Web Application Firewall

FAQs

Issue   06
Date   2024-11-07

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 About WAF

1.1 WAF Basics

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 CDN or 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.

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 back-to-source IP addresses on the origin servers.

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

- Cloud mode: **Whitelisting WAF Back-to-Source 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.

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.

What Is a Protection IP Address?

A protection IP address in WAF is the IP address of a website you use WAF to protect.

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 back-to-source IP addresses used by WAF to forward healthy traffic. WAF back-to-source IP addresses must be whitelisted on your origin server. For more details, see **How Do I Whitelist Back-to-Source IP Addresses 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.

Which CVE Vulnerabilities Can WAF Defend Against?

WAF can defend against the following CVE vulnerabilities: CVE-2017-7525, CVE-2019-17571, CVE-2018-1270, CVE-2016-1000027, CVE-2022-22965, CVE-2022-22968, and CVE-2018-20318.

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.

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.

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.

1.2 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.

1.3 What Objects Does WAF Protect?

Web Application Firewall (WAF) 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 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.

1.4 Does WAF Block Customized POST Requests?

No. WAF does not block user-defined POST requests.

Figure 1-1 shows the detection process of the WAF built-in protection rules for original HTTP/HTTPS requests.

Figure 1-1 WAF engine work process
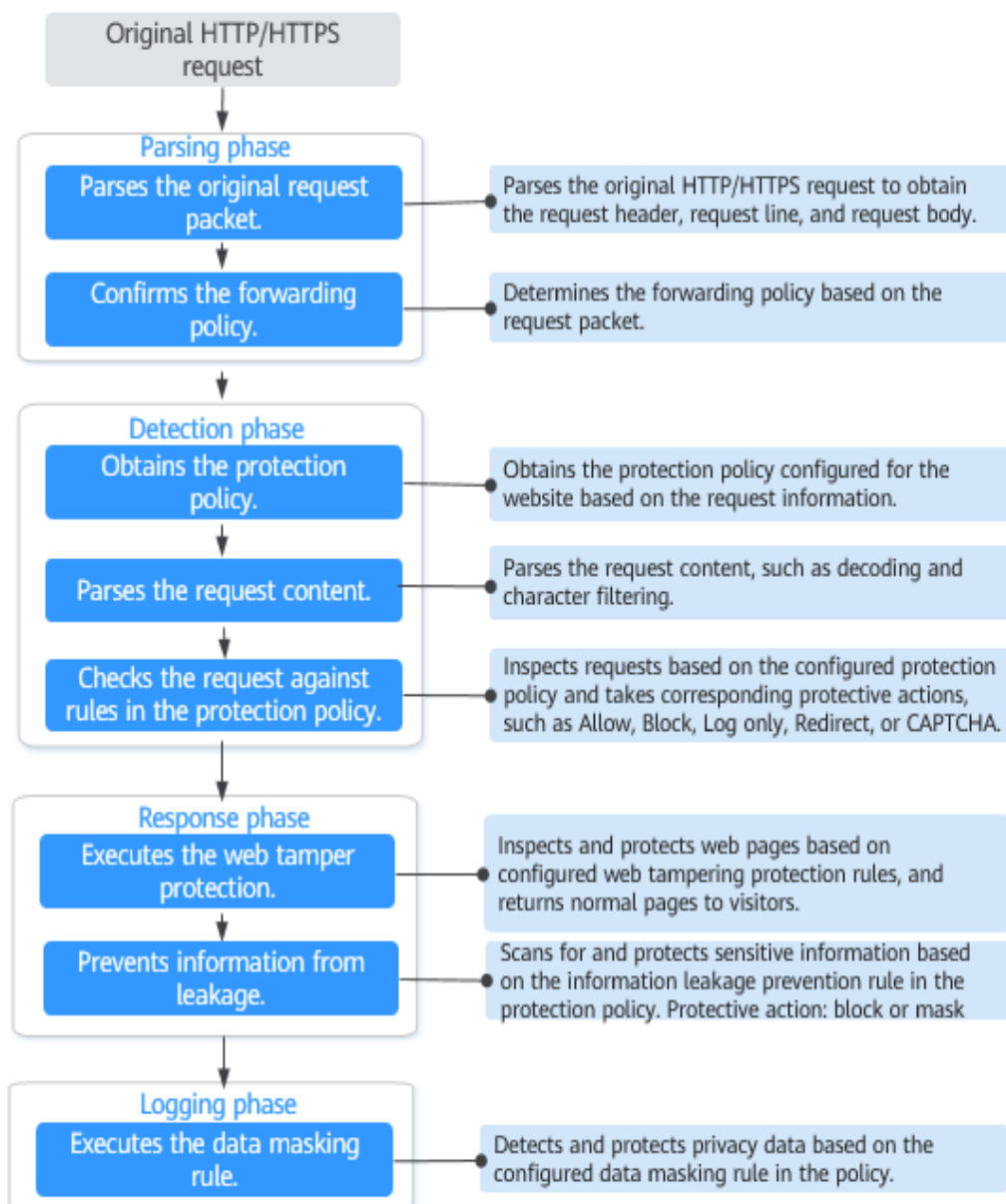
For details about the WAF protection process, see **Configuration Guidance**.

1.5 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 1-1 describes the differences

Table 1-1 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

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

1.6 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

1.7 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.

1.8 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 1-2 How WAF Works
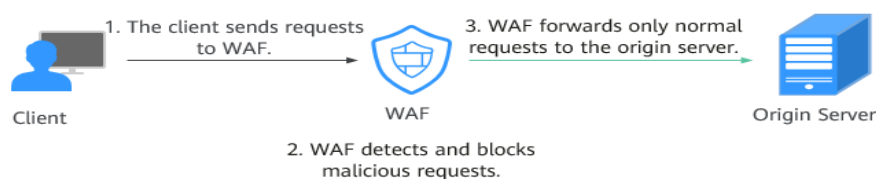
- Nginx forwarding

  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 1-3 How Nginx Works
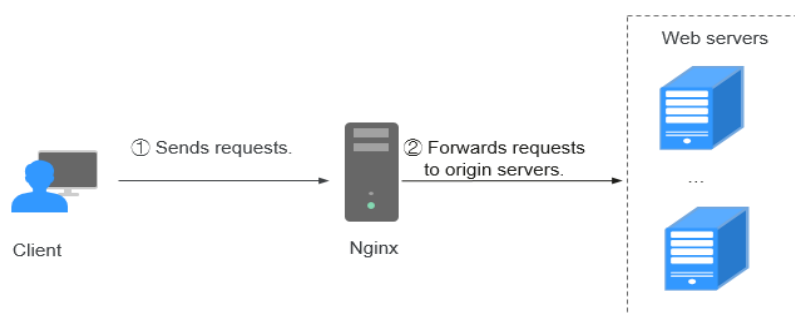
1.9 What Are the Differences Between WAF and CFW?

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 1-2 lists differences between WAF and CFW.

Table 1-2 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 the Internet border and VPC border 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 NAT traffic, to prevent intrusions, penetration attacks, and unauthorized connections to the outside.

Category	WAF	CFW
Deployment mode	WAF can be deployed in cloud mode, ELB mode, and dedicated mode. ● **Cloud Mode**: 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.

1.10 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.

1.11 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.

1.12 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).

Follow the procedure below to complete the configuration.

Configuration Procedure

Step 1 **Buy 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

1.13 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.

1.14 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.

1.15 Will Traffic Be Permitted After WAF Is Switched to the Bypassed Mode?

For cloud WAF instances, if you switch the instance protection mode to **Bypassed**, requests are directly sent to the original backend server without passing through WAF.

The **Bypassed** mode can be enabled only when 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 proxies are configured between the client and WAF.

