Web Application Firewall

Best Practices

Issue	36
Date	2021-07-29



HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2021. 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 Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks 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 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 Mitigating Web Security Vulnerabilities 1
1.1 Apache Dubbo Deserialization Vulnerability 1
1.2 DoS Vulnerability in the Open-Source Component Fastjson 2
1.3 Remote Code Execution Vulnerability of Fastjson 2
1.4 Oracle WebLogic wls9-async Deserialization Remote Command Execution Vulnerability (CNVD-C-2019-48814) 3
2 Configuring the Minimum TLS Version and Cipher Suite to Better Secure Connections 6
3 Configuring CC Attack Protection 15
3.1 Overview 15
3.2 IP Address-based Rate Limiting 15
3.3 Cookie-based CC Attack Protection 18
4 Configuring Anti-Crawler Rules to Prevent Crawler Attacks 21
5 Configuring an Access Control Policy on an ECS or ELB to Protect Origin Servers 29
6 Configuring Basic Web Protection 35
7 Handling False Alarms to Get Improved Basic Web Protection 39
8 Connecting a Domain to WAF 45
8.1 Preparations 45
8.2 Connecting a Domain to WAF for Websites with no Proxy Used 47
9 Combining CDN and WAF to Get Improved Protection and Load Speed 52
10 Combining AAD and WAF to Get All-Round Protection 59
11 Obtaining the Client IP Address 67
A Change History 72

 Copyright © Huawei Technologies Co., Ltd.

1 Mitigating Web Security Vulnerabilities

1.1 Apache Dubbo Deserialization Vulnerability

On February 10, 2020, Apache Dubbo officially released the CVE-2019-17564 vulnerability notice, and the vulnerability level is important. When the user selects the HTTP protocol for communication, Apache Dubbo will perform a deserialization operation when accepting a POST request from a remote call from the attackers. Since there is no security check, it can cause deserialization to execute arbitrary code. Now, HUAWEI CLOUD WAF provides protection against this vulnerability.

Affected Versions

This vulnerability affects Apache Dubbo 2.7.0 to 2.7.4, 2.6.0 to 2.6.7, and all 2.5.*x* versions.

Secure Version

Apache Dubbo 2.7.5 (**https://github.com/apache/dubbo/tree/dubbo-2.7.5**)

Solutions

Upgrade Apache Dubbo to version 2.7.5.

If a quick upgrade is not possible or you want to defend against more vulnerabilities, use HUAWEI CLOUD WAF. The procedure is as follows:

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**.

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

----End

 Copyright © Huawei Technologies Co., Ltd.

1.2 DoS Vulnerability in the Open-Source Component Fastjson

On September 3, 2019, the HUAWEI CLOUD security team detected a DoS vulnerability in multiple versions of the widely used open-source component Fastjson. An attacker can exploit this vulnerability to construct malicious requests and send them to the server that uses Fastjson. As a result, the memory and CPU of the server are used up, and the server breaks down, causing service breakdown. HUAWEI CLOUD WAF provides protection against this vulnerability.

Affected Versions

Versions earlier than Fastjson 1.2.60

Secure Version

Fastjson 1.2.60

Official Solution

Upgrade the open-source component Fastjson to 1.2.60.

Mitigation

WAF can detect and defend against this vulnerability. The procedure is as follows:

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**.

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

----End

1.3 Remote Code Execution Vulnerability of Fastjson

On July 12, 2019, the HUAWEI CLOUD Emergency Response Center detected that the open-source component Fastjson had a remote code execution vulnerability. This vulnerability is an extension of the anti-serialization vulnerability of Fastjson 1.2.24 detected in 2017 and can be directly used to obtain server permissions, causing serious damage.

Affected Versions

Versions earlier than Fastjson 1.2.51

Secure Version

Fastjson 1.2.51 or later

 Copyright © Huawei Technologies Co., Ltd.

Official Solution

Upgrade Fastjson to 1.2.51 or the latest 1.2.58 version.

Mitigation

The built-in protection rules of HUAWEI CLOUD WAF can defend against this vulnerability. The procedure is as follows:

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**.

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

----End

1.4 Oracle WebLogic wls9-async Deserialization Remote Command Execution Vulnerability (CNVD-C-2019-48814)

On April 17, 2019, the HUAWEI CLOUD Emergency Response Center detected that China National Vulnerability Database (CNVD) released a security bulletin on the Oracle WebLogic wls9-async component. The component has a defect in deserializing input information. Attackers can send well-constructed malicious HTTP requests to obtain the permission of the target server and execute arbitrary code remotely without authorization. CNVD rates the vulnerability as "high-risk."

Vulnerability ID

CNVD-C-2019-48814

Vulnerability Name

Oracle WebLogic wls9-async Deserialization Remote Command Execution Vulnerability

Vulnerability Description

The WebLogic wls9-async component has a defect. The website built on the WebLogic Server has security risks. Attackers can construct HTTP requests to obtain the permission of the target server and execute arbitrary code remotely without authorization.

Affected Products

- Oracle WebLogic Server 10.X
- Oracle WebLogic Server 12.1.3

 Copyright © Huawei Technologies Co., Ltd.

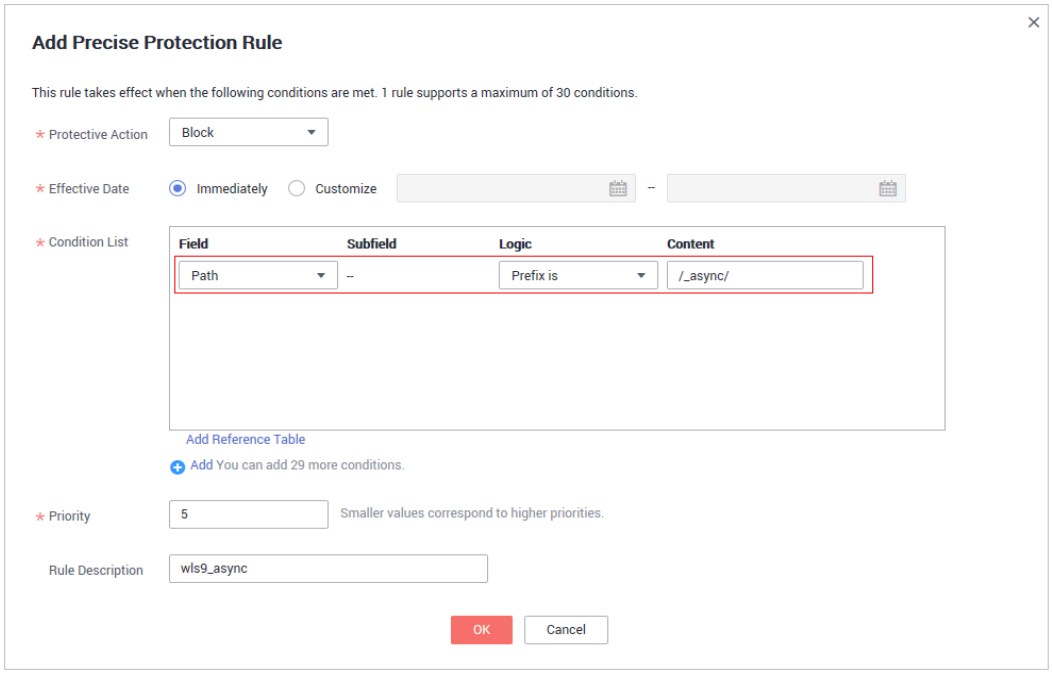
Official Solution

The patch for fixing this vulnerability has not been released.

Mitigation

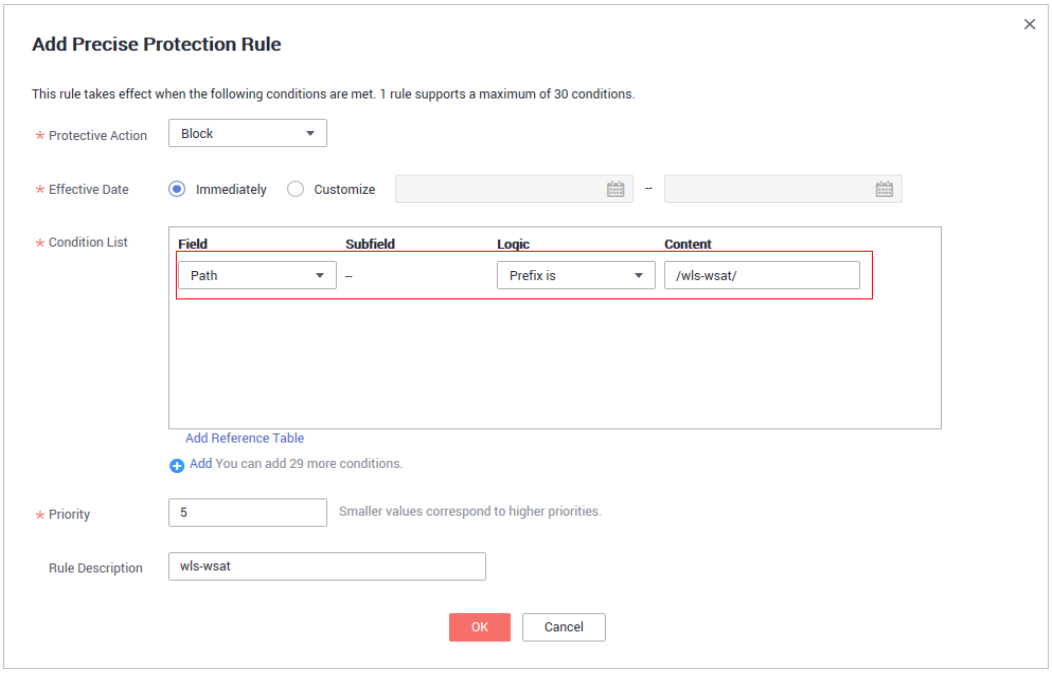
Configure precise protection rules to restrict access from the URLs whose prefixes are **/_async/** or **/wls-wsat/** by referring to **Figure 1-1** and **Figure 1-2** and block remote code execution requests initiated by exploiting this vulnerability. For details, see **Configuring a Precise Protection Rule**.

Figure 1-1 async configuration



 Copyright © Huawei Technologies Co., Ltd.

Figure 1-2 wls-wsat configuration



 Copyright © Huawei Technologies Co., Ltd.

2 Configuring the Minimum TLS Version and Cipher Suite to Better Secure Connections

HTTPS is a network protocol constructed based on Transport Layer Security (TLS) and HTTP for encrypted transmission and identity authentication. When you **add a domain name to WAF**, set **Client Protocol** to **HTTPS**. Then, you can configure the minimum TLS version and cipher suite to harden website security. The details are as follows:

- Minimum TLS version

  The minimum TLS version that can be used by a client to access the website. After you configure the minimum TLS version, only the requests over the connections secured with the minimum TLS version or the later version can access your website. This helps you meet security requirements for industrial websites.

  NOTE

  - Up to now, four TLS versions (TLS v1.0, TLS v1.1, TLS v1.2 and TLS v1.3) have been released, among which TLS v1.0 and TLS v1.1 have been released for a long time. Some encryption algorithms (such as SHA1 and RC4) used by TLS v1.0 and TLS v1.1 are vulnerable to attacks. TLS v1.0 and TLS v1.1 cannot meet the geometric growth of data transmission encryption requirements, which might bring potential security risks. To ensure the security of the communication and meet the Payment Card Industry Data Security Standard (PCI DSS), PCI Security Standards Council (PCI SSC) stated that it no longer accepted TLS v1.0 as of June 30, 2018. Vendors of mainstream browsers, such as Mozilla Firefox, Apple Safari, Google Chrome, and Microsoft Edge, also declared that they would stop supporting TLS v1.0 and TLS v1.1 by 2020.
  - You can query the TLS version supported by the website through other tools.

- Cipher suites

  A cipher suite is a set of algorithms that help secure a network connection through TLS. A more secure cipher suite can better secure the confidentiality and data integrity of websites.

 Copyright © Huawei Technologies Co., Ltd.

Recommended Minimum TLS Versions for Different Scenarios

The default minimum TLS version configured in WAF is **TLS v1.0**. To ensure website security, configure an appropriate TLS version for your service requirements. **Table 2-1** lists the recommended minimum TLS versions for different scenarios.

Table 2-1 Recommended minimum TLS versions

Scenario	Minimum TLS Version (Recommended)	Protection Effect
Websites that handle critical business data, such as sites used in banking, finance, securities, and e-commerce.	TLS v1.2	WAF automatically blocks website access requests that use TLS v1.0 or TLS v1.1.
Websites with basic security requirements, for example, small- and medium-sized enterprise websites.	TLS v1.1	WAF automatically blocks website access requests that use TLS v1.0.
Client applications with no special security requirements	TLS v1.0	Requests using any TLS protocols can access the website.

Recommended Cipher Suites

The default cipher suite in WAF is **Cipher suite 1**. Cipher suite 1 offers a good mix of browser compatibility and security. For details about each cipher suite, see **Table 2-2**.

Table 2-2 Description of cipher suites

Cipher Suite Name	Encryption Algorithm	Description
Default cipher suite	ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!AESGCM	• Compatibility: Good. A wide range of browsers are supported. • Security: Average

Copyright © Huawei Technologies Co., Ltd.

Cipher Suite Name	Encryption Algorithm	Description
Cipher suite 1	ECDHE-ECDSA-AES256-GCM-SHA384:HIGH:!MEDIUM:!LOW:!aNULL:!eNULL:!DES:!MD5:!PSK:!RC4:!kRSA:!SRP:!3DES:!DSS:!EXP:!CAMELLIA:@STRENGTH	The default configurations are recommended. • Compatibility: Good. A wide range of browsers are supported. • Security: Good
Cipher suite 2	EECDH+AESGCM:EDH+AESGCM	• Compatibility: Average. Strict compliance with forward secrecy requirements of PCI DSS and excellent protection, but browsers of earlier versions may be unable to access the website. • Security: Excellent
Cipher suite 3	ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH	• Compatibility: Average. Earlier versions of browsers may be unable to access the website. • Security: Excellent. Multiple algorithms, such as ECDHE, DHE-GCM, and RSA-AES-GCM, are supported.
Cipher suite 4	ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!eNULL:!NULL:!EDH	• Compatibility: Good. A wide range of browsers are supported. • Security: Average. The GCM algorithm is supported.

The cipher suites provided by WAF are compatible with the latest browsers and clients, but are incompatible with some browsers of earlier versions. Compatible browsers or clients of a certain cipher suite may vary depending on the TLS version configured. Using TLS v1.0 as an example, **Table 2-3** describes the browser and client compatibility.

NOTICE

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

Copyright © Huawei Technologies Co., Ltd.

Table 2-3 Incompatible browsers and clients for cipher suites under TLS v1.0

Browser/Client	Default Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4
Google Chrome 63 /macOS High Sierra 10.13.2	Not compatible	Compatible	Compatible	Compatible	Not compatible
Google Chrome 49/ Windows XP SP3	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
Internet Explorer 6 /Windows XP	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
Internet Explorer 8 /Windows XP	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
Safari 6/iOS 6.0.1	Compatible	Compatible	Not compatible	Compatible	Compatible
Safari 7/iOS 7.1	Compatible	Compatible	Not compatible	Compatible	Compatible
Safari 7/OS X 10.9	Compatible	Compatible	Not compatible	Compatible	Compatible
Safari 8/iOS 8.4	Compatible	Compatible	Not compatible	Compatible	Compatible
Safari 8/OS X 10.10	Compatible	Compatible	Not compatible	Compatible	Compatible
Internet Explorer 7/Windows Vista	Compatible	Compatible	Not compatible	Compatible	Compatible
Internet Explorer 8, 9, or 10 /Windows 7	Compatible	Compatible	Not compatible	Compatible	Compatible
Internet Explorer 10 /Windows Phone 8.0	Compatible	Compatible	Not compatible	Compatible	Compatible

 Copyright © Huawei Technologies Co., Ltd.

Browser/Client	Default Cipher Suite	Cipher Suite 1	Cipher Suite 2	Cipher Suite 3	Cipher Suite 4
Java 7u25	Compatible	Compatible	Not compatible	Compatible	Compatible
OpenSSL 0.9.8y	Not compatible	Not compatible	Not compatible	Not compatible	Not compatible
Safari 5.1.9/OS X 10.6.8	Compatible	Compatible	Not compatible	Compatible	Compatible
Safari 6.0.4/OS X 10.8.4	Compatible	Compatible	Not compatible	Compatible	Compatible

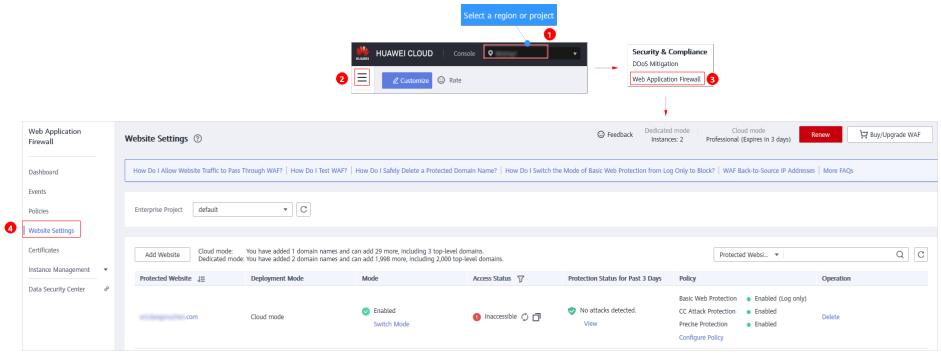
Configuring the Minimum TLS Version and Cipher Suite

The following describes how to configure TLS v1.2 and cipher suite 1 as the minimum TLS version and how to verify that the configuration takes effect.

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

Step 2 Go to the **Website Settings** page by following the steps shown in **Figure 2-1**.

Figure 2-1 Accessing to the Website Settings page

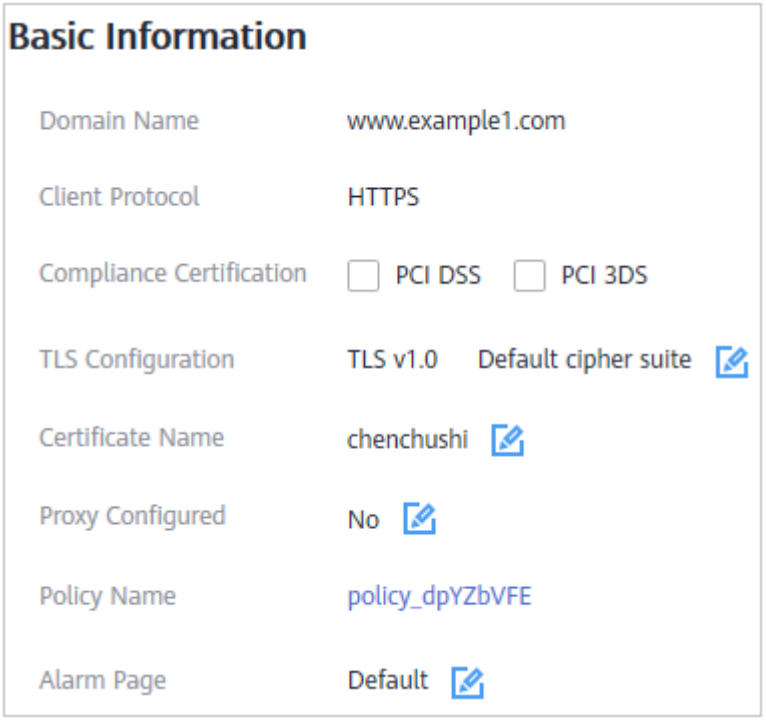


Step 3 In the **Protected Website** column, click the domain name of the website to go to the basic information page.

Step 4 Click  in the **TLS Configuration** row. **Figure 2-2** shows an example.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-2 TLS configuration modification



NOTE

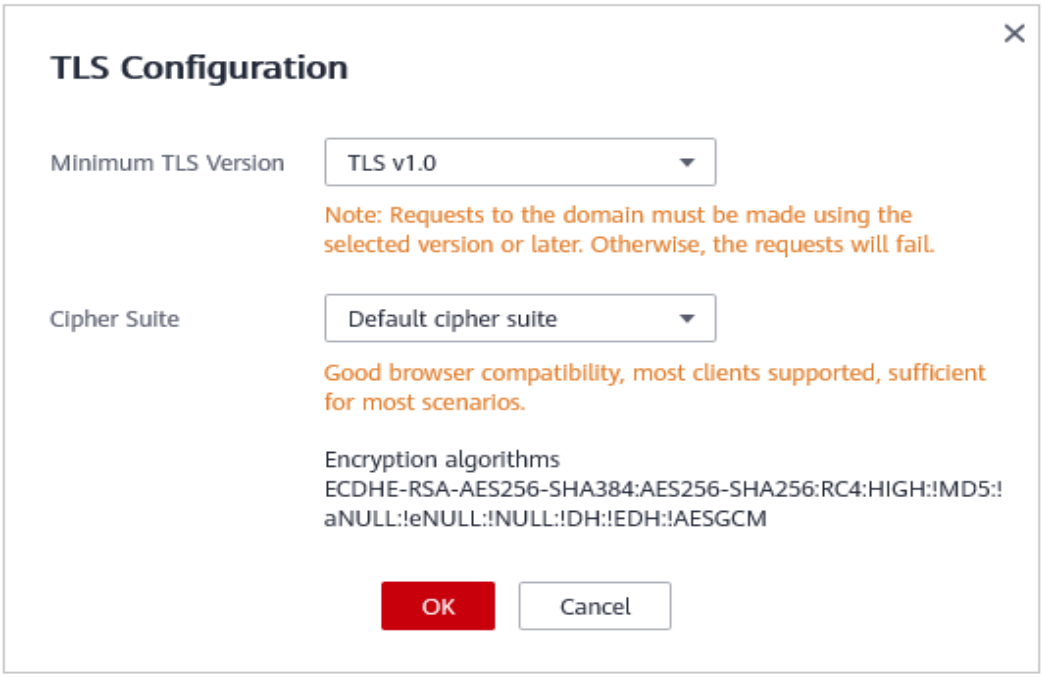
WAF allows you to enable PCI DSS and PCI 3-Domain Secure (3DS) compliance certification checks with just a few clicks. After they are enabled, WAF will configure the minimum TLS version in accordance with the PCI DSS and PCI 3DS compliance certification requirements.

