Web Application Firewall

Getting Started

Issue	01
Date	2024-05-14

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

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	Reference Document
Cloud Mode - CNAME Access	**Connection a Website to WAF (Cloud Mode - CNAME Access)**
Cloud - ELB Access	**Connecting WAF to WAF Protection (Cloud Mode - ELB Access)**
Dedicated mode	**Connecting a Website to WAF (Dedicated Mode)**

Step 3: Configure a Protection Policy

After your website is connected to WAF, WAF automatically 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 Configuring CC Attack Protection Rules to Defend Against CC Attacks

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.

You can create custom CC attack protection rules by IP address, cookie, and referer to limit access to specific URLs on your website. WAF will precisely identify and mitigate CC attacks based on rules you create.

This topic walks you through how to configure a CC attack protection rule.

Process

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

Preparations

1. 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.

2. Make sure that your account has sufficient balance, or you may fail to pay to your WAF orders.
3. 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 **Tenant Guest** and **Server Administrator** roles. ● **Tenant Guest**: A global role, which must be assigned in the global project. ● **Server Administrator**: A project-level role, which must be assigned in the same project.
WAF FullAccess	All permissions for WAF	System-defined policy	None.
WAF ReadOnlyAccess	Read-only permissions for WAF.	System-defined policy	

Step 1: Buy WAF

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**.

This topic covers how to purchase cloud WAF, add a website to a cloud WAF in CNAME access mode, and configure and enable CC attack protection rules. For details, see **Buying a Dedicated WAF Instance**.

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**: The **Standard** or higher is recommended.
   - **Expansion Package** and **Required Duration**: Select them based on site requirements.
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

Before adding a website to WAF, you need to collect some details of the website.

Table 2-2 Domain name information required

Required Information	Parameter	Description	Example Value
Whether a proxy is used for the domain name	Proxy Configured	● **Layer-7 proxy**: Web proxy products for layer-7 request forwarding are used, products such as anti-DDoS, CDN, and other cloud acceleration services. ● **Layer-4 proxy**: Web proxy products for layer-4 forwarding are used, products such as anti-DDoS. ● **No proxy**: No proxy products are deployed in front of WAF.	No proxy
Configuration parameters	Domain Name	The domain name is used by visitors to access your website. A domain name consists of letters separated by dots (.). It is a human readable address that maps to the machine readable IP address of your server.	www.example.com

Required Information	Parameter	Description	Example Value
	Protected Port	The service port corresponding to the domain name of the website you want to protect. ● Standard ports – 80: default port when the client protocol is HTTP – 443: default port when the client protocol is HTTPS ● Non-standard ports Ports other than ports 80 and 443	80
	Client Protocol	Protocol used by a client (for example, a browser) to access the website. WAF supports HTTP and HTTPS.	HTTP
	Server Protocol	Protocol used by WAF to forward requests from the client (such as a browser). The options are **HTTP** and **HTTPS**.	HTTP
	Server address	Public IP address or domain name of the origin server for a client (such as a browser) to access. Generally, a public IP address maps to the A record of the domain name configured on the DNS, and a domain name to the CNAME record.	XXX.XXX.1.1
(Optional) Certificate	Certificate Name	If you set **Client Protocol** to **HTTPS**, you are required to configure a certificate on WAF and associate the certificate with the domain name. **NOTICE** Only .pem certificates can be used in WAF. If the certificate is not in PEM format, convert it into pem format by referring to **How Do I Convert a Certificate into PEM Format?**	-

For details, see **Connecting a Website to WAF (Cloud Mode - CNAME Access)**.

Step 3: Enable CC Attack Protection

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.
   a. Set **Rate Limit Mode** based on site requirements.
      i. 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.

         Choose **Source** > **Per IP address** to limit access by IP address.
      ii. In some cases, it may be difficult for WAF to obtain real IP addresses of website visitors. 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.

         Choose **Source** > **Per user**: Web visitors are identified based on the cookie or header of a request.

   b. **Trigger**: At least one condition needs to be configured. The rule takes effect only when all conditions you configure are met.

   c. Set other parameters based on your situation.
5. Confirm the configuration and click **Confirm**.

