

# Cloud Firewall

# User Guide

**Issue** 03  
**Date** 2024-01-10



**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 Purchasing CFW</b>	<b>1</b>
<b>2 Changing CFW Specifications</b>	<b>6</b>
<b>3 Checking the CFW Dashboard</b>	<b>9</b>
<b>4 Managing EIP Protection</b>	<b>14</b>
4.1 Enabling EIP Protection	14
4.2 Viewing EIP Information	16
<b>5 Managing VPC Border Firewalls</b>	<b>18</b>
5.1 VPC Border Firewall Overview	18
5.2 VPC Mode	18
5.2.1 Step 1: Create a Firewall (VPC Mode)	18
5.2.2 Step 2: Manage Protected VPCs	20
5.2.3 Step 3: Configure Routes on the VPC Side	22
5.2.4 Step 4: Enable or Disable a VPC Border Firewall	23
<b>6 Managing ACL Rules</b>	<b>25</b>
6.1 Adding a Protection Rule	25
6.2 Managing Protection Rules in Batches	35
6.3 Configuring a Rule Priority	43
6.4 Managing the Blacklist and the Whitelist	44
6.4.1 Adding an Item to the Blacklist or Whitelist	44
6.4.2 Editing the Blacklist or Whitelist	46
6.4.3 Removing a Blacklisted or Whitelisted Item	48
6.5 Managing IP Address Groups	49
6.5.1 Adding Custom IP Address Groups	49
6.5.2 Viewing a Predefined Address Group	51
6.5.3 Adding an IP Address	52
6.5.4 Delete an IP Address Group	54
6.6 Managing Service Groups	55
6.6.1 Adding a Custom Service Group	55
6.6.2 Viewing a Predefined Service Group	56
6.6.3 Adding a Service	57
6.6.4 Deleting a User-defined Service Group	59

6.7 Managing Domain Name Groups.....	60
6.7.1 Adding a Domain Name Group.....	60
6.7.2 Deleting a Domain Name Group.....	62
6.8 Policy Assistant.....	63
6.9 Managing Protection Rules.....	64
6.9.1 Checking the ACL Rule List.....	64
6.9.2 Editing a Protection Rule.....	66
6.9.3 Copying a Protection Rule.....	66
6.9.4 Deleting a Rule.....	67
<b>7 Configuring Intrusion Prevention.....</b>	<b>69</b>
<b>8 Managing Intrusion Prevention.....</b>	<b>72</b>
8.1 Checking the IPS Rule Library.....	72
8.2 Modifying the Action of a Basic Protection Rule.....	74
8.3 Customizing IPS Signatures.....	76
<b>9 Managing the Antivirus Function.....</b>	<b>81</b>
<b>10 Security Dashboard.....</b>	<b>83</b>
<b>11 Traffic Analysis.....</b>	<b>85</b>
11.1 Viewing Inbound Traffic.....	85
11.2 Viewing Outbound Traffic.....	86
11.3 Viewing Inter-VPC Traffic.....	88
<b>12 Auditing Logs.....</b>	<b>90</b>
12.1 Querying Logs.....	90
12.2 Log Management.....	95
12.2.1 Log Settings.....	95
12.2.2 Changing the Log Storage Duration.....	96
12.2.3 Adding Alarm Notifications.....	97
12.2.4 Log Structuring.....	101
12.2.5 Visualization.....	103
12.2.6 Quick Analysis.....	105
12.2.7 Log Field Description.....	107
<b>13 System Management.....</b>	<b>112</b>
13.1 Alarm Notification.....	112
13.2 Network Packet Capture.....	117
13.2.1 Creating a Packet Capture Task.....	117
13.2.2 Viewing a Packet Capture Task.....	121
13.2.3 Downloading Packet Capture Results.....	123
13.3 Configuring DNS Resolution.....	124
<b>14 Audit.....</b>	<b>126</b>
14.1 Operations Recorded by CTS.....	126

---

14.2 Viewing Audit Logs.....	128
<b>15 Monitoring.....</b>	<b>129</b>
15.1 CFW Monitored Metrics.....	129
15.2 Configuring Alarm Monitoring Rules.....	130
15.3 Viewing Monitoring Metrics.....	131
<b>A Change History.....</b>	<b>132</b>

# 1 Purchasing CFW

You can purchase multiple firewalls in a region and assign them different resources and policies.

CFW can be billed in yearly/monthly (prepaid) or pay-per-use (postpaid) mode. You can purchase the CFW standard or professional edition in yearly/monthly mode. The pay-per-use billing mode supports the CFW professional edition, as needed.

## Prerequisites


The current account has the BSS Administrator and CFW FullAccess permissions.


## Constraints

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 [Can CFW Be Used Across Clouds or Regions?](#)

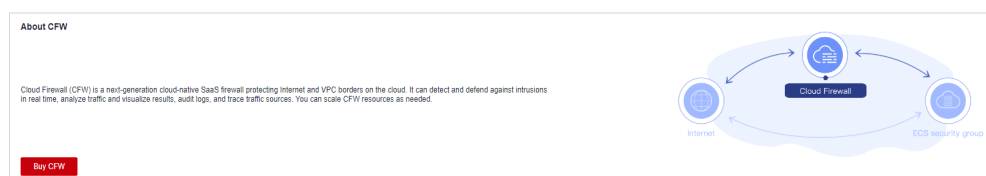
## Purchasing a Firewall in Yearly/Monthly Mode

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 1-1](#).

**Figure 1-1** CFW Dashboard



**Step 4** Click **Buy CFW** and configure parameters on the **Buy CFW** page. For more information, see [Table 1-1](#).

**Table 1-1** Yearly/Monthly CFW parameters

Parameter	Description
Billing Mode	<b>Yearly/Monthly</b>
Region	Region where the CFW is to be purchased. <b>NOTICE</b> 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>
Edition	Edition. <ul style="list-style-type: none"> <li>Standard</li> </ul>
Engine	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.
Add EIP Protection Capacity	(Optional) Number of additional EIPs to be protected. Value range: 0 to 2000 <b>NOTE</b> 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.
Add Peak Traffic Protection Capacity	(Optional) Additional peak inbound or outbound traffic. The value range is 0 to 2000 Mbit/s per month. (The value must be an integer multiple of 5.) <b>NOTE</b> <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>
Add VPCs	(Optional) Select the number of VPCs you want to add. The value range is 0 to 100. <b>NOTE</b> <ul style="list-style-type: none"> <li>Only the professional edition supports inter-VPC protection.</li> <li>By default, 2 VPCs are protected by the professional edition (included in the package fee). If you have 3 VPCs, you only need to enter 1.</li> <li>For each VPC you add, the protected peak traffic increases by 200 Mbit/s.</li> </ul>



Parameter	Description
Enterprise Project	<p>Select an enterprise project from the drop-down list.</p> <p>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> 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>
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>
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

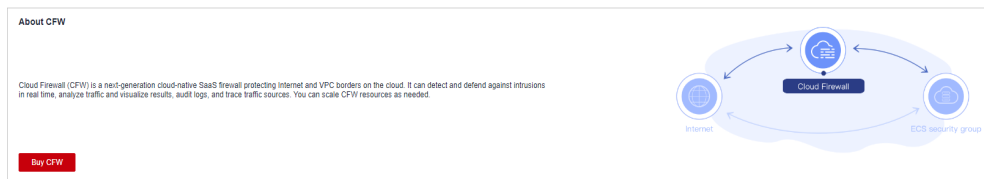
## Purchasing a Firewall in Pay-per-Use Mode

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 1-2](#).

**Figure 1-2** CFW Dashboard



**Step 4** Click **Buy CFW**. For details about the parameters on the **Buy CFW** page, see [Table 1-2](#).

**Table 1-2** Parameters for purchasing a pay-per-use CFW

Parameter	Description
Billing Mode	If you select <b>Pay-per-use</b> , you will be charged for the protection on your workloads from purchase to unsubscription.
Region	Region where the CFW is to be purchased. <b>NOTICE</b> 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>
Edition	Currently, only the professional edition is supported.
Engine	Firewall engine. 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.
Enterprise Project	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 learn more, see <a href="#">Enabling the Enterprise Center</a> . You can use enterprise projects to more efficiently manage cloud resources and project members. <b>NOTE</b> 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.
Firewall Name	Firewall name. It must meet the following requirements: <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	<b>Tags:</b> It is recommended that you use the TMS predefined tag function to add the same tag to different cloud resources.

**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 right corner of the management console.

# 2 Changing CFW Specifications


After purchasing CFW, you can upgrade to a higher edition or modify expansion packages, increasing or decreasing protected EIPs, VPCs, and peak Internet border traffic.


## Constraints

Only yearly/monthly firewalls support the change of the service edition and the number of expansion packages. **Pay-per-use** firewalls support only the professional edition and are charged based on the actual protection status.

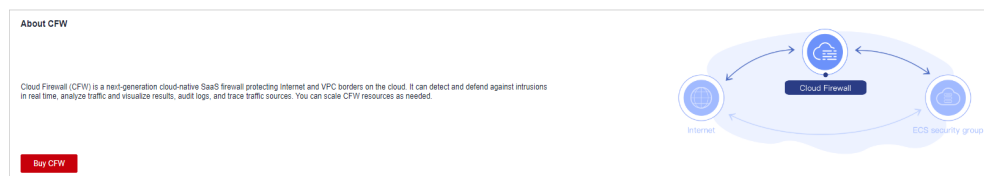
## Upgrading an Edition

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 2-1](#).

**Figure 2-1** CFW Dashboard





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

**Step 5** In the upper right corner of the page, click **Upgrade to Professional Edition**. The CFW purchase page is displayed.

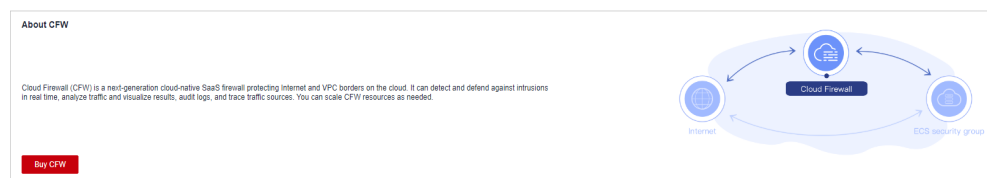
**Step 6** Confirm the edition specifications and click **Buy Now**.

- 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

## Modifying Extension Packages

- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 2-2](#).




**Figure 2-2** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the **Firewall Details** area, click **Modify** next to **Used/Available EIP Protection Quota**, **Protected VPCs/VPC Protection Quota**, or **Peak Traffic Protection** to go to the **Change CFW Edition** page.
- Step 6** Change the number of extension packages.



By default, the number of extension packages cannot be reduced to 0. To set it to 0, perform the operations in [Unsubscribing from an Extension Package](#).

**Figure 2-3** Adding EIP protection capacity

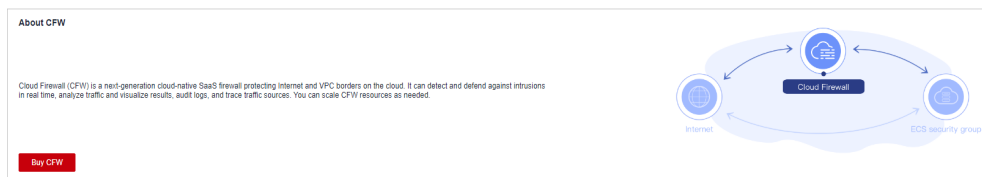
	Edition Capacity	Added Capacity	Total
Version	 Standard	<a href="#">Modify Capacity</a>	 Standard
Add EIP Protection Capacity	Total Protected EIPs: 30	<div style="border: 1px solid red; padding: 2px;">                     Add EIP Protection Capacity   <input type="text" value="10"/> </div>	Total Protected EIPs: 30

- 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

## Unsubscribing from an Extension Package

- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 2-4](#).

**Figure 2-4** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** Hover your cursor over the edition name in the upper right corner of the page. Click **Unsubscribe**.
- Step 6** Select the extension package 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


# 3 Checking the CFW Dashboard

The dashboard page displays the CFW overview, edition, and protection statistics, including the engine type, total number of EIPs and protected EIPs, peak traffic available for protection, and log storage space.

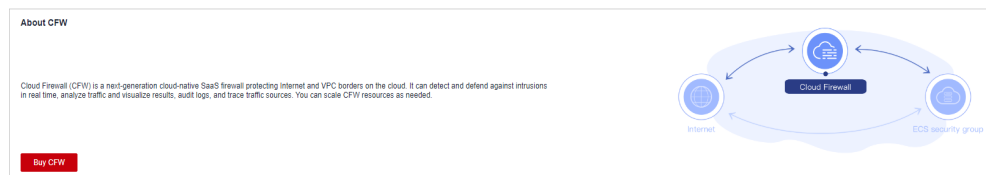
## Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 3-1](#).

**Figure 3-1** CFW Dashboard



**Step 4** (Optional) If the current account has only one firewall instance, the firewall details page will be automatically displayed. In this case, skip this step.

Check the information about each firewall instance under the account. Click a name in the **Name/ID** column or click **View** in the **Operation** column.

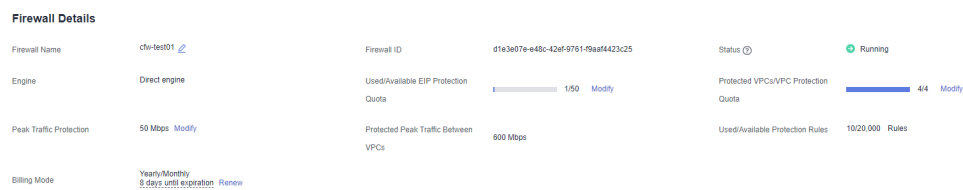
**Table 3-1** Firewall instance parameters

Parameter	Description
Name/ID	Name and ID of the firewall.
Status	Firewall status.


Parameter	Description
Edition	Firewall edition. Standard and professional editions are supported.
Available EIP Protection	Maximum number of EIPs that can be protected by the firewall.
Peak Traffic Protection	Maximum peak traffic that can be protected by the firewall.
Billing Mode	Billing mode of the current firewall.
Enterprise Project	Enterprise project that the firewall belongs to.
Operation	Check instance details.

**Step 5** View details about the firewall. For more information, see [Table 3-2](#).

**Figure 3-2** Firewall details



**Table 3-2** Detailed firewall information

Parameter	Description
Firewall Name	Firewall instance name. You can click  to change the name.
Firewall ID	Firewall instance ID.
Status	Firewall status. It takes about 5 minutes to update the firewall status after purchase or unsubscription.
Engine	Firewall engine type.
Used/Available EIP Protection Quota	<i>Number of protected EIPs/ Total number of EIPs</i> under a CFW instance.
Protected VPCs/VPC Protection Quota	<i>Number of protected VPCs/ Total number of VPCs</i> under a firewall instance.
Peak Traffic Protection	Peak north-south traffic that can be protected.

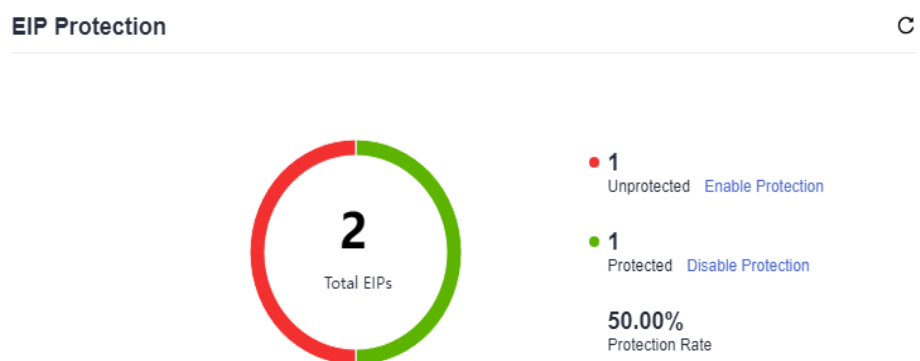


Parameter	Description
Protected Peak Traffic Between VPCs	Peak east-west traffic that can be protected.
Used/Available Protection Rules	<i>Number of created protection rules/ Total number of protection rules that can be created under a firewall instance.</i>
Billing Mode	Bling mode

**Step 6** View firewall protection statistics. For more information, see [Table 3-3](#).

- EIP Protection
- Inter-VPC Protection

**Figure 3-3** Protection statistics



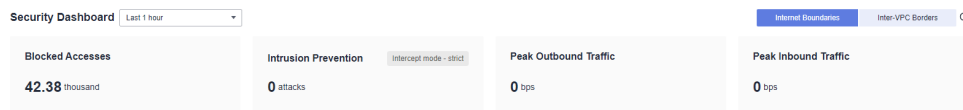
**Table 3-3** Firewall protection statistics

Parameter	Description
Total EIPs	The total number of EIPs, both the protected and the unprotected.
Total VPCs	The total number of VPCs, both the protected and the unprotected.
Unprotected	The number of unprotected EIPs/VPCs.
Protected	Number of protected EIPs/VPCs.
Protection Rate	The percentage of the number of protected EIPs/VPCs to the total number of EIPs/VPCs.

**Step 7** In the **Security Dashboard** area, view the CFW protection details at the Internet and VPC borders. For details about the parameters, see [Table 3-4](#).

The query time can be **Last 1 hour**, **Last 24 hours**, or **Last 7 days**.

**Figure 3-4** Security Dashboard



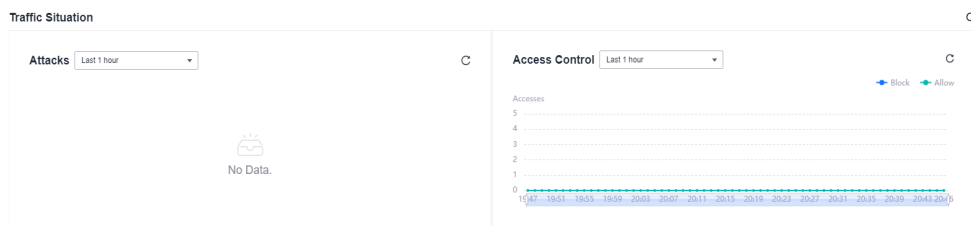
**Table 3-4** Security Dashboard

Parameter	Description
Blocked Accesses	Number of times accesses are blocked based on protection rules.
Intrusion Prevention	Intrusion prevention mode and the number of intercepted attacks.
Peak Outbound Traffic	Maximum traffic initiated from internal services to the Internet.
Peak Inbound Traffic	Maximum traffic initiated from the Internet to internal servers.
Peak Inter-VPC Traffic	Maximum traffic between VPCs.

**Step 8** In the **Traffic Situation** area, check the Internet and VPC border traffic trends. **Table 3-5** describes the traffic trend parameters.

The query time can be **Last 1 hour**, **Last 24 hours**, or **Last 7 days**.

**Figure 3-5** Traffic Situation



**Table 3-5** Traffic Situation parameters

Parameter	Description
Attacks	Blocked and allowed accesses.
Access Control	Traffic blocked and allowed based on protection rules.

**Step 9** In the **Traffic Trend** area, click **Internet Boundaries** or **Inter-VPC Borders** to check the corresponding statistics.

**Internet Boundaries:** Select an EIP and a query duration from the drop-down list boxes to view inbound and outbound traffic.

VPC boundary: Select a query duration to view the traffic between VPCs.

 **NOTE**

The traffic data of all EIPs and VPCs under the current account is displayed.

**Step 10** Configure tags to identify firewalls so that you can classify and trace firewall instances.

----**End**

# 4 Managing EIP Protection

## 4.1 Enabling EIP Protection

If EIP protection is not enabled, your service traffic will not be filtered by CFW.

To use CFW to protect traffic, after you enable protection, you also need to configure access control policies or enable IPS. For details about how to configure access control policies, see [Adding a Protection Rule](#). For details about IPS, see [Configuring Intrusion Prevention Policies](#).


This section describes how to synchronize EIP information and enable EIP protection.


### Constraints

Currently, IPv6 addresses cannot be protected.

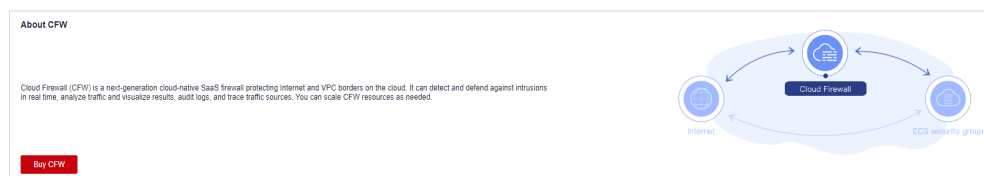
### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 4-1](#).

**Figure 4-1** CFW Dashboard

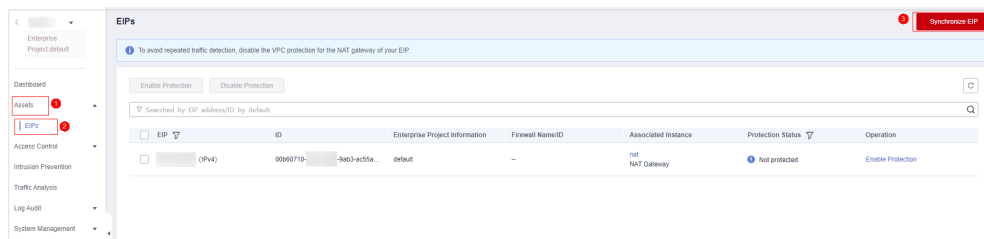


**Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

**Step 5** In the navigation pane, choose **Assets > EIPs**. The EIP page is displayed. The EIP information is automatically updated to the list. See [Figure 4-2](#).

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

**Figure 4-2** EIPs



### NOTICE

Currently, IPv6 addresses cannot be protected.

**Step 6** Enable EIP protection.

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

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

### NOTE

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

----End

## Follow-up Operations

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

- To configure a protection rule, see [Adding a Protection Rule](#).
- To configure basic protection, see [Configuring Intrusion Prevention Policies](#).

## Related Operations



Disabling EIP protection

- To disable an EIP, click **Disable Protection** in the **Operation** column of the EIP.

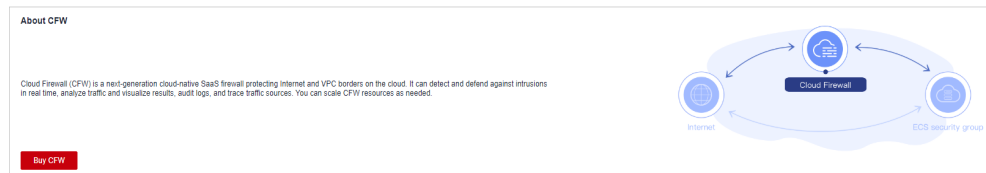
- To disable multiple EIPs, select them and click **Disable Protection** above the table.

## 4.2 Viewing EIP Information


### 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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 4-3](#).

**Figure 4-3** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane, choose **Assets > EIPs**.
- Step 6** View EIP information.

You can set filter conditions to search for an EIP. Enter a condition and press **Enter** to add it. Click  to start search.

**Table 4-1** Internet border firewall EIP parameters

Parameter	Description
Total EIPs	Number of EIPs under the current account.
Used/Available EIP Protection Capacity	<i>Number of protected EIPs</i> / <i>Total number of EIPs</i> under the current CFW instance.
Unprotected EIPs	Total number of unprotected EIPs under the current account.
Auto Protect New EIP	If this function is enabled, protection will be automatically enabled for your new EIPs, and EIP traffic will pass through and be protected by the firewall. <b>NOTE</b> It can be enabled for only one firewall instance.

**Table 4-2** EIP parameters

Parameter Name	Description
EIP/ID	IP address and ID of an EIP.
Protection Status	EIP protection status.
Firewall Name/ID	Name and ID of a firewall.
Enterprise Project	Enterprise project that an EIP belongs to. This option is only available when you are logged in using an enterprise account, or when you have enabled enterprise projects.
Associated Instance	Name and ID of the instance bound to an EIP.
Tags	EIP tag. You can add tags to classify and manage EIPs.

----End

# 5 Managing VPC Border Firewalls

## 5.1 VPC Border Firewall Overview

The VPC border firewall supports access control for communication traffic between two VPCs, visualizing and protecting internal service access.

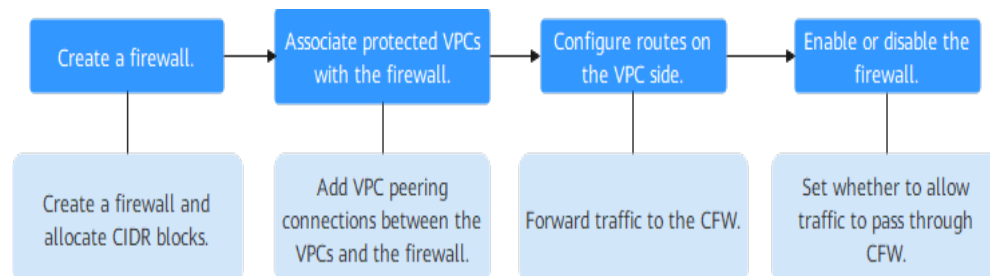
### Constraints

- Only the professional edition supports VPC border firewalls.
- To use public network CIDR blocks other than 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, and 100.64.0.0/10 as private network CIDR blocks, [submit a service ticket](#), or CFW may fail to forward traffic between your VPCs.