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

Step 5 In the displayed **TLS Configuration** dialog box, select **TLS v1.2** as the minimum TLS version and **Cipher suite 1**. Figure 2-3 shows an example.

 Copyright © Huawei Technologies Co., Ltd.

Figure 2-3 TLS Configuration



Step 6 Click **OK**.

----End

Verification

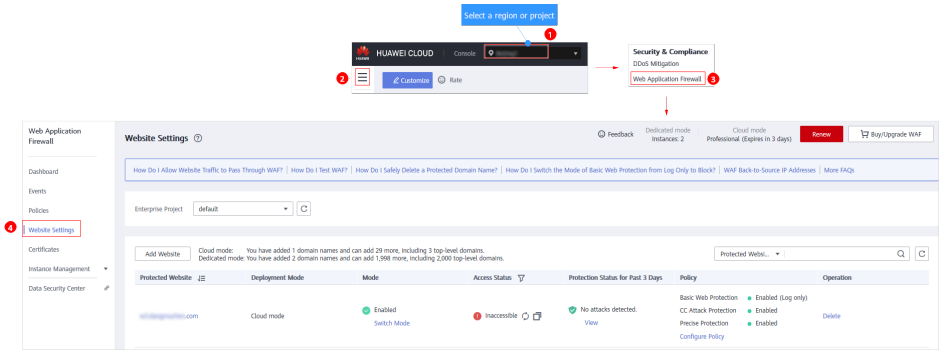
If the **Minimum TLS Version** is set to **TLS v1.2**, verify that the website can be accessed over connections secured by TLS v1.2 or later but cannot be accessed over connections secured by TLS v1.1 or earlier.

You can run commands on the local PC to check whether the TLS is configured successfully. Before the verification, ensure that **OpenSSL** has been installed on your local PC.

Step 1 Copy the CNAME record of the protected domain name and use the CNAME record to obtain WAF back-to-source IP addresses.

1. **Log in to the management console**.
2. Go to the **Website Settings** page by following the steps shown in **Figure 2-4**.

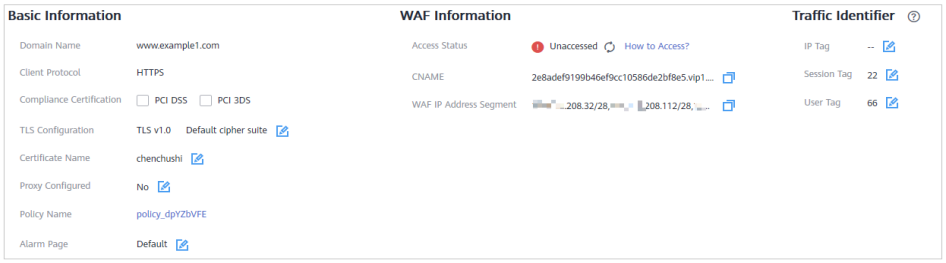
Figure 2-4 Accessing to the Website Settings page



 Copyright © Huawei Technologies Co., Ltd.

3. In the **Protected Website** column, click the domain name of the website to go to the basic information page.
4. In the **CNAME** row, click to copy the CNAME record. **Figure 2-5** shows an example.

Figure 2-5 Copying the CNAME record



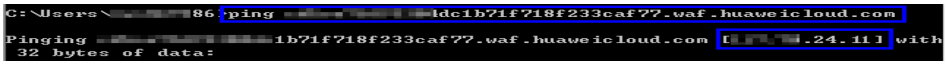
Step 2 Obtain the WAF back-to-source IP addresses.

1. In the command line interface (CLI) of the Windows OS, run the following command to obtain WAF back-to-source IP addresses:

   ping *CNAME record*

   The command output displays WAF back-to-source IP addresses. **Figure 2-6** shows an example.

Figure 2-6 ping cname

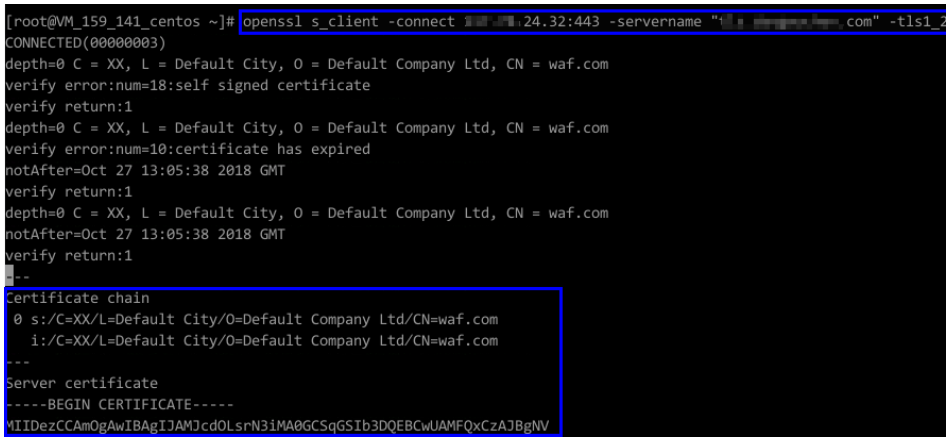


Step 3 Run the following command to verify that the protected website can be accessed using TLS v1.2.

openssl s_client -connect *WAF back-to-source IP address* **-servername** "*Domain name of the protected website*" **-tls1_2**

If the certificate information similar to the one shown in **Figure 2-7** is displayed, the website can be accessed using TLS v1.2.

Figure 2-7 Verifying TLS v1.2



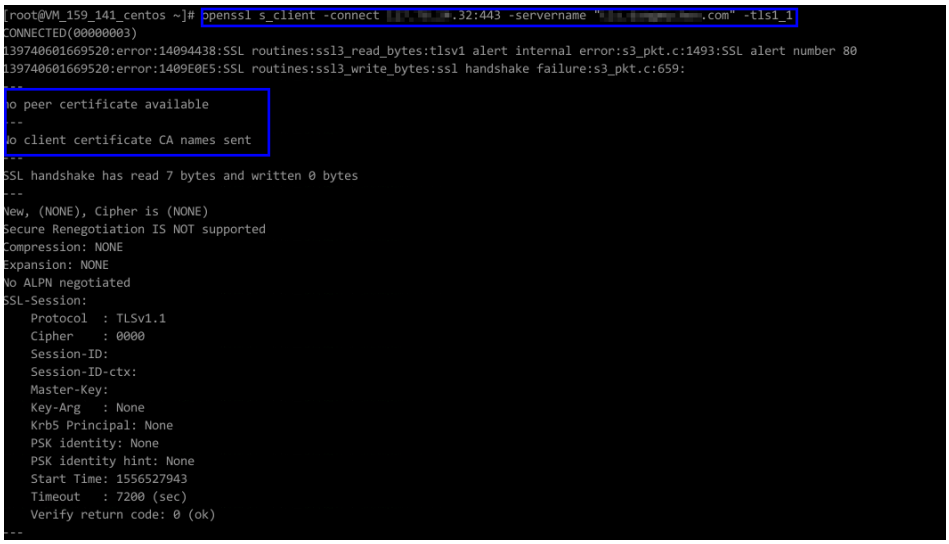
Step 4 Run the following command to verify that the protected website cannot be accessed using TLS v1.1.

 Copyright © Huawei Technologies Co., Ltd.

openssl s_client -connect *WAF back-to-source IP address* **-servername** "*Protected domain name*" **-tls1_1**

If no certificate information is displayed, as shown in **Figure 2-8**, WAF has blocked the access that used TLS v1.1.

Figure 2-8 Verifying TLS v1.1



----End

 Copyright © Huawei Technologies Co., Ltd.

3 Configuring CC Attack Protection

3.1 Overview

This section guides you through configuring IP address-based rate limiting and cookie-based protection rules against Challenge Collapsar (CC) attacks.

Introduction to Web Application Firewall

Web Application Firewall (WAF) is used to defend against web attacks, such as cross-site scripting (XSS), SQL injection, webshell, and CC attacks. CC attack is a type of denial of service (DoS) attack. In a CC attack, the attacker uses a proxy server to generate and send disguised requests to the target host.

How to Determine Whether a CC attack Occurs?

If you find that the website processing speed decreases and network bandwidth usage is high, your website may suffer from CC attacks. In this case, check whether the number of access logs or network connections increases significantly. If yes, your website suffers from CC attacks. Then you can configure the protection policies to block CC attacks, thereby ensuring website availability.

NOTE

- WAF protects application-layer traffic against DoS attacks, such as HTTP GET attacks.
- WAF does not provide protection against layer 4 or lower traffic, such as ACK Flood and UDP flood attacks. It is recommended that Anti-DDoS and Advanced Anti-DDoS (AAD) be used to defend against such attacks.

3.2 IP Address-based Rate Limiting

If no proxy is used between WAF and web visitors, limiting source IP addresses is an effective way to detect attacks. IP address-based rate limiting policies are recommended.

 Copyright © Huawei Technologies Co., Ltd.

Attack Examples

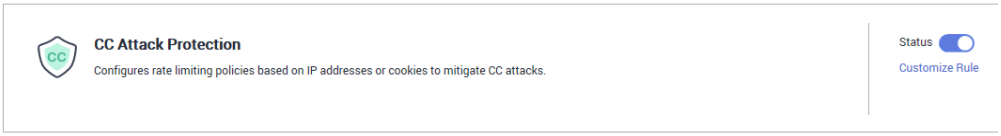
Attackers can use several hosts to continuously send HTTP POST requests to website **www.hwexample.com**. Those malicious requests will use up website resources, such as the website connections and bandwidth. As a result, the website fails to respond normal requests and its competitiveness decreases sharply.

Protective Measures

1. Based on the access statistics, check whether a large number of requests are sent from a specific IP address. If yes, it is likely that the website is hit by CC attacks.
2. Log in to the management console and route website traffic to WAF. For details, see **Connecting a Domain Name to WAF**.
3. Locate the row containing the domain name (website) you want to apply the policy to. In the **Policy** column, click **Configure Policy**. On the displayed page, in the **CC Attack Protection** area, verify that CC attack protection is enabled.

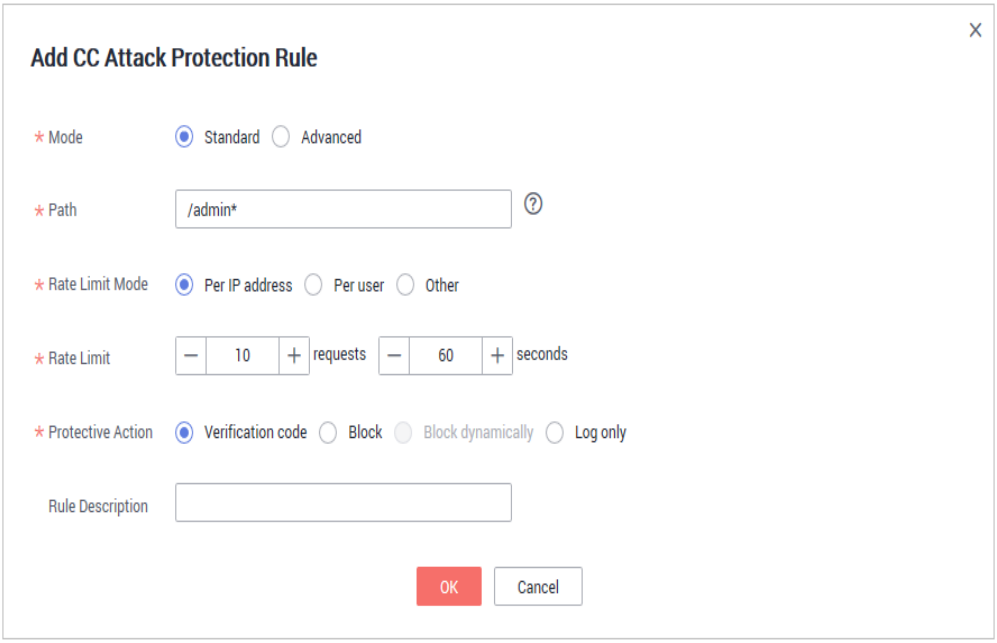
   Clicking  can change the status. **Figure 3-1** shows an example.

   Figure 3-1 CC Attack Protection configuration area

4. Then, add a CC attack protection rule. Specify a path, set **Rate Limit Mode** to **Per IP address**, **Rate Limit** based on service features, and **Protective Action** to **Verification code** to prevent blocking legitimate users. **Figure 3-2** shows the settings.

   Figure 3-2 Per IP address

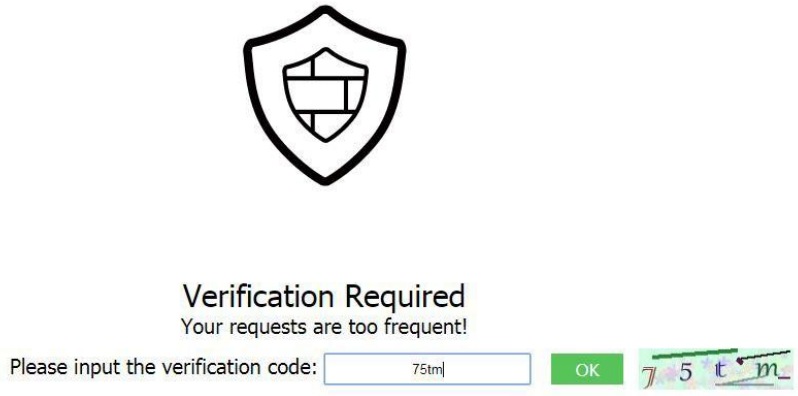
   

 Copyright © Huawei Technologies Co., Ltd.

- **Path**: Part of the URL without the domain name
  - Prefix match: A path ending with * indicates that the path is used as a prefix. For example, if the path to be protected is **/admin/test.php** or **/adminabc**, set **Path** to **/admin***.
  - Exact match: The path to be entered must match the path to be protected. For example, if the path to be protected is **/admin**, set **Path** to **/admin**.

  NOTE
  - The path supports prefix and exact matches only and does not support regular expressions.
  - The path cannot contain two or more consecutive slashes. For example, **///admin**. If you enter **///admin**, the WAF engine converts **///** to **/**.
- **Rate Limit Mode**: Select **Per IP address** to distinguish a single web visitor based on the IP address.
- **Rate Limit**: Number of requests allowed from a website visitor in the rate limiting period. The visitor's access request is denied if the limit is reached.
- **Protective Action**: To prevent legitimate requests from being blocked, select **Verification code**.
  - **Verification code**: A verification code is required if your website visitor's requests reaches **Rate Limit** you configured. WAF allows requests that trigger the rule as long as the website visitors complete the required verification.
  - **Block**: Requests are blocked if the number of requests exceeds the configured rate limit.
  - **Log only**: Requests are logged only but not blocked if the number of requests exceeds the configured rate limit.

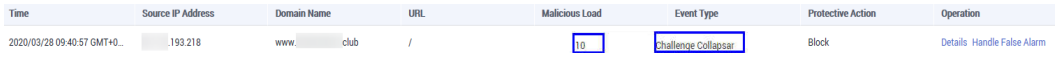
If the number of access requests exceeds the configured rate limit, the visitors are required to enter a verification code to continue the access.



Switch to the **Events** page to view details about attack events. **Figure 3-3** shows an example.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-3 Querying CC attack event logs



3.3 Cookie-based CC Attack Protection

In some cases, it may be difficult to obtain source IP addresses of visitors for a website. For example, websites use proxies that do not use the **X-Forwarded-For** HTTP header field. Configuring the cookie field to identify visitors is recommended.

Attack Examples

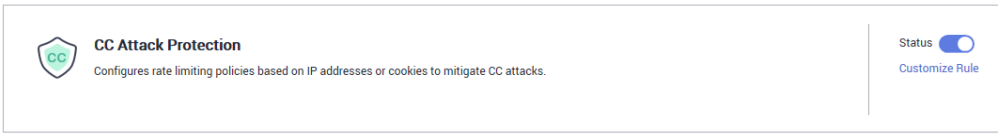
Attackers may control several hosts and disguise as normal visitors to continuously send HTTP POST requests to website **www.hwexample.com** through the same IP address or many different IP addresses. As a result, the website may respond slowly or even fails to respond to normal requests as the attackers exhausted website resources like connections and bandwidth.

Protective Measures

1. Based on the access statistics, check whether a large number of requests are sent from a specific IP address. If yes, it is likely that the website is hit by CC attacks.
2. Log in to the management console and route website traffic to WAF. For details, see **Connecting a Domain Name to WAF**.
3. Locate the row containing the domain name (website) you want to apply the policy to. In the **Policy** column, click **Configure Policy**. On the displayed page, in the **CC Attack Protection** area, verify that CC attack protection is enabled.

   Clicking  can change the status. **Figure 3-4** shows an example.

   Figure 3-4 CC Attack Protection configuration area

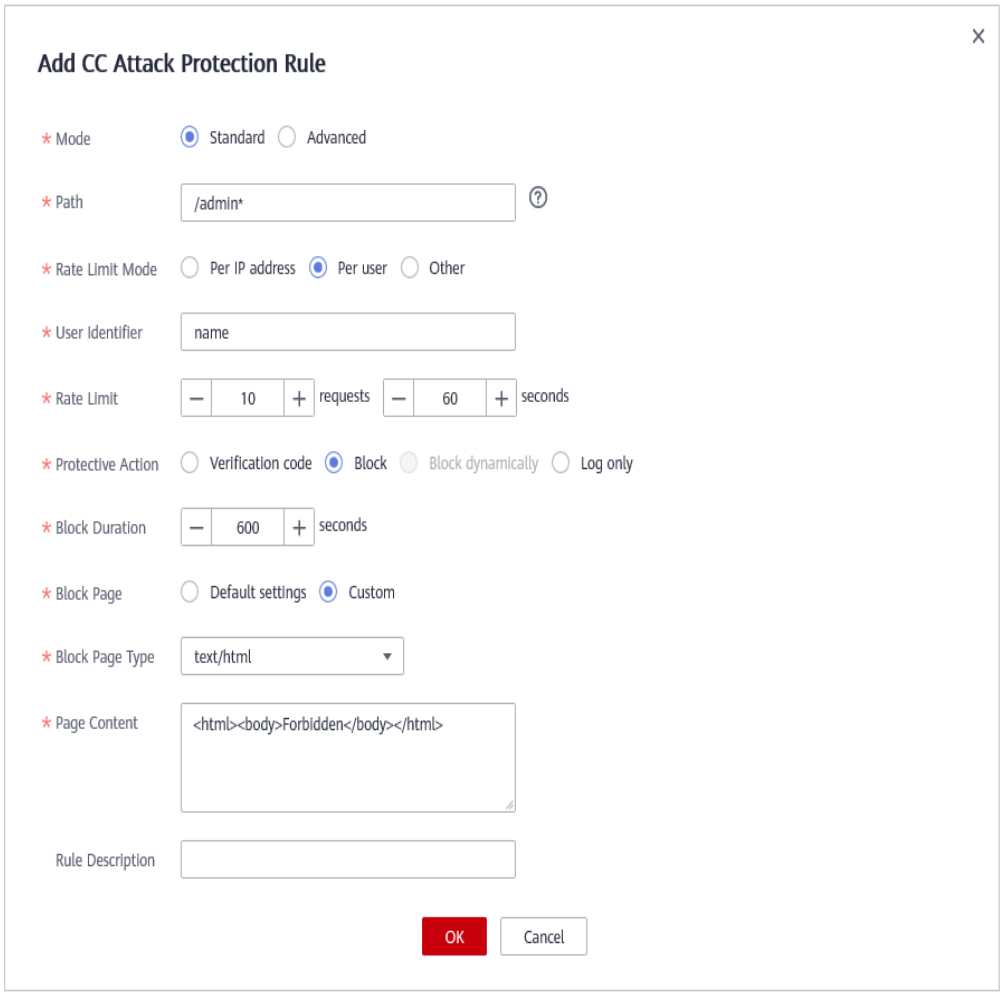
4. Add a CC attack protection rule. Set **Rate Limit Mode** to **Per user** and enter the user identifier, which is the variable in the cookie field. To identify visitors more effectively, use **sessionid** or **token**. **Figure 3-5** shows an example configuration.

   NOTE

   With a CC attack protection rule, you can configure **Protective Action** to **Block** and specify a block duration. Then, once an attack is blocked, the attacker will be blocked until the block duration expires. These settings are recommended if your applications have high security requirements.

