Cloud Firewall

Practices

Issue	03
Date	2024-01-10

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

1 CFW Best Practices

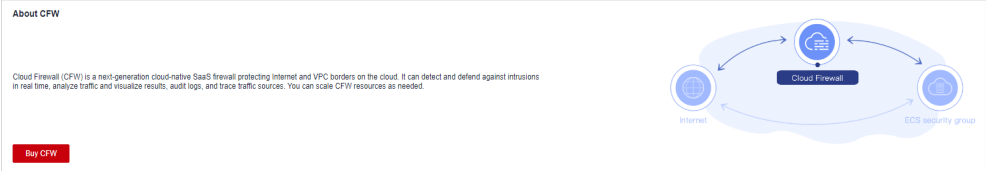
Enabling EIP Protection

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 In the navigation pane, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 1-1**.

Figure 1-1 CFW Dashboard

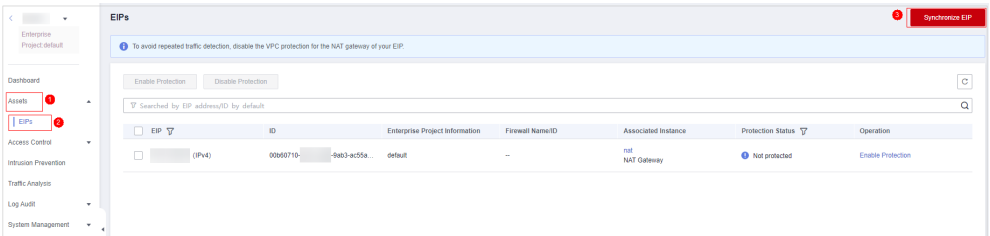


Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

Step 5 In the navigation pane, choose **Assets** > **EIPs**. The **EIPs** page is displayed.

(Optional) Manually refresh the list. Click **Synchronize EIP** in the upper right corner of the page to import your EIP information to the list and refresh the EIP list.

Figure 1-2 EIPs



NOTICE

- Currently, IPv6 addresses cannot be protected.

Step 6 Enable EIP protection.

- Enable protection for a single EIP. In the row of the EIP, click **Enable Protection** in the **Operation** column.
- Enable protection for multiple EIPs. Select the EIPs to be protected and click **Enable Protection** above the table.

Step 7 On the page that is displayed, check the information and click **Bind and Enable**. Then the **Protection Status** changes to **Protected**.

NOTE

After EIP protection is enabled, the default access control policy is **Allow**.

----End

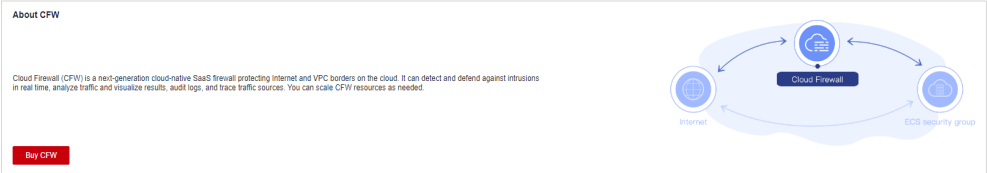
Enabling Intrusion Prevention

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 In the navigation pane, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 1-3**.

Figure 1-3 CFW Dashboard



Step 4 In the navigation pane, choose **Attack Defense** > **Intrusion Prevention**.

Step 5 On the **Intrusion Prevention** page, select the **Protection Mode**.

- **Observe**: Attacks are detected and recorded in logs.
- **Intercept**: Attacks and abnormal IP address access are automatically intercepted.
  - **Intercept mode-loose**: The protection granularity is coarse. In this mode, only attacks with high threat and high certainty are blocked.
  - **Intercept mode-moderate**: The protection granularity is medium. This mode meets protection requirements in most scenarios.
  - **Intercept mode-strict**: The protection granularity is fine-grained, and all attack requests are intercepted. Configure false alarm masking rules after

the service has been running for a period of time, and then enable strict mode.