### Configuration Process

The following figure shows the configuration process in VPC mode.

Figure 5-1 Configuration process in VPC mode



## 5.2 VPC Mode

### 5.2.1 Step 1: Create a Firewall (VPC Mode)

A VPC border firewall can collect statistics on the traffic between VPCs, helping you detect abnormal traffic. This section describes how to create a VPC border firewall.





## Constraints

Only the professional edition supports VPC border firewalls.

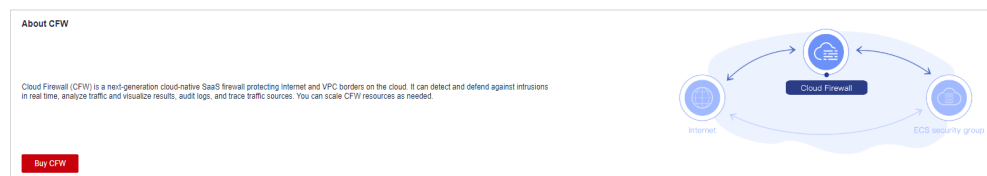
## Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 5-2](#).

**Figure 5-2** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Assets > Inter-VPC Border Firewalls**.

**Step 6** Click **Create Firewall**.

**Step 7** Configure a CIDR block. An inspection VPC will be automatically created by default.

**Figure 5-3** Network planning

**Matching Condition**

* Source	IP address ▼	10.1.1.2 ✕
* Destination	Domain name ▼	www.example.com
		Test
		✔ The domain name is valid.
* Service	Service ▼	TCP/0-65535/0-65535 ✕

**NOTE**

Pay attention to the following restrictions during network planning:

- After a firewall is created, its CIDR block cannot be modified.
- This CIDR block cannot overlap with the private CIDR block to be protected, or routing conflicts and protection failures may occur.
- The CIDR block 10.6.0.0/16-10.7.0.0/16 is reserved for CFW and cannot be specified.

**Step 8** Click **OK**.

----End

## Related Operations

**Unsubscription:** To unsubscribe from a VPC border firewall, you must unsubscribe from the CFW instance associated with it.

### 5.2.2 Step 2: Manage Protected VPCs

After creating a VPC border firewall, you need to associate VPCs with the firewall. For details, see [Associating a Protected VPC with the Firewall](#).


If a VPC does not need to be protected, you can disassociate the VPC from the firewall. For details, see [Disassociating a Protected VPC from a Firewall](#).


## Constraints

Before disassociating a protected VPC from a cloud firewall, delete the route pointing to the cloud firewall in [5.2.3 Step 3: Configure Routes on the VPC Side](#).

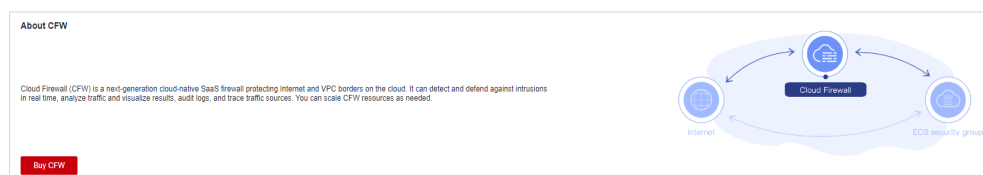
## Associating a Protected VPC with the Firewall

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 5-4](#).

**Figure 5-4** CFW Dashboard




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

**Step 5** In the navigation pane, choose **Assets > Inter-VPC Border Firewalls**.

**Step 6** In the **Operation** column of a VPC, click **Associate Firewall**.

**Step 7** On the **Associate Firewall** page, configure [parameters for the protected VPC](#).

**Table 5-1** Parameters for adding a protected VPC


Parameter Name		Description
Protection Type		The value cannot be changed. The default value <b>VPC</b> is used.
VPC		Name and CIDR block of the protected VPC.
Firewall Route	Protected VPC CIDR Block	By default, the CIDR block of the selected VPC is used. You can modify the CIDR block or click  <b>Add</b> to add a CIDR block.
	Next Hop Type	The value cannot be changed. The default value is <b>VPC peering</b> .
	Next Hop	The value cannot be changed. The VPC uses this VPC peering connection to forward traffic to the firewall.
	Description	(Optional) Enter the description of the VPC.
Route	Configure VPC route	If it is selected, the routes pointing to 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 and whose next hop type is a firewall peering connection will be added to all the route tables of the VPC.  <b>CAUTION</b> Before selecting it, confirm that it will not affect your network.


**Step 8** Click **OK** to associate the protected VPC with the firewall.

----End

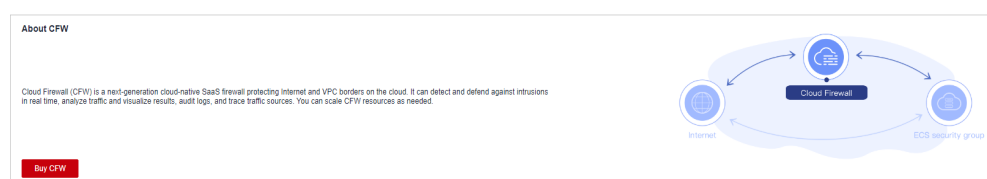
## Disassociating a Protected VPC from a Firewall

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 5-5](#).

**Figure 5-5** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane, choose **Assets > Inter-VPC Border Firewalls**.
- Step 6** In the **Operation** column of a VPC, click **Disassociate**.
- Step 7** In the confirmation dialog box, click **OK**.

 **NOTE**

If a VPC has a route whose next hop is the peering connection created by the firewall, the VPC cannot be deleted. To delete this VPC, delete the route first.



----End

## Follow-up Operations

After a VPC is added, perform the operations in [5.2.3 Step 3: Configure Routes on the VPC Side](#).

## 5.2.3 Step 3: Configure Routes on the VPC Side

### 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 tree on the left, click  in the upper left corner. Click **Virtual Private Cloud** under **Networking** and choose **Virtual Private Cloud > Route Tables**.
- Step 4** In the **Name** column, click the route table name of a VPC. The **Summary** page is displayed.
- Step 5** Click **Add Route**. For more information, see [Table 5-2](#).

**Table 5-2** Route parameters

Parameter	Description
Destination Type	Select the destination address type. The value can be <b>IP address</b> or <b>IP address group</b> .
Destination	Destination CIDR block.
Next Hop Type	Select <b>VPC peering connection</b> from the drop-down list.
Next Hop	Select the VPC peering connection associated with the traffic diversion VPC.

Parameter	Description
Description	(Optional) Supplementary information about the route. <b>NOTE</b> Enter up to 255 characters. Angle brackets (< or >) are not allowed.


----End


## 5.2.4 Step 4: Enable or Disable a VPC Border Firewall

After a firewall is configured, it is in **Disabled** state by default. You can manually enable or disable inter-VPC protection.

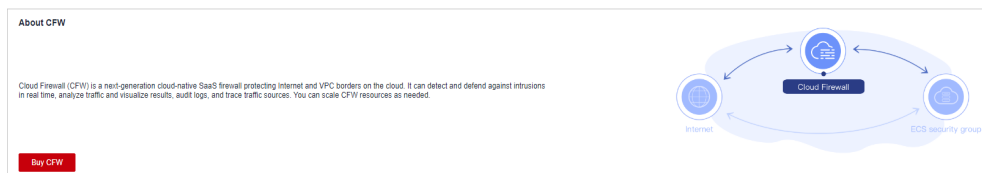
### Enabling a Firewall

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 5-6](#).

**Figure 5-6** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Assets > Inter-VPC Border Firewalls**.


**Step 6** In the upper part of the page, click **Enable Protection** next to **Firewall Status**.


**Step 7** Click **OK**.

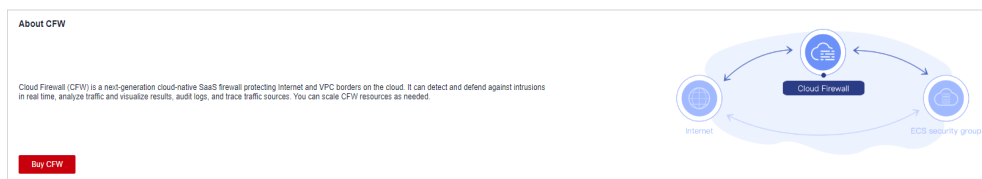
----End

### Disabling a Firewall

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 5-7](#).

**Figure 5-7** CFW Dashboard

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

**Step 5** In the navigation pane, choose **Assets > Inter-VPC Border Firewalls**.

**Step 6** In the upper part of the page, click **Disable Protection** next to **Firewall Status**.

**Step 7** Click **OK**.

----End

## Follow-up Operations

To add a protected VPC after a firewall is enabled, Perform the operations in [Associating a Protected VPC with the Firewall](#) and [5.2.3 Step 3: Configure Routes on the VPC Side](#).

# 6 Managing ACL Rules

---

## 6.1 Adding a Protection Rule

Access control policies can help you manage and control the traffic between servers and external networks in a refined manner, prevent the spread of internal threats, and enhance the depth of security strategies.

After EIP protection is enabled, the default status of the access control policy is **Allow**. If you want to allow only several EIPs, you are advised to add a protection rule with the lowest priority to block all traffic.

---

**⚠ CAUTION**

If your IP address is a back-to-source WAF IP address, you are advised to configure a protection rule or the whitelist to allow its access. Exercise caution when configuring a protection rule to block access, which may affect your services.

- For details back-to-source IP addresses, see [What Are Back-to-Source IP Addresses?](#)
  - For details about how to configure the whitelist, see [6.4.1 Adding an Item to the Blacklist or Whitelist](#).
- 

### Prerequisites

You have synchronized assets and enabled EIP protection. See [4.1 Enabling EIP Protection](#).

### Specification Limitations


To enable VPC border protection, NAT protection, and private IP address protection, use the professional edition of CFW and enable the [VPC firewall](#) protection.


## Constraints

- Up to 20,000 protection rules can be added.
- A single protection rule can be associated with a maximum of five service groups.
- Each protection rule can be associated with up to two IP address groups.
- Domain names in Chinese are not supported.
- Predefined address groups can be configured only for the source addresses in inbound rules (whose **Direction** is set to **Inbound**).
- If NAT 64 protection is enabled and IPv6 access is used, allow traffic from the 192.19.0.0/16 CIDR block to pass through. NAT64 will translate source IP addresses into the CIDR block 198.19.0.0/16 for ACL access control.

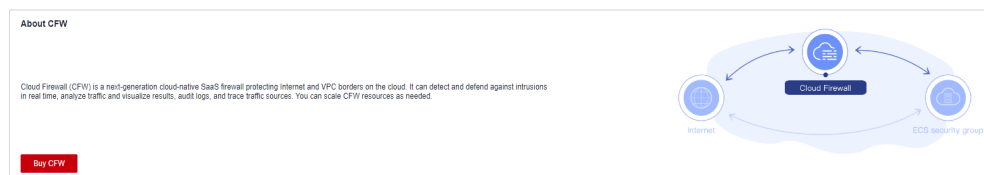
## Adding an Internet Boundary Protection Rule

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-1](#).

**Figure 6-1** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Access Control > Access Policies**.

**Step 6** Add a protection rule.

Click **Add Rule**. In the displayed page, enter new protection information. For details, see [Table 6-1](#).

**Table 6-1** Internet boundary rule parameters




Parameter	Description	Example Value
Name	Rule name.	test



Parameter	Description	Example Value
Direction	Select a traffic direction if the protection rule is set to <b>EIP</b> . <ul style="list-style-type: none"> <li>● <b>Inbound</b>: Traffic from external networks to the internal server.</li> <li>● <b>Outbound</b>: Traffic from internal servers to external networks.</li> </ul>	Inbound
Source	Source address of access traffic. <ul style="list-style-type: none"> <li>● <b>IP address</b> can be configured in the following formats:                             <ul style="list-style-type: none"> <li>– A single IP address, for example, <b>192.168.10.5</b></li> <li>– Consecutive IP addresses, for example, <b>192.168.0.2-192.168.0.10</b></li> <li>– Address segment, for example, <b>192.168.2.0/24</b></li> </ul> </li> <li>● <b>IP address group</b>: A collection of IP addresses. For details about how to add custom IP address groups, see <a href="#">Adding an IP Address Group</a>. For details about a pre-defined address group, see <a href="#">6.5.2 Viewing a Predefined Address Group</a>.</li> </ul> <p><b>NOTE</b> If <b>Direction</b> is set to <b>Inbound</b>, a predefined address group can be configured for the source address.</p> <ul style="list-style-type: none"> <li>● <b>Countries and regions</b>: If <b>Direction</b> is set to <b>Inbound</b>, you can control access based on continents, countries, and regions.</li> <li>● <b>Any</b>: any source address</li> </ul>	<b>IP address, 192.168.10.5</b>

Parameter	Description	Example Value
Destination	<p>Destination address of access traffic.</p> <ul style="list-style-type: none"> <li>● <b>IP address:</b> You can set a single IP address, consecutive IP addresses, or an IP address segment. <ul style="list-style-type: none"> <li>– A single IP address, for example, <b>192.168.10.5</b></li> <li>– Consecutive IP addresses, for example, <b>192.168.0.2-192.168.0.10</b></li> <li>– Address segment, for example, <b>192.168.2.0/24</b></li> </ul> </li> <li>● <b>IP address group:</b> A collection of IP addresses. For details about how to add custom IP address groups, see <a href="#">Adding an IP Address Group</a>.</li> <li>● <b>Countries and regions:</b> If <b>Direction</b> is set to <b>Outbound</b>, you can control access based on continents, countries, and regions.</li> <li>● <b>Domain name:</b> If <b>Direction</b> is set to <b>Outbound</b>, you can enter a multi-level single domain name (for example, top-level domain name <b>example.com</b> and level-2 domain name <b>www.example.com</b>) or a wildcard domain name (<b>*.example.com</b>).</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>– Mandatory for a single domain name. Click <b>Test</b> to check the validity of the domain name and perform DNS resolution. For details, see <a href="#">Configuring DNS Resolution</a>. (Currently, up to 600 IP addresses can be resolved from a domain name.)</li> <li>– If the domain name is a wildcard domain name, DNS resolution is not required. Only HTTP/HTTPS applications can be added.</li> </ul> <ul style="list-style-type: none"> <li>● <b>Domain name group:</b> If <b>Direction</b> is set to <b>Outbound</b>, a collection of multiple domain names is supported.</li> </ul> <p><b>NOTE</b></p> <p>To protect a domain name, you are advised to configure a domain name group.</p> <ul style="list-style-type: none"> <li>● <b>Any:</b> any destination address</li> </ul>	Any

Parameter	Description	Example Value
Service	<p>Set the protocol type and port number of the access traffic.</p> <ul style="list-style-type: none"> <li>● <b>Service:</b> Set <b>Protocol Type</b>, <b>Source Port</b>, and <b>Destination Port</b>. <ul style="list-style-type: none"> <li>– <b>Protocol Type:</b> The value can be TCP, UDP, or ICMP.</li> <li>– <b>Source/Destination Port:</b> If <b>Protocol Type</b> is set to <b>TCP</b> or <b>UDP</b>, you need to set the port number.</li> </ul> </li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>– To specify all the ports of an IP address, set <b>Port</b> to <b>1-65535</b>.</li> <li>– You can specify a single port. For example, to manage access on port 22, set <b>Port</b> to <b>22</b>.</li> <li>– To set a port range, use a hyphen (-) between the starting and ending ports. For example, to manage access on ports 80 to 443, set <b>Port</b> to <b>80-443</b>.</li> </ul> <ul style="list-style-type: none"> <li>● <b>Service group:</b> A collection of services (protocols, source ports, and destination ports) are supported. For details about how to add a custom service group, see <a href="#">Adding a Service Group</a>. For details about a pre-defined service group, see <a href="#">6.6.2 Viewing a Predefined Service Group</a>.</li> <li>● <b>Any:</b> any protocol type or port number</li> </ul>	<p><b>Service Protocol Type:</b> TCP <b>Source Port:</b> 80 <b>Destination Port:</b> 80-443</p>
Action	<p>Set the action to be taken when traffic passes through the firewall.</p> <ul style="list-style-type: none"> <li>● <b>Allow:</b> Traffic is forwarded.</li> <li>● <b>Block:</b> Traffic is not forwarded.</li> </ul>	Allow
Allow Long Connection	<p>If only one service is configured in the current protection rule and <b>Protocol Type</b> is set to <b>TCP</b> or <b>UDP</b>, you can configure the service session aging time.</p> <ul style="list-style-type: none"> <li>● <b>Yes:</b> Configure the long connection duration.</li> <li>● <b>No:</b> Retain the default durations. The default connection durations for different protocols are as follows: <ul style="list-style-type: none"> <li>– TCP: 1800s</li> <li>– UDP: 60s</li> </ul> </li> </ul> <p><b>NOTE</b> Up to 100 rules can be configured with long connections.</p>	Yes

Parameter	Description	Example Value
Long Connection Duration	This parameter is mandatory if <b>Allow Long Connection</b> is set to <b>Yes</b> . Configure the long connection duration. Configure the hour, minute, and second. <b>NOTE</b> The duration range is 1 second to 1000 days.	60 hours 60 minutes 60 seconds
Tags	(Optional) Tags are used to identify rules. You can use tags to classify and search for security policies.	-
Priority	Priority of the rule. Its value can be: <ul style="list-style-type: none"> <li>• <b>Pin on top</b>: indicates that the priority of the policy is set to the highest.</li> <li>• <b>Lower than the selected rule</b>: indicates that the policy priority is lower than a specified rule.</li> </ul> <b>NOTE</b> A smaller value indicates a higher priority.	Pin on top
Status	Whether a policy is enabled.  : enabled  : disabled	
Description	(Optional) Usage and application scenario	-

**Step 7** Click **OK**.


 **NOTE**


After EIP protection is enabled, the default status of the access control policy is **Allow**. If you want to allow only several EIPs, you are advised to add a protection rule with the lowest priority to block all traffic.

----End

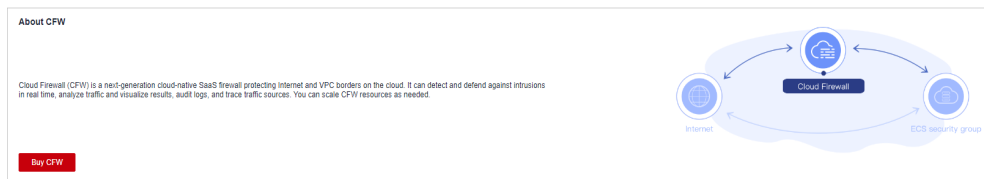
## Adding a VPC Border Protection Rule

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-2](#).

**Figure 6-2** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Access Control > Access Policies**. Click the **Inter-VPC Borders** tab.




**Step 6** Add a protection rule.

Click **Add Rule**. In the displayed dialog box, enter new protection information. For details, see [Table 6-2](#).

**Table 6-2** Adding a protection rule

Parameter	Description	Example Value
Name	Name of the custom security policy.	test
Source	Source of data packets in the access traffic. <ul style="list-style-type: none"> <li>● <b>IP address:</b> You can set a single IP address, consecutive IP addresses, or an IP address segment.                             <ul style="list-style-type: none"> <li>– A single IP address, for example, <b>192.168.10.5</b></li> <li>– Consecutive IP addresses, for example, <b>192.168.0.2-192.168.0.10</b></li> <li>– Address segment, for example, <b>192.168.2.0/24</b></li> </ul> </li> <li>● <b>IP address group:</b> A collection of IP addresses. For details, see <a href="#">Adding an IP Address Group</a>.</li> <li>● <b>Any:</b> any source address</li> </ul>	<b>IP address, 192.168.10.5</b>
Destination	Destination address of access traffic. <ul style="list-style-type: none"> <li>● <b>IP address:</b> You can set a single IP address, consecutive IP addresses, or an IP address segment.                             <ul style="list-style-type: none"> <li>– A single IP address, for example, <b>192.168.10.5</b></li> <li>– Consecutive IP addresses, for example, <b>192.168.0.2-192.168.0.10</b></li> <li>– Address segment, for example, <b>192.168.2.0/24</b></li> </ul> </li> <li>● <b>IP address group:</b> A collection of IP addresses. For details, see <a href="#">Adding an IP Address Group</a>.</li> <li>● <b>Any:</b> any destination address</li> </ul>	Any

Parameter	Description	Example Value
Service	<p>Set the protocol type and port number of the access traffic.</p> <ul style="list-style-type: none"> <li>● <b>Service:</b> Set <b>Protocol Type</b>, <b>Source Port</b>, and <b>Destination Port</b>. <ul style="list-style-type: none"> <li>– <b>Protocol Type:</b> The value can be <b>TCP</b>, <b>UDP</b>, or <b>ICMP</b>.</li> <li>– <b>Source/Destination Port:</b> If <b>Protocol Type</b> is set to <b>TCP</b> or <b>UDP</b>, you need to set the port number.</li> </ul> </li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>– To specify all the ports of an IP address, set <b>Port</b> to <b>1-65535</b>.</li> <li>– You can specify a single port. For example, to manage access on port 22, set <b>Port</b> to <b>22</b>.</li> <li>– To set a port range, use a hyphen (-) between the starting and ending ports. For example, to manage access on ports 80 to 443, set <b>Port</b> to <b>80-443</b>.</li> </ul> <ul style="list-style-type: none"> <li>● <b>Service group:</b> A collection of services (protocols, source ports, and destination ports) is supported. For details about how to add a custom service group, see <a href="#">6.6.1 Adding a Custom Service Group</a>. For details about predefined service groups, see <a href="#">6.6.2 Viewing a Predefined Service Group</a>.</li> <li>● <b>Any:</b> any protocol type or port number</li> </ul>	<p><b>Service Protocol Type:</b> TCP <b>Source Port:</b> 80 <b>Destination Port:</b> 80-443</p>
Action	<p>Set the action to be taken when traffic passes through the firewall.</p> <ul style="list-style-type: none"> <li>● <b>Allow:</b> Traffic is forwarded.</li> <li>● <b>Block:</b> Traffic is not forwarded.</li> </ul>	Allow
Allow Long Connection	<p>If only one service is configured in the current protection rule and <b>Protocol Type</b> is set to <b>TCP</b> or <b>UDP</b>, you can configure the service session aging time.</p> <ul style="list-style-type: none"> <li>● <b>Yes:</b> Configure the long connection duration.</li> <li>● <b>No:</b> Retain the default durations. The default connection durations for different protocols are as follows: <ul style="list-style-type: none"> <li>– TCP: 1800s</li> <li>– UDP: 60s</li> </ul> </li> </ul> <p><b>NOTE</b> Up to 100 rules can be configured with long connections.</p>	Yes

Parameter	Description	Example Value
Long Connection Duration	This parameter is mandatory if <b>Allow Long Connection</b> is set to <b>Yes</b> . Configure the long connection duration. Configure the hour, minute, and second. <b>NOTE</b> The duration range is 1 second to 1000 days.	60 hours 60 minutes 60 seconds
Tag	(Optional) Tags are used to identify rules. You can use tags to classify and search for security policies.	-
Priority	Priority of the rule. Its value can be: <ul style="list-style-type: none"> <li>• <b>Pin on top</b>: indicates that the priority of the policy is set to the highest.</li> <li>• <b>Lower than the selected rule</b>: indicates that the policy priority is lower than a specified rule.</li> </ul> <b>NOTE</b> A smaller value indicates a higher priority.	Pin on top
Status	Whether a policy is enabled.  : enabled  : disabled	
Description	(Optional) Usage and application scenario	-

**Step 7** Click **OK**.

 **NOTE**

After EIP protection is enabled, the default status of the access control policy is **Allow**. If you want to allow only several EIPs, you are advised to add a protection rule with the lowest priority to block all traffic.

----End

### 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 6-3](#). Its priority is the lowest. The other allows the traffic of a specified IP address, as shown in [Figure 6-4](#). Its priority is the highest.

**Figure 6-3** Blocking all traffic

**Matching Condition**

\* Direction  Inbound  Outbound

\* Source

\* Destination

\* Service

---

**Protection Action**

Action  Allow  Block

**Figure 6-4** Allowing a specified IP address

**Matching Condition**

\* Direction  Inbound  Outbound

\* Source

\* 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 **Ireland**.



