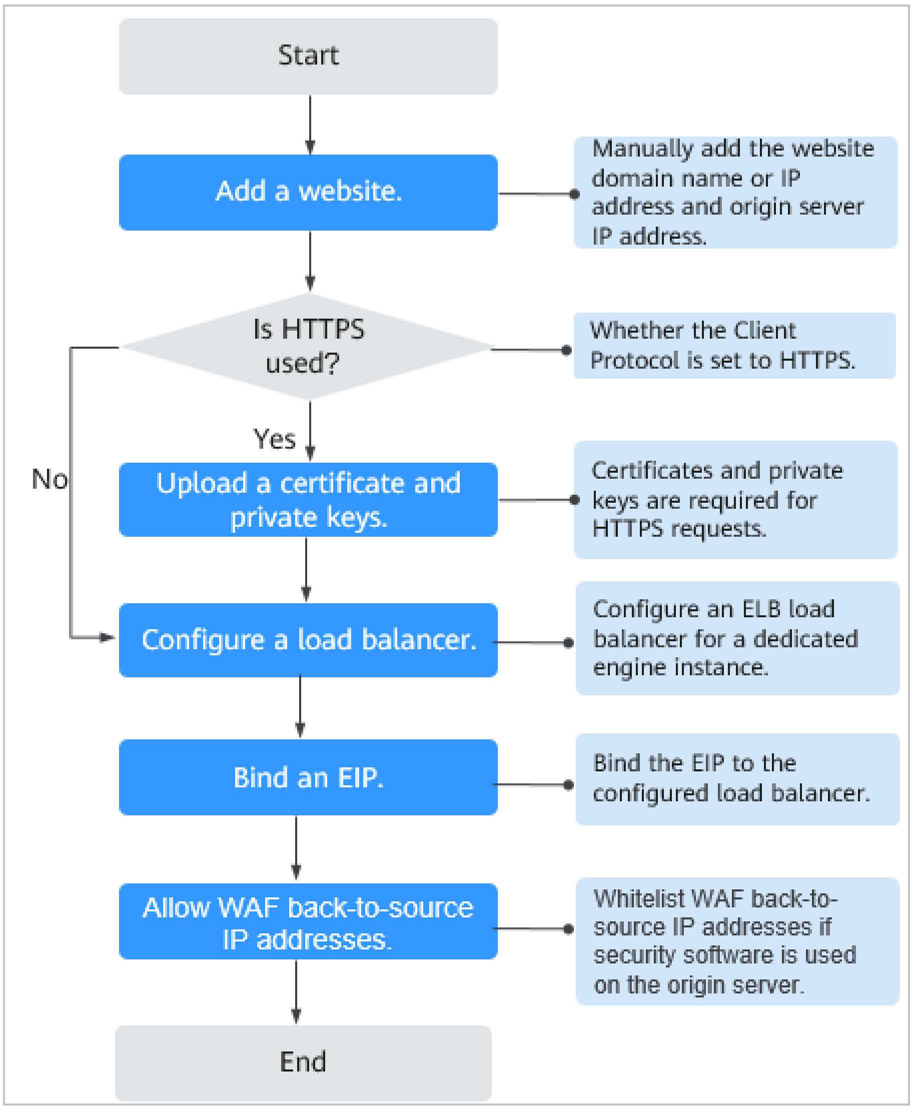

Start
Add a domain name to WAF.
Configure domain name, client protocol, server address, and others.
Is HTTPS used?
Check whether HTTPS is used as client protocol.
Yes
No
Upload a certificate and private key.
A certificate and private key are required for HTTPS workloads.
Test WAF.
Ensure that WAF works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

Figure 5-2 Process of connecting a website to a dedicated WAF instance


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

For more details, see **Adding a Domain Name to WAF**.

- If **Access Status** for protected website is **Inaccessible**, rectify the fault by referring to **Why Is My Domain Name or IP Address Inaccessible?**
- If your website becomes inaccessible after it is connected to WAF, rectify the issue by referring to **How Do I Troubleshoot 404/502/504 Errors?**

5.1.2 Which Non-Standard Ports Does WAF Support?

WAF can protect web applications that use WebSocket/WebSockets (enabled by default), HTTP or HTTPS through standard ports 80 and 443 or non-standard ports. Non-standard ports supported by WAF vary depending on the WAF edition you are using.

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.

Standard Ports

WAF can protect the following standard ports.

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

Non-standard Ports That Can Be Protected by Cloud WAF

Cloud WAF can protect many non-standard ports. Note that these non-standard ports are specified by WAF not the ports you use for your services. Which non-standard ports can be protected by WAF depends on WAF editions you are using.

Table 5-1 Non-standard ports that can be protected by cloud WAF

Edition	Non-standard Port That Can Be Protected	
	HTTP	HTTPS
Standard (pay-per-use)	81, 82, 83, 84, 86, 87, 88, 89, 800, 808, 5000, 7009, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8686, 8800, 8888, 8889, 8999, and 9001	4443, 5048, 5049, 5443, 6443, 7072, 7073, 7443, 8033, 8081, 8082, 8083, 8084, 8443, 8712, 8803, 8804, 8805, 8843, 9443, 8553, 8663, 9553, 9663, 18000, 18110, 18381, 18443, 18980, 19000, and 28443

Edition	Non-standard Port That Can Be Protected	
	HTTP	HTTPS
Professional	81, 82, 83, 84, 85, 86, 87, 88, 89, 97, 133, 134, 140, 141, 144, 151, 800, 808, 881, **888,** 1000, 1090, 1135, 1139, 1688, 3128, 3333, 3501, 3601, 4444, 5000, 5001, 5080, 55222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7080, 77081, 7082, 7083, 7088, 7097, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8004, 8007, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8024, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8182, 8232, 8334, 8336, 8686, 8800, 8813, 8814, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9007, 9020, 9021, 9022, 9023, 9024, 9025, 9026, 9027, 9028, 9029, 9037, 9050, 9077, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 9099, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9802, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9945, 9770, 10000, 10001, 10080, 10087, 11000, 12601, 13000, 14000, 18080, 18180, 18280, 19101, 19501, 21028, 23333, 27777, 28080, 30002, 30086, 33332, 33334, 33702, 40010, 48299, 48800, 52725, 52726, 60008, 60010	447, 882, 1818, 4006, 4430, 4443, 5048, 5049, 5100, 5443, 6443, 7072, 7073, 7443, 8033, 8043, 8081, 8082, 8083, 8084, 8211, 8221, 8224, 8231, 8243, 8244, 8281, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8810, 8815, 8817, 8836, 8838, 8840, 8842, 8843, 9005, 9053, 9090, 9443, 9553, 9663, 9681, 9682, 9999, 10002, 10300, 10301, 11001, 11003, 13001, 13003, 13080, 14003, 14443, 17618, 17718, 17818, 18000, 18001, 18010, 18110, 18381, 18443, 18980, 19000, 20000, 28443, and 60009

Edition	Non-standard Port That Can Be Protected	
	HTTP	HTTPS
Platinum	81, 82, 83, 84, 85, 86, 87, 88, 89, 97, 133, 134, 140, 141, 144, 151, 800, 808, 881, **888,** 1000, 1090, 1135, 1139, 1688, 3128, 3333, 3501, 3601, 4444, 5000, 5001, 5080, 5222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7081, 7082, 7083, 7088, 7097, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8004, 8006, 8007, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8024, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8182, 8232, 8334, 8336, 8686, 8800, 8813, 8814, 8888, 8889, 8899, 8989, 8999, 9000, 9001, 9002, 9003, 9007, 9020, 9021, 9022, 9023, 9024, 9025, 9026, 9027, 9028, 9029, 9037, 9050, 9077, 9080, 9081, 9082, 9099, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9770, 9802, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 9945, 10000, 10001, 10080, 10087, 11000, 12601, 13000, 14000, 18080, 18180, 18280, 23333, 27777, 28080, 30086, 33702, 48299, 48800	447, 882, 1818, 4006, 4430, 4443, 5048, 5049, 5443, 6443, 7072, 7073, 7443, 8033, 8043, 8081, 8082, 8083, 8084, 8211, 8221, 8224, 8231, 8243, 8244, 8281, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8810, 8815, 8817, 8836, 8838, 8840, 8842, 8843, 8848, 8910, 8920, 8950, 9005, 9053, 9090, 9182, 9184, 9190, 9443, 9553, 9663, 9681, 9682, 9999, 10002,10300, 10301, 11001, 11003, 13001, 13003, 13080, 14003, 17618, 17718, 17818, 18000, 18001, 18010, 18110, 18381, 18443, 18980, 19000, 28443, and 60009

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

If you use dedicated WAF instances, you can select any non-standard ports listed in **Table 5-2**.

Table 5-2 Non-standard ports that can be protected by dedicated waf instances

HTTP	HTTPS
81, 82, 83, 84, 86, 87, 88, 89, 97, 800, 808, 1000, 1090, 3128, 3333, 3501, 3601, 4444, 5000, 5080, 5222, 5555, 5601, 6001, 6666, 6699, 6788, 6789, 6842, 6868, 6969, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7070, 7080, 7081, 7082, 7083, 7088, 7097, 7510, 7777, 7800, 7979, 8000, 8001, 8002, 8003, 8008, 8009, 8010, 8011, 8012, 8013, 8014, 8015, 8016, 8017, 8020, 8021, 8022, 8025, 8026, 8070, 8077, 8078, 8080, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8093, 8094, 8095, 8096, 8097, 8098, 8106, 8118, 8181, 8334, 8336, 8686, 8800, 8888, 8889, 8989, 8999, 9000, 9001, 9002, 9003, 9021, 9023, 9027, 9037, 9080, 9081, 9082, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 9180, 9200, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 9770, 9802, 9945, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 10000, 10001, 10080, 12601, 19101, 19501, 19998, 21028, 28080, 30002, 33332, 33334, 33702, 40010, 48800, 52725, 52726, 60008, 60010	4443, 5443, 6443, 7072, 7073, 7443, 8033, 8081, 8082, 8083, 8084, 8443, 8445, 8553, 8663, 8712, 8750, 8803, 8804, 8805, 8843, 9443, 9553, 9663, 9999, 18000, 18010, 18110, 18381, 18443, 18980, 19000, and 28443

5.1.3 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

5.1.4 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.

5.1.5 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.

5.1.6 How Do I Configure Non-standard Ports When Adding a Protected Domain Name?

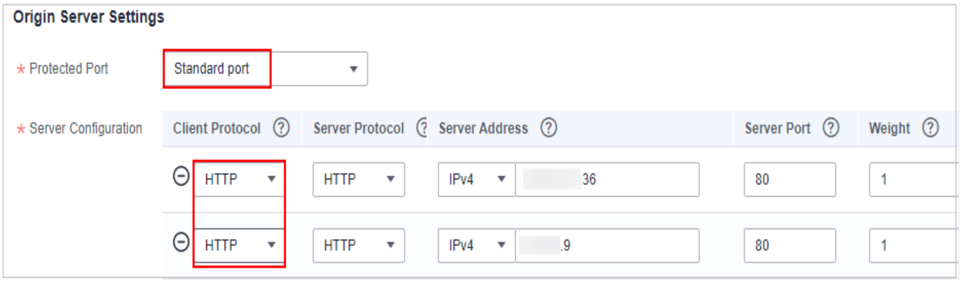
When you add a domain name to WAF, **Port** must be configured to the service port of your website. You can configure it by referring to the following instructions:

- 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 5-3** and **Figure 5-4** show standard port configurations when the client protocol is HTTP or HTTPS.

Figure 5-3 Port 80



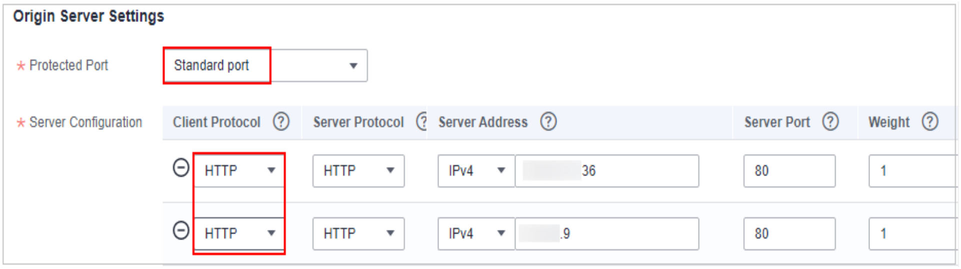
Origin Server Settings

* Protected Port: Standard port

* Server Configuration

Client Protocol	Server Protocol	Server Address		Server Port	Weight
HTTP	HTTP	IPv4	[redacted]36	80	1
HTTP	HTTP	IPv4	[redacted].9	80	1

Figure 5-4 Port 443



Origin Server Settings

* Protected Port: Standard port

* Server Configuration

Client Protocol	Server Protocol	Server Address	Server Port	Weight
HTTP	HTTP	IPv4 [redacted]36	80	1
HTTP	HTTP	IPv4 [redacted].9	80	1

NOTE

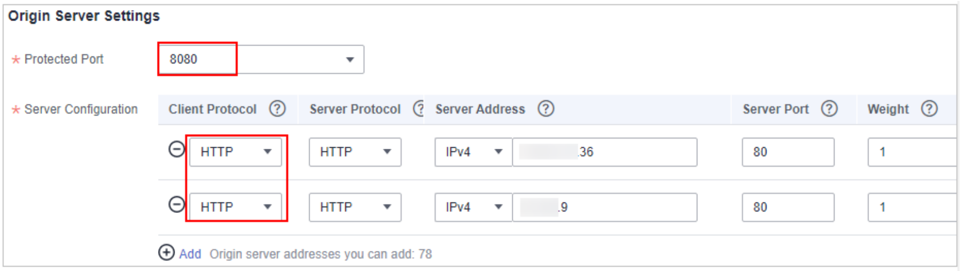
If **Client Protocol** is set to **HTTPS**, a certificate is required.

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 5-5** and **Figure 5-6** show the configuration of non-standard HTTP or HTTPS port, respectively.

Figure 5-5 Other HTTP port besides port 80



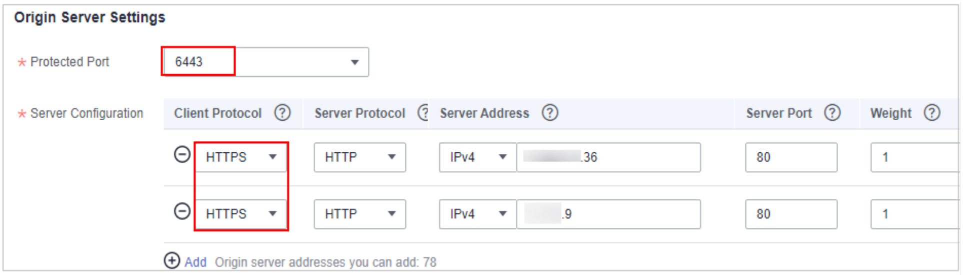
Origin Server Settings

* Protected Port: 8080

* Server Configuration

Client Protocol	Server Protocol	Server Address	Server Port	Weight
HTTP	HTTP	IPv4 [redacted]36	80	1
HTTP	HTTP	IPv4 [redacted].9	80	1

Figure 5-6 Other HTTPS port besides port 443



Origin Server Settings

* Protected Port: 6443

* Server Configuration

Client Protocol	Server Protocol	Server Address	Server Port	Weight
HTTPS	HTTP	IPv4 [redacted].36	80	1
HTTPS	HTTP	IPv4 [redacted].9	80	1

NOTE

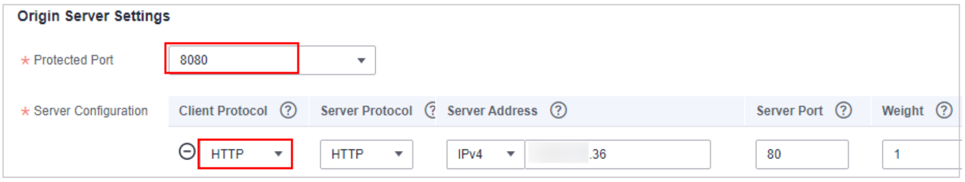
If **Client Protocol** is set to **HTTPS**, a certificate is required.

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 5-7** and **Figure 5-8**.

Figure 5-7 Protecting port 8080



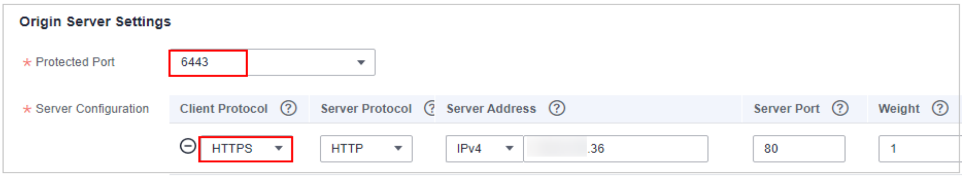
Origin Server Settings

* Protected Port: 8080

* Server Configuration

Client Protocol	Server Protocol	Server Address	Server Port	Weight
HTTP	HTTP	IPv4 [redacted].36	80	1

Figure 5-8 Protecting port 6443



Origin Server Settings

* Protected Port: 6443

* Server Configuration

Client Protocol	Server Protocol	Server Address	Server Port	Weight
HTTPS	HTTP	IPv4 [redacted].36	80	1

5.1.7 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.

For more details, see **Adding a Domain Name to WAF**.

5.1.8 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 buy.

Table 5-3 Domain name information required

Information	Parameter	Description	Example
Whether a proxy is used for the domain name	Proxy Configured	This parameter must be set to **Yes** if a layer-7 web proxy, such as CDN and cloud acceleration service, has been deployed for your website before you connect the website to WAF.	-
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
	Standard/Non-standard Port	The service port corresponding to the domain name of the website you want to protect. ● Standard ports – 80: default port when the client protocol is HTTP – 443: default port when the client protocol is HTTPS ● Non-standard ports Ports other than ports 80 and 443 **NOTICE** If your website uses a non-standard port, check whether the WAF edition you plan to buy can protect the non-standard port before you make a purchase. For details, see **Which Non-Standard Ports Does WAF Support?**	80
	HTTP/2 Used	HTTP/2 can be used only for access between the client and WAF on the condition that at least one origin server has **HTTPS** used for **Client Protocol**.	-
	Client Protocol	Protocol used by a client (for example, a browser) to access the website. WAF supports HTTP and HTTPS.	HTTP
	Server Protocol	Protocol used by WAF to forward requests from the client (such as a browser). The options are **HTTP** and **HTTPS**.	HTTP

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

5.1.9 How Do I Safely Delete a Protected Domain Name?

To delete a website, see **Removing 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.

5.1.10 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.

5.1.11 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.

5.1.12 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.

5.1.13 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, perform local verification by referring to **Testing WAF** before modifying the DNS configuration.
- To prevent other users from configuring your domain names on WAF in advance (this will cause interference on your domain name protection), add the subdomain name and TXT record on your DNS management platform. WAF can determine which user owns the domain name based on the subdomain name and TXT record.

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 5-4**.

Table 5-4 Operation guide

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

Procedure

For details, see **Connecting a Domain Name to WAF**.

5.1.14 What Can I Do If the Message "Illegal server address" Is Displayed When I Add a Domain Name?

Symptom

When a user adds a domain name to be protected, the system displays a message indicating that the origin server address is invalid.

Possible Causes

- **Server Address** is set to a private IP address reserved for internal use.
- The protected object and origin server addresses are set to the same IP address.

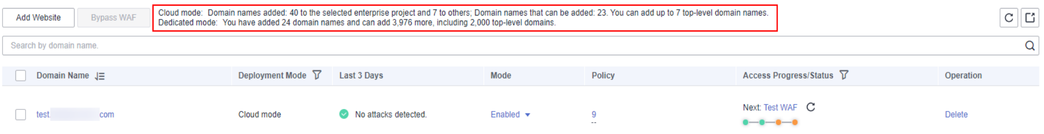
Handling Suggestions

Set **Server Address** to the actual origin server IP address (public IP address) or an independent back-to-source domain name, which cannot be the same as the protected domain name.

5.1.15 Why Am I Seeing That My Domain Quota Is Insufficient When There Is Still Remaining Quota?

The domain name quota contains top-level and second-level domain names. This happens when your quota for the top-level domain name is used up but you try to add a top-level domain name to WAF.

On the **Website Settings** page, you can view your domain name quota.



Cloud mode: Domain names added: 40 to the selected enterprise project and 7 to others; Domain names that can be added: 23. You can add up to 7 top-level domain names.
Dedicated mode: You have added 24 domain names and can add 3,976 more, including 2,000 top-level domains.

Search by domain name.

Domain Name	Deployment Mode	Last 3 Days	Mode	Policy	Access Progress/Status	Operation
test.[redacted]com	Cloud mode	✓ No attacks detected.	Enabled ▾	9 --	Next: Test WAF	Delete

5.1.16 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.

5.1.17 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.

5.2 Certificate Management

5.2.1 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.

5.2.2 Do I Need to Import the Certificates That Have Been Uploaded to ELB to WAF?

You can select a created certificate or import a new certificate. You need to import the certificate that has been uploaded to ELB to WAF.

5.2.3 How Do I Convert a Certificate into PEM Format?

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

Table 5-5 Certificate conversion commands

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

NOTE

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

5.3 Server Configuration

5.3.1 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:

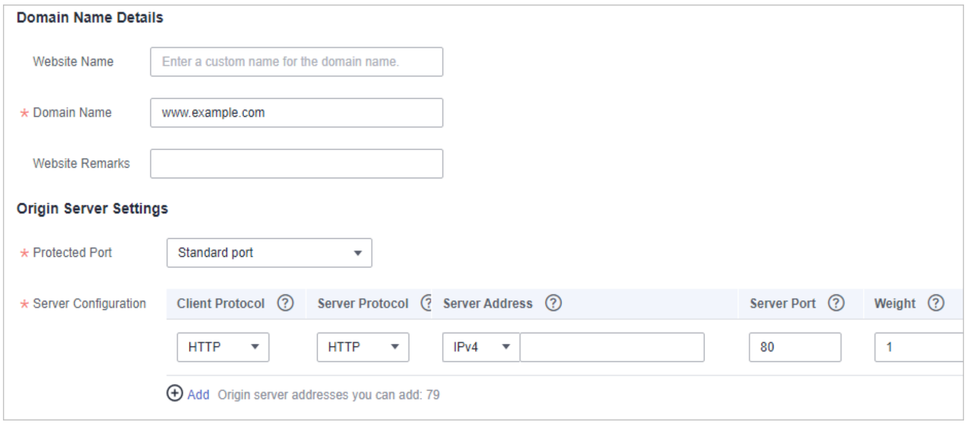
HTTP Access - 302 Redirection Response

Set **Client Protocol** and **Server Protocol** to **HTTP**. **Figure 5-9** 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 5-9 HTTP mode



Domain Name Details

Website Name: Enter a custom name for the domain name.