Effective Time of WAF Bypassed Working Mode

After you switch the protection mode to **Bypassed**, it takes 3 to 5 minutes for the switch to work.

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 **Bypassed** in the **Operation** column. In the dialog box displayed, click **Confirm**.

After you select **Bypassed**, the **Status** of the domain name is **Bypassed**.

----End

1.16 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**.

1.17 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 1-3**.

Table 1-3 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.

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

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

1.18 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.

1.19 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.

📖 **NOTE**

> In the following configurations, WAF does not insert HWWAFSESID (session ID) and HWWAFSESTIME (session timestamp) fields into your customer request cookies:
>
> - **Protection Action** is set to **Allow**.
> - In global whitelist protection rules, **All protection** is selected for **Ignore WAF Protection**.
> - The protection mode is **Suspended**.
> - Basic web protection is disabled.

1.20 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, you can select cloud mode or 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

1.21 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.

1.22 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 About Purchase and Specifications Change

2.1 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**.

2.2 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**.

2.3 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**.

2.4 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.

2.5 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.

2.6 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 2-1 lists the QPS specifications supported by each WAF edition.

Table 2-1 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	200,000 QPS
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

2.7 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.

You can change specifications of your WAF instance as follows before you renew it:

• Upgrade WAF specifications

- – Upgrade your WAF instance from the current edition to a higher edition.
- – Increase the quantity of domain name, QPS, or rule expansion packages.

  For details, see **Changing Cloud WAF Edition and Specifications**.
- Decrease WAF specifications
  - – Unsubscribe from your current instance edition and subscribe to a lower edition
  - – Decrease the quantity of domain name, QPS, bandwidth, and/or rule expansion packages.

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.

2.8 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 a standard, professional, or platinum edition cloud WAF. You can also purchase an expansion package on the **Product Details** page.

For details, see **Expansion Packages**.

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

Buying an Expansion Package Separately

Step 1 Log in to the management 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 **Instance Management** > **Product Details**.

Step 5 Click **Change Specifications** to go to the **Change WAF Specifications** page.

- To change the WAF edition: In the **Edition** row, click **Change Edition** in the **Details** column. In the displayed **Change Edition** pane, select an edition and click **OK**.

- To change expansion packages: In the **Details** column of the **Domain Name Quota**, **QPS Quota**, and **Rule Quota** rows, increase or decrease the number of expansion packages, respectively.

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

- Billing information: Changing specifications does not change the billing mode or expiration date.

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

Step 7 Check the order details and read the *Web Application Firewall Disclaimer*. Then, select *I have read and agree to the WAF Disclaimer*, and click **Pay Now**.

Step 8 On the payment page, select a payment method and pay for your order.

----End

2.9 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 about QPS expansion packages, see **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.

2.10 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**.

2.11 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**.

2.12 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 upper left 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

3 Website Connect Issues

3.1 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.

3.2 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.

3.3 How Do I Whitelist Back-to-Source IP Addresses 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.
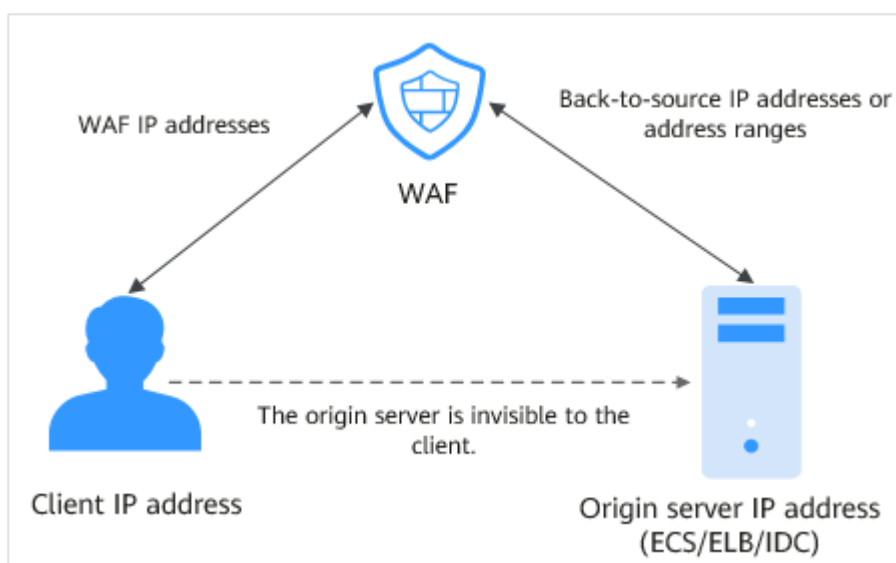
What Are Back-to-Source IP Addresses?

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 back-to-source IP addresses due to scale-out or new clusters. For your legacy domain names, WAF back-to-source 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 disaster recovery 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 3-1 Back-to-source IP address

WAF Back-to-Source IP Address Check Mechanism

A back-to-source 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 Back-to-Source 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 back-to-source IP addresses are blocked, the website may fail to be accessed or it opens extremely slowly. To fix this, add the WAF back-to-source 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 of the page and choose **Security** > **Web Application Firewall**.

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

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

Figure 3-2 WAF Back-to-Source IP Addresses
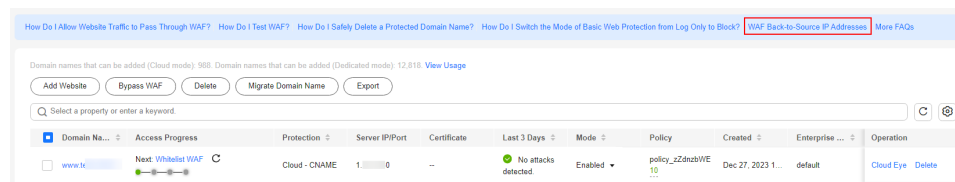
Step 6 In the displayed dialog box, click **Copy** to copy all the addresses.

Figure 3-3 WAF Back-to-Source IP Addresses dialog box
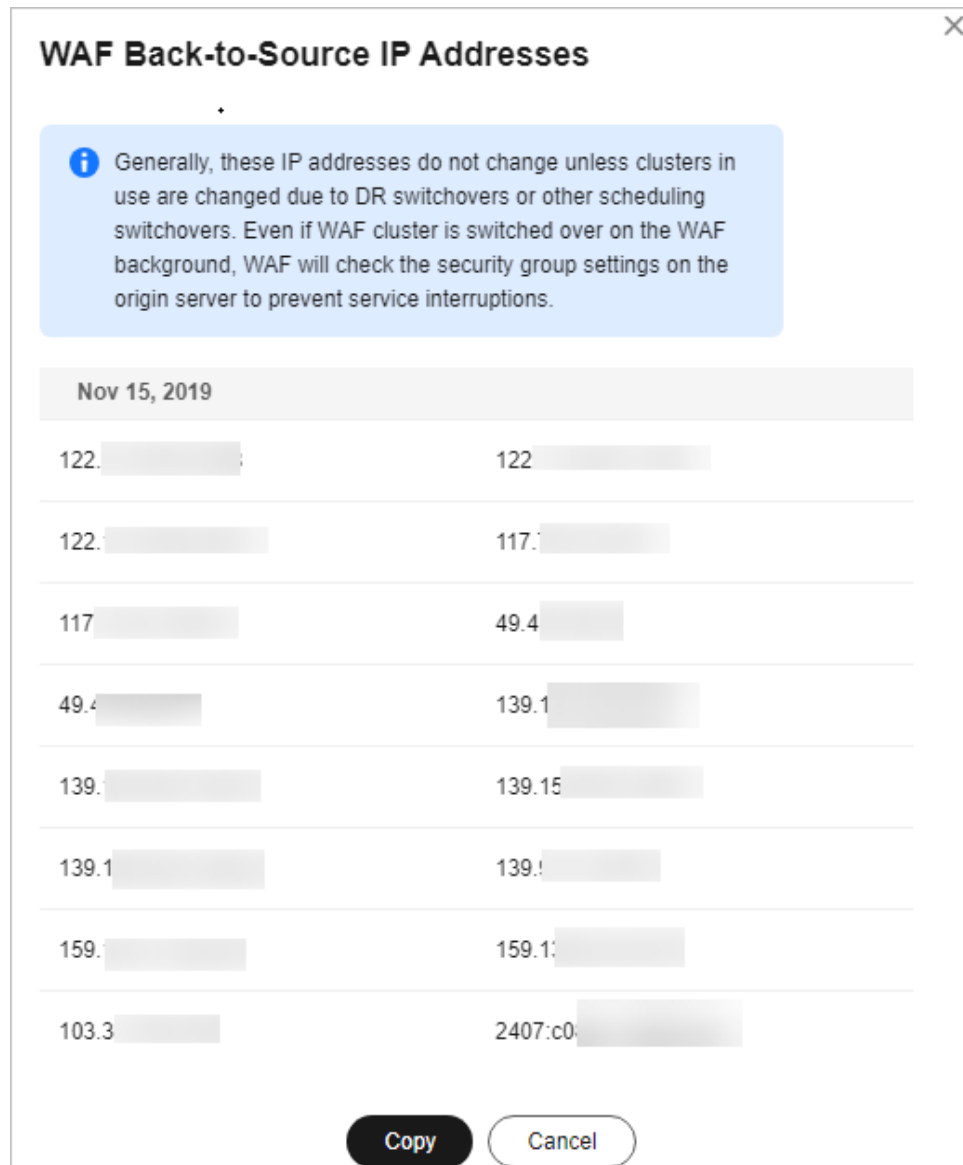
Step 7 Open the security software on the origin server and add the copied IP addresses to the whitelist.

