

# Cloud Firewall

## Getting Started

**Issue** 01  
**Date** 2023-07-21



**Copyright © Huawei Cloud Computing 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 Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI 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.

---

# Contents

---

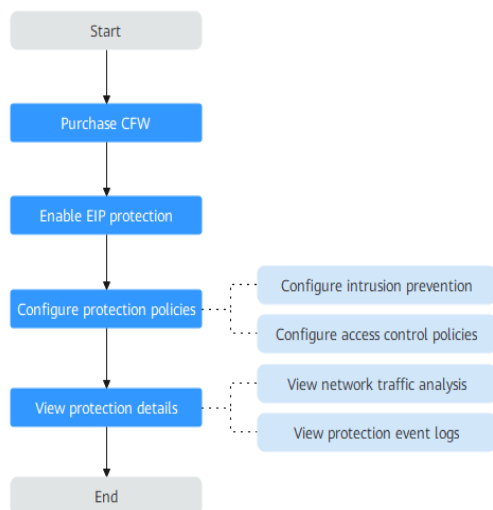
|                                                     |           |
|-----------------------------------------------------|-----------|
| <b>1 Overview</b>                                   | <b>1</b>  |
| <b>2 Step 1: Purchase CFW</b>                       | <b>2</b>  |
| <b>3 Step 2: Enable EIP Protection</b>              | <b>6</b>  |
| <b>4 Step 3: Configure a Protection Policy</b>      | <b>8</b>  |
| 4.1 Configuring Intrusion Prevention                | 8         |
| 4.2 Configuring an Access Control Policy            | 11        |
| <b>5 (Optional) Step 4: View Protection Details</b> | <b>13</b> |
| 5.1 Viewing Network Traffic Analysis                | 13        |
| 5.2 Viewing Protection Event Logs                   | 15        |
| <b>6 Getting Started with Common Practices</b>      | <b>19</b> |

# 1 Overview

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.

This document describes how to use CFW to protect the Internet border. The following figure shows [the process of using CFW](#).

**Figure 1-1** Process



# 2 Step 1: Purchase CFW

You can purchase CFW in yearly/monthly mode.

## Edition Description

CFW provides the standard edition, and the professional edition. You can use access control, intrusion prevention, traffic analysis, and log audit functions on the console.


**Table 2-1** Editions


| Feature                |                                                                                                                               | Standard               | Professional                                          |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|------------------------|-------------------------------------------------------|
| Protection             | Protected EIPs at Internet boundary                                                                                           | 20 (expandable)        | 50 (expandable)                                       |
|                        | Peak protection traffic at Internet boundary                                                                                  | 10 Mbit/s (expandable) | 50 Mbit/s (expandable)                                |
|                        | Protected VPCs                                                                                                                | ×                      | 2 (expandable)                                        |
|                        | Max. peak protection traffic between VPCs                                                                                     | ×                      | 200 Mbit/s (can be increased with the number of VPCs) |
| Access traffic control | ACL access control for public network assets (based on IP addresses, domain names, domain groups, and geographical locations) | √                      | √                                                     |
|                        | North-south traffic protection and cloud resource (including EIP) protection against risks on the Internet                    | √                      | √                                                     |

| Feature             |                                                                                        | Standard | Professional |
|---------------------|----------------------------------------------------------------------------------------|----------|--------------|
|                     | North-south traffic audit and log query                                                | √        | √            |
|                     | East-west traffic protection, asset protection between VPCs, and full traffic analysis | ×        | √            |
|                     | East-west traffic monitoring to obtain inter-VPC traffic data in real time             | ×        | √            |
| Protection policies | Intrusion prevention system (IPS)                                                      | √        | √            |
|                     | Custom IPS signature database                                                          | ×        | √            |
|                     | Virtual patching                                                                       | √        | √            |
|                     | Sensitive directories and reverse shells                                               | √        | √            |
|                     | Antivirus                                                                              | ×        | √            |

## Purchasing a Firewall in Yearly/Monthly Mode

**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** Click **Buy CFW** and configure parameters on the **Buy CFW** page. For more information, see [Table 2-2](#).

