

Alibaba Cloud

Cloud Firewall Overview

Document Version: 20220620

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).
5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
 Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
<code>Courier font</code>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

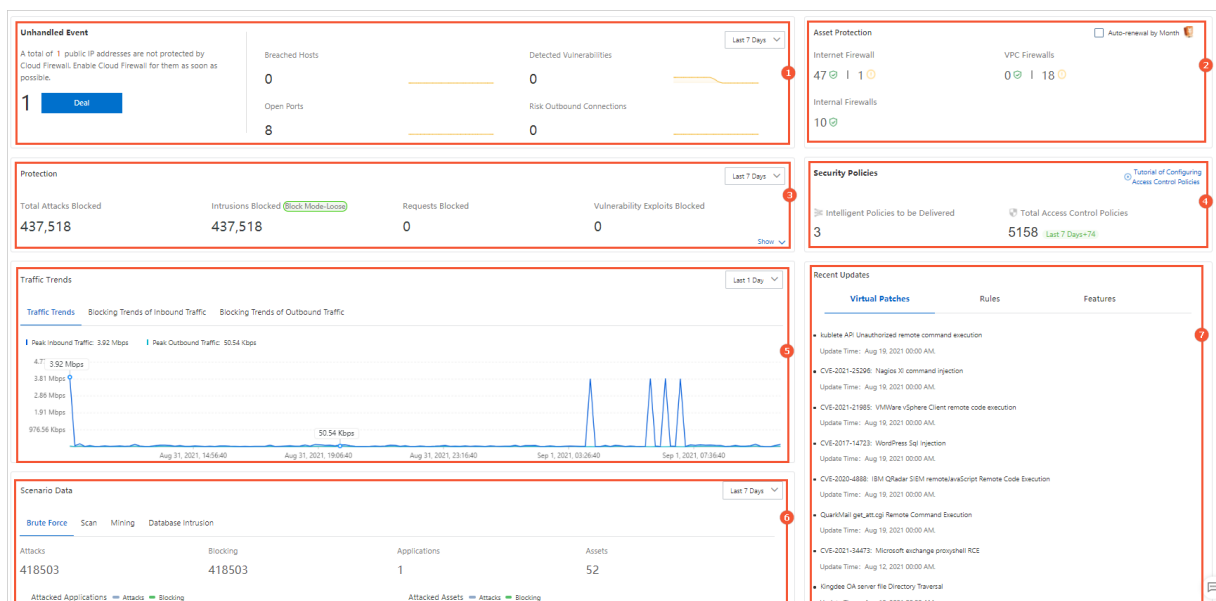
1.Overview	05
2.Traffic topology visualization	09
3.Authorize Cloud Firewall to access other cloud resources	11
4.Upgrade and renewal	18

1. Overview

The Overview page of the Cloud Firewall console displays the overall protection capabilities and statistics on your Cloud Firewall. The statistics include unhandled events, protected assets, security protection data, security policies, traffic trends, scenario-specific data, and recent updates. On the Overview page, you can obtain the overall security status of your network assets.

Go to the Overview page

Log on to the [Cloud Firewall console](#). In the left-side navigation pane, click **Overview**. The **Overview** page appears, as shown in the following figure.

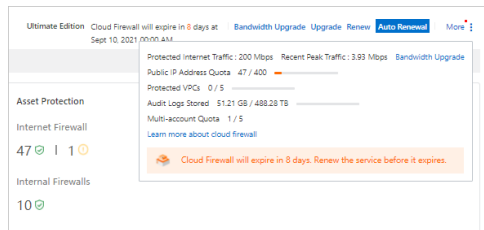


The **Overview** page consists of seven sections. You can click the following links to view the individual sections:

- [Unhandled Event](#) (marked by 1)
- [Asset Protection](#) (marked by 2)
- [Protection](#) (marked by 3)
- [Security Policies](#) (marked by 4)
- [Traffic Trends](#) (marked by 5)
- [Scenario Data](#) (marked by 6)
- [Recent Updates](#) (marked by 7)

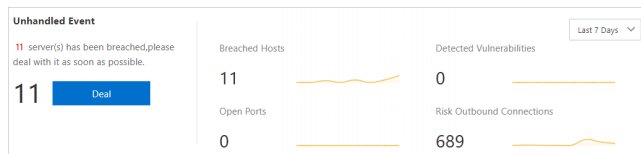
In the upper-right corner of the **Overview** page, you can view the edition and remaining validity period of your Cloud Firewall. You can also perform the following operations:

- Click **Bandwidth Upgrade**, **Upgrade**, **Renew**, or **Auto Renewal** to perform specific operations. For more information, see [Upgrade and renewal](#).
- Click **More** to view the details of your Cloud Firewall. The details include **Protected Internet Traffic**, **Recent Peak Traffic**, **Public IP Address Quota**, **Protected VPCs**, **Audit Logs Stored**, and **Multi-account Quota**.



