

# Web Application Firewall

## Getting Started

**Issue** 01  
**Date** 2024-07-19



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.**

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

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

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

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

## **Huawei Cloud Computing Technologies Co., Ltd.**

Address: Huawei Cloud Data Center Jiaoxinggong Road  
Qianzhong Avenue  
Gui'an New District  
Gui Zhou 550029  
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

---

# Contents

---

<b>1 Before You Start.....</b>	<b>1</b>
<b>2 Blocking Heavy-Traffic CC Attacks Through CC Attack Protection Rules.....</b>	<b>4</b>
<b>3 Blocking Malicious Traffic Through IP Address Blacklist or Whitelist Rules.....</b>	<b>12</b>
<b>4 Common Tasks.....</b>	<b>17</b>

# 1 Before You Start

---

Web Application Firewall (WAF) examines HTTP/HTTPS requests to identify and block malicious traffic, keeping your core service data secure and web server performance stable. This document describes how to quickly use WAF to protect your workloads.

## Overview

A glance at WAF:

- [What is WAF?](#)
- [WAF Editions and Their Differences](#)
- [Features](#)
- [How Is WAF Billed?](#)
- [What Types of Protections Rule Can WAF Provide?](#)

## Step 1: Buy a WAF Instance

1. [Log in to Huawei Cloud management console](#). On the console page, choose **Security & Compliance > Web Application Firewall**.
2. In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, select a WAF mode.

WAF provides three access modes, CNAME and ELB access modes for cloud WAF and dedicated access mode for dedicated WAF. For their differences, see [Edition Differences](#).

### – [Buying a Cloud WAF Instance](#)

#### NOTE

- To use ELB-access cloud WAF, you need to [submit a service ticket](#) to enable it for you first. ELB-access cloud WAF is available in some regions. For details, see [Functions](#).
  - If you want to use the ELB access mode, make sure you are using standard, professional, or platinum cloud WAF. When you are using cloud WAF, the quotas for the domain name, QPS, and rule extension packages are shared between the ELB access and CNAME access modes.
- ### – [Buying a Dedicated WAF Instance](#)

## Step 2: Connect a Website to WAF

After buying a WAF instance, you need to add it to WAF, or WAF cannot check HTTP or HTTPS requests.

Access Mode	Protection Scenario	Reference Document
Cloud Mode - CNAME Access	<ul style="list-style-type: none"><li>Service servers are deployed on any cloud or in on-premises data centers.</li><li>Protected objects: domain names</li></ul>	<a href="#">Connection a Website to WAF (Cloud Mode - CNAME Access)</a>
Cloud - ELB Access	<ul style="list-style-type: none"><li>Service servers are deployed on Huawei Cloud. This mode is suitable for large enterprise websites having high security requirements on service stability.</li><li>Protected objects: domain names and IP addresses</li></ul>	<a href="#">Connecting WAF to WAF Protection (Cloud Mode - ELB Access)</a>
Dedicated mode	<ul style="list-style-type: none"><li>Service servers are deployed on Huawei Cloud. This mode is suitable for large enterprise websites that have a large service scale and have customized security requirements.</li><li>Protected objects: domain names and IP addresses</li></ul>	<a href="#">Connecting a Website to WAF (Dedicated Mode)</a>

## Step 3: Configure a Protection Policy

After your website is connected to WAF, WAF applies a protection policy to your website and enables **General Check** (with **Protective Action** set to **Log only** and **Protection Level** set to **Medium**) in **Basic Web Protection** and enables **Scanner check** (with **Protective Action** set to **Log only**) in **Anti-Crawler** protection.

- If you do not have special security requirements, you can retain the default settings and view WAF protection logs on the **Events** page at any time. For details, see [Viewing Protection Event Logs](#).
- If your website were under attacks, you can configure a custom protection policy based on attack details on the **Dashboard** and **Events** pages. For details, see [Adding Rules to One or More Policies](#).