* Domain Name: www.example.com

Website Remarks:

Origin Server Settings

* Protected Port: Standard port

* Server Configuration

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

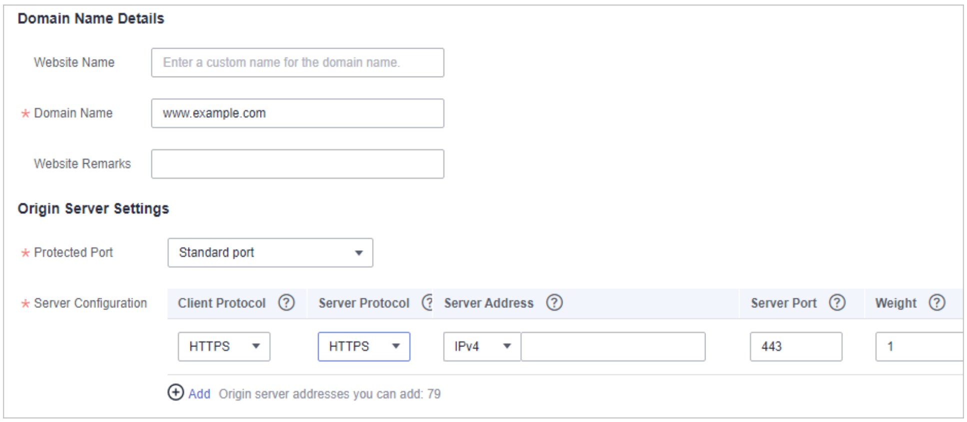
⊕ Add Origin server addresses you can add: 79

HTTPS Forcible Conversion

Set **Client Protocol** and **Server Protocol** to **HTTPS**. **Figure 5-10** 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.



Domain Name Details

Website Name: Enter a custom name for the domain name.

* Domain Name: www.example.com

Website Remarks:

Origin Server Settings

* Protected Port: Standard port

* Server Configuration

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

Add Origin server addresses you can add: 79

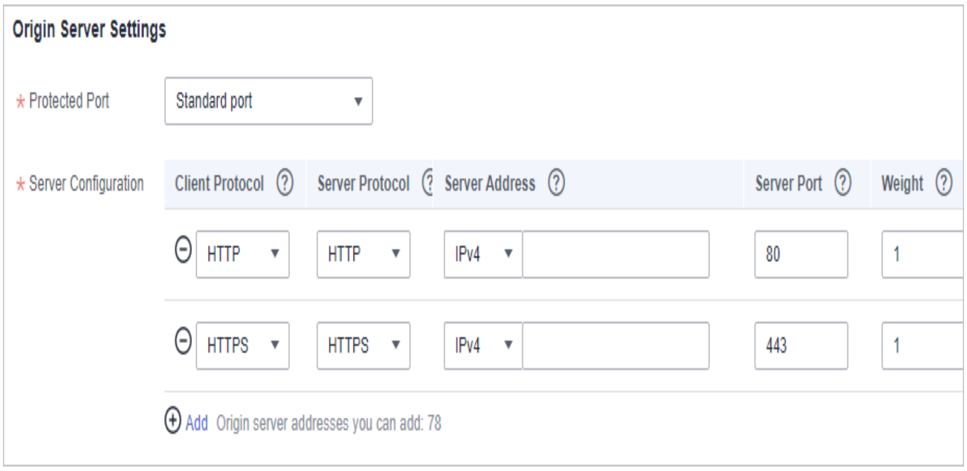
Figure 5-10 HTTPS redirection

HTTP and HTTPS

Set **Client Protocol** and **Server Protocol**. **Figure 5-11** 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.



Origin Server Settings

* Protected Port: Standard port

* Server Configuration

Client Protocol	Server Protocol	Server Address		Server Port	Weight
HTTP	HTTP	IPv4		80	1
HTTPS	HTTPS	IPv4		443	1

Add Origin server addresses you can add: 78

Figure 5-11 HTTP and HTTPS forwarding

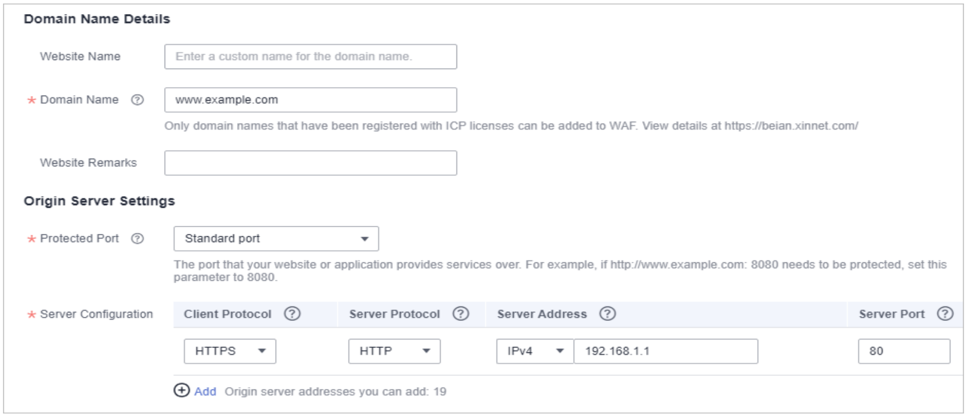
HTTPS Offloading

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 5-12 HTTPS offloading



Domain Name Details

Website Name: Enter a custom name for the domain name.

* Domain Name: www.example.com

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

Website Remarks:

Origin Server Settings

* Protected Port: Standard port

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.

* Server Configuration

Client Protocol	Server Protocol	Server Address	Server Port
HTTPS	HTTP	IPv4 192.168.1.1	80

Origin server addresses you can add: 19

5.3.2 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?**

5.3.3 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.

For details, see **Adding a Domain Name to WAF**.

5.4 Domain Name Resolution

5.4.1 How Do I Modify DNS Record on Huawei Cloud DNS?

If your website can be accessible directly through a client (such as a browser) before you add the website domain name to WAF, after the domain name is added to WAF, point the domain name to the WAF CNAME using your DNS platform. In this way, the traffic destined for your website goes to WAF first. WAF then checks the traffic, blocks attacks, and forwards only normal traffic to the origin server.

This topic uses Huawei Cloud DNS as an example to describe how to modify DNS record. The methods to modify DNS record on other platform are similar.

Prerequisites

- You have selected **Cloud** for **Protection** when adding the website domain name to WAF.
- To ensure that WAF forwards requests properly, verify WAF and domain name connection locally before modifying the DNS configuration by referring to **Testing WAF**.

Constraints

- The CNAME record must be unique for the same host record. You need to change the existing CNAME record of your domain name to WAF CNAME record.
- Record sets of different types in the same zone may conflict with each other. For example, for the same host record, the CNAME record conflicts with other records such as A record, MX record, and TXT record. If the record type cannot be directly changed, you can delete the conflicting records and add a CNAME record. Deleting other records and adding a CNAME record should be completed in as short time as possible. If no CNAME record is added after the A record is deleted, domain resolution may fail.
- To prevent other users from configuring your domain name on WAF before you add it to WAF (this will interfere with WAF protection for your domain name), add the subdomain name and TXT record on your DNS management platform. This helps WAF identify real domain name ownership.
- A modified record set takes effect when the cache duration specified by the TTL of the original record set expires. If the carrier sets a longer cache duration, the record set will take effect after this period of time elapses.

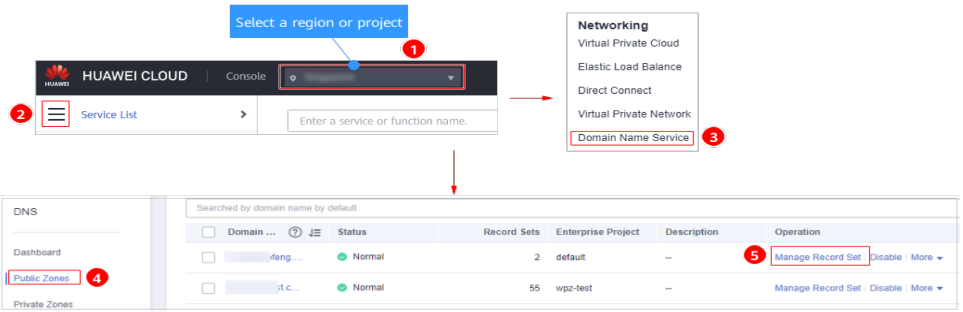
Procedure

Go to the **Website Settings** page on the WAF console and click ⧉ in the **Access Status** column in the domain row to copy the CNAME record.

Perform the following steps to modify DNS record:

1. Access the DNS resolution page, as shown in **Figure 5-13**.

Figure 5-13 DNS page



Domain ...	Status	Record Sets	Enterprise Project	Description	Operation
[redacted]feng....	Normal	2	default	--	Manage Record Set | Disable | More
[redacted]t c...	Normal	55	wpz-test	--	Manage Record Set | Disable | More

2. In the **Operation** column of the target domain name, click **Modify**. The **Modify Record Set** page is displayed.
3. In the displayed **Modify Record Set** dialog box, change the record.
   - **Name**: Domain name configured in WAF
   - **Type**: Select **CNAME - Map one domain to another**.
   - **Line**: **Default**
   - **TTL (s)**: The recommended value is **5 min**. A larger TTL value will make it slower for synchronization and update of DNS records.
   - **Value**: Change it to the copied CNAME value from WAF.
   - Keep other settings unchanged.

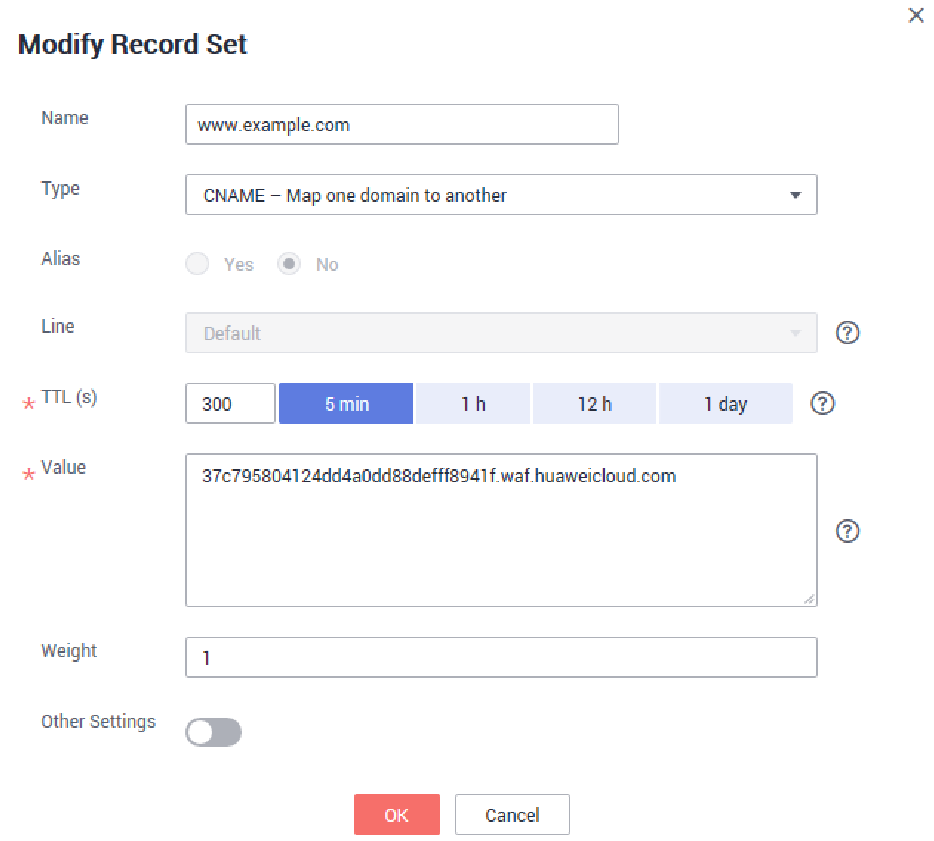
NOTE

About modifying the resolution record:

- The CNAME record must be unique for the same host record. The existing CNAME record must be changed to the WAF CNAME record.
- Record sets of different types in the same zone may conflict with each other. For example, for the same host record, the CNAME record conflicts with another record, such as the A record, MX record, or TXT record. If the record type cannot be changed, you can delete the conflicting records and add a CNAME record. Deleting other records and adding a CNAME record should be completed in as short time as possible. If no CNAME record is added after the A record is deleted, domain resolution may fail.

For details about the restrictions on domain name resolution types, see **Why Is a Message Indicating Conflict with an Existing Record Set Displayed When I Add a Record Set?**

Figure 5-14 Modifying a record set



Modify Record Set

Name: www.example.com

Type: CNAME – Map one domain to another

Alias: ○ Yes ● No

Line: Default

* TTL (s): 300 [✓ 5 min] 1 h 12 h 1 day

* Value: 37c795804124dd4a0dd88defff8941f.waf.huaweicloud.com

Weight: 1

Other Settings: ○

4. Click **OK**.

5.4.2 How Do I Verify Domain Ownership Using Huawei Cloud DNS?

Verification by DNS typically requires operations from your domain name administrator. If you are managing your domain name on Huawei Cloud and the domain name is in your account, perform the verification in Huawei Cloud DNS.

NOTICE

If your domain name is hosted on other platforms, such as www.net.cn, www.xinnet.com, and www.dnspod.cn, perform the verification on the corresponding platform. For example, if your domain name is hosted on Alibaba Cloud, perform the verification on Alibaba Cloud.

For example, the following shows how to add a TXT record **2019030700000022ams1xbyevdn4jvahact9xzpicb565k9443mryw2qe99mbzpb** for domain name **domain3.com**. The procedure to verify domain ownership using HUAWEI CLOUD DNS is similar.

Prerequisites

You have obtained the configuration information (host record and record value) required for domain name verification.

Procedure

Step 1 Log in to the management console.

Step 2 Choose **Domain Name Service** under **Network** to go to the **Domain Name Service** page.

Step 3 In the navigation pane on the left, choose > **Public Zones**.

Step 4 On the displayed **Public Zones** page, click domain name **domain3.com**.

Step 5 On the **Record Sets** tab page, in the upper left corner, click **Add Record Set**.

NOTE

If there is a TXT record of domain name **domain3.com** in the domain name list, click **Modify** in the **Operation** column. Modify the record in the displayed **Modify Record Set** dialog box.

- **Name**: Enter the prefix of the host record returned by the domain name service provider on the domain name verification page.

  The returned host record varies depending on the domain name service provider. The following are two examples:

  Example:

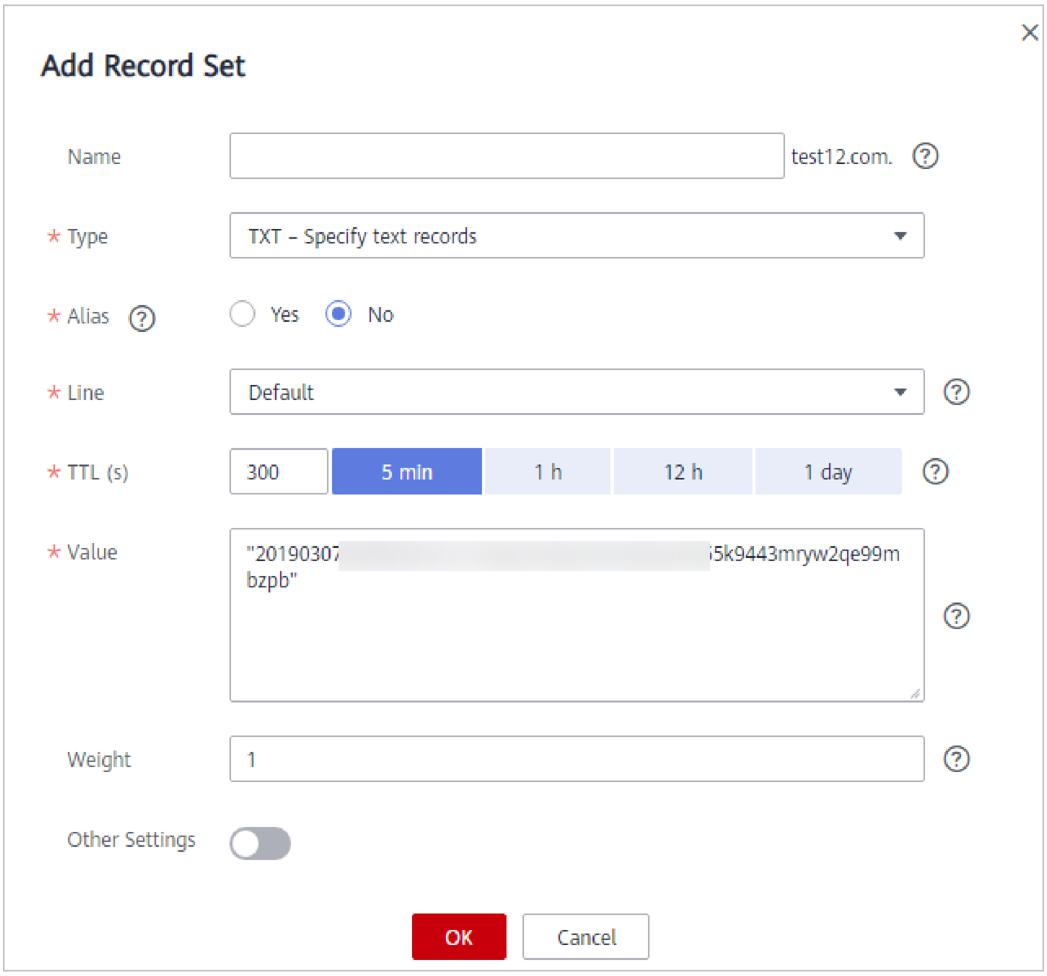
  – If the host record returned by the domain name service provider is **_dnsauth.domain3.com**, set **Name** to **_dnsauth**.

  – If the host record returned by the domain name service provider is **domain3.com**, leave **Name** empty.
- **Type**: Select **TXT – Specify text records**.
- **Line**: Select **Default**.
- **TTL (s)**: The recommended value is **5 min**. A larger TTL value will make it slower for synchronization and update of DNS records.
- **Value**: Enter the record value returned by the domain name service provider on the domain ownership verification page.

  NOTE

  Record values must be quoted with quotation marks and then pasted in the text box.
- Keep other settings unchanged.

Figure 5-15 Adding a record set



Add Record Set

Name: test12.com.

* Type: TXT – Specify text records

* Alias: ○ Yes ● No

* Line: Default

* TTL (s): 300 | 5 min | 1 h | 12 h | 1 day

* Value: "20190307[redacted]5k9443mryw2qe99mbzpb"

Weight: 1

Other Settings

Step 6 Click **OK**.

If the status of the record set is **Normal**, the record set is added successfully.

NOTE

- DNS configuration records can be deleted only after the certificate is issued or revoked.
- Check whether the DNS record is correctly configured. If not, the certificate cannot be issued.
- After the domain ownership verification completes, it takes a period of time for the CA to confirm the verification. During this period, the certificate is in the **Pending domain name verification** state. The certificate enters the **Pending organization verification** state only after the CA has confirmed your domain ownership.

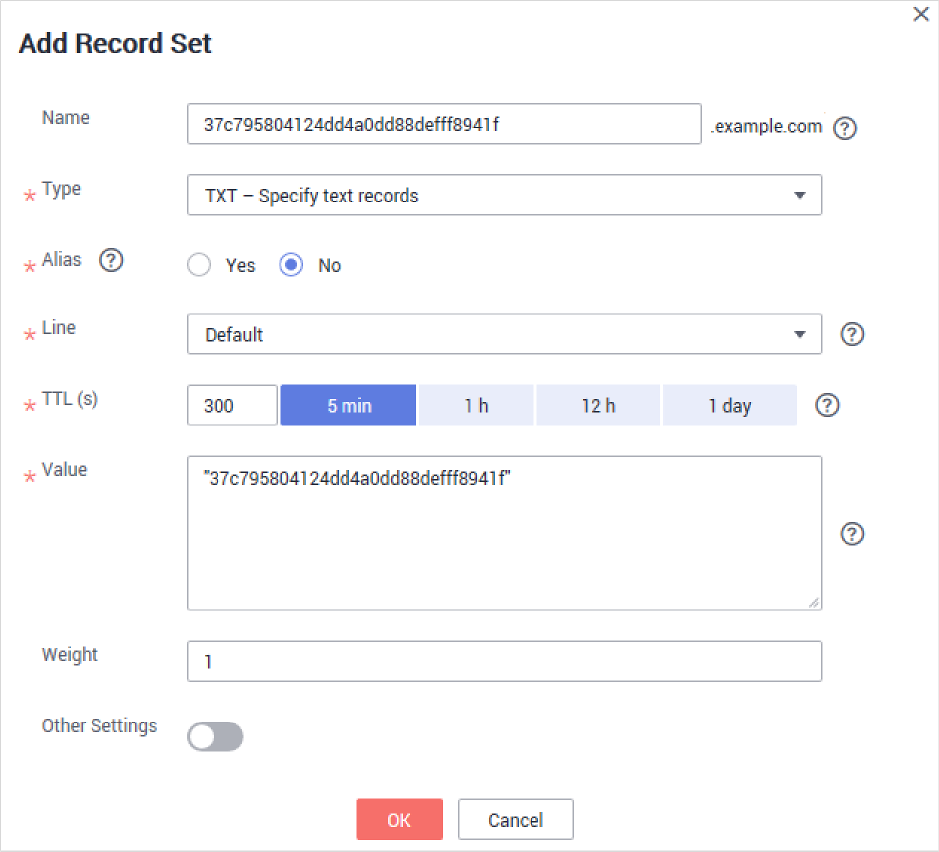
----End

5.4.3 How Do I Configure the TXT Record on HUAWEI CLOUD DNS Service?

After you add the domain name of the proxy, such as Advanced Anti-DDoS (AAD), in WAF, configured the subdomain name and TXT record at your DNS provider to protect your domain names. If other users configure the same domain name in WAF, your protection for the domain name will be adversely affected.

If you use the DNS service on HUAWEI CLOUD, add double quotation marks ("") to the TXT record and paste them in the text box, for example, "37c795804124dd4a0dd88defff8941f".

Figure 5-16 Adding a record set



Add Record Set

Name: 37c795804124dd4a0dd88defff8941f .example.com

* Type: TXT – Specify text records

* Alias: ○ Yes ● No

* Line: Default

* TTL (s): 300

* Value: "37c795804124dd4a0dd88defff8941f"

Weight: 1

Other Settings

For details about how to configure a subdomain name and TXT record on the DNS service on HUAWEI CLOUD, see **What Are Impacts If No Subdomain Name and TXT Record Are Configured?**

5.4.4 What Are Impacts If No Subdomain Name and TXT Record Are Configured?

If the domain name uses a proxy product, such as advanced anti-DDoS, but the subdomain name and TXT record are not configured on the corresponding DNS platform, WAF cannot identify the domain name ownership.