Unhandled Event

This section displays the following information about your assets: **Breached Hosts**, **Detected Vulnerabilities**, **Open Ports**, and **Risk Outbound Connections**.



In this section, you can perform the following operations:

- Specify a time range for a query: In the upper-right corner of the section, click the time drop-down list and select a specific time range. Available options are **Last 1 Day** and **Last 7 Days**.
- Handle an exception event: Move the pointer over a specific type of exception event and click **Handle Now**. On the page that appears, you can view and handle the exception events of this type. For example, click **Handle Now** for **Risk Outbound Connections**. The **Outbound Connections** page appears, and you can handle the exception events of this type.

For more information about how to handle different types of exception events, see the following topics:

- [Breach awareness](#)
- [Vulnerability protection](#)
- [Internet access](#)
- [Outbound connections](#)

Asset Protection

This section displays the protection status of your assets. In this section, you can view the number of public IP addresses that are protected by the **Internet firewall**, **virtual private cloud (VPC) firewalls**, or **internal firewalls**. You can also view the number of public IP addresses that are not protected by these firewalls.

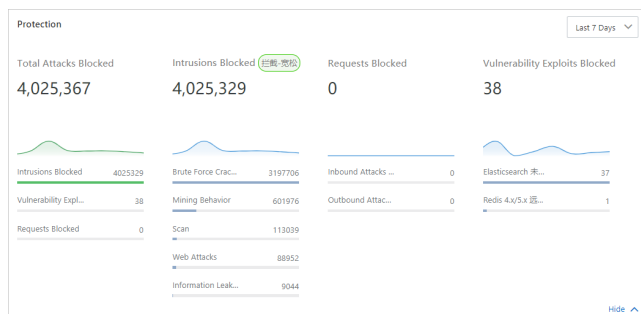


In the upper-right corner of this section, select **Auto-renewal by Month** to enable Cloud Firewall to continuously protect your network assets.

If an asset is not protected, you can enable the required firewall on the **Firewall Settings** page of the . For more information, see [互联网边界防火墙](#) and [Enable or disable VPC Firewall](#).

Protection

This section displays the numbers of times that specific modules are triggered to protect your assets. In this section, you can view **Total Attacks Blocked**, **Intrusions Blocked**, **Requests Blocked**, and **Vulnerability Exploits Blocked**.



In this section, you can perform the following operations:

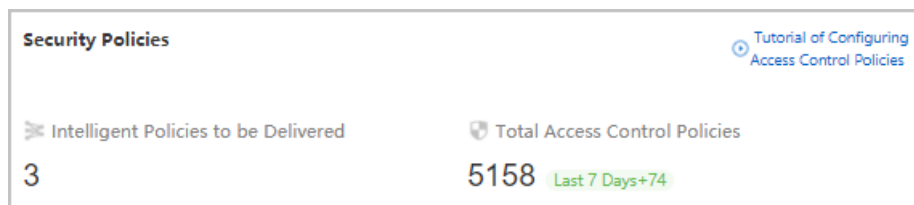
- Specify a time range for a query: In the upper-right corner of the section, click the time drop-down list and select a specific time range. Available options are **Last 1 Day** and **Last 7 Days**.
- View details: Click **Show** in the lower-right corner to view the statistics on different protection modules.

For more information about the protection modules, see the following topics:

- [Intrusion prevention](#)
- [Overview of access control policies](#)
- [Vulnerability protection](#)

Security Policies

This section displays the statistics on access control policies. In this section, you can view **Intelligent Policies to be Delivered** and **Total Access Control Policies**. You can also view the change in Total Access Control Policies from the last seven days.



