

Alibaba Cloud

Cloud Firewall FAQ

Document Version: 20220701

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.Relationships between Cloud Firewall and other Alibaba Cloud...	05
2.FAQ about bandwidth supported by Cloud Firewall	06
3.What are the differences between Cloud Firewall and ECS secu...	07
4.FAQ about Cloud Firewall authorization	08
5.FAQ about network traffic analysis	09
6.FAQ about access control policies	12
7.FAQ about the Internet firewall	14
8.FAQ about VPC Firewall	17
9.FAQ about Cloud Firewall logs	18
10.How do I troubleshoot network connection failures?	19
11.What are the priorities of rules that are used by Cloud Firew...	20
12.Why am I unable to activate Cloud Firewall for my account?	21
13.Why are ICMP detection packets periodically sent by Cloud Fi...	23
14.FAQ about firewall protection for some public IP addresses of...	24

1. Relationships between Cloud Firewall and other Alibaba Cloud services

Position of Cloud Firewall in the Alibaba Cloud architecture

Cloud Firewall provides the following types of firewalls:

- **Internet firewall:** The Internet firewall is deployed in front of elastic IP addresses (EIPs) and serves as the first protection node for the outbound traffic from an EIP to the Internet. The Internet firewall is used to control the traffic of the EIPs. Cloud Firewall Premium Edition, Enterprise Edition, and Ultimate Edition support the Internet firewall.
- **VPC firewall:** A virtual private cloud (VPC) firewall is deployed between VPCs to control the traffic of the private IP addresses of Elastic Compute Service (ECS) instances. Cloud Firewall Enterprise Edition and Ultimate Edition support VPC firewalls.
- **Internal firewall:** An internal firewall serves as a security group to control inbound and outbound traffic between ECS instances. Cloud Firewall Enterprise Edition and Ultimate Edition support internal firewalls.

Relationship between Cloud Firewall and other security services such as WAF and Anti-DDoS Pro or Anti-DDoS Premium

The preceding figure shows the relationships between Cloud Firewall and other security services such as Web Application Firewall (WAF) and Anti-DDoS Pro or Anti-DDoS Premium. Cloud Firewall protects the origin IP addresses of both WAF instances and Anti-DDoS Pro or Anti-DDoS Premium instances.

Relationship between Cloud Firewall and CDN

When you use Cloud Firewall together with Alibaba Cloud Content Delivery Network (CDN), Cloud Firewall protects the origin IP addresses of CDN edge nodes.

Relationship between Cloud Firewall and OSS or ApsaraDB RDS

You cannot use Cloud Firewall together with Object Storage Service (OSS) or ApsaraDB RDS.

The default IP address whitelist contains only the 127.0.0.1 IP address. This indicates that your RDS instance denies access from all IP addresses over the Internet or an internal network. You can configure a whitelist on the **Data Security** page of the ApsaraDB RDS console. You can also configure a whitelist by using the ApsaraDB RDS API. After you update a whitelist, you do not need to restart your RDS instance. This avoids interruptions to your workloads.

If you use a self-managed RDS database that is deployed on an ECS instance, you can use VPC firewalls to protect the self-managed database. For more information, see [Create an access control policy for a VPC firewall](#).

2. FAQ about bandwidth supported by Cloud Firewall

Which types of traffic consume the purchased bandwidth of Cloud Firewall?


Internet traffic consumes the purchased bandwidth of Cloud Firewall. However, the mutual access traffic between virtual private clouds (VPCs) does not consume the bandwidth. For example, if an elastic IP address (EIP) is under a DDoS attack, the traffic to the EIP consumes the purchased bandwidth regardless of whether Cloud Firewall blocks the attack. This is because the traffic is Internet traffic.

What do I do if the volume of my business traffic exceeds the purchased bandwidth of Cloud Firewall?