 Copyright © Huawei Technologies Co., Ltd.

Figure 3-5 Adding a CC attack protection rule



- **Path**: Part of the URL without the domain name
  - Prefix match: The path ending with * indicates that the path is used as a prefix. For example, if the path to be protected is **/admin/test.php** or **/adminabc**, set **Path** to **/admin***.
  - Exact match: The path to be entered must match the path to be protected. For example, if the path to be protected is **/admin**, set **Path** to **/admin**.

  NOTE
  - The path supports prefix and exact matches only and does not support regular expressions.
  - The path cannot contain two or more consecutive slashes. For example, **///admin**. If you enter **///admin**, the WAF engine converts **///** to **/**.
- **Rate Limit Mode**: Select **Per user** to distinguish a single web visitor based on the cookie.
- **User Identifier**: To identify visitors more effectively, use **sessionid** or **token**.

 Copyright © Huawei Technologies Co., Ltd.

- **Rate Limit**: Number of requests allowed from a web visitor in the rate limiting period. The visitor's access request is denied if the limit is reached.
- **Protective Action**: Select **Block**. Then specify **Block Duration**. Once an attack is blocked, the attacker will be blocked until the block duration expires. These settings are recommended if your applications have high security requirements.
  - **Verification code**: A verification code is required if your website visitor's requests reaches **Rate Limit** you configured. WAF allows requests that trigger the rule as long as the website visitors complete the required verification.
  - **Block**: Requests are blocked if the number of requests exceeds the configured rate limit.
  - **Log only**: Requests are logged only but not blocked if the number of requests exceeds the configured rate limit.
- **Block Page**: Select **Default settings** or **Custom**.

 Copyright © Huawei Technologies Co., Ltd.

4 Configuring Anti-Crawler Rules to Prevent Crawler Attacks

Web crawlers facilitate network information collection and query, but they also introduce the following negative impacts:

- Web crawlers always consume too much server bandwidth and increase server load as they use specific policies to browser as much information of high value on a website as possible.
- Bad actors may use web crawlers to launch DoS attacks against websites. As a result, websites may fail to provide normal services due to resource exhaustion.
- Bad actors may use web crawlers to steal mission-critical data on your websites, which will damage your economic interests.

WAF provides three anti-crawler policies, robot detection by identifying User-Agent, website anti-crawler by checking browser validity, and CC attack protection by limiting the access frequency, to comprehensively mitigate crawler attacks against your websites.

Prerequisites

The domain name has been connected to WAF.

Enabling Robot Detection to Identify User-Agent

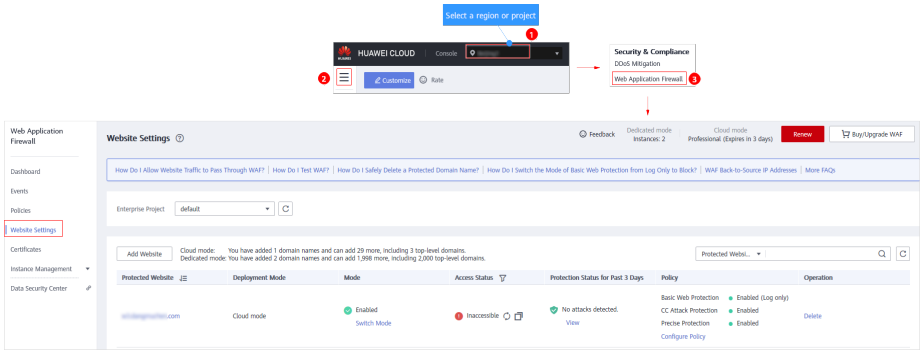
If you enable robot detection, WAF can detect and block threats such as malicious crawlers, scanners, and web shells.

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

Step 2 Go to the **Website Settings** page by following the steps shown in **Figure 4-1**.

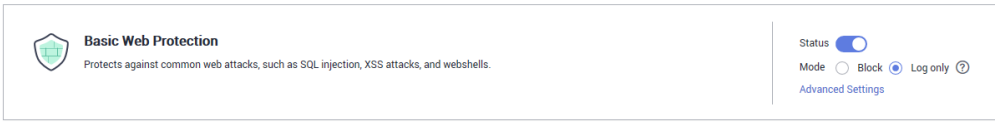
 Copyright © Huawei Technologies Co., Ltd.

Figure 4-1 Accessing to the Website Settings page

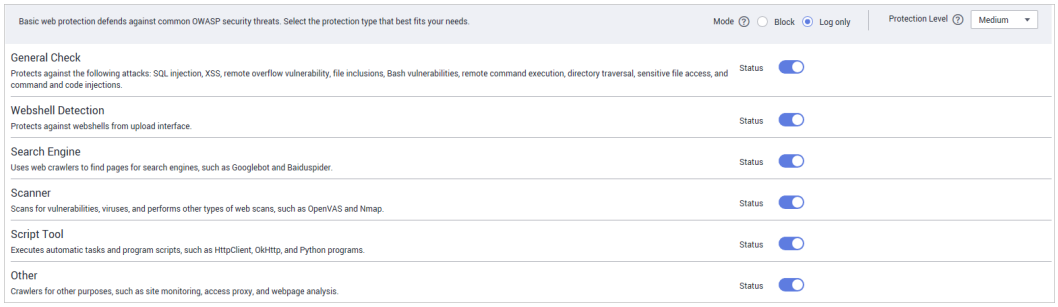


Step 3 Locate the row containing the website domain name you want to apply the policy to. In the **Policy** column, click **Configure Policy**. On the displayed page, in the **Basic Web Protection** area, verify that its **Status** is . **Figure 4-2** shows an example.

Figure 4-2 Basic Web Protection configuration area

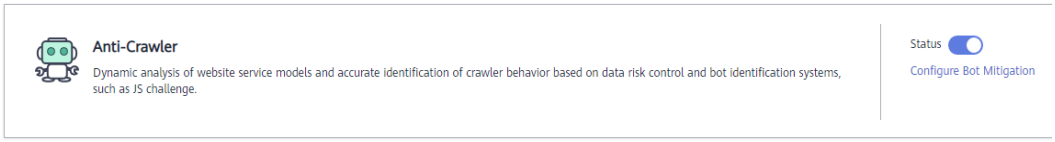


Step 4 Click **Advanced Settings**. On the **Protection Status** page, enable **General Check** and **Webshell Detection**.



Step 5 In the **Anti-Crawler** configuration area, enable anti-crawler using the toggle on the right, as shown in **Figure 4-3**. If you enable this function, click **Configure Bot Mitigation**.

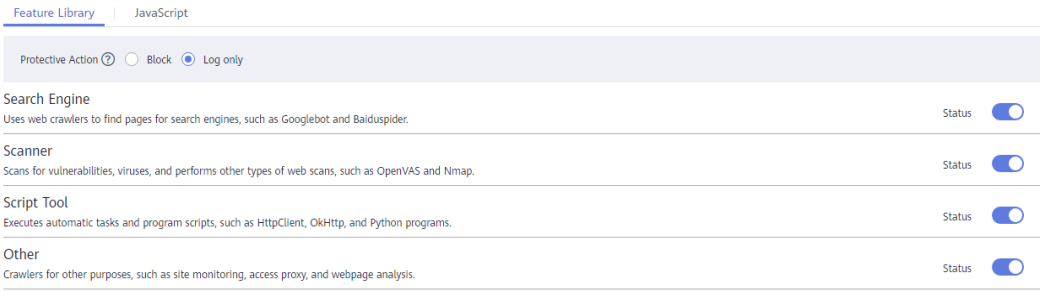
Figure 4-3 Anti-Crawler configuration area



Step 6 On the **Feature Library** page, enable all robot detection features, as shown in **Figure 4-4**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-4 Feature Library



----End

If WAF detects that a malicious crawler or scanner is crawling your website, WAF immediately blocks it and logs the event. You can view the crawler protection logs on the **Events** page.



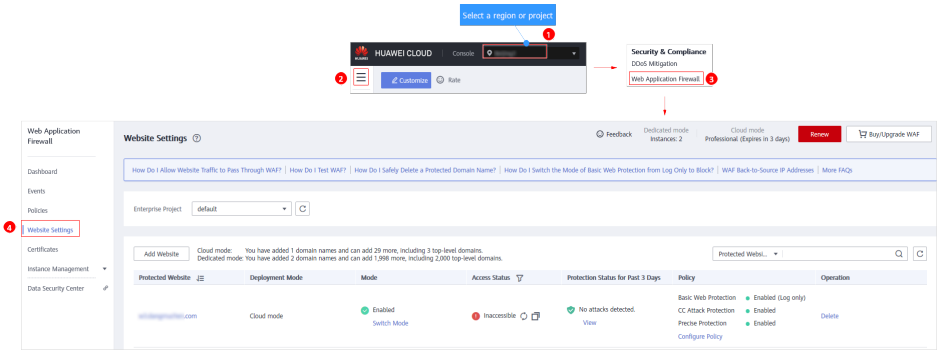
Enabling Anti-Crawler Protection to Verify Browser Validity

If you enable anti-crawler protection, WAF dynamically analyzes website service models and accurately identifies crawler behavior based on data risk control and bot identification approaches.

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

Step 2 Go to the **Website Settings** page by following the steps shown in **Figure 4-5**.

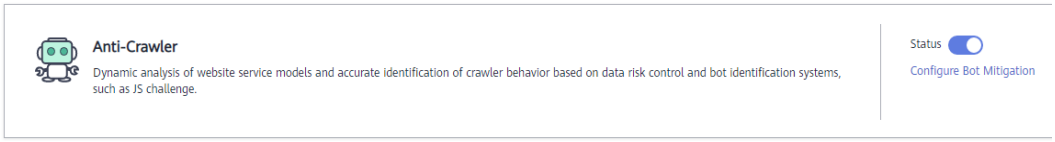
Figure 4-5 Accessing to the Website Settings page



Step 3 In the **Policy** column of the row containing the target domain name, click **Configure Policy** to go to the configuration page.

Step 4 In the **Anti-Crawler** configuration area, enable anti-crawler using the toggle on the right, as shown in **Figure 4-6**. If you enable this function, click **Configure Bot Mitigation**.

Figure 4-6 Anti-Crawler configuration area



 Copyright © Huawei Technologies Co., Ltd.

Step 5 Select the **JavaScript** tab and configure **Status** and **Protective Action**.

JavaScript anti-crawler is disabled by default. To enable it, click  and click **OK** in the displayed dialog box.  indicates that the JavaScript anti-crawler is enabled.

NOTICE

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

  CDN caching may impact JS anti-crawler performance and page accessibility.

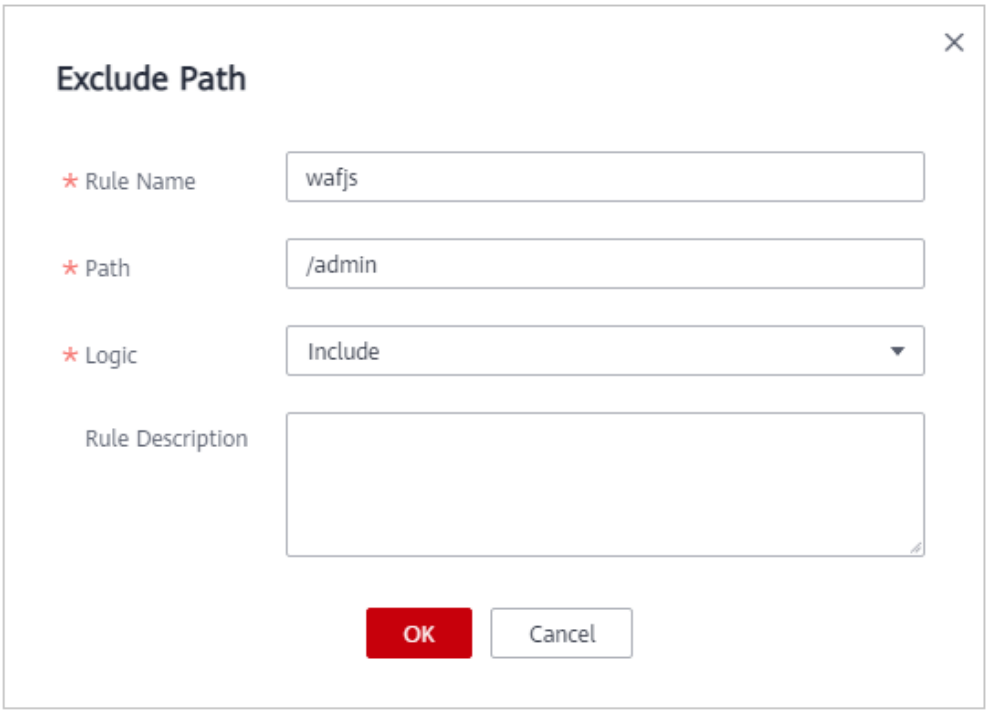
Step 6 Configure a JavaScript-based anti-crawler rule by referring to **Table 4-1**.

Two protective actions are provided: **Protect all paths** and **Protect a specified path**.

- To protect all paths except a specified path

  Select **Protect all paths**, but then in the upper left corner of the page, click **Exclude Path**. Configure the required parameters in the displayed dialog box and click **OK**.

  Figure 4-7 Exclude Path



- To protect a specified path only

  Select **Protect a specified path**. In the upper left corner of the page, click **Add Path**. In the displayed dialog box, configure required parameters and click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Figure 4-8 Add Path

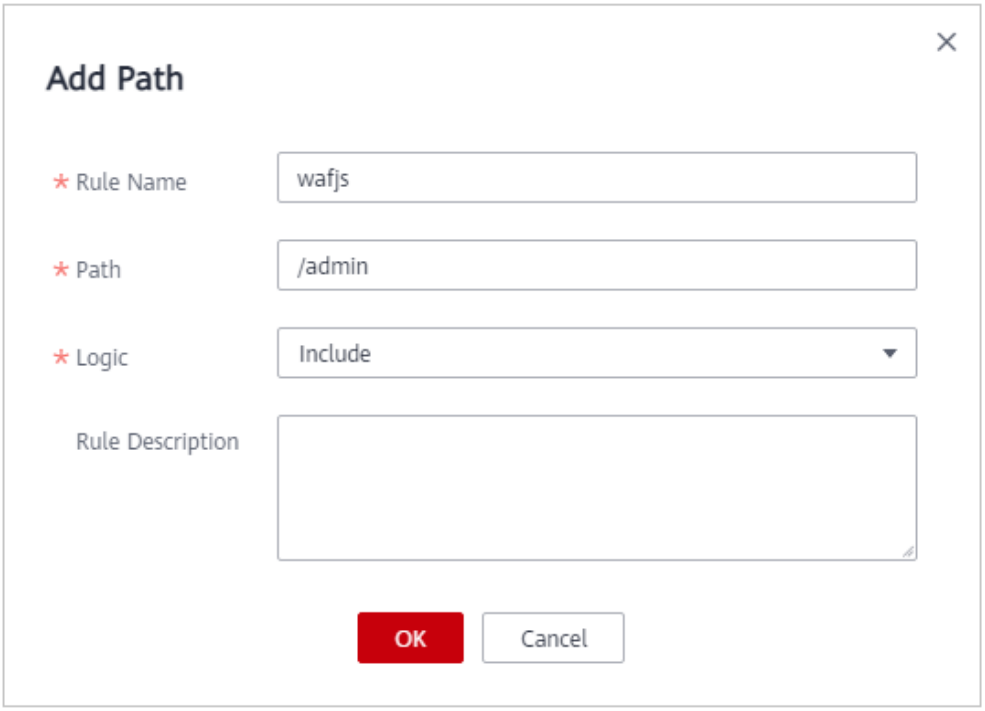


Table 4-1 Parameters of a JavaScript-based anti-crawler protection rule

Parameter	Description	Example Value
Rule Name	Name of the rule	wafjs

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Path	A part of the URL, not including the domain name A URL is used to define the address of a web page. The basic URL format is as follows: Protocol name://Domain name or IP address[:Port]/[Path/.../File name]. For example, if the URL is **http://www.example.com/admin**, set **Path** to **/admin**. **NOTE** • The path does not support regular expressions. • The path cannot contain two or more consecutive slashes. For example, **///admin**. If you enter **///admin**, WAF converts **///** to **/**.	/admin
Logic	Select a logical relationship from the drop-down list.	Include
Rule Description	A brief description of the rule.	None

----End

If you enable anti-crawler, web visitors can only access web pages through a browser.

Copyright © Huawei Technologies Co., Ltd.

```
</body>
</html>
[root@VM_0_9_centos ~]# curl http://cloudsecuritylab.tech/ --user-agent 'xpymep.exe'
<html>
<head>
<meta http-equiv="Server" content="HuaweiCloudWAF">
</head>
<body>
<noscript>
<h1><strong>Please Enable JavaScript and Cookie.</strong></h1>
</noscript>
<h1> <span id = "open_cookie"/> </h1>
<script type="text/javascript">
(function(t,a,c){"function"===typeof window.define&&window.define.amd?window.define(c):"undefined"!=
=typeof module&&module.exports?module.exports=c():a.exports?a.exports=c():a[t]=c()})("fe",this,fu
ion(){var t=function(a){if(!(this instanceof t))return new t(a);this.options=this.extend(a,{swfConta
inerId:"fingerprintjs2",swfPath:"flash/compiled/FontList.swf",detectScreenOrientation:!0,sortPlugins
For:[/palemoon/i],userDefinedFonts:[]});this.nativeForEach=Array.prototype.forEach;this.nativeMap=Ar
ray.prototype.map};
t.prototype={extend:function(a,c){if(null==a)return c;for(var b in a)null!=a[b]&&c[b]!==a[b]&&(c[b]=
a[b]);return c},get:function(a){var c=this,b={data:[],addPreprocessedComponent:function(a){var b=a.v
alue;"function"===typeof c.options.preprocessor&&(b=c.options.preprocessor(a.key,b));this.data.push(
{key:a.key,value:b})}},b=this.userAgentKey(b),b=this.languageKey(b),b=this.colorDepthKey(b),b=this.d
eviceMemoryKey(b),b=this.pixelRatioKey(b),b=this.hardwareConcurrencyKey(b),b=this.screenResolutionKe
y(b),
b=this.availableScreenResolutionKey(b),b=this.timezoneOffsetKey(b),b=this.platformKey(b),b=this.plug
```

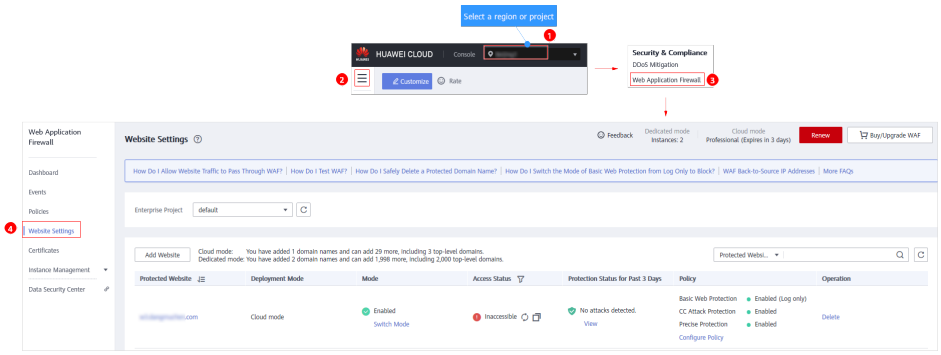
Configuring CC Attack Protection to Limit Access Frequency

A CC attack protection rule uses a specific IP address, cookie, or referer to limit the access to a specific path (URL), mitigating the impact of CC attacks on web services.

Step 1 Log in to the management console.

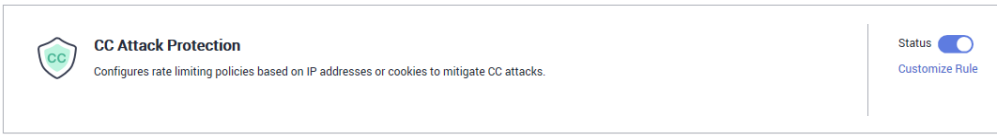
Step 2 Go to the **Website Settings** page by following the steps shown in **Figure 4-9**.

Figure 4-9 Accessing to the Website Settings page



Step 3 Locate the row containing the website domain name you want to apply the policy to. In the **Policy** column, click **Configure Policy**. On the displayed page, in the **CC Attack Protection** area, verify that its **Status** is . **Figure 4-10** shows an example.