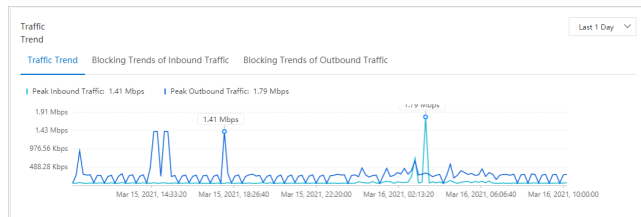
You can click the number below **Intelligent Policies to be Delivered**. The **Intelligent Policy Recommendation** panel of the **Access Control** page appears. In this panel, you can view and apply the intelligent policies that are recommended by Cloud Firewall. For more information, see [Apply intelligent policies](#).

You can click the number below **Total Access Control Policies**. The **Access Control** page appears. On this page, you can view and manage access control policies.

In the upper-right corner of this section, you can click **Tutorial of Configuring Access Control Policies** to view the video of **Configure Access Control Policies for the Internet Firewall**.

Traffic Trends

This section displays the trends in the overall traffic of your assets that are protected by Cloud Firewall, as well as the changes in the sessions whose inbound or outbound traffic is blocked by Cloud Firewall.

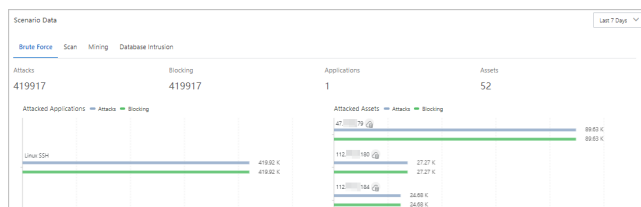


In this section, you can perform the following operations:

- Specify a time range for a query: In the upper-right corner of the section, click the time drop-down list and select a specific time range. Available options are **Last 1 Day** and **Last 7 Days**.
- View a specific trend: Click the **Traffic Trends**, **Blocking Trends of Inbound Traffic**, or **Blocking Trends of Outbound Traffic** tab to view the specific trend.

Scenario Data

This section displays the information about brute-force attacks, scanning risks, mining activities, and database intrusions that Cloud Firewall detects on your assets.



In this section, you can perform the following operations:

- Specify a time range for a query: In the upper-right corner of the section, click the time drop-down list and select a specific time range. Available options are **Last 1 Day** and **Last 7 Days**.
- View the data of a specific scenario: Click the **Brute Force**, **Scan**, **Mining**, or **Database Intrusion** tab to view the data of a specific scenario. The following list describes the data on each tab:
 - **Brute Force**: displays the statistics on brute-force attacks and the rankings of attacked applications and assets. The statistics include **Attacks**, **Blocking**, **Applications**, and **Assets**.
 - **Scan**: displays the statistics on scanning risks and the rankings of scanned applications and assets. The statistics include **Attacks**, **Blocking**, **Applications**, and **Assets**.
 - **Mining**: displays the statistics on mining programs and the rankings of attacked applications and assets. The statistics include **Attacks**, **Blocking**, **Applications**, and **Assets**.
 - **Database Intrusion**: displays the statistics on database intrusions and the rankings of attacked applications and assets. The statistics include **Attacks**, **Blocking**, **Applications**, and **Assets**.

Recent Updates

This section displays the update records of **virtual patches**, **rules**, and **features** of Cloud Firewall.

Recent Updates	
Virtual Patches	Rules
<ul style="list-style-type: none"> • CVE-2021-25283: SaltStack wheel_async Unauthorized File Upload Update Time: 2021-02-26 • Weaver-OA validate.jsp capitalid Sql Injection Update Time: 2021-02-25 • CVE-2020-10220: rConfig commands.inc.php SQL injection Update Time: 2021-02-25 	
Features	

You can click the **Virtual Patches**, **Rules**, or **Features** tab to view specific update records.

2.Traffic topology visualization

The traffic topology visualization feature allows you to view the traffic topologies of cloud assets that are protected by Cloud Firewall. The topologies display traffic of cloud assets at the Internet and virtual private cloud (VPC) boundaries.

Supported editions

The traffic topology visualization feature is available only in the Enterprise Edition and Ultimate Edition of Cloud Firewall.

Access the Traffic Topology Visualization tab

Log on to the [Cloud Firewall console](#). On the **Overview** page, click the **Traffic Topology Visualization** tab.

Overview

The Overview section displays **Public IP Address**, **vpc**, **Traffic**, and **Intrusion Prevention Mode**.

You can view the following information in the Overview section:

- **Public IP Address:**

- **Total IP Addresses:** the total number of public IP addresses of the assets within the current Alibaba Cloud account.
- **Unprotected IP Addresses:** the total number of IP addresses for which the Internet firewall is disabled.