If the volume of your business traffic exceeds the purchased bandwidth, the excess traffic is not protected by Cloud Firewall. Cloud Firewall can protect only the traffic whose volume does not exceed the bandwidth. To enable Cloud Firewall to protect the excess business traffic, you must increase the bandwidth. For more information about how to increase the bandwidth, see [Upgrade Cloud Firewall and change configurations](#).

If the volume of your business traffic exceeds the purchased bandwidth, we recommend that you perform the following operations:

- In the Cloud Firewall console, observe the traffic trends displayed on the **Overview** page and the VPC traffic information displayed on the **Traffic Analysis > VPC Access** page. Identify suspicious IP addresses based on Cloud Firewall logs and handle the risks.
- If the volume of your business traffic exceeds the purchased bandwidth, Cloud Firewall sends you a notification email. We recommend that you check your email on a regular basis and handle issues based on the information that is provided in the email.

 **Note** If the volume of your business traffic exceeds the purchased bandwidth, Cloud Firewall sends you a notification email within 24 hours.

3. What are the differences between Cloud Firewall and ECS security groups?

A security group is a virtual internal firewall that is provided by Elastic Compute Service (ECS) to control the traffic between ECS instances.

Cloud Firewall provides the Internet firewall to control the traffic at the Internet boundaries, virtual private cloud (VPC) firewalls to control the traffic between VPCs, and internal firewalls to control the traffic between ECS instances.

Internal firewalls that are provided by Cloud Firewall use the technology of security groups. The policies that are configured on the **Internal Firewall** tab of the **Access Control** page in the [Cloud Firewall console](#) are automatically synchronized with the policies that are configured on the **Security Groups** page in the [ECS console](#).


Unique features of Cloud Firewall

- Application-based access control. For example, you can allow HTTP traffic so that HTTP services can run on any port.
- Domain name-based access control. For example, you can allow ECS instances to send requests only to **.aliyun.com*.
- Intrusion prevention. Cloud Firewall prevents against common system vulnerabilities and brute-force attacks.
- The monitor mode of access control policies.
- Complete traffic logs and real-time traffic analysis.

Enhanced features of Cloud Firewall

Cloud Firewall provides the following enhancements to security groups:

- If no policy is set to allow in a policy group, the ECS instances in the policy group cannot communicate with each other.

 **Note** After all policies in a policy group are deleted, the policy group is considered as a policy group to which no policies have been added.

- The number of policies configured for internal firewalls (rules in ECS security groups) is limited. To ensure security, you can configure access control policies for VPC firewalls. This way, fewer policies need to be configured for internal firewalls. You can also increase the quota of access control policies for VPC firewalls. To increase the quota, submit a .

4. FAQ about Cloud Firewall authorization

Why do I need to authorize Cloud Firewall to access other resources before I can use it?

Before you can view the requests to the cloud services, responses to the requests, and access between the cloud services over an internal network in the Cloud Firewall console, you must authorize your Cloud Firewall to access resources. These resources include Elastic Compute Service (ECS) instances, virtual private clouds (VPCs), and Server Load Balancer (SLB) instances. Then, you can use the analysis results to configure access control policies. You need to authorize Cloud Firewall to access resources. Otherwise, Cloud Firewall cannot collect data from the resources. When Cloud Firewall is authorized to access resources, you can collect data and view analysis results in the Cloud Firewall console.

To authorize Cloud Firewall to access cloud resources, you must use an Alibaba Cloud account or a RAM user that has the AliyunRAMFullAccess permission. For more information about how to authorize Cloud Firewall to access resources, see [Authorize Cloud Firewall to access other cloud resources](#).

When I create a VPC firewall for a Cloud Enterprise Network (CEN) instance, the system prompts that I do not have permissions. Why?

The CEN instance within your Alibaba Cloud account is attached a VPC that belongs to a different Alibaba Cloud account and your Cloud Firewall is not authorized to access the cloud resources within the Alibaba Cloud account to which the VPC belongs.


When you create a VPC firewall before the authorization is complete, the **It is not allowed to be created because of the existing unauthorized network instance** message appears.