**Figure 6-5** Intercepting the access traffic from Ireland

**Matching Condition**

\* Direction  Inbound  Outbound

\* Source   ⊗

⚠ 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

## Configuration Example - NAT Protection

Assume your private IP address is **10.1.1.2** and the external domain name accessed through the NAT gateway is **www.example.com**. Configure NAT protection as follows and set other parameters based on your deployment:

**Figure 6-6** Configuring a NAT protection rule

**Basic Information**

Rule Type  EIP  NAT

\* Name

---

**Matching Condition**

\* Source   ⊗

\* Destination

Test  
✔ The domain name is valid.

\* Service   ⊗



## 6.2 Managing Protection Rules in Batches

You can add and export protection rules in batches.

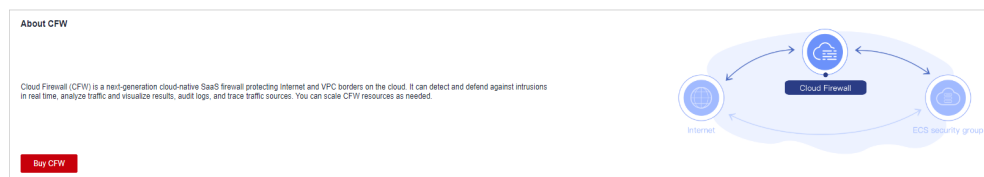
### Constraints

Only the professional edition supports the import and export of VPC border protection policies.

## Importing Protection Rules in Batches

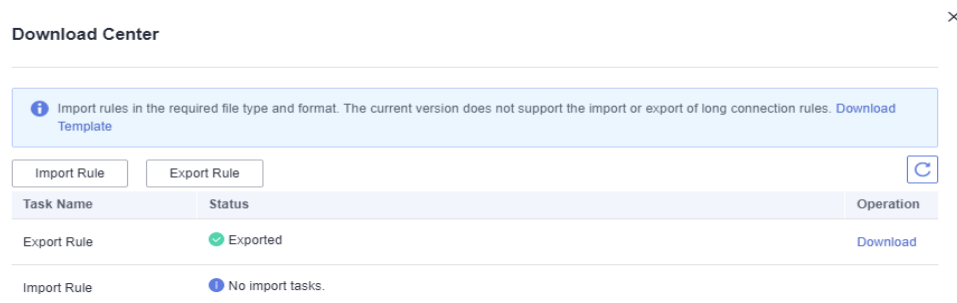
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-7](#).

**Figure 6-7** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane, choose **Access Control > Access Policies**.
- Step 6** Click **Download Center** on the upper right of the list.

**Figure 6-8** Download Center



- Step 7** Click **Download Template** to download the rule import template to the local host.
- Step 8** Fill in the template. For details, see [Parameters of Rule Import Template - Protection Rule Table \(Internet Border Protection Rule\)](#) and [Parameters of Rule Import Template - VPC Protection Rule Table \(VPC Border Protection Rule\)](#).

### NOTICE

- A maximum of 640 rules and members can be imported at a time on each tab page.
- Do not change the template file format, or it may fail to be imported.

**Step 9** After filling in the template, click **Import Rule** to import the template.

 **NOTE**

- Rule import takes several minutes.
- During rule import, you cannot add, edit, or delete access policies, IP address groups, and service groups.


**Step 10** Click **Download Center** to view the status of the rule import task. If the **Status** is **Imported**, the import succeeded.


**Step 11** Return to the protection rule list to view the imported protection rule.

----End

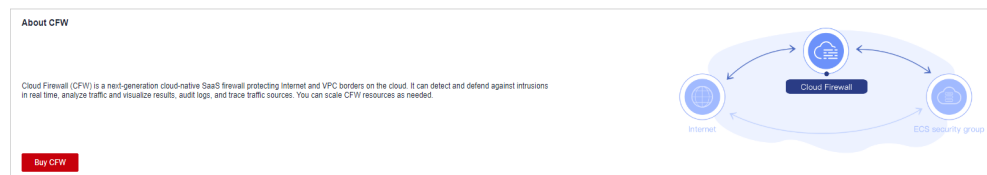
## Exporting Protection Rules in Batches

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-9](#).

**Figure 6-9** CFW Dashboard

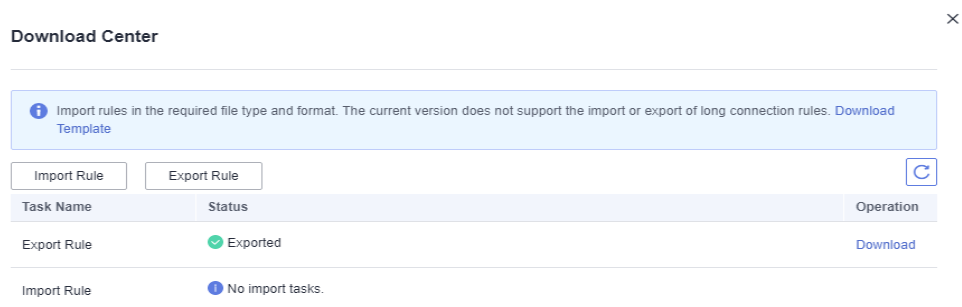


**Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

**Step 5** In the navigation pane, choose **Access Control > Access Policies**.

**Step 6** Click **Download Center** on the upper right of the list.

**Figure 6-10** Download Center



**Step 7** Click **Export Rule** to export rules to a local PC.

----End

## Parameters of Rule Import Template - Protection Rule Table (Internet Border Protection Rule)

**Table 6-3** Protection rule table parameters

Parameter	Description	Example Value
Order	Order number of a rule.	1
Acl Name	Name of the rule. The name can contain up to 255 characters, including letters, numbers, underscores (_), hyphens (-), and spaces.	test
Protection Rule	Protection type of a security policy. <ul style="list-style-type: none"><li>● <b>EIP protection:</b> Protect EIP traffic. Only EIPs can be configured.</li><li>● <b>NAT protection:</b> Protect NAT traffic. Private IP addresses can be configured.</li></ul>	EIP protection
Direction	Direction of protected traffic. <ul style="list-style-type: none"><li>● <b>Inbound:</b> Traffic from external networks to the internal server.</li><li>● <b>Outbound:</b> Traffic from the customer server to external networks.</li></ul>	Outbound
Action Type	<b>Allow</b> or <b>Block</b> . It specifies the action taken by the firewall to process traffic.	Allow
ACL Address Type	Select <b>IPv4</b> . It is the type of IP addresses to be protected.	IPv4
Status	Whether a policy is enabled. <ul style="list-style-type: none"><li>● <b>Enabled:</b> The rule is in effect.</li><li>● <b>Disabled:</b> The rule is not in effect.</li></ul>	Enabled
Description	Rule description	test
Source Address Type	Source address type of data packets in the access traffic. <ul style="list-style-type: none"><li>● <b>IP Address.</b> You can configure a single IP address, consecutive IP addresses, or an IP address segment.</li><li>● <b>IP Address Group.</b> You can configure multiple IP addresses.</li><li>● <b>Region:</b> Protection can be performed by region.</li></ul>	IP Address

Parameter	Description	Example Value
Source Address	<p>If <b>Source Address Type</b> is set to <b>IP Address</b>, you need to configure this parameter.</p> <p>The following input formats are supported:</p> <ul style="list-style-type: none"> <li>• A single IP address, for example, <b>192.168.10.5</b></li> <li>• Consecutive IP addresses, for example, <b>192.168.0.2-192.168.0.10</b></li> <li>• Address segment, for example, <b>192.168.2.0/24</b></li> </ul>	192.168.10.5
Source Address Group Name	<p>If <b>Source Address Type</b> is set to <b>IP Address Group</b>, you must configure this parameter.</p> <p>The following input formats are supported:</p> <ul style="list-style-type: none"> <li>• The value can contain letters, digits, underscores (_), hyphens (-), or spaces.</li> <li>• The name can contain up to 255 characters.</li> </ul>	s_test
Source Continent Region	<p>If <b>Source Address Type</b> is set to <b>Region</b>, you need to configure <b>Source Continent Region</b>.</p> <p>Enter the continent information according to the continent-region-info table.</p>	AS: Asia
Source Country Region	<p>If <b>Source Address Type</b> is set to <b>Region</b>, you need to configure <b>Source Country Region</b>.</p> <p>Enter the country information according to the country-region-info table.</p>	CN: Chinese mainland
Destination Address Type	<p>Destination address type of data packets in the access traffic.</p> <ul style="list-style-type: none"> <li>• <b>IP Address</b>. You can configure a single IP address, consecutive IP addresses, or an IP address segment.</li> <li>• <b>IP Address Group</b>. You can configure multiple IP addresses.</li> <li>• <b>Domain name</b>: A domain name consists of letters separated by dots (.). It is a human readable address that maps to the machine readable IP address of your server.</li> <li>• <b>Domain name group</b>. You can set a collection of domain names.</li> <li>• <b>Region</b>: Protection can be performed by region.</li> </ul>	IP Address

Parameter	Description	Example Value
Destination Address	If <b>Destination Address Type</b> is set to <b>IP Address</b> , you must configure this parameter. It can be: <ul style="list-style-type: none"> <li>• A single IP address, for example, <b>192.168.10.5</b></li> <li>• Consecutive IP addresses, for example, <b>192.168.0.2-192.168.0.10</b></li> <li>• Address segment, for example, <b>192.168.2.0/24</b></li> </ul>	192.168.10.6
Destination Address Group Name	If <b>Destination Address Type</b> is set to <b>IP Address Group</b> , you must configure this parameter. The following input formats are supported: <ul style="list-style-type: none"> <li>• The value can contain letters, digits, underscores (_), hyphens (-), or spaces.</li> <li>• The name can contain up to 255 characters.</li> </ul>	d_test
Destination Continent Region	If <b>Destination Address Type</b> is set to <b>Region</b> , you need to set <b>Destination Continent Region</b> . Enter the continent information according to the continent-region-info table.	AS: Asia
Destination Country Region	If <b>Destination Address Type</b> is set to <b>Region</b> , you need to set <b>Destination Country Region</b> . Enter the country information according to the country-region-info table.	CN: Chinese mainland
Domain Name	If <b>Destination Address Type</b> is set to <b>Domain Name</b> , you must configure this parameter. The domain name is used by visitors to access your website. A domain name consists of letters separated by dots (.). It is a human readable address that maps to the machine readable IP address of your server.	www.example.com
Destination Domain Group Name	If <b>Destination Address Type</b> is set to <b>Domain Group Name</b> , you need to configure <b>Destination Domain Group Name</b> . Enter a domain group name.	Domain group 1

Parameter	Description	Example Value
Service Type	Service type. It can be: <ul style="list-style-type: none"> <li>• <b>Service</b>. You can configure a single service.</li> <li>• <b>Service Group</b>. You can configure multiple services.</li> </ul>	Service
Protocol/ Source Port/ Destination Port	Type to be put under access control. <ul style="list-style-type: none"> <li>• Its value can be <b>TCP, UDP, ICMP, or Any</b>.</li> <li>• Source ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: <b>80-443</b>).</li> <li>• Destination ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: <b>80-443</b>).</li> </ul>	TCP/443/443
Service Group Name	Service group name. The name can contain up to 255 characters, including letters, numbers, underscores (_), hyphens (-), and spaces.	service_test
Group Tag	Tags are used to identify rules. You can use tags to classify and search for security policies.	k=a

## Parameters of Rule Import Template - VPC Protection Rule Table (VPC Border Protection Rule)

Table 6-4 VPC protection rule table parameters

Parameter	Description	Example Value
Order	Order number of a rule.	1
Acl Name	Name of the rule. The name can contain up to 255 characters, including letters, numbers, underscores (_), hyphens (-), and spaces.	test
Action Type	<b>Allow</b> or <b>Block</b> . It specifies the action taken by the firewall to process traffic.	Allow
Status	Whether a policy is enabled. <ul style="list-style-type: none"> <li>• <b>Enabled</b>: The rule is in effect.</li> <li>• <b>Disabled</b>: The rule is not in effect.</li> </ul>	Enabled

Parameter	Description	Example Value
Description	Rule description	test
Source Address Type	Source address type of data packets in the access traffic. <ul style="list-style-type: none"> <li>● <b>IP Address.</b> You can configure a single IP address, consecutive IP addresses, or an IP address segment.</li> <li>● <b>IP Address Group.</b> You can configure multiple IP addresses.</li> </ul>	IP Address
Source Address	If <b>Source Address Type</b> is set to <b>IP Address</b> , you need to configure this parameter. The following input formats are supported: <ul style="list-style-type: none"> <li>● A single IP address, for example, <b>192.168.10.5</b></li> <li>● Consecutive IP addresses, for example, <b>192.168.0.2-192.168.0.10</b></li> <li>● Address segment, for example, <b>192.168.2.0/24</b></li> </ul>	192.168.10.5
Source Address Group Name	If <b>Source Address Type</b> is set to <b>IP Address Group</b> , you must configure this parameter. The following input formats are supported: <ul style="list-style-type: none"> <li>● The value can contain letters, digits, underscores (_), hyphens (-), or spaces.</li> <li>● The name can contain up to 255 characters.</li> </ul>	s_test
Destination Address Type	Destination address type of data packets in the access traffic. <ul style="list-style-type: none"> <li>● <b>IP Address.</b> You can configure a single IP address, consecutive IP addresses, or an IP address segment.</li> <li>● <b>IP Address Group.</b> You can configure multiple IP addresses.</li> </ul>	IP Address Group
Destination Address	If <b>Destination Address Type</b> is set to <b>IP Address</b> , you must configure this parameter. It can be: <ul style="list-style-type: none"> <li>● A single IP address, for example, <b>192.168.10.5</b></li> <li>● Consecutive IP addresses, for example, <b>192.168.0.2-192.168.0.10</b></li> <li>● Address segment, for example, <b>192.168.2.0/24</b></li> </ul>	192.168.10.6



Parameter	Description	Example Value
Destination Address Group Name	If <b>Destination Address Type</b> is set to <b>IP Address Group</b> , you must configure this parameter. The following input formats are supported: <ul style="list-style-type: none"><li>• The value can contain letters, digits, underscores (_), hyphens (-), or spaces.</li><li>• The name can contain up to 255 characters.</li></ul>	d_test
Service Type	Service type. It can be: <ul style="list-style-type: none"><li>• <b>Service</b>. You can configure a single service.</li><li>• <b>Service Group</b>. You can configure multiple services.</li></ul>	Service
Protocol/ Source Port/ Destination Port	Type to be put under access control. <ul style="list-style-type: none"><li>• Its value can be <b>TCP</b>, <b>UDP</b>, <b>ICMP</b>, or <b>Any</b>.</li><li>• Source ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: <b>80-443</b>).</li><li>• Destination ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: <b>80-443</b>).</li></ul>	TCP/443/443
Service Group Name	Service group name. The name can contain up to 255 characters, including letters, numbers, underscores (_), hyphens (-), and spaces.	service_test
Group Tag	Tags are used to identify rules. You can use tags to classify and search for security policies.	k=a


## 6.3 Configuring a Rule Priority


This section describes how to adjust the priorities of rules.

The value 1 indicates the highest priority. A larger value indicates a lower priority.

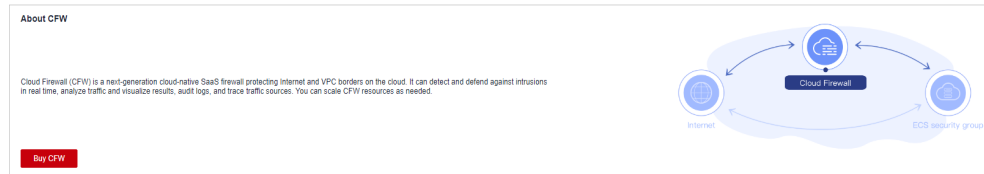
### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-11](#).

**Figure 6-11** CFW Dashboard



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

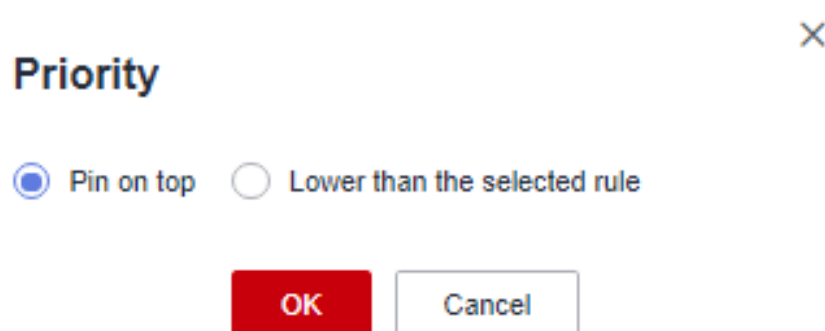
**Step 5** In the navigation pane, choose **Access Control > Access Policies**.

**Step 6** In the **Operation** column of a rule, click **Configure Priority**.

**Step 7** Select **Pin on top** or **Lower than the selected rule**.

- If you select **Pin on top**, the policy is set to the highest priority.
- If you select **Lower than the selected rule**, you need to select a rule. The policy priority will be lower than the selected rule.

**Figure 6-12** Configuring priority



**Step 8** Click **OK**.

----End

## 6.4 Managing the Blacklist and the Whitelist

### 6.4.1 Adding an Item to the Blacklist or Whitelist

After EIP protection is enabled, all access is allowed by default. You can configure blacklist or whitelist rules to block or allow access requests from specific IP addresses.

**CAUTION**

If your IP address is a back-to-source WAF IP address, you are advised to configure a protection rule or the whitelist to allow its access. Exercise caution when configuring the blacklist, which may affect your services.

- For details back-to-source IP addresses, see [What Are Back-to-Source IP Addresses?](#)
- For details about how to configure protection rules, see [6.1 Adding a Protection Rule](#).

## Specification Limitations


The CFW blacklist and whitelist each allows up to 2000 items. If there are too many IP addresses to be specified, you can put them in an IP address group dedicated to the blacklist or whitelist. For more information, see [6.5.1 Adding Custom IP Address Groups](#).


## Impact on the System

CFW directly allows whitelisted IP addresses and segments and blocks blacklisted ones without checking. To check the access and traffic statistics of these IP addresses, search for them by following the instructions in [12.1 Querying Logs](#).

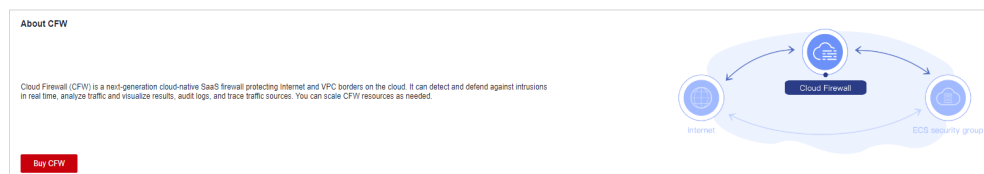
## Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-13](#).

**Figure 6-13** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Access Control > Access Policies**. Click the **Blacklist** or **Whitelist** tab.

**Step 6** Click **Add**. Set the address direction, IP address, protocol type, and port number. For details, see [Table 6-5](#).

**Table 6-5** Blacklist and whitelist parameters

Parameter	Description
Direction	You can select <b>Source</b> or <b>Destination</b> . <ul style="list-style-type: none"><li>• <b>Source:</b> The IP address or IP address group that sends data packets.</li><li>• <b>Destination:</b> The destination IP address or IP address group that receives data packets.</li></ul>
IP Address	You can configure a single IP address, consecutive IP addresses, or an IP address segment.
Protocol Type	Its value can be <b>TCP</b> , <b>UDP</b> , <b>ICMP</b> , or <b>Any</b> .
Port	If <b>Protocol Type</b> is set to <b>TCP</b> or <b>UDP</b> , set the ports to be allowed or blocked. <b>NOTE</b> <ul style="list-style-type: none"><li>• To specify all the ports of an IP address, set <b>Port</b> to <b>1-65535</b>.</li><li>• You can specify a single port. For example, to allow or block the access from port 22 of an IP address, set <b>Port</b> to <b>22</b>.</li><li>• To set a port range, use a hyphen (-) between the starting and ending ports. For example, to allow or block the access from ports 80-443 of an IP address, set <b>Port</b> to <b>80-443</b>.</li></ul>
Description	Description of the blacklist or whitelist

**Step 7** Click **OK**.


----End


## 6.4.2 Editing the Blacklist or Whitelist

You can modify the IP address, direction, name, protocol type, and more configurations in the blacklist or whitelist.

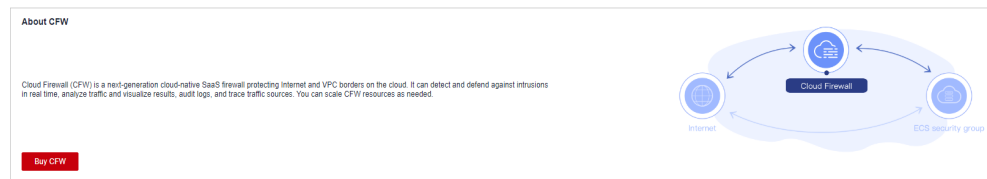
### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-14](#).

**Figure 6-14** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Access Control > Access Policies**. Click the **Blacklist** or **Whitelist** tab.

**Step 6** In the row containing the desired rule, click **Edit** in the **Operation** column.

Modify the parameters. For details about the parameters, see [Blacklist and whitelist](#).

**Table 6-6** Blacklist and whitelist parameters

Parameter	Description
Direction	You can select <b>Source</b> or <b>Destination</b> . <ul style="list-style-type: none"> <li>• <b>Source:</b> The IP address or IP address group that sends data packets.</li> <li>• <b>Destination:</b> The destination IP address or IP address group that receives data packets.</li> </ul>
IP Address	You can configure a single IP address, consecutive IP addresses, or an IP address segment.
Protocol Type	Its value can be <b>TCP</b> , <b>UDP</b> , <b>ICMP</b> , or <b>Any</b> .
Port	If <b>Protocol Type</b> is set to <b>TCP</b> or <b>UDP</b> , set the ports to be allowed or blocked. <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• To specify all the ports of an IP address, set <b>Port</b> to <b>1-65535</b>.</li> <li>• You can specify a single port. For example, to allow or block the access from port 22 of an IP address, set <b>Port</b> to <b>22</b>.</li> <li>• To set a port range, use a hyphen (-) between the starting and ending ports. For example, to allow or block the access from ports 80-443 of an IP address, set <b>Port</b> to <b>80-443</b>.</li> </ul>
Description	Description of the blacklist or whitelist

**Step 7** Click **OK**.


----End


## 6.4.3 Removing a Blacklisted or Whitelisted Item

You can remove an item from the blacklist or whitelist.

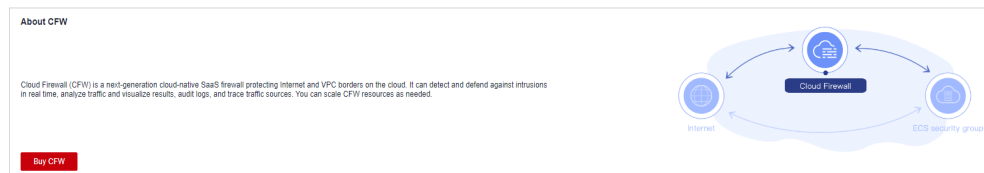
### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-15](#).

**Figure 6-15** CFW Dashboard



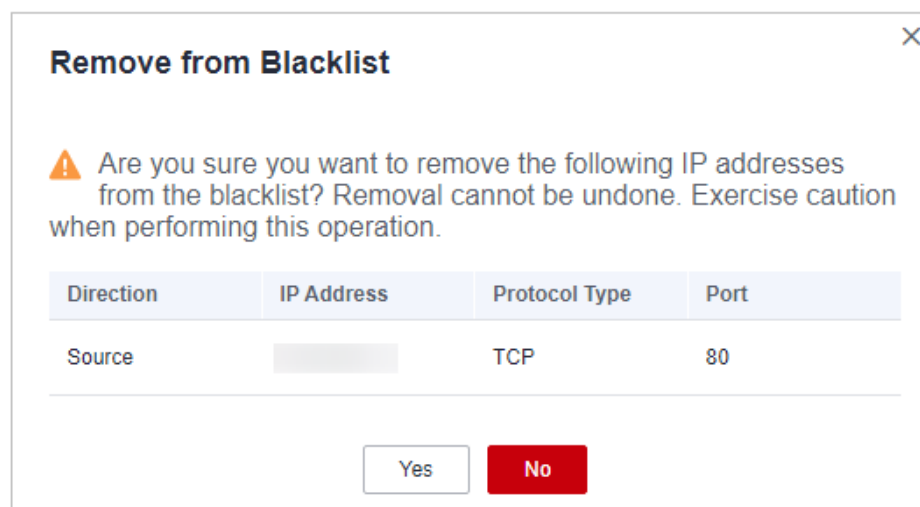
**Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

**Step 5** In the navigation pane, choose **Access Control > Access Policies**. Click the **Blacklist** or **Whitelist** tab.