You can click **Enable Firewall** to go to the **Internet Firewall** tab of the **Firewall Settings** page. On the Internet Firewall tab, enable the Internet firewall for the IP addresses that are not protected.

- **vpc:**

- **Total VPCs:** the total number of VPCs that are attached to Cloud Enterprise Network (CEN) instances and VPCs that are connected by using Express Connect circuits within the current Alibaba Cloud account.
- **Unprotected VPCs:** the number of VPCs that are not protected by Cloud Firewall.


You can click **Enable Firewall** to go to the **VPC Firewall** tab of the **Firewall Settings** page. On the VPC Firewall tab, you can enable the firewalls for the VPCs that are not protected.

- **Traffic:**

- **Peak Traffic in Last 7 Days:** the peak value of traffic that is protected by Cloud Firewall within the previous seven days.
- **Peak Outbound Traffic:** the peak value of outbound traffic that is protected by Cloud Firewall within the previous seven days.
- **Peak Inbound Traffic:** the peak value of inbound traffic that is protected by Cloud Firewall within the previous seven days.

- **Intrusion Prevention Mode:**

The value below Intrusion Prevention Mode is synchronized from the **Prevention Configuration** page. For more information, see [防护配置](#).

 **Notice** After Cloud Firewall is activated, **Block Mode** is enabled by default. Cloud Firewall automatically determines the level based on your traffic condition. The threat intelligence, basic protection, and virtual patching modules block threats only after you enable **Monitor Mode**. If you do not enable **Monitor Mode**, the modules only monitor threats and malicious traffic.

- **Attack:**
 - **Blocked Attacks:** the number of attacks that are blocked by Cloud Firewall.
 - **Total Attacks:** the total number of attacks on the cloud assets that are protected by Cloud Firewall.
- **ACL:** the number of created access control policies.

Internet Firewall

The Internet Firewall section displays the topology of traffic between the Internet assets within the current Alibaba Cloud account and the Internet.

You can perform the following operations in this section:





- You can click the icon of a cloud asset to view the public IP address of the asset. You can view **Unprotected IP Address** and **Protected IP Address** on the left side of the page.
- You can click an IP address to view the details about the inbound and outbound traffic of the IP address on the left side of the page.

On the **Inbound** tab, you can view the following information: **IP**, **Open Port**, **Intelligent Policy Recommended**, and **Access Control Policy**.

On the **Outbound** tab, you can view the following information: **Outbound Domain**, **Outbound IP Address**, **Intelligent Policy Recommended**, and **Access Control Policy**.

VPC Firewall

The VPC Firewall section displays the **All VPCs** and **Connected VPC** tabs.

- **All VPCs:** This tab displays the VPCs that are connected by using Express Connect circuits within the current Alibaba Cloud account and the VPCs that are attached to CEN instances. The  icon indicates a protected VPC, and the  icon indicates an unprotected VPC. You can move the pointer over a VPC to view the detailed information about the VPC.
- **Connected VPC:** This tab displays the details about the VPCs that are connected by using Express Connect circuits and the VPCs that are attached to CEN instances. The  icon indicates a VPC that is connected by using an Express Connect circuit. The  icon indicates a VPC that is attached to a CEN instance. You can click **Show** to view the traffic topologies between VPCs.

You can view the total number of the VPCs that are connected by using Express Connect circuits, the VPCs that are attached to CEN instances, and all connected VPCs on the left side of the page. You can click the name of a VPC to view the specific traffic topology.

3. Authorize Cloud Firewall to access other cloud resources

The first time you log on to the Cloud Firewall console, you must authorize your Cloud Firewall to access the other cloud resources within your account before you can use features provided by Cloud Firewall. This topic describes how to authorize Cloud Firewall by using the AliyunServiceRoleForCloudFW service-linked role and how to delete this role.

Prerequisites

An Alibaba Cloud account or a Resource Access Management (RAM) user that has permissions to create or delete service-linked roles is used.


For more information about how to grant RAM users the permissions on service-linked roles, see [FAQ](#).

Context

To provide features such as access control, monitoring, and analysis on cloud traffic, Cloud Firewall must access the other cloud resources within your account, such as ECS instances, VPCs, SLB instances, Log Service, bastion hosts, CEN instances, Security Center, and ApsaraDB RDS instances. You can use the AliyunServiceRoleForCloudFW service-linked role to authorize Cloud Firewall. This role is automatically created. You do not need to manually create or modify a service-linked role. For more information, see [Service-linked roles](#).

