Cloud Firewall

User Guide

Issue	03
Date	2024-10-09

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

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

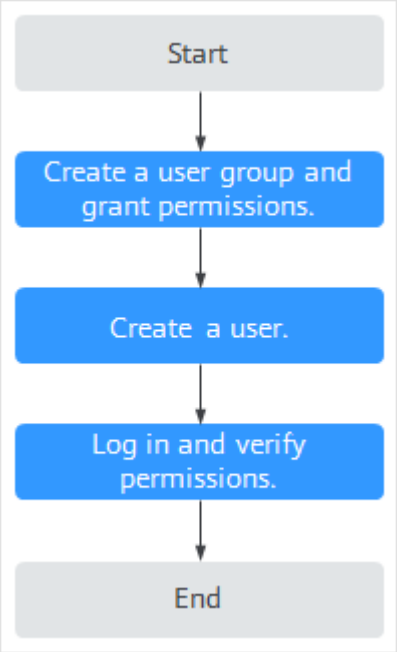
Learn about the permissions supported by CFW in **Table 1-1** and choose policies or roles based on your requirements.

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



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

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

2. **Creating an IAM User**.

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

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

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

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

2 Checking the 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 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 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.
- View firewall instance information: Click **Firewall List** in the upper right corner. For details about parameters, see **Firewall instance information**.

Figure 2-1 Viewing firewall instance information

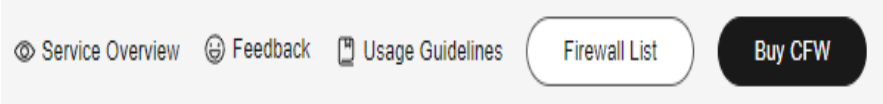


Table 2-1 Firewall instance information

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

Parameter	Description
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	

Step 5 In the **Resource Overview** area, view the protection status of all cloud resources (EIPs and VPCs) in the current region under the current account.

Step 6 View firewall instance information.

Table 2-2 describes the parameters in the **Firewall Details** area on the right part of the page.

Table 2-2 Firewall instance details

Parameter		Description
Basic Information	Version	Firewall edition. Standard and professional editions are supported.
	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.
	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.

Parameter		Description
	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.
Other Information	Billing Mode	Billing mode
	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 and trace firewall instances. For details about Tag Management Service (TMS), see **Resource Tag Overview**.

Step 7 On the **Operations Dashboard** page, view the overall protection data of cloud resources.

Click the **Internet Boundaries** or **Inter-VPC Borders** tab to view the corresponding overall protection data.

In the upper right corner, change the query range.

- View the blocking results of access control policies and the maximum inbound and outbound traffic.
- **Traffic Trend** displays the inbound, outbound, and overall traffic trends..

  Table 2-3 Values

Time Range	Average	Maximum
Last 1 hour	Average value within every minute	Maximum value within every minute
Last 24 hours	Average value within 5 minutes	Maximum value within 5 minutes
Last 7 days	Average value within one hour	Maximum value within one hour

- **Attacks**: View the traffic blocked or allowed by intrusion prevention.

- **Access Control**: View the traffic blocked or allowed by access control policies.

----End

3 Purchasing and Changing the Specifications of CFW

3.1 Purchasing Yearly/Monthly Cloud Firewall

Yearly/Monthly 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

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

Constraints

- CFW can be used only in the region where it was purchased. To use CFW 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 SMEs that need to defend against network intrusions and server compromises, or need to obtain Multi-Layer Protection Scheme (MLPS) certification.
- Professional edition

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

Standard Edition Firewalls

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

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

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

Step 4 Click **Buy CFW** and configure parameters on the **Buy CFW** page. For more information, see **Table 3-1**.

Table 3-1 Parameters for purchasing the standard edition CFW

Parameter		Description
Billing Mode		Yearly/Monthly
Region		Region where the CFW is to be purchased. **NOTICE** CFW can be used in the selected region only. To use CFW in another region, switch to the corresponding region and then purchase it. For details about the regions where CFW is available, see **Can CFW Be Used Across Clouds or Regions?**
Edition	-	Select the standard edition.
	Add EIP Protection Capacity	(Optional) Number of additional EIPs to be protected. Value range: 0 to 2000. **NOTE** By default, 20 public IP addresses are protected by the standard edition (included in the package fee). If you have 65 public IP addresses, you only need to enter 45.
	Add Internet Border Protection Bandwidth	(Optional) Additional peak inbound or outbound traffic. The value range is 0 to 2000 Mbit/s per month. (The value must be an integer multiple of 5.) **NOTE** • By default, up to 10 Mbit/s is protected by the standard edition (included in the package fee). 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.

Parameter		Description
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	Select the enterprise project to which you belong from the drop-down list. The purchased CFW then belongs to that enterprise project and protects all resources in that project. This option is only available if you have logged in using an enterprise account, or if you have enabled enterprise projects. To use this function, **Enable Enterprise Center**. You can use an enterprise project to centrally manage your cloud resources and members by project. **NOTE** Value **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.
	Tags	You can use a tag for multiple cloud resources. You are advised to predefine tags in TMS. For details, see **Resource Tag Overview**.
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 **Buy Now**.

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

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

----End

Professional Edition Firewalls

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

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

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

Step 4 Click **Buy CFW** and configure parameters on the **Buy CFW** page. For more information, see **Table 3-2**.

Table 3-2 Parameters for purchasing a professional edition CFW

Parameter		Description
Basic settings	Billing Mode	Yearly/Monthly
	Region	Region where the CFW is to be purchased. **NOTICE** CFW can be used in the selected region only. To use CFW in another region, switch to the corresponding region and then purchase it. For details about the regions where CFW can be purchased, see **Function Overview**.
Edition	-	Select the professional edition.
	Add EIP Protection Capacity	(Optional) Number of additional EIPs to be protected. Value range: 0 to 2000. **NOTE** By default, 50 public IP addresses are protected by the professional edition (included in the package fee). If you have 65 public IP addresses, you only need to enter **15**.
	Add Internet Border Protection Bandwidth	(Optional) Additional peak inbound or outbound traffic. The value range is 0 to 5000 Mbit/s per month. (The value must be an integer multiple of 5.) **NOTE** • By default, up to 50 Mbit/s is protected by the professional edition (included in the package fee). If your protection traffic is 200 Mbit/s, you only need to enter **150**. • The protection traffic is determined based on the maximum inbound or outbound traffic, whichever is higher.
	Add VPCs	(Optional) Select the number of VPCs to be expanded. The value ranges from 0 to 500. **NOTE** • Only the professional edition supports inter-VPC protection. • By default, 2 VPCs are protected by the professional edition (included in the package fee). If you have 3 VPCs, you only need to enter 1. • For each VPC you add, the protected peak traffic increases by 200 Mbit/s.

Parameter		Description
Advanced Settings	Enterprise Project	Select the enterprise project to which you belong from the drop-down list. The purchased CFW then belongs to that enterprise project and protects all resources in that project. This option is only available if you have logged in using an enterprise account, or if you have enabled enterprise projects. To use this function, **Enable Enterprise Center**. You can use an enterprise project to centrally manage your cloud resources and members by project. **NOTE** Value **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.
	Firewall Name	Firewall name. It must meet the following requirements: • Only letters (A to Z and a to z), numbers (0 to 9), spaces, and the following characters are allowed: -_ • The value can contain 1 to 48 characters.
	Tags	You can use a tag for multiple cloud resources. You are advised to predefine tags in TMS. For details, see **Resource Tag Overview**.
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 **Buy Now**.

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

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

----End

3.2 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.

Prerequisites

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

Constraints

- CFW can be used only in the region where it was purchased. To use CFW in another region, switch to that region and purchase it. For details about the regions where CFW is available, see **Function Overview**.
- A maximum of 1 Gbit/s bandwidth traffic (total traffic passing through the firewall) can be protected.
- Only the professional edition supports the pay-per-use billing mode.

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 and select a region or project.

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

Step 4 Click **Buy CFW** and configure parameters. For details, see **Table 3-3**.

Table 3-3 Parameters for purchasing pay-per-use 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.
Region	Region where the CFW is to be purchased. **NOTICE** CFW can be used in the selected region only. To use CFW in another region, switch to the corresponding region and then purchase it. For details about the regions where CFW can be purchased, see **Function Overview**.
Edition	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.

Parameter	Description
Enterprise Project	Select the enterprise project to which you belong from the drop-down list. The purchased CFW then belongs to that enterprise project and protects all resources in that project. This option is only available if you have logged in using an enterprise account, or if you have enabled enterprise projects. To use this function, **Enable Enterprise Center**. You can use an enterprise project to centrally manage your cloud resources and members by project. **NOTE** Value **default** indicates the default enterprise project. Resources that are not allocated to any enterprise projects under your account are displayed in the default enterprise project.
Tags	It is recommended that you use the TMS predefined tag function to add the same tag to different cloud resources.

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

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

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

----End

3.3 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) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details page.

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

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

Step 7 Confirm the order details, select **I have read and agreed to the Huawei Cloud Firewall Service Statement**, and click **Next**.

Step 8 Select a payment method and pay for your order.

----End

Related Operations

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

3.4 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.

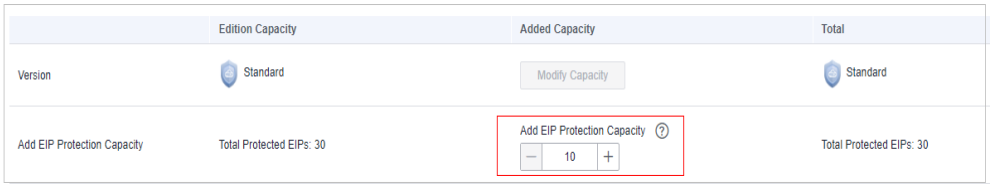
Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details page.

Step 5 In the **Firewall Details** area, click **Modify** next to **Used/Available EIP Protection Quota**, **Protected VPCs/VPC Protection Quota**, or **Peak Traffic Protection** to go to the **Change CFW Edition** page.

Step 6 Change the number of extension packages.

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

Figure 3-1 Adding EIP protection capacity



Step 7 Confirm the order details, select **I have read and agreed to the Huawei Cloud Firewall Service Statement**, and click **Next**.

Step 8 Select a payment method and pay for your order.

----End

Unsubscribing from an Extension Package

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

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

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

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

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

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

4 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.

To use CFW to protect traffic, you also need to configure access control policies or enable IPS. For details about how to configure access control policies, see **Adding a Protection Rule**. For details about IPS, see **Configuring Intrusion Prevention Policies**.

Constraints

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

Impacts on Services

Enabling or disabling EIP protection does not interrupt services, ensuring smooth traffic switchover.

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 and select a region or project.

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

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

- 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.

NOTICE

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

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

NOTE

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

----End

Related Operations

- Disabling EIP protection
  - To disable an EIP, click **Disable Protection** in the **Operation** column of the EIP.
  - To disable multiple EIPs, select them and click **Disable Protection** above the table.
- Enabling automatic protection for new EIPs: Enable **Auto Protect New EIP** above the list. Protection will be automatically enabled for new EIPs, and EIP traffic will pass through and be protected by the firewall.

Follow-up Operations

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 **Adding an Internet Boundary Protection Rule** or **6.3 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 **7.2 Blocking Network Attacks**.

5 Enabling VPC Border Traffic Protection

5.1 VPC Border Firewall Overview

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

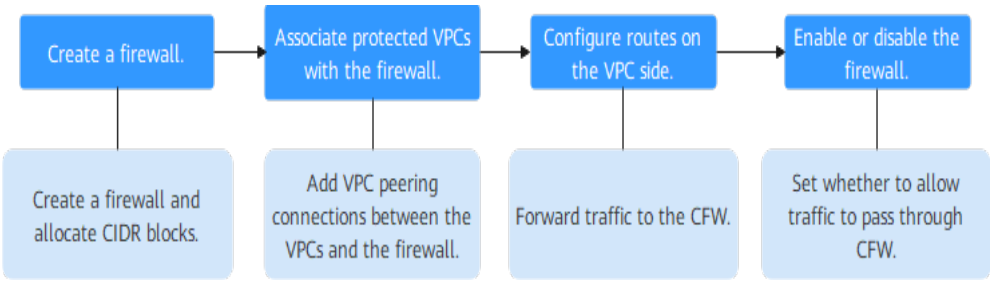
Constraints

- Only the professional edition supports VPC border firewalls.
- Only VPCs in the enterprise project to which the current account belongs can be protected.
- To use public network CIDR blocks other than 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, and 100.64.0.0/10 as private network CIDR blocks, **submit a service ticket**, or CFW may fail to forward traffic between your VPCs.

