Cloud Firewall

FAQs

Issue 10

Date 2024-01-15

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property 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 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 Consulting

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?

CFW supports cross-account protection. Before protection, perform the following operations:

- For details about Internet border cross-account protection, see **Multi-Account Management Overview**.
- For VPC border cross-account protection, when you add VPC attachments in "Step 3: Configure an Enterprise Router", share the enterprise router of account A with account B, and then add attachments in account B. Subsequent configurations are still performed on account A. For details about an inter-VPC border firewall, see **VPC Border Firewall Overview**.

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	Cloud Firewall (CFW) is a next-generation cloud-native firewall. It protects Internet and VPC borders 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.	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). For details about WAF, see **What Is Web Application Firewall?**
Protection	• EIP and VPC borders • Basic protection against web attacks • Defense against external intrusions and protection of proactive connections to external systems	• WAF protects web applications on Huawei Cloud and other clouds and on-premises applications through domain names or IP addresses. • Comprehensive protection against web attacks
Features	• Asset management and intrusion defense: It detects and defends against intrusions into cloud assets that are accessible over the Internet in real time. • Access control: You can control access at Internet borders. • Traffic Analysis and log audit: CFW controls, analyzes, and visualizes VPC traffic, audits logs, and traces traffic sources.	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.

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.

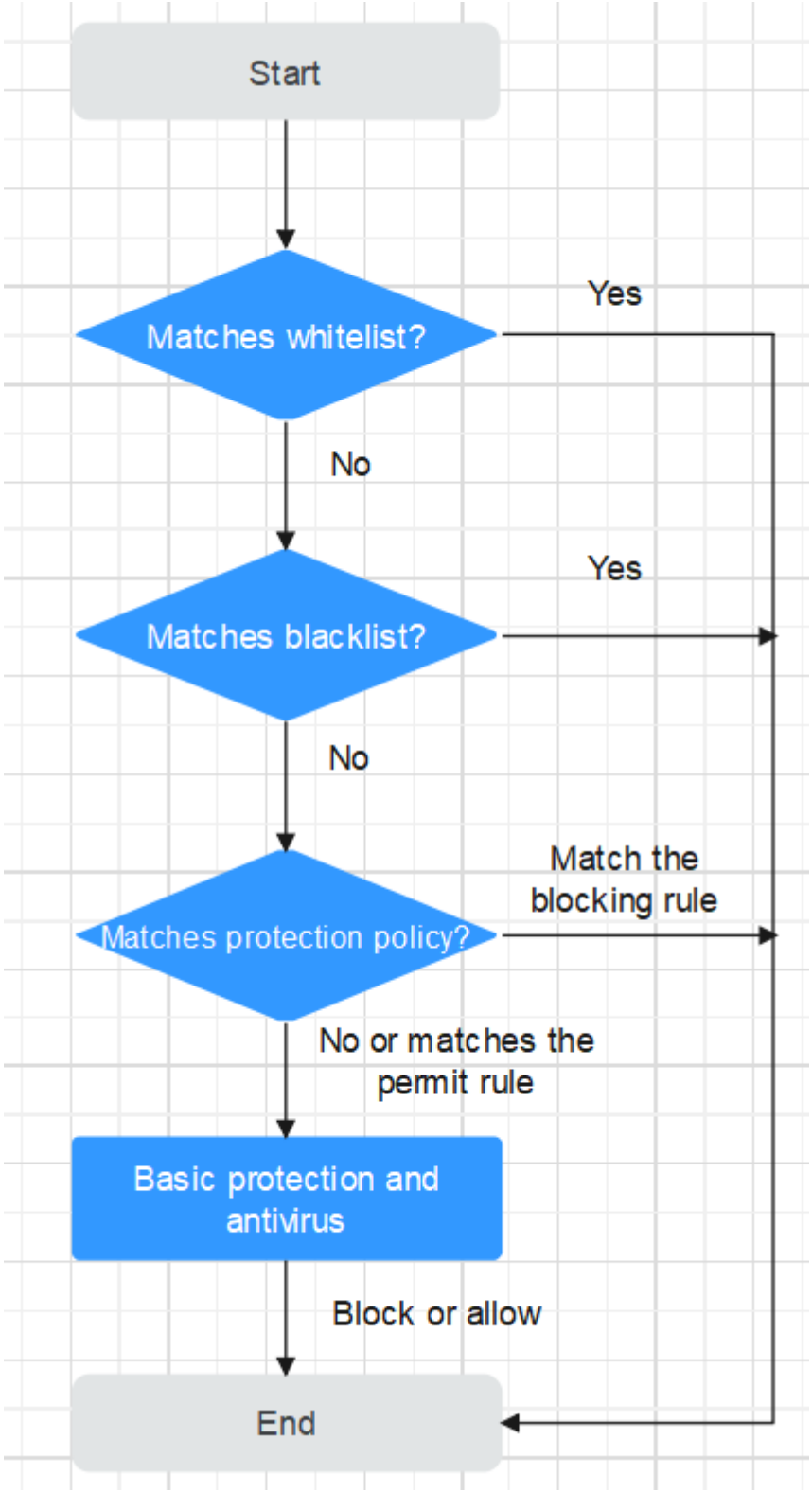
Table 1-2 Differences between CFW, security groups, and network ACLs