Procedure

- 1.
2. In the **Service-Linked Role for Cloud Firewall** dialog box, click **OK**.

 **Note** If the AliyunServiceRoleForCloudFW service-linked role is created, the dialog box does not appear, and you can directly use Cloud Firewall in the console.

After you click **OK**, Alibaba Cloud automatically creates the AliyunServiceRoleForCloudFW service-linked role.

You can view the service-linked role on the **RAM Roles** page of the [RAM console](#). Your Cloud Firewall can access the other cloud resources within your account only after the AliyunServiceRoleForCloudFW service-linked role is created. The resources include ECS instances, VPCs, SLB instances, Log Service, bastion hosts, CEN instances, Security Center, and ApsaraDB RDS instances.

Create RAM Role AliyunServiceRoleForCloudFW			
RAM Role Name	Note	Created	Actions
AliyunServiceRoleForCloudFW (Service Linked Role)	Service Linked Role for CloudFW. CloudFW will use this role to access your resources in other services.	Jun 16, 2021, 15:39:54	Delete

Permissions of the AliyunServiceRoleForCloudFW service-linked role

By default, the AliyunServiceRoleForCloudFW service-linked role is attached with the AliyunServiceRolePolicyForCloudFW policy. The following code block provides the permissions defined in the AliyunServiceRolePolicyForCloudFW policy:

```
{
  "Version": "1",
```

```

    "Statement": [
      {
        "Action": [
          "ecs:DescribeInstances",
          "ecs:DescribeTags",
          "ecs:JoinSecurityGroup",
          "ecs:LeaveSecurityGroup",
          "ecs:AuthorizeSecurityGroupEgress",
          "ecs:DescribeRegions",
          "ecs:DescribeVpcs",
          "ecs:RevokeSecurityGroupEgress",
          "ecs:ModifySecurityGroupAttribute",
          "ecs>DeleteSecurityGroup",
          "ecs:RevokeSecurityGroup",
          "ecs:DescribeSecurityGroupAttribute",
          "ecs:CreateSecurityGroup",
          "ecs:AuthorizeSecurityGroup",
          "ecs:DescribeSecurityGroups",
          "ecs:DescribeSecurityGroupReferences",
          "ecs:ModifySecurityGroupPolicy",
          "ecs:ModifySecurityGroupRule",
          "ecs:ModifySecurityGroupEgressRule",
          "ecs:CreateNetworkInterface",
          "ecs>DeleteNetworkInterface",
          "ecs:DescribeNetworkInterfaces",
          "ecs:CreateNetworkInterfacePermission",
          "ecs:DescribeNetworkInterfacePermissions",
          "ecs>DeleteNetworkInterfacePermission",
          "ecs:AttachNetworkInterface",
          "ecs:DetachNetworkInterface"
        ],
        "Resource": "*",
        "Effect": "Allow"
      },
      {
        "Action": [
          "vpc:DescribeVpcs",
          "vpc:DescribeNatGateways",
          "vpc:DescribeSnatTableEntries",
          "vpc:DescribeForwardTableEntries",
          "vpc:DescribeBandwidthPackages",
          "vpc:DescribeEipAddresses",
          "vpc:DescribeRouterInterfaces",
          "vpc:DescribeRouteTableList",
          "vpc:DescribeRouteTables",
          "vpc:DescribeVSwitches",
          "vpc:CreateRouteEntry",
          "vpc>DeleteRouteEntry",
          "vpc:CreateVpc",
          "vpc>DeleteVpc",
          "vpc:CreateVSwitch",
          "vpc>DeleteVSwitch",
          "vpc:DescribeZones",
          "vpc:CreateVirtualBorderRouter",

