

# Cloud Firewall

## FAQ

**Issue** 03  
**Date** 2024-10-12



**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.

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

Address: Huawei Industrial Base  
Bantian, Longgang  
Shenzhen 518129  
People's Republic of China

Website: <https://www.huawei.com>

Email: [support@huawei.com](mailto:support@huawei.com)

# 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 About the Product.....</b>	<b>1</b>
1.1 Does CFW Support Off-Cloud Servers?.....	1
1.2 Can CFW Be Shared Across Accounts?.....	1
1.3 What Are the Differences Between CFW and WAF?.....	1
1.4 What Are the Differences Between CFW, Security Groups, and Network ACLs?.....	2
1.5 How Does CFW Control Access?.....	4
1.6 What Are the Priorities of the Protection Settings in CFW?.....	4
1.7 Can WAF and CFW Be Deployed Together?.....	6
1.8 How Long Are CFW Logs Stored by Default?.....	6
<b>2 Regions and AZs.....</b>	<b>7</b>
2.1 What Are Regions and AZs?.....	7
2.2 Can CFW Be Used Across Clouds or Regions?.....	8
<b>3 Troubleshooting.....</b>	<b>9</b>
3.1 What Do I Do If Service Traffic is Abnormal?.....	9
3.2 Why Are Traffic and Attack Logs Incomplete?.....	14
3.3 Why Does a Protection Rule Not Take Effect?.....	15
3.4 What Do I Do If IPS Blocks Normal Services?.....	16
3.5 Why Is No Data Displayed on the Access Control Logs Page?.....	17
<b>4 Network Traffic.....</b>	<b>18</b>
4.1 How Do I Calculate the Number of Protected VPCs and the Peak Protection Traffic at the VPC Border?.....	18
4.2 How Does CFW Collect Traffic Statistics?.....	18
4.3 What Is the Protection Bandwidth Provided by CFW?.....	19
4.4 What Do I Do If My Service Traffic Exceeds the Protection Bandwidth?.....	19
4.5 What Are the Differences Between the Data Displayed in Traffic Trend Module and the Traffic Analysis Page?.....	19
4.6 How Do I Verify the Validity of an Outbound HTTP/HTTPS Domain Protection Rule?.....	20
<b>5 Billing.....</b>	<b>21</b>
5.1 How Is CFW Billed?.....	21
5.2 How Do I Change My CFW Edition?.....	21
5.3 Can I Switch Between Yearly/Monthly and Pay-per-Use Payments for CFW?.....	22
5.4 How Do I Renew CFW?.....	22

---

5.5 How Do I Unsubscribe from CFW?..... 23

# 1 About the Product

---

## 1.1 Does CFW Support Off-Cloud Servers?

No. CFW can protect region-level services on the cloud.

## 1.2 Can CFW Be Shared Across Accounts?

No. You can only use and manage CFW resources under your account.

## 1.3 What Are the Differences Between CFW and WAF?

CFW and WAF are two different Huawei Cloud products that can be used to protect your Internet borders, VPC borders, and web services.

[Table 1-1](#) describes the differences between WAF and CFW.

**Table 1-1** Differences between CFW and WAF

Item	CFW	WAF
Definition	<p>Cloud Firewall (CFW) is a next-generation cloud-native firewall. It protects the Internet border and VPC border on the cloud by real-time intrusion detection and prevention, global unified access control, full traffic analysis, log audit, and tracing. It employs AI for intelligent defense, and can be elastically scaled to meet changing business needs, helping you easily handle security threats. CFW is a basic service that provides network security protection for user services on the cloud.</p>	<p>WAF keeps web services stable and secure. It examines all HTTP and HTTPS requests to detect and block the following attacks: Structured Query Language (SQL) injection, cross-site scripting (XSS), web shells, command and code injections, file inclusion, sensitive file access, third-party vulnerability exploits, Challenge Collapsar (CC) attacks, malicious crawlers, and cross-site request forgery (CSRF).</p> <p>For details about WAF, see <a href="#">What Is Web Application Firewall?</a></p>
Protection	<ul style="list-style-type: none"> <li>• EIP border and VPC border</li> <li>• Basic protection against web attacks</li> <li>• Defense against external intrusions and protection of proactive connections to external systems</li> </ul>	<ul style="list-style-type: none"> <li>• WAF protects web applications on Huawei Cloud and other clouds and on-premises applications through domain names or IP addresses.</li> <li>• Comprehensive protection against web attacks</li> </ul>
Features	<ul style="list-style-type: none"> <li>• Asset management and intrusion defense: It detects and defends against intrusions into cloud assets that are accessible over the Internet in real time.</li> <li>• Access control: You can control access at Internet borders.</li> <li>• Traffic Analysis and log audit: CFW controls, analyzes, and visualizes VPC traffic, audits logs, and traces traffic sources.</li> </ul>	<p>WAF identifies and blocks a wide range of suspicious attacks, such as SQL injections, XSS attacks, web shell upload, command or code injections, file inclusion, unauthorized sensitive file access, third-party vulnerability exploits, CC attacks, malicious crawlers, and CSRF.</p>

## 1.4 What Are the Differences Between CFW, Security Groups, and Network ACLs?

CFW, security groups, and network ACLs allow you to set access control policies based on IP addresses or IP address groups to protect your Internet borders, VPC borders, ECSs, and subnets.

