Web Application Firewall

Troubleshooting

 Issue
 01

 Date
 2025-04-25





Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

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

Trademarks and Permissions

NUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

1 Troubleshooting Website Connection Exceptions	1
1.1 Why Is My Domain Name or IP Address Inaccessible?	1
1.2 Why Does the Requested Page Respond Slowly After My Website Is Connected to WAF?	7
1.3 What Can I Do If Files Cannot Be Uploaded After a Website Is Connected to WAF?	8
2 Troubleshooting Certificate and Cipher Suite Issues	9
2.1 How Do I Fix an Incomplete Certificate Chain?	9
2.2 Why Does My Certificate Not Match the Key?	13
2.3 Why Are HTTPS Requests Denied on Some Mobile Phones?	14
2.4 What Do I Do If the Protocol Is Not Supported and the Client and Server Do Not Support Commo SSL Protocol Versions or Cipher Suites?	n 15
2.5 Why Is the Bar Mitzvah Attack on SSL/TLS Detected?	15
3 Troubleshooting Traffic Forwarding Exceptions	16
3.1 What Is Error Code 404, 502, or 504 Returned to Visitors After My Website or Application Is Connected to WAF?	16
3.2 Why Am I Seeing Error Code 418?	26
3.3 Why Am I Seeing Error Code 523?	26
3.4 Why Was My Website Redirected So Many Times?	28
3.5 Why Am I Seeing Error Code 414 Request-URI Too Large?	29
3.6 What Do I Do If the CPU Usage of the Origin Server Reaches 100%?	31
3.7 What Is the Connection Timeout Duration of WAF? Can I Manually Set the Timeout Duration?	32
4 Checking Whether Normal Requests Are Blocked Mistakenly	33
4.1 How Do I Handle False Alarms as WAF Blocks Normal Requests to My Website?	33
4.2 Why Does WAF Block Normal Requests as Invalid Requests?	35
4.3 Why Is the Handle False Alarm Button Grayed Out?	35
5 Checking for Permission Exceptions	37
5.1 Why Cannot I Access the Dedicated Engine Page?	37
5.2 Why Cannot I Select an SCM Certificate When Adding a Domain Name to WAF?	37

Troubleshooting Website Connection Exceptions

1.1 Why Is My Domain Name or IP Address Inaccessible?

Symptoms

After a domain name or IP address is added to WAF, the connection between WAF and the domain name or IP address fails to be established.

NOTICE

- WAF automatically checks the access status of protected websites every 30 minutes. If WAF detects that a protected website has received 20 access requests within 5 minutes, it considers that the website has been successfully connected to WAF.
- By default, WAF checks only the access status of domain names added or updated over the last two weeks. If a domain name was added to WAF two

weeks ago and has not been modified in the last two weeks, you can click \bigcirc in the **Access Status** column to refresh its status.

Troubleshooting and Solutions for Cloud WAF Instances

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

Figure 1-1 Troubleshooting for Cloud WAF



Table 1-1 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 ^O 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.	 Access the protected website for many times within 1 minute. 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.
	 In Windows OSs, choose Start > Run. Then enter cmd and press Enter.
	2. Ping the CNAME record (for example, ping e59e684e2278043ae98a5423 aef8ee329.vip.huaweicloudw af.com) of the domain name to obtain the WAF IP address.
	 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 the following record to the hosts file: <i>WAF IP address mapped to the domain name Protected domain name</i> .
	 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.

Possible Cause	Solution
	If there are incorrect domain name settings, remove the domain name from WAF and add it to WAF again.
Cause 4: DNS record or the back-to-source IP addresses of proxies not configured	Check whether the website connected to WAF uses proxies such as advanced anti-DDoS, CDN, and cloud acceleration service.
	• Yes. If yes, ensure that Use Layer-7 Proxy is set to Yes for the website.
	 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.

Possible Cause	Solution	
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:	
	 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:	
	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.	

Troubleshooting and Solutions for Dedicated WAF

Refer to **Figure 1-2** and **Table 1-2** to fix connection failures.

Figure 1-2 Troubleshooting for dedicated mode



Possible Cause	Solution
Cause 1: Access Status for Domain Name/IP Address not updated	In the Access Status column for the website, click \bigcirc 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.	 Access the protected website many times within 1 minute. In the Access Status column for the website, click to update the status.
Cause 3: Incorrect domain name or IP address settings	Check domain name or IP address settings by referring to View the basic information about the domain name. If there are incorrect settings for the domain name or IP address, remove this domain name or IP address from WAF and add it to WAF again.
Cause 4: No load balancer configured for the dedicated WAF instance or no EIP bound to the load balancer configured for the dedicated WAF instance	 Configure a load balancer for dedicated WAF instances by referring to Configuring a Load Balancer. Binding an EIP to a Load Balancer.
Cause 5: Incorrect load balancer configured or incorrect EIP bound to the load balancer	 After you configure a load balancer, ensure that Health Check Result for the dedicated WAF instances added to the load balancer is Healthy. For details about troubleshooting, see How Do I Troubleshoot an Unhealthy Backend Server? After you bind an EIP to the load balancer, check the EIP status.