Configuration Process

The following figure shows the configuration process in VPC mode.

Figure 5-1 Configuration process in VPC mode



5.2 VPC Mode

5.2.1 Creating a Firewall (VPC Mode)

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

Constraints

Only the professional edition supports VPC border firewalls.

Procedure

Step 1 Log in to the management console.

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

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

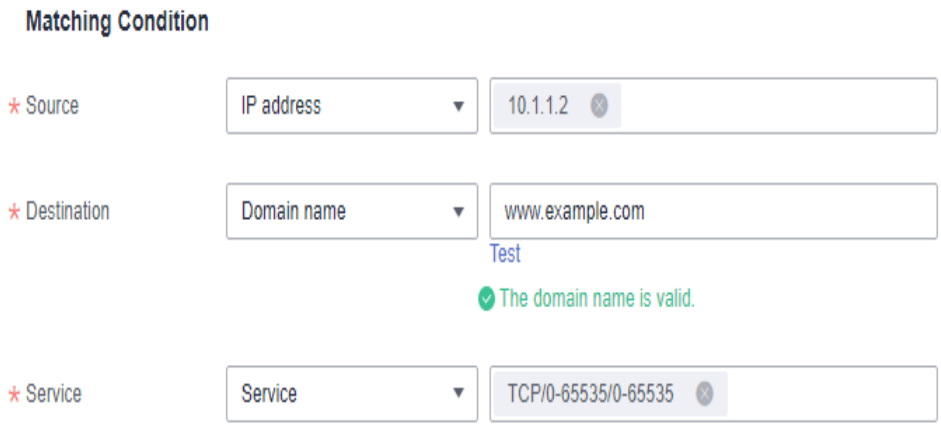
Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details page.

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

Step 6 Click **Create Firewall**.

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

Figure 5-2 Network planning



NOTE

Pay attention to the following restrictions during network planning:

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

Step 8 Click **OK**.

----End

5.2.2 Managing Protected VPCs

After creating a VPC border firewall, you need to associate VPCs with the firewall. For details, see **Associating a Protected VPC with the Firewall**.

If a VPC does not need to be protected, you can disassociate the VPC from the firewall. For details, see **Disassociating a Protected VPC from a Firewall**.

Constraints

Before disassociating a protected VPC from a firewall, delete the route pointing to the firewall in **5.2.3 Configuring VPC Route**.

Associating a Protected VPC with the Firewall

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

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

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

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

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

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

Step 7 On the **Associate Firewall** page, configure **parameters for the protected VPC**.

Table 5-1 Parameters for adding a protected VPC

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

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

----End

Disassociating a Protected VPC from a Firewall

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

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

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

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

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

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

Step 7 In the confirmation dialog box, click **OK**.

NOTE

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

----End

Follow-up Operations

After VPCs are associated, perform the operations in **5.2.3 Configuring VPC Route** to add routes.

5.2.3 Configuring VPC Route

Configure routes on the VPC side.

Procedure

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

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

Step 3 In the navigation tree on the left, click  in the upper left corner. Click **Virtual Private Cloud** under **Networking** and choose **Virtual Private Cloud** > **Route Tables**.

Step 4 In the **Name/ID** column, click the route table name of a VPC. The **Summary** page is displayed.

Step 5 Click **Add Route**. For more information, see **Table 5-2**.

Table 5-2 Route parameters

Parameter	Description
Destination Type	Select the destination address type. The value can be **IP address** or **IP address group**.
Destination	Destination CIDR block.
Next Hop Type	Select **VPC peering connection** from the drop-down list.
Next Hop	Select the VPC peering connection associated with the traffic diversion VPC.
Description	(Optional) Supplementary information about the route. **NOTE** Enter up to 255 characters. Angle brackets (< or >) are not allowed.

----End

5.2.4 Enabling or Disabling a VPC Border Firewall

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

Enabling a Firewall

Step 1 Log in to the management console.

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

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

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

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

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

Step 7 Click **OK**.

----End

Disabling a Firewall

Step 1 Log in to the management console.

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

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

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

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

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

Step 7 Click **OK**.

----End

Follow-up Operations

To add a protected VPC after a firewall is enabled, perform the operations in **Associating a Protected VPC with the Firewall** and **5.2.3 Configuring VPC Route**.

6 Configuring Access Control Policies to Control Traffic

6.1 Access Control Policy Overview

After protection is enabled, CFW access control policies allow all traffic by default. Proper access control policies help you implement refined management and control on traffic between internal servers and the Internet, prevent internal threats from spreading, and enhance in-depth security.

Access Control Policy Types

Access control policies are classified into protection rules and blacklist/whitelist. **Differences between protection rules and blacklist/whitelist** shows more details. If traffic hits a policy, the action of the policy will be taken.

Table 6-1 Differences between protection rules and blacklist/whitelist

Type	Protected Object	Network Type	Action	Configuration Method
Protection rules	• 5-tuple • IP address groups • Geographical locations • Domain names and domain name groups	• EIP • Private IP address	• If **Block** is selected, traffic will be blocked. • If **Allow** is selected, traffic will be allowed by protection rules and then checked by the intrusion prevention system (IPS).	**6.2.1 Adding Protection Rules to Block or Allow Traffic**

Type	Protected Object	Network Type	Action	Configuration Method
Blacklist	• 5-tuple • IP address groups		Traffic is blocked directly.	6.3 Adding Blacklist or Whitelist Items to Block or Allow Traffic
Whitelist			Traffic is allowed by CFW and not checked by other functions.	

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 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.

Wildcard Rule

Parameter	Input	Description
Source/Destination	0.0.0.0/0	All IP addresses
Domain name	www.example.com	Domain name www.example.com
Domain name	*.example.com	All domain names ending with **example.com**, for example, **test.example.com**
Service - Source port or destination port	1-65535	All ports

Parameter	Input	Description
Service - Source port or destination port	80-443	All ports in the range 80 to 443
Service - Source port or destination port	• 80 • 443	Ports 80 and 443

References

- For details about how to add a single rule to protect traffic, see **6.2.1 Adding Protection Rules to Block or Allow Traffic**. For details about how to add a single blacklist or whitelist item to protect traffic, see **6.3 Adding Blacklist or Whitelist Items to Block or Allow Traffic**.
- For details about how to add protection policies in batches, see **6.5.1 Importing and Exporting Protection Policies**.
- Follow-up operations after adding a policy:
  - Policy hits: For details about the protection overview, see **6.4 Viewing Protection Information Using the Policy Assistant**. For details about logs, see **Access Control Logs**.
  - For details about the traffic trend and statistics, see **8 Viewing Traffic Statistics**. For details about traffic records, see **Traffic Logs**.

6.2 Configuring Protection Rules to Block or Allow Traffic

6.2.1 Adding Protection Rules to Block or Allow Traffic

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

You can configure protection rules in the following scenarios:

- Protect the traffic of public network assets at the Internet border. For details, see **Adding an Internet Boundary Protection Rule**.
- Protect the access traffic between VPCs, or between a VPC and an IDC. For details, see **Adding a VPC Border Protection Rule**.

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 **6.3 Adding Blacklist or Whitelist Items to Block or Allow Traffic**.

Prerequisites

EIP protection must be enabled for Internet border traffic protection (EIP protection). For details, see **4 Enabling Internet Border Traffic Protection**.

Specification Limitations

To enable VPC border protection and NAT (private IP address) protection, use the CFW professional edition and enable VPC firewall protection. For details, see **VPC Border Firewall**.

Constraints

- CFW does not support application-level gateways (ALGs). ALG can analyze the fields in application-layer payloads and dynamically adjust policies for multi-channel protocols (such as FTP and SIP) whose payloads contain port numbers and IP addresses. However, CFW only support static policies for ports. To allow multi-channel protocol communication, you are advised to configure a rule to allow traffic from all ports.
- 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.
- Up to 20,000 protection rules can be added.
- The restrictions on a single protection rule are as follows:
  - A maximum of two source IP address groups and two destination IP address groups can be associated.
  - A maximum of five service groups can be associated.
- 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.
- Predefined address groups can be configured only for the source addresses in inbound rules (whose **Direction** is set to **Inbound**).
- If NAT 64 protection is enabled and IPv6 access is used, allow traffic from the 198.19.0.0/16 CIDR block to pass through. NAT64 will translate source IP addresses into the CIDR block 198.19.0.0/16 for ACL access control.

Adding an Internet Boundary Protection Rule

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

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

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

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

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

Step 6 Add a protection rule.

Click the **Internet Boundaries** tab and click **Add Rule**. In the displayed page, enter new protection information. For details, see **Table 6-2**.

Table 6-2 Internet boundary rule parameters

Parameter	Description
Rule Type	Protection type of a rule. • **EIP**: Protect EIP traffic. Only EIPs can be configured. • **NAT**: Protect NAT traffic. Private IP addresses can be configured. **NOTE** By default, EIP rules are configured. NAT rules can be configured after the professional firewall and **VPC border firewall** are configured.
Name	Name of the custom security policy.
Direction	Select a traffic direction if you set **Protection Rule** to **EIP protection**. • **Inbound**: Cloud assets (EIPs) are accessed from the Internet. • **Outbound**: Cloud assets (EIPs) access the Internet.
Source	Source address of access traffic. • **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: A collection of EIPs. For details about how to add custom IP address groups, see **Adding Custom IP Address Groups**. For details about how to add a predefined address group, see **Viewing a Predefined Address Group**. **NOTE** If **Direction** is set to **Inbound**, a predefined address group can be configured for the source address. • **Countries and regions**: If **Direction** is set to **Inbound**, you can control access based on continents, regions, and countries. • **Any**: any source address

Parameter	Description
Destination	Destination address of access traffic. • **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**: A collection of EIPs. For details about how to add custom IP address groups, see **Adding an IP Address Group**. • **Countries and regions**: If **Direction** is set to **Outbound**, you can control access based on continents, regions, countries. • **Domain name**: If **Direction** is set to **Outbound**, you can enter a multi-level single domain name (for example, top-level domain name **example.com** and level-2 domain name **www.example.com**) or a wildcard domain name (***.example.com**). **NOTE** – Mandatory for a single domain name. Click **Test** to check the validity of the domain name and perform DNS resolution. For details, see **Configuring DNS Resolution**. (Currently, up to 600 IP addresses can be resolved from a domain name.) – If the domain name is a wildcard domain name, DNS resolution is not required. Only the HTTP or HTTPS application type can be added. • **Domain name group**: If **Direction** is set to **Outbound**, a collection of multiple domain names is supported. **NOTE** To protect a domain name, you are advised to configure a domain name group. • **Any**: any destination address

Parameter	Description
Service	• **Service**: Set **Protocol Type**, **Source Port**, and **Destination Port**. – **Protocol Type**: The value can be TCP, UDP, or ICMP. – **Source/Destination Port**: If **Protocol Type** is set to **TCP** or **UDP**, you need to set the port number. **NOTE** – To specify all the ports of an IP address, set **Port** to **1-65535**. – You can specify a single port. For example, to manage access on port 22, set **Port** to **22**. – To set a port range, use a hyphen (-) between the starting and ending ports. For example, to manage access on ports 80 to 443, set **Port** to **80-443**. • **Service group**: A collection of services (protocols, source ports, and destination ports) is supported. For details about how to add a custom service group, see **Adding a Service Group**. For details about a pre-defined service group, see **6.8.2 Viewing a Predefined Service Group**. • **Any**: any protocol type or port number
Protective 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. **NOTE** • 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.

Parameter	Description
Allow Long Connection	If only one service is configured in the current protection rule and **Protocol Type** is set to **TCP** or **UDP**, you can configure the service session aging time. • **Yes**: Configure the long connection duration. • **No**: Retain the default durations. The default connection durations for different protocols are as follows: – TCP: 1800s – UDP: 60s **NOTE** Up to 50 rules can be configured with long connections.
Long Connection Duration	This parameter is mandatory if **Allow Long Connection** is set to **Yes**. Configure the long connection duration. Configure the hour, minute, and second. **NOTE** The duration range is 1 second to 1000 days.
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 7 Click **OK** to complete the protection rule configuration.

----End

Adding a VPC Border Protection Rule

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

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

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

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

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

Step 6 Add a protection rule.

Click **Add Rule**. In the displayed dialog box, enter new protection information. For details, see **Table 6-3**.