If your origin servers are deployed on Huawei Cloud ECSs or your website uses Huawei Cloud ELB load balancers, whitelist WAF back-to-source 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

3.4 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.

3.5 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.

3.6 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.

3.7 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.

3.8 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.

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

Background

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.

Causes

Your domain name might have been added to WAF under another account. A domain name can only be added to WAF once.

Solution

If you want to add it to WAF under the current account, delete it from another account first.

3.10 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).

3.11 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**.

3.12 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 3-4 Adding a record set

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

3.13 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. On the top of the page, click ⑦ next to **Inaccessible**. In the dialog box displayed, copy the subdomain name and 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 3-5** shows the example.

Figure 3-5 DNS page
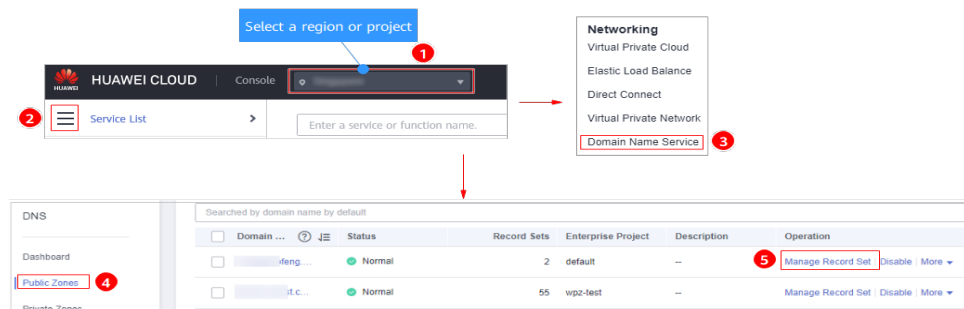
2. In the upper left corner, click **Add Record Set** to go to the **Add Record Set** page.

    –   **Name**: Paste the TXT record copied in **Step 1.4** 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 1.4** and paste them in the text box, for example, "37c795804124dd4a0dd88defff8941f".

    –   Keep other settings unchanged.

Figure 3-6 Adding a record set

3. Click **OK**.

----End

3.14 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.

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

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

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

3.15 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.

- Cloud

  Switch the WAF protection 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 3-7**, 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 3-7 Dedicated WAF instance deployment architecture (private network load balancers deployed behind dedicated WAF instances)
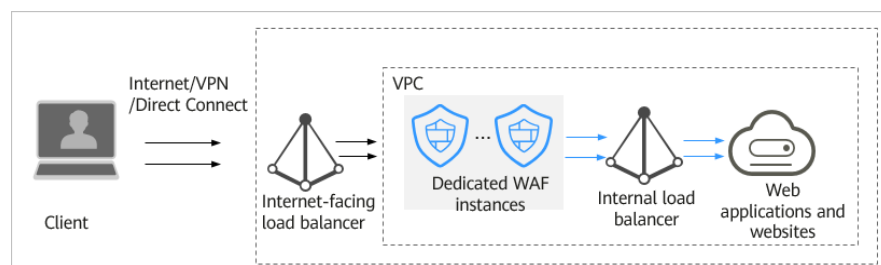
  – If your website has no private network load balancer deployed behind the dedicated WAF instance, as shown in **Figure 3-8**, unbind the EIP from the dedicated WAF instance and then bind the EIP to the origin server. In doing so, your website traffic will bypass WAF and directly go to the origin server.

Figure 3-8 Dedicated WAF instance deployment architecture (no private network load balancer deployed behind dedicated WAF instances)
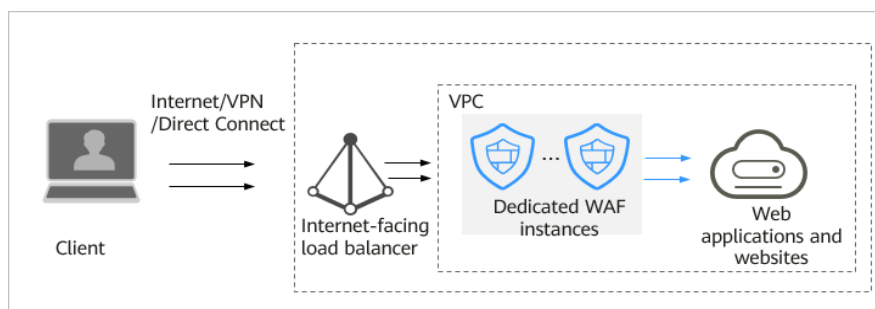
Constraints

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 on 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, choose **Website Settings**.

Step 5 In the row containing the target domain name, click **Bypassed** in the **Operation** column. In the dialog box displayed, click **Confirm**.

After you select **Bypassed**, the **Status** of the domain name is **Bypassed**.

----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 3-9** shows an example.

Figure 3-9 Unbinding an EIP from an internet-facing load balancer

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 3-10 Load balancer list

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 3-11** shows an example.

Figure 3-11 Removing a dedicated WAF instance from an internet-facing load balancer
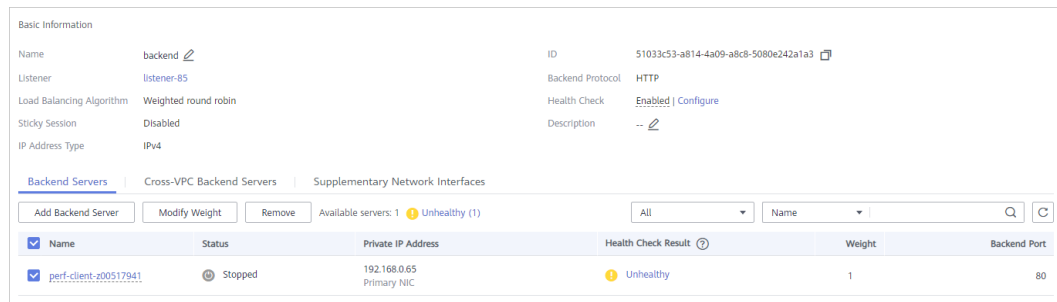
Step 5 In the displayed dialog box, click **Yes**.