To prevent other users from configuring your domain name on WAF before you add it to WAF (this will interfere with WAF protection for your domain name), add the subdomain name and TXT record on your DNS management platform. This helps WAF identify real domain name ownership.

How to Determine

Your domain name is in gray in the domain name list, and the working mode is **Suspended** and cannot be switched to **Enabled**. If this symptom occurs, your domain name has been occupied by another user.

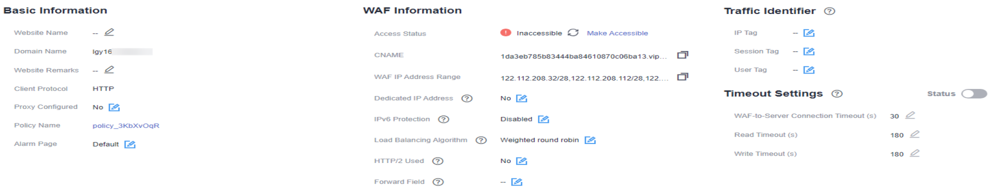
Solution

Go to your DNS provider, add a subdomain name, and configure a TXT record for the subdomain name. The following uses domain name ***www.example.com*** as an example to describe how to configure the DNS service on Huawei Cloud.

Step 1 Obtain the values of **Subdomain Name** and **TXT Record**.

1. Log in to the management console.
2. Click ☰ in the upper left corner of the management console and choose **Security** > **Web Application Firewall**. In the navigation pane, choose **Website Settings**.
3. In the **Domain Name** column, click domain name ***www.example.com*** to go to the **Basic Information** page.
4. In the **Access Status** row, click **Make Accessible**.

Figure 5-17 Domain name access information



Basic Information

Website Name --
Domain Name lgy16[redacted]
Website Remarks --
Client Protocol HTTP
Proxy Configured No
Policy Name policy_3KbXvOqR
Alarm Page Default

WAF Information

Access Status Inaccessible Make Accessible
CNAME 1da3eb785b83444ba84610870c06ba13.vip...
WAF IP Address Range 122.112.208.32/28,122.112.208.112/28,122....
Dedicated IP Address No
IPv6 Protection Disabled
Load Balancing Algorithm Weighted round robin
HTTP/2 Used No
Forward Field --

Traffic Identifier

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

Timeout Settings Status

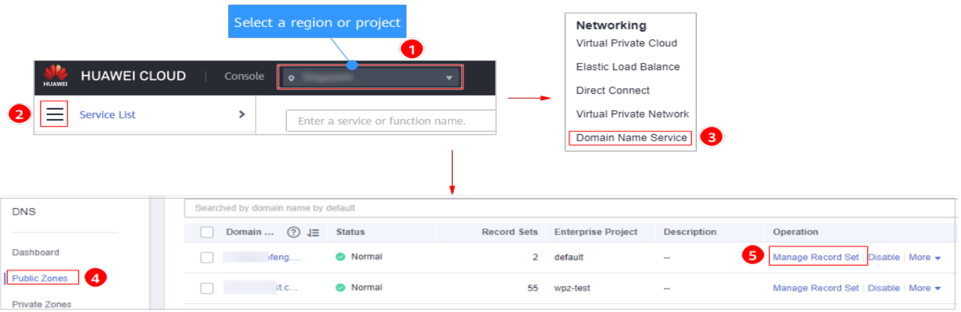
WAF-to-Server Connection Timeout (s) 30
Read Timeout (s) 180
Write Timeout (s) 180

5. In the displayed dialog box, click ❐ to copy the TXT record.

Step 2 Add a WAF subdomain name and TXT record at your DNS provider.

1. In the **Operation** column of domain name ***www.example.com***, click **Add Record Set**. **Figure 5-18** shows the example.

Figure 5-18 DNS page

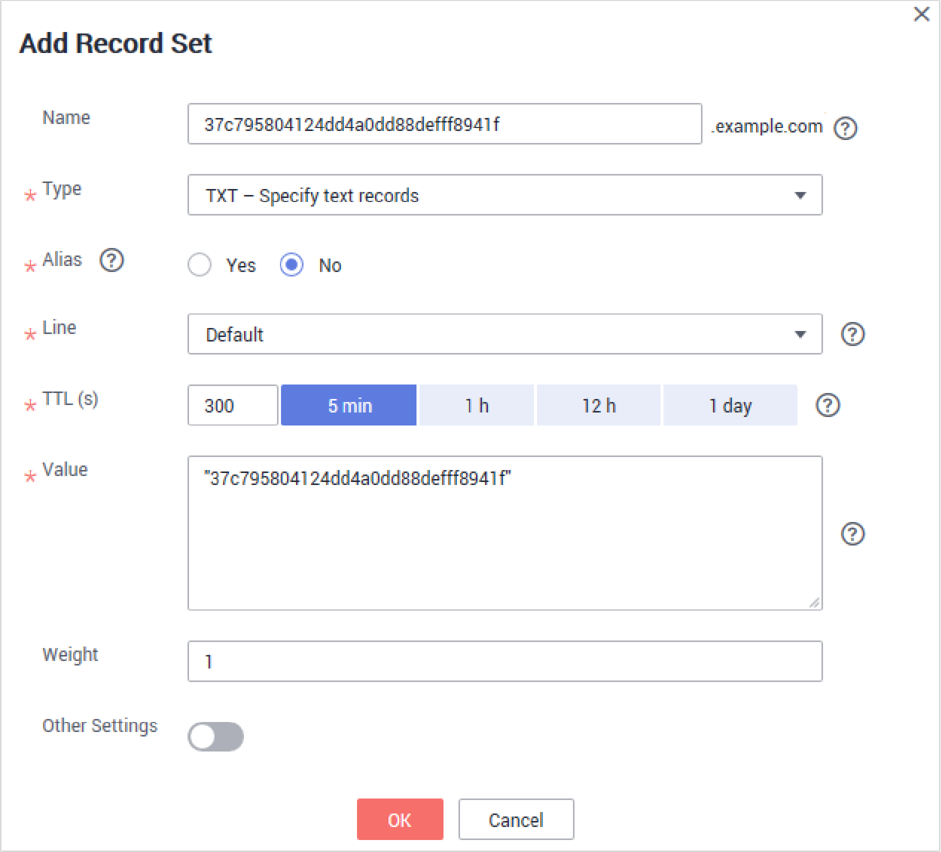


Domain ...	Status	Record Sets	Enterprise Project	Description	Operation
[redacted]feng....	Normal	2	default	--	Manage Record Set | Disable | More
[redacted]t.c...	Normal	55	wpz-test	--	Manage Record Set | Disable | More

2. In the upper left corner, click **Add Record Set** to go to the **Add Record Set** page.
   - **Name**: Paste the TXT record copied in **Step 1.5** to the text box.
   - **Type**: Select **TXT – Specify text records**.
   - **Alias**: Select **No**.
   - **Line**: Select **Default**.
   - **TTL (s)**: The recommended value is **5 min**. A larger TTL value will make it slower for synchronization and update of DNS records.

- **Value**: Add quotation marks to the TXT record copied from **Step 1.5** and paste them in the text box, for example, "37c795804124dd4a0dd88defff8941f".
- Keep other settings unchanged.

Figure 5-19 Adding a record set



Add Record Set

Name: 37c795804124dd4a0dd88defff8941f .example.com

* Type: TXT – Specify text records

* Alias: ○ Yes ● No

* Line: Default

* TTL (s): 300 | 5 min | 1 h | 12 h | 1 day

* Value: "37c795804124dd4a0dd88defff8941f"

Weight: 1

Other Settings:

3. Click **OK**.

----End

5.5 Operations After Connecting Websites to WAF

5.5.1 Can I Access a Website Using an IP Address After a Domain Name Is Connected to WAF?

After a domain name is connected to WAF, you can enter the origin server IP address in the address bar of the browser to access the website. However, your origin server IP address is easily exposed. As a result, attackers can bypass WAF and attack your origin server.

You are advised to configure origin server protection according to the instructions in **Origin Server Protection**.

5.5.2 How Do I Test WAF?

Before you direct the traffic to WAF, perform local verification to ensure that all configurations are correct.

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

For details, see **Testing WAF**.

5.5.3 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.

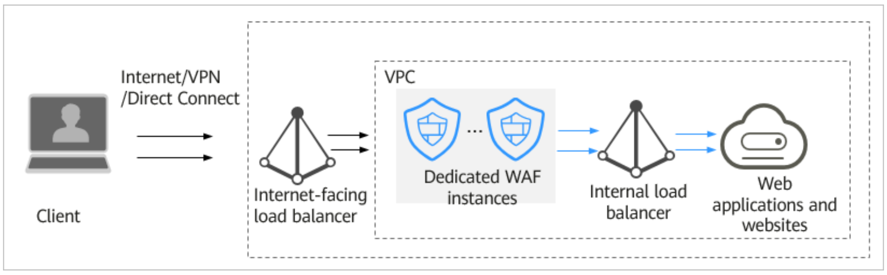
If you select **Cloud - CNAME** or **Dedicated** for **Protection**, take the following steps to route your website traffic to origin servers.

- 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.

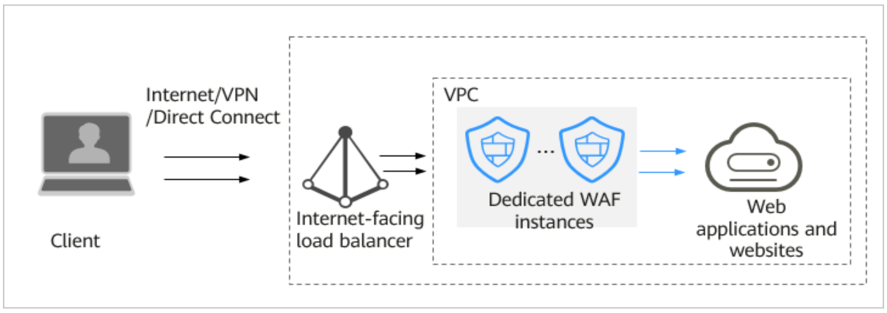
- Dedicated mode
  - If your website has a private network load balancer deployed behind the dedicated WAF instance, as shown in **Figure 5-20**, unbind the EIP from the internet-facing load balancer and then bind the EIP to the private load balancer. In doing so, your website traffic will bypass WAF and directly go to the origin server.

    Figure 5-20 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 5-21**, 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 5-21 Dedicated WAF instance deployment architecture (no private network load balancer deployed behind dedicated WAF instances)



Constraints

You can switch the WAF working mode to **Bypassed** only when **Cloud mode** is selected for the website and your website encounters any of the following issues:

- 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.

Configuring CNAME Access in Cloud Mode

The following procedure walks you through how to configure the WAF **Bypassed** mode.

Step 1 Log in to the management console.

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

Step 3 Click in the upper left corner 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

Procedure for Bypassing a Dedicated WAF Instance in Scenarios Where a Private Network Load Balancer Is Deployed Behind a WAF Instance

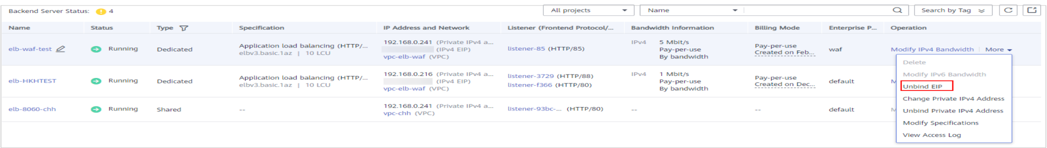
You can unbind the EIP from the public network load balancer and then bind it to the private load balancer so that the traffic to your protected website can bypass WAF and directly go to the origin server.

Step 1 Click in the upper left corner of the management console and select a region or project.

Step 2 Click ☰ in the upper left corner of the page and choose **Elastic Load Balance** under **Network** to go to the **Load Balancers** page.

Step 3 On the **Load Balancers** page, locate the row that contains the internet-facing load balancer, click **More** in the **Operation** column, and select **Unbind IPv4 EIP**. **Figure 5-22** shows an example.

Figure 5-22 Unbinding an EIP from an internet-facing load balancer



Name	Status	Type	Specification	IP Address and Network	Listener (Frontend Protocol/...	Bandwidth Information	Billing Mode	Enterprise P...	Operation
elb-waf-test	Running	Dedicated	Application load balancing (HTTP/... elbv3.basic.1az | 10 LCU	192.168.0.241 (Private IPv4 a... [redacted] (IPv4 EIP) vpc-elb-waf (VPC)	listener-85 (HTTP/85)	IPv4 5 Mbit/s Pay-per-use By bandwidth	Pay-per-use Created on Feb...	waf	Modify IPv4 Bandwidth | More
elb-HKHTEST	Running	Dedicated	Application load balancing (HTTP/... elbv3.basic.1az | 10 LCU	192.168.0.216 (Private IPv4 a... [redacted] (IPv4 EIP) vpc-elb-waf (VPC)	listener-3729 (HTTP/88) listener-f366 (HTTP/80)	IPv4 1 Mbit/s Pay-per-use By bandwidth	Pay-per-use Created on Dec...	default	M
elb-8060-chh	Running	Shared	--	192.168.0.241 (Private IPv4 a... vpc-chh (VPC)	listener-93bc-... (HTTP/80)	--	--	default	M

Step 4 In the displayed dialog box, click **Yes** to unbind the EIP from the load balancer.

Step 5 On the **Load Balancers** page, locate the row that contains the private load balancer, click **More** in the **Operation** column, and select **Bind IPv4 EIP**.

Step 6 In the displayed **Bind IPv4 EIP** dialog box, select the public IP address you unbind in **Step 3** and click **OK**.

----End

Procedure for Bypassing a Dedicated WAF Instance in Scenarios Where No Private Network Load Balancer Is Deployed Behind WAF Instances

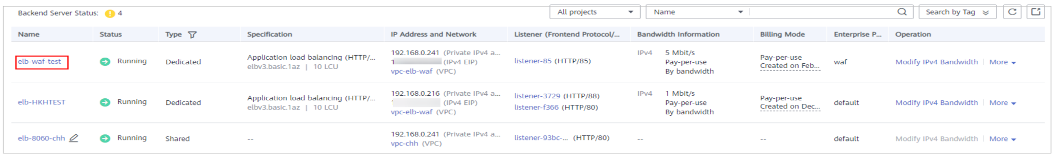
You can remove the dedicated WAF instance from the public network load balancer and add the origin server to the internet-facing load balancer so that the traffic to your website can bypass WAF and directly go to the origin server.

Step 1 Click in the upper left corner of the management console and select a region or project.

Step 2 Click ☰ in the upper left corner of the page and choose **Elastic Load Balance** under **Network** to go to the **Load Balancers** page.

Step 3 Click the name of the load balancer you want in the **Name** column to go to the **Basic Information** page.

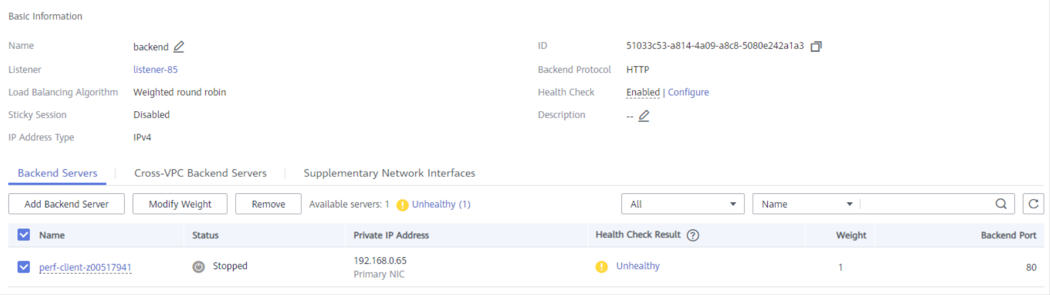
Figure 5-23 Load balancer list



Name	Status	Type	Specification	IP Address and Network	Listener (Frontend Protocol/...	Bandwidth Information	Billing Mode	Enterprise P...	Operation
elb-waf-test	Running	Dedicated	Application load balancing (HTTP/... elbv3.basic.1az | 10 LCU	192.168.0.241 (Private IPv4 a... 1[redacted] (IPv4 EIP) vpc-elb-waf (VPC)	listener-85 (HTTP/85)	IPv4 5 Mbit/s Pay-per-use By bandwidth	Pay-per-use Created on Feb...	waf	Modify IPv4 Bandwidth | More
elb-HKHTEST	Running	Dedicated	Application load balancing (HTTP/... elbv3.basic.1az | 10 LCU	192.168.0.216 (Private IPv4 a... [redacted] (IPv4 EIP) vpc-elb-waf (VPC)	listener-3729 (HTTP/88) listener-f366 (HTTP/80)	IPv4 1 Mbit/s Pay-per-use By bandwidth	Pay-per-use Created on Dec...	default	Modify IPv4 Bandwidth | More
elb-8060-chh	Running	Shared	--	192.168.0.241 (Private IPv4 a... vpc-chh (VPC)	listener-93bc-... (HTTP/80)	--	--	default	Modify IPv4 Bandwidth | More

Step 4 Click the **Backend Server Groups** tab, select the dedicated WAF instance you want to remove, and click **Remove** in the **Operation** column. **Figure 5-24** shows an example.

Figure 5-24 Removing a dedicated WAF instance from an internet-facing load balancer



Basic Information

Name: backend

ID: 51033c53-a814-4a09-a8c8-5080e242a1a3

Listener: listener-85

Backend Protocol: HTTP

Load Balancing Algorithm: Weighted round robin

Health Check: Enabled | Configure

Sticky Session: Disabled

Description: --

IP Address Type: IPv4

Available servers: 1 Unhealthy (1)

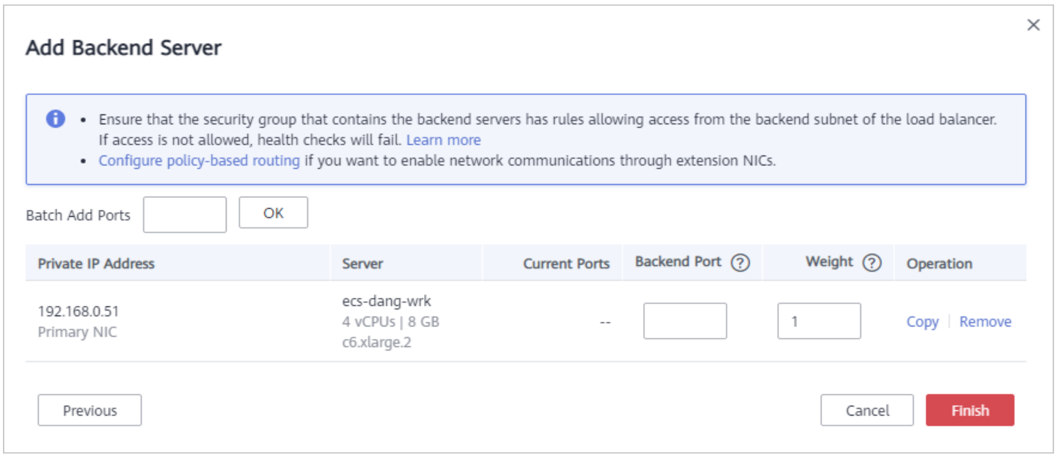
☑ Name	Status	Private IP Address	Health Check Result	Weight	Backend Port
☑ perf-client-z00517941	Stopped	192.168.0.65 Primary NIC	Unhealthy	1	80

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

Step 6 Click **Add Backend Server** and select servers in the displayed **Add Backend Server** dialog box.

Step 7 Click **Next**, configure a backend port, and click **Finish**.

Figure 5-25 Adding origin servers as backend servers



Add Backend Server

- Ensure that the security group that contains the backend servers has rules allowing access from the backend subnet of the load balancer. If access is not allowed, health checks will fail. Learn more
- Configure policy-based routing if you want to enable network communications through extension NICs.

Batch Add Ports

Private IP Address	Server	Current Ports	Backend Port	Weight	Operation
192.168.0.51 Primary NIC	ecs-dang-wrk 4 vCPUs | 8 GB c6.xlarge.2	--		1	Copy | Remove

----End

6 Service Interruption Check

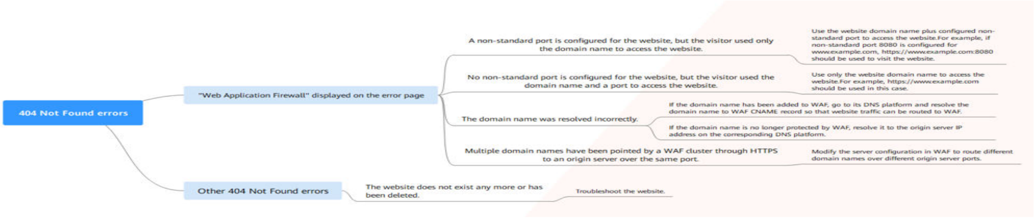
6.1 How Do I Troubleshoot 404/502/504 Errors?

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

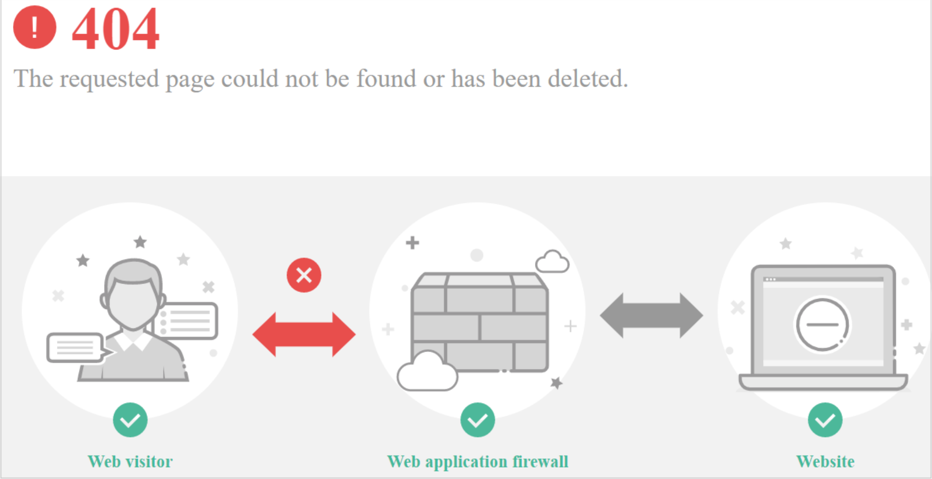
Refer to **Figure 6-1** to fix the 404 Not Found error occurred after your website is connected to WAF.

Figure 6-1 Troubleshooting for 404 Not Found error


404 Not Found errors
"Web Application Firewall" displayed on the error page
A non-standard port is configured for the website, but the visitor used only the domain name to access the website.
Use the website domain name plus configured non-standard port to access the website.For example, if non-standard port 8080 is configured for www.example.com, https://www.example.com:8080 should be used to visit the website.
No non-standard port is configured for the website, but the visitor used the domain name and a port to access the website.
Use only the website domain name to access the website.For example, https://www.example.com should be used in this case.
The domain name was resolved incorrectly.
If the domain name has been added to WAF, go to its DNS platform and resolve the domain name to WAF CNAME record so that website traffic can be routed to WAF.
If the domain name is no longer protected by WAF, resolve it to the origin server IP address on the corresponding DNS platform.
Multiple domain names have been pointed by a WAF cluster through HTTPS to an origin server over the same port.
Modify the server configuration in WAF to route different domain names over different origin server ports.
Other 404 Not Found errors
The website does not exist any more or has been deleted.
Troubleshoot the website.