Table 6-3 VPC border protection rule parameters

Parameter	Description
Name	Name of the custom security policy.
Direction	You do not need to configure it for an inter-VPC protection rule.
Source	Source address of access traffic. • **IP address**: You can set a single IP address, consecutive IP addresses, or an IP address segment. – A single IP address, for example, **192.168.10.5** – Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** – Address segment, for example, **192.168.2.0/24** • **IP address group**: A collection of IP addresses. For details, see **Adding an IP Address Group**. • **Any**: any source address
Destination	Destination address of access traffic. • **IP address**: You can set a single IP address, consecutive IP addresses, or an IP address segment. – A single IP address, for example, **192.168.10.5** – Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** – Address segment, for example, **192.168.2.0/24** • **IP address group**: A collection of IP addresses. For details, see **Adding an IP Address Group**. • **Any**: any destination address
Service	Set the protocol type and port number of the access traffic. • **Service**: Set **Protocol Type**, **Source Port**, and **Destination Port**. – **Protocol Type**: The value can be **TCP**, **UDP**, or **ICMP**. – **Source/Destination Port**: If **Protocol Type** is set to **TCP** or **UDP**, you need to set the port number. **NOTE** – To specify all the ports of an IP address, set **Port** to **1-65535**. – You can specify a single port. For example, to manage access on port 22, set **Port** to **22**. – To set a port range, use a hyphen (-) between the starting and ending ports. For example, to manage access on ports 80 to 443, set **Port** to **80-443**. • **Service group**: A collection of services (protocols, source ports, and destination ports) is supported. For details about how to add a custom service group, see **6.8.1 Adding a Custom Service Group**. For details about predefined service groups, see **6.8.2 Viewing a Predefined Service Group**. • **Any**: any protocol type or port number

Parameter	Description
Protective 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. **NOTE** • 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.
Allow Long Connection	If only one service is configured in the current protection rule and **Protocol Type** is set to **TCP** or **UDP**, you can configure the service session aging time. • **Yes**: Configure the long connection duration. • **No**: Retain the default durations. The default connection durations for different protocols are as follows: – TCP: 1800s – UDP: 60s **NOTE** Up to 50 rules can be configured with long connections.
Long Connection Duration	This parameter is mandatory if **Allow Long Connection** is set to **Yes**. Configure the long connection duration. Configure the hour, minute, and second. **NOTE** The duration range is 1 second to 1000 days.
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 7 Click **OK** to complete the protection rule configuration.

----End

Adding a NAT Traffic Protection Rule

Step 1 Log in to the management console.

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

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

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

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

Step 6 Add a protection rule.

Click **Add Rule**. In the displayed **Add Rule** page, enter the protection information.

Table 6-4 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 **NAT**, ensure that: • The professional edition firewall is used. • The VPC border firewalls have been configured. For details, see . For details, see **Managing VPC Border Firewalls**.
Name	Name of the custom security policy.
Direction	Select **SNAT**.
Source	Source address of access traffic. • **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**: A collection of private IP addresses. For details, see **Adding an IP Address Group**. • **Countries and regions**: A continent, a region, or a country • **Any**: any source address

Parameter	Description
Destination	Destination address of access traffic. • **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**: A collection of private IP addresses. For details about how to add IP address groups, see **Adding an IP Address Group**. • **Countries and regions**: A continent, a region, or a country • **Domain Name/Domain Name Group**: When **Direction** is set to **Outbound**, the protection of a domain name or domain name group is supported. – **Application**: Supports the protection for domain names or wildcard domain names. Application-layer protocols such as HTTP and HTTPS are supported. Domain names are used for matching. – **Network**: Supports protection for one or multiple domain names. Applies to network-layer protocols and supports all protocols. The resolved IP addresses are used for matching. **NOTE** – To protect the domain names of HTTP and HTTPS applications, you can select any options. – To protect the wildcard domain names of HTTP and HTTPS applications, select **Application** and then select any option from the drop-down list. – To protect a single domain name of other application types (such as FTP, MySQL, and SMTP), select **Network** and select any option from the drop-down list. (If **Application Domain Name Group** is selected, up to 600 IP addresses can be resolved.) – If you need to configure the wildcard domain names or application domain name groups of the HTTP/HTTPS applications, and the network domain groups of other application types for the same domain name, ensure that the priority of the **Network** protection rule is higher than that of the **Application** protection rule. – For details about application and network types, see **6.7.1 Adding a Domain Name Group**. • **Any**: any destination address

Parameter	Description
Service	• **Service**: Set **Protocol Type**, **Source Port**, and **Destination Port**. – **Protocol Type**: The value can be TCP, UDP, or ICMP. – **Source/Destination Port**: If **Protocol Type** is set to **TCP** or **UDP**, you need to set the port number. **NOTE** – To specify all the ports of an IP address, set **Port** to **1-65535**. – You can specify a single port. For example, to manage access on port 22, set **Port** to **22**. – To set a port range, use a hyphen (-) between the starting and ending ports. For example, to manage access on ports 80 to 443, set **Port** to **80-443**. • **Service group**: A collection of services (protocols, source ports, and destination ports) is supported. For details about how to add a custom service group, see **Adding a Service Group**. For details about a pre-defined service group, see **6.8.2 Viewing a Predefined Service Group**. • **Any**: any protocol type or port number
Protective 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. **NOTE** • 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.

Parameter	Description
Allow Long Connection	If only one service is configured in the current protection rule and **Protocol Type** is set to **TCP** or **UDP**, you can configure the service session aging time. • **Yes**: Configure the long connection duration. • **No**: Retain the default durations. The default connection durations for different protocols are as follows: – TCP: 1800s – UDP: 60s **NOTE** Up to 50 rules can be configured with long connections.
Long Connection Duration	This parameter is mandatory if **Allow Long Connection** is set to **Yes**. Configure the long connection duration. Configure the hour, minute, and second. **NOTE** The duration range is 1 second to 1000 days.
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 7 Click **OK** to complete the protection rule configuration.

NOTE

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

----End

Related Operations

For details about how to add protection rules in batches, see **6.5.1 Importing and Exporting Protection Policies**.

6.2.2 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 **6.2.1 Adding Protection Rules to Block or Allow Traffic**.

Allowing the Inbound Traffic from a Specified IP Address

Configure two protection rules. One of them blocks all traffic, as shown in **Figure 6-1**. Its priority is the lowest. The other allows the traffic of a specified IP address, as shown in **Figure 6-2**. Its priority is the highest.

Figure 6-1 Blocking all traffic

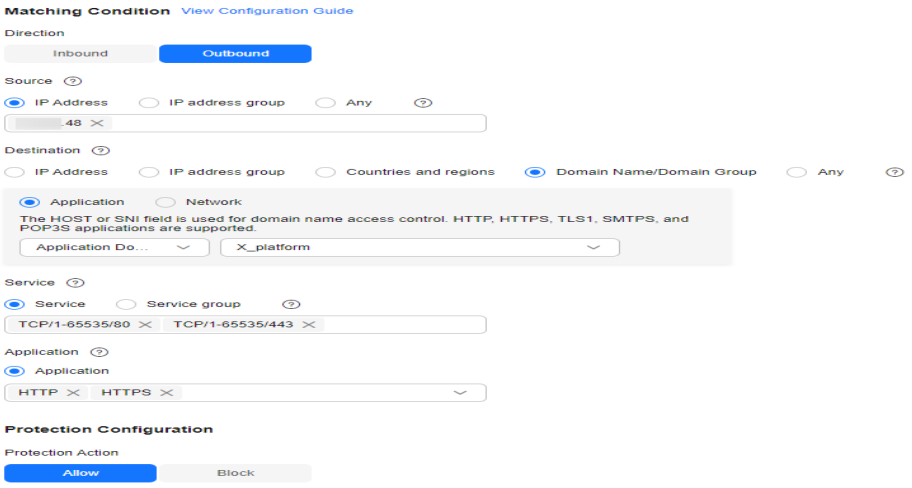
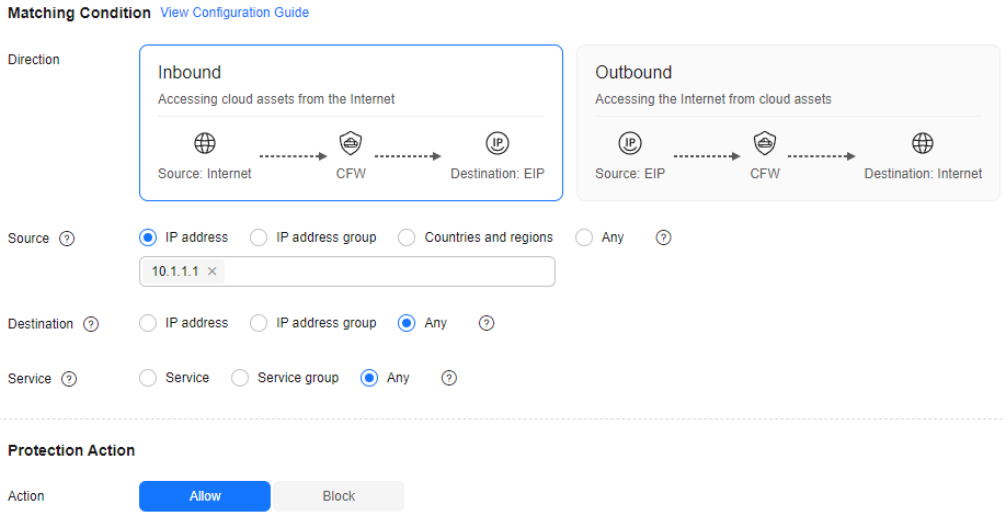


Figure 6-2 Allowing a specified IP address



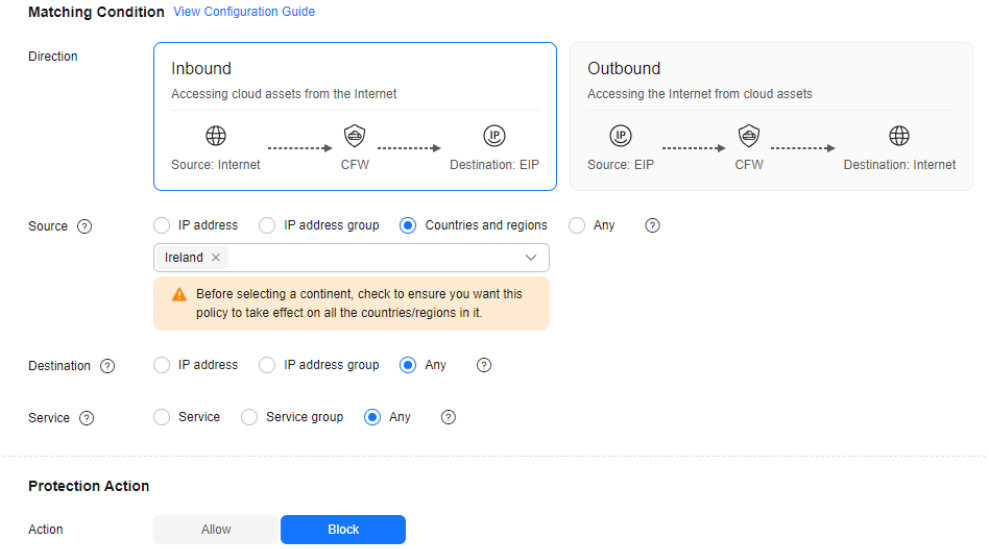
6.2.3 Example 2: Blocking Access from a Region

This section describes how to block access traffic from a region. For more parameter settings, see **6.2.1 Adding Protection Rules to Block or Allow Traffic**.