Table 1-2 Solutions for dedicated mode

Troubleshooting and Solutions for Cloud Load Balancer Access Mode

For **Cloud Mode - Load balancer**, refer to **Figure 1-3** and **Table 1-3** to fix connection failures.



Figure 1-3 Troubleshooting for Cloud - Load Balancer Access Mode

Table 1-3 Troubleshooting for website connection failure in WAF - Cloud load

 balancer access mode

Possible Cause	Solution
Cause 1: Access Status for Domain Name/IP Address not updated	In the Access Status column for the website, click \bigcirc 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.	 Access the protected website for many times within 1 minute. In the Access Status column for the website, click to update the status.
Cause 3: Incorrect domain name or IP address settings	View the basic information about the domain name. Check whether the domain name or IP address settings are correct. If there are incorrect settings, remove the domain name or IP address from WAF and add it to WAF again.

1.2 Why Does the Requested Page Respond Slowly After My Website Is Connected to WAF?

Symptom

After a website is connected to WAF, the website becomes slow.

Possible Causes

You may have configured forcible redirection from HTTP to HTTPS at the backend of the server but enabled only forwarding from HTTPS (client protocol) to HTTP (origin server protocol) on WAF. This makes WAF redirects requests, which leads to an infinite loop.

Solution

To address this issue, add HTTP-to-HTTP and HTTPS-to-HTTPS forwarding rules. The procedure is as follows:

- **Step 1** Log in to the WAF console.
- **Step 2** In the navigation pane on the left, choose **Website Settings**.
- **Step 3** In the domain name list, click the target domain name.
- Step 4 In the Origin Servers area, click Edit.
- **Step 5** In the **Edit Server Information** dialog box, add two forwarding rules, one for HTTP to HTTP and the other for HTTPS to HTTPS.

Figure 1-4 Example configuration

Edit Server Information				
Client Protocol ⑦ Server Protocol ⑦	Server Address (?)	Server Port 📀	Weight	Active/Standby 🧿
Θ HTTP \checkmark HTTP \checkmark	IPv4 v	80	1	Active se V
Θ HTTPS \checkmark HTTP \checkmark	IPv4 V .6	80	1	Active se 🗸
Add Origin server addresses you can add: 48 If you plan to configure multiple pieces of server inform	nation, specify at least one active server.			
IPv6 Protection	Enable Disable			
Your domain name supports the client protocol HTTPS using the certificate				
International Existing certificates/12222	~			

----End

For details about how to configure a forwarding rule, see **Why Was My Website Redirected So Many Times?**

1.3 What Can I Do If Files Cannot Be Uploaded After a Website Is Connected to WAF?

After your website is connected to WAF, the size of the file each time you can upload to the website is limited as follows:

- Cloud mode CNAME access: 1 GB
- Cloud mode Load balancer access mode: 10 GB
- Dedicated mode: 10 GB

To upload a file larger than what is allowed, upload the file through any of the following:

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

2 Troubleshooting Certificate and Cipher Suite Issues

2.1 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.

📃 Certificate	×
General Details Certification Path	
Certification path	
Certificate status: This certificate is OK.	View Certificate
	ОК

Figure 2-1 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 2-2 Details

<u>न</u> Certifi	cate			×
General	Details	Certification Path		
Show:	<all></all>		~	
Field			Value	^
Ver Ser	rsion rial numbe	er	V3 0f654cbd2c252d537907c70e	
🔄 Sig	nature al	gorithm	sha256RSA	
Sig	nature ha	ash algorithm	sha256	
	uer lid from		Giobalsign RSA OV SSL CA 201 Tuesday, July 2, 2019 2:52:0	
l val	lid to		Sunday, May 23, 2021 6:23:4	
- Sul	hiect		* huaweidoud.com. Huawei S	~
		Ed	it Properties Copy to File	
			O	<

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

Expo (rt File Format Certificates can be exported in a variety of file formats.
5	Select the format you want to use:
	O DER encoded binary X.509 (.CER)
	Base-64 encoded X.509 (.CER)
	O Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
	O Personal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
	Enable certificate privacy
	O Microsoft Serialized Certificate Store (.SST)

Figure 2-3 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 2-4.

Figure 2-4 Certificate rebuilding



Step 5 Upload the certificate again.

----End

2.2 Why Does My Certificate Not Match the Key?

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

Solution

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

Related Operations

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

2.3 Why Are HTTPS Requests Denied on Some Mobile Phones?

Symptom

Open the browser on the mobile phone and access the protected domain name. If a page similar to Figure 2-5 is displayed, the HTTPS request on the mobile phone is abnormal.