- If the page shown in **Figure 6-2** is displayed, the possible causes and solutions are as follows:

Figure 6-2 404 page

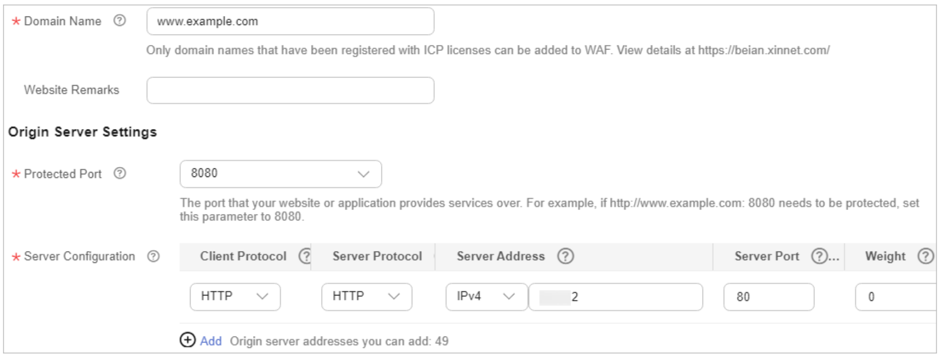


404

The requested page could not be found or has been deleted.

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 6-3**. 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 6-3 Configuration of a non-standard port



* Domain Name: www.example.com

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

Website Remarks:

Origin Server Settings

* Protected Port: 8080

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.

* Server Configuration

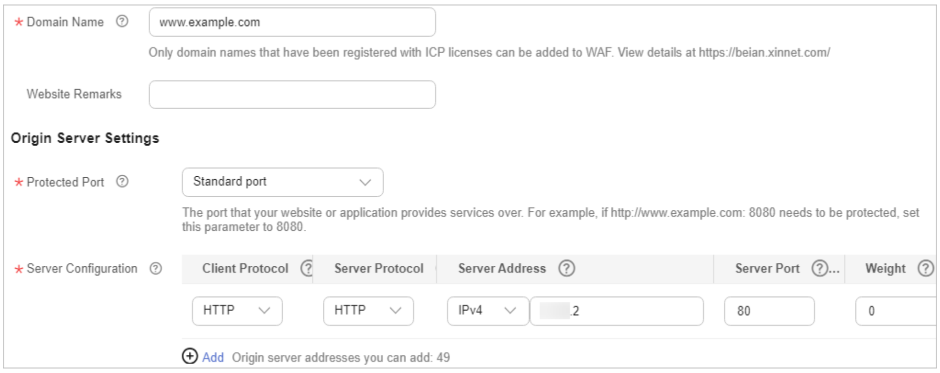
Client Protocol	Server Protocol	Server Address		Server Port	Weight
HTTP	HTTP	IPv4	[redacted]2	80	0

Origin server addresses you can add: 49

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 6-4** is configured.

Figure 6-4 Non-standard port not configured



* Domain Name: www.example.com

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

Website Remarks:

Origin Server Settings

* Protected Port: Standard port

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.

* Server Configuration

Client Protocol	Server Protocol	Server Address		Server Port	Weight
HTTP	HTTP	IPv4	[redacted].2	80	0

Add Origin server addresses you can add: 49

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 **Routing Website Traffic to WAF**.
- 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 6-2**, 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 6-5** to fix the issue.

Figure 6-5 Troubleshooting process for 502 Bad Gateway error

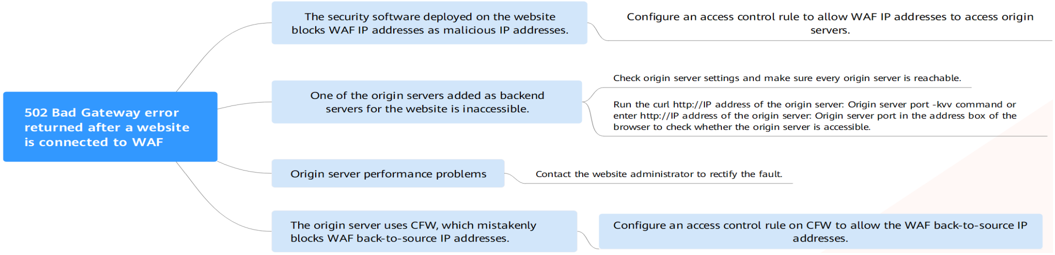

502 Bad Gateway error returned after a website is connected to WAF
The security software deployed on the website blocks WAF IP addresses as malicious IP addresses.
Configure an access control rule to allow WAF IP addresses to access origin servers.
One of the origin servers added as backend servers for the website is inaccessible.
Check origin server settings and make sure every origin server is reachable.
Run the curl http://IP address of the origin server: Origin server port -kvv command or enter http://IP address of the origin server: Origin server port in the address box of the browser to check whether the origin server is accessible.
Origin server performance problems
Contact the website administrator to rectify the fault.
The origin server uses CFW, which mistakenly blocks WAF back-to-source IP addresses.
Configure an access control rule on CFW to allow the WAF back-to-source IP addresses.

Table 6-1 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. ● 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.
Cause 4: The origin server uses CFW, which blocks WAF IP addresses.	Troubleshooting methods: ● If the origin server uses CFW, view the block logs on the CFW console to check whether related events are generated. ● View the access control policy in CFW and check whether the back-to-source IP address of WAF is blocked. On the CFW, allow the back-to-source IP address. For details, see **Configuring an Access Control Policy**.

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.

Step 7 Check whether each origin server can be accessed properly.

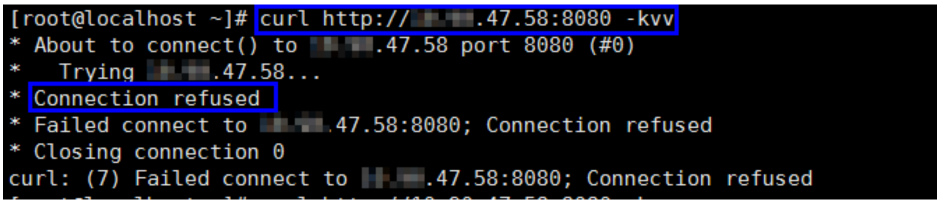
- Run the following command on the server:

```
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 6-6 Command output for checking origin server