Blocking Access from a Region

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

Figure 6-3 Intercepting the access traffic from **Ireland**



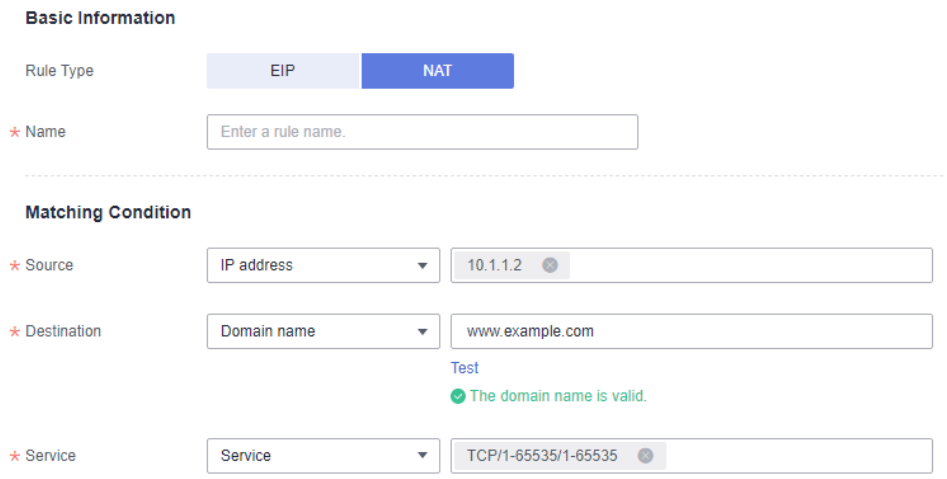
6.2.4 Example 4: Configuring SNAT Protection Rules

This section describes how to configure SNAT-based defense. For more parameter settings, see **6.2.1 Adding Protection Rules to Block or Allow 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 6-4 Configuring a NAT protection rule



6.3 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 **6.5.1 Importing and Exporting Protection Policies**.

CAUTION

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

- For details about the back-to-source IP addresses, see **What Are Back-to-Source IP Addresses?**
- For details about how to configure protection rules, see **6.2.1 Adding Protection Rules to Block or Allow Traffic**.

Specification Limitations

- CFW supports up to 2,000 blacklist items and 2,000 whitelist items. If there are too many IP addresses to be specified, you can put them in an IP address group and select the IP address group when configuring protection rules.
  - For details about how to add an IP address group, see **6.6.1 Adding Custom IP Address and Address Groups**.
  - For details about how to add a protection rule, see **6.2.1 Adding Protection Rules to Block or Allow 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 **9.2 Querying Logs**.

Adding Blacklist or Whitelist Items to Block or Allow Traffic

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

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

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

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

Step 5 In the navigation pane, choose **Access Control** > **Access Policies**. Click the tab of a protected object, and then click the **Blacklist** or **Whitelist** tab.

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

Table 6-5 Blacklist and whitelist parameters

Parameter	Description
Direction	You can select **Source** or **Destination**. • **Source**: The IP address or IP address group that sends data packets. • **Destination**: The destination IP address or IP address group that receives data packets.
IP Address	You can configure a single IP address, consecutive IP addresses, or an IP address segment.
Protocol Type	Its value can be **TCP**, **UDP**, **ICMP**, or **Any**.
Port	If **Protocol Type** is set to **TCP** or **UDP**, set the ports to be allowed or blocked. **NOTE** • To specify all the ports of an IP address, set **Port** to **1-65535**. • You can specify a single port. For example, to allow or block the access from port 22 of an IP address, set **Port** to **22**. • To set a port range, use a hyphen (-) between the starting and ending ports. For example, to allow or block the access from ports 80-443 of an IP address, set **Port** to **80-443**.
Description	Description of the blacklist or whitelist

Step 7 Click **OK**.

----End

Related Operations

- For details about how to edit and remove blacklist or whitelist items, see **6.5.4 Managing the Blacklist and the Whitelist**.
- For details about how to add blacklist or whitelist items in batches, see **6.5.1 Importing and Exporting Protection Policies**.

6.4 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) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details page.

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

Step 6 View statistics about the protection rules of a firewall instance.

- **Policy Dashboard**: Number of accesses that hit policies (protection rules, blacklist, and whitelist), numbers of allowed and blocked accesses, and the allow and block policies that were frequently hit within a specified time range.
- **Policy Hits**: Hits of a rule within a specified time range.
- **Visualizations**: Top 5 items ranked by certain parameters regarding blocked attacks within a specified time range. For more information, see **Table 6-6**. You can click a record to view policy matching details. For more information, see **Table 9-2**.

Table 6-6 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.

Parameter	Description
Top Blocked IP Address Regions	Regions of blocked IP addresses. You can click **Destination of outbound access** or **Source of inbound access** to check IP addresses.

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

----End

6.5 Managing Access Control Policies

6.5.1 Importing and Exporting Protection Policies

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

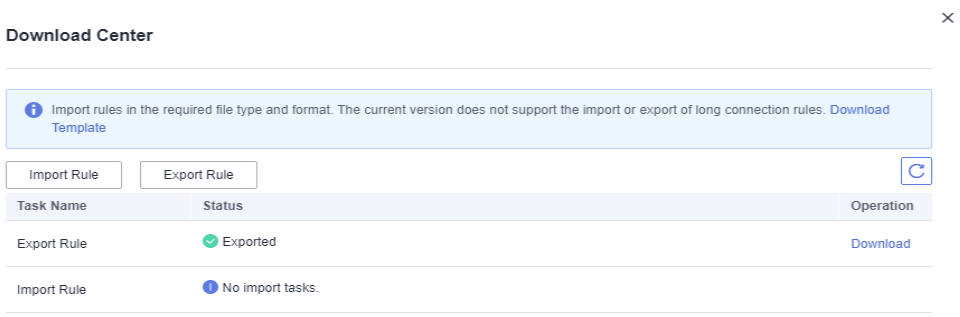
Step 3 In the navigation pane on the left, click  and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

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

Figure 6-5 Download Center



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

Step 8 Configure protection policy information as required.

- 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 **6.3 Adding Blacklist or Whitelist Items to Block or Allow Traffic**.
- For details about IP address group parameters, see **6.6.1 Adding Custom IP Address and Address Groups**.
- For details about service group parameters, see **6.8.1 Adding a Custom Service Group**.
- For details about domain name group parameters, see **6.7 Domain Name Management**.

NOTICE

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

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

NOTE

- Rule import takes several minutes.
- During rule import, you cannot add, edit, or delete access policies, IP address groups, and service groups.
- The priority of the imported policies is lower than that of the created policies.

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

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

----End

Exporting Protection Rules in Batches

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

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

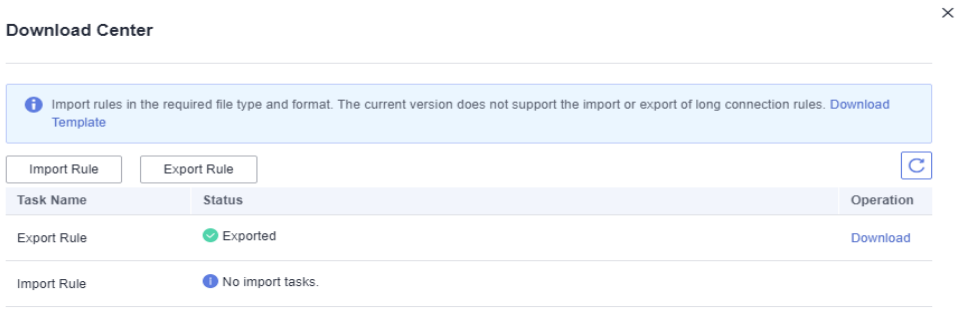
Step 3 In the navigation pane on the left, click  and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

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

Figure 6-6 Download Center



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

----End

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

Table 6-7 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

Parameter	Description	Example Value
ACL Address Type	Select **IPv4**. It is the type of IP addresses to be protected.	IPv4
Status	Whether a policy is enabled. • **Enable**: The rule is enabled. • **Disabled**: The rule is not in effect.	Enabled
Description	Rule description	test
Source Address Type	Source address type of data packets in the access traffic. • **IP Address**. You can configure a single IP address, consecutive IP addresses, or an IP address segment. • **IP Address Group**. You can configure multiple IP addresses. • **Region**: Protection can be performed by region.	IP Address
Source Address	If **Source Address Type** is set to **IP Address**, you need to configure this parameter. The following input formats are supported: • A single IP address, for example, **192.168.10.5** • Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** • A single address segment, for example, **192.168.2.0/24** **NOTE** 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	Destination address type of data packets in the access traffic. • **IP Address**. You can configure a single IP address, consecutive IP addresses, or an IP address segment. • **IP Address Group**. You can configure multiple IP addresses. • **Domain name**: A domain name consists of letters separated by dots (.). It is a human readable address that maps to the machine readable IP address of your server. • **Domain name group**. You can set a collection of domain names. • **Region**: Protection can be performed by region.	IP Address Group
Destination Address	If **Destination Address Type** is set to **IP Address**, you must configure this parameter. It can be: • A single IP address, for example, **192.168.10.5** • Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** • A single address segment, for example, **192.168.2.0/24** **NOTE** 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
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 6-8 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	Source address type of data packets in the access traffic. • **IP Address**. You can configure a single IP address, consecutive IP addresses, or an IP address segment. • **IP Address Group**. You can configure multiple IP addresses.	IP Address

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** **NOTE** 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	Destination address type of data packets in the access traffic. • **IP Address**. You can configure a single IP address, consecutive IP addresses, or an IP address segment. • **IP Address Group**. You can configure multiple IP addresses.	IP Address Group
Destination Address	If **Destination Address Type** is set to **IP Address**, you must configure this parameter. It can be: • A single IP address, for example, **192.168.10.5** • Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** • A single address segment, for example, **192.168.2.0/24** **NOTE** 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
Group Tag	Tags are used to identify rules. You can use tags to classify and search for security policies.	k=a

6.5.2 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) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details page.

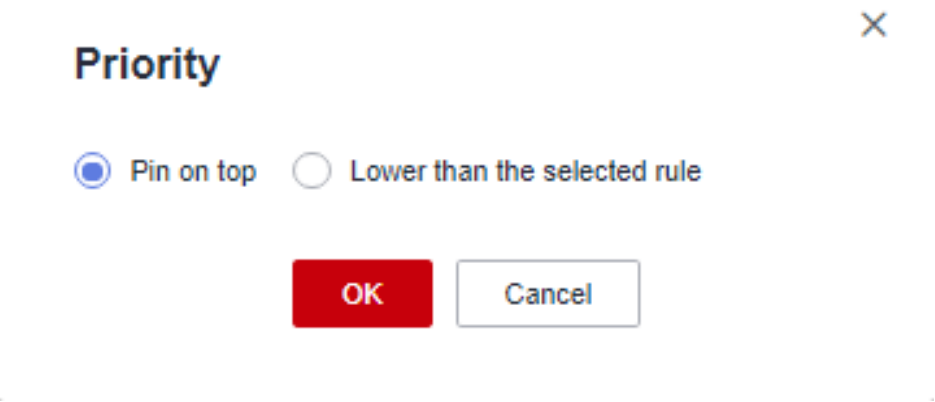
Step 5 In the navigation pane, choose **Access Control** > **Access Policies**.

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

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

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

Figure 6-7 Configuring priority



Step 8 Click **OK**.

----End

6.5.3 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) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details page.

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

Table 6-9 Protection rule parameters

Parameter	Description
Priority	Priority of the rule. **NOTE** A smaller value indicates a higher priority.
Name	Custom rule name
Direction	Traffic direction of the protection rule.
Source	Source of data packets in the access traffic.
Destination	Destination of data packets in the access traffic.
Service	• Its value can be **TCP**, **UDP**, **ICMP**, or **Any**. • Source Port: Source ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: **80-443**). • Destination Port: Destination ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: **80-443**).
Action	• **Allow**: Allow the traffic to pass through the firewall. • **Block**: Block the traffic from passing through the firewall.
Hits	Total number of actions that have been triggered by the rule (since the last reset). For details, see **Access Control Logs**.
Status	Status of the rule. It can be enabled or disabled.
Tags	Tag of a rule.

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

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

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

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

Step 8 Click **OK**.

----End

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

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

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

Step 7 Modify parameters and click **OK**. The default priority of the new protection rule is **1** (highest priority).

----End

Deleting a Rule

Step 1 Log in to the management console.

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

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

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

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

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

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

WARNING

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

----End

6.5.4 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) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details page.

Step 5 In the navigation pane, choose **Access Control** > **Access Policies**. Click the tab of a protected object, and then click the **Blacklist** or **Whitelist** tab.

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

Modify the parameters. For details about the parameters, see **Blacklist and whitelist**.

Table 6-10 Blacklist and whitelist parameters

Parameter	Description
Direction	You can select **Source** or **Destination**. • **Source**: The IP address or IP address group that sends data packets. • **Destination**: The destination IP address or IP address group that receives data packets.
IP Address	You can configure a single IP address, consecutive IP addresses, or an IP address segment.
Protocol Type	Its value can be **TCP**, **UDP**, **ICMP**, or **Any**.
Port	If **Protocol Type** is set to **TCP** or **UDP**, set the ports to be allowed or blocked. **NOTE** • To specify all the ports of an IP address, set **Port** to **1-65535**. • You can specify a single port. For example, to allow or block the access from port 22 of an IP address, set **Port** to **22**. • To set a port range, use a hyphen (-) between the starting and ending ports. For example, to allow or block the access from ports 80-443 of an IP address, set **Port** to **80-443**.
Description	Description of the blacklist or whitelist

Step 7 Click **OK**.