----End

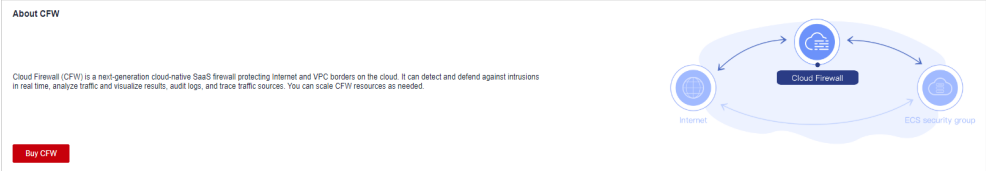
Configuring an Inbound Access Policy

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 In the navigation pane, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 1-4**.

Figure 1-4 CFW Dashboard

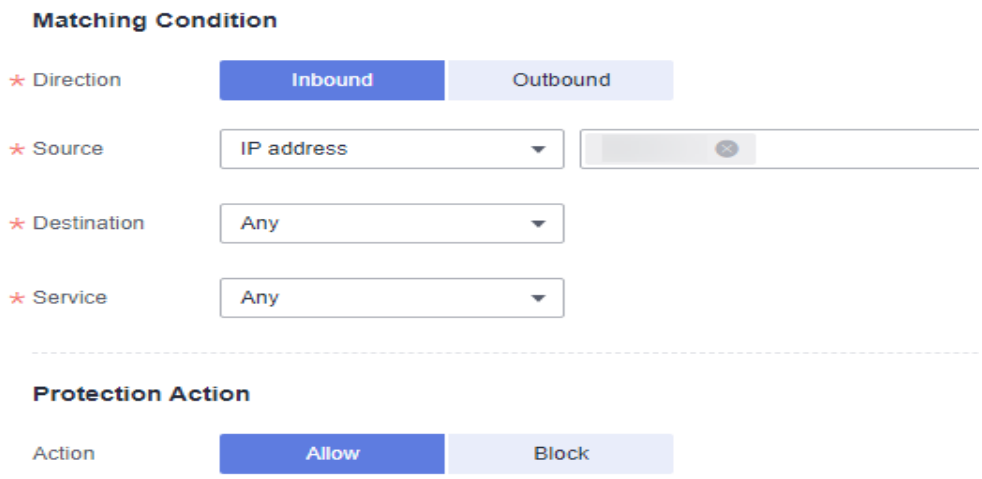


Step 4 In the navigation pane, choose **Access Control** > **Access Policies**.

Step 5 Click **Add Rule**. Configure parameters in the **Add Rule** dialog box.

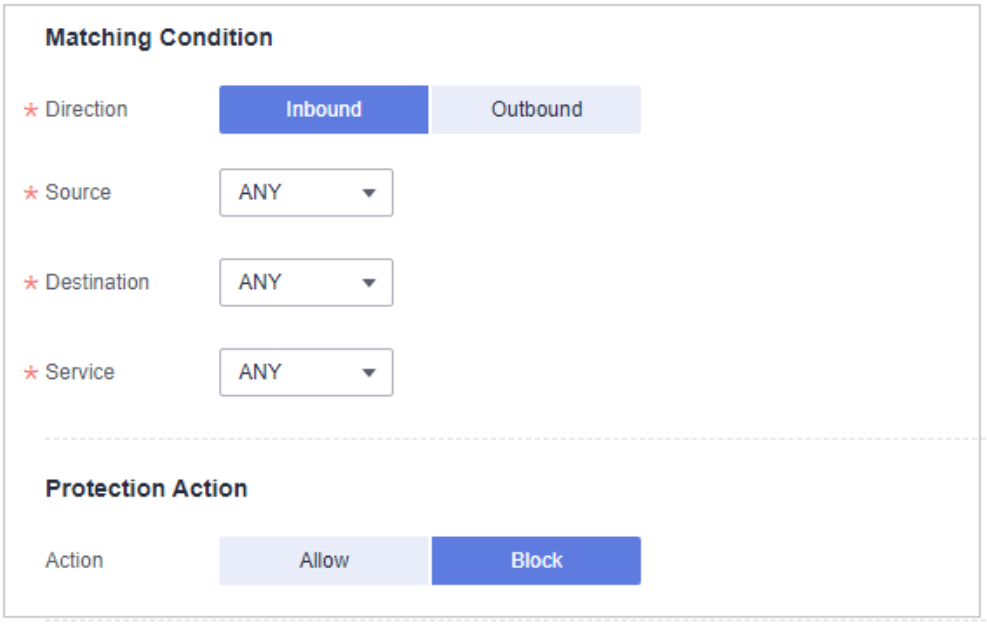
- Add a protection rule to allow certain traffic. In the **Add Rule** dialog box, configure the source IP address. Set **Destination** and **Service** to **ANY** and set **Action** to **Allow**.