Related Information

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

3 Configuring a Precise Protection Rule to Block Requests with Empty Fields

You can combine common HTTP fields, such as **IP**, **Path**, **Referer**, **User Agent**, and **Params** in a protection rule to let WAF allow, block, or only log the requests that match the combined conditions. In addition, **JavaScript challenge** verification is supported. WAF returns a piece of JavaScript code that can be automatically executed by a normal browser to the client. If the client properly executes JavaScript code, WAF allows all requests from the client within a period of time (30 minutes by default). During this period, no verification is required. If the client fails to execute the code, WAF blocks the requests.

This topic walks you through how WAF blocks a request with null field.

Process

Procedure	Description
Preparations	Sign up for a HUAWEI ID, enable Huawei Cloud services, top up your account, and assign WAF permissions to the account.
Step 1: Buy WAF	Purchase WAF and select the region and WAF mode.
Step 2: Add a Website to WAF	Add the website you want to protect to WAF for traffic inspection and forwarding.
Step 4: Configure a Precise Protection Rule	Configure the Referer field in the rule to block requests with null fields.

Preparations

1. 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.

2. Make sure that your account has sufficient balance, or you may fail to pay to your WAF orders.
3. 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 **Tenant Guest** and **Server Administrator** roles. ● **Tenant Guest**: A global role, which must be assigned in the global project. ● **Server Administrator**: A project-level role, which must be assigned in the same project.
WAF FullAccess	All permissions for WAF	System-defined policy	None.
WAF ReadOnlyAccess	Read-only permissions for WAF.	System-defined policy	

Step 1: Buy WAF

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**.

This topic will start from how to purchase cloud WAF to how to add a website to a cloud WAF in CNAME access mode, and configure and enable CC attack protection rules. For details, see **Buying a Dedicated WAF Instance**.

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**: The **Standard** or higher is recommended.

  - **Expansion Package** and **Required Duration**: Select them based on site requirements.

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

Before adding a website to WAF, you need to collect some details of the website.

Table 3-2 Domain name information required

Required Information	Parameter	Description	Example Value
Whether a proxy is used for the domain name	Proxy Configured	● **Layer-7 proxy**: Web proxy products for layer-7 request forwarding are used, products such as anti-DDoS, CDN, and other cloud acceleration services. ● **Layer-4 proxy**: Web proxy products for layer-4 forwarding are used, products such as anti-DDoS. ● **No proxy**: No proxy products are deployed in front of WAF.	No proxy
Configuration parameters	Domain Name	The domain name is used by visitors to access your website. A domain name consists of letters separated by dots (.). It is a human readable address that maps to the machine readable IP address of your server.	www.example.com
	Protected Port	The service port corresponding to the domain name of the website you want to protect. ● Standard ports – 80: default port when the client protocol is HTTP – 443: default port when the client protocol is HTTPS ● Non-standard ports Ports other than ports 80 and 443	80

Required Information	Parameter	Description	Example Value
	Client Protocol	Protocol used by a client (for example, a browser) to access the website. WAF supports HTTP and HTTPS.	HTTP
	Server Protocol	Protocol used by WAF to forward requests from the client (such as a browser). The options are **HTTP** and **HTTPS**.	HTTP
	Server address	Public IP address or domain name of the origin server for a client (such as a browser) to access. Generally, a public IP address maps to the A record of the domain name configured on the DNS, and a domain name to the CNAME record.	XXX.XXX.1.1
(Optional) Certificate	Certificate Name	If you set **Client Protocol** to **HTTPS**, you are required to configure a certificate on WAF and associate the certificate with the domain name. **NOTICE** Only .pem certificates can be used in WAF. If the certificate is not in PEM format, convert it into pem format by referring to **How Do I Convert a Certificate into PEM Format?**	-

For details, see **Connecting a Website to WAF (Cloud Mode - CNAME Access)**.