----End

Removing a Blacklisted or Whitelisted Item

Step 1 Log in to the management console.

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

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

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

Step 5 In the navigation pane, choose **Access Control** > **Access Policies**. Click the tab of a protected object, and then click the **Blacklist** or **Whitelist** tab.

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

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

WARNING

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

----End

6.6 Managing IP Address Groups

6.6.1 Adding Custom IP Address and Address Groups

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

Constraints

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

Adding Custom Address Groups

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

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

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

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

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

Step 6 Click the **IP Address Groups** tab. Click **Add IP Address Group** and configure parameters in the **Add IP Address Group** slide-out panel. For more information, see **IP address group parameters**.

Table 6-11 IP address group parameters

Parameter	Description
IP Address Group Name	Name of an IP address group. It must meet the following requirements: • Only uppercase letters (A to Z), lowercase letters (a to z), numbers (0 to 9), and the following special characters are allowed: -_ • The length cannot exceed 255 characters.
Description	Usage and application scenario of a rule It must meet the following requirements: • Only letters (A to Z and a to z), numbers (0 to 9), spaces, and the following characters are allowed: -_ • The length cannot exceed 255 characters.
IP Addresses	Enter IP addresses and click **Parse** to add them to the IP address list. The input can be: • A single IP address. Example: **192.168.10.5** • Address segment. Example: **192.168.2.0/24** • Consecutive IP addresses. Example: **192.168.0.2-192.168.0.10** • Multiple IP addresses. Use commas (,), semicolons (;), line breaks, tab characters, or spaces to separate them. Example: 192.168.1.0,192.168.1.0/24.

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

----End

Adding an IP Address to a Custom Address Group

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

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

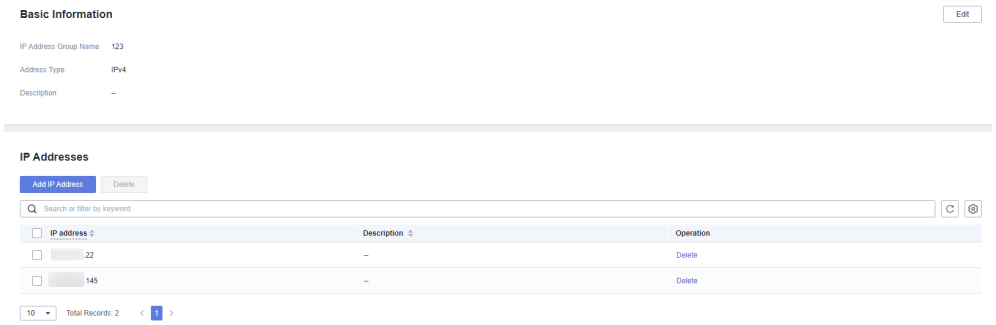
Step 3 In the navigation pane on the left, click  and choose **Security & Compliance** > **Cloud Firewall**. The **Dashboard** page will be displayed.

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

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

Step 6 Click the **IP Address Groups** tab. Click the name of an IP address group. The **IP Address Group Details** slide-out panel is displayed.

Figure 6-8 IP address group information



Step 7 Click **Add IP Address**.

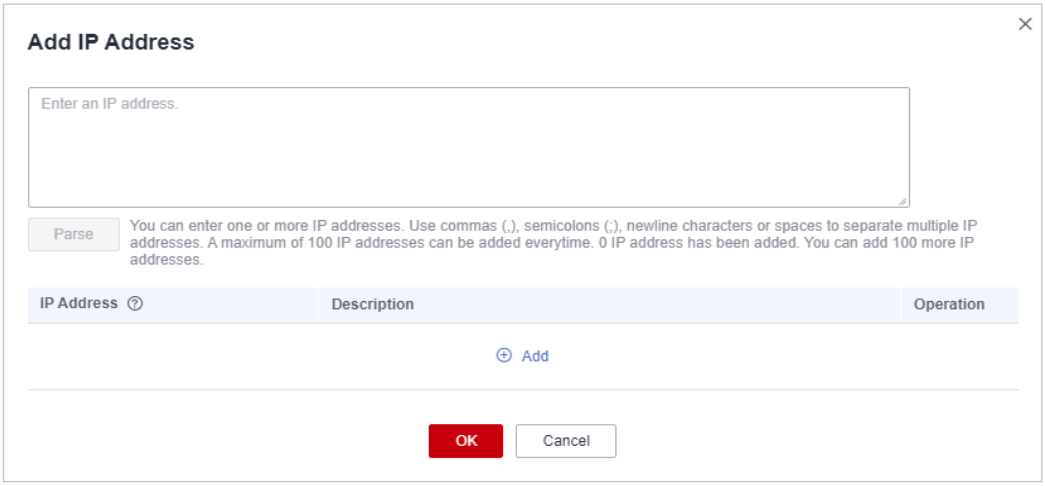
- To add IP addresses in batches, enter the IP addresses in the text box and click **Parse**.

  The input can be:

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

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

Figure 6-9 Adding an IP address



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

----End

Related Operations

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

Follow-up Operations

An IP address group takes effect only after it is set in a protection rule. For more information, see **6.2.1 Adding Protection Rules to Block or Allow Traffic**.

6.6.2 Viewing a Predefined Address Group

CFW provides you with predefined address groups, including **NAT64 Address Set** and **WAF_Back-to-Source_IP_Addresses**. You are advised to allow access from both the address groups.

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

  NOTE

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

- **WAF_Back-to-Source_IP_Addresses**: provides back-to-source IP addresses of WAF in cloud mode. For more information, see **What Are Back-to-Source IP Addresses?**

  CAUTION

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

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

Viewing a Predefined Address Group

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

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

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

Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details 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 Group** tab and click the name of an address group. On the details page that is displayed, view the address group information.

----End

6.6.3 Deleting Custom IP Address Groups

This section describes how to delete custom IP address groups.

Constraints

The address group referenced by a protection rule cannot be deleted. Modify or delete the rule first.

Deleting Custom IP Address Groups

Step 1 Log in to the management console.

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

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

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

WARNING

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

----End

6.7 Domain Name Management

6.7.1 Adding a Domain Name Group

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

The options are as follows:

- **Website filtering**: Layer 7 protocol parsing. Websites are matched based on domain names. HTTP/HTTPS is supported.
- **DNS resolution**: Layer 4 protocol parsing. Domain names are filtered based on resolved IP addresses. TCP, UDP, and ICMP are supported.

Constraints

- The domain names in a domain name group can be referenced by protection rules for up to 40,000 times, and wildcard domain names can be referenced for up to 2,000 times.

URL Filtering (Layer 7 Protocol Parsing)

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

Address Resolution (Layer 4 Protocol Parsing)

- A firewall instance can have up to 1,000 domain names.
- A DNS resolution 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.

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 and select a region or project.

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

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

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

Step 6 Click the **Domain Name Groups** tab. Click **Add Domain Name Group** and configure **parameters**.

Table 6-12 Domain name group parameters

Parameter	Description
Domain Name Group Type	The options are as follows: • **Website filtering**: Layer 7 protocol parsing. Websites are matched based on domain names. HTTP/HTTPS is supported. • **DNS resolution**: Layer 4 protocol parsing. Domain names are filtered based on resolved IP addresses. TCP, UDP, and ICMP are supported.
Group Name	Name of a user-defined domain name group.
Description	(Optional) Enter remarks for the domain name group.
Domain Name	Enter one or multiple domain names. • You can enter a multi-level single domain name (for example, top-level domain name **example.com** and level-2 domain name **www.example.com**) or a wildcard domain name (***.example.com**). • Multiple domain names are separated by commas (,), semicolons (;), line breaks, or spaces. **NOTE** Domain names must be unique.

----End

Adding a Domain Name to a Domain Group

Step 1 Log in to the management console.

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

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

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

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

Step 6 Click the **Domain Name Groups** tab. Click the name of a domain name group. The **Domain Name Groups** slide-out panel is displayed.

Step 7 Click **Add Domain** and enter domain name information.

You can click  to add multiple services.

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

----End

Related Operation

- Exporting domain name groups: Click **Export** above the list.
- Batch deleting domain names: Select domain names **in the domain name list** and click **Delete** above the list.
- To edit a domain name group, click the name of the target domain name group and click **Edit** on the right of **Basic Information**.
- A domain name group takes effect only after it is set in a protection rule. For more information, see **6.2.1 Adding Protection Rules to Block or Allow Traffic**.
- To view the IP addresses resolved by a domain name group of the DNS resolution type, click the domain name group name to go to the **Basic Information** page, and click **IP address** in the **Operation** column of the domain name list.

6.7.2 Deleting a Domain Name Group

Constraints

The domain name group referenced by a protection rule cannot be deleted. Modify or delete the rule first.

Deleting a Domain Name Group

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

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

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

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

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

Step 6 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**.

WARNING

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

----End

6.8 Service Group Management

6.8.1 Adding a Custom Service Group

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

Constraints

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

Adding a Custom Service Group

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

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

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

Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details 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 6-13 Service group parameters

Parameter	Description
Service Group Name	Name of a service group
Description	Usage and application scenario

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

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

----End

Adding a Service to a Custom Service Group

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

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

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

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

Step 7 Click **Add Service**. The **Add Service** dialog box is displayed.

Table 6-14 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**). **NOTE** If **Protocol** is set to **ICMP**, you do not need to specify any port number.	80

Parameter	Description	Example Value
Destination Port	Destination ports to be allowed or blocked. You can configure a single port or consecutive port groups (example: **80-443**). **NOTE** 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

Related Operations

- Exporting service address groups: Click **Export** above the list.
- Batch deleting services: Select services on the service group page and click **Delete** above the list.

Follow-up Operations

A service group takes effect only after it is set in a protection rule. For more information, see **6.2.1 Adding Protection Rules to Block or Allow Traffic**.

6.8.2 Viewing a Predefined Service Group

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

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

Viewing a Predefined Service Group

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

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

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

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

6.8.3 Deleting a User-defined Service Group

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

This section describes how to delete a custom service group.

Constraints

The service group referenced by a protection rule cannot be deleted. Modify or delete the rule first.

Deleting 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) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details 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**.

WARNING

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

----End

7 Attack Defense

7.1 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 **4 Enabling Internet Border Traffic Protection**.
- For details about how to enable VPC traffic protection, see **5 Enabling VPC Border Traffic Protection**.

Defense Against Network Attacks and Virus Files

The following methods can be used:

- IPS provides you with basic protection functions, and, with many years of attack defense experience, it detects and defends against a wide range of common network attacks and effectively protects your assets.
  - IPS provides four protection modes. For details about how to configure it, see **Adjusting the IPS Protection Mode to Block Network Attacks**.
    - **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.

- IPS provides multiple types of rule libraries. For details, see **Table 7-1**. Different rules are enabled for different interception modes. For details, see **Default Actions of Rule Groups in Different Protection Modes**.

Table 7-1 Intrusion prevention rule libraries

Function	Description	Check Type	Configuration Method
Basic defense	A built-in rule library. It covers common network attacks and provides basic protection capabilities for your assets.	• Scan for threats and scan vulnerabilities. • Check whether traffic contains phishing, Trojans, worms, hacker tools, spyware, password attacks, vulnerability attacks, SQL injection attacks, XSS attacks, and web attacks. • Checks whether there are protocol anomalies, buffer overflow, access control, suspicious DNS activities, and other suspicious behaviors in traffic.	For details about how to view and modify rule library settings, see **7.5.1 Modifying the Protection Action of an Intrusion Prevention Rule**.
Virtual patch	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.		

Function	Description	Check Type	Configuration Method
Custom IPS signature (supported only by the professional edition)	If the built-in rule library cannot meet your requirements, you can customize signature rules.	The check types are the same as those of **Basic defense**. Signature rules of the HTTP, TCP, UDP, POP3, SMTP and FTP protocols can be added.	For details, see **7.5.2 Customizing IPS Signatures**.

- Sensitive directory scan can defend against scanning attacks on sensitive directories on cloud servers. For details, see **Enabling Sensitive Directory Scan Defense**.
- Reverse shell detection can defend against network attacks in reverse shell mode. For details, see **Enabling Reverse Shell Defense**.
- Antivirus can 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.

  For details about antivirus, see **7.3 Blocking Virus-infected Files**.