  Figure 1-5 Allowing a specified IP address



- Add a rule to block all traffic. In the **Add Rule** dialog box, set the addresses to **Any** and **Action** to **Block**. Ensure that the rule has the lowest priority.

Figure 1-6 Blocking all traffic



----End

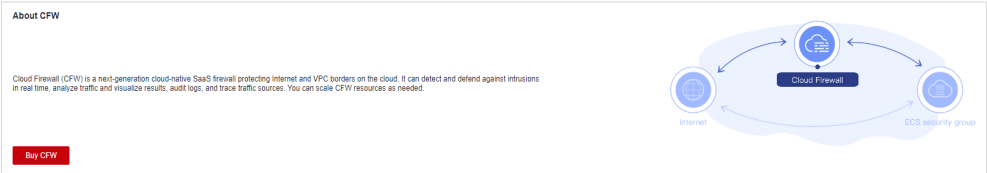
Configuring an Outbound Access Policy

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 In the navigation pane, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 1-7**.

Figure 1-7 CFW Dashboard

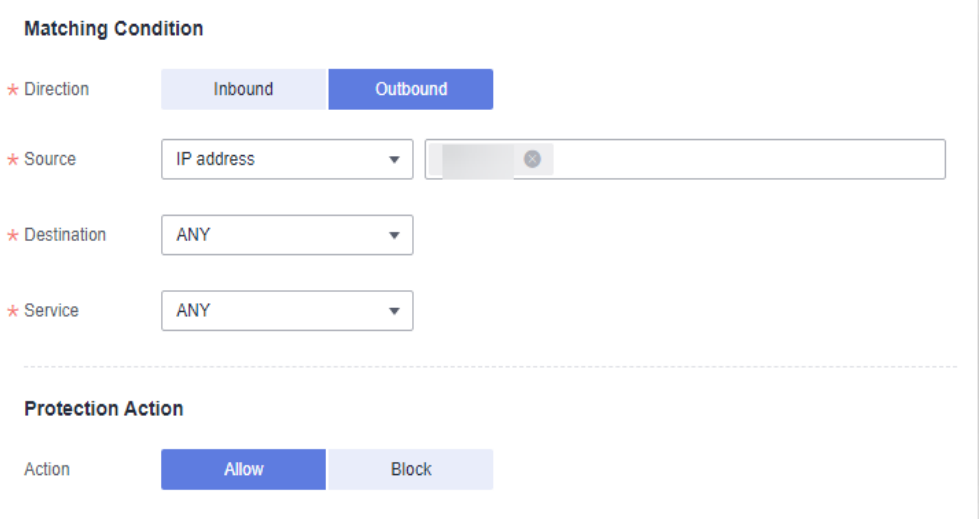


Step 4 In the navigation pane, choose **Access Control** > **Access Policies**.

Step 5 Click **Add Rule**. Configure parameters in the **Add Rule** dialog box.