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

Step 7 Click **Next**, configure the service port, and click **Finish**.

----End

4 Protection Rules

4.1 Which Protection Levels Can Be Set for Basic Web Protection?

Basic Web Protection has three protection levels. The default protection level is **Medium**. For details, see **Table 4-1**.

Table 4-1 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**.

4.2 What Is the Peak Rate of CC Attack Protection?

It depends on the WAF edition you are using. For details, see **Table 4-2**.

Table 4-2 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
Professional	● Service requests: 5,000 QPS ● WAF-to-Server connections: 6,000 per domain name	200,000 QPS
Platinum	● Service requests: 10,000 QPS ● WAF-to-Server connections: 6,000 per domain name	1,000,000QPS

Edition	Peak rate of normal service requests	Peak rate of CC attack protection
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

4.3 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.

4.4 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**.

4.5 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 4-1** shows an example.

Figure 4-1 Verification failed
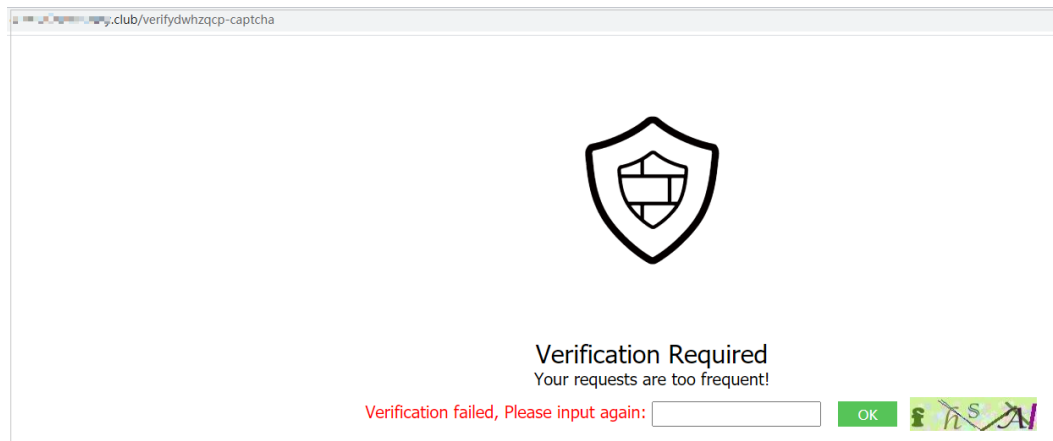
After **Verification code** is configured, a verification code is required when the number of requests exceeds the maximum limit within a specified period. Upon completing the verification, the access limit is lifted.

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 4-3**.

Figure 4-2 Configure Cache Policy
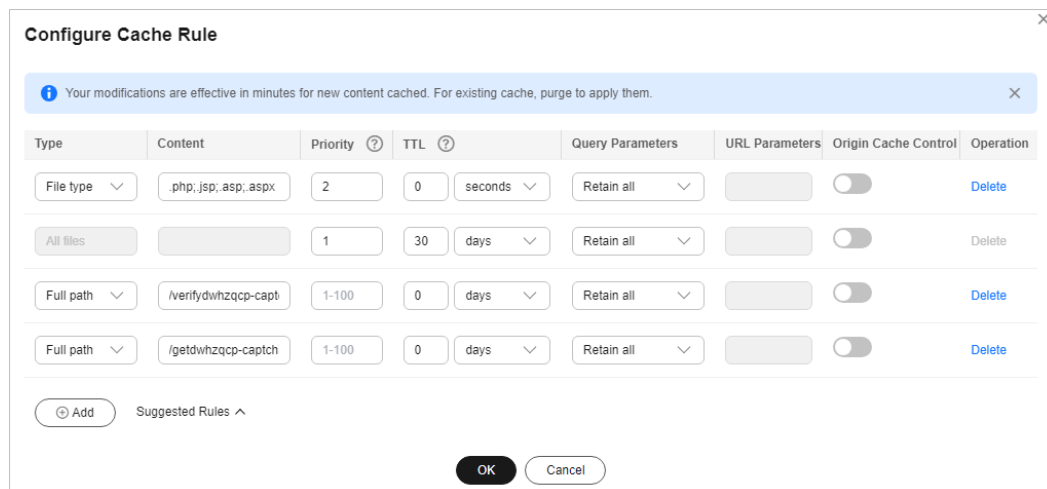
Table 4-3 Parameters for configuring static URL cache policy

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**
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 4-3 Configured cache policies
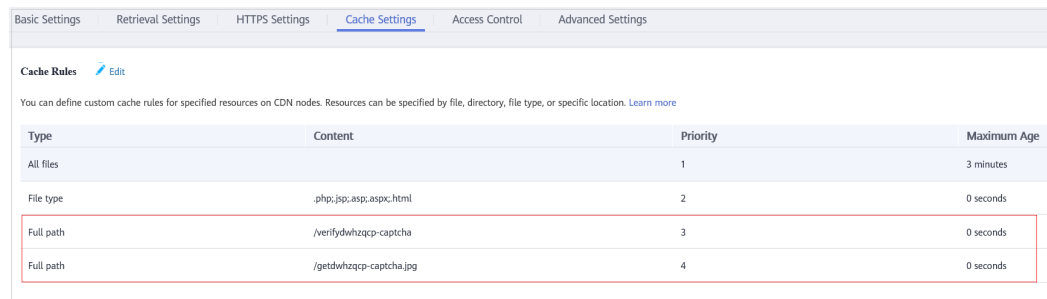
After the configuration is complete, it takes 3 to 5 minutes for the configured cache policies to take effect.

----End

4.6 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.

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

4.7 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.

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

4.8 Why Does a Requested Page Fail to Respond to the Client After the JavaScript-based 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 4-4** shows how JavaScript verification works.

Figure 4-4 JavaScript anti-crawler detection process
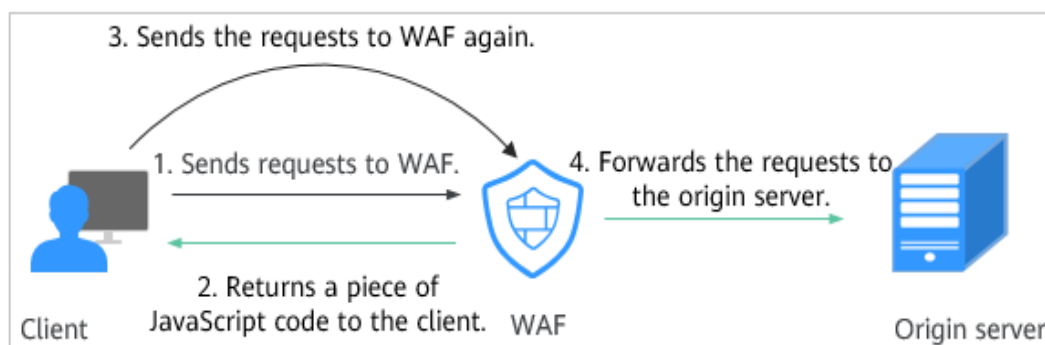
- If the client is a crawler, it cannot be triggered by the received JavaScript code and will not send a request to WAF again. The client fails JavaScript authentication.
- If a client crawler fabricates a WAF authentication request and sends the request to WAF, the WAF will block the request. The client 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.