Figure 2-5 Access failed



Causes

The uploaded certificate chain is incomplete.

Solution

Fix the issue by referring to How Do I Fix an Incomplete Certificate Chain?

2.4 What Do I Do If the Protocol Is Not Supported and the Client and Server Do Not Support Common SSL Protocol Versions or Cipher Suites?

Symptom

After a domain name is connected to WAF, the website cannot be accessed. A message is displayed, indicating that the protocol is not supported. The client and server do not support common SSL protocol versions or cipher suites.

Solution

Select the default cipher suite for **Cipher Suite** in the **TLS Configuration** dialog box. For details, see **Configuring PCI DSS/3DS Certification Check and TLS Version**.

Figure 2-6 TLS Configuration

		TLS Configurat	tion
·		Certificate Name	11
Deale Information		Туре	International
Website Name - <i>Q</i>	Website Remarks	Minimum TLS Version	TLS v1.0 V Note: Requests to the domain must be made using the selected version or later. Otherwise the request will fail
CNAME (New) 🕜 20443ff4c5c34f91b925330e58847737 🗗	CNAME (Old) 20443ff4c5c34f91b925330e58847737.	Cipher Suite	TLS v1.2 is recommended because it is more secure.
Client Protocol Client Protocol HTTPS International	Compliance Certification PCI DSS PCI 3DS	L	Good browser compatibility, most clients supported, sufficient for most scenarios. Encryption algorithms ECDHE-RSA-ARES26-SHA384 AES256- SHA256 RC4 HIGH:IMD51aNULL:INULL:IDH:IEDH:IAE SGCM
11 <i>L</i>	TLS v1.0 Default cipher suite 2		Confirm

2.5 Why Is the Bar Mitzvah Attack on SSL/TLS Detected?

The Bar Mitzvah attack is a cryptographic attack targeting SSL/TLS protocols. The attack exploits a vulnerability in the RC4 cryptographic algorithm. This vulnerability can disclose ciphertext in SSL/TLS encrypted traffic in some cases, such as passwords, credit card data, or other privacy data, to hackers.

Solution

To solve this problem, you can set the minimum TLS version to TLS v1.2 and cipher suite to cipher suite 2. For details, see **Configuring PCI DSS/3DS Certification Check and TLS Version**.

3 Troubleshooting Traffic Forwarding Exceptions

3.1 What Is Error Code 404, 502, or 504 Returned to Visitors After My Website or Application Is Connected to WAF?

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

404 Not Found Troubleshooting Process and Suggestions

Refer to **Figure 3-1** to fix the 404 Not Found error occurred after your website is connected to WAF.



Figure 3-1 Troubleshooting for 404 Not Found error

• If the page shown in Figure 3-2 is displayed, the possible causes and solutions are as follows:

Figure 3-2 404 page



Cause 1: A non-standard port is configured when you add the domain name to WAF, but the visitors use the domain name and standard port or use only the domain name to access the website. For example, a non-standard port is configured as shown in **Figure 3-3**. A visitor uses https://www.example.com or https://www.example.com:80 to access the website. As a result, 404 error page is displayed.

Figure 3-3 Configuration of a non-standard port



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

Cause 2: No non-standard port is configured when the domain name is added to WAF. The visitors use the domain name and a non-standard port or the non-standard port configured for origin server port to access the website. For example, access **http://www.example.com:8080** when the protection service shown in **Figure 3-4** is configured.

Figure 3-4 Non-standard port not configured

Protected Port					
Standard port	View Port	ts You Can Use			
Standard ports 80 and 443 are the default ports reserved for HTTP and HTTPS protocols, respectively.					
Server Configuration	n				
Client Protocol	Server Protocol Server Address	Server Port	Weight	Operation	
HTTPS V	HTTP V IPv4 V Enter a public IP adc	80	1	Delete	
HTTPS V	HTTP V IPv4 V Enter a public IP add	80	1	Delete	

NOTE

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

Solution: Use only the domain name to access the website. For example, **https://www.example.com**.

Cause 3: The domain name is incorrectly resolved.

Solution:

- If the domain name has been added to WAF, resolve the domain name to WAF by referring to Routing Website Traffic to WAF.
- If the domain name is no longer protected by WAF, resolve it to the origin server IP address on the DNS hosting platform.

Cause 4: If a WAF cluster pointed multiple domain names through HTTPS to an origin server over the same port, origin servers cannot tell which domain name a request originated from. This is because WAF uses persistent connections to forward requests to origin servers and Nginx identifies domain names based on Host and SNI. So, there might be a probability that requests destined for domain name A was mistakenly forwarded to domain name B, which causes 404 not found errors.

Solution: Modify the server configuration in WAF to route different domain names over different origin server ports.