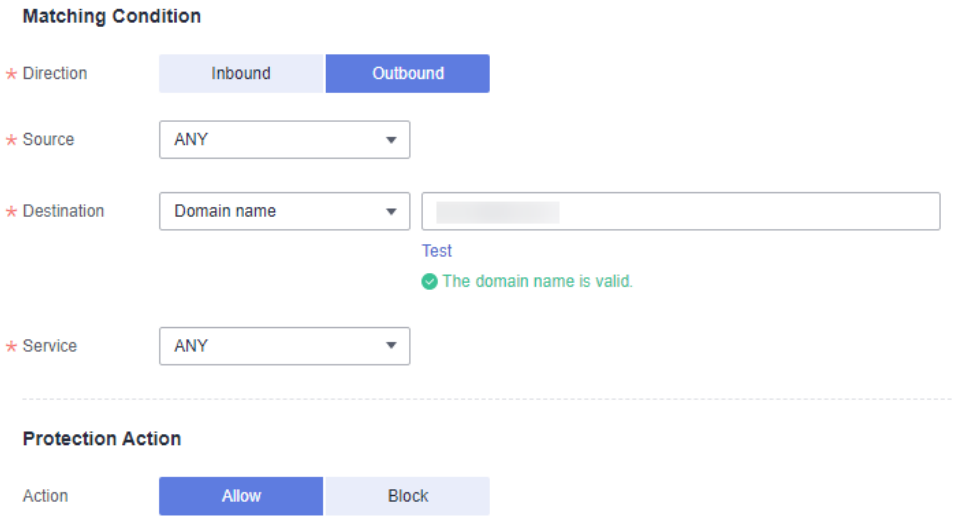
- Add a protection rule to allow certain traffic. In the **Add Rule** dialog box, configure the source IP address. Set **Destination** and **Service** to **ANY** and set **Action** to **Allow**.

Figure 1-8 Allowing a specific IP address (outbound)



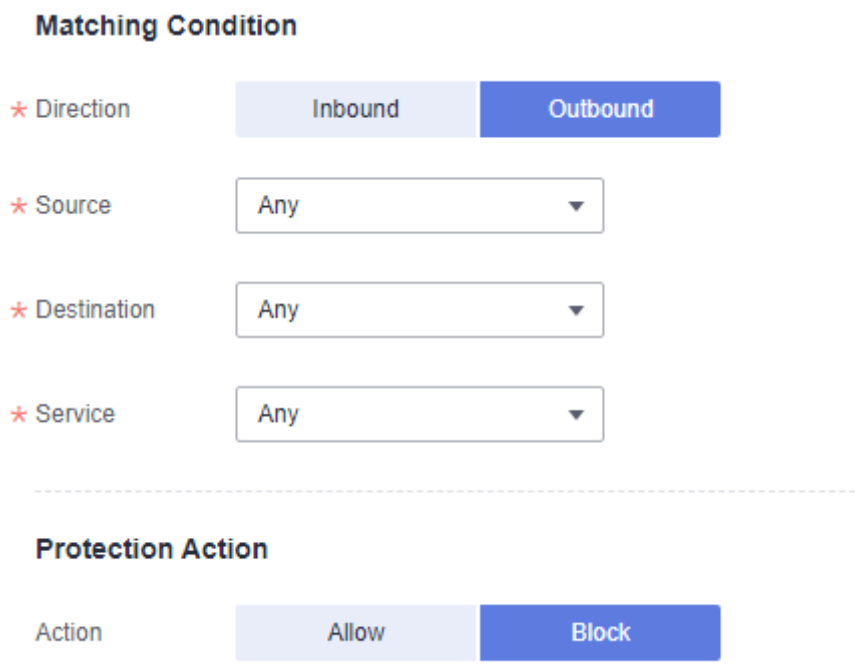
- In the **Add Rule** dialog box, set **Source** to **Any**, **Destination** to **Domain name**, **Service** to **Any**, and **Action** to **Allow**.

  Figure 1-9 Configuring a policy to allow outbound traffic (domain name specified)



- Add a rule to block all traffic. In the **Add Rule** dialog box, set **Source**, **Destination**, and **Service** to **ANY** and set **Action** to **Block**. Ensure that the rule has the lowest priority.

Figure 1-10 Blocking all traffic (outbound)



----End

Viewing Protection Details

Perform the operations in **View Protection Details**.

2 Configuring Access Policies for IP Address Groups and Service Groups

After a protected object is connected to CFW, you can configure access control policies for IP address groups and service groups, and verify the effect of the policies. This section uses the configuration of IP address and service groups as an example to describe how to configure IP address and service access control policies in batches.