Item	CFW	Security group	Network ACL
Definition	Cloud Firewall (CFW) is a next-generation cloud-native firewall. It protects Internet and VPC borders 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 **Security Groups and Security Group Rules**.	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 **Network ACL**.
Protected objects	• Internet boundary • VPC boundary • SNAT scenario	ECS	Subnet
Features	• Filtering by 5-tuple (source IP address, destination IP address, protocol, source port, and destination port) • Filtering by geographical location, domain name, domain name group, and blacklist/whitelist • Intrusion prevention system (IPS) and antivirus (AV).	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 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**.

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

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.

1.7 Can WAF, Advanced Anti-DDoS, and CFW Be Deployed Together?

Yes. WAF has three modes: exclusive mode, ELB mode, and cloud mode. The traffic trend varies depending on the mode. The details are as follows:

- Exclusive mode/ELB mode: Internet -> Advanced Anti-DDoS -> CFW -> WAF (dedicated mode/ELB mode) -> Origin server
- Cloud mode: Internet -> Advanced Anti-DDoS -> WAF (cloud mode) -> CFW -> Origin server

NOTE

- If you have purchased Advanced Anti-DDoS or WAF in cloud mode, exercise caution when configuring traffic blocking rules. You are advised to configure traffic permitting rules or whitelists.
- If you have purchased WAF in dedicated or ELB mode, configure it based on service requirements.
- For details, see **Precautions for Using CFW with WAF, Advanced Anti-DDoS, and CDN**.

2 Regions and AZs

2.1 What Are Regions and AZs?

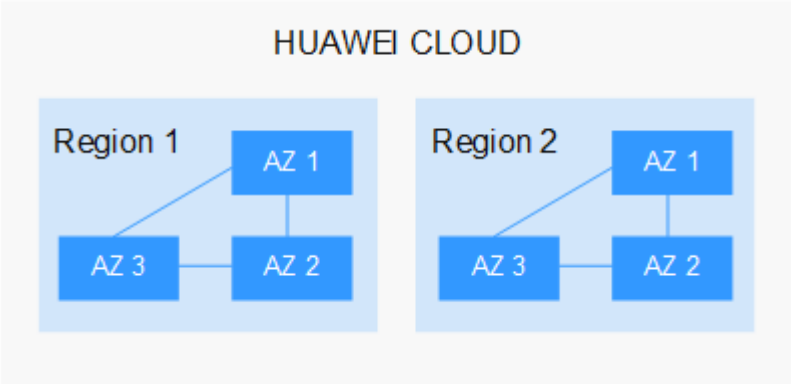
Concepts

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.

Figure 2-1 shows the relationship between the regions and AZs.

Figure 2-1 Region and AZ



Huawei Cloud provides services in many regions around the world. You can select a region and AZ as needed.