• If the response page is not similar the one shown in Figure 3-2, the possible causes and solutions are as follows:

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

Solution: Check the website.

502 Bad Gateway Troubleshooting Process and Solutions

Your website can be accessed normally after it is connected to WAF. However, after a period of time, the error code 502 is reported frequently. Refer to **Figure 3-5** to fix the issue.



Figure 3-5 Troubleshooting process for 502 Bad Gateway error

Possible Cause	Solution
Cause 1 : Your website is using another security protection software. Such software considers WAF back-to-source IP addresses as malicious and blocks the requests forwarded	Configure an access control policy on the origin server to whitelist the WAF back-to- source IP addresses.
by WAF.	 Cloud mode: For details, see How Do I Whitelist Back- to-Source IP Addresses of Cloud WAF?
	 Dedicated mode: See Whitelisting Back-to-Source IP Addresses of Dedicated WAF Instances.
Cause 2: Multiple backend servers are configured for the website. However, one backend server is inaccessible.	Repeat Step 1 to Step 8 to ensure that all origin servers can be accessed.
Cause 3: Your website server may have performance issues.	Contact your website administrator to rectify the fault.
Cause 4: The origin server uses CFW, which blocks WAF back-to-source IP addresses.	 Troubleshooting methods: If the origin server uses CFW, view the block logs on the CFW console to check whether related events are generated. View the access control policy in CFW and check whether the back-to-source IP address of WAF is blocked. On the CFW console, allow WAF back-to-source IP addresses. For details, see Configuring an Access Control Policy.

Table 3-1 Troubleshooting 502 Bad Gateway error

If one of your backend website servers is unreachable, perform the following steps to ensure that the website server configuration is correct.

NOTICE

It takes about two minutes for server information modification to take effect.

- Step 1 Log in to the management console.
- **Step 2** Click ^{SC} in the upper left corner of the management console and select a region or project.
- **Step 3** Click in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- **Step 4** In the navigation pane on the left, choose **Website Settings**.
- **Step 5** In the **Protected Website** column, click the target domain name to go to the **Basic Information** page.
- **Step 6** In the **Origin Servers** area, click **Edit**. On the displayed **Edit Server Information** page, check whether the client protocol, server protocol, origin server address, and port used by the origin server are correct.

Figure 3-6 Server Configuration

Edit Server Information				
Client Protocol	Server Protocol	Server Address	Server Port	
HTTPS 👻	HTTP -	IPv4 👻	80	
Add You can add 49 more configurations.				
Your domain name supports the client protocol HTTPS using the certificate test02 Import New Certificate CK Cancel				

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

• Run the following command on the server: curl http://xx.xx.xx:yy -kvv

NOTE

- *xx.xx.xx* indicates the IP address of the origin server. *yy* indicates the port of the origin server. *xx.xx.xx* and *yy* must belong to the same origin server.
- The host where the **curl** command can be run must meet the following requirements:
 - The network communication is normal.
 - The curl command has been installed. curl must be manually installed on the host running a Windows operating system. curl is installed along with other operating systems.

Figure 3-7 Command output for checking origin server



- If the command output indicates that the connection is normal, the website can be accessed.
- If the command output returns **connection refused**, the origin server is unreachable and website cannot be accessed. Go to **Step 8**.
- Enter **http://***origin server address: origin server port* in the address box of the browser and press **Enter**.
 - If the website can be accessed, the website access is normal.
 - If the website cannot be accessed, the origin server is unreachable and the website cannot be accessed. Go to Step 8.
- Step 8 Check whether the origin server runs properly.

If not, restart it.

----End

504 Gateway Timeout Troubleshooting Process and Solutions

After you connect your website to WAF, the possibility of 504 gateway timeout errors rises as your website traffic increases. In some other cases, there might be a possibility of 504 gateway timeout error if the visitors access your website through origin server IP addresses. Refer to **Figure 3-8** to fix 504 gateway timeout errors.





Possible Cause	Troubleshooting	Solution
Cause 1: Backend server performance issues (such as too many connections or high CPU usage)	If the origin server performance is insufficient, check the origin server access logs and access traffic to analyze issues.	 Optimize the server configurations, including TCP network parameters and ulimit parameters. If your website is connected to WAF in cloud mode through ELB load balancers, you are advised to create more backend server groups or create new load balancers to support increasing service workloads.
		 Add more backend server groups. For details, see Adding Backend Servers to a Load Balancer (Shared). To create a load
		balancer, see Step 1 to Step 8 .
		 If you configure Client Protocol to HTTPS, to relieve burden on backend servers, configure HTTP for Server Protocol for WAF forwarding traffic to backend servers. If there are redirection errors, rectify the fault by referring to Why Is My Website Redirected Too Many Times?
		For details, see Editing Server Information.
		 Use CC attack protection rules to block malicious traffic.

