Cloud Firewall

User Guide

Issue	12
Date	2024-03-06

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Purchasing CFW

1.1 Purchasing Standard Edition

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

This section describes how to purchase the standard edition firewall.

Prerequisites

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

Constraints

- Cloud firewalls can be used in the selected region only. To use a cloud firewall in another region, switch to the corresponding region and then purchase it. For details about the regions where cloud firewall can be purchased, see **Function Overview**.
- Only CFW instances in the enterprise project to which the current account belongs can be purchased.

Editions

CFW provides standard edition and professional edition. For details about function differences between editions, see **Editions**.

The application scenarios for different editions are as follows:

- Standard edition

  Suitable for SMEs that need to defend against network intrusions and server compromises, or need to obtain Multi-Layer Protection Scheme (MLPS) certification.
- Professional edition

  Suitable for large and medium-sized enterprises that need to defend against network intrusions and server compromises, control internal network security, or obtain Multi-Layer Protection Scheme (MLPS) certification.

Procedure

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

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

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

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

Table 1-1 cloud firewall parameters

Parameter	Description
Billing Mode	Yearly/Monthly
Region	Region where the cloud firewall is to be purchased. **NOTICE** 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 can be purchased, see **Function Overview**.
Edition	Standard edition
Engine	Direct engine. 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 **NOTE** 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 5000 Mbit/s per month. (The value must be an integer multiple of 5.) **NOTE** • 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. • The protection traffic is determined based on the maximum inbound or outbound traffic, whichever is higher.

Parameter	Description
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 use this function, **Enable Enterprise Center**. You can use an enterprise project to centrally manage your cloud resources and members by project. **NOTE** Value **default** 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: ● Only letters (A to Z and a to z), numbers (0 to 9), spaces, and the following characters are allowed: -_ ● The value can contain 1 to 48 characters.
Advanced Settings	**Tag**: You can use a tag for multiple cloud resources. You are advised to predefine tags in TMS. For details, see **Resource Tag Overview**. If your organization has configured a tag policy for cloud firewalls, you need to add tags in compliance with the policy. If a tag does not comply with the tag policies, firewall instance creation may fail. Contact your organization administrator to learn more about tag policies.
Required Duration	Service duration. After selecting a duration, you can select **Auto-renew**. 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 **Auto-Renewal Rules** when enabling auto-renewal.

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

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

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

----End

Effective Conditions

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

Related Operations

- **Changing CFW Specifications**: The standard edition can be upgraded to the professional edition. You can also increase the number of expansion packages as required.
- **How Do I Renew CFW?**
- **How Do I Unsubscribe from CFW?**

1.2 Purchasing Professional Edition

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

This section describes how to purchaseprofessional edition.

Prerequisites

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

Constraints

- Cloud firewalls can be used in the selected region only. To use a cloud firewall in another region, switch to the corresponding region and then purchase it. For details about the regions where cloud firewall can be purchased, see **Function Overview**.
- Only CFW instances in the enterprise project to which the current account belongs can be purchased.

Editions

CFW provides standard edition and professional edition. For details about function differences between editions, see **Editions**.

The application scenarios for different editions are as follows:

- Standard edition

  Suitable for SMEs that need to defend against network intrusions and server compromises, or need to obtain Multi-Layer Protection Scheme (MLPS) certification.
- Professional edition

  Suitable for large and medium-sized enterprises that need to defend against network intrusions and server compromises, control internal network security, or obtain Multi-Layer Protection Scheme (MLPS) certification.

Procedure

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

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

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

Step 4 Click **Buy CFW** and configure parameters on the **Buy CFW** page. For more information, see **Table 1-2**.

Table 1-2 cloud firewall parameters

Parameter	Description
Billing Mode	Yearly/Monthly
Region	Region where the cloud firewall is to be purchased. **NOTICE** 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 can be purchased, see **Function Overview**.
Edition	Professional edition
Engine	Direct engine. 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 **NOTE** 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 5000 Mbit/s per month. (The value must be an integer multiple of 5.) **NOTE** • 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. • The protection traffic is determined based on the maximum inbound or outbound traffic, whichever is higher.
Added VPCs	(Optional) Select the number of VPCs to be expanded. The value ranges from 0 to 500. **NOTE** • Only the professional edition supports inter-VPC protection. • 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. • For each VPC you add, the protected peak traffic increases by 200 Mbit/s.

Parameter	Description
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 use this function, **Enable Enterprise Center**. You can use an enterprise project to centrally manage your cloud resources and members by project. **NOTE** Value **default** 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: ● Only letters (A to Z and a to z), numbers (0 to 9), spaces, and the following characters are allowed: -_ ● The value can contain 1 to 48 characters.
Advanced Settings	**Tag**: You can use a tag for multiple cloud resources. You are advised to predefine tags in TMS. For details, see **Resource Tag Overview**. If your organization has configured a tag policy for cloud firewalls, you need to add tags in compliance with the policy. If a tag does not comply with the tag policies, firewall instance creation may fail. Contact your organization administrator to learn more about tag policies.
Required Duration	Service duration. After selecting a duration, you can select **Auto-renew**. 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 **Auto-Renewal Rules** when enabling auto-renewal.

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

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

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

----End

Effective Conditions

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

Follow-up Operations

After purchasing a firewall, you need to configure the VPC border firewall before adding a VPC border protection policy. For details about how to configure the VPC border firewall, see **VPC Border Firewall Overview**.

Related Operations

- **Changing CFW Specifications**: You can add extended packages as required.
- **How Do I Renew CFW?**
- **How Do I Unsubscribe from CFW?**

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.

Upgrading an Edition

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

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

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

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

Step 5 In the upper left 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 on the left, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

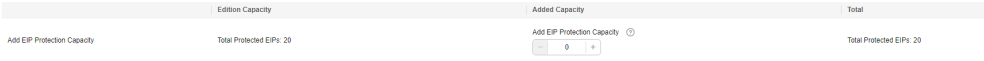
Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column to go to the details page.

Step 5 In the **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 2-1 Adding EIP protection capacity



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

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

Step 5 Hover your cursor over the edition name in the upper left 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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Check the information about each firewall instance under the account. Click **View** in the **Operation** column.

Figure 3-1 Firewall instances

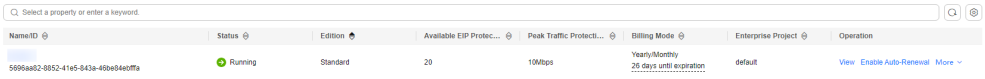


Table 3-1 Firewall instance parameters

Parameter	Description
Name/ID	Name and ID of the firewall.
Status	Firewall status.
Edition	Firewall edition. Standard and professional editions are supported.

Parameter	Description
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

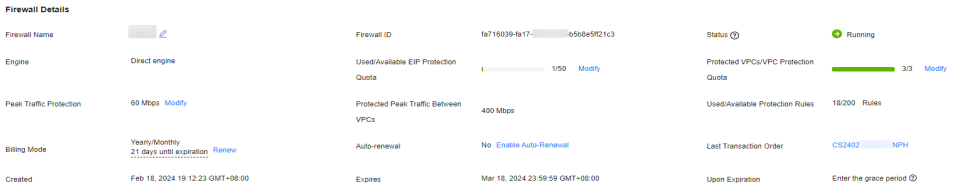


Table 3-2 Detailed firewall information

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	*Number of protected EIPs*/*Total number of EIPs* under a CFW instance.
Protected VPCs/VPC Protection Quota	*Number of protected VPCs*/*Total number of VPCs* under a firewall instance.
Peak Traffic Protection	Peak north-south traffic that can be protected.
Protected Peak Traffic Between VPCs	Peak east-west traffic that can be protected.

Parameter	Description
Used/Available Protection Rules	*Number of created protection rules*/*Total number of protection rules that can be created* under a firewall instance.
Billing Mode	Bling mode
Auto-renewal	Indicates whether the system automatically renews the service based on the subscription period when the service expires.
Upon Expiration	Billing policy after the firewall instance expires.
Last Transaction Order	Latest transaction order of the firewall instance.
Created	Time at which the firewall instance is created.
Expires	Estimated expiration time of the firewall instance.
Upon Expiration	Billing policy after the firewall instance expires.

Step 6 View firewall protection statistics. For more information, see **Table 3-3**.

- EIP Protection
- Inter-VPC Protection

Figure 3-3 Protection statistics

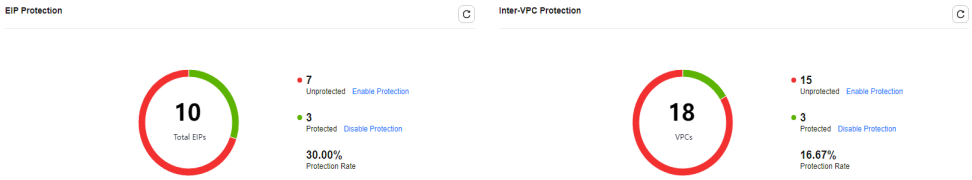


Table 3-3 Firewall protection statistics

Parameter	Description
Total EIPs	Total number of EIPs, both the protected and the unprotected.
Total VPCs	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 **Operation Dashboard**: View the Internet border and VPC border protection details. 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 Operations Dashboard

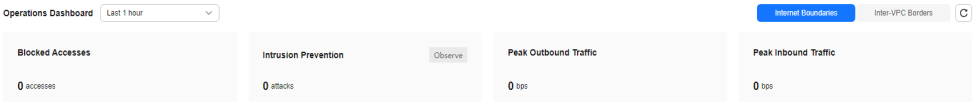


Table 3-4 Operations Dashboard

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 **Traffic Situation**: View the traffic trend at the Internet border and VPC border. For details, see **Table 3-5**.

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

Figure 3-5 Traffic Situation

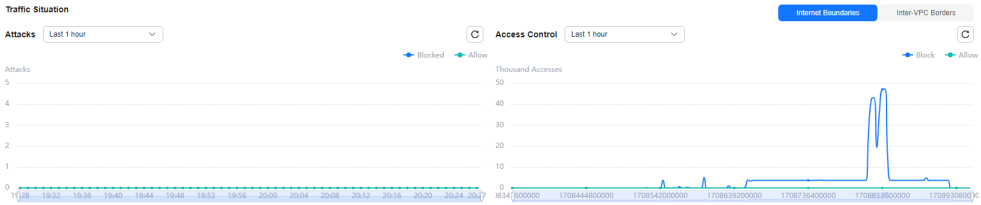
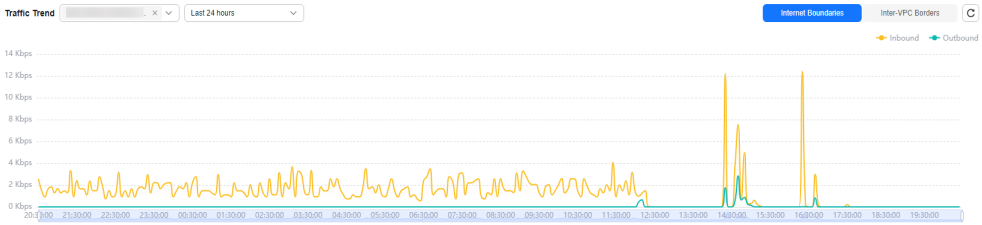


Table 3-5 Traffic trend parameters

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.

Figure 3-6 Traffic Trend



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.
- An EIP can only be protected by one firewall.
- Only EIPs in the enterprise project to which the current account belongs can 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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation pane, choose **Assets** > **EIPs**. The EIP page is displayed. The EIP information is automatically updated to the list.

Step 6 Enable EIP protection.

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

NOTICE

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

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

NOTE

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

----End

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

This section describes how to view the information about an EIP, such as its ID and protection status.

Procedure

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

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

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

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

Step 5 In the navigation pane, choose **Assets** > **EIPs**.

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 Quota	*Number of protected EIPs*/*Total number of EIPs* 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. **NOTE** It can be enabled for only one firewall instance.

Table 4-2 EIP parameters

Parameter	Description
EIP/ID	IP address and ID of an EIP.
Protection Status	EIP protection status.
Firewall Name/ID	Name and ID of the firewall instance that protects the EIP
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.

Parameter	Description
Owner	Member account that an EIP belongs to. This field is displayed only for users who have enabled multi-account management.

----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.
- Traffic diversion depends on the enterprise router
- Only VPCs in the enterprise project to which the current account belongs can be protected.
- 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 and Usage Process

The new and old versions of the VPC border firewall in enterprise router are available in different regions due to dependency reasons.

- New version: For details about the configuration process, see **Table 5-1**. For details about the configuration document, see **Enterprise Router Mode (New)**.
- Old version: For details about the configuration process, see **Figure 5-3**. For details about the configuration document, see **Enterprise Router Mode (Old)**.

NOTE

Difference between new and old versions:

The pages for creating a VPC border firewall differ, as shown in **VPC border firewall (new version)** and **VPC border firewall (old version)**.

Figure 5-1 VPC border firewall (new version)

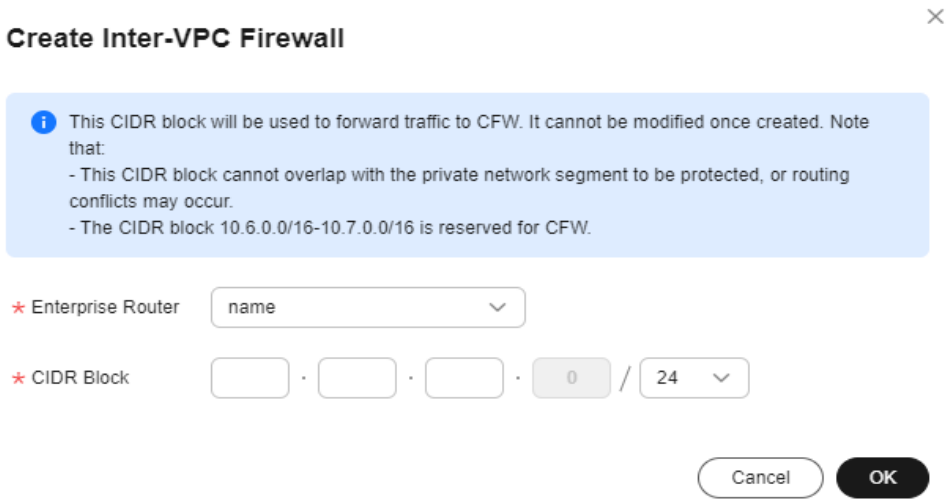


Figure 5-2 Creating a VPC border firewall (old version)

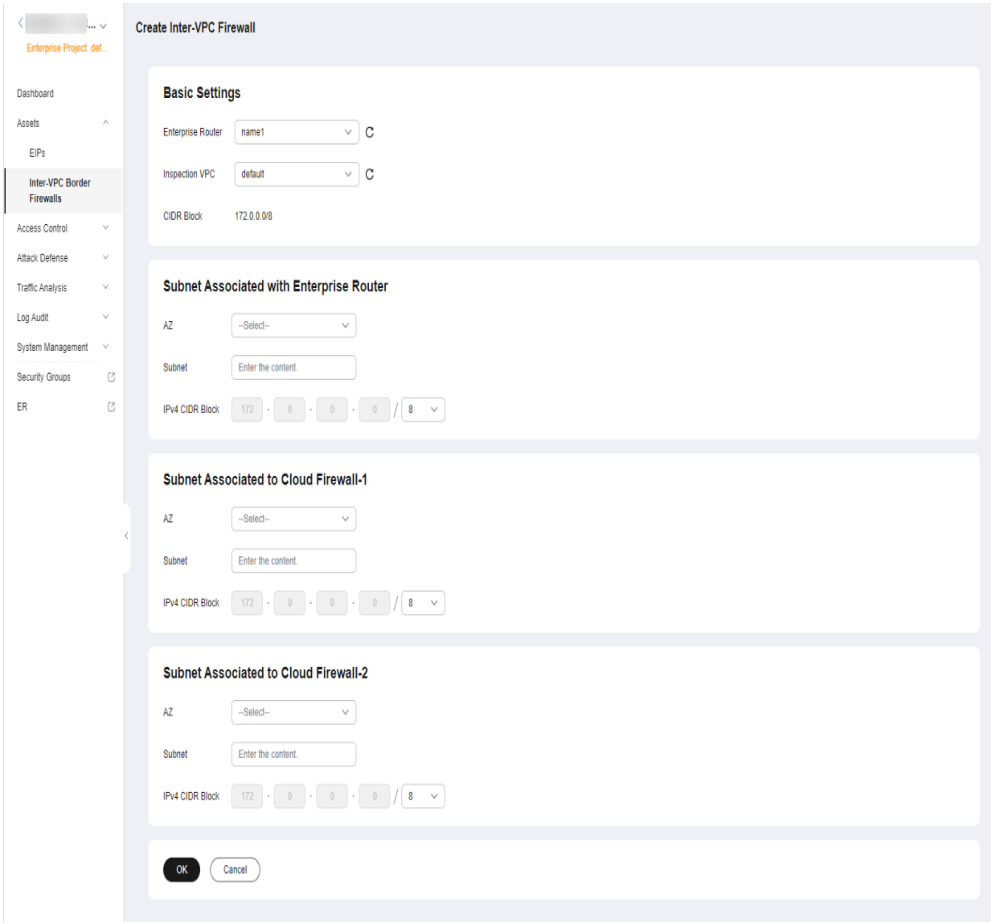
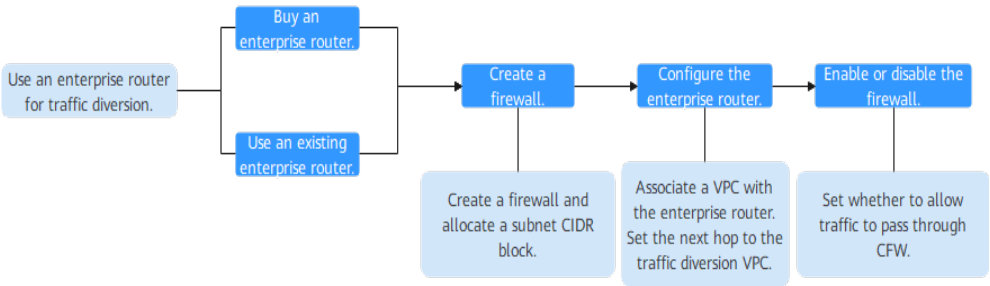


Table 5-1 Configuration and usage process in enterprise router mode (new)

Procedure	Description
Step 1: Create a Firewall	Plan CIDR blocks for traffic diversion on the VPC border firewall. **NOTE** The traffic diversion VPC does not occupy the VPC protection quotas under your account.
Step 2: Add VPC Attachments	Add connections between protected VPCs and an enterprise router.
Step 3: Create and Configure Route Tables	In the enterprise router, create an association route table and a propagation route table to transmit traffic between VPCs and firewall.
Step 4: Modify VPC Route Tables	Add a route pointing to the enterprise router for each VPC.
(Optional) Verifying Connectivity	You are advised to test the network connectivity before enabling protection.
Step 5: Enable or Disable a VPC Border Firewall	Enable or disable inter-VPC traffic protection.
(Optional) Adding a Protected VPC	Add a VPC to be protected.

The following figure shows the configuration process in enterprise router mode (old).

Figure 5-3 Configuration process of the enterprise router mode



5.2 Enterprise Router Mode (New)

5.2.1 Step 1: Create a Firewall

A VPC border firewall can collect statistics on the traffic between VPCs, helping you detect abnormal traffic. Before enabling a VPC border firewall, create it and associate it with an enterprise router first.

Prerequisites

The current account must have an available enterprise router. (See **Enterprise router constraints**.)

- For details about Enterprise Router pricing, see **Pricing**.
- For details about how to purchase an enterprise router, see **Creating an Enterprise Router**.

Constraints

When creating a firewall, select an enterprise router and configure an IPv4 CIDR block for traffic diversion.

- An enterprise router is used for traffic diversion. It must meet the following requirements:
  - Not associated with other firewall instances.
  - Belongs to the current account and is not shared with other users.
  - **Default Route Table Association**, **Default Route Table Propagation**, and **Auto Accept Shared Attachments** must be disabled.
- A CIDR block is used to forward traffic to CFW. It must comply with the following restrictions:
  - This CIDR block cannot overlap with the private network segment to be protected, or routing conflicts may occur.
  - The CIDR block 10.6.0.0/16-10.7.0.0/16 is reserved for CFW and cannot be specified.