[Table 1-2](#) describes the differences between them.

**Table 1-2** Differences between CFW, security groups, and network ACLs

Item	CFW	Security group	Network ACL
Definition	Cloud Firewall (CFW) is a next-generation cloud-native firewall. It protects the Internet border and VPC border on the cloud by real-time intrusion detection and prevention, global unified access control, full traffic analysis, log audit, and tracing. It employs AI for intelligent defense, and can be elastically scaled to meet changing business needs, helping you easily handle security threats. CFW is a basic service that provides network security protection for user services on the cloud.	A security group is a collection of access control rules for instances, such as cloud servers, containers, and databases, that have the same security requirements and that are mutually trusted within a VPC. You can define different access control rules for a security group, and these rules are then applied to all the instances added to this security group. For details about security groups, see <a href="#">Security Groups and Security Group Rules</a> .	A network ACL is an optional layer of security for your subnets. After you associate one or more subnets with a network ACL, you can control traffic in and out of the subnets. For details about network ACLs, see <a href="#">Network ACL</a> .
Protected objects	<ul style="list-style-type: none"> <li>• Internet boundary</li> <li>• VPC boundary</li> <li>• SNAT scenario</li> </ul>	ECS	Subnet
Features	<ul style="list-style-type: none"> <li>• Filtering by 5-tuple (source IP address, destination IP address, protocol, source port, and destination port)</li> <li>• Filtering by geographical location, domain name, domain name group, and blacklist/whitelist</li> <li>• Intrusion prevention system (IPS) and antivirus (AV).</li> </ul>	Filtering by 3-tuple (protocol, port, and peer IP address)	Filtering by 5-tuple (source IP address, destination IP address, protocol, source port, and destination port)



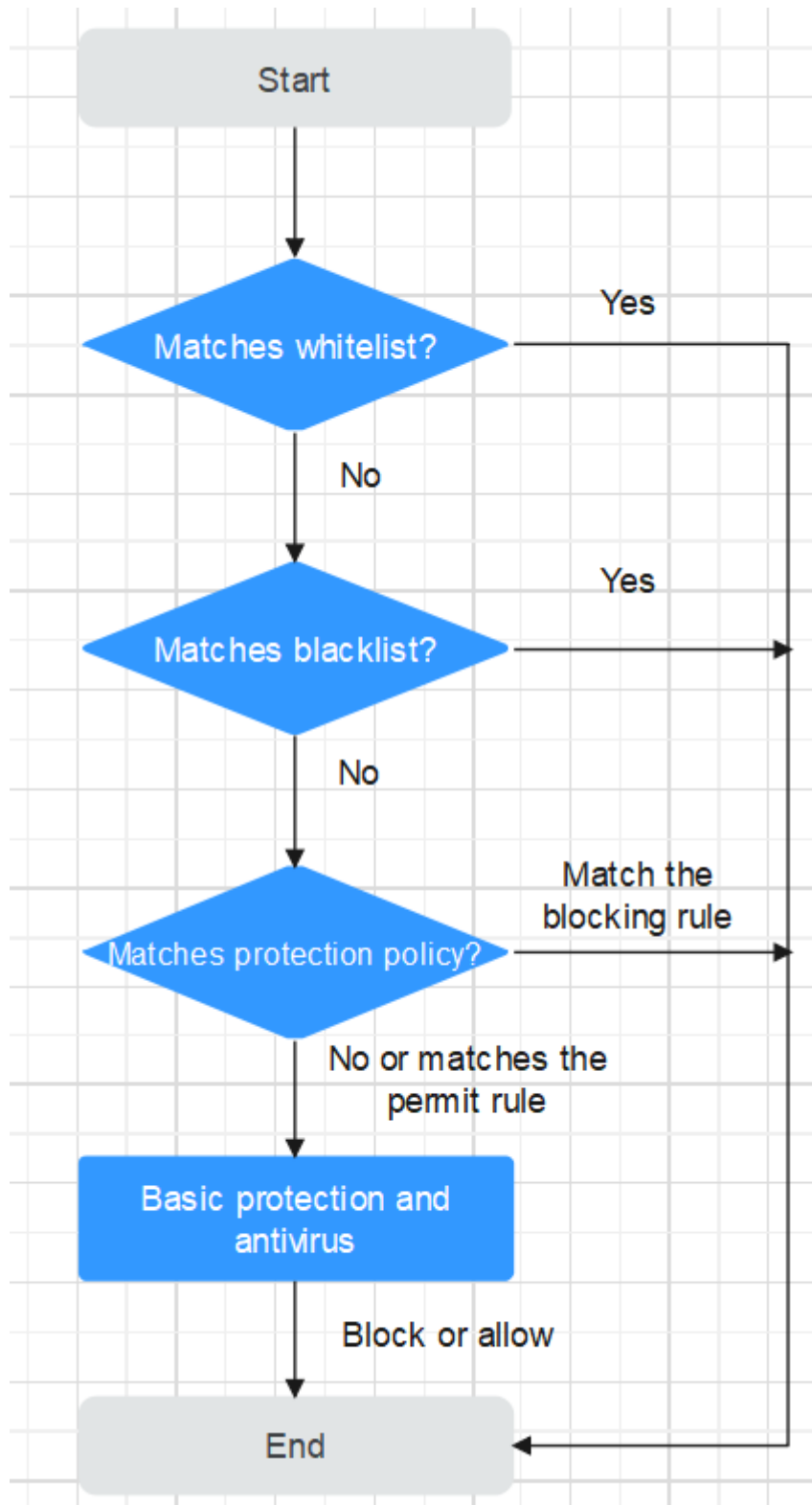
## 1.5 How Does CFW Control Access?