 Table 3-2 Troubleshooting 504 Gateway Timeout errors

Possible Cause	Troubleshooting	Solution
 Cause 2 The WAF back-to-source IP addresses are not whitelisted or service port is not enabled in the security group. WAF back-to-source IP addresses are blocked by the firewall on the origin server. 	 Follow the solutions below for troubleshooting: Check whether your origin server has security groups, firewalls, and security software deployed. Capture packets on the client and WAF, respectively, at the same time to check whether the origin server firewall proactively discards packets of the persistent connection to WAF. 	 Configure an access control policy that allows only WAF back-to-source IP addresses on origin servers. Cloud mode: For details, see How Do I Whitelist Back-to- Source IP Addresses of Cloud WAF on My Origin Server? Dedicated mode: Whitelisting the Back- to-Source IP Addresses of Your Dedicated WAF Instances Disable other firewalls and security software on origin servers.

Possible Cause	Troubleshooting	Solution
Cause 3: Connection timeout and read timeout NOTE • A 504 error occurs if the origin server is too slow to respond, for example, a slow response to database queries, a long upload time for a large file, or a faulty origin server. • The timeout for WAF to forward traffic to an origin server is 60s or 180s. A 504 error occurs if WAF fails to forward traffic within the configured timeout.	 Troubleshooting methods: Bypass WAF and directly access the origin server and then check the response time. View the origin server response time in access logs stored in Log Tank Service (LTS). Bypass WAF, test the file upload function, and check the file size. 	 Database queries are slow. Tune services to shorten the query duration and improve user experience. Modify the request interaction mode so that the persistent connection can have some data transmitted within 60 seconds, such as ACK packets, heartbeat packets, keep-alive packets, and other packets that can keep the session alive. It takes a long time to upload large files. Tune services to shorten the file upload time. An FTP server is recommended for file upload. Upload the file through an IP address or a domain name that is not protected by WAF. The default timeout for a dedicated WAF instance to respond to origin servers is 120s. The origin server is faulty. Check whether the origin server works properly.

Possible Cause	Troubleshooting	Solution
Cause 4: The bandwidth of the origin server is insufficient. When the access traffic is heavy, the origin server cannot handle all the traffic with its current bandwidth.	 Troubleshooting methods: If you have a layer-7 load balancer deployed in the rear of WAF, you can query 504 logs on the load balancer. If you have a layer-4 load balancer deployed in the rear of WAF, you can query logs in the Traffic exceeded the bandwidth threshold field on the load balancer. If you have an EIP bound to the backend WAF instances, check the EIP traffic monitoring when 504 errors rise to the peak volume. 	Increase the bandwidth of the origin server.
Cause 5: WAF back- to-source IP addresses are blocked by CFW used by origin servers.	 Troubleshooting methods: If the origin server uses CFW, view the block logs on the CFW console to check whether related events are generated. View the access control policy in CFW and check whether the back-to-source IP address of WAF is blocked. 	On the CFW console, allow WAF back-to-source IP addresses. For details, see Configuring an Access Control Policy .

Create a load balancer. Use the EIP of the load balancer as the IP address of the origin server and connect the EIP to WAF.

NOTICE

It takes about two minutes for server information modification to take effect.

- Step 1 Create a shared load balancer.
- Step 2 Log in to the management console.
- **Step 3** Click in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- **Step 4** In the navigation pane on the left, choose **Website Settings**.
- **Step 5** In the **Domain Name** column, click the domain name. Its information is displayed.
- **Step 6** In the **Origin Servers** area, click Edit. On the **Edit Server Information** page displayed, click **Add** to add a backend server.

Figure 3-9 Server Configuration

lient Protocol	Server Protocol	Server Address	Server Port
HTTPS 👻	HTTP -	IPv4 •	80
Add. You can add 4t	9 more configurations	tt	
Add You can add 49	9 more configurations.		

- Step 7 Set the Server Address to the EIP bound to the load balancer.
- Step 8 Click OK.

----End

3.2 Why Am I Seeing Error Code 418?

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

• If you confirm that the request is a normal service request, you can handle the false alarm to prevent the recurrence of the protection event.

For details, see Handling False Alarms.

 If you confirm that the protection event is not a false alarm, your website is attacked and the malicious request is blocked by WAF.

3.3 Why Am I Seeing Error Code 523?

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

The following figure shows the traffic flow that may cause error code 523.



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

Error code 523 will return if a website has been connected to different types of WAF instances, such as instances of cloud CNAME, dedicated, and cloud load balancer access modes, more than four times.

Solution

Route website traffic to bypass redundant WAF instances.

- **Step 1** Log in to the WAF management console.
- **Step 2** In the navigation pane on the left, choose **Website Settings**.
- **Step 3** Locate the website for which error code 523 is returned, retain one configuration, and delete the website from redundant WAF instances. For details, see **Deleting a Website from WAF**.