```
[root@localhost ~]# curl http://[redacted].47.58:8080 -kvv
* About to connect() to [redacted].47.58 port 8080 (#0)
*   Trying [redacted].47.58...
* Connection refused
* Failed connect to [redacted].47.58:8080; Connection refused
* Closing connection 0
curl: (7) Failed connect to [redacted].47.58:8080; Connection refused
```

  - 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.

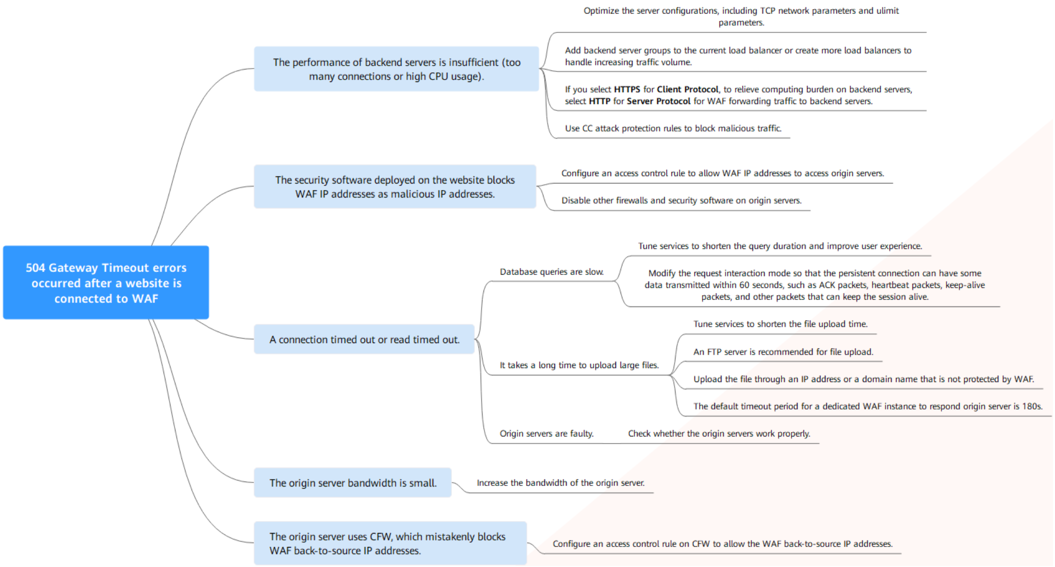
If not, restart it.

----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 6-7** to fix 504 gateway timeout errors.

Figure 6-7 Troubleshooting process for 504 Gateway Timeout errors



504 Gateway Timeout errors occurred after a website is connected to WAF

The performance of backend servers is insufficient (too many connections or high CPU usage).

Optimize the server configurations, including TCP network parameters and ulimit parameters.

Add backend server groups to the current load balancer or create more load balancers to handle increasing traffic volume.

If you select **HTTPS** for **Client Protocol**, to relieve computing burden on backend servers, select **HTTP** for **Server Protocol** for WAF forwarding traffic to backend servers.

Use CC attack protection rules to block malicious traffic.

The security software deployed on the website blocks WAF IP addresses as malicious IP addresses.

Configure an access control rule to allow WAF IP addresses to access origin servers.

Disable other firewalls and security software on origin servers.

A connection timed out or read timed out.

Database queries are slow.

Tune services to shorten the query duration and improve user experience.

Modify the request interaction mode so that the persistent connection can have some data transmitted within 60 seconds, such as ACK packets, heartbeat packets, keep-alive packets, and other packets that can keep the session alive.

It takes a long time to upload large files.

Tune services to shorten the file upload time.

An FTP server is recommended for file upload.

Upload the file through an IP address or a domain name that is not protected by WAF.

The default timeout period for a dedicated WAF instance to respond origin server is 180s.

Origin servers are faulty.

Check whether the origin servers work properly.

The origin server bandwidth is small.

Increase the bandwidth of the origin server.

The origin server uses CFW, which mistakenly blocks WAF back-to-source IP addresses.

Configure an access control rule on CFW to allow the WAF back-to-source IP addresses.

Table 6-2 Troubleshooting 504 Gateway Timeout errors

Possible Cause	Troubleshooting	Solution
Cause 1: Backend server performance issues (such as too many connections or high CPU usage)	If the origin server performance is insufficient, check the origin server access logs and access traffic to analyze issues.	● 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 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.
Cause 2 ● 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.	Follow the solutions below for troubleshooting: ● 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.	● Configure an access control policy on the origin server to whitelist WAF IP addresses. For details, see **How Do I Whitelist IP Address Ranges of Cloud WAF?** ● Disable other firewalls and security software on origin servers.

Possible Cause	Troubleshooting	Solution
Cause 3: Connection timeout and read timeout **NOTE** ● 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.	Troubleshooting methods: ● 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.	● Database queries are slow. – Tune services to shorten the query duration and improve user experience. – Modify the request interaction mode so that the persistent connection can have some data transmitted within 60 seconds, such as ACK packets, heartbeat packets, keep-alive packets, and other packets that can keep the session alive. ● It takes a long time to upload large files. – Tune services to shorten the file upload time. – An FTP server is recommended for file upload. – Upload the file through an IP address or a domain name that is not protected by WAF. ● The 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.	Troubleshooting methods: ● 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.
Cause 5: **WAF IP addresses are blocked by CFW used by origin servers.**	Troubleshooting methods: ● If the origin server uses CFW, view the block logs on the CFW console to check whether related events are generated. ● View the access control policy in CFW and check whether the back-to-source IP address of WAF is blocked.	On the CFW console, allow the back-to-source IP address. For details, see **Configuring an Access Control Policy**.

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**.

Step 7 Set the **Server Address** to the EIP bound to the load balancer.

Step 8 Click **OK**.

----End

6.2 Why Is My Domain Name or IP Address Inaccessible?

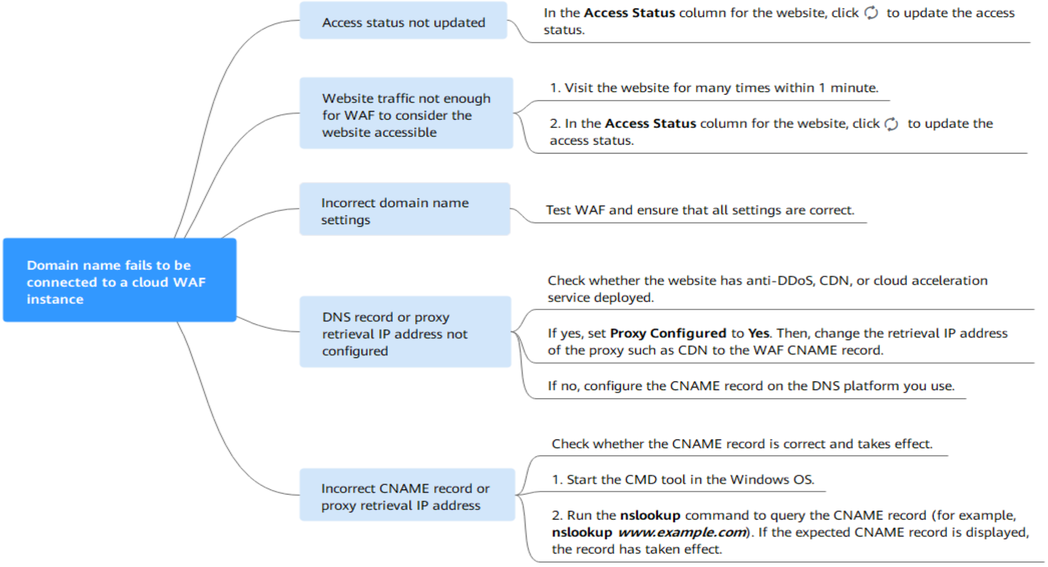
Symptoms

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 6-8** and **Table 6-3** to fix connection failures for websites protected in cloud mode.

Figure 6-8 Troubleshooting for Cloud WAF



Domain name fails to be connected to a cloud WAF instance

Access status not updated

In the **Access Status** column for the website, click ⟳ to update the access status.

Website traffic not enough for WAF to consider the website accessible

1. Visit the website for many times within 1 minute.

2. In the **Access Status** column for the website, click ⟳ to update the access status.

Incorrect domain name settings

Test WAF and ensure that all settings are correct.

DNS record or proxy retrieval IP address not configured

Check whether the website has anti-DDoS, CDN, or cloud acceleration service deployed.

If yes, set **Proxy Configured** to **Yes**. Then, change the retrieval IP address of the proxy such as CDN to the WAF CNAME record.

If no, configure the CNAME record on the DNS platform you use.

Incorrect CNAME record or proxy retrieval IP address

Check whether the CNAME record is correct and takes effect.

1. Start the CMD tool in the Windows OS.

2. Run the **nslookup** command to query the CNAME record (for example, **nslookup** ***www.example.com***). If the expected CNAME record is displayed, the record has taken effect.

Table 6-3 Solutions for failures of WAF instances

Possible Cause	Solution
Cause 1: **Access Status** of **Protected Website** not updated	In the **Access Status** column for the protected website, click ⟳ to update the status.
Cause 2: Website access traffic not enough for WAF to consider the website accessible **NOTICE** After you connect a website to WAF, the website is considered accessible only when WAF detects at least 20 requests to the website within 5 minutes.	1. Access the protected website for many times within 1 minute. 2. In the **Access Status** column for the website, click ⟳ to update the status.

Possible Cause	Solution
Cause 3: Incorrect domain name settings	**NOTICE** WAF can protect the website using the following types of domain names: ● Top-level domain names, for example, example.com ● Single domain names/Second-level domains, for example, www.example.com ● Wildcard domain names, for example, *.example.com Domain names example.com and www.example.com are different. Ensure that correct domain names are added to WAF. Perform the following steps to ensure that the domain name settings are correct. 1. In Windows OSs, choose **Start** > **Run**. Then enter **cmd** and press **Enter**. 2. Ping the CNAME record of the domain name to obtain the WAF back-to-source IP address. 3. Use a text editor to open the **hosts** file. Generally, the **hosts** file is stored in the **C:\Windows\System32\drivers\etc\** directory. 4. Add a record into the **hosts** file in the format of ***DomainName WAF back-to-source IP address***. 5. Save the **hosts** file after the record is added. In the CLI, run the **ping** *Domain name added to WAF* command, for example, ping www.example.com. If the WAF back-to-source IP address in **2** is displayed in the command output, the domain name settings are correct. For details, see **Testing WAF**. If there are incorrect domain name settings, remove the

Possible Cause	Solution
	domain name from WAF and add it to WAF again.
Cause 4: DNS record or the back-to-source IP addresses of proxies not configured	Check whether the website connected to WAF uses proxies such as advanced anti-DDoS, CDN, and cloud acceleration service. ● Yes. – Change the back-to-source IP address of the proxy such as CDN to the CNAME record of WAF. – (Optional) Add a WAF subdomain name and TXT record at your DNS provider. ● If no, contact your DNS service provider to configure a CNAME record for the domain name. For details, see **Connecting a Domain Name to WAF**.
Cause 5: Incorrect DNS record or proxy back-to-source address	Perform the following steps to check whether the domain name CNAME record takes effect: 1. In Windows OSs, choose **Start** > **Run**. Then enter **cmd** and press **Enter**. 2. Run a **nslookup** command to query the CNAME record. If the command output displays the CNAME record of WAF, the record takes effect. Using www.example.com as an example, the output is as follows: `nslookup www.example.com` If the CNAME record fails to take effect, modify the DNS record or back-to-source address. For details, see **Connecting a Domain Name to WAF**.

6.3 How Do I Handle False Alarms as WAF Blocks Normal Requests to My Website?

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

NOTICE

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

In the row containing the false alarm event, click **Details** in the **Operation** column and view the event details. If you are sure that the event is a false positive, handle it as a false alarm by referring to **Table 6-4**. 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 6-4 Handling false alarms

Type of Hit Rule	Hit Rule	Handling Method
WAF built-in protection rules	● Basic web protection rules Basic web protection defends against common web attacks, such as SQL injection, XSS attacks, remote buffer overflow attacks, file inclusion, Bash vulnerability exploits, remote command execution, directory traversal, sensitive file access, and command and code injections. Basic web protection also detects web shells and evasion attacks. ● Feature-based anti-crawler protection Feature-based anti-crawler identifies and blocks crawler behavior from search engines, scanners, script tools, and other crawlers.	In the row containing the attack event, click **Handle as False Alarm** in the **Operation** column. For details, see **Handling False Alarms**.

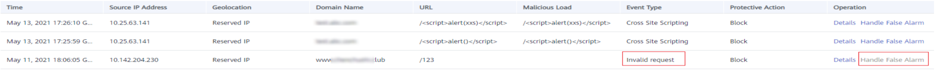
Type of Hit Rule	Hit Rule	Handling Method
Custom protection rules	● CC attack protection rules ● Precise protection rules ● Blacklist and whitelist rules ● Geolocation access control rules ● Web tamper protection rules ● JavaScript anti-crawler protection ● Information leakage prevention rules ● Data masking rules	Go to the page displaying the hit rule and delete it.
Other	Invalid access requests **NOTE** If either of the following cases, WAF blocks the access request as an invalid request: ● When **form-data** is used for POST or PUT requests, the number of parameters in a form exceeds 8,192. ● The URI contains more than 2,048 parameters. ● The number of headers exceeds 512.	Allow the blocked requests by referring to **Configuring a Precise Protection Rule**. The **Handle as False Alarm** button is grayed out for events that are generated against a precise protection rule.

6.4 Why Does WAF Block Normal Requests as Invalid Requests?

Symptom

After a website is connected to WAF, a normal access request is blocked by WAF. On the **Events** page, the corresponding **Event Type** reads **Invalid request**, and the **Handle False Alarm** button is grayed out, as shown in **Figure 6-9**.

Figure 6-9 Normal requests blocked by WAF as invalid requests



Time	Source IP Address	Geolocation	Domain Name	URL	Malicious Load	Event Type	Protective Action	Operation
May 13, 2021 17:26:10 G...	10.25.63.141	Reserved IP	[redacted]	/<script>alert(xxs)</script>	/<script>alert(xxs)</script>	Cross Site Scripting	Block	Details Handle False Alarm
May 13, 2021 17:25:59 G...	10.25.63.141	Reserved IP	[redacted]	/<script>alert()</script>	/<script>alert()</script>	Cross Site Scripting	Block	Details Handle False Alarm
May 11, 2021 18:06:05 G...	10.142.204.230	Reserved IP	www[redacted]lub	/123		Invalid request	Block	Details Handle False Alarm

Possible Cause

If either of the following cases, WAF blocks the access request as an invalid request:

- When **form-data** is used for POST or PUT requests, the number of parameters in a form exceeds 8,192.

- The URI contains more than 2,048 parameters.
- The number of headers exceeds 512.

Solution

If you confirm that the blocked request is a normal request, allow it by **configuring a precise protection rule**.

6.5 Why Is the Handle False Alarm Button Grayed Out?

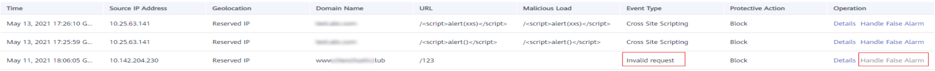
Verify that you have the permissions for WAF. For details, see **WAF Permissions Management**.

NOTICE

If you have enabled **Enterprise Project**, select an enterprise project and handle false alarms in the project.

- 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.
- If either of the following numbers in an access request exceeds 512, WAF will block the request as an invalid request and gray out the **Handle False Alarm** button.
  - 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.

Figure 6-10 Normal requests blocked by WAF as invalid requests



Time	Source IP Address	Geolocation	Domain Name	URL	Malicious Load	Event Type	Protective Action	Operation
May 13, 2021 17:26:10 G...	10.25.63.141	Reserved IP	[redacted]	/<script>alert(xxs)</script>	/<script>alert(xxs)</script>	Cross Site Scripting	Block	Details Handle False Alarm
May 13, 2021 17:25:59 G...	10.25.63.141	Reserved IP	[redacted]	/<script>alert()</script>	/<script>alert()</script>	Cross Site Scripting	Block	Details Handle False Alarm
May 11, 2021 18:06:05 G...	10.142.204.230	Reserved IP	www[redacted]lub	/123		Invalid request	Block	Details Handle False Alarm

To handle an invalid request, refer to **Why Does WAF Block Normal Requests as Invalid Requests?**

6.6 How Do I Whitelist IP Address Ranges of Cloud WAF?

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

NOTICE

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

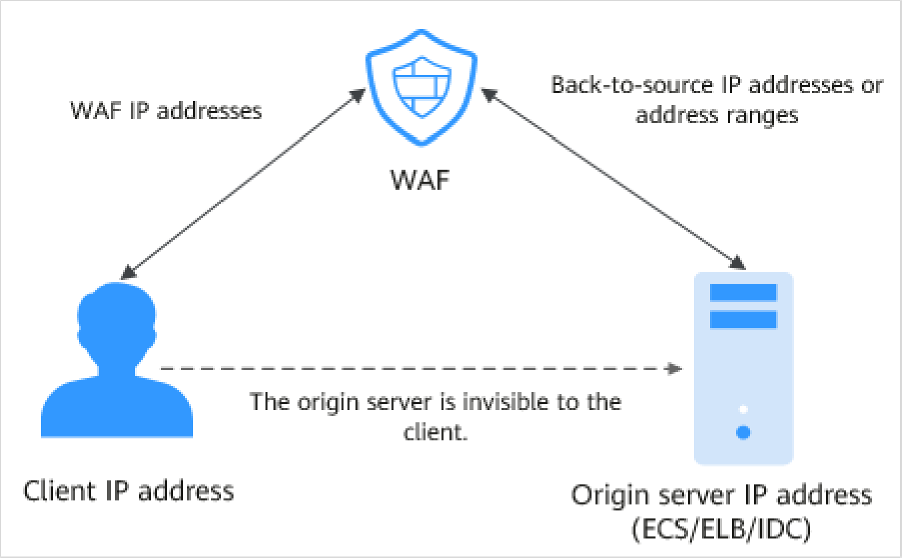
What Are Back-to-Source IP Addresses?

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

NOTE

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

Figure 6-11 Back-to-source IP address


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

WAF Back-to-Source IP Address Check Mechanism

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

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.

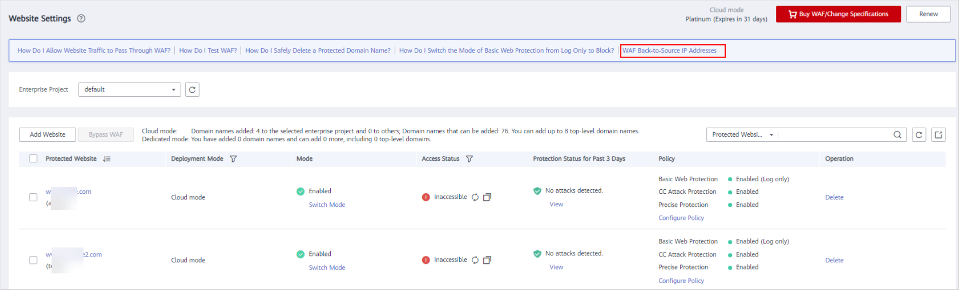
Step 2 Click in the upper left corner of the management console and select a region or project.

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**.

Figure 6-12 WAF Back-to-Source IP Addresses



Website Settings

Cloud mode
Platinum (Expires in 31 days)

How Do I Allow Website Traffic to Pass Through WAF? | How Do I Test WAF? | How Do I Safely Delete a Protected Domain Name? | How Do I Switch the Mode of Basic Web Protection from Log Only to Block? | WAF Back-to-Source IP Addresses

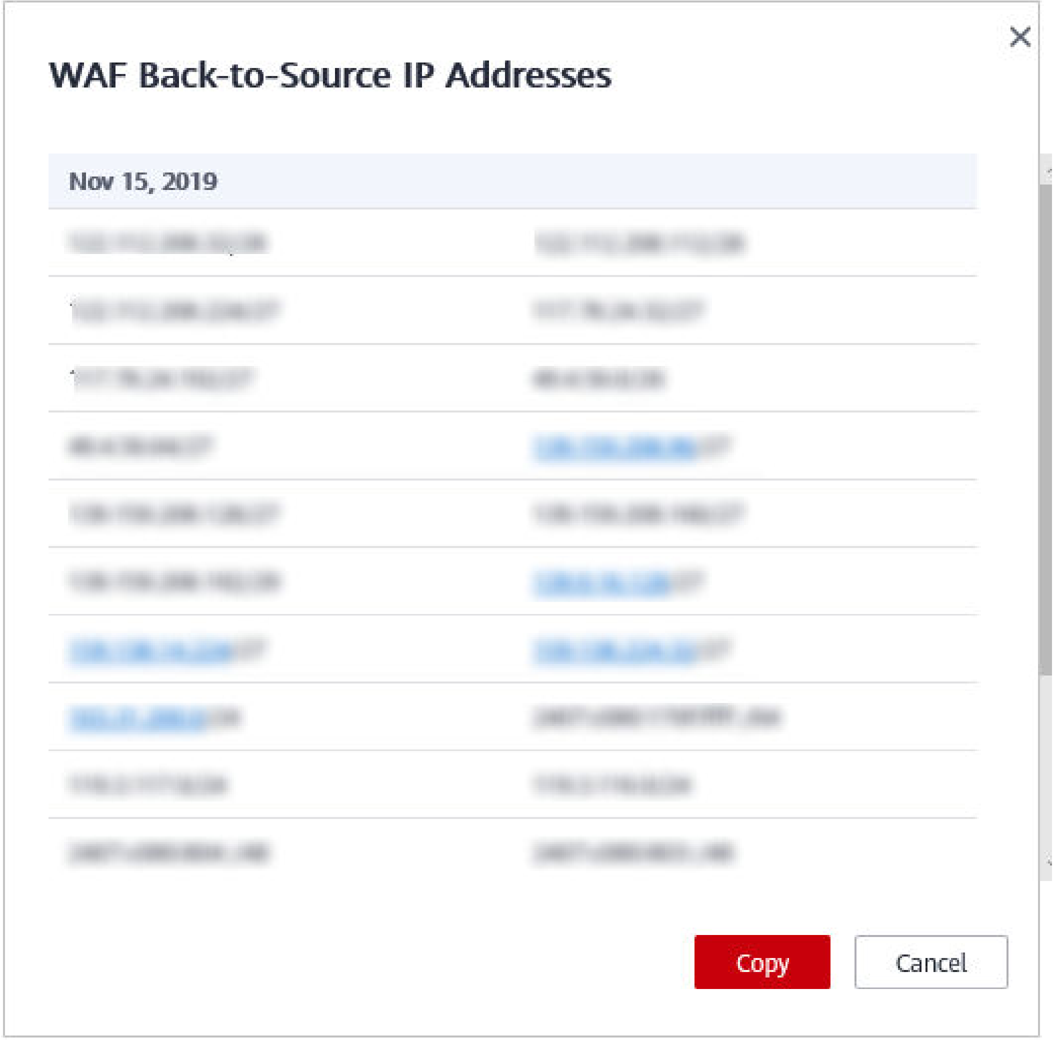
Enterprise Project: default

Cloud mode: Domain names added: 4 to the selected enterprise project and 0 to others; Domain names that can be added: 76. You can add up to 8 top-level domain names.
Dedicated mode: You have added 0 domain names and can add 0 more, including 0 top-level domains.

Protected Website	Deployment Mode	Mode	Access Status	Protection Status for Past 3 Days	Policy	Operation
[redacted]	Cloud mode	Enabled Switch Mode	Inaccessible	No attacks detected. View	Basic Web Protection ● Enabled (Log only) CC Attack Protection ● Enabled Precise Protection ● Enabled Configure Policy	Delete
[redacted]	Cloud mode	Enabled Switch Mode	Inaccessible	No attacks detected. View	Basic Web Protection ● Enabled (Log only) CC Attack Protection ● Enabled Precise Protection ● Enabled Configure Policy	Delete

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

Figure 6-13 WAF Back-to-Source IP Addresses dialog box



WAF Back-to-Source IP Addresses

Nov 15, 2019

[redacted]

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

If your origin servers are deployed on Huawei Cloud ECSs or your website uses Huawei Cloud ELB load balancers, whitelist WAF IP addresses on these original servers or load balancers by referring to **Configuring an Access Control Policy on an ECS or ELB to Protect Origin Servers**.

----End

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

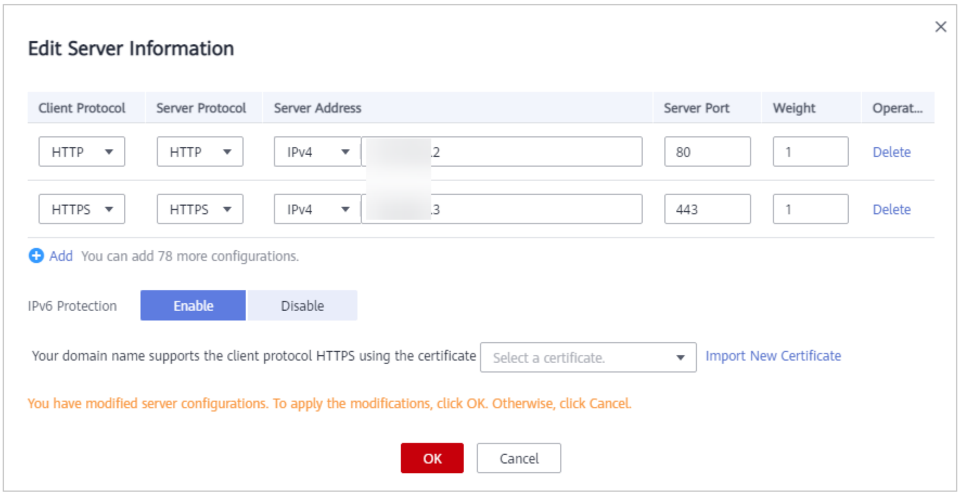
- The default timeout for connections from a browser to WAF is 120 seconds. The value varies depending on your browser settings and cannot be changed on the WAF console.
- The default timeout duration for connections between WAF and your origin server is 30 seconds. You can customize a timeout duration 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.

6.8 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). For details, see **Editing Server Information**. **Figure 6-14** shows the finished server settings.

Figure 6-14 Example configuration



Edit Server Information

Client Protocol	Server Protocol	Server Address		Server Port	Weight	Operat...
HTTP	HTTP	IPv4	[redacted]2	80	1	Delete
HTTPS	HTTPS	IPv4	[redacted]3	443	1	Delete

Add You can add 78 more configurations.

IPv6 Protection: Enable | Disable

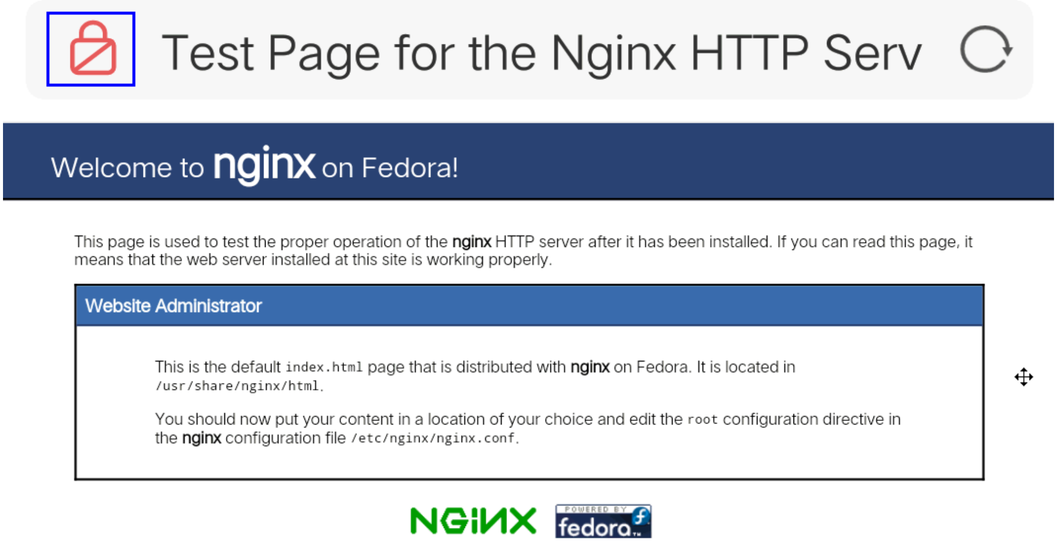
Your domain name supports the client protocol HTTPS using the certificate: Select a certificate. Import New Certificate

You have modified server configurations. To apply the modifications, click OK. Otherwise, click Cancel.

6.9 Why Are HTTPS Requests Denied on Some Mobile Phones?

If your visitors receive a page similar to the one in **Figure 6-15** 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 6-15 Access failed



Test Page for the Nginx HTTP Serv

Welcome to nginx on Fedora!

This page is used to test the proper operation of the nginx HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working properly.

Website Administrator

This is the default `index.html` page that is distributed with nginx on Fedora. It is located in `/usr/share/nginx/html`.

You should now put your content in a location of your choice and edit the `root` configuration directive in the nginx configuration file `/etc/nginx/nginx.conf`.

6.10 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:

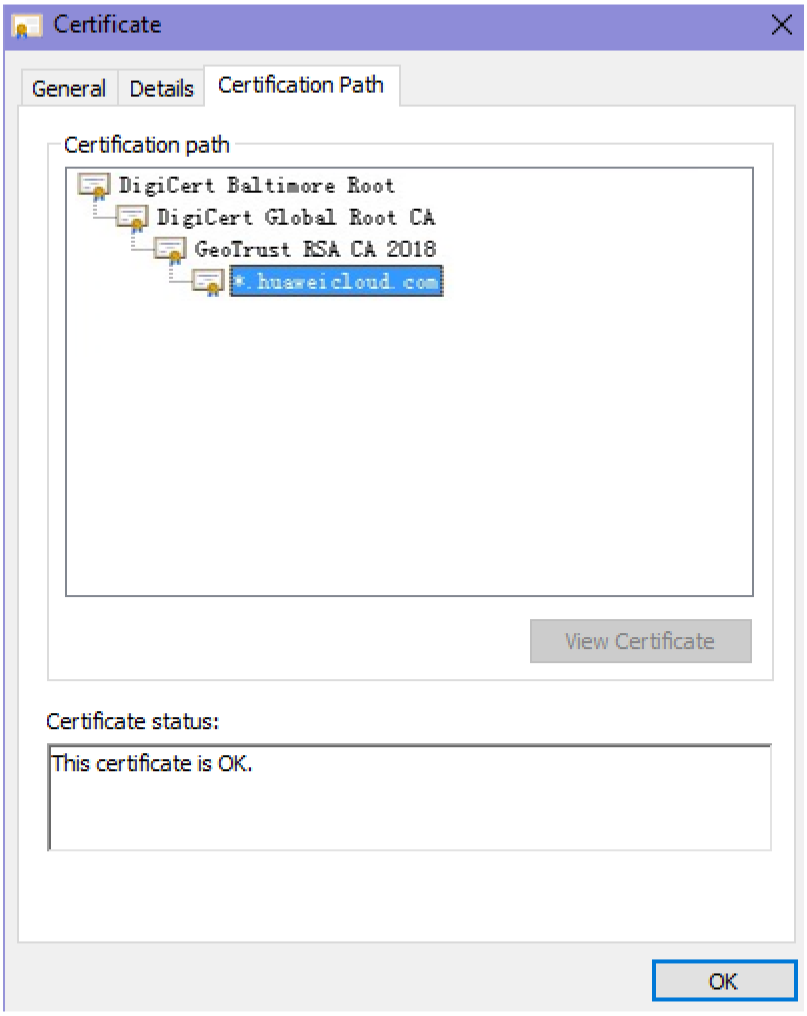
- Manually build up a complete certificate chain and upload the certificate. (This function is available soon.)
- Upload the correct certificate.

The latest Google Chrome version supports automatic verification of the trust chain. The following describes how to manually create a complete certificate chain (using a Huawei Cloud certificate as an example):

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 6-16** shows an example.

Figure 6-16 Viewing the certificate chain



Certification path

DigiCert Baltimore Root
DigiCert Global Root CA
GeoTrust RSA CA 2018
*.huaweicloud.com

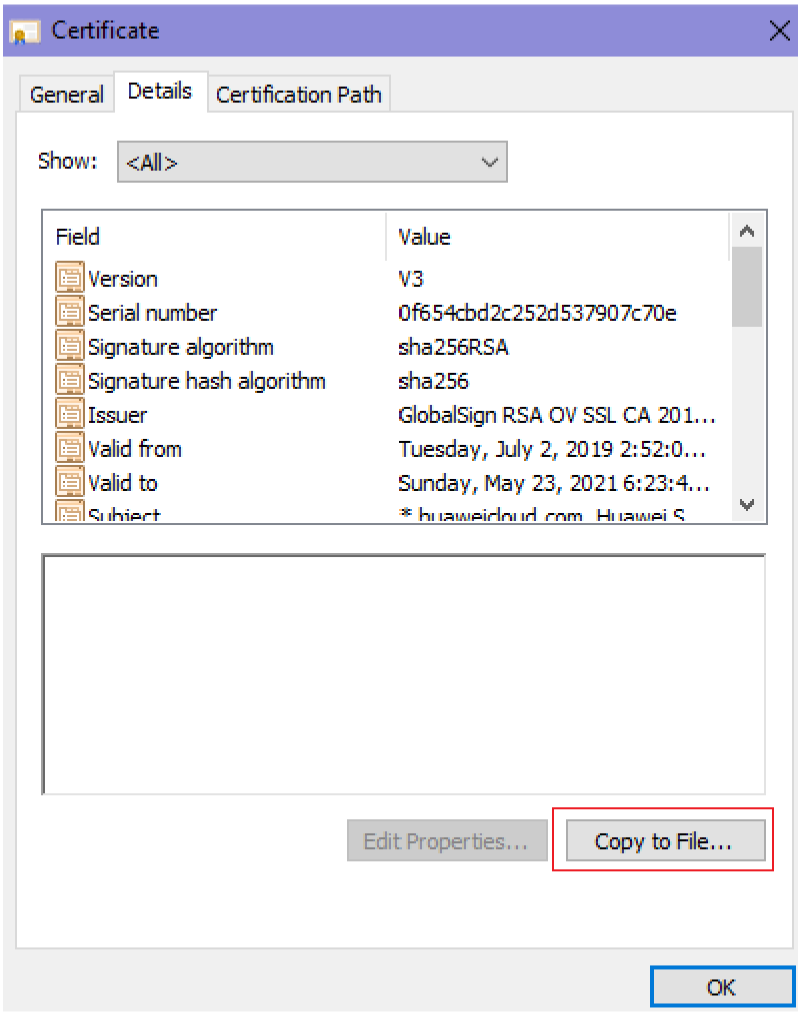
Certificate status:

This certificate is OK.

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

1. Select the certificate name and click the **Details** tab. **Figure 6-17** shows an example.

Figure 6-17 Details

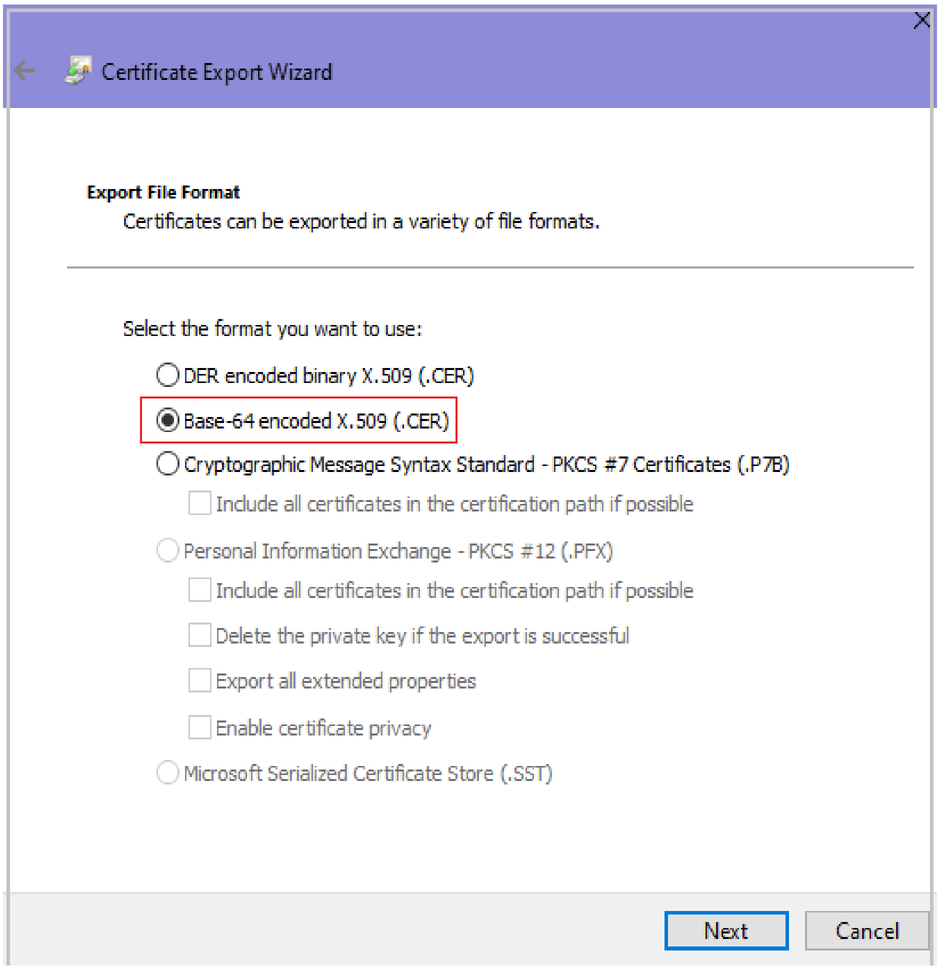


Show: <All>

Field	Value
Version	V3
Serial number	0f654cbd2c252d537907c70e
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	GlobalSign RSA OV SSL CA 201...
Valid from	Tuesday, July 2, 2019 2:52:0...
Valid to	Sunday, May 23, 2021 6:23:4...
Subject	*.huaweicloud.com, Huawei S

2. Click **Copy to File**, and then click **Next** as prompted.
3. Select **Base-64 encoded X.509 (.CER)** and click **Next**. **Figure 6-18** shows an example.

Figure 6-18 Certificate Export Wizard



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

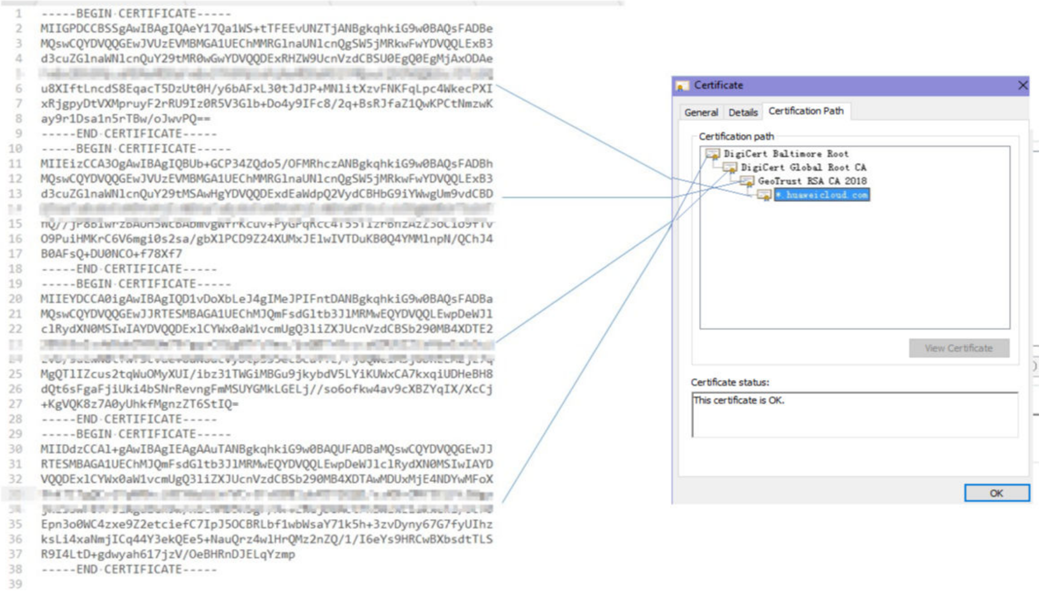
□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

Step 4 Rebuild the certificate. After all certificates are exported to the local PC, open the certificate file in Notepad and rebuild the certificate according to the sequence shown in **Figure 6-19**.

Figure 6-19 Certificate rebuilding



