Cloud Firewall

User Guide

Issue 17

Date 2025-08-07

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 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 1-1**).

Prerequisites

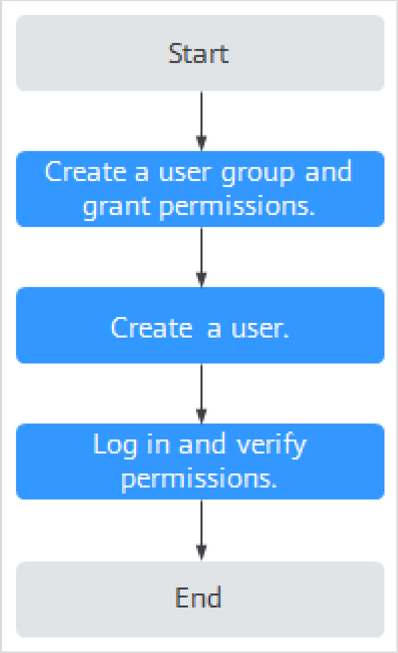
Learn about the permissions supported by CFW in **Table 1-1** and choose policies or roles based on your requirements.

Table 1-1 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 1-1 Process for granting permissions


Start
Create a user group and grant permissions.
Create a user.
Log in and verify permissions.
End

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. **Create an IAM user and add it to the user group**.

   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, switch to the region where it is expected to have the access permission, and verify user permissions.

   - Choose **Cloud Firewall** in the service list. Click **Buy CFW** on the CFW console. If you cannot buy CFW (assuming that only the **CFW ReadOnlyAccess** permission is granted), the **CFW ReadOnlyAccess** policy has already taken effect.
   - Choose any other service in **Service List**. Assume that the current policy contains only the **CFW ReadOnlyAccess** permission. If a message appears indicating that you have insufficient permissions to access the service, the **CFW ReadOnlyAccess** policy has already taken effect.

2 Purchasing and Changing the Specifications of CFW

2.1 Purchasing Yearly/Monthly Cloud Firewall

Yearly/Monthly payment is a prepaid billing mode and is cost-effective for long-term use.

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

Prerequisites

To use an IAM user, ensure the IAM user has been granted the BSS Administrator and CFW FullAccess permissions. For details, see **Creating a User Group and Granting Permissions**.

Constraints

- CFW can be used only in the region where it was purchased. To use it in another region, switch to that region and purchase it. For details about the regions where CFW is available, see **Function Overview**.

Editions

CFW supports the yearly/monthly (prepaid) and pay-per-use billing modes.

- Yearly/Monthly CFW instances support the standard edition, and professional edition.
- Pay-per-use CFW instances support the professional edition.

For details about the feature differences between editions, see **Editions**.

The application scenarios for different editions are as follows:

- Standard edition

  Suitable for small- and medium-sized enterprises that need to defend against cybersecurity threats like 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, obtain MLPS certification, or have key event assurance requirements.

Purchasing CFW

Perform the following operations to purchase a firewall instance of the desired edition.

Standard Edition Firewalls

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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

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

Table 2-1 Parameters for purchasing the standard edition CFW

Parameter		Description
Billing Mode		Yearly/Monthly
Region		Region where the CFW is to be purchased. CFW can be used in the selected region only. To use CFW in another region, switch to the corresponding region and then purchase it. For details about the regions where CFW is available, see **Can CFW Be Used Across Clouds or Regions?**
Edition	-	Select the standard edition.
	Add EIP Protection Capacity	(Optional) The number of additional EIPs to be protected. Value range: 0 to 2,000. Configure additional capacities to purchase. For example, 20 EIPs are protected by the standard edition (included in the package fee) by default. If you have 65 EIPs, you only need to enter **45**.

Parameter		Description
	Internet Border Protection Bandwidth	(Optional) Additional peak inbound or outbound traffic. The value range is 0 to 50,000 Mbit/s per month. (The value must be an integer multiple of 5.) ● Configure additional capacities to purchase. For example, up to 10 Mbit/s is protected by the standard edition (included in the package fee) by default. If your protection traffic is 200 Mbit/s, you only need to enter **190**. ● The protection traffic is determined based on the maximum inbound or outbound traffic, whichever is higher.
Advanced Settings	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.
	Enterprise Project	Enterprise project. In the drop-down list, select an enterprise project. The firewall will be put under that enterprise project for billing management, but its protection scope will not be affected. The firewall can protect the resources of all enterprise projects. This option is only available if you have enabled enterprise projects, or if you are logged in using an enterprise master account. To use this function, **enable Enterprise Center**. You can use an enterprise project to centrally manage your cloud resources and members by 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.
	Tags	(Optional) 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 CFW, you need to add tags in compliance with the policy. If a tag does not comply with the tag policies, firewall instance creation may fail. Contact your organization administrator to learn more about tag policies.

Parameter	Description
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 information and click **Next**.

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

Professional Edition Firewalls

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

Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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

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

Table 2-2 Parameters for purchasing the professional edition CFW

Parameter		Description
Basic Settings	Billing Mode	Yearly/Monthly
	Region	Region where the CFW is to be purchased. CFW can be used in the selected region only. To use CFW in another region, switch to the corresponding region and then purchase it. For details about the regions where CFW is available, see **Can CFW Be Used Across Clouds or Regions?**
Edition	-	Edition. Select the professional edition.

Parameter		Description
	Add EIP Protection Capacity	(Optional) The number of additional EIPs to be protected. Value range: 0 to 2,000. Configure additional capacities to purchase. For example, 50 EIPs are protected by the professional edition (included in the package fee) by default. If you have 65 EIPs, you only need to enter **15**.
	Internet Border Protection Bandwidth	(Optional) Additional peak inbound or outbound traffic. The value range is 0 to 50,000 Mbit/s per month. (The value must be an integer multiple of 5.) ● Configure additional capacities to purchase. For example, up to 50 Mbit/s per month is protected by the standard edition (included in the package fee) by default. If your protection traffic is 200 Mbit/s per month, you only need to enter **150**. ● The protection traffic is determined based on the maximum inbound or outbound traffic, whichever is higher.
	Protected VPCs	(Optional) Select the number of VPCs to be expanded. The value ranges from 0 to 1,000. ● Only the professional edition supports inter-VPC protection. ● By default, two VPCs are protected by the professional edition (included in the package fee). If you have three VPCs, you only need to enter **1**. ● For each VPC you add, the protected peak traffic increases by 200 Mbit/s.
Advanced Settings	Enterprise Project	Enterprise project. In the drop-down list, select an enterprise project. The firewall will be put under that enterprise project for billing management, but its protection scope will not be affected. The firewall can protect the resources of all enterprise projects. This option is only available if you have enabled enterprise projects, or if you are logged in using an enterprise master account. To use this function, **enable Enterprise Center**. You can use an enterprise project to centrally manage your cloud resources and members by project. Value **default** indicates the default enterprise project. The original resources of your account and the resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.

Parameter		Description
	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.
	Tags	(Optional) 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 CFW, you need to add tags in compliance with the policy. If a tag does not comply with the tag policies, firewall instance creation may fail. Contact your organization administrator to learn more about tag policies.
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 information and click **Next**.

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

After the payment is successful, you can view the purchased firewall edition on the **Dashboard** page of the console.

References

- For details about how to view the basic information and overall protection capabilities of a firewall instance, see **CFW Dashboard**.
- If the current firewall specifications cannot meet service requirements, you can upgrade the firewall edition or purchase an expansion package. For details, see **Upgrading a CFW** and **Changing the Number of CFW Expansion Packages**.
- For details about how to purchase a firewall in pay-per-use mode, see **Purchasing a Pay-per-Use CFW**.
- If you no longer need the firewall, unsubscribe from it. For details, see **Unsubscribing from CFW**.

2.2 Purchasing a Pay-per-Use CFW

Pay-per-use billing is a postpaid billing mode. A pay-per-use CFW can be provisioned and deleted at any time. CFW instances are billed by second. The system generates a bill every hour based on the protected traffic and deducts the billed amount from the account balance.

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

Only the professional edition in certain regions can be billed in pay-per-use mode. For details about the regions that support pay-per-use billing, see **Function Overview**.

Prerequisites

To use an IAM user, ensure the IAM user has been granted the BSS Administrator and CFW FullAccess permissions. For details, see **Creating a User Group and Granting Permissions**.

Constraints

- CFW can be used only in the region selected during purchase. To use it in another region, switch to the corresponding region and then purchase it. The pay-per-use billing mode firewall is supported only in certain regions. For details, see **Function Overview**.
- The maximum protection bandwidth is 1 Gbit/s. (It refers to the total traffic passing through the firewall, that is, the Internet border protection bandwidth plus the VPC border protection bandwidth).
- Only the CFW professional edition supports pay-per-use billing.

Purchasing a Pay-per-Use Professional CFW

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

Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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**. The **Buy CFW** page is displayed.

Table 2-3 Parameters for CFW

Parameter	Description
Billing Mode	If you select **Pay-per-use**, you will be charged for the protection on your workloads from purchase to unsubscription.

Parameter	Description
Region	Region where the CFW is to be purchased. CFW can be used in the selected region only. To use CFW in another region, switch to the corresponding region and then purchase it. For details about the regions where CFW is available, see **Can CFW Be Used Across Clouds or Regions?**
Edition	Currently, only the professional edition is supported.
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.
Enterprise Project	Enterprise project. Select the enterprise project that you belong to from the drop-down list. The purchased CFW instance will be put under that enterprise project for billing management, and will be able to protect the resources of all enterprise projects. This option is only available if you have enabled enterprise projects, or if you are logged in using an enterprise master account. To use this function, **enable Enterprise Center**. You can use an enterprise project to centrally manage your cloud resources and members by project. Value **default** indicates the default enterprise project. The original resources of your account and the resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.
Tags	(Optional) It is recommended that you use the TMS predefined tag function to add the same tag to different cloud resources. If your organization has configured a tag policy for CFW, you need to add tags in compliance with the policy. If a tag does not comply with the tag policies, firewall instance creation may fail. Contact your organization administrator to learn more about tag policies.

Step 5 Confirm the information and click **Next**.

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

After the payment is successful, you can view the purchased firewall edition on the **Dashboard** page of the console.

References

- For details about how to view the basic information and overall protection capabilities of a firewall instance, see **CFW Dashboard**.
- If the current firewall specifications cannot meet service requirements, you can upgrade the firewall edition or purchase an expansion package. For details, see **Upgrading a CFW** and **Changing the Number of CFW Expansion Packages**.
- For details about how to purchase a yearly/monthly firewall, see **Purchasing Yearly/Monthly Cloud Firewall**.
- If you no longer need the firewall, unsubscribe from it. For details, see **Unsubscribing from CFW**.

2.3 Upgrading a CFW

If the functions of the current CFW cannot meet your requirements, you can upgrade the CFW edition.

Constraints

Only yearly/monthly firewalls support the upgrade of the service edition. **Pay-per-use** firewalls support only the professional edition and are charged based on the protected traffic.

Upgrading the Standard Edition to the Professional Edition

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

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

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

Step 4 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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

Effective Conditions

After the payment is successful, you can view the purchased firewall edition on the **Dashboard** page of the console.

References

- **How Do I Renew CFW?**
- **How Do I Unsubscribe from CFW?**

2.4 Changing the Number of CFW Expansion Packages

After purchasing a CFW, you can increase or decrease the number of protected EIPs and VPCs and the peak traffic at the Internet border.

Constraints

- Only the number of expansion packages of yearly/monthly firewalls can be changed.
- Peak protection traffic at Internet boundary: 5 Gbit/s for a standard edition CFW and 10 Gbit/s for a professional edition CFW.

Modifying 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.

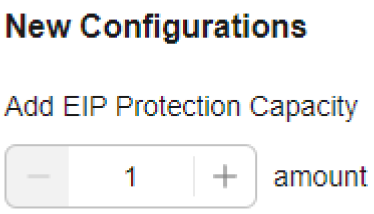
Step 3 In the navigation pane on the left, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

Step 4 In the **Firewall Details** area, click **Modify** on the right of **Used/Available EIP Protection Quota**, **Used/Available VPC Protection Quota**, or **Internet Border Protection Bandwidth**. The protection capacity modification page is displayed.

Step 5 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



New Configurations

Add EIP Protection Capacity

− 1 + amount

Step 6 Confirm the order details. Select the check box to acknowledge the risks and possible costs, and to agree to the change. Click **Next** in the lower right corner.

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

----End

Unsubscribing from an Extension Package

Step 1 Log in to the management console.

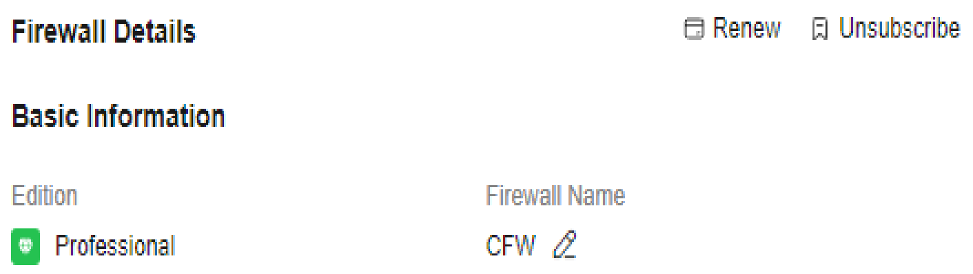
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Figure 2-2 Unsubscribing



Firewall Details

Basic Information

Edition: Professional

Firewall Name: CFW

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 CFW Dashboard

On the **Dashboard** page, you can view the basic information, overall protection capabilities, traffic topology , and statistics of firewall instances to learn about the security status and traffic of cloud assets at any time.

Constraints

VPC border protection details can be viewed only after a **VPC border firewall** is configured.

Checking the Dashboard

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

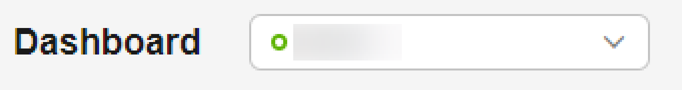
Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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) Switch or view firewall instances.

- Switch to another firewall instance: Select a firewall from the drop-down list in the upper left corner of the page.

  Figure 3-1 Switching to another firewall instance

- View firewall instance information: Click **Firewall List** in the upper right corner. For details, see **Table 3-1**.

  Figure 3-2 Viewing firewall instance information

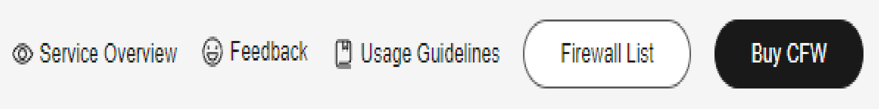
  

Table 3-1 Firewall instance information

Parameter	Description
Firewall Name/ID	Name and ID of the firewall.
Status	Firewall status.
Edition	Edition of a firewall.
Available EIP Protection Quota	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	View details.

Step 5 On the **Dashboard** page, you can check the following modules:

- **Resource Overview**
- **Security Events**
- **Protection Rules**
- **Operations Dashboard**
- **Firewall Details**

----End

Resource Overview

You can view the protection status of all cloud resources (EIPs and VPCs) in the current region under the current account.

Security Events

View the overall protection details of intrusion prevention to quickly locate cloud assets that need protection.

- In the upper right corner, change the query range, from 5 minutes to 7 days.
- Add a protection policy to handle the IP addresses of the abnormal external connections.
  a. Click the number of **Abnormal External Destination IP Addresses**.
  b. In the displayed dialog box, select an IP address.
  c. Generate an address group:
     - Create as an address group: A new address group will be generated.
     - Add to an existing address group: Add the item to an existing address group.

d. Add the address group to the protection rule or blacklist/whitelist. For details, see **Access Control Policy Overview**.

Protection Rules

View the number of inactive policies and the total number of policies.

For details about the policies that are not matched, click the number of **Policies Inactive for Over a Month** to go to the **Policy Assistant** page and view the policies at the bottom.

Operations Dashboard

- Click the **Internet Borders** or **Inter-VPC Borders** tab to view the overall protection data of the corresponding resources.
- In the upper right corner, change the query range, from 5 minutes to 7 days.
- **Peak Inbound/Outbound Traffic**, **Inbound/Outbound 95th Percentile Bandwidth**, and **Access Control**:

  View the traffic blocked by access control policies, the 95th percentile inbound and outbound bandwidth, and the maximum inbound and outbound traffic. For details, see **Table 3-2**.

  Table 3-2 Peak inbound/outbound traffic, inbound/outbound 95th percentile bandwidth, and access control

Time Range	Value
Last 1 hour	Maximum value within every minute
Last 24 hours	Maximum value within every 5 minutes
Last 7 days	Maximum value within every hour
Custom	● 5 minutes to 6 hours: maximum value within every minute ● 6 hours (included) to 3 days: maximum value within every 5 minutes ● 3 (included) to 7 days (included): maximum value within every 30 minutes

  – Peak traffic: The system collects bandwidth in every statistical period. The maximum value within a certain period of time is regarded as the peak traffic.

    For example, if the outbound peak traffic is 100 bit/s, the maximum bandwidth within a certain period of time (for example, 24 hours) is 100 bit/s.

  – 95th percentile bandwidth: The system collects bandwidth in every statistical period, and sorts the bandwidth values in descending order, and removes the top 5% bandwidth values. The remaining maximum bandwidth is the 95th percentile bandwidth.

For example, if the 95th percentile bandwidth in the outbound direction is 100 bit/s, that means after the bandwidth values are sorted in descending order and the highest 5% value is removed within a certain period of time (for example, 24 hours), the remaining maximum bandwidth is 100 bit/s.

- **Traffic Trend**:

  Inbound, outbound, and overall traffic changes. You can select **Average** or **Maximum** in the upper right corner. For details about how they are calculated, see **Table 3-3**.

Table 3-3 Traffic trend statistics

Time Range	Average	Maximum
Last 1 hour	Average value within every minute	Maximum value within every minute
Last 24 hours	Average value within every 5 minutes	Maximum value within every 5 minutes
Last 7 days	Average value within every hour	Maximum value within every hour
Custom	● 5 minutes to 6 hours: average value within every minute ● 6 hours (included) to 3 days: average value within every 5 minutes ● 3 (included) to 7 days (included): average value within every 30 minutes	● 5 minutes to 6 hours: maximum value within every minute ● 6 hours (included) to 3 days: maximum value within every 5 minutes ● 3 (included) to 7 days (included): maximum value within every 30 minutes
Note: Data is updated in real time based on traffic statistics.		

- **Attacks**: View the accesses allowed or blocked by the intrusion prevention feature. For details about its configuration, see **Configuring Intrusion Prevention**.
- **Access Control**: View the accesses blocked or allowed by the access control policy. For details about its configuration, see **Access Control**.

Firewall Details

View details about the firewall instance in the **Firewall Details** area on the right of the page. For details about the parameters, see **Table 3-4**.

Table 3-4 Firewall instance details

Parameter		Description	Related Operations
Basic Information	Edition	Edition of the firewall. Options: **Standard**, **Professional**	For details about how to upgrade the edition, see **Upgrading a CFW**.
	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.	-
	Enterprise Project	Enterprise project that the firewall belongs to.	-
Flavor	Used/ Available EIP Protection Quota	*Number of protected EIPs/Total number of EIPs* under the current CFW instance.	For details about how to purchase or unsubscribe from an expansion package, see **Changing the Number of CFW Expansion Packages**.
	Used/ Available VPC Protection Quota	*Number of protected VPCs/Total number of VPCs* under a firewall instance.	
	Internet Border Protection Bandwidth	Maximum inbound or outbound traffic of all EIPs protected by CFW.	
	VPC Border Protection Bandwidth	Peak east-west traffic that can be protected. Maximum total traffic of all VPCs protected by CFW.	
	Used/ Available Protection Rules	*Number of created protection rules/Total number of protection rules that can be created* under a firewall instance.	

Parameter		Description	Related Operations
Transaction Details	Billing Mode	Billing mode.	For details about the billing modes, see **Billing Modes**.
	Upon Expiration	Billing policy after the firewall instance expires.	
	Created	Time at which the firewall instance is created.	
	Expires	Estimated expiration time of the firewall instance.	
	Last Transaction Order	Latest transaction order of the firewall instance.	
Tags		Configure tags to identify firewalls so that you can classify firewall instances. For details about Tag Management Service (TMS), see **Resource Tag Overview**.	-

4 CFW Protection

4.1 Enabling Internet Border Traffic Protection

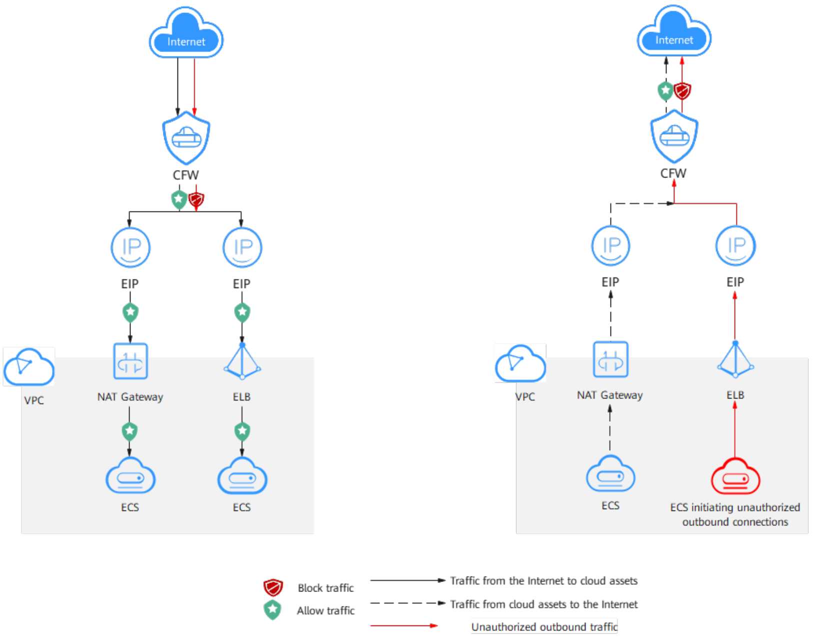
CFW protects Internet border traffic by protecting EIPs. After EIP protection is enabled, your service traffic will pass through CFW. By default, all traffic is allowed.

After protection is enabled, you can configure an access control policy or IPS mode. CFW will block or allow traffic based on the configuration. For details about how to configure access control, see **Configuring Protection Rules**. For details about IPS, see **Configuring Intrusion Prevention**.

What Is Internet Border Traffic?

Internet border traffic, a type of north-south traffic, is exchanged between cloud assets and the Internet. It includes inbound traffic (from the Internet to cloud assets) and outbound traffic (from cloud assets to the Internet).

Figure 4-1 Internet border traffic protection


Internet
CFW
EIP
EIP
VPC
NAT Gateway
ELB
ECS
ECS
Internet
CFW
EIP
EIP
VPC
NAT Gateway
ELB
ECS
ECS initiating unauthorized outbound connections
Block traffic
Allow traffic
Traffic from the Internet to cloud assets
Traffic from cloud assets to the Internet
Unauthorized outbound traffic

Protected Objects

ECSs, NAT gateways, ELBs, and other resources bound to EIPs.

Protection Specifications

The Internet border protection specifications include the number of protected EIPs and the Internet border protection bandwidth.

Table 4-1 Internet border protection specifications

Specifications	Description	Yearly/Monthly Billing	Pay-per-Use Billing
Protected EIPs	Total number of EIPs that can be protected by the current firewall instance.	It depends on the number of added EIP protection quota you purchased. For details about the default quota, see **Features**. If the quota is insufficient, you can purchase an extension package. For details, see **Modifying an Extension Package**.	Up to 1,000 EIPs, and up to 1 Gbit/s traffic protection for Internet and VPC borders are available. The capacities cannot be expanded.

Specifications	Description	Yearly/Monthly Billing	Pay-per-Use Billing
Internet Border Protection Bandwidth	Maximum Internet border traffic that can be protected by the current firewall instance. The value is the maximum inbound or outbound traffic.		

Constraints

- Currently, IPv6 addresses cannot be protected.
- An EIP can only be protected by one firewall.
- The number of EIPs that can be protected by a single firewall instance by default is as follows:
  - Yearly/Monthly CFW:
    - Standard edition: 20
    - Professional edition: 50

    You can purchase expansion packages to increase the number to a maximum of 2,000. For details, see **Changing the Number of CFW Expansion Packages**.
  - Pay-per-use firewall (professional edition): 1,000. It cannot be increased.

Impacts on Services

- If no protection rule or blacklist is configured to block all traffic, enabling or disabling EIP protection will not interrupt services.
- If there is a protection rule or blacklist in effect that blocks all traffic, enabling EIP protection may interrupt services. Before enabling protection, check for persistent connections and services that do not support session reestablishment.
  - For details about how to edit a protection rule, see **Managing Protection Rules**.
  - For details about how to edit a blacklist, see **Managing the Blacklist and the Whitelist**.

Enabling Internet Border Traffic Protection

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

Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Enable EIP protection.

IPv6 protection is not supported for EIPs. An EIP can be protected by only one firewall.

- 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 that you want to enable protection and click **Enable Protection** above the list.

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

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

----End

Auto-protecting New EIPs

If auto-protection on new EIPs is enabled, CFW automatically synchronizes EIPs on the hour and enables protection for new EIPs. The traffic of the EIPs will be protected by the firewall.

How to enable: Go to the **Assets** > **EIPs** page and enable **Auto Protect New EIP**.

NOTE

If you have configured **multi-account protection** and enabled **Auto Protect New EIP**, notice that the result of auto protection varies by user operations:

- If you wait for CFW to automatically synchronize and protect new EIPs, all the new EIPs under all accounts (including the current account) will be protected.
- If you opened the **Assets** > **EIPs** page or call the API for **querying EIPs** before the automatic synchronization and protection, the EIPs under the current account will be automatically protected, but you will need to manually enable protection for the new EIPs under other accounts.

Follow-up Operations

- For details about how to view the traffic trend and statistics of CFW, see **Traffic Analysis**. For details about traffic records, see **Traffic Logs**.
- After protection is enabled, all traffic is allowed by default. CFW will block traffic based on the policies you configure.
  - To implement traffic control, configure a protection policy. For details, see **Configuring Protection Rules to Block or Allow Internet Border Traffic** or **Adding Blacklist or Whitelist Items to Block or Allow Traffic**.

        - Allow or block traffic based on protection rules.
            - Traffic allowing rule: The allowed traffic will be checked by functions such as intrusion prevention system (IPS) and antivirus.
            - Traffic blocking rule: Traffic will be directly blocked.
        - Allow or block traffic based on the blacklist and whitelist:
            - Whitelist: Traffic will be directly allowed without being checked by other functions.
            - Blacklist: Traffic will be directly blocked.
    - For details about how to block network attacks, see **Configuring Intrusion Prevention**.

Related Operations

- Disabling EIP protection

  ⚠ CAUTION

  If EIP protection is disabled, CFW no longer protects the EIP traffic, and EIPs may be exposed to attacks. **Exercise caution when performing this operation.**

    - 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.
- Exporting the EIP list: Click **Export** above the list and select an export scope.
- To protect the EIPs of other accounts, see **Multi-account Protection**.
- To disable firewall protection for EIPs, click **CFW Kill Switch** in the upper right corner of the list. In the dialog box that is displayed, click **OK**.
    - To restore EIP protection, click **One-Click Restore** in the upper part of the page.
    - The EIP cannot be enabled or disabled during the escape or recovery. After the operation is successful, the EIP can be enabled or disabled.

4.2 Enabling VPC Border Traffic Protection

4.2.1 VPC Border Firewall Overview

CFW can protect VPC traffic. After protection is enabled, your service traffic will pass through CFW. All traffic will be allowed by default.

After protection is enabled, you can configure an access control policy or IPS mode. CFW will block or allow traffic based on the configuration. For details about how to configure access control, see **Configuring Protection Rules**. For details about IPS, see **Configuring Intrusion Prevention**.

This section describes the basic concept of VPC border and related CFW configuration.

What Is VPC Border Traffic?

VPC border traffic, a type of east-west traffic, is exchanged between a VPC and an integrated data center (IDC), or between two VPCs. You can configure a VPC border firewall on CFW and use Enterprise Router to visualize and protect internal service access.

A VPC border firewall supports cross-account protection. For example, if account A has VPC_A and account B has VPC_B, you only need to configure an enterprise router and a firewall under account A, share the enterprise router with account B, and add an attachment to VPC_B. In this way, the VPCs of accounts A and B can both be protected.

Figure 4-2 Traffic between a VPC and an IDC

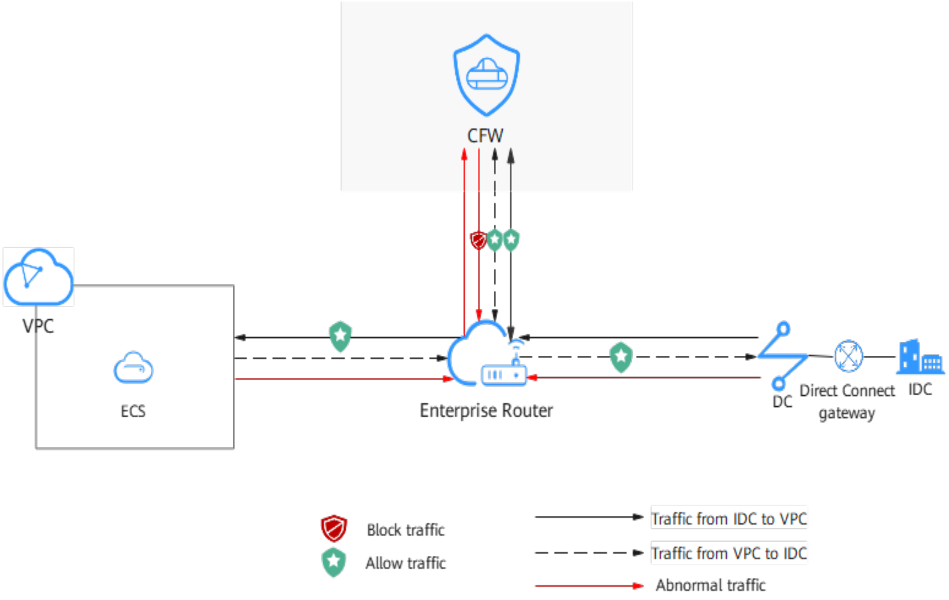
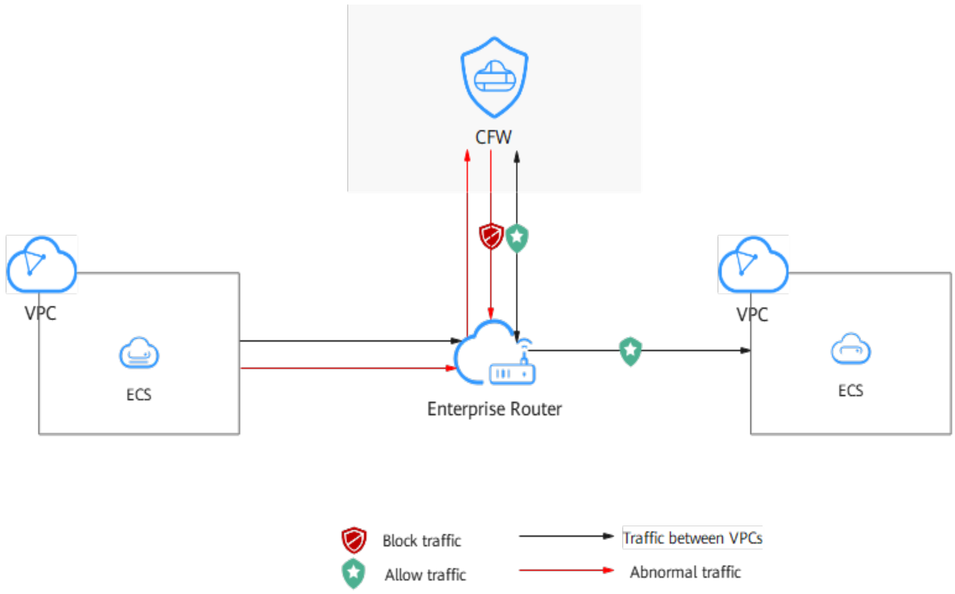


Figure 4-3 Traffic between VPCs



Supported Protected Objects

- VPC
- Virtual gateway (VGW) attachment
- VPN
- Global DC gateway (DGW)

Protection Specifications

The protection specifications of a VPC border firewall include the number of protected VPCs and the VPC border protection bandwidth.

Table 4-2 VPC border firewall protection specifications

Specifications	Description	Yearly/Monthly Billing	Pay-per-Use Billing
Protected VPCs	Total number of VPCs that can be protected by the current firewall instance.	It depends on the number of protected VPCs. By default, two VPCs and 200 Mbit/s VPC border traffic can be protected. If the quota is insufficient, you can purchase expansion packages. For details, see **Modifying an Extension Package**.	Up to 20 VPCs, and up to 1 Gbit/s traffic protection for Internet and VPC borders are available. The capacities cannot be expanded.
VPC Border Protection Bandwidth	Maximum VPC border traffic that can be protected by the current firewall instance.		

Constraints

- Only the professional edition supports VPC border firewalls.
- The number of VPCs that can be protected by a single firewall instance by default is as follows:
  - Professional edition (yearly/monthly): 2

    You can purchase expansion packages to increase the number to a maximum of 1,000. For details, see **Changing the Number of CFW Expansion Packages**.
  - Professional edition (pay-per-use): 20. It cannot be increased.
- Traffic diversion depends on the enterprise router.
- To use public network CIDR blocks other than 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, or the 100.64.0.0/10 segment reserved for carrier-level NAT as private network CIDR blocks, **modify private network CIDR blocks** or **submit a service ticket** to expand your private IP CIDR blocks, or CFW may fail to forward traffic between your VPCs.

Impacts on Services

- If there is no protection rule or blacklist that blocks all traffic, enabling or disabling VPC protection will not interrupt services.
- If a protection rule or blacklist is configured to block all traffic, enabling VPC protection may interrupt services. Before enabling protection, check for persistent connections and services that do not support session reestablishment.
  - For details about how to edit a protection rule, see **Managing Protection Rules**.
  - For details about how to edit a blacklist, see **Managing the Blacklist and the Whitelist**.

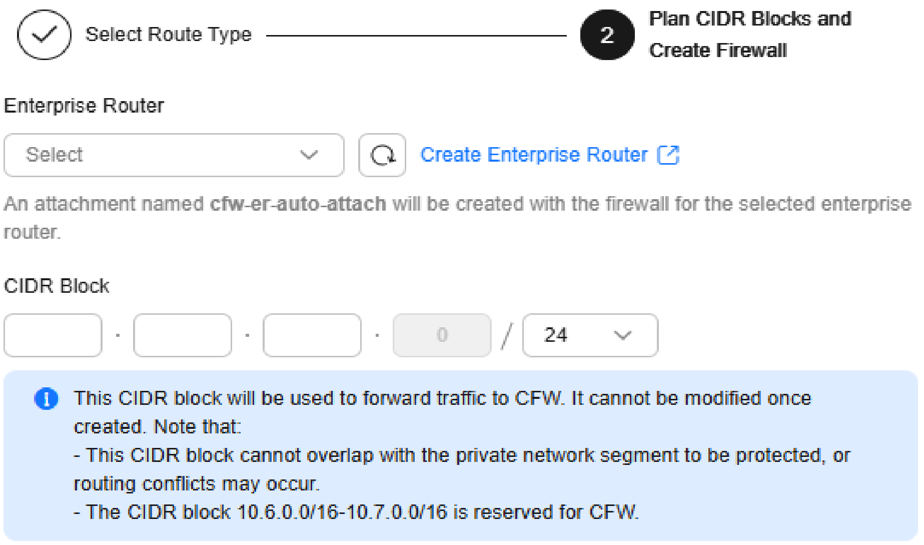
Configuration and Usage Process

Because of dependency issues, the new and old versions of the VPC border firewall in enterprise router mode are used in different projects. You can check which version you are using on the firewall configuration page.

VPC Border Firewall (New Version)

Figure 4-4 shows the configuration page. **Table 4-3** shows the configuration process. For details about the configuration document, see **Enterprise Router Mode (New)**.

Figure 4-4 VPC border firewall (new version)



An attachment named **cfw-er-auto-attach** will be created with the firewall for the selected enterprise router.

This CIDR block will be used to forward traffic to CFW. It cannot be modified once created. Note that:
- 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.