## Step 4: View Protection Logs

On the **Events** page, view the protection details of the configured protection policy and handle the source IP address.

- To quickly whitelist a source IP address, locate the row that contains the corresponding event, choose **Handle as False Alarm** in the **Operation** column, and configure a global protection whitelist rule.
- To block or allow a source IP address, add it to an IP address blacklist or whitelist.

For details, see [Handling False Alarms](#).

# 2 Blocking Heavy-Traffic CC Attacks Through CC Attack Protection Rules

---

A CC attack protection rule can limit access to your website based on the IP address or cookie of a visitor. If the number of access requests from a visitor exceeds the threshold you configure, you can require the visitor to enter a verification code to continue the access, or block the request and return a custom page of certain type to the visitor.

In heavy-traffic CC attacks, a single zombie server can send far more packets than a common user does. In this scenario, a rate limiting rule is the most effective method to fend off this type of CC attacks.

WAF provides different website access modes: cloud CNAME access mode, cloud load balancer access mode, and dedicated mode. The application scenarios of each access mode are as follows:

- Cloud - CNAME access
  - Service servers are deployed on any cloud or in on-premises data centers.
  - Protected objects: domain names
- Cloud - Load balancer access mode
  - Service servers are deployed on Huawei Cloud.  
This mode suitable for large enterprise websites having high security requirements on service stability.
  - Protected objects: domain names and IP addresses
- Dedicated mode
  - Service servers are deployed on Huawei Cloud.  
This mode is suitable for large enterprise websites that have a large service scale and have customized security requirements.
  - Protected objects: domain names and IP addresses

This topic describes how to configure an IP-based CC attack protection rule to limit access traffic. We use WAF cloud CNAME access mode in this example.

## Process

Procedure	Description
<b>Preparations</b>	Sign up for a HUAWEI ID, enable Huawei Cloud services, top up your account, and assign WAF permissions to the account.
<b>Step 1: Buy WAF</b>	Purchase WAF and select the region and WAF mode.
<b>Step 2: Add a Website to WAF</b>	Add the website you want to protect to WAF for traffic inspection and forwarding.
<b>Step 3: Enable CC Attack Protection</b>	Configure and enable CC attack protection rules to mitigate CC attacks against the protected website.

## Preparations

- Before purchasing WAF, create a Huawei account and subscribe to Huawei Cloud. For details, see [Registering a HUAWEI ID and Enabling HUAWEI CLOUD Services](#) and [Real-Name Authentication](#).  
If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
- Make sure that your account has sufficient balance, or you may fail to pay to your WAF orders.
- Make sure your account has WAF permissions assigned. For details, see [Creating a User Group and Granting Permissions](#).

**Table 2-1** System policies supported by WAF

Role/Policy Name	Description	Category	Dependencies
WAF Administrator	Administrator permissions for WAF	System-defined role	Dependent on the <b>Tenant Guest</b> and <b>Server Administrator</b> roles. <ul style="list-style-type: none"> <li><b>Tenant Guest:</b> A global role, which must be assigned in the global project.</li> <li><b>Server Administrator:</b> A project-level role, which must be assigned in the same project.</li> </ul>



Role/Policy Name	Description	Category	Dependencies
WAF FullAccess	All permissions for WAF	System-defined policy	None.
WAF ReadOnlyAccess	Read-only permissions for WAF.	System-defined policy	

## Step 1: Buy the Standard Edition Cloud WAF

This topic covers how to buy the standard edition cloud WAF, connect a website to WAF in cloud CNAME access mode, and configure and enable CC attack protection rules.

1. [Log in to Huawei Cloud management console.](#)
2. On the management console page, choose **Security & Compliance > Web Application Firewall**.
3. In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, select a WAF mode.
  - **Region:** Select the region nearest to your services WAF will protect.
  - **Edition:** Select **Standard**.
  - **Expansion Package** and **Required Duration:** Retain default settings.
4. Confirm the product details and click **Buy Now** in the lower right corner of the page.
5. Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.
6. On the payment page, select a payment method and pay for your order.