Selecting a Region

When selecting a region, consider the following factors:

- Location

  You are advised to select a region close to you or your target users. This reduces network latency and improves access rate.

  - If you or your users are in the Asia Pacific region and outside the Chinese mainland, select the **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore** region.
  - If you or your users are in Africa, select the **AF-Johannesburg** region.
  - If you or your users are in Latin America, select the **LA-Santiago** region.

- Resource price

  Resource prices may vary in different regions. For details, see **Product Pricing Details**.

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.

Regions and Endpoints

Before using an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

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 About Functions

3.1 What Details Can I Get from Logs?

On the **Log Query** page, you can view attack event logs, access control logs, and traffic logs.

- Attack event log: Information about the traffic detected by IPS, including the risk level, affected port, matched rule, and attack event type. If traffic is incorrectly blocked, you can modify the IPS protection action.
- Access control log: All traffic that matches the access control policy.
- Traffic log: All traffic passing through the firewall.

3.2 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 works 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**.

3.3 What Are the Precautions for Configuring a Protection Rule to Block IP Addresses?

Pay attention to the following points when configuring a protection rule to block IP addresses:

1. You are advised to preferentially configure accurate IP addresses (for example, 192.168.10.5) to reduce network segment configurations and avoid incorrect interception.
2. Exercise caution when configuring protection rules to block reverse proxy IP addresses, such as the back-to-source IP addresses of CDN, Advanced Anti-DDoS, and WAF. You are advised to configure protection rules or whitelist to permit reverse proxy IP addresses.

3. Forward proxy IP addresses (such as company egress IP addresses) have a large impact scope. Exercise caution when configuring protection rules to block forward proxy IP addresses.
4. When configuring region protection, you need to consider the situation that the public IP address may be changed.

3.4 Why Are Unprotected EIPs Displayed in CFW Attack Logs?

CFW collects information about all the attacked EIPs for you to better determine defense policies.

4 Troubleshooting

4.1 How Do I Troubleshoot CFW Protection When Service Traffic Is Abnormal?

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

Locating Method

Step 1 Disable CFW protection.

- 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**.

Step 2 Observe the service running status.

- If the services are restored, go to **Troubleshooting Methods**.
- If the fault persists, the traffic interruption is not caused by CFW but common faults:
  - 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**.

----End

Troubleshooting Methods

Step 1 In the **Access Control Logs** tab, search for logs about the blocked IP address or domain name.

- If a record exists, click the **Rule** column to go to the matched blocking policy. For details about subsequent operations, see **Scenario 1: Incorrect Protection Policy**.

- If no records exist, go to **Step 2**.

Step 2 In the **Attack Event Logs** tab, search for logs about the blocked IP address or domain name.

- If a record exists, copy the information in the **Rule ID** column. For details about subsequent operations, see **Scenario 2: Incorrect Interception by the Intrusion Prevention Function**.
- If no records exist, go to **Step 3**.

Step 3 If services are restored after EIP protection or the VPC border firewall is disabled, you are advised to disable firewall protection and **submit a service ticket**.

Step 4 (Optional) To monitor the firewall status and quickly detect exceptions, you are advised to:

- Configure alarm notification on the CFW console. For details, see **Alarm Notification**.
- Configure CFW alarm rules on the Cloud Eye console. For details, see **Setting Monitoring Alarm Rules**. For details about supported monitoring metrics, see **CFW Metrics**.

----End

Scenario 1: Incorrect Protection Policy

Possible causes

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.