5.FAQ about network traffic analysis

Traffic from unknown applications accounts for a large proportion in traffic analysis. Does this occur because Cloud Firewall cannot identify the types of applications that generate traffic from the Internet?

Possible causes:

- A large amount of traffic is generated from the Internet, and the traffic does not comply with standard protocols. As a result, Cloud Firewall cannot identify the application type for the traffic.
- The destination server blocks network traffic and returns a large number of RST packets. The RST packets are counted in the inbound or outbound traffic. A large number of RST packets causes a large proportion of traffic from applications whose type is **Unknown**.

 **Note** You can log on to the , choose **Log Analysis > Log Audit** in the left-side navigation pane, and then click the **Event Logs** or **Traffic Logs** tab to view the source and purpose of the traffic from unknown applications. Then, you can determine whether the traffic is normal.

You can view the details of unknown applications on the following pages in the :

- **Internet Access**

In the left-side navigation pane, choose **Traffic Analysis > Internet Access**. In the lower part of the page that appears, select **Unknown** from the application type drop-down list.

You can view Internet access activities from applications whose type is **Unknown**.

- **All Access Activities**

In the left-side navigation pane, choose **Traffic Analysis > All Access Activities**. In the **Rankings of Visits by Traffic** section, you can view the inbound and outbound traffic of applications whose type is **Unknown**.

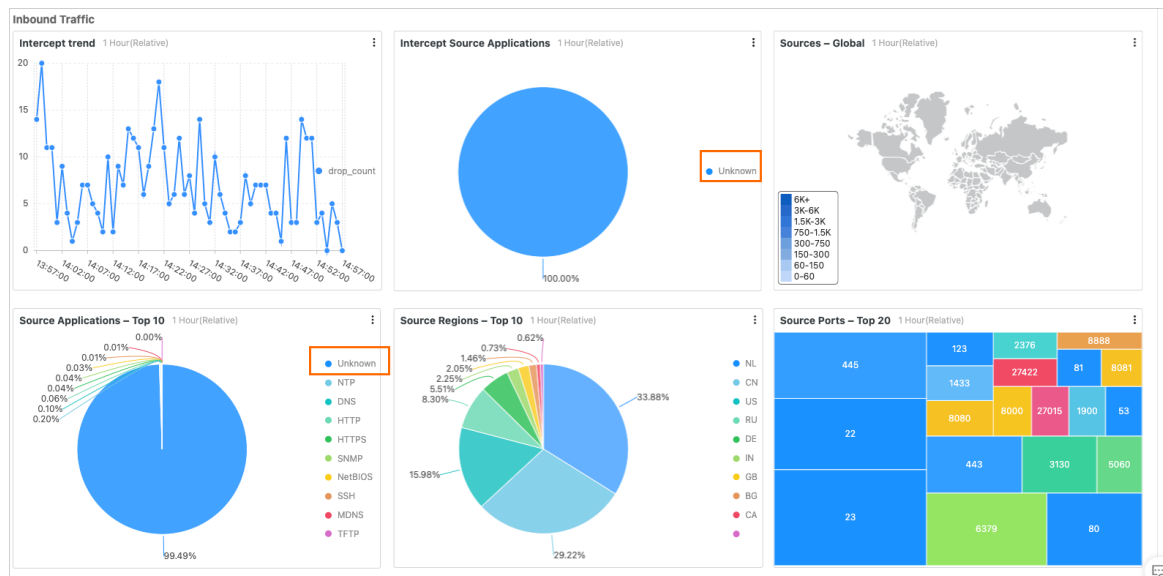
- **Log Audit**

In the left-side navigation pane, choose **Log Analysis > Log Audit**. On the page that appears, click the **Event Logs** or **Traffic Logs** tab. Then, click the **Internet Firewall** or **VPC Firewall** tab. In the **Application** column of the log list, you can view the applications whose type is **Unknown**.