## Step 2: Add a Website to WAF

1. In the navigation pane on the left, choose **Website Settings**.
2. In the upper left corner of the website list, click **Add Website**.
3. Select **Cloud - CNAME** and click **Configure Now**.
4. On the **Add Domain Name** page, set the parameters by referring to [Figure 2-1](#).

**Figure 2-1 Add Domain Name**

**Basic Settings**

Protected Domain Name <sup>②</sup>  
 [Quick Add Domain Names Hosted on Cloud](#)

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

Website Name (Optional)

Website Remarks (Optional)

Protected Port <sup>②</sup>  
 [View Ports You Can Use](#)

<sup>③</sup> Standard ports 80 and 443 are the default ports reserved for HTTP and HTTPS protocols, respectively.

Server Configuration <sup>②</sup>

Client Protocol	Server Protocol	Server Address	Server Port	Weight	Operation
HTTP	HTTP	IPv4 <input type="text" value="Enter a public IP ad"/>	80	1	Delete

[Add Address](#) Origin server addresses you can add: 49

Proxy Your Website Uses <sup>②</sup>

Layer-7 proxy
  Layer-4 proxy
  No proxy

**Table 2-2 Key parameters**

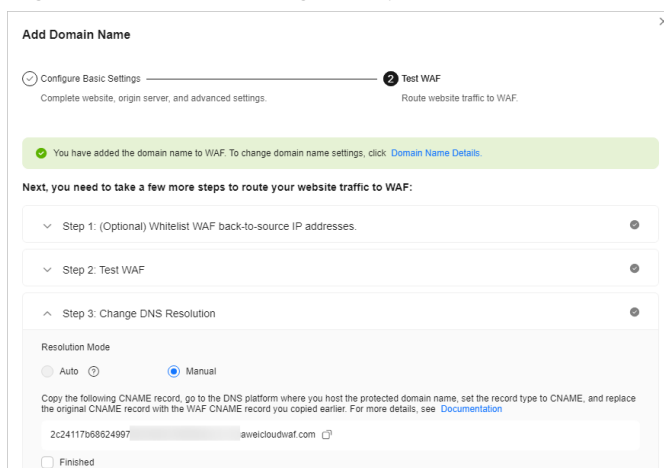
Parameter	Description	Example
Protected Domain Name	The domain name you want to add to WAF for protection.	www.example.com
Protected Port	The port over which the website service traffic goes. To protect port 80 or 443, select <b>Standard port</b> from the drop-down list.	Standard ports

Parameter	Description	Example
Server Configuration	<p>Server address configuration. You need to configure the client protocol, server protocol, server weights, server address, and server port.</p> <ul style="list-style-type: none"> <li>● <b>Client Protocol:</b> protocol used by a client to access a server. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>● <b>Server Protocol:</b> protocol used by WAF to forward client requests. The options are <b>HTTP</b> and <b>HTTPS</b>.</li> <li>● <b>Server Address:</b> public IP address (generally corresponding to the A record of the domain name configured on the DNS) or domain name (generally corresponding to the CNAME record of the domain name configured on the DNS) of the web server that a client accesses. The following IP address formats are supported: <ul style="list-style-type: none"> <li>– IPv4, for example, XX.XXX.1.1</li> <li>– IPv6, for example, fe80:0000:0000:0000:0000:0000:0000:0000</li> </ul> </li> <li>● <b>Server Port:</b> service port over which the WAF instance forwards client requests to the origin server.</li> <li>● <b>Weight:</b> Requests are distributed across backend origin servers based on the load balancing algorithm you select and the weight you assign to each server.</li> </ul>	<p><b>Client Protocol:</b> <b>HTTP.</b></p> <p><b>Server Protocol:</b> <b>HTTP</b></p> <p><b>Server Address:</b> XXX.XXX.1.1</p> <p><b>Server Port: 80</b></p>