Procedure

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

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

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

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

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

Step 6 Click **Create Firewall**, select an enterprise router, and configure a CIDR block.

- An enterprise router is used for traffic diversion. It must meet the following requirements:
  - Not associated with other firewall instances.
  - Belongs to the current account and is not shared with other users.
  - **Default Route Table Association**, **Default Route Table Propagation**, and **Auto Accept Shared Attachments** must be disabled.
- After a CIDR block is configured, an inspection VPC is created by default to forward traffic to CFW. A CFW-associated subnet is automatically allocated to

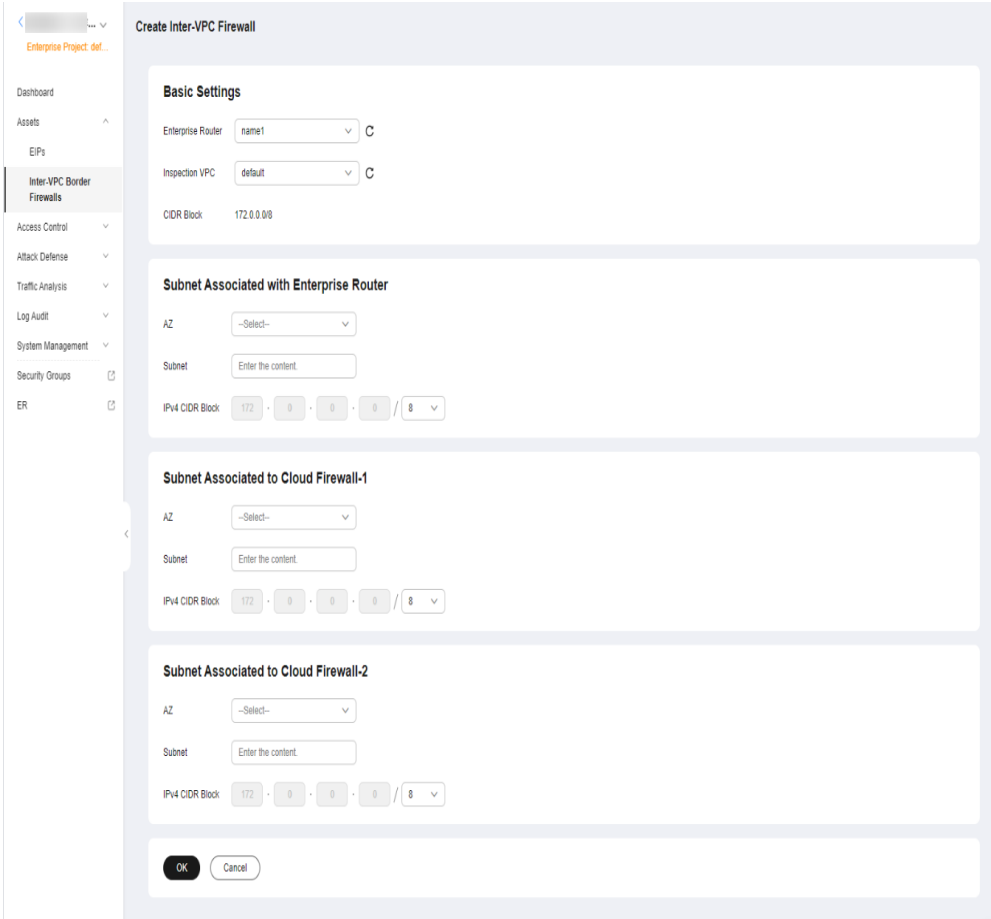
forward traffic to an enterprise router. Pay attention to the following restrictions:

- After a firewall is created, its CIDR block cannot be modified.
- The CIDR block must meet the following requirements:
  - Only private network address segments (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) are supported. Otherwise, route conflicts may occur in public network access scenarios, such as SNAT.
  - The CIDR block 10.6.0.0/16-10.7.0.0/16 is reserved for CFW and cannot be used.
  - This CIDR block cannot overlap with the private CIDR block to be protected, or routing conflicts and protection failures may occur.

NOTE

If the page shown in **Figure 5-4** is displayed, you are using the old CFW version. For details about how to configure the VPC border firewall, see **Enterprise Router Mode (Old)**.

Figure 5-4 Creating a VPC border firewall (old version)



Step 7 Click **OK**. The firewall will be created in 3 to 5 minutes.

During the creation, you can only check the **Dashboard** page. The firewall status will change to **Upgrading**.

----End

Related Operations

Unsubscription: To unsubscribe from a VPC border firewall, you must unsubscribe from the CFW instance associated with it. For details, see **How Do I Unsubscribe from CFW?**

5.2.2 Step 2: Add VPC Attachments

This section describes how to add connections to protected VPCs.

Procedure

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

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

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

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

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

Step 6 Click **Edit Protected VPCs** next to the firewall status. Add attachments on the enterprise router page that is displayed. For details about the supported attachment types, see **Attachment Overview**.

Assume you want to protect two VPCs. (At least two VPC attachments are required to connect the two VPCs to the enterprise router.) For details, see **Adding VPC Attachments to an Enterprise Router**.

NOTE

- After a firewall is created, a firewall connection (named **cfw-er-auto-attach** and connected to the CFW instance) is automatically generated. You need to manually add a connection for each protected VPC.

  For example, the VPC1 connection is named **vpc-1**, the VPC2 connection is named **vpc-2**, and the VPC3 connection is named **vpc-3**.
- To use the enterprise router of account A to protect VPCs under account B, share the router with account B. For details, see **Creating a Sharing**.

----End

5.2.3 Step 3: Create and Configure Route Tables

This section describes how to create and configure an association route table and a propagation route table.

Creating Two Route Tables

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 service list, click **Enterprise Router** under **Networking**. Click **Manage Route Table**.

Step 4 Create an association route table and a propagation route table, used for connecting to a protected VPC and a firewall, respectively.

Click the **Route Tables** tab. Click **Create Route Table**. For more information, see **Table 5-2**.

Table 5-2 Route table parameters

Parameter	Description
Name	Route table name. It must meet the following requirements: ● Must contain 1 to 64 characters. ● Can contain letters, digits, underscores (_), hyphens (-), and periods (.).
Description	Route table description
Tag	During the route table creation, you can tag the route table resources. Tags identify cloud resources for purposes of easy categorization and quick search. For details about tags, see **Tag Overview**.

NOTE

Create two route tables, to be used as an association route table and a propagation route table, respectively.

----End

Configuring Associations for a Route Table

Step 1 In the service list, click **Enterprise Router** under **Networking**. Click **Manage Route Table**.

Step 2 Configure associations. On the route table configuration page, select the association table, click the **Associations** tab, and click **Create Association**. For more information, see **Table 5-3**.

Figure 5-5 Creating an association

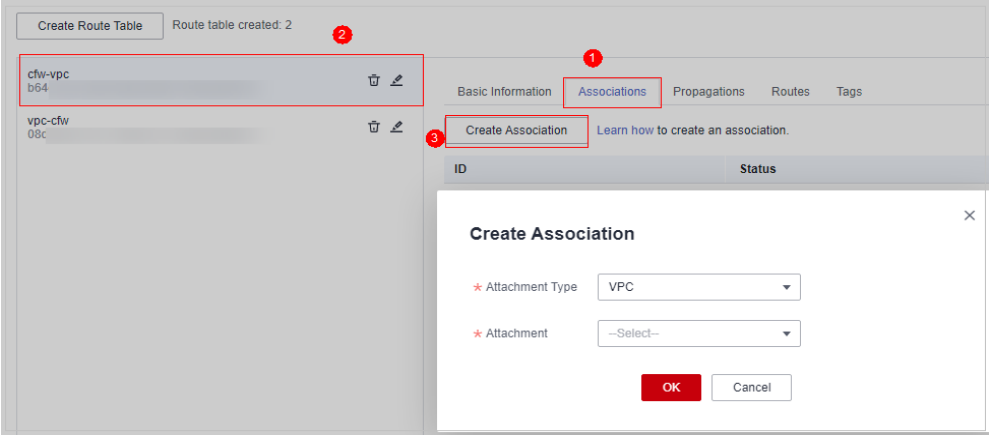


Table 5-3 Association parameters

Parameter	Description
Attachment Type	Select **VPC**.
Attachment	Select an item from the **Attachment** drop-down list.

NOTE

Add at least two associations. An association is required for each protected VPC you add.

For example, select attachment **vpc-1** for VPC1 and **vpc-2** for VPC2. To add VPC3 for protection, add an association and select attachment **vpc-3**.

Step 3 Configure routes. Click the **Routes** tab and click **Create Route**. Create routes as needed. For more information, see **Table 5-4**.

Figure 5-6 Creating a route

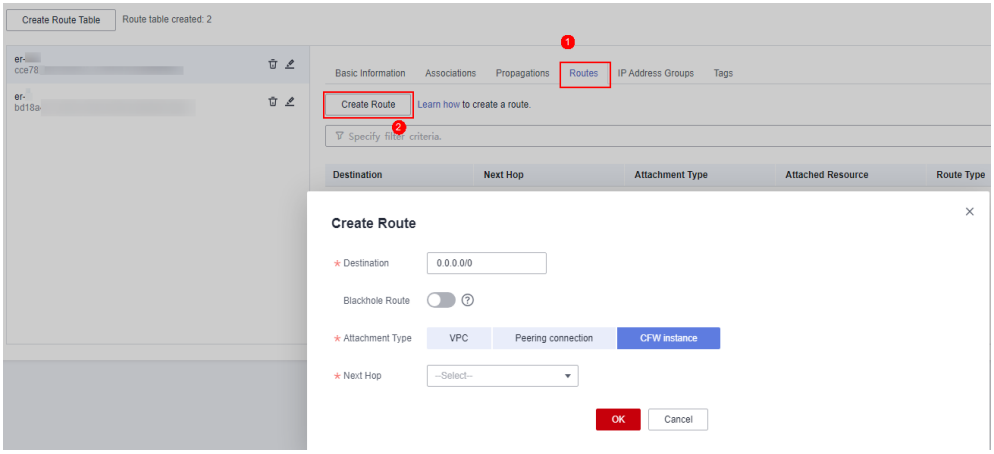


Table 5-4 Route parameters

Parameter	Description
Destination	Set it to **0.0.0.0/0**.
Blackhole Route	You are advised to disable this function. If it is enabled, the packets from a route that matches the destination address of the blackhole route will be discarded.
Attachment Type	Set it to **CFW instance**.
Next Hop	Select the automatically generated firewall attachment **cfw-er-auto-attach**.

----End

Configuring Propagations for a Route Table

Step 1 In the service list, click **Enterprise Router** under **Networking**. Click **Manage Route Table**.

Step 2 Configure associations. On the route table configuration page, select the propagation table, click the **Associations** tab, and click **Create Association**. For more information, see **Table 5-5**.

Figure 5-7 Creating an association

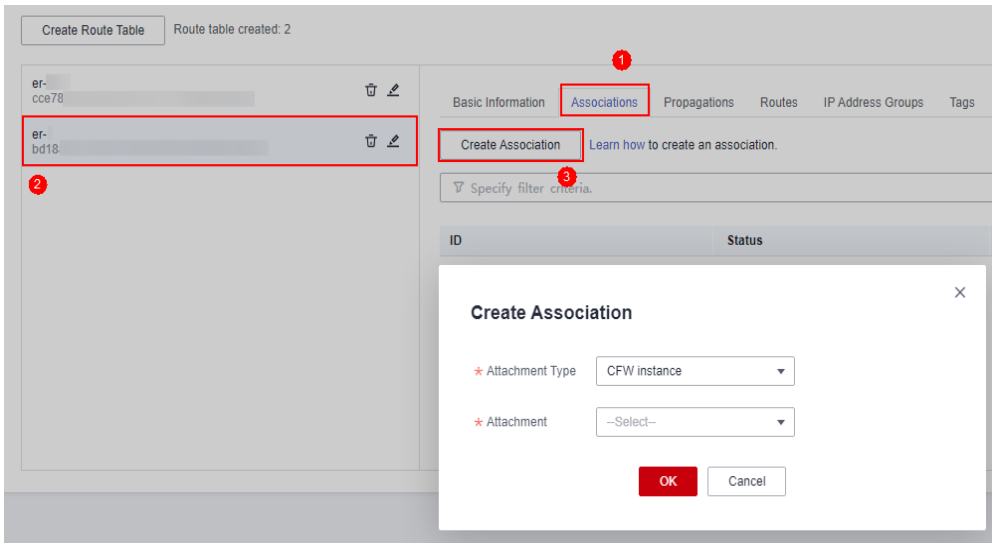


Table 5-5 Association parameters

Parameter	Description
Attachment Type	Set it to **CFW instance**.
Attachment	Select the automatically generated firewall attachment **cfw-er-auto-attach**.

Step 3 Configure propagations. Click the **Propagations** tab, and click **Create Propagation**. For more information, see Table 5-6.

Figure 5-8 Creating a propagation

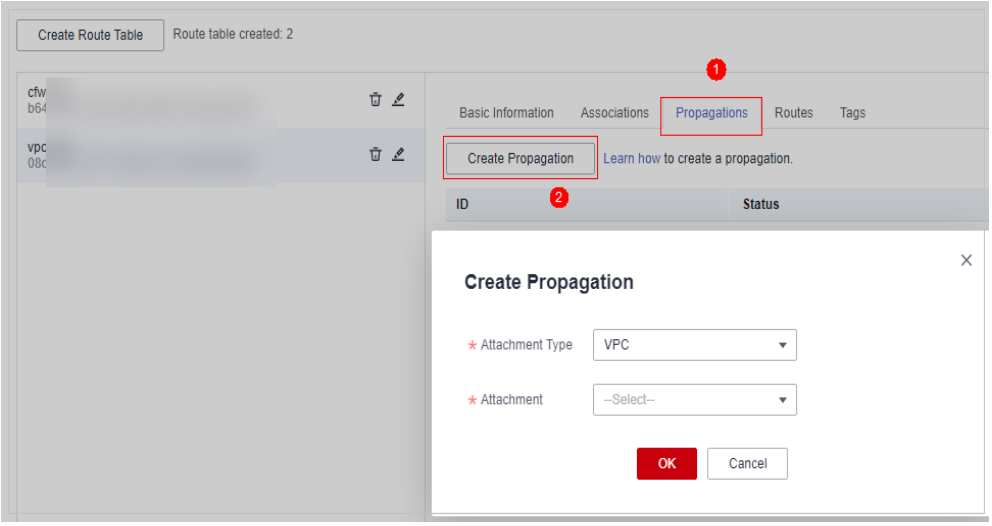


Table 5-6 Propagation parameters

Parameter	Description
Attachment Type	Select **VPC**.
Attachment	Select an item from the **Attachment** drop-down list.

NOTE

- Add at least two propagations. A propagation is required for each protected VPC you add.

  For example, select attachment **vpc-1** for VPC1 and **vpc-2** for VPC2. To add VPC3 for protection, add a propagation and select attachment **vpc-3**.
- After a propagation is created, its route information will be extracted to the route table of the enterprise router, and a propagation route will be generated. In the same route table, the destinations of different propagation routes may be the same, and cannot be modified or deleted.
- You can add static routes for the attachments in a route table. The destinations of static routes in a table must be unique, and can be modified or deleted.
- If a static route and a propagation route in the same route table happen to use the same destination, the static route takes effect first.

----End

5.2.4 Step 4: Modify VPC Route Tables

This section describes how to modify the route table of a protected VPC to direct the route to an enterprise router.

You need to modify the route tables of at least two VPCs. Each time a protected VPC is added, you need to add a route for that VPC.

Procedure

Step 1 In the service list, click **Virtual Private Cloud** under **Networking**. In the navigation pane, choose **Route Tables**.

Step 2 In the **Name/ID** column, click the route table name of a VPC. The **Summary** page is displayed.

Step 3 Click **Add Route**. For more information, see **Table 5-7**.

Table 5-7 Route parameters

Parameter	Description
Destination Type	Select **IP address**.
Destination	Destination CIDR block. **NOTE** The value cannot conflict with existing routes or subnet CIDR blocks in the VPC.
Next Hop Type	Select **Enterprise Router** from the drop-down list.
Next Hop	Select a resource for the next hop. The enterprise routers you created are displayed in the drop-down list.
Description	(Optional) Supplementary information about the route. **NOTE** Enter up to 255 characters. Angle brackets (< or >) are not allowed.

NOTE

You need to add routes for at least two VPCs. Each time a protected VPC is added, you need to add a route for that VPC.

----End

5.2.5 (Optional) Verifying Connectivity

Prerequisites

- You have completed configuration.
- Each of the two VPCs has an ECS.

Method

Ping ECSs in the VPC from each other to check whether they can properly communication when there is no traffic passing through the firewall.

Locating Faults

Step 1 Check whether the two route tables of the enterprise router are correctly configured. For details, see **Configuring Associations for a Route Table** and **Configuring Propagations for a Route Table**.

Step 2 Check whether the default route table of the VPC directs routes to the enterprise router.

Procedure

1. In the service list, click **Virtual Private Cloud** under **Networking**. In the navigation pane, choose **Route Tables**. In the **Name/ID** column, click the route table name of the VPC to be protected.

2. Check whether there is a route whose **Next Hop Type** is **Enterprise Router**. If there are no such routes, click **Add Route**. The following table describes the parameters.

Table 5-8 Route parameters

Parameter	Description
Destination Type	Select **IP address**.
Destination	Destination CIDR block. **NOTE** The value cannot conflict with existing routes or subnet CIDR blocks in the VPC.
Next Hop Type	Select **Enterprise Router** from the drop-down list.
Next Hop	Select a resource for the next hop. The enterprise routers you created are displayed in the drop-down list.
Description	(Optional) Supplementary information about the route. **NOTE** Enter up to 255 characters. Angle brackets (< or >) are not allowed.

----End

5.2.6 Step 5: Enable or Disable a VPC Border Firewall

A new firewall is disabled by default. Traffic passes through the enterprise router without being forwarded to the new firewall. You can enable or disable a VPC border firewall as needed.

Before enabling this function, you are advised to test the network connectivity. For details, see **(Optional) Verifying Connectivity**.

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

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

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

Step 6 Click **Enable Protection** to the right of **Firewall Status**.

Step 7 Click **OK**.

----End

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

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

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

Step 6 Click **Disable Protection** on the right of **Firewall Status**.

Step 7 Click **OK**. Your VPC will not be protected by the firewall.

----End

Follow-up Operations

- For details about how to add a protected VPC, see **(Optional) Adding a Protected VPC**.
- After the firewall is enabled, you need to configure inter-VPC protection rules. For details, see **Adding a VPC Border Protection Rule**.

5.2.7 (Optional) Adding a Protected VPC

After configuring a VPC border firewall, you can add a protected VPC.

Step 1: Add VPC Attachments

For details, see **Adding VPC Attachments to an Enterprise Router**.

NOTE

To use the enterprise router of account A to protect VPCs under account B, share the router with account B. For details, see **Creating a Sharing**.

Step 2: Configure Associations and Propagations

Step 1 In the service list, click **Enterprise Router** under **Networking**. Click **Manage Route Table**.

Step 2 Configure associations. On the route table configuration page, select the association table, click the **Associations** tab, and click **Create Association**. For more information, see **Table 5-9**.