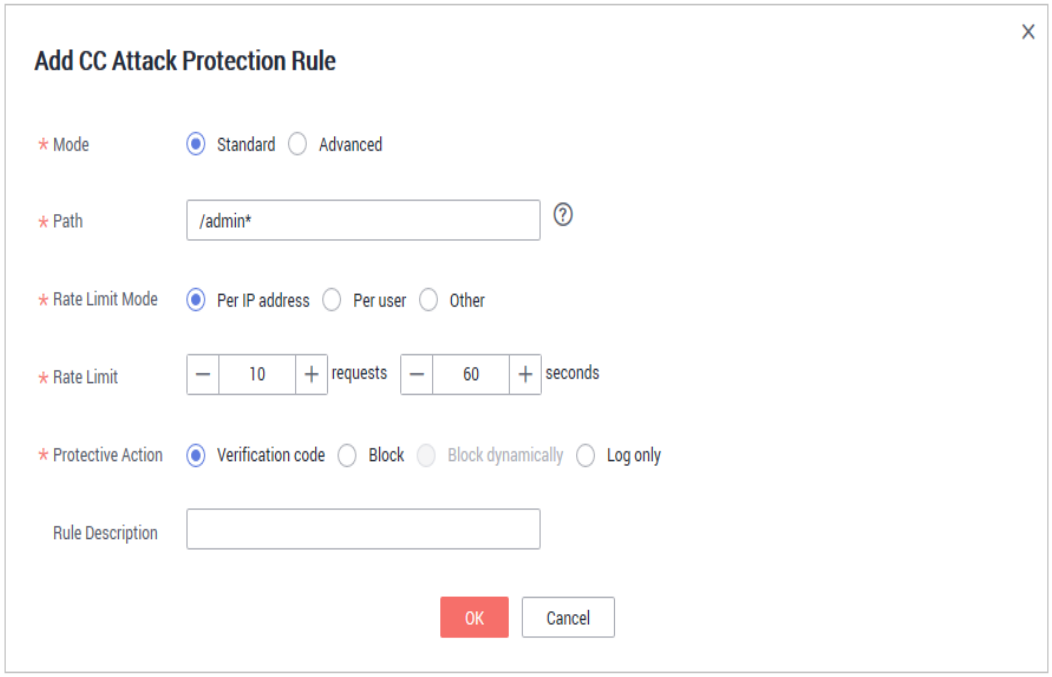
Figure 4-10 CC Attack Protection configuration area



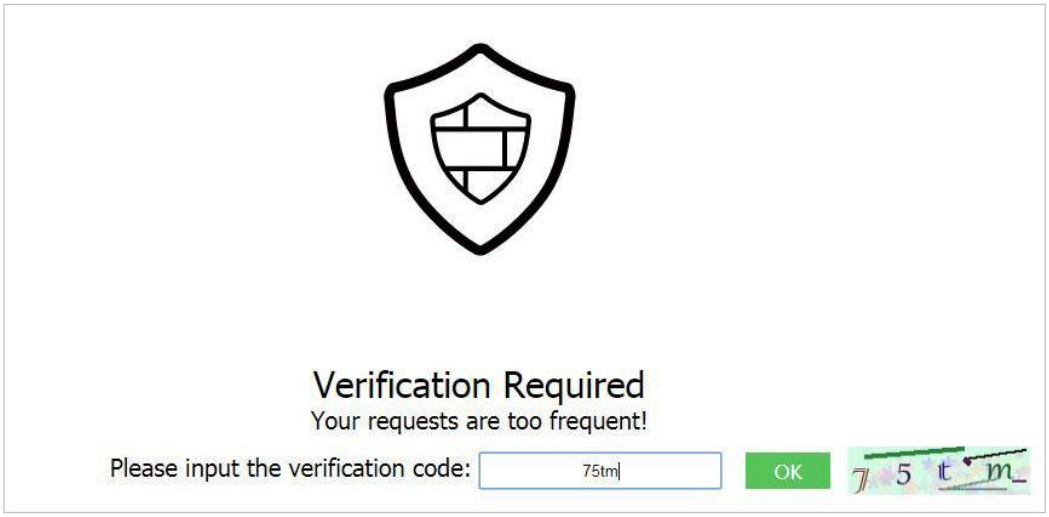
Copyright © Huawei Technologies Co., Ltd.

Step 4 In the upper left corner of the **CC Attack Protection** page, click **Add Rule**. The following uses IP address-based rate limiting and human-machine verification as examples to describe how to add an IP address-based rate limiting rule, as shown in **Figure 4-11**.

Figure 4-11 Rate limiting by IP address



If the number of access requests exceeds the configured rate limit, the visitors are required to enter a verification code to continue the access.



----End

Copyright © Huawei Technologies Co., Ltd.

5 Configuring an Access Control Policy on an ECS or ELB to Protect Origin Servers

After you connect your website to Web Application Firewall (WAF), configure an access control policy on your origin server to allow only the WAF back-to-source IP addresses. This prevents hackers from obtaining your origin server IP addresses and then bypassing WAF to attack origin servers.

This topic walks you through how to check whether origin servers have exposure risks and how to configure access control policies. This topic applies to scenarios where your origin servers are deploying on HUAWEI CLOUD ECSs or you use ELB load balancers for your website.

NOTE

WAF will forward incoming traffic destined for the origin servers no matter whether you configure access control rules on the origin servers. However, if you have no access control rules configured on the origin servers, bad actors may bypass WAF and directly attack your origin servers once they obtain your origin server IP addresses.

Precautions

- Before configuring an access control policy on an origin server, ensure that you have connected all domain names of websites hosted on Elastic Cloud Server (ECS) or having Elastic Load Balance (ELB) deployed to WAF.
- The following issued should be considered when you configure a security group:
  - If you enable the WAF bypassed mode for your website but do not disable security group and network ACL configurations, the origin server may become inaccessible from the Internet.
  - If new WAF back-to-source IP addresses are assigned to WAF after a security group is configured for your website, the website may respond 5xx errors frequently.

How Do I Check Whether the Origin Server IP Address Is Exposed?

In a non-HUAWEI CLOUD environment, use a Telnet tool to establish a connection over the service port of the public IP address of your origin server (or enter the IP address of your web application in the browser). Then, check whether the connection is established.

 Copyright © Huawei Technologies Co., Ltd.

- Connection established

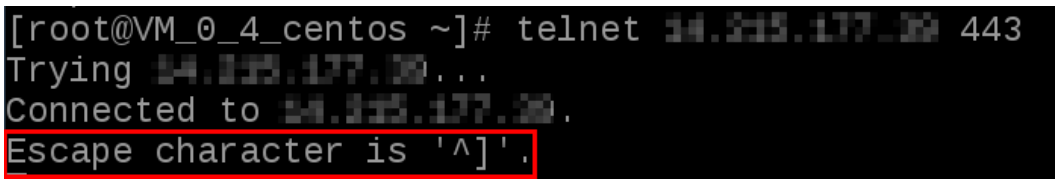
  The origin server has exposed to the public. Once a hacker obtains the public IP address of the origin server, the hacker can bypass WAF and directly attack the origin server.

- Connection not established

  The origin server is hidden from the public and there is no exposure risk.

For example, to check whether the origin server is exposed, check whether the origin server IP address that has been protected by WAF can be connected over port 443. If information similar to that shown in **Figure 5-1** is displayed, the connection is established and the origin server IP address is exposed.

Figure 5-1 Testing



Obtaining WAF Back-to-Source IP Addresses

A back-to-source IP address is a source IP address used by WAF to forward client requests to origin servers. To origin servers, all web requests come from WAF and all source IP addresses are WAF back-to-source IP addresses. The real client IP address is encapsulated into the HTTP X-Forwarded-For (XFF) header field. For more details, see **How Do I Whitelist the WAF Back-to-Source IP Address Ranges?**

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

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

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

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

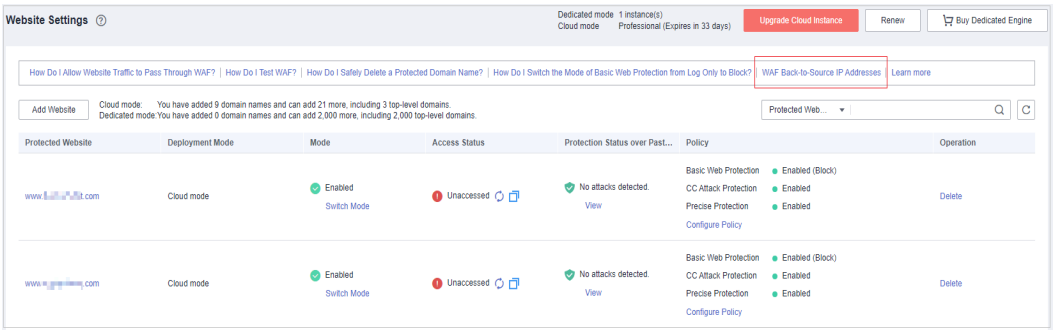
Step 5 On the right of the website list, click the **WAF Back-to-Source IP Addresses** link.

NOTE

WAF back-to-source IP addresses are periodically updated. Whitelist the new IP addresses in time to prevent those IP addresses from being blocked by origin servers.

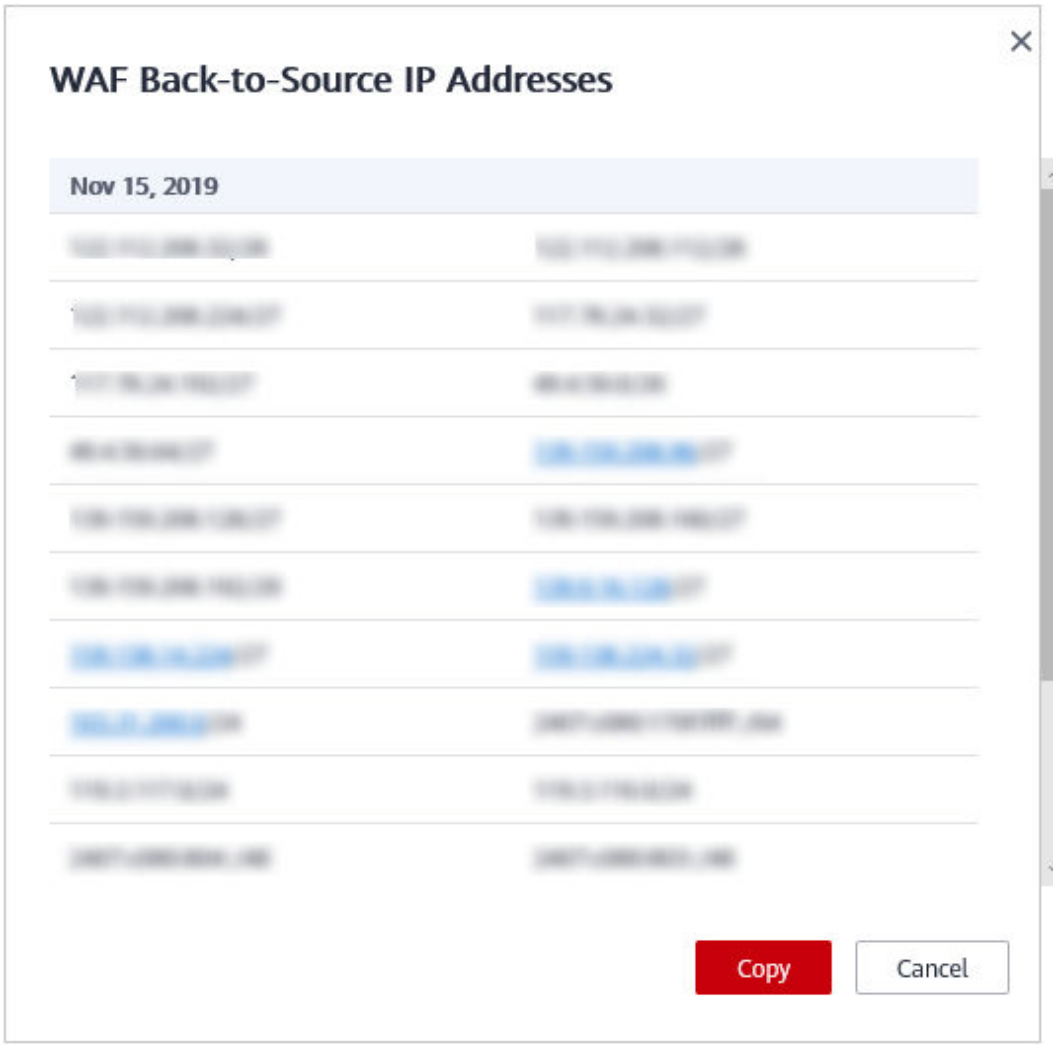
 Copyright © Huawei Technologies Co., Ltd.

Figure 5-2 WAF Back-to-Source IP Addresses



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

Figure 5-3 WAF Back-to-Source IP Addresses dialog box



----End

 Copyright © Huawei Technologies Co., Ltd.

Configuring an Inbound Rule for an ECS

If your origin server is deployed on a HUAWEI CLOUD ECS, perform the following steps to configure a security group rule to allow only the WAF back-to-source IP addresses to access the origin server.

NOTICE

Ensure that all WAF back-to-source IP addresses are whitelisted by an inbound rule of the security group configured for the ECS. Otherwise, website may become inaccessible.

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 **Compute** > **Elastic Cloud Server**.

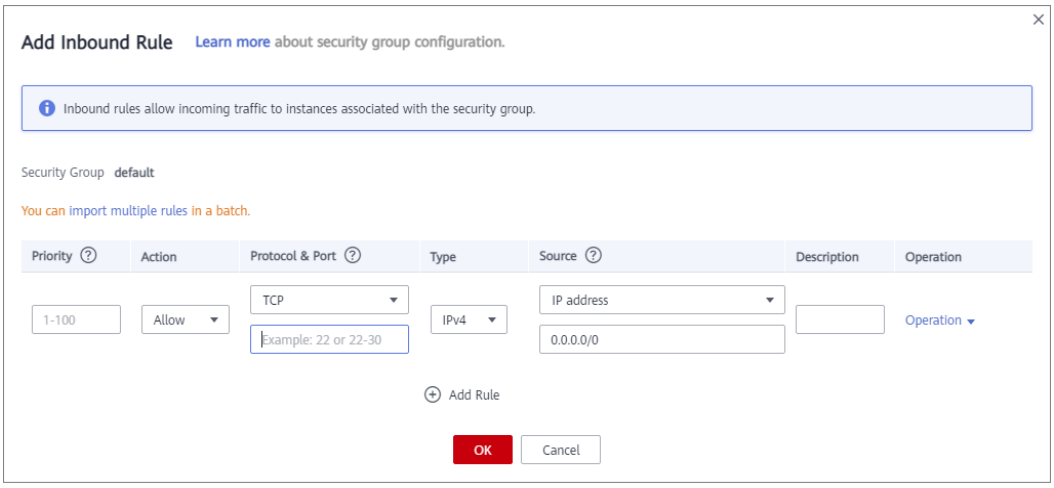
Step 4 Locate the row containing the ECS you want. In the **Name/ID** column, click the ECS name to go to the ECS details page.

Step 5 Click the **Security Groups** tab. Then, click **Change Security Group**.

Step 6 Click the security group name to view the details.

Step 7 Click the **Inbound Rules** tab and then **Add Rule** to go to the **Add Inbound Rule** page. **Figure 5-4** shows an example. **Table 5-1** describes the parameters.

Figure 5-4 Add Inbound Rule



 Copyright © Huawei Technologies Co., Ltd.

Table 5-1 Inbound rule parameters

Parameter	Description
Protocol & Port	Protocol and port for which the security group rule takes effect. If you select **TCP (Custom ports)**, enter the origin server port number in the text box below the TCP box.
Source	Add all WAF back-to-source IP addresses copied in **Step 6** one by one. **NOTE** One IP address is configured in a rule. Click **Add Rule** to add more rules. A maximum of 10 rules can be added.

Step 8 Click **OK**.

Then, the security group rules allow all inbound traffic from the WAF back-to-source IP addresses.

To check whether the security group rules take effect, refer to **How Do I Check Whether the Origin Server IP Address Is Exposed?** If a connection cannot be established over the service port but the website is still accessible, the configuration takes effect.

----End

Enabling ELB Access Control

If your origin server is deployed on backend servers of a HUAWEI CLOUD ELB load balancer, perform the following steps to configure an access control list to allow only the WAF back-to-source IP addresses to access the origin server.

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

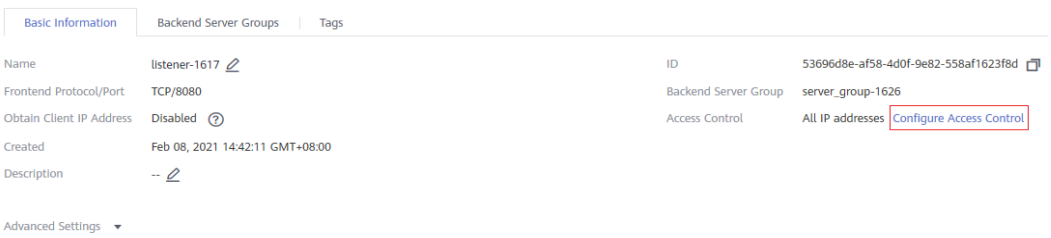
Step 2 Click in the upper left corner of the management console and select a region or project.

Step 3 Click in the upper left corner of the page and choose **Networking** > **Elastic Load Balance**.

Step 4 Locate the load balancer you want. In the **Listener** column, click the listener name to go to the details page.

Step 5 On the displayed page, click the **Listeners** tab. On the **Basic Information** tab, click **Configure Access Control** next to **Access Control**. **Figure 5-5** shows an example.

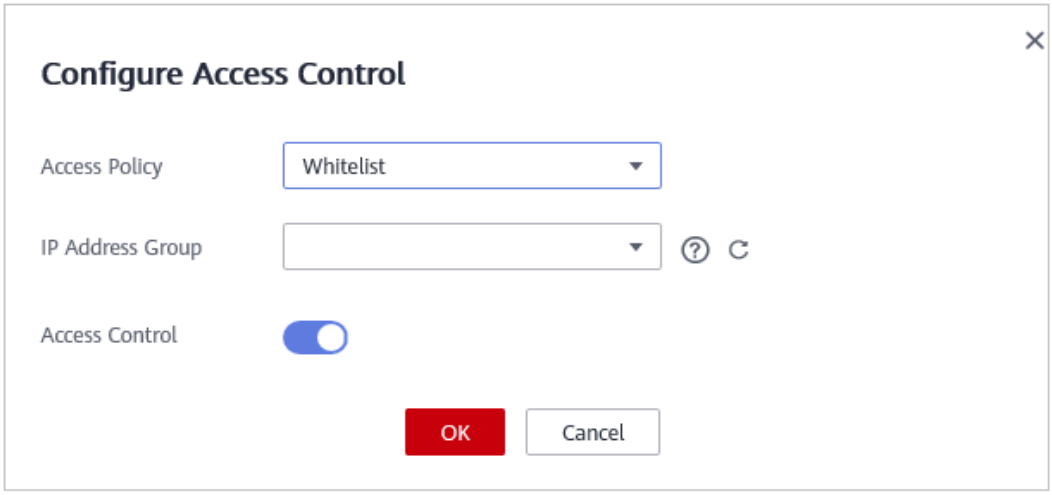
Figure 5-5 Configuring Access Control



 Copyright © Huawei Technologies Co., Ltd.

Step 6 In the displayed dialog box, select **Whitelist** for **Access Policy**. **Figure 5-6** shows an example.

Figure 5-6 Configuring whitelist access control



Step 7 Select the IP address group including only WAF back-to-source IP addresses obtained in **Step 6**.

NOTE

If no such an IP address group exists, click **Create IP Address Group** and add all WAF back-to-source IP addresses to the IP address group you are creating.

Step 8 Click **OK**.

To check whether the security group rules take effect, refer to **How Do I Check Whether the Origin Server IP Address Is Exposed?** If a connection cannot be established over the service port but the website is still accessible, the configuration takes effect.

----End

Copyright © Huawei Technologies Co., Ltd.

6 Configuring Basic Web Protection

This topic describes best practices in basic web protection.

Application Scenarios

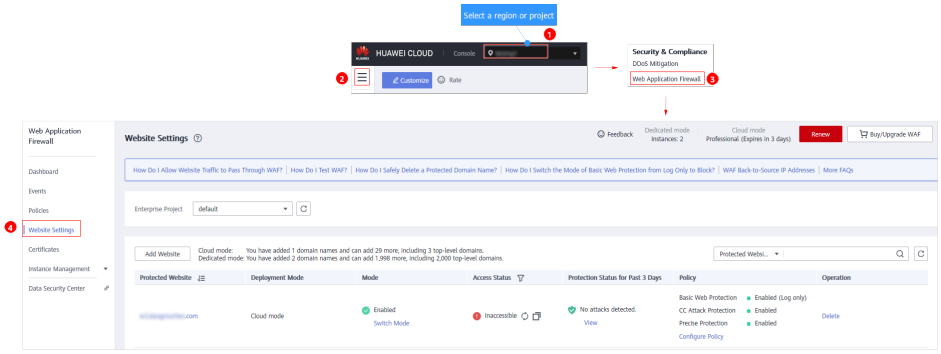
Web Application Firewall (WAF) keeps web services stable and secure. It examines all HTTP and HTTPS requests to detect and block the following attacks: Structured Query Language (SQL) injection, cross-site scripting (XSS), web shells, command and code injections, file inclusion, sensitive file access,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

Protection Policy

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

Step 2 Go to the **Website Settings** page by following the steps shown in **Figure 6-1**.

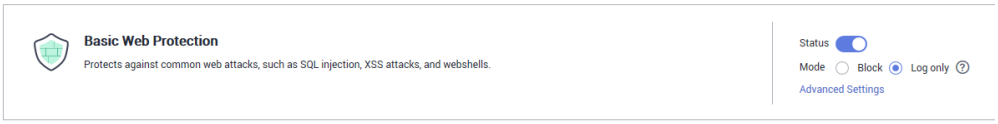
Figure 6-1 Accessing to the Website Settings page



Step 3 In the **Policy** column of the row containing the target domain name, click **Configure Policy**. The protection configuration page is displayed.