**Table 2-2** Yearly/Monthly CFW parameters

| Parameter | Description                                                                                                                                                                                                                                                                                                          |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Region    | Region where the CFW is to be purchased.<br><b>NOTICE</b><br>CFW can be used in the selected region only. To use CFW in another region, switch to the corresponding region and then purchase it. For details about the regions where CFW is available, see <a href="#">Can CFW Be Used Across Clouds or Regions?</a> |

| Parameter                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Edition                              | <p>Edition.</p> <ul style="list-style-type: none"> <li>• Standard</li> <li>• Professional</li> </ul> <p><b>NOTE</b><br/>For details about the differences between versions, see <a href="#">Editions</a>.</p>                                                                                                                                                                                                                                                                                                                                                                      |
| Engine                               | <p>Direct engine. You can implement fine-grained application control, for example, by using policies and limiting sessions. You can also take advantage of intrusion prevention, virus filtering, and defense functions to enhance access security, defend against attacks, and identify and control applications.</p>                                                                                                                                                                                                                                                             |
| Add EIP Protection Capacity          | <p>(Optional) Number of additional EIPs to be protected.<br/>Value range: 0 to 2000</p> <p><b>NOTE</b><br/>By default, 20 public IP addresses are protected by the standard edition (included in the package fee). If you have 65 public IP addresses, you only need to enter 45.</p>                                                                                                                                                                                                                                                                                              |
| Add Peak Traffic Protection Capacity | <p>(Optional) Additional peak inbound or outbound traffic. The value range is 0 to 5000 Mbit/s per month. (The value must be an integer multiple of 5.)</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• By default, up to 10 Mbit/s per month is protected by the standard edition (included in the package fee). If your protection traffic is 200 Mbit/s per month, you only need to enter 190 Mbit/s per month.</li> <li>• The protection traffic is determined based on the maximum inbound or outbound traffic, whichever is higher.</li> </ul>               |
| Enterprise Project                   | <p>Select an enterprise project from the drop-down list. This option is only available if you have logged in using an enterprise account, or if you have enabled enterprise projects. To use this function, <a href="#">Enable Enterprise Center</a>. You can use an enterprise project to centrally manage your cloud resources and members by project.</p> <p><b>NOTE</b><br/>Value <b>default</b> indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.</p> |
| Firewall Name                        | <p>Firewall name.</p> <p>It must meet the following requirements:</p> <ul style="list-style-type: none"> <li>• Only letters (A to Z and a to z), numbers (0 to 9), spaces, and the following characters are allowed: - _</li> <li>• The value can contain 1 to 48 characters.</li> </ul>                                                                                                                                                                                                                                                                                           |

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advanced Settings | <p><b>Tag:</b> You can use a tag for multiple cloud resources. You are advised to predefine tags in TMS. For details, see <a href="#">Resource Tag Overview</a>.</p> <p>If your organization has configured a tag policy for CFW, you need to add tags in compliance with the policy. If a tag does not comply with the tag policies, firewall instance creation may fail. Contact your organization administrator to learn more about tag policies.</p> |
| Required Duration | <p>Service duration.</p> <p>After selecting a duration, you can select <b>Auto-renew</b>. If you select and agree to service auto renewal, the system automatically generates a renewal order based on the subscription period and renews the service before it expires. Note the <a href="#">Auto-Renewal Rules</a> when enabling auto-renewal.</p>                                                                                                     |

**Step 5** Confirm the purchase information and click **Buy Now**.

**Step 6** Confirm the order details, select **I have read and agreed to the Huawei Cloud Firewall Service Statement**, and click **Next**.

**Step 7** Select a payment method and pay for your order.

----End

## Effective Conditions

Your CFW instance is purchased when your instance edition and its quota information are shown in the upper left corner of the management console.



# 3 Step 2: Enable EIP Protection


---


When you use CFW for the first time, you need to synchronize assets and enable protection for EIP assets so that your service traffic can pass through CFW.

After EIP protection is enabled, the default action of CFW is **Allow**. CFW will block traffic based on your protection policy.