Figure 5-9 Creating an association

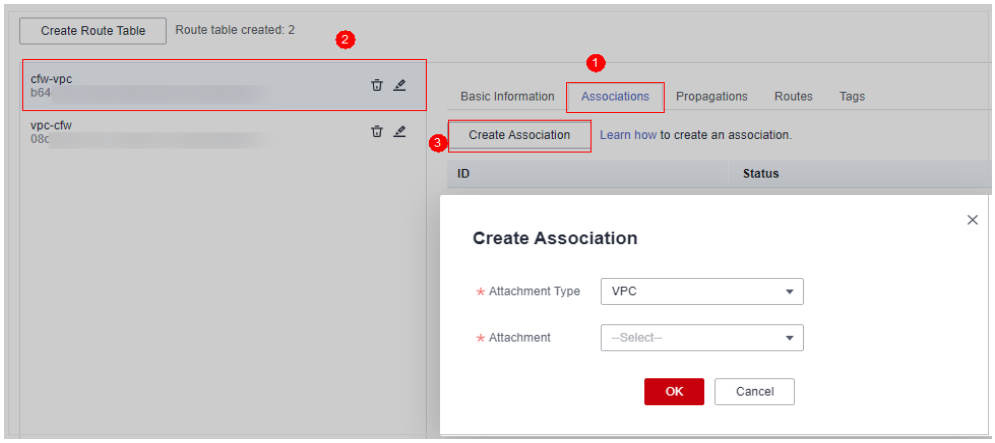


Table 5-9 Association parameters

Parameter	Description
Attachment Type	Select **VPC**.
Attachment	Select an item from the **Attachment** drop-down list.

NOTE

Add at least two associations. An association is required for each protected VPC you add.

For example, select attachment **vpc-1** for VPC1 and **vpc-2** for VPC2. To add VPC3 for protection, add an association and select attachment **vpc-3**.

Step 3 Configure propagations. Select the propagation route table, click the **Propagations** tab, and click **Create Propagation**. For more information, see **Table 5-10**.

Figure 5-10 Creating a propagation

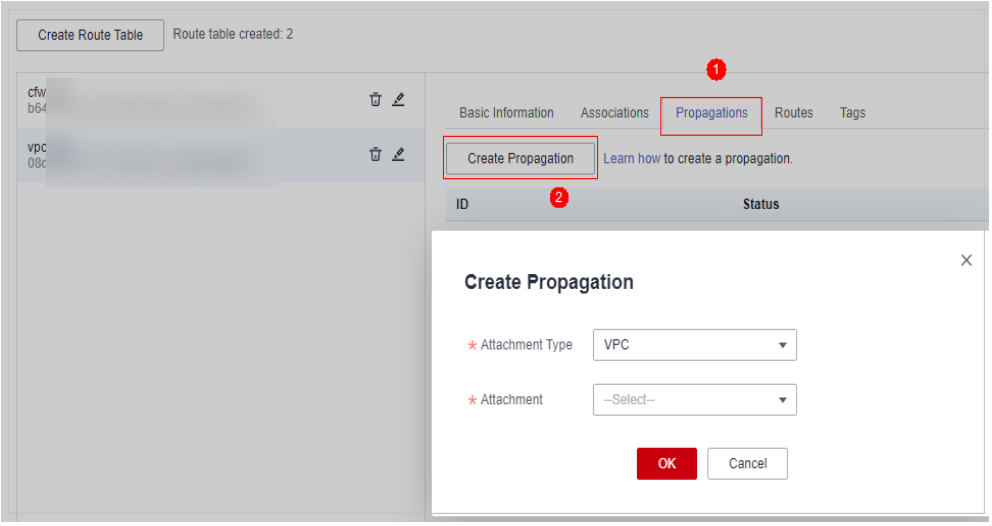


Table 5-10 Propagation parameters

Parameter	Description
Attachment Type	Select **VPC**.
Attachment	Select an item from the **Attachment** drop-down list.

NOTE

- Add at least two propagations. A propagation is required for each protected VPC you add.

  For example, select attachment **vpc-1** for VPC1 and **vpc-2** for VPC2. To add VPC3 for protection, add a propagation and select attachment **vpc-3**.
- After a propagation is created, its route information will be extracted to the route table of the enterprise router, and a propagation route will be generated. In the same route table, the destinations of different propagation routes may be the same, and cannot be modified or deleted.
- You can add static routes for the attachments in a route table. The destinations of static routes in a table must be unique, and can be modified or deleted.
- If a static route and a propagation route in the same route table happen to use the same destination, the static route takes effect first.

----End

Step 3: Modify VPC Route Tables

Step 1 In the service list, click **Virtual Private Cloud** under **Networking**. In the navigation pane, choose **Route Tables**.

Step 2 In the **Name/ID** column, click the route table name of a VPC. The **Summary** page is displayed.

Step 3 Click **Add Route**. For more information, see **Table 5-11**.

Table 5-11 Route parameters

Parameter	Description
Destination Type	Select **IP address**.
Destination	Destination CIDR block. **NOTE** The value cannot conflict with existing routes or subnet CIDR blocks in the VPC.
Next Hop Type	Select **Enterprise Router** from the drop-down list.
Next Hop	Select a resource for the next hop. The enterprise routers you created are displayed in the drop-down list.
Description	(Optional) Supplementary information about the route. **NOTE** Enter up to 255 characters. Angle brackets (< or >) are not allowed.

NOTE

You need to add routes for at least two VPCs. Each time a protected VPC is added, you need to add a route for that VPC.

----End

5.3 Enterprise Router Mode (Old)

5.3.1 Creating a VPC Border Firewall

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

Prerequisites

- You have an enterprise router.
- To create a VPC border firewall, you need to configure an inspection VPC that consumes a VPC protection quota for traffic diversion. The current account must have a VPC that does not transmit traffic and has no subnets associated, and the VPCs under the account can create at least 2 route tables.

Procedure

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

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

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

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

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

Step 6 Configure the subnets associated with the enterprise router and the cloud firewall, respectively. Click **Create Firewall**. Configure the enterprise router and associated subnets.

Figure 5-11 Creating a VPC border firewall (old version)

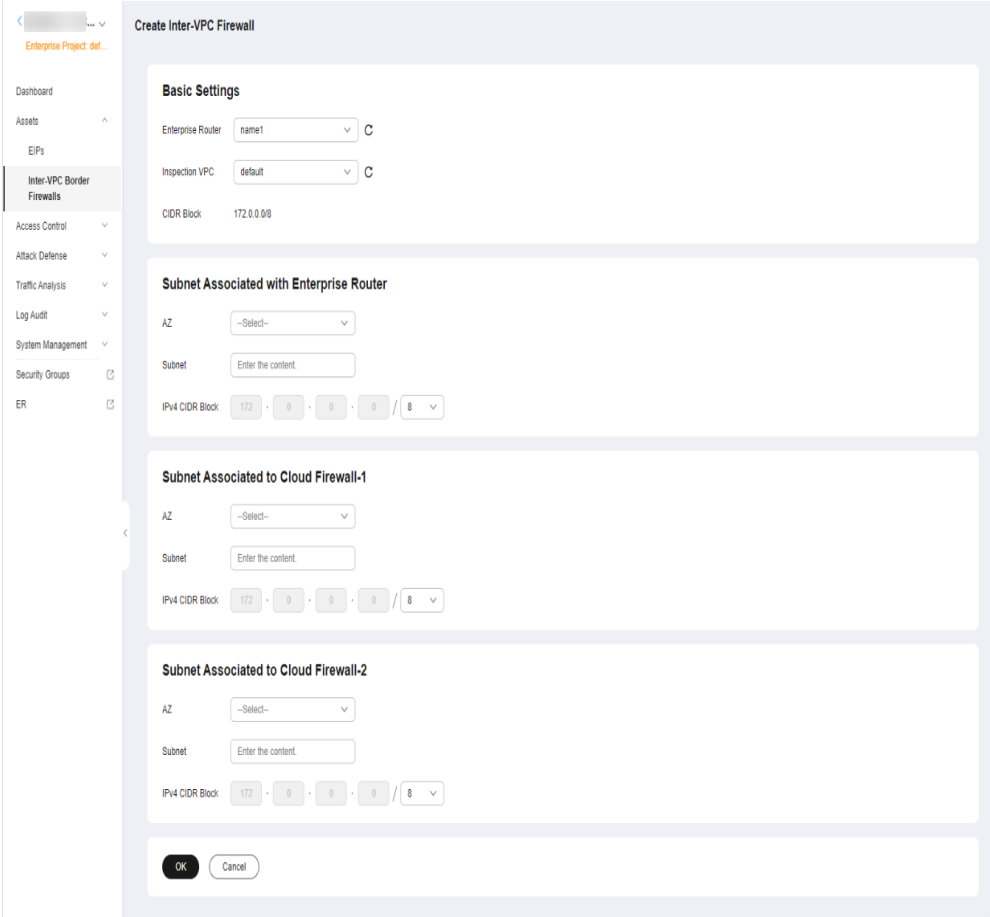


Table 5-12 Parameters for a VPC border firewall

Parameter	Description	Example Value
Enterprise Router	Select an enterprise router. For details, see **Viewing Enterprise Routers**.	cfw-er

Parameter	Description	Example Value
Inspection VPC	Select a VPC. The inspection VPC cannot use the network segments already specified in other VPCs associated with the enterprise router.	vpc-cfw-er
IPv4 Segment	After you select a VPC, the IPv4 address is automatically displayed.	xx.xx.0.0/16
AZ	Select an AZ.	AZ1
Subnet (Subnet Associated with Enterprise Router)	Subnet name.	cfw-er-1
Subnet (Subnet Associated to Cloud Firewall-1)		cfw-er-2
Subnet (Subnet Associated to Cloud Firewall-2)		cfw-er-3
IPv4 CIDR Block (Subnet Associated with Enterprise Router)	IPv4 CIDR Block **NOTE** • Ensure the value must not conflict with existing subnets. • Ensure the three subnet segments do not conflict with each other.	xx.xx.1.0/24
IPv4 CIDR Block (Subnet 1 Associated with a Cloud Firewall-1)		xx.xx.2.0/24
IPv4 CIDR Block (Subnet Associated to Cloud Firewall-2)		xx.xx.3.0/24

Step 7 Click **OK**. The firewall will be created in 3 to 5 minutes.

During the creation, you can only check the **Dashboard** page. The firewall status will change to **Upgrading**.

----End

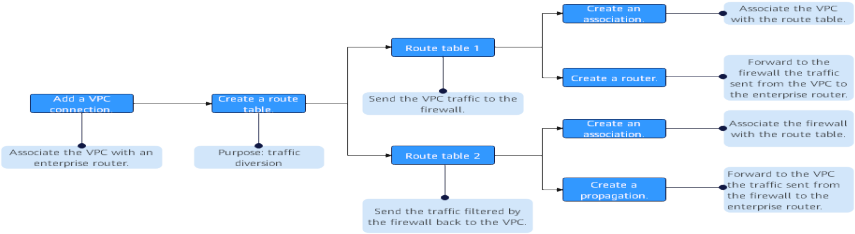
5.3.2 Configuring an Enterprise Router

This section describes how to associate a firewall with an enterprise router and configure traffic diversion.

How to Configure

The process of configuring an enterprise router is as follows.

Figure 5-12 Process of configuring an enterprise router



Prerequisites

A firewall has been created.

Constraints

- **Default Route Table Association**, **Default Route Table Propagation**, and **Auto Accept Shared Attachments** must be disabled.
- Only the professional edition supports inter-VPC firewall 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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

Step 6 Choose **Configure Enterprise Router**. On the displayed page, add attachments to an enterprise router. For details about the attachment types that can be added, see **Attachment Overview**.

Assume you want to protect two VPCs. (At least two VPC attachments are required to connect the two VPCs to the enterprise router.) For details, see **Adding VPC Attachments to an Enterprise Router**.

NOTE

- Add at least three connections, for example, the firewall connection **cfw-er-auto** (automatically generated after the firewall is created), the VPC1 connection **vpc-1**, and the VPC2 connection **vpc-2**.
- To use the enterprise router of account A to protect VPCs under account B, share the router with account B. For details, see **Creating a Sharing**.

Step 7 Create two route tables to connect to the firewall and the VPC to be protected, respectively.

Click the **Route Tables** tab. Click **Create Route Table**.

Create a route table, as shown in **Figure 5-13**. For more information, see **Route table parameters**.

Figure 5-13 Creating a route table

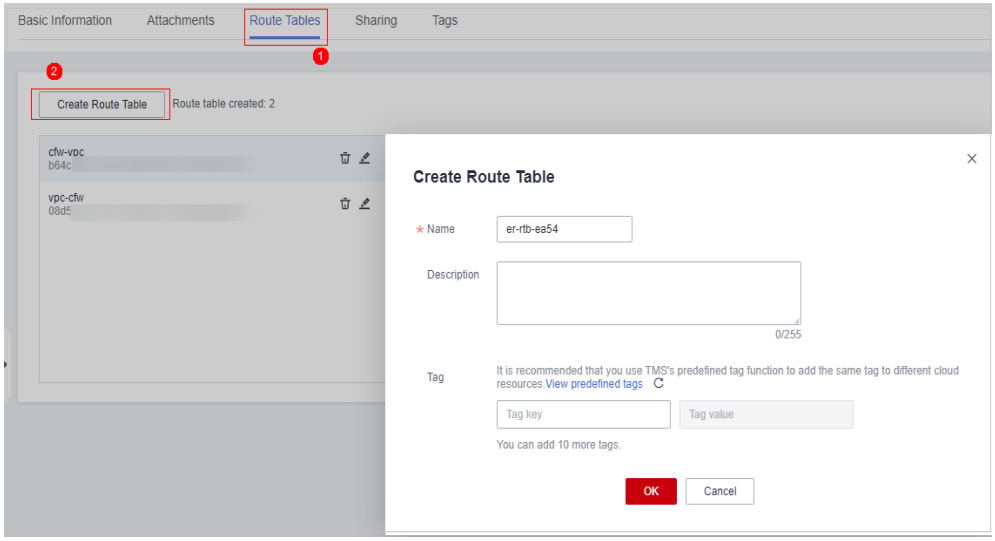


Table 5-13 Route table parameters

Parameter	Description	Example Value
Name	Route table name. It must meet the following requirements: ● Must contain 1 to 64 characters. ● Can contain letters, digits, underscores (_), hyphens (-), and periods (.).	er-rlb-4cd1
Description	Route table description	-
Tag	During the route table creation, you can tag the route table resources. Tags identify cloud resources for purposes of easy categorization and quick search. For details about tags, see **Tag Overview**.	-

Step 8 Configure the association and routing.

1. Select the route table to be connected to the VPC. Click the **Associations** tab and click **Create Association**.

   For more information, see **Association parameters**.

Figure 5-14 Creating an association

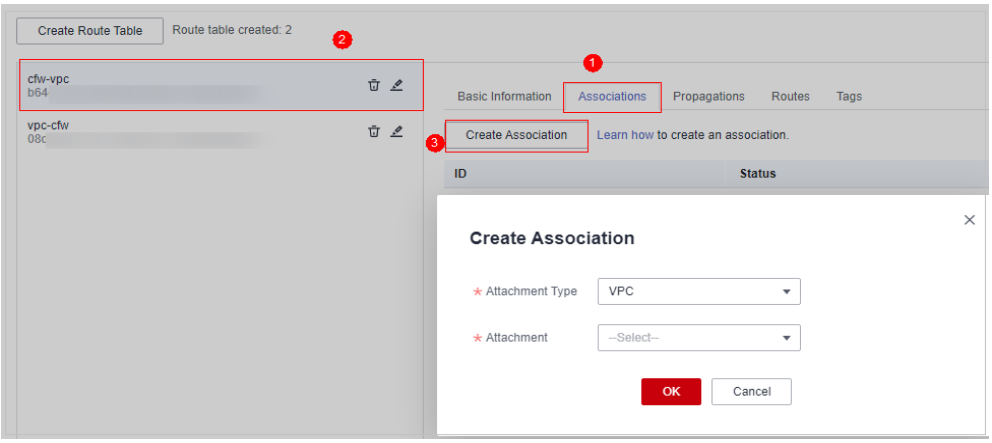


Table 5-14 Association parameters

Parameter	Description	Example Value
Attachment Type	Select **VPC**.	VPC

Parameter	Description	Example Value
Attachment	Select an item from the **Attachment** drop-down list.	er-attach-01

2. Create a route for the route table. Click the **Routes** tab and click **Create Route**. You can create one or more routes as needed.

   Create a route table, as shown in **Figure 5-15**. For more information, see **Route parameters**.

Figure 5-15 Creating a route

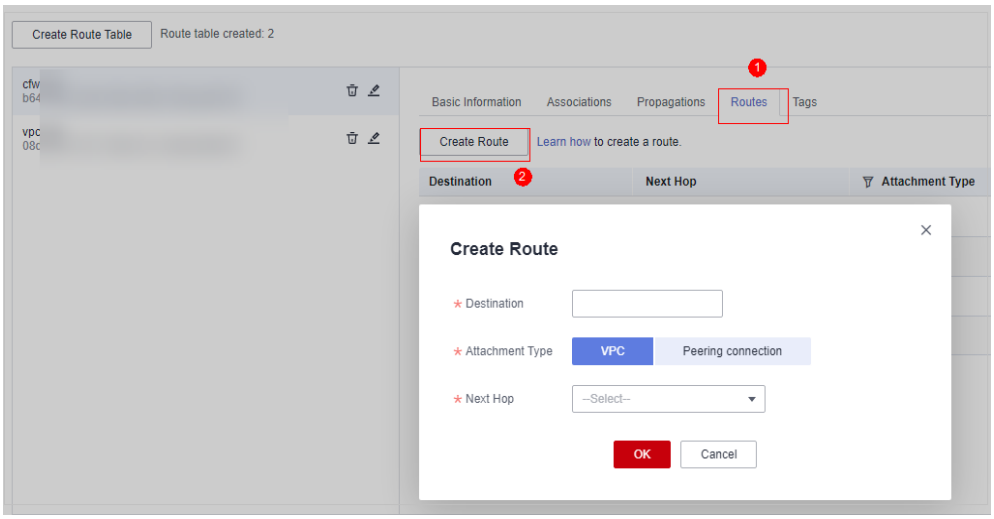


Table 5-15 Route parameters

Parameter	Description	Example Value
Destination	Set the destination address. It can be a VPC CIDR block or subnet CIDR block. **NOTE** If your ECS is bound to an EIP, you need to specify the network segment when configuring the route. The value **0.0.0.0/0** is not allowed.	192.168.2.0/24
Attachment Type	Select **VPC**.	VPC
Next Hop	Select the VPC attachment of the firewall.	er-Inspection

Step 9 Configure the association and propagation.

1. Select the route table to be connected to the firewall. Click the **Associations** tab and click **Create Association**.

   For more information, see **Association parameters**.

Figure 5-16 Creating an association

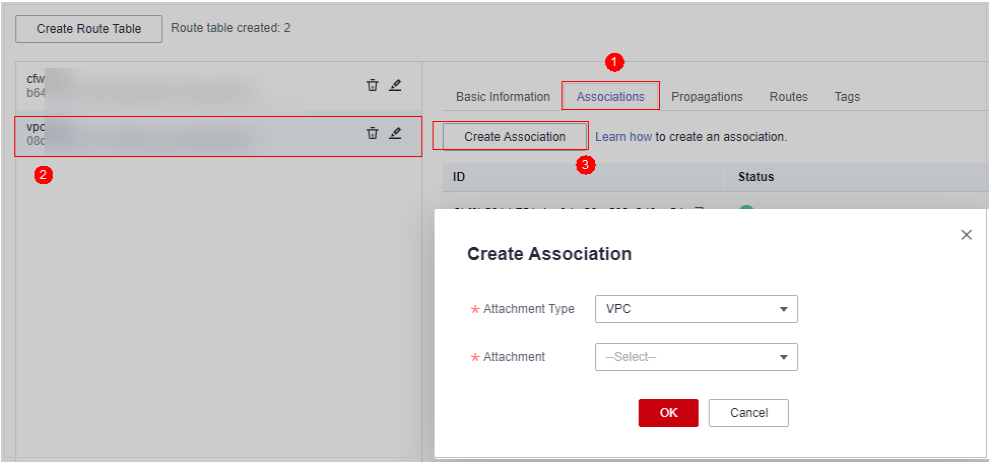


Table 5-16 Association parameters

Parameter	Description	Example Value
Attachment Type	Select **VPC**.	VPC
Attachment	Select an item from the **Attachment** drop-down list.	er-Inspection

2. Create a propagation for the route table. Click the **Propagations** tab and click **Create Propagation**.

   For more information, see **Propagation parameters**.