Step 4 In the **Basic Web Protection** configuration area, view the protection status. **Figure 6-2** shows an example.

Figure 6-2 Basic Web Protection configuration area

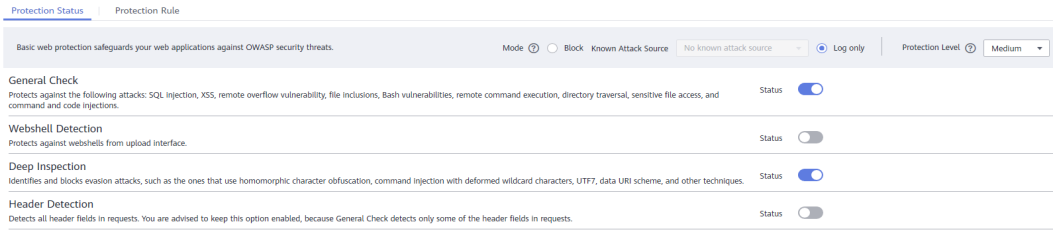


By default, **Basic Web Protection** is enabled and its mode is **Log only**.

- Protection status
  - : The corresponding check in **Basic Web Protection** is enabled.
  - : The corresponding check in **Basic Web Protection** is disabled.
- Protection mode: block or log only
  - **Block**: WAF blocks and logs the detected attacks.
  - **Log only**: WAF only logs the detected attacks.

Step 5 Click **Advanced Settings**. The **Basic Web Protection** page is displayed, as shown in **Figure 6-3**.

Figure 6-3 Basic web protection



- **Protection Level**: high, medium, and low. The default level is **Low**.

  Table 6-1 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	WAF blocks the requests with no attack signature but have specific attack patterns. **High** is recommended if you want to block SQL injection, XSS, and command injection attacks.

- Specify the protection type.

 Copyright © Huawei Technologies Co., Ltd.

By default, **General Check** and **Scanner** are enabled. Enable other protection types if needed.

----End

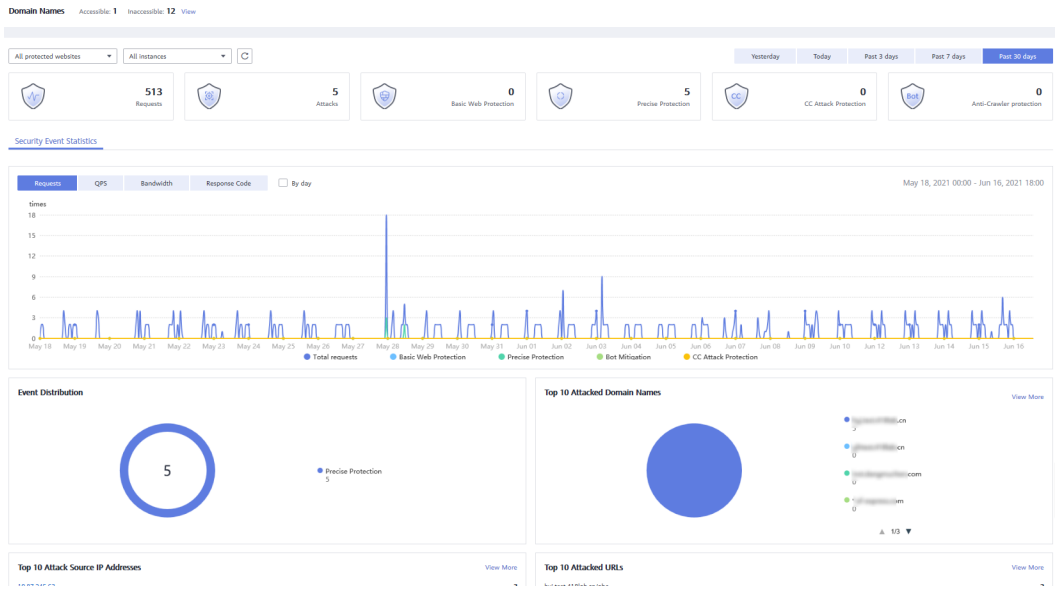
Usage Instructions

- If you are not familiar with your website's traffic pattern, select the **Log only** mode for one to two weeks and analyze the logs for those days.
  - If no record of blocking legitimate requests is found, switch to the **Block** mode.
  - If legitimate requests are blocked, adjust the protection level or configure false alarm masking rules to prevent legitimate requests from being blocked.
- Note the following points in your operations:
  - Do not transfer the original SQL statement or JAVA SCRIPT code in a legitimate HTTP request.
  - Do not use special keywords (such as UPDATE and SET) in a legitimate URL. For example, **https://www.example.com/abc/update/mod.php?set=1**.
  - Use Object Storage Service (OBS) or other secure methods to upload files that exceed 50 MB rather than via a web browser.

Protection Effect

Go to the **Dashboard** page and view the protection event logs. **Figure 6-4** shows an example.

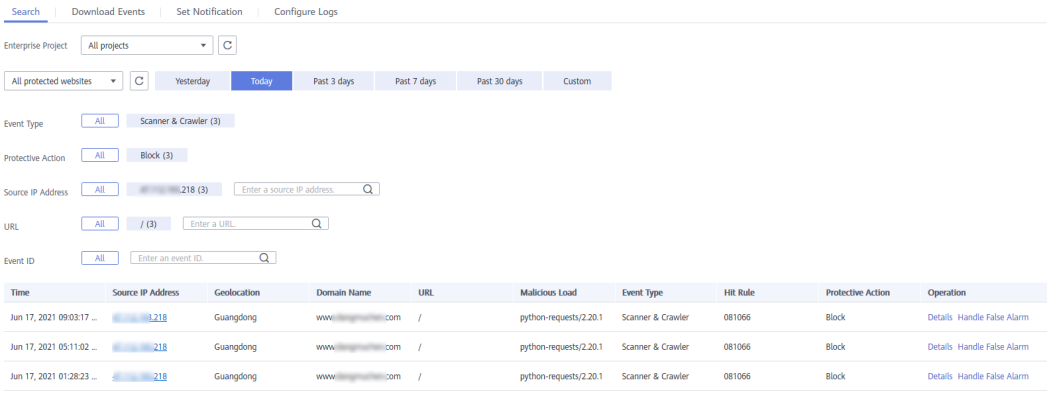
Figure 6-4 Viewing event logs



You can also view protection logs generated in yesterday, today, past 3 days, past 7 days, 30 days, or user-defined time range on the **Events** page. Click **Details** to view event details. **Figure 6-5** shows an example.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-5 Viewing protection events



 Copyright © Huawei Technologies Co., Ltd.

7 Handling False Alarms to Get Improved Basic Web Protection

After you connect your website to Web Application Firewall (WAF) and enable basic web protection, WAF detects and blocks requests that match the rules you configured. If a normal request matches a basic web protection rule and is blocked by WAF, you can handle the event as false alarm. In this way, WAF will no longer block the same type of request.

Prerequisites

You can view false alarm events on the **Events** page.

Constraints

An event can only be handled as a false alarm once.

Application scenarios

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

Impact on the System

- The event will not be displayed on the **Events** page and you will not receive any alarm notifications about the event.
- If an event is handled as a false alarm, the matched rule will be added to the false alarm masking rule list. You can view, disable, delete, or modify the rule on the **False Alarm Masking** page under **Policies**.

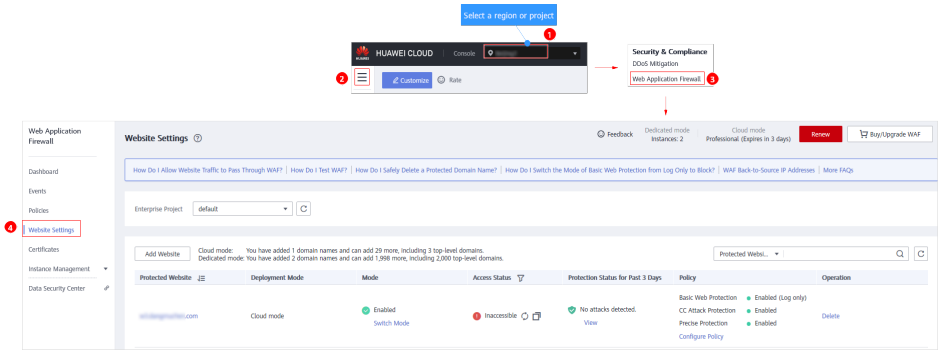
Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Log in to the management console.

Step 2 Go to the **Website Settings** page by following the steps shown in **Figure 7-1**.

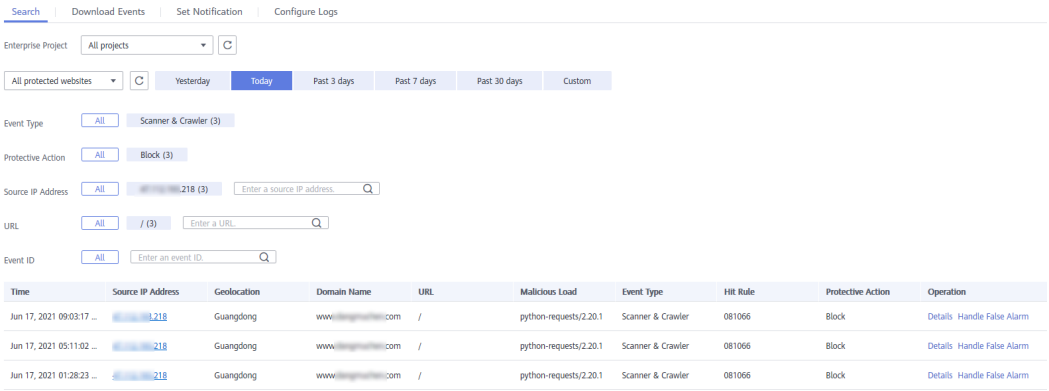
Figure 7-1 Accessing to the Website Settings page



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

Step 4 In the event list, search for false alarms by protected website, event type, source IP address, and URL. **Figure 7-2** shows an example.

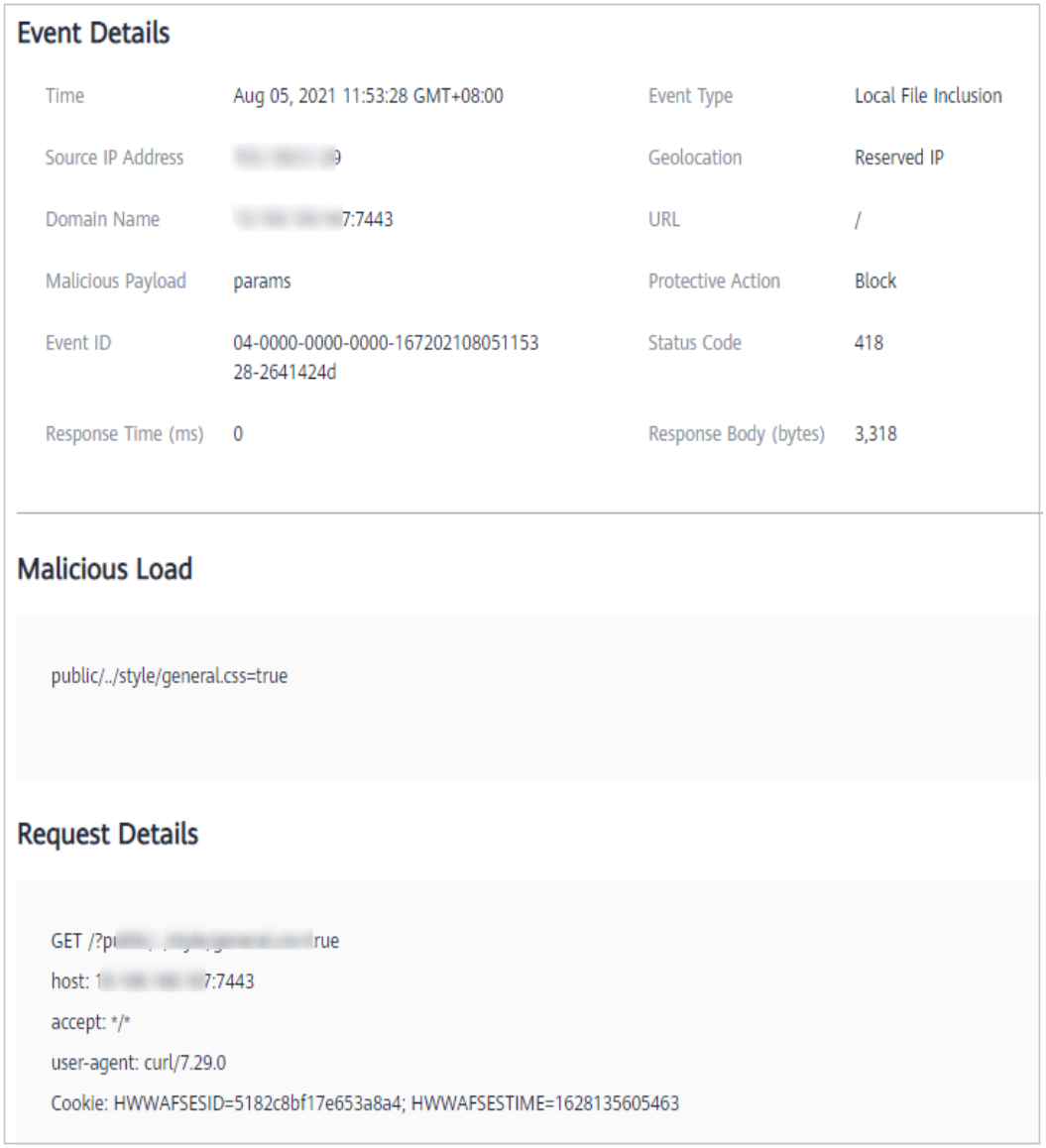
Figure 7-2 Viewing protection events



Step 5 In the **Operation** column of an event you consider as a false alarm, click **Details**. On the displayed page, confirm that the event is a false alarm. **Figure 7-3** shows an example.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-3 Event Details

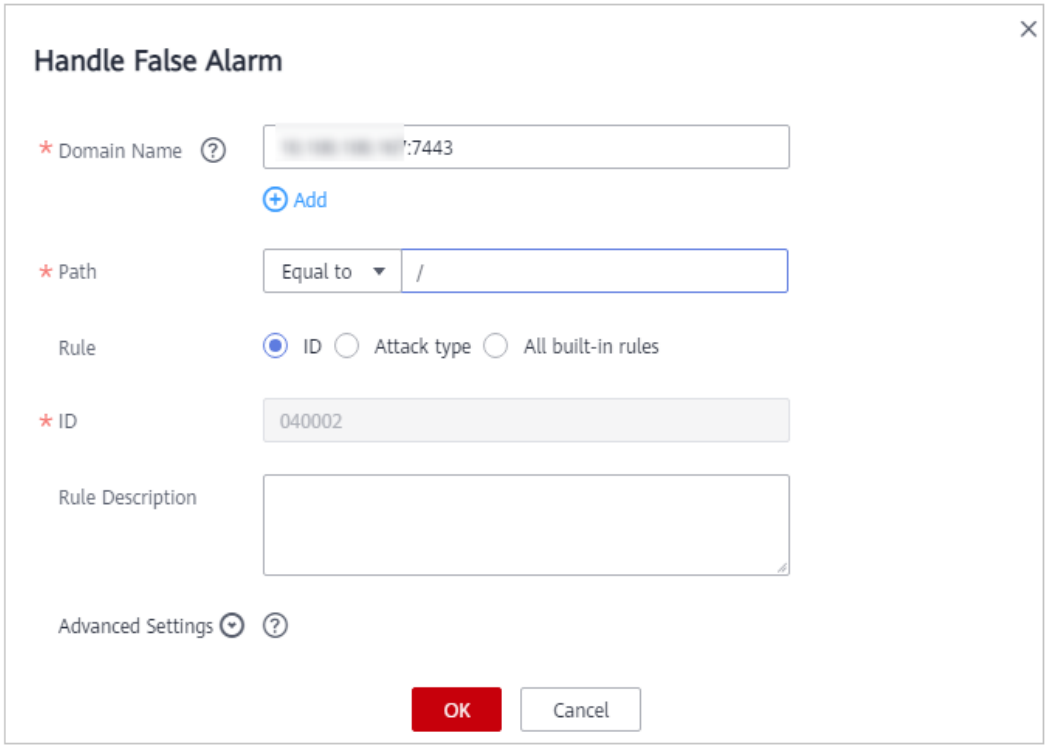


Step 6 In the row containing the event, click **Handle False Alarm** in the **Operation** column.

Step 7 In the displayed dialog box, click **OK**.

 Copyright © Huawei Technologies Co., Ltd.

Figure 7-4 Handle False Alarm



- Click **Add** to add other protected domain names to apply the false alarm masking rule to these domain names.
- Path

  Part of the URL (excluding a domain name) that a false alarm is reported for. The default value is the source path of the event.
  - Prefix match: If you select **Prefix is**, the entered path is used as the prefix. For example, if the path to be protected is **/admin/test.php** or **/adminabc**, set **Path** to **/admin**.
  - Exact match: The path to be entered must be **Equal to** the path to be protected. For example, if the path to be protected is **/admin/test.php**, set **Path** to **/admin/test.php**.

----End

Verification

A false alarm will be deleted within about a minute after the handling configuration is done. It will no longer be displayed in the event list. You can clear the cache, refresh the browser, and access the page again to verify whether the false alarm was successfully handled. If the requested page responds normally, the configuration takes effect.

Follow-up Procedure

- **Downloading Events**

  On the **Events** page, you can download the event data of all protected domain names for the past five days. A CSV file of the protection event data for the current day is generated at 00:00:00 the next day.

Copyright © Huawei Technologies Co., Ltd.

- **Configuring False Alarm Masking Rules**

  You can configure a false alarm masking rule to ignore some rule IDs or event types. For example, if you do not want to check a specific URL for XSS attacks, you can configure a false alarm masking rule to mask XSS checks for the URL.

Basic Web Protection Check Items

WAF basic web protection defends against common Open Web Application Security Project (OWASP) security threats. WAF uses built-in semantic analysis and regular expression engines for basic web protection to detect and block threats such as malicious scanners, IP addresses, and web shells. You can enable all protection rules in basic web protection or only the ones you want. For details, see **Table 7-1**.

Table 7-1 Check item description

Check Item	Description
General Check	WAF 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. **NOTE** If you enable **General Check**, WAF checks your websites based on the built-in rules.
Webshell Detection	WAF protects web applications from web shells. **NOTE** If you enable **Webshell Detection**, WAF detects web page Trojans inserted through the upload interfaces.
Deep Inspection	WAF identifies and blocks evasion attacks, such as the ones that use homomorphic character obfuscation, command injection with deformed wildcard characters, UTF7, data URI scheme, and other techniques. **NOTE** If you enable **Deep Inspection**, WAF detects and defends against evasion attacks in depth.
Header Detection	This check is disabled by default. If this check is disabled, only some of the header fields in the received requests are checked against **General Check**. **NOTE** If you enable **Header Detection**, WAF inspects all header fields in the received requests.

Basic Web Protection Levels

WAF provides three basic web protection levels, **Low**, **Medium**, and **High**. The default level is **Medium**. The lower the protection level, the higher the false negative rate and the lower the false positive rate. For details, see **Table 7-2**.

Copyright © Huawei Technologies Co., Ltd.

Table 7-2 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	WAF blocks the requests with no attack signature but have specific attack patterns. **High** is recommended if you want to block SQL injection, XSS, and command injection attacks.

Copyright © Huawei Technologies Co., Ltd.

8 Connecting a Domain to WAF

8.1 Preparations

After your domain is successfully set up, WAF protects it from common web attacks and CC attacks.

Website Service Review

Sort out all website services you want to protect with WAF. This helps you learn about status quo and specific data for making right decisions in configuring protection policies.

Table 8-1 Website services

Item	Description
Website and Service Information	
Daily peak traffic of website/web application services, including the bandwidth (in Mbit/s) and QPS	Use it as the basis for selecting the service bandwidth and QPS specifications.
Major user group (for example, major area that the requests originate from)	Determine the attack source and then set geolocation access control rules to block users from these areas.
Whether the service is a C/S architecture	If yes, check whether there is an app client, Windows client, Linux client, code callback, or any other client.
Location where the origin server is deployed	Decide which region to buy.
Operating system (Linux or Windows) and web service middleware (Apache, Nginx, or IIS) of the origin server	Check whether access control is enabled for the origin server. If yes, whitelist WAF back-to-source IP addresses.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Domain protocol	Check whether WAF supports the communication protocol used by your site.
Service port	Check whether your service ports are within the port range supported by WAF.
Whether TLSv1.0 or weak encryption suite is supported	Check whether WAF supports the encryption suite used by your site.
Whether the client supports Server Name Indication (for HTTPS services)	If your domain name supports HTTPS, the client and server must support Server Name Indication (SNI).
Service interaction	Understand the service interaction process and service processing logic to facilitate subsequent configuration of protection policies.
Active users	Determine the severity of an attack event to take a low-risk measure to respond it.
Services and Attacks	
Service types and features (such as games, cards, websites, or apps)	Help analyze the attack signatures.
Inbound traffic range and connection status of a single user or a single IP address	Help determine whether a rate limiting policy can be configured per IP address.
User group attribute	For example, individual users, Internet cafe users, or proxy users
Whether your website experienced large-volumetric attacks, the attack type, and maximum peak traffic	Determine whether a DDoS protection service is required and determine the DDoS protection specifications based on the peak attack traffic.
Whether your website experienced CC attacks and the maximum peak QPS in a CC attack	Configure the protection policies based on attack signatures.
Whether the pressure test has been performed	Evaluate the request processing performance of the origin server to determine whether service anomaly occurs due to attacks.