Table 4-3 Configuration and usage process in enterprise router mode (new)

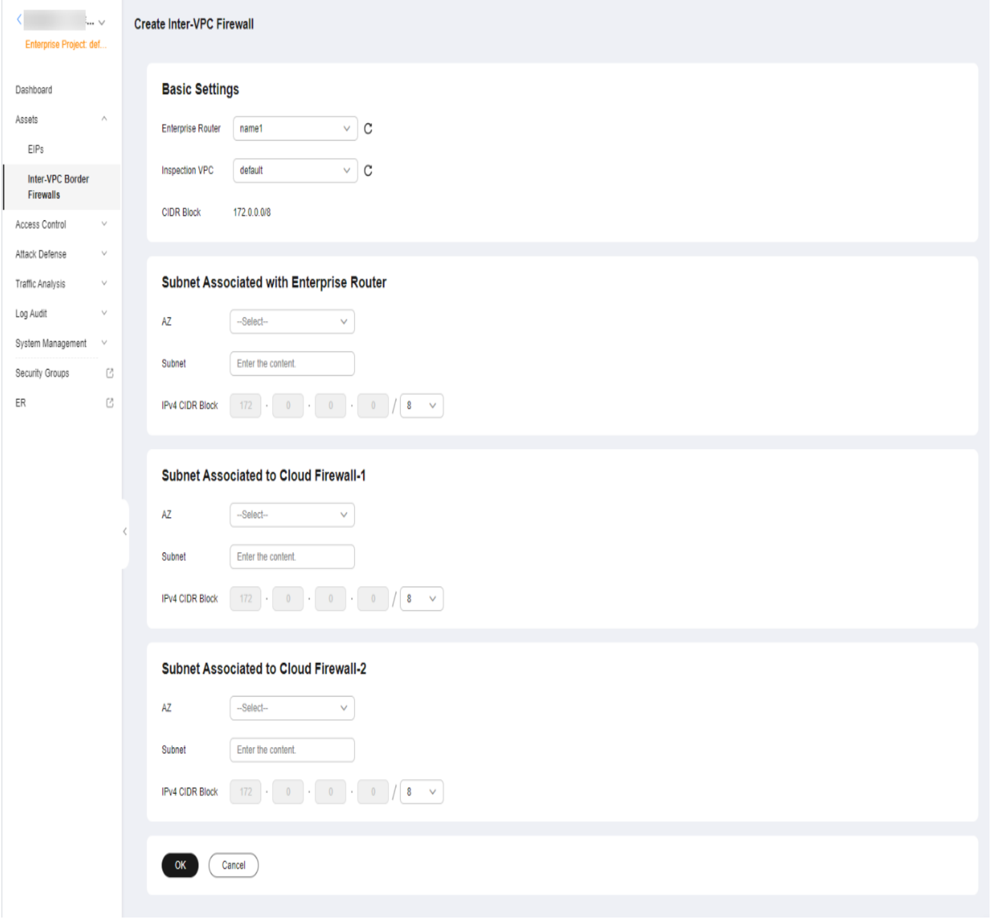
Procedure	Description
Creating a VPC Border Firewall	Plan CIDR blocks for traffic diversion on the VPC border firewall. **NOTE** The traffic diversion VPC does not occupy the VPC protection quotas under your account.
Configuring the Enterprise Router to Direct Traffic to the Cloud Firewall	Use an enterprise router to transmit traffic among VPCs and CFW. ● Add connections between protected VPCs and an enterprise router. ● In the enterprise router, create an association route table and a propagation route table to transmit traffic between VPCs and firewall. ● Add a route pointing to the enterprise router for each VPC.
Enabling the VPC Border Firewall and Ensuring the Traffic Passes Through CFW	Enable VPC border traffic protection and check whether the traffic passes through CFW.
Adding a VPC Border Protection Rule	Allow or block traffic based on protection rules. (Allowed traffic will be checked by IPS and antivirus functions.)
Adding Blacklist or Whitelist Items to Block or Allow Traffic	Allow or block traffic based on the blacklist and whitelist. (Traffic allowed or blocked in this way will not be checked by other functions.)

Procedure	Description
Access Control Logs	Check whether protection policies take effect.
Adding a Protected VPC	Add a VPC to be protected.

VPC Border Firewall (Old Version)

Figure 4-5 shows the configuration page. Figure 4-6 shows the configuration process. For details about the configuration document, see Enterprise Router Mode (Old).

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



Create Inter-VPC Firewall

Basic Settings

Enterprise Router: name1

Inspection VPC: default

CIDR Block: 172.0.0.0/8

Subnet Associated with Enterprise Router

AZ: --Select--

Subnet: Enter the content.

IPv4 CIDR Block: 172 . 0 . 0 . 0 / 8

Subnet Associated to Cloud Firewall-1

AZ: --Select--

Subnet: Enter the content.

IPv4 CIDR Block: 172 . 0 . 0 . 0 / 8

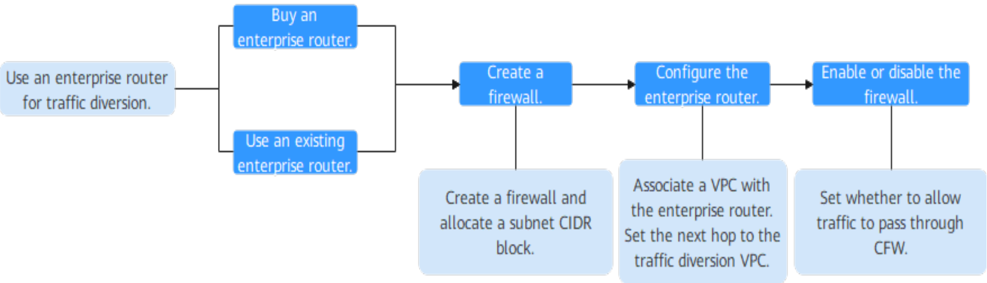
Subnet Associated to Cloud Firewall-2

AZ: --Select--

Subnet: Enter the content.

IPv4 CIDR Block: 172 . 0 . 0 . 0 / 8

Figure 4-6 Configuration process in enterprise router mode


Use an enterprise router for traffic diversion.
Buy an enterprise router.
Use an existing enterprise router.
Create a firewall.
Configure the enterprise router.
Enable or disable the firewall.
Create a firewall and allocate a subnet CIDR block.
Associate a VPC with the enterprise router. Set the next hop to the traffic diversion VPC.
Set whether to allow traffic to pass through CFW.

4.2.2 Enterprise Router Mode (New)

4.2.2.1 Creating a VPC Border 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 **Billing**.
- For details about how to create an enterprise router, see **Creating an Enterprise Router**.

  You are advised to deselect **Default Route Table Association** and **Default Route Table Propagation** while creating a route.

Constraints

Only the professional edition supports VPC border firewalls.

Precautions

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.

Creating 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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

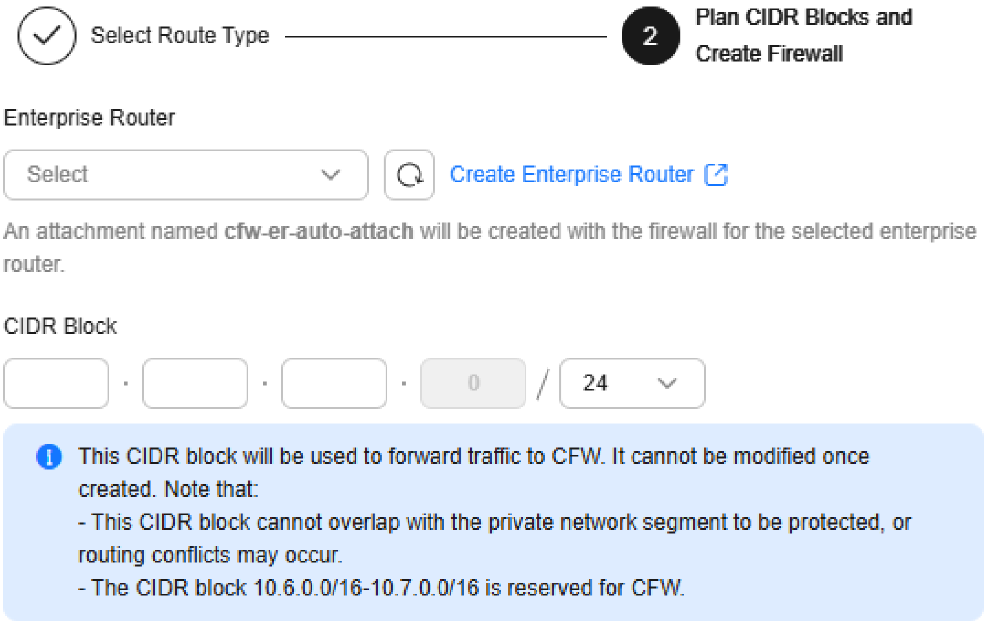
Step 5 In the navigation pane, choose **Assets** > **Inter-VPC Border Firewalls**.

Step 6 Click **Create Inter-VPC Firewall**.

Step 7 In the displayed dialog box, set **Route type** to **Enterprise Router**, and click **Next**.

Step 8 Select an enterprise router and configure a proper CIDR block.

Figure 4-7 Creating a VPC Border Firewall



An attachment named **cfw-er-auto-attach** will be created with the firewall for the selected enterprise router.

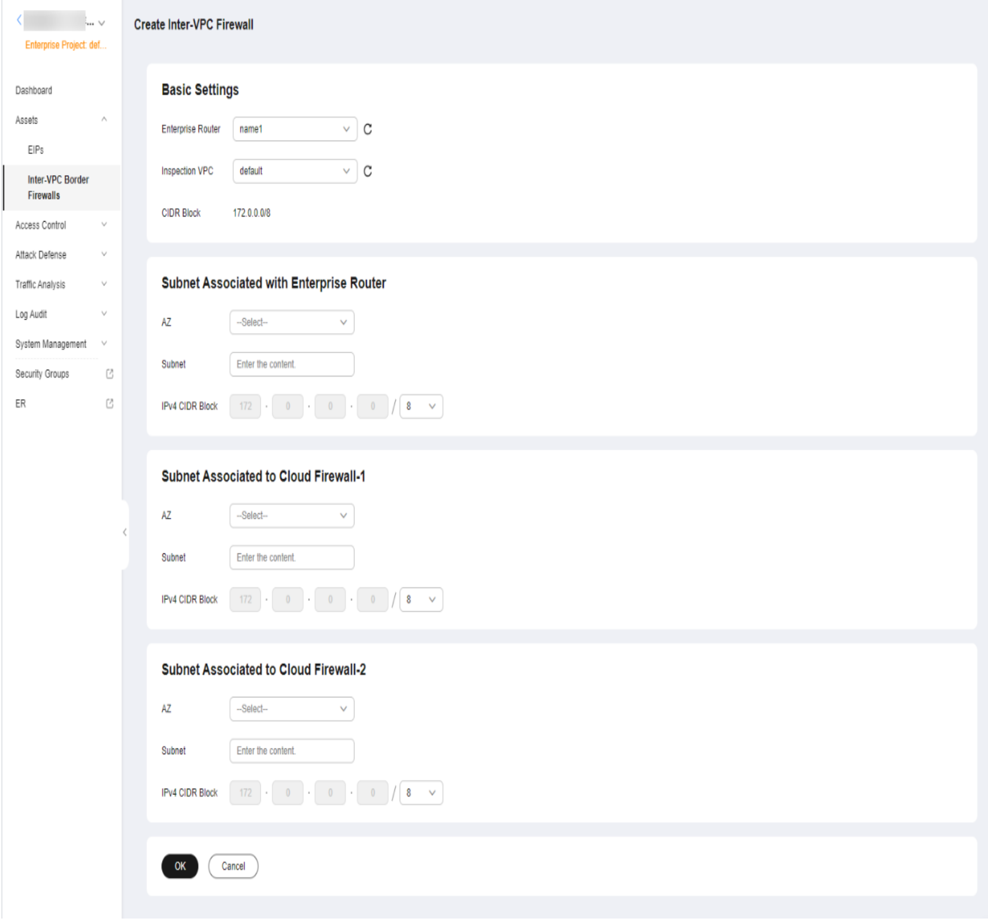
This CIDR block will be used to forward traffic to CFW. It cannot be modified once created. Note that:
- This CIDR block cannot overlap with the private network segment to be protected, or routing conflicts may occur.
- The CIDR block 10.6.0.0/16-10.7.0.0/16 is reserved for CFW.

- 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 specified.

  - This CIDR block cannot overlap with the private CIDR block to be protected, or routing conflicts and protection failures may occur.

- If the page shown in **Figure 4-8** 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 4-8 Creating a VPC border firewall (old version)



Create Inter-VPC Firewall

Basic Settings

Enterprise Router: name1

Inspection VPC: default

CIDR Block: 172.0.0.0/8

Subnet Associated with Enterprise Router

AZ: --Select--

Subnet: Enter the content.

IPv4 CIDR Block: 172 . 0 . 0 . 0 / 8

Subnet Associated to Cloud Firewall-1

AZ: --Select--

Subnet: Enter the content.

IPv4 CIDR Block: 172 . 0 . 0 . 0 / 8

Subnet Associated to Cloud Firewall-2

AZ: --Select--

Subnet: Enter the content.

IPv4 CIDR Block: 172 . 0 . 0 . 0 / 8

Step 9 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

References

Disabling a firewall: After a firewall is created, it cannot be deleted or unsubscribed from. You can disable firewall protection. For details, see **Disabling VPC Border Protection**. If VPC border protection is no longer required, after you disable protection, you still need to **manually restore the configuration of the enterprise router**.

4.2.2.2 Configuring the Enterprise Router to Direct Traffic to the Cloud Firewall

This document describes how to use an enterprise router to divert traffic to CFW and verify network connectivity.

Prerequisites

Ensure the communication is normal when the traffic does not pass through the firewall. For details about traffic verification, see **Verifying Network Connectivity**.

Configuration Principle and Process

Figure 4-9 shows the traffic flow when an enterprise router is configured. **Figure 4-10** shows the process for configuring an enterprise router.

Figure 4-9 Traffic flow

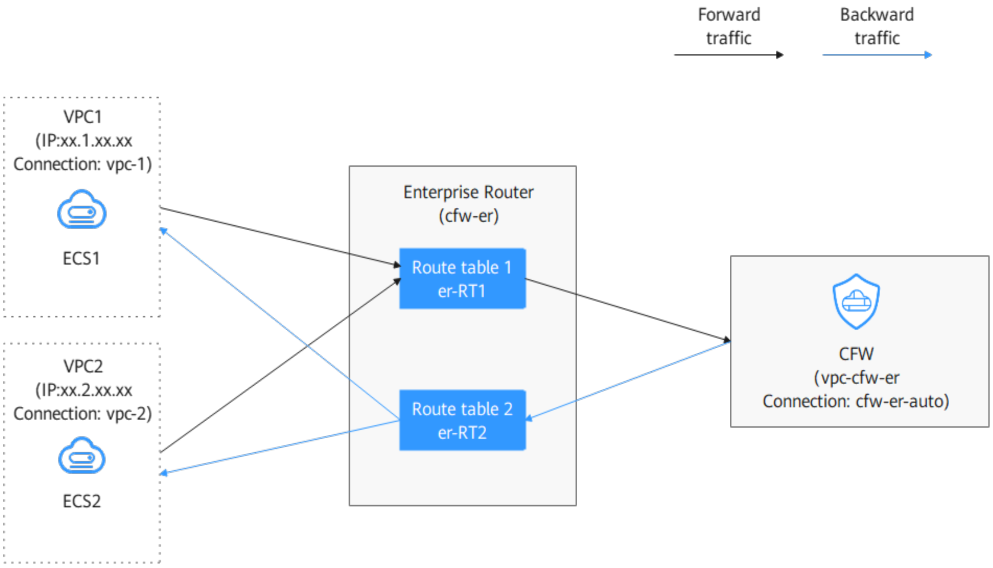
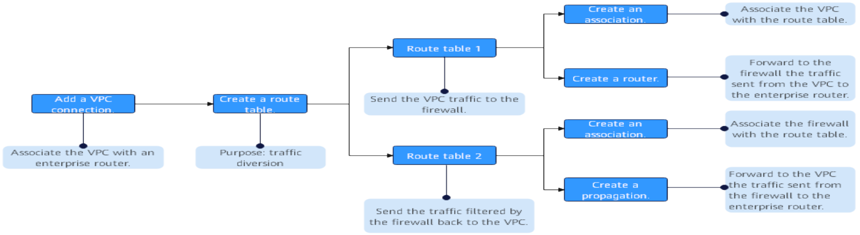


Figure 4-10 Operation process


Add a VPC connection.
Associate the VPC with an enterprise router.
Create a route table.
Purpose: traffic diversion
Route table 1
Send the VPC traffic to the firewall.
Route table 2
Send the traffic filtered by the firewall back to the VPC.
Create an association.
Associate the VPC with the route table.
Create a router.
Forward to the firewall the traffic sent from the VPC to the enterprise router.
Create an association.
Associate the firewall with the route table.
Create a propagation.
Forward to the VPC the traffic sent from the firewall to the enterprise router.

Diverting Traffic to the CFW

Select a configuration mode based on whether an enterprise router has been configured for the current service.

Configuring the Enterprise Router to Direct Traffic to the Cloud Firewall

Step 1 A VPC border firewall has been created. For details, see **Creating a VPC Border Firewall**.

Step 2 In the navigation pane on the left, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

Step 3 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

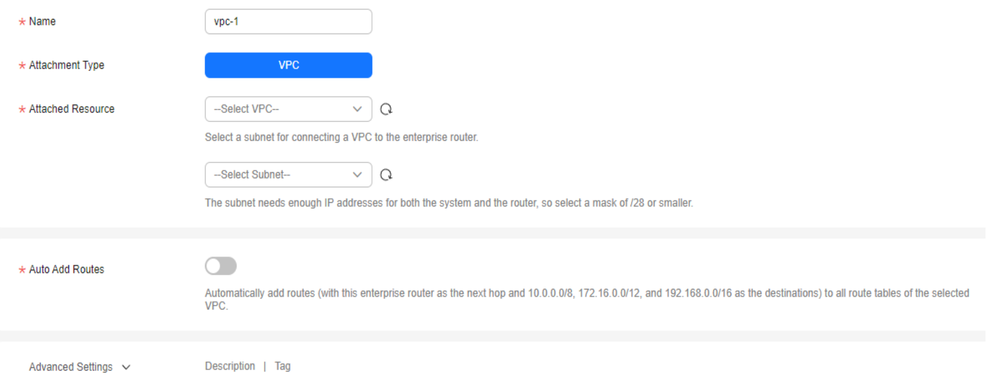
Step 4 In the navigation pane, choose **Assets** > **Inter-VPC Border Firewalls**.

Step 5 Add VPC attachments.

Click **Edit Protected VPC** next to **Firewall Status**. The enterprise router page is displayed. 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 a VPC Attachment to an Enterprise Router**.

Figure 4-11 Adding VPC attachments



* Name: vpc-1

* Attachment Type: VPC

* Attached Resource: --Select VPC--

Select a subnet for connecting a VPC to the enterprise router.

--Select Subnet--

The subnet needs enough IP addresses for both the system and the router, so select a mask of /28 or smaller.

* Auto Add Routes

Automatically add routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the selected VPC.

Advanced Settings

Description | Tag

NOTE

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

  For example, the VPC1 attachment is named **vpc-1**, the VPC2 attachment is named **vpc-2**, and the VPC3 attachment is named **vpc-3**.
- To use the enterprise router of account A to protect VPCs under account B, share the router with account B, and add an attachment in account B. For details, see **Creating a Sharing**. After the sharing is successful, add attachments in account B. Subsequent configurations should still be performed on account A.

Step 6 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 4-4**.

Table 4-4 Route table parameters

Parameter	Description
Name	Route table name. It must meet the following requirements: ● Must contain 1 to 64 characters. ● Can contain letters, numbers, 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**.

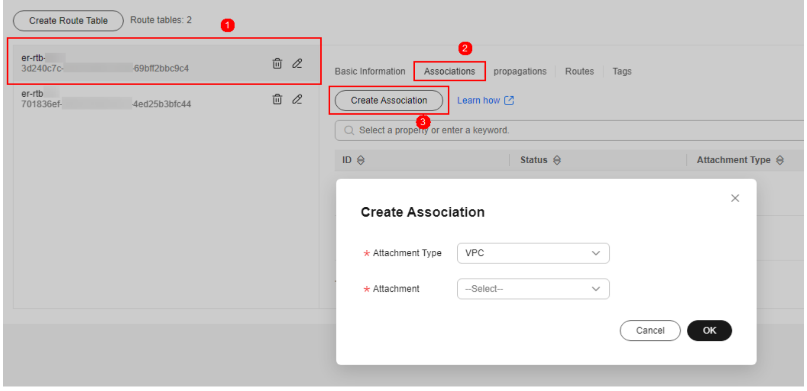
Step 7 Configure the association route table.

1. 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 4-5**.

   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**.

Figure 4-12 Creating an association



er-rtb-[redacted]
3d240c7c-[redacted]69bff2bbc9c4

er-rtb[redacted]
701836ef-[redacted]4ed25b3bfc44

* Attachment Type: VPC

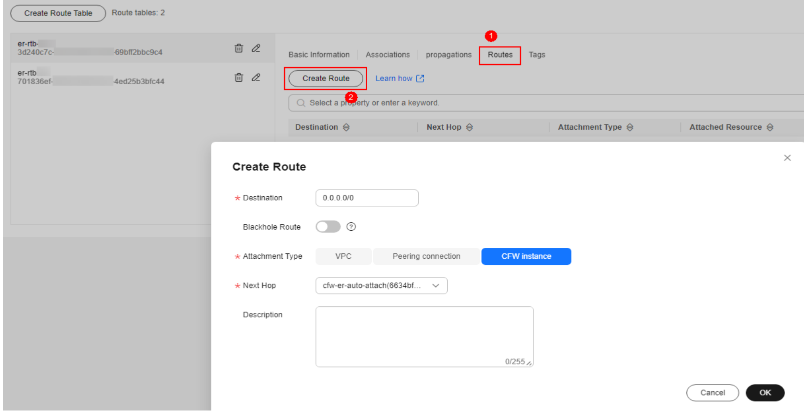
* Attachment: --Select--

Table 4-5 Association parameters

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

2. Configure routes. Click the **Routes** tab and click **Create Route**. Create routes as needed. For more information, see **Table 4-6**.

Figure 4-13 Creating a route



Create Route

* Destination: 0.0.0.0/0

Blackhole Route: off

* Attachment Type: VPC | Peering connection | CFW instance (selected)

* Next Hop: cfw-er-auto-attach(6634bf...

Description: 0/255

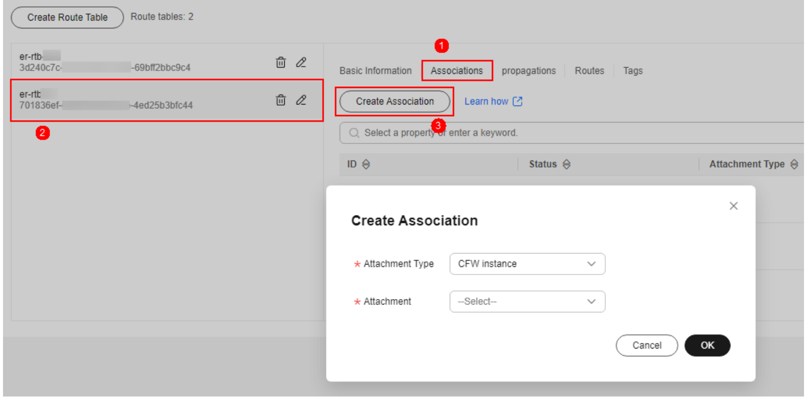
Table 4-6 Route parameters

Parameter	Description
Destination	Set the destination address. – If **0.0.0.0/0** is configured, all the traffic (IPv4) of the VPC is protected by CFW. – If a CIDR block is configured, the traffic of the CIDR block is protected by CFW.
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 **Attachment Type** to **CFW instance**.
Next Hop	Select the automatically generated firewall attachment **cfw-er-auto-attach**.
Description	(Optional) Description of a route.

Step 8 Configure the propagation route table.

1. 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 4-7**.

Figure 4-14 Creating an association



Create Association

* Attachment Type: CFW instance

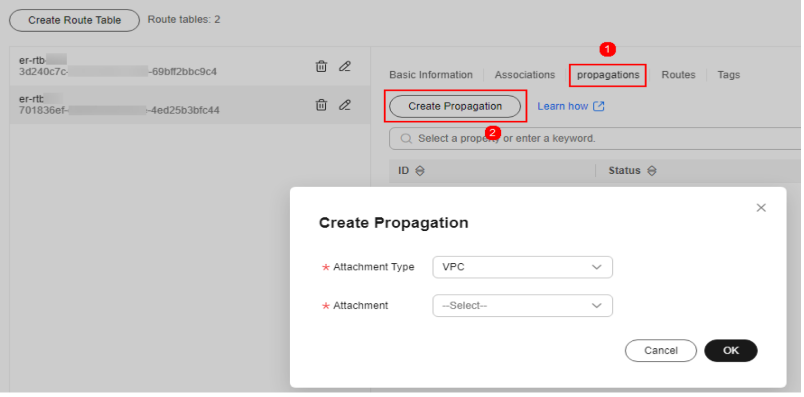
* Attachment: --Select--

Table 4-7 Association parameters

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

2. Set the propagation function. Click the **Propagations** tab and click **Create Propagation**. For more information, see **Table 4-8**.

Figure 4-15 Creating a propagation



Create Propagation

* Attachment Type: VPC

* Attachment: --Select--

Table 4-8 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.

Step 9 Modify the VPC route table.

1. In the service list, click **Virtual Private Cloud** under **Networking**. In the navigation pane, choose **Route Tables**.
2. In the **Name/ID** column, click the route table name of a VPC. The **Summary** page is displayed.
3. Click **Add Route**. For details, see **Table 4-9**.

   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.

Table 4-9 Route parameters

Parameter	Description
Destination Address Type	Select **IP address**.
Destination	Destination CIDR block. It cannot conflict with existing routes or subnet CIDR blocks in the VPCs. For example, to protect traffic between two VPCs, set the destination address of the route of VPC1 to the CIDR block of VPC2.
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) Description of a route. Enter up to 255 characters. Angle brackets (< or >) are not allowed.

----End

Modifying an Enterprise Router to Direct Traffic to Cloud Firewall

Step 1 A VPC border firewall has been created. For details, see **Creating a VPC Border Firewall**.

Step 2 **Log in to the management console**.

Step 3 Click 📍 in the upper left corner of the management console and select a region or project.

Step 4 In the navigation pane, click ≡ in the upper left corner and choose **Networking** > **Enterprise Router**.

Step 5 Delete the associations and propagations of the firewall VPC (**vpc-cfw-er**) from the default route table **er-RT1**.

Click the route table and click the **Associations** tab. In the **Operation** column of the firewall VPC, click **Delete**. In the confirmation dialog box, click **Yes**.

Click the **Propagations** tab. In the **Operation** column of the firewall VPC, click **Delete**. In the confirmation dialog box, click **Yes**.

Step 6 Create route table **er-RT2**.

Click **Create Route Table**. For details, see **Table 4-10**.

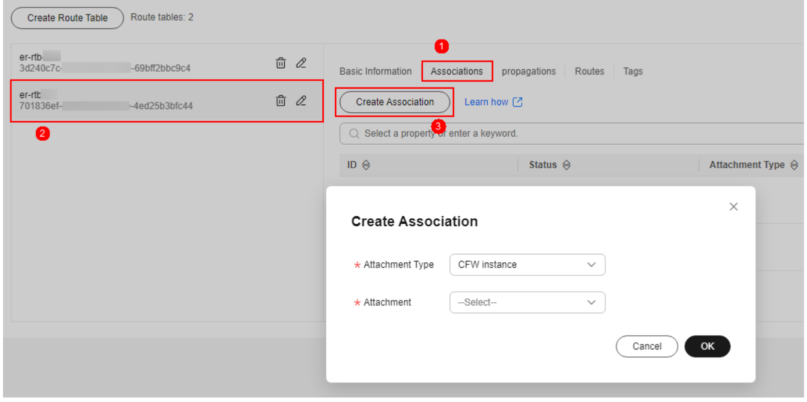
Table 4-10 Route table parameters

Parameter	Description	Example Value
Name	Route table name. The name: ● Must contain 1 to 64 characters. ● Can contain letters, numbers, underscores (_), hyphens (-), and periods (.).	er-RT2
Tags	During the route table creation, you can add tags to the route table resources for easy categorization and quick search. For details about tags, see **Tag Overview**.	**Tag key**: **test** **Tag value**: **01**
Description	Route table description	-

Step 7 Configure the route table **er-RT2**. Set the associations and propagations.

1. Select the route table **er-RT2**, click the **Associations** tab, and click **Create Association**. See **Creating an association**. For more information, see **Table 4-11**.

Figure 4-16 Creating an association



* Attachment Type: CFW instance

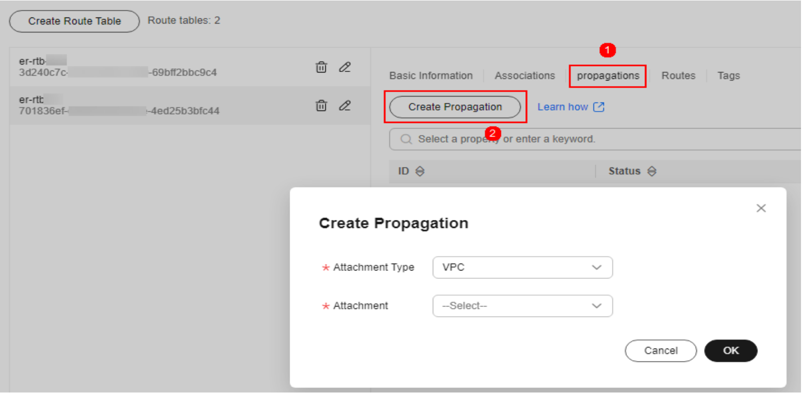
* Attachment: --Select--

Table 4-11 Association parameters

Parameter	Description	Example Value
Attachment Type	Set **Attachment Type** to **CFW instance**.	CFW instance
Attachment	Select an item from the **Attachment** drop-down list.	cfw-er-auto

2. Create propagations for the route table (**er-RT2**). Click the **Propagations** tab and click **Create Propagation**. For details, see **Table 4-12**.

Figure 4-17 Creating a propagation



* Attachment Type: VPC

* Attachment: --Select--

Table 4-12 Propagation parameters

Parameter	Description	Example Value
Attachment Type	Select **VPC**.	VPC
Attachment	Select an item from the **Attachment** drop-down list.	vpc-1

Table 4-13 Propagation parameters

Parameter	Description	Example Value
Attachment Type	Select **VPC**.	VPC
Attachment	Select an item from the **Attachment** drop-down list.	vpc-2

NOTE

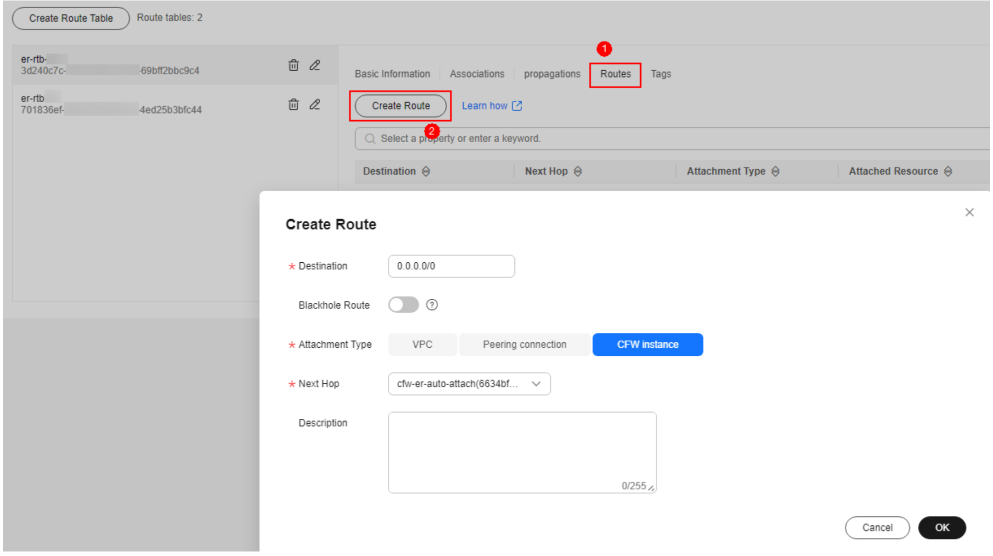
- Add at least two propagations. A propagation is required for each protected VPC you add.

  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.

Step 8 Configure the default route table **er-RT1**.

1. Add a static route. Select the route table **er-RT1**, click the **Routes** tab, click **Create Route**, and configure the following parameters:
   - **Destination**: **0.0.0.0/0**
   - **Attachment Type**: **CFW instance**
   - **Next Hop**: **cfw-er-auto** (attachment of the firewall VPC)

Figure 4-18 Adding a static route



Create Route

* Destination: 0.0.0.0/0
Blackhole Route: off
* Attachment Type: VPC | Peering connection | [✓ CFW instance]
* Next Hop: cfw-er-auto-attach(6634bf...
Description: 0/255

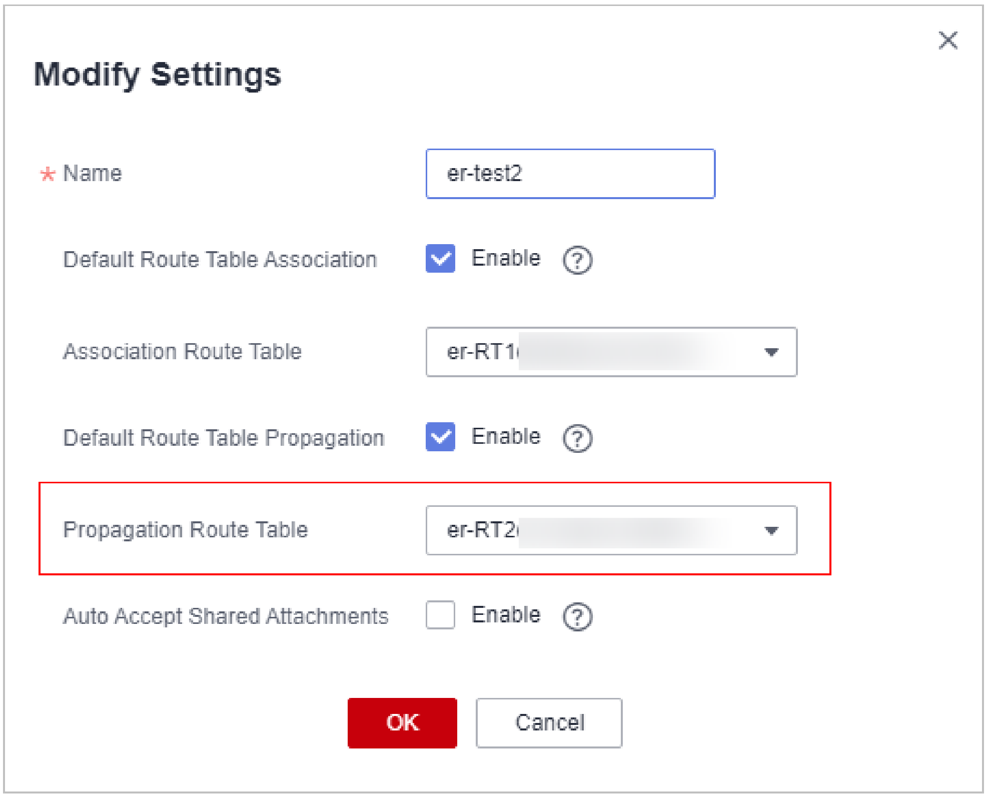
2. Delete all the propagations in the route table **er-RT1**.

   Click the **Propagations** tab. In the **Operation** column, click **Delete**. In the confirmation dialog box, click **Yes**.

Step 9 (Optional) You are advised to change the propagation route table of the enterprise router to the new route table (**er-RT2**), so that you simply need to configure an attachment when adding a VPC.

Go to the **Enterprise Router** page, choose **More** > **Modify Settings**, and set the propagation route table to **er-RT2**, as shown in **Figure 4-19**.

Figure 4-19 Modifying configurations



Modify Settings

* Name: er-test2

Default Route Table Association: ☑ Enable

Association Route Table: er-RT1[redacted]

Default Route Table Propagation: ☑ Enable

Propagation Route Table: er-RT2[redacted]

Auto Accept Shared Attachments: □ Enable

To use the enterprise router of account A to protect VPCs under account B, share the router with account B, and add an attachment in account B. For details, see **Creating a Sharing**. After the sharing is successful, add attachments to account B.

----End

Follow-up Operations

After the configuration, enable VPC border protection. For details, see **Enabling the VPC Border Firewall and Ensuring the Traffic Passes Through CFW**.

4.2.2.3 Enabling the VPC Border Firewall and Ensuring the Traffic Passes Through CFW

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

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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

Verifying That Traffic Passes Through CFW

Step 1 Generate traffic. For details, see **Verifying Network Connectivity**.

Step 2 View logs. In the navigation pane, choose **Log Audit** > **Log Query**. Click the **Traffic Logs** tab and click **VPC Border Firewall**.

- If a log is generated, CFW is protecting the traffic between VPCs.
- If no logs are recorded, check the configurations of the enterprise router. For details, see **Configuring the Enterprise Router to Direct Traffic to the Cloud Firewall**.

----End

References

For details about how to disable VPC border protection, see **Disabling VPC Border Protection**.

Follow-up Operations

- For details about how to add a protected VPC, see **Adding a Protected VPC**.
- For details about how to view the traffic trend and statistics of CFW, see **Traffic Analysis**. For details about traffic records, see **Traffic Logs**.
- After protection is enabled, all traffic is allowed by default. CFW will block traffic based on the policies you configure.

- To implement traffic control, configure a protection policy. For details, see **Configuring Protection Rules to Block or Allow VPC Border Traffic** or **Adding Blacklist or Whitelist Items to Block or Allow Traffic**.
  - Allow or block traffic based on protection rules.
    - Traffic allowing rule: The allowed traffic will be checked by functions such as intrusion prevention system (IPS) and antivirus.
    - Traffic blocking rule: Traffic will be directly blocked.
  - Allow or block traffic based on the blacklist and whitelist:
    - Whitelist: Traffic will be directly allowed without being checked by other functions.
    - Blacklist: Traffic will be directly blocked.
- For details about how to block network attacks, see **Configuring Intrusion Prevention**.

4.2.3 Enterprise Router Mode (Old)

4.2.3.1 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.