```
-----BEGIN·CERTIFICATE-----
MIIGPDCCBSSgAwIBAgIQAeY17Qa1WS+tTFEEvUNZTjANBgkqhkiG9w0BAQsFADBe
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMR0wGwYDVQQDExRHZW9UcnVzdCBSU0EgQ0EgMjAxODAe
[redacted]
u8XIftLncdS8EqacT5DzUt0H/y6bAFxL30tJdJP+MNlitXzvFNKFqLpc4WkecPXI
xRjgpyDtVXMpruyF2rRU9Iz0R5V3Glb+Do4y9IFc8/2q+BsRJfaZ1QwKPCtNmzwK
ay9r1Dsa1n5rTBw/oJwvPQ==
-----END·CERTIFICATE-----
-----BEGIN·CERTIFICATE-----
MIIEizCCA3OgAwIBAgIQBUb+GCP34ZQdo5/OFMRhczANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
[redacted]
O9PuiHMKrC6V6mgi0s2sa/gbX1PCD9Z24XUMxJElwIVTDuKB0Q4YMMlnpN/QChJ4
B0AFsQ+DU0NCO+f78Xf7
-----END·CERTIFICATE-----
-----BEGIN·CERTIFICATE-----
MIIEYDCCA0igAwIBAgIQD1vDoXbLeJ4gIMeJPIFntDANBgkqhkiG9w0BAQsFADBa
MQswCQYDVQQGEwJJRTESMBAGA1UEChMJQmFsdGltb3JlMRMwEQYDVQQLEwpDeWJl
clRydXN0MSIwIAYDVQQDExlCYWx0aW1vcmUgQ3liZXJUcnVzdCBSb290MB4XDTE2
[redacted]
MgQTlIZcus2tqWuOMyXUI/ibz31TWGiMBGu9jkybdV5LYiKUWxCA7kxqiUDHeBH8
dQt6sFgaFjiUki4bSNrRevngFmMSUYGMkLGELj//so6ofkw4av9cXBZYqIX/XcCj
+KgVQK8z7A0yUhkfMgnzZT6StIQ=
-----END·CERTIFICATE-----
-----BEGIN·CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIEAgAAuTANBgkqhkiG9w0BAQUFADBaMQswCQYDVQQGEwJJ
RTESMBAGA1UEChMJQmFsdGltb3JlMRMwEQYDVQQLEwpDeWJlclRydXN0MSIwIAYD
VQQDExlCYWx0aW1vcmUgQ3liZXJUcnVzdCBSb290MB4XDTAwMDUxMjE4NDYwMFoX
[redacted]
Epn3o0WC4zxe9Z2etciefC7IpJ5OCBRLbf1wbWsaY71k5h+3zvDyny67G7fyUIhz
ksLi4xaNmjICq44Y3ekQEe5+NauQrz4wlHrQMz2nZQ/1/I6eYs9HRCwBXbsdtTLS
R9I4LtD+gdwyah617jzV/OeBHRnDJELqYzmp
-----END·CERTIFICATE-----
```

This certificate is OK.

Step 5 Upload the certificate again.

----End

6.11 Why Does My Certificate Not Match the Key?

After an HTTPS certificate is uploaded to the AAD or WAF console, a message is displayed indicating that the certificate and key do not match.

Solution

Possible Cause	How to Fix
The uploaded certificate does not match the uploaded private key.	1. Run the following commands to check the MD5 hash values of the certificate and private key file: **openssl x509 -noout -modulus -in** *<certificate file>*|**openssl md5** **openssl rsa -noout -modulus -in** *<private key file>*|**openssl md5** 2. Check whether the MD5 values of the certificate and private key file are the same. If they are different, the certificate file and private key file are associated with different domain names, and the content of the certificate does not match that of the private key file. 3. If the certificate does not match the private key file, upload the correct certificate and private key file.
Incorrect RSA private key format	1. Run the following command to generate a new private key: **openssl rsa -in <***private key file***> -out <***New private key file***>** 2. Upload the private key again.

Related Operations

- **How Do I Fix an Incomplete Certificate Chain?**
- **Why Are HTTPS Requests Denied on Some Mobile Phones?**

6.12 Why Am I Seeing Error Code 418?

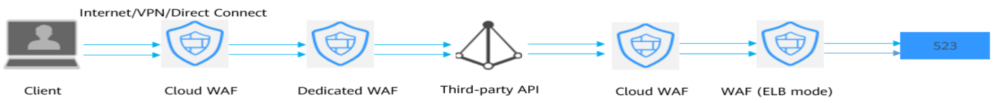
If the request contains malicious load and is intercepted by WAF, error 418 is reported when you access the domain name protected by WAF. You can view WAF protection logs to view the cause. For details about event logs, see **Viewing Protection Event Logs**.

- 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.

  For details, see **Handling False Alarms**.
- If you confirm that the protection event is not a false alarm, your website is attacked and the malicious request is blocked by WAF.

6.13 Why Am I Seeing Error Code 523?

If a request goes through WAF over four times, WAF will block the request and return error code 523 to avoid endless loops. If error code 523 is returned for your website requests, check how many WAF instances you are using.



Cause 1: A website is connected to more than four WAF instances.

Error code 523 will return if a website has been connected to different types of WAF instances more than 4 times.

Solution

Route website traffic to bypass redundant WAF instances.

Step 1 Log in to the WAF management console.

Step 2 In the navigation pane on the left, choose **Website Settings**.

Step 3 Locate the website for which 523 error code is returned, retain one configuration, and delete the website from redundant WAF instances. For details, see **Deleting a 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 Huawei Cloud 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

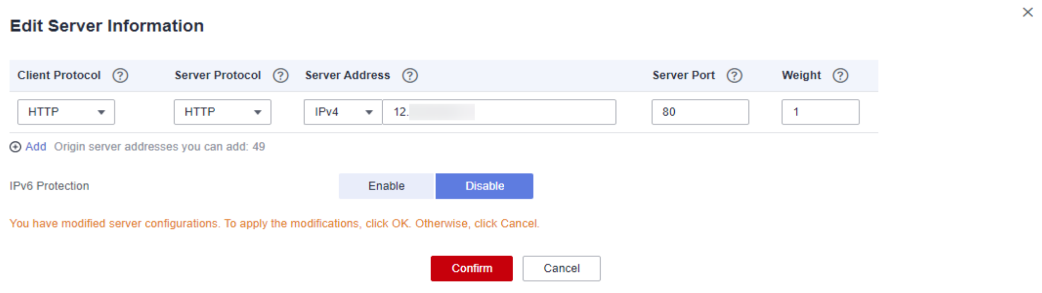
Cause 3: Origin Server IP address Was Mistakenly Set to an IP Address of WAF or A Proxy in Front of WAF

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. For details, see **Editing Server Information**.

Figure 6-20 Changing the origin server address



Edit Server Information

Client Protocol	Server Protocol	Server Address		Server Port	Weight
HTTP	HTTP	IPv4	12.[redacted]	80	1

Add Origin server addresses you can add: 49

IPv6 Protection Enable Disable

You have modified server configurations. To apply the modifications, click OK. Otherwise, click Cancel.

Confirm Cancel

6.14 Why Does the Website Login Page Continuously Refreshed After a Domain Name Is Connected to WAF?

After you connect the domain name of your website to WAF, all website requests are forwarded to WAF first. Then, WAF forwards only the normal traffic to the origin server. For each request from the client, WAF generates an identifier based on the access IP address and user agent. WAF has multiple back-to-source IP addresses that will be randomly allocated. When the back-to-source-IP address changes, the identifier of the request changes accordingly. As a result, the session is directly deleted by WAF, and the login page keeps refreshing. To avoid this problem, you are advised to use session cookies to keep session persistent.

6.15 Why Does the Requested Page Respond Slowly After the HTTP Forwarding Policy Is Configured?

In this case, add two forwarding policies. One is HTTP to HTTP forwarding, and the other is HTTPS to HTTPS forwarding.

For details about how to configure a forwarding rule, see **How Do I Solve the Problem of Excessive Redirection Times?**

6.16 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:

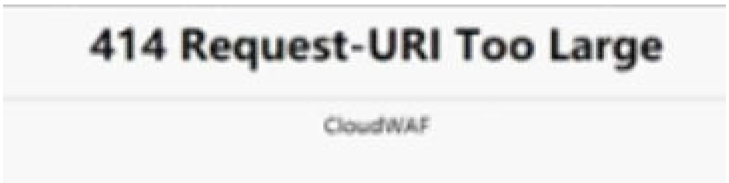
- IP address
- Separate web server that is not protected by WAF
- FTP server

6.17 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 6-21**.

Figure 6-21 Error Code 414 Request-URI Too Large



414 Request-URI Too Large

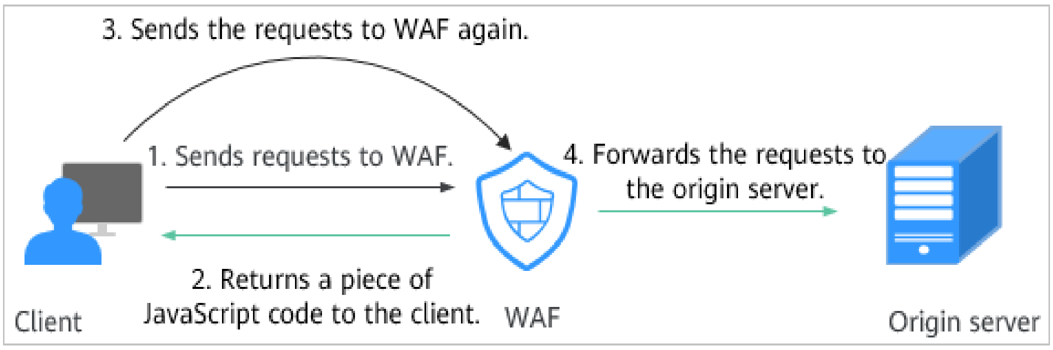
CloudWAF

Possible Causes

The client browser cannot parse JavaScript. In this situation, the client browser caches the page that contains the JavaScript code returned by WAF. Each time the protected website is requested, the cached page is accessed. WAF then verifies that the access request is from an invalid browser or crawler. The access request verification fails. As a result, an infinite loop occurs, the URI length exceeds the browser limit, and the website becomes inaccessible.

After JavaScript anti-crawler is enabled, WAF returns a piece of JavaScript code to the client when the client sends a request. If the client sends a normal request to the website, triggered by the received JavaScript code, the client will automatically send the request to WAF again. WAF then forwards the request to the origin server. This process is called JavaScript verification. **Figure 6-22** shows how JavaScript verification works.

Figure 6-22 JavaScript anti-crawler detection process


3. Sends the requests to WAF again.
1. Sends requests to WAF.
4. Forwards the requests to the origin server.
2. Returns a piece of JavaScript code to the client.
Client
WAF
Origin server

- 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.

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.

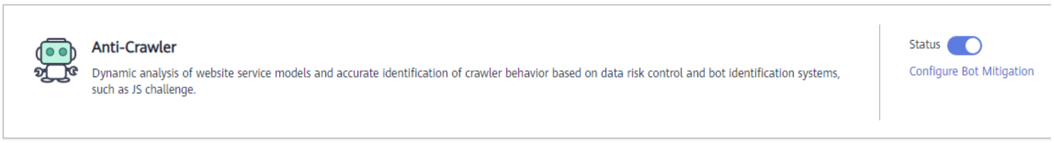
Step 3 Click ☰ in the upper left corner and choose **Web Application Firewall** under **Security**.

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 6-23 Anti-Crawler configuration area

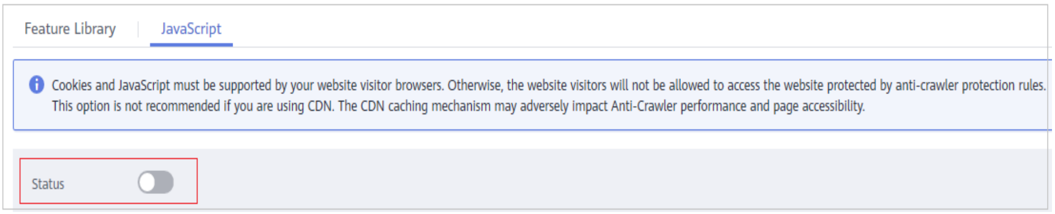


Anti-Crawler

Dynamic analysis of website service models and accurate identification of crawler behavior based on data risk control and bot identification systems, such as JS challenge.

Step 7 Click the **JavaScript** tab and disable the JavaScript anti-crawler protection. Its status changes to .

Figure 6-24 Disabling JavaScript anti-crawler protection



Cookies and JavaScript must be supported by your website visitor browsers. Otherwise, the website visitors will not be allowed to access the website protected by anti-crawler protection rules. This option is not recommended if you are using CDN. The CDN caching mechanism may adversely impact Anti-Crawler performance and page accessibility.

----End

6.18 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?

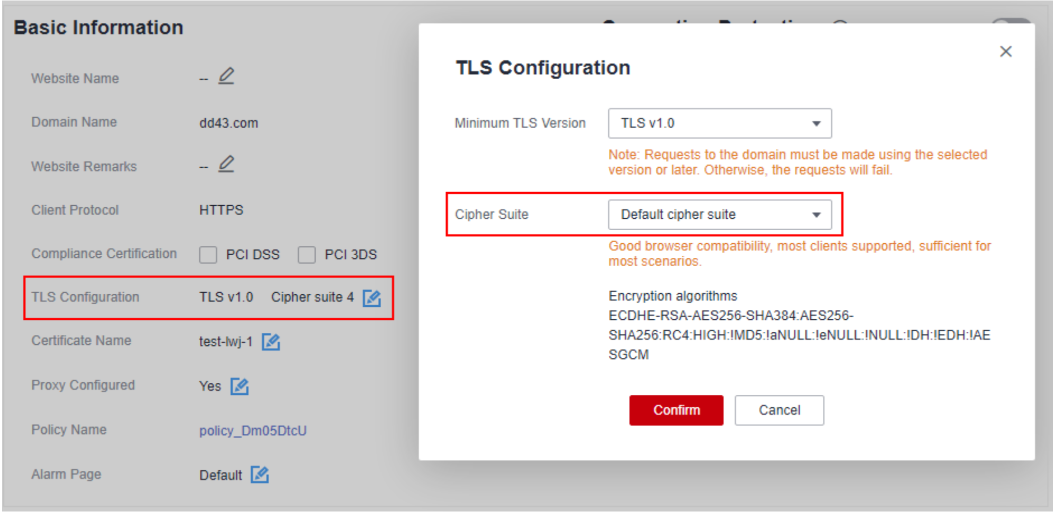
Symptom

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**.

Figure 6-25 TLS Configuration



Basic Information

Website Name --
Domain Name dd43.com
Website Remarks --
Client Protocol HTTPS
Compliance Certification □ PCI DSS □ PCI 3DS
TLS Configuration TLS v1.0 Cipher suite 4
Certificate Name test-lwj-1
Proxy Configured Yes
Policy Name policy_Dm05DtcU
Alarm Page Default

TLS Configuration

Minimum TLS Version: TLS v1.0

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

Cipher Suite: Default cipher suite

Good browser compatibility, most clients supported, sufficient for most scenarios.

Encryption algorithms
ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM

6.19 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.

6.20 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.

7 Protection Rule Configuration

7.1 Basic Web Protection

7.1.1 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

7.1.2 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 7-1**.

Table 7-1 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**.

For details about basic web protection, see **Configuring Basic Web Protection Rules**.

7.2 CC Attack Protection Rules

7.2.1 What Is the Peak Rate of CC Attack Protection?

It depends on the WAF edition you are using. For details, see **Table 7-2**.

Table 7-2 Peak rate of CC attack protection

Edition	Peak rate of normal service requests	Peak rate of CC attack protection
Standard	● 2,000 QPS ● WAF-to-Server connections: 6,000 per domain name	100,000QPS

Edition	Peak rate of normal service requests	Peak rate of CC attack protection
Professional	● Service requests: 5,000 QPS ● WAF-to-Server connections: 6,000 per domain name	300,000QPS
Platinum	● Service requests: 10,000 QPS ● WAF-to-Server connections: 6,000 per domain name	1,000,000QPS