Scenario

If your service is deployed in an enterprise that has many IP addresses and services, you need to configure access control policies for users' IP address groups and service groups to permit or block certain access requests.

Prerequisites

- A website to be protected has been connected to CFW.
- Intrusion prevention has been enabled and **Action** has been set to **Block**.

Configuring an Access Control Policy

- For details about how to add an IP address group, see **Adding an IP Address Group**.
- For details about how to add a service group, see **Adding a Service Group**.
- For details about how to add a protection rule, see **Adding a Protection Rule**.

Verifying a Rule

Perform the operations in **View Protection Details**.

3 Precautions for Using CFW with WAF, Advanced Anti-DDoS, and CDN

This section describes where CFW is deployed in the network architecture and how to configure CFW when it is used with other Huawei Cloud services.

Application Scenarios

If you purchase other Huawei Cloud products, service traffic is protected by multiple layers. In this case, reverse proxies may translate request IP addresses.

If a reverse proxy service (such as CDN, Advanced Anti-DDoS, or cloud WAF) is deployed before CFW, you need to configure a policy to permit the back-to-origin IP addresses so that traffic can be forwarded to and checked by CFW. For details, see **Configuring Policies**. If you purchase dedicated or ELB-mode WAF instances, configure policies based on service requirements.

NOTE

If you purchase dedicated WAF instances, there are two protection scenarios:

- You have enabled CFW protection for the EIPs bound to public network ELB load balancers.

  If there is an attack from the client, CFW prints the attack event on the **Internet Border Firewall** tab under **Attack Event Logs**.

  The destination IP address of the event is the EIP bound to the public ELB load balancer, and the source IP address is the IP address of the client.

- You have enabled VPC border firewall and associated with the VPC where the origin server resides. No protection is enabled for EIPs bound to the ELB load balancer.

  If there is an attack from the client, CFW prints the attack event on the **VPC Border Firewall** tab under **Attack Event Logs**.

  The destination IP address of the event is the private IP address of the origin server, and the source IP address is the private IP address of the traffic ingress (such as the Nginx server).

After the traffic passes through the reverse proxy, the source IP address is translated into the back-to-origin IP address. In this case, if an external attack occurs, CFW cannot obtain the real IP address of the attacker. You can obtain the real IP address based on the **X-Forwarded-For** field. For details, see **Viewing X-Forwarded-For**.

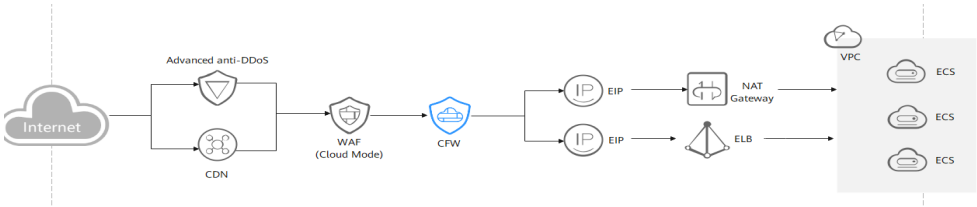
Traffic Flow

Web Application Firewall (WAF), Advanced Anti-DDoS (AAD), and Content Delivery Network (CDN) work as reverse proxies. If these services are deployed, the source IP addresses received by CFW is the back-to-origin IP addresses returned by these services.

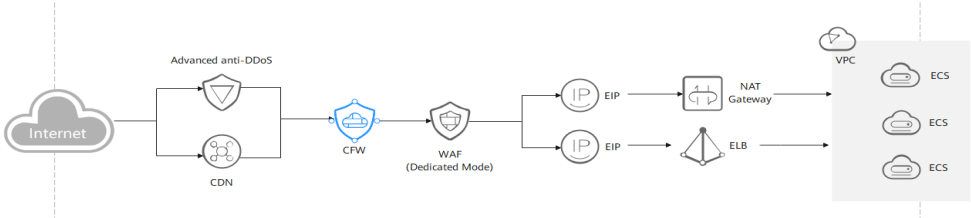
WAF supports three modes: cloud, dedicated, and ELB modes. The architecture varies depending on the mode, but the deployment positions of Advanced Anti-DDoS and CDN are fixed.