Parameter	Description	Example
Proxy Your Website Uses	<ul style="list-style-type: none"> <li>• <b>Layer-7 proxy:</b> Web proxy products for layer-7 request forwarding are used, products such as anti-DDoS, CDN, and other cloud acceleration services.</li> <li>• <b>Layer-4 proxy:</b> Web proxy products for layer-4 forwarding are used, products such as anti-DDoS.</li> <li>• <b>No proxy:</b> No proxy products are deployed in front of WAF.</li> </ul> <p>In our example, no proxies are used.</p>	No proxy

5. Click **Next**. The basic information about the domain name is configured.

**Figure 2-2** Basic settings completed




6. Complete steps **Whitelist WAF Back-to-Source IP Addresses** and **Test WAF** as prompted.

7. Complete DNS resolution.

Configure the CNAME record on the DNS platform hosting your domain name. For details, contact your DNS provider.



The following uses Huawei Cloud DNS as an example to show how to configure a CNAME record. The following configuration is for reference only.

- a. Copy the CNAME value provided by WAF in **Figure 2-2**.
- b. Click  in the upper left corner of the page and choose **Networking > Domain Name Service**.
- c. In the navigation pane on the left, choose **Public Zones**.
- d. In the **Operation** column of the target domain name, click **Manage Record Set**. The **Record Sets** tab page is displayed.
- e. In the row containing the desired record set, click **Modify** in the **Operation** column.

- f. In the displayed **Modify Record Set** dialog box, change the record value.
  - **Name:** Domain name configured in WAF
  - **Type:** Select **CNAME-Map one domain to another**.
  - **Line:** **Default**
  - **TTL (s):** The recommended value is **5 min**. A larger TTL value will make it slower for synchronization and update of DNS records.
  - **Value:** Change it to the CNAME record copied in [7.a](#).
  - Keep other settings unchanged.
- g. Click **OK**.

### Step 3: Configure a CC Attack Protection Rule

**Configuration example:** You can configure such a CC rule to mitigate CC attacks. If an IP address accessed any path under the current domain name more than 1000 times within 30 seconds, this rule will block requests from the IP address for 10 hours. This rule can be used as a preventive configuration for common small and medium-sized websites

1. In the navigation pane on the left, choose **Policies**.
2. Click the name of the target policy to go to the protection configuration page.
3. In the **CC Attack Protection** area, enable it.
  -  : enabled
  -  : disabled
4. In the upper left corner of the **CC Attack Protection** rule list, click **Add Rule**. In the dialog box displayed, configure the CC attack protection rule by referring to [Figure 2-3](#).
  - **Rate Limit Mode:** Select **Source** and then **Per IP address** to distinguish a single web visitor based on IP addresses.
  - **Trigger:** At least one condition needs to be configured. The rule takes effect only when all conditions you configure are met.
  - Set other parameters based on your situation.

**Figure 2-3** Add CC Attack Protection Rule

**Add CC Attack Protection Rule**

Restrictions and precautions vary by mode. ?

\* Rule Name:

Rule Description:

\* Rate Limit Mode: **Source** | Destination

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

Per IP address |  Per user |  Other

\* Request Aggregation:

Keep this function enabled if you added a wildcard domain name to WAF so that requests to all domain names that match the wildcard domain are counted for triggering this rule. For example, if you added \*.a.com to WAF, requests to all matched domain names such as b.a.com and c.a.com are counted.

\* Trigger:

Field	Subfield	Logic	Content
Path	--	Prefix is	/login.php

\* Rate Limit:  requests  seconds  All WAF instances ?

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

\* Effective Date:  Immediate

\* Block Duration:  seconds

\* Block Page:  Default settings |  Custom

5. Confirm the configuration and click **Confirm**.

## Related Information

For more details, see [Configuring a CC Attack Protection Rule](#).