Solution

- If the 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:
  - Search for the blocking rule of the IP address or domain name in the **ACL 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

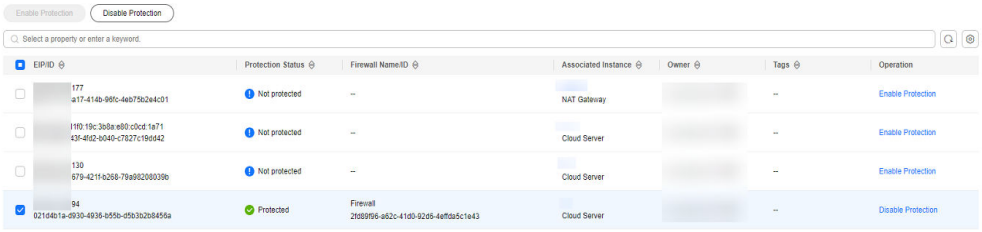
The network O&M personnel of a company found that an ECS cannot access the Internet through the bound EIP **xx.xx.xx.94**.

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.

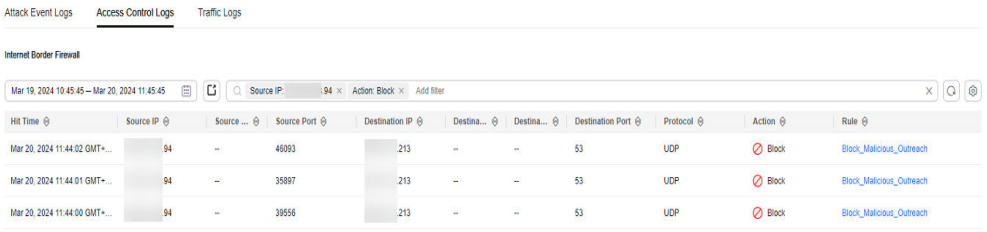
During the firewall is disabled, the traffic of the EIP is not processed and related logs are not displayed.

Figure 4-1 EIPs



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.94**. A blocking rule named **Block-Malicious-Outreach** was found, and this rule blocked the traffic from the EIP **xx.xx.xx.94** to the Internet.

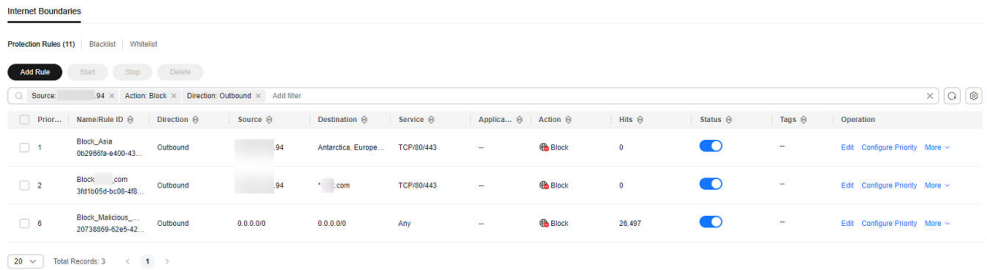
Figure 4-2 Filtering access control logs



Step 3 The administrator searched for "Source: xx.xx.xx.94; 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 4-3 Searching for a protection rule



> **CAUTION**
>
> According to **Figure 4-3**, there were three valid rules whose source IP addresses contain **xx.xx.xx.94**, 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 4-3**).

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

Scenario 2: Incorrect Interception by the Intrusion Prevention Function

Solution

- In the corresponding module (such as IPS), set the protection mode 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.90** cannot be accessed. It was suspected that the service was blocked by the firewall.

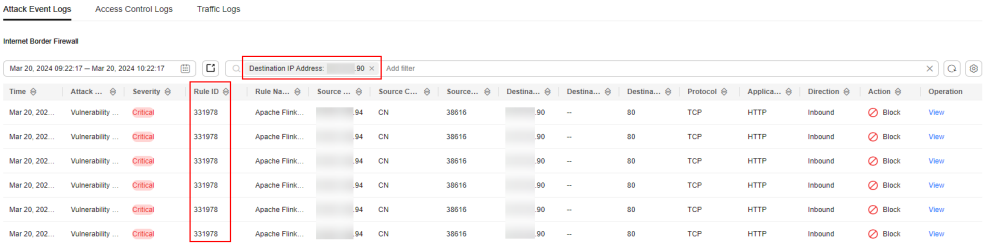
The firewall administrator took the following measures:

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.