4.9 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 4-5 Enabling **Other**
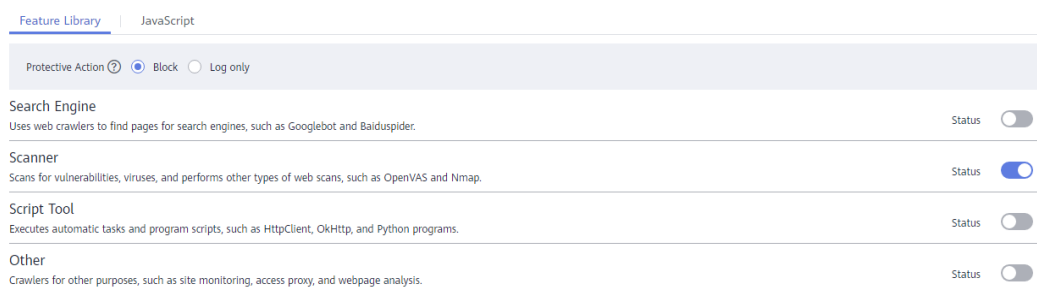
For details, see **Configuring Anti-Crawler Rules**.

4.10 How Does JavaScript Anti-Crawler Detection Work?

Figure 4-6 shows how JavaScript anti-crawler detection works, which includes JavaScript challenges (step 1 and step 2) and JavaScript authentication (step 3).

Figure 4-6 JavaScript Anti-Crawler protection process
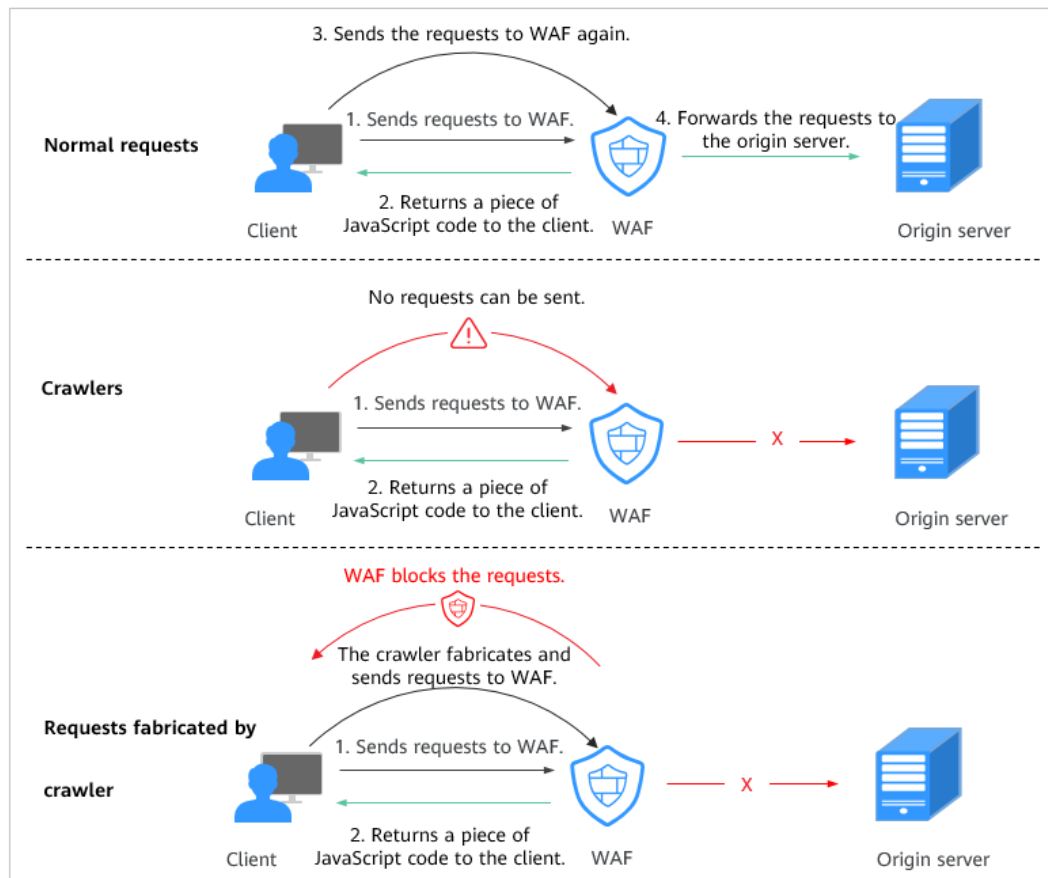
After JavaScript anti-crawler is enabled, WAF returns a piece of JavaScript code to the client when the client sends a request.

- If the client sends a normal request to the website, triggered by the received JavaScript code, the client will automatically send the request to WAF again. WAF then forwards the request to the origin server. This process is called JavaScript verification.

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

- If a client crawler fabricates a WAF authentication request and sends the request to WAF, the WAF will block the request. The client fails JavaScript authentication.

By collecting statistics on the number of JavaScript challenge and authentication responses, the system calculates how many requests the JavaScript anti-crawler defends. As shown in **Figure 4-7**, 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 4-7 Parameters of a JavaScript anti-crawler protection rule
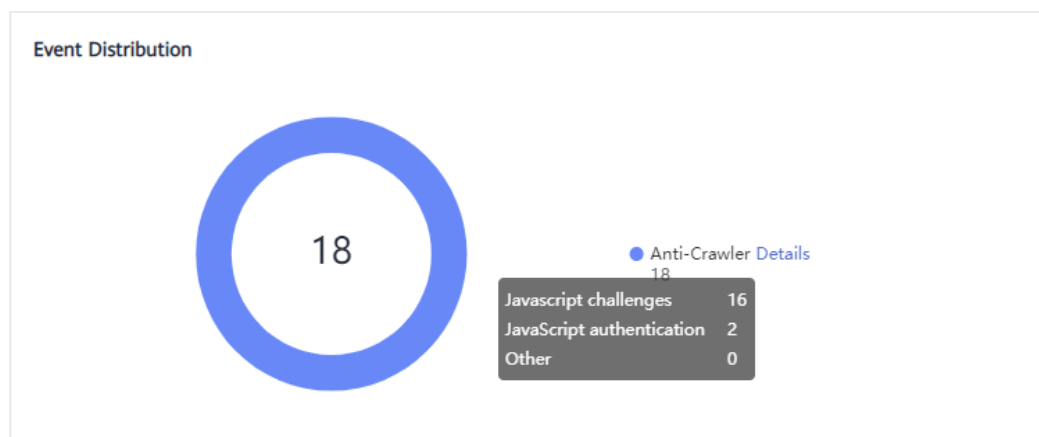
> **NOTICE**
>
> WAF only logs JavaScript challenge and JavaScript authentication events. No other protective actions can be configured for JavaScript challenge and authentication.

4.11 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.

For details about how to configure WAF and CDN, see **Combining CDN and WAF to Get Improved Protection and Load Speed**.

4.12 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 4-8 Selecting Allow for Protective Action

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

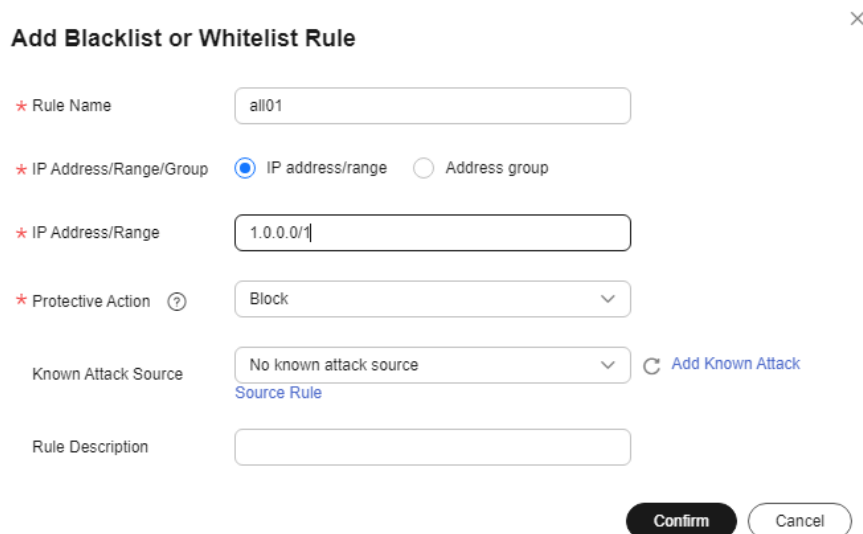**Figure 4-9** Blocking all access requests

----End

4.13 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 of the page and choose **Security** > **Web Application Firewall**.