```

```

        "vpc:ConnectRouterInterface",
        "vpc:ModifyRouterInterfaceAttribute",
        "vpc>DeleteRouterInterface",
        "vpc>CreateRouterInterface",
        "vpc>DeleteVirtualBorderRouter",
        "vpc:DeactivateRouterInterface",
        "vpc:DescribeVirtualBorderRouters",
        "vpc:DescribePhysicalConnections",
        "vpc:ModifyVirtualBorderRouterAttribute",
        "vpc:DescribeVpcAttribute",
        "vpc:DescribeVSwitchAttributes",
        "vpc:DescribeHaVips",
        "vpc:DescribeVpnConnections",
        "vpc:DescribeVpnRouteEntries",
        "vpc:DescribeVpnPbrRouteEntries",
        "vpc:DescribeVpnGateways",
        "vpc:DescribeSslVpnServers",
        "vpc:AssociateEipAddress",
        "vpc:UnassociateEipAddress",
        "vpc>CreateRouteTable",
        "vpc>DeleteRouteTable",
        "vpc:AssociateRouteTable",
        "vpc:UnassociateRouteTable",
        "vpc>CreateSnatEntry",
        "vpc>DeleteSnatEntry",
        "vpc:DescribeSnatTableEntries",
        "vpc:DescribeRouteEntryList"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "slb:DescribeRegions",
        "slb:DescribeLoadBalancers",
        "slb:DescribeLoadBalancerAttribute",
        "slb:DescribeLoadBalancerUDPListenerAttribute",
        "slb:DescribeLoadBalancerTCPListenerAttribute",
        "slb:DescribeLoadBalancerHTTPListenerAttribute",
        "slb:DescribeLoadBalancerHTTPSListenerAttribute",
        "slb:DescribeHealthStatus",
        "slb:DescribeAccessControlListAttribute"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "log:PostLogStoreLogs",
        "log:GetProject",
        "log:ListProject",
        "log:GetLogStore",
        "log:ListLogStores",
        "log:CreateLogStore",

```

```

        "log:CreateProject",
        "log:GetIndex",
        "log:CreateIndex",
        "log:UpdateIndex",
        "log:CreateDashboard",
        "log:ClearLogStoreStorage",
        "log:UpdateLogStore",
        "log:UpdateDashboard",
        "log:CreateSavedSearch",
        "log:UpdateSavedSearch",
        "log:DeleteLogStore",
        "log:DeleteSavedSearch",
        "log:GetSavedSearch",
        "log:ListSavedSearch",
        "log:DeleteDashboard",
        "log:GetDashboard",
        "log:ListDashboard"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "yundun-bastionhost:DescribeInstance",
        "yundun-bastionhost:DescribeRegions",
        "yundun-bastionhost:DescribeInstances",
        "yundun-bastionhost:DescribeInstanceBastionhost",
        "yundun-bastionhost:DescribeInstanceAttribute"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "cen:DescribeCens",
        "cen:DescribeCenAttachedChildInstances",
        "cen:DescribeCenAttachedChildInstanceAttribute",
        "cen:AttachCenChildInstance",
        "cen:DetachCenChildInstance",
        "cen:PublishRouteEntries",
        "cen:WithdrawPublishedRouteEntries",
        "cen:DescribePublishedRouteEntries",
        "cen:DescribeCenRegionDomainRouteEntries",
        "cen:ModifyCenAttribute",
        "cen:CreateCenRouteMap",
        "cen:DeleteCenRouteMap",
        "cen:ModifyCenRouteMap",
        "cen:DescribeCenRouteMaps",
        "cen:DescribeCenChildInstanceRouteEntries",
        "cen:CreateCenChildInstanceRouteEntryToCen",
        "cen:DeleteCenChildInstanceRouteEntryToCen",
        "cen:ListTransitRouters",
        "cen:CreateTransitRouter",
        "cen:DeleteTransitRouter",
    ]
}

```

```

        "cen:ListTransitRouterAttachments",
        "cen:CreateTransitRouterVpcAttachment",
        "cen:DeleteTransitRouterVpcAttachment",
        "cen:UpdateTransitRouterVpcAttachmentAttribute",
        "cen:UpdateTransitRouterPeerAttachmentAttribute",
        "cen:CreateTransitRouterVbrAttachment",
        "cen:DeleteTransitRouterVbrAttachment",
        "cen:ListTransitRouterPeerAttachments",
        "cen:ListTransitRouterVpcAttachments",
        "cen:ListTransitRouterVbrAttachments",
        "cen:ListTransitRouterAvailableResource",
        "cen:CreateTransitRouterRouteTable",
        "cen:UpdateTransitRouterRouteTable",
        "cen:DeleteTransitRouterRouteTable",
        "cen:ListTransitRouterRouteTables",
        "cen:CreateTransitRouterRouteEntry",
        "cen:DeleteTransitRouterRouteEntry",
        "cen:ListTransitRouterRouteEntries",
        "cen:ListTransitRouterRouteTableAssociations",
        "cen:AssociateTransitRouterAttachmentWithRouteTable",
        "cen:DissociateTransitRouterAttachmentFromRouteTable",
        "cen:ListTransitRouterRouteTablePropagations",
        "cen:EnableTransitRouterRouteTablePropagation",
        "cen:DisableTransitRouterRouteTablePropagation",
        "cen:ModifyCenUserQuota"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "netana:DescribeNetworkQuotas",
        "netana:DescribeNetworkQuotaRequestResult",
        "netana:CreateNetworkQuotaRequest"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "yundun-sas:DescribeVulList",
        "yundun-sas:DescribeVulDetails"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "rds:DescribeDBInstances"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": "ecs:CreateSecurityGroup"
}