Protection Actions

- **Observe**: The firewall records the traffic that matches the current rule in **Attack Event Logs** and does not block the traffic.
- **Intercept**: The firewall records the traffic that matches the current rule in **Attack Event Logs** and blocks it.
- **Disable**: The firewall does not log or block the traffic that matches the current rule.

References

For details about the protection overview, see **7.4 Viewing Attack Defense Information on the Dashboard**. For details about logs, see **Attack Event Logs**.

7.2 Blocking Network Attacks

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

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 and select a region or project.

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

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

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

Step 6 Select a proper protection mode.

- **Observe**: Attacks are detected and recorded in logs but are not intercepted.
- **Intercept**: Attacks and abnormal IP address access are automatically intercepted.
  - **Intercept mode - loose**: The protection granularity is coarse. In this mode, only attacks with high threat and high certainty are blocked.
  - **Intercept mode - moderate**: The protection granularity is medium. This mode meets protection requirements in most scenarios.
  - **Intercept mode - strict**: The protection granularity is fine-grained, and all attack requests are intercepted.

NOTE

- You are advised to use the **observe** mode for a period of time before using the **intercept** mode. For details about how to view attack event logs, see **Attack Event Logs**
- If packets are incorrectly blocked by a defense rule, you can modify the action of the rule in the basic defense rule library. For details, see **7.5 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 and select a region or project.

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

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

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

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

- **Action**:
  - **Observe**: If the firewall detects a sensitive directory scanning attack, it only records the attack 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.
- **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 and select a region or project.

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

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

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

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

- **Action**:
  - **Observe**: If the firewall detects a reverse shell attack, it only records the attack 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.
- **Duration**: If **Action** is set to **Block IP**, you can set the blocking duration. The value range is 60s to 3,600s.
- **Mode**:
  - **Conservative**: coarse-grained protection. If a single session is attacked for four times, observation or interception is triggered. It ensures that no false positives are reported.
  - **Sensitive**: fine-grained protection. If a single session is attacked for two times, observation or interception is triggered. It ensures that attacks can be detected and handled.

----End

Follow-up Operations

For details about the protection overview, see **7.4 Viewing Attack Defense Information on the Dashboard**. For details about logs, see **Attack Event Logs**.

7.3 Blocking Virus-infected Files

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

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

Specification Limitations

Antivirus is available only in the professional edition.

Enabling Antivirus 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) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details page.

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

Step 6 Click  to enable antivirus.

NOTE

After antivirus is enabled, **Current Action** is **Disable** by default. For details about how to change the defense action, see **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 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details page.

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

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

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

----End

Follow-up Operations

For details about the protection overview, see **7.4 Viewing Attack Defense Information on the Dashboard**. For details about logs, see **Attack Event Logs**.

7.4 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, sensitive directory scan defense, and antivirus) 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) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details page.

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

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

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

- **Security Dashboard**: Number of attacks detected by IPS, numbers of allowed and blocked accesses, and number of attacked ports.
- **Attacks**: Number of times that IPS blocks or allows traffic.
- **Visualizations**: Top 5 items ranked by certain parameters regarding the attacks detected or blocked by IPS. For more information, see **Table 7-2**. You can click a record to view attack details. For more information, see **Table 9-1**.

Table 7-2 Security dashboard statistics parameters

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

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

----End

Related Operations

For details about logs, see **Attack Event Logs**.

7.5 IPS Rule Management

7.5.1 Modifying the Protection Action of an Intrusion Prevention Rule

For rules in the basic defense 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 **7.5.2 Customizing IPS Signatures**.

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

-	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**: The firewall records the traffic that matches the current rule in **Attack Event Logs** and does not block the traffic.
- **Intercept**: The firewall records the traffic that matches the current rule in **Attack Event Logs** and blocks it.
- **Disable**: 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) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details page.

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

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

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

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

Figure 7-1 Changing the current action

NOTE

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

----End

Related Operations

- 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**.

7.5.2 Customizing IPS Signatures

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

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

CAUTION

User-defined signatures need to be specific. General signatures may match too much traffic and affect traffic forwarding performance.

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**.

Customizing IPS Signatures

Step 1 Log in to the management console.

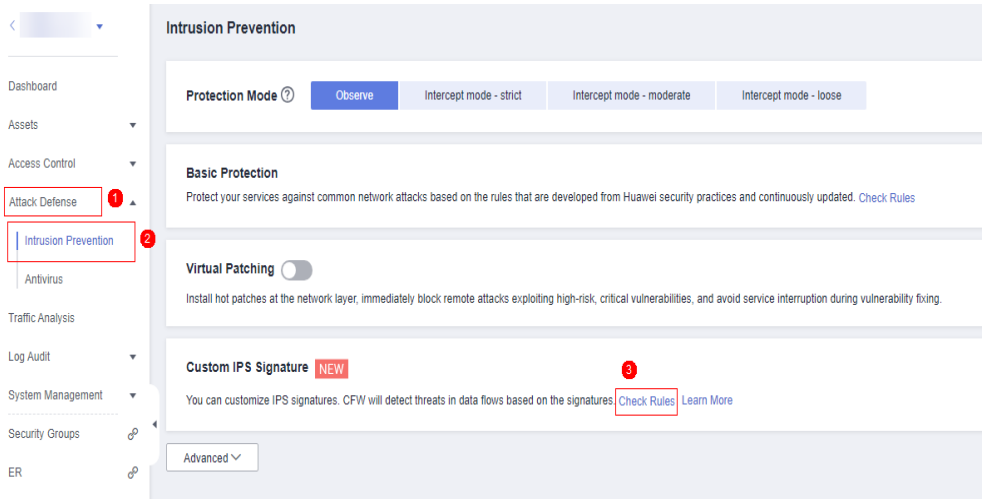
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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

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

Figure 7-2 Custom IPS signature



Step 6 Click **Add Custom IPS Signature** in the upper right corner of the list. For more information, see **Table 7-3**.

Table 7-3 Custom IPS signature parameters

Parameter Name	Description
Name	Feature name. It must meet the following requirements: • Only uppercase letters (A to Z), lowercase letters (a to z), numbers (0 to 9), and the following special characters are allowed: -_ • A maximum of 255 characters are allowed.

Parameter Name	Description
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. • **Include** • **Exclude** **NOTE** You are advised to select **Any**.
Source Port	Set **Source Port** if **Source Type** is set to **Include** or **Exclude**. • You can set one or more ports. Use commas (,) to separate multiple ports. Example: **80,100** • You can also set a port range. Use hyphens (-) to separate ports, for example, 80-443.
Destination Type	Destination port type. Its value can be: • **Any**: Any port type. All ports match this type. • **Include** • **Exclude** **NOTE** You are advised to select **Any**.
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.

Parameter Name	Description
Action	Action taken by the firewall when it detects traffic with the feature. • **Observe**: Attacks are detected and recorded in logs. For details about how to query logs, see **9.2 Querying Logs**. • **Intercept**: Attacks are automatically blocked. **NOTE** Before you enable the **Intercept** mode, you are advised to select **Observe** first and check whether the attack logs are correct for a period of time.

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

Step 7 Click **OK**.

----End

Related Operations

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

Follow-up Operations

For details about the protection overview, see **7.4 Viewing Attack Defense Information on the Dashboard**. For details about logs, see **Attack Event Logs**.

8 Viewing Traffic Statistics

8.1 Viewing Inbound Traffic

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

Prerequisites

EIP protection has been enabled. For details, see **4 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) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details 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.
- **Inbound Traffic**: Inbound request traffic and response traffic. The traffic statistics of up to 30 EIPs can be queried at a time.

Table 8-1 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**: Top 5 items ranked by certain parameters regarding inbound traffic within a specified time range. For more information, see **Table 8-2**. You can click a data record to view the traffic details. A maximum of 50 data records can be viewed.

  Table 8-2 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.
Application Distribution	Application information about inbound traffic.

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

----End

8.2 Viewing Outbound Traffic

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

Prerequisites

EIP protection has been enabled. For details, see **4 Enabling Internet Border Traffic Protection**.

Viewing Outbound Traffic

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

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

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

Step 4 (Optional) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details 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.
- **Outbound Traffic**: Outbound request traffic and response traffic. The traffic statistics of up to 30 EIPs can be queried at a time.

  Table 8-3 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**: Top 5 items ranked by certain parameters regarding outbound traffic within a specified time range. For more information, see **Table 8-4**. You can click a data record to view the traffic details. A maximum of 50 data records can be viewed.

Table 8-4 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 Access Source IP Addresses	Source IP addresses of outbound traffic.
Top Open Ports	Destination ports of outbound traffic.
Application Distribution	Application information about outbound traffic.

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

----End

8.3 Viewing Inter-VPC Traffic

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

Prerequisites

The VPC border firewall has been configured and enabled. For details, see **5 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) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details page.

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

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

- **Traffic Dashboard**: Information about the maximum traffic between VPCs.
- **Inter-VPC Access**: Request and response traffic between VPCs.

  Table 8-5 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**: Top 5 items ranked by certain parameters regarding inter-VPC traffic within a specified time range. For more information, see **Table 8-6**. You can click a data record to view the traffic details. A maximum of 50 data records can be viewed.

  Table 8-6 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.

----End

9 Viewing CFW Protection Logs

9.1 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**.

Log Storage Mode

Function	Storage Duration	Billing Mode	Access Mode	Log Field Description
Log query	7 days	Free	Automatic access	**9.2 Querying Logs**
Log management	1 – 360 days	Separate billing by traffic	You need to manually connect to LTS. For details, see **9.3.1 Configuring Logs**. For details about how to use the LTS log function, see **Log Management Description**.	**9.3.3 Log Field Description**

Log Types

The following types of logs are provided:

- Attack event log: Events detected by attack defense functions, such as IPS, are recorded. You can modify the protection action if traffic is improperly blocked. For details, see **7.5.1 Modifying the Protection Action of an Intrusion Prevention Rule**. For details about how to modify the protection action of antivirus, see **Modifying the Virus Defense Action for Better Protection Effect**.
- Access control logs: All traffic that matches the access control policies are recorded. For details about how to modify a protection rule, see **6.5.3 Managing Protection Rules**. For details about how to modify the blacklist or whitelist, see **Editing the Blacklist or Whitelist**.
- Traffic logs: All traffic passing through the firewall is recorded.

Handling Improper Blocking

- If improper blocking is recorded in access control logs, check whether your protection rules, blacklist, and whitelist configurations are correct.
- 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.	**9.3.1 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 360 days.	**9.3.2 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
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.	**9.3.3 Log Field Description**

References

- For details about the protection overview of access control policies, see **6.4 Viewing Protection Information Using the Policy Assistant**.
- For details about the traffic defense overview and trend, see **8 Viewing Traffic Statistics**.
- For details about the overall network attack defense, see **7.4 Viewing Attack Defense Information on the Dashboard**.

9.2 Querying Logs

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

- Attack event log: Events detected by attack defense functions, such as IPS, are recorded. You can modify the protection action if traffic is improperly blocked. For details, see **7.5.1 Modifying the Protection Action of an Intrusion Prevention Rule**. For details about how to modify the protection action of antivirus, see **Modifying the Virus Defense Action for Better Protection Effect**.
- Access control logs: All traffic that matches the access control policies are recorded. For details about how to modify a protection rule, see **6.5.3 Managing Protection Rules**. For details about how to modify the blacklist or whitelist, see **Editing the Blacklist or Whitelist**.
- Traffic logs: All traffic passing through the firewall is recorded.

NOTE

One or multiple types of logs can be recorded in LTS. You can view log data in the past 1 to 360 days. For details, see **9.3 Log Management**.

Prerequisites

- You have performed operations in **4 Enabling Internet Border Traffic Protection**.
- You have enabled **basic intrusion prevention**.

Constraints

- Logs can be stored for up to seven days.

- Up to 100,000 records can be exported for a single log.

Attack Event Logs

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

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

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

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

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

Figure 9-1 Attack event logs

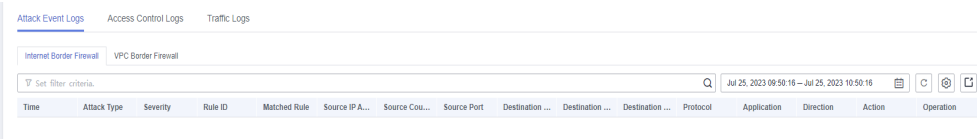


Table 9-1 Attack event log parameters

Parameter	Description
Time	Time when an attack occurred.
Attack Type	Type of the attack event, including IMAP, DNS, FTP, HTTP, POP3, TCP, and UDP.
Severity	It can be **Critical**, **High**, **Medium**, or **Low**.
Rule ID	Rule ID
Rule Name	Matched rule in the library.
Source IP Address	Source IP address of an attack event.
Source Country/ Region	Geographical location of the attack source IP address.
Source Port	Source port of an attack.
Destination IP Address	Attacked IP address.