CFW allows you to configure ACL policies based on a 5-tuple, IP address group, service group, domain name, blacklist, and whitelist. You can also configure ACL policies based on the intrusion prevention system (IPS). The IPS can work in observation or block mode. In block mode, the firewall detects and blocks traffic that matches the IPS rules. For details, see [Configuring Access Control Policies](#).

## 1.6 What Are the Priorities of the Protection Settings in CFW?

The priorities of the protection settings that take effect in CFW in descending order are as follows: Whitelist > Blacklist > Protection policy (ACL) > Basic Protection (IPS) = Antivirus.

Figure 1-1 Protection priorities



- For details about how to set the blacklist or whitelist, see [Managing Blacklists and Whitelists](#).
- For details about how to add a protection rule, see [Adding a Protection Rule](#).

- For details about how to set the IPS protection mode, see [Configuring Intrusion Prevention](#). For details about how to customize IPS rules, see [Customizing IPS Signatures](#).
- For details about how to enable virus defense, see [Enabling Antivirus](#).

## 1.7 Can WAF and CFW Be Deployed Together?

Yes. When both CFW and WAF are deployed, traffic passes through WAF and then CFW. The traffic trend is as follows: Internet -> WAF (cloud mode) -> CFW -> Origin server.

### NOTE

Exercise caution when configuring traffic blocking rules. You are advised to configure traffic permitting rules or whitelists.

## 1.8 How Long Are CFW Logs Stored by Default?

You can query and export logs generated within the last seven days for free. For details, see [Querying Logs](#).

You can record one or multiple logs in LTS and view logs generated in the past 1 to 360 days. For details, see [Log Management](#).

### NOTE

LTS is billed by traffic and is billed separately from CFW. For details about LTS pricing, see [LTS Pricing](#).

# 2 Regions and AZs

---

## 2.1 What Are Regions and AZs?

### Concepts

A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- Regions are divided from the dimensions of geographical location and network latency. Public services, such as Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP), and Image Management Service (IMS), are shared within the same region. Regions are classified as universal regions and dedicated regions. A universal region provides universal cloud services for common tenants. A dedicated region provides services of the same type only or for specific tenants.
- An AZ contains one or more physical data centers. Each AZ has independent cooling, fire extinguishing, moisture-proof, and electricity facilities. Within an AZ, computing, network, storage, and other resources are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

### Selecting a Region

If you or your users are in Europe, select the **EU-Dublin** region.

### Selecting an AZ

When determining whether to deploy resources in the same AZ, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs in the same region.
- For low network latency, deploy resources in the same AZ.

## 2.2 Can CFW Be Used Across Clouds or Regions?

### In Which Regions Is CFW Available?

For details about CFW and the regions supported by each function, see [Function Overview](#).

### Can CFW Be Used Across Regions?

No. CFW can be used only in the region selected during purchase.

 **NOTE**

If a message is displayed indicating that CFW cannot be purchased in the selected region, you can choose: VPC [Network ACLs](#) and [Security Groups](#).

### Can CFW Be Used Across Clouds?

No. Currently, CFW only protects services deployed on Huawei Cloud.

# 3 Troubleshooting

---

## 3.1 What Do I Do If Service Traffic is Abnormal?

This section describes how to rectify the fault if your service traffic is abnormal and may be interrupted by CFW.