Figure 5-17 Creating a propagation

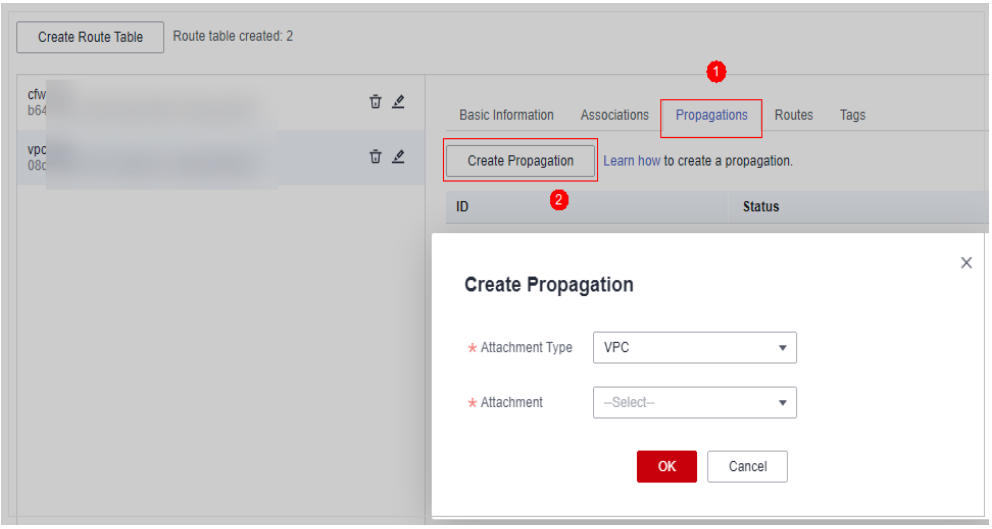


Table 5-17 Propagation parameters

Parameter	Description	Example Value
Attachment Type	Select **VPC**.	VPC
Attachment	Select an item from the **Attachment** drop-down list.	er-attach-02

NOTE

- After a propagation is created, its route information will be extracted to the route table of the enterprise router, and a propagation route will be generated. In the same route table, the destinations of different propagation routes may be the same, and cannot be modified or deleted.
- You can add static routes for the attachments in a route table. The destinations of static routes in a table must be unique, and can be modified or deleted.
- If a static route and a propagation route in the same route table happen to use the same destination, the static route takes effect first.

----End

Verifying Configurations

Prerequisites

- You have completed configuration.
- Each of the two VPCs has an ECS.

Method

Ping ECSs in the VPC from each other to check whether they can properly communication if there is no traffic passing through the firewall.

Troubleshooting

Step 1 Check whether the two route tables of the enterprise router are correctly configured. For details, see **Step 8** and **Step 9**.

Step 2 Check whether the default route table of the VPC directs routes to the enterprise router.

Procedure

1. In the service list, click **Virtual Private Cloud** under **Networking**. In the navigation pane, choose **Route Tables**. In the **Name/ID** column, click the route table name of the VPC to be protected.

2. Check whether there is a route whose **Next Hop Type** is **Enterprise Router**. If there are no such routes, click **Add Route**. The following table describes the parameters.

Table 5-18 Route parameters

Parameter	Description	Example Value
Destination	Destination CIDR block. A route destination must be unique, and cannot overlap with any subnets in the VPC. **NOTE** The value cannot conflict with existing routes or subnet CIDR blocks in the VPC.	192.168.0.0/16
Next Hop Type	Select **Enterprise Router** from the drop-down list.	Enterprise Router
Next Hop	Select a resource for the next hop. Only the resources of the next hop type you selected are displayed in the drop-down list.	er-01
Description	(Optional) Supplementary information about the route. **NOTE** Enter up to 255 characters. Angle brackets (< or >) are not allowed.	-

----End

5.3.3 Enabling or Disabling a VPC Border Firewall

A new firewall is disabled by default. Traffic passes through the enterprise router without being forwarded to the new firewall. You can enable or disable a VPC border firewall as needed.

Prerequisites

- You have purchased the CFW professional edition.
- You have configured an enterprise router.

Constraints

- Only the professional edition supports inter-VPC firewall 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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

Step 6 In the **Operation** column, click **Enable Protection** or **Disable Protection**.

----End

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

Prerequisites

You have synchronized assets and enabled EIP protection. See **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.
- Up to 20 source/destination IP addresses can be added to a protection rule.
- 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 198.19.0.0/16 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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

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
Rule Type	Protection type of a rule. • **EIP**: Protect EIP traffic. Only EIPs can be configured. • **NAT**: Protect NAT traffic. Private IP addresses can be configured. **NOTE** • Only the professional edition supports the configuration of rule types. • To configure **NAT**, ensure that: – The professional edition has been enabled. For more information, see **Upgrading an Edition**. – The VPC border firewalls have been configured. For details, see **Managing VPC Border Firewalls**.	EIP protection
Name	Name of the custom security policy.	test
Direction	Select a traffic direction if the protection rule is set to **EIP**. • **Inbound**: Traffic from external networks to the internal server. • **Outbound**: Traffic from internal servers to external networks.	Inbound
Source	Source address of access traffic. • **IP address** can be configured in the following formats: – A single IP address, for example, **192.168.10.5** – Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** – Address segment, for example, **192.168.2.0/24** • IP address group: A collection of IP addresses. For details about how to add custom IP address groups, see **Adding Custom IP Address Groups**. For details about how to add a predefined address group, see **Viewing a Predefined Address Group**. **NOTE** If **Direction** is set to **Inbound**, a predefined address group can be configured for the source address. • **Countries and regions**: If **Direction** is set to **Inbound**, you can control access based on continents, regions, and countries. • **Any**: any source address	**IP address, 192.168.10.5**

Parameter	Description	Example Value
Destination	Destination address of access traffic. • **IP address**: You can set a single IP address, consecutive IP addresses, or an IP address segment. – A single IP address, for example, **192.168.10.5** – Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** – Address segment, for example, **192.168.2.0/24** • **IP address group**: A collection of IP addresses. For details about how to add custom IP address groups, see **Adding an IP Address Group**. • **Countries and regions**: If **Direction** is set to **Outbound**, you can control access based on continents, regions, countries. • **Domain name/Domain name group**: When **Direction** is set to **Outbound**, the protection of the domain name or domain name group is supported. – **Application**: Supports the protection for domain names or wildcard domain names. Application-layer protocols such as HTTP and HTTPS are supported. Domain names are used for matching. – **Network**: Supports protection for one or multiple domain names. Applies to network-layer protocols and supports all protocols. The resolved IP addresses are used for matching.	Any

Parameter	Description	Example Value
	NOTE – To protect the domain names of HTTP and HTTPS applications, you can select any options. – To protect the wildcard domain names of HTTP and HTTPS applications, select **Application** and then select any option from the drop-down list. – To protect a single domain name of other application types (such as FTP, MySQL, and SMTP), select **Network** and select any option from the drop-down list. (If **Application Domain Name Group** is selected, up to 600 IP addresses can be resolved.) – To protect multiple domain names of other application types (such as FTP, MySQL, and SMTP), select **Network** and **Network Domain Group** from the drop-down list. – If you need to configure the wildcard domain names or application domain name groups of the HTTP/HTTPS applications, and the network domain groups of other application types for the same domain name, ensure that the priority of the **Network** protection rule is higher than that of the **Application** protection rule. – For details about application and network types, see **Adding a Domain Name Group**. ● **Any**: any destination address	
Service	● **Service**: Set **Protocol Type**, **Source Port**, and **Destination Port**. – **Protocol Type**: The value can be TCP, UDP, or ICMP. – **Source/Destination Port**: If **Protocol Type** is set to **TCP** or **UDP**, you need to set the port number. **NOTE** – To specify all the ports of an IP address, set **Port** to **1-65535**. – You can specify a single port. For example, to manage access on port 22, set **Port** to **22**. – 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 **Port** to **80-443**. ● **Service group**: A collection of services (protocols, source ports, and destination ports) is supported. For details about how to add a custom service group, see **Adding a Service Group**. For details about a pre-defined service group, see **Viewing a Predefined Service Group**. ● **Any**: any protocol type or port number	**Service** **Protocol Type**: **TCP** **Source Port**: **80** **Destination Port**: **80-443**

Parameter	Description	Example Value
Action	Set the action to be taken when traffic passes through the firewall. ● **Allow**: Traffic is forwarded. ● **Block**: Traffic is not forwarded.	Allow
Allow Long Connection	If only one service is configured in the current protection rule and **Protocol Type** is set to **TCP** or **UDP**, you can configure the service session aging time. ● **Yes**: Configure the long connection duration. ● **No**: Retain the default durations. The default connection durations for different protocols are as follows: – TCP: 1800s – UDP: 60s **NOTE** Up to 100 rules can be configured with long connections.	Yes
Long Connection Duration	This parameter is mandatory if **Allow Long Connection** is set to **Yes**. Configure the long connection duration. Configure the hour, minute, and second. **NOTE** 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: ● **Pin on top**: indicates that the priority of the policy is set to the highest. ● **Lower than the selected rule**: indicates that the policy priority is lower than a specified rule.	Pin on top
Status	Whether a policy is enabled. : enabled : disabled	
Description	(Optional) Usage and application scenario	-

Step 7 Click **OK** to complete the protection rule configuration.

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

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

Step 5 In the navigation pane, choose **Access Control** > **Access Policies**. 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 address of access traffic. • **IP address**: You can set a single IP address, consecutive IP addresses, or an IP address segment. – A single IP address, for example, **192.168.10.5** – Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** – Address segment, for example, **192.168.2.0/24** • **IP address group**: A collection of IP addresses. For details, see Adding an IP Address Group. • **Any**: any source address	**IP address, 192.168.10.5**

Parameter	Description	Example Value
Destination	Destination address of access traffic. ● **IP address**: You can set a single IP address, consecutive IP addresses, or an IP address segment. – A single IP address, for example, **192.168.10.5** – Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** – Address segment, for example, **192.168.2.0/24** ● **IP address group**: A collection of IP addresses. For details, see **Adding an IP Address Group**. ● **Any**: any destination address	Any
Service	Set the protocol type and port number of the access traffic. ● **Service**: Set **Protocol Type**, **Source Port**, and **Destination Port**. – **Protocol Type**: The value can be **TCP**, **UDP**, or **ICMP**. – **Source/Destination Port**: If **Protocol Type** is set to **TCP** or **UDP**, you need to set the port number. **NOTE** – To specify all the ports of an IP address, set **Port** to **1-65535**. – You can specify a single port. For example, to manage access on port 22, set **Port** to **22**. – 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 **Port** to **80-443**. ● **Service group**: A collection of services (protocols, source ports, and destination ports) is supported. For details about how to add a custom service group, see **Adding a Custom Service Group**.For details about predefined service groups, see . ● **Any**: any protocol type or port number	**Service** **Protocol Type**: **TCP** **Source Port**: **80** **Destination Port**: **80-443**
Action	Set the action to be taken when traffic passes through the firewall. ● **Allow**: Traffic is forwarded. ● **Block**: Traffic is not forwarded.	Allow

Parameter	Description	Example Value
Allow Long Connection	If only one service is configured in the current protection rule and **Protocol Type** is set to **TCP** or **UDP**, you can configure the service session aging time. ● **Yes**: Configure the long connection duration. ● **No**: Retain the default durations. The default connection durations for different protocols are as follows: – TCP: 1800s – UDP: 60s **NOTE** Up to 100 rules can be configured with long connections.	Yes
Long Connection Duration	This parameter is mandatory if **Allow Long Connection** is set to **Yes**. Configure the long connection duration. Configure the hour, minute, and second. **NOTE** 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: ● **Pin on top**: indicates that the priority of the policy is set to the highest. ● **Lower than the selected rule**: indicates that the policy priority is lower than a specified rule. **NOTE** 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** to complete the protection rule configuration.

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 6-1**. Its priority is the lowest. The other allows the traffic of a specified IP address, as shown in **Figure 6-2**. Its priority is the highest.

Figure 6-1 Blocking all traffic

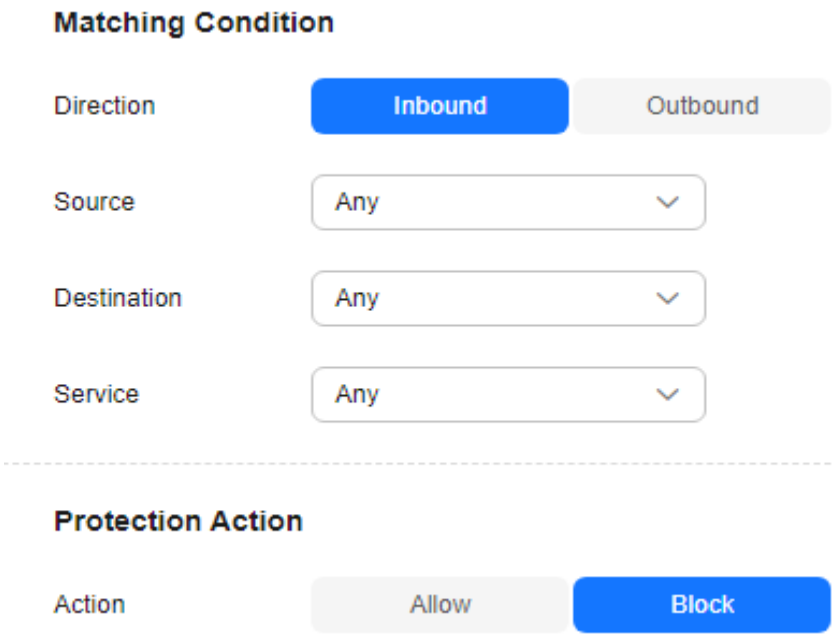
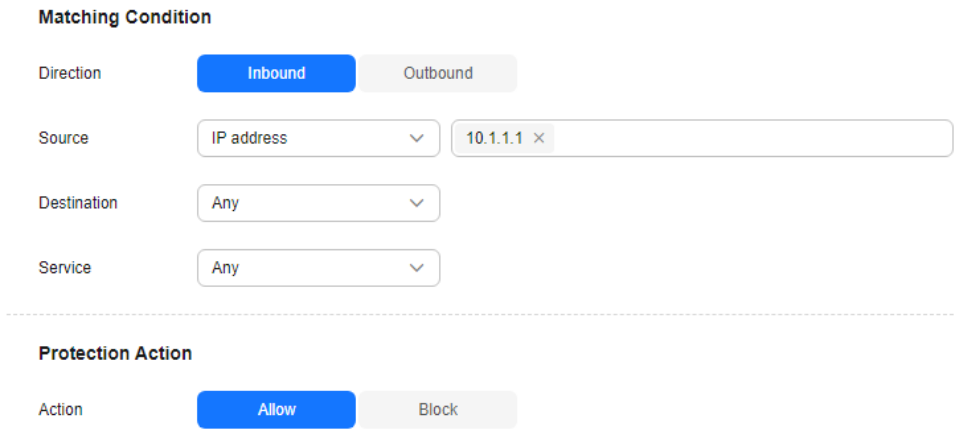


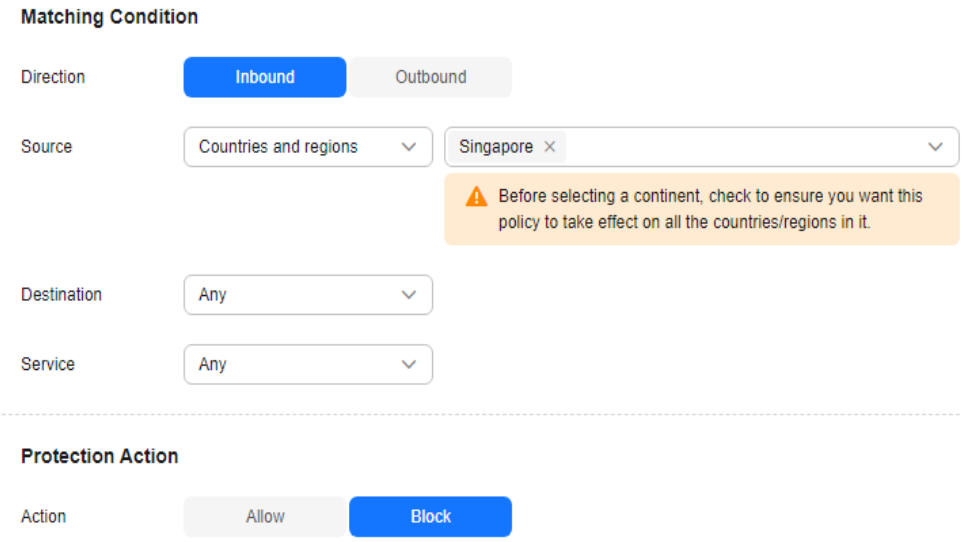
Figure 6-2 Allowing a specified IP address



Configuration Example - Blocking Access from a Region

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

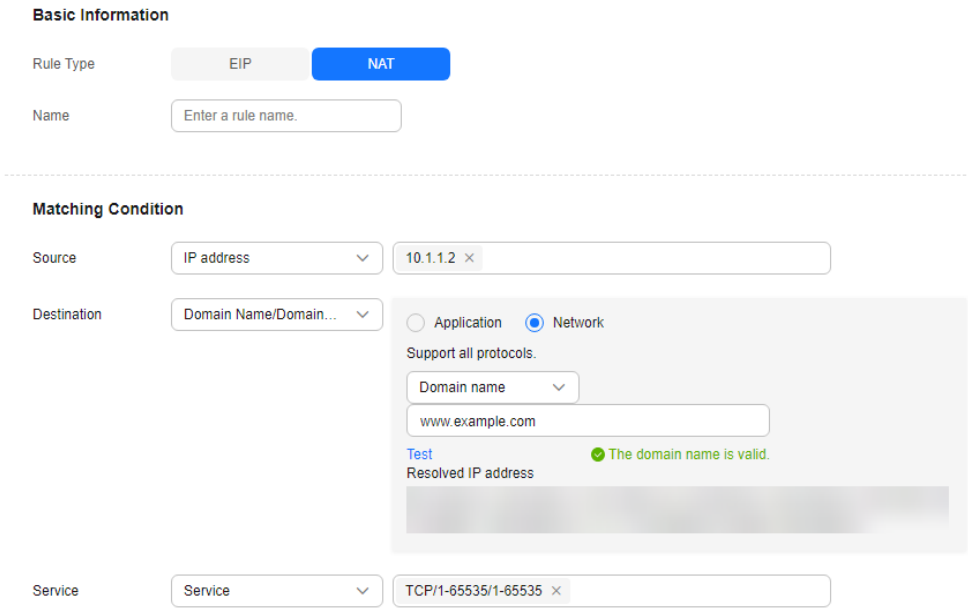
Figure 6-3 Intercepting the access traffic from Singapore



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 6-4 Configuring a NAT protection rule



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

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

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

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

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.
- The priority of the imported policies is lower than that of the created policies.