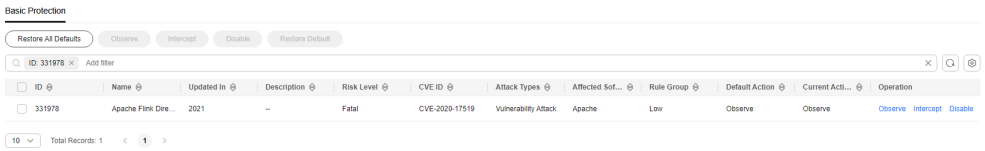
Step 2 The administrator chose **Log Audit** > **Log Query** and clicked the **Attack Event Logs** tab. The logs about the access to the destination IP address **xx.xx.xx.90** were displayed. The IPS rule whose ID was 331978 blocked the traffic.

Figure 4-4 Filtering attack event logs



Step 3 The administrator clicked **Details** in the **Operation** column, clicked **Payload Content** in the display page, and **created a packet capture task** to determine that the service is normal. The administrator searched for the rule whose ID is 331978 from the list on the **Basic Protection** tab page by referring to **Modifying the Action of a Basic Protection Rule**.

Figure 4-5 Rule 331978



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 331978 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

4.2 Why Are Traffic and Attack Logs Incomplete on the Traffic Analysis Page?

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.

4.3 Why Does a Configured Policy 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.

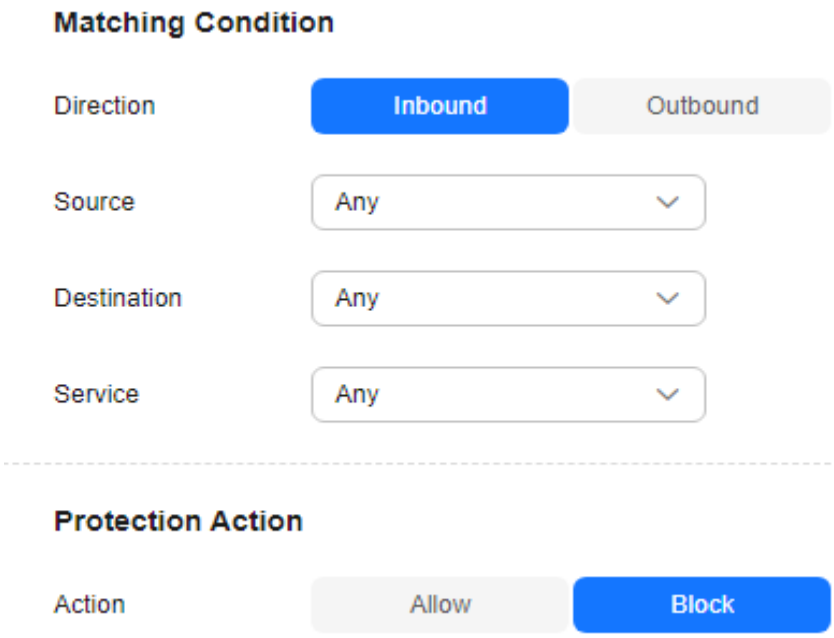
Step 3 In the navigation pane on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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 to go to the 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 4-6** and configure other parameters as needed.

Figure 4-6 Blocking all traffic



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**.

4.4 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**.

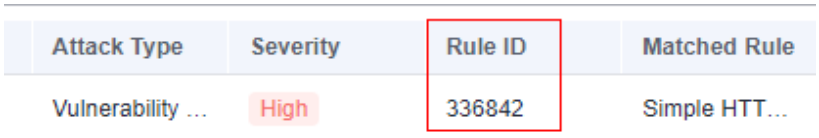
Step 2 Click  in the upper left corner of the management console and select a region or project.

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 to go to the 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 4-7 Rule ID



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.

----End

4.5 What Do I Do If There Is No Data in Access Control Logs?

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**.

4.6 What Are the Precautions for Configuring a NAT64 Defense Policy?

A firewall instance cannot protect the real source IP address before NAT64 translation. If you enable IPv6 translation for EIPs, NAT64 will translate a source IP address into a CIDR block of 198.19.0.0/16 for ACL access control.