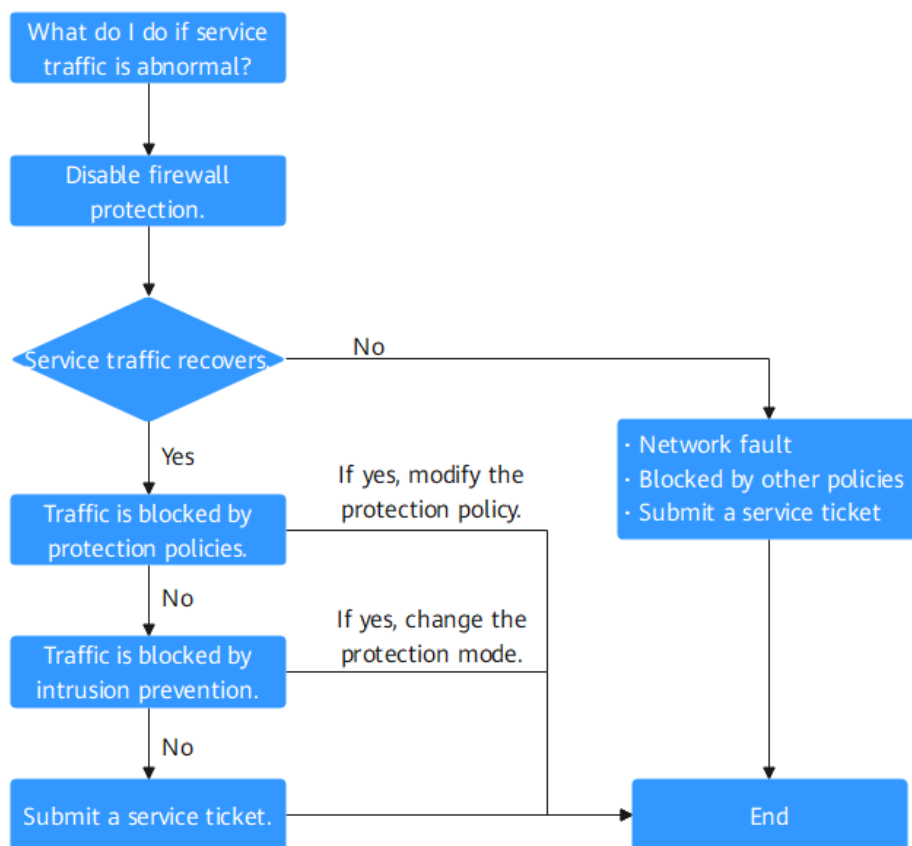
### Symptom

Service traffic is abnormal. For example:

- An EIP cannot access the Internet.
- A server cannot be accessed.

## Troubleshooting Methods

**Figure 3-1** Procedure of checking traffic exceptions



**Table 3-1** Procedure of checking traffic exceptions

No.	Possible Cause	Solution
1	Traffic interruption not caused by CFW	See <a href="#">Cause 1: Traffic Interruption Not Caused by CFW.</a>
2	Traffic blocked by protection policies	See <a href="#">Cause 2: Traffic Blocked by Protection Policies.</a>
3	Traffic blocked by intrusion prevention	See <a href="#">Cause 3: Traffic Blocked by Intrusion Prevention.</a>

### Cause 1: Traffic Interruption Not Caused by CFW

You can disable protection on the CFW console and observe the service status. If the service does not recover, it indicates the traffic interruption was not caused by CFW.

To disable protection, perform the following steps:

- EIP traffic fault: Disable the CFW protection in EIPs whose services are interrupted. For details, see [Disabling EIP Protection](#).
- SNAT or inter-VPC access failure: Disable the VPC border firewall. For details, see [Disabling a VPC Border Firewall](#).

If problem persists, refer to the following common fault causes:

- Network fault: The route configuration is incorrect, or the NE is faulty.
- Policy-based interception: Interception caused by incorrect configurations of other security services, network ACLs, or security groups.

If you need assistance from Huawei Cloud, you can [create a service ticket](#).

## Cause 2: Traffic Blocked by Protection Policies

Traffic is blocked probably because a blocking rule is configured in the access control policy, or the normal services are blacklisted. In this case, CFW blocks related sessions, causing service loss.

You can take the following measures:

In the [Access Control Logs](#) tab, search for logs about the blocked IP address or domain name.

- If no records are found, see [Table 3-1](#) under Cause 3.
- If a record is found, click the **Rule** column to go to the matched blocking policy.
  - If normal services are blacklisted, you can:
    - Delete the blacklist policy.
    - Add a whitelist policy for the IP address/domain name. (The whitelist takes precedence over the blacklist. After the whitelist policy is added, the blacklist policy becomes invalid and the traffic is directly permitted.)
  - If the traffic is blocked by a blocking rule, you can:
    - Find the blocking rule of the IP address or domain name in the access control rule list and disable the policy.
    - Modify the matching condition of the blocking policy and remove the IP address or domain name information.
    - Add a protection rule whose **Action** is **Allow** and **Priority** is **Pin on top**. For details, see [Adding a Protection Rule](#).

### Case

Handling process: Detect a fault -> Disable protection -> View logs -> Modify a policy -> Restore protection -> Confirm logs

The network O&M personnel of a company found that an ECS cannot access the Internet through the bound EIP **xx.xx.xx.126**.

The firewall administrator took the following measures:



**Step 1** To ensure that the IP address can be used for external communication during fault locating, the firewall administrator logged in to the CFW console, and chose **Assets > EIPs**, and disables protection for the EIP.

During the firewall is disabled, the traffic of the EIP is not processed and related logs are not displayed.

**Figure 3-2** EIPs

EIP ID	Protection Status	Firewall Name/ID	Associated Instance	Owner	Tags	Operation
177 a17-414b-96fc-4eb75b2e4c01	Not protected	--	NAT Gateway		--	Enable Protection
119-136-3d3a-e0c0cd-1a71 43b-462-3040-c7827c19d942	Not protected	--	Cloud Server		--	Enable Protection
130 679-4211a258-79a9200039b	Not protected	--	Cloud Server		--	Enable Protection
94 02144b1a-4930-4938-855b-0563328455a	Protected	Firewall 2f689f66-a82c-41d0-9208-4eff9a5c1e43	Cloud Server		--	Disable Protection

**Step 2** The administrator chose **Log Audit > Log Query** and clicked the **Access Control Logs** tab. He searched for the blocking logs of the access source IP address **xx.xx.xx.126**. A blocking rule named **Block-Malicious-Outreach** was found, and this rule blocked the traffic from the attack source IP address to the Internet.