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

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

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

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

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. • **EIP protection**: Protect EIP traffic. Only EIPs can be configured. • **NAT protection**: Protect NAT traffic. Private IP addresses can be configured.	EIP protection
Direction	Direction of protected traffic. • **Inbound**: Traffic from external networks to the internal server. • **Outbound**: Traffic from the customer server to external networks.	Outbound
Action Type	**Allow** or **Block**. It specifies the action taken by the firewall to process traffic.	Allow
ACL Address Type	Select **IPv4**. It is the type of IP addresses to be protected.	IPv4

Parameter	Description	Example Value
Status	Whether a policy is enabled. ● **Enable**: The rule is enabled. ● **Disabled**: The rule is not in effect.	Enabled
Description	Rule description	test
Source Address Type	Source address type of data packets in the access traffic. ● **IP Address**. You can configure a single IP address, consecutive IP addresses, or an IP address segment. ● **IP Address Group**. You can configure multiple IP addresses. ● **Region**: Protection can be performed by region.	IP Address
Source Address	If **Source Address Type** is set to **IP Address**, you need to configure this parameter. The following input formats are supported: ● A single IP address, for example, **192.168.10.5** ● Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** ● Address segment, for example, **192.168.2.0/24**	192.168.10.5
Source Address Group Name	If **Source Address Type** is set to **IP Address Group**, you must configure this parameter. The following input formats are supported: ● The value can contain letters, digits, underscores (_), hyphens (-), or spaces. ● The name can contain up to 255 characters.	s_test
Source Continent Region	If **Source Address Type** is set to **Region**, you need to configure **Source Continent Region**. Enter the continent information according to the **continent-region-info** sheet of the template table.	AS: Asia
Source Country Region	If **Source Address Type** is set to **Region**, you need to configure **Source Country Region**. Enter the country information according to the **country-region-info** sheet of the template table.	CN: Chinese mainland

Parameter	Description	Example Value
Destination Address Type	Destination address type of data packets in the access traffic. ● **IP Address**. You can configure a single IP address, consecutive IP addresses, or an IP address segment. ● **IP Address Group**. You can configure multiple IP addresses. ● **Domain name**: 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. ● **Domain name group**. You can set a collection of domain names. ● **Region**: Protection can be performed by region.	IP Address Group
Destination Address	If **Destination Address Type** is set to **IP Address**, you must configure this parameter. It can be: ● A single IP address, for example, **192.168.10.5** ● Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** ● Address segment, for example, **192.168.2.0/24**	192.168.10.6
Destination Address Group Name	If **Destination Address Type** is set to **IP Address Group**, you must configure this parameter. The following input formats are supported: ● The value can contain letters, digits, underscores (_), hyphens (-), or spaces. ● The name can contain up to 255 characters.	d_test
Destination Continent Region	If **Destination Address Type** is set to **Region**, you need to set **Destination Continent Region**. Enter the continent information according to the **continent-region-info** sheet of the template table.	AS: Asia

Parameter	Description	Example Value
Destination Country Region	If **Destination Address Type** is set to **Region**, you need to set **Destination Country Region**. Enter the country information according to the **country-region-info** sheet of the template table.	CN: Chinese mainland
Domain Name	If **Destination Address Type** is set to **Domain Name**, 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 **Destination Address Type** is set to **Domain Group Name**, you need to configure **Destination Domain Group Name**. Enter a domain group name.	Domain group 1
Service Type	Service type. It can be: ● **Service**. You can configure a single service. ● **Service Group**. You can configure multiple services.	Service
Protocol/ Source Port/ Destination Port	Type to be put under access control. ● Its value can be **TCP**, **UDP**, **ICMP**, or **Any**. ● Source ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: **80-443**). ● Destination ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: **80-443**).	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	**Allow** or **Block**. It specifies the action taken by the firewall to process traffic.	Allow
Status	Whether a policy is enabled. ● **Enabled**: The rule is in effect. ● **Disabled**: The rule is not in effect.	Enabled
Description	Rule description	test
Source Address Type	Source address type of data packets in the access traffic. ● **IP Address**. You can configure a single IP address, consecutive IP addresses, or an IP address segment. ● **IP Address Group**. You can configure multiple IP addresses.	IP Address
Source Address	If **Source Address Type** is set to **IP Address**, you need to configure this parameter. The following input formats are supported: ● A single IP address, for example, **192.168.10.5** ● Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** ● Address segment, for example, **192.168.2.0/24**	192.168.10.5
Source Address Group Name	If **Source Address Type** is set to **IP Address Group**, you must configure this parameter. The following input formats are supported: ● The value can contain letters, digits, underscores (_), hyphens (-), or spaces. ● The name can contain up to 255 characters.	s_test

Parameter	Description	Example Value
Destination Address Type	Destination address type of data packets in the access traffic. ● **IP Address**. You can configure a single IP address, consecutive IP addresses, or an IP address segment. ● **IP Address Group**. You can configure multiple IP addresses.	IP Address Group
Destination Address	If **Destination Address Type** is set to **IP Address**, you must configure this parameter. It can be: ● A single IP address, for example, **192.168.10.5** ● Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** ● Address segment, for example, **192.168.2.0/24**	192.168.10.6
Destination Address Group Name	If **Destination Address Type** is set to **IP Address Group**, you must configure this parameter. The following input formats are supported: ● The value can contain letters, digits, underscores (_), hyphens (-), or spaces. ● The name can contain up to 255 characters.	d_test
Service Type	Service type. It can be: ● **Service**. You can configure a single service. ● **Service Group**. You can configure multiple services.	Service
Protocol/ Source Port/ Destination Port	Type to be put under access control. ● Its value can be **TCP**, **UDP**, **ICMP**, or **Any**. ● Source ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: **80-443**). ● Destination ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: **80-443**).	TCP/443/443

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

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

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

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.

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 about the back-to-source IP addresses, see **What Are Back-to-Source IP Addresses?**
- For details about how to configure protection rules, see **Adding a Protection Rule**.

Specification Limitations

The CFW blacklist and whitelist each allows up to 2,000 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 **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 **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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation pane, choose **Access Control** > **Access Policies**. 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 **Source** or **Destination**. ● **Source**: The IP address or IP address group that sends data packets. ● **Destination**: The destination IP address or IP address group that receives data packets.
Protocol Type	Its value can be **TCP**, **UDP**, **ICMP**, or **Any**.
Port	If **Protocol Type** is set to **TCP** or **UDP**, set the ports to be allowed or blocked. **NOTE** ● To specify all the ports of an IP address, set **Port** to **1-65535**. ● You can specify a single port. For example, to allow or block the access from port 22 of an IP address, set **Port** to **22**. ● 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 **Port** to **80-443**.
Description	Description of the blacklist or whitelist
IP Addresses	● User-defined IP address: Enter one or more IP addresses in the text box and click **Parse** to add the IP addresses to the list. ● Pre-defined address group: Click **Add Pre-defined IP Address Group**. In the dialog box that is displayed, select an address group. For more information, see **Viewing a Predefined Address Group**. **CAUTION** After **WAF_Back-to-Source_IP_Addresses** is added to the blacklist or whitelist, if a back-to-source IP address changes, you need to manually update it in 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 on the left, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation pane, choose **Access Control** > **Access Policies**. 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 **Source** or **Destination**. ● **Source**: The IP address or IP address group that sends data packets. ● **Destination**: The destination IP address or IP address group that receives data packets.
Protocol Type	Its value can be **TCP**, **UDP**, **ICMP**, or **Any**.
Port	If **Protocol Type** is set to **TCP** or **UDP**, set the ports to be allowed or blocked. **NOTE** ● To specify all the ports of an IP address, set **Port** to **1-65535**. ● You can specify a single port. For example, to allow or block the access from port 22 of an IP address, set **Port** to **22**. ● 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 **Port** to **80-443**.
Description	Description of the blacklist or whitelist
IP Addresses	● User-defined IP address: Enter one or more IP addresses in the text box and click **Parse** to add the IP addresses to the list. ● Pre-defined address group: Click **Add Pre-defined IP Address Group**. In the dialog box that is displayed, select an address group. For more information, see **Viewing a Predefined Address Group**. **CAUTION** After **WAF_Back-to-Source_IP_Addresses** is added to the blacklist or whitelist, if a back-to-source IP address changes, you need to manually update it in 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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

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.

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

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

Step 5 In the navigation 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: ● Only uppercase letters (A to Z), lowercase letters (a to z), numbers (0 to 9), and the following special characters are allowed: -_ ● The length cannot exceed 255 characters.
Description	Usage and application scenario of a rule It must meet the following requirements: ● Only letters (A to Z and a to z), numbers (0 to 9), spaces, and the following characters are allowed: -_ ● The length cannot exceed 255 characters.
IP Addresses	Enter IP addresses and click **Parse** to add them to the IP address list. 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.

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

----End

Follow-up Operations

- After an address group is added, if you need to add IP addresses, see **Adding an IP Address**.
- An IP address group takes effect only after it is set in a protection rule. For more information, see **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 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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation 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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation 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.

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.

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

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

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

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

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

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

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

Table 6-8 Service group parameters

Parameter	Description
Service Group Name	Name of a service group
Description	Usage and application scenario
Services	• **Protocol**: Select a protocol. Supported protocols include TCP, UDP, and ICMP. • **Source Port**: Set the source port to be allowed or blocked. You can configure a single port or consecutive port groups (example: **80-443**). • **Destination Port**: Set the destination port to be allowed or blocked. You can configure a single port or consecutive port groups (example: **80-443**). • **Description**: Usage and application scenario of the service group

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

----End

Follow-up Operations

- If you need to add protocols or ports after adding a service group, see **Adding a Service**.
- A service group takes effect only after it is set in a protection rule. For more information, see **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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation pane, choose **Access Control** > **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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

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

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

Table 6-9 Service parameters

Parameter Name	Description	Example Value
Protocol	Its value can be **TCP**, **UDP**, or **ICMP**.	TCP
Source Port	Source ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: **80-443**).	80
Destination Port	Destination ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: **80-443**).	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 custom 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 on the left, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

WARNING

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:

- **Application Domain Name Group**: Supports the protection for domain names or wildcard domain names. Application-layer protocols such as HTTP/HTTPS are supported. Domain names are used for matching.
- **Network Domain Name Group**: Supports protection for one or multiple domain names. Applies to network-layer protocols and supports all protocols. The resolved IP addresses are used for matching.

Matching Policy

- **Application Domain Name Group**: CFW compares the HOST field in sessions with the application domain names. If they are consistent, the corresponding protection rule is hit.
- **Network Domain Name Group**: CFW obtains the IP addresses resolved by DNS every 15 seconds, if the four-tuple of a session matches the network domain name rule and the resolved address has been saved (that is, the IP address has been obtained from the DNS server), the corresponding protection rule is hit.

  A single domain name can resolve up to 1,000 IP addresses. Each domain group can resolve up to 1,500 IP addresses. If the number of resolution results reaches the upper limit, no domain names can be added to the domain group.

NOTE

You are advised to use the application domain name group (for example, the domain name accelerated by CDN) for the domain names that have a large number of mapping addresses or rapidly changing mapping results.

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.

Application Domain Name Group (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.

Network Domain Name Group (Layer 4 Protocol Parsing)

- A domain name group can have up to 15 domain names.
- Each domain name can resolve up to 1,000 IP addresses.
- Each domain name group can resolve up to 1,500 IP addresses.
- A firewall instance can have up to 1,000 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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

Step 6 (Optional) To add a network domain group, click the **Network Domain Name Group** tab.

Step 7 Click **Add Domain Name Group** and configure **parameters**.

Table 6-10 Domain name group parameters

Parameter	Description
Group Name	Name of a user-defined domain name group.
Domain Name Group Type	Application/Network
Description	(Optional) Enter remarks for the domain name group.

Parameter	Description
Domain Name	Enter one or multiple domain names. ● You can enter a multi-level single domain name (for example, top-level domain name **example.com** and level-2 domain name **www.example.com**) or a wildcard domain name (***.example.com**). ● Multiple domain names are separated by commas (,), semicolons (;), line breaks, or spaces. **NOTE** Domain names must be unique.

----End

Related Operation

- To edit a domain name group, click the name of the target domain name group and click **Edit** on the right of **Basic Information**.
- A domain name group takes effect only after it is set in a protection rule. For more information, see **Adding a Protection Rule**.
- To view the IP addresses resolved by a domain name group of the network domain name group 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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

Step 6 (Optional) To delete a network domain group, click the **Network Domain Name Group** tab.

Step 7 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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation pane, choose **Access Control** > **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 6-11**. You can click a record to view policy matching details. For more information, see **Table 12-2**.

Table 6-11 Policy assistant statistics parameters

Parameter	Description
Top Policies By Hits	Policies that match and block traffic.

Parameter	Description
Top Blocked Outbound IP Addresses	Blocked outbound IP addresses. You can click **Source** or **Destination** to view the source or destination IP addresses.
Top Blocked Inbound IP Addresses	Blocked inbound IP addresses. You can click **Source** or **Destination** to view the source or destination IP addresses.
Top Blocked Destination Ports	Blocked destination ports. You can click **Outbound** or **Inbound** to view ports in the corresponding direction.
Top Blocked IP Address Regions	Regions of blocked IP addresses. You can click **Destination of outbound access** or **Source of inbound access** 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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

Table 6-12 Protection rule parameters

Parameter	Description
Priority	Priority of the rule. **NOTE** A smaller value indicates a higher priority.
Name/Rule ID	Custom rule name and ID
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	• Its value can be **TCP**, **UDP**, **ICMP**, or **Any**. • Source Port: Source ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: **80-443**). • Destination Port: Destination ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: **80-443**).
Action	• **Allow**: Allow the traffic to pass through the firewall. • **Block**: Block the traffic from passing through the firewall.
Hits	Total number of actions that have been triggered by the rule (since the last reset). For details, see **Access Control Logs**.
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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

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

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

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

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

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

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

Step 6 In the row of a rule, choose **More** > **Delete** in the **Operation** column.

Step 7 In the **Delete Rule** dialog box, click **OK**.

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

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

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

Table 7-1 Intrusion prevention functions

Function	Description
Protection Mode	• **Observe**: Attacks are detected and recorded in logs but are not intercepted. • **Intercept**: Attacks and abnormal IP address access are automatically intercepted. – **Intercept mode - loose**: The protection granularity is coarse. In this mode, only attacks with high threat and high certainty are blocked. – **Intercept mode - moderate**: The protection granularity is medium. This mode meets protection requirements in most scenarios. – **Intercept mode - strict**: The protection granularity is fine-grained, and all attack requests are intercepted. **NOTE** • You are advised to use the **observe** mode for a period of time before using the **intercept** mode. For details about how to view attack event logs, see **Attack Event Logs** • If packets are incorrectly intercepted, you can modify the action of a single defense rule in the basic defense rule library. For details about operations, see **Managing Intrusion Prevention**.
Basic Protection	Basic protection on your assets. It is enabled by default. Its functions are as follows: • Scan for threats and scan vulnerabilities. • Detects whether traffic contains phishing, Trojan horses, worms, hacker tools, spyware, password attacks, vulnerability attacks, SQL injection attacks, XSS attacks, and web attacks. • Checks whether there are protocol anomalies, buffer overflow, access control, suspicious DNS activities, and other suspicious behaviors in traffic. **NOTE** For details about how to view basic defense rules, see **Checking the IPS Rule Library**.
Virtual Patching	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. New IPS rules are displayed in the virtual patch rule library. To view the rule library, click **View Virtual Patch**. For details about the parameters in the rule library, see **Checking the IPS Rule Library**. **Auto Update**: After this function is enabled, rules in the virtual patch take effect. Protection is implemented in real time and protection actions can be manually modified.

Function		Description
Custom IPS Signature		If the basic defense rule library does not meet your requirements, you can create custom IPS signatures. Only the professional edition support custom IPS signatures. For details, see **Customizing IPS Signatures**.
Advanced	Sensitive Directory Scan Defense	Defense against scan attacks on sensitive directories on your servers. **Action**: ● **Observe**: If a sensitive directory scanning attack is detected, CFW records it in logs only. For details about how to view attack logs, see **Attack Event Logs**. ● **Block session**: If the firewall detects a sensitive directory scan attack, it blocks the current session. ● **Block IP**: If CFW detects a sensitive directory scan attack, it blocks the attack IP address for a period of time. **Duration**: If **Action** is set to **Block IP**, you can set the blocking duration. The value range is 60s to 3,600s. **Threshold**: CFW performs the specified action if the scan frequency of a sensitive directory reaches this threshold.
	Reverse Shell Defense	Defense against reverse shells. **Action**: ● **Observe**: If a reverse shell attack is detected, it is only recorded in attack logs. For details about how to view attack logs, see **Attack Event Logs**. ● **Block session**: If the firewall detects a reverse shell attack, it blocks the current session. ● **Block IP**: If CFW detects a reverse shell attack, it blocks the attack IP address for a period of time. **Duration**: If **Action** is set to **Block IP**, you can set the blocking duration. The value range is 60s to 3,600s. **Mode**: ● **Conservative**: 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. ● **Sensitive**: 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.

----End

Follow-up Operations

After the intrusion prevention policy is configured, you can choose **Security Dashboard** to view the protection details. For details, see **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 **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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

Step 6 Check basic protection rules. For more information, see **Basic protection rule parameters**.

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 **Low**, **Medium**, **High**, or **Fatal**.
CVE	CVE ID of the rule.
Rule Type	Type of detected attacks, including vulnerability attacks, access control, and hacker tools.
Affected Software	Software affected by the attack.
Rule Group	Group that the role belongs to. Its types are the same as those of **Protection Mode**, including **Observe**, **strict**, **moderate**, and **loose**.
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	Operation performed by firewall on the traffic that matches the current rule. If you click **Restore All Defaults**, the current actions of all the rules in the list will be restored to the default actions. ● **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.

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

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

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

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 8-1 Changing the current action

ID	Name	Updated In	Description	Risk Level	CVE ID	Attack Type	Affected Sof...	Rule Group	Default Action	Current Acti...	Operation
10008	Beholdl Software ...	1999	--	Low	1999-1030	Other DoS	Web Page Counter	Strictly	Observe	Observe	Observe Intercept Disable
10010	OVActionD SNM...	2001	--	Low	2001-0552	Code Execution (...	Openview Networ...	Strictly	Observe	Observe	Observe Intercept Disable
10013	B2 B2Config.PHP...	2002	--	Low	2002-0734	Other Events	B2	Strictly	Observe	Observe	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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation pane, choose **Attack Defense** > **Intrusion Prevention**. Click **Check Rules** in the **Custom IPS Signature** area.

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: ● Only uppercase letters (A to Z), lowercase letters (a to z), numbers (0 to 9), and the following special characters are allowed: -_ ● A maximum of 255 characters are allowed.
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: ● **Any** ● Server to client ● Client to server
Protocol Type	Protocol type of the feature.
Source Type	Source port type. Its value can be: ● **Any** ● **Include** ● **Exclude** **NOTE** You are advised to select **Any**.
Source Port	Set **Source Port** if **Source Type** is set to **Include** or **Exclude**. ● You can set one or more ports. Use commas (,) to separate multiple ports. Example: **80,100** ● You can also set a port range. Use hyphens (-) to separate ports, for example, 80-443.
Destination Type	Destination port type. Its value can be: ● **Any** ● **Include** ● **Exclude** **NOTE** You are advised to select **Any**.

Parameter Name	Description
Destination Port	Set **Destination Port** if **Destination Type** is set to **Include** or **Exclude**. ● You can set one or more ports. Use commas (,) to separate multiple ports. Example: **80,100** ● You can also set a port range. Use hyphens (-) to separate ports, for example, 80-443.
Action	Action taken by the firewall when it detects traffic with the feature. ● **Observe**: Attacks are detected and recorded in logs. For details about how to query logs, see **Querying Logs**. ● **Intercept**: Attacks are automatically blocked. **NOTE** Before you enable the **Intercept** mode, you are advised to select **Observe** first and check whether the attack logs are correct for a period of time.

Parameter Name	Description
Content	Content matching the feature rule. ● **Content**: content field that matches the feature, for example, **cfw**. ● **Content Option**: Select a rule for content matching. – **Hexadecimal**: The content must be in hexadecimal format. Example: 0x1F – **Case insensitive**: Match content without checking cases. – **URL**: Match the fields that are consistent with the content in URLs. ● **Relative Position** specifies the start position in a feature matching. – **Head**: The start position depends on the **Offset** from the head. For example, if **Offset** is **10**, the content check starts from the eleventh bit. **NOTE** If **Content Option** is set to **URL**, the matching position of the header starts from the end of the domain name (including the port number). For example, if the URL is www.example.com/test and the **Offset** is **0**, the content check starts from the slash (/) following **com**. If the URL is www.example.com:80/test and the **Offset** is **0**, the content check starts from the slash (/) after **80**. – **After previous content**: Packet capture starts from the specified position. Formula: Start position = Length of the previous **Content** field + Previous **Offset** + **Offset** + 1 For example, if the previous content is **test**, the previous **offset** is 10, and the current offset is 5, the start position is the 20th (4+10+5+1) bit. ● **Offset** specifies the start position of feature matching. For example, if the offset is 10, the start position is the eleventh bit. ● **Depth** specifies the end position of feature matching. For example, if the depth is 65,535, the end position is the 65,535th bit. **NOTE** ● **Depth** must be greater than the length of the **Content** field. ● Up to four items can be added to an IPS signature.

