Web Application Firewall

Getting Started

Issue 03

Date 2024-01-31

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.

Contents

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.

   WAF provides three access methods, CNAME and ELB access methods for cloud WAF and dedicated access 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 have purchased cloud WAF (standard, professional, or platinum edition), CNAME and ELB access methods share the domain name, bandwidth, and rule extension packages you have purchased.

   – **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	Take the following steps to connect your website to a cloud WAF instance through CNAME records: 1. **Add a Domain Name to WAF (Cloud Mode - CNAME Access)** 2. **Whitelist WAF IP Addresses** 3. **Test WAF** 4. **Route Website Traffic to WAF**
Cloud - ELB Access	**Add a Website to WAF (Cloud Mode - ELB Access)**
Dedicated mode	Take the following five steps to connect a website to a dedicated WAF instance: 1. **Add a Website to WAF (Dedicated Mode)** 2. **Configuring a Load Balancer** 3. **Bind an EIP to a Load Balancer** 4. **Whitelist IP addresses of Dedicated WAF Instances** 5. **Test Dedicated WAF Instances**

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 **More** > **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**.