## 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** (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 EIP page is displayed. The EIP information is automatically updated to the list.

**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.

---

### NOTICE

- Currently, IPv6 addresses cannot be protected.
  - An EIP can only be protected by one firewall.
  - Only EIPs in the enterprise project to which the current account belongs can be protected.
-

**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 action of the access control policy is **Allow**.

----**End**



# 4 Step 3: Configure a Protection Policy

---

## 4.1 Configuring Intrusion Prevention

CFW provides you with basic defense functions, and, with many years of attack defense experience, it detects and defends against a wide range of common network attacks and effectively protects your assets.

### 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** (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 **Attack Defense > Intrusion Prevention**.

**Table 4-1** Intrusion prevention functions

| Function         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protection Mode  | <ul style="list-style-type: none"> <li>● <b>Observe:</b> Attacks are detected and recorded in logs but are not intercepted.</li> <li>● <b>Intercept:</b> Attacks and abnormal IP address access are automatically intercepted.                             <ul style="list-style-type: none"> <li>- <b>Intercept mode - loose:</b> The protection granularity is coarse. In this mode, only attacks with high threat and high certainty are blocked.</li> <li>- <b>Intercept mode - moderate:</b> The protection granularity is medium. This mode meets protection requirements in most scenarios.</li> <li>- <b>Intercept mode - strict:</b> The protection granularity is fine-grained, and all attack requests are intercepted.</li> </ul> </li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>● You are advised to use the <b>observe</b> mode for a period of time before using the <b>intercept</b> mode. For details about how to view attack event logs, see <a href="#">Attack Event Logs</a></li> <li>● If packets are incorrectly intercepted, you can modify the action of a single defense rule in the basic defense rule library. For details about operations, see <a href="#">Managing Intrusion Prevention</a>.</li> </ul> |
| Basic Protection | <p>Basic protection on your assets. It is enabled by default. Its functions are as follows:</p> <ul style="list-style-type: none"> <li>● Scan for threats and scan vulnerabilities.</li> <li>● Detects whether traffic contains phishing, Trojan horses, worms, hacker tools, spyware, password attacks, vulnerability attacks, SQL injection attacks, XSS attacks, and web attacks.</li> <li>● Checks whether there are protocol anomalies, buffer overflow, access control, suspicious DNS activities, and other suspicious behaviors in traffic.</li> </ul> <p><b>NOTE</b><br/>For details about how to view basic defense rules, see <a href="#">Checking the IPS Rule Library</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Virtual Patching | <p>Hot patches are provided for IPS at the network layer to intercept high-risk remote attacks in real time and prevent service interruption during vulnerability fixing.</p> <p>New IPS rules are displayed in the virtual patch rule library. To view the rule library, click <b>View Virtual Patch</b>. For details about the parameters in the rule library, see <a href="#">Checking the IPS Rule Library</a>.</p> <p><b>Auto Update:</b> After this function is enabled, rules in the virtual patch take effect. Protection is implemented in real time and protection actions can be manually modified.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Function             |                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Custom IPS Signature |                                  | <p>If the basic defense rule library does not meet your requirements, you can create custom IPS signatures.</p> <p>Only the professional edition support custom IPS signatures. For details, see <a href="#">Customizing IPS Signatures</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Advanced             | Sensitive Directory Scan Defense | <p>Defense against scan attacks on sensitive directories on your servers.</p> <p><b>Action:</b></p> <ul style="list-style-type: none"> <li>● <b>Observe:</b> If a sensitive directory scanning attack is detected, CFW records it in logs only. For details about how to view attack logs, see <a href="#">Attack Event Logs</a>.</li> <li>● <b>Block session:</b> If the firewall detects a sensitive directory scan attack, it blocks the current session.</li> <li>● <b>Block IP:</b> If CFW detects a sensitive directory scan attack, it blocks the attack IP address for a period of time.</li> </ul> <p><b>Duration:</b> If <b>Action</b> is set to <b>Block IP</b>, you can set the blocking duration. The value range is 60s to 3,600s.</p> <p><b>Threshold:</b> CFW performs the specified action if the scan frequency of a sensitive directory reaches this threshold.</p>                                                                                                                                                                                                                                                                 |
|                      | Reverse Shell Defense            | <p>Defense against reverse shells.</p> <p><b>Action:</b></p> <ul style="list-style-type: none"> <li>● <b>Observe:</b> If a reverse shell attack is detected, it is only recorded in attack logs. For details about how to view attack logs, see <a href="#">Attack Event Logs</a>.</li> <li>● <b>Block session:</b> If the firewall detects a reverse shell attack, it blocks the current session.</li> <li>● <b>Block IP:</b> If CFW detects a reverse shell attack, it blocks the attack IP address for a period of time.</li> </ul> <p><b>Duration:</b> If <b>Action</b> is set to <b>Block IP</b>, you can set the blocking duration. The value range is 60s to 3,600s.</p> <p><b>Mode:</b></p> <ul style="list-style-type: none"> <li>● <b>Conservative:</b> coarse-grained protection. If a single session is attacked for four times, observation or interception is triggered. It ensures that no false positives are reported.</li> <li>● <b>Sensitive:</b> fine-grained protection. If a single session is attacked for two times, observation or interception is triggered. It ensures that attacks can be detected and handled.</li> </ul> |