# 3 Blocking Malicious Traffic Through IP Address Blacklist or Whitelist Rules

By default, WAF allows access from all IP addresses. If you find that your website is accessed from malicious IP addresses, you can add a WAF blacklist or whitelist rule to block malicious IP addresses.

WAF provides different website access modes: cloud CNAME access mode, cloud load balancer access mode, and dedicated mode. The application scenarios of each access mode are as follows:

- Cloud - CNAME access
  - Service servers are deployed on any cloud or in on-premises data centers.
  - Protected objects: domain names
- Cloud - Load balancer access mode
  - Service servers are deployed on Huawei Cloud.  
This mode suitable for large enterprise websites having high security requirements on service stability.
  - Protected objects: domain names and IP addresses
- Dedicated mode
  - Service servers are deployed on Huawei Cloud.  
This mode is suitable for large enterprise websites that have a large service scale and have customized security requirements.
  - Protected objects: domain names and IP addresses

The following example shows you how to configure an IP address whitelist or blacklist rule. In this example, we use the WAF cloud load balancer access mode.

## Process

Procedure	Description
<b>Preparations</b>	Sign up for a HUAWEI ID, enable Huawei Cloud services, top up your account, and assign WAF permissions to the account.

Procedure	Description
<a href="#">Step 1: Buy the Standard Edition Cloud WAF</a>	Purchase WAF and select the region and WAF mode.
<a href="#">Step 2: Add a Website to WAF in Load Balancer Access Mode</a>	Add the website you want to protect to WAF for traffic inspection and forwarding.
<a href="#">Step 4: Configure an IP Address Blacklist or Whitelist Rule</a>	Add blacklist and whitelist rules to block malicious IP addresses.

## Preparations

- Before purchasing WAF, create a Huawei account and subscribe to Huawei Cloud. For details, see [Registering a HUAWEI ID and Enabling HUAWEI CLOUD Services](#) and [Real-Name Authentication](#).  
If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.
- Make sure that your account has sufficient balance, or you may fail to pay to your WAF orders.
- Make sure your account has WAF permissions assigned. For details, see [Creating a User Group and Granting Permissions](#).

**Table 3-1** System policies supported by WAF

Role/Policy Name	Description	Category	Dependencies
WAF Administrator	Administrator permissions for WAF	System-defined role	Dependent on the <b>Tenant Guest</b> and <b>Server Administrator</b> roles. <ul style="list-style-type: none"> <li><b>Tenant Guest:</b> A global role, which must be assigned in the global project.</li> <li><b>Server Administrator:</b> A project-level role, which must be assigned in the same project.</li> </ul>
WAF FullAccess	All permissions for WAF	System-defined policy	None.
WAF ReadOnlyAccess	Read-only permissions for WAF.	System-defined policy	



## Step 1: Buy the Standard Edition Cloud WAF

You can use the load balancer access mode only after you purchase the standard, professional, or platinum edition cloud WAF. The following describes how to buy the standard edition cloud WAF.

1. [Log in to Huawei Cloud management console.](#)
2. On the management console page, choose **Security & Compliance > Web Application Firewall**.
3. In the upper right corner of the page, click **Buy WAF**. On the purchase page displayed, select a WAF mode.
  - **Region:** Select the region nearest to your services WAF will protect.
  - **Edition:** Select **Standard**.
  - **Expansion Package** and **Required Duration:** Retain default settings.
4. Confirm the product details and click **Buy Now** in the lower right corner of the page.
5. Check the order details and read the *WAF Disclaimer*. Then, select the box and click **Pay Now**.
6. On the payment page, select a payment method and pay for your order.

### NOTE

After the purchase is complete, [submit a service ticket](#) to enable WAF cloud load balancer access mode.