Prerequisites

- The domain information (such as the IP address and port number of the origin server) has been added to WAF.

 Copyright © Huawei Technologies Co., Ltd.

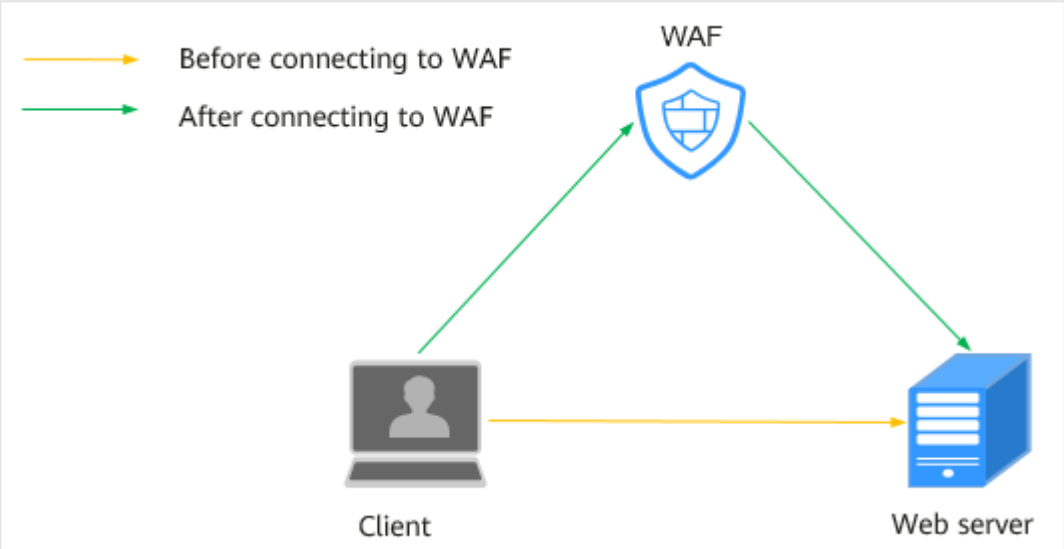
- An administrator account is available for you to change DNS records for WAF to take effect.
- The pressure test has been performed.
- The IP addresses of trusted clients have been whitelisted if your website has trusted clients (such as certain monitoring systems, APIs invoked by internal IP addresses or IP address ranges, and program clients).

8.2 Connecting a Domain to WAF for Websites with no Proxy Used

If your website is not added to WAF, DNS resolves your domain name to the IP address of the origin server. If your website is added to WAF, DNS resolves your domain name to the CNAME of WAF. In this way, the traffic passes through WAF. WAF inspects every traffic coming from the client and filters out malicious traffic. This section describes how to change DNS settings for WAF to take effect.

Schematic Diagram

Figure 8-1 No proxy used



Prerequisites

- Website domain names are available.
- **WAF has been purchased**.
- The website information (such as the IP address and port number of the origin server) **has been added to WAF**.
- The account to update the DNS configuration is available.
- (Optional) WAF back-to-source IP addresses have been whitelisted. If non-HUAWEI CLOUD security software is used on the origin server, whitelist the WAF back-to-source IP addresses to prevent normal traffic from being blocked. For details, see **Configuring an Access Control Policy on an ECS or ELB to Protect Origin Servers**.

Copyright © Huawei Technologies Co., Ltd.

- (Optional) WAF testing has been performed before changing DNS settings. This can prevent service interruption due to incorrect configurations. For details, see **Testing WAF**.

Scenario

- If the **Type** of the domain name host record added on DNS is **CNAME - Map one domain to another**, complete the configuration based on the instructions in **CNAME Access**.

For details, see **Record Set Types and Configuration Rules**

CNAME Access

If the **Type** of the domain name host record added on DNS is **CNAME - Map one domain to another**, add the domain name to WAF by following the steps below.

The methods to change DNS settings at different domain registrars are similar. HUAWEI CLOUD Domain Name Service (DNS) is used as an example.

Step 1 Obtain the CNAME record.

- If you are adding a domain name, perform the following operations to obtain the CNAME record of the domain name after configuring the basic information about the domain name:

  Click **Copy** to obtain the CNAME record of the domain name. See **Figure 8-2** or **Figure 8-3**.

  Figure 8-2 Connecting a domain name to WAF (proxy used)

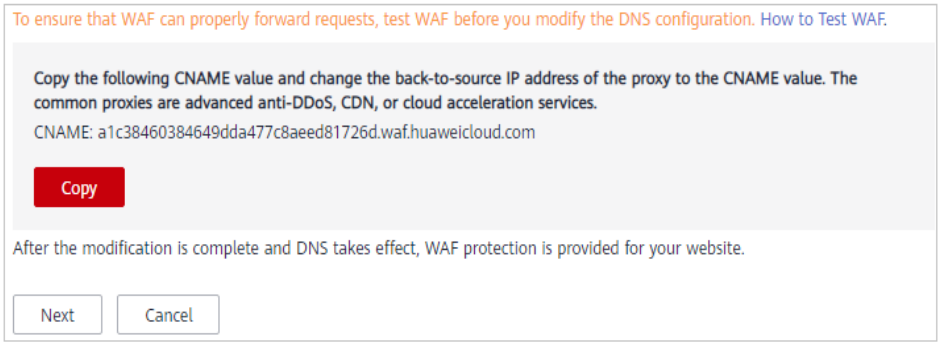
  

  Figure 8-3 Connecting a domain name to WAF (no proxy used)

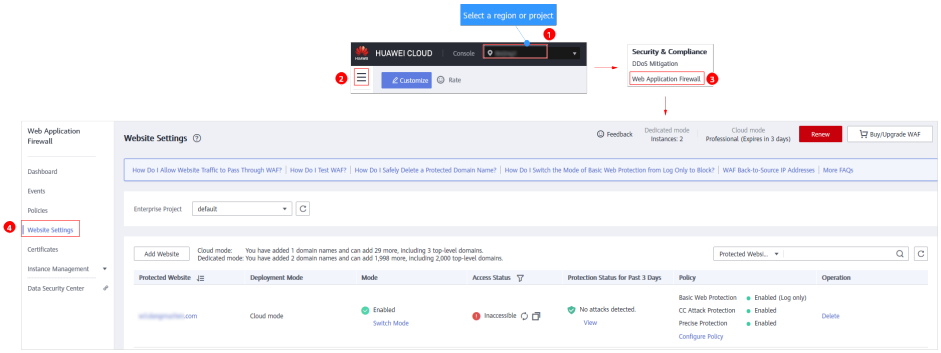
  

- If you have added a domain name, perform the following steps to obtain the CNAME record of the domain name:

 Copyright © Huawei Technologies Co., Ltd.

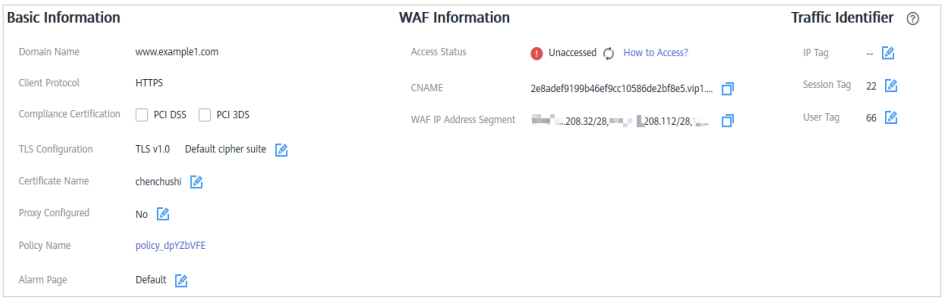
a. Go to the **Website Settings** page by following the steps shown in **Figure 8-4**.

Figure 8-4 Accessing to the Website Settings page



b. In the row of the desired domain name, under the **Protected Website** column, click the domain name you want to test.

Figure 8-5 Basic Information

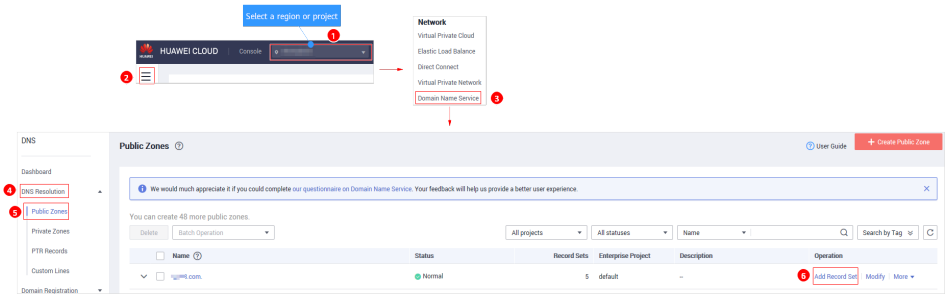


c. In the **CNAME** row, click  to copy the CNAME record.

Step 2 Change the DNS settings.

1. Access the DNS resolution page, as shown in **Figure 8-6**.

Figure 8-6 DNS page



2. In the **Operation** column of the target domain name, click **Modify**. The **Modify Record Set** page is displayed.
3. In the displayed **Modify Record Set** dialog box, change the record value, as shown in **Figure 8-7**.
   - **Name**: Domain name configured in WAF
   - **Type**: Select **CNAME - Map one domain to another**.

 Copyright © Huawei Technologies Co., Ltd.

- **Line**: **Default**
- **TTL (s)**: The recommended value is **5 min**. A larger TTL value will make it slower for synchronization and update of DNS records.
- **Value**: Change it to the copied CNAME value from WAF.
- Keep other settings unchanged.

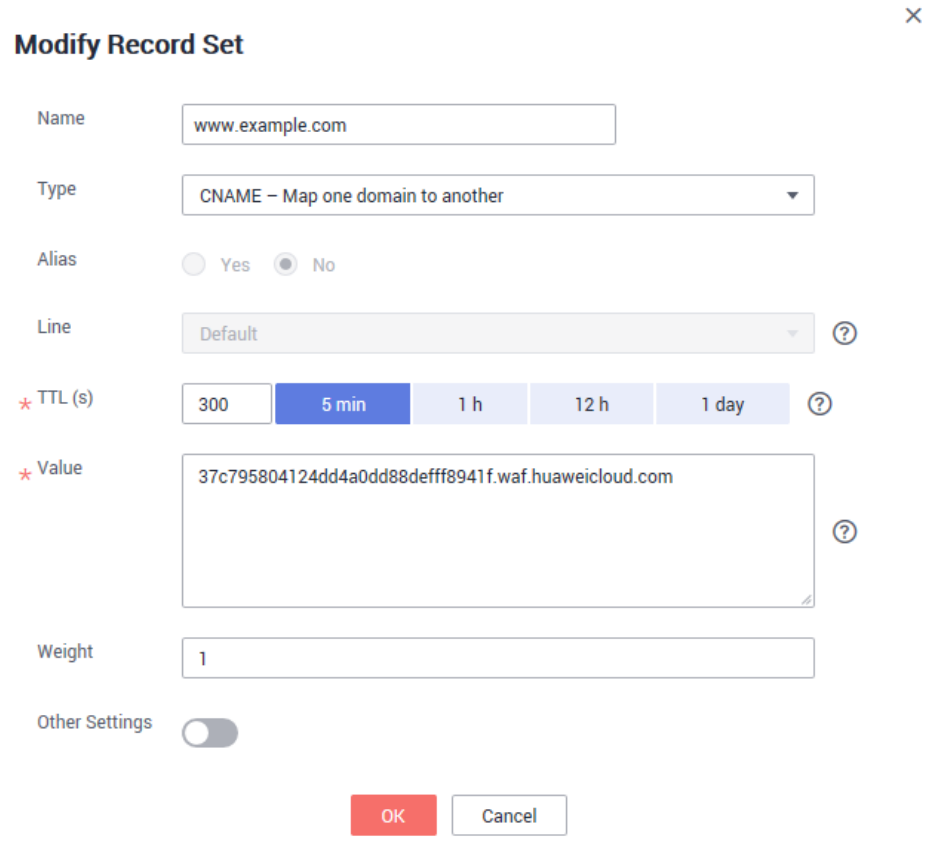
NOTE

About modifying the resolution record:

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

For details, see **Why Is a Message Indicating Conflict with an Existing Record Displayed When I Add a Record Set?**

Figure 8-7 Modifying a record set



4. Click **OK**.

Step 3 (Optional) Ping the IP address of your domain name to check whether the new DNS settings take effect.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

It takes some time for the new DNS settings to take effect. If ping fails, wait for 5 minutes and ping again.

----End

 Copyright © Huawei Technologies Co., Ltd.

9 Combining CDN and WAF to Get Improved Protection and Load Speed

How the Combination Works

- When a user accesses a website that uses HUAWEI CLOUD CDN, the local DNS server will redirect all domain requests to CDN using CNAME records. **CDN** uses a group of predefined policies (such as the content type, geographical location, and network load status) to respond visitors with the nearest CDN IP address so that visitors can obtain requested website content as quickly as possible.

  Objects supported by CDN: domain names of web applications on HUAWEI CLOUD, other cloud platforms, or on-premises data centers
- 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).

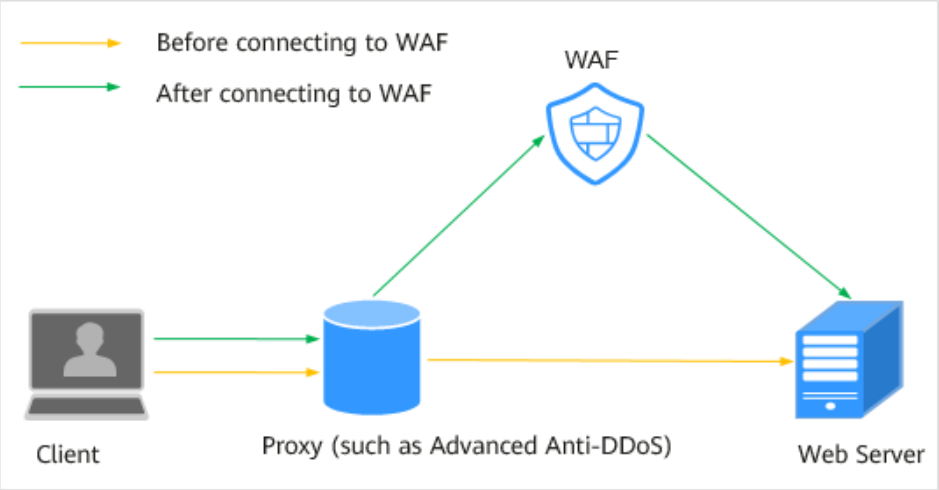
  WAF offers the cloud, dedicated, and ELB mode to protect websites. You can add either domain names or IP addresses to WAF. Before you start, get familiar with the following differences:

  - Cloud mode: protects your web applications on HUAWEI CLOUD, other cloud platforms, or on-premises data centers through domain names.
  - Dedicated or ELB mode: protects your web applications on HUAWEI CLOUD through domain names or IP addresses.

The combination of CDN and WAF can protect websites on HUAWEI CLOUD, other clouds, or on-premises and improve website response time. **Figure 9-1** shows the configuration diagram.

 Copyright © Huawei Technologies Co., Ltd.

Figure 9-1 WAF configuration when a proxy is used



After you deploy CDN and WAF for your website, traffic is accelerated by CDN and then forwarded to WAF. WAF checks received traffic and forwards only the normal traffic to the origin server. The combination protects the website against attacks while improving the website response speed and availability.



The configurations are as follows:

- Cloud mode

  Point your website domain name to CDN and then change the CDN back-to-source address to the WAF CNAME record. After that, you can also add a WAF subdomain name and TXT record on your DNS management platform in case others have connected the website domain name to WAF before you configure CDN.

- Dedicated mode

  Resolve the website domain name to CDN and change the CDN back-to-source IP address to the EIP bound to the load balancer configured for dedicated WAF instance.

- ELB mode

  Resolve the website domain name to CDN and change the CDN back-to-source IP address to the EIP bound to the load balancer configured for the dedicated WAF instance.

Prerequisites

The domain name or IP address has been connected to **CDN**, and the configuration in **Table 9-1** have been completed.

 Copyright © Huawei Technologies Co., Ltd.

Table 9-1 Configurations required in different WAF modes

Deployment Mode	Description
Cloud	1. You have **purchased a cloud WAF instance**. 2. The website domain name details (such as the IP address and port of the origin server) **have been added to the cloud WAF instance**. 3. You have obtained the permissions from the DNS service provider to add domain names. 4. (Optional) WAF back-to-source IP addresses have been whitelisted. If non-HUAWEI CLOUD security software is used on the origin server, whitelist the WAF back-to-source IP addresses to prevent normal traffic from being blocked. For details, see **Configuring an Access Control Policy on an ECS or ELB to Protect Origin Servers**. **NOTICE** To ensure that the WAF policy takes effect for the real source IP address, ensure that **Yes** is selected for **Proxy Configured** when you add the domain name to WAF. For details, see **Viewing Basic Information**
Dedicated mode	1. You have **purchased a dedicated WAF instance**. 2. The website domain name details (such as the IP address and port of the origin server) **have been added to the dedicated WAF instance**. 3. You have **configured a load balancer for the dedicated WAF instance**. 4. You have **bound an EIP to the load balancer**. 5. **Whitelist back-to-source IP addresses of dedicated WAF instances on the origin servers**.
ELB mode	1. You have **purchased a load-balancing WAF instance**. 2. You have **added the domain name to the load-balancing WAF instance**. 3. You have **bound a dedicated load balancer** to the WAF instance. 4. **Whitelist back-to-source IP addresses of load balancing WAF instances on the origin servers**.

Copyright © Huawei Technologies Co., Ltd.

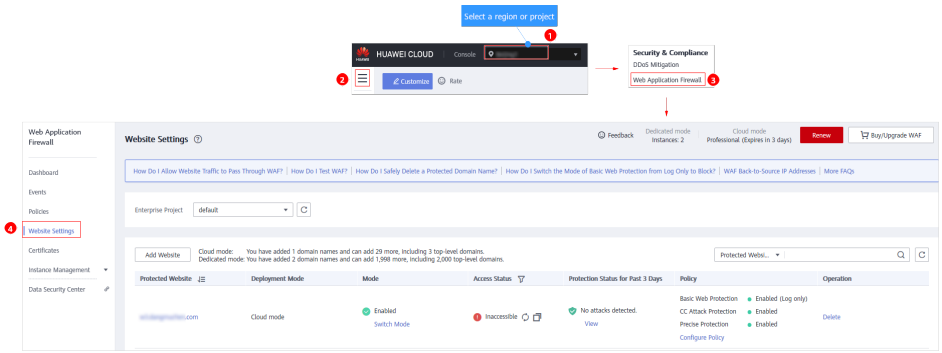
Cloud WAF Configuration

The following uses HUAWEI CLOUD CDN as an example to describe how to configure domain name resolution. If you use HUAWEI CLOUD CDN, perform the following steps directly. If you use non-HUAWEI CLOUD CDN, configure domain name resolution on non-HUAWEI CLOUD CDN based on the instructions in the following steps.

Step 1 Obtain settings of **CNAME**, **Subdomain Name**, and **TXT Record**.

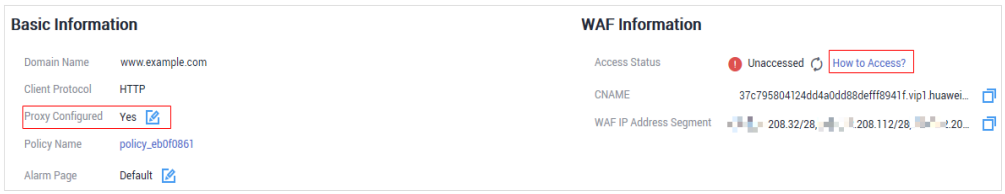
1. Log in to the management console.
2. Go to the **Website Settings** page by following the steps shown in **Figure 9-2**.

Figure 9-2 Accessing to the Website Settings page



3. In the **Protected Website** column, click the domain name you want to go to the **Basic Information** page.
4. On the page for configuring basic domain information, click in the row where the CNAME is located to copy **CNAME**. In the row of **Access Status**, click **How to Access**. In the **Access Guide** dialog box, copy **Subdomain Name** and **TXT Record**.

Figure 9-3 Domain name access information



Step 2 **Change the origin server domain name of the primary origin server of CDN to the CNAME of WAF.**

Step 3 (Optional) Add a WAF subdomain name and TXT record at your DNS provider.

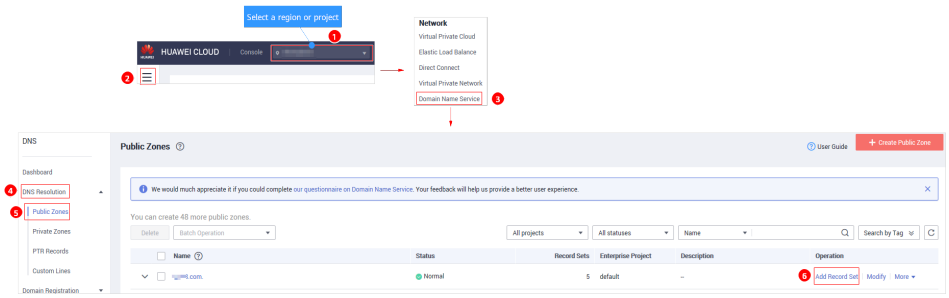
NOTE

To prevent others from configuring your domain names on WAF in advance (this will cause interference on your domain name protection), this step is recommended.