**Step 6** In the row of an IP address, click **Delete** in the **Operation** column.

**Step 7** In the **Remove from Blacklist** or **Remove from Whitelist** dialog box, click **Yes**.

**Figure 6-16** Removing a blacklisted item



**Figure 6-17** Removing a whitelisted item**WARNING**

Removed items cannot be restored. Exercise caution when performing this operation.

----End

## 6.5 Managing IP Address Groups

### 6.5.1 Adding Custom IP Address Groups


An IP address group contains multiple IP addresses. An IP address group frees you from repeatedly modifying access rules and allows you to manage access rules in batch.


#### Constraints

- An IP address group can contain up to 640 IP addresses.
- A firewall instance can contain up to 3800 IP address groups.
- A firewall instance can contain up to 30,000 IP addresses.

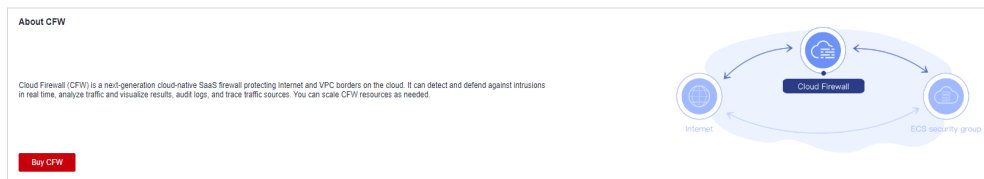
#### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-18](#).

**Figure 6-18** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation tree on the left, choose **Access Control > IP Address Groups**. The **IP Address Groups** page is displayed.
- Step 6** Click **Add IP Address Group**. On the **Basic Information** page configure the parameters. For more information, see [IP address group parameters](#).

**Table 6-7** IP address group parameters

Parameter	Description
IP Address Group Name	Name of an IP address group. It must meet the following requirements: <ul style="list-style-type: none"> <li>Only uppercase letters (A to Z), lowercase letters (a to z), numbers (0 to 9), and the following special characters are allowed: -_</li> <li>The length cannot exceed 255 characters.</li> </ul>
Description	Usage and application scenario of a rule It must meet the following requirements: <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 length cannot exceed 255 characters.</li> </ul>
IP Addresses	Enter IP addresses and click <b>Parse</b> to add them to the IP address list. The input can be: <ul style="list-style-type: none"> <li>A single IP address. Example: <b>192.168.10.5</b></li> <li>Address segment. Example: <b>192.168.2.0/24</b></li> <li>Consecutive IP addresses. Example: <b>192.168.0.2-192.168.0.10</b></li> <li>Multiple IP addresses. Use commas (,), semicolons (;), line breaks, tab characters, or spaces to separate them. Example: <b>192.168.1.0,192.168.1.0/24.</b></li> </ul>

- Step 7** Confirm the information and click **OK**. The IP address group is added.

----End



## Follow-up Operations

- [6.5.3 Adding an IP Address](#)
- An IP address group takes effect only after it is set in a protection rule. For more information, see [6.1 Adding a Protection Rule](#).

## 6.5.2 Viewing a Predefined Address Group

CFW provides you with predefined address groups, including **NAT64 Address Set** and **WAF\_Back-to-Source\_IP\_Addresses**. You are advised to allow access from both the address groups.

- **NAT64 Address Set:** If the IPv6 EIP function is enabled, CFW will convert a source IPv6 address to an IP address in this address group. For details about the IPv6 EIP function, see [Assigning or Releasing an IPv6 EIP](#).

### NOTE

If you have enabled the IPv6 EIP function, you are advised to allow traffic from **NAT64 Address Set**.

- **WAF\_Back-to-Source\_IP\_Addresses:** provides back-to-source IP addresses of Huawei Cloud WAF in cloud mode. For more information, see [What Are Back-to-Source IP Addresses?](#)


### CAUTION


- If these groups are specified in a protection rule and the back-to-source IP address changes, you do not need to manually update the rule. The firewall automatically updates the IP address in the address group every day.
- If these groups are added to the blacklist or whitelist, and the back-to-source IP address changes, you need to manually update the blacklist or whitelist.

You can only view predefined address groups, but cannot add IP addresses to it, or modify or delete it.

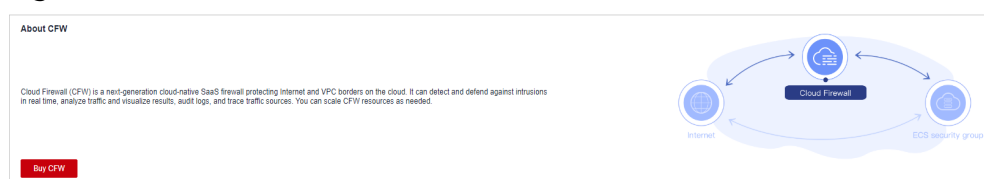
## Viewing a Predefined Address Group

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-19](#).

**Figure 6-19** CFW Dashboard





- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
  - Step 5** In the navigation tree on the left, choose **Access Control > IP Address Groups**. The **IP Address Groups** page is displayed.
  - Step 6** Click the **Predefined Address Group** tab and click the name of an address group. On the details page that is displayed, view the address group information.
- End

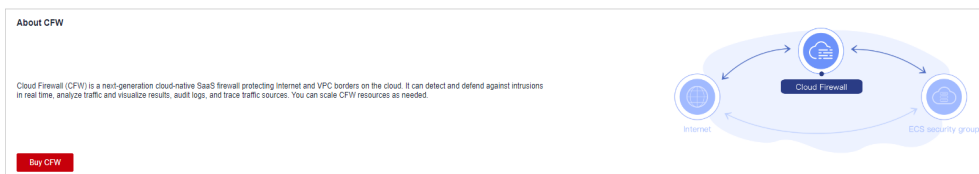
### 6.5.3 Adding an IP Address

This section describes how to add custom IP addresses to a group.

#### Procedure

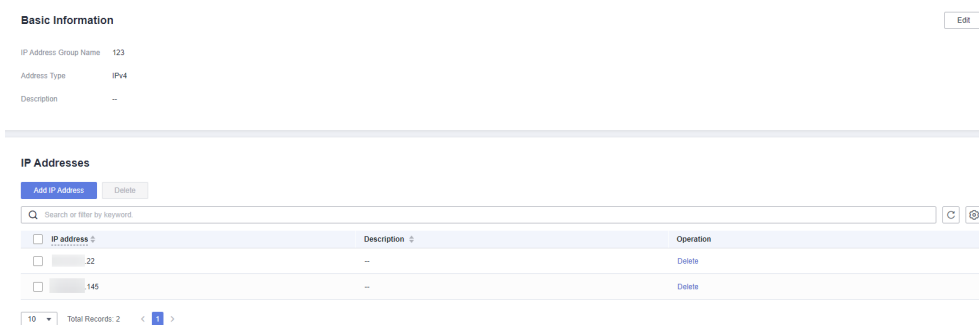
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-20](#).

**Figure 6-20** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation tree on the left, choose **Access Control > IP Address Groups**. The **IP Address Groups** page is displayed.
- Step 6** Click the name of an IP address group. Check its basic information and IP address list.

**Figure 6-21** IP address group information



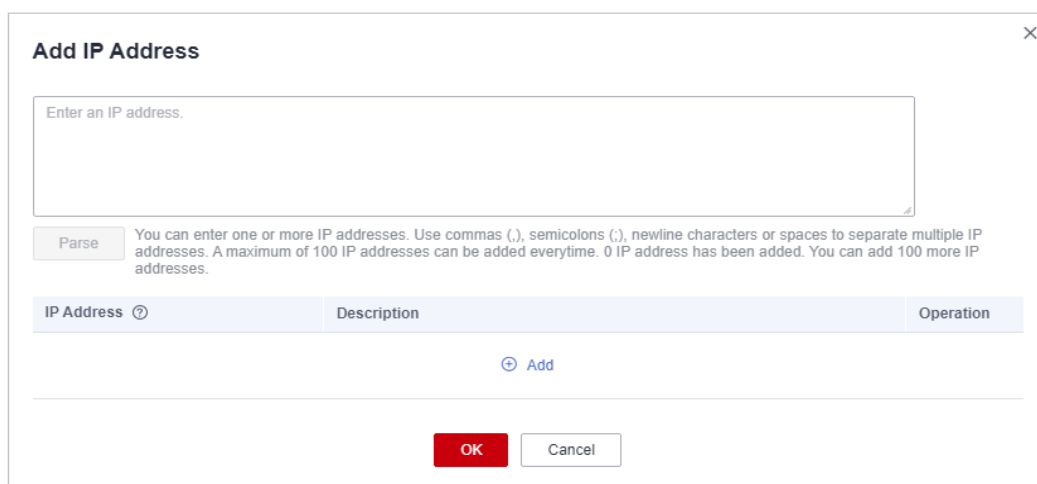
**Step 7** In the **IP Addresses** area, click **Add IP Address**.

- To add IP addresses in batches, enter the IP addresses in the text box and click **Parse**.

The input can be:

- A single IP address. Example: **192.168.10.5**
- Address segment. Example: **192.168.2.0/24**
- Consecutive IP addresses. Example: **192.168.0.2-192.168.0.10**
- Multiple IP addresses. Use commas (,), semicolons (;), line breaks, tab characters, or spaces to separate them. Example:  
192.168.1.0,192.168.1.0/24.
- To add a single IP address, click **Add**, and enter the IP address and description.

**Figure 6-22** Adding an IP address



**Table 6-8** IP address parameters

Parameter	Description	Example Value
IP Address	You can set a single IP address, multiple consecutive IP addresses, or an IP address segment, for example, <b>10.1.1.1</b> , <b>10.1.1.2/24</b> , or <b>10.1.1.1-10.1.1.2</b> .	10.1.1.1
Description	Usage and application scenario of a group	-

**Step 8** In the **Add IP Address** dialog box, add IP addresses. You can click **Add** to add more IP addresses.

**Step 9** Confirm the information and click **OK**.

----End



## Related Operation

Batch deletion: In the **IP Addresses** area, select IP addresses and click **Delete** above the list.

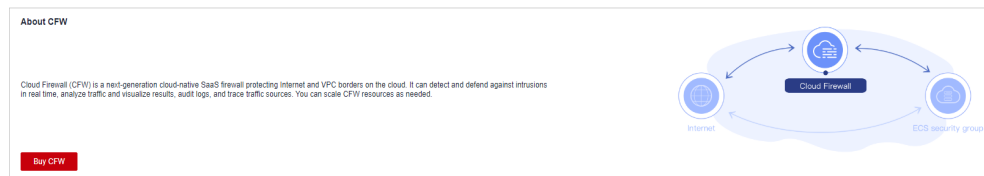
### 6.5.4 Delete an IP Address Group

This section describes how to delete custom IP address groups.

#### Procedure

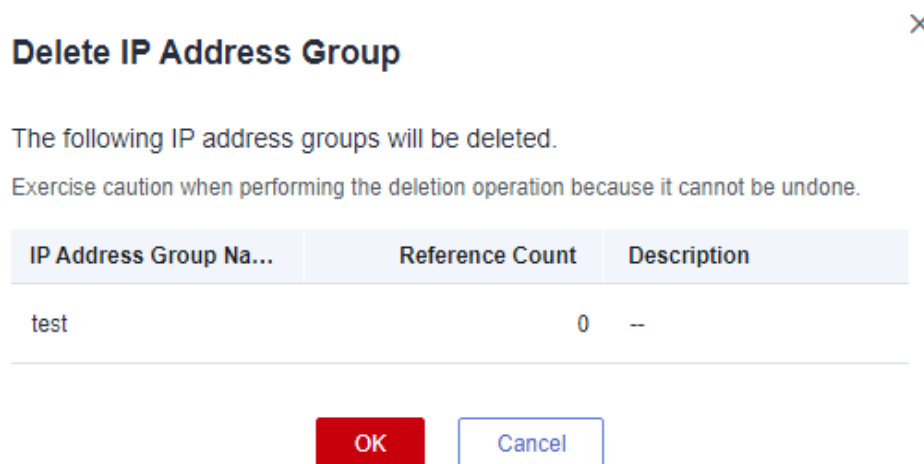
- Step 1** [Log in to the management console.](#)
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-23](#).

**Figure 6-23** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane, choose **Access Control > IP Address Groups**.
- Step 6** In the row of an IP address group, click **Delete** in the **Operation** column.
- Step 7** In the **Delete IP Address Group** dialog box, click **Yes**.

**Figure 6-24** Delete an IP address group



**WARNING**

Deleted IP address groups cannot be restored. Exercise caution when performing this operation.

----End

## 6.6 Managing Service Groups

### 6.6.1 Adding a Custom Service Group


A service group is a collection of services (protocols, source ports, and destination ports). A service group frees you from repeatedly modifying access rules and simplifies security group rule management.


#### Constraints

- A service group can have up to 64 services.
- A firewall instance can have up to 512 service groups.
- A firewall instance can have up to 900 services.

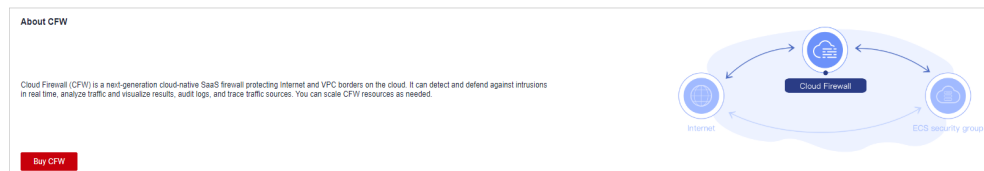
#### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-25](#).

**Figure 6-25** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Access Control > Service Groups**.

**Step 6** Click **Add Service Group**. On the displayed **Basic Information** page, enter the service group name and description.

**Figure 6-26** Basic information

**Table 6-9** Service group parameters

Parameter	Description
Service Group Name	Name of a service group
Description	Usage and application scenario
Services	<ul style="list-style-type: none"> <li>● <b>Protocol:</b> Select a protocol. Supported protocols include TCP, UDP, and ICMP.</li> <li>● <b>Source Port:</b> Set the source port to be allowed or blocked. You can configure a single port or consecutive port groups (example: <b>80-443</b>).</li> <li>● <b>Destination Port:</b> Set the destination port to be allowed or blocked. You can configure a single port or consecutive port groups (example: <b>80-443</b>).</li> <li>● <b>Description:</b> Usage and application scenario of the service group</li> </ul>

**Step 7** Confirm the information and click **OK**.

----End

## Follow-up Operations

- [6.6.3 Adding a Service](#)
- A service group takes effect only after it is set in a protection rule. For more information, see [6.1 Adding a Protection Rule](#).


## 6.6.2 Viewing a Predefined Service Group


CFW provides predefined service groups, including **Web Service**, **Database**, and **Remote Login and Ping**, suitable for protecting web services, databases, and servers, respectively.

You can only view predefined service groups, but cannot add services to it, or modify or delete it.

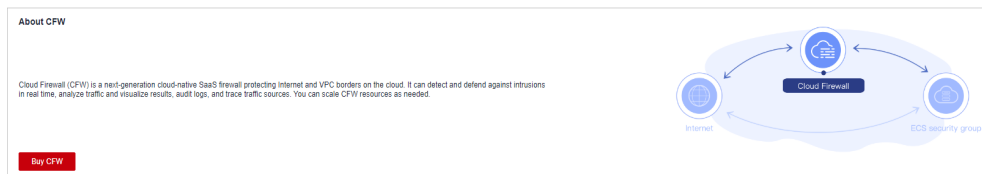
## Viewing a Predefined Service Group

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-27](#).

**Figure 6-27** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Access Control > Service Groups**.

**Step 6** Click the **Pre-defined Service Groups** tab and click the name of a service group. On the details page that is displayed, view the service group information.


----End


### 6.6.3 Adding a Service

This section describes how to add a service (protocol, source port, and destination port) to a custom service group.

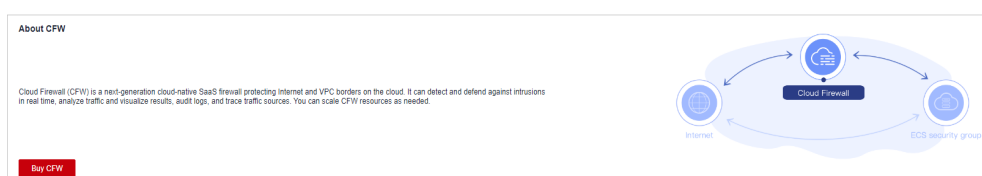
#### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-28](#).

**Figure 6-28** CFW Dashboard

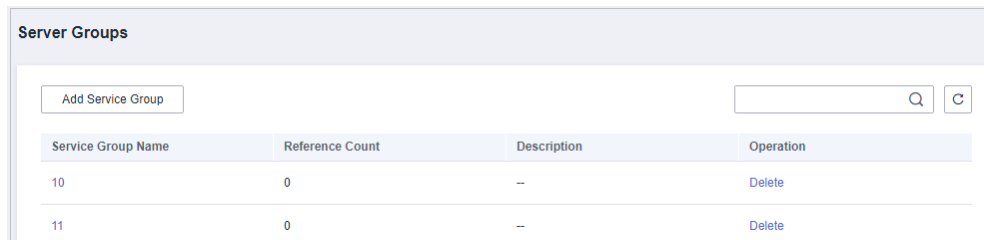


**Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

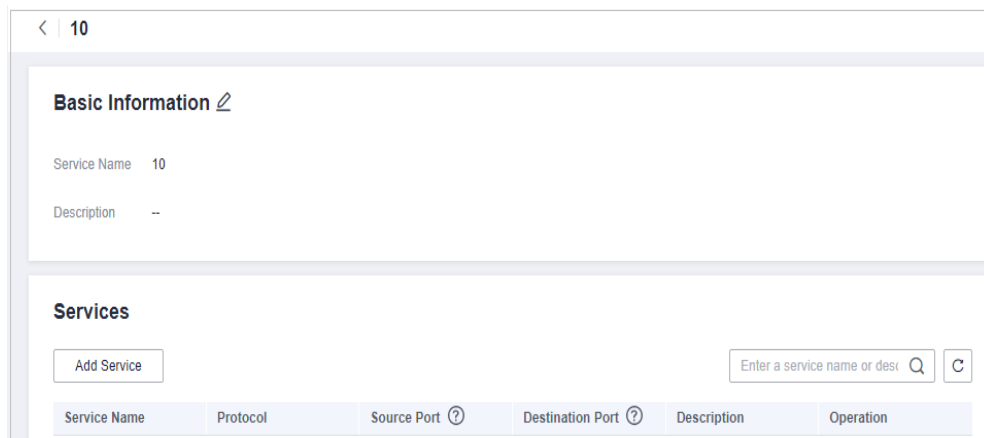
**Step 5** In the navigation pane, choose **Access Control > Service Groups**.

**Step 6** Click a service group name. The basic information and service list are displayed.

**Figure 6-29** Service group name

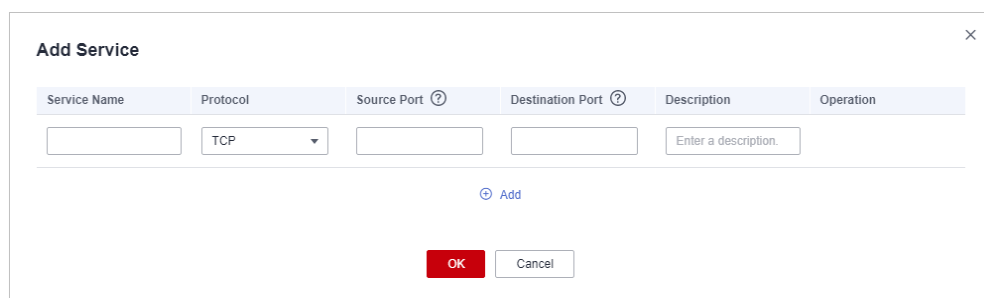


**Figure 6-30** Basic information and service list



**Step 7** Click **Add Service** in the **Services** area. The **Add Service** dialog box is displayed.

**Figure 6-31** Adding a service



**Table 6-10** Service parameters

Parameter Name	Description	Example Value
Service Name	User defined service name	test



Parameter Name	Description	Example Value
Protocol	Its value can be <b>TCP, UDP, or ICMP</b> .	TCP
Source Port	Source ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: <b>80-443</b> ).	80
Destination Port	Destination ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: <b>80-443</b> ).	80
Description	Usage and application scenario	-

**Step 8** On the **Add Service** page, click  **Add** to add multiple services.

**Step 9** Confirm the information and click **OK**.

----End

## Related Operation

To batch delete services, select services in the service list and click **Delete** above the list.


### 6.6.4 Deleting a User-defined Service Group


A service group is a collection of ports. You can use service groups to easily protect high-risk ports and manage access rules, free from repeated editing of access rules.

This section describes how to delete a user-defined service group.

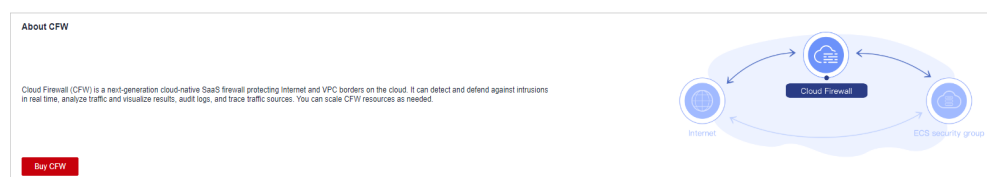
#### Deleting a Service Group

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-32](#).

**Figure 6-32** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane, choose **Access Control > Service Groups**.
- Step 6** In the row containing the desired service group, click **Delete** in the **Operation** column.
- Step 7** In the displayed dialog box, confirm the deletion information and click **Yes**.



Deleted service groups cannot be restored. Exercise caution when performing this operation.

---

----End

## 6.7 Managing Domain Name Groups

### 6.7.1 Adding a Domain Name Group

A domain name group is a collection of multiple domain names or wildcard domain names. You can configure domain name groups to protect domains in batches.

The options are as follows:

- **Website filtering:** Layer 7 protocol parsing. Websites are matched based on domain names. HTTP/HTTPS is supported.
- **DNS resolution:** Layer 4 protocol parsing. Domain names are filtered based on resolved IP addresses. TCP, UDP, and ICMP are supported. For details about IP address resolution, see [13.3 Configuring DNS Resolution](#).

#### Constraints

- Domain names in Chinese cannot be added to domain name groups.
- The domain names in a domain name group can be referenced by protection rules for up to 40,000 times, and wildcard domain names can be referenced for up to 2,000 times.

#### URL Filtering (Layer 7 Protocol Parsing)

- A domain name group can have up to 1,500 domain names.
- A firewall instance can have up to 500 domain name groups.
- A firewall instance can have up to 2,500 domain names.


#### Address Resolution (Layer 4 Protocol Parsing)


- A domain name group can have up to 15 domain names.
- Each domain name can resolve up to 1000 IP addresses.
- Each domain name group can resolve up to 1,500 IP addresses.

- A firewall instance can have up to 1000 domain names.

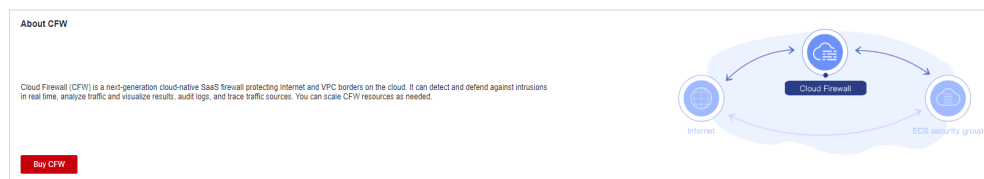
## Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-33](#).

**Figure 6-33** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Access Control > Domain Name Groups**.

**Step 6** Click **Add Domain Name Group** and configure [parameters](#).

**Table 6-11** Domain name group parameters

Parameter	Description
Group Name	Name of a user-defined domain name group.
Domain Name Group Type	The options are as follows: <ul style="list-style-type: none"> <li>• <b>Website filtering</b>: Layer 7 protocol parsing. Websites are matched based on domain names. HTTP/HTTPS is supported.</li> <li>• <b>DNS resolution</b>: Layer 4 protocol parsing. Domain names are filtered based on resolved IP addresses. TCP, UDP, and ICMP are supported. For details about IP address resolution, see <a href="#">13.3 Configuring DNS Resolution</a>.</li> </ul>
Description	(Optional) Enter remarks for the domain name group.

Parameter	Description
Domain Name	<p>Enter one or multiple domain names.</p> <ul style="list-style-type: none"> <li>You can enter a multi-level single domain name (for example, top-level domain name <b>example.com</b> and level-2 domain name <b>www.example.com</b>) or a wildcard domain name (<b>*.example.com</b>).</li> <li>Multiple domain names are separated by commas (,), semicolons (;), line breaks, or spaces.</li> </ul> <p><b>NOTE</b> Domain names must be unique.</p>

----End

## Related Operation

- To edit a domain name group, click **Edit** in the **Operation** column.
- A domain name group takes effect only after it is set in a protection rule. For more information, see [6.1 Adding a Protection Rule](#).
- To view the IP addresses resolved by a domain name group of the DNS resolution type, click the domain name group name to go to the **Basic Information** page, and click **IP address** in the **Operation** column of the domain name list.