The following figures show the traffic flow.

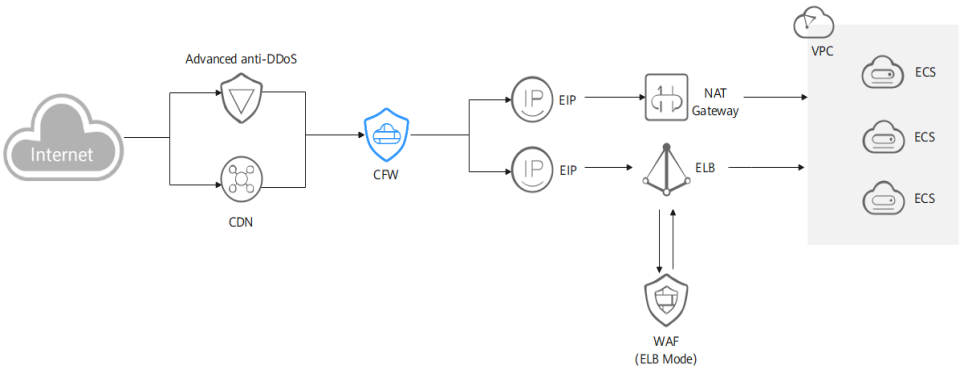
- Cloud WAF



- Dedicated WAF



- ELB-mode WAF



Configuring Policies

- You are advised to create a policy with the highest priority to permit all back-to-origin IP addresses. In this way, traffic still goes to CFW for check.
- If you whitelist back-to-origin IP addresses, the traffic is directly permitted to pass through and will not be checked by CFW.

CAUTION

You are not advised to block back-to-origin IP addresses or add them to a blacklist. Otherwise, all traffic from such IP addresses will be blocked and your services may be affected.

- For details about how to add a protection rule, see **Adding a Protection Rule**.
- For details about how to set the whitelist, see **Managing the Blacklist and the Whitelist**.
- For details about the protection priority of CFW, see **What Are the Priorities of the Protection Settings in CFW?**
- For details about how to obtain the back-to-origin IP addresses of WAF, see **Step 2: Whitelisting WAF IP Addresses**.

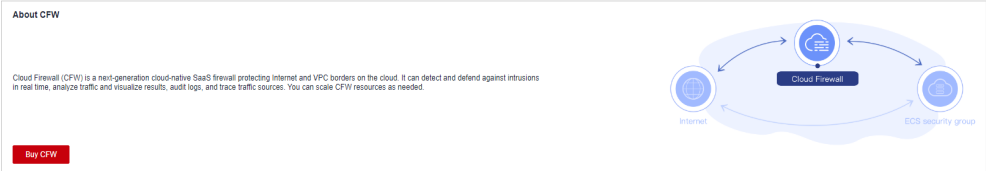
Viewing X-Forwarded-For

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 In the navigation pane, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 3-1**.

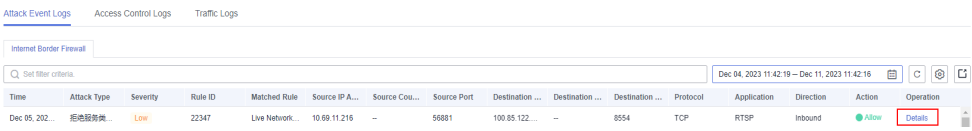
Figure 3-1 CFW Dashboard



Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

Step 5 In the navigation pane, choose **Log Audit** > **Log Query**. Click **Attack Event Logs** tab. In the **Operation** column of the target event, click **Details**.