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

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

Step 5 In the navigation pane, choose **Attack Defense** > **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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation pane, choose **Attack Defense** > **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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

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

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

Step 5 In the navigation pane, choose **Traffic Analysis** > **Inbound Traffic**.

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

- **Traffic Dashboard**: Information about the highest traffic from the Internet to internal servers.
- **Inbound Traffic**: Inbound request and response traffic.
- **Visualizations**: Top 5 items ranked by certain parameters regarding inbound traffic within a specified time range. For more information, see **Table 11-1**. You can click a data record to view the traffic details. A maximum of 50 data records can be viewed.

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

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

Step 5 In the navigation pane, choose **Traffic Analysis** > **Outbound Traffic**.

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

- **Traffic Dashboard**: Information about the highest traffic when internal servers access the Internet.
- **Outbound Traffic**: Outbound request and response traffic.
- **Visualizations**: Top 5 items ranked by certain parameters regarding outbound traffic within a specified time range. For more information, see **Table 11-2**. You can click a data record to view the traffic details. A maximum of 50 data records can be viewed.

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 **Enabling EIP Protection**.
- The VPC border firewall has been configured and enabled. For details, see **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 on the left, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation pane, choose **Traffic Analysis** > **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**. You can click a data record to view the traffic details. A maximum of 50 data records can be viewed.

Table 11-3 Inter-VPC traffic parameters

Parameter	Description
Top Access Source IP Addresses	Source IP address of inter-VPC traffic.
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 **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 **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 **Querying Logs**.
- If logs are recorded in LTS, you can view log data in the past 1 to 360 days. For details, see **Log Management**.

Prerequisites

- You have performed operations in **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 on the left, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

Figure 12-1 Attack event logs

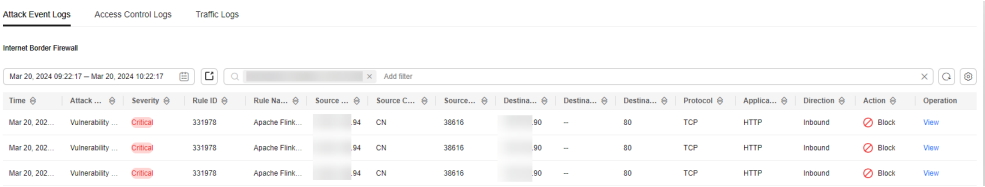


Table 12-1 Attack event log parameters

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 **Critical**, **High**, **Medium**, or **Low**.
Rule ID	Rule ID
Rule Name	Matched rule in the library.
Source IP Address	Source IP address of an attack event.
Source Country/ Region	Geographical location of the attack source IP address.
Source Port	Source port of an attack.
Destination IP Address	Attacked IP address.
Destination Country/ Region	Geographical location of the attack target IP address.
Destination Port	Destination port of an attack.
Protocol	Protocol type of an attack.
Application	Application type of an attack.

Parameter	Description
Direction	It can be outbound or inbound.
Action	The value can be **Allow**, **Block**, **Block IP**, or **Discard**.
Operation	You can click View to view the basic information and attack payload of an event.

----End

Access Control Logs

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

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

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

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

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

Figure 12-2 Access control logs

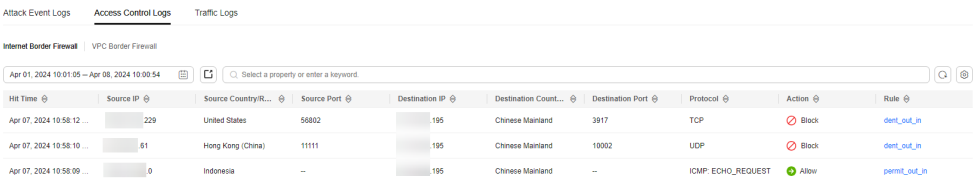


Table 12-2 Access control log parameters

Parameter	Description
Hit Time	Time of access.
Source IP	Source IP address of the access.
Source Country/ Region	Geographical location of the source IP address.
Source Port	Source port for access control. It can be a single port or consecutive port groups (example: **80-443**).

Parameter	Description
Destination IP	Destination IP address.
Destination URL	Destination domain name
Destination Country/ Region	Geographical location of the destination IP address.
Destination Port	Destination port for access control. It can be a single port or consecutive port groups (example: **80-443**).
Protocol	Protocol type for access control.
Action	Action taken on an event. It can be **Observe**, **Block**, or **Allow**.
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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

Figure 12-3 Traffic logs

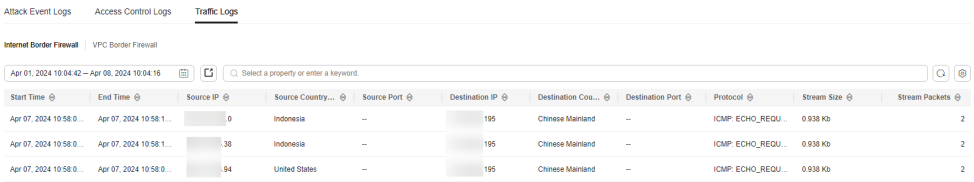


Table 12-3 Traffic log parameters

Parameter	Description
Start Time	Time when traffic protection started.

Parameter	Description
End Time	Time when traffic protection ended.
Source IP	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	Destination IP address.
Destination URL	Destination domain name to be accessed
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 **Querying Logs**.
- If logs are recorded in LTS, you can view log data in the past 1 to 360 days. For details, see **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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation pane on the left, choose **Log Audit** > **Log Management**. The Log Management page is displayed. Click **Configure LTS Synchronization**. Toggle on to enable the cloud log interconnection service.

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

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

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

NOTE

- Logs can be stored for 1 to 360 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 **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 on the left, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

Click **Add Alarm Rule** in the upper right corner to add an alarm.

- For details about how to create a keyword alarm, see **Table 12-4**.
- For details about how to create SQL alarms, see **Table 12-5**.

Table 12-4 Parameters for setting a keyword alarm condition

Category	Parameter	Description
Basic Info	Rule Name	Name of the alarm rule. A name can contain 1 to 64 characters, including only letters, digits, hyphens (-), and underscores (_). It cannot start or end with a hyphen or underscore. **NOTE** After an alarm is created, the rule name can be modified. After the modification, move the cursor over the rule name to view the new and original rule names. The original rule name created for the first time cannot be changed.
	Description	Rule description. Enter up to 64 characters.
Statistical analysis	Statistics	**By keyword**: applicable to scenarios where keywords are used to search for and configure log alarms.
	Query condition	**Log Group Name**: Select a log group.
		Log Stream Name: Select a log stream. **NOTE** If a log group contains more than one log stream, you can select multiple log streams when creating a keyword alarm rule.
		Query Time Range: Specify the query period of the statement. It is one period earlier than the current time. For example, if **Query Time Range** is set to one hour and the current time is 9:00, the period of the query statement is 8:00–9:00. • The value ranges from 1 to 60 in the unit of minutes. • The value ranges from 1 to 24 in the unit of hours.
		Keywords: Enter keywords that you want LTS to monitor in logs. Exact and fuzzy matches are supported. A keyword is case-sensitive and contains up to 1024 characters.

Category	Parameter	Description
	Check Rule	Configure a condition that will trigger the alarm. **Matching Log Events**: When the number of log events that contain the configured keywords reaches the specified value, an alarm is triggered. Four comparison operators are supported: greater than (**>**), greater than or equal to (**>=**), less than (**<**), and less than or equal to (**<=**). The number of queries refers to the **Query Frequency** set in **Advanced Settings** and the number of times the condition must be met to trigger the alarm. The number of queries must be greater than or equal to the number of times the condition must be met. **NOTE** ● The alarm severity can be **critical** (default), **major**, **minor**, or **info**. ● Number of queries: 1–10

Category	Parameter	Description
Advanced Settings	Query Frequency	The options for this parameter are: ● **Hourly**: The query is performed at the top of each hour. ● **Daily**: The query is run at a specific time every day. ● **Weekly**: The query is run at a specific time on a specific day every week. ● **Custom interval**: You can specify the interval from 1 minute to 60 minutes or from 1 hour to 24 hours. For example, if the current time is 9:00 and the **Custom interval** is set to 5 minutes, the first query is at 9:00, the second query is at 9:05, the third query is at 9:10, and so on. **NOTE** When the query time range is set to a value larger than 1 hour, the query frequency must be set to every 5 minutes or a lower frequency. ● **CRON**: CRON expressions support schedules down to the minute and use 24-hour format. Examples: – **0/10 * * * ***: The query starts from 00:00 and is performed every 10 minutes. That is, queries start at 00:00, 00:10, 00:20, 00:30, 00:40, 00:50, 01:00, and so on. For example, if the current time is 16:37, the next query is at 16:50. – **0 0/5 * * ***: The query starts from 00:00 and is performed every 5 hours at 00:00, 05:00, 10:00, 15:00, 20:00, and so on. For example, if the current time is 16:37, the next query is at 20:00. – **0 14 * * ***: The query is performed at 14:00 every day. – **0 0 10 * ***: The query is performed at 00:00 on the 10th day of every month.
Advanced Settings	Restores	Configure a policy for sending an alarm clearance notification. If alarm clearance notification is enabled and the trigger condition has not been met for the specified number of statistical periods, an alarm clearance notification is sent. Last statistical periods: 1–10

Category	Parameter	Description
Advanced Settings	Notify When	• **Alarm triggered**: Specify whether to send a notification when an alarm is triggered. If this option is enabled, an alarm notification will be sent when the trigger condition is met. • **Alarm cleared**: Specify whether to send a notification when an alarm is cleared. If this option is enabled, a notification will be sent when the policy is met.
Advanced Settings	Frequency	You can select **Once**, **Every 5 minutes**, **Every 10 minutes**, **Every 15 minutes**, **Every 30 minutes**, **Every hour**, **Every 3 hours**, or **Every 6 hours** to send alarms. **Once** indicates that a notification is sent once an alarm is generated. **Every 10 minutes** indicates that the minimum interval between two notifications is 10 minutes, preventing alarm storms.
Advanced Settings	Alarm Action Rules	Select a created alarm action rule from the drop-down list. If no alarm action rule is available, click **Create Alarm Action Rule** on the right.
Advanced Settings	Language	Specify the language (**Chinese (simplified)** or **English**) in which alarms are sent.
Advanced Settings	Notify	Specify whether to send a notification when the alarm is cleared. This option is enabled by default. If this option is enabled, a notification will be sent when the policy is met.
Advanced Settings	Send notification	Enable or disable alarm notification. If you enable **Send notification**, you need to select a Simple Message Notification (SMN) topic, time zone, and language. You can select multiple topics.

Table 12-5 Parameters for creating a SQL alarm condition

Category	Parameter	Description
Basic Info	Rule Name	Name of the alarm rule. Enter 1 to 64 characters and do not start or end with a hyphen (-) or underscore (_). Only letters, digits, hyphens, and underscores are allowed. **NOTE** After an alarm is created, the rule name can be modified. After the modification, move the cursor over the rule name. The new and original rule names are displayed. The original rule name created for the first time cannot be changed.
	Description	Rule description. Enter up to 64 characters.
Statistical analysis	Statistics	**By SQL**: applicable to the scenarios where alarm rules are configured based on the old SQL engine.

Category	Parameter	Description
	Charts	You can add a chart in two ways. ● **Configure from Scratch**: Click **Configure from Scratch** and then select a log group and stream. Set parameters as follows: **Log Group Name**: (Required) Select a log group. **Log Stream Name**: (Required) Select a log stream. **Query Time Range**: (Optional) the period specified for querying logs. It can be 1 to 60 minutes or 1 to 24 hours. **Query Statement**: Required. ● Click + Import Configuration . On the displayed **Custom** page, select a log group and stream, select a chart, and click **OK**. If there are no charts available or the charts do not fit your needs, click **Create Chart**. Configure the chart parameters, click **OK**, and click **Save and Back** in the upper right corner to return to the **Create Alarm Rule** right panel. You can see that the chart you just created has been selected, and the query statement has been filled in. Specify the query time range (1 to 60 minutes or 1 to 24 hours). When the query frequency is set to every 1 to 4 minutes, the query time range can only be set to a value no larger than 1 hour. You can click + Import Configuration to add more charts. **NOTE** – Click to go to the visualization page of the log stream. – Click to delete an added chart. – Click **Preview** to view the data after visualized analysis. You must click **Preview**; otherwise, the alarm rule cannot be saved. – Up to three charts can be added. – The chart and the query statement are required.

Category	Parameter	Description
	Check Rule	Enter a specific conditional expression. When the expression execution result is **true**, an alarm is generated. **NOTE** ● Condition expressions support Chinese characters. ● Condition expressions cannot contain only numbers or start with a number. Basic syntax and syntax across multiple charts are supported. ● Basic syntax – Basic arithmetic operators: addition (+), subtraction (–), multiplication (x), division (/), and modulo (%). Example: **x * 10 + y > 100** – Comparison operators: greater than (>), greater than or equal to (>=), less than (<), less than or equal to (<=), equal to (==), and not equal to (!=). Example: **x >= 100**. – Logical operators: && (and) and || (or). Example: **x > 0 && y < 200** – Logical negation (!). Example: **!(x < 1 && x > 100)** – Numeric constants: They are processed as 64-bit floating point numbers. Example: **x > 10** – String constants. Example: **str =="string"** – Boolean constants: true and false. Example: **(x < 100)!=true** – Parentheses: Parentheses are used to change the order of operations. Example: **x *(y + 10) < 200** – contains function: It is used to check whether a string contains a substring. For example, if you run **contains(str, "hello")** and **true** is returned, the string contains the **hello** substring. ● Syntax across multiple charts – Basic arithmetic operators: addition (+), subtraction (–), multiplication (x), division (/), and modulo (%). – Comparison operators: greater than (>), greater than or equal to (>=), less than (<), less than or equal to (<=), equal to (==), and not equal to (!=). – Logical operators: && (and) and || (or). – Logical negation (!)

Category	Parameter	Description
		– contains function – Parentheses () **NOTE** ● Specify the number of queries and the number of times the condition must be met to trigger the alarm. The number of queries must be greater than or equal to the number of times the condition must be met. ● The alarm severity can be **critical** (default), **major**, **minor**, or **info**. ● Number of queries: 1–10
Advanced Settings	Query Frequency	The options for this parameter are: ● **Hourly**: The query is performed at the top of each hour. ● **Daily**: The query is run at a specific time every day. ● **Weekly**: The query is run at a specific time on a specific day every week. ● **Custom interval**: You can specify the interval from 1 minute to 60 minutes or from 1 hour to 24 hours. For example, if the current time is 9:00 and the **Custom interval** is set to 5 minutes, the first query is at 9:00, the second query is at 9:05, the third query is at 9:10, and so on. **NOTE** When the query time range is set to a value larger than 1 hour, the query frequency must be set to every 5 minutes or a lower frequency. ● **CRON**: CRON expressions support schedules down to the minute and use 24-hour format. Examples: – **0/10 * * * ***: The query starts from 00:00 and is performed every 10 minutes at 00:00, 00:10, 00:20, 00:30, 00:40, 00:50, 01:00, and so on. For example, if the current time is 16:37, the next query is at 16:50. – **0 0/5 * * ***: The query starts from 00:00 and is performed every 5 hours at 00:00, 05:00, 10:00, 15:00, 20:00, and so on. For example, if the current time is 16:37, the next query is at 20:00. – **0 14 * * ***: The query is performed at 14:00 every day. – **0 0 10 * ***: The query is performed at 00:00 on the 10th day of every month.

Category	Parameter	Description
Advanced Settings	Restores	Configure a policy for sending an alarm clearance notification. If alarm clearance notification is enabled and the trigger condition has not been met for the specified number of statistical periods, an alarm clearance notification is sent. Last statistical periods: 1–10
Advanced Settings	Notify When	• **Alarm triggered**: Specify whether to send a notification when an alarm is triggered. If this option is enabled, an alarm notification will be sent when the trigger condition is met. • **Alarm cleared**: Specify whether to send a notification when an alarm is cleared. If this option is enabled, a notification will be sent when the recovery policy is met.
Advanced Settings	Frequency	You can select **Once**, **Every 5 minutes**, **Every 10 minutes**, **Every 15 minutes**, **Every 30 minutes**, **Every hour**, **Every 3 hours**, or **Every 6 hours** to send alarms. **Once** indicates that a notification is sent once an alarm is generated. **Every 10 minutes** indicates that the minimum interval between two notifications is 10 minutes, preventing alarm storms.
Advanced Settings	Alarm Action Rules	Select a created alarm action rule from the drop-down list. If no alarm action rules are available, click **Create Alarm Action Rule** on the right.
Advanced Settings	Language	Specify the language (**Chinese (simplified)** or **English**) in which alarms are sent.

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

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

Step 5 In the navigation pane 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**.

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.

   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 **Log Settings**.
- Log structuring has been completed. For details, see **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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation pane 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 12-6 Chart parameters

Chart Type	Description
Table Chart	• **Records per Page**: number of log events displayed per page. The value can be 10 (default), 20, 30, or 50. • **Filtering**: After the filtering function is enabled, you can filter results the right of the table header. Currently, only single-column search is supported. • **Sorting**: After the sorting function is enabled, you can select the ascending or descending order on the table header.
Bar Chart	• **X Axis**: Select a field from the drop-down list box as the X axis. Digits and strings are supported. • **Y Axis**: Select a field from the drop-down list box as the Y axis. Only numeric data is supported. • **X Axis Title** and **Y Axis Title**: Set the titles for the X axis and Y axis. • **Y Axis Range**: Set the minimum and maximum values for the Y axis. • **Max Shown Categories**: The value can be 20, 40, 50 (default), 80, and 100. • **Show Labels**: Set this parameter based on your requirements. • **Stacked**: Set this parameter based on your requirements. If you enable it, labels cannot be shown.

Chart Type	Description
Line Chart	• **X Axis**: Select a field from the drop-down list box as the X axis. The value can be a number or a string. • **Y Axis**: Select a field from the drop-down list box as the Y axis. Only numeric data is supported. • **X Axis Title** and **Y Axis Title**: Set the titles for the X axis and Y axis. • **Y Axis Range**: Set the minimum and maximum values for the Y axis. • **Line**: Select **Curved** or **Straight**. • **Show Data Markers**: Set this parameter based on your requirements.
Pie Chart	• **Category**: Select a field from the drop-down list box as the category. Only strings are supported. • **Value**: Select a field from the drop-down list box. Only numeric data is supported. • **Label Position**: Select **Inside** or **Outside**. This parameter can be set only after you enable **Show Labels**. • **Shown Categories**: 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 **Others**. • **Coxcomb Chart**: In a coxcomb chart, the radius of pie slices differs depending on the percentage of the data that the slices represent. • **Show Labels**: Set this parameter based on your requirements.
Number Chart	• **Data Column**: 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. • **Add Comparison Data**: Set this parameter based on your requirements. • **Comparison Data**: 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. • **Description**: You can add a description for numbers. • **Data Unit** and **Comparison Data Unit**: Set the units based on your requirements. • **Advanced Settings**: You can set **Number Format**, **Data Text Size**, **Comparison Data Text Size**, and **Unit Text Size**.

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

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

Step 5 In the navigation pane 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.

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

Field	Type	Description
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. ● **internet**: Internet border traffic log ● **nat**: NAT border traffic log ● **vpc**: inter-VPC traffic log
vsys	long	Firewall protection direction. ● **1**: north-south ● **2**: east-west
direction	string	Traffic direction. ● **out2in**: inbound ● **in2out**: outbound
action	string	Response action of the firewall. ● **permit** ● **deny** ● **block** ● **drop**
packet	string	Original data packet of the attack log. **NOTE** 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. ● Vulnerability exploit ● Vulnerability scan ● Trojan ● Worms ● Phishing ● Web attacks ● Application DDoS ● Buffer overflow ● Password attacks ● Mail ● Access control ● Hacking tools ● Hijacking ● Protocol exception ● Spam ● Spyware ● DDoS flood ● Suspicious DNS activities ● Other suspicious behaviors
level	string	Level of detected threats. ● **CRITICAL** ● **HIGH** ● **MIDDLE** ● **LOW**
source	string	Defense for the detected attack. ● **0**: basic protection ● **1**: virtual patch
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. ● **internet**: Internet border traffic log ● **nat**: NAT border traffic log ● **vpc**: inter-VPC traffic log
dst_host	string	Destination domain name
vsys	long	Firewall protection direction. ● **1**: north-south ● **2**: east-west
protocol	string	Protocol type
app	string	Application type
direction	string	Traffic direction. ● **out2in**: inbound ● **in2out**: outbound
action	string	Response action of the firewall. ● **permit** ● **deny**
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. ● **out2in**: inbound ● **in2out**: outbound
action	string	Response action of the firewall. ● **permit** ● **deny**
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. ● **internet**: Internet border traffic log ● **nat**: NAT border traffic log ● **vpc**: inter-VPC traffic log
dst_host	string	Destination domain name
vsys	long	Firewall protection direction. ● **1**: north-south ● **2**: east-west
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.