## 6.7.2 Deleting a Domain Name Group


### Constraints

A domain name group that is being referenced cannot be deleted.

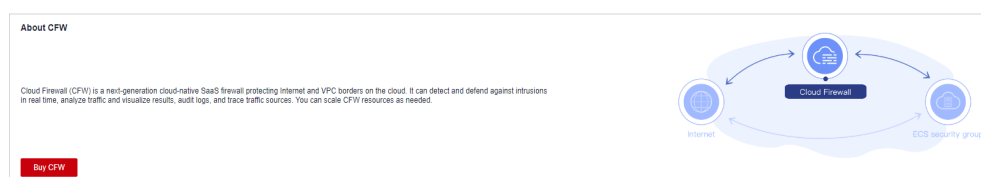
### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-34](#).

**Figure 6-34** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane, choose **Access Control > Domain Name Groups**.
- Step 6** Locate the row that contains the item to be deleted. Click **Delete** in the **Operation** column. In the displayed dialog box, enter **DELETE** and click **OK**.

---

**WARNING**

Deleted domain names cannot be restored. Exercise caution when performing this operation.



---

----End

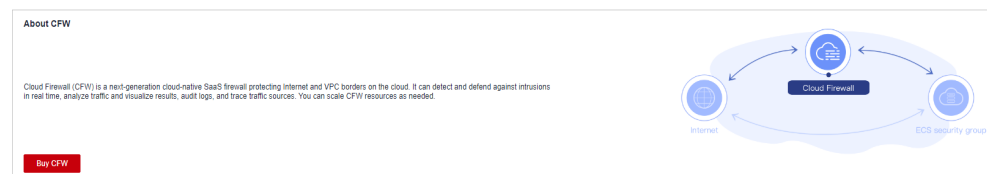
## 6.8 Policy Assistant

After a protection policy is configured, you can use the policy assistant to check policy hits and adjust policies.

### 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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-35](#).

**Figure 6-35** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane, choose **Access Control > Policy Assistant**.
- Step 6** View statistics about the protection rules of a firewall instance.
- **Policy Dashboard:** Number of accesses that hit policies (protection rules, blacklist, and whitelist), numbers of allowed and blocked accesses, and the allow and block policies that were frequently hit within a specified time range.
  - **Policy Hits:** Hits of a rule within a specified time range.

- **Visualizations:** Top 5 items ranked by certain parameters regarding blocked attacks within a specified time range. For more information, see [Table 6-12](#). You can click a record to view policy matching details. For more information, see [Table 12-2](#).

**Table 6-12** Policy assistant statistics parameters

Parameter	Description
Top Policies By Hits	Policies that match and block traffic.
Top Blocked Outbound IP Addresses	Blocked outbound IP addresses. You can click <b>Source</b> or <b>Destination</b> to view the source or destination IP addresses.
Top Blocked Inbound IP Addresses	Blocked inbound IP addresses. You can click <b>Source</b> or <b>Destination</b> to view the source or destination IP addresses.
Top Blocked Destination Ports	Blocked destination ports. You can click <b>Outbound</b> or <b>Inbound</b> to view ports in the corresponding direction.
Top Blocked IP Address Regions	Regions of blocked IP addresses. You can click <b>Destination of outbound access</b> or <b>Source of inbound access</b> to check IP addresses.

- **Inactive Policies:** Policies that have not been hit or enabled for more than three months. You are advised to modify or delete the policies in a timely manner.

----End


## 6.9 Managing Protection Rules


### 6.9.1 Checking the ACL Rule List

You can view the current access control information in the list, including the action, direction, and priority of the source and destination IP addresses.

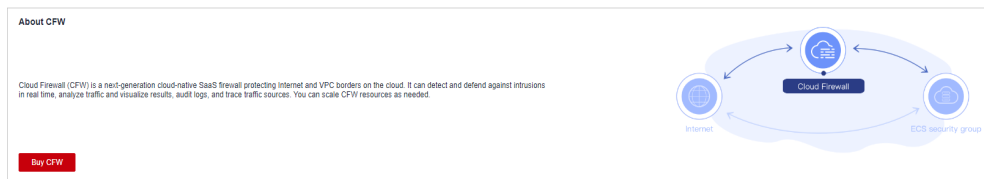
#### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-36](#).

**Figure 6-36** CFW Dashboard



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

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

**Table 6-13** Protection rule parameters

Parameter	Description
Priority	Priority of the rule. <b>NOTE</b> A smaller value indicates a higher priority.
Name	Name of the rule
Direction	Traffic direction of the protection rule.
Source	Source of data packets in the access traffic.
Destination	Destination of data packets in the access traffic.
Service	<ul style="list-style-type: none"> <li>Its value can be <b>TCP</b>, <b>UDP</b>, <b>ICMP</b>, or <b>Any</b>.</li> <li>Source Port: Source ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: <b>80-443</b>).</li> <li>Destination Port: Destination ports to be allowed or blocked. It can be a single port or port groups (example: <b>80-443</b>).</li> </ul>
Action	<ul style="list-style-type: none"> <li><b>Allow</b>: Allow the traffic to pass through the firewall.</li> <li><b>Block</b>: Block the traffic from passing through the firewall.</li> </ul>
Hits	Total number of actions that have been triggered by the rule (since the last reset). For details, see <a href="#">Access Control Logs</a> .
Status	Status of the rule. It can be enabled or disabled.
Tag	Tag of a rule.

**Step 6** (Optional) Select a direction and a protocol type from the drop-down list boxes.


----End

## 6.9.2 Editing a Protection Rule

You can modify the direction, name, source type, and more configurations of a protection rule.

### 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.


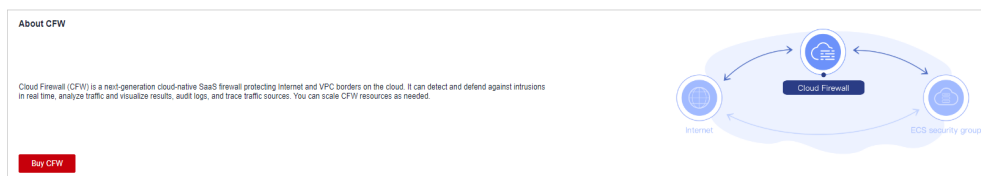
**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-37](#).

Figure 6-37 CFW Dashboard



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

**Step 5** In the navigation pane, choose **Access Control > Access Policies**.

**Step 6** In the row of a rule, click **Edit** in the **Operation** column.

**Step 7** In the displayed **Edit Rule** dialog box, modify the rule parameters.

**Step 8** Click **OK**.

----End


## 6.9.3 Copying a Protection Rule


After adding a protection rule, you can copy a rule and modify parameters to quickly create a new protection rule on the **Access Policies** page.

The default priority of a new protection rule is **1** (highest priority).

### Procedure

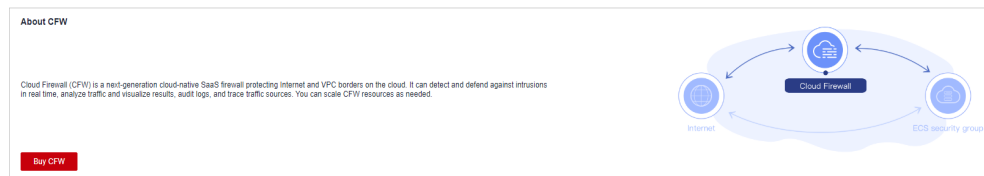
**Step 1** Log in to the management console.

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-38](#).



**Figure 6-38** CFW Dashboard





- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane, choose **Access Control > Access Policies**.
- Step 6** In the row of a rule, choose **More > Copy** in the **Operation** column.
- Step 7** Modify parameters and click **OK**. The default priority of a new protection rule is **1** (highest priority).

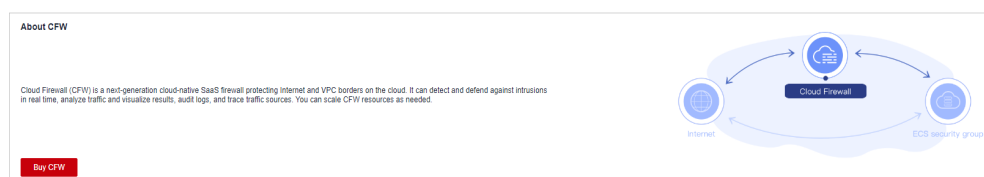
----End

## 6.9.4 Deleting a Rule

### 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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 6-39](#).

**Figure 6-39** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane, choose **Access Control > Access Policies**.
- Step 6** In the row of a rule, choose **More > Delete** in the **Operation** column.
- Step 7** In the **Delete Rule** dialog box, click **Yes**.

 **WARNING**

Deleted rules cannot be restored. Exercise caution when performing this operation.

---

----End

# 7 Configuring Intrusion Prevention

CFW provides you with basic protection 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.


Basic protection cannot be disabled, but can be changed with protection mode. Basic protection functions scan traffic for attacks, threats, and vulnerabilities, such as phishing, Trojans, worms, hacker tools, spyware, password attacks, vulnerability exploits, SQL injection attacks, XSS attacks, and web attacks. They also check for exceptions in protocols, buffer overflow, access control, and suspicious DNS activities.


## Constraints

Only firewalls of the professional edition support **Custom IPS Signature**.

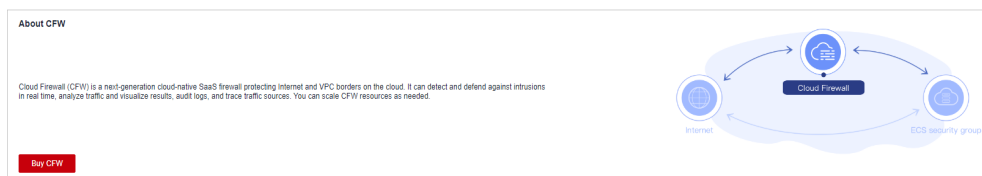
## Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 7-1](#).

**Figure 7-1** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Attack Defense > Intrusion Prevention**.

**Table 7-1** 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, see <a href="#">Basic Protection Rule Management</a>"Basic Protection Rule Management" in <i>Cloud Firewall User Guide</i>.</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> 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>
Custom IPS Signature	<p>If the basic defense rule library does not meet your requirements, you can create custom IPS signatures. Only professional edition firewalls support custom IPS signatures. For details, see <a href="#">Customizing IPS Signatures</a>"Customizing IPS Signatures" in <i>Cloud Firewall User Guide</i>.</p>

Function		Description
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

## Follow-up Operations

After the intrusion prevention policy is configured, you can choose **Security Dashboard** to view the protection details. For details, see [10 Security Dashboard](#).



# 8 Managing Intrusion Prevention

## 8.1 Checking the IPS Rule Library

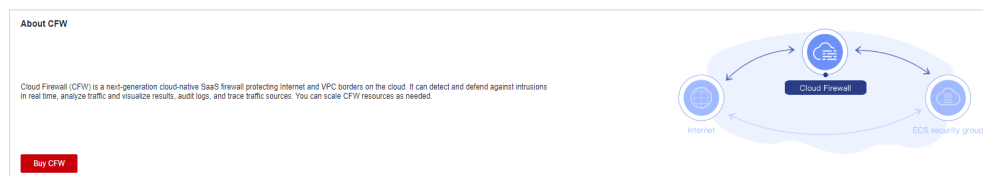
Basic protection cannot be disabled, but can be changed with protection mode. Basic protection functions scan traffic for attacks, threats, and vulnerabilities, such as phishing, Trojans, worms, hacker tools, spyware, password attacks, vulnerability exploits, SQL injection attacks, XSS attacks, and web attacks. They also check for exceptions in protocols, buffer overflow, access control, and suspicious DNS activities.

If the rules in the IPS rule library cannot meet your requirements, you can customize IPS signature rules. For details, see [8.3 Customizing IPS Signatures](#).

### Procedure

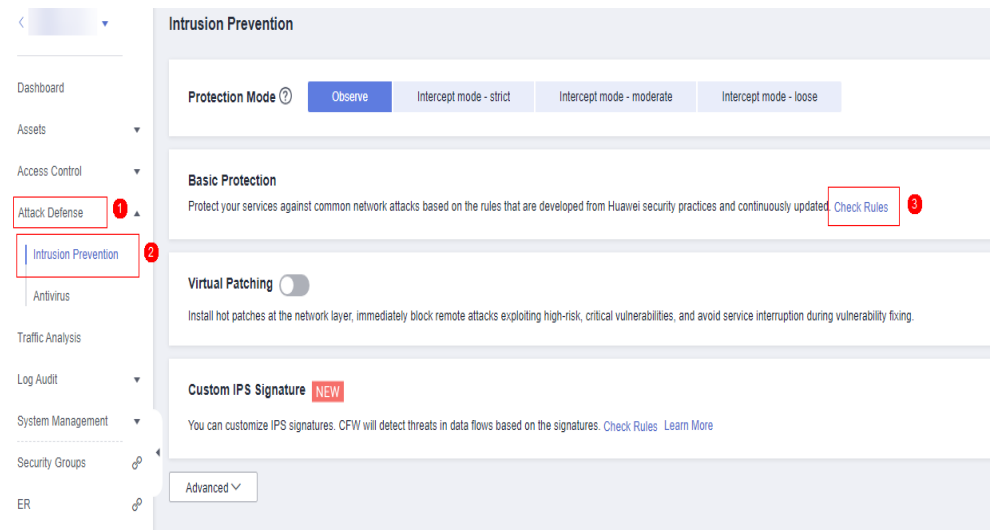
- Step 1** [Log in to the management console](#).
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 8-1](#).

**Figure 8-1** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane, choose **Attack Defense > Intrusion Prevention**. Click **Check Rules** under **Basic Protection**. The **Basic Protection** tab is displayed.

**Figure 8-2** Checking rules



**Step 6** Check basic protection rules. For more information, see [Basic protection rule parameters](#).

**Figure 8-3** Basic protection rules

ID	Name	Updated In	Description	Risk Level	CVE ID	Rule Type	Affected Sof...	Rule Group	Default Action	Current Action	Operation
1005	Apache Subversi...	2016	--	High	CVE-2015-5343	Buffer Overflow	Apache	Strictly	Observe	Observe	Observe Intercep
1005	Linux Kernel SC...	2019	--	Fatal	CVE-2016-9555	Application DDoS	Others	Medium	Observe	Observe	Observe Intercep
1005	Sun Solaris IPv6...	2021	--	High	CVE-2009-0304	Vulnerability Attack	Sun	Observe	Observe	Observe	Observe Intercep
1005	Windows TCP IP...	2021	--	High	CVE-2021-24086	Vulnerability Attack	Others	Strictly	Observe	Observe	Observe Intercep
1040	Philly J ICMP S...	2015	--	Low	--	Trojan	Others	Strictly	Observe	Observe	Observe Intercep
1040	DDoS Win32 Ag...	2015	--	Medium	--	Trojan	Others	Strictly	Observe	Observe	Observe Intercep
1040	PWS Win32Lmi...	2015	--	Medium	--	Trojan	Others	Strictly	Observe	Observe	Observe Intercep
1040	Overfobar.net...	2015	--	Low	--	Trojan	Others	Strictly	Observe	Observe	Observe Intercep
1050	Microsoft DNS S...	2012	--	Fatal	CVE-2011-1966	Suspicious DNS ...	Others	Medium	Observe	Observe	Observe Intercep
1050	Microsoft Windo...	2010	--	Fatal	CVE-2006-3441	Suspicious DNS ...	Microsoft Windows	Medium	Observe	Observe	Observe Intercep

**Table 8-1** Basic protection rule parameters

Parameter	Description
ID	ID of a rule.
Name	Name of a rule.
Updated In	The year when the rule was updated.
Description	Rule description.
Risk Level	Risk level of a rule. It can be <b>Low</b> , <b>Medium</b> , <b>High</b> , or <b>Fatal</b> .
CVE	CVE ID of the rule.
Rule Type	Type of detected attacks, including vulnerability attacks, access control, and hacker tools.

Parameter	Description
Affected Software	Software affected by the attack.
Rule Group	Group that the rule belongs to. Its types are the same as those of <b>Protection Mode</b> , including <b>Observe</b> , <b>strict</b> , <b>moderate</b> , and <b>loose</b> .
Default Action	Default action of the current rule, which is determined by the current protection mode. The action can be observe, intercept, or disable.
Current Action	<p>Operation performed by firewall on the traffic that matches the current rule.</p> <p>If you click <b>Restore All Defaults</b>, the current actions of all the rules in the list will be restored to the default actions.</p> <ul style="list-style-type: none"> <li>• <b>Observe</b>: The firewall logs the traffic that matches the current rule and does not block the traffic.</li> <li>• <b>Intercept</b>: The firewall logs and blocks the traffic that matches the current rule.</li> <li>• <b>Disable</b>: The firewall does not log or block the traffic that matches the current rule.</li> </ul>

**Step 7** (Optional) To view the parameter details of a type of rules, set filter criteria in the input box above the list.

----End

## 8.2 Modifying the Action of a Basic Protection Rule

Basic protection cannot be disabled, but can be changed with protection mode. Basic protection functions scan traffic for attacks, threats, and vulnerabilities, such as phishing, Trojans, worms, hacker tools, spyware, password attacks, vulnerability exploits, SQL injection attacks, XSS attacks, and web attacks. They also check for exceptions in protocols, buffer overflow, access control, and suspicious DNS activities.


### Constraints


- The action of a manually modified rule remains unchanged even if **Protection Mode** is changed.
- The constraints on manually modified actions are as follows:
  - The actions of up to 3000 rules can be manually changed to observation.
  - The actions of up to 3000 rules can be manually changed to interception.
  - The actions of up to 128 rules can be manually changed to disabling.



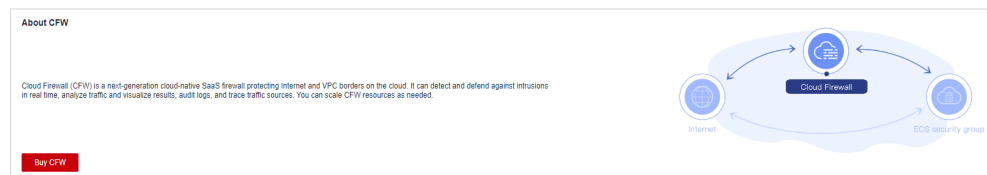
## Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 8-4](#).

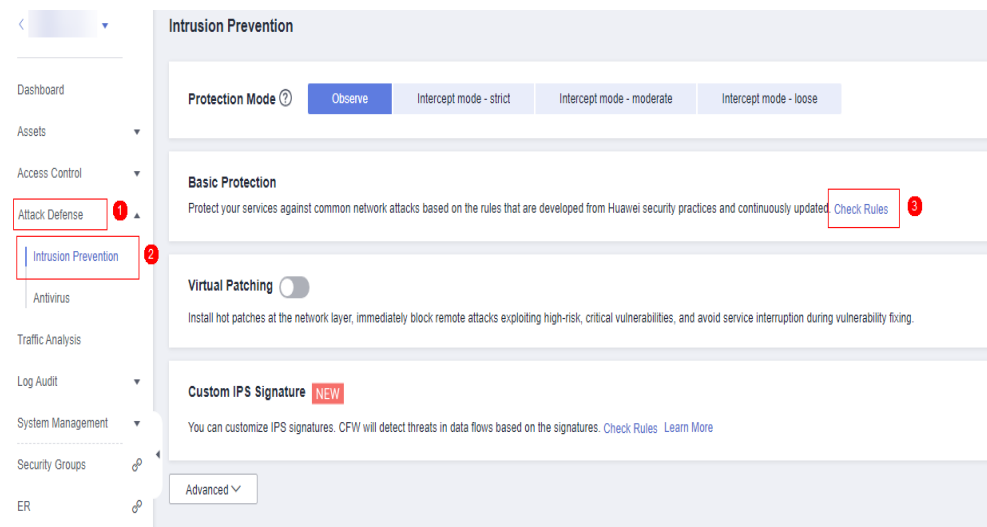
**Figure 8-4** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Attack Defense > Intrusion Prevention**. Click **Check Rules** under **Basic Protection**. The **Basic Protection** tab is displayed.

**Figure 8-5** Checking rules



**Step 6** (Optional) To view the parameter details of a type of rules, set filter criteria in the input box above the list.

**Step 7** Click an action in the **Operation** column.

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

**Figure 8-6** Changing the current action

ID	Name	Updated In	Description	Risk Level	CVE ID	Rule Type	Affected Sof...	Rule Group	Default Action	Current Action	Operation
1050	Microsoft DNS S...	2012	--	Fatal	CVE-2011-1966	Suspicious-DNS...	Others	Medium	Intercept	Intercept	Observe   Intercept   Disable
1050	Microsoft Windo...	2010	--	Fatal	CVE-2006-3441	Suspicious-DNS...	Microsoft Windows	Medium	Intercept	Intercept	Observe   Intercept   Disable
1050	Microsoft Windo...	2010	--	Fatal	CVE-2006-3441	Suspicious-DNS...	Microsoft Windows	Medium	Intercept	Intercept	Observe   Intercept   Disable

**NOTE**

- The action of a manually modified rule remains unchanged even if **Protection Mode** is changed. To restore the default action, select a rule and click **Restore Default**.
- The constraints on manually modified actions are as follows:
  - The actions of up to 3000 rules can be manually changed to observation.
  - The actions of up to 3000 rules can be manually changed to interception.
  - The actions of up to 128 rules can be manually changed to disabling.

----End

### 8.3 Customizing IPS Signatures

You can configure network detection signature rules in CFW. CFW will detect threats in data traffic based on signatures.


HTTP, TCP, UDP, POP3, SMTP and FTP protocols can be configured in user-defined IPS signatures.


#### Constraints

- Only the professional edition supports custom IPS signatures.
- A maximum of 500 features can be added.
- Custom IPS signatures are not affected by the change of the basic protection mode.
- **Content** can be set to **URI** only if **Direction** is set to **Client to server** and **Protocol Type** is set to **HTTP**.

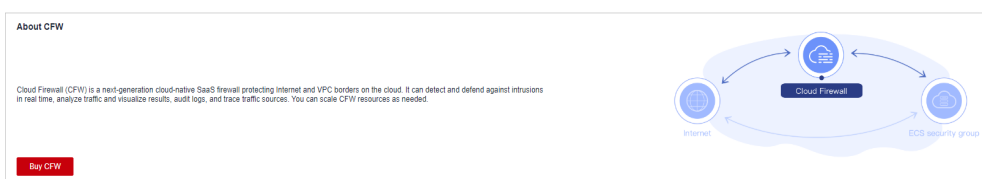
#### Procedure

**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.

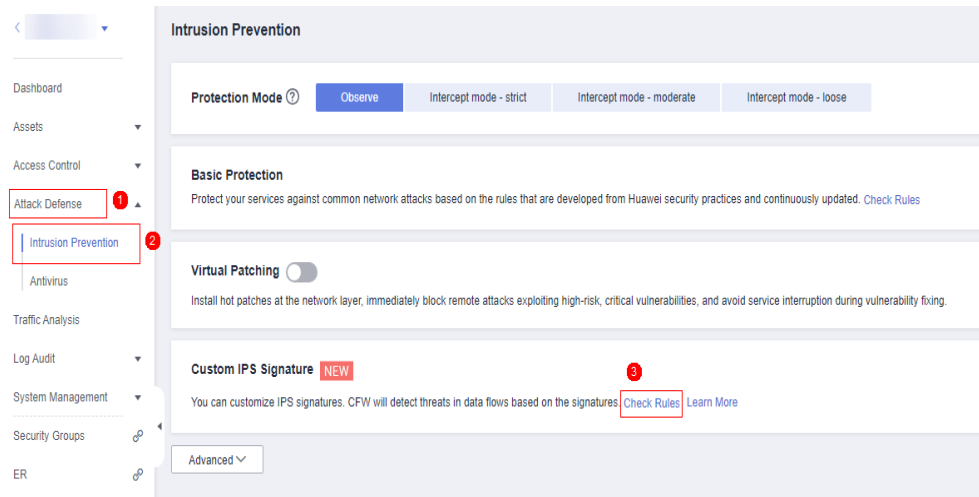
**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 8-7**.

**Figure 8-7** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane, choose **Attack Defense > Intrusion Prevention**. Click **Check Rules** in the **Custom IPS Signature** area.

**Figure 8-8** Custom IPS signature



- Step 6** Click **Add Custom IPS Signature** in the upper right corner of the list. For more information, see [Table 8-2](#).