For IPv6 access, you are advised to allow traffic from the predefined address group **NAT64 Address Set**. Access from all the IP addresses in the 198.19.0.0/16 CIDR block will be allowed. You can configure the blacklist or a blocking policy to block specific IP addresses.

- For details about the IPv6 EIP function, see **Assigning or Releasing an IPv6 EIP**.
- For details about **NAT64 Address Set**, see **NAT64 Address Set**.
- For details about how to configure the blacklist, see **Adding an Item to the Blacklist or Whitelist**.
- For details about how to configure a blocking policy, see **Adding a Protection Rule**.

4.7 Why Some Permissions Become Invalid After a System Policy Is Granted to an Enterprise Project?

Certain CFW functions depend on cloud services such as Elastic Cloud Server (ECS) and Virtual Private Cloud (VPC). Some functions of these cloud services do not support enterprise projects, so some permissions may become invalid after the **CFW FullAccess** and **CFW ReadOnlyAccess** system policies are granted to enterprise projects.

To avoid this problem, log in to your Huawei Cloud account to create two system policies. For details, see **Creating Custom Policies**.

- For the cloud services that CFW depends on, if they do not support enterprise projects, add the following content to grant permissions to them. For Log Tank Service (LTS), grant all permissions to it on the CFW page.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "vpc:quotas:list",
                "vpc:publicipTags:get"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:availabilityZones:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "lts:groups:list",
                "lts:groups:get",
            ]
        }
    ]
}
```

- CFW depends on the following global service permissions:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "eps:resources:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "tms:predefineTags:list"
            ]
        }
    ]
}
```

4.8 How Does Huawei Cloud CFW Detect and Defend Against Attacks Exploiting the Apache Log4j Remote Code Execution Vulnerability?

Apache Log4j2 has a remote code execution vulnerability (CVE-2021-44228). When Apache Log4j2 processes user input during log processing, attackers can construct special requests to trigger remote code execution. The POC has been disclosed and the risk is high.

On December 16, Apache announced that in versions earlier than 2.16.0, there was a remote code execution vulnerability (CVE-2021-45046).

Apache Log4j2 is a widely used Java-based logging utility. If you are an Apache Log4j2 user, check your system and implement timely security hardening.

Huawei Cloud CFW can detect and intercept the Apache Log4j2 remote code execution vulnerability.

Vulnerability Name

Apache Log4j remote code execution vulnerability

Affected Products

Affected versions:

2.0-beat9 <= Apache Log4j 2.x < 2.16.0 (Version 2.12.2 is not affected.)

Affected applications and components: spring-boot-starter-log4j2, Apache Solr, Apache Flink, and Apache Druid.

Secure versions:

Apache Log4j 1.x

Apache Log4j 2.16.0

Mitigation

Step 1 Rectify the fault by following the instructions provided on the Huawei Cloud website (**Apache Log4j2 Remote Code Execution Vulnerability**).

Step 2 Log in to the CFW console and perform the following operations:

1. Purchase the CFW standard edition. For details, see **Purchasing CFW**.
2. Enable **Basic protection** on the **Intrusion Prevention** page and set **Action** to **Block**. For details, see **Configuring Intrusion Prevention**.

----End

4.9 How Does Huawei Cloud CFW Detect and Defend Against Attacks Exploiting the Spring Framework Remote Code Execution Vulnerability?

Spring Framework is a lightweight open-source application framework for developing enterprise Java applications. A remote code execution vulnerability (CVE-2022-22965) 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.

Huawei Cloud CFW can detect and intercept attacks that exploit the Spring Framework remote code execution vulnerability.

Vulnerability Name

Spring Framework remote code execution vulnerability

Affected Versions

- JDK 9 or later
- Applications developed using the Spring Framework or derived framework

Mitigation

Step 1 See **Spring Framework Remote Code Execution Vulnerability**.