CFW supports the following alarms:

- Attack alarm: An alarm is triggered when the IPS detects an attack.
- High traffic warning: An alarm is triggered if the traffic reaches the specified percentage of the traffic processing capability you purchased.
- EIP not protected: An alarm is triggered when the current account has EIPs that are not protected.
- Abnormal external connection alarm: An alarm is triggered when risky external IP addresses or domain names are detected.

NOTE

- Simple Message Notification (SMN) is a paid service. For details, see **Product 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**.

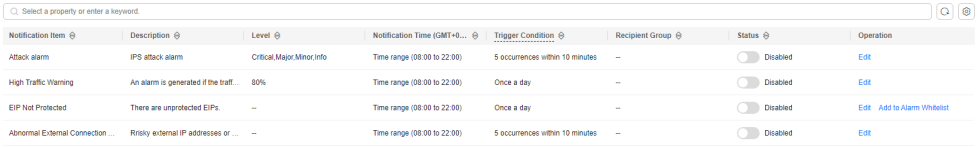
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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

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

Figure 13-1 Alarm notifications



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

Figure 13-2 Notification item settings - attack alarm

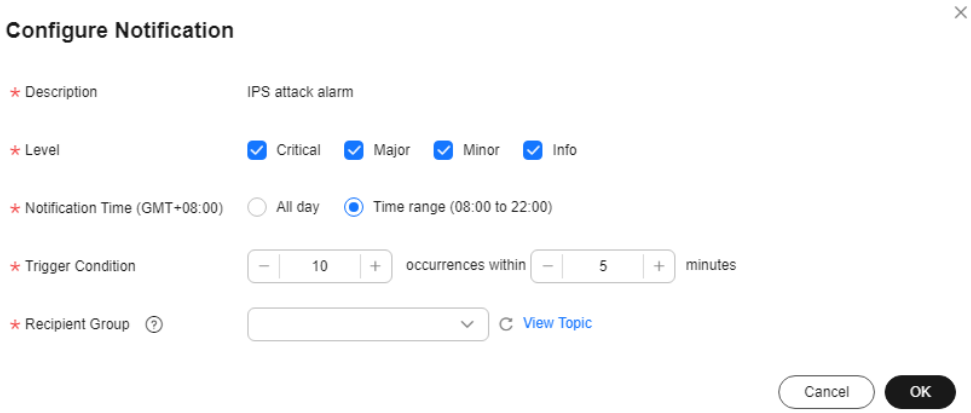


Table 13-1 Attack alarm parameters

Parameter	Description
Description	IPS attack alarm
Level	Select the risk levels that trigger notifications. The options are **Serious**, **High**, **Medium**, and **Low**. Multiple options can be selected. For example, if you select **High** and **Medium**, 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. **NOTE** 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. If there are no topics, click **View Topic** and perform the following steps to create a topic: 1. Create a topic. For details, see **Creating a Topic**. 2. Add one or more subscriptions to the topic. You will need to provide a phone number, email address, function, platform application endpoint, DMS endpoint, or HTTP/HTTPS endpoint for receiving alarm notifications. For details, see **Adding a Subscription**. 3. Confirm the subscription.

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**.

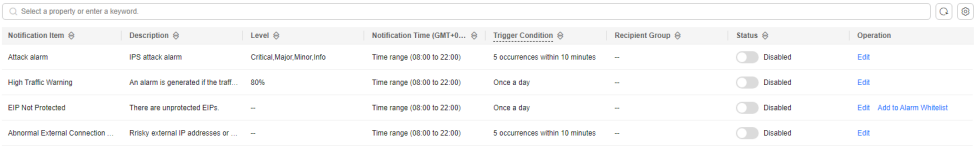
Step 2 Click  in the upper left corner of the management console and select a region or project.

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

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

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

Figure 13-3 Alarm notifications



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

Figure 13-4 Notification item settings - high traffic warning

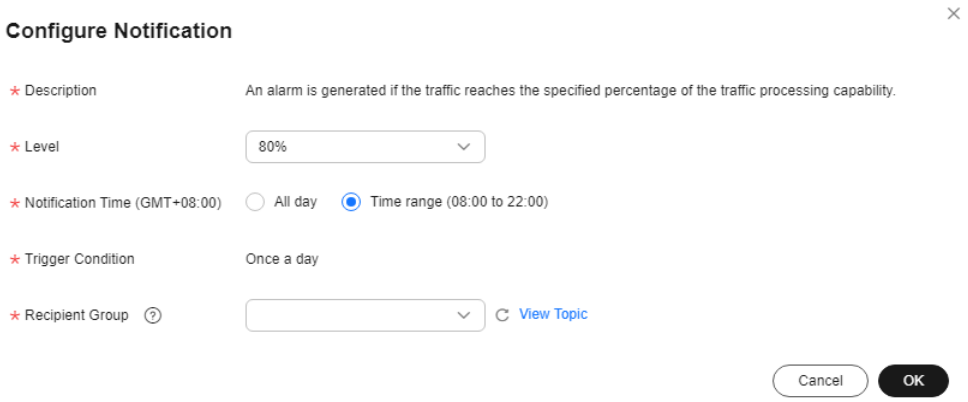


Table 13-2 High traffic warning parameters

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 **70%**, **80%**, or **90%**. If this parameter is set to **80%**, 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. If there are no topics, click **View Topic** and perform the following steps to create a topic: 1. Create a topic. For details, see **Creating a Topic**. 2. Add one or more subscriptions to the topic. You will need to provide a phone number, email address, function, platform application endpoint, DMS endpoint, or HTTP/HTTPS endpoint for receiving alarm notifications. For details, see **Adding a Subscription**. 3. Confirm the subscription.

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**.

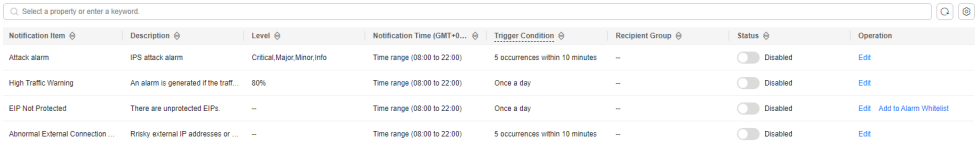
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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

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

Figure 13-5 Alarm notifications



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 13-6 Notification settings - EIP Not Protected

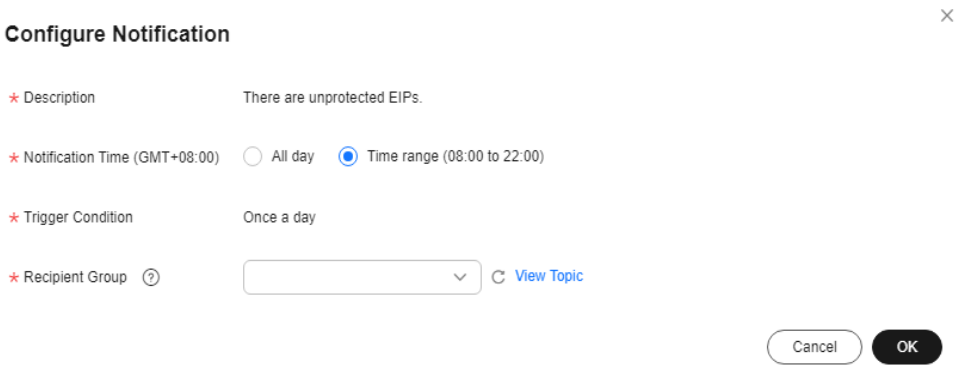


Table 13-3 Parameters of the alarm **EIP Not Protected**

Parameter	Description
Description	This alarm indicates there are unprotected EIPs.
Notification Time	Select a time range for sending notifications.
Trigger Condition	Once a day

Parameter	Description
Recipient Group	Select a topic from the drop-down list to configure the endpoints for receiving alarm notifications. If there are no topics, click **View Topic** and perform the following steps to create a topic: 1. Create a topic. For details, see **Creating a Topic**. 2. Add one or more subscriptions to the topic. You will need to provide a phone number, email address, function, platform application endpoint, DMS endpoint, or HTTP/HTTPS endpoint for receiving alarm notifications. For details, see **Adding a Subscription**. 3. Confirm the subscription.

Step 7 Click **OK**.

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

----End

Abnormal External Connection Alarm

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

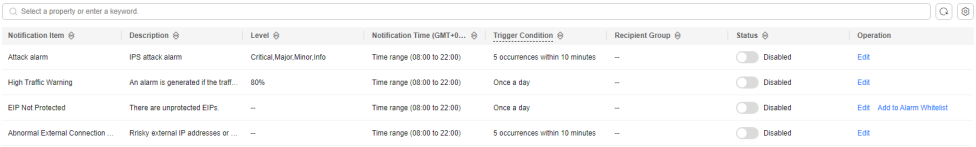
Step 2 Click  in the upper left corner of the management console and select a region or project.

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

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

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

Figure 13-7 Alarm notifications



Step 6 In the **Operation** column of the **Abnormal External Connection Alarm** alarm, click **Edit**, and configure notification item parameters. For details, see **Table 13-4**.

Figure 13-8 Notification item settings - abnormal external connection alarm

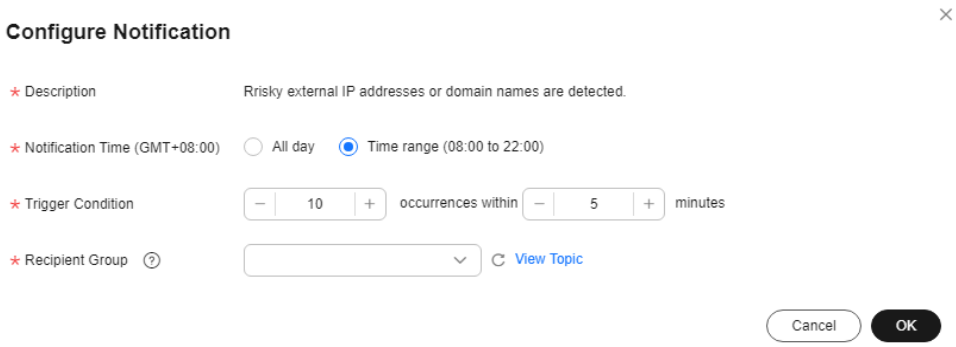


Table 13-4 Parameters of **Abnormal External Connection Alarm**

Parameter	Description
Description	This alarm indicates there are unprotected EIPs.
Notification Time	Select a time range for sending notifications.
Trigger Condition	Configure the trigger condition. **NOTE** Alarm notifications are sent if the number of abnormal external connections is at least equal to the threshold configured for a certain period.
Recipient Group	Select a topic from the drop-down list to configure the endpoints for receiving alarm notifications. If there are no topics, click **View Topic** and perform the following steps to create a topic: 1. Create a topic. For details, see **Creating a Topic**. 2. Add one or more subscriptions to the topic. You will need to provide a phone number, email address, function, platform application endpoint, DMS endpoint, or HTTP/HTTPS endpoint for receiving alarm notifications. For details, see **Adding a Subscription**. 3. Confirm the subscription. After the subscription is added, confirm the subscription.

Step 7 Click **OK**.

Step 8 After confirming that the information is correct, click in the **Status** column of the row where the **Abnormal External Connection Alarm** is located to enable this function.

----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.

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

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

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

Step 6 Click **Create Capture Task** and configure parameters.

Table 13-5 Packet capture task parameters

Parameter Name	Description	Example Value
Task Name	Task name. It must meet the following requirements: ● 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.	cfw
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: ● Any ● TCP ● UDP ● ICMP	Any
Source Address	It can be: ● A single IP address, for example, **192.168.10.5** ● Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** ● Address segment, for example, **192.168.2.0/24**	192.168.10.5
Source Port	(Optional) Source port. The input rules are as follows: ● If this parameter is left blank, it indicates all port numbers (1 to 65535). ● Enter a single port number in the range 1 to 65535.	80

Parameter Name	Description	Example Value
Destination Address	It can be: • A single IP address, for example, **192.168.10.5** • Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** • Address segment, for example, **192.168.2.0/24**	192.168.10.6
Destination Port	(Optional) Destination port. The input rules are as follows: • If this parameter is left blank, it indicates all port numbers (1 to 65535). • Enter a single port number in the range 1 to 65535.	-

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.
- **Viewing a Packet Capture Task**
- **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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation 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 13-6**

Table 13-6 Packet capture task parameters

Parameter Name	Description
Task Name	Task name
Status	Task status. • **Running**: The packet capture command has been delivered and the task is in progress. • **Completed**: The packet capture result has been uploaded and the task is complete. • **Exception**: Packet capture data upload times out due to network problems, and some packet capture results are lost. **NOTE** To retry a task, you can click **Copy** in its **Operation** column to create and execute it again. • **Stopping**: The task is being stopped and the packet capture result is being uploaded. • **Expired**: The packet capture result has been uploaded and the task has been manually stopped.
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.
- **Creating a Packet Capture Task**
- **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 on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation 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**.

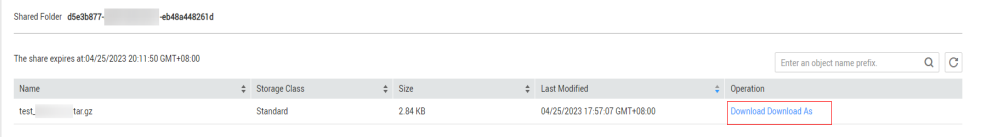
- You can click **Copy link**, and paste and open the link it in a new browser tab. Switch back to this dialog box, click **Copy access code**, paste the copied code to the **Extraction Code** text box on the new tab, and click **Obtain Shared File List**.

NOTE

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

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

Figure 13-9 Downloading the packet capture result



----End

13.3 Multi-Account Management

13.3.1 Multi-Account Management Overview

CFW provides secure and reliable cross-account data aggregation and resource access capabilities. If the accounts in your organization are centrally managed, you can use CFW to protect the EIPs of all member accounts in the organization in a unified manner.

Assume that account A needs to manage the assets of account B. To use CFW to protect the assets of organization members, perform the following operations:

1. If account A is an organization administrator, skip this step. If account A is not an organization administrator, the organization administrator should add account A as a delegated administrator. For details, see **Specifying a Delegated Administrator**.
2. The organization administrator or delegated administrator invites account B to join the organization. For details, see **Inviting an Account to Join Your Organization**.
3. In CFW, add account B to the list on the **Multi-Account Management** page. For details, see **Adding an Account to an Organization**.

For details about the organization service, see **Overview of Organizations**.

NOTE

To request the EIP information of account B, CFW automatically creates a service agency in accounts A and B.

- The agency is a cloud service agency. Its permissions is **CFWServiceLinkedAgencyPolicy** name is **ServiceLinkedAgencyForCloudFirewall**, and **Scope** is **All resources**.
- If account B is deleted, CFW automatically deletes the agency associated with the service in account B.
- If you unsubscribe from CFW, CFW automatically deletes the agencies associated with account A and all member accounts.

13.3.2 Adding an Account to an Organization

This section describes how to add an account to an organization to perform EIP protection.

Prerequisites

- You applied for the Organizations service and created an organization. For details, see **Overview of Organizations**.
- CFW has been set as a trusted service. For details, see **Enabling or Disabling a Trusted Service**.
- The current account is an organization management account or a delegated administrator account. For details, see **Specifying a Delegated Administrator**.

Procedure

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

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

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

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

Step 5 In the navigation pane, choose **System Management** > **Multi-Account Management**.

Step 6 Click **Add Account**. Select accounts in the navigation tree on the left. The selected accounts are automatically added to the **Selected** area on the right.

NOTE

The added accounts belong to the same organization. For details about organization accounts, see **Overview of an Account**.

Step 7 Click **OK**. The added account is displayed in the account list.

----End

Follow-up Operations

Asset synchronization: After adding an organization member account, click **Synchronize EIP**. The EIPs of the added account will be displayed on the CFW console. For details, see **Enabling EIP Protection**.

Related Operations

- **Viewing Multi-Account Management**
- Deleting an organization member account: Select an account and click **Delete Account** above the list.

13.3.3 Viewing Multi-Account Management

On the **Multi-Account Management** page, you can view the organization member accounts that have been added to CFW for asset protection and the EIP protection details of these accounts.

Prerequisites

- You applied for the Organizations service and created an organization. For details, see **Overview of Organizations**.
- CFW has been set as a trusted service. For details, see **Enabling or Disabling a Trusted Service**.
- The current account is an organization management account or a delegated administrator account. For details, see **Specifying a Delegated Administrator**.

Constraints

The number of accounts that can be protected by a single firewall instance is as follows:

- Standard edition: 20
- Professional edition: 50

Viewing Account Management

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

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

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

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

Step 5 In the navigation pane, choose **System Management** > **Multi-Account Management**.

Step 6 Check the account list. For more information, see **Table 13-7**.

Table 13-7 Parameters in the account list

Parameter Name	Description
Account Name	Account name.
EIPs	Number of EIPs under an account.
Protected EIPs	Number of EIPs protected by the firewall.

Parameter Name	Description
Unprotected EIPs	Number of EIPs that are not protected by the firewall.

----End

Related Operations

- **Adding an Account to an Organization**
- Deleting an organization member account: Select an account and click **Delete Account** above the list.

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

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

Step 5 In the navigation 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

13.5 Security Reports

13.5.1 Creating a Security Report

You can obtain security reports to learn about the security status of your assets in a timely manner. CFW sends log reports to you based on the time period and receiving mode you configured.

This section describes how to create a security report.

Constraints

- Up to 10 security reports can be created for a CFW instance.
- A security report is retained for only three months. You are advised to periodically download security reports for audit.
- A custom security report cannot be modified. If you need to modify a custom security report, delete it and create a new one.

Procedure

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

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

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

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

Step 5 In the navigation tree on the left, choose **System Management** > **Security Report**. The **Security Report** page is displayed.

Step 6 Click **Create Template**. For details about the parameters, see **Parameters of the security report template**.

Table 13-8 Parameters of the security report template

Parameter	Description
Report Name	Name of the custom security report

Parameter	Description
Report Type	• **Daily** Statistical period: 00:00:00 to 24:00:00 every day A report will be sent to the recipients the day after it is generated. • **Weekly** Statistical period: 00:00:00 on Monday to 24:00:00 on Sunday A report will be sent to the recipients at the specified time after it is generated. • **Custom**: Customize a time range. **Statistical Period**: Configure a statistical period for your report. A report will be sent to the specified recipients after it is generated.
Statistical Period	If **Report Type** is set to **Custom**, you need to set **Statistical Period**.
Report Schedule	When **Report Type** is set to **Daily** or **Weekly**, you need to set the report sending time. By default, the log report of the previous statistical period is sent. **NOTE** To ensure correctness, the report sending time may be delayed.
Recipient Group	Select a topic from the drop-down list to configure the endpoints for receiving the log report. If there are no topics, click **View Topic** and perform the following steps to create a topic: 1. Create a topic. For details, see **Creating a Topic**. 2. Add one or more subscriptions to the topic. You will need to provide a phone number, email address, function, platform application endpoint, DMS endpoint, or HTTP/HTTPS endpoint for receiving alarm notifications. For details, see **Adding a Subscription**. 3. Confirm the subscription. After the subscription is added, confirm the subscription.

Step 7 Click **OK**. A security report is created.