```

```
{
  "Action": "ram:CreateServiceLinkedRole",
  "Resource": "*",
  "Effect": "Allow",
  "Condition": {
    "StringEquals": {
      "ram:ServiceName": "cen.aliyuncs.com"
    }
  }
},
{
  "Action": [
    "resourcemanager:ListAccounts"
  ],
  "Resource": "*",
  "Effect": "Allow"
},
{
  "Action": "ram>DeleteServiceLinkedRole",
  "Resource": "*",
  "Effect": "Allow",
  "Condition": {
    "StringEquals": {
      "ram:ServiceName": "cloudfw.aliyuncs.com"
    }
  }
}
]
```

For more information about the policy syntax, see [Policy elements](#).

Delete a service-linked role

If you no longer use Cloud Firewall, you can delete the AliyunServiceRoleForCloudFW service-linked role. Before you can delete the service-linked role, make sure that your Cloud Firewall expires and is automatically released. After your Cloud Firewall is released, perform the following steps:

1. Log on to the [RAM console](#).
2. In the left-side navigation pane, click **RAM Roles**.
3. Search for the AliyunServiceRoleForCloudFW service-linked role and click **Delete** in the Actions column.
4. Click **OK**.

FAQ

Why is the AliyunServiceRoleForCloudFW service-linked role not automatically created for my RAM user?

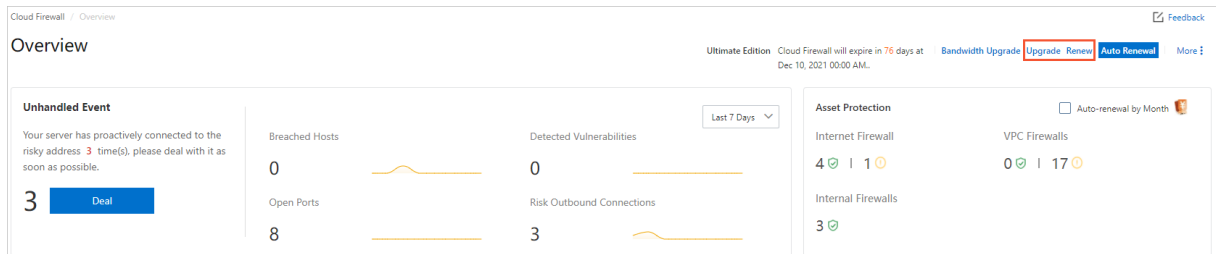
The AliyunServiceRoleForCloudFW service-linked role can be automatically created or deleted only if your RAM user has the required permissions. To obtain the permissions, you must attach the following policy to your RAM user. For more information, see [Grant permissions to a RAM role](#).


```
{
  "Statement": [
    {
      "Action": [
        "ram:CreateServiceLinkedRole"
      ],
      "Resource": "acs:ram:*:Alibaba Cloud account ID:role/*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": [
            "cloudfw.aliyuncs.com"
          ]
        }
      }
    }
  ],
  "Version": "1"
}
```

4. Upgrade and renewal

Cloud Firewall has the Premium Edition, Enterprise Edition, and Ultimate Edition. You can upgrade your Cloud Firewall to the required edition to use more features.

To upgrade or renew your Cloud Firewall, you can click **Upgrade** or **Renew** in the upper-right corner of the **Overview** page in the Cloud Firewall console.



For more information about the features that are supported by different editions, see [Features](#).

For more information about how to upgrade and renew Cloud Firewall, see [Renew the subscription to Cloud Firewall](#).

Note We recommend that you renew your Cloud Firewall before it expires for Cloud Firewall to protect your network as expected.