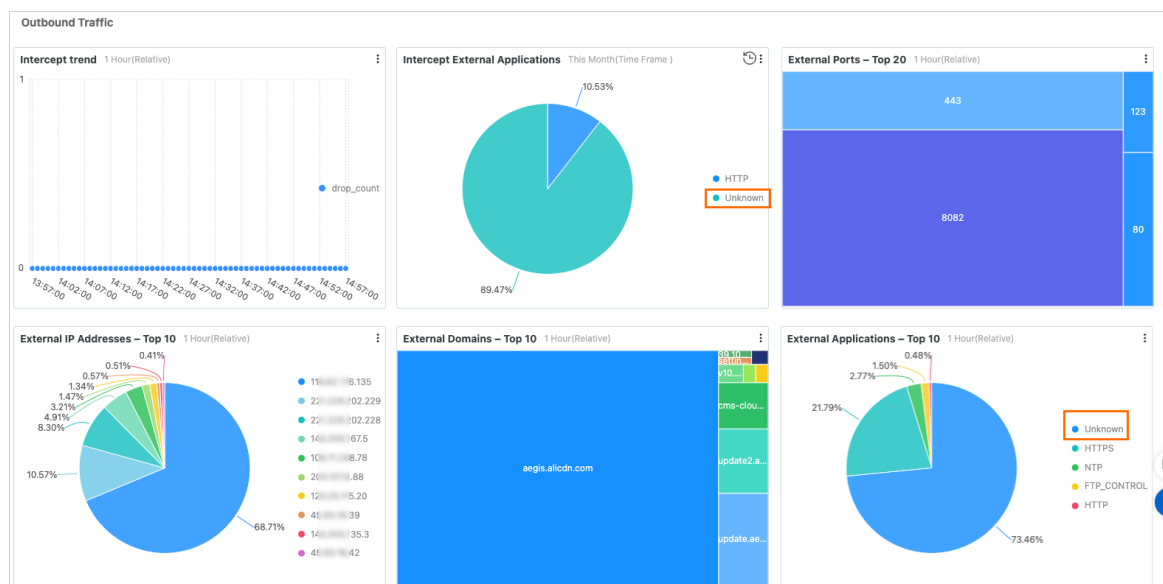
- **Log Analysis**


In the left-side navigation pane, choose **Log Analysis > Log Analysis > Reports**. In the **Inbound Traffic** and **Outbound Traffic** sections, you can view the applications whose type is **Unknown** in the top 10 inbound applications, top 10 outbound applications, and intercepted applications.

○ Inbound Traffic



○ Outbound Traffic



Note You can click the  icon in the upper-right corner of each section to perform operations. For example, you can select a time range, download chart data, and download charts.

On the Traffic Analysis > All Access Activities page, the system displays a large proportion of traffic from unknown ISPs. Why?

For inbound traffic from countries or regions outside China, the system displays only the names of the countries or regions. Cloud Firewall marks the Internet service providers (ISPs) of such traffic as unknown. Therefore, if a large amount of inbound traffic from regions outside China occurs, the system displays a large proportion of traffic from unknown ISPs.

In the left-side navigation pane of the , you can choose **Log Analysis > Log Audit > Traffic Logs** to view the region and ISP for an IP address.

The tags of domain names are displayed on the Outbound Connections page. What are the meanings of the tags?

Cloud Firewall automatically adds tags based on the Internet information about the domain names or destination IP addresses that are involved in outbound activities. The tags include **New**, **Periodic**, **Malicious download**, **Popular website**, **Ore pooled**, **Threat Intelligence**, and **DDoS Trojan**.