To prevent service interruptions due to such deletions, perform the following operations before removing a website from WAF:

Cloud mode: Go to your DNS provider and resolve your domain name to the IP address of the origin server. Otherwise, the traffic to your domain name cannot be routed to the origin server.

Dedicated mode: Remove redundant WAF instances from the backend server group of the load balancer so that no requests are forwarding to those WAF instances. For details, see **Changing a Backend Server Group**.

----End

Cause 2: A Third-party Interface That Uses Huawei Cloud WAF Was Called

When a request is forwarded to the third-party API, header and cookie are forwarded without being changed. Only the host is modified. This makes WAF count the requests without clearing historical records.

Solution

Modify the header field in the reverse proxy request. The operations are as follows:

NOTICE

This method can be used only when Nginx is deployed after WAF on the user traffic link.

Step 1 Use **proxy_set_header** to redefine the request header sent to the proxy server. Run the following command to open the Nginx configuration file:

(The following command is used when Nginx is installed in the **/opt/nginx/** directory. Change the directory based on your situation.)

vi /opt/nginx/conf/nginx.conf

Step 2 Add **proxy_set_header X-CloudWAF-Traffic-Tag 0** to the Nginx configuration file. The following is an example:

location ^~/test/ {

 proxy_set_header Host \$proxy_host;
 proxy_set_header X-CloudWAF-Traffic-Tag 0;

 proxy_pass http://x.x.x.x;
}

----End

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

If the origin server address is mistakenly set to the back-to-source IP address of WAF or an IP address of the proxy in front of WAF, the website requests go to an endless loop and error code 523 is returned.

Solution

Check the origin server configurations and enter a correct origin server address. For details, see **Editing Server Information**.

Figure 3-10 Changing the origin server address

Edit Server Infor	mation					
Client Protocol 🧿	Server Protocol 🧿	Server Address 🧿		Server Port ⑦	Weight ᠀	Active/Standby ⑦
HTTP V	HTTP V	IPv4 ~ .6		80	1	Active se V
 Add Origin server addr you plan to configure mu 	esses you can add: 49 Itiple pieces of server infor	mation, specify at least one active se	ver.			
v6 Protection		Enable	able			

3.4 Why Was My Website Redirected So Many Times?

If you configure your web server to redirect HTTP requests to HTTPS, but configure only one piece of server information with client protocol set to HTTPS and server protocol set to HTTP in WAF, there will be an infinite loop.

You can configure two pieces of server information, one from HTTP (client protocol) to HTTP (server protocol), and the other from HTTPS (client protocol) to HTTPS (server protocol). For details, see **Editing Server Information**. **Figure 3-11** shows the finished server settings.

Figure 3-11 Example configuration

Edit Server In	nformation				
Client Protocol	Server Protocol (?)	Server Address (?)	Server Port	? Weight ?	Active/Standby 📀
⊖ (http ∨	HTTP V	IPv4 ~ .3	80	1	Active se V
Θ HTTPS 、	HTTP V	IPv4 ~ .6	80	1	Active se V
Add Origin server	r addresses you can add: 48				
If you plan to configu	re multiple pieces of server inforr	nation, specify at least one active server.			
IPv6 Protection		Enable Disat	ble		
Your domain name si	upports the client protocol HTTP	S using the certificate			
International	Existing certificates/12222	~			

3.5 Why Am I Seeing Error Code 414 Request-URI Too Large?

Symptoms

After a protected website is connected to WAF, the website is inaccessible and the error message "414 Request-URI Too Large" is displayed, as shown in Figure 3-12.

Figure 3-12 Error Code 414 Request-URI Too Large



Possible Causes

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

After JavaScript anti-crawler is enabled, WAF returns a piece of JavaScript code to the client when the client sends a request. If the client sends a normal request to the website, triggered by the received JavaScript code, the client will automatically send the request to WAF again. WAF then forwards the request to the origin server. This process is called JavaScript verification. **Figure 3-13** shows how JavaScript verification works.



Figure 3-13 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.

Handling Suggestions

Disable the JavaScript anti-crawler protection by performing the following steps:

- Step 1 Log in to the management console.
- **Step 2** Click ¹⁰ in the upper left corner of the management console and select a region or project.
- **Step 3** Click in the upper left corner and choose **Web Application Firewall** under **Security & Compliance**.
- **Step 4** Click the name of the target policy to go to the protection configuration page.
- **Step 5** Click the **Anti-Crawler** configuration area and toggle it on or off if needed.
 - 🔍 : enabled.
 - disabled.
- **Step 6** Click the **JavaScript** tab and disable the JavaScript anti-crawler protection. Its status changes to

Figure 3-14 Disabling JavaScript anti-crawler protection

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

3.6 What Do I Do If the CPU Usage of the Origin Server Reaches 100%?

Symptom

The website has been added to and protected with WAF, but the CPU usage of the origin server still surged to 100%.