**Figure 3-3** Filtering access control logs

Received	Source	Source Country/Region	Source Port	Destination IP Address	Destination Country...	Destination URL	Destination Port	Protocol	Action	Rule
Dec 22, 2023 10:07:40 ...	126	Chinese Mainland	44315		Sweden	--	123	UDP	Block	Block-Malicious-Outreach
Dec 22, 2023 10:07:30 ...	126	Chinese Mainland	60106		Switzerland	--	123	UDP	Block	Block-Malicious-Outreach
Dec 22, 2023 10:07:19 ...	126	Chinese Mainland	60167		Sweden	--	123	UDP	Block	Block-Malicious-Outreach
Dec 22, 2023 10:07:09 ...	126	Chinese Mainland	48206		United Kingdom	--	123	UDP	Block	Block-Malicious-Outreach

**Step 3** The administrator searched for "Source: xx.xx.xx.126; Action: Block; Direction: Outbound; Status: Enabled" in the access control policy list. Three available policies that contain the IP address were found.

The policy contained the **Block-Malicious-Outreach** blocking rule. According to the value of the **Hits** column, a large number of sessions have been blocked.

**Figure 3-4** Searching for a protection rule

Prio...	Name	Direction	Source	Destination	Service	Action	Hits	Status	Tags	Operation
1	Block-...com	Outbound	120.48.165.126	*.com	TCP:855351-85535	Block	0	Enabled	--	Edit   Configure Priority   More
3	Block-Malicious-Outreach	Outbound	0.0.0.0	0.0.0.0	Any	Block	9,821	Enabled	test@rest	Edit   Configure Priority   More
4	Allow-Asia	Outbound	126	Antarctica, Africa, North...	Any	Block	0	Enabled	--	Edit   Configure Priority   More

**CAUTION**

According to [Figure 3-4](#), there were three valid rules whose source IP addresses contain **xx.xx.xx.126**, including **Block-xxx-com** (with the highest priority), **Block-Malicious-Outreach**, and **Allow-Asia** (with the lowest priority). Besides the blocking rule **Block-Malicious-Outreach**, the administrator checked whether the two other two rules may intercept normal services.

Finally, it is found that the EIP accessed suspicious IP addresses so that an administrator configured a blocking rule it, but the configured destination was incorrect. As a result, all external traffic is blocked by mistake (see the second protection rule in [Figure 3-4](#)).

- Step 4** The administrator changed the destination address to a specific IP address that needs to be blocked, and enabled protection for the EIP on the **Assets > EIPs** page of the CFW console. After protection was restored, the traffic of the EIP was normally forwarded by CFW.
- Step 5** The administrator viewed the external connection logs related to the IP address in the traffic logs and confirmed that the service was restored.

----End

### Cause 3: Traffic Blocked by Intrusion Prevention

The protection mode of intrusion prevention functions, such as IPS, is too strict, blocking normal traffic.

You can take the following measures:

In the **Attack Event Logs** tab, search for logs about the blocked IP address or domain name.

- If no records are found, [submit a service ticket](#).
- If a record is found, perform either of the following operations:
  - Copy the rule ID. In the corresponding module (such as IPS), set the protection mode of the rule with that ID to **Observe**. For details about the intrusion prevention module, see [Configuring Intrusion Prevention](#).
  - Add the IP addresses that do not need to be protected by CFW to the whitelist. For details about how to configure the whitelist, see [Adding an Item to the Blacklist or Whitelist](#).

#### Case

Handling process: Detect a fault -> Change the protection status -> View logs -> Confirm services -> Modify the policy -> Restore the protection status -> Confirm logs

The O&M personnel of a company found that a service on the server whose IP address was **xx.xx.xx.99** cannot be accessed. It was suspected that the service was blocked by the firewall.

The firewall administrator took the following measures:

**Step 1** To quickly recover the service, the administrator logged in to the CFW console, choose **Attack Defense > Intrusion Prevention**, and changed the protection mode from **Intercept mode - strict** to **Observe**.

During this period, the firewall did not intercept attack traffic but only logged the attack traffic.

**Step 2** The administrator chose **Log Audit > Log Query** and clicked the **Attack Event Logs** tab. The logs about the access to the destination IP address **xx.xx.xx.99** were displayed. The IPS rule whose ID was 334841 blocked the traffic.

**Figure 3-5** Filtering attack event logs

Time	Attack	Severity	Rule ID	Rule Name	Source	Source C...	Source...	Destina...	Destina...	Destina...	Protocol	Applica...	Direction	Action	Operation
Mar 20, 2024 09:22:17	Vulnerability	Critical	331978	Apache Flank...	94	CN	38616	90	--	80	TCP	HTTP	Inbound	Block	View
Mar 20, 2024 09:22:17	Vulnerability	Critical	331978	Apache Flank...	94	CN	38616	90	--	80	TCP	HTTP	Inbound	Block	View
Mar 20, 2024 09:22:17	Vulnerability	Critical	331978	Apache Flank...	94	CN	38616	90	--	80	TCP	HTTP	Inbound	Block	View
Mar 20, 2024 09:22:17	Vulnerability	Critical	331978	Apache Flank...	94	CN	38616	90	--	80	TCP	HTTP	Inbound	Block	View
Mar 20, 2024 09:22:17	Vulnerability	Critical	331978	Apache Flank...	94	CN	38616	90	--	80	TCP	HTTP	Inbound	Block	View
Mar 20, 2024 09:22:17	Vulnerability	Critical	331978	Apache Flank...	94	CN	38616	90	--	80	TCP	HTTP	Inbound	Block	View

**Step 3** The administrator clicked **Details** in the **Operation** column, clicked **Payload Content** in the display page, and **created a packet capture task** to verify that the service is normal. The administrator searched for the rule whose ID is 334841 from the list on the **Basic Protection** tab page by referring to **Modifying the Action of a Basic Protection Rule**.