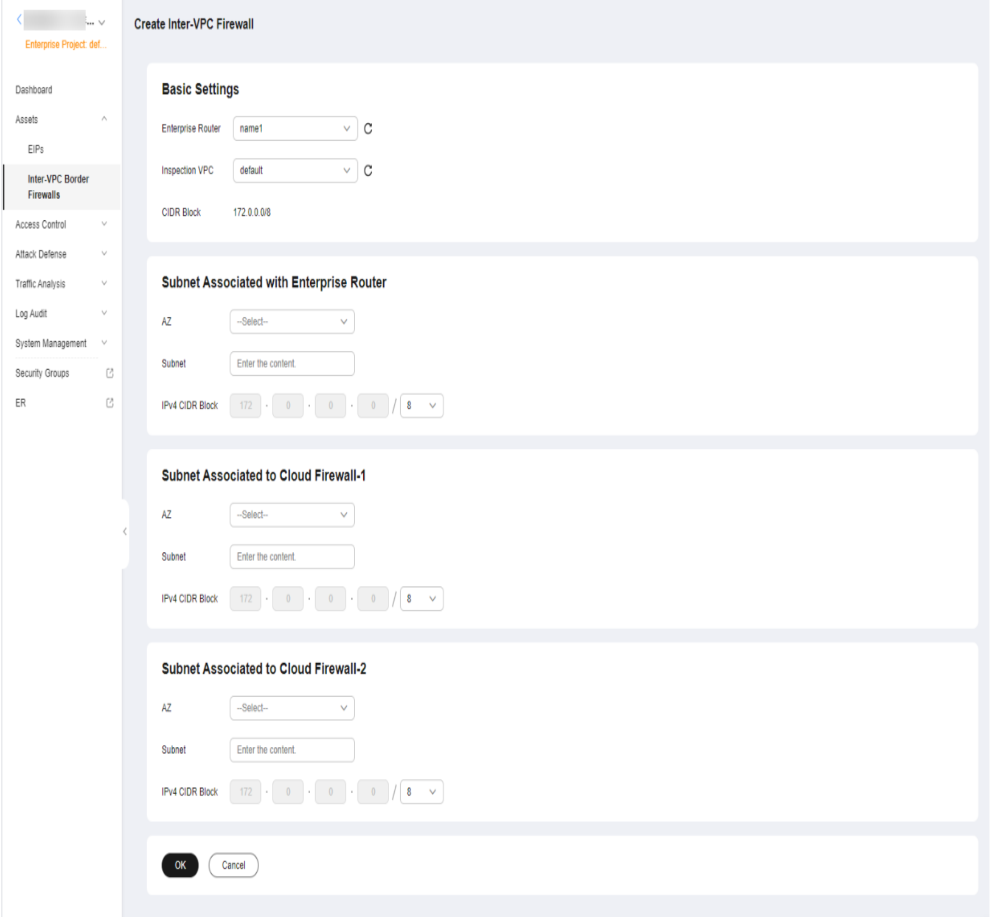
Step 3 In the navigation pane on the left, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

Step 4 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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 4-20 Creating a VPC border firewall (old version)



Create Inter-VPC Firewall

Basic Settings

Enterprise Router: name1

Inspection VPC: default

CIDR Block: 172.0.0.0/8

Subnet Associated with Enterprise Router

AZ: --Select--

Subnet: Enter the content.

IPv4 CIDR Block: 172 . 0 . 0 . 0 / 8

Subnet Associated to Cloud Firewall-1

AZ: --Select--

Subnet: Enter the content.

IPv4 CIDR Block: 172 . 0 . 0 . 0 / 8

Subnet Associated to Cloud Firewall-2

AZ: --Select--

Subnet: Enter the content.

IPv4 CIDR Block: 172 . 0 . 0 . 0 / 8

Table 4-14 Parameters for a VPC border firewall

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

Parameter	Description	Example Value
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

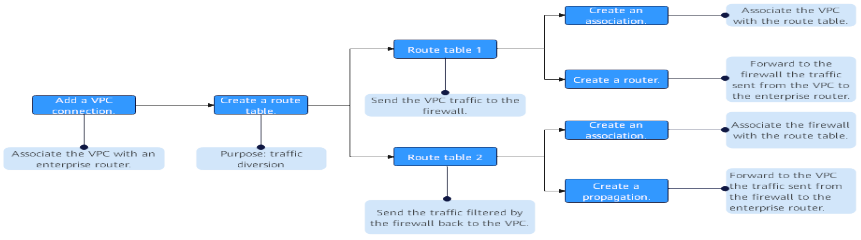
4.2.3.2 Configuring an Enterprise Router

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 4-21 Process of configuring an enterprise router


Add a VPC connection.
Associate the VPC with an enterprise router.
Create a route table.
Purpose: traffic diversion
Route table 1
Send the VPC traffic to the firewall.
Route table 2
Send the traffic filtered by the firewall back to the VPC.
Create an association.
Associate the VPC with the route table.
Create a router.
Forward to the firewall the traffic sent from the VPC to the enterprise router.
Create an association.
Associate the firewall with the route table.
Create a propagation.
Forward to the VPC the traffic sent from the firewall to the 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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click **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

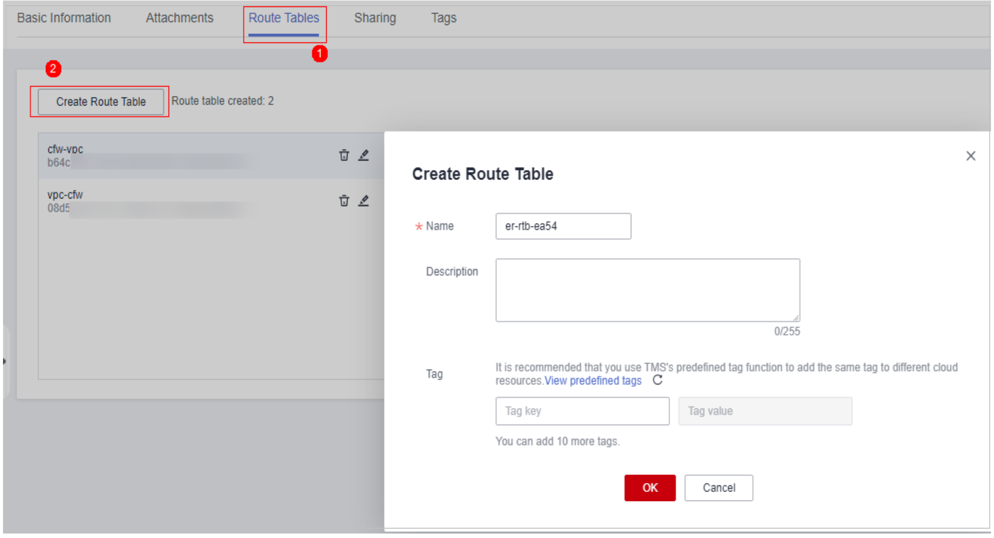
- Add at least three connections, for example, the firewall connection **cfw-er-auto** (automatically generated after the firewall is created), the VPC1 connection **vpc-1**, and the VPC2 connection **vpc-2**.
- To use the enterprise router of account A to protect VPCs under account B, share the router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

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 4-22**. For more information, see **Route table parameters**.

Figure 4-22 Creating a route table



Route table created: 2

cfw-vpc
b64c[redacted]

vpc-cfw
08d5[redacted]

Name: er-rtb-ea54

Description:

0/255

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

You can add 10 more tags.

Table 4-15 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	-

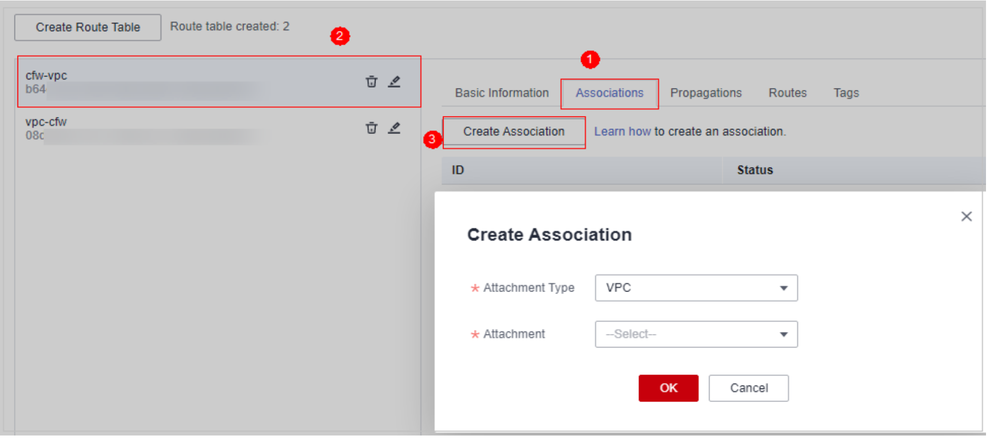
Parameter	Description	Example Value
Tag	During the route table creation, you can tag the route table resources. Tags identify cloud resources for purposes of easy categorization and quick search. For details about tags, see **Tag Overview**.	-

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 4-23 Creating an association



Create Association

* Attachment Type: VPC

* Attachment: --Select--

Table 4-16 Association parameters

Parameter	Description	Example Value
Attachment Type	Select **VPC**.	VPC
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 4-24**. For more information, see **Route parameters**.

Figure 4-24 Creating a route

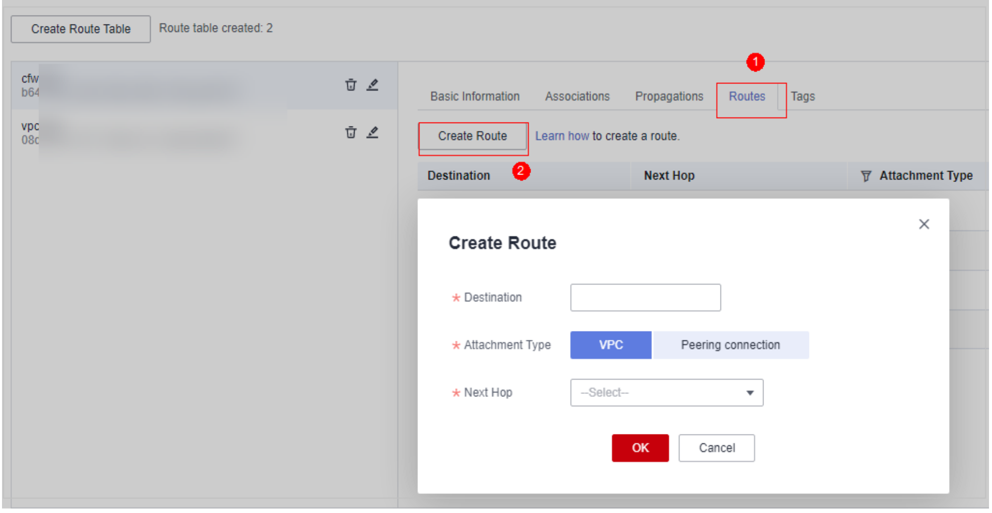


Table 4-17 Route parameters

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 4-25 Creating an association

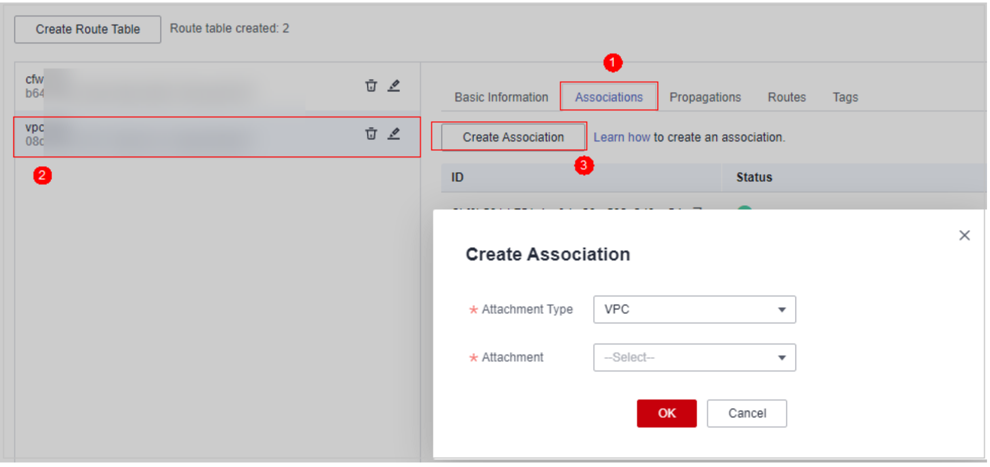


Table 4-18 Association parameters

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 4-26 Creating a propagation

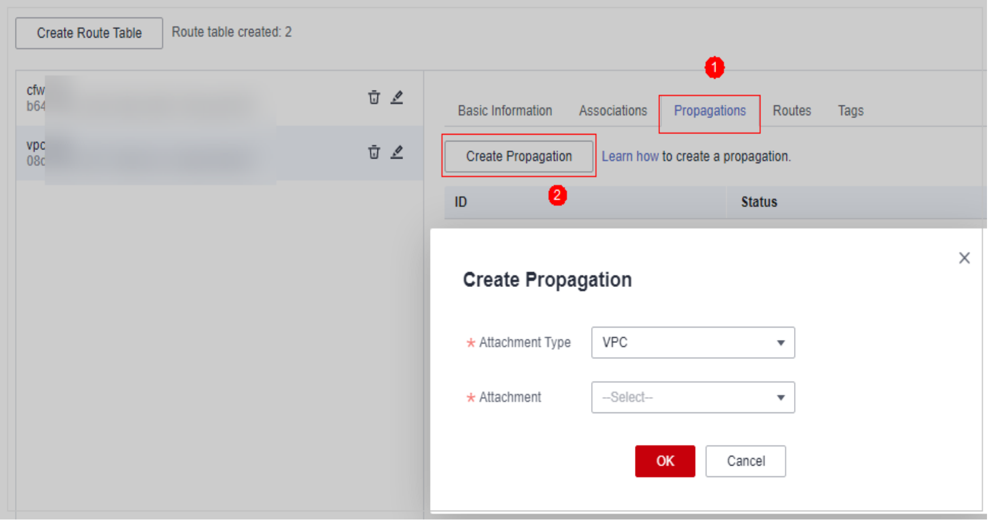


Table 4-19 Propagation parameters

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 4-20 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

4.2.3.3 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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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

4.2.4 Managing VPC Border Firewalls

4.2.4.1 Adding a Protected VPC

Scenario

After configuring a VPC border firewall, you need to configure routes to forward traffic to CFW.

This section describes how to quickly configure and modify routes.

Prerequisites

You have configured the VPC border firewall. For details, see **Enterprise Router Mode (New)**.

Step 1: Add VPC Attachments

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

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**. After the sharing is successful, add attachment to account B. Subsequent configurations are still performed under account A.

Step 2: Configure Associations and Propagations

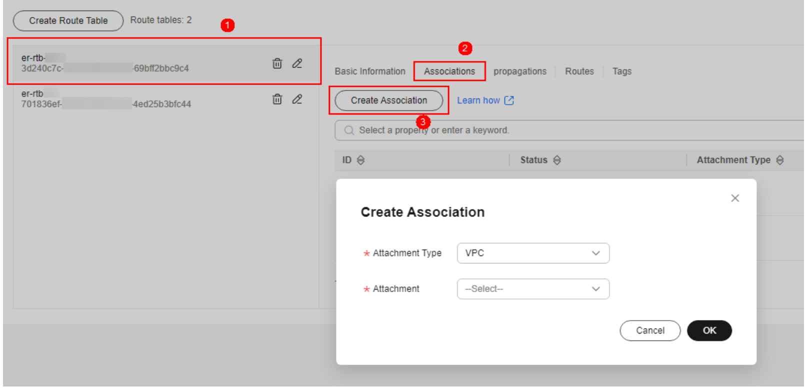
Step 1 In the upper left corner, click ☰ and choose **Networking** > **Enterprise Router**. Click **Manage Route Table**.

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 4-21**.

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**.

Figure 4-27 Creating an association



Create Association

* Attachment Type: VPC

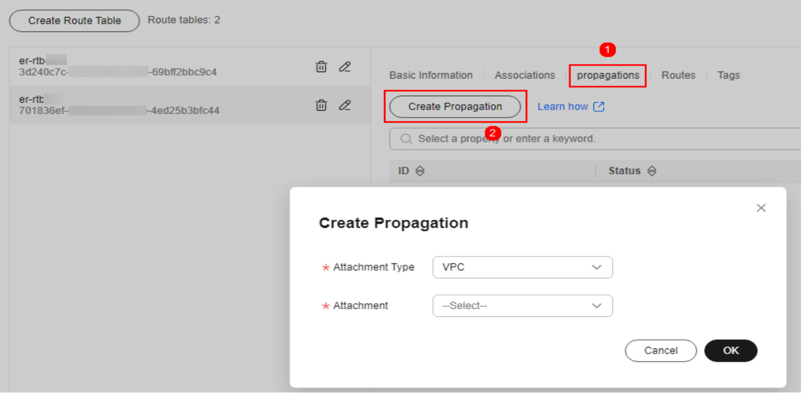
* Attachment: --Select--

Table 4-21 Association parameters

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

Step 3 Configure propagations. Select the propagation route table, click the **Propagations** tab, and click **Create Propagation**. For more information, see Table 4-22.

Figure 4-28 Creating a propagation



Create Propagation

* Attachment Type: VPC

* Attachment: --Select--

Table 4-22 Propagation parameters

Parameter	Description
Attachment Type	Select **VPC**.

Parameter	Description
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 details, see **Table 4-23**.

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.

Table 4-23 Route parameters

Parameter	Description
Destination Address Type	Select **IP address**.
Destination	Destination CIDR block. It cannot conflict with existing routes or subnet CIDR blocks in the VPCs. For example, to protect traffic between two VPCs, set the destination address of the route of VPC1 to the CIDR block of VPC2.
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.

Parameter	Description
Description	(Optional) Description of a route. Enter up to 255 characters. Angle brackets (< or >) are not allowed.

----End

Related Operations

- For details about VPC border firewalls, see **VPC Border Firewall Overview**.
- For details about how to configure a VPC border firewall, see **Enterprise Router Mode (New)**.

4.2.4.2 Modifying a Private CIDR Block

To use public network CIDR blocks other than 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, or the 100.64.0.0/10 segment reserved for carrier-level NAT as private network CIDR blocks, modify the CIDR private network segment or **submit a service ticket** to expand your private IP CIDR blocks; otherwise, CFW may fail to forward traffic between your VPCs.

Modifying a Private CIDR Block

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

Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click **Edit Private IP Address Segment** next to **Custom Private IP Address Segment**.

----End

Related Operations

- For details about VPC border firewalls, see **VPC Border Firewall Overview**.
- For details about how to configure a VPC border firewall, see **Enterprise Router Mode (New)**.

4.2.4.3 Disabling VPC Border Protection

If your workloads are blocked by mistake, you can temporarily disable the VPC border firewall. The firewall does not check any traffic while it is disabled.

If you no longer need VPC border traffic protection, manually restore the configuration of the enterprise router after disabling the protection. For details, see **Restoring the Enterprise Router Configuration After VPC Border Protection Is Permanently Disabled**.

Impacts on Services

After the firewall is disabled, traffic at the VPC border will not be protected. Exercise caution when performing this operation.

Disabling a VPC Border Firewall (New 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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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**.

----End

Disabling VPC Border Firewall (Old)

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

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

----End

4.2.4.4 Restoring the Enterprise Router Configuration After VPC Border Protection Is Permanently Disabled

If you no longer need VPC border traffic protection, manually restore the configuration of the enterprise router after **disabling VPC border protection**.

This section describes how to restore enterprise router configurations. After the restoration, traffic will be transmitted from VPC1 to VPC2 through the enterprise router without passing through CFW.

⚠ WARNING

If you disable VPC protection and restore the enterprise router configuration, CFW will not protect the traffic between VPCs. Exercise caution when performing this operation.

Scenario

The protection from the VPC border firewall is no longer required.

Restoring Enterprise Router Configurations

Step 1 Disable VPC border firewall protection. For details, see **Disabling VPC Border Protection**.

Step 2 In the upper left corner, click ☰ and choose **Networking** > **Enterprise Router**. Click **Manage Route Table**.

Step 3 Configure propagation routes (automatically generated after propagation is configured) in the association route table.

1. On the **Routes** tab page of the association route table, click **Create Route**. Set **Destination Address** and **Next Hop** to those of the protected VPC specified in the configurations of the propagation route table.
   - An association route table is used for transmitting traffic from VPC to CFW. For details about how to configure it, see **Step 7**.

     A propagation route table is used for transmitting traffic from CFW to VPC. For details about how to configure it, see **Step 8**.
   - The number of routes added to the association route table must be the same as the number of routes displayed in the propagation route table.
2. (Optional) Delete the propagation route table.

   NOTE

   This step is optional. Traffic will be transmitted from VPC1 to VPC2 through the enterprise router even if the propagation route table is not deleted.
3. For more information about how to delete a CFW connection, see **Submitting a Service Ticket**.

----End

4.3 Enabling NAT Gateway Traffic Protection

Scenario

If ECSs or other resources in a VPC connect to the Internet through the NAT gateway, they are exposed to security risks, such as unauthorized access, data leakage, and malicious attacks. To address these risks, CFW protects the traffic between service VPCs and NAT gateways, blocking unauthorized outbound connections and malicious traffic. It also supports fine-grained access control based on private IP addresses to block unauthorized traffic access.

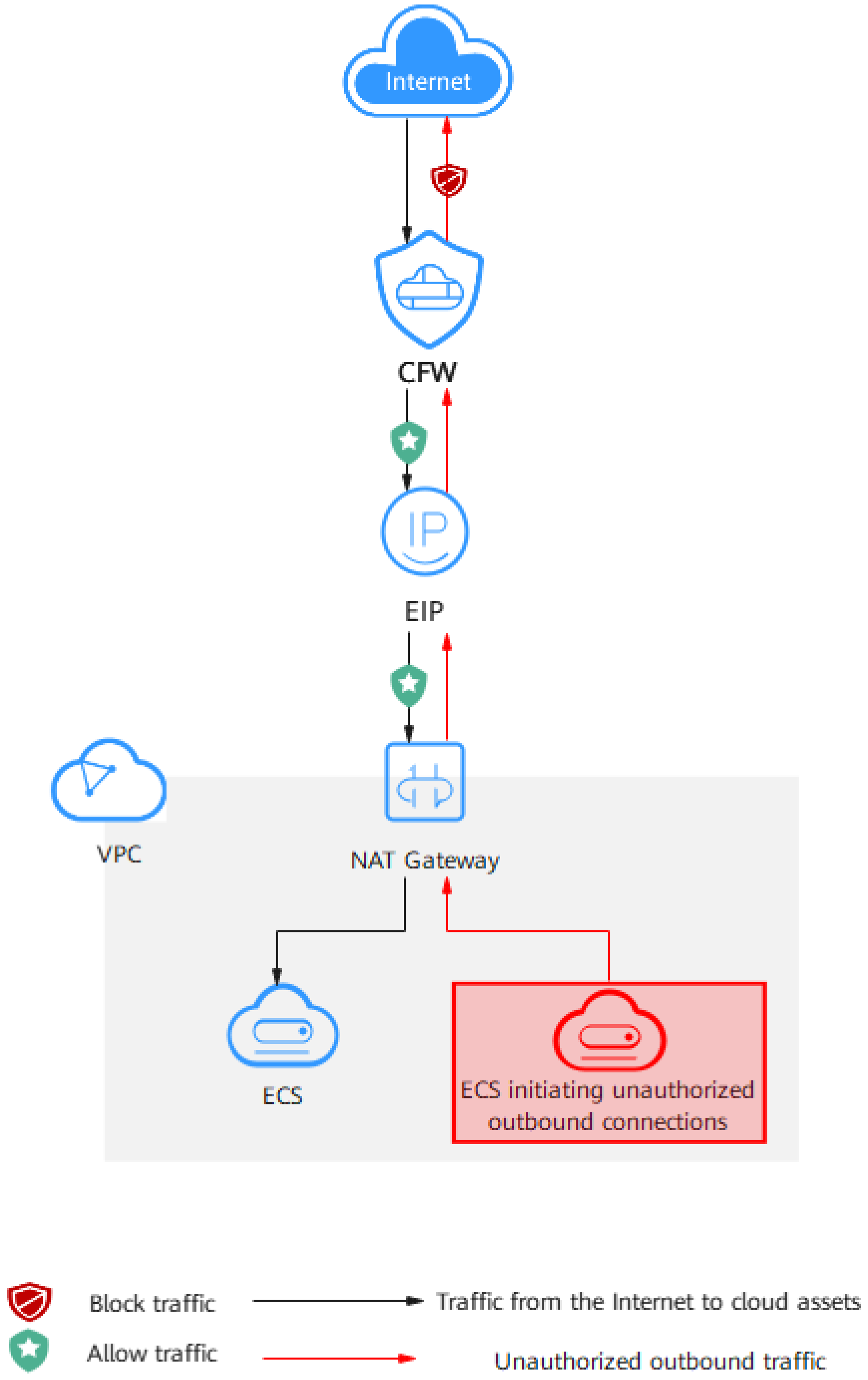
This section describes how to use the VPC border firewall to protect NAT gateway traffic. To protect the traffic exchanged between an EIP and the Internet, see **Enabling Internet Border Traffic Protection**.

What Is NAT Gateway Traffic?

NAT gateway traffic refers to the traffic between a NAT gateway and the Internet. It can be protected in two scenarios:

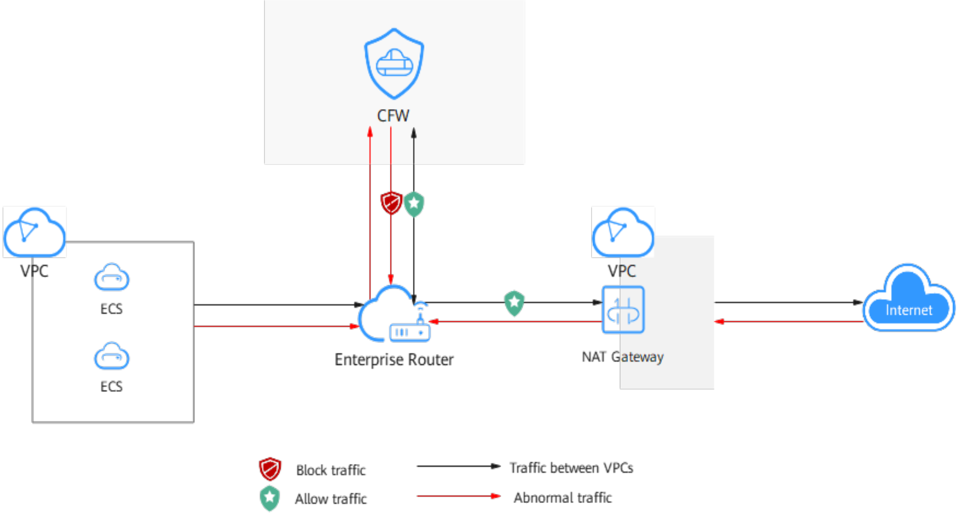
- If the EIP bound to the NAT gateway is used to connect to the Internet, CFW protects all traffic passing through the NAT gateway. This is suitable for coarse-grained protection.

Figure 4-29 Protecting a NAT gateway through an EIP


Internet
CFW
EIP
VPC
NAT Gateway
ECS
ECS initiating unauthorized outbound connections
Block traffic
Allow traffic
Traffic from the Internet to cloud assets
Unauthorized outbound traffic

- Create a VPC border firewall. Connect it to the VPC of the NAT gateway and the service VPC by using an enterprise router. The firewall can protect private IP traffic.

Figure 4-30 Protecting a NAT gateway through a VPC



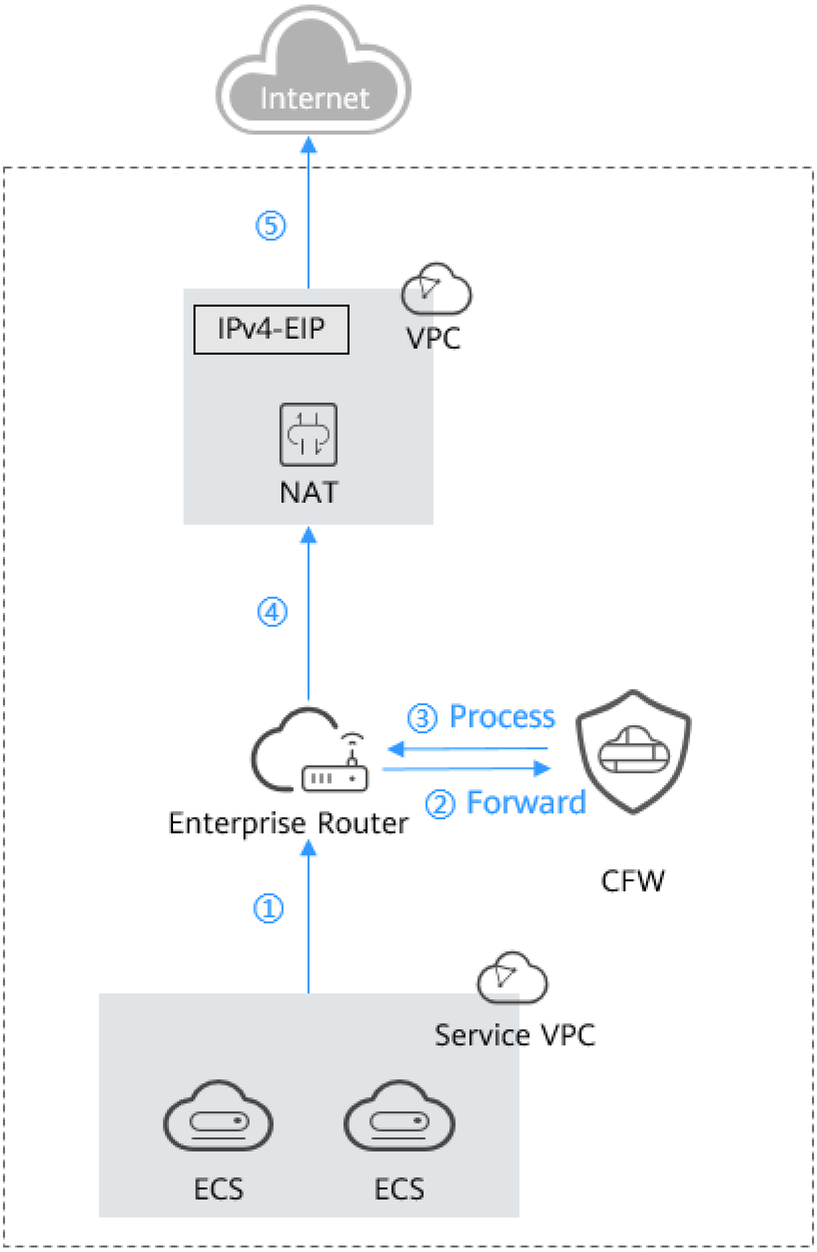
Networking

SNAT and DNAT networking diagrams are as follows.

SNAT Networking

SNAT protection provides fine-grained access control for outbound access. It is suitable if the VPC of the NAT gateway is isolated from the service VPC, and multiple VPCs or subnets use EIPs to access the Internet.

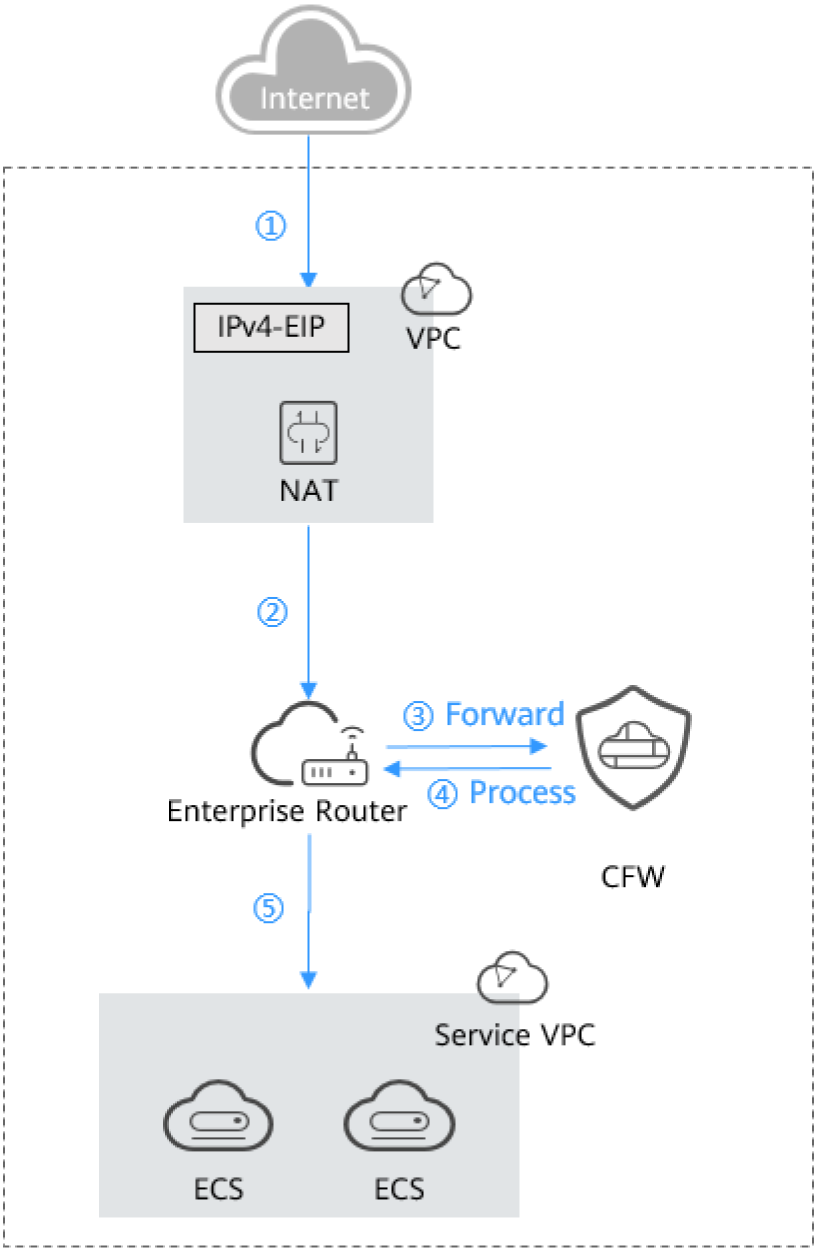
After an ECS initiates an outbound access request, the traffic is forwarded to the firewall through the enterprise router. The firewall blocks or allows the traffic based on SNAT protection rules, and forwards secure traffic to the enterprise router. The enterprise router forwards the traffic to the NAT gateway, which then forwards the traffic to the Internet based on SNAT rules.



DNAT Networking

DNAT provides fine-grained access control for the access from the Internet to internal resources. It is suitable if the VPC of the NAT gateway is isolated from the service VPC, and multiple VPCs or subnets use the NAT gateway to receive access from the Internet.

After the Internet initiates access to an internal resource, the traffic is forwarded to the enterprise router based on the DNAT rule of the NAT gateway. The enterprise router forwards the traffic to the firewall. The firewall blocks or allows the traffic based on SNAT protection rule, and forwards secure traffic to the enterprise router, which then forwards the traffic to the service VPC.



Impacts on Services

- If there is no protection rule or blacklist that blocks all traffic, enabling or disabling VPC protection will not interrupt services.
- If a protection rule or blacklist is configured to block all traffic, enabling VPC protection may interrupt services. Before enabling protection, check for persistent connections and services that do not support session reestablishment.
  - For details about how to edit a protection rule, see **Managing Protection Rules**.
  - For details about how to edit a blacklist, see **Managing the Blacklist and the Whitelist**.

Constraints

- Only the **professional edition** supports NAT gateway traffic protection.
- Traffic diversion depends on the enterprise router.
- By default, CFW supports standard private CIDR blocks. To configure other CIDR blocks, **modify private CIDR blocks** or **submit a service ticket** to expand the private CIDR block capacity. Otherwise, CFW may fail to forward traffic between VPCs.
- To let the DNAT gateway divert east-west traffic to the CFW cluster and configure DNAT rules, submit a service ticket to ask service O&M personnel to upgrade CFW. The old version does not support DNAT functions and may cause traffic loss.

Enabling NAT Gateway Traffic Protection

A firewall has been created. For details, see **Creating a VPC Border Firewall**.

Step 1: Connect VPC1 and VPC-NAT to an Enterprise Router

1. Add VPC connections.

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

   NOTE

   Two connections need to be added. Set their **Attached Resource** to **VPC1** and **VPC-NAT**, respectively.

2. Create two route tables.

   a. In the upper left corner, click ≡ and choose **Networking** > **Enterprise Router**. Click **Manage Route Table**.

   b. 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 4-24**.

Table 4-24 Route table parameters

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

3. Configure the association route table.

   a. Create associations to VPC1 and VPC-NAT. On the route table configuration page, click the **Associations** tab and click **Create Association**. For more information, see **Table 4-25**.

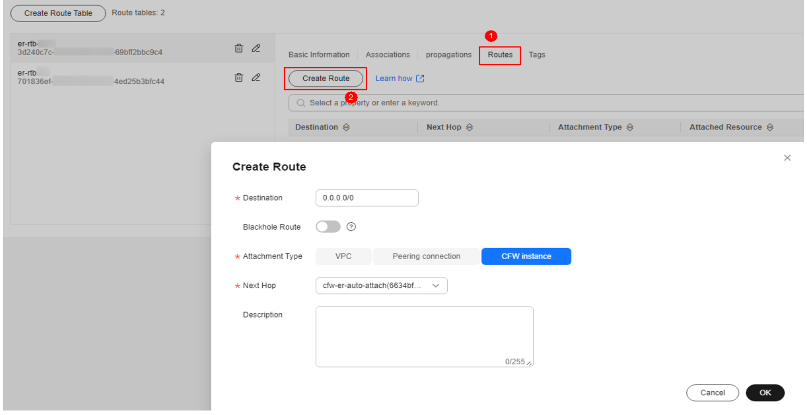
      Two associations need to be created. Set their **Attachment** to the VPC1 and VPC-NAT attachments, respectively.

Table 4-25 Association parameters

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

   b. Add a static route to the firewall. Click the **Routes** tab and click **Create Route**. For more information, see **Table 4-26**.

Figure 4-31 Creating a route



Create Route

* Destination: 0.0.0.0/0

Blackhole Route: ○

* Attachment Type: VPC | Peering connection | CFW instance

* Next Hop: cfw-er-auto-attach(6634bf...