Possible Causes

The website may be under CC attacks.

If you find that the website loading speed decreases and network bandwidth usage surges, the website may be under CC attacks. In this case, check the number of access logs or network connections. If the number of access logs or network connections increases significantly, the website is under CC attacks.

Solution

- **Step 1** Ensure that protection rules and the policy used for the website work in the block mode.
- Step 2 Configure a CC protection rule and set the protection path to / to protect all paths of the website. Set a high rate limit, observe the request traffic, and check whether the attack is mitigated. Then, adjust the rule based on the protection effect. Figure 3-15 shows an example.

Figure 3-15 Full-path protection

Add CC Attack F	Protection Rule	8				
ate Limit Mode 🏼 🔊						
Source D	estination					
equests from a specif ddress (or user) in the	ic source are limited way you configure.	I. For example, if traffic	from an IP address (or user) excee	ds the rate limit you configure	in this rule, WAF limits tra	affic rate of the IF
ate Limit Type						
Per IP address	Per user	Other				
ep this function enab	oled if you added a v	vildcard domain name t	to WAF so that requests to all doma	in names that match the wildo	card domain are counted t	for triggering this
eep this function enable. For example, if yo	oled if you added a v u added *.a.com to v Subfield	vildcard domain name f WAF, requests to all ma	to WAF so that requests to all doma alched domain names such as b.a.(Logic	in names that match the wild com and c.a.com are counted.	card domain are counted f	for triggering this Operation
eep this function enable. For example, if yo igger Field Path ~	Jied if you added a v u added *.a.com to v Subfield	wildcard domain name i WAF, requests to all ma	to WAF so that requests to all doma atched domain names such as b.a.d Logic	in names that match the wild com and c.a.com are counted. Content	Case-Sen	for triggering this Operation Delete
eep this function enat lee. For example, if yo igger Field Path	oled if you added a v u added *.a.com to v Subfield	wildcard domain name 1 WAF, requests to all ma	to WAF so that requests to all doma atched domain names such as b.a.d Logic	in names that match the wildo com and c.a.com are counted.	Case-Sen	for triggering this Operation Delete
eep this function enat lee. For example, if yo igger Field Path ~	u can add 29 more of	wildcard domain name ! WAF, requests to all ma	to WAF so that requests to all doma atched domain names such as b.a.d Logic Include	in names that match the wildo com and c.a.com are counted. Content / / / /	Case-Sen	for triggering this Operation Delete
eep this function enat lile. For example, if yo rigger Field Path ~ - Add Condition You ate Limit ③	u added * a.com to t Subfield	wildcard domain name i WAF, requests to all ma	to WAF so that requests to all doma atched domain names such as b.a.d Logic Include	in names that match the wild com and c.a.com are counted. Content / / / / / / / / / / / / / / / / / / /	Case-Sen	for triggering this Operation Delete
iceop this function enatule. For example, if your rigger Field Path + Add Condition Your ate Limit ③ - 10	u added *.a.com to * Subfield u can add 29 more of requests	WIdcard domain name i WAF, requests to all mi conditions.(The rule is o 60 + second	to WAF so that requests to all doma atched domain names such as b.a.d Logic Include only applied when all conditions are	in names that match the wildo com and c.a.com are counted.	Case-Sen	for triggering this Operation Delete

Step 3 View protection logs. Add IP addresses that have launched a large number of attacks to the blacklist and block them immediately. For details, see **Configuring an IP Blacklist or Whitelist Rule**

----End

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

- The default timeout for connections from a browser to WAF is 120 seconds. The value varies depending on your browser settings and cannot be changed on the WAF console.
- The default timeout for connections between WAF and your origin server is 30 seconds. You can customize a timeout on the WAF console as long as you are using a dedicated WAF instance or professional or enterprise cloud WAF.

On the **Basic Information** page, enable **Timeout Settings** and click \checkmark . Then, specify **WAF-to-Server connection timeout (s)**, **Read timeout (s)**, and **Write timeout (s)** and click \checkmark to save settings.

4 Checking Whether Normal Requests Are Blocked Mistakenly

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

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

NOTICE

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

In the row containing the false alarm event, click **Details** in the **Operation** column and view the event details. If you are sure that the event is a false positive, handle it as a false alarm by referring to **Table 4-1**. 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.