Step 4 In the navigation pane on the left, choose **Policies**.
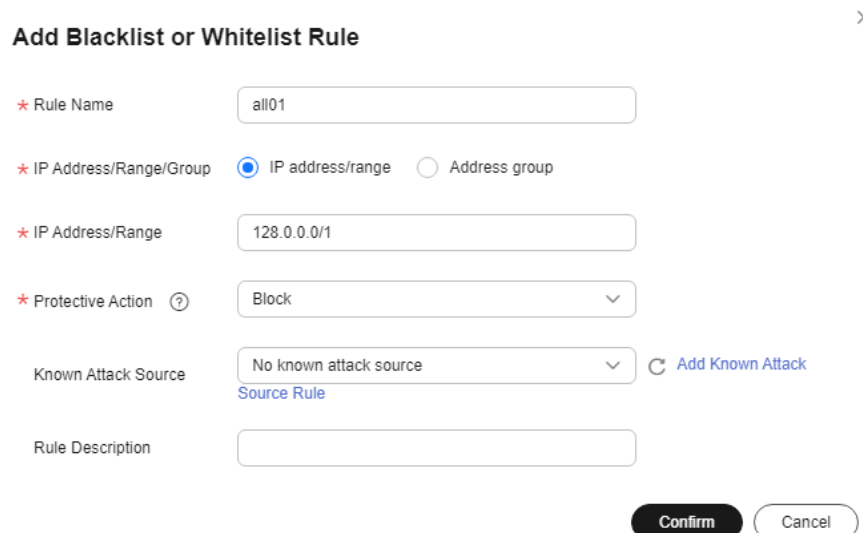
Step 5 Click the name of the target policy to go to the protection configuration page.

Step 6 In the **Blacklist and Whitelist** configuration area, enable the protection.

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 4-10 Blocking IP address range 1.0.0.0/1

Figure 4-11 Blocking IP address range 128.0.0.0/1

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 4-12**.

Figure 4-12 Allowing the access of a specified IP address

----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 of the page 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 **Precise Protection** configuration area, enable the protection.

Figure 4-13 Precise Protection configuration area
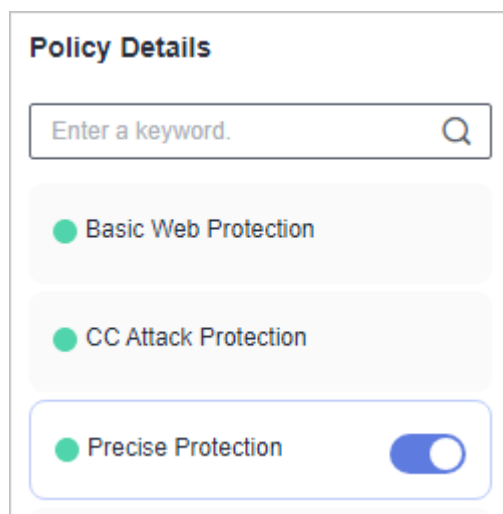
Step 7 Click **Customize Rule**. In the upper left corner of the displayed page, click **Add Rule**.

Step 8 In the displayed **Add Precise Protection Rule** dialog box, add a protection rule as shown in **Figure 4-14** 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 4-14 Blocking all requests
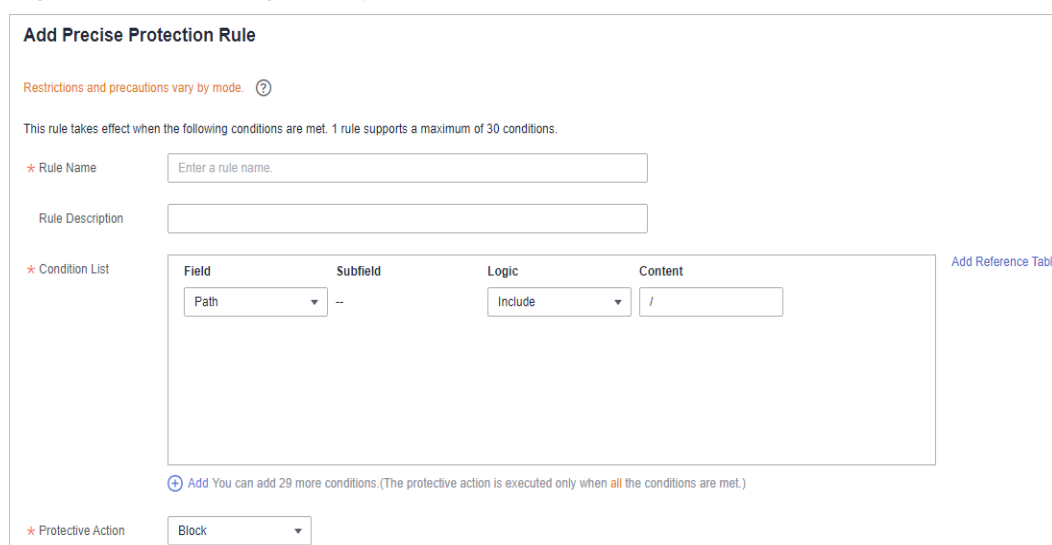
Step 9 Click **Add Rule**. In the displayed **Add Precise Protection Rule** dialog box, add a rule for the specified IP address.

For example, if you want to allow 192.168.2.3 to access the website, add a protection rule as shown in **Figure 4-15**.

⚠️ **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 4-15 Allowing the access of a specified IP address

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

----End

4.14 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 4-4**.

🔵 **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 4-4 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.

4.15 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 of the page 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 Click the **Web Tamper Protection** configuration area and check whether this function is enabled.

- If this function is enabled ( ), go to **Step 7**.

- If this function is disabled ( ), click to enable the function. Refresh the page several minutes later.

Step 7 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

4.16 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 4-5** describes the differences between the two types of rules.

Table 4-5 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.

4.17 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.

5 Certificate Management

This topic lists some frequently asked questions (FAQs) about how to use a certificate.

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.

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.

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 5-1** before uploading it.

Table 5-1 Certificate conversion commands

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

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

☐ **NOTE**

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

6 Protection Event Logs

6.1 Can I Obtain WAF Logs Using APIs?

You can call an API to view WAF protection logs.

You can also analyze, view, and download events on the LTS console. For details, see **Downloading Events Data**.

6.2 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**.

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

This depends on which WAF access mode is used for the website.

Cloud Mode - CNAME Access and Dedicated Mode

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 **Yes** for **Use Layer-7 Proxy** 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 no proxy is used, WAF obtains the source IP address from the **remote_ip** field.

6.4 How Long Can WAF Protection Logs Be Stored?

WAF stores protection event logs generated over the last 30 days for free. You can check them on the WAF console.

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).

6.5 Can I Query Protection Events of a Batch of Specified IP Addresses at Once?

WAF does not support batch query of protection events of a batch of specified IP addresses at once. On the **Events** page, you can view events by a certain combination of **Event Type**, **Protective Action**, **Source IP Address**, **URL**, and **Event ID**.

Figure 6-1 Events

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

6.6 Will WAF Record Unblocked Events?

No. WAF blocks attack events based on the configured protection rules and records only blocked attack events in protection event logs.