Dedicated WAF	The following lists the specifications of a single instance. ● Specifications: WI-500. Referenced performance: – HTTP services - Recommended QPS: 5,000. Maximum QPS: 10,000. – HTTPS services - Recommended QPS: 4,000. Maximum QPS: 8,000. – WebSocket service - Maximum concurrent connections: 5,000 – Maximum WAF-to-server persistent connections: 60,000 ● Specifications: WI-100. Referenced performance: – HTTP services - Recommended QPS: 1,000. Maximum QPS: 2,000. – HTTPS services - Recommended QPS: 800. Maximum QPS: 1,600 – WebSocket service - Maximum concurrent connections: 1,000 – Maximum WAF-to-server persistent connections: 60,000 **NOTICE** Maximum QPS values are for reference only. They may vary depending on your businesses. The real-world QPS is related to the request size and the type and quantity of protection rules you customize.	● Specifications: WI-500. Referenced performance: Maximum QPS: 20,000 ● Specifications: WI-100. Referenced performance: Maximum QPS: 4,000

7.2.2 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**.

7.2.3 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.

NOTICE

Cookie-based identification may not be supported if the URL request configured in a CC attack protection policy is an API called by another service.

7.2.4 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**.

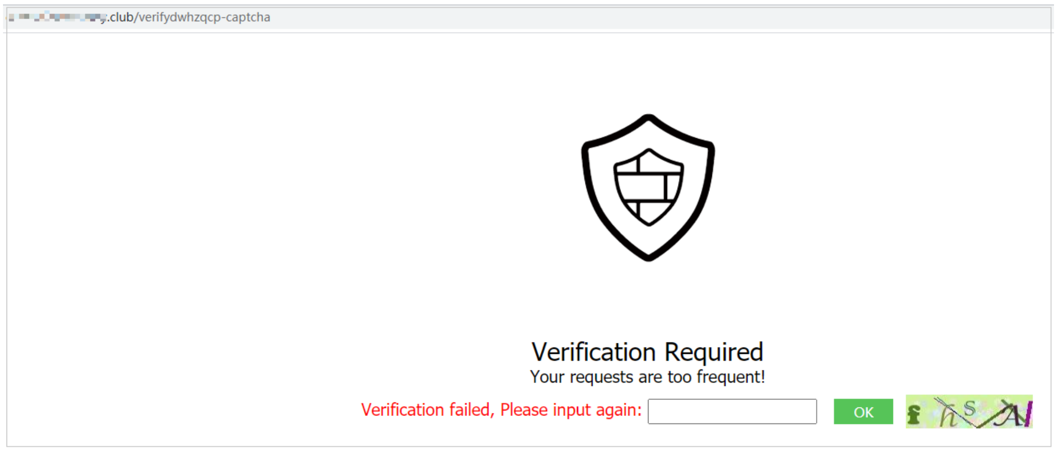
For details, see **Configuring a CC Attack Protection Rule**.

7.2.5 Why Cannot the Verification Code Be Refreshed When Verification Code Is Configured in a CC Attack Protection Rule?

Symptom

After you add a CC attack rule with **Protective Action** set to **Verification code** on WAF, the verification code cannot be refreshed and the verification fails when the website is requested. **Figure 7-1** shows an example.

Figure 7-1 Verification failed



[redacted].club/verifydwhzqcp-captcha

Verification Required

Your requests are too frequent!

Verification failed, Please input again:

After **Verification code** is configured, a verification code is required when the number of requests exceeds the maximum limit within a specified period. Upon completing the verification, the access limit is lifted.

For details, see **Configuring a CC Attack Protection Rule**.

Possible Causes

When a domain name is connected to both WAF and Content Delivery Network (CDN), and the value for **Path** of the CC attack protection rule contains a static page, the static page is cached by CDN. As a result, the verification code cannot be refreshed and the verification fails.

Handling Suggestions

In CDN, configure cache policies to bypass the cache for static URLs.

NOTICE

After the configuration is complete, it takes 3 to 5 minutes for the configured cache policies 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 of the page and choose **Content Delivery & Edge Computing** > **Content Delivery Network**.

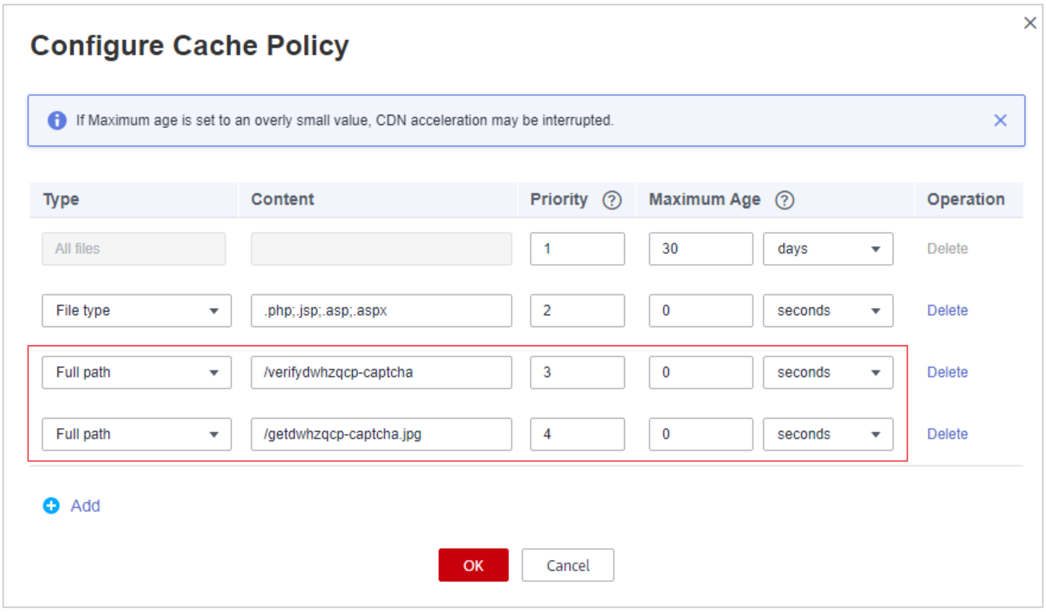
Step 4 In the navigation pane, choose **Domains**.

Step 5 In the **Domain Name** column, click the name of the target domain name.

Step 6 Click the **Cache Settings** tab and click **Edit**.

Step 7 In the displayed **Configure Cache Policy** dialog box, click **Add** below the policy list and add two cache policy rules by referring to **Table 7-3**.

Figure 7-2 Configure Cache Policy



Configure Cache Policy

If Maximum age is set to an overly small value, CDN acceleration may be interrupted.

Type	Content	Priority	Maximum Age		Operation
All files		1	30	days	Delete
File type	.php;.jsp;.asp;.aspx	2	0	seconds	Delete
Full path	/verifydwhzqcp-captcha	3	0	seconds	Delete
Full path	/getdwhzqcp-captcha.jpg	4	0	seconds	Delete

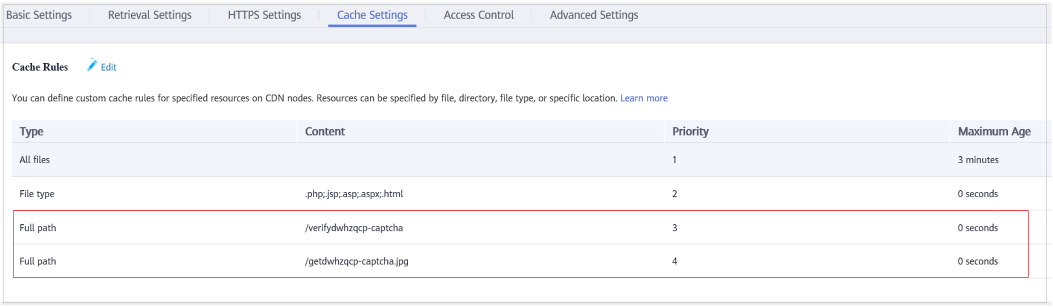
Table 7-3 Parameters for configuring static URL cache policy

Parameter	Configuration Description
Type	Select **Full path**.
Content	The content of the two policies to be added are as follows: ● **/verifydwhzqcp-captcha** ● **/getdwhzqcp-captcha.jpg**

Parameter	Configuration Description
Priority	Set the two policies to the highest priority.
Maximum Age	Set this parameter to **0 seconds**, indicating that static URLs are not cached.

Step 8 Click **OK**.

Figure 7-3 Configured cache policies



Cache Rules

You can define custom cache rules for specified resources on CDN nodes. Resources can be specified by file, directory, file type, or specific location.

Type	Content	Priority	Maximum Age
All files		1	3 minutes
File type	.php;.jsp;.asp;.aspx;.html	2	0 seconds
Full path	/verifydwhzqcp-captcha	3	0 seconds
Full path	/getdwhzqcp-captcha.jpg	4	0 seconds

After the configuration is complete, it takes 3 to 5 minutes for the configured cache policies to take effect.

----End

7.3 Precise Protection rules

7.3.1 Can a Precise Protection Rule Take Effect in a Specified Period?

Precise access protection rules can take effect in a specified period.

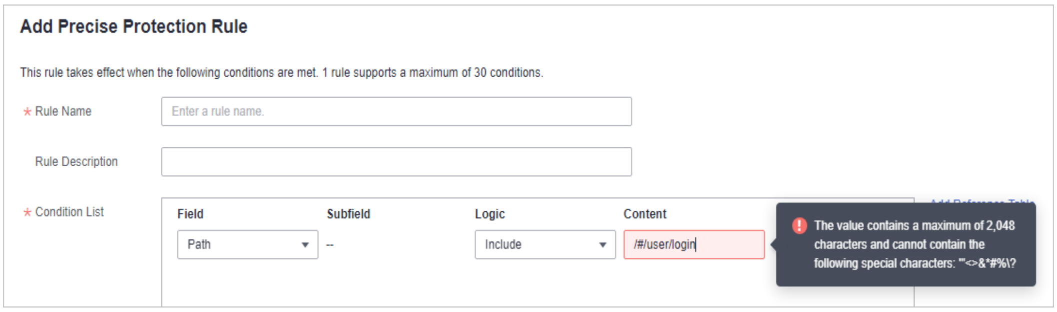
You can set precise protection rules to filter access requests based on a combination of common HTTP fields (such as IP address, path, referer, user agent, and params) to allow or block the requests that match the conditions.

For details about how to configure, see **Configuring Precise Protection Rules**.

7.3.2 Can a Path Containing # Be Matched in a Precise Protection Rule?

The path added to a precise protection rule cannot contain special characters ('"<>&*# %\?).

The number sign (#) is a client parameter. Parameters following the number sign (#) are not transferred to the server for web page location. WAF and browsers do not consider the content following the number sign (#) as URL parameters. Therefore, the parameters cannot be obtained.



Add Precise Protection Rule

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

* Rule Name: Enter a rule name.

Rule Description:

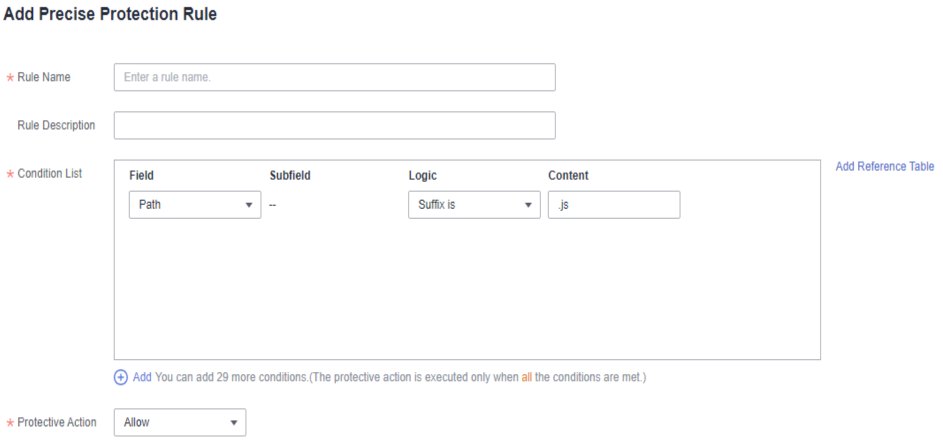
* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/#/user/login

The value contains a maximum of 2,048 characters and cannot contain the following special characters: "'<>&*#%\?

7.3.3 How Can I Allow Access from .js Files?

You can configure a precise protection rule in WAF to allow access from paths with the suffix .js. The configuration is as follows:



Add Precise Protection Rule

* Rule Name: Enter a rule name.

Rule Description:

* Condition List

Field	Subfield	Logic	Content
Path	--	Suffix is	.js

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

* Protective Action: Allow

7.4 IP Address Blacklist and Whitelist

7.4.1 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.

7.4.2 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.

7.4.3 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.

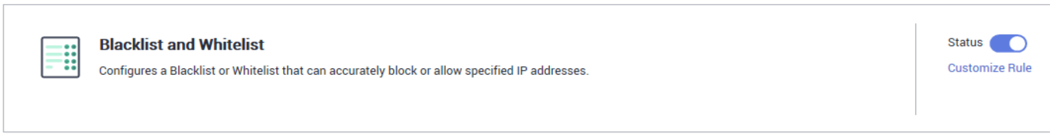
Step 3 Click ☰ in the upper left corner and choose **Security** > **Web Application Firewall**.

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

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

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

Figure 7-4 Blacklist and Whitelist configuration area



Blacklist and Whitelist

Configures a Blacklist or Whitelist that can accurately block or allow specified IP addresses.

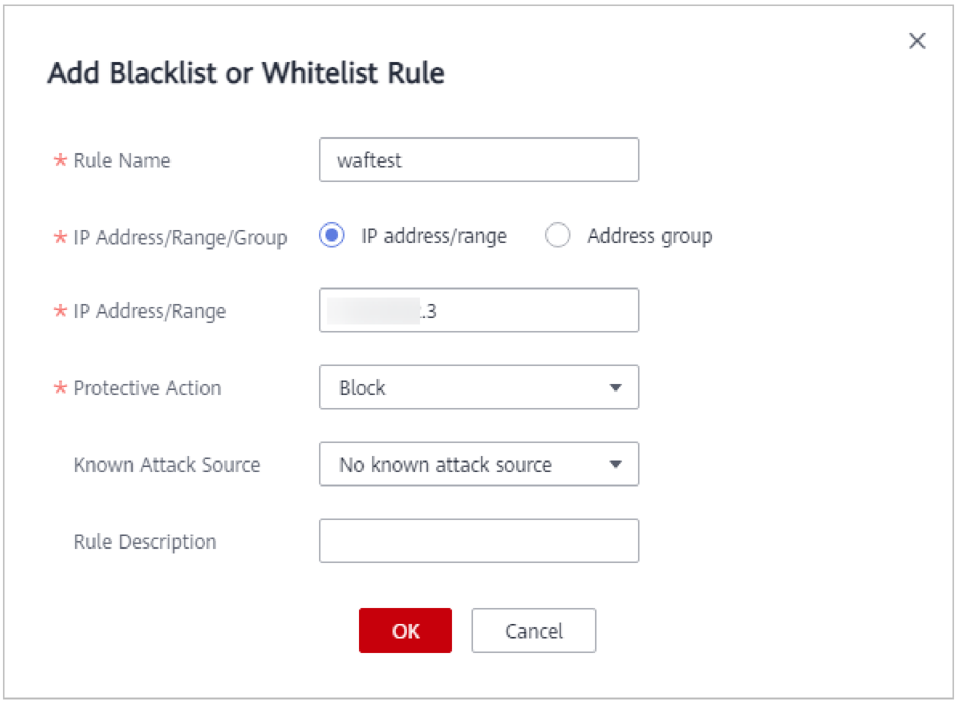
Step 7 In the upper left corner above the **Blacklist and Whitelist** list, click **Add Rule**.

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 7-5 Adding a blacklist or whitelist rule



Add Blacklist or Whitelist Rule

* Rule Name: waftest

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

* IP Address/Range: [redacted].3

* Protective Action: Block

Known Attack Source: No known attack source

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.

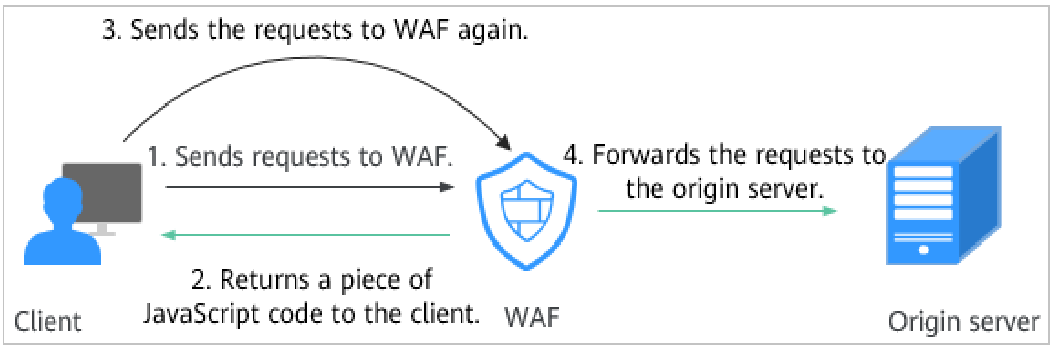
----End

7.5 Anti-Crawler Protection

7.5.1 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 7-6** shows how JavaScript verification works.

Figure 7-6 JavaScript anti-crawler detection process


3. Sends the requests to WAF again.
1. Sends requests to WAF.
4. Forwards the requests to the origin server.
2. Returns a piece of JavaScript code to the client.
Client
WAF
Origin server

- 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.

NOTICE

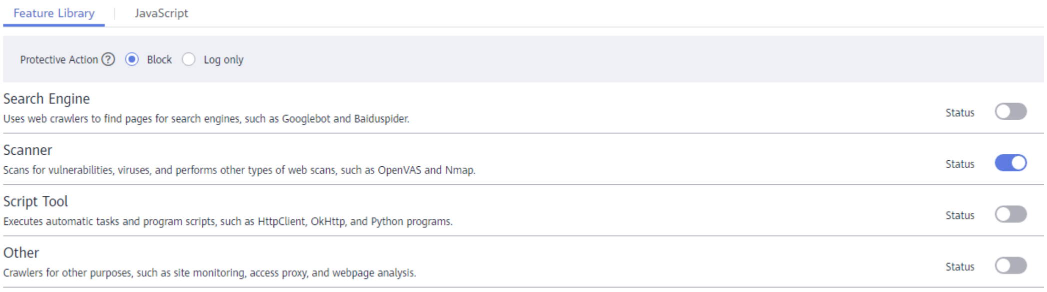
- To enable the JavaScript anti-crawler protection, the browser on the client must have JavaScript and cookies enabled.
- If the client does not meet the preceding requirements, only steps 1 and 2 can be performed. In this case, the client request fails to obtain the page.

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

7.5.2 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 7-7 Enabling **Other**



Feature Library | JavaScript

Protective Action ⓘ ● Block ○ Log only

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

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

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

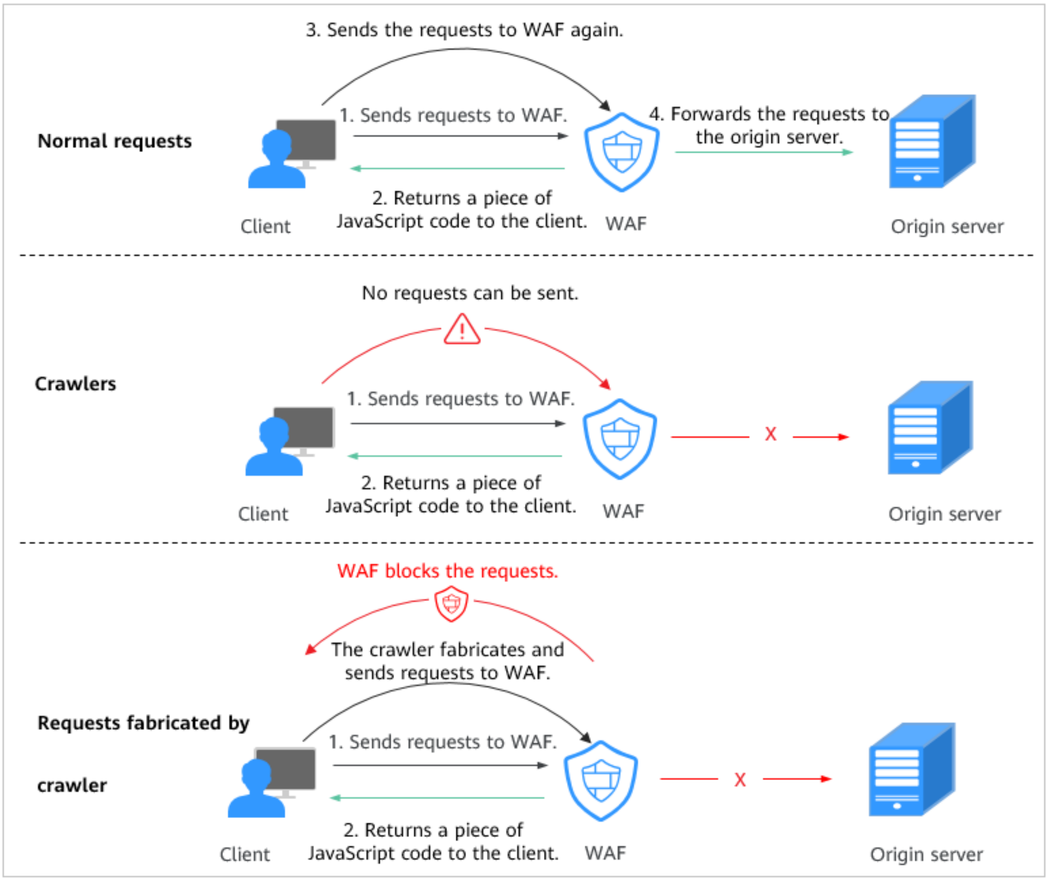
Other
Crawlers for other purposes, such as site monitoring, access proxy, and webpage analysis. Status ○

For details, see **Configuring Anti-Crawler Rules**.

7.5.3 How Does JavaScript Anti-Crawler Detection Work?

Figure 7-8 shows how JavaScript anti-crawler detection works, which includes JavaScript challenges (step 1 and step 2) and JavaScript authentication (step 3).

Figure 7-8 JavaScript Anti-Crawler protection process

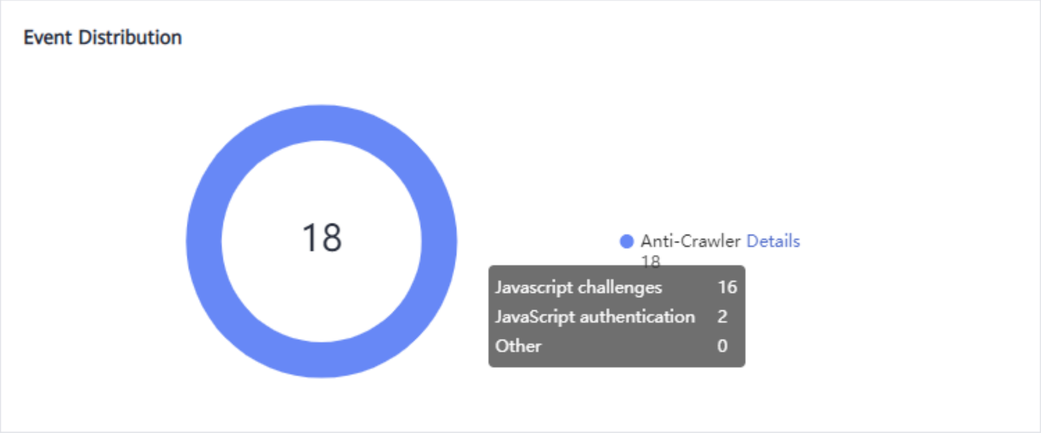

3. Sends the requests to WAF again.
Normal requests
1. Sends requests to WAF.
4. Forwards the requests to the origin server.
2. Returns a piece of JavaScript code to the client.
Client
WAF
Origin server
No requests can be sent.
Crawlers
1. Sends requests to WAF.
X
2. Returns a piece of JavaScript code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

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 7-9**, 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 7-9 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.

7.6 Others

7.6.1 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.

7.6.2 Can I Export or Back Up the WAF Configuration?

The current WAF configuration cannot be exported or backed up.

7.6.3 How Do I Allow Requests from Only IP Addresses in a Specified Geographical Region?

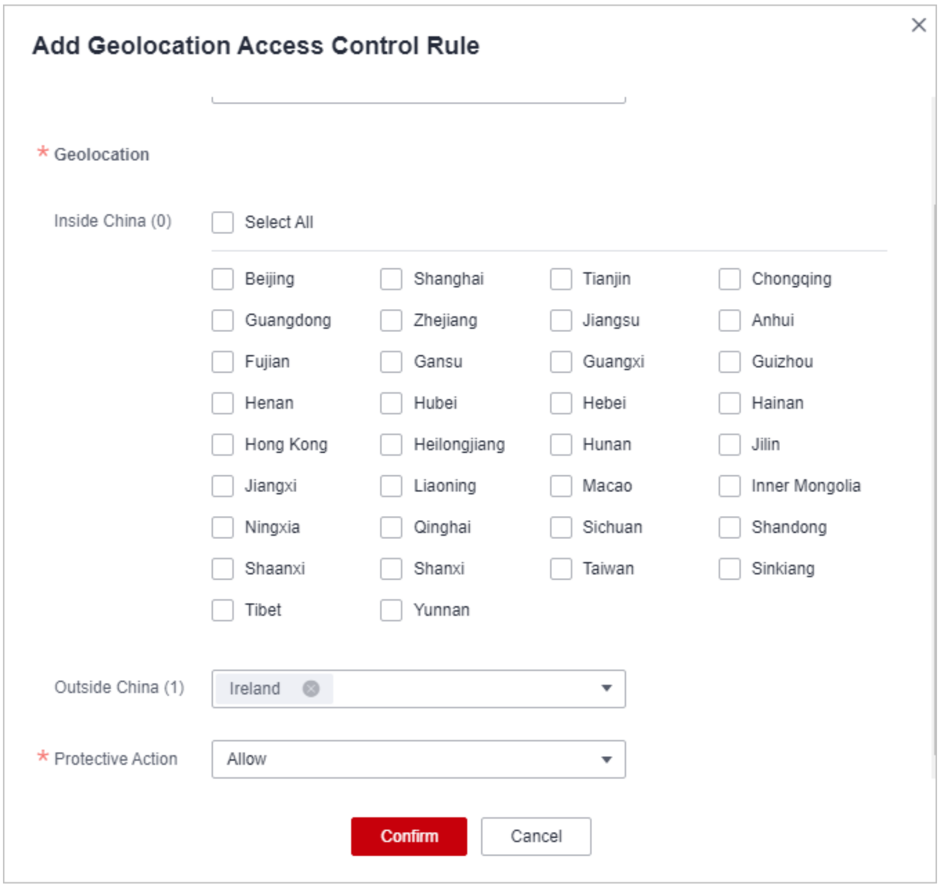
If you allow only IP addresses in a region to access the protected domain name, for example, only IP addresses from **Ireland** can access the protected domain name, take the following steps:

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 **Ireland** for **Geolocation** and select **Allow** for **Protective Action**.

Figure 7-10 Selecting Allow for Protective Action



Add Geolocation Access Control Rule

* Geolocation

Inside China (0) □ Select All

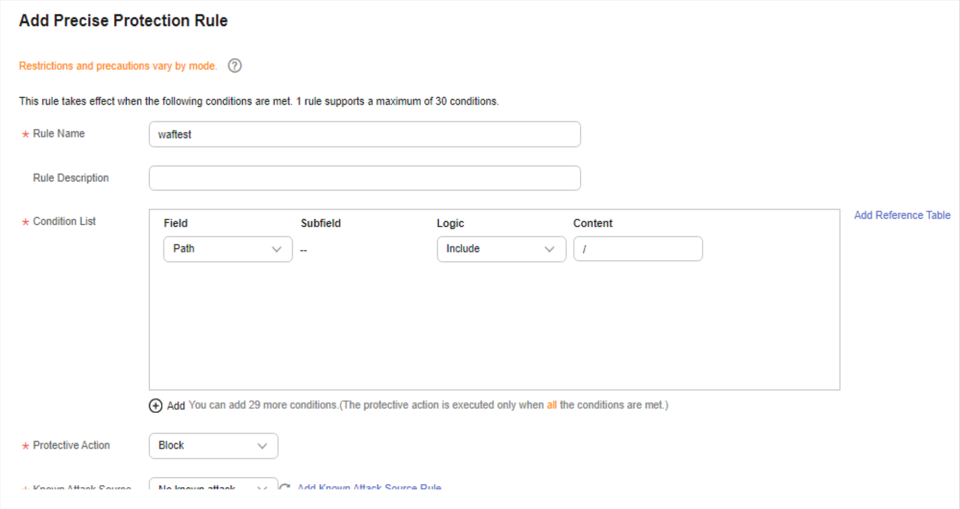
□ Beijing □ Shanghai □ Tianjin □ Chongqing
□ Guangdong □ Zhejiang □ Jiangsu □ Anhui
□ Fujian □ Gansu □ Guangxi □ Guizhou
□ Henan □ Hubei □ Hebei □ Hainan
□ Hong Kong □ Heilongjiang □ Hunan □ Jilin
□ Jiangxi □ Liaoning □ Macao □ Inner Mongolia
□ Ningxia □ Qinghai □ Sichuan □ Shandong
□ Shaanxi □ Shanxi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

Outside China (1): Ireland

* Protective Action: Allow

Step 2 Configure a precise protection rule to block all requests.

Figure 7-11 Blocking all access requests



Add Precise Protection Rule

Restrictions and precautions vary by mode.

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

* Rule Name: waftest

Rule Description:

* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/

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