**Figure 3-6** Rule 334841

ID	Name	Updated In	Description	Risk Level	CVE ID	Rule Type	Affected Softw...	Rule Group	Default Action	Current Action	Operation
334841	Cross-site Scripting	2021	--	High	--	Vulnerability Attack	Others	Strictly	Intercept	Intercept	Observe Intercept Disable

**Step 4** The administrator clicked **Observe** in the **Operation** column. This rule did not block the traffic matching the signature but only logged the traffic.

**Step 5** The administrator set the protection mode to **Intercept mode - strict** and went to the **Basic Protection** tab to confirm that the **Current Status** of the rule 334841 was still **Observe**.

**Step 6** In the **Attack Event Logs** tab, after the service session matched the rule, the **Action** of the log was **Allow**. The service was restored.

----End

## Submitting a Service Ticket

If the preceding methods cannot solve your problem, [submit a service ticket](#).

## 3.2 Why Are Traffic and Attack Logs Incomplete?

Traffic and attack logs are recorded only when CFW is enabled. If it is disabled, no logs are generated for this period until it is enabled again.


To let CFW generate full logs, keep it enabled all along.


### 3.3 Why Does a Protection Rule Not Take Effect?

#### All Traffic Is Allowed Even If a Rule Is Configured to Allow Only Several EIPs

After EIP protection is enabled on CFW, the access control policy allows all traffic by default. If you want to allow traffic of only several EIPs, you need to configure a protection rule to block all traffic and set the lowest priority.

**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.

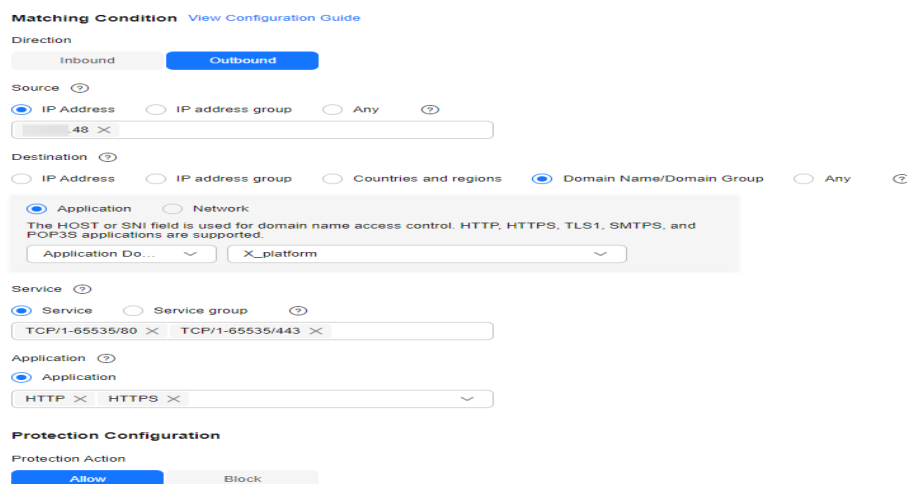
**Step 3** In the navigation pane on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.

**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 of a firewall to go to its details page.

**Step 5** In the navigation pane, choose **Access Control > Access Policies**. The **Access Policies** page is displayed. Click the **Internet Boundaries** or **Inter-VPC Borders** tab.

**Step 6** Configure a global blocking rule. Click **Add Rule**. Use the parameter settings shown in [Figure 3-7](#) and configure other parameters as needed.

**Figure 3-7** Blocking all traffic



The screenshot shows the 'Matching Condition' configuration page for a Cloud Firewall rule. The 'Direction' is set to 'Outbound'. Under 'Source', 'IP Address' is selected with a value of '48'. Under 'Destination', 'Domain Name/Domain Group' is selected. Under 'Service', 'Service' is selected with values 'TCP/1-65535/80' and 'TCP/1-65535/443'. Under 'Application', 'Application' is selected with values 'HTTP' and 'HTTPS'. Under 'Protection Configuration', 'Protection Action' is set to 'Block'.

#### NOTE

You are advised to enable the rules after adding all required ones.

**Step 7** Configure an allow rule. For details about how to add a protection rule, see [Adding a Protection Rule](#).

- Step 8** Set the priority of the global blocking rule in the **Step 6** to the lowest. For details, see [Setting the Priority](#).
- Step 9** Enable all rules. You are advised to enable the allow rules prior to the blocking rules.
- End

## Blocked IP Addresses Are Still Allowed Through Even If a Global Blocking Rule Is Configured

The protection rules configured on CFW are applied based on the EIP management list. If you have enabled global blocking (0.0.0.0/0) but the traffic of EIPs not in an allow rule is allowed through, check whether the IP addresses are in the EIP list. If not, synchronize the resource configuration. For details, see [Enabling EIP Protection](#).

