

# Web Application Firewall

## Getting Started

**Issue** 01  
**Date** 2023-02-22



**Copyright © Huawei 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 Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI 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.

# Security Declaration

## Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

# Contents

---

<b>1 Getting Started with WAF.....</b>	<b>1</b>
--	----------

# 1 Getting Started with WAF

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 services.

## 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. For details, see [Buying Cloud 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	Take the following steps to connect your website to a cloud WAF instance through CNAME records: <ol style="list-style-type: none"><li>1. <a href="#">Add a Domain Name to WAF (Cloud Mode)</a></li><li>2. <a href="#">Whitelist WAF IP Addresses</a></li><li>3. <a href="#">Test WAF</a></li><li>4. <a href="#">Route Website Traffic to WAF</a></li></ol>

Access Mode	Reference Document
Dedicated mode	Take the following five steps to connect a website to a dedicated WAF instance: <ol style="list-style-type: none"><li>1. <a href="#">Add a Website to WAF (Dedicated Mode)</a></li><li>2. <a href="#">Configuring a Load Balancer</a></li><li>3. <a href="#">Bind an EIP to a Load Balancer</a></li><li>4. <a href="#">Whitelist IP Addresses of Dedicated WAF Instances</a></li><li>5. <a href="#">Test Dedicated WAF Instances</a></li></ol>

### 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](#).