----End

## 4.2 Configuring an Access Control Policy

The default status of an access control policy is **Allow**. Configure a proper access control policy for fine-grained management and control, preventing the spread of internal threats and enhancing security. For details about how to configure an access control policy, see [Adding an Internet Boundary Protection Rule](#). For details about how to block all access and allow only certain traffic, see [Configuration Example - Allowing the Inbound Traffic from a Specified IP Address](#). For details about how to block the access traffic of a region, see [Configuration Example - Blocking Access from a Region](#).

### Configuration Example - Allowing the Inbound Traffic from a Specified IP Address

Configure two protection rules. One of them blocks all traffic, as shown in [Figure 4-1](#). Its priority is the lowest. The other allows the traffic of a specified IP address, as shown in [Figure 4-2](#). Its priority is the highest.

**Figure 4-1** Blocking all traffic

**Matching Condition**

|             |                                          |                                |
|-------------|------------------------------------------|--------------------------------|
| Direction   | <input checked="" type="radio"/> Inbound | <input type="radio"/> Outbound |
| Source      | <input type="text" value="Any"/>         |                                |
| Destination | <input type="text" value="Any"/>         |                                |
| Service     | <input type="text" value="Any"/>         |                                |

---

**Protection Action**

|        |                             |                                        |
|--------|-----------------------------|----------------------------------------|
| Action | <input type="radio"/> Allow | <input checked="" type="radio"/> Block |
|--------|-----------------------------|----------------------------------------|

**Figure 4-2** Allowing a specified IP address

**Matching Condition**

Direction  Inbound  Outbound

Source  10.1.1.1 ×

Destination

Service

---

**Protection Action**

Action  Allow  Block

### Configuration Example - Blocking Access from a Region

The following figure shows a rule that blocks all access traffic from **Singapore**.

**Figure 4-3** Intercepting the access traffic from Singapore

**Matching Condition**

Direction  Inbound  Outbound

Source  Singapore ×

**⚠ Before selecting a continent, check to ensure you want this policy to take effect on all the countries/regions in it.**

Destination

Service

---

**Protection Action**

Action  Allow  Block

# 5 (Optional) Step 4: View Protection Details


---


## 5.1 Viewing Network Traffic Analysis

You can view details about the inbound and outbound traffic and attack trend on cloud servers in real time to check for abnormal traffic.

### Viewing Inbound Traffic

**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 **Traffic Analysis > Inbound Traffic**.

**Step 6** View the statistics on the traffic passing through the firewall. You can select the query duration from the drop-down list.

- **Traffic Dashboard:** Information about the highest traffic from the Internet to internal servers.
- **Inbound Traffic:** Inbound request and response traffic.
- **Visualizations:** Top 5 items ranked by certain parameters regarding inbound traffic within a specified time range. For more information, see [Table 5-1](#). You can click a data record to view the traffic details. A maximum of 50 data records can be viewed.