Description: 0/255

Table 4-26 Route parameters

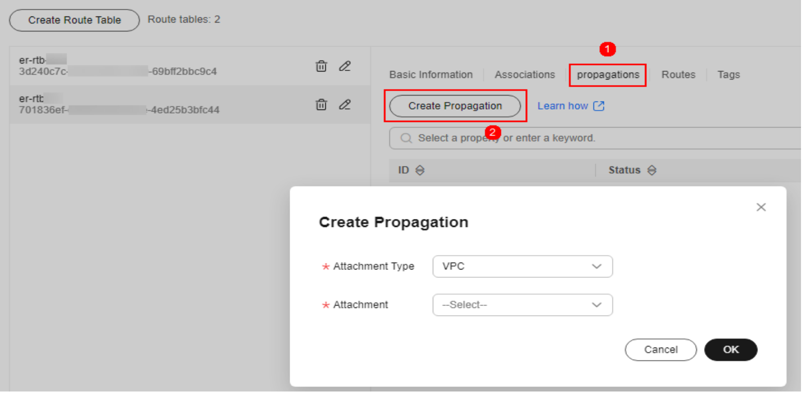
Parameter	Description
Destination	Set the destination address. ● If **0.0.0.0/0** is configured, all the traffic (IPv4) of the VPC is protected by CFW. ● If a CIDR block is configured, the traffic of the CIDR block is protected by CFW.
Blackhole Route	You are advised to disable this function. If it is enabled, the packets from a route that matches the destination address of the blackhole route will be discarded.
Attachment Type	Set **Attachment Type** to **CFW instance**.

Parameter	Description
Next Hop	Select the automatically generated firewall attachment **cfw-er-auto-attach**.
Description	(Optional) Description of a route.

4. Configure the propagation route table.

   a. Create a propagation for VPC1. On the route table setting page, click the **Propagations** tab and click **Create Propagation**. For more information, see **Table 4-27**.

Figure 4-32 Creating a propagation



* Attachment Type: VPC

* Attachment: --Select--

Table 4-27 Propagation parameters

Parameter	Description
Attachment Type	Select **VPC**.
Attachment	Select the VPC1 attachment from the **Attachment** drop-down list.

   b. Add a static route to VPC-NAT. Click the **Routes** tab and click **Create Route**. For more information, see **Table 4-28**.

Table 4-28 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	Select **VPC**.

Parameter	Description
Next Hop	Select the VPC-NAT attachment from the drop-down list.

Step 2: Configure a NAT Gateway

1. Add an SNAT rule.
   a. Return to the Enterprise Router page. In the navigation pane of **Network Console**, choose **NAT Gateway** > **Public NAT Gateways**.
   b. Click the name of a public network NAT gateway. The **Basic Information** tab is displayed. Click the **SNAT Rules** tab.
   c. Click **Add SNAT Rule**. For details, see **Table 4-29**.

Table 4-29 Adding an SNAT rule

Parameter	Description
Scenario	Scenario where the SNAT rule is used. Select **VPC**.
CIDR Block	Select **Custom** to enable servers in this subnet to use the SNAT rule to access the Internet. ● **Custom**: Customize a CIDR block or enter the IP address of a VPC.
EIP	EIP used for accessing the Internet. You can select only an EIP that is not bound to any resource, an EIP that is bound to a DNAT rule whose **Port Type** is not set to **All ports** in the current public NAT gateway, or an EIP that is bound to an SNAT rule of the current public NAT gateway. You can select multiple EIPs at once. Up to 20 EIPs can be selected for each SNAT rule. If you have selected multiple EIPs for an SNAT rule, one EIP will be chosen randomly.
Monitoring	Monitoring of the number of SNAT connections. You can set alarm rules to monitor your SNAT connections and keep informed of any changes in a timely manner.
Description	Supplementary information about the SNAT rule. Enter up to 255 characters.

2. Configure the VPC-NAT route table.
   a. In the service list, click **Virtual Private Cloud** under **Networking**. In the navigation pane, choose **Route Tables**.

b. In the **Name** column, click the route table name of a VPC. The **Summary** page is displayed.

c. Click **Add Route**. For details, see **Table 4-30**.

Table 4-30 Route parameters

Parameter	Description
Destination Type	Select **IP address**.
Destination	Destination CIDR block. Enter the IP address of VPC1. The CIDR block cannot conflict with existing routes or subnet CIDR blocks in the VPCs.
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. Enter up to 255 characters. Angle brackets (< or >) are not allowed.

Step 3: Configure a route table for VPC1

1. On the **Route Tables** page, in the **Name** column, click the route table name of VPC1. The **Summary** page is displayed.
2. Click **Add Route**. For details, see **Table 4-31**.

Table 4-31 Route parameters

Parameter	Description
Destination Type	Select **IP address**.
Destination	Destination CIDR block. Set it to **0.0.0.0/0**.
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. Enter up to 255 characters. Angle brackets (< or >) are not allowed.

Step 4: Enable a VPC Border Firewall

1. In the navigation pane, choose **Assets** > **Inter-VPC Border Firewalls**.
2. Click **Enable Protection** to the right of **Firewall Status**.
3. Click **OK**.

Follow-up Operations

- Fine-grained protection for private IP addresses: Configure NAT protection rules. For details, see **Configuring Protection Rules to Block or Allow NAT Gateway Border Traffic**.
- Interception of network attacks: Configure intrusion prevention. For details, see **Configuring Intrusion Prevention**.
- For details about how to view the traffic trend and statistics of CFW, see **Traffic Analysis**. For details about traffic records, see **Traffic Logs**.
- After protection is enabled, all traffic is allowed by default. CFW will block traffic based on the policies you configure.
  - To implement traffic control, configure a protection policy. For details, see **Configuring Protection Rules to Block or Allow NAT Gateway Border Traffic** or **Adding Blacklist or Whitelist Items to Block or Allow Traffic**.
    - Allow or block traffic based on protection rules.
      - Traffic allowing rule: The allowed traffic will be checked by functions such as intrusion prevention system (IPS) and antivirus.
      - Traffic blocking rule: Traffic will be directly blocked.
    - Allow or block traffic based on the blacklist and whitelist:
      - Whitelist: Traffic will be directly allowed without being checked by other functions.
      - Blacklist: Traffic will be directly blocked.
  - For details about how to block network attacks, see **Configuring Intrusion Prevention**.

References

For details about how to disable NAT gateway protection, see **Disabling VPC Border Protection**.

5 Access Control

5.1 Access Control Policy Overview

CFW allows all traffic by default. If no access control policies are configured, all the communication between internal servers and the Internet will be allowed. Unauthorized access or the lateral threat movement will go unchecked. You can configure access control policies in Cloud Firewall to allow or block specific traffic and implement multi-dimensional protection.

Access Control Policy Types

Access control policies include protection rules, traffic filtering configuration, the blacklist, and the whitelist. **Table 5-1** describes their differences. If traffic hits a policy, the action specified in the policy will be performed. For details about the priority of each configuration, see **Priority of Access Control Policies**.

Table 5-1 Protection policies

-	Protection Rule	Blacklist	Whitelist	Traffic Filtering
Protected object	• 5-tuples • IP address groups • Geographical locations • Domain names and domain name groups (layer-4 and layer-7 traffic) • Applications	• 5-tuples • IP address groups	• 5-tuples • IP address groups	IP address

-	Protection Rule	Blacklist	Whitelist	Traffic Filtering
Network type	- EIP - Private IP address	- EIP - Private IP address	- EIP - Private IP address	- EIP - Private IP address
Action	- If **Block** is selected, traffic will be blocked. - If **Allow** is selected, traffic will be allowed by protection rules and then checked by IPS.	Traffic is blocked directly.	Traffic is allowed by CFW and not checked by other functions.	Traffic is blocked directly.
Scenario and characteristics	Identify specified traffic based on its characteristics. It is suitable for fine-grained control of specific traffic. For example, you can specify protocol types, port numbers, and applications in a rule.	Quickly block identified security threats. It is suitable for handling known malicious traffic.	Quickly allow trusted traffic. It is suitable for trusted IP addresses.	Quickly block abnormal traffic based on the configured characteristics. It is suitable for quickly blocking a large number of IP addresses.
Protection log	**Access Control Logs**	**Access Control Logs**	**Access Control Logs**	**Attack Event Logs**
Configuration method	**Configuring Protection Rules to Block or Allow Internet Border Traffic**	**Adding Blacklist or Whitelist Items to Block or Allow Traffic**	**Adding Blacklist or Whitelist Items to Block or Allow Traffic**	**Quickly Block Malicious Traffic Through Traffic Blocking**

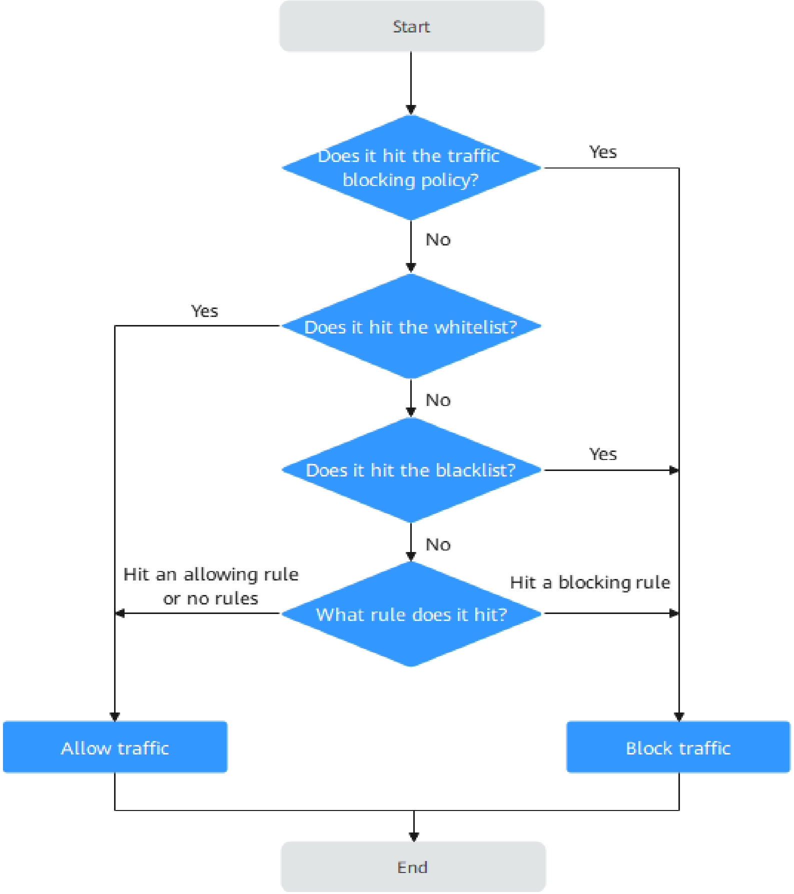
CAUTION

Traffic filtering is a new function. If you cannot access the **Access Control** > **Traffic Filtering** page on the console, please **submit a service ticket** to upgrade the firewall engine.

Priority of Access Control Policies

The priorities of CFW access control policies in descending order are as follows: Traffic blocking > Whitelist > Blacklist > Protection policy (ACL).

Figure 5-1 Protection priority


Start
Does it hit the traffic blocking policy?
Yes
No
Does it hit the whitelist?
Yes
No
Does it hit the blacklist?
Yes
No
Hit an allowing rule or no rules
What rule does it hit?
Hit a blocking rule
Allow traffic
Block traffic
End

For details about the protection sequence of all CFW policies, see **What Is the Protection Sequence of CFW?**

Specification Limitations

To enable VPC border protection and NAT protection, use the CFW professional edition and enable **VPC firewall** protection.

Precautions for Configuring a Blocking Policy

The precautions for configuring a protection rule or a blacklist item for blocking IP addresses are as follows:

1. You are advised to preferentially configure specific IP addresses (for example, 192.168.10.5) to reduce network segment configurations and avoid improper blocking.

2. Exercise caution when configuring protection rules to block reverse proxy IP addresses, such as the CDN, Advanced Anti-DDoS, and WAF back-to-source IP addresses. You are advised to configure protection rules or whitelist to permit reverse proxy IP addresses.
3. Blocking forward proxy IP addresses (such as company egress IP addresses) can have a large impact. Exercise caution when configuring protection rules to block forward proxy IP addresses.
4. When configuring region protection, take possible EIP changes into consideration.

Elements in a Protection Rule

Protection rules can identify and match different traffic elements to allow or block related traffic.

Element	Description	Configuration Type	Configuration Supported By Different Rules
Source	The party that initiates a connection.	● IP address: Access control is performed on the traffic from a specific IP address. ● IP address group: Access control is performed on the traffic from a series of IP addresses. ● Region: Access control is performed on the traffic from the IP addresses in a specific region. ● **Any**: any source address	● Internet border: – Inbound: IP address, IP address group, region, and **Any** – Outbound: IP address, IP address group, and **Any** ● NAT gateway: – Inbound: IP address, IP address group, region, and **Any** – Outbound: IP address, IP address group, and **Any** ● VPC border rule: IP address, IP address group, and **Any**

Element	Description	Configuration Type	Configuration Supported By Different Rules
Destination	The party that receives a connection.	- IP address: Access control is performed on the traffic sent to a specific IP address. - IP address group: Access control is performed on the traffic sent to a series of IP addresses. - Region: Access control is performed on the traffic sent to the IP addresses in a specific region. - Domain name or domain name group: Access control is performed on the traffic sent to specific domain name addresses. To set the destination to a domain name or domain name group in a protection rule, choose from the following domain name types: – Application: HTTP, HTTPS, TLS, SMTPS, or POPS. CFW preferentially control the access to domain names based on the Host or SNI field. – Network: CFW performs DNS resolution to obtain the IP address of a domain name and controls access to the IP address. - **Any**: any destination address	- Internet border: – Inbound: IP address, IP address group, and **Any** – Outbound: IP address, IP address group, region, domain name, domain name group, and **Any** - NAT gateway: – Inbound: IP address, IP address group, and **Any** – Outbound: IP address, IP address group, region, domain name, domain name group, and **Any** - VPC border rule: IP address, IP address group, domain name, domain name group, and **Any**
Service	Traffic protocol type or port number	Service and service group: A service or a set of services. You can specify the protocol type, source port, and destination port to identify a service.	The ICMP protocol does not support port configuration.

Element	Description	Configuration Type	Configuration Supported By Different Rules
		Service: Set **Protocol Type**, **Source Port**, and **Destination Port**. ● Protocol: Transport layer protocol. It can be TCP, UDP, or ICMP. ● Source port: Access is controlled based on traffic source ports. ● Destination port: Access is controlled based on traffic destination ports.	
		Service Group. A set of services.	
		Any: Select **Any** if you are not sure about the protocol type.	
Application	Application layer protocol	The application layer protocol can be HTTP, HTTPS, SMTP, SMTPS, SSL, or POP3. If you are not sure about the protocol type, select **Any**.	It varies according to the selected protocol type.

Example configuration:

Parameter	Input	Description
Source/Destination	0.0.0.0/0	All IP addresses
Domain name	www.example.com	Domain name www.example.com
	*.example.com	All domain names ending with **example.com**, for example, **test.example.com**
Service - Source port or destination port	1-65535	All ports
	80-443	All ports in the range 80 to 443
	● 80 ● 443	Ports 80 and 443

References

- For details about how to add a blacklist or whitelist for traffic protection, see **Adding Blacklist or Whitelist Items to Block or Allow Traffic**. For details about how to add a protection rule for traffic protection, see:
  - For details about how to protect the traffic from the Internet to cloud assets (EIPs), see **Accessing from the Internet to Assets on the Cloud (Inbound)**.
  - For details about how to protect the traffic from cloud assets (EIPs) to the Internet, see **Accessing from the Cloud Assets to the Internet (Outbound)**.
  - For details about how to protect the access traffic between VPCs, or between a VPC and an IDC, see **Configuring Protection Rules to Block or Allow VPC Border Traffic**.
  - For details about how to protect the traffic of private network assets at the Internet border, see **Configuring Protection Rules to Block or Allow NAT Gateway Border Traffic**.
- For details about how to add protection policies in batches, see **Importing and Exporting Protection Policies**.
- Follow-up operations after adding a policy:
  - Policy hits: For details about the protection overview, see **Viewing Protection Information Using the Policy Assistant**. For details about logs, see **Access Control Logs**.
  - For details about the traffic trend and statistics, see **Traffic Analysis**. For details about traffic records, see **Traffic Logs**.
- If your traffic is incorrectly blocked by a protection policy, troubleshoot the problem by referring to **What Can I Do If Services Cannot Be Accessed After a Policy Is Configured on CFW?**

5.2 Configuring an Access Control Policy

5.2.1 Configuring Protection Rules to Block or Allow Internet Border Traffic

After protection is enabled, CFW allows all traffic by default. You can configure protection rules to block or allow traffic.

Protection Rule Description

The protected objects, actions, and application scenarios of protection rules are as follows.

Name	Description
Protected object	● 5-tuples ● IP address groups ● Geographical locations ● Domain names and domain name groups (layer-4 and layer-7 traffic) ● Applications
Network type	● EIP ● Private IP address
Action	● If **Block** is selected, traffic will be blocked. ● If **Allow** is selected, traffic will be allowed by protection rules and then checked by IPS.
Scenario	You can configure protection rules in the following scenarios: ● This section describes how to protect the traffic of public network assets (EIPs) at the Internet border. – Protect the traffic from the Internet to cloud assets (EIPs). For details, see **Accessing from the Internet to Assets on the Cloud (Inbound)**. – Protect the traffic from cloud assets (EIPs) to the Internet. For details, see **Accessing from the Cloud Assets to the Internet (Outbound)**. ● Protect the traffic of private network assets at the Internet border. For details, see **Configuring Protection Rules to Block or Allow NAT Gateway Border Traffic**. ● Protect the access traffic between VPCs, or between a VPC and an IDC. For details, see **Configuring Protection Rules to Block or Allow VPC Border 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 Blacklist or Whitelist Items to Block or Allow Traffic**.

Constraints

- CFW does not support application-level gateways (ALGs). If ALG-related services (such as SIP and FTP) are available, you are advised to add a rule to allow the traffic to pass through all the ports of data channels.
- To use CFW persistent connections, enable a bidirectional bypass policy. If you only enable a unidirectional policy, the client will need to re-initiate

connections in certain scenarios, such as enabling or disabling protection, and expanding engine capacities. You can also **create a service ticket** to evaluate the risks of related issues.

- Quota:
  - Up to 20,000 protection rules can be added.
  - The restrictions on a single protection rule are as follows:
    - For IPv4, up to 4,000 source and 4,000 destination IP addresses are allowed. For IPv6, up to 2,000 source and 2,000 destination IP addresses are allowed.
    - A maximum of 20 source IP addresses and 20 destination IP addresses can be added.
    - A maximum of five source IP address groups and five destination IP address groups can be associated. A maximum of 1,666 IP address group members can be associated with each protection rule.
    - A maximum of five service groups can be associated.
- Restrictions on domain name protection:
  - Domain names in Chinese are not supported.
  - Restrictions on application-layer domain name reference:
    - Each firewall instance can reference up to 60,000 domain names.
    - Each firewall instance can reference up to 1,000 wildcard domain names.
    - Each protection rule can reference up to 20,000 domain names.
    - Each protection rule can reference up to 128 wildcard domain names.

    Calculation: If both rule A and rule B of a firewall reference domain name 1 and domain name group A (containing domain names 2 and 3), then the number of domain names referenced by rule A or rule B is 3, and the number of domain names referenced by the firewall instance is 6.
  - A network domain name group can store up to 1,000 DNS resolution results. If the number of DNS resolution results exceeds 1,000, domain names may fail to be accessed. For domain names with a large number of resolution results or frequent changes, if the protected traffic is HTTP or HTTPS traffic, you are advised to use the application domain name group to add policies.
  - Domain name protection depends on the DNS server you configure. The default DNS server may be unable resolute complete IP addresses. You are advised to configure **DNS resolution** if the domain names of your services need to be accessed.
- Restrictions on regions: A protection rule with its source or destination set to a region (geographical location) takes effect only for IPv4 protected objects.
- 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.

Impacts on Services

When configuring a blocking rule, if address translation or proxy is involved, evaluate the impact of blocking IP addresses with caution.

Adding an Internet Border Protection Rule

The procedures for adding a protection rule in scenarios are as follows.

Accessing from the Internet to Assets on the Cloud (Inbound)

Step 1 Enable EIP protection. For details, see **Enabling Internet Border Traffic Protection**.

Step 2 (Optional) To add multiple IP addresses, domain names, and services (protocols, source ports, and destination ports), add their groups first.

- For details about how to add multiple IP addresses, see **Managing IP Address Groups**.
- For details about how to add multiple domain names, see **Managing Domain Name Groups**.
- For details about how to add multiple services, see **Managing Service Groups**.

Step 3 In the navigation pane on the left of the CFW console, choose **Access Control** > **Internet Border Protection Rules**.

Step 4 Add a protection rule.

On the **Protection Rules > EIP** tab, click **Add Rule**. In the displayed dialog box, enter information. For details, see **Table 5-2**.

Table 5-2 Internet boundary rule parameters (inbound direction)

Parameter	Description
Rule Type	To protect EIP traffic, select **EIP** by default. Only EIPs can be configured in this case. For details about how to configure private IP addresses, see **Adding a DNAT Traffic Protection Rule**. **NOTE** For the standard edition firewall, the rule type parameter is not involved. Only EIP rules can be configured.
Name	Name of the custom security policy.
Direction	Traffic direction of the protection rule. Select **Inbound**. ● **Inbound**: Cloud assets (EIPs) are accessed from the Internet. ● **Outbound**: Cloud assets (EIPs) access the Internet.

Parameter	Description
Source	Set the party that originates a session. ● **IP address**: Enter EIPs. This parameter can be configured in the following formats: – A single EIP, for example, *xx.xx*.**10.5** – Consecutive EIPs, for example, *xx.xx*.**0.2**-*xx.xx*.**0.10** – EIP segment, for example, *xx.xx*.**2.0/24** – Multiple inconsecutive IP addresses can be added one by one. ● **IP address group**. You can configure multiple EIPs. If **Direction** is set to **Inbound**, a predefined address group can be configured for the source address. For details about how to add a user-defined IP address group, see **Adding an IP Address Group**. For details about how to view a predefined IP address group, see **Viewing a Predefined Address Group**. ● **Countries and regions**: If **Direction** is set to **Inbound**, you can control access based on continents, countries, and regions. ● **Any**: any source address
Destination	Set the recipient of a session. ● **IP address**: Enter EIPs. This parameter can be configured in the following formats: – A single EIP, for example, *xx.xx*.**10.5** – Consecutive EIPs, for example, *xx.xx*.**0.2**-*xx.xx*.**0.10** – EIP segment, for example, *xx.xx*.**2.0/24** – Multiple inconsecutive IP addresses can be added one by one. ● **IP address group**. You can configure multiple EIPs. For details about how to add a custom IP address group, see **Adding a User-defined IP Address Group**. ● **Any**: any destination address

Parameter	Description
Service	● **Service**: Set **Protocol Type**, **Source Port**, and **Destination Port**. – **Protocol**: The value can be **TCP**, **UDP**, or **ICMP**. – **Source/Destination Port**: If **Protocol** is set to **TCP** or **UDP**, you need to set the port number. ■ 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). For details about how to add a custom service group, see **Adding a Service Group**. For details about predefined service groups, see **Viewing a Predefined Service Group**. ● **Any**: any protocol type or port number
Application	(Optional) Configure protection policies for application-layer protocols. ● When **Service** is set to **Any**, all application types are supported. ● If **Service** is set to **Service** and **Protocol** is set to **TCP**, TCP applications, such as HTTP and HTTPS, are supported. ● If **Service** is set to **Service** and **Protocol** is set to **UDP**, UDP applications, such as DNS and RDP, are supported.
Protection Action	Set the action to be taken when traffic passes through the firewall. ● **Allow**: Traffic is forwarded. ● **Block**: Traffic is not forwarded.
Status	Whether a policy is enabled. ● ●: enabled ● ○: disabled

Parameter	Description
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. A smaller value indicates a higher priority. The default priority of the first protection rule is 1. You do not need to configure its priority.
Schedule Management	(Optional) Click **Schedule Management** and configure when the rule is in effect. Select or **add a schedule**.
Allow Long Connection	If only one service is configured in the current protection rule and **Protocol** is set to **TCP** or **UDP**, you can configure the service session aging time (unit: second). Up to 50 rules can be configured with persistent connections. - **Yes**: Configure the persistent connection duration. - **No**: Retain the default durations. The default connection durations for different protocols are as follows: – TCP: 1800s – UDP: 60s
Long Connection Duration	If **Allow Long Connection** is set to **Yes**, you need to set the persistent connection duration and set **hour**, **minute**, and **second**. The duration range is 1 second to 1,000 days.
Tags	(Optional) Tags are used to identify rules. You can use tags to classify and search for security policies.
Description	(Optional) Usage and application scenario

Step 5 Click **OK** to complete the protection rule configuration.

After a protection rule is configured and enabled, it takes effect immediately.

----End

Accessing from the Cloud Assets to the Internet (Outbound)

Step 1 Enable EIP protection. For details, see **Enabling Internet Border Traffic Protection**.

Step 2 (Optional) To add multiple IP addresses, domain names, and services (protocols, source ports, and destination ports), add their groups first.

- For details about how to add multiple IP addresses, see **Managing IP Address Groups**.

- For details about how to add multiple domain names, see **Managing Domain Name Groups**.
- For details about how to add multiple services, see **Managing Service Groups**.

Step 3 In the navigation pane on the left of the CFW console, choose **Access Control** > **Internet Border Protection Rules**.

Step 4 Add a protection rule.

On the **EIP** tab, click **Add Rule**. In the displayed dialog box, enter information. For details, see **Table 5-3**.

Table 5-3 Internet boundary rule parameters (outbound direction)

Parameter	Description
Rule Type	To protect EIP traffic, select **EIP** by default. Only EIPs can be configured in this case. For details about how to configure private IP addresses, see **Adding a DNAT Traffic Protection Rule**. **NOTE** For the standard edition firewall, the rule type parameter is not involved. Only EIP rules can be configured.
Name	Name of the custom security policy.
Direction	Traffic direction of the protection rule. Select **Outbound**. ● **Inbound**: Cloud assets (EIPs) are accessed from the Internet. ● **Outbound**: Cloud assets (EIPs) access the Internet.
Source	Set the party that originates a session. ● **IP address**: Enter EIPs. This parameter can be configured in the following formats: – A single EIP, for example, *xx.xx.***10.5** – Consecutive EIPs, for example, *xx.xx.***0.2-***xx.xx.***0.10** – EIP segment, for example, *xx.xx.***2.0/24** – Multiple inconsecutive IP addresses can be added one by one. ● **IP address group**. You can configure multiple EIPs. If **Direction** is set to **Inbound**, a predefined address group can be configured for the source address. For details about how to add a user-defined IP address group, see **Adding an IP Address Group**. For details about how to view a predefined IP address group, see **Viewing a Predefined Address Group**. ● **Any**: any source address

Parameter	Description
Destination	Set the recipient of a session. ● **IP address**: Enter EIPs. This parameter can be configured in the following formats: – A single EIP, for example, *xx.xx*.**10.5** – Consecutive EIPs, for example, *xx.xx*.**0.2-***xx.xx*.**0.10** – EIP segment, for example, *xx.xx*.**2.0/24** – Multiple inconsecutive IP addresses can be added one by one. ● **IP address group**. You can configure multiple EIPs. For details about how to add a custom IP address group, see **Adding a User-defined IP Address Group**. ● **Countries and regions**: A continent, a country, or a region ● **Domain Name/Domain Name Group**: Domain names or domain groups can be protected. – **Application**: Supports the protection for domain names or wildcard domain names. Application-layer protocols such as HTTP, HTTPS, TLS, SMTPS, and POPS 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. **NOTE** – To protect the domain names of HTTP, HTTPS, TLS, SMTPS, and POPS applications, you can select any options. – To protect the wildcard domain names of HTTP, HTTPS, TLS, SMTPS, or POPS, you select any option under **Application**. (A wildcard domain name is in the format of ***.***Domain name*. The wildcard character * matches any character or string. For example, ***.example.com**.) – 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 **Domain name** 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, TLS, SMTPS, and POPS 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-type domain names, see **Managing Domain Name Groups**. – For details about how to verify the policy validity after the outbound HTTP or HTTPS domain name or domain name group is configured, see **How Do I Verify the Validity of an Outbound HTTP/HTTPS Domain Name Protection Rule?**

Parameter	Description
	- **Any**: any destination address
Service	- **Service**: Set **Protocol Type**, **Source Port**, and **Destination Port**. – **Protocol**: The value can be **TCP**, **UDP**, or **ICMP**. – **Source/Destination Port**: If **Protocol** is set to **TCP** or **UDP**, you need to set the port number. ■ 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). For details about how to add a custom service group, see **Adding a Service Group**. For details about predefined service groups, see **Viewing a Predefined Service Group**. - **Any**: any protocol type or port number
Application	(Optional) Configure a protection policy for application-layer protocols. This parameter is mandatory when **Destination** is set to **Domain Name/domain Group**. - When **Service** is set to **Any**, all application types are supported. - If **Service** is set to **Service** and **Protocol** is set to **TCP**, TCP applications, such as HTTP and HTTPS, are supported. - If **Service** is set to **Service** and **Protocol** is set to **UDP**, UDP applications, such as DNS and RDP, are supported.
Protection Action	Set the action to be taken when traffic passes through the firewall. - **Allow**: Traffic is forwarded. - **Block**: Traffic is not forwarded.
Status	Whether a policy is enabled. - 🔵: enabled - ⚪: disabled

Parameter	Description
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. A smaller value indicates a higher priority. The default priority of the first protection rule is 1. You do not need to configure its priority.
Schedule Management	(Optional) Click **Schedule Management** and configure when the rule is in effect. Select or **add a schedule**.
Allow Long Connection	If only one service is configured in the current protection rule and **Protocol** is set to **TCP** or **UDP**, you can configure the service session aging time (unit: second).
Long Connection Duration	If **Allow Long Connection** is set to **Yes**, you need to set the persistent connection duration and set **hour**, **minute**, and **second**.
Tags	(Optional) Tags are used to identify rules. You can use tags to classify and search for security policies.
Description	(Optional) Usage and application scenario

Step 5 Click **OK** to complete the protection rule configuration.

After a protection rule is configured and enabled, it takes effect immediately.

----End

Viewing Protection Rule Hits

After your services run for a period of time, you can view the number of rule hits in the **Hits** column of the protection rule list.

Follow-up Operations

Checking protection outcomes

- Policy hits: For details about the protection overview, see **Viewing Protection Information Using the Policy Assistant**. For details about logs, see **Access Control Logs**.
- For details about the traffic trend and statistics, see **Traffic Analysis**. For details about traffic records, see **Traffic Logs**.

References

- For details about how to add protection rules in batches, see **Importing and Exporting Protection Policies**.

- For details about how to adjust rule priority, see **Adjusting the Priority of a Protection Rule**.

5.2.2 Configuring Protection Rules to Block or Allow VPC Border Traffic

After protection is enabled, CFW allows all traffic by default. You can configure protection rules to block or allow traffic.

Protection Rule Description

The protected objects, actions, and application scenarios of protection rules are as follows.

Name	Description
Protected objects	● 5-tuples ● IP address groups ● Geographical locations ● Domain names and domain name groups (layer-4 and layer-7 traffic) ● Application
Network types	● EIPs ● Private IP addresses
Actions	● If **Block** is selected, traffic will be blocked. ● If **Allow** is selected, traffic will be allowed by protection rules and then checked by IPS.
Scenarios	You can configure protection rules in the following scenarios: ● This section describes how to protect the access traffic between VPCs, or between a VPC and an IDC. ● Protect the traffic of public network assets (EIPs) at the Internet border. For details, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**. ● Protect the traffic of private network assets at the Internet border. For details, see **Configuring Protection Rules to Block or Allow NAT Gateway Border 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 Blacklist or Whitelist Items to Block or Allow Traffic**.

Specification Limitations

Only the professional edition supports VPC border traffic protection.

Constraints

- CFW does not support application-level gateways (ALGs). If ALG-related services (such as SIP and FTP) are available, you are advised to add a rule to allow the traffic to pass through all the ports of data channels.
- To use CFW persistent connections, enable a bidirectional bypass policy. If you only enable a unidirectional policy, the client will need to re-initiate connections in certain scenarios, such as enabling or disabling protection, and expanding engine capacities. You can also **create a service ticket** to evaluate the risks of related issues.
- Quota:
  - Up to 20,000 protection rules can be added.
  - The restrictions on a single protection rule are as follows:
    - For IPv4, up to 4,000 source and 4,000 destination IP addresses are allowed. For IPv6, up to 2,000 source and 2,000 destination IP addresses are allowed.
    - A maximum of 20 source IP addresses and 20 destination IP addresses can be added.
    - A maximum of five source IP address groups and five destination IP address groups can be associated. A maximum of 1,666 IP address group members can be associated with each protection rule.
    - A maximum of five service groups can be associated.
- Restrictions on domain name protection:
  - Domain names in Chinese are not supported.
  - Restrictions on application-layer domain name reference:
    - Each firewall instance can reference up to 60,000 domain names.
    - Each firewall instance can reference up to 1,000 wildcard domain names.
    - Each protection rule can reference up to 20,000 domain names.
    - Each protection rule can reference up to 128 wildcard domain names.

    Calculation: If both rule A and rule B of a firewall reference domain name 1 and domain name group A (containing domain names 2 and 3), then the number of domain names referenced by rule A or rule B is 3, and the number of domain names referenced by the firewall instance is 6.
  - A network domain name group can store up to 1,000 DNS resolution results. If the number of DNS resolution results exceeds 1,000, domain names may fail to be accessed. For domain names with a large number of resolution results or frequent changes, if the protected traffic is HTTP or HTTPS traffic, you are advised to use the application domain name group to add policies.

  – Domain name protection depends on the DNS server you configure. The default DNS server may be unable resolute complete IP addresses. You are advised to configure **DNS resolution** if the domain names of your services need to be accessed.

- Restrictions on regions: A protection rule with its source or destination set to a region (geographical location) takes effect only for IPv4 protected objects.
- 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.

Impacts on Services

When configuring a blocking rule, if address translation or proxy is involved, evaluate the impact of blocking IP addresses with caution.

Adding a VPC Border Protection Rule

Step 1 Enable VPC border firewall protection. For details, see **Enabling VPC Border Traffic Protection**.

Step 2 (Optional) To add multiple IP addresses, domain names, and services (protocols, source ports, and destination ports), add their groups first.

- For details about how to add multiple IP addresses, see **Managing IP Address Groups**.
- For details about how to add multiple domain names, see **Managing Domain Name Groups**.
- For details about how to add multiple services, see **Managing Service Groups**.

Step 3 In the navigation pane on the left of the CFW console, choose **Access Control** > **VPC Border Protection Rules**.

Step 4 Add a protection rule.

On the **Protection Rules** tab, click **Add Rule**. In the displayed dialog box, enter information. For details, see **Table 5-4**.

Table 5-4 VPC border protection rule parameters

Parameter	Description
Name	Name of the custom security policy.

Parameter	Description
Source	Set the party that originates a session. - **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
Destination	Set the recipient of a session. - **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**. - **Domain Name/Domain Name Group**: Domain names or domain groups can be protected. **Application**: Supports the protection for domain names or wildcard domain names. Application-layer protocols such as HTTP, HTTPS, TLS, SMTPS, and POPS are supported. Domain names are used for matching. - **Any**: any destination address

Parameter	Description
Service	Set the protocol and port number of the access traffic. ● **Service**: Set **Protocol Type**, **Source Port**, and **Destination Port**. – **Protocol**: The value can be **TCP**, **UDP**, or **ICMP**. – **Source/Destination Port**: If **Protocol** is set to **TCP** or **UDP**, you need to set the port number. ■ 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). For details about how to add a custom service group, see **Adding a Service Group**. ● **Any**: any protocol type or port number
Application	(Optional) Configure a protection policy for application-layer protocols. This parameter is mandatory when **Destination** is set to **Domain Name/domain Group**. ● If **Service** is set to **Any**, all application types are supported. ● If **Service** is set to **Service** and **Protocol** is set to **TCP**, TCP applications, such as HTTP and HTTPS, are supported. ● If **Service** is set to **Service** and **Protocol** is set to **UDP**, UDP applications, such as DNS and RDP, are supported.
Protection Action	Set the action to be taken when traffic passes through the firewall. ● **Allow**: Traffic is forwarded. ● **Block**: Traffic is not forwarded.
Status	Whether a policy is enabled. ● ◉: enabled ● ○: disabled
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.

Parameter	Description
Schedule Management	(Optional) Click **Schedule Management** and configure when the rule is in effect. Select or **add a schedule**.
Allow Long Connection	If only one service is configured in the current protection rule and **Protocol** is set to **TCP** or **UDP**, you can configure the service session aging time (unit: second).
Long Connection Duration	If **Allow Long Connection** is set to **Yes**, you need to set the persistent connection duration and set **hour**, **minute**, and **second**.
Tag	(Optional) Tags are used to identify rules. You can use tags to classify and search for security policies.
Description	(Optional) Usage and application scenario

Step 5 Click **OK** to complete the protection rule configuration.

----End

Viewing Protection Rule Hits

After your services run for a period of time, you can view the number of rule hits in the **Hits** column of the protection rule list.

Follow-up Operations

Checking protection outcomes:

- Policy hits: For details about the protection overview, see **Viewing Protection Information Using the Policy Assistant**. For details about logs, see **Access Control Logs**.
- For details about the traffic trend and statistics, see **Traffic Analysis**. For details about traffic records, see **Traffic Logs**.

References

- For details about how to add protection rules in batches, see **Importing and Exporting Protection Policies**.
- For details about how to adjust rule priority, see **Adjusting the Priority of a Protection Rule**.

5.2.3 Configuring Protection Rules to Block or Allow NAT Gateway Border Traffic

After protection is enabled, CFW allows all traffic by default. You can configure protection rules to block or allow traffic.

Protection Rule Description

The protected objects, actions, and application scenarios of protection rules are as follows.