Type of Hit Rule	Hit Rule	Handling Method	
WAF built-in protection rules	 Basic web protection rules Basic web protection defends against common web attacks, such as SQL injection, XSS attacks, remote buffer overflow attacks, file inclusion, Bash vulnerability exploits, remote command execution, directory traversal, sensitive file access, and command and code injections. Basic web protection also detects web shells and evasion attacks. Feature-based anti-crawler protection Feature-based anti-crawler identifies and blocks crawler behavior from search engines, scanners, script tools, and other crawlers. 	In the row containing the attack event, click Handle as False Alarm in the Operation column. For details, see Handling False Alarms .	
Custom protection rules	 CC attack protection rules Precise protection rules Blacklist and whitelist rules Geolocation access control rules Web tamper protection rules JavaScript anti-crawler protection Information leakage prevention rules Data masking rules 	Go to the page displaying the hit rule and delete it.	
Other	 Invalid access requests NOTE If any of the following cases, WAF blocks the access request as an invalid request: When form-data is used for POST or PUT requests, the number of parameters in a form exceeds 8,192. The URL contains more than 2,048 parameters. The number of headers exceeds 512. 	The Handle as False Alarm button is grayed out for events that are generated against a precise protection rule. To allow the blocked requests, see Configuring a Precise Protection Rule.	

Table 4-1 Handling	false	alarms
--------------------	-------	--------

4.2 Why Does WAF Block Normal Requests as Invalid Requests?

Symptom

After a website is connected to WAF, a normal access request is blocked by WAF. On the **Events** page, the corresponding **Event Type** reads **Invalid request**, and the **Handle False Alarm** button is grayed out, as shown in **Figure 4-1**.

Figure 4-1 Normal requests blocked by WAF as invalid requests

Time	Source IP Address	Geolocation	Domain Name	URL	Malicious Load	Event Type	Protective Action	Operation
May 13, 2021 17:26:10 G	10.25.63.141	Reserved IP	1001-001-001	/ <script>alert(xxs)</script>	/ <script>alert(xxs)</script>	Cross Site Scripting	Block	Details Handle False Alarm
May 13, 2021 17:25:59 G	10.25.63.141	Reserved IP	1001-001-001	/ <script>alert()</script>	/ <script>alert()</script>	Cross Site Scripting	Block	Details Handle False Alarm
May 11, 2021 18:06:05 G	10.142.204.230	Reserved IP	www.lub	/123		Invalid request	Block	Details Handle False Alarm

Possible Cause

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

- When **form-data** is used for POST or PUT requests, the number of parameters in a form exceeds 8,192.
- The URL contains more than 2,048 parameters.
- The number of headers exceeds 512.

Solution

If you confirm that a blocked request is a normal request, allow it by referring to **Configuring a Precise Protection Rule**.

4.3 Why Is the Handle False Alarm Button Grayed Out?

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

NOTICE

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

- For events generated based on custom rules (such as a CC attack protection rule, precise protection rule, blacklist rule, whitelist rule, or geolocation access control rule), they cannot be handled as false alarms. To ignore such an event, delete or disable the custom rule hit by the event.
- If either of the following numbers in an access request exceeds 512, WAF will block the request as an invalid request and gray out the **Handle False Alarm** button.
 - When **form-data** is used for POST or PUT requests, the number of parameters in a form exceeds 8,192.

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

Figure 4-2 Normal requests blocked by WAF as invalid requests

Time	Source IP Address	Geolocation	Domain Name	URL	Malicious Load	Event Type	Protective Action	Operation
May 13, 2021 17:26:10 G	10.25.63.141	Reserved IP	1001-001-001	/«script>alert(xxs)«/script>	/ <scriptsalert(xxs)< scripts<="" td=""><td>Cross Site Scripting</td><td>Block</td><td>Details Handle False Alarm</td></scriptsalert(xxs)<>	Cross Site Scripting	Block	Details Handle False Alarm
May 13, 2021 17:25:59 G	10.25.63.141	Reserved IP	1000 allo	/ <script>alert()</script>	/ <script>alert()</script>	Cross Site Scripting	Block	Details Handle False Alarm
May 11, 2021 18:06:05 G	10.142.204.230	Reserved IP	www.tub	/123		Invalid request	Block	Details Handle False Alarm

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

5 Checking for Permission Exceptions

5.1 Why Cannot I Access the Dedicated Engine Page?

Symptom

Error message "Failed to request IAM. Please check the current user's IAM permissions." is displayed when a user attempted to access the **Dedicate Engine** page under **Instance Management**.

Possible Cause

The IAM ReadOnly permission is not granted to the login account.

Solution

Assign the IAM ReadOnly permission to your account. For details, see Assigning Permissions to an IAM User.

To assign the minimum authorization scope to a user group, select **All resources** in the **Select Scope** step, or the authorization will fail to work.

5.2 Why Cannot I Select an SCM Certificate When Adding a Domain Name to WAF?

Symptom

SSL certificates cannot be selected when adding a domain name to WAF. A message is displayed, indicating that the account does not have the permission to access the **scm cert download** API.

Causes

The account you use does not have the **SCM Administrator** or **SCM FullAccess** permissions.

Solution

Go to the IAM console and assign the **SCM Administrator** and **SCM FullAccess** permissions to the account. Then, you can select the SCM certificate under the same account when adding a domain name to WAF.