1. Access the DNS resolution page, as shown in **Figure 9-4**.

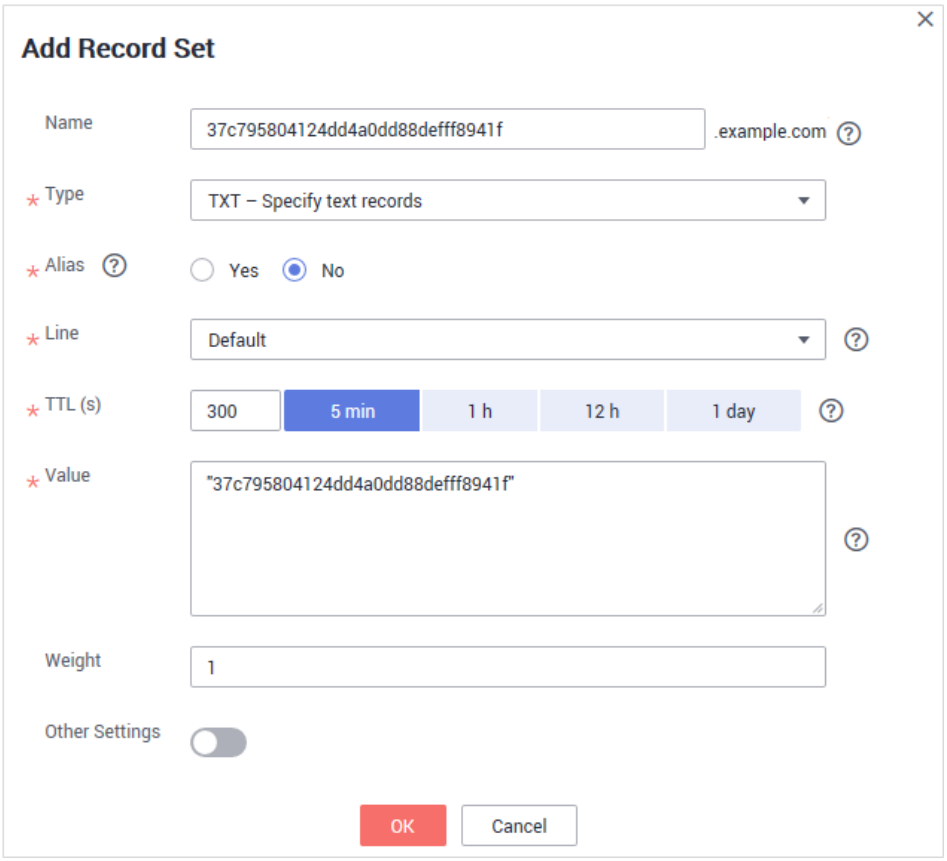
Copyright © Huawei Technologies Co., Ltd.

Figure 9-4 DNS page



2. In the upper right corner of the page, click **Add Record Set**. The **Add Record Set** page is displayed. **Figure 9-5** shows an example.
   - **Name**: TXT record copied in **Step 1.4**.
   - **Type**: Select **TXT – Specify text records**.
   - **Alias**: Select **No**.
   - **Line**: **Default**
   - **TTL (s)**: The recommended value is **5 min**. A larger TTL value will make it slower for synchronization and update of DNS records.
   - **Value**: Add quotation marks to the TXT record copied in **Step 1.4** and paste them in the text box, for example, **TXT record**.
   - Keep other settings unchanged.

Figure 9-5 Adding a record set



3. Click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Step 4 (Optional) Ping the IP address of your domain name to check whether the new DNS settings take effect.

NOTE

It takes some time for the new DNS settings to take effect. If ping fails, wait for 5 minutes and ping again.

----End

Dedicated/ELB Mode WAF Configuration

Perform the following steps to complete configurations on HUAWEI CLOUD CDN:

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, choose **Storage** > **CDN**.

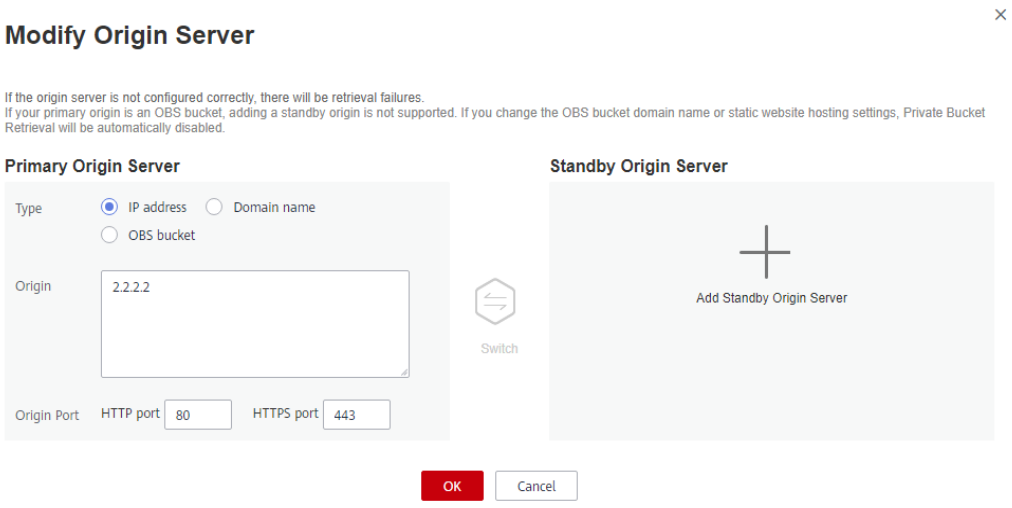
Step 4 In the navigation pane on the left, choose **Domains**.

Step 5 In the domain list, click the domain name you want to modify or click **Settings** in the **Operation** column.

Step 6 Click the **Basic Settings** tab. In the **Origin Server Settings** area, click **Edit**.

Step 7 In the **Modify Origin Server** dialog box displayed, modify the IP address of the origin server. Figure 9-6 shows an example.

Figure 9-6 Modify Origin Server



 Copyright © Huawei Technologies Co., Ltd.

NOTICE

- If you use a dedicated WAF instance, enter the **EIP bound to the load balancer** in the **Origin** text box.
- If you use a load-balancing WAF instance, enter the **EIP bound to the load balancer configured for the WAF instance** in the **Origin** text box.

Step 8 Click **OK**.

----End

Verification

If **Access Status** is **Accessible**, the traffic destined for your website domain name or IP address is routed to WAF.

NOTICE

If WAF detects 20 access requests to a website within 5 minutes, WAF considers that the website has been successfully connected to WAF.

If a domain name fails to be connected to WAF, its access status is **Inaccessible**. To fix this issue, see **Why Is the Access Status of a Domain Name or IP Address Inaccessible?**

Copyright © Huawei Technologies Co., Ltd.

10 Combining AAD and WAF to Get All-Round Protection

How the Combination Works

- **Advanced Anti-DDoS (AAD)** works as a proxy and uses AAD IP address to forward requests to origin servers. All public network traffic is diverted to the AAD IP address so that the origin server is hidden from the public. This protects origin servers from DDoS attacks.

  Objects supported by AAD: domain names of web applications on HUAWEI CLOUD, other cloud platforms, or on-premises data centers
- 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).

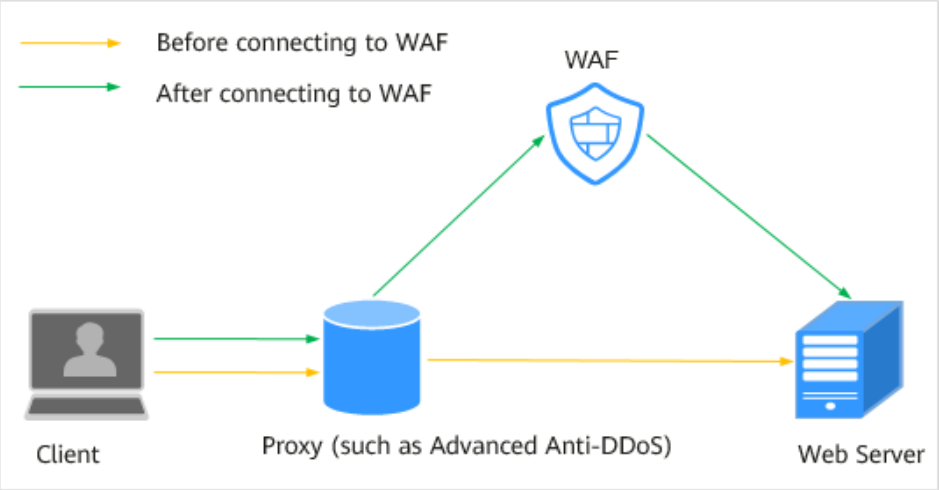
  WAF offers the cloud, dedicated, and ELB mode to protect websites. You can add either domain names or IP addresses to WAF. Before you start, get familiar with the following differences:

  – Cloud mode: protects your web applications on HUAWEI CLOUD, other cloud platforms, or on-premises data centers through domain names.
  – Dedicated or ELB mode: protects your web applications on HUAWEI CLOUD through domain names or IP addresses.

You can deploy both AAD and WAF to protect your websites hosted on HUAWEI CLOUD, other clouds, or in on-promises data centers. The combination of AAD and WAF can protect your website against DDoS attacks (such as NTP flood, SYN flood, ACK flood, ICMP flood, and HTTP Get flood attacks), web application attacks (such as SQL injection, cross-site scripting, web shells, command/code injection, file inclusion, sensitive file access, third-party application vulnerability attacks, CC attacks, malicious crawler scanning, and cross-site request forgery). **Figure 10-1** shows the configuration.

 Copyright © Huawei Technologies Co., Ltd.

Figure 10-1 WAF configuration when a proxy is used



If you configure AAD and WAF for your website, website traffic goes to AAD first. AAD scrubs incoming traffic and forwards clean traffic to WAF. WAF blocks attacks and forwards only the normal traffic to the origin server. In this way, two layers of protection are implemented on your website.



The configurations are as follows:

- Cloud mode

  Resolve the website domain name to AAD and change the AAD back-to-source IP address to WAF CNAME record. To prevent others from configuring your domain names on WAF in advance (this will cause interference on your domain name protection), add the subdomain name and TXT record on your DNS management platform.

- Dedicated mode

  Point the website domain name to AAD and change the AAD back-to-source IP address to the EIP bound to the load balancer configured for your dedicated WAF instance.

- ELB mode

  Resolve the website domain name to AAD and change the AAD back-to-source IP address to the EIP bound to the load balancer configured for the dedicated WAF instance.

Prerequisites

You have **purchased an AAD instance**, **connected your website service to the instance**, and completed the configurations shown in **Table 10-1**.

 Copyright © Huawei Technologies Co., Ltd.

Table 10-1 Configurations required in different WAF modes

Deployment Mode	Description
Cloud mode	1. You have **purchased a cloud WAF instance**. 2. You have **added the website domain name to your cloud WAF instance** and configured other details, including origin server IP address and port. 3. You have obtained the permissions from the DNS service provider to add domain names. 4. (Optional) You have whitelisted WAF back-to-source IP addresses. If non-HUAWEI CLOUD security software is used on the origin server, whitelist the WAF back-to-source IP addresses to prevent normal traffic from being blocked. For details, see **Configuring an Access Control Policy on an ECS or ELB to Protect Origin Servers**. **NOTICE** To ensure that the WAF policy takes effect for the real source IP address, ensure that **Yes** is selected for **Proxy Configured** when you add the domain name to WAF. For details, see **Viewing Basic Information**
Dedicated mode	1. You have **purchased a dedicated WAF instance**. 2. You have **added website domain name to your dedicated WAF instance** and configured other details, including origin server IP address and port. 3. You have **configured a load balancer for the dedicated WAF instance**. 4. You have **bound an EIP to the load balancer**. 5. You have **whitelisted back-to-source IP addresses of dedicated WAF instances**.
ELB mode	1. You have **purchased a load-balancing WAF instance**. 2. You have **added the domain name to the load-balancing WAF instance**. 3. You have **bound a load balancer** to the load-balancing WAF instance. 4. You have **whitelisted back-to-source IP addresses of the load-balancing WAF instance**.

 Copyright © Huawei Technologies Co., Ltd.

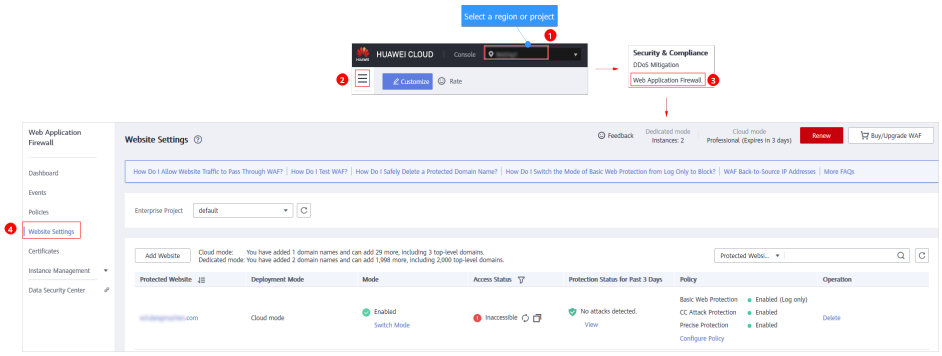
Cloud WAF Configuration

The methods to configure the DNS server are similar. The following uses HUAWEI CLOUD AAD as an example.

Step 1 Obtain settings of **CNAME**, **Subdomain Name**, and **TXT Record**.

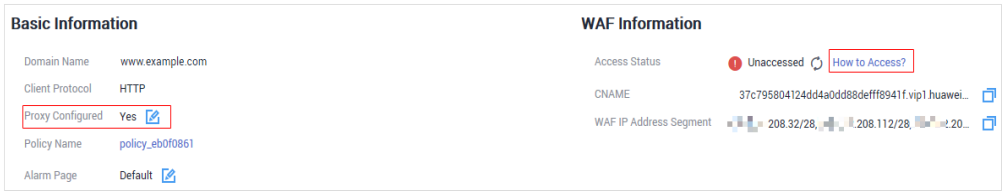
1. Log in to the management console.
2. Go to the **Website Settings** page by following the steps shown in **Figure 10-2**.

Figure 10-2 Accessing to the Website Settings page



3. In the **Protected Website** column, click the domain name you want to go to the **Basic Information** page.
4. On the page for configuring basic domain information, click  in the row where the CNAME is located to copy **CNAME**. In the row of **Access Status**, click **How to Access**. In the **Access Guide** dialog box, copy **Subdomain Name** and **TXT Record**.

Figure 10-3 Domain name access information

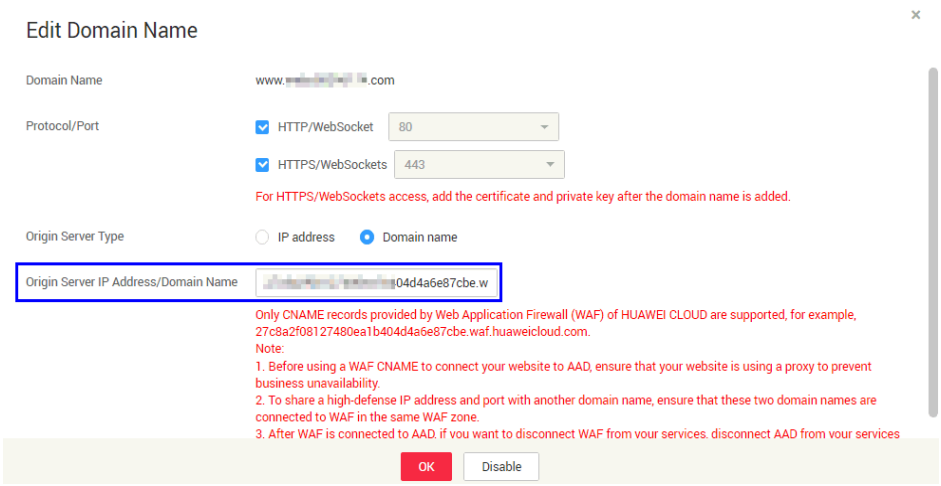


Step 2 Change the AAD back-to-source IP address.

1. Click  at the top of the page and choose **Security & Compliance** > **DDoS Mitigation**. In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Domain Name Access** to go to the domain name configuration page.
2. In the **Operation** column of the target domain name, click **Edit**. On the displayed page, set **Origin Server IP Address/Domain Name** to the copied WAF CNAME record. **Figure 10-4** shows an example.

Copyright © Huawei Technologies Co., Ltd.

Figure 10-4 Domain configuration



3. Click **OK**.

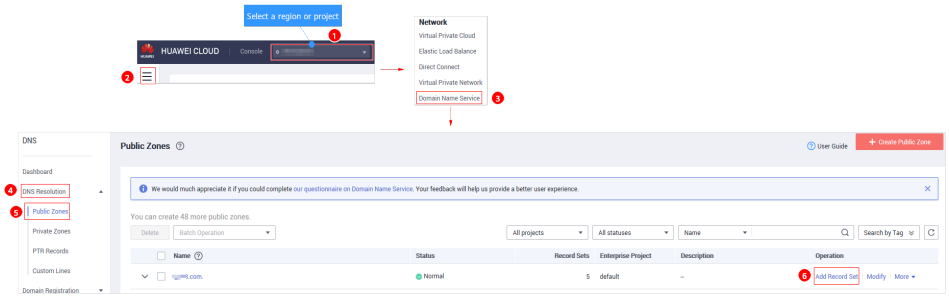
Step 3 (Optional) Add a WAF subdomain name and TXT record at your DNS provider.

NOTE

To prevent others from configuring your domain names on WAF in advance (this will cause interference on your domain name protection), this step is recommended.

1. Access the DNS resolution page, as shown in **Figure 10-5**.

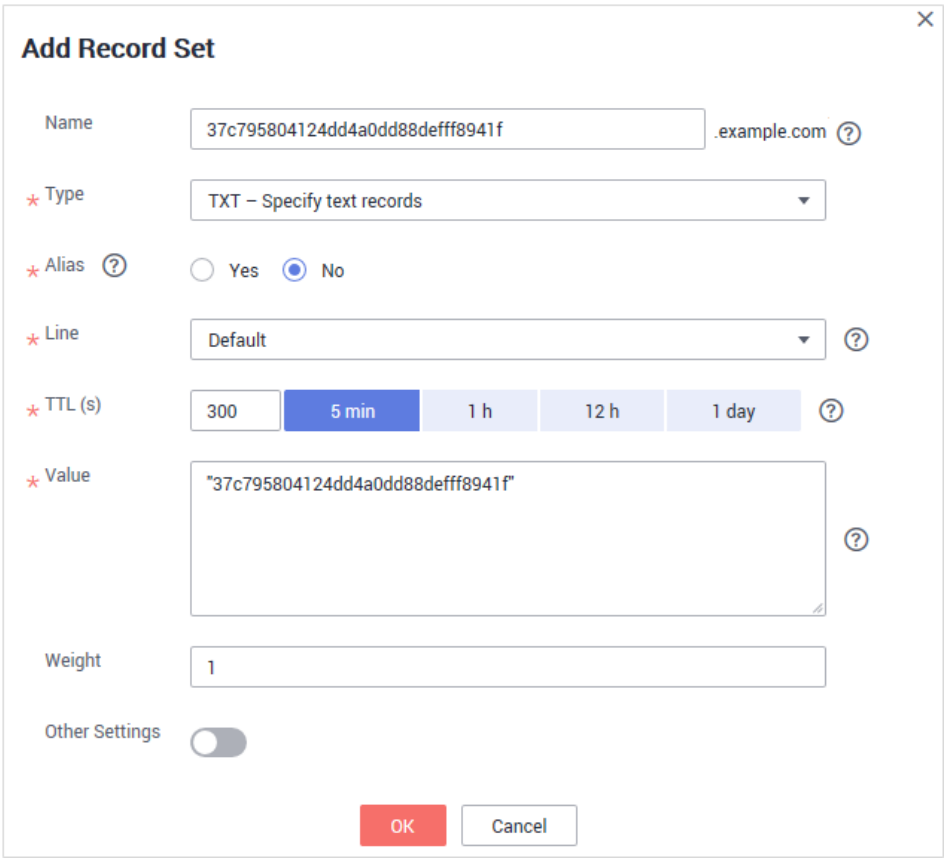
Figure 10-5 DNS page



2. In the upper right corner of the page, click **Add Record Set**. The **Add Record Set** page is displayed. **Figure 10-6** shows an example.
   - **Name**: TXT record copied in **Step 1.4**.
   - **Type**: Select **TXT – Specify text records**.
   - **Alias**: Select **No**.
   - **Line**: **Default**
   - **TTL (s)**: The recommended value is **5 min**. A larger TTL value will make it slower for synchronization and update of DNS records.
   - **Value**: Add quotation marks to the TXT record copied in **Step 1.4** and paste them in the text box, for example, **TXT record**.
   - Keep other settings unchanged.