Parameter	Description
Destination Country/ Region	Geographical location of the attack target IP address.
Destination Port	Destination port of an attack.
Protocol	Protocol type of an attack.
Application	Application type of an attack.
Direction	It can be outbound or inbound.
Action	Action of the firewall. It can be: • **Allow** • **Block** • **Block IP** • **Discard**
Operation	You can click **Details** to view the basic information and attack payload of an event.

----End

Access Control Logs

Step 1 Log in to the management console.

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

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

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

Step 5 In the navigation pane, choose **Log Audit** > **Log Query**. Click the **Access Control Logs** tab and check the traffic details in the past week. For details about how to modify the action taken on an IP address, see **6.2.1 Adding Protection Rules to Block or Allow Traffic** or **6.3 Adding Blacklist or Whitelist Items to Block or Allow Traffic**.

Figure 9-2 Access control logs

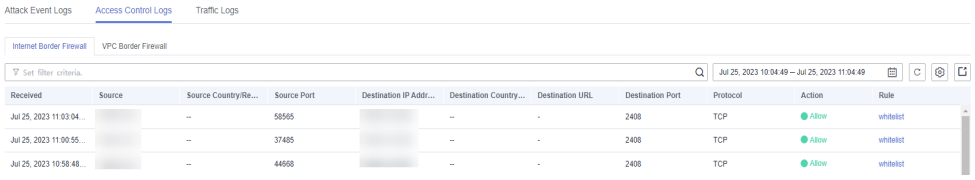


Table 9-2 Access control log parameters

Parameter	Description
Received	Time of access.
Source	Source IP address of the access.
Source Country/ Region	Geographical location of the source IP address.
Source Port	Source port for access control. It can be a single port or consecutive port groups (example: **80-443**).
Destination IP Address	Destination IP address.
Destination Country/ Region	Geographical location of the destination IP address.
Destination Port	Destination port for access control. It can be a single port or consecutive port groups (example: **80-443**).
Protocol	Protocol type for access control.
Action	Action taken on an event. It can be **Observe**, **Block**, or **Allow**.
Rule	Type of an access control rule. It can be a blacklist or whitelist.

----End

Traffic Logs

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

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

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

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

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

Figure 9-3 Traffic logs

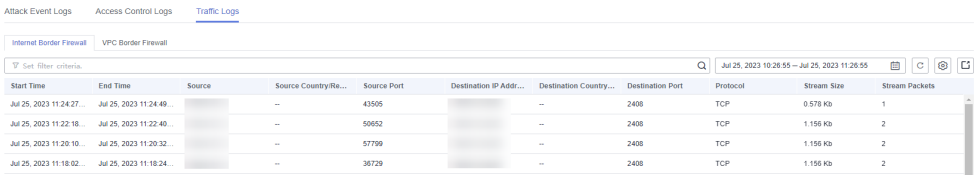


Table 9-3 Traffic log parameters

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

----End

Related Operations

Exporting logs: Click  in the upper right corner to export the logs in the list.

9.3 Log Management

9.3.1 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.

NOTICE

- On the **Log Query** page, you can check and export log data of the last seven days. For details, see **9.2 Querying Logs**.
- LTS is billed by traffic and is billed separately from WAF. 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) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details page.

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

Step 6 Create log groups and log streams. For details, see **Creating Log Groups and Log Streams**.

NOTE

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

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

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

NOTE

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

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

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

----End

9.3.2 Changing the Log Storage Duration

Logs are stored for seven days by default. The storage duration can be set to 1 to 360 days. Logs that exceed the storage duration will be automatically deleted. For log data that needs to be stored for a long time (log persistence), LTS can dump the logs to OBS for medium- and long-term storage.

Prerequisites

Logs have been dumped to LTS by configuring **9.3.1 Configuring Logs**.

Changing the Log Storage Duration

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

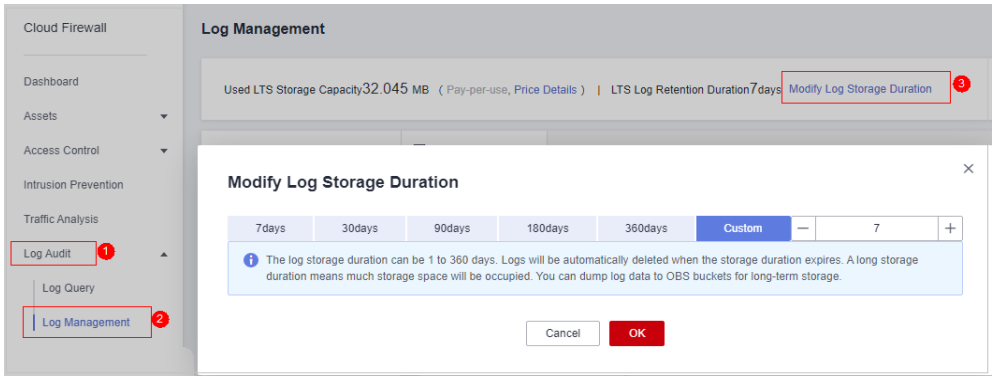
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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

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

Figure 9-4 Modifying log storage duration



NOTE

- Logs can be stored for 1 to 360 days. Logs that exceed the specified storage duration are automatically deleted.
- The longer the storage duration, the larger the occupied storage. For details about how to dump logs to other cloud services for long-term storage, see **Log Transfer Overview**.

----End

9.3.3 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
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

Field	Type	Description
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
attack_type	string	Type of the attack. • Vulnerability exploit • Vulnerability scan • Trojan • Worms • Phishing • Web attacks • Application DDoS • Buffer overflow • Password attacks • Mail • Access control • Hacking tools • Hijacking • Protocol exception • Spam • Spyware • DDoS flood • Suspicious DNS activities • Other suspicious behaviors
level	string	Level of detected threats. • **CRITICAL** • **HIGH** • **MIDDLE** • **LOW**

Field	Type	Description
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
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

Field	Type	Description
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
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

Field	Type	Description
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
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

10 System Management

10.1 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.

NOTE

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

Prerequisites

The SMN service has been enabled.

Attack Alarms

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

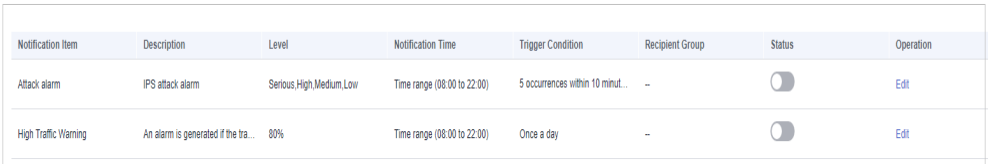
Step 2 Click  in the upper left corner of the management console and select a region or project.

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

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

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

Figure 10-1 Alarm notifications



Step 6 In the **Operation** column of **Attack alarm**, click **Edit**, and configure notification item parameters. For details, see **Table 10-1**.

Figure 10-2 Notification item settings - attack alarm

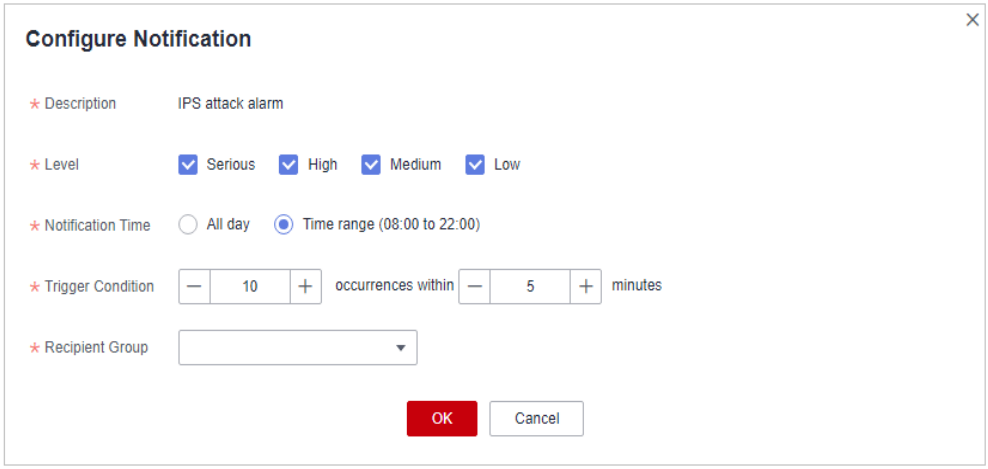


Table 10-1 Attack alarm parameters

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

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

Step 7 Click **OK**.

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

----End

High Traffic Warning

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

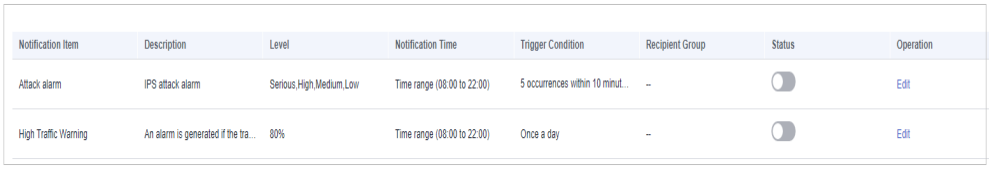
Step 2 Click  in the upper left corner of the management console and select a region or project.

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

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

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

Figure 10-3 Alarm notifications



Step 6 In the **Operation** column of **High Traffic Warning**, click **Edit**, and configure notification item parameters. For details, see **Table 10-2**.

Figure 10-4 Notification item settings - high traffic warning

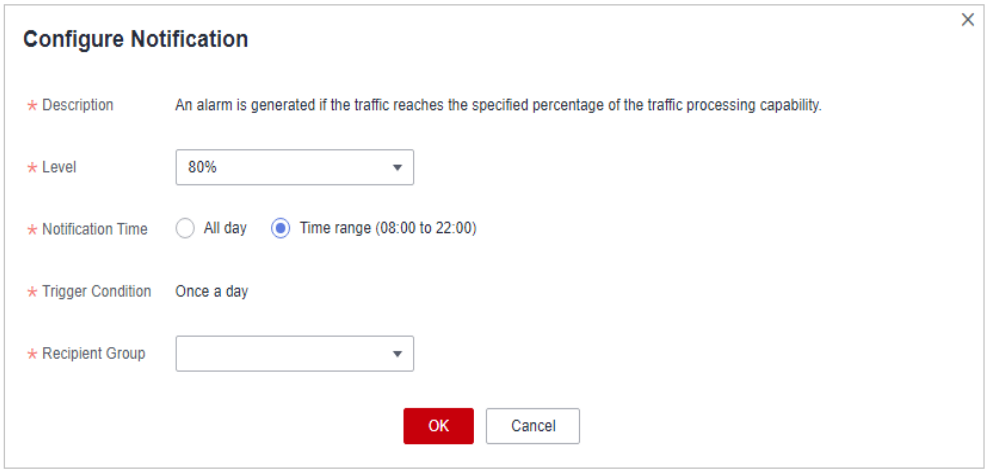


Table 10-2 High traffic warning parameters

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

Step 7 Click **OK**.

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

----End

EIP Not Protected

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

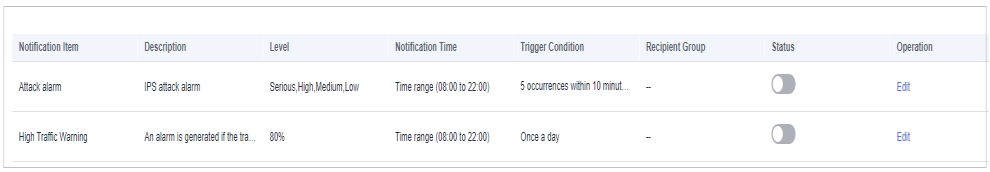
Step 2 Click in the upper left corner of the management console and select a region or project.

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

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

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

Figure 10-5 Alarm notifications



Step 6 In the **Operation** column of the **EIP Not Protected** alarm, click **Edit**, and configure notification item parameters. For details, see **Table 10-3**.