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

6.7 Why Is the Traffic Statistics on WAF Inconsistent with That on the Origin Server?

In any of the following scenarios, the traffic statistics displayed on the WAF **Dashboard** page may be inconsistent with that displayed on the origin server:

- Web page compression

  WAF enables compression by default. The web pages between the client (such as a browser) and WAF may be compressed (depending on the compression option of the browser), but the origin server may not support compression.

- Connection reuse

  WAF reuses socket connections with the origin server, which reduces the bandwidth usage between the origin server and WAF.

- Attack requests

  Attack requests blocked by WAF do not consume the bandwidth of the origin server.

- Other abnormal requests

  If the origin server times out or cannot be connected, the bandwidth of the origin server is not consumed.

- TCP retransmission

  WAF collects bandwidth statistics at layer 7, but the network adapter of the origin server collects bandwidth statistics at layer 4. If the network connection is poor, TCP retransmission occurs. The bandwidth measured by the network adapter is calculated repeatedly, but the data transmitted at layer 7 is not calculated repeatedly. In this case, the bandwidth displayed on WAF is lower than that displayed on the origin server.

6.8 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.

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

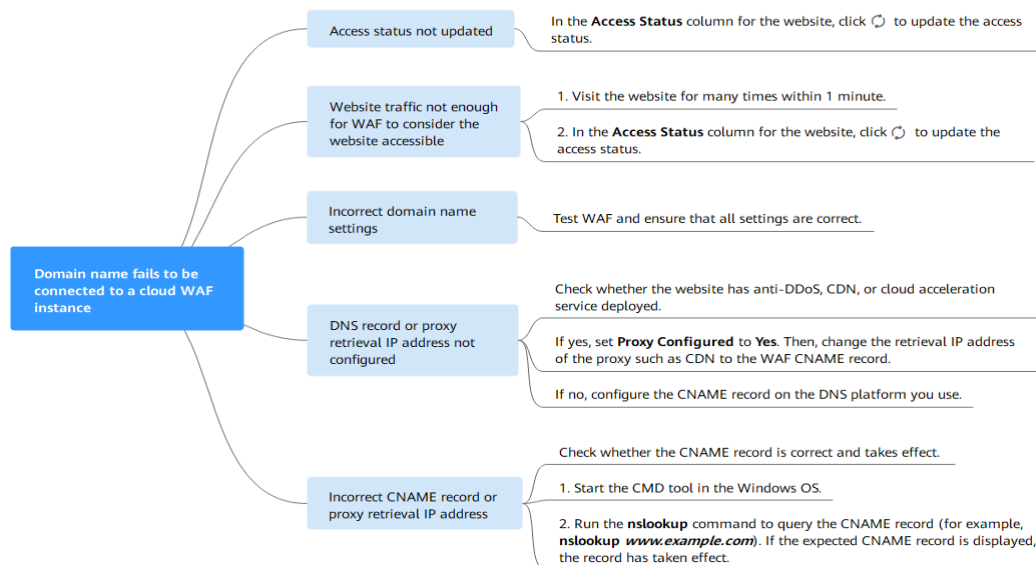# 7 Why Is My Domain Name or IP Address Inaccessible?

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 7-1** and **Table 7-1** to fix connection failures for websites protected in cloud mode.

Figure 7-1 Troubleshooting for Cloud WAF

Table 7-1 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 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 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 IP address in **2** is displayed in the command output, the domain name settings are correct. If there are incorrect domain name settings, remove the domain name from WAF and add it to WAF again.

Possible Cause	Solution
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 **Adding 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 work, modify the DNS record or the back-to-source address of the in-use proxy. For details, see **Adding a Domain Name to WAF**.

8 How Do I Fix an Incomplete Certificate Chain?

If the certificate provided by the certificate authority is not found in the built-in trust store on your platform and the certificate chain does not have a certificate authority, the certificate is incomplete. If you use the incomplete certificate to access the website corresponding to the protected domain name, the access will fail.

Use either of the following methods to fix it:

- Make a complete certificate chain manually and upload the certificate.
- 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 **View and export the certificate.**

1. Click the padlock in the address bar to view the certificate status.

2. Locate the row that shows **Secure Connection**, click ❯, and click **Valid Certificate** in address bar.

3. Click the **Details** tab. In the lower right corner of the page, click **Copy to File…** to export the certificate to the local PC.