## 3.4 What Do I Do If IPS Blocks Normal Services?

If normal service traffic is intercepted, perform either of the following operations:

- Query the ID of the rule that blocks traffic and modify the action of the rule in the IPS rule library. For details, see [Querying Hit Rules and Modifying Protection Actions](#).
- Use a less strict IPS protection mode. For details, see [Configuring Intrusion Prevention](#).

### Querying Hit Rules and Modifying Protection Actions



- 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 on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.
- 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 of a firewall to go to its details page.
- Step 5** In the navigation pane, choose **Log Audit > Log Query**. Click the **Attack Event Logs** query and record the **Rule ID** of the rule that blocks traffic.

Figure 3-8 Rule ID

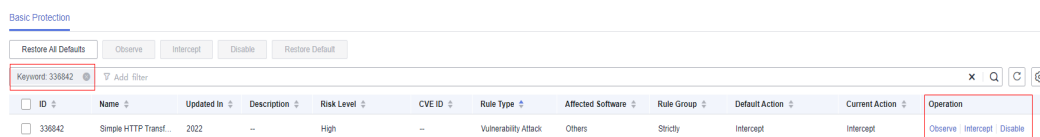
Attack Type	Severity	Rule ID	Matched Rule
Vulnerability ...	High	336842	Simple HTT...

- Step 6** In the navigation pane, choose **Attack Defense > Intrusion Prevention**. Click **View Effective Rules** under **Basic Protection**. The **Basic Protection** tab is displayed.

**Step 7** Search for the rule by its ID. In the **Operation** column, change its action to **Observe** or **Disable**.

- **Observe:** The firewall logs the traffic that matches the current rule and does not block the traffic.
- **Disable:** The firewall does not log or block the traffic that matches the current rule.

**Figure 3-9** Changing the protection mode of a rule



The screenshot shows the 'Basic Protection' page in the Cloud Firewall console. At the top, there are buttons for 'Restore All Defaults', 'Observe', 'Intercept', 'Disable', and 'Restore Default'. Below this is a search bar with the keyword '336842' and an 'Add Filter' button. A table lists the protection rules. The first rule is highlighted, and its 'Operation' column is expanded to show 'Observe', 'Intercept', and 'Disable' options.

ID	Name	Updated In	Description	Risk Level	CVE ID	Rule Type	Affected Software	Rule Group	Default Action	Current Action	Operation
336842	Simple HTTP Transf...	2022	--	High	--	Vulnerability Attack	Others	Strictly	Intercept	Intercept	Observe   Intercept   Disable

-----End

## 3.5 Why Is No Data Displayed on the Access Control Logs Page?

Access control logs record the traffic that matches the ACL protection policy. To view access control logs, configure the ACL policy first.

- For details about how to add a protection rule, see [Adding a Protection Rule](#).
- For details about the records of all traffic passing through CFW, see [Traffic Logs](#).
- For details about attack event records, see [Attack Event Logs](#).

# 4 Network Traffic

---

## 4.1 How Do I Calculate the Number of Protected VPCs and the Peak Protection Traffic at the VPC Border?

Pay-per-use firewalls are charged based on the actual protection status. The maximum bandwidth of a pay-per-use firewall (total traffic that can pass through the firewall) is 1 Gbit/s.

Yearly/Monthly CFW: By default, the CFW professional edition protects two VPCs, providing 200 Mbit/s protection for VPC border traffic. To protect more inter-VPC traffic, you can purchase more VPC protection quotas. Each quota provides 200 Mbit/s protection for VPC border traffic.

For example, CFW protects two VPCs (200 Mbit/s in total) by default. To protect 1 Gbit/s VPC border traffic, you need to purchase four more quotas (4 x 200 Mbit/s). The VPC border protection traffic = Default protection traffic (200 Mbit/s) + 4 x VPC protection quotas (200 Mbit/s) = 1 Gbit/s.

## 4.2 How Does CFW Collect Traffic Statistics?

Currently, CFW collects traffic statistics based on sessions. Traffic data is reported when the connection is terminated.

### NOTE

- The overall traffic of the session is counted from the time the session starts to the time it ends.
- The Internet border involves inbound (internet originated) traffic and outbound (server originated) traffic.

## 4.3 What Is the Protection Bandwidth Provided by CFW?

CFW protects traffic exchanged between the Internet border and VPCs. You can increase the protection bandwidth as required. CFW protection bandwidth varies according to the edition you purchase.

- Internet direction: 10 Mbit/s for the standard edition, and 50 Mbit/s for the professional edition.

### NOTE

The value of the protection bandwidth in the Internet direction is the maximum value of inbound or outbound traffic.

### NOTE

If your traffic is higher than the current protection bandwidth, purchase more protection capacity. For details, see [Modifying Extension Packages](#).

## 4.4 What Do I Do If My Service Traffic Exceeds the Protection Bandwidth?

If your actual service traffic exceeds the protection bandwidth you purchased, packet loss may occur. You can purchase more EIP protection capacity as needed.

For details about how to purchase an expansion package, see [Adding the EIP Protection Capacity](#).