 Copyright © Huawei Technologies Co., Ltd.

Figure 10-6 Adding a record set



3. Click **OK**.

Step 4 (Optional) Ping the IP address of your domain name to check whether the new DNS settings take effect.

NOTE

It takes some time for the new DNS settings to take effect. If ping fails, wait for 5 minutes and ping again.

----End

Dedicated/ELB WAF Configuration

Perform the following steps to complete configurations on HUAWEI CLOUD AAD:

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 & Compliance** > **DDoS Mitigation**.

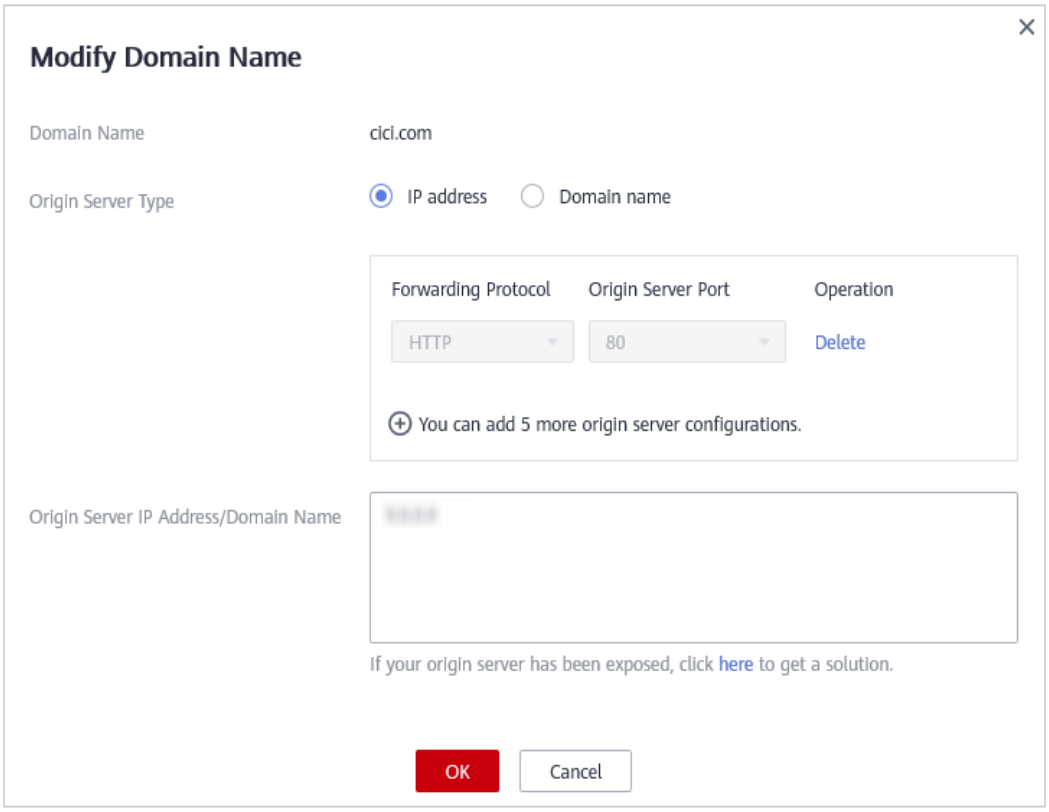
Step 4 In the navigation pane on the left, choose **Advanced Anti-DDoS** > **Domain Name Access** to go to the **Domain Name Access** page.

Step 5 In the row containing the domain name you want, click **Modify** in the **Operation** column.

 Copyright © Huawei Technologies Co., Ltd.

Step 6 In the **Modify Domain Name** dialog box, change the origin server IP address. **Figure 10-7** shows an example.

Figure 10-7 Changing the origin server IP address



NOTICE

- If you use a dedicated WAF instance, enter the **EIP bound to the load balancer** in the **Origin** text box.
- If you use a load-balancing WAF instance, enter the **EIP bound to the load balancer configured for the WAF instance** in the **Origin** text box.

Step 7 Click **OK**.

----End

Verification

If **Access Status** is **Accessible**, the traffic destined for your website domain name or IP address is routed to WAF.

NOTICE

If WAF detects 20 access requests to a website within 5 minutes, WAF considers that the website has been successfully connected to WAF.

 Copyright © Huawei Technologies Co., Ltd.

If a domain name fails to be connected to WAF, its access status is **Inaccessible**. To fix this issue, see **Why Is the Access Status of a Domain Name or IP Address Inaccessible?**

 Copyright © Huawei Technologies Co., Ltd.

11 Obtaining the Client IP Address

A client IP address refers to an IP address of a visitor (or the device a visitor uses to initiate the request). Sometimes, a web application needs to require the client IP address. For example, a voting system needs to obtain the client IP addresses to ensure that each client casts only once.

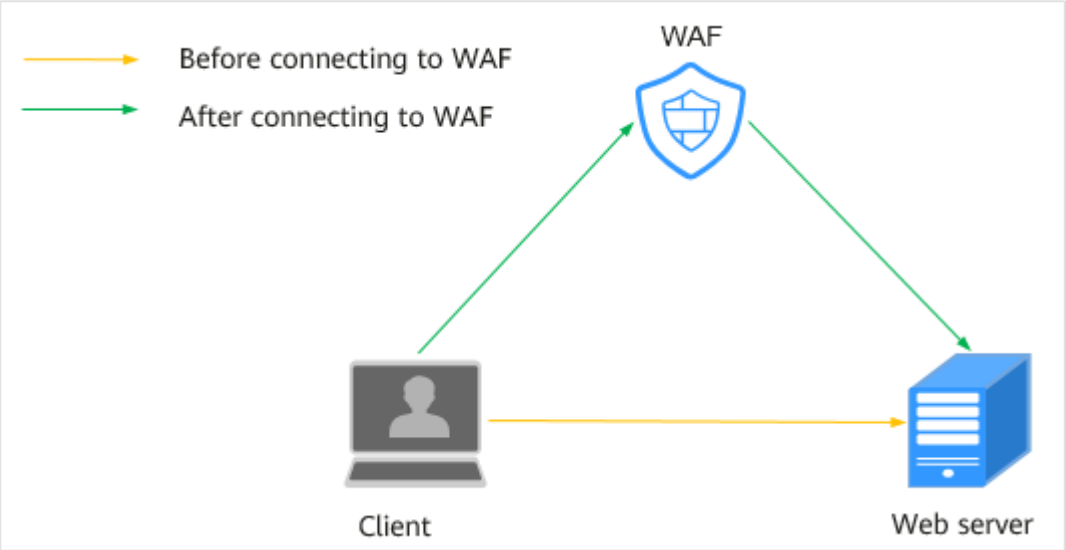
You can obtain the client IP address directly from WAF when your website is connected to WAF. You can also obtain the client IP address by configuring the website server.

The following describes how to obtain the client IP address from WAF and how to configure different types of web application servers, including Tomcat, Apache, Nginx, IIS 6, and IIS 7, to obtain the client IP address.

Background

Generally, a browser request does not directly reach the web server. Proxy servers, such as CDN, WAF, and advanced anti-DDoS, may be deployed between the browser and the origin server. Using WAF as an example, see **Figure 11-1**.

Figure 11-1 WAF deployment diagram



 Copyright © Huawei Technologies Co., Ltd.

NOTE

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

In this case, the access request may be forwarded by multiple layers of security or acceleration proxies before reaching the origin server. So, how does the server obtain the real IP address of the client that initiates the request?

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

Then, you can obtain the client IP address from the **X-Forwarded-For** field, the first IP address in which is the client IP address.

Obtaining the Client IP Address from WAF

After a website is connected to WAF, WAF is deployed between the client and server as a reverse proxy to protect the website. You can use either of the following methods to obtain the client IP address:

- Using the **X-Forwarded-For** field to obtain the client IP address

  The client IP address is placed in the **X-Forwarded-For** HTTP header field. The format is as follows:

  ```
  X-Forwarded-For: Client IP address,Proxy 1-IP address,Proxy 2-IP address,...
  ```

  NOTE

  The first IP address included in the **X-Forwarded-For** field is the client IP address.

  The methods to obtain the **X-Forwarded-For** field by invoking the SDK interface in different programming languages are as follows:

  - **ASP**

    ```
    Request.ServerVariables("HTTP_X_FORWARDED_FOR")
    ```

  - **ASP.NET(C#)**

    ```
    Request.ServerVariables["HTTP_X_FORWARDED_FOR"]
    ```

  - **PHP**

    ```
    $_SERVER["HTTP_X_FORWARDED_FOR"]
    ```

  - **JSP**

    ```
    request.getHeader("HTTP_X_FORWARDED_FOR")
    ```

- Using the **X-Real-IP** field to obtain the client IP address (modifications caused by reverse proxies is considered)

  The methods to obtain the **X-Real-IP** field by invoking the SDK interface in different programming languages are as follows:

  - **ASP**

    ```
    Request.ServerVariables("HTTP_X_REAL_IP")
    ```

  - **ASP.NET(C#)**

    ```
    Request.ServerVariables["HTTP_X_REAL_IP"]
    ```

  - **PHP**

 Copyright © Huawei Technologies Co., Ltd.

```
$_SERVER["HTTP_X_REAL_IP"]
```

- **JSP**

```
request.getHeader("HTTP_X_REAL_IP")
```

How Does Tomcat Obtain the Client IP Address from Access Logs?

If Tomcat is deployed on your origin server, you can enable the X-Forwarded-For function of Tomcat to obtain the client IP address.

Step 1 Open the **server.xml** file in the **tomcat/conf/** directory. Partial information about the AccessLogValve logging function is as follows:

```
<Host name="localhost"  appBase="webapps" unpackWARs="true" autoDeploy="true">
      <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
           prefix="localhost_access_log." suffix=".txt"
           pattern="%h %l %u %t "%r" %s %b" />
```

Step 2 Add **%{X-Forwarded-For}i** to **pattern**. Part of the modified **server.xml** file is as follows:

```
<Host name="localhost"  appBase="webapps" unpackWARs="true" autoDeploy="true">
      <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
           prefix="localhost_access_log." suffix=".txt"
           pattern="%{X-Forwarded-For}i %h %l %u %t "%r" %s %b" />
</Host>
```

Step 3 View the **localhost_access_log** file to obtain the client IP address from the **X-Forwarded-For** field.

----End

How Does Apache Obtain the Client IP Address from Access Logs?

If Apache is deployed on your origin server, you can run the commands to install third-party module mod_rpaf of Apache, and modify the **http.conf** file to obtain the client IP address.

Step 1 Run the following commands to install third-party module mod_rpaf of Apache:

```
wget https://github.com/gnif/mod_rpaf/archive/v0.6.0.tar.gz
tar xvfz mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/usr/local/apache/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
```

Step 2 Open the **httpd.conf** configuration file and modify the file content as follows:

```
LoadModule rpaf_module   modules/mod_rpaf-2.0.so ##Load module mod_rpaf.
<IfModule mod_rpaf.c>
RPAFenable On
RPAFsethostname On
RPAFproxy_ips 127.0.0.1 <Reverse proxy IP address>
RPAFheader X-Forwarded-For
</IfModule>
```

Step 3 Define the log format.

```
LogFormat "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" common
```

Step 4 Enable customized logs.

```
CustomLog"[Apache server directory]/logs/$access.log"common
```

Step 5 Restart the Apache server for the configuration to take effect.

```
/[Apache server directory]/httpd/bin/apachectl restart
```

 Copyright © Huawei Technologies Co., Ltd.

Step 6 View the **access.log** file to obtain the client IP address from the **X-Forwarded-For** field.

----End

How Does Nginx Obtain the Client IP Address from Access Logs?

If an Nginx reverse proxy is deployed on your origin server, you can configure location information on the Nginx reverse proxy so that the backend web server can use similar functions to obtain the client IP address

Step 1 Configure the following information in the corresponding location of the Nginx reverse proxy to obtain the information about the client IP address:

```
Location ^ /<uri> {
    proxy_pass  ....;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
}
```

Step 2 Enable the backend web server to use similar functions to obtain the client IP address.

```
request.getAttribute("X-Forwarded-For")
```

----End

How Does IIS 6 Obtain the Client IP Address from Access Logs?

If you have deployed an IIS 6 server on your origin server, you can install the **F5XForwardedFor.dll** plug-in and obtain the client IP address from the access logs recorded by the IIS 6 server.

Step 1 Download the **F5XForwardedFor** module.

Step 2 Copy the **F5XForwardedFor.dll** file in the **x86\Release** or **x64\Release** directory to a specified directory (for example, **C:\ISAPIFilters**) based on the operating system version of your server. Ensure that the IIS process has the read permission on the directory.

Step 3 Open the IIS manager, right-click the website that is currently open, and choose **Attribute** from the shortcut menu. The **Attribute** page is displayed.

Step 4 On the **Attribute** page, switch to **ISAPI filter** and click **Add**. In the dialog box that is displayed, configure the following information:

- **Filter Name**: Set this parameter to **F5XForwardedFor**.
- **Executable file**: Set this parameter to the full path of **F5XForwardedFor.dll**, for example, **C:\ISAPIFilters\F5XForwardedFor.dll**.

Step 5 Click **OK** to restart the IIS 6 server.

Step 6 View the access logs recorded by the IIS 6 server (the default log path is **C:\WINDOWS\system32\LogFiles**, and the IIS log file name extension is **.log**). You can obtain client IP address from the **X-Forwarded-For** field.

----End

Copyright © Huawei Technologies Co., Ltd.

How Does IIS 7 Obtain the Client IP Address from Access Logs?

If you have deployed an IIS 7 server on your origin server, you can install the **F5XForwardedFor.dll** module and obtain the client IP address from the access logs recorded by the IIS 7 server.

Step 1 Download the **F5XForwardedFor** module.

Step 2 Copy the **F5XFFHttpModule.dll** and **F5XFFHttpModule.ini** files in the **x86\Release** or **x64\Release** directory to a specified directory (for example, **C:\x_forwarded_for\x86** or **C:\x_forwarded_for\x64**) based on the operating system version of your server. Ensure that the IIS process has the read permission for the directory.

Step 3 On the server home page, double-click **Modules** to go to the **Modules** page.

Step 4 Click **Configure Native Module**. In the dialog box displayed, click **Register**.

Step 5 In the displayed dialog box, register the downloaded DLL file according to the operating system, and then click **OK**.

- x86 operating system: registration module **x_forwarded_for_x86**
  - **Name**: **x_forwarded_for_x86**
  - **Path**: **C:\x_forwarded_for\x86\F5XFFHttpModule.dll**
- x86 operating system: registration module **x_forwarded_for_x64**
  - **Name**: **x_forwarded_for_x64**
  - **Path**: **C:\x_forwarded_for\x64\F5XFFHttpModule.dll**

Step 6 After the registration is complete, select the newly registered module (**x_forwarded_for_x86** or **x_forwarded_for_x64**) and click **OK**.

Step 7 In **ISAPI and CGI restriction**, add the registered DLL files by operating system and change **Restriction** to **Permitting**.

- x86 operating system:
  - **ISAPI or CGI path**: **C:\x_forwarded_for\x86\F5XFFHttpModule.dll**
  - **Description**: **x86**
- x64 operating system:
  - **ISAPI or CGI path**: **C:\x_forwarded_for\x64\F5XFFHttpModule.dll**
  - **Description**: **x64**

Step 8 Restart the IIS 7 server and wait for the configuration to take effect.

Step 9 View the access logs recorded by the IIS 7 server (the default log path is **C:\WINDOWS\system32\LogFiles**, and the IIS log file name extension is **.log**). You can obtain the client IP address from the **X-Forwarded-For** field.

----End

 Copyright © Huawei Technologies Co., Ltd.

A Change History

Released On	Description
2021-07-29	This issue is the thirty-sixth official release. Added descriptions of how to verify the configuration in **Combining CDN and WAF to Get Improved Protection and Load Speed** and **Combining AAD and WAF to Get All-Round Protection**.
2021-07-20	This issue is the thirty-fifth official release. Modified the entry to the management console.
2021-06-25	This issue is the thirty-fourth official release. Optimized descriptions in **Connecting a Domain to WAF for Websites with no Proxy Used**.
2021-06-08	This issue is the thirty-third official release. • Optimized the descriptions of prerequisites in **Combining CDN and WAF to Get Improved Protection and Load Speed**. • Optimized the descriptions of prerequisites in **Combining AAD and WAF to Get All-Round Protection**.
2021-05-20	This issue is the thirty-second official release. Added the configuration policies for dedicated and load-balancing WAF instances in **Combining AAD and WAF to Get All-Round Protection**.
2021-05-14	This issue is the thirty-first official release. Added the configuration policies for dedicated and load-balancing WAF instances in **Combining CDN and WAF to Get Improved Protection and Load Speed**.
2021-04-08	This issue is the thirtieth official release. Optimized descriptions in **Connecting a Domain to WAF for Websites with no Proxy Used**.

 Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2021-03-19	This is the twenty-ninth official release. Optimized descriptions in **Configuring the Minimum TLS Version and Cipher Suite to Better Secure Connections**.
2020-11-27	This issue is the twenty-eighth official release. • Optimized descriptions in **Configuring an Access Control Policy on an ECS or ELB to Protect Origin Servers**. • Optimized descriptions in **Handling False Alarms to Get Improved Basic Web Protection**. • Optimized descriptions in **Obtaining the Client IP Address**.
2020-11-20	This issue is the twenty-seventh official release. • Optimized descriptions in **Configuring the Minimum TLS Version and Cipher Suite to Better Secure Connections**. • Optimized descriptions in **Configuring Anti-Crawler Rules to Prevent Crawler Attacks**.
2020-08-17	This issue is the twenty-sixth official release. Optimized descriptions in **Obtaining the Client IP Address**.
2020-05-14	This issue is the twenty-fifth official release. Optimized descriptions in **Configuring the Minimum TLS Version and Cipher Suite to Better Secure Connections**.
2020-04-16	This issue is the twenty-fourth official release. Optimized descriptions.
2020-04-02	This issue is the twenty-third official release. Updated some screenshots.
2020-02-27	This issue is the twenty-second official release. Updated screenshots and descriptions in **Handling False Alarms to Get Improved Basic Web Protection**
2020-02-14	This issue is the twenty-first official release. Added section **Apache Dubbo Deserialization Vulnerability**.
2020-01-03	This issue is the twentieth official release. Modified the title in **Obtaining the Client IP Address**.

Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2019-12-19	This is the nineteen official release. • Added the method for the IIS server to obtain the real IP address of a visitor in **Handling False Alarms to Get Improved Basic Web Protection**. • Optimized descriptions in **Combining CDN and WAF to Get Improved Protection and Load Speed**.
2019-12-16	This issue is the eighteenth official release. Updated the operation entry figure.
2019-12-05	This is the seventeenth official release. Optimized descriptions in **Obtaining the Client IP Address**.
2019-10-21	This is the sixteenth official release. • Optimized descriptions in **Configuring the Minimum TLS Version and Cipher Suite to Better Secure Connections**. • Optimized the description in **CC Attack Defense** • Optimized descriptions in **Handling False Alarms to Get Improved Basic Web Protection**. • Optimized descriptions in **Combining AAD and WAF to Get All-Round Protection**. • Optimized descriptions in **Combining CDN and WAF to Get Improved Protection and Load Speed**.
2019-09-06	This is the fifteenth official release. Added section **DoS Vulnerability in the Open-Source Component Fastjson**.
2019-09-04	This is the fourteenth official release. Optimized descriptions in **Connecting a Domain to WAF for Websites with no Proxy Used**.
2019-08-30	This is the thirteenth official release. Optimized descriptions in **Combining CDN and WAF to Get Improved Protection and Load Speed**.
2019-08-27	This is the twelfth official release. Optimized descriptions in **Configuring Anti-Crawler Rules to Prevent Crawler Attacks**.
2019-08-01	This is the eleventh official release. Added section **Combining CDN and WAF to Get Improved Protection and Load Speed**.

Copyright © Huawei Technologies Co., Ltd.

Released On	Description
2019-07-12	This issue is the tenth official release. Added section **Remote Code Execution Vulnerability of Fastjson**.
2019-06-21	This is the ninth official release. Added section **Obtaining the Client IP Address**.
2019-06-04	This is the eighth official release. • Added section **Handling False Alarms to Get Improved Basic Web Protection**. • Added section **Domain Setup**.
2019-05-16	This is the seventh official release. • Added section **Configuring an Access Control Policy on an ECS or ELB to Protect Origin Servers**. • Added section **Configuring Basic Web Protection**.
2019-05-05	This is the sixth official release. Optimized descriptions in **Configuring the Minimum TLS Version and Cipher Suite to Better Secure Connections**.
2019-04-28	This is the fifth official release. Added **Configuring the Minimum TLS Version and Cipher Suite to Better Secure Connections**.
2019-04-23	This is the fourth official release. • Added section **Oracle WebLogic wls9-async Deserialization Remote Command Execution Vulnerability (CNVD-C-2019-48814)**. • Optimized the description in **CC Attack Defense** • Optimized descriptions in **Configuring Anti-Crawler Rules to Prevent Crawler Attacks**.
2018-11-08	This is the third official release. Optimized some descriptions.
2018-10-15	This is the second official release. Updated screenshots and descriptions.
2018-05-11	This is the first official release.

Copyright © Huawei Technologies Co., Ltd.