**Table 8-2** Custom IPS signature parameters

Parameter Name	Description
Name	Feature name. It must meet the following requirements: <ul style="list-style-type: none"> <li>Only uppercase letters (A to Z), lowercase letters (a to z), numbers (0 to 9), and the following special characters are allowed: -_</li> <li>A maximum of 255 characters are allowed.</li> </ul>
Risk Level	Risk level of the feature.
Rule Type	Rule type of the feature.
Affected Software	Affected software.
OS	OS.
Direction	Direction of the traffic matching the feature. Its value can be: <ul style="list-style-type: none"> <li><b>Any</b></li> <li>Server to client</li> <li>Client to server</li> </ul>

Parameter Name	Description
Protocol Type	Protocol type of the feature.
Source Type	Source port type. Its value can be: <ul style="list-style-type: none"> <li>• <b>Any</b></li> <li>• <b>Include</b></li> <li>• <b>Exclude</b></li> </ul> <b>NOTE</b> You are advised to select <b>Any</b> .
Source Port	Set <b>Source Port</b> if <b>Source Type</b> is set to <b>Include</b> or <b>Exclude</b> . <ul style="list-style-type: none"> <li>• You can set one or more ports. Use commas (,) to separate multiple ports. Example: <b>80,100</b></li> <li>• You can also set a port range. Use hyphens (-) to separate ports, for example, 80-443.</li> </ul>
Destination Type	Destination port type. Its value can be: <ul style="list-style-type: none"> <li>• <b>Any</b></li> <li>• <b>Include</b></li> <li>• <b>Exclude</b></li> </ul> <b>NOTE</b> You are advised to select <b>Any</b> .
Destination Port	Set <b>Destination Port</b> if <b>Destination Type</b> is set to <b>Include</b> or <b>Exclude</b> . <ul style="list-style-type: none"> <li>• You can set one or more ports. Use commas (,) to separate multiple ports. Example: <b>80,100</b></li> <li>• You can also set a port range. Use hyphens (-) to separate ports, for example, 80-443.</li> </ul>
Action	Action taken by the firewall when it detects traffic with the feature. <ul style="list-style-type: none"> <li>• <b>Observe</b>: Attacks are detected and recorded in logs. For details about how to query logs, see <a href="#">12.1 Querying Logs</a>.</li> <li>• <b>Intercept</b>: Attacks are automatically blocked.</li> </ul> <b>NOTE</b> Before you enable the <b>Intercept</b> mode, you are advised to select <b>Observe</b> first and check whether the attack logs are correct for a period of time.

Parameter Name	Description
Content	<p>Content matching the feature rule.</p> <ul style="list-style-type: none"> <li>● <b>Content:</b> content field that matches the feature, for example, <b>cfw</b>.</li> <li>● <b>Content Option:</b> Select a rule for content matching. <ul style="list-style-type: none"> <li>– <b>Hexadecimal:</b> The content must be in hexadecimal format. Example: 0x1F</li> <li>– <b>Case insensitive:</b> Match content without checking cases.</li> <li>– <b>URL:</b> Match the fields that are consistent with the content in URLs.</li> </ul> </li> <li>● <b>Relative Position</b> specifies the start position in a feature matching. <ul style="list-style-type: none"> <li>– <b>Head:</b> The start position depends on the <b>Offset</b> from the head. For example, if <b>Offset</b> is <b>10</b>, the content check starts from the eleventh bit.</li> <li>– <b>After previous content:</b> Packet capture starts from the specified position. Formula: Start position = Length of the previous <b>Content</b> field + Previous <b>Offset</b> + <b>Offset</b> + 1 For example, if the previous content is <b>test</b>, the previous <b>offset</b> is 10, and the current offset is 5, the start position is the 20th (4+10+5+1) bit.</li> </ul> </li> <li>● <b>Offset</b> specifies the start position of feature matching. For example, if the offset is 10, the start position is the eleventh bit.</li> <li>● <b>Depth</b> specifies the end position of feature matching. For example, if the depth is 65,535, the end position is the 65,535th bit.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>● <b>Depth</b> must be greater than the length of the <b>Content</b> field.</li> <li>● Up to four items can be added to an IPS signature.</li> </ul>

**Step 7** Click **OK**.

----End

## Related Operations

- To copy an IPS feature, click **Copy** in the **Operation** column, modify parameters, and click **OK**.
- To modify an IPS signature, click **Edit** in the **Operation** column.
- To delete IPS signatures in batches, select signatures and click **Delete** above the list.

- To modify actions in batches, select signatures and click **Observe** or **Intercept** above the list.

# 9 Managing the Antivirus Function

The anti-virus function identifies and processes virus files through virus feature detection to prevent data damage, permission change, and system breakdown caused by virus files.


The antivirus function can check access via HTTP, SMTP, POP3, FTP, IMAP4, and SMB.


## Specification Limitations

- Antivirus is available only in the professional edition.

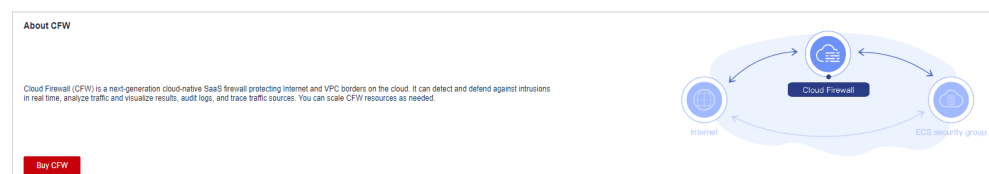
## Enabling Antivirus

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 9-1](#).

**Figure 9-1** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Attack Defense > Antivirus**.

**Step 6** Click  to enable antivirus.


 NOTE


After antivirus is enabled, **Current Action** is **Disable** by default. For details about how to change the defense action, see [Changing a Defense Action](#).

----End

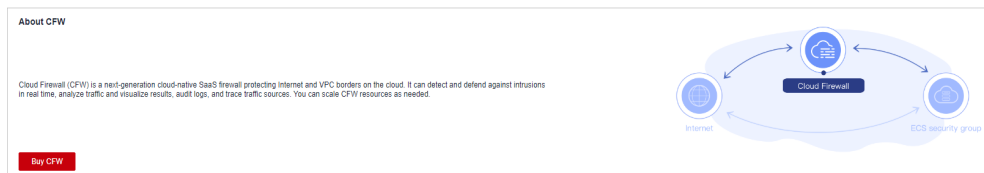
## Changing a Defense Action

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 9-2](#).

**Figure 9-2** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Attack Defense > Antivirus**.

**Step 6** Click an action in the **Operation** column of a rule.

- **Observe:** The firewall checks the traffic of a protocol. If attack traffic is detected, the firewall records it in **attack event logs** but does not block it.
- **Block:** The firewall checks the traffic of a protocol. If attack traffic is detected, the firewall records it in **attack event logs** and blocks it.
- **Disable:** The firewall does not perform virus checks on the traffic of a protocol.

----End





# 10 Security Dashboard

You can easily check IPS defense information on the security dashboard and adjust defense policies in a timely manner.

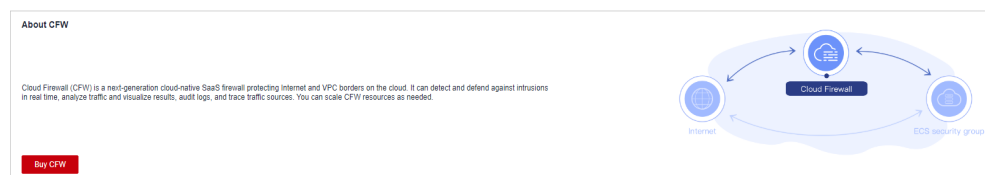
## Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 10-1](#).

**Figure 10-1** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Attack Defense > Security Dashboard**.

**Step 6** In the upper part of the page, click the **Internet Boundaries** or **Inter-VPC Borders** tab.

**Step 7** View statistics about protection rules of a firewall instance. You can select a query duration from the drop-down list.

- **Security Dashboard:** Number of attacks detected by IPS, numbers of allowed and blocked accesses, and number of attacked ports.
- **Attacks:** Number of times that IPS blocks or allows traffic.
- **Visualizations:** Top 5 items ranked by certain parameters regarding the attacks detected or blocked by IPS. For more information, see [Table 10-1](#). You

can click a record to view attack details. For more information, see [Table 12-1](#).

**Table 10-1** Security dashboard statistics parameters

Parameter	Description
Attack Types	Attack type.
Top Internal Attack Source IP Addresses	IP addresses of the assets that are on your cloud but launch attacks on external IP addresses.
Top External Attack Source IP Addresses	External IP addresses that launch attacks on your cloud assets.
Top External Attack Source Regions	Regions of the external IP addresses that launch attacks on your cloud assets.
Top Attack Destination IP Addresses	Destination IP addresses in attacks.
Top Attacked Ports	Attacked ports.

- Top attack statistics: Top 50 attacks detected or blocked by IPS within a specified time range.
  - **Top Attack Targets:** Destination IP addresses, ports, and applications.
  - **Top Attack Sources:** Source IP addresses and types.

----End

# 11 Traffic Analysis



## 11.1 Viewing Inbound Traffic

The **Inbound Traffic** page displays the protected traffic from the Internet to EIPs on the cloud. CFW collects traffic statistics based on sessions. Traffic data is reported when the connection is terminated.

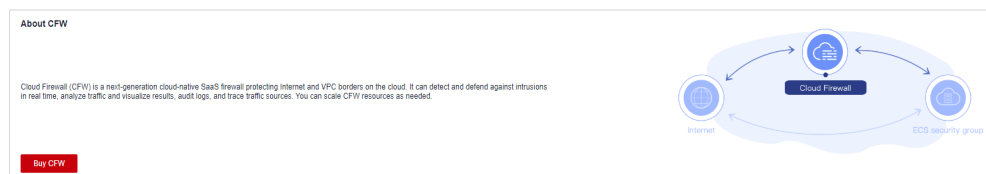
### Prerequisites

EIP protection has been enabled. For details, see [4.1 Enabling EIP Protection](#).

### 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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 11-1](#).

**Figure 11-1** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane, choose **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 11-1](#). Click a record to view the traffic details.

**Table 11-1** 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

## 11.2 Viewing Outbound Traffic


The **Outbound Traffic** page displays the protected traffic from EIPs on the cloud to the Internet. CFW collects traffic statistics based on sessions. Traffic data is reported when the connection is terminated.


### Prerequisites

EIP protection has been enabled. For details, see [4.1 Enabling EIP Protection](#).

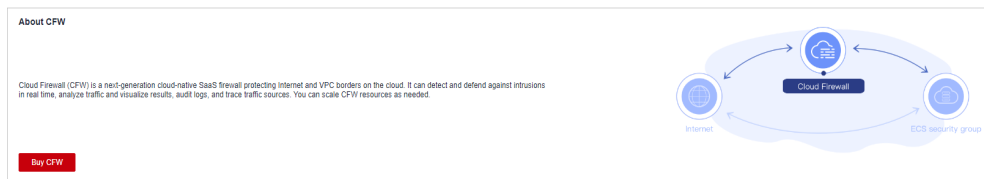
### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 11-2](#).

**Figure 11-2** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane, choose **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 11-2](#). Click a record to view the traffic details.

**Table 11-2** 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

## 11.3 Viewing Inter-VPC Traffic


The **Inter-VPC Access** page displays the traffic between the protected VPCs.


### Prerequisites

- EIP protection has been enabled. For details, see [4.1 Enabling EIP Protection](#).
- The VPC border firewall has been configured and enabled. For details, see [5 Managing VPC Border Firewalls](#).

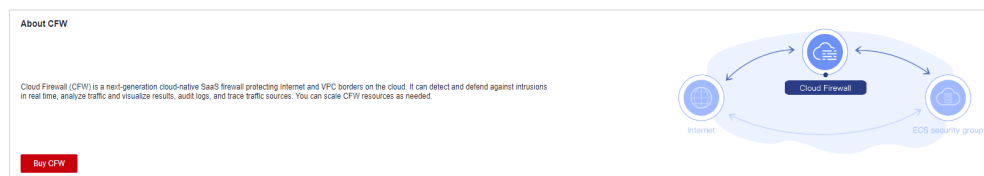
### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 11-3](#).

**Figure 11-3** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Traffic Analysis > Inter-VPC Access**.

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

- **Traffic Dashboard:** Information about the maximum traffic between VPCs.
- **Inter-VPC Access:** Request and response traffic between VPCs.
- **Visualizations:** Top 5 items ranked by certain parameters regarding inter-VPC traffic within a specified time range. For more information, see [Table 11-3](#). Click a record to view the traffic details.

**Table 11-3** Inter-VPC traffic parameters

Parameter	Description
Top Access Source IP Addresses	Source IP address of inter-VPC traffic.

Parameter	Description
Top Destination IP Addresses	Destination IP addresses of inter-VPC traffic.
Top Open Ports	Destination port of inter-VPC traffic.
Application Distribution	Application information about inter-VPC traffic.

- Private IP Address Accesses: Top 50 private IP addresses with the highest traffic within a specified period.

----End

# 12 Auditing Logs

## 12.1 Querying Logs

CFW allows you to query logs generated within the last seven days. The following types of logs are available:

- 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. For details, see [8.2 Modifying the Action of a Basic Protection Rule](#).
- Access control log: all traffic that matches the access control policy. For details about how to modify the protection rule, see [6.9.2 Editing a Protection Rule](#).
- Traffic log: all traffic passing through the firewall.

### NOTE

- On the **Log Query** page, you can check and export log data of the last seven days. For details, see [12.1 Querying Logs](#).
- If logs are recorded in LTS, you can view log data in the past 1 to 365 days. For details, see [12.2 Log Management](#).

### Prerequisites


- You have performed operations in [4.1 Enabling EIP Protection](#).
- You have enabled [basic intrusion prevention](#).

### Constraints


- Logs can be stored for up to seven days.
- Up to 100,000 records can be exported for a single log.

### Attack Event Logs

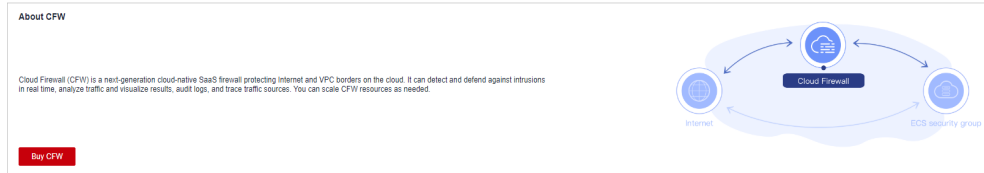
**Step 1** [Log in to the management console](#).

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



**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 12-1**.

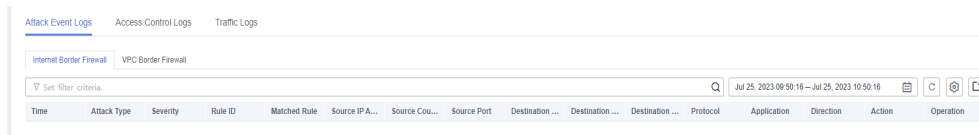
**Figure 12-1** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Log Audit > Log Query**. The **Attack Event Logs** tab page is displayed. You can view details about attack events in the past week.

**Figure 12-2** Attack event logs



**Table 12-1** 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, High, Medium, or Low</b> .
Rule ID	Rule ID
Matched Rule	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.


Parameter	Description
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	Action taken on an event. It can be <b>Observe</b> , <b>Block</b> , or <b>Allow</b> .
Operation	You can click <b>Details</b> to view the basic information and attack payload of an event.

----End

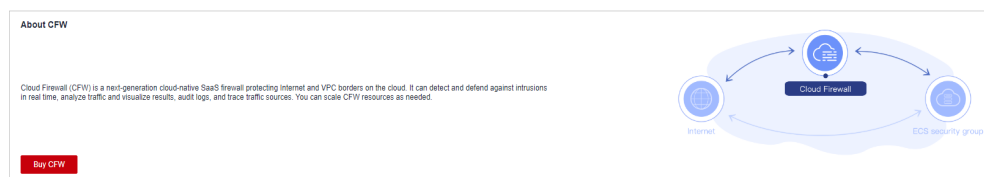
## Access Control Logs

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 12-3](#).

**Figure 12-3** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Log Audit > Log Query**. Click the **Access Control Logs** tab and check the traffic details in the past week. For details about how to modify the response action of an IP address, see [6.1 Adding a Protection Rule](#) or [6.4.1 Adding an Item to the Blacklist or Whitelist](#).

**Figure 12-4** Access control logs

Received	Source	Source Country/Region	Source Port	Destination IP Address	Destination Country/Region	Destination URL	Destination Port	Protocol	Action	Rule
Jul 25, 2023 11:02:04...		--	58565		--	--	2408	TCP	Allow	whitelist
Jul 25, 2023 11:00:55...		--	37485		--	--	2408	TCP	Allow	whitelist
Jul 25, 2023 10:58:48...		--	44668		--	--	2408	TCP	Allow	whitelist


**Table 12-2** Access control log parameters


Parameter	Description
Received	Time of an access.
Source	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 Address	Destination IP address.
Destination Country/Region	Geographical location of the destination IP address.
Destination URL	Destination domain name.
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.
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

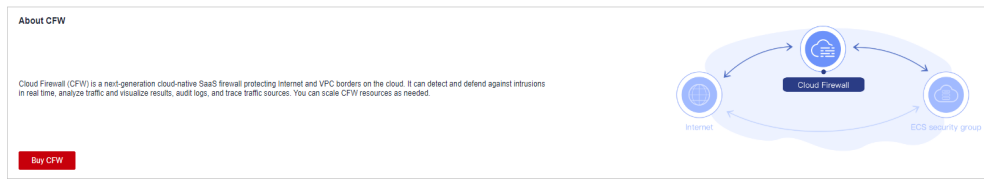
## Traffic Logs

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 12-5](#).

**Figure 12-5** CFW Dashboard



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

**Step 5** In the navigation pane, choose **Log Audit > Log Query**. Click the **Traffic Log** tab to view the number of traffic bytes and packets in the past week.

**Figure 12-6** Traffic logs

Start Time	End Time	Source	Source Country/Region	Source Port	Destination IP Address	Destination Country/Region	Destination Port	Protocol	Stream Size	Stream Packets
Jul 25, 2023 11:24:27	Jul 25, 2023 11:24:49		--	43505		--	2408	TCP	0.578 Kb	1
Jul 25, 2023 11:22:18	Jul 25, 2023 11:22:40		--	50652		--	2408	TCP	1.156 Kb	2
Jul 25, 2023 11:20:10	Jul 25, 2023 11:20:32		--	57799		--	2408	TCP	1.156 Kb	2
Jul 25, 2023 11:18:02	Jul 25, 2023 11:18:24		--	36729		--	2408	TCP	1.156 Kb	2

**Table 12-3** Traffic log parameters

Parameter	Description
Start Time	Time when traffic protection started.
End Time	Time when traffic protection ended.
Source	Source IP address of the traffic
Source Country/Region	Geographical location of the access source IP address.
Source Port	Source port of the traffic.
Destination IP Address	Destination IP address.
Destination Country/Region	Geographical location of the destination IP address.
Destination Port	Destination port of the traffic.
Protocol	Protocol type of the traffic.
Stream Size	Total number of bytes of protected traffic.
Stream Packets	Total number of protected packets.

----End

## 12.2 Log Management

### 12.2.1 Log Settings

You can record attack event logs, access control logs, and traffic logs to Log Tank Service (LTS) and use these logs to quickly and efficiently perform real-time decision analysis, device O&M, and service trend analysis.


LTS analyzes and processes a large number of logs. It enables you to process logs in real-time, efficiently, and securely.


#### NOTICE

- On the **Log Query** page, you can check and export log data of the last seven days. For details, see [12.1 Querying Logs](#).
- If logs are recorded in LTS, you can view log data in the past 1 to 365 days. For details, see [12.2 Log Management](#).
- LTS is billed by traffic and is billed separately from WAF. For details about LTS pricing, see [LTS Pricing](#).

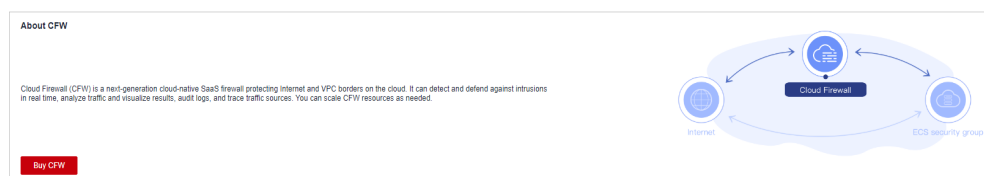
### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 12-7](#).

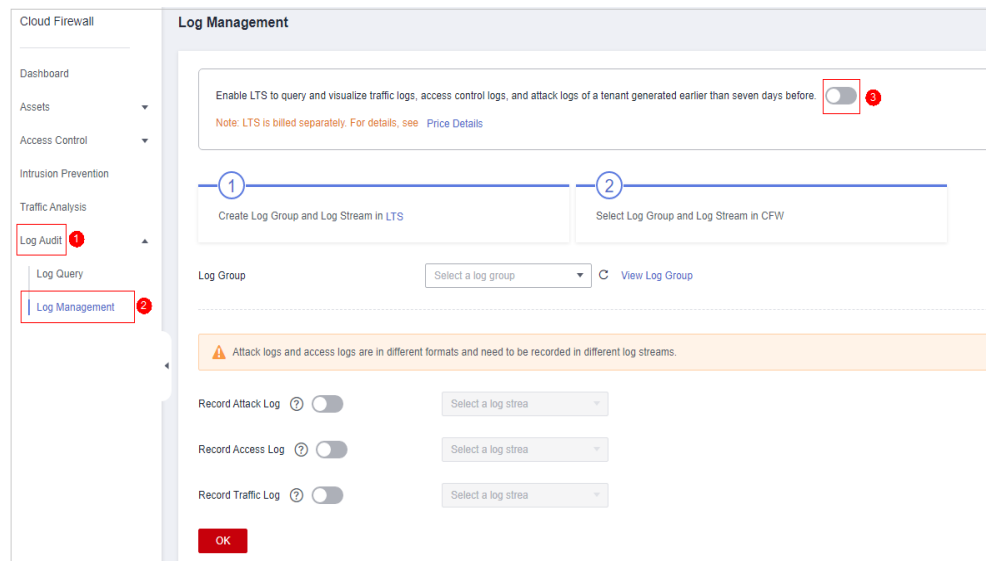
**Figure 12-7** CFW Dashboard



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

**Step 5** In the navigation pane on the left, choose **Log Audit > Log Management**. The Log Management page is displayed. Click  to enable interconnection with LTS.

**Figure 12-8** Enabling log management



**Step 6** Create log groups and log streams. For details, see [Creating Log Groups and Log Streams](#).

**NOTE**

To make it easier for you to view, you are advised to:

- Add **-cfw** as the suffix when creating a log group.
- When creating log streams, add the suffixes **-attack**, **-access**, and **-flow** to attack event logs, access control logs, and traffic logs.

**Step 7** Select a created log group or log stream. Click **OK**.

**NOTE**

- The formats of attack logs, access logs, and traffic logs are different. You need to configure different log streams for them.
- Attack logs: record attack alarm information, including the attack event type, protection rule, protection action, quintuple, and attack payload.

Access logs: record information about the traffic that matches the ACL policy, including the matching time, quintuple, response action, and the matched access control rule.

Traffic logs: record information about all traffic passing through the CFW, including the start time, end time, quintuple, number of bytes, and number of packets.

----End

## 12.2.2 Changing the Log Storage Duration


Logs are stored for seven days by default. The storage duration can be set to 1 to 365 days. Logs that exceed the storage duration will be automatically deleted. For log data that needs to be stored for a long time (log persistence), LTS can dump the logs to OBS for medium- and long-term storage.


### Prerequisites

Logs have been dumped to LTS by configuring [12.2.1 Log Settings](#).

## 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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 12-9](#).

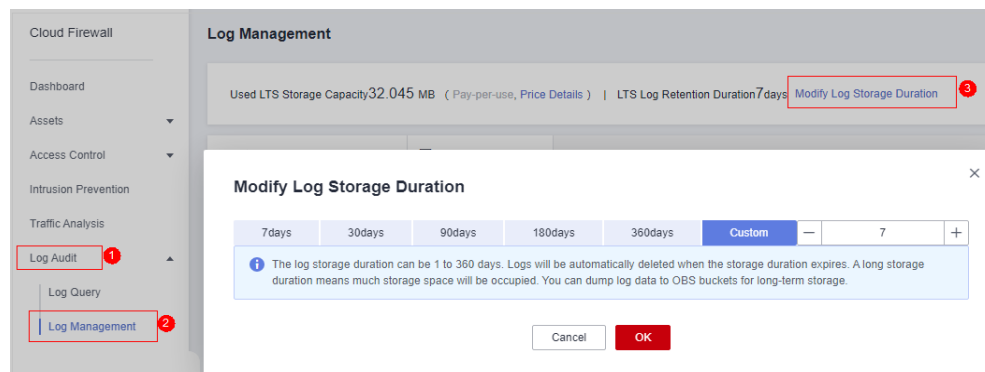
**Figure 12-9** CFW Dashboard



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

**Step 5** In the navigation pane on the left, choose **Log Audit > Log Management**. On the displayed page, click **Modify Log Storage Duration**.