Name	Description
Protected objects	● 5-tuples ● IP address groups ● Geographical locations ● Domain names and domain name groups (layer-4 and layer-7 traffic) ● Applications
Network types	● EIPs ● Private IP addresses
Actions	● If **Block** is selected, traffic will be blocked. ● If **Allow** is selected, traffic will be allowed by protection rules and then checked by IPS.
Scenarios	You can configure protection rules in the following scenarios: ● This section describes how to protect the traffic of private network assets at the Internet border. – For details about DNAT traffic, see **Adding a DNAT Traffic Protection Rule**. – For details about SNAT traffic, see **Adding a SNAT Traffic Protection Rule**. ● Protect the traffic of public network assets (EIPs) at the Internet border. For details, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**. ● Protect the access traffic between VPCs, or between a VPC and an IDC. For details, see **Configuring Protection Rules to Block or Allow VPC Border 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 Blacklist or Whitelist Items to Block or Allow Traffic**.

Specification Limitations

Only the **professional edition** supports NAT traffic (private IP address) protection.

Constraints

- CFW does not support application-level gateways (ALGs). If ALG-related services (such as SIP and FTP) are available, you are advised to add a rule to allow the traffic to pass through all the ports of data channels.

- To use CFW persistent connections, enable a bidirectional bypass policy. If you only enable a unidirectional policy, the client will need to re-initiate connections in certain scenarios, such as enabling or disabling protection, and expanding engine capacities. You can also **create a service ticket** to evaluate the risks of related issues.
- Quota:
  - Up to 20,000 protection rules can be added.
  - The restrictions on a single protection rule are as follows:
    - For IPv4, up to 4,000 source and 4,000 destination IP addresses are allowed. For IPv6, up to 2,000 source and 2,000 destination IP addresses are allowed.
    - A maximum of 20 source IP addresses and 20 destination IP addresses can be added.
    - A maximum of five source IP address groups and five destination IP address groups can be associated. A maximum of 1,666 IP address group members can be associated with each protection rule.
    - A maximum of five service groups can be associated.
- Restrictions on domain name protection:
  - Domain names in Chinese are not supported.
  - Restrictions on application-layer domain name reference:
    - Each firewall instance can reference up to 60,000 domain names.
    - Each firewall instance can reference up to 1,000 wildcard domain names.
    - Each protection rule can reference up to 20,000 domain names.
    - Each protection rule can reference up to 128 wildcard domain names.

    Calculation: If both rule A and rule B of a firewall reference domain name 1 and domain name group A (containing domain names 2 and 3), then the number of domain names referenced by rule A or rule B is 3, and the number of domain names referenced by the firewall instance is 6.
  - A network domain name group can store up to 1,000 DNS resolution results. If the number of DNS resolution results exceeds 1,000, domain names may fail to be accessed. For domain names with a large number of resolution results or frequent changes, if the protected traffic is HTTP or HTTPS traffic, you are advised to use the application domain name group to add policies.
  - Domain name protection depends on the DNS server you configure. The default DNS server may be unable resolute complete IP addresses. You are advised to configure **DNS resolution** if the domain names of your services need to be accessed.
- Restrictions on regions: A protection rule with its source or destination set to a region (geographical location) takes effect only for IPv4 protected objects.
- **Pre-defined Address Groups** can be configured only for **Source** address for a DNAT rule.

- 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.

Impacts on Services

When configuring a blocking rule, if address translation or proxy is involved, evaluate the impact of blocking IP addresses with caution.

Adding a DNAT Traffic Protection Rule

Step 1 Enable NAT traffic protection. For details, see **Enabling NAT Gateway Traffic Protection**.

Step 2 (Optional) To add multiple IP addresses, domain names, and services (protocols, source ports, and destination ports), add their groups first.

- For details about how to add multiple IP addresses, see **Managing IP Address Groups**.
- For details about how to add multiple domain names, see **Managing Domain Name Groups**.
- For details about how to add multiple services, see **Managing Service Groups**.

Step 3 In the navigation pane on the left of the CFW console, choose **Access Control** > **Internet Border Protection Rules**.

Step 4 Add a protection rule.

On the **Protection Rules** tab, click **NAT**. In the displayed dialog box, click **Add Rule**, enter information. For details, see **Table 5-5**.

Table 5-5 DNAT protection rule parameters

Parameter	Description
Rule Type	Select **NAT** to protect the traffic of the NAT gateway. Private IP addresses can be configured. **NOTE** To select the NAT rule, ensure that: ● The professional edition firewall is used. For details about how to upgrade your edition, see **Upgrading a CFW**. ● The VPC border firewalls have been configured. For details, see **Managing VPC Border Firewalls**.
Name	Name of the custom security policy.
Direction	Select **DNAT**.

Parameter	Description
Source	Set the party that originates a session. ● **IP address**: Enter EIPs. This parameter can be configured in the following formats: – A single EIP, for example, *xx.xx*.**10.5** – Consecutive EIPs, for example, *xx.xx*.**0.2-***xx.xx*.**0.10** – EIP segment, for example, *xx.xx*.**2.0/24** ● **IP address group**. You can configure multiple EIPs. If **Direction** is set to **Inbound**, a predefined address group can be configured for the source address. For details about user-defined and predefined IP address groups, see **Managing IP Address Groups**. ● **Countries and regions**: A continent, a country, or a region ● **Any**: any source address
Destination	Set the recipient of a session. ● **IP address**: Enter private IP addresses. 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**. You can configure multiple private IP addresses. For details about how to add an IP address group, see **Adding a User-defined IP Address Group**. ● **Any**: any destination address

Parameter	Description
Service	● **Service**: Set **Protocol Type**, **Source Port**, and **Destination Port**. – **Protocol**: The value can be **TCP**, **UDP**, or **ICMP**. – **Source/Destination Port**: If **Protocol** is set to **TCP** or **UDP**, you need to set the port number. ■ 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). For details about user-defined and predefined service groups, see **Managing Service Groups**. ● **Any**: any protocol type or port number
Application	(Optional) Configure protection policies for application-layer protocols. ● When **Service** is set to **Any**, all application types are supported. ● If **Service** is set to **Service** and **Protocol** is set to **TCP**, TCP applications, such as HTTP and HTTPS, are supported. ● If **Service** is set to **Service** and **Protocol** is set to **UDP**, UDP applications, such as DNS and RDP, are supported.
Protection Action	Set the action to be taken when traffic passes through the firewall. ● **Allow**: Traffic is forwarded. ● **Block**: Traffic is not forwarded.
Status	Whether a policy is enabled. ● ◉: enabled ● ○: disabled
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.

Parameter	Description
Schedule Management	(Optional) Click **Schedule Management** and configure when the rule is in effect. Select or **add a schedule**.
Allow Long Connection	If only one service is configured in the current protection rule and **Protocol** is set to **TCP** or **UDP**, you can configure the service session aging time (unit: second).
Long Connection Duration	If **Allow Long Connection** is set to **Yes**, you need to set the persistent connection duration and set **hour**, **minute**, and **second**.
Tag	(Optional) Tags are used to identify rules. You can use tags to classify and search for security policies.
Description	(Optional) Usage and application scenario

Step 5 Click **OK** to complete the protection rule configuration.

----End

Adding a SNAT Traffic Protection Rule

Step 1 Enable NAT traffic protection. For details, see **Enabling NAT Gateway Traffic Protection**.

Step 2 (Optional) To add multiple IP addresses, domain names, and services (protocols, source ports, and destination ports), add their groups first.

- For details about how to add multiple IP addresses, see **Managing IP Address Groups**.
- For details about how to add multiple domain names, see **Managing Domain Name Groups**.
- For details about how to add multiple services, see **Managing Service Groups**.

Step 3 In the navigation pane on the left of the CFW console, choose **Access Control** > **Internet Border Protection Rules**.

Step 4 Add a protection rule.

On the **Protection Rules** tab, click **NAT**. In the displayed dialog box, click **Add Rule**, enter information. For details, see **Table 5-6**.

Table 5-6 SNAT protection rule parameters

Parameter	Description
Rule Type	Select **NAT** to protect the traffic of the NAT gateway. Private IP addresses can be configured. **NOTE** To select the NAT rule, ensure that: ● The professional edition firewall is used. For details about how to upgrade your edition, see **Upgrading a CFW**. ● The VPC border firewalls have been configured. For details, see **Managing VPC Border Firewalls**.
Name	Name of the custom security policy.
Direction	Select **SNAT**.
Source	Set the party that originates a session. ● **IP address**: Enter private IP addresses. 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**: You can add multiple private IP addresses to an IP address group. For details about how to add an IP address group, see **Adding an IP Address Group**. ● **Any**: any source address

Parameter	Description
Destination	Set the recipient of a session. ● **IP address**: Enter EIPs. This parameter can be configured in the following formats: – A single EIP, for example, *xx.xx*.**10.5** – Consecutive EIPs, for example, *xx.xx*.**0.2-***xx.xx*.**0.10** – EIP segment, for example, *xx.xx*.**2.0/24** ● **IP address group**. You can configure multiple EIPs. If **Direction** is set to **Inbound**, a predefined address group can be configured for the source address. For details about user-defined and predefined IP address groups, see **Managing IP Address Groups**. ● **Countries and regions**: A continent, a country, or a region ● **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, HTTPS, TLS, SMTPS, and POPS 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. NOTE – To protect the domain names of HTTP, HTTPS, TLS, SMTPS, and POPS applications, you can select any options. – To protect the wildcard domain names of HTTP, HTTPS, TLS, SMTPS, or POPS, you select any option under **Application**. (A wildcard domain name is in the format of *****.*Domain name*. The wildcard character * matches any character or string. For example, ***.example.com**.) – 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 **Domain name** is selected, up to 600 IP addresses can be resolved.) – If you need to configure the wildcard domain names or application domain name groups of the HTTP, HTTPS, TLS, SMTPS, and POPS 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-type domain names, see **Adding a Domain Name Group**. ● **Any**: any destination address

Parameter	Description
Service	● **Service**: Set **Protocol Type**, **Source Port**, and **Destination Port**. – **Protocol**: The value can be **TCP**, **UDP**, or **ICMP**. – **Source/Destination Port**: If **Protocol** is set to **TCP** or **UDP**, you need to set the port number. ■ 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). For details about how to add a custom service group, see **Adding a Service Group**. For details about predefined service groups, see **Viewing a Predefined Service Group**. ● **Any**: any protocol type or port number
Application	(Optional) Configure protection policies for application-layer protocols. ● When **Service** is set to **Any**, all application types are supported. ● If **Service** is set to **Service** and **Protocol** is set to **TCP**, TCP applications, such as HTTP and HTTPS, are supported. ● If **Service** is set to **Service** and **Protocol** is set to **UDP**, UDP applications, such as DNS and RDP, are supported.
Protection Action	Set the action to be taken when traffic passes through the firewall. ● **Allow**: Traffic is forwarded. ● **Block**: Traffic is not forwarded.
Status	Whether a policy is enabled. ● : enabled ● : disabled
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.

Parameter	Description
Schedule Management	(Optional) Click **Schedule Management** and configure when the rule is in effect. Select or **add a schedule**.
Allow Long Connection	If only one service is configured in the current protection rule and **Protocol** is set to **TCP** or **UDP**, you can configure the service session aging time (unit: second).
Long Connection Duration	If **Allow Long Connection** is set to **Yes**, you need to set the persistent connection duration and set **hour**, **minute**, and **second**.
Tag	(Optional) Tags are used to identify rules. You can use tags to classify and search for security policies.
Description	(Optional) Usage and application scenario

Step 5 Click **OK** to complete the protection rule configuration.

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

----End

Viewing Protection Rule Hits

After your services run for a period of time, you can view the number of rule hits in the **Hits** column of the protection rule list.

Follow-up Operations

Checking protection outcomes:

- Policy hits: For details about the protection overview, see **Viewing Protection Information Using the Policy Assistant**. For details about logs, see **Access Control Logs**.
- For details about the traffic trend and statistics, see **Traffic Analysis**. For details about traffic records, see **Traffic Logs**.

References

- For details about how to add protection rules in batches, see **Importing and Exporting Protection Policies**.
- For details about how to adjust rule priority, see **Adjusting the Priority of a Protection Rule**.

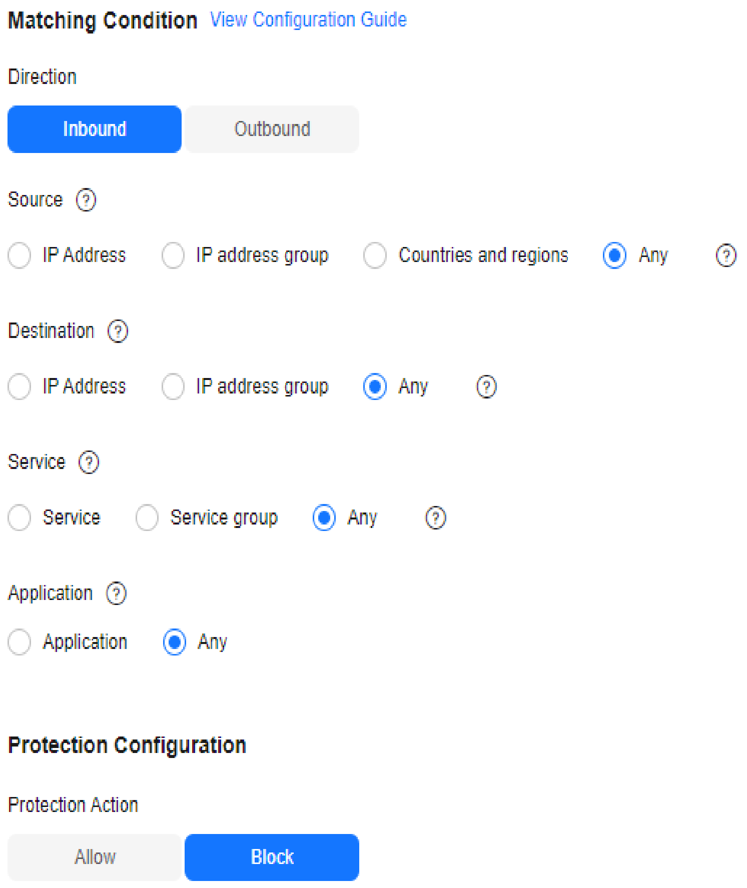
5.2.4 Example 1: Allowing the Inbound Traffic from a Specified IP Address

This section describes how to allow access traffic from a specified IP address in the inbound direction. For more parameter settings, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.

Allowing the Inbound Traffic from a Specified IP Address

Configure two protection rules. One of them blocks all traffic, as shown in **Figure 5-2**. Its priority is the lowest. The other allows the traffic of a specified IP address, as shown in **Figure 5-3**, and its priority is the highest. Configure other parameters as needed.

Figure 5-2 Blocking all traffic



Matching Condition View Configuration Guide

Direction

[✓ Inbound] Outbound

Source ?

○ IP Address ○ IP address group ○ Countries and regions ● Any ?

Destination ?

○ IP Address ○ IP address group ● Any ?

Service ?

○ Service ○ Service group ● Any ?

Application ?

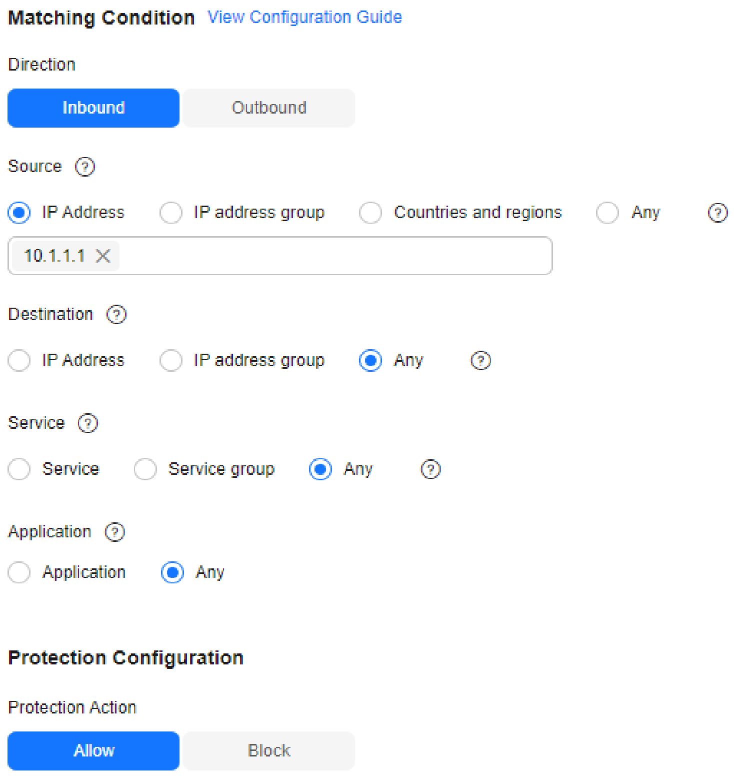
○ Application ● Any

Protection Configuration

Protection Action

Allow [✓ Block]

Figure 5-3 Allowing a specified IP address



Matching Condition View Configuration Guide

Direction

Inbound | Outbound

Source

● IP Address ○ IP address group ○ Countries and regions ○ Any

10.1.1.1 ×

Destination

○ IP Address ○ IP address group ● Any

Service

○ Service ○ Service group ● Any

Application

○ Application ● Any

Protection Configuration

Protection Action

Allow | Block

Follow-up Operations

Checking protection outcomes

- Policy hits: For details about the protection overview, see **Viewing Protection Information Using the Policy Assistant**. For details about logs, see **Access Control Logs**.
- For details about the traffic trend and statistics, see **Traffic Analysis**. For details about traffic records, see **Traffic Logs**.

References

- For details about protection rule parameters, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.
- For details about blacklist and whitelist configuration, see **Adding Blacklist or Whitelist Items to Block or Allow Traffic**.
- For details about how to batch add protection policies, see **Importing and Exporting Protection Policies**.
- For details about how to block network attacks, see **Configuring Intrusion Prevention**.
- For details about antivirus, see **Configuring Virus Defense**.

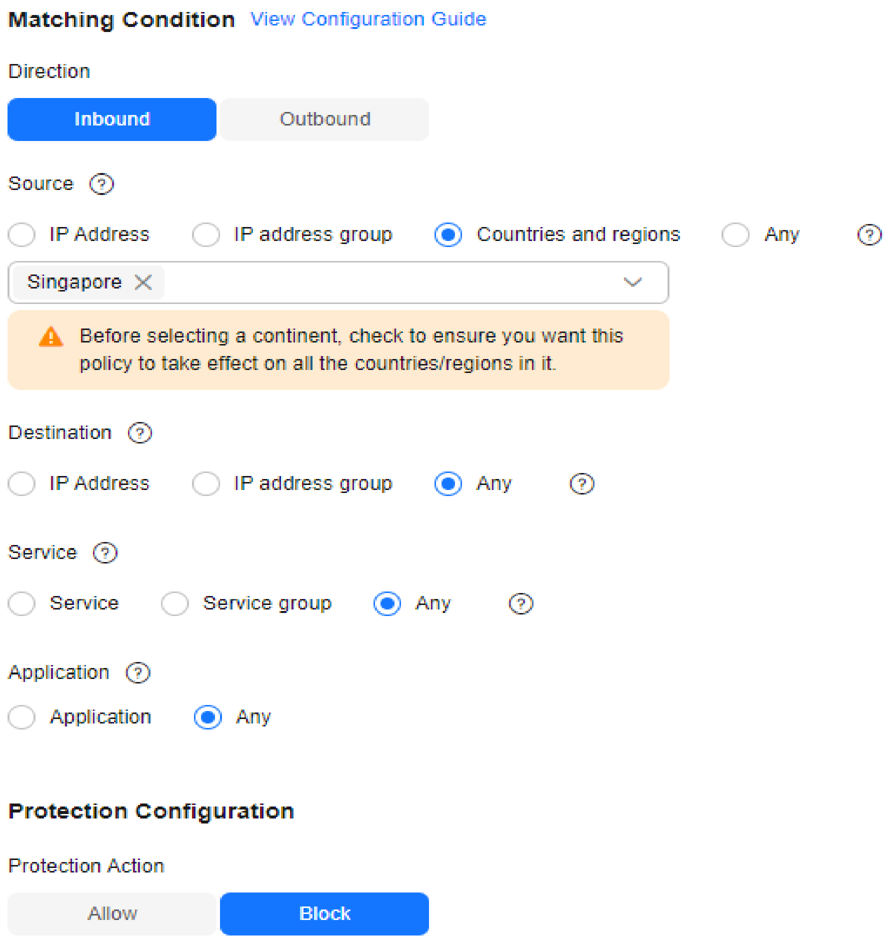
5.2.5 Example 2: Blocking Access from a Region

This section describes how to block access traffic from a region. For more parameter settings, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.

Blocking Access from a Region

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

Figure 5-4 Intercepting the access traffic from Singapore



Matching Condition View Configuration Guide

Direction: Inbound (selected) | Outbound

Source: ○ IP Address ○ IP address group ● Countries and regions ○ Any

Singapore

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

Destination: ○ IP Address ○ IP address group ● Any

Service: ○ Service ○ Service group ● Any

Application: ○ Application ● Any

Protection Configuration

Protection Action: Allow | Block (selected)

Follow-up Operations

Checking protection outcomes

- Policy hits: For details about the protection overview, see **Viewing Protection Information Using the Policy Assistant**. For details about logs, see **Access Control Logs**.
- For details about the traffic trend and statistics, see **Traffic Analysis**. For details about traffic records, see **Traffic Logs**.

References

- For details about protection rule parameters, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.
- For details about blacklist and whitelist configuration, see **Adding Blacklist or Whitelist Items to Block or Allow Traffic**.
- For details about how to batch add protection policies, see **Importing and Exporting Protection Policies**.

- For details about how to block network attacks, see **Configuring Intrusion Prevention**.
- For details about antivirus, see **Configuring Virus Defense**.

5.2.6 Example 3: Allowing Traffic from a Service to a Platform

This section describes how to allow traffic from a service to a platform. For more parameter settings, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.

Domain Name Group Types

CFW provides two types of domain name groups: application domain name groups (layer 7 protocol parsing) and network domain name groups (layer 4 protocol parsing). **Table 5-7** describes the differences between them.

Table 5-7 Domain name group types

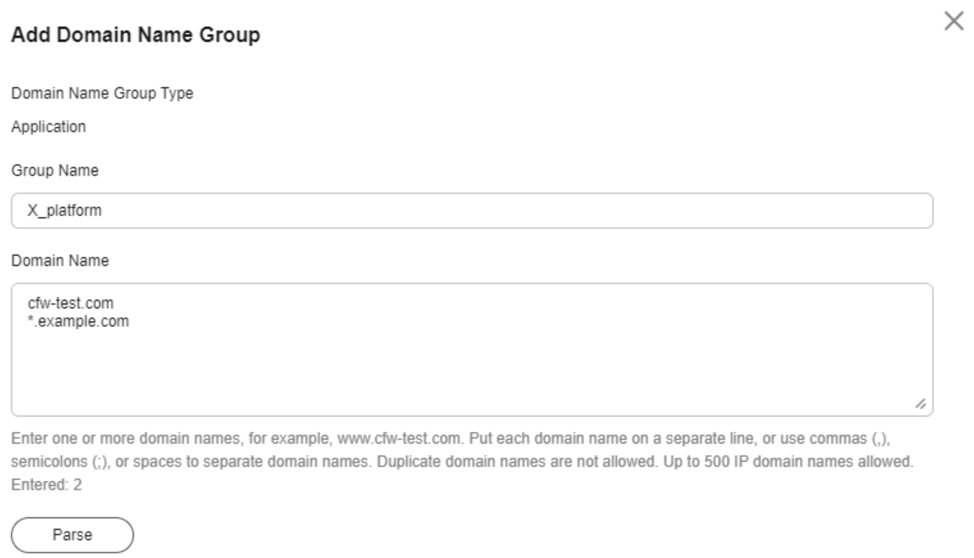
-	Application Domain Name Group (Layer 7 Protocol Parsing)	Network Domain Name Group (Layer 4 Protocol Parsing)
Protected object	● Domain names ● Wildcard domain names	● A single domain name ● Multiple domain names
Protocol Type	Application layer protocols, including HTTP, HTTPS, TLS, SMTPS, and POPS.	Network layer protocols. All protocol types are supported.
Match rule	The match is based on domain name. The service compares the HOST field in sessions with the application domain names. If they are consistent, the corresponding protection rule is hit.	The filtering is based on the resolved IP addresses. The service 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.
Suggestion	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.	

Allowing Traffic from a Service to a Platform

To allow an EIP (xx.xx.xx.48) to access **cfw-test.com** and ***.example.com**, configure parameters as follows. The parameters not mentioned below can be configured as needed.

- Create an application domain name group and configure the platform domain names, as shown in **Figure 5-5**.
- Configure the following protection rules:
  - One of the rule blocks all traffic, as shown in **Figure 5-6**. The priority is the lowest.
  - The other rule allows the traffic from the EIP to the platform, as shown in **Figure 5-7**. The priority is the highest.

Figure 5-5 Adding the domain name group of a platform



Add Domain Name Group

Domain Name Group Type

Application

Group Name

X_platform

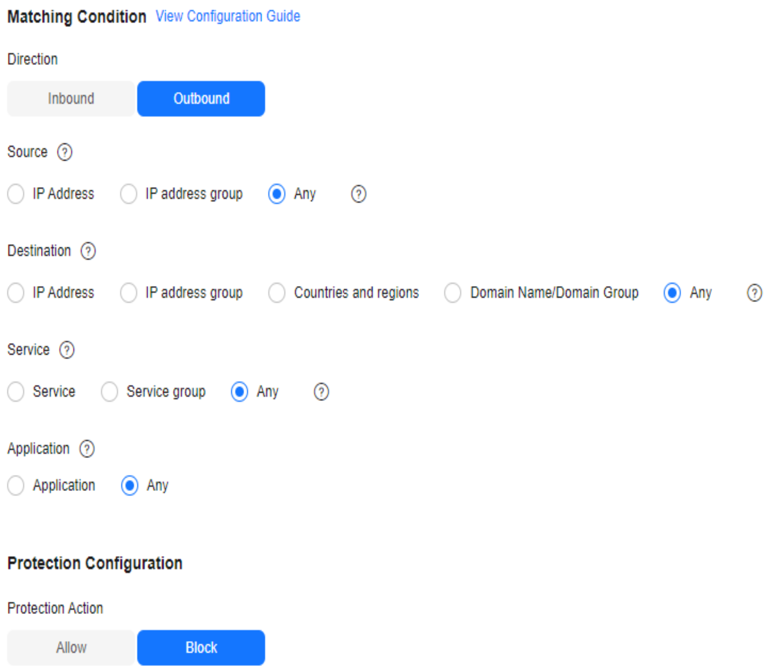
Domain Name

cfw-test.com
*.example.com

Enter one or more domain names, for example, www.cfw-test.com. Put each domain name on a separate line, or use commas (,), semicolons (;), or spaces to separate domain names. Duplicate domain names are not allowed. Up to 500 IP domain names allowed.

Entered: 2

Figure 5-6 Blocking all traffic



Matching Condition View Configuration Guide

Direction

Inbound [✓ Outbound]

Source ⓘ

○ IP Address ○ IP address group ● Any ⓘ

Destination ⓘ

○ IP Address ○ IP address group ○ Countries and regions ○ Domain Name/Domain Group ● Any ⓘ

Service ⓘ

○ Service ○ Service group ● Any ⓘ

Application ⓘ

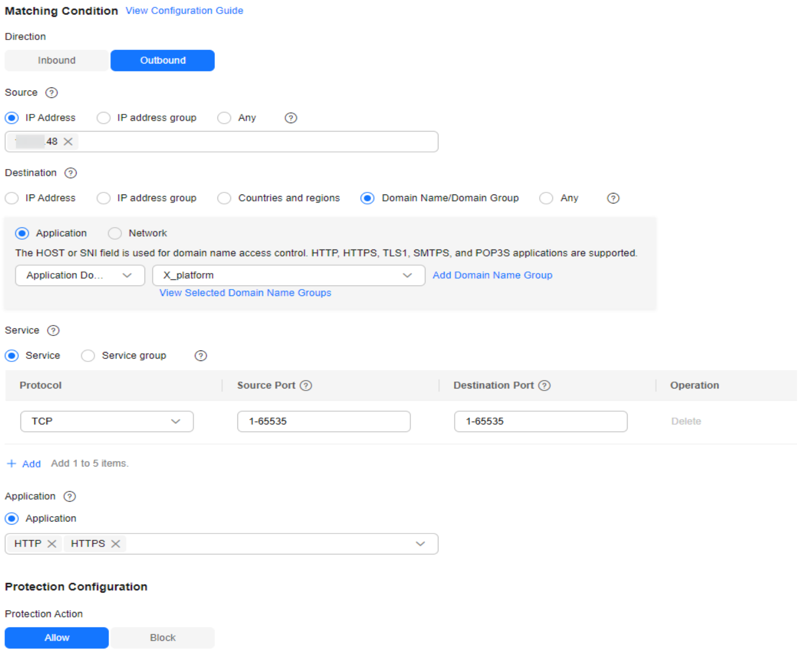
○ Application ● Any

Protection Configuration

Protection Action

Allow [✓ Block]

Figure 5-7 Allowing the traffic from an EIP to a platform



Matching Condition View Configuration Guide

Direction

Inbound [✓ Outbound]

Source ⓘ

● IP Address ○ IP address group ○ Any ⓘ

[redacted]48 ×

Destination ⓘ

○ IP Address ○ IP address group ○ Countries and regions ● Domain Name/Domain Group ○ Any ⓘ

● Application ○ Network

The HOST or SNI field is used for domain name access control. HTTP, HTTPS, TLS1, SMTPS, and POP3S applications are supported.

Application Do... | X_platform | Add Domain Name Group

View Selected Domain Name Groups

Service ⓘ

● Service ○ Service group ⓘ

Protocol	Source Port ⓘ	Destination Port ⓘ	Operation
TCP	1-65535	1-65535	Delete

+ Add Add 1 to 5 items.

Application ⓘ

● Application

HTTP × HTTPS ×

Protection Configuration

Protection Action

[✓ Allow] Block

Follow-up Operations

Checking protection outcomes

- Policy hits: For details about the protection overview, see **Viewing Protection Information Using the Policy Assistant**. For details about logs, see **Access Control Logs**.
- For details about the traffic trend and statistics, see **Traffic Analysis**. For details about traffic records, see **Traffic Logs**.

References

- For details about protection rule parameters, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.
- For details about blacklist and whitelist configuration, see **Adding Blacklist or Whitelist Items to Block or Allow Traffic**.
- For details about how to batch add protection policies, see **Importing and Exporting Protection Policies**.
- For details about how to block network attacks, see **Configuring Intrusion Prevention**.
- For details about antivirus, see **Configuring Virus Defense**.

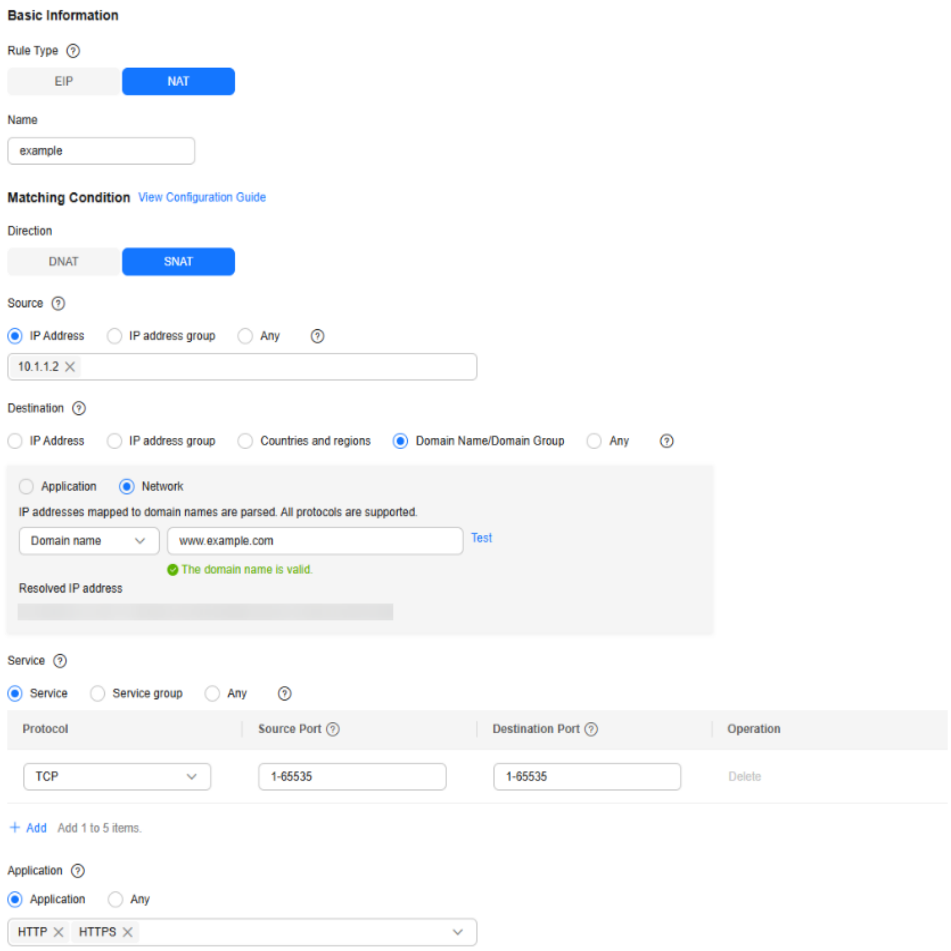
5.2.7 Example 4: Configuring SNAT Protection Rules

This section describes how to configure SNAT-based defense. For more parameter settings, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.

SNAT Protection Configuration

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 5-8 Configuring a NAT protection rule



Basic Information

Rule Type: EIP [✓ NAT]

Name: example

Matching Condition

Direction: DNAT [✓ SNAT]

Source: ● IP Address ○ IP address group ○ Any

10.1.1.2

Destination: ○ IP Address ○ IP address group ○ Countries and regions ● Domain Name/Domain Group ○ Any

○ Application ● Network

IP addresses mapped to domain names are parsed. All protocols are supported.

Domain name: www.example.com

The domain name is valid.

Resolved IP address

Service: ● Service ○ Service group ○ Any

Protocol	Source Port	Destination Port	Operation
TCP	1-65535	1-65535	Delete

Add 1 to 5 items.

Application: ● Application ○ Any

HTTP, HTTPS

Follow-up Operations

Checking protection outcomes

- Policy hits: For details about the protection overview, see **Viewing Protection Information Using the Policy Assistant**. For details about logs, see **Access Control Logs**.
- For details about the traffic trend and statistics, see **Traffic Analysis**. For details about traffic records, see **Traffic Logs**.

References

- For details about protection rule parameters, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.
- For details about blacklist and whitelist configuration, see **Adding Blacklist or Whitelist Items to Block or Allow Traffic**.
- For details about how to batch add protection policies, see **Importing and Exporting Protection Policies**.
- For details about how to block network attacks, see **Configuring Intrusion Prevention**.
- For details about antivirus, see **Configuring Virus Defense**.

5.2.8 Adding Blacklist or Whitelist Items to Block or Allow Traffic

After protection is enabled, CFW allows all traffic by default. You can configure the blacklist to block access requests from IP addresses or configure the whitelist to allow them.

This topic describes how to add a single blacklist or whitelist item. For details about how to add items in batches, see **Importing and Exporting Protection Policies**.

Blacklist and Whitelist Policy Description

The protected objects, actions, and application scenarios of blacklist and whitelist policies are as follows.

Name	Description
Protected object	● 5-tuples ● IP address groups
Network type	● EIP ● Private IP address
Action	● Blacklist: The traffic is directly blocked. ● Whitelist: Traffic is allowed by CFW and not checked by other functions.
Scenario	● Blacklist: Block known malicious traffic. ● Whitelist: Allow trusted IP address 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 the blacklist, 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 protection rules, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.

Specification Limitations

- CFW allows up to 2000 blacklist items and 2000 whitelist items.
  - If the number of IP addresses to be added to the blacklist exceeds the upper limit, you can use the traffic blocking function to quickly block IP addresses. For details, see **Quickly Block Malicious Traffic Through Traffic Blocking**.
  - The whitelist is not the only way to control traffic. If you have too many IP addresses to manage, you can also create IP address groups and reference them in protection rules to allow their traffic.

    - For details about how to add an IP address group, see **Adding User-defined Address Groups**.
    - For details about how to add a protection rule, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.
- To protect private IP addresses, use the professional edition firewall and enable **VPC border firewall** protection.

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**.
- When configuring a blacklist, if address translation or proxy is involved, evaluate the impact of blocking IP addresses with caution.

Adding Blacklist or Whitelist Items to Block or Allow Internet Border Traffic

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

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

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

Step 4 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

Step 5 In the navigation pane on the left of the CFW console, choose **Access Control** > **Internet Border Protection Rules**.

Step 6 Click the **Blacklist** or **Whitelist** tab.

Step 7 Click **Add**. Set the address direction, IP address, protocol type, and port number. For details, see **Table 5-8**.

Table 5-8 Blacklist and whitelist parameters on the Internet border

Parameter	Description
Direction	You can select **Source** or **Destination**. ● **Source**: the party that originates a session. ● **Destination**: the recipient of a session.
Protocol Type	Its value can be **TCP**, **UDP**, or **Any**.

Parameter	Description
Port	If **Protocol Type** is set to **TCP** or **UDP**, set the ports to be allowed or blocked. ● 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**.
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.
Description	(Optional) remarks of the blacklist or whitelist

Step 8 Click **OK**.

----End

Adding Blacklist or Whitelist Items to Block or Allow VPC Border Traffic

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

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

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

Step 4 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

Step 5 In the navigation pane on the left of the CFW console, choose **Access Control** > **VPC Border Protection Rules**.

Step 6 Click the **Blacklist** or **Whitelist** tab.

Step 7 Click **Add**. Set the address direction, IP address, protocol type, and port number. For details, see **Table 5-9**.

Table 5-9 VPC border blacklist/whitelist

Parameter	Description
Direction	You can select **Source** or **Destination**. ● **Source**: the party that originates a session. ● **Destination**: the recipient of a session.
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. ● 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**.
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.
Description	(Optional) remarks of the blacklist or whitelist

Step 8 Click **OK**.