----End

13.5.2 Viewing/Downloading a Security Report

This section describes how to view a created security report and its information.

Viewing/Downloading the Latest Security Report

Step 1 Log in to the management console.

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

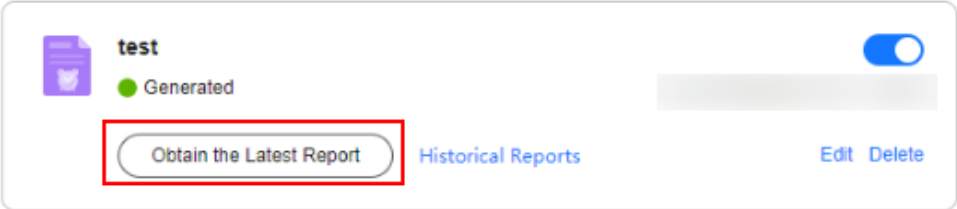
Step 3 In the navigation pane on the left, click and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

Step 5 In the navigation tree on the left, choose **System Management** > **Security Report**. The **Security Report** page is displayed.

Step 6 Click **Obtain the Latest Report** of the target report. The security report preview page is displayed.

Figure 13-10 Obtaining the latest report



Step 7 In the security report preview page, click **Download** in the lower right corner.

----End

Viewing/Downloading Historical Security Report

Step 1 Log in to the management console.

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

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

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

Step 5 In the navigation tree on the left, choose **System Management** > **Security Report**. The **Security Report** page is displayed.

Step 6 Click the **Historical Report** of the target report. The **Historical Reports** page is displayed and you can view the report list.

Figure 13-11 Obtaining historical reports

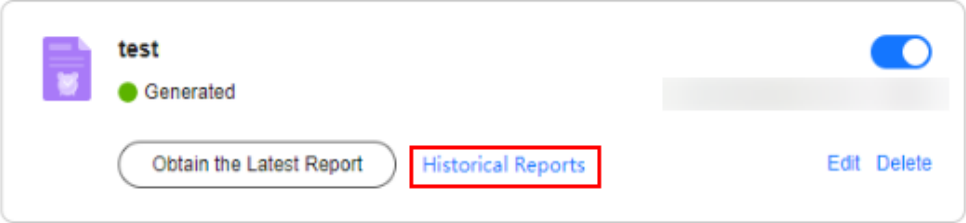
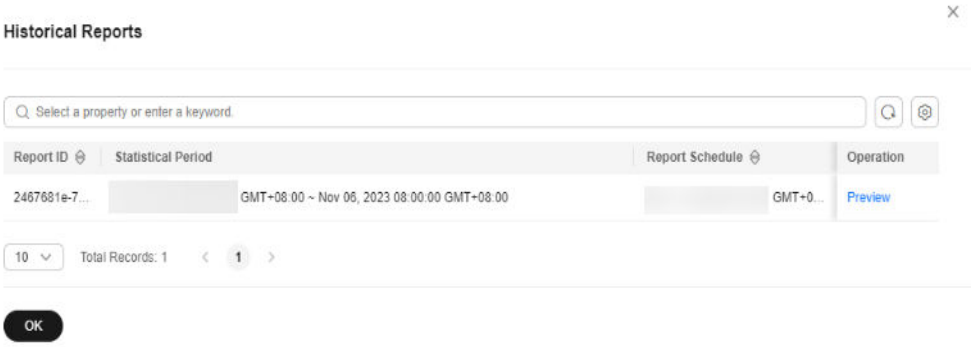


Figure 13-12 Historical reports



Step 7 Click **Preview** in the **Operation** column of a report to view the report information.

Step 8 In the security report preview page, click **Download** in the lower right corner.

----End

13.5.3 Managing Security Reports

This section describes how to manage security reports, including enabling, disabling, modifying, and deleting security reports.

Enabling/Disabling the Security Report Function

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

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

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

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

Step 5 In the navigation tree on the left, choose **System Management** > **Security Report**. The **Security Report** page is displayed.

Step 6 Toggle on or off the switch in the upper right corner of the target report to change the status.

- : enabled
- : disabled

----End

Modifying a Security Report

Step 1 Log in to the management console.

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

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

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

Step 5 In the navigation tree on the left, choose **System Management** > **Security Report**. The **Security Report** page is displayed.

Step 6 Click **Edit** in the lower right corner of the target report to modify the report information.

Table 13-9 Parameters of the security report template

Parameter	Description
Report Name	Name of a security report
Report Type	• **Daily** Statistical period: 00:00:00 to 24:00:00 every day A report will be sent to the recipients the day after it is generated. • **Weekly** Statistical period: 00:00:00 on Monday to 24:00:00 on Sunday A report will be sent to the recipients at the specified time after it is generated.
Report Schedule	When **Report Type** is set to **Daily** or **Weekly**, you need to set the report sending time. By default, the log report of the previous statistical period is sent.

Parameter	Description
Recipient Group	Select a topic from the drop-down list to configure the endpoints for receiving the log report. If there are no topics, click **View Topic** and perform the following steps to create a topic: 1. Create a topic. For details, see **Creating a Topic**. 2. Add one or more subscriptions to the topic. You will need to provide a phone number, email address, function, platform application endpoint, DMS endpoint, or HTTP/HTTPS endpoint for receiving alarm notifications. For details, see **Adding a Subscription**. 3. Confirm the subscription. After the subscription is added, confirm the subscription.

Step 7 Click **OK**. A security report is created.

----End

Deleting a Security Report

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

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

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

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

Step 5 In the navigation tree on the left, choose **System Management** > **Security Report**. The **Security Report** page is displayed.

Step 6 Click **Delete** in the lower right corner of the target report to delete the report.

----End

14 Permissions Management

14.1 Creating a User Group and Granting Permissions

This section describes how to use **Identity and Access Management (IAM)** to implement fine-grained permissions control for your CFW resources. With IAM, you can:

- Create IAM users for employees in different departments based on your organizational structure. Each IAM user has their own security credentials used to access CFW resources.
- Grant only the permissions required for users to perform a task.
- Entrust an account or cloud service to perform professional and efficient O&M on your CFW resources.

If your Huawei account does not require individual IAM users, skip this chapter.

This topic describes the procedure for granting permissions (see **Figure 14-1**).

Prerequisites

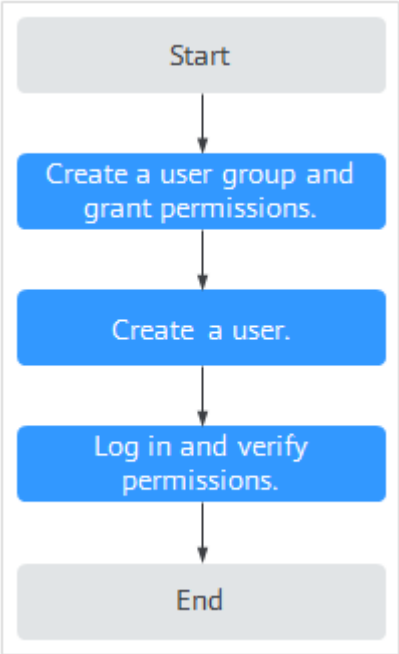
Learn about the permissions supported by CFW in **Table 14-1** and choose policies or roles based on your requirements.

Table 14-1 System policies supported by CFW

Role Name	Description	Category	Dependency
CFW FullAccess	All permissions for CFW	System-defined policy	None
CFW ReadOnlyAccess	Read-only permissions for CFW	System-defined policy	None

Process Flow

Figure 14-1 Process for granting permissions



1. **Create a user group and assign permissions.**.

   Create a user group on the IAM console, and attach the **CFW ReadOnlyAccess** policy to the group.

2. **Creating an IAM User**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the CFW console by using the newly created user, and verify that the user only has **CFW Administrator** permissions for CFW.

   – Choose **Cloud Firewall** in the service list. Click Buy CFW on the CFW console. If you cannot buy CFW (assuming that only the **CFW FullAccess** permission is granted), the **CFW FullAccess** policy has already taken effect.

   – Choose any other service in **Service List**. Assume that the current policy contains only the **CFW FullAccess** permission. If a message appears indicating that you have insufficient permissions to access the service, the **CFW FullAccess** policy has already taken effect.

14.2 CFW Custom Policies

Custom policies can be created to supplement the system-defined policies of CFW. For details about the actions supported by custom policies, see **CFW Permissions and Supported Actions**.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.

- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. The following section contains examples of common CFW custom policies.

CFW Example Custom Policies

- Example 1: Allowing users to create a CFW instance

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cfw:instance:create"
                                ]
        }
    ]
}
```

- Example 2: Not allowing users to remove items from a blacklist or whitelist

  A deny policy must be used together with other policies. If the permissions assigned to a user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **CFW FullAccess** policy to a user but also forbid the user from deleting web tamper protection rules (**cfw:blackWhite:delete**). Create a custom policy with the action to delete web tamper protection rules, set its **Effect** to **Deny**, and assign both this policy and the **CFW FullAccess** policy to the group the user belongs to. Then the user can perform all operations on CFW except removing items from a blacklist or whitelist. Example:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "cfw:blackWhite:delete"
            ]
        },
    ]
}
```

- Multi-action policy

  A custom policy can contain the actions of multiple services that are of the project-level type. The following is an example policy containing actions of multiple services:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cfw:instance:get",
                "cfw:eipStatistics:get"
            ]
        },
       {
            "Effect": "Allow",
            "Action": [
                "hss:hosts:switchVersion",
                "hss:hosts:manualDetect",
                "hss:manualDetectStatus:get"
```

```
            ]
        }
    ]
}
```

14.3 CFW Permissions and Supported Actions

This topic describes fine-grained permissions management for your CFW instances. If your Huawei Cloud account does not need individual IAM users, then you may skip over this section.

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and assign permissions policies to these groups. Users inherit permissions from the groups to which they are added and can perform specified operations on cloud services based on the permissions.

You can grant users permissions by using **roles** and **policies**. Roles are provided by IAM to define service-based permissions depending on user's job responsibilities. Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions.

NOTICE

If the peak TPS is greater than 2000, local authentication is required.

Supported Actions

CFW provides system-defined policies that can be directly used in IAM. You can also create custom policies and use them to supplement system-defined policies, implementing more refined access control.

- Permission: A statement in a policy that allows or denies certain operations.
- Action: Specific operations that are allowed or denied.

Permission	Action
Create a cloud firewall	cfw:instance:create
Add CFW capacity	cfw:instance:alterSpec
Delete a cloud firewall	cfw:instance:delete
Query a cloud firewall	cfw:instance:get
Query the cloud firewall list	cfw:instance:list
Enable or disable EIP protection	cfw:eip:operate
Query the EIP list	cfw:eip:list
Query EIP statistics	cfw:eipStatistics:get
Query policy statistics	cfw:policyStatistics:get

Permission	Action
Create an ACL rule	cfw:acl:create
Modify an ACL rule	cfw:acl:put
Delete an ACL rule	cfw:acl:delete
Query the ACL rule list	cfw:acl:list
Configure ACL rule priority	cfw:acl:setPriority
Create a blacklist or whitelist	cfw:blackWhite:create
Modify a blacklist or whitelist	cfw:blackWhite:put
Delete a blacklist or whitelist	cfw:blackWhite:delete
Query a blacklist or whitelist	cfw:blackWhite:list
Create an IP address group	cfw:ipGroup:create
Modify an IP address group	cfw:ipGroup:put
Delete an IP address group	cfw:ipGroup:delete
Query the IP address group list	cfw:ipGroup:list
Query the details of an IP address group	cfw:ipGroup:get
Add a member to an IP address group	cfw:ipMember:create
Update a member in an IP address group.	cfw:ipMember:put
Delete a member from an IP address group	cfw:ipMember:delete
Query IP address group members	cfw:ipMember:list
Create a service group	cfw:serviceGroup:create
Modify a service group	cfw:serviceGroup:put
Delete a service group	cfw:serviceGroup:delete
Query the details about a service group	cfw:serviceGroup:get
Query the service group list	cfw:serviceGroup:list
Add a member to a service group	cfw:serviceMember:create

Permission	Action
Update a member in a service group	cfw:serviceMember:put
Delete a member from a service group	cfw:serviceMember:delete
Query service group members	cfw:serviceMember:list
Query the ACL log list	cfw:accessControlLog:list
Query the traffic log list	cfw:flowLog:list
Query the attack log list	cfw:attackLog:list
Query the traffic log report	cfw:flowLogReport:get
Query the ACL log report	cfw:accessControlLogReport:get
Query the ACL log report	cfw:attackLogReport:get
Enable basic protection	cfw:ips:start
Disable basic protection	cfw:ips:stop
Query basic protection status	cfw:ipsStatus:get
Configure the IPS mode	cfw:ipsMode:operate
Query the IPS mode	cfw:ipsMode:get
Create a packet capture task	cfw:captureTask:create
Query the packet capture task list	cfw:captureTask:list
Batch delete packet capture tasks	cfw:captureTask:delete
Stop a packet capture task	cfw:captureTask:stop
Download packet capture results	cfw:captureTask:getResult
Query CFW instance resources	cfw:resource:list

15 Audit

15.1 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 15-1 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

15.2 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)**.

16 Monitoring

16.1 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 16-1 CFW metrics

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
used_protection_bandwidth	Boundary Protection Bandwidth Usage (Mbps)	Used Internet 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)
protection_bandwidth_usage	Boundary Protection Bandwidth Usage (%)	Internet 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
internet_protection_bandwidth_usage	Internet Boundary Protection Bandwidth Usage (Mbps)	Bandwidth usage (Mbps) for protection at the Internet boundary. Unit: bit/s	≥ 0 Value type: Float	CFW	Every minute
vpc_protection_bandwidth_usage	Inter-VPC Protection Bandwidth Usage (Mbps)	Bandwidth usage (Mbps) for inter-VPC protection. Unit: bit/s	≥ 0 Value type: Float	CFW	Every minute
internet_protection_bandwidth_usage_rate	Internet Boundary Protection Bandwidth Usage (%)	Bandwidth usage (%) for protection at the Internet boundary. Unit: %	≥ 0 Value type: Float	CFW	Every minute
vpc_protection_bandwidth_usage_rate	Inter-VPC Protection Bandwidth Usage (%)	Bandwidth usage (%) for inter-VPC protection. Unit: %	≥ 0 Value type: Float	CFW	Every minute

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Minute)
internet_protection_pps	Internet Boundary Firewall PPS	PPS of protected objects at the Internet boundary. Unit: N/A	≥ 0 Value type: Float	CFW	Every minute
vpc_protection_pps	Inter-VPC Firewall PPS	PPS of inter-VPC protected objects. Unit: N/A	≥ 0 Value type: Float	CFW	Every minute
ips_hit_count	IPS Rule Hits	Number of times that traffic matches IPS rules.	≥ 0 Value type: Int	CFW	Every minute
ips_deny_count	IPS Rule Block Count	Number of times that traffic is blocked based on IPS rules. Unit: N/A	≥ 0 Value type: Int	CFW	Every minute
acl_hit_count	ACL Rule Hits	Number of times that traffic matches ACL rules. Unit: N/A	≥ 0 Value type: Int	CFW	Every minute
acl_deny_count	ACL Rule Block Count	Number of times that traffic is blocked based on ACL rules. Unit: N/A	≥ 0 Value type: Int	CFW	Every minute

Dimension

Key	Value
fw_instance_id	Firewall ID

16.2 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 Configure parameters as prompted. Key parameters are described below. For more information, see **Creating an Alarm Rule**.

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

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

----End

16.3 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 **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

17 Managing Projects and Enterprise Projects

Selections are available only if you have enabled the enterprise project function, or your account is an enterprise account. An enterprise project provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.

Creating a Project and Assigning Permissions

- Creating a project

  Log in to the management console, click the username in the upper right corner, and select **Identity and Access Management**. In the navigation pane on the left, choose **Projects**. In the right pane, click **Create Project**. On the displayed **Create Project** page, select a region and enter a project name.

- Granting permissions

  You can assign permissions (of resources and operations) to user groups to associate projects with user groups. You can add users to a user group to control which projects they can access and what resources they can perform operations on. To do so, perform the following operations:

  a. On the **User Groups** page, locate the target user group and click **Configure Permission** in the **Operation** column. The **User Group Permissions** page is displayed. Locate the row that contains the target project, click **Configure Policy**, and select the required policies for the project.

  b. On the **Users** page, locate the target user and click **Modify** in the **Operation** column. In the **User Groups** area, add a user group for the user.

Creating an Enterprise Project and Assigning Permissions

- Creating an enterprise project

  On the management console, click **Enterprise** in the upper right corner. The **Enterprise Management** page is displayed. In the navigation pane on the left, choose **Enterprise Project Management**. In the right pane, click **Create Enterprise Project** and enter a name.

NOTE

Enterprise is available on the management console only if you have enabled the enterprise project, or you have an enterprise account. To enable this function, contact customer service.

- Granting permissions

  You can add a user group to an enterprise project and configure a policy to associate the enterprise project with the user group. You can add users to a user group to control which projects they can access and what resources they can perform operations on. To do so, perform the following operations:

  a. Locate the row that contains the target enterprise project, click **More** in the **Operation** column, and select **View User Group**. On the displayed **User Groups** page, click **Add User Group**. In the displayed **Add User Group** dialog box, select the user groups you want to add and move them to the right pane. Click **Next** and select the policies.

  b. In the navigation pane on the left, choose **Personnel Management** > **User Management**. Locate the row that contains the target user, click **More** in the **Operation** column, and select **Add to User Group**. In the displayed **Add to User Group** dialog box, select the user groups for which policies have been configured and click **OK**.

- Associating HSS with enterprise projects

  You can use enterprise projects to manage cloud resources.

  – Selecting an enterprise project when purchasing CFW

    On the page for buying HSS, select an enterprise project from the **Enterprise Project** drop-down list.

  – Adding resources

    On the **Enterprise Project Management** page, you can add existing resources to an enterprise project.

    Value **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.

  For more information, see **Creating an Enterprise Project**.

A Change History

Date	Description
2024-03-06	This issue is the twelfth official release. Added: • Description about the virtual patch rule library in **Configuring Intrusion Prevention** • Description about abnormal external connection alarms in section **Alarm Notification**. • **Security Reports** Optimized: Domain name/domain group content in section **Adding a Protection Rule**.
2023-12-20	This issue is the eleventh official release. Added: • **Viewing a Predefined Address Group** • **Viewing a Predefined Service Group**
2023-10-13	This is the tenth official release. Added: • Description about traffic situation and traffic trend in **Checking the CFW Dashboard**. • **Policy Assistant** • **Security Dashboard** • **Traffic Analysis** and its subsections • The **EIP Not Protected** alarm in **Alarm Notification**.
2023-08-11	This is the ninth official release. Optimized: • **Managing VPC Border Firewalls** and its subsections • Added the geographical location parameters in **Querying Logs**.

Date	Description
2023-07-14	This is the eighth official release. Added: • **Managing the Antivirus Function** • **Managing Projects and Enterprise Projects** Optimized: • Added related concepts in **VPC Border Firewall Overview**.
2023-05-31	This is the seventh official release. Added: • Security overview and traffic trend in **Checking the CFW Dashboard**. • Sensitive directory scan defense and reverse shell detection in **Configuring Intrusion Prevention**. • **Customizing IPS Signatures** • Log report in **Traffic Analysis**. • **Permissions Management** Optimized: • Added examples for protection rule parameters in **Adding a Protection Rule**. • Import rule parameters in **Managing Protection Rules in Batches**.
2023-04-25	This is the sixth official release. Added: • **Adding a Domain Name Group** • **Network Packet Capture** • Added **VPC Border Firewall Overview** in "Managing Firewalls Between VPCs".
2023-03-30	This is the fifth official release. Added: • **Managing VPC Border Firewalls** and its subsections • **Managing Intrusion Prevention** • **Alarm Notification** • Information about the CFW professional edition.
2022-12-30	This is the fourth official release. Added **Audit**.
2022-10-31	This is the third official release. Added supported regions in **Purchasing CFW**. Added **Monitoring**.

Date	Description
2022-09-30	This is the second official release. Added **Configuring DNS Resolution**.
2022-07-30	This is the first official release.