Figure 10-6 Notification settings - EIP Not Protected

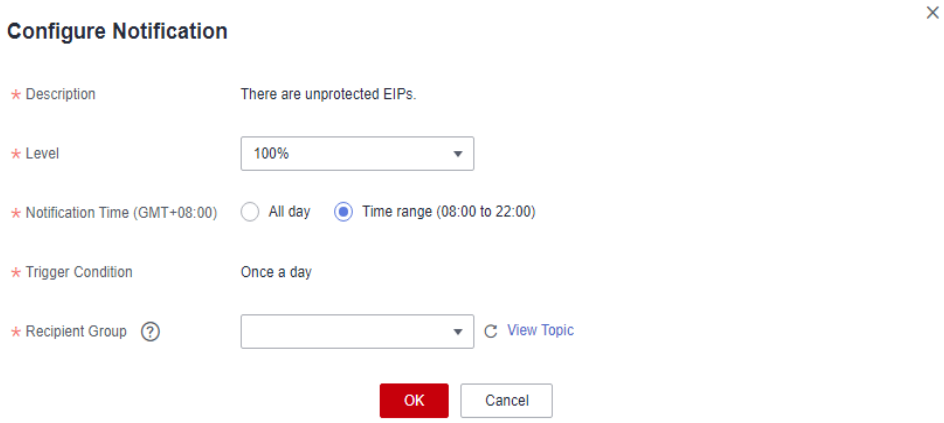


Table 10-3 Parameters of the alarm **EIP Not Protected**

Parameter	Description
Description	This alarm indicates there are unprotected EIPs.
Level	The default value is **100%**.
Notification Time	Select a time range for sending notifications.
Trigger Condition	Once a day
Recipient Group	Select a topic from the drop-down list to configure the endpoints for receiving alarm notifications.

Step 7 Click **OK**.

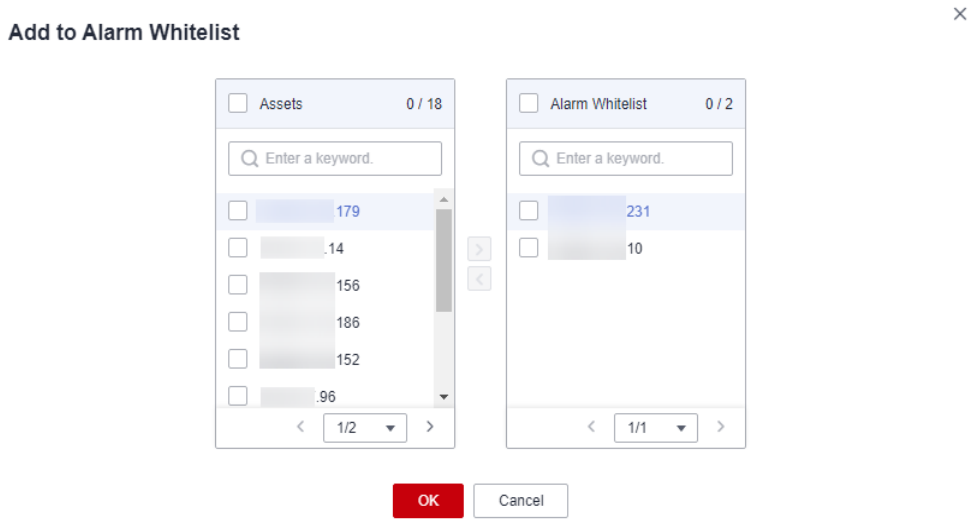
Step 8 In the **Status** column of **EIP Not Protected**, click  to enable it.

----End

Related Operations

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

Figure 10-7 Add to Alarm Whitelist



10.2 Network Packet Capture

10.2.1 Creating a Packet Capture Task to Check the Network Status

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

Specification Limitations

Only the professional edition instances can capture network packets.

Constraints

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

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

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

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

Figure 10-8 Creating a packet capture task

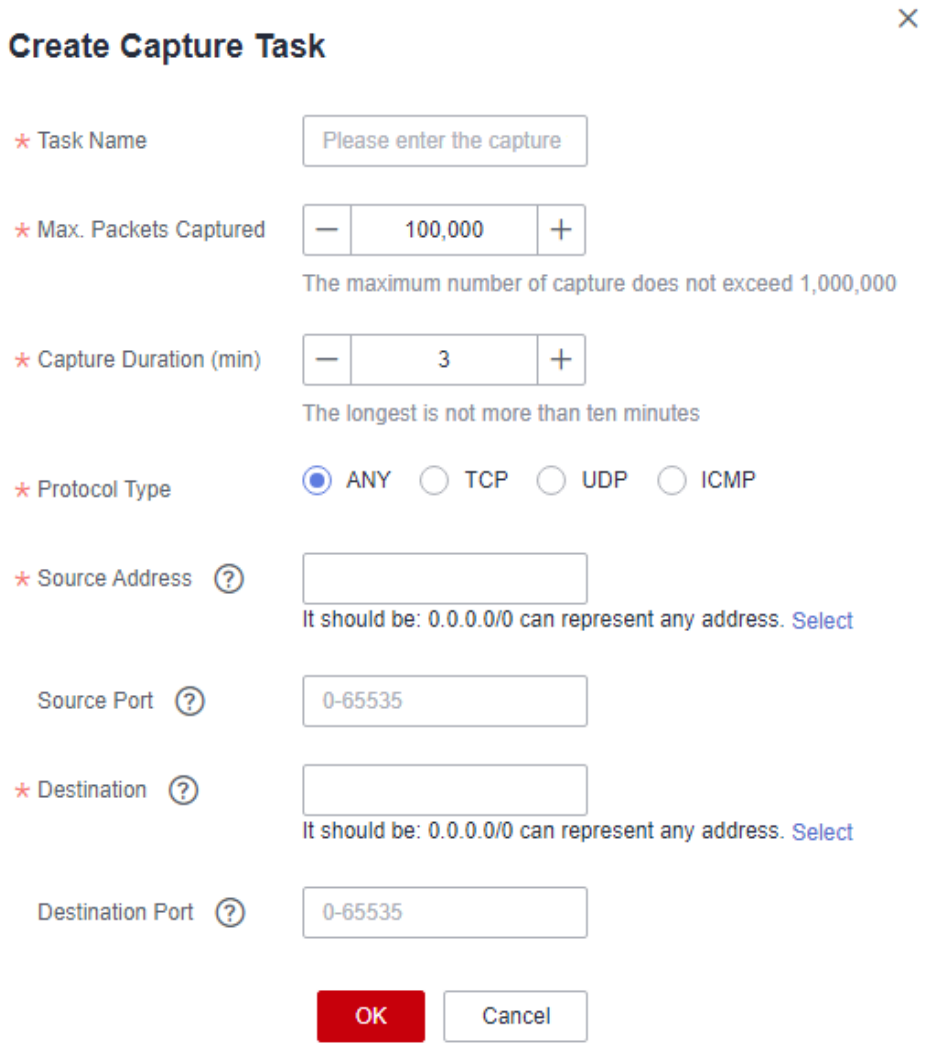


Table 10-4 Packet capture task parameters

Parameter Name	Description	Example Value
Task Name	Task name. It must meet the following requirements: • Only uppercase letters (A to Z), lowercase letters (a to z), numbers (0 to 9), and the following special characters are allowed: -_ • Enter up to 30 characters.	cfw
Max. Packets Captured	Maximum number of captured packets. Enter an integer in the range 1 to 1,000,000.	100000
Capture Duration (min)	Maximum duration for capturing packets. Enter an integer in the range 1 to 10.	3
Protocol Type	Protocol type of captured packets. It can be: • Any • TCP • UDP • ICMP	Any
Source Address	It can be: • A single IP address, for example, **192.168.10.5** • Consecutive IP addresses, for example, **192.168.0.2-192.168.0.10** • Address segment, for example, **192.168.2.0/24**	192.168.10.5
Source Port	(Optional) Source port. The input rules are as follows: • If this parameter is left blank, it indicates all port numbers (1 to 65535). • Enter a single port number in the range 1 to 65535.	80

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

Step 7 Click **OK**.

----End

Related Operations

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

10.2.2 Viewing a Packet Capture Task

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

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

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

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

Step 7 Check the packet capture task. For more information, see **Table 10-5**

Table 10-5 Packet capture task parameters

Parameter Name	Description
Task Name	Task name
Status	Task status. • **Running**: The packet capture command has been delivered and the task is in progress. • **Completed**: The packet capture result has been uploaded and the task is complete. • **Exception**: Packet capture data upload times out due to network problems, and some packet capture results are lost. **NOTE** To retry a task, you can click **Copy** in its **Operation** column to create and execute it again. • **Stopping**: The task is being stopped and the packet capture result is being uploaded. • **Expired**: The packet capture result has been uploaded and the task has been manually stopped.
Protocol Type	Protocol type specified for packet capture.
IP Address	IP addresses specified for packet capture, including the source and destination addresses.
Port	Ports specified for packet capture, including the source and destination ports.
Max. Packets Captured	Maximum number of captured packets in the current task.
Packet Capture Time	Start time and end time of a packet capture task.
Capture Duration (min)	Duration of packet capture.
Remaining Retention Period (Days)	Number of days for storing a packet capture task. The default value is 7.
Capture Size	Size of captured packets.

----End

Related Operations

- To copy a task, click **Copy** in its **Operation** column. In the displayed dialog box, enter the task name and click **OK**.
- To stop a packet capture task, click **Stop** in its **Operation** column.
- To delete packet capture tasks, select them and click **Delete** above the list.
- **10.2.1 Creating a Packet Capture Task to Check the Network Status**
- **10.2.3 Downloading Packet Capture Results**

10.2.3 Downloading Packet Capture Results

Constraints

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

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

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

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

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

NOTE

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

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

Step 7 Obtain the packet capture result.

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

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

NOTE

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

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

----End

10.3 Configuring a DNS Server

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

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

Constraints

A maximum of two DNS servers can be customized.

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

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

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

NOTE

Currently, only two specified DNS servers can be added.

Step 7 Click **Apply**.

NOTE

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

----End

10.4 Security Report Management

10.4.1 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) If the current account has only one firewall instance, the firewall details page is displayed. If there are multiple firewall instances, click **View** in the **Operation** column of a firewall to go to its details page.

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

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

Table 10-6 Parameters of the security report template

Parameter	Description
Report Name	Name of the custom security report

Parameter	Description
Report Type	• **Daily** Statistical period: 00:00:00 to 24:00:00 every day A report will be sent to the recipients the day after it is generated. • **Weekly** Statistical period: 00:00:00 on Monday to 24:00:00 on Sunday A report will be sent to the recipients at the specified time after it is generated. • **Custom**: Customize a time range. **Statistical Period**: Configure a statistical period for your report. A report will be sent to the specified recipients after it is generated.
Statistical Period	If **Report Type** is set to **Custom**, you need to set **Statistical Period**.
Report Schedule	When **Report Type** is set to **Daily** or **Weekly**, you need to set the report sending time. By default, the log report of the previous statistical period is sent. **NOTE** To ensure correctness, the report sending time may be delayed.
Recipient Group	Select a topic from the drop-down list to configure the endpoints for receiving the log report.

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

----End

10.4.2 Viewing/Downloading a Security Report

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

Viewing/Downloading the Latest Security Report

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

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

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

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

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

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

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

----End

Viewing/Downloading Historical Security Report

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

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

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

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

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

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

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

10.4.3 Managing Security Reports

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

Enabling/Disabling the Security Report Function

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

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

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

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

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

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

-  : enabled
-  : disabled

----End

Modifying a Security Report

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

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

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

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

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

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

Table 10-7 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.

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

----End

Deleting a Security Report

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

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

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

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

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

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

----End

11 Viewing Audit Logs

11.1 Operations Recorded by CTS

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

CFW operations recorded by CTS lists details about the CFW operations on CTS.

Table 11-1 CFW operations recorded by CTS

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

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

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

11.2 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)**.

12 Viewing Monitoring Metrics

12.1 CFW Monitored Metrics

Description

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

Namespace

SYS.CFW

NOTE

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

Metrics

Table 12-1 CFW metrics

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

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

Dimension

Key	Value
fw_instance_id	Firewall ID

12.2 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 .

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

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

----End

12.3 Viewing Monitoring Metrics

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

Prerequisites

CFW alarm rules have been configured in Cloud Eye. For more details, see **12.2 Configuring Alarm Monitoring Rules**.

Viewing Monitoring Metrics

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

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

Step 3 Hover your mouse over  in the upper left corner of the page and choose **Management & Governance** > **Cloud Eye**.

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

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

----End