**Figure 12-10** Modifying log storage duration



### NOTE

- Logs can be stored for 1 to 365 days. Logs that exceed the specified storage duration are automatically deleted.
- The longer the storage duration, the larger the occupied storage. For details about how to dump logs to other cloud services for long-term storage, see [Log Transfer Overview](#).

----End

## 12.2.3 Adding Alarm Notifications


You can create alarm rules to monitor logs in real time. When a log meets the preset rules, an alarm is generated and sent to you by SMS message or email. This function can be used to monitor exceptions in real time.


## Prerequisites

Logs have been dumped to LTS by configuring [12.2.1 Log Settings](#).

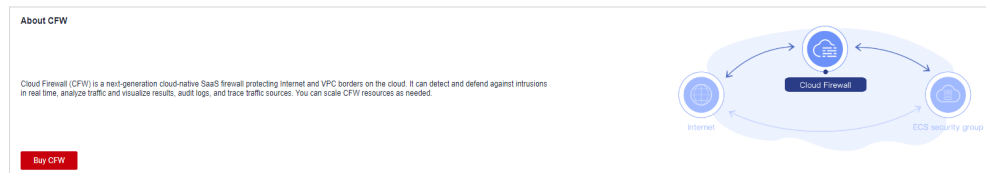
## Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 12-11](#).

**Figure 12-11** CFW Dashboard



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

**Step 5** In the navigation pane on the left, choose **Log Audit > Log Management**.

Click **Create Alarm Rule** in the upper right corner. [Creating an alarm rule](#) describes the parameters for creating an alarm rule.



Figure 12-12 Creating an alarm rule

### Create Alarm Rule ?

★ Rule Name

Description

★ Statistics By keyword By SQL

★ Log Group Name  C

★ Enterprise Project Name  View Enterprise Projects

★ Log Stream Name  C

★ Keywords  Examples

Query Time Range

---

**Trigger**

★ Query Frequency

★ Matching Log Events ?

---

**Advanced Settings**

★ Alarm Severity

★ Send Notifications No Yes

★ SMN Topic  C create a new topic

please go to the SMN page. Ensure the topic has been authorized on the SMN page, and APM is selected so services can publish messages. Otherwise, threshold notifications will not be sent. For further details, please [Configuring Topic Policies](#).

★ Timezone/Language C

Timezone/Language is user preference configuration, you can go to user center [Modify](#)

**Table 12-4** Parameters for creating an alarm rule

Parameter	Description	Example Value
Rule Name	Name of the alarm rule. <b>NOTE</b> Can contain only letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot start with a period or underscore, or end with a period. Can contain 1 to 64 characters.	test
Description	Rule description. <b>NOTE</b> Enter up to 64 characters.	-
Statistics	Possible values are <b>By keyword</b> and <b>By SQL</b> .	<b>By keyword</b>
Log Group Name	Select a log group.	-
Enterprise Project Name	Select an enterprise project. This parameter is displayed only when the enterprise project function is enabled for the current account.	-
Log Stream Name	Select a log stream.	-
Keywords	Enter keywords that you want LTS to monitor in logs. <b>NOTE</b> <ul style="list-style-type: none"> <li>Keywords cannot start with an asterisk (*) or question mark (?).</li> <li>Exact and fuzzy matches are supported. A keyword is case sensitive and contains up to 1024 characters.</li> </ul>	_time
Query Time Range	Time range for the keyword query, which is one period earlier than the current time. <ul style="list-style-type: none"> <li>The value ranges from 1 to 60 in the unit of minutes.</li> <li>The value ranges from 1 to 24 in the unit of hours.</li> </ul>	1 h
Query Frequency	Sets the query frequency.	<b>Hourly</b>
Matching Log Events	When the number of log events that contain the configured keywords reaches the specified value, an alarm is triggered.	>10

Parameter	Description	Example Value
Alarm Severity	Possible values are <b>critical</b> (default), <b>major</b> , <b>minor</b> , and <b>info</b> .	<b>critical</b>
Send Notifications	Possible values are <b>No</b> (default) and <b>Yes</b> .	<b>No</b>
SMN Topic	If you select <b>Yes</b> for <b>Send Notifications</b> , you need to select a Simple Message Notification (SMN) topic, time zone, language, and message template. You can select multiple topics.	-

**Step 6** Confirm the information and click **OK**.

----End

## 12.2.4 Log Structuring

Log data can be structured or unstructured. Structured data is quantitative data or can be defined by unified data models. It has a fixed length and format. Unstructured data has no pre-defined data models and cannot be fit into two-dimensional tables of databases.


During log structuring, logs with fixed or similar formats are extracted from a log stream based on your defined structuring method and irrelevant logs are filtered out. You can then use SQL syntax to query and analyze the structured logs.


### Prerequisites

Logs have been dumped to LTS by configuring [12.2.1 Log Settings](#).

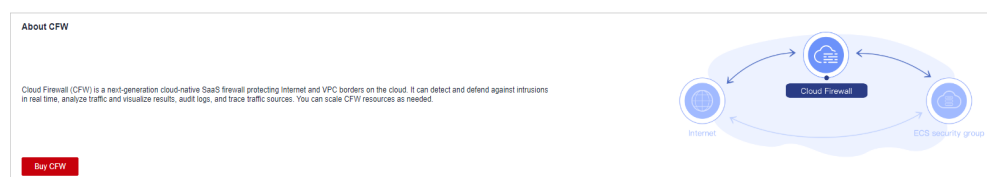
### Procedure

**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.

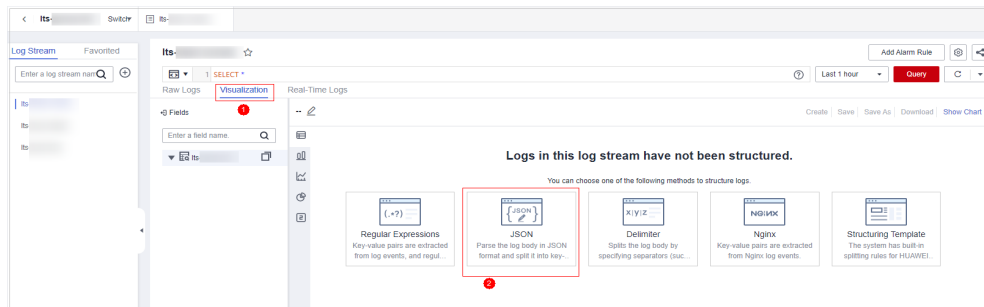
**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 12-13](#).

**Figure 12-13** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane on the left, choose **Log Audit > Log Management**. Select the target log group and log stream.
- Step 6** Click the **Visualization** tab and select **JSON**.

**Figure 12-14** Log structuring



**Step 7** Extract log fields.

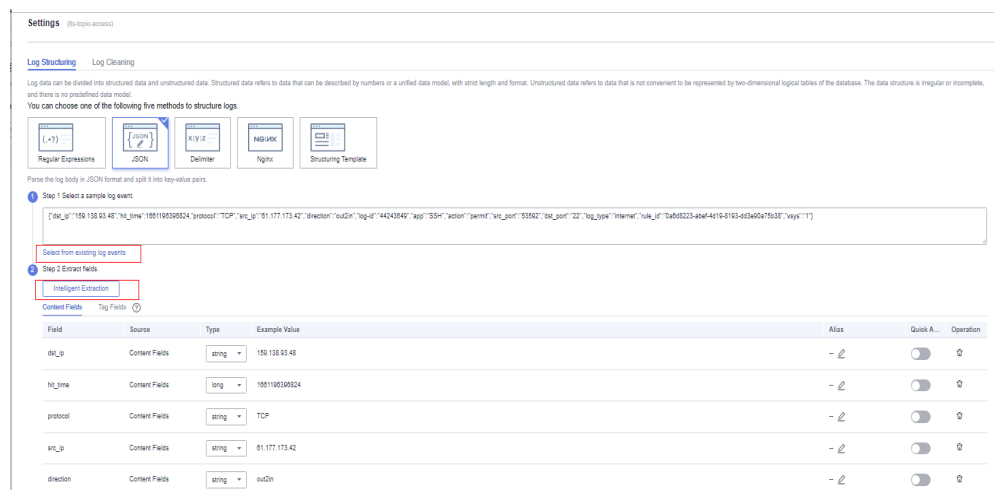
1. Click **Step 1 Select a sample log event**, select a log event, or enter a log event in the text box, and click **OK**.

**NOTE**

Select a typical log.

2. Click **Intelligent Extraction** in **Step 2 Extract fields** to extract the log fields.

**Figure 12-15** Obtaining log fields



**NOTE**

- The **float** data type has seven digit precision.
- To have higher accuracy, you are advised to change the field type to **String** when the accuracy exceeds seven digits.

**Step 8** Click **Save**. The type of extracted fields cannot be changed after the structuring is complete.

----End

## 12.2.5 Visualization


Visualization allows you to query and analyze structured log fields using SQL statements. After log structuring, wait about 1–2 minutes for SQL query and analysis.


### Prerequisites

- Logs have been dumped to LTS by configuring [12.2.1 Log Settings](#).
- Log structuring has been completed. For details, see [12.2.4 Log Structuring](#).

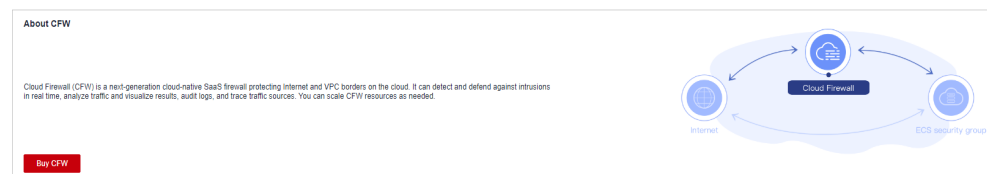
### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 12-16](#).

**Figure 12-16** CFW Dashboard



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

**Step 5** In the navigation pane on the left, choose **Log Audit > Log Management**. Select the target log group and log stream.

**Step 6** Click the **Visualization** tab and select the chart type you want to use to display your query results.

Currently, five chart types are supported, as described in [Chart parameters](#).

**Table 12-5** Chart parameters

Chart Type	Description
Table Chart	<ul style="list-style-type: none"> <li>● <b>Records per Page:</b> number of log events displayed per page. The value can be 10 (default), 20, 30, or 50.</li> <li>● <b>Filtering:</b> After the filtering function is enabled, you can filter results the right of the table header. Currently, only single-column search is supported.</li> <li>● <b>Sorting:</b> After the sorting function is enabled, you can select the ascending or descending order on the table header.</li> </ul>
Bar Chart	<ul style="list-style-type: none"> <li>● <b>X Axis:</b> Select a field from the drop-down list box as the X axis. Digits and strings are supported.</li> <li>● <b>Y Axis:</b> Select a field from the drop-down list box as the Y axis. Only numeric data is supported.</li> <li>● <b>X Axis Title and Y Axis Title:</b> Set the titles for the X axis and Y axis.</li> <li>● <b>Y Axis Range:</b> Set the minimum and maximum values for the Y axis.</li> <li>● <b>Max Shown Categories:</b> The value can be 20, 40, 50 (default), 80, and 100.</li> <li>● <b>Show Labels:</b> Set this parameter based on your requirements.</li> <li>● <b>Stacked:</b> Set this parameter based on your requirements. If you enable it, labels cannot be shown.</li> </ul>
Line Chart	<ul style="list-style-type: none"> <li>● <b>X Axis:</b> Select a field from the drop-down list box as the X axis. The value can be a number or a string.</li> <li>● <b>Y Axis:</b> Select a field from the drop-down list box as the Y axis. Only numeric data is supported.</li> <li>● <b>X Axis Title and Y Axis Title:</b> Set the titles for the X axis and Y axis.</li> <li>● <b>Y Axis Range:</b> Set the minimum and maximum values for the Y axis.</li> <li>● <b>Line:</b> Select <b>Curved</b> or <b>Straight</b>.</li> <li>● <b>Show Data Markers:</b> Set this parameter based on your requirements.</li> </ul>

Chart Type	Description
Pie Chart	<ul style="list-style-type: none"> <li>● <b>Category:</b> Select a field from the drop-down list box as the category. Only strings are supported.</li> <li>● <b>Value:</b> Select a field from the drop-down list box. Only numeric data is supported.</li> <li>● <b>Label Position:</b> Select <b>Inside</b> or <b>Outside</b>. This parameter can be set only after you enable <b>Show Labels</b>.</li> <li>● <b>Shown Categories:</b> The value can be 5, 10 (default), 20, 30, or 40. For example, if there are 20 categories and you only want to show 10, the first 10 categories will be represented by 10 slices, and the rest are grouped as one slice labeled as <b>Others</b>.</li> <li>● <b>Coxcomb Chart:</b> In a coxcomb chart, the radius of pie slices differs depending on the percentage of the data that the slices represent.</li> <li>● <b>Show Labels:</b> Set this parameter based on your requirements.</li> </ul>
Number Chart	<ul style="list-style-type: none"> <li>● <b>Data Column:</b> Select a field as the data source. Numeric data is recommended. After you select a field, the first data in the field column is displayed in the chart.</li> <li>● <b>Add Comparison Data:</b> Set this parameter based on your requirements.</li> <li>● <b>Comparison Data:</b> Select a field as the source of the comparison data. Numeric data is recommended. After you select the absolute value of the comparison data, the difference between the absolute value and the values in the selected data column is displayed in the chart. Comparison data can be used only after the comparison value is set.</li> <li>● <b>Description:</b> You can add a description for numbers.</li> <li>● <b>Data Unit</b> and <b>Comparison Data Unit:</b> Set the units based on your requirements.</li> <li>● <b>Advanced Settings:</b> You can set <b>Number Format</b>, <b>Data Text Size</b>, <b>Comparison Data Text Size</b>, and <b>Unit Text Size</b>.</li> </ul>

----End



## 12.2.6 Quick Analysis

Quick analysis helps you collect and query log data. You can view statistics on logs by searching for specified fields.

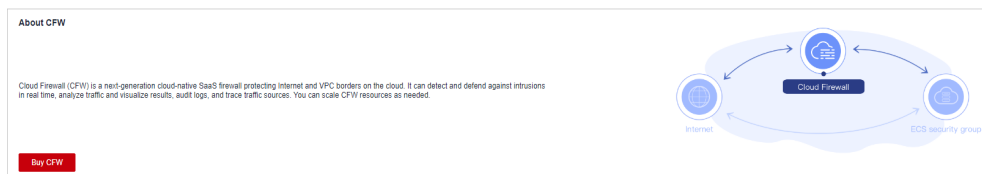
### Prerequisites


Logs have been dumped to LTS by configuring [12.2.1 Log Settings](#).

## Procedure

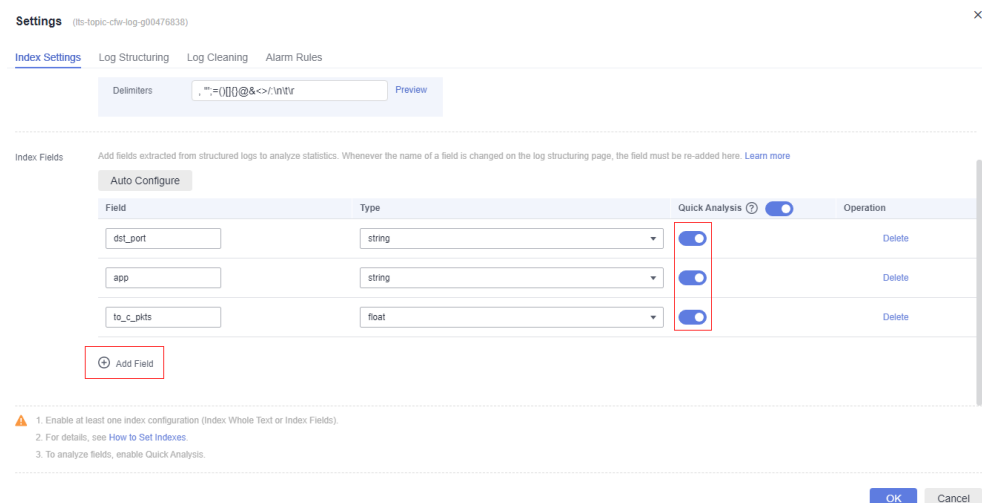
- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner of the management console and select a region or project.
- Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 12-17](#).

**Figure 12-17** CFW Dashboard



- Step 4** (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.
- Step 5** In the navigation pane on the left, choose **Log Audit > Log Management**. Select the target log group and log stream.
- Step 6** Click  in the upper right corner of the page. On the **Index Settings** tab of the **Settings** page, add fields and enable quick analysis.

**Figure 12-18** Setting quick analysis



- Step 7** Click **OK**. The quick analysis task is created.

----End



## 12.2.7 Log Field Description

### Attack Event Logs

Field	Type	Description
src_ip	string	Source IP address
src_port	string	Source port number
dst_ip	string	Destination IP address
dst_port	string	Destination port number
protocol	string	Protocol type
app	string	Application type
src_region_name	string	Source region name
src_region_id	string	Source region ID
dst_region_name	string	Destination region name
dst_region_id	string	Destination region ID
log_type	string	Log type. <ul style="list-style-type: none"> <li>● <b>internet</b>: Internet border traffic log</li> <li>● <b>nat</b>: NAT border traffic log</li> <li>● <b>vpc</b>: inter-VPC traffic log</li> </ul>
vsys	long	Firewall protection direction. <ul style="list-style-type: none"> <li>● <b>1</b>: north-south</li> <li>● <b>2</b>: east-west</li> </ul>
direction	string	Traffic direction. <ul style="list-style-type: none"> <li>● <b>out2in</b>: inbound</li> <li>● <b>in2out</b>: outbound</li> </ul>
action	string	Response action of the firewall. <ul style="list-style-type: none"> <li>● <b>permit</b></li> <li>● <b>deny</b></li> </ul>
packet	string	Original data packet of the attack log. <b>NOTE</b> The encoding format is Base64.
attack_rule	string	Defense rule that works for the detected attack
attack_rule_id	string	ID of the defense rule that works for the detected attack

Field	Type	Description
attack_type	string	Type of the attack. <ul style="list-style-type: none"> <li>• Vulnerability exploit</li> <li>• Vulnerability scan</li> <li>• Trojan</li> <li>• Worms</li> <li>• Phishing</li> <li>• Web attacks</li> <li>• Application DDoS</li> <li>• Buffer overflow</li> <li>• Password attacks</li> <li>• Mail</li> <li>• Access control</li> <li>• Hacking tools</li> <li>• Hijacking</li> <li>• Protocol exception</li> <li>• Spam</li> <li>• Spyware</li> <li>• DDoS flood</li> <li>• Suspicious DNS activities</li> <li>• Other suspicious behaviors</li> </ul>
level	string	Level of detected threats. <ul style="list-style-type: none"> <li>• <b>CRITICAL</b></li> <li>• <b>HIGH</b></li> <li>• <b>MIDDLE</b></li> <li>• <b>LOW</b></li> </ul>
source	string	Defense for the detected attack. <ul style="list-style-type: none"> <li>• <b>0</b>: basic protection</li> <li>• <b>1</b>: virtual patch</li> </ul>
event_time	long	Attack time

### Access Control Logs

Field	Type	Description
rule_id	string	ID of the triggering rule
src_ip	string	Source IP address
src_port	string	Source port number

Field	Type	Description
dst_ip	string	Destination IP address
dst_port	string	Destination port number
src_region_name	string	Source region name
src_region_id	string	Source region ID
dst_region_name	string	Destination region name
dst_region_id	string	Destination region ID
log_type	string	Log type. <ul style="list-style-type: none"> <li>● <b>internet</b>: Internet border traffic log</li> <li>● <b>nat</b>: NAT border traffic log</li> <li>● <b>vpc</b>: inter-VPC traffic log</li> </ul>
dst_host	string	Destination domain name
vsys	long	Firewall protection direction. <ul style="list-style-type: none"> <li>● <b>1</b>: north-south</li> <li>● <b>2</b>: east-west</li> </ul>
protocol	string	Protocol type
app	string	Application type
direction	string	Traffic direction. <ul style="list-style-type: none"> <li>● <b>out2in</b>: inbound</li> <li>● <b>in2out</b>: outbound</li> </ul>
action	string	Response action of the firewall. <ul style="list-style-type: none"> <li>● <b>permit</b></li> <li>● <b>deny</b></li> </ul>
hit_time	long	Time of an access

## Traffic Logs

Field	Type	Description
src_ip	string	Source IP address
src_port	string	Source port number
dst_ip	string	Destination IP address
dst_port	string	Destination port number

Field	Type	Description
protocol	string	Protocol type
app	string	Application type
direction	string	Traffic direction. <ul style="list-style-type: none"> <li>• <b>out2in</b>: inbound</li> <li>• <b>in2out</b>: outbound</li> </ul>
action	string	Response action of the firewall. <ul style="list-style-type: none"> <li>• <b>permit</b></li> <li>• <b>deny</b></li> </ul>
src_region_name	string	Source region name
src_region_id	string	Source region ID
src_vpc	string	ID of the VPC that the source IP address belongs to
dst_region_name	string	Destination region name
dst_region_id	string	Destination region ID
dst_vpc	string	ID of the VPC that the destination IP address belongs to
log_type	string	Log type. <ul style="list-style-type: none"> <li>• <b>internet</b>: Internet border traffic log</li> <li>• <b>nat</b>: NAT border traffic log</li> <li>• <b>vpc</b>: inter-VPC traffic log</li> </ul>
dst_host	string	Destination domain name
vsys	long	Firewall protection direction. <ul style="list-style-type: none"> <li>• <b>1</b>: north-south</li> <li>• <b>2</b>: east-west</li> </ul>
hit_time	long	Time of an access
to_s_bytes	long	Number of bytes sent from the client to the server
to_c_bytes	long	Number of bytes sent from the server to the client
to_s_pkts	long	Number of packets sent from the client to the server
to_c_pkts	long	Number of packets sent from the server to the client

Field	Type	Description
bytes	long	Number of bytes of the protected traffic
packets	long	Number of packets in the protected traffic
start_time	long	Stream start time
end_time	long	Stream end time

# 13 System Management

## 13.1 Alarm Notification

After alarm notification is enabled, CFW will send notifications to you through the method you specified (such as email or SMS) so that you can monitor the firewall status and quickly detect exceptions.

### NOTE


- Simple Message Notification (SMN) is a paid service. For details, see [SMN Pricing Details](#).
- Before setting alarm notification, you are advised to create a message topic in SMN. For details, see [Before You Publish a Message](#).


### Prerequisites

The SMN service has been enabled.

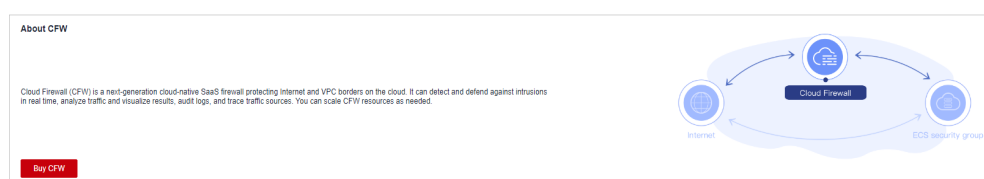
### Attack Alarms

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 13-1](#).

**Figure 13-1** CFW Dashboard



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

**Step 5** In the navigation pane, choose **System Management > Notifications**.

**Figure 13-2** Alarm notifications

Notification Item	Description	Level	Notification Time	Trigger Condition	Recipient Group	Status	Operation
Attack alarm	IPS attack alarm	Serious,High,Medium,Low	Time range (08:00 to 22:00)	5 occurrences within 10 minut...	-	<input type="checkbox"/>	<a href="#">Edit</a>
High Traffic Warning	An alarm is generated if the tra...	80%	Time range (08:00 to 22:00)	Once a day	-	<input type="checkbox"/>	<a href="#">Edit</a>

**Step 6** In the **Operation** column of **Attack alarm**, click **Edit**, and configure notification item parameters. For details, see [Table 13-1](#).

**Figure 13-3** Notification item settings - attack alarm

**Configure Notification** ✕

★ Description IPS attack alarm

★ Level  Serious  High  Medium  Low

★ Notification Time  All day  Time range (08:00 to 22:00)

★ Trigger Condition - 10 + occurrences within - 5 + minutes

★ Recipient Group

**Table 13-1** Attack alarm parameters

Parameter	Description
Description	IPS attack alarm
Level	Select the risk levels that trigger notifications. The options are <b>Serious</b> , <b>High</b> , <b>Medium</b> , and <b>Low</b> . Multiple options can be selected. For example, if you select <b>High</b> and <b>Medium</b> , the firewall will notify you by SMS message or email when detecting an intrusion with a high- or medium-level risk.
Notification Time	Select a time range for sending notifications.
Trigger Condition	Configure the trigger condition. <b>NOTE</b> Alarm notifications are sent if the number of attacks is at least equal to the threshold configured for a certain period.