**Table 5-1** Inbound traffic parameters


| Parameter                      | Description                                                           |
|--------------------------------|-----------------------------------------------------------------------|
| Top Access Source IP Addresses | Source IP addresses of inbound traffic.                               |
| Top Access Source Regions      | Geographical locations of the source IP addresses of inbound traffic. |
| Top Destination IP Addresses   | Destination IP addresses of inbound traffic.                          |
| Top Open Ports                 | Destination ports of inbound traffic.                                 |
| Application Distribution       | Application information about inbound traffic.                        |


- IP analysis: Top 50 traffic records in a specified period.
  - **EIPs**: Traffic information about destination IP addresses.
  - **Source IP Addresses**: Traffic information about source IP addresses.

----End

## Viewing Outbound Traffic

**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 **Traffic Analysis > Outbound Traffic**.

**Step 6** View the statistics on the traffic passing through the firewall. You can select the query duration from the drop-down list.

- **Traffic Dashboard**: Information about the highest traffic when internal servers access the Internet.
- **Outbound Traffic**: Outbound request and response traffic.
- **Visualizations**: Top 5 items ranked by certain parameters regarding outbound traffic within a specified time range. For more information, see [Table 5-2](#). You can click a data record to view the traffic details. A maximum of 50 data records can be viewed.

**Table 5-2** Outbound traffic parameters

| Parameter                      | Description                                                            |
|--------------------------------|------------------------------------------------------------------------|
| Top Destination IP Addresses   | Destination IP addresses of outbound traffic.                          |
| Top Destination Regions        | Geographical locations of the source IP addresses of outbound traffic. |
| Top Access Source IP Addresses | Source IP addresses of outbound traffic.                               |
| Top Open Ports                 | Destination ports of outbound traffic.                                 |
| Application Distribution       | Application information about outbound traffic.                        |

- IP analysis: Top 50 traffic records in a specified period.
  - **External IP Address:** Traffic information about the destination IP address.
  - **Assets Initiating Internet Connections:** Traffic information whose source IP addresses are public IP addresses.
  - **Assets Initiating Private Network Connections:** Traffic information whose source IP addresses are private IP addresses.

----End


## 5.2 Viewing Protection Event Logs


For details about how to view attack traffic detected by the cloud firewall in attack logs, see [Attack Event Logs](#).

You can also view all traffic allowed or blocked in access control logs to adjust access control policies. For details, see [Access Control Logs](#).

### Attack Event Logs

**Step 1** [Log in to the management console](#).

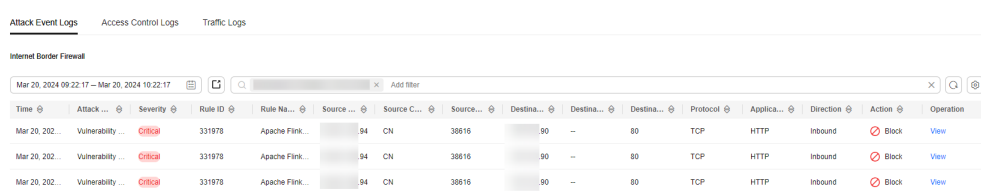
**Step 2** Click  in the upper left corner of the management console and select a region or project.

**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**. The **Attack Event Logs** tab page is displayed. You can view details about attack events in the past week.