## Step 2: Add a Website to WAF in Load Balancer Access Mode

**Step 1** In the navigation pane on the left, choose **Website Settings**.

**Step 2** In the upper left corner of the website list, click **Add Website**.

**Step 3** Select **Cloud - Load balancer** and click **Configure Now**.

**Step 4** On the **Add Domain Name** page, set the parameters by referring to [Figure 3-1](#).

- **ELB (Load Balancer):** Select an ELB load balancer. Make sure you have added the server address corresponding to the protected website to the ELB load balancer.
- **ELB Listener:** Select **All listeners**.
- **Domain Name:** Enter the domain name or IP address you want to protect. We use **www.example.com** in this example.
- **Policy:** **System-generated policy** is selected by default.

**Figure 3-1** Domain name settings

The screenshot shows a configuration form for domain name settings. It includes the following elements:

- ELB (Load Balancer):** A dropdown menu with the value 'elb-c00474594' and a refresh icon.
- ELB Listener:** Two buttons: 'All listeners' (highlighted in blue) and 'Specific listener' (greyed out).
- Website Name:** A text input field with the placeholder text 'Enter a custom name for the domain name.'
- Domain Name:** A text input field containing 'www.example.com'.
- Website Remarks:** An empty text input field.
- Policy:** A dropdown menu with a help icon and the value 'System-generated policy'.

**Step 5** Click **Confirm**.

----End

## Step 4: Configure an IP Address Blacklist or Whitelist Rule

**Step 1** In the navigation pane on the left, choose **Policies**.

**Step 2** Click the name of the target policy to go to the protection configuration page.

**Step 3** Choose **Blacklist and Whitelist** and enable it.

-  : enabled.
-  : disabled.

**Step 4** Above the blacklist and whitelist rule list, click **Add Rule** and configure a rule as shown in [Figure 3-2](#).

- **IP Address/Range/Group:** Select **IP address/range**. To block multiple IP addresses, select **Address group**.
- **IP Address/Range:** Configure the IP addresses or IP address ranges you want to block.
- **Protective Action:** Select **Block**.

**Figure 3-2** Blocking a specified ip address

**Add Blacklist or Whitelist Rule**

\* Rule Name

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

\* IP Address/Range

\* Protective Action

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

\* Apply  Immediate  Custom

Rule Description

**Confirm**

**Step 5** Click **Confirm**.

----End

## Related Information

For details, see [Configuring IP Address Blacklist and Whitelist Rules to Block or Allow Specified IP Addresses](#).

# 4 Common Tasks

WAF provides a series of common practices for you. These practices can help you start WAF protection for your workloads quickly.

**Table 4-1** Common practices

Practice		Description
Connecting a domain name to WAF	<a href="#">Connecting a Domain Name to WAF for Websites with no Proxy Used</a>	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.
	<a href="#">Combining CDN and WAF to Get Improved Protection and Load Speed</a>	The combination of CDN and WAF can protect websites on Huawei Cloud, other clouds, or on-premises and improve website response time.
	<a href="#">Combining WAF and Layer-7 Load Balancers to Protect Services over Any Ports</a>	This topic walks you through how to combine dedicated WAF instances and layer-7 load balancers to protect your services over non-standard ports that cannot be protected with WAF alone. For ports that can be protected with WAF, see <a href="#">Ports Supported by WAF</a> .
Protecting websites with WAF policies	<a href="#">Configuring CC Attack Protection</a>	This section guides you through configuring IP address-based rate limiting and cookie-based protection rules against Challenge Collapsar (CC) attacks.