Parameter	Description
Recipient Group	Select a topic from the drop-down list to configure the endpoints for receiving alarm notifications.


**Step 7** Click **OK**.


**Step 8** In the **Status** column of **Attack alarm**, click  to enable it.

----End

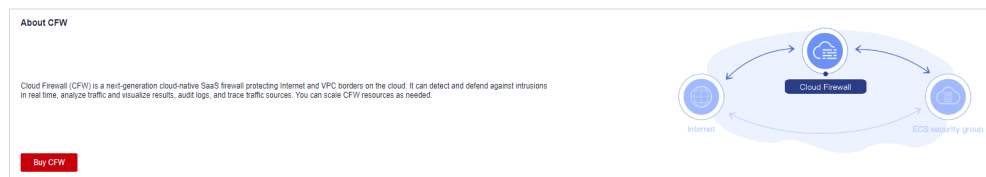
## High Traffic Warning

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 13-4](#).



**Figure 13-4** CFW Dashboard



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

**Step 5** In the navigation pane, choose **System Management > Notifications**.

**Figure 13-5** Alarm notifications

Notification Item	Description	Level	Notification Time	Trigger Condition	Recipient Group	Status	Operation
Attack alarm	IPS attack alarm	Serious,High,Medium,Low	Time range (08:00 to 22:00)	5 occurrences within 10 minut...	-		<a href="#">Edit</a>
High Traffic Warning	An alarm is generated if the tra...	80%	Time range (08:00 to 22:00)	Once a day	-		<a href="#">Edit</a>

**Step 6** In the **Operation** column of **High Traffic Warning**, click **Edit**, and configure notification item parameters. For details, see [Table 13-2](#).



**Figure 13-6** Notification item settings - high traffic warning

**Configure Notification**

\* Description An alarm is generated if the traffic reaches the specified percentage of the traffic processing capability.

\* Level

\* Notification Time  All day  Time range (08:00 to 22:00)

\* Trigger Condition Once a day

\* Recipient Group

**OK** Cancel

**Table 13-2** High traffic warning parameters

Parameter	Description
Description	An alarm is generated if the traffic reaches the specified percentage of the traffic processing capability you purchased.
Level	Select a percentage. When the maximum peak inbound or outbound traffic reaches the percentage of the traffic processing capability you purchased, an alarm notification is triggered. For example, you can select <b>70%</b> , <b>80%</b> , or <b>90%</b> . If this parameter is set to <b>80%</b> , an alarm notification is sent when the used traffic reaches 80% of the purchased traffic.
Notification Time	Select a time range for sending notifications.
Trigger Condition	Once a day
Recipient Group	Select a topic from the drop-down list to configure the endpoints for receiving alarm notifications.


**Step 7** Click **OK**.


**Step 8** In the **Status** column of **High Traffic Warning**, click  to enable it.

----End

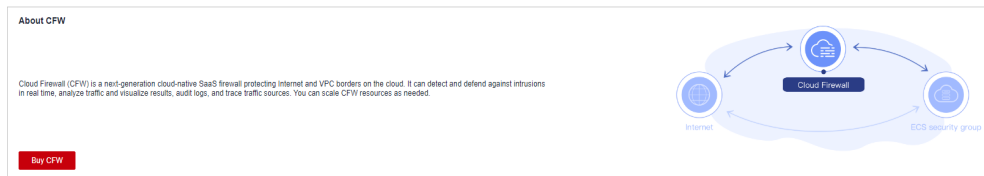
## EIP Not Protected

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

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

**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in **Figure 13-7**.

**Figure 13-7** CFW Dashboard



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

**Step 5** In the navigation pane, choose **System Management > Notifications**.

**Figure 13-8** Alarm notifications

Notification Item	Description	Level	Notification Time	Trigger Condition	Recipient Group	Status	Operation
Attack alarm	IPS attack alarm	Serious,High,Medium,Low	Time range (08:00 to 22:00)	5 occurrences within 10 minut...	-	<input type="checkbox"/>	Edit
High Traffic Warning	An alarm is generated if the tra...	80%	Time range (08:00 to 22:00)	Once a day	-	<input type="checkbox"/>	Edit

**Step 6** In the **Operation** column of the **EIP Not Protected** alarm, click **Edit**, and configure notification item parameters. For details, see **Table 13-3**.

**Figure 13-9** Notification settings - EIP Not Protected

×

**Configure Notification**

★ Description: There are unprotected EIPs.

★ Level:

★ Notification Time (GMT+08:00):  All day  Time range (08:00 to 22:00)

★ Trigger Condition: Once a day

★ Recipient Group ?  [View Topic](#)

**Table 13-3** Parameters of the alarm **EIP Not Protected**

Parameter	Description
Description	This alarm indicates there are unprotected EIPs.
Level	The default value is <b>100%</b> .

Parameter	Description
Notification Time	Select a time range for sending notifications.
Trigger Condition	Once a day
Recipient Group	Select a topic from the drop-down list to configure the endpoints for receiving alarm notifications.

**Step 7** Click **OK**.

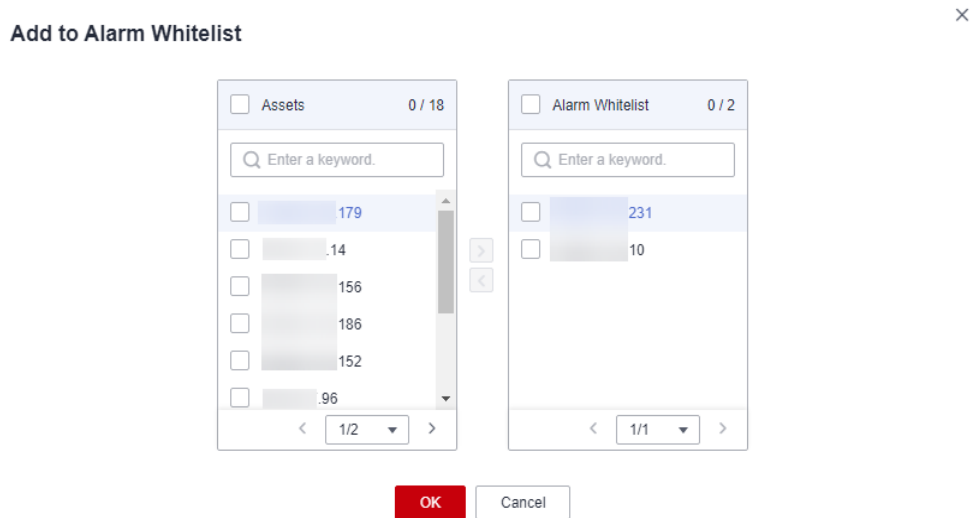
**Step 8** In the **Status** column of **EIP Not Protected**, click  to enable it.

----End

## Related Operations

To add assets to the **EIP Not Protected** alarm whitelist, click **Add to Alarm Whitelist** in the **Operation** column of the alarm. Select EIPs, add them to the whitelist on the right, and click **OK**. The whitelisted EIPs will no longer trigger this alarm.

**Figure 13-10** Add to Alarm Whitelist



## 13.2 Network Packet Capture

### 13.2.1 Creating a Packet Capture Task

You can create network packet capture tasks to locate network faults and attacks.

## Specification Limitations


Only the professional edition instances can capture network packets.


## Constraints

- Only one packet capture task can be executed at a time.
- A maximum of 20 packet capture tasks can be created every day.
- A maximum of 1 million packets can be captured.

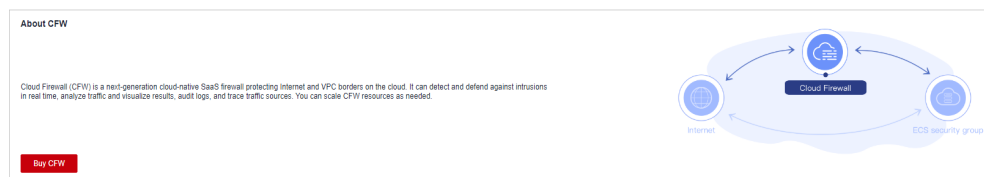
## Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 13-11](#).

**Figure 13-11** CFW Dashboard



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

**Step 5** In the navigation tree on the left, choose **System Management > Packet Capture**.

**Step 6** Click **Create Capture Task** and configure [parameters](#).

Figure 13-12 Creating a packet capture task

✕

### Create Capture Task

\* Task Name

\* Max. Packets Captured     
The maximum number of capture does not exceed 1,000,000

\* Capture Duration (min)     
The longest is not more than ten minutes

\* Protocol Type  ANY  TCP  UDP  ICMP

\* Source Address    
It should be: 0.0.0.0/0 can represent any address. [Select](#)

Source Port  

\* Destination    
It should be: 0.0.0.0/0 can represent any address. [Select](#)

Destination Port

Table 13-4 Packet capture task parameters

Parameter Name	Description	Example Value
Task Name	Task name. It must meet the following requirements: <ul style="list-style-type: none"> <li>Only uppercase letters (A to Z), lowercase letters (a to z), numbers (0 to 9), and the following special characters are allowed: -_</li> <li>Enter up to 30 characters.</li> </ul>	cfw

Parameter Name	Description	Example Value
Max. Packets Captured	Maximum number of captured packets. Enter an integer in the range 1 to 1,000,000.	100000
Capture Duration (min)	Maximum duration for capturing packets. Enter an integer in the range 1 to 10.	3
Protocol Type	Protocol type of captured packets. It can be: <ul style="list-style-type: none"> <li>• Any</li> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> </ul>	Any
Source Address	It can be: <ul style="list-style-type: none"> <li>• A single IP address, for example, <b>192.168.10.5</b></li> <li>• Consecutive IP addresses, for example, <b>192.168.0.2-192.168.0.10</b></li> <li>• Address segment, for example, <b>192.168.2.0/24</b></li> </ul>	192.168.10.5
Source Port	(Optional) Source port. The input rules are as follows: <ul style="list-style-type: none"> <li>• If this parameter is left blank, it indicates all port numbers (1 to 65535).</li> <li>• Enter a single port number in the range 1 to 65535.</li> </ul>	80
Destination Address	It can be: <ul style="list-style-type: none"> <li>• A single IP address, for example, <b>192.168.10.5</b></li> <li>• Consecutive IP addresses, for example, <b>192.168.0.2-192.168.0.10</b></li> <li>• Address segment, for example, <b>192.168.2.0/24</b></li> </ul>	192.168.10.6
Destination Port	(Optional) Destination port. The input rules are as follows: <ul style="list-style-type: none"> <li>• If this parameter is left blank, it indicates all port numbers (1 to 65535).</li> <li>• Enter a single port number in the range 1 to 65535.</li> </ul>	-

**Step 7** Click **OK**.

----End


## Related Operations


- To copy a task, click **Copy** in its **Operation** column. In the displayed dialog box, enter the task name and click **OK**.
- To stop a packet capture task, click **Stop** in its **Operation** column.
- To delete packet capture tasks, select them and click **Delete** above the list.
- [13.2.2 Viewing a Packet Capture Task](#)
- [13.2.3 Downloading Packet Capture Results](#)

## 13.2.2 Viewing a Packet Capture Task

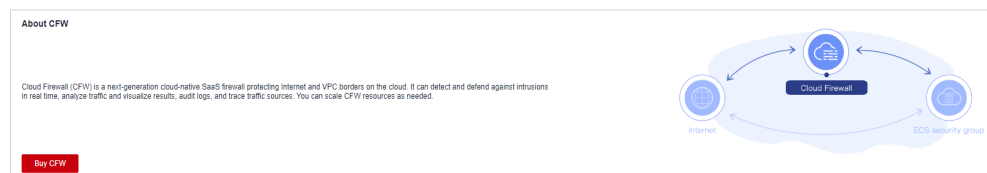
### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 13-13](#).

**Figure 13-13** CFW Dashboard



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

**Step 5** In the navigation tree on the left, choose **System Management > Packet Capture**.

**Step 6** (Optional) Search for a task by task name or IP address.

- Task name search supports fuzzy match. The input rules are as follows:
  - Only uppercase letters (A to Z), lowercase letters (a to z), numbers (0 to 9), and the following special characters are allowed: - \_
  - Enter up to 30 characters.
- To search by IP address, enter a single complete IP address, for example, 0.0.0.0.

**Step 7** Check the packet capture task. For more information, see [Table 13-5](#)

**Table 13-5** Packet capture task parameters

Parameter Name	Description
Task Name	Task name
Status	<p>Task status.</p> <ul style="list-style-type: none"><li>● <b>Running:</b> The packet capture command has been delivered and the task is in progress.</li><li>● <b>Completed:</b> The packet capture result has been uploaded and the task is complete.</li><li>● <b>Exception:</b> Packet capture data upload times out due to network problems, and some packet capture results are lost.</li></ul> <p><b>NOTE</b> To retry a task, you can click <b>Copy</b> in its <b>Operation</b> column to create and execute it again.</p> <ul style="list-style-type: none"><li>● <b>Stopping:</b> The task is being stopped and the packet capture result is being uploaded.</li><li>● <b>Expired:</b> The packet capture result has been uploaded and the task has been manually stopped.</li></ul>
Protocol Type	Protocol type specified for packet capture.
IP Address	IP addresses specified for packet capture, including the source and destination addresses.
Port	Ports specified for packet capture, including the source and destination ports.
Max. Packets Captured	Maximum number of captured packets in the current task.
Packet Capture Time	Start time and end time of a packet capture task.
Capture Duration (min)	Duration of packet capture.
Remaining Retention Period (Days)	Number of days for storing a packet capture task. The default value is 7.
Capture Size	Size of captured packets.

----End

## Related Operations

- To copy a task, click **Copy** in its **Operation** column. In the displayed dialog box, enter the task name and click **OK**.
- To stop a packet capture task, click **Stop** in its **Operation** column.
- To delete packet capture tasks, select them and click **Delete** above the list.
- [13.2.1 Creating a Packet Capture Task](#)



- [13.2.3 Downloading Packet Capture Results](#)

## 13.2.3 Downloading Packet Capture Results


### Constraints


For an abnormal task, its possible packet capture results are as follows:

- The packet capture data is completely lost and cannot be downloaded.
- Some packet capture data is lost. Existing data can be downloaded.

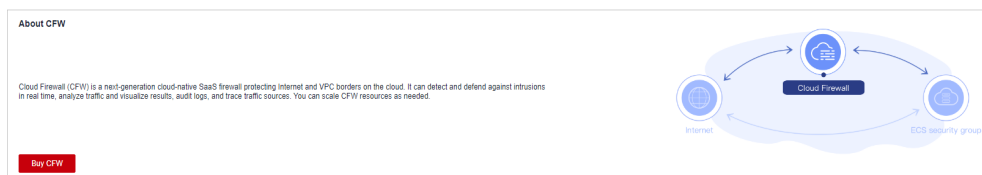
### Procedure

**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, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 13-14](#).

**Figure 13-14** CFW Dashboard



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

**Step 5** In the navigation tree on the left, choose **System Management > Packet Capture**.

**Step 6** In the row of a task, click **Download** in the **Operation** column to view the packet capture result.

#### NOTE

For an abnormal task, its possible packet capture results are as follows:

- The packet capture data is completely lost and cannot be downloaded.
- Some packet capture data is lost. Existing data can be downloaded.

**Step 7** Obtain the packet capture result.

- You can click **Copy all** to share the link with others.
- You can click **Open URL** to open it in a new browser tab. Switch back to this dialog box, click **Copy access code**, paste the copied code to the **Extraction Code** text box on the new tab, and click **Obtain Shared File List**.
- You can click **Copy link**, and paste and open the link it in a new browser tab. Switch back to this dialog box, click **Copy access code**, paste the copied code to the **Extraction Code** text box on the new tab, and click **Obtain Shared File List**.

**NOTE**

You can switch between Chinese and English in the lower left corner of the browser.

**Step 8** Click **Download** or **Download As**.

----End

## 13.3 Configuring DNS Resolution

Select a default DNS server or add a DNS server IP address. The domain name protection policy will be delivered to the specified servers.


If the current account has multiple firewalls, the DNS resolution operation only applies to specified firewalls.

### Constraints

A maximum of two DNS servers can be customized.

### 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.


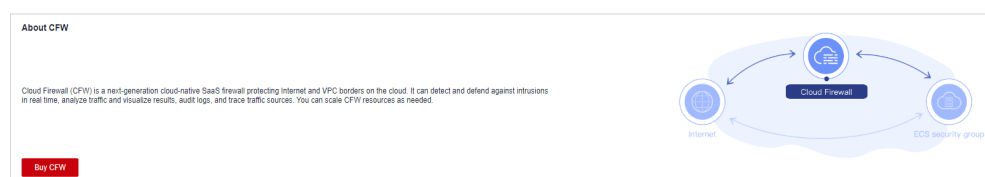
**Step 3** In the navigation pane, click  and choose **Security & Compliance > Cloud Firewall**. The **Dashboard** page will be displayed, as shown in [Figure 13-15](#).

Figure 13-15 CFW Dashboard



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

**Step 5** In the navigation tree on the left, choose **System Management > DNS Resolution**.

**Step 6** Select the default DNS server or add a custom DNS server.

**NOTE**

Currently, only two specified DNS servers can be added.

**Step 7** Click **Apply**.

 **NOTE**

If the current account has multiple firewalls, the DNS resolution operation only applies to specified firewalls.

**----End**

# 14 Audit

## 14.1 Operations Recorded by CTS

CTS provides records of operations on CFW. With CTS, you can query, audit, and backtrack these operations. For details, see the *Cloud Trace Service User Guide*.

[CFW operations recorded by CTS](#) lists details about the CFW operations on CTS.

**Table 14-1** CFW operations recorded by CTS

Operation	Resource Type	Trace Name
EIP protection	cfw	eipOperateProtectService
Enable EIP protection	cfw	eipOperateProtectServiceEnable
Disable EIP protection	cfw	eipOperateProtectServiceDisable
Creating an ACL rule	acl	addRuleAclService
Modify an ACL rule	acl	updateRuleAclService
Delete an ACL rule	acl	deleteRuleAclService
Configure ACL rule priority	acl	setACLRulePriority
Create a blacklist	black_white_list	addBlackListService
Modify a blacklist	black_white_list	updateBlackListService
Delete a blacklist	black_white_list	deleteBlackListService
Create a whitelist	black_white_list	addWhiteListService
Modify a whitelist	black_white_list	updateWhiteListService
Delete a whitelist	black_white_list	deleteWhiteListService

Operation	Resource Type	Trace Name
Create an IP address group	address_group	addAddressSetInfoService
Update an IP address group	address_group	updateAddressSetInfoService
Delete an IP address group	address_group	deleteAddressSetInfoService
Add a member to an IP address group	address_group	addAddressItemsService
Update a member in an IP address group.	address_group	updateAddressItemService
Delete a member from an IP address group	address_group	deleteAddressItemService
Create a service group	service_group	addServiceSetService
Update a service group	service_group	updateServiceSetService
Delete a service group	service_group	deleteServiceSetService
Add a member to a service group	service_group	addServiceItemsService
Update a member in a service group	service_group	updateServiceItemService
Delete a member from a service group	service_group	deleteServiceItemService
Create an east-west CFW instance	cfw_instance	createEWFirewallInstance
Create a south-north CFW instance	cfw_instance	createSNFirewallInstance
Update a firewall	cfw_instance	updateFirewallInstance
Delete a firewall	cfw_instance	deleteFirewallInstance
Upgrade a firewall	cfw_instance	upgradeFirewallInstance
Add a tag	cfw_instance	createTags
Delete a tag	cfw_instance	deleteTags
Freeze a firewall	cfw_instance	freezeFirewallInstance
Update attack logs and deliver configurations	alarm_config	updateAlarmConfig
Update a user's DNS server configurations	dns_server	updateDnsServer

Operation	Resource Type	Trace Name
Create an east-west firewall	cfw	createEastWestFirewall
Enable an east-west firewall	cfw	enableEwFirewallProtect
Disable an east-west firewall	cfw	disableEwFirewallProtect
Purchase a firewall	cfw	addFirewallOrder
Delete a firewall	cfw	deleteFirewall
Upgrade a firewall	cfw	changeFirewall
Modify or create an IPS protection mode	ips	createOrUpdateIpsMode
Enable a virtual patch	ips	enableVirtualPatches
Disable a virtual patch	ips	disableVirtualPatches
Create log management configurations	log_config	createLogConfig
Modify log management configurations	log_config	updateLogConfig
Import an ACL	import	importCFW

## 14.2 Viewing Audit Logs

After you enable CTS, the system starts recording operations on CFW. You can view the operation records of the last seven days on the CTS console.

For details about how to view audit logs, see [Querying Real-Time Traces \(for New Console\)](#).

# 15 Monitoring

## 15.1 CFW Monitored Metrics

### Description

This topic describes metrics reported by CFW to Cloud Eye as well as their namespaces. You can use Cloud Eye to query the metrics of the monitored object and alarms generated for CFW.

### Namespace

SYS.CFW

#### NOTE

A namespace is an abstract collection of resources and objects. Multiple namespaces can be created in a single cluster with the data isolated from each other. This enables namespaces to share the same cluster services without affecting each other.

### Metrics

**Table 15-1** CFW metrics

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
used_protection_bandwidth	Internet Boundary Protection Bandwidth Usage (Mbps)	Used bandwidth detected by CFW in the last 5 minutes Unit: KB/s	≥ 0 Value type: Float	CFW	5

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
protecti on_ban dwidth_ usage	Internet Boundary Protection Bandwidth Usage (%)	Bandwidth usage rate detected by CFW within 5 minutes.  Unit: %  Usage rate = Use bandwidth/ Percentage of the used bandwidth to the bandwidth quota.	≥ 0  Value type: Float	CFW	5



## Dimension

Key	Value
fw_instance_id	Firewall ID

## 15.2 Configuring Alarm Monitoring Rules

You can set CFW alarm rules to customize the monitored objects and notification policies, and set parameters such as the alarm rule name, monitored object, metric, threshold, monitoring scope, and whether to send notifications. This helps you learn the CFW protection status in a timely manner.

### 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** Hover your mouse over  in the upper left corner of the page and choose **Management & Governance > Cloud Eye.**
- Step 4** In the navigation pane on the left, choose **Alarm Management > Alarm Rules.**
- Step 5** In the upper right corner of the page, click **Create Alarm Rule.**
- Step 6** Set the parameters as prompted. The key parameters are as follows. For details about more parameters, see .



- **Alarm Type: Metric**
- **Resource Type: Cloud Firewall**
- **Dimension: Cloud Firewall Instances**

**Step 7** Click **Create**. In the displayed dialog box, click **OK**.

----End

## 15.3 Viewing Monitoring Metrics


You can view CFW metrics on the management console to learn about the CFW protection status in a timely manner and set protection policies based on the metrics.


### Prerequisites

CFW alarm rules have been configured in Cloud Eye. For more details, see [15.2 Configuring Alarm Monitoring Rules](#).

### 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** Hover your mouse over  in the upper left corner of the page and choose **Management & Governance > Cloud Eye**.

**Step 4** In the navigation pane on the left, choose **Cloud Service Monitoring > Cloud Firewall**.

**Step 5** In the row containing the dedicated CFW instance, click **View Metric** in the **Operation** column.

----End

# A Change History

Date	Description
2024-01-10	<p>This is the third official release.</p> <p>Added:</p> <ul style="list-style-type: none"><li>• Added the description about purchasing firewalls in pay-per-use mode in <a href="#">1 Purchasing CFW</a>.</li><li>• <a href="#">5 Managing VPC Border Firewalls</a></li><li>• <a href="#">6.5.2 Viewing a Predefined Address Group</a></li><li>• <a href="#">6.6.2 Viewing a Predefined Service Group</a></li></ul>
2023-11-30	<p>This is the second official release.</p> <p>Added:</p> <ul style="list-style-type: none"><li>• Security overview and traffic trend in <a href="#">3 Checking the CFW Dashboard</a>.</li><li>• <a href="#">6.7.1 Adding a Domain Name Group</a></li><li>• <a href="#">6.8 Policy Assistant</a></li><li>• Sensitive directory scan defense and reverse shell detection in <a href="#">7 Configuring Intrusion Prevention</a>.</li><li>• <a href="#">8 Managing Intrusion Prevention</a></li><li>• <a href="#">10 Security Dashboard</a></li><li>• <a href="#">11 Traffic Analysis</a> and its subsections</li><li>• <a href="#">13.1 Alarm Notification</a></li></ul>
2023-02-28	<p>This is the first official release.</p>