### NOTE

You can configure high traffic warning in CFW. An alarm will be sent if your service traffic reaches the specified proportion of purchased bandwidth. For more information, see [Alarm Notification](#).

## 4.5 What Are the Differences Between the Data Displayed in Traffic Trend Module and the Traffic Analysis Page?

The methods of collecting traffic statistics on the two modules are different.

- The **Traffic Trend** area on the **Dashboard** page displays the inbound, inter-VPC, and outbound traffic based on traffic statistics in real time.
- In the **Traffic Analysis** module, traffic data is collected based on session statistics and reported when the connection is terminated. The following traffic data is displayed:
  - **Inbound Traffic**
  - **Outbound Traffic**
  - **Inter-VPC Access**



## 4.6 How Do I Verify the Validity of an Outbound HTTP/HTTPS Domain Protection Rule?

To verify the validity, perform the following steps:

**Step 1** Send an HTTP or HTTPS request.

- Method 1: Use the **curl** command. For example:  

```
curl -k "https://www.example.com"
```
- Method 2: Use a browser to access the domain name.

---

 **CAUTION**

Do not run the **telnet** command to test the domain name.

If the **telnet** command is used to test the domain name and port (for example, **telnet www.example.com 80**), only TCP handshake traffic is generated, and no complete HTTP or HTTPS requests will be simulated. In this case, the application type will be identified as unknown and will not hit the HTTP or HTTPS application policy.

---

**Step 2** Log in to the CFW management console and view the number of hits and log records of the protection rule. If new hits and records are found, the rule takes effect. If not, modify the protection rule in a timely manner.

1. Choose **Access Control > Access Policies**. On the **Protection Rules** tab, view the number of rule hits.
2. Choose **Log Audit > Log Query**. On the **Access Control Logs** tab, view the protection records of the rule.

----End

# 5 Billing

---

## 5.1 How Is CFW Billed?

CFW can be billed in yearly/monthly (prepaid) or pay-per-use mode. For details, see [Pricing](#).

In the standard edition, you can increase the number of protected EIPs and peak Internet border traffic.

In the professional edition, you can increase the number of protected EIPs, peak Internet border traffic, and the number of protected VPCs.

- For details about CFW billing mode, see [Billing](#).
- For more information, see [Editions](#).


## 5.2 How Do I Change My CFW Edition?


The CFW standard edition can be upgraded to the professional edition, but the professional edition cannot be changed to the standard edition. To change to a lower edition, unsubscribe from the current edition and purchase the required one.

For details about unsubscription, see [How Do I Unsubscribe from CFW?](#)

### Upgrading the Standard Edition to the Professional Edition

**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 on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.

**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 of a firewall to go to its details page.

- Step 5** In the upper right corner of the page, click **Upgrade to Professional Edition**. The CFW purchase page is displayed.
- Step 6** Confirm the edition specifications and click **Buy Now**.
- Step 7** Confirm the order details, select **I have read and agreed to the Huawei Cloud Firewall Service Statement**, and click **Next**.
- Step 8** Select a payment method and pay for your order.

----End

## 5.3 Can I Switch Between Yearly/Monthly and Pay-per-Use Payments for CFW?

No. Yearly/Monthly packages and pay-per-use subscriptions cannot be changed to each other.

You are advised to unsubscribe from CFW and purchase it again. For details, see [How Do I Unsubscribe from CFW?](#)

## 5.4 How Do I Renew CFW?

This section describes how to renew CFW when it is about to expire. After the renewal, you can continue to use CFW.



- Before your CFW subscription expires, the system will send an SMS message or email to remind you to renew it.
- After your CFW expires, there is a retention period for you.

This period varies depending on account. For details, see [Retention Period](#).

### NOTE

To avoid unnecessary loss caused by security issues, renew your subscription before the retention period expires.

### Procedure

- 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 on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.
- Step 4** In the upper right corner of the **Firewall Details** area, click **Renew**.
- Step 5** Select a renewal duration and optionally select **Renew on the standard renewal date**.
- Step 6** Confirm the price and click **Pay**.

**Step 7** Select a payment method and make your payment. Once the order is paid for, the renewal is complete.

----End


## 5.5 How Do I Unsubscribe from CFW?


This section describes how to unsubscribe from CFW billed in yearly/monthly mode.

The original CFW configurations will be deleted after unsubscription and cannot be restored. You are advised to export protection policies before unsubscription, and import them after you purchase another CFW instance. For details about how to import and export policies, see [Managing Protection Rules in Batches](#).

### Procedure (for Yearly/Monthly Firewalls)

**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 on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.

**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 of a firewall to go to its details page.

**Step 5** Click **Unsubscribe** in the upper right corner of the **Firewall Details** area.

**Step 6** Confirm the resource to be unsubscribed from and click **OK**.


**Step 7** After confirming that the information is correct, select **I understand that a handling fee will be charged for this unsubscription**.


**Step 8** Click **Next** and complete the subsequent operations.

----End

### Procedure (for Pay-per-Use Firewalls)

**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 on the left, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed.

**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 of a firewall to go to its details page.

**Step 5** In the upper right corner of the **Firewall Details** area, click **Delete**.

**Step 6** Confirm the resource to be unsubscribed from, enter **DELETE**, and click **OK**.

----**End**