Practice		Description
	<a href="#">Configuring Anti-Crawler Rules to Prevent Crawler Attacks</a>	WAF provides three anti-crawler policies, bot detection by identifying User-Agent, website anti-crawler by checking browser validity, and CC attack protection by limiting the access frequency, to help mitigate crawler attacks against your websites.
	<a href="#">Verifying a Global Protection Whitelist Rule by Simulating Requests with Postman</a>	After your website is connected to WAF, you can use an API test tool to send HTTP/HTTPS requests to the website and verify that WAF protection rules take effect.  This topic uses Postman as an example to describe how to verify a global protection whitelist (formerly false alarm masking) rule.
	<a href="#">Combining WAF and HSS to Get Improved Web Tamper Protection</a>	With HSS and WAF in place, you can stop worrying about web page tampering.
Using WAF for web vulnerability protection	<a href="#">Java Spring Framework Remote Code Execution Vulnerability</a>	Spring Framework is a lightweight open-source application framework for developing enterprise Java applications. A remote code execution (RCE) vulnerability was disclosed in the Spring framework and classified as critical. This vulnerability can be exploited to attack Java applications running on JDK 9 or later versions.
	<a href="#">Apache Dubbo Deserialization Vulnerability</a>	On February 10, 2020, Apache Dubbo officially released the CVE-2019-17564 vulnerability notice, and the vulnerability severity is medium. Unsafe deserialization occurs within a Dubbo application which has HTTP remoting enabled. An attacker may submit a POST request with a Java object in it to completely compromise a Provider instance of Apache Dubbo, if this instance enables HTTP. Now, Huawei Cloud WAF provides protection against this vulnerability.
	<a href="#">DoS Vulnerability in Open-Source Component Fastjson</a>	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.

Practice		Description
	<a href="#">Remote Code Execution Vulnerability of Fastjson</a>	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 deserialization vulnerability of Fastjson 1.2.24 detected in 2017 and can be directly used to obtain server permissions, causing serious damage.
	<a href="#">Oracle WebLogic wls9-async Deserialization Remote Command Execution Vulnerability (CNVD-C-2019-48814)</a>	On April 17, 2019, the Huawei Cloud Emergency Response Center detected that China National Vulnerability Database (CNVD) released a security bulletin for the Oracle WebLogic wls9-async component. This 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."
LTS log analysis	<a href="#">Using LTS to Query and Analyze WAF Access Logs</a>	If you enable LTS for WAF logging, <a href="#">Log Tank Service (LTS)</a> will log attack and access logs for WAF. With LTS, users can perform real-time decision analysis, device O&M management, and service trend analysis in a timely and efficient manner.
	<a href="#">Using LTS to Analyze How WAF Blocks Spring Core RCE Vulnerability</a>	This topic walks you through on how to enable the LTS quick analysis for WAF attack logs and use the Spring rule ID to quickly query and analyze the logs of the blocked Spring Core RCE vulnerabilities.
	<a href="#">Using LTS to Configure Block Alarms for WAF Rules</a>	This topic walks you through how to enable LTS quick analysis for WAF attack logs and configure alarm rules to analyze WAF attack logs and generate alarms. In this way, you can gain insight into the protection status of your workloads in WAF in real time and make informed decisions.
Configuring TLS encryption	<a href="#">Configuring the Minimum TLS Version and Cipher Suite to Better Secure Connections</a>	HTTPS is a network protocol constructed based on Transport Layer Security (TLS) and HTTP for encrypted transmission and identity authentication.  When you <a href="#">add a domain name to WAF</a> , set <b>Client Protocol</b> to <b>HTTPS</b> . Then, you can configure the minimum TLS version and cipher suite to harden website security.

Practice		Description
Protecting origin servers	<a href="#">Configuring ECS and ELB Access Control Policies to Protect Origin Servers</a>	<p>This topic describes how to protect origin servers deployed on ECSs or added to ELB backend server groups. It helps you:</p> <ul style="list-style-type: none"> <li>• Identify publicly accessible origin servers.</li> <li>• Configure access control policy to protect origin servers.</li> </ul>
Obtaining real client IP addresses	<a href="#">Obtaining Real Client IP Addresses</a>	<p>This topic 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.</p>
Security and governance	<a href="#">Building a WAF with ModSecurity</a>	<p>ModSecurity is an open-source cross-platform web application firewall (WAF). It can protect websites by checking the data received and sent by web servers.</p> <p>This solution helps you deploy a web application firewall (WAF) on ECSs in just a few clicks with open-source ModSecurity. With the flexibility and efficiency of Nginx, this solution effectively enhances web security.</p>