----End

References

- For details about how to edit and remove blacklist or whitelist items, see **Managing the Blacklist and the Whitelist**.
- For details about how to add blacklist or whitelist items in batches, see **Importing and Exporting Protection Policies**.
- For details about how to quickly import a large number of blacklists, see **Quickly Block Malicious Traffic Through Traffic Blocking**.
- For details about how to add refined access control configuration, you can configure protection rules. For details, see **Configuring an Access Control Policy**.
- For details about how to block malicious attacks, see **Attack Defense**.

5.2.9 Quickly Block Malicious Traffic Through Traffic Blocking

During routine O&M, you may encounter attacks from a large number of malicious IP addresses. You need to quickly block the traffic. However, manually configuring the blacklist is inefficient. CFW provides the one-click traffic blocking function, which allows you to block all malicious access by simply adding the malicious IP addresses to the firewall.

Traffic Blocking Policy Description

The protected objects, actions, and application scenarios of traffic blocking policies are as follows.

Name	Description
Protected object	IP addresses
Network type	● EIP ● Private IP address
Action	Traffic is blocked directly.
Scenario	● Defense against malicious traffic attacks: In the case of a DoS attack, malicious traffic can be quickly blocked to ensure network security. ● Preventing incorrect internal connections: If an internal device connects to a malicious server by mistake, sensitive information may be leaked. Quickly blocking connections can effectively prevent system damage. ● Service risk control and management: Service operation needs to restrict the access to non-service-related resources to ensure the smooth running of core services.

Constraints

- Only the following formats are supported:
  - IP address, for example, **10.0.0.0**.
  - Multiple consecutive IP addresses, for example, **10.0.0.0-10.0.1.0**.
  - Address segment, for example, **10.0.0.0/16**.
- Only files in **.txt** or **.csv** format or text input is supported.
- Number of IP addresses that can be added to a single firewall instance:
  - Standard edition: 100,000
  - Professional edition: 500,000
- Only the professional edition supports NAT traffic protection. All editions support EIP traffic protection.

Impact on the System

- After an IP address is added to the traffic blocking list, traffic destined for and from this IP address will be blocked.
- When configuring an IP address to be blocked, if address translation or proxy is involved, evaluate the impact of blocking IP addresses with caution.

Quickly Block Malicious Traffic Through Traffic Blocking

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

Step 5 In the navigation pane, choose **Access Control** > **Traffic Filtering**. The **Traffic Blocking** page is displayed.

Step 6 Click ○ to enable the traffic blocking function.

NOTE

If a blocked file exists in the list, check the IP address and then enable this button.

Step 7 To add the IP addresses to be blocked, click **Add Object** and set parameters.

Table 5-10 Add object

Parameter	Description
Mode	Select the method of adding the blocked IP address. ● **Append**: The existing IP addresses remain unchanged, and the newly imported IP addresses are added. ● **Overwrite**: The newly imported IP addresses will replace the existing IP addresses.
Effective Scope	Select the object to be blocked. ● EIP ● NAT (Only the professional edition can protect NAT traffic.)

Parameter	Description
Content Type	Selects a type. ● File upload: Click **Add**. Only files in **.txt** or **.csv** format can be uploaded or text input is supported. ● Text input: Enter an IP address in the **IP Address** text box. The total text length cannot exceed 4,000 characters. The following formats are supported: ● IP address, for example, **10.0.0.0**. ● Multiple consecutive IP addresses, for example, **10.0.0.0-10.0.1.0**. ● Address segment, for example, **10.0.0.0/16**.

Step 8 Click **OK**. **Added** is displayed in the **Status** column.

If the file fails to be added, modify the file or text as prompted and add the file again.

----End

Follow-up Operations

For details about how to view logs, see **Attack Event Logs**.

NOTE

A log record is generated every minute. Each record summarizes the data in the minute.

References

- Viewing or exporting IP address information: Click **Download** in the **Operation** column of the row that contains the target IP address. The downloaded file contains all added IP address information.
- Deleting IP address information: Click **Delete** in the **Operation** column of the row that contains the IP address, enter **DELETE**, and click **OK**.

  NOTE

  The deletion operation cannot be performed on the content added at a time. When the deletion operation is performed, all IP addresses within the **EIP** or **NAT** will be cleared.

5.3 Viewing Protection Information Using the Policy Assistant

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

Viewing Protection Information Using the Policy Assistant

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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 5-11**. Click a record to view the policy matching details. For details, see **Table 8-2**.

Table 5-11 Policy assistant statistics parameters

Parameter	Description
Top Policies By Hits	Policies that match and block traffic.
Top Blocked Outbound IP Addresses	Blocked outbound IP addresses. You can click **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 a week, a month, three months, or six months. You are advised to modify or delete the policies in a timely manner.

----End

References

- For details about how to add a blacklist or whitelist for traffic protection, see **Adding Blacklist or Whitelist Items to Block or Allow Traffic**. For details about how to add a protection rule for traffic protection, see:
  - For details about how to protect the traffic from the Internet to cloud assets (EIPs), see **Accessing from the Internet to Assets on the Cloud (Inbound)**.
  - For details about how to protect the traffic from cloud assets (EIPs) to the Internet, see **Accessing from the Cloud Assets to the Internet (Outbound)**.
  - For details about how to protect the access traffic between VPCs, or between a VPC and an IDC, see **Configuring Protection Rules to Block or Allow VPC Border Traffic**.
  - For details about how to protect the traffic of private network assets at the Internet border, see **Configuring Protection Rules to Block or Allow NAT Gateway Border Traffic**.
- For details about how to add protection policies in batches, see **Importing and Exporting Protection Policies**.
- If your traffic is incorrectly blocked by a protection policy, troubleshoot the problem by referring to **What Can I Do If Services Cannot Be Accessed After a Policy Is Configured on CFW?**

5.4 Managing ACL Policies

5.4.1 Importing and Exporting Protection Policies

You can add and export protection rules, blacklist/whitelist items, IP address groups, domain name groups, and service groups in batches.

Specification Limitations

To import and export VPC border protection policies, use the **Professional** edition.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

Step 5 In the navigation pane on the left, choose **Access Control** > **Internet Border Protection Rules** or **VPC Border Protection Rules**.

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

Step 7 Click **Download Template** to download the rule import template to the local host.

Step 8 Configure protection policy information as required.

- Import restrictions:
  - 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.
- Parameter description:
  - Protection rule parameters:
    - For details about Internet border protection rule parameters, see **Parameters of Rule Import Template - Rule-Acl-Table (Internet Border Protection Rules)**.
    - For details about VPC border protection rule parameters, see **Parameters of Rule Import Template - Vpc-Rule-Acl-Table (VPC Border Protection Rule)**.
  - For details about the blacklist and whitelist parameters, see **Adding Blacklist or Whitelist Items to Block or Allow Traffic**.
  - For details about IP address group parameters, see **Managing IP Address Groups**.
  - For details about service group parameters, see **Managing Service Groups**.
  - For details about domain name group parameters, see **Managing Domain Name Groups**.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

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

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

----End

Parameters for Importing a Rule Template

Fill in the template by referring to the following parameter descriptions.

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

Table 5-12 Internet border 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 immediately and takes effect. ● **Disabled**: The rule is not in effect.	Enabled
Description	Rule description	test
Source Address Type	Select the type of the party that originates a session. ● **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** ● A single address segment, for example, **192.168.2.0/24** To specify multiple IP addresses or IP address segments, configure multiple rules. Specify different IP addresses (segments) in these rules but use the same settings for other parameters.	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 continent information based on the **continent-region-info** sheet.	AS: Asia

Parameter	Description	Example Value
Source Country Region	If **Source Address Type** is set to **Region**, you need to configure **Source Country Region**. Enter country and region information based on the **country-region-info** sheet.	CN: Chinese mainland
Destination Address Type	Select the type of the recipient of a session. ● **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** ● A single address segment, for example, **192.168.2.0/24** To specify multiple IP addresses or IP address segments, configure multiple rules. Specify different IP addresses (segments) in these rules but use the same settings for other parameters.	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

Parameter	Description	Example Value
Destination Continent Region	If **Destination Address Type** is set to **Region**, you need to set **Destination Continent Region**. Enter continent information based on the **continent-region-info** sheet.	AS: Asia
Destination Country Region	If **Destination Address Type** is set to **Region**, you need to set **Destination Country Region**. Enter country and region information based on the **country-region-info** sheet.	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

Parameter	Description	Example Value
Applications	Application type, such as **HTTP**, **HTTPS**, **DNS**, and **RDP**.	HTTP
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-Rule-Acl-Table (VPC Border Protection Rule)

Table 5-13 VPC border 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	Set the type of the party that originates a session. ● **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

Parameter	Description	Example Value
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** - A single address segment, for example, **192.168.2.0/24** To specify multiple IP addresses or IP address segments, configure multiple rules. Specify different IP addresses (segments) in these rules but use the same settings for other parameters.	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
Destination Address Type	Select the type of the recipient of a session. - **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** - A single address segment, for example, **192.168.2.0/24** To specify multiple IP addresses or IP address segments, configure multiple rules. Specify different IP addresses (segments) in these rules but use the same settings for other parameters.	192.168.10.6

Parameter	Description	Example Value
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
Service Group Name	Service group name. The name can contain up to 255 characters, including letters, numbers, underscores (_), hyphens (-), and spaces.	service_test
Applications	Application type, such as **HTTP**, **HTTPS**, **DNS**, and **RDP**.	HTTP
Group Tag	Tags are used to identify rules. You can use tags to classify and search for security policies.	k=a

References

- For details about how to add a protection rule, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.
- For details about how to batch add blacklist or whitelist items, see **Adding Blacklist or Whitelist Items to Block or Allow Traffic**.
- Checking protection outcomes
  - Policy hits: For details about the protection overview, see **Viewing Protection Information Using the Policy Assistant**. For details about logs, see **Access Control Logs**.

  - For details about the traffic trend and statistics, see **Traffic Analysis**. For details about traffic records, see **Traffic Logs**.
- For details about how to adjust rule priority, see **Adjusting the Priority of a Protection Rule**.

5.4.2 Adjusting the Priority of a Protection Rule

When traffic hits a rule, the action of the rule will be performed, and CFW will not match the traffic against other protection rules. You are advised to set the priorities of the allowing rules to be higher than those of the blocking rules, and set the priorities of specific rules to be higher than those of general rules.

This section describes how to adjust the priorities of protection rules.

Priority

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

Adjusting the Priority of a 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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

Step 5 In the navigation pane on the left, choose **Access Control** > **Internet Border Protection Rules** or **VPC Border Protection Rules**.

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 group or rule. The policy priority will be lower than the selected rule.

Step 8 Click **OK**.

----End

References

- For details about how to add a protection rule, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.
- For details about how to batch add blacklist or whitelist items, see **Adding Blacklist or Whitelist Items to Block or Allow Traffic**.
- Checking protection outcomes:

  - Policy hits: For details about the protection overview, see **Viewing Protection Information Using the Policy Assistant**. For details about logs, see **Access Control Logs**.
  - For details about the traffic trend and statistics, see **Traffic Analysis**. For details about traffic records, see **Traffic Logs**.
- For details about how to batch add protection policies, see **Importing and Exporting Protection Policies**.

5.4.3 Managing Protection Rules

This section describes the protection rule parameters page and how to edit, copy, and delete a protection rule.

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

Viewing Protection Rules

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

Step 5 In the navigation pane on the left, choose **Access Control** > **Internet Border Protection Rules** or **VPC Border Protection Rules**.Select the **Internet Border** or **VPC Border** tab as required.

Table 5-14 Protection rule parameters

Parameter	Description
Priority	Priority of the rule. A smaller value indicates a higher priority.
Name/Rule ID	Custom rule name and ID
Rule Type	Protection type of the rule. It can be an EIP or NAT rule.
Direction	Traffic direction of the protection rule.
Source	The party that originates a session.
Destination	The recipient of a session.

Parameter	Description
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**).
Application	Application type in the access traffic.
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.
Schedule Management	Time when the rule takes effect.
Status	Status of the rule. It can be enabled or disabled.
Tags	Tag of a rule.
Created	Time when the current rule is created.
Update Time	Time when the current rule was last edited.
Last Used	Time when the current rule was last used.

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

----End

Editing a 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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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

Copying a 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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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 the new protection rule is **1** (highest priority).

----End

Deleting a Rule

⚠ WARNING

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

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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, enter **DELETE** and click **OK**.

----End

References

- For details about how to add a protection rule, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.
- For details about how to batch add blacklist or whitelist items, see **Adding Blacklist or Whitelist Items to Block or Allow Traffic**.
- Checking protection outcomes:
  - Policy hits: For details about the protection overview, see **Viewing Protection Information Using the Policy Assistant**. For details about logs, see **Access Control Logs**.
  - For details about the traffic trend and statistics, see **Traffic Analysis**. For details about traffic records, see **Traffic Logs**.
- For details about how to batch add protection policies, see **Importing and Exporting Protection Policies**.
- For details about how to adjust rule priority, see **Adjusting the Priority of a Protection Rule**.

5.4.4 Managing the Blacklist and the Whitelist

This section describes how to edit and remove items in a blacklist or whitelist.

Editing the Blacklist or Whitelist

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

Step 5 Click the **Blacklist** or **Whitelist** tab.

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

Modify parameters. For details, see **Adding Blacklist or Whitelist Items to Block or Allow Traffic**.

Step 7 Click **OK**.

----End

Removing a Blacklisted or Whitelisted Item

⚠ WARNING

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

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

Step 5 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 displayed **Remove from Blacklist** or **Remove from Whitelist** dialog box, confirm the information, enter **DELETE**, and click **OK**.

----End

5.4.5 Managing Schedules

You can configure schedules to make rules take effect only within the specified time range.

This section describes how to add, copy, and delete a schedule.

Scenario

- Policy test: Set a validity period for a test policy. During the test, the policy automatically takes effect. After the test is complete, the policy automatically becomes invalid.
- Public network exposure control: Allow services to open ports to external systems only in a necessary period of time (for example, only during office hours), reducing exposure to the public network as well as security risks.
- Temporary access: Configure a policy to temporarily allow public network access. The policy will become invalid as scheduled even if you forget to delete it.

Adding a Schedule

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click the **Schedule Management** tab. Click **Add Schedule** and configure parameters.

Table 5-15 Schedule parameters

Parameter		Description
Schedule Name		Name of a user-defined schedule
Description		(Optional) Usage and application scenario
Periodic Schedule	Add Periodic Schedule	(Optional) time periods in a week. A rule will take effect in the specified periods every week. If the time zone of a resource is different from your local time zone, set **CFW time zone** to the time zone of the region where the resource is located.
Absolute Schedule	Time Settings	Configure **Time Settings** if the time zone of a resource is different from your local time zone. The firewall engine is executed based on the time of **CFW time zone**. ● **Local time zone**: Time zone of the client browser. ● **CFW time zone**: Time zone of the CFW instance. It is the time zone of the current region.
Absolute Schedule	Start Time	Time when a rule takes effect
	End Time	(Optional) time when a rule expires

Step 7 Click **OK**.

----End

Follow-up Operations

To make a schedule take effect, you need to select it in the protection rule. For details, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.

References

- Copying a schedule: In the **Operation** column of a schedule, click **Copy**.
- Editing a schedule: Click the name of a schedule. In the dialog box that is displayed, modify parameters and click **OK**.
- Deleting a schedule: Note that the schedules referenced by protection rules cannot be deleted.
  - To delete a single schedule, locate the row that contains the target schedule and click **Delete** in the **Operation** column. In the dialog box that is displayed, confirm the information, enter **DELETE**, and click **OK**.
  - To delete multiple schedules, select schedules and click **Delete** above the list. In the displayed dialog box, confirm the information, enter **DELETE**, and click **OK**.

5.5 Managing Object Groups

5.5.1 Managing IP Address Groups

Scenario

An IP address group contains multiple IP addresses. You can reference an IP address group in an access rule to implement unified traffic control for that group. The updates of the IP address group will be automatically synchronized to all the policies associated with it. This helps you quickly modify policies and avoid repeated configuration, improving O&M efficiency.

Constraints

- To adding User-defined IP addresses and address groups:
  - A firewall instance can have up to 3,800 IP address groups.
  - An IP address group can contain up to 640 IP addresses. A maximum of 100 IP addresses can be added to an IP address group at a time.
  - A firewall instance can contain up to 30,000 IP addresses.
- You can only view predefined address groups, but cannot add IP addresses to it, or modify or delete it.
- The address group referenced by a protection rule cannot be deleted. Modify or delete the rule first.

Adding User-defined Address Groups

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click **Add IP Address Group** on the **IP Address Groups** tab page. In the displayed **Add IP Address Group** dialog box, configure parameters, as shown in Table 5-16.

Table 5-16 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 rules are as follows: ● A single IP address, for example, **192.168.10.5** ● Address segment, for example, **192.168.2.0/24** ● Consecutive IP addresses, for 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.

After adding an IP address group for the first time, you need to add IP addresses to it. For details, see **Adding an IP Address to a User-defined Address Group**.

----End

Adding an IP Address to a User-defined Address Group

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

Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click the name of an IP address group on the **IP Address Groups** tab. The **IP Address Group Details** dialog box is displayed.

Step 7 Click **Add IP Address**. The **Add IP Address** slide-out panel is displayed.

- 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, for example, **192.168.10.5**

  – Address segment, for example, **192.168.2.0/24**

  – Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10**

  – Multiple IP addresses. Separate them using commas (,), semicolons (;), tab characters, or spaces, or put each value on a separate line.

- To add a single IP address, click **Add**, and enter the IP address and description.

Step 8 Confirm the information and click **OK**.

----End

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 configure policies to allow access from both the address groups.

- **NAT64 Address Set**: provides the IP addresses that have been converted. 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.

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

Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click the **IP Address Groups** tab. Click the **Pre-defined Address Groups** tab and click the name of an address group. On the details page that is displayed, view the address group information.

----End

Deleting User-defined IP Address Groups

⚠ **WARNING**

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

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

Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click the **IP Address Groups** tab. In the **Operation** column of an IP address group, click **Delete**.

Step 7 In the displayed dialog box, confirm the information, enter **DELETE**, and click **OK**.

----End

Related Operations

- Exporting IP address groups: Click **Export** above the list and select a data range.
- Batch deleting IP addresses: In the **IP Address Group Details** slide-out panel, select IP addresses and click **Delete** above the list.

5.5.2 Managing Domain Name Groups

Scenario

A domain name group is a collection of domain names or wildcard domain names. (The standard format of a wildcard domain name is ***.***_Domain_name_, where ***** is a wildcard character that matches any or string, for example, ***.example.com**.) You can reference a domain name group in an access rule to implement unified traffic control for that group. The updates of the domain name group will be automatically synchronized to all the policies associated with it. This helps you quickly modify policies and avoid repeated configuration, improving O&M efficiency.

Domain Name Group Types

CFW provides two types of domain name groups: application domain name groups (layer 7 protocol parsing) and network domain name groups (layer 4 protocol parsing). **Table 5-17** describes the differences between them.

Table 5-17 Domain name group types

-	Application Domain Name Group (Layer 7 Protocol Parsing)	Network Domain Name Group (Layer 4 Protocol Parsing)
Protected object	● Domain names ● Wildcard domain names	● A single domain name ● Multiple domain names
Protocol Type	Application layer protocols, including HTTP, HTTPS, TLS, SMTPS, and POPS.	Network layer protocols. All protocol types are supported.
Match rule	The match is based on domain name. The service compares the HOST field in sessions with the application domain names. If they are consistent, the corresponding protection rule is hit.	The filtering is based on the resolved IP addresses. The service 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.
Suggestion	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

- For adding a domain name group:
  - Domain names in Chinese cannot be added to domain name groups.
- The constraints on the two types of domain name groups are as follows:
  - Application domain name group (layer 7 protocol parsing)
    - A firewall instance can have up to 500 domain name groups.

    - A firewall instance can have up to 2,500 domain names.
    - An application domain name group can contain up to 1500 domain names. Up to 500 domain names can be added at a time.
  - Network domain name group (layer 4 protocol parsing)
    - A firewall instance can have up to 1,000 domain names.
    - A network domain name group can have up to 15 domain names.
    - Each domain name group can resolve up to 1,500 IP addresses.
    - Each domain name can resolve up to 1,000 IP addresses.
- The domain name group referenced by a protection rule cannot be deleted. Modify or delete the rule first.

Adding a Domain Name Group

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

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

Step 7 Click the **Domain Name Groups** tab. Click **Add Domain Name Group** and configure parameters as described in Table 5-18.

Table 5-18 Domain name group parameters

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

Parameter	Description
Domain Name	Enter domain names and click **Parse** to add them to the domain name list. The rules are as follows: ● You can enter a multi-level 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. ● Domain names must be unique.

Step 8 Confirm the information and click **OK**.

After adding a domain name group for the first time, you need to add domain names to it. For details, see **Adding a Domain Name to a Domain Name Group**.

----End

Adding a Domain Name to a Domain Name Group

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

Step 2 Click in the upper left corner of the management console. Select a region.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

Step 5 Click the **Domain Name Groups** tab. Click the name of a domain name group. The **Domain Name Groups** dialog box is displayed.

Step 6 Click **Add Domain** and enter domain name information.

You can click **Add** to add multiple domain names.

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

----End

Deleting a Domain Name Group

⚠ WARNING

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

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

Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

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

Step 7 Click the **Domain Name Groups** tab. 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**.

----End

Related Operations

- Exporting domain name groups: Click **Export** above the list and select a data range.
- Batch deleting domain names: Select domain names in the domain name list and click **Delete** above the list.
- Editing a domain name group: Click the name of a domain name group and modify parameters.
- A domain name group takes effect only after it is set in a protection rule. For more information, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.
- Viewing the IP addresses resolved by a domain name group of the network domain name group type: Click a domain name group name to go to the **Basic Information** page, and click **IP address** in the **Operation** column of the domain name list.

5.5.3 Managing Service Groups

Scenario

A service group is a collection of services (protocols, source ports, and destination ports). You can reference a service group in an access rule to implement unified traffic control for that group. The updates of the service group will be automatically synchronized to all the policies associated with it. This helps you quickly modify policies and avoid repeated configuration, improving O&M efficiency.

Constraints

- For adding a user-defined service group and services:
  - 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.

- You can only view predefined service groups, but cannot add services to it, or modify or delete it.
- The service group referenced by a protection rule cannot be deleted. Modify or delete the rule first.

Adding a User-defined 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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click the **Service Groups** tab. Click **Add Service Group** and configure parameters in the **Add Service Group** area. Enter the service group name and description.

Table 5-19 Service group parameters

Parameter	Description
Service Group Name	Name of a service group
Description	Usage and application scenario
Services	● **Protocol**: Select a protocol from 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**.

After adding a service group for the first time, you need to add services to it. For details, see **Adding a Service to a User-defined Service Group**.

A service group takes effect only after it is set in a protection rule. For more information, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.

----End

Adding a Service to a User-defined 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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click the **Service Groups** tab. Click the name of a service group. The **Service Group Details** dialog box is displayed.

Step 7 Click **Add Service**.

Table 5-20 Adding a service

Parameter	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**). If **Protocol** is set to **ICMP**, you do not need to specify any port number.	80
Destination Port	Destination ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: **80-443**). If **Protocol** is set to **ICMP**, you do not need to specify any port number.	80
Description	Usage and application scenario	-

Step 8 You can click **Add** to add multiple services.

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

----End

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.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click the **Service Groups** tab. 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

Deleting a User-defined Service Group

⚠ WARNING

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

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click the **Service Groups** tab. In the **Operation** column of a service group, click **Delete**.

Step 7 In the displayed dialog box, confirm the information, enter **DELETE**, and click **OK**.

----End

Related Operations

- Exporting service groups: Click **Export** above the list and select a data range.
- Deleting services in batches: On the **Service Groups** tab, select services and click **Delete** above the list.

6 Attack Defense

6.1 Attack Defense Overview

CFW can defend against network attacks and virus files. You are advised to set **Protection Mode** to **Intercept** in a timely manner.

Prerequisites

At least one type of traffic protection has been enabled.

- For details about how to enable EIP traffic protection, see **Enabling Internet Border Traffic Protection**.
- For details about how to enable VPC traffic protection, see **Enabling VPC Border Traffic Protection**.
- For details about how to enable traffic protection for private IP addresses, see **Enabling NAT Gateway Traffic Protection**.

Defense Against Network Attacks and Virus Files

CFW provides intrusion prevention (IPS), sensitive directory scan, antivirus, and reverse shell detection to defend against network attacks and virus-infected files. For details, see **Table 6-1**.

Table 6-1 Attack defense

Feature	Check Type	Configuration Guide
IPS	● Scan for threats and vulnerabilities. ● Check whether traffic contains phishing, Trojans, worms, hacker tools, spyware, brute-force 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.	**Adjusting the IPS Protection Mode to Block Network Attacks**
Sensitive directory scan defense	Attacks on the sensitive directories of cloud servers	**Enabling Sensitive Directory Scan Defense**
Reverse shell defense	Network attacks through reverse shells	**Enabling Reverse Shell Defense**
Antivirus	Identify and process virus-infected files through virus feature detection to prevent data damage, permission change, and system breakdown caused by virus-infected files. HTTP, SMTP, POP3, FTP, IMAP4 and SMB protocols can be checked.	**Configuring Virus Defense**

Protection Actions

- **Observe**: No rules are enabled. The firewall records the traffic that matches the current rule in **Attack Event Logs** and does not block the traffic.
- **Intercept**: Rules are enabled. The firewall records the traffic that matches the current rule in **Attack Event Logs** and blocks it.
- **Disable**: Rules are disabled. The firewall does not log or block the traffic that matches the current rule.

References

For details about the protection overview, see **Viewing Attack Defense Information on the Dashboard**. For details about logs, see **Attack Event Logs**.

The following typical attack defense methods are provided:

- **Using CFW to Defend Against Access Control Attacks**
- **Using CFW to Defend Against Hacker Tools**
- **Using CFW to Prevent Suspicious DNS Activities**
- **Using CFW to Defend Against Trojans**
- **Using CFW to Defend Against Vulnerability Exploits**
- **Using CFW to Defend Against Worms**

6.2 Configuring Intrusion Prevention

CFW provides **attack defense** to help you detect common network attacks.

Impacts on Services

If the **Intercept** mode is enabled, the IPS function blocks various threats and malicious traffic. To change the protection mode, you are advised to enable the **Observe** mode and check false alarms for a period of time and then switch to the **Intercept** mode.

Intrusion Prevention System (IPS)

IPS detects and defends against access traffic in real time based on the attack defense experience and rules accumulated over the years, blocking common network attacks and effectively protecting your assets.

IPS provides multiple types of rule libraries:

- Basic protection: A built-in rule library. It covers common network attacks and provides basic protection capabilities for your assets. You can change the protection mode to change the protection status of the rule library. For details, see **Adjusting the IPS Protection Mode to Block Network Attacks**. For details about how to change the protection status of a single rule, see **Modifying the Protection Action of an Intrusion Prevention Rule**.
- 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.

  Updated rules are added to the virtual patch library first. You can determine whether to add the rules to the basic defense library.

  To add defense rules, enable this function to apply virtual patch rules. The protection action can be manually modified.
- Custom IPS signature (supported only by the professional edition): If the built-in rule library cannot meet your requirements, you can customize signature rules. For details, see **Adding a Custom IPS Signature**.

  Signature rules of the HTTP, TCP, UDP, POP3, SMTP and FTP protocols can be added.

Adjusting the IPS Protection Mode to Block Network Attacks

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

Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Select a protection mode. The **Intercept** status of a rule varies depending on the protection mode. For details, see **Default Actions of Rule Groups in Different Protection Modes**. For details about how to modify an IPS rule, see **Modifying the Protection Action of an Intrusion Prevention Rule**.

- **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 a rule blocks normal traffic, you can modify the action of the rule. For details, see **IPS Rule Management**.

----End

Enabling Sensitive Directory Scan Defense

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

Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click **Advanced**. In the **Sensitive Directory Scan Defense** area, click ○ to enable protection.

- **Action**:
  - **Observe**: Detected sensitive directory scanning attacks are only recorded in **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.

    NOTE

    After **Block IP** is configured, CFW continuously blocks IP addresses. If address translation or proxy is involved, evaluate the impact of blocking IP addresses with caution.
- **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.

----End

Enabling Reverse Shell Defense

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

Step 2 Click 📍 in the upper left corner of the management console. Select a region.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click **Advanced**. In the **Reverse Shell Defense** module, click ○ to enable defense.

- **Action**:
  - **Observe**: Detected reverse shell attacks are only recorded in **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.

    NOTE

    After **Block IP** is configured, CFW continuously blocks IP addresses. If address translation or proxy is involved, evaluate the impact of blocking IP addresses with caution.
- **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

Disabling IPS Basic Protection

- If custom IPS rules have been added, IPS basic protection cannot be disabled.
- If IPS basic protection is disabled, the virtual patch, sensitive directory scan prevention, and reverse shell detection prevention functions will be disabled with it.

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 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

Step 4 In the navigation pane, choose **Attack Defense** > **Intrusion Prevention**.

Step 5 Click ● next to **Basic Protection** to disable basic protection.

----End

Follow-up Operations

For details about the protection overview, see **Viewing Attack Defense Information on the Dashboard**. For details about logs, see **Attack Event Logs**.

References

For details about how to handle incorrect IPS blocking, see **What Do I Do If IPS Blocks Normal Services?**

6.3 Configuring Virus Defense

You can enable virus defense to block virus-infected files, and modify defense actions to improve security performance.

Scenario

Viruses are getting complex. Traditional antivirus measures cannot cope with them in a timely manner. Cloud Firewall provides antivirus to detect and handle virus-infected files, so that they will not cause data damage, permission changes, or system breakdown.

Cloud Firewall supports antivirus for HTTP, SMTP, POP3, FTP, IMAP4, and SMB protocols.

Specification Limitations

Antivirus is available only in the professional edition.

Enabling Antivirus to Block Virus-infected Files

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click ○ to enable antivirus.

After antivirus is enabled, **Current Action** is **Disable** by default. For details about how to change the defense action, see **Modifying the Virus Defense Action for Better Protection Effect**.

----End

Modifying the Virus Defense Action for Better Protection Effect

Step 1 Log in to the management console.

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

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

Step 4 In the navigation pane, choose **Attack Defense** > **Antivirus**.

Step 5 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

Follow-up Operations

For details about the protection overview, see **Viewing Attack Defense Information on the Dashboard**. For details about logs, see **Attack Event Logs**.

References

- For details about attack defense, see **Attack Defense Overview**.
- For details about how to block network attacks, see **Configuring Intrusion Prevention**.

6.4 Viewing Attack Defense Information on the Dashboard

On the security dashboard, you can quickly view protection information about attack defense functions (IPS, reverse shell defense, antivirus, and sensitive directory scan defense) and adjust IPS protection mode in a timely manner.

Viewing IPS Protection Information on the Dashboard

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 In the upper part of the page, click the **Internet Borders** 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 specific parameters of the attacks detected or blocked by IPS. For details, see **Table 6-2**. Click a data record to view attack event details. For details, see **Table 8-1**.

Table 6-2 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 Sources**: Source IP addresses and types.
  - **Top Attack Targets**: Destination IP addresses, ports, and applications.

  NOTE

  - If the IP address is normal, click **Add to Whitelist** in the **Operation** column to add it to the whitelist. CFW will directly allow traffic from the IP address.
  - If the IP address is malicious, click **Create Address Group** or **Add to Address Group** to add one or multiple IP addresses to an address group. Then, manually configure the protection rule to block malicious attacks. For details, see **Configuring Protection Rules to Block or Allow Internet Border Traffic**.

----End

References

- For details about logs, see **Attack Event Logs**.
- For details about attack defense capabilities, see **Attack Defense Overview**.
- For details about how to handle incorrect IPS blocking, see **What Do I Do If IPS Blocks Normal Services?**
- For details about how to modify the IPS action, see **Configuring Intrusion Prevention**. For details about how to modify the virus defense action, see **Configuring Virus Defense**.

6.5 IPS Rule Management

6.5.1 Modifying the Protection Action of an Intrusion Prevention Rule

For rules in the basic defense rule library and the virtual patch rule library, you can manually modify their protection actions. After the modification, their actions do not change with the IPS protection mode.

If the rules in the rule library cannot meet your requirements, you can customize IPS signature rules. For details, see **Adding a Custom IPS Signature**.

Constraints

The restrictions on modifying an IPS rule are as follows:

- 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.

Default Actions of Rule Groups in Different Protection Modes

-	Observe Mode	Intercept mode - strict	Intercept mode - medium	Intercept mode - loose
Observe rule group	Observe	Disable	Disable	Disable
Strict rule group	Observe	Intercept	Disable	Disable
Medium rule group	Observe	Intercept	Intercept	Disable
Loose rule group	Observe	Intercept	Intercept	Intercept

NOTE

- **Observe**: No rules are enabled. The firewall records the traffic that matches the current rule in **Attack Event Logs** and does not block the traffic.
- **Intercept**: Rules are enabled. The firewall records the traffic that matches the current rule in **Attack Event Logs** and blocks it.
- **Disable**: Rules are disabled. The firewall does not log or block the traffic that matches the current rule.

Modifying the Action of a Basic 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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click **View Effective Rules** under **Basic Protection**. The **Basic Protection** tab is displayed.

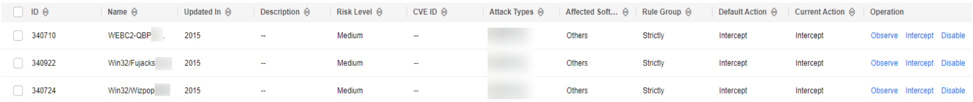
Step 7 (Optional) To view the parameter details of a type of rules, set filter criteria in the input box above the list.

Step 8 Click an action in the **Operation** column.

If no **Operation** column is displayed on the current page, return to the previous page and enable **Basic Protection**.

- **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 6-1 Changing the current action



□	ID	Name	Updated In	Description	Risk Level	CVE ID	Attack Types	Affected Soft...	Rule Group	Default Action	Current Action	Operation
□	340710	WEBC2-QBP[redacted].	2015	--	Medium	--	[redacted]	Others	Strictly	Intercept	Intercept	Observe Intercept Disable
□	340922	Win32/Fujacks[redacted]	2015	--	Medium	--	[redacted]	Others	Strictly	Intercept	Intercept	Observe Intercept Disable
□	340724	Win32/Wizpop[redacted]	2015	--	Medium	--	[redacted]	Others	Strictly	Intercept	Intercept	Observe Intercept Disable

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

References

- Restoring the default actions of some rules: On the **Basic Protection** tab, select rules and click **Restore Default**.
- Restoring the default actions of all rules: On the **Basic Protection** tab, select rules and click **Restore All Defaults**.

- For details about how to set the overall IPS protection action, see **Configuring Intrusion Prevention**.

6.5.2 Adding a Custom IPS Signature

Scenario

Companies need customized intrusion detection solutions to cope with diverse complex attacks. Signature rules that are too general may cause a large number of false positives, reducing defense efficiency. CFW supports refined custom IPS signature rules for HTTP, TCP, UDP, POP3, SMTP, and FTP protocols. It can identify malicious traffic through accurate signature matching.

You can add custom IPS signatures. Be specific when configuring custom signatures. If your rules are too general, they may cause false matching and performance deterioration.

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**.

Adding a Custom IPS Signature

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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 left corner of the list. For more information, see **Table 6-3**.

Table 6-3 Custom IPS signature parameters

Parameter	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**: Any direction. Traffic in any direction that meets other specified conditions matches the current rule. - Server to client - Client to server
Protocol Type	Protocol type of the feature.
Source Type	Source port type. Its value can be: - **Any**: Any port type. All ports match this type. You are advised to select **Any**. - **Include** - **Exclude**
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**: Any port type. All ports match this type. You are advised to select **Any**. - **Include** - **Exclude**

Parameter	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 logged. For details about how to query logs, see **Querying Logs**. ● **Intercept**: Attacks are automatically blocked. 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	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

References

- Managing IPS features:
  - To copy an IPS signature, 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.
- For details about attack defense, see **Attack Defense Overview**.
- For details about how to block network attacks, see **Configuring Intrusion Prevention**.

Follow-up Operations

For details about the protection overview, see **Viewing Attack Defense Information on the Dashboard**. For details about logs, see **Attack Event Logs**.

7 Traffic Analysis

7.1 Viewing Inbound Traffic

The inbound traffic page displays the traffic from the Internet to the cloud EIPs protected by the current firewall instance. The data is collected from sessions. The statistics of a session is reported only after it is terminated.

Prerequisites

EIP protection is enabled and there is already traffic passing through the EIP. For details, see **Enabling Internet Border Traffic Protection**.

Viewing Inbound Traffic

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

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

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

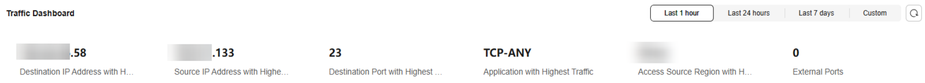
Step 4 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Check statistics on the traffic passing through the firewall within a time range, from 5 minutes to 7 days.

- **Traffic Dashboard**: Information about the highest traffic from the Internet to internal servers.

Figure 7-1 Inbound traffic - traffic dashboard



Traffic Dashboard

[redacted].58
Destination IP Address with H...

[redacted].133
Source IP Address with Highe...

23
Destination Port with Highest ...

TCP-ANY
Application with Highest Traffic

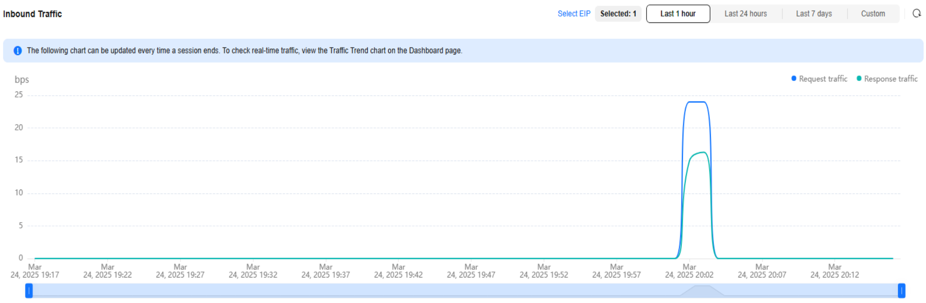
[redacted]
Access Source Region with H...