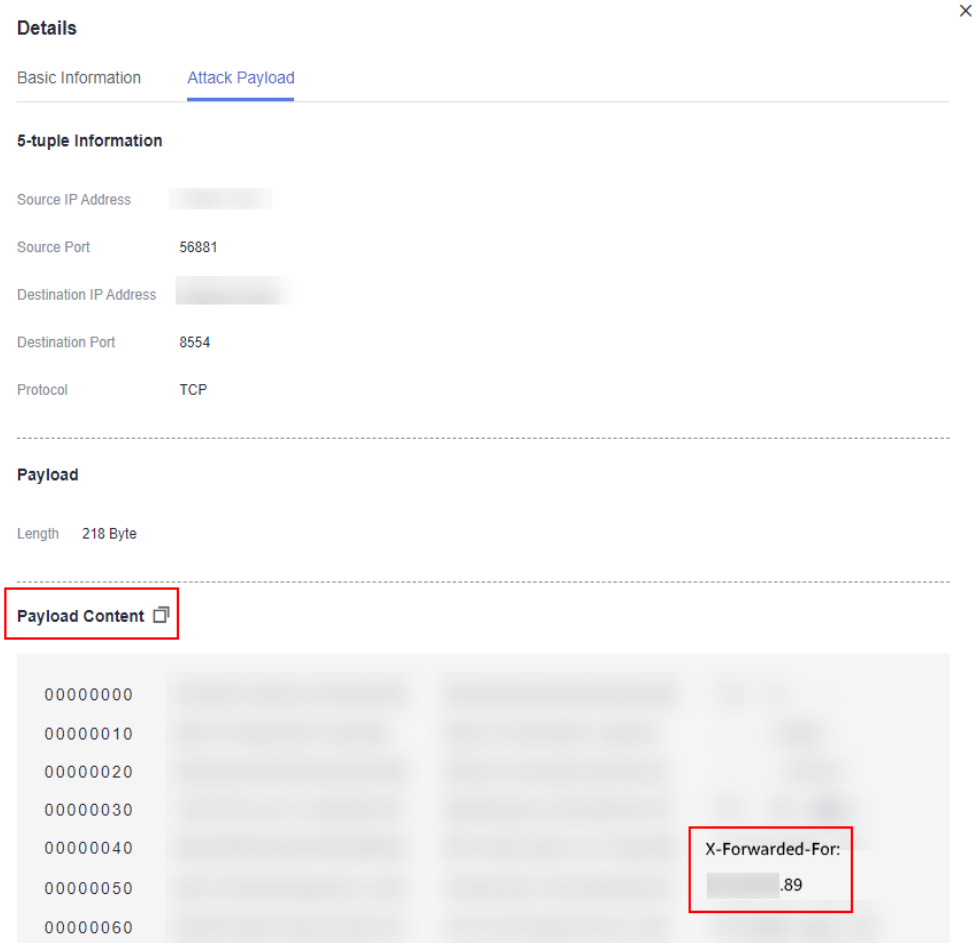
Figure 3-2 Viewing attack event log details



Step 6 In the **Details** page, click the **Attack Payload** tab, and obtain the value of **X-Forwarded-For** field.

- Method 1: Check **X-Forwarded-For** (all IP addresses from the client to the last proxy server) in the **Payload Content** area.

Figure 3-3 X-Forwarded-For in the payload



- Method 2: Copy the **Payload Content** and use the Base64 tool to obtain the decoding result.
  - **X-Forwarded-For**: all IP addresses from the client to the last proxy server

  For example, the client IP address obtained in **Example of the Base64 decoding result** is **xx.xx.xx.89**, and only cloud WAF is used.

Figure 3-4 Example of the Base64 decoding result

```
dGET /api/dbstat/gettablessize HTTP/1.1
X-Real-IP: [redacted].89
X-Hwwaf-Real-IP: [redacted].89
X-Hwwaf-Client-IP: [redacted].89
X-Forwarded-For: [redacted].89
Host: [redacted].net
X-Forwarded-Proto: https
X-CloudWAF-Traffic-Tag: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/[redacted]
Referer: http://c.bookmall.top/api/dbstat/gettablessize
Accept-Encoding: gzip
```

----End

A Change History

Released On	Description
2024-01-10	This issue is the third official release. Added **Precautions for Using CFW with WAF, Advanced Anti-DDoS, and CDN**.
2023-11-30	This is the second official release. Optimized: Description about checking protection details in **Configuring Access Policies for IP Address Groups and Service Groups**.
2022-12-30	This issue is the first official release.