Step 4: Configure a Precise Protection Rule

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

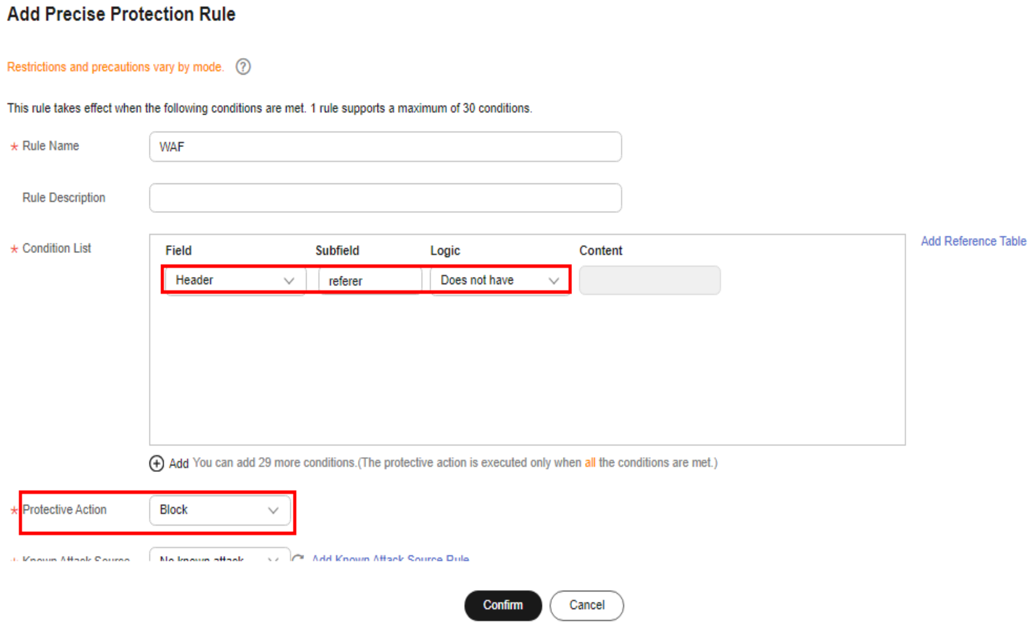
Step 2 Click the name of the target policy to go to the protection configuration page.

Step 3 Click the **Precise Protection** configuration box to enable the precise protection.

- : enabled.
- : disabled.

Step 4 Above the precise protection rule list, click **Add Rule** and configure a rule as shown in **Figure 3-1**.

Figure 3-1 Blocking requests with a null referer field.



Add Precise Protection Rule

Restrictions and precautions vary by mode.

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

* Rule Name: WAF

Rule Description:

* Condition List

Field	Subfield	Logic	Content
Header	referer	Does not have	

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

* Protective Action: Block

* Known Attack Source: No known attack

Step 5 Click **Confirm**.

----End

Related Information

For details, see **Configure Precise Protection Rules to Enable Custom Protection**.

4 Getting Started with Common Practices

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	**Connecting a Domain Name 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.
	Combining CDN and WAF to Get Improved Protection and Load Speed	The combination of CDN and WAF can protect websites on Huawei Cloud, other clouds, or on-premises and improve website response time.
	Combining WAF and Layer-7 Load Balancers to Protect Services over Any Ports	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 **Ports Supported by WAF**.
Protecting websites with WAF policies	**Configuring CC Attack Protection**	This section guides you through configuring IP address-based rate limiting and cookie-based protection rules against Challenge Collapsar (CC) attacks.

Practice		Description
	Configuring Anti-Crawler Rules to Prevent Crawler Attacks	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.
	Verifying a Global Protection Whitelist Rule by Simulating Requests with Postman	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.
	Combining WAF and HSS to Get Improved Web Tamper Protection	With HSS and WAF in place, you can stop worrying about web page tampering.
Using WAF for web vulnerability protection	**Java Spring Framework Remote Code Execution Vulnerability**	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.
	Apache Dubbo Deserialization Vulnerability	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.
	DoS Vulnerability in 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.

Practice		Description
	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 deserialization vulnerability of Fastjson 1.2.24 detected in 2017 and can be directly used to obtain server permissions, causing serious damage.
	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 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	**Using LTS to Query and Analyze WAF Access Logs**	If you enable LTS for WAF logging, **Log Tank Service (LTS)** 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.
	Using LTS to Analyze How WAF Blocks Spring Core RCE Vulnerability	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.
	Using LTS to Configure Block Alarms for WAF Rules	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	**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.

Practice		Description
Protecting origin servers	**Configuring ECS and ELB Access Control Policies to Protect Origin Servers**	This topic describes how to protect origin servers deployed on ECSs or added to ELB backend server groups. It helps you: ● Identify publicly accessible origin servers. ● Configure access control policy to protect origin servers.
Obtaining real client IP addresses	**Obtaining Real Client IP Addresses**	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.
Security and governance	**Building a WAF with ModSecurity**	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. 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.