**Figure 5-1** Attack event logs




**Table 5-3** Attack event log parameters


| Parameter                  | Description                                                                          |
|----------------------------|--------------------------------------------------------------------------------------|
| Time                       | Time when an attack occurred.                                                        |
| Attack Type                | Type of the attack event, including IMAP, DNS, FTP, HTTP, POP3, TCP, and UDP.        |
| Severity                   | It can be <b>Critical</b> , <b>High</b> , <b>Medium</b> , or <b>Low</b> .            |
| Rule ID                    | Rule ID                                                                              |
| Rule Name                  | Matched rule in the library.                                                         |
| Source IP Address          | Source IP address of an attack event.                                                |
| Source Country/Region      | Geographical location of the attack source IP address.                               |
| Source Port                | Source port of an attack.                                                            |
| Destination IP Address     | Attacked IP address.                                                                 |
| Destination Country/Region | Geographical location of the attack target IP address.                               |
| Destination Port           | Destination port of an attack.                                                       |
| Protocol                   | Protocol type of an attack.                                                          |
| Application                | Application type of an attack.                                                       |
| Direction                  | It can be outbound or inbound.                                                       |
| Action                     | The value can be <b>Allow</b> , <b>Block</b> , <b>Block IP</b> , or <b>Discard</b> . |
| Operation                  | You can click View to view the basic information and attack payload of an event.     |

----End

## Access Control Logs

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

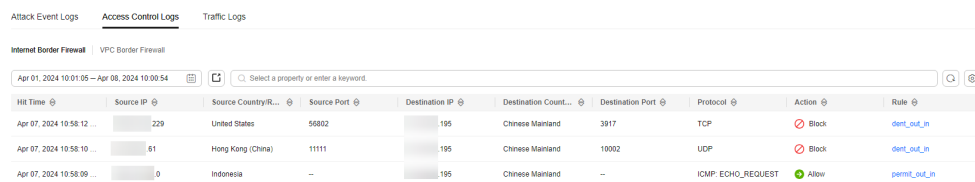
**Step 2** Click  in the upper left corner of the management console and select a region or project.

**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 **Access Control Logs** tab and check the access control traffic details in the past week.

**Figure 5-2** Access control logs



| Hit Time                  | Source IP | Source Country/Region | Source Port | Destination IP | Destination Country/Region | Destination Port | Protocol           | Action | Rule          |
|---------------------------|-----------|-----------------------|-------------|----------------|----------------------------|------------------|--------------------|--------|---------------|
| Apr 07, 2024 10:58:12 ... | 229       | United States         | 58802       | 195            | Chinese Mainland           | 3917             | TCP                | Block  | deny_out_in   |
| Apr 07, 2024 10:58:10 ... | 51        | Hong Kong (China)     | 11111       | 195            | Chinese Mainland           | 10002            | UDP                | Block  | deny_out_in   |
| Apr 07, 2024 10:58:09 ... | 0         | Indonesia             | -           | 195            | Chinese Mainland           | -                | ICMP: ECHO_REQUEST | Allow  | permit_out_in |

**Table 5-4** Access control log parameters

| Parameter                  | Description                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------|
| Hit Time                   | Time of access.                                                                                                    |
| Source IP                  | Source IP address of the access.                                                                                   |
| Source Country/Region      | Geographical location of the source IP address.                                                                    |
| Source Port                | Source port for access control. It can be a single port or consecutive port groups (example: <b>80-443</b> ).      |
| Destination IP             | Destination IP address.                                                                                            |
| Destination URL            | Destination domain name                                                                                            |
| Destination Country/Region | Geographical location of the destination IP address.                                                               |
| Destination Port           | Destination port for access control. It can be a single port or consecutive port groups (example: <b>80-443</b> ). |
| Protocol                   | Protocol type for access control.                                                                                  |

| Parameter | Description                                                                           |
|-----------|---------------------------------------------------------------------------------------|
| Action    | Action taken on an event. It can be <b>Observe</b> , <b>Block</b> , or <b>Allow</b> . |
| Rule      | Type of an access control rule. It can be a blacklist or whitelist.                   |

----End

# 6 Getting Started with Common Practices

After configuring intrusion prevention and access control policies, you can use a series of common practices provided by CFW for your workloads quickly.

**Table 6-1** Common practices

| Practice                                                                             | Description                                                                                                                                                                           |
|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Configuring Access Policies for IP Address Groups and Service Groups</a> | Configure IP address groups and service groups (ports and protocols) in batches. This policy applies to enterprises or multiple IP addresses or port protocols need to be configured. |
| <a href="#">Configuring an Inter-VPC Border Firewall</a>                             | Configure a VPC border firewall, which applies to scenarios where inter-VPC traffic protection is required.                                                                           |