Step 2 Log in to the CFW console and perform the following operations:

1. Purchase the CFW standard edition. For details, see **Purchasing CFW**.
2. Enable **Basic protection** on the **Intrusion Prevention** page and set **Action** to **Block**. For details, see **Configuring Intrusion Prevention**.

----End

5 Network Traffic

5.1 What Does Traffic Analysis Provide?

On the **Traffic Analysis** page, you can view the internet inbound and outbound traffic and attack trend of your assets in the **Last 1 hour**, **Last 24 hours**, and **Last 7 days**.

5.2 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 and outbound traffic, or internet originated traffic and server originated traffic.

5.3 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**.

5.4 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.
- Inter-VPC protection: No protection bandwidths are provided in the standard edition. The professional edition protects 200 Mbit/s traffic per month by default.

NOTE

The protection traffic you need should be determined based on the maximum inbound or outbound traffic, whichever is higher. If your traffic is higher than the current protection bandwidth, purchase more protection capacity. For details, see **Adding the EIP Protection Capacity**..

5.5 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, outbound, and inter-VPC 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**

6 APIs

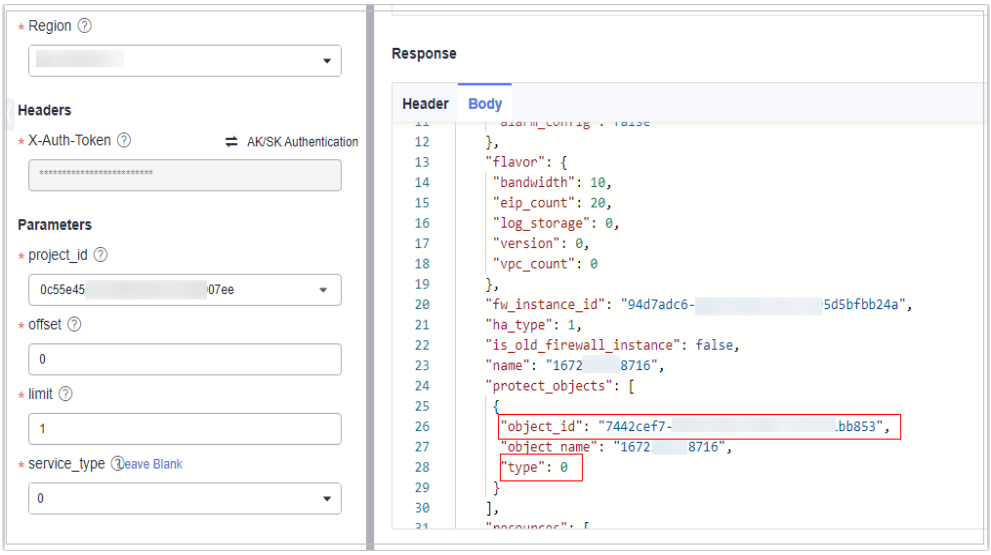
6.1 What is Object_Id?

Object_Id is the ID of a protected object. It is used to distinguish Internet border protection from VPC border protection after CFW is created.

You can obtain the value by calling the API of **Querying a Firewall Instance**.

- If **type** is **0**, **Object_Id** indicates the ID of a protected Internet border object.
- If **type** is **1**, **Object_Id** indicates the ID of a protected VPC border object.