0
External Ports

- **Inbound Traffic**: Inbound request traffic and response traffic. The traffic statistics of up to 30 EIPs can be queried at a time.

  The data displayed is the average bits per second (bps) of the sessions ended at the specified time in **traffic logs**.

Figure 7-2 Inbound traffic



The following chart can be updated every time a session ends. To check real-time traffic, view the Traffic Trend chart on the Dashboard page.

Table 7-1 Value description

Time Range	Value
Last 1 hour	Average value within every minute
Last 24 hours	Average value within every 5 minutes
Last 7 days	Average value within every hour
Custom	– 5 minutes to 6 hours: average value within every minute – 6 hours (included) to 3 days: average value within every 5 minutes – 3 (included) to 7 days (included): average value within every 30 minutes

- **Visualizations**: View the top 5 items ranked by specific parameters of inbound traffic within a specified period. For more information, see **Table 7-2**. You can click a data record to view the traffic details. A maximum of 50 data records can be viewed.

Figure 7-3 Inbound traffic - visualized statistics

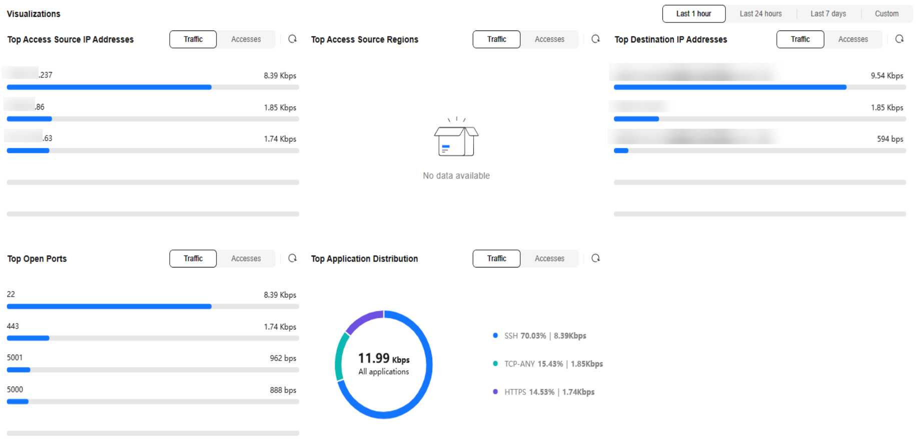
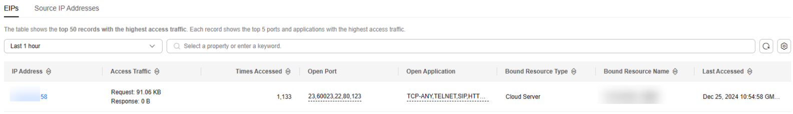


Table 7-2 Inbound traffic parameters

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.
Top Application Distribution	Application information about inbound traffic.

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

    Figure 7-4 EIP analysis

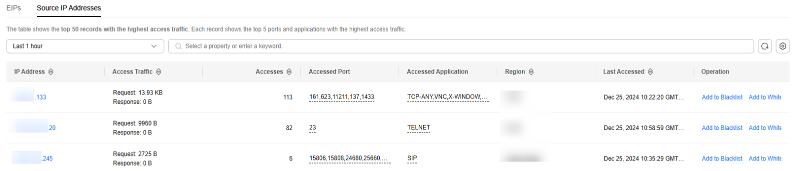
    

    The table shows the **top 50 records with the highest access traffic**. Each record shows the top 5 ports and applications with the highest access traffic.

IP Address	Access Traffic	Times Accessed	Open Port	Open Application	Bound Resource Type	Bound Resource Name	Last Accessed
[redacted]58	Request: 91.06 KB Response: 0 B	1,133	23,60023,22,80,123	TCP-ANY,TELNET,SIP,HTT...	Cloud Server	[redacted]	Dec 25, 2024 10:54:58 GM...

  - **Source IP Addresses**: Traffic information about source IP addresses.

    Figure 7-5 Source IP address analysis

    The table shows the **top 50 records with the highest access traffic**. Each record shows the top 5 ports and applications with the highest access traffic.

IP Address	Access Traffic	Accesses	Accessed Port	Accessed Application	Region	Last Accessed	Operation
[redacted].133	Request: 13.93 KB Response: 0 B	113	161,623,11211,137,1433	TCP-ANY,VNC,X-WINDOW,...	[redacted]	Dec 25, 2024 10:22:20 GMT...	Add to Blacklist Add to White
[redacted].20	Request: 9960 B Response: 0 B	82	23	TELNET	[redacted]	Dec 25, 2024 10:58:59 GMT...	Add to Blacklist Add to White
[redacted].245	Request: 2725 B Response: 0 B	6	15806,15808,24680,25660,...	SIP	[redacted]	Dec 25, 2024 10:35:29 GMT...	Add to Blacklist Add to White

----End

References

- For details about how to view the traffic from the EIP to the Internet, see **Viewing Outbound Traffic**.
- For details about how to check traffic exceptions, see **What Can I Do If Services Cannot Be Accessed After a Policy Is Configured on CFW?**
- For details about what to do if traffic exceeds the protection bandwidth, see **What Do I Do If My Service Traffic Exceeds the Protection Bandwidth?**

7.2 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 is enabled and there is already traffic passing through the EIP. For details, see **Enabling Internet Border Traffic Protection**.

Specification Limitations

To view data of **private network assets initiating Internet connections**, enable the VPC border firewall in the CFW professional edition. For details, see **VPC border firewall**.

Viewing Outbound Traffic

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

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

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

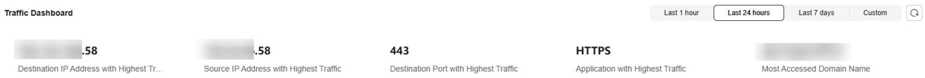
Step 4 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Check statistics on the traffic passing through the firewall within a time range, from 5 minutes to 7 days.

- **Traffic Dashboard**: Information about the highest traffic when internal servers access the Internet.

Figure 7-6 Outbound traffic - traffic dashboard



Traffic Dashboard

Last 1 hour | Last 24 hours | Last 7 days | Custom

[redacted].58
Destination IP Address with Highest Tr...

[redacted].58
Source IP Address with Highest Traffic

443
Destination Port with Highest Traffic

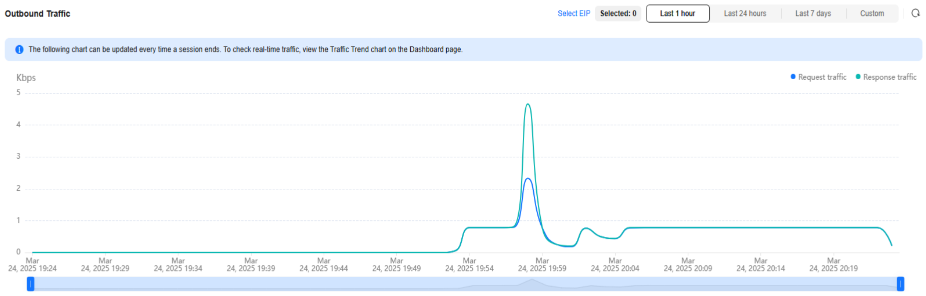
HTTPS
Application with Highest Traffic

[redacted]
Most Accessed Domain Name

- **Outbound Traffic**: Outbound request traffic and response traffic. The traffic statistics of up to 30 EIPs can be queried at a time.

  The data displayed is the average bits per second (bps) of the sessions ended at the specified time in **traffic logs**.

Figure 7-7 Outbound traffic



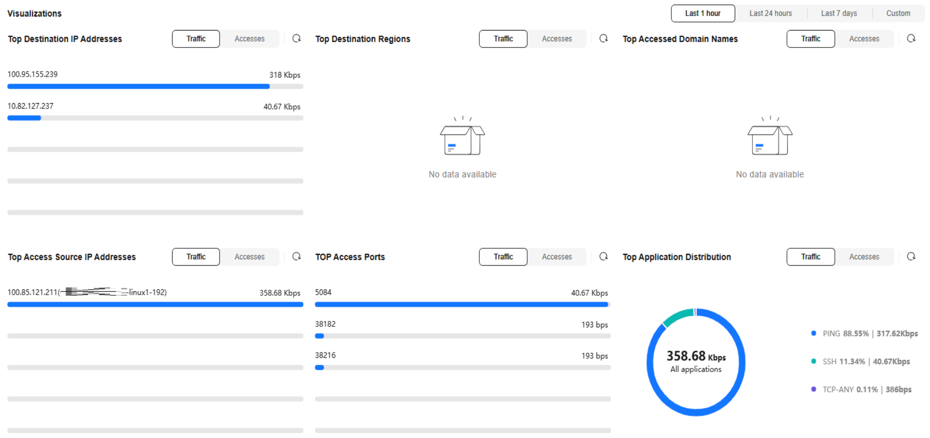
The following chart can be updated every time a session ends. To check real-time traffic, view the Traffic Trend chart on the Dashboard page.

Table 7-3 Value description

Time Range	Value
Last 1 hour	Average value within every minute
Last 24 hours	Average value within every 5 minutes
Last 7 days	Average value within every hour
Custom	– 5 minutes to 6 hours: average value within every minute – 6 hours (included) to 3 days: average value within every 5 minutes – 3 (included) to 7 days (included): average value within every 30 minutes

- **Visualizations**: View the top 5 items ranked by specific parameters of outbound traffic within a specified period. For more information, see **Table 7-4**. You can click a data record to view the traffic details. A maximum of 50 data records can be viewed.

Figure 7-8 Outbound traffic - visualized statistics



Visualizations

Last 1 hour | Last 24 hours | Last 7 days | Custom

Top Destination IP Addresses — Traffic | Accesses

100.95.155.239	318 Kbps
10.82.127.237	40.67 Kbps

Top Destination Regions — Traffic | Accesses

No data available

Top Accessed Domain Names — Traffic | Accesses

No data available

Top Access Source IP Addresses — Traffic | Accesses

100.85.121.211([redacted]-linux1-192)	358.68 Kbps

TOP Access Ports — Traffic | Accesses

5084	40.67 Kbps
38182	193 bps
38216	193 bps

Top Application Distribution — Traffic | Accesses

358.68 Kbps
All applications

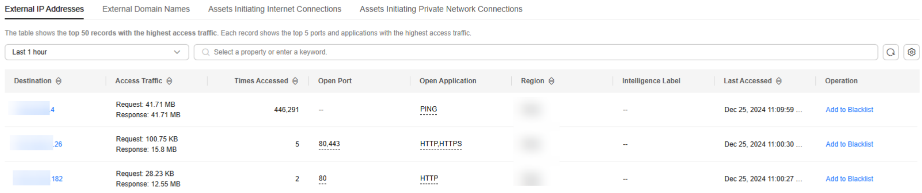
● PING	88.55%	317.62Kbps
● SSH	11.34%	40.67Kbps
● TCP-ANY	0.11%	386bps

Table 7-4 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 Accessed Domain Names	Domain name information about outbound traffic
Top Access Source IP Addresses	Source IP addresses of outbound traffic.
TOP Access Ports	Destination ports of outbound traffic.
Top 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.

Figure 7-9 External IP addresses



External IP Addresses | External Domain Names | Assets Initiating Internet Connections | Assets Initiating Private Network Connections

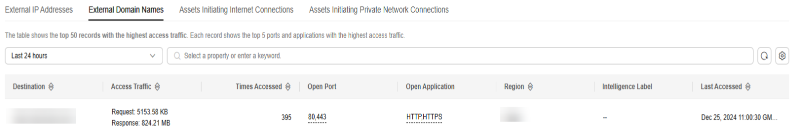
The table shows the **top 50 records with the highest access traffic**. Each record shows the top 5 ports and applications with the highest access traffic.

Last 1 hour | Select a property or enter a keyword.

Destination	Access Traffic	Times Accessed	Open Port	Open Application	Region	Intelligence Label	Last Accessed	Operation
[redacted].4	Request: 41.71 MB Response: 41.71 MB	446,291	--	PING	[redacted]	--	Dec 25, 2024 11:09:59 ...	Add to Blacklist
[redacted].26	Request: 100.75 KB Response: 15.8 MB	5	80,443	HTTP,HTTPS	[redacted]	--	Dec 25, 2024 11:00:30 ...	Add to Blacklist
[redacted].182	Request: 28.23 KB Response: 12.55 MB	2	80	HTTP	[redacted]	--	Dec 25, 2024 11:00:27 ...	Add to Blacklist

  - **External Domain Names**: domain name information

Figure 7-10 External domain names


External IP Addresses
External Domain Names
Assets Initiating Internet Connections
Assets Initiating Private Network Connections

The table shows the **top 50 records with the highest access traffic**. Each record shows the top 5 ports and applications with the highest access traffic.

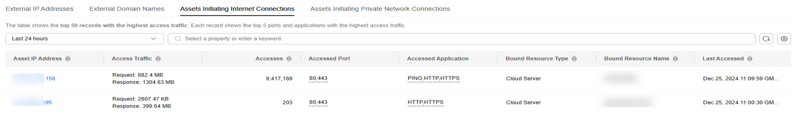
Last 24 hours

Select a property or enter a keyword.

Destination	Access Traffic	Times Accessed	Open Port	Open Application	Region	Intelligence Label	Last Accessed
[redacted]	Request: 5153.58 KB Response: 824.21 MB	395	80,443	HTTP,HTTPS	[redacted]	--	Dec 25, 2024 11:00:30 GM...

- **Assets Initiating Internet Connections**: Traffic information whose source IP addresses are public IP addresses.

Figure 7-11 Assets initiating Internet connections


External IP Addresses
External Domain Names
Assets Initiating Internet Connections
Assets Initiating Private Network Connections

The table shows the **top 50 records with the highest access traffic**. Each record shows the top 5 ports and applications with the highest access traffic.

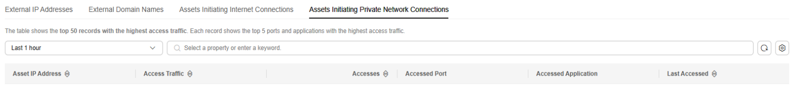
Last 24 hours

Select a property or enter a keyword.

Asset IP Address	Access Traffic	Accesses	Accessed Port	Accessed Application	Bound Resource Type	Bound Resource Name	Last Accessed
[redacted].156	Request: 882.4 MB Response: 1304.63 MB	9,417,169	80,443	PING,HTTP,HTTPS	Cloud Server	[redacted]	Dec 25, 2024 11:09:59 GM...
[redacted]95	Request: 2807.47 KB Response: 399.64 MB	203	80,443	HTTP,HTTPS	Cloud Server	[redacted]	Dec 25, 2024 11:00:30 GM...

- **Assets Initiating Private Network Connections**: Traffic information whose source IP addresses are private IP addresses.

Figure 7-12 Assets initiating private network connections


External IP Addresses
External Domain Names
Assets Initiating Internet Connections
Assets Initiating Private Network Connections

The table shows the **top 50 records with the highest access traffic**. Each record shows the top 5 ports and applications with the highest access traffic.

Last 1 hour

Select a property or enter a keyword.

Asset IP Address	Access Traffic	Accesses	Accessed Port	Accessed Application	Last Accessed

NOTE

Private IP address information is visible only to users who enable the VPC border firewall in the CFW professional edition.

----End

References

- For details about how to view the statistics about the traffic from the Internet to the EIPs on the cloud, see **Viewing Inbound Traffic**.
- For details about how to check traffic exceptions, see **What Can I Do If Services Cannot Be Accessed After a Policy Is Configured on CFW?**
- For details about what to do if traffic exceeds the protection bandwidth, see **What Do I Do If My Service Traffic Exceeds the Protection Bandwidth?**

7.3 Viewing Inter-VPC Traffic

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

Prerequisites

VPC border traffic protection is enabled, and there is already traffic passing through the VPC. For details, see **Enabling VPC Border Traffic Protection**.

Viewing Inter-VPC Traffic

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

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

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

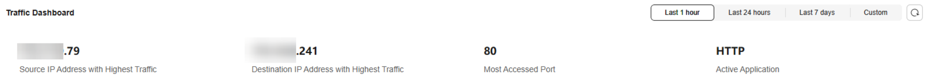
Step 4 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Check the statistics on the traffic passing through CFW within a time range, from 5 minutes to 7 days.

- **Traffic Dashboard**: Information about the maximum traffic between VPCs.

Figure 7-13 Inter-VPC access traffic - traffic dashboard



Traffic Dashboard

[redacted].79
Source IP Address with Highest Traffic

[redacted].241
Destination IP Address with Highest Traffic

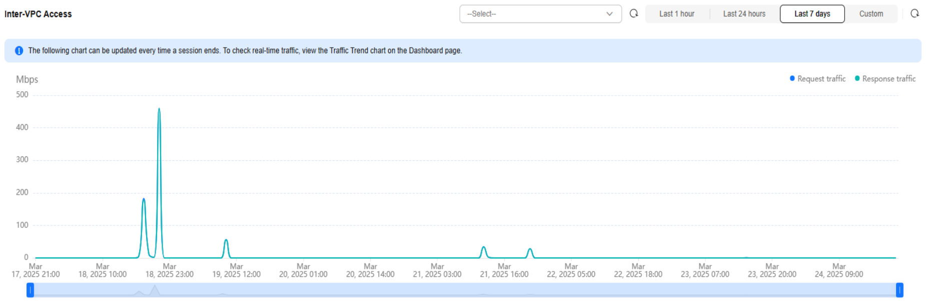
80
Most Accessed Port

HTTP
Active Application

- **Inter-VPC Access**: Request and response traffic between VPCs.

  The data displayed is the average bits per second (bps) of the sessions ended at the specified time in **traffic logs**.

Figure 7-14 Inter-VPC access



Inter-VPC Access

The following chart can be updated every time a session ends. To check real-time traffic, view the Traffic Trend chart on the Dashboard page.

Table 7-5 Value description

Time Range	Value
Last 1 hour	Average value within every minute
Last 24 hours	Average value within every 5 minutes
Last 7 days	Average value within every hour
Custom	– 5 minutes to 6 hours: average value within every minute – 6 hours (included) to 3 days: average value within every 5 minutes – 3 (included) to 7 days (included): average value within every 30 minutes

- **Visualizations**: View the top 5 items ranked by specific parameters of inter-VPC traffic within a specified period. For more information, see **Table 7-6**. You can click a data record to view the traffic details. A maximum of 50 data records can be viewed.

Figure 7-15 Inter-VPC access traffic - visualized statistics

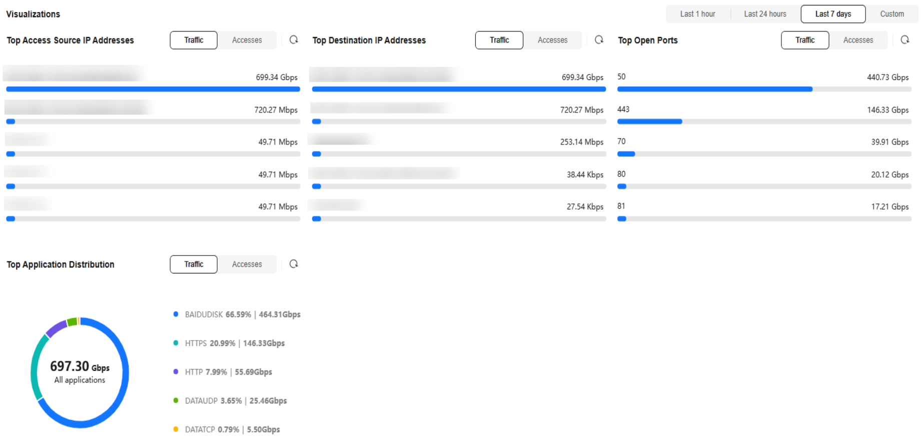
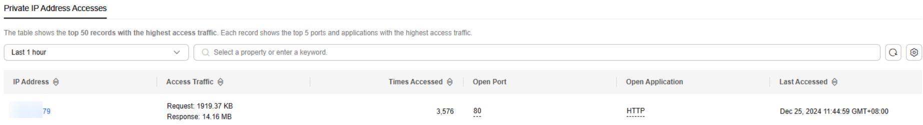


Table 7-6 Inter-VPC traffic parameters

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.

Figure 7-16 Private IP address accesses


Private IP Address Accesses
Last 1 hour
Select a property or enter a keyword.

The table shows the **top 50 records with the highest access traffic**. Each record shows the top 5 ports and applications with the highest access traffic.

IP Address	Access Traffic	Times Accessed	Open Port	Open Application	Last Accessed
[redacted]79	Request: 1919.37 KB Response: 14.16 MB	3,576	80	HTTP	Dec 25, 2024 11:44:59 GMT+08:00

----End

References

- For details about how to check traffic exceptions, see **What Can I Do If Services Cannot Be Accessed After a Policy Is Configured on CFW?**

- For details about what to do if traffic exceeds the protection bandwidth, see **What Do I Do If My Service Traffic Exceeds the Protection Bandwidth?**

8 Log Audit

8.1 Protection Log Overview

This section describes the following content:

- The two log storage modes provided by CFW. For details, see **Log Storage Mode**.
- Supported log types. For details, see **Log Types**.
- How to handle improper blocking recorded in logs. For details, see **Handling Improper Blocking**.
- For details about how to dump logs to LTS, see **Log Management Description**.

Log Storage Mode

Function	Storage Duration	Billing Mode	Access Mode	Log Field Description
Log query	7 days	Free	Automatic access	**Querying Logs**
Log managem ent	1 to 365 days	Separate billing by traffic	You need to manually connect to LTS. For details, see **Configuring Logs**. For details about how to use the LTS log function, see **Log Management Description**.	**Log Field Description**

Log Types

The following types of logs are provided:

- Attack event logs: The events detected by attack defense functions, such as IPS, are recorded.
- Access control logs: All traffic that matches the access control policy are recorded.
- Traffic logs: All traffic passing through the firewall is recorded.

NOTE

SecMaster supports one-click access to CFW log data. There is a delay in log reporting. If you let SecMaster access the logs of a CFW instance that was newly purchased, you can view the CFW logs on SecMaster the next day.

Handling Improper Blocking

- If improper blocking is recorded in access control logs, your normal workloads may be blocked by IPS. In this case, check the policy configuration. For details about how to modify protection rules, see **Managing Protection Rules**. For details about how to modify the blacklist and whitelist, see **Editing the Blacklist or Whitelist**.
- If improper blocking is recorded in attack event logs, your normal workloads may be blocked by IPS.
  - If the traffic from an IP address is improperly blocked, add it to the whitelist.
  - If the traffic from multiple IP addresses is blocked, check logs to see whether it is blocked by a single rule or multiple rules.
    - Blocked by a single rule: Modify the protection action of the rule. For details, see **Modifying the Action of a Basic Protection Rule**.
    - Blocked by multiple rules: Modify the protection mode. For details, see **Adjusting the IPS Protection Mode to Block Network Attacks**.

Log Management Description

Function	Description	Configuration Method
Configuring logs	Interconnect logs with LTS and create a log group and a log stream.	**Configuring Logs**
Modifying log storage duration	(Optional) By default, logs are stored for seven days. You can set the storage duration in the range 1 to 365 days.	**Changing the Log Storage Duration**
Log search and analysis	(Optional) Use proper log collection functions, efficient search methods, and professional analysis tools to implement comprehensive monitoring and refined management of your system and applications.	For details, see **Log Search and Analysis**.

Function	Description	Configuration Method
Log visualization	(Optional) Visualize log data in tables and charts.	See **Log Visualization**.
Configuring alarm rules	(Optional) Monitor keywords in logs. Collect statistics on the occurrences of keywords in logs within a specified period to monitor the service running status in real time.	For details, see **Log Alarms**.
Viewing log fields	Learn the meaning of fields in a log.	**Log Field Description**

References

- For details about the protection overview of access control policies, see **Viewing Protection Information Using the Policy Assistant**.
- For details about the traffic defense overview and trend, see **Traffic Analysis**.
- For details about the overall network attack defense, see **Viewing Attack Defense Information on the Dashboard**.

8.2 Querying Logs

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

- Attack event logs: The events detected by attack defense functions, such as IPS, are recorded.
- Access control logs: All traffic that matches the access control policy are recorded.
- Traffic logs: All traffic passing through the firewall is recorded.

One or multiple types of logs can be recorded in LTS. You can view log data in the past 1 to 365 days. For details, see **Log Management**.

Constraints

- Logs can be stored for up to seven days.
- For each type of logs, up to 10,000 records can be viewed, and up to 100,000 records can be exported.
- Traffic logs are collected based on sessions. Data about a connection is not reported until connection is terminated.
- On the log query page, the geographical locations (source countries/regions) of IPv6 addresses cannot be displayed.

Checking Logs

Perform the following operations to view logs.

Attack Event Logs

Step 1 Log in to the management console.

Step 2 Click ⚲ in the upper left corner of the management console. Select a region.

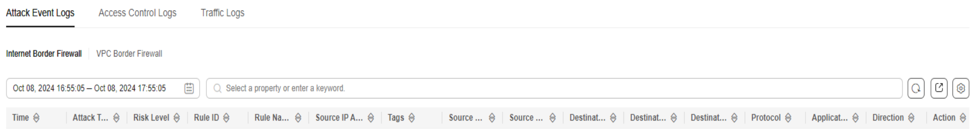
Step 3 In the navigation pane on the left, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

Step 4 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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.

(Optional) Quickly filter log data. You can select what to include (default) or exclude (select **Exclude**) in the search criteria.

Figure 8-1 Attack event logs



Oct 08, 2024 16:55:05 – Oct 08, 2024 17:55:05

Time	Attack T...	Risk Level	Rule ID	Rule Na...	Source IP A...	Tags	Source ...	Source ...	Destinat...	Destinat...	Destinat...	Protocol	Applicat...	Direction	Action

Table 8-1 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.
Risk Level	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. If the source IP address is a WAF back-to-source IP address, **Source IP Address** displays the WAF back-to-source IP address and the real IP address. The first IP address corresponding to X-Forwarded-For is displayed in **RealIP**, that is, the real IP address of the client.

Parameter	Description
Tags	IP address type identifier. - Other tags: IP addresses that are not WAF back-to-source IP addresses. No special actions required. - **WAF back-to-source IP addresses**: **Source IP Address** is a WAF back-to-source IP address. If the **Action** of this record is **Block**, **Block IP**, or **Discard**, you need to manually set the action to **Allow**. Operation: Find the rule based on its ID. In the **Operation** column of the rule, click **Observe**.
Source Country/ Region	Geographical location of the attack source IP address.
Source Port	Source port of an attack.
Destination IP Address	Attacked IP address.
Destination Country/ Region	Geographical location of the attack target IP address.
Destination Port	Destination port of an attack.
Protocol	Protocol type of an attack.
Application	Application type of an attack.
Direction	It can be outbound or inbound.
Action	Action of the firewall. It can be: - **Allow** - **Block** - **Block IP** - **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. Select a region.

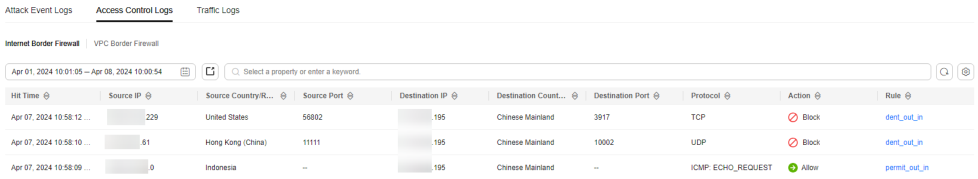
Step 3 In the navigation pane on the left, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

Step 4 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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 action taken on an IP address, see **Configuring Protection Rules to Block or Allow Internet Border Traffic** or **Adding Blacklist or Whitelist Items to Block or Allow Traffic**.

(Optional) Quickly filter log data. You can select what to include (default) or exclude (select **Exclude**) in the search criteria.

Figure 8-2 Access control logs



Hit Time	Source IP	Source Country/R...	Source Port	Destination IP	Destination Count...	Destination Port	Protocol	Action	Rule
Apr 07, 2024 10:58:12 ...	[redacted]229	United States	56802	[redacted].195	Chinese Mainland	3917	TCP	Block	dent_out_in
Apr 07, 2024 10:58:10 ...	[redacted].61	Hong Kong (China)	11111	[redacted].195	Chinese Mainland	10002	UDP	Block	dent_out_in
Apr 07, 2024 10:58:09 ...	[redacted].0	Indonesia	--	[redacted].195	Chinese Mainland	--	ICMP: ECHO_REQUEST	Allow	permit_out_in

Table 8-2 Access control log parameters

Parameter	Description
Hit Time	Time of an access.
Source IP Address	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**).
Destination IP Address	Destination IP address.
Destination Host	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. Select a region.

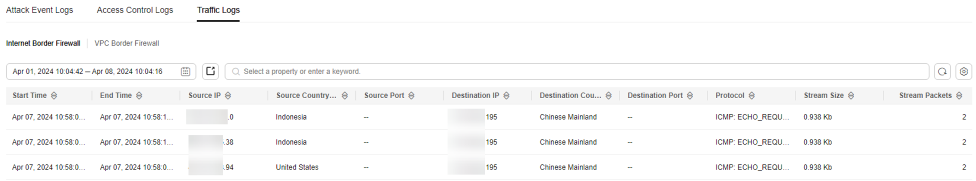
Step 3 In the navigation pane on the left, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

Step 4 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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.

(Optional) Quickly filter log data. You can select what to include (default) or exclude (select **Exclude**) in the search criteria.

Figure 8-3 Traffic logs



Start Time	End Time	Source IP	Source Country...	Source Port	Destination IP	Destination Cou...	Destination Port	Protocol	Stream Size	Stream Packets
Apr 07, 2024 10:58:0...	Apr 07, 2024 10:58:1...	[redacted].0	Indonesia	--	[redacted]195	Chinese Mainland	--	ICMP: ECHO_REQU...	0.938 Kb	2
Apr 07, 2024 10:58:0...	Apr 07, 2024 10:58:1...	[redacted].38	Indonesia	--	[redacted]195	Chinese Mainland	--	ICMP: ECHO_REQU...	0.938 Kb	2
Apr 07, 2024 10:58:0...	Apr 07, 2024 10:58:0...	[redacted].94	United States	--	[redacted]195	Chinese Mainland	--	ICMP: ECHO_REQU...	0.938 Kb	2

Table 8-3 Traffic log parameters

Parameter	Description
Start Time	Time when traffic protection started.
End Time	Time when traffic protection ended.
Source IP Address	Source IP address of the traffic
Source Country/ Region	Geographical location of the source IP address.
Source Port	Source port of the traffic.
Destination IP Address	Destination IP address.
Destination Country/ Region	Geographical location of the destination IP address.
Destination Port	Destination port of the traffic.
Protocol	Protocol type of the traffic.

Parameter	Description
Stream Size	Total number of bytes of protected traffic.
Stream Packets	Total number of protected packets.

----End

References

- Exporting logs: Click ⧉ in the upper right corner to export the logs in the list.
- CFW provides the network packet capture function. You can capture traffic by IP address, port number, or protocol type to quickly locate network faults and identify security risks. For details, see **Network Packet Capture**.

Follow-up Operations

- If improper blocking is recorded in access control logs, your normal workloads may be blocked by IPS. In this case, check the policy configuration. For details about how to modify protection rules, see **Managing Protection Rules**. For details about how to modify the blacklist and whitelist, see **Editing the Blacklist or Whitelist**.
- If improper blocking is recorded in attack event logs, your normal workloads may be blocked by IPS.
  - If the traffic from an IP address is improperly blocked, add it to the whitelist.
  - If the traffic from multiple IP addresses is blocked, check logs to see whether it is blocked by a single rule or multiple rules.
    - Blocked by a single rule: Modify the protection action of the rule. For details, see **Modifying the Action of a Basic Protection Rule**.
    - Blocked by multiple rules: Modify the protection mode. For details, see **Adjusting the IPS Protection Mode to Block Network Attacks**.

8.3 Log Management

8.3.1 Configuring Logs

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.

⚠ **CAUTION**

- On the **Log Query** page, you can check and export log data of the last seven days. For details, see **Querying Logs**.
- LTS is billed by traffic and is billed separately from CFW. For details about LTS pricing, see **LTS Pricing**.

Configuring 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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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**.

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. Select a log group, enable and select log streams, and click **OK**.

- 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.
- After the configuration is complete, if a message indicating insufficient permissions is displayed, grant the **LTS FullAccess** permission.

----End

8.3.2 Changing the Log Storage Duration

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

Changing the Log Storage Duration

Step 1 Dump logs to LTS. For details, see **Configuring Logs**.

Step 2 **Log in to the management console**.

Step 3 Click 📍 in the upper left corner of the management console and select a region or project.

Step 4 In the navigation pane on the left, click ☰ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

Step 5 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

Step 6 In the navigation pane on the left, choose **Log Audit** > **Log Management**. On the displayed page, click **Modify Log Storage Duration**.

- Logs can be stored for 1 to 365 days. Logs that exceed the specified storage duration are automatically deleted.
- A long storage duration means much storage space will be occupied. For details about how to transfer logs to other cloud services for long-term storage, see **Log Transfer**.
- If a message indicating insufficient permissions is displayed, grant the **LTS FullAccess** permission.

----End

8.3.3 Log Field Description

This section describes the log fields interconnected with LTS.

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** ● **MEDIUM** ● **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

9 System Management

9.1 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.

⚠ CAUTION

- 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**.

Setting Alarm Notifications

Perform the following operations to set alarm notifications:

Attack Alarm

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

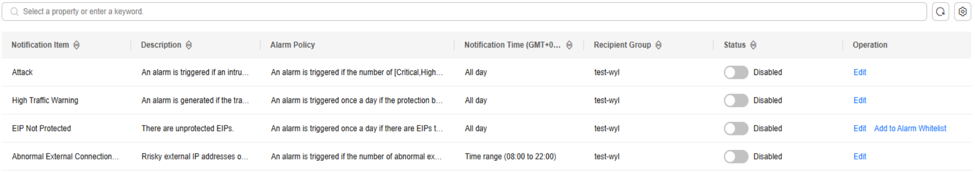
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Figure 9-1 Alarm notifications



Select a property or enter a keyword.

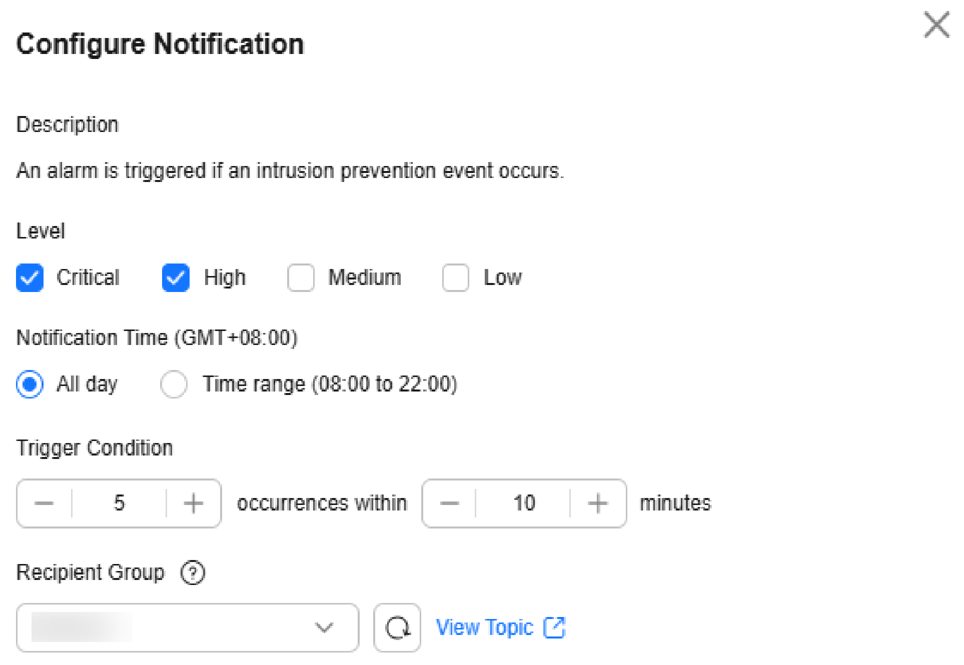
Notification Item	Description	Alarm Policy	Notification Time (GMT+0...	Recipient Group	Status	Operation
Attack	An alarm is triggered if an intru...	An alarm is triggered if the number of [Critical,High...	All day	test-wyl	Disabled	Edit
High Traffic Warning	An alarm is generated if the tra...	An alarm is triggered once a day if the protection b...	All day	test-wyl	Disabled	Edit
EIP Not Protected	There are unprotected EIPs.	An alarm is triggered once a day if there are EIPs t...	All day	test-wyl	Disabled	Edit Add to Alarm Whitelist
Abnormal External Connection...	Rrisky external IP addresses o...	An alarm is triggered if the number of abnormal ex...	Time range (08:00 to 22:00)	test-wyl	Disabled	Edit

Step 6 In the **Operation** column of **Attack alarm**, click **Edit**, and configure notification item parameters. For details, see **Table 9-1**.

NOTE

The notification settings take effect immediately after being modified.

Figure 9-2 Notification item settings - attack alarm



Configure Notification

Description

An alarm is triggered if an intrusion prevention event occurs.

Level

☑ Critical ☑ High □ Medium □ Low

Notification Time (GMT+08:00)

● All day ○ Time range (08:00 to 22:00)

Trigger Condition

5 occurrences within 10 minutes

Recipient Group

[redacted]

Table 9-1 Attack alarm parameters

Parameter	Description
Description	IPS attack alarm

Parameter	Description
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. CFW sends notifications only within the alarm notification period. If an exception is detected outside this period, no notifications will be sent.
Trigger Condition	Configure the trigger condition. Alarm notifications are sent if the number of attacks 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.

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**.