* Protective Action: Block

----End

7.6.4 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**.

For more details, see **Switching WAF Working Mode**.

Table 7-4 describes the protection mechanism.

Table 7-4 Supported protection mechanism

Protection Rule	Protective Action
Basic web protection rules	● Block ● Log only
CC attack protection rules	● Verification code ● Block ● Block dynamically ● Log only
Precise protection rules	● Block ● Allow ● Log only
Blacklist and whitelist rules	● Block ● Allow ● Log only
Geolocation access control rules	● Block ● Allow ● Log only

Protection Rule	Protective Action
Website anti-crawler protection	Protective actions for feature-based anti-crawler rules: ● Block ● Log only

NOTE

- **Block**: WAF blocks and logs detected attacks.
- **Log only**: WAF only logs detected attacks.

7.6.5 What Types of Protection Rules Does WAF Support?

Table 7-5 lists all protection rules you can use in WAF.

Table 7-5 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.

Protection Rule	Description
Website anti-crawler protection	This function dynamically analyzes website service models and accurately identifies crawler behavior based on data risk control and bot identification systems, such as JS Challenge.
Information leakage prevention rules	You can add two types of information leakage prevention rules. ● Sensitive information filtering: prevents disclosure of sensitive information (such as ID numbers, phone numbers, and email addresses). ● Response code interception: blocks the specified HTTP status codes.
Global protection whitelist rules	This function ignores certain attack detection rules for specific requests.
Data masking rules	You can configure data masking rules to prevent sensitive data such as passwords from being displayed in event logs.

7.6.6 Which of the WAF Protection Rules Support the Log-Only Protective Action?

In WAF, **Log only** is available for **Protective Action** in basic web protection rules.

Log only is available for **Protective Action** in CC attack protection rules, precise protection rules, blacklist and whitelist rules, geolocation access control rules, and anti-crawler rules.

7.6.7 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.

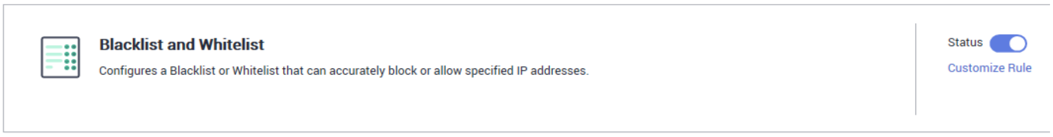
Step 3 Click ☰ in the upper left corner and choose **Web Application Firewall** under **Security**.

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 7-12 Blacklist and Whitelist configuration area



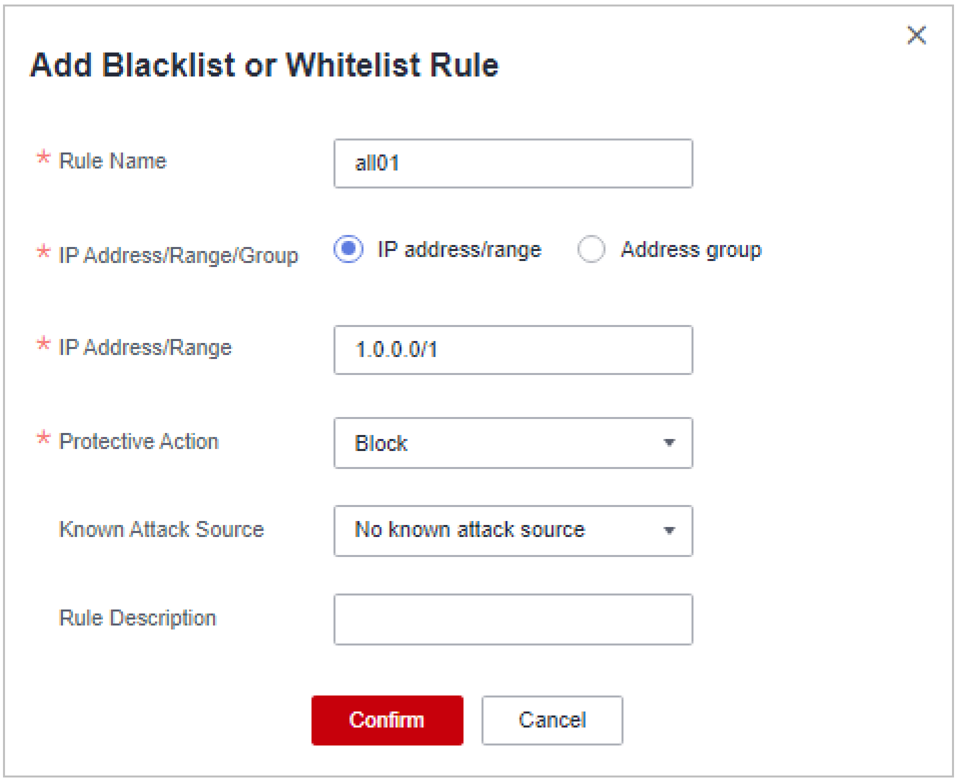
Blacklist and Whitelist

Configures a Blacklist or Whitelist that can accurately block or allow specified IP addresses.

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 7-13 Blocking IP address range 1.0.0.0/1



Add Blacklist or Whitelist Rule

* Rule Name: all01

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

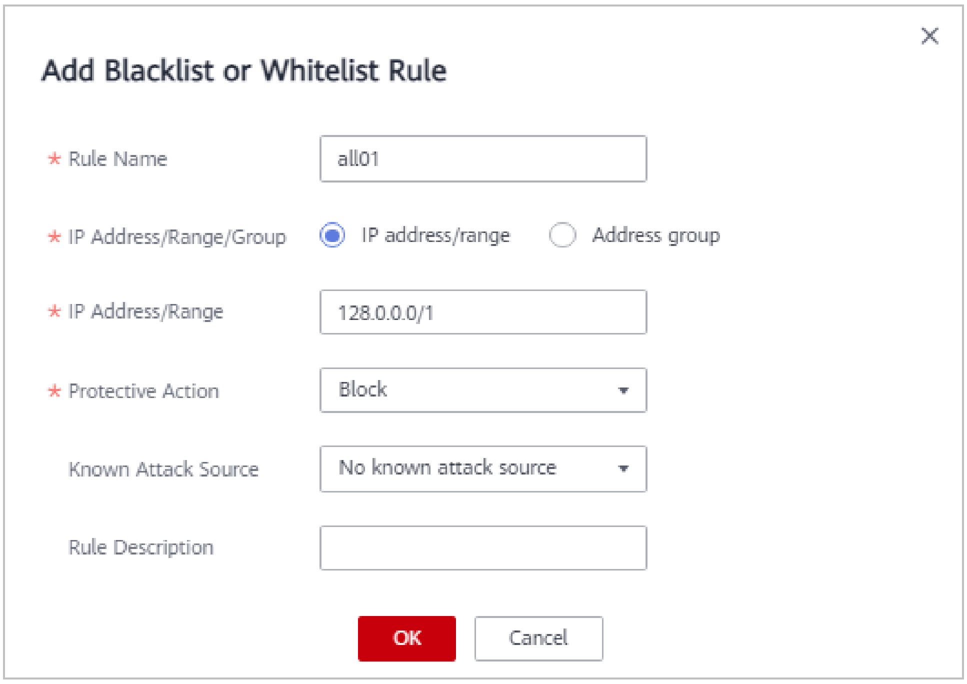
* IP Address/Range: 1.0.0.0/1

* Protective Action: Block

Known Attack Source: No known attack source

Rule Description:

Figure 7-14 Blocking IP address range 128.0.0.0/1



Add Blacklist or Whitelist Rule

* Rule Name: all01

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

* IP Address/Range: 128.0.0.0/1

* Protective Action: Block

Known Attack Source: No known attack source

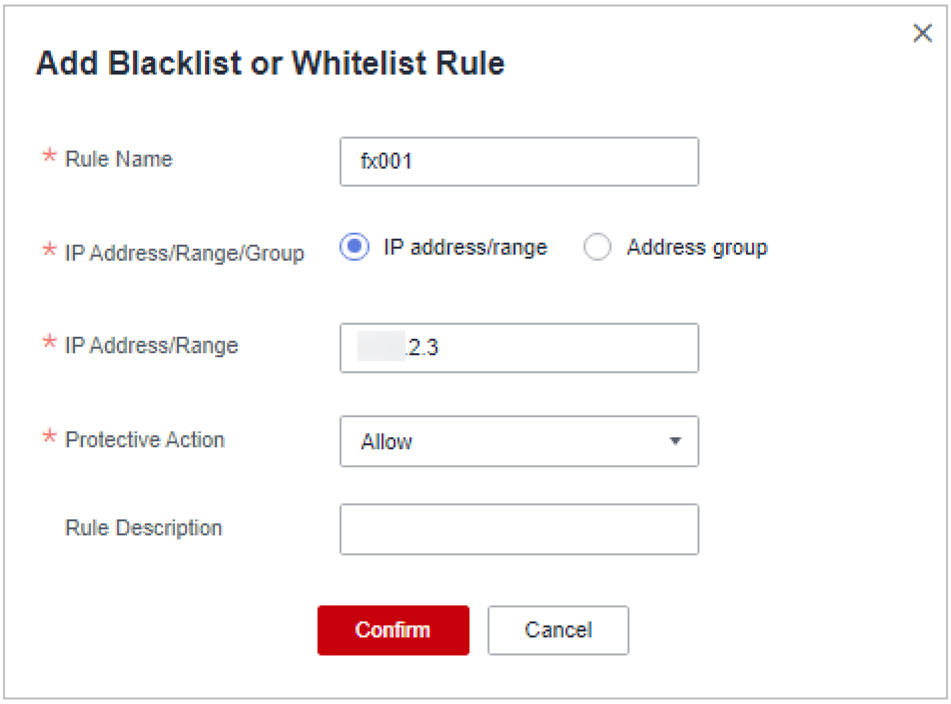
Rule Description:

OK Cancel

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 7-15**.

Figure 7-15 Allowing the access of a specified IP address



Add Blacklist or Whitelist Rule

* Rule Name: fx001

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

* IP Address/Range: [redacted]2.3

* Protective Action: Allow

Rule Description:

Confirm Cancel

----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.

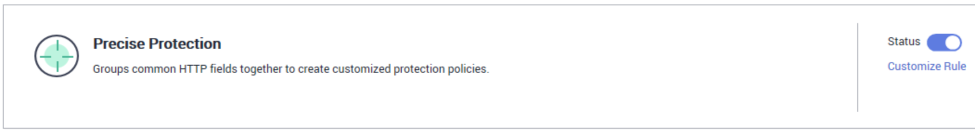
Step 3 Click ☰ in the upper left corner and choose **Web Application Firewall** under **Security**.

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 7-16 Precise Protection configuration area



Precise Protection

Groups common HTTP fields together to create customized protection policies.

Status ●

Customize Rule

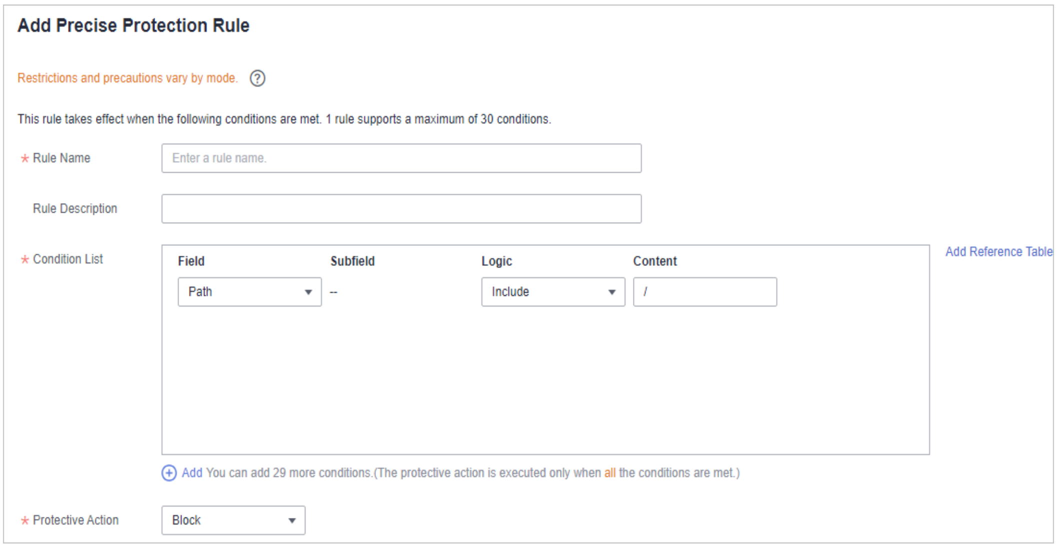
Step 7 Click **Customize Rule**. In the upper left corner of the displayed page, click **Add Rule**.

Step 8 In the displayed **Add Precise Protection Rule** dialog box, add a protection rule as shown in **Figure 7-17** 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 7-17 Blocking all requests



Add Precise Protection Rule

Restrictions and precautions vary by mode. ?

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

* Rule Name: Enter a rule name.

Rule Description:

* Condition List

Field	Subfield	Logic	Content
Path	--	Include	/

Add Reference Table

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

* Protective Action: Block

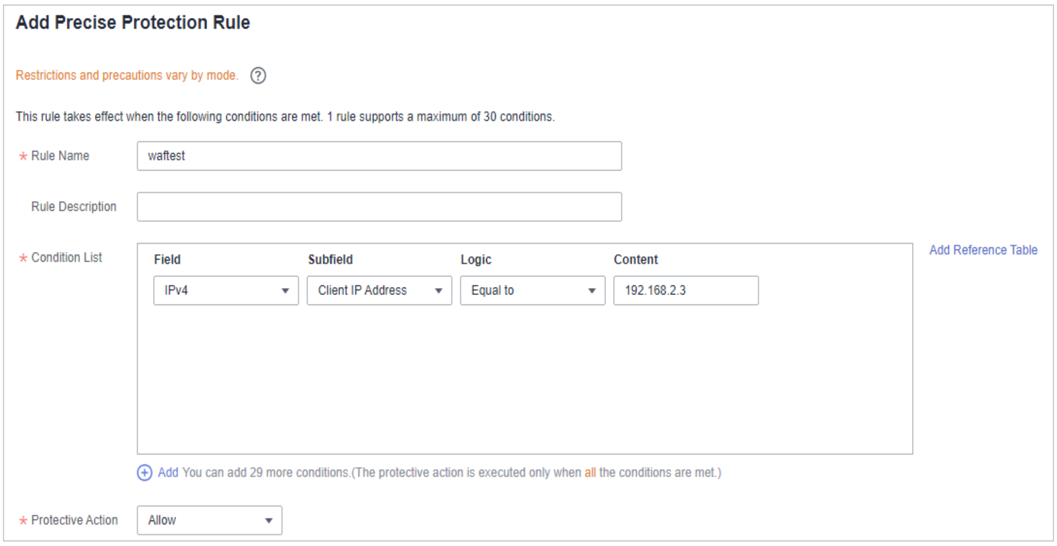
Step 9 Click **Add Rule**. In the displayed **Add Precise Protection Rule** dialog box, add a rule for the specified IP address.

For example, if you want to allow 192.168.2.3 to access the website, add a protection rule as shown in **Figure 7-18**.

⚠ 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 7-18 Allowing the access of a specified IP address



Add Precise Protection Rule

Restrictions and precautions vary by mode. ?

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

* Rule Name: waftest

Rule Description:

* Condition List

Field	Subfield	Logic	Content
IPv4	Client IP Address	Equal to	192.168.2.3

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

* Protective Action: Allow

You can also add a whitelist rule for specified IP addresses or IP address range by referring to **Step 9**.

----End

7.6.8 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 7-6**.

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 7-6 System-generated policies

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

7.6.9 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.

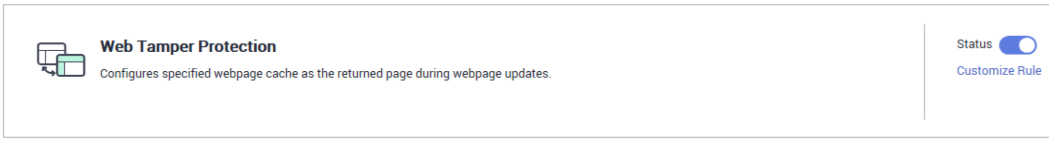
Step 3 Click ☰ in the upper left corner and choose **Web Application Firewall** under **Security**.

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 7-19 Web Tamper Protection configuration area



Web Tamper Protection

Configures specified webpage cache as the returned page during webpage updates.

- 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

7.6.10 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 7-7** describes the differences between the two types of rules.

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

Protection Rules	Protection	WAF Inspection Sequence
Blacklist and whitelist rules	This type or rules can block, log only, or allow access requests from a specified IP address or IP address range.	Blacklist and whitelist rules have the highest priority. WAF checks access requests based on the protection rules and the triggering sequence.
Precise protection rules	You can combine common HTTP fields, such as **IP**, **Path**, **Referer**, **User Agent**, and **Params** in a protection rule to let WAF allow or block the requests that match the combined conditions.	Precise protection rules have lower priority compared with blacklist and whitelist rules.

7.6.11 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.

WAF does not provide such compliance functions. The website administrator needs to perform related security configuration at the backend.

8 Protection Event Logs

8.1 Can I Obtain WAF Logs Using APIs?

You can call an API to view WAF protection logs.

You can also download protection events on the WAF console. For details, see **Downloading Events Data**.

8.2 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**.

8.3 How Does WAF Obtain the Real Client IP Address for a Request?

WAF forwards requests to the backend based on protection rules. If IP address-based rules (such as blacklist and whitelist, geographical location, and IP address-based precise access rules) are configured for WAF, WAF checks the real IP addresses first and then allows or blocks the request according to the configured rules. WAF obtains real IP addresses in accordance with the following principles:

- If you select **Lay-4 proxy** or **Layer-7 proxy** for **Proxy Configured** when you add a domain name to WAF, WAF obtains the source IP address in the following sequence:
  a. The source IP header list configured in **upstream** is preferentially used, that is, the IP address tag configured on the basic information page of the domain name. For details, see **Configuring a Traffic Identifier for a Known Attack Source**. If no IP address is available, go to **b**.

NOTE

If you want to use a TCP connection IP address as the client IP address, set **IP Tag** to **remote_addr**.

b. Obtain the value of the **cdn-src-ip** field in the source IP header list configured in the config file. If no value is obtained, go to **c**.

c. Obtain the value of the **x-real-ip** field. If no value is obtained, go to **d**.

d. Obtain the first public IP address from the left of the **x-forwarded-for** field. If no public IP address is obtained, go to **e**.

e. Obtain the value of the **remote_addr** field, which includes the IP address used for establishing the TCP connection.

- If you select **No proxy** for **Proxy Configured** when you add a domain name to WAF, WAF obtains the source IP address from the **remote_ip** field.

8.4 How Long Can WAF Protection Logs Be Stored?

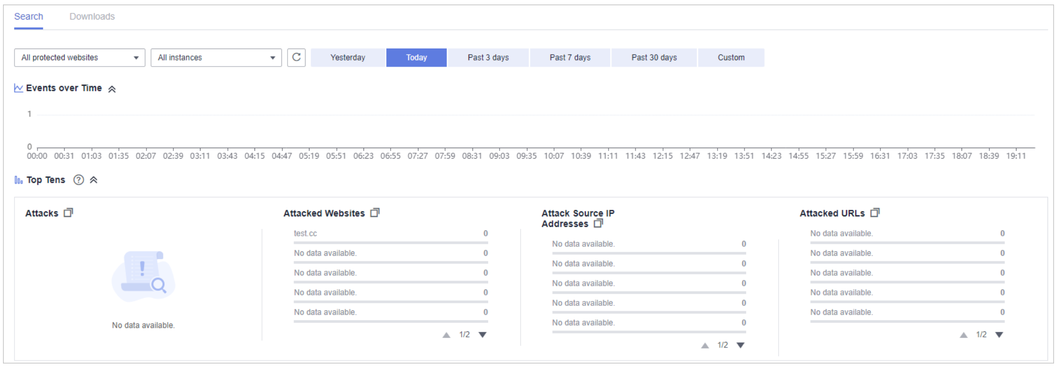
On the WAF console, you can view logs for the last 30 days and download logs for all protected websites for the last five days for free.

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).

8.5 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 8-1 Events



For details about protection events, see **Viewing Protection Event Logs**.

8.6 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.

For details about event logs, see **Viewing Protection Event Logs**.

8.7 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.

8.8 Why Is the Number of Logs on the Dashboard Page Inconsistent with That on the Configure Logs Tab?

If the attack source, hit rule, load location, and URL are consistent for multiple attacks, only one log is displayed on the **Configure Logs** tab. So, the **Dashboard** page displays more logs.

A Change History

Released On	Description
2024-03-22	This issue is the fifth official release. Added the following content: **Most Frequently Asked Questions**
2024-02-23	This issue is the fourth official release. Added or optimized some FAQs related to dedicated WAF instances.
2023-03-23	This issue is the third official release. Added the following content: ● **Can I Obtain WAF Logs Using APIs?** ● **WAF Instance Specifications Change** ● **Purchasing WAF** ● **Protection Event Logs**
2022-10-10	This issue is the second official release. Added the following content: ● **How Do I Change the WAF Instance Edition to a Lower One and Reduce Number of Packages?** ● **Where and When Can I Buy a Domain, QPS, or Rule Expansion Package?**
2022-09-15	This issue is the first official release.