Step 2 Check the certificate chain. Open the certificate you export. Select the **Certificate Path** tab and then click the certificate name to view the certificate status.
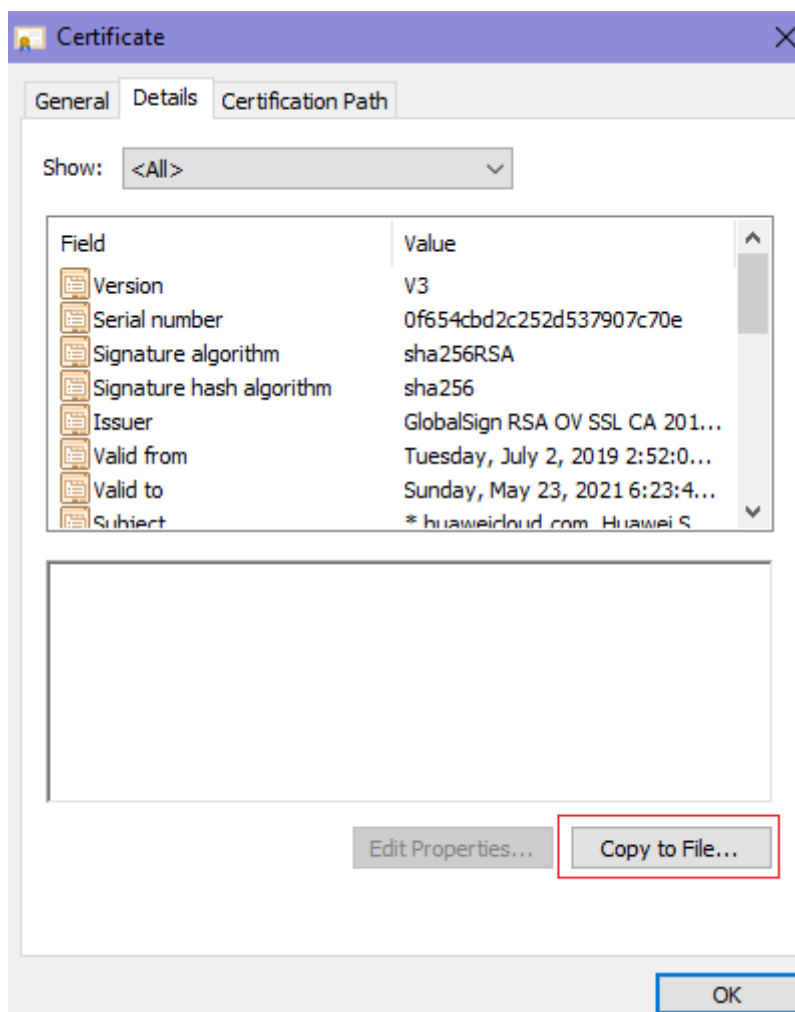
Figure 8-1 Viewing the certificate chain
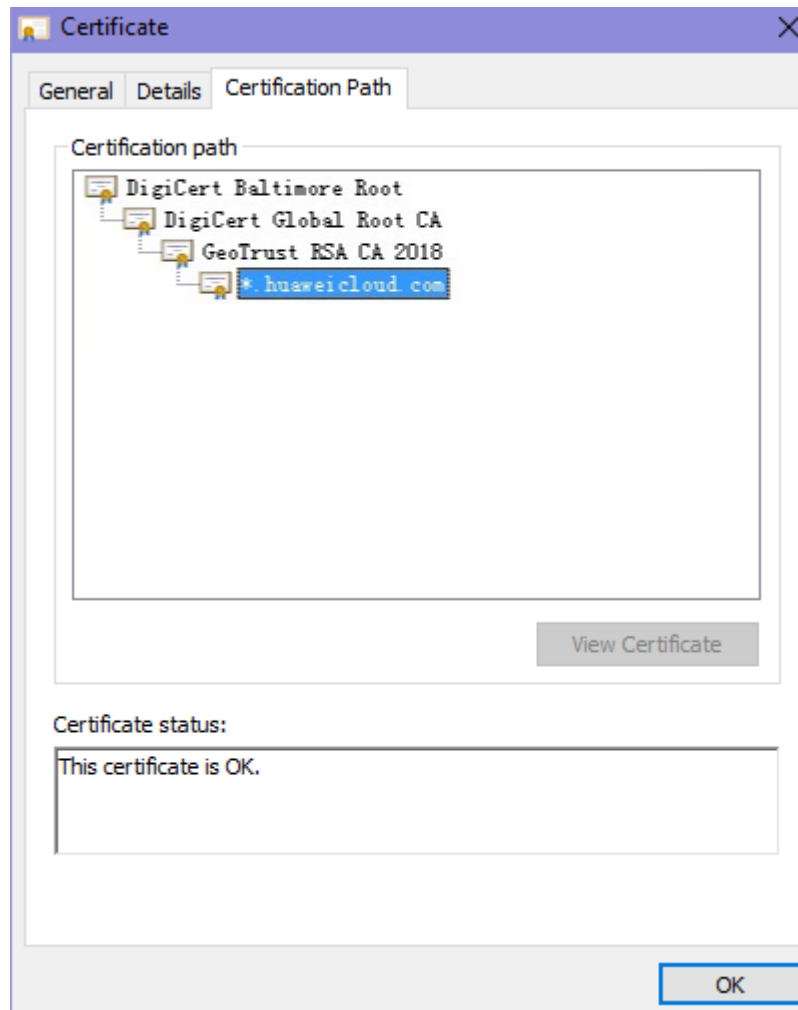
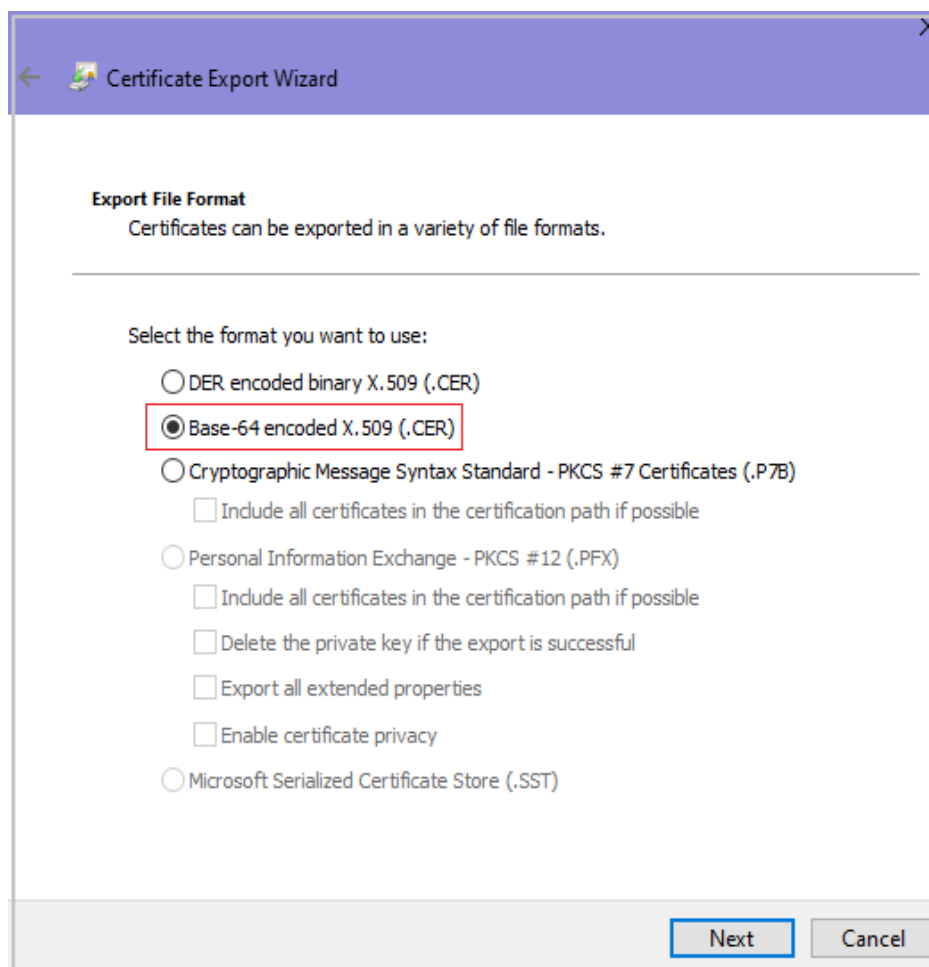**Step 3** Save the certificates to the local PC one by one.

1. Select the certificate name and click the **Details** tab.

Figure 8-2 Details

2. Click **Copy to File**, and then click **Next** as prompted.
3. Select **Base-64 encoded X.509 (.CER)** and click **Next**. **Figure 8-3** shows an example.

Figure 8-3 Certificate Export Wizard

Step 4 Rebuild the certificate. After all certificates are exported to the local PC, open the certificate file in Notepad and rebuild the certificate according to the sequence shown in **Figure 8-4**.

Figure 8-4 Certificate rebuilding
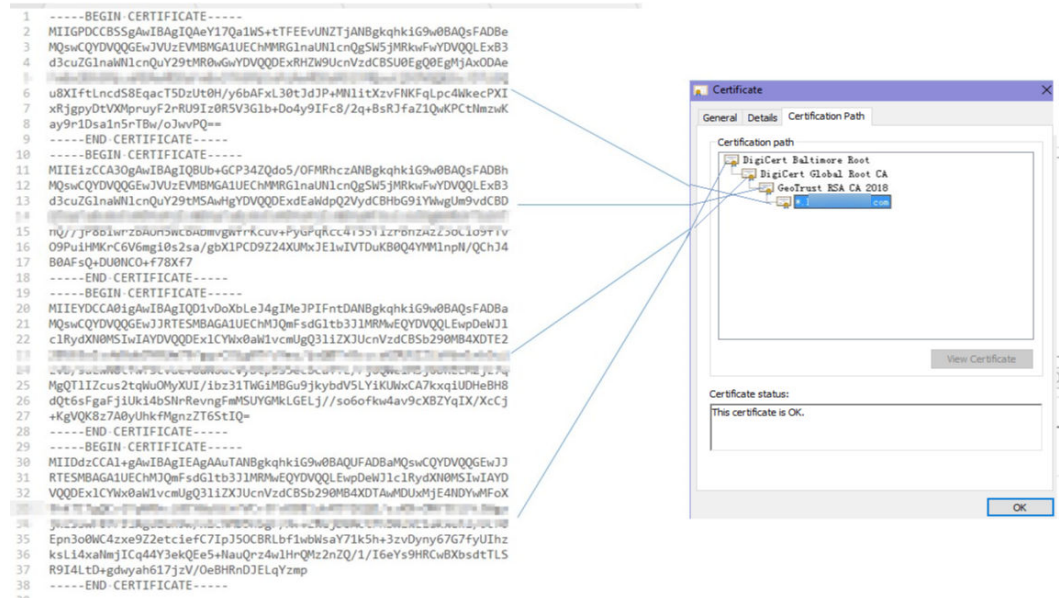
Step 5 Upload the certificate again.

----End