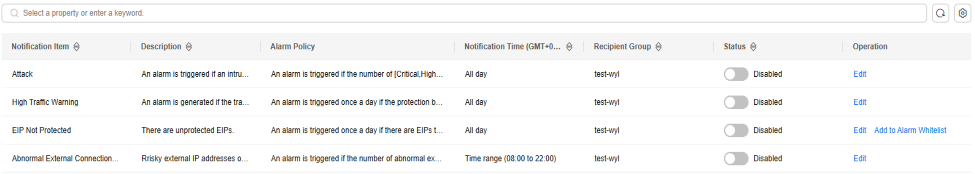
Step 2 Click 📍 in the upper left corner of the management console and select a region or project.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Figure 9-3 Alarm notifications



Select a property or enter a keyword.

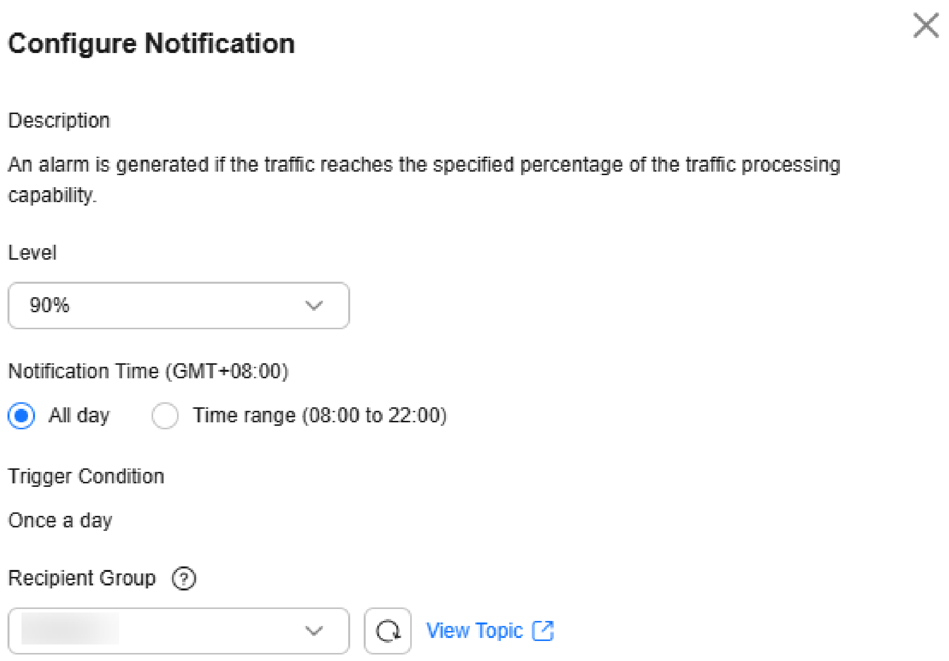
Notification Item	Description	Alarm Policy	Notification Time (GMT+0...	Recipient Group	Status	Operation
Attack	An alarm is triggered if an intru...	An alarm is triggered if the number of [Critical,High...	All day	test-wyl	Disabled	Edit
High Traffic Warning	An alarm is generated if the tra...	An alarm is triggered once a day if the protection b...	All day	test-wyl	Disabled	Edit
EIP Not Protected	There are unprotected EIPs.	An alarm is triggered once a day if there are EIPs t...	All day	test-wyl	Disabled	Edit Add to Alarm Whitelist
Abnormal External Connection...	Rrisky external IP addresses o...	An alarm is triggered if the number of abnormal ex...	Time range (08:00 to 22:00)	test-wyl	Disabled	Edit

Step 6 In the **Operation** column of **High Traffic Warning**, click **Edit**, and configure notification item parameters. For details, see **Table 9-2**.

NOTE

The notification settings take effect immediately after being modified.

Figure 9-4 Notification item settings - high traffic warning



Configure Notification

Description

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

Level

90%

Notification Time (GMT+08:00)

● All day ○ Time range (08:00 to 22:00)

Trigger Condition

Once a day

Recipient Group

[redacted]

Table 9-2 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.

Parameter	Description
Notification Time	Select a time range for sending notifications. CFW sends notifications only within the alarm notification period. If an exception is detected outside this period, no notifications will be sent.
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**.

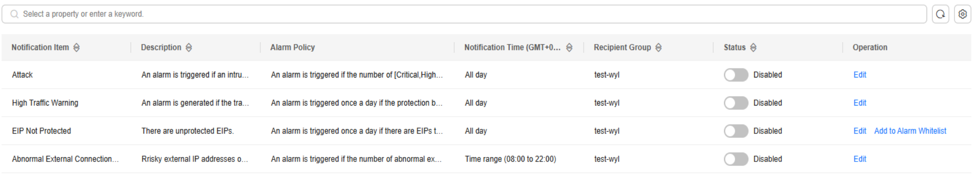
Step 2 Click in the upper left corner of the management console and select a region or project.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Figure 9-5 Alarm notifications



Select a property or enter a keyword.

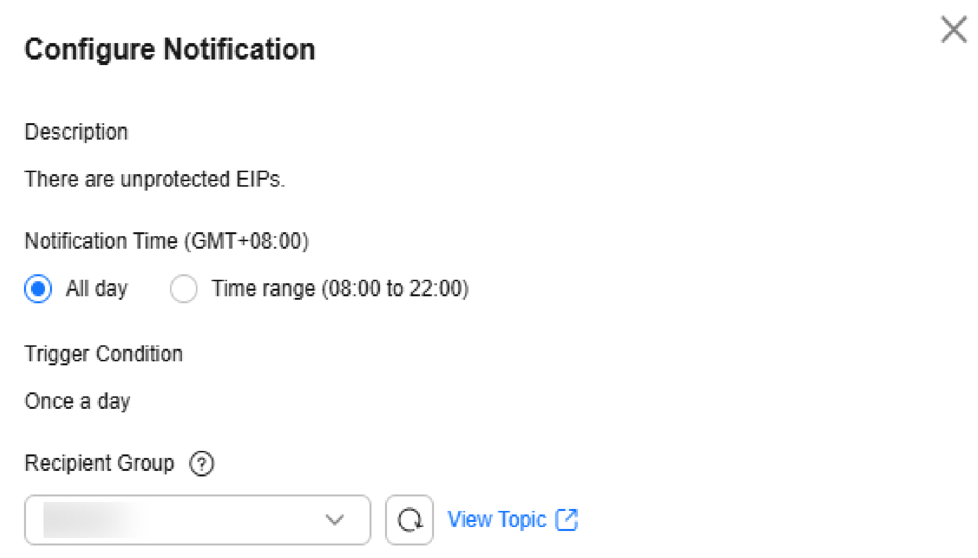
Notification Item	Description	Alarm Policy	Notification Time (GMT+0...	Recipient Group	Status	Operation
Attack	An alarm is triggered if an intru...	An alarm is triggered if the number of [Critical,High...	All day	test-wyl	Disabled	Edit
High Traffic Warning	An alarm is generated if the tra...	An alarm is triggered once a day if the protection b...	All day	test-wyl	Disabled	Edit
EIP Not Protected	There are unprotected EIPs.	An alarm is triggered once a day if there are EIPs t...	All day	test-wyl	Disabled	Edit Add to Alarm Whitelist
Abnormal External Connection...	Rrisky external IP addresses o...	An alarm is triggered if the number of abnormal ex...	Time range (08:00 to 22:00)	test-wyl	Disabled	Edit

Step 6 In the **Operation** column of the **EIP Not Protected** alarm, click **Edit**, and configure notification item parameters. For details, see **Table 9-3**.

NOTE

The notification settings take effect immediately after being modified.

Figure 9-6 Notification settings - EIP Not Protected



Configure Notification

Description

There are unprotected EIPs.

Notification Time (GMT+08:00)

● All day ○ Time range (08:00 to 22:00)

Trigger Condition

Once a day

Recipient Group

[redacted]

Table 9-3 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. CFW sends notifications only within the alarm notification period. If an exception is detected outside this period, no notifications will be sent.
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 **EIP Not Protected**, click ○ to enable it.

----End

Abnormal External Connection Alarm

Step 1 Log in to the management console.

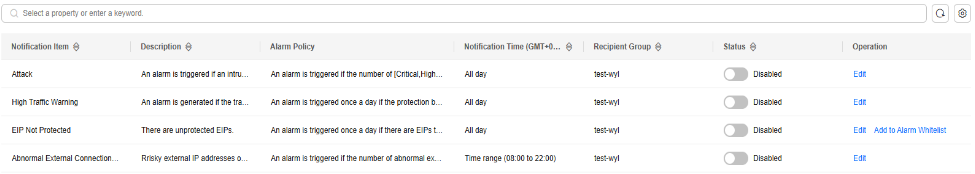
Step 2 Click in the upper left corner of the management console and select a region or project.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Figure 9-7 Alarm notifications



Select a property or enter a keyword.

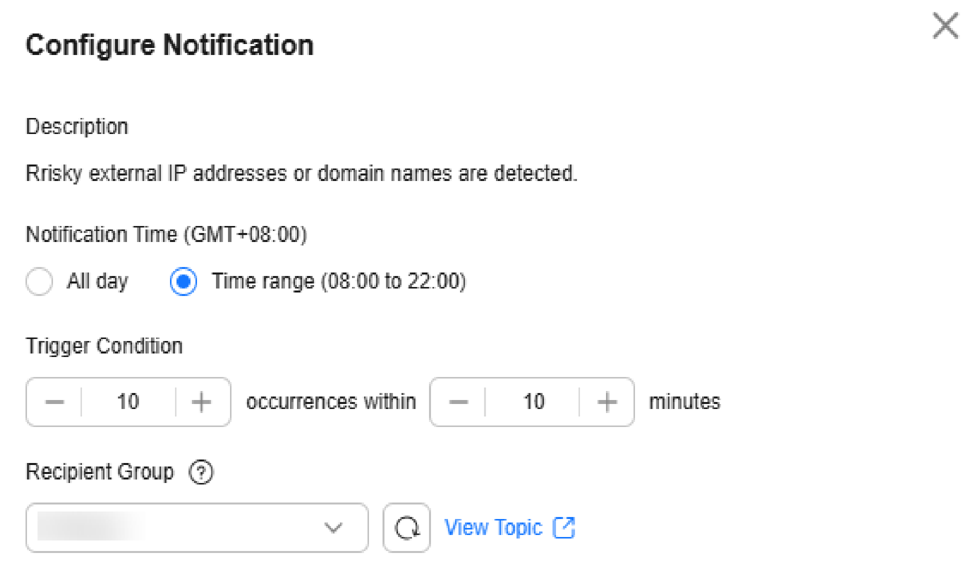
Notification Item	Description	Alarm Policy	Notification Time (GMT+0...	Recipient Group	Status	Operation
Attack	An alarm is triggered if an intru...	An alarm is triggered if the number of [Critical,High...	All day	test-wyl	Disabled	Edit
High Traffic Warning	An alarm is generated if the tra...	An alarm is triggered once a day if the protection b...	All day	test-wyl	Disabled	Edit
EIP Not Protected	There are unprotected EIPs.	An alarm is triggered once a day if there are EIPs t...	All day	test-wyl	Disabled	Edit Add to Alarm Whitelist
Abnormal External Connection...	Rrisky external IP addresses o...	An alarm is triggered if the number of abnormal ex...	Time range (08:00 to 22:00)	test-wyl	Disabled	Edit

Step 6 In the **Operation** column of the **Abnormal External Connection Alarm** alarm, click **Edit**, and configure notification item parameters. For details, see **Table 9-4**.

NOTE

The notification settings take effect immediately after being modified.

Figure 9-8 Notification item settings - abnormal external connection alarm



Configure Notification

Description

Rrisky external IP addresses or domain names are detected.

Notification Time (GMT+08:00)

○ All day ● Time range (08:00 to 22:00)

Trigger Condition

10 occurrences within 10 minutes

Recipient Group

[redacted]

Table 9-4 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. CFW sends notifications only within the alarm notification period. If an exception is detected outside this period, no notifications will be sent.
Trigger Condition	Configure the trigger condition. 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

References

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.

9.2 Network Packet Capture

Scenario

Data is transmitted between devices as packets, a process that is usually invisible. Data flows cannot be quickly checked, making it difficult locate problems and handle network delay, connection failures, or security threats. CFW provides a network packet capture tool to accurately filter traffic by source/destination IP address, port, and protocol. It helps you quickly obtain the original data packet content, detect attacks, and identify security risks.

This section describes how to create a packet capture task to check the network status, view packet capture tasks, and download their results.

Constraints

- Only the professional edition instances can capture network packets.
- You can create up to of 20 packet capture tasks every day, but only one can be executed at a time.
- A maximum of 1 million packets can be captured.
- 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.

Creating a Packet Capture Task to Check the Network Status

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Click **Create Capture Task** and configure parameters. For details, see **Table 9-5**.

Table 9-5 Packet capture task parameters

Parameter	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.	100,000

Parameter	Description	Example Value
Capture Duration (min)	Maximum duration for capturing packets. Enter an integer in the range 1 to 10.	3
IP Type	IP address type for packet capture. The value is **IPv4** by default.	IPv4
Protocol Type	Protocol type of captured packets. It can be: ● Any ● TCP ● UDP ● ICMP	Any
Source Address	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 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
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

Viewing a Packet Capture Task

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 (Optional) Choose whether to search for a task by task name or IP address, enter keywords, and click 🔍.

- 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 View the information about the packet capture task. For details, see **Table 9-6**.

Table 9-6 Packet capture task parameters

Parameter	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.

Parameter	Description
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

Downloading Packet Capture Results

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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.

Step 7 Share or download the packet capture result. Set the **download range of the packet capture results** as required.

NOTE

The sharing link is valid within 30 minutes after it is generated. Please use it in a timely manner or generate a new one after it is invalid.

- **Unlimited**: Any person can download the packet capture file through the link.
  - Share the packet capture result: Click **Copy all** in the lower right corner and share the information with others.
  - Download the packet capture result: Click **Open URL** in the lower right corner to go to the browser, click **Copy** next to **Access Code**, paste the code to **Extraction Code**, and click **Obtain Shared File List**.

- **Specified EIP**: Set the CIDR blocks where users are allowed to download the packet capture results through the generated link.

  After setting the CIDR blocks, click **Generate Link**. All packet capture result files are displayed in the list below.

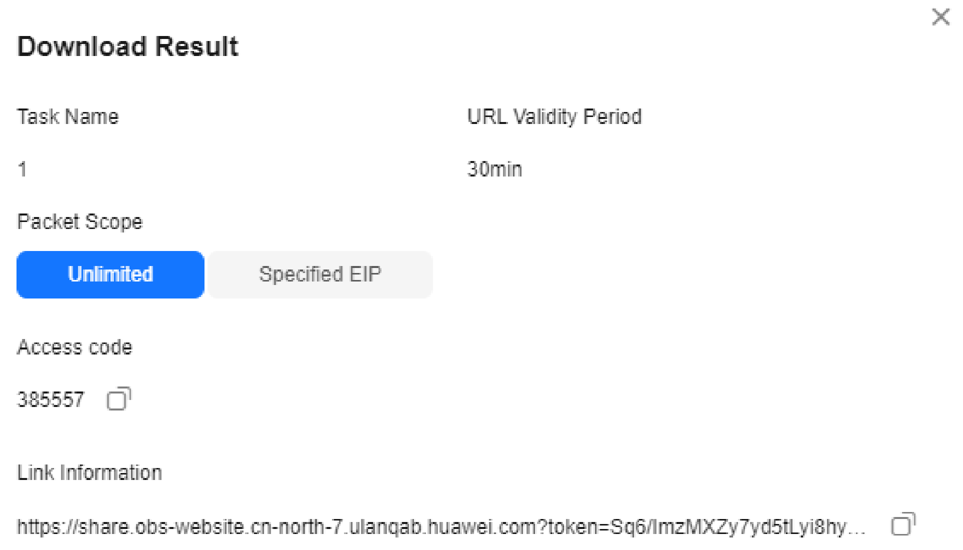
  - Share one or more packet capture results: Click **Copy link** in the **URL** column and share the information with others.

    The recipient end can paste the link to the browser to download the packet capture result files.

  - Download the packet capture result:

    - Download a single result: Click **Download** in the **URL** column of the list.
    - Download all results: Click **Download All** in the lower right corner.

Figure 9-9 Downloading the packet capture result



Download Result

Task Name
1

URL Validity Period
30min

Packet Scope
Unlimited | Specified EIP

Access code
385557

Link Information
https://share.obs-website.cn-north-7.ulanqab.huawei.com?token=Sq6/ImzMXZy7yd5tLyi8hy...

NOTE

- A maximum of three CIDR blocks can be added at a time.
- When you open the **Download Result** page again, you can modify the CIDR blocks and generate new links.
- If your CIDR block is not included in the configured CIDR blocks, you can receive the shared link but cannot download the packet capture result.

Step 8 Check whether the data in the captured packet files is consistent with service data. Identify and evaluate the risks in network communication.

----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.
- For details about how to enable Internet border traffic protection, see **Enabling Internet Border Traffic Protection**.
- For details about how to enable VPC border traffic protection, see **Enabling VPC Border Traffic Protection**.
- For details about how to enable NAT gateway traffic protection, see **Enabling NAT Gateway Traffic Protection**.

9.3 Multi-account Protection

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 any member account in the organization in a unified manner.

Constraints

- An account can only manage the EIPs of its member accounts in a unified manner.
- EIPs cannot be protected across regions. To use CFW in another region, switch to that region and purchase a firewall. For details, see **Purchasing and Changing the Specifications of CFW**.
- The number of accounts that can be protected by a single firewall instance is as follows:
  - Yearly/Monthly CFW:
    - Standard edition: 20
    - Professional edition: 50
  - Pay-per-use CFW (professional edition): 20

Example Configuration

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. Account A (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, use account A to add account B to the list on the **Multi-Account Management** page. For details, see **Step 5**.

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 permission 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.

Adding an Account to an Organization

Step 1 (Optional) Enable the Enterprise Center. For details, see **Enabling Enterprise Center**.

If the Enterprise Center has been enabled, skip this step.

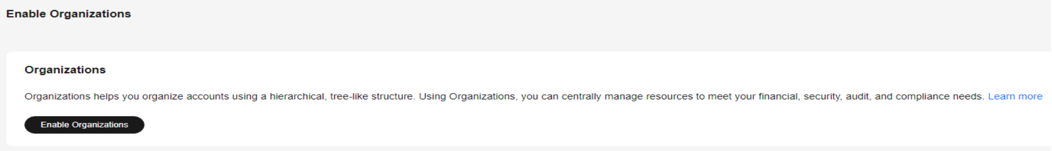
Step 2 (Optional) Enable the Organizations service and create an organization.

If the Organizations service has been enabled, skip this step.

If you are already in an organization, leave the organization before creating another organization. For details, see **Removing a Member Account from Your Organization**.

1. **Log in to the management console**.
2. Click ☰ in the upper left corner and choose **Management & Governance** > **Organizations**.
3. Go to the page for enabling the Organizations service, and click **Enable Organizations**.

Figure 9-10 Enabling Organizations



Enable Organizations

Organizations

Organizations helps you organize accounts using a hierarchical, tree-like structure. Using Organizations, you can centrally manage resources to meet your financial, security, audit, and compliance needs. Learn more

After the Organizations service is enabled, your organization and the root are automatically created, and your login account is defined as the management account.

Step 3 Set CFW as a trusted service. For details, see **Enabling or Disabling a Trusted Service**.

Step 4 Ensure the current account is an organization management account or a delegated administrator account. For details, see **Specifying a Delegated Administrator**.

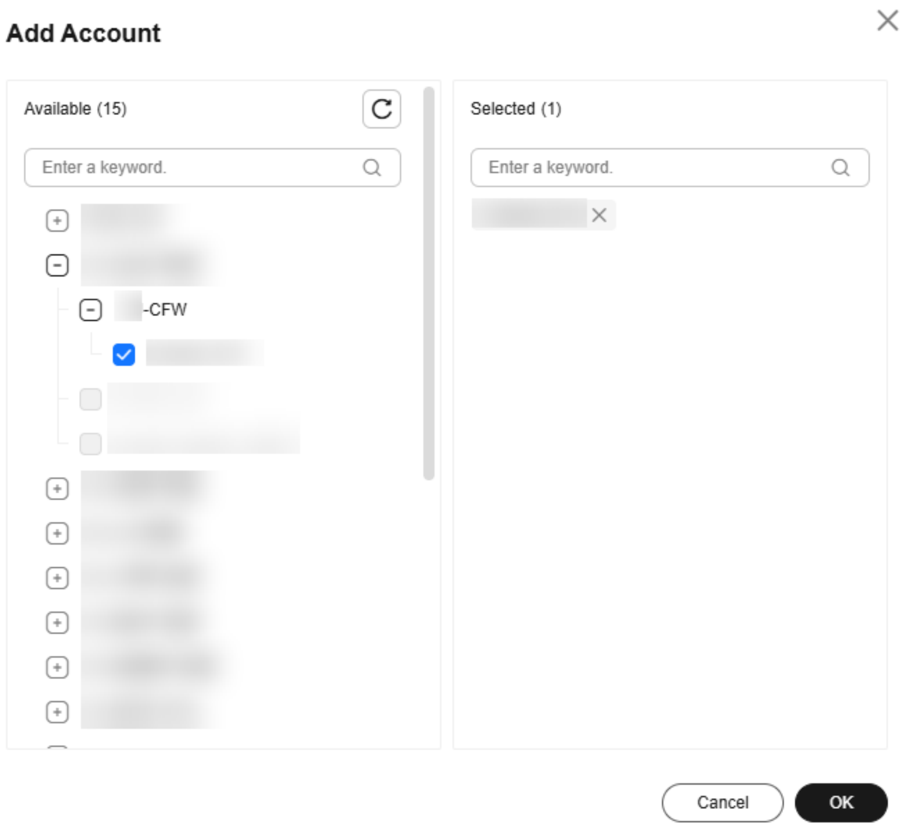
Step 5 Add a member account to an organization.

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

2. (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.
3. In the navigation pane, choose **System Management** > **Multi-Account Management**.
4. 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.

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

   Figure 9-11 Adding an account to an organization

5. Click **OK**. The added account is displayed in the account list.
6. (Optional) View the EIP resources of organization members.
   1. In the navigation pane, choose **Assets** > **EIPs**.
   2. Click **Synchronize EIP** in the upper right corner to synchronize EIPs to the list.

----End

Viewing Accounts in an Organization

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Check the account list. For details, see **Table 9-7**.

Table 9-7 Parameters in the account list

Parameter	Description
Account Name	Account name.
EIPs	Number of EIPs under an account.
Protected EIPs	Number of EIPs protected by the firewall.
Unprotected EIPs	Number of EIPs that are not protected by the firewall.

----End

Verifying the Configuration

After the configuration is successful, view the EIPs of other accounts on the **Assets** > **EIPs** page. Check the owner accounts of the EIPs in the **Owner** column.

References

- Deleting an organization member account: Select an account and click **Delete Account** above the list.
- **Using CFW to Protect EIPs Across Accounts**
- **Using CFW to Protect VPCs Across Accounts**

9.4 Configuring a DNS Server

Scenario

Domain Name System (DNS) servers are key components for network communication. They convert domain names into IP addresses. CFW uses a default DNS server for domain name resolution. If the default DNS server cannot meet your requirements, or your system depends on another DNS server to resolve domain names, you can change the default DNS server or set a custom DNS server. The domain name protection policies will use the configured DNS server for IP address resolution and delivery.

If your account has multiple firewalls, the DNS resolution setting applies only to the firewall where this setting is configured.

This section describes how to change the default DNS server or set a custom a DNS server.

Constraints

A maximum of two DNS servers can be customized.

Configuring a DNS Server

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the page.

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

Step 6 Select the DNS server or click **Add** under the **Custom DNS Server**.

NOTE

Currently, only two specified DNS servers can be added.

Step 7 Click **Apply**.

If the current account has multiple firewalls, the DNS resolution setting only applies to the firewall where this setting is configured.

----End

Follow-up Operations

After the DNS service is configured, you need to add protection rules. For details, see **Configuring an Access Control Policy**.

9.5 Security Report Management

9.5.1 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.

Creating 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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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, see Table 9-8.

Table 9-8 Parameters of the security report template

Parameter	Description
Report Name	Name of the custom 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. ● **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**.

Parameter	Description
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. - If **Report Type** is set to **Custom**, the report is automatically sent after being generated.
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

Follow-up Operations

For details about how to download and view security reports, see **Viewing/Downloading a Security Report**.

References

For details about how to enable, disable, modify, and delete security reports, see **Managing Security Reports**.

9.5.2 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.

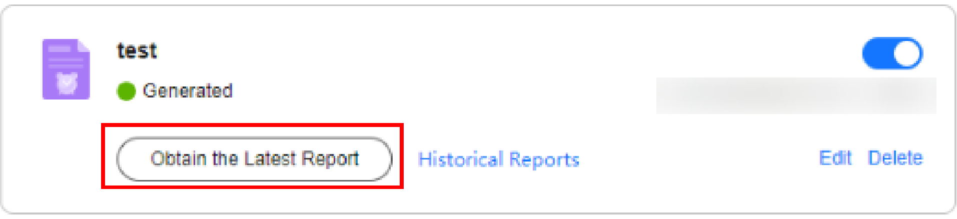
Step 3 In the navigation pane on the left, click ≡ and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

Step 4 (Optional) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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 9-12 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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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 9-13 Obtaining historical reports

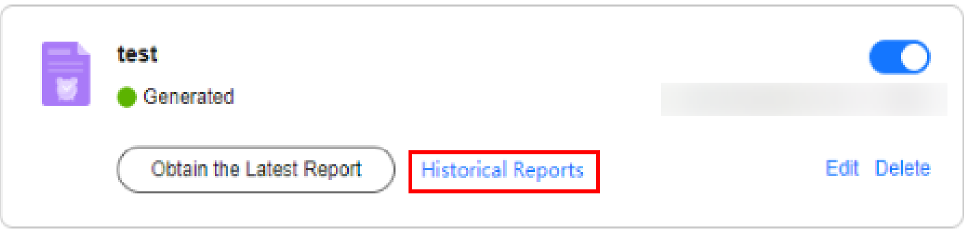
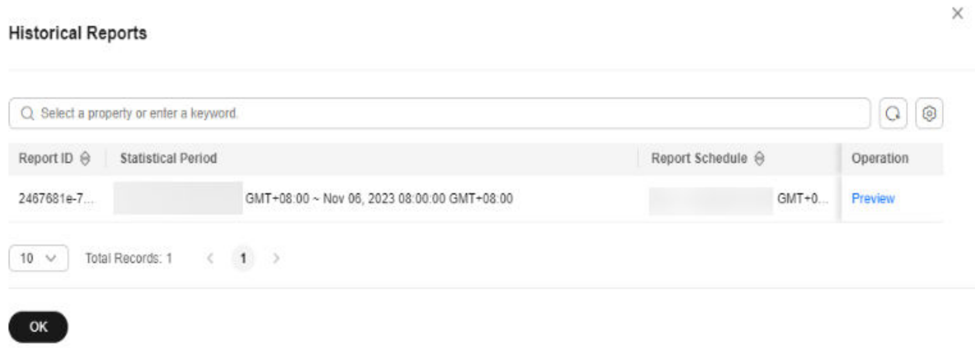


Figure 9-14 Historical reports



Historical Reports

Select a property or enter a keyword.

Report ID	Statistical Period	Report Schedule	Operation
2467681e-7...	[redacted] GMT+08:00 ~ Nov 06, 2023 08:00:00 GMT+08:00	[redacted] GMT+0...	Preview

10 Total Records: 1 1

OK

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

9.5.3 Managing Security Reports

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

Constraints

- 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.

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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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 9-9 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.
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) Switch to another firewall instance. Select a firewall from the drop-down list in the upper left corner of the 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

10 Permissions Management

10.1 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"
                        ]
                }
        ]
}
```

10.2 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
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

Permission	Action
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
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

Permission	Action
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

11 Using Cloud Eye to Monitor CFW

11.1 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.

Constraints

The following metrics are supported only in **CN North-Ulanqab1**, **CN-Hong Kong**, and **CN East-Shanghai1**:

- internet_protection_traffic
- vpc_protection_traffic
- internet_protection_traffic_inbound
- internet_protection_traffic_outbound
- ips_allow_count

Metrics

The metrics described in **Table 11-1** are old. You are advised to use the metric in **Table 11-2**.

Table 11-1 CFW metrics (not recommended)

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Original Metric)
used_protection_bandwidth	Boundary Protection Bandwidth Usage (Mbps)	Used Internet bandwidth detected by CFW in the last 5 minutes	≥ 0 Value type: Float	KB/s	1000(SI)	CFW	5 minutes
protection_bandwidth_usage	Boundary Protection Bandwidth Usage (%)	Internet bandwidth usage rate detected by CFW within 5 minutes. Usage rate = Use bandwidth/Percentage of the used bandwidth to the bandwidth quota.	≥ 0 Value type: Float	Percentage	N/A	CFW	5 minutes

Table 11-2 CFW metrics

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Original Metric)
internet_protection_bandwidth_usage	Internet Boundary Protection Bandwidth Usage (Mbps)	Bandwidth usage (Mbps) for protection at the Internet boundary.	≥ 0 Value type: Float	Bit/s	1000(SI)	CFW	Every minute
vpc_protection_bandwidth_usage	Inter-VPC Protection Bandwidth Usage (Mbps)	Bandwidth usage (Mbps) for inter-VPC protection.	≥ 0 Value type: Float	Bit/s	1000(SI)	CFW	Every minute
internet_protection_bandwidth_usage_rate	Internet Boundary Protection Bandwidth Usage (%)	Bandwidth usage (%) for protection at the Internet boundary.	≥ 0 Value type: Float	%	N/A	CFW	Every minute
vpc_protection_bandwidth_usage_rate	Inter-VPC Protection Bandwidth Usage (%)	Bandwidth usage (%) for inter-VPC protection.	≥ 0 Value type: Float	%	N/A	CFW	Every minute

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Original Metric)
internet_protection_pps	Internet Boundary Firewall PPS	PPS of protected objects at the Internet border.	≥ 0 Value type: Float	/	N/A	CFW	Every minute
vpc_protection_pps	Inter-VPC Firewall PPS	PPS of inter-VPC protected objects.	≥ 0 Value type: Float	/	N/A	CFW	Every minute
ips_hit_count	IPS Rule Hits	Number of times that traffic matches IPS rules.	≥ 0 Value type: Int	/	N/A	CFW	Every minute
ips_deny_count	IPS Rule Block Count	Number of times that traffic is blocked based on IPS rules.	≥ 0 Value type: Int	/	N/A	CFW	Every minute
acl_hit_count	ACL Rule Hits	Number of times that traffic matches ACL rules.	≥ 0 Value type: Int	/	N/A	CFW	Every minute
acl_deny_count	ACL Rule Block Count	Number of times that traffic is blocked based on ACL rules.	≥ 0 Value type: Int	/	N/A	CFW	Every minute
internet_protection_bandwidth_usage_inbound	Inbound Protection Bandwidth	Inbound Internet protection bandwidth of the firewall.	≥ 0 Value type: Float	Bit/s	1000(SI)	CFW	Every minute

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Original Metric)
internet_protection_bandwidth_usage_outbound	Outbound Protection Bandwidth	Outbound Internet protection bandwidth of the firewall.	≥ 0 Value type: Float	Bit/s	1000(SI)	CFW	Every minute
internet_protection_bandwidth_usage_rate_inbound	Inbound Protection Bandwidth Usage	This metric = Inbound Internet protection bandwidth of the firewall/ Internet Border Protection Bandwidth	≥ 0 Value type: Float	%	N/A	CFW	Every minute
internet_protection_bandwidth_usage_rate_outbound	Outbound Protection Bandwidth Usage	Outbound Internet protection bandwidth usage (%).	≥ 0 Value type: Float	%	N/A	CFW	Every minute
internet_protection_pps_inbound	Inbound PPS	PPS of Internet access to firewall-protected objects.	≥ 0 Value type: Float	/	N/A	CFW	Every minute
internet_protection_pps_outbound	Outbound PPS	PPS of firewall-protected objects accessing the Internet.	≥ 0 Value type: Float	/	N/A	CFW	Every minute

Metric ID	Metric Name	Description	Value Range	Unit	Number System	Monitored Object (Dimension)	Monitoring Period (Original Metric)
internet_protection_traffic	Internet Protection Traffic	Traffic of the protected objects of a firewall.	≥ 0 Value type: Float	- KB - MB - GB - Byte	1000(SI)	CFW	Every minute
vpc_protection_traffic	Inter-VPC Protection Traffic	Traffic between the VPCs protected by a firewall.	≥ 0 Value type: Float	- KB - MB - GB - Byte	1000(SI)	CFW	Every minute
internet_protection_traffic_inbound	Inbound Internet Protection Traffic	Inbound Internet protection traffic of a firewall.	≥ 0 Value type: Float	- KB - MB - GB - Byte	1000(SI)	CFW	Every minute
internet_protection_traffic_outbound	Outbound Internet Protection Traffic	Outbound Internet protection traffic of a firewall.	≥ 0 Value type: Float	- KB - MB - GB - Byte	1000(SI)	CFW	Every minute
ips_allow_count	IPS Rule Allow Count	Number of times that traffic is allowed based on IPS rules.	≥ 0 Value type: int	/	N/A	CFW	Every minute

Dimension

Key	Value
fw_instance_id	Firewall ID

11.2 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.

Configuring Alarm Monitoring Rules

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

11.3 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.

Viewing Monitoring Metrics

Step 1 Configure alarm rules on the Cloud Eye console. For details, see Configuring Alarm Monitoring Rules.

Step 2 In the navigation pane on the left of the Cloud Eye console, choose **Cloud Service Monitoring** > **Cloud Firewall**.

Step 3 In the row containing the dedicated CFW instance, click **View Metric** in the **Operation** column.

----End

12 CTS Auditing

12.1 Operations Recorded by CTS

Cloud Trace Service (CTS) records the operations on CFW. With CTS, you can query, audit, and backtrack these operations. For details about CTS and how to enable and configure it, see **Getting Started with CTS**.

Table 12-1 describes the CFW operations recorded by CTS.

Table 12-1 CFW operations recorded by CTS

Operation	Resource Type	Trace Name
EIP protection	eip_protection_operation	eipOperateProtectService
Enable EIP protection	eip_protection_operation	eipOperateProtectServiceEnable
Disable EIP protection	eip_protection_operation	eipOperateProtectServiceDisable
Create an ACL rule	acl	createACLRule
Modify an ACL rule	acl	createACLRule
Delete an ACL rule	acl	deleteACLRule
Configure ACL rule priority	acl	modifyACLRule
View ACL rule hits **NOTE** The number of hits here is the number of hits in the policy list. The count continues to increase unless reset to 0.	acl	showRuleHitCount
Configure ACL priority	acl	setACLRulePriority

Operation	Resource Type	Trace Name
Create a blacklist	black_white_list	createBlackList
Modify a blacklist	black_white_list	modifyBlackList
Delete a blacklist	black_white_list	deleteBlackList
Create a whitelist	black_white_list	createWhiteList
Modify a whitelist	black_white_list	modifyWhiteList
Delete a whitelist	black_white_list	deleteWhiteList
Create an IP address group	address_group	createIPAddressGroup
Update an IP address group	address_group	updateIPAddressGroup
Delete an IP address group	address_group	deleteIPAddressGroup
Delete address groups in batches	address_group	batchDeleteIPAddressGroup
Add a member to an IP address group	address_group_member	addIPAddressGroupMember
Update a member in an IP address group	address_group_member	updateIPAddressGroupMember
Delete a member from an IP address group	address_group_member	deleteIPAddressGroupMember
Create a service group	service_group	addServiceGroup
Update a service group	service_group	updateServiceGroup
Delete a service group	service_group	deleteServiceGroup
Delete service groups in batches	service_group	batchDeleteServiceGroup
Add a member to a service group	service_group_member	addServiceGroupMember
Update a member in a service group	service_group_member	updateServiceGroupMember
Delete a member from a service group	service_group_member	deleteServiceGroupMember
Create a domain name group	domain_set	addDomainSet
Update a domain group	domain_set	updateDomainSet

Operation	Resource Type	Trace Name
Delete a domain name group	domain_set	deleteDomainSet
Delete domain name groups in batches	domain_set	batchDeleteDomainSet
Add domain names in batches	domain_set	batchAddDomain
Delete a domain name	domain	deleteDomainName
Create a schedule	schedule	createSchedule
Update a schedule	schedule	updateSchedule
Delete a schedule	schedule	deleteSchedule
Delete schedules in batches	schedule	batchDeleteSchedule
Create a packet capture task	capture	createCaptureTask
Stop a packet capture task	capture	deleteCaptureTask
Delete a packet capture task	capture	cancelCaptureTask
Create an east-west firewall	cfw	createEWFirewallInstance
Create a north-south firewall	cfw	createSNFirewallInstance
Update a firewall	cfw	updateFirewallInstance
Delete a firewall	cfw	deleteFirewallInstance
Upgrade a firewall	cfw	upgradeFirewallInstance
Add a tag	cfw	createTags
Delete a tag	cfw	deleteTags
Freeze a firewall **NOTE** A firewall may be frozen due to the following reasons: ● The account is in arrears. ● The account is frozen, for example, due to violations.	cfw	freezeFirewallInstance

Operation	Resource Type	Trace Name
Change the firewall name	cfw	changeFirewallName
Update attack logs and deliver configuration	alarm_config	updateAlarmConfig
Update a user's DNS server configurations	dns_server	updateDnsServer
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
Change the antivirus status	cfw	changeAntiVirusRuleStatus
Change the status of an antivirus rule	cfw	changeAntiVirusStatus
Change the sensitive directory scan status or the reverse shell rule status	cfw	changeAdvanceIpsRuleStatus
Modify log management configuration	log_config	changeLogConfig
Import an ACL	import	importCFW
Display the firewall list	queryFirewallInstanceListService	listFirewallInstanceList
Display firewalls by tag	getInstancesByTagsService	listInstancesByTags

12.2 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)**.