Figure 6-1 Object_Id and type



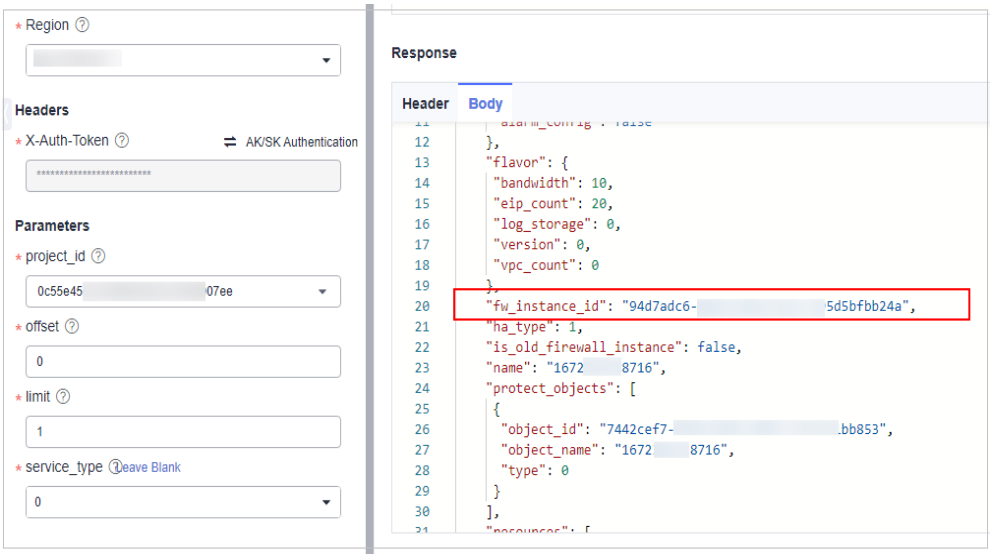
6.2 What Is Firewall_Instance_Id?

Firewall_Instance_Id is a CFW instance ID. It is automatically generated by the system after CFW is created.

- By default, if **fw_instance_Id** is not specified, information about the first firewall under the account is returned. If **fw_instance_Id** is specified, information about the firewall with this **fw_instance_Id** is returned.
- If **object_Id** is specified, information about the firewall with this **object_Id** is returned by default. If both **fw_instance_Id** and **object_Id** are specified, the specified **object_Id** must belong to the specified firewall.

You can obtain the value by calling the API of **Querying a Firewall Instance**.

Figure 6-2 Firewall_Instance_Id



7 Billing

7.1 How Is CFW Billed?

CFW can be billed in yearly/monthly (prepaid) 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**.

7.2 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 an 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 to go to the 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

7.3 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, click **Renew**.

Step 5 On the renewal management page, complete the renewal.

For details, see **Renewal Rules**.

----End

7.4 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, see **Managing Protection Rules in Batches**.

Procedure

Step 1 **Log in to the management console**.

Step 2 In the upper right part of the page, click **Billing & Costs**. The **Billing Center** page is displayed.

Step 3 In the navigation pane on the left, choose **Orders** > **Cloud Service Unsubscriptions**.

Step 4 Complete the unsubscription operations.

For more details, see **Unsubscription Rules**.

----End

A Change History

Date	Description
2024-01-15	This is the tenth official release. Added: • **Can WAF, Advanced Anti-DDoS, and CFW Be Deployed Together?** • **How Do I Troubleshoot CFW Protection When Service Traffic Is Abnormal?** • **What Are the Differences Between the Data Displayed in Traffic Trend Module and the Traffic Analysis Page?**
2023-12-20	This is the ninth official release. Added **What Are the Precautions for Configuring a NAT64 Defense Policy?**.
2023-10-13	This is the eighth official release. Added: • **What Are the Differences Between CFW, Security Groups, and Network ACLs?** • **What Do I Do If IPS Blocks Normal Services?**
2023-08-11	This is the seventh official release. Added: **How Do I Calculate the Number of Protected VPCs and the Peak Protection Traffic at the VPC Border?**

Date	Description
2023-07-14	This is the sixth official release. Added: • **What Are the Priorities of the Protection Settings in CFW?** • **What Do I Do If There Is No Data in Access Control Logs?** Added description about cross-account usage in **Can CFW Be Shared Across Accounts?**.
2023-05-31	This is the fifth official release. Added: • **Why Some Permissions Become Invalid After a System Policy Is Granted to an Enterprise Project?** • **How Do I Change My CFW Edition?**
2023-01-19	This is the fourteenth official release. Added: • "Billing" section. • **APIs**
2022-10-28	This is the third official release. Modified the description about protection bandwidth in **What Is the Protection Bandwidth Provided by CFW?**
2022-09-30	This is the second official release. Added **Why Does a Configured Policy Not Take Effect?**.
2022-07-30	This is the first official release.