Outbound Connections Last 7 Days 2022-04-17 20:19:45 - 2022-04-24 20:19:45

Outbound Domains	Outbound IP Addresses	Assets	Protocol Analysis
0 Risky 87 All	1 Risky 1606 All	0 Risky 17 All	0 Risky 11 All

Outbound traffic Visualized analysis

Outbound Domains Outbound IP Addresses Assets

Total Outbound Domains: 87 Domains Not Covered by Policies: 87 Risky Domains: 0 Domains Followed: 0 Ignored: 0 Ignored / Followed

All Products All Categories All Intelligence Tags Domain Name Search

Domain Name	Traffic	Requests	Category	Intelligence Tag	Recommended Operation
ac...com	All Intelligence Tags	88.21 K	Alibaba Cloud Products	-	Ignore ⋮
up...com	New	6.08 K	Alibaba Cloud Products	-	Ignore ⋮
up...com	Periodic	5.77 K	Alibaba Cloud Products	-	Ignore ⋮
cms...com	Malicious download	3.12 K	Alibaba Cloud Products	-	Ignore ⋮
	Popular website				
	Ore pooled				
	Threat Intelligence				
	DDoS Trojan				

- **New**: Cloud Firewall identifies an outbound activity for the first time.
- **Periodic**: Your assets periodically communicate with a domain name or a destination IP address in outbound connections.
- **Malicious download, Ore pooled, or Threat Intelligence**: Cloud Firewall considers the outbound activity risky. Check whether the outbound activity is a false positive. If the outbound activity is malicious, we recommend that you configure an access control policy to control related activities. For more information, see [Create access control policies for outbound and inbound traffic on the Internet firewall](#).
- **Popular website**: A domain name is frequently accessed by your server or business.
- **DDoS Trojan**: Cloud Firewall considers that the outbound activity may trigger DDoS attacks.

6. FAQ about access control policies

I configured an outbound access control policy whose Application is set to HTTP or HTTPS for a domain name. How do I check whether the policy is valid?


Do not run the telnet command. We recommend that you run the curl command or enter a domain name in the address bar of your browser to check whether the policy is valid. For example, you can run the `curl -k "https://www.aliyundoc.com"` command, and then view the number of times that the policy is hit and the audit logs.

How do I determine the priority of an access control policy?

The priorities of access control policies determine the order in which the policies take effect. Cloud Firewall automatically determines the priorities of access control policies. By default, a smaller value indicates a higher priority. You can adjust the priority of a policy. For more information, see [Change the priority of an access control policy](#).

If you have configured multiple access control policies, Cloud Firewall matches policies against the traffic that arrives at Cloud Firewall based on the priorities of the policies. If Cloud Firewall matches a policy, Cloud Firewall no longer checks other policies. If an Allow policy is matched, the traffic is allowed. If a Deny policy is matched, the traffic is blocked.

- For access control policies of the Internet firewall for inbound and outbound traffic, a smaller value indicates a higher priority.

 **Notice** The priority of each access control policy is unique.

- For access control policies of internal firewalls, a smaller value indicates a higher priority. This also applies to the rules of security groups.

The priorities range from 1 to 100. Different access control policies can have the same priority. If multiple policies have the same priority, Deny policies take precedence over other policies.

What do I do if the number of policy groups or policies for an internal firewall reaches the upper limit?

What are the differences between common policy groups and enterprise policy groups?

Policy groups configured on an internal firewall between Elastic Compute Service (ECS) instances are classified into common and enterprise policy groups.

- A common policy group applies to the basic security groups of ECS instances and functions as a virtual firewall to provide stateful packet inspection (SPI) and packet filtering capabilities. You can use a common policy group to isolate security domains on the cloud. You can configure access control policies to allow or block inbound and outbound traffic between ECS instances in a common policy group.
- An enterprise policy group applies to the advanced security groups of ECS instances and supports

more ECS instances than a common policy group. You can configure access control policies for an unlimited number of private IP addresses. Enterprise policy groups are best suited to enterprises that require efficient O&M on large-scale networks.

The following table lists the differences between common and enterprise policy groups.

Feature	Common policy group	Enterprise policy group
VPC	Supported.	Supported.
Policy priority configuration	Supported.	Not supported.
Authorization of other policy groups	Supported.	Not supported.
Number of private IP addresses allowed	2,000	65,536
Communication between ECS instances in the same policy group	Not supported. By default, a common policy group allows all outbound traffic and requires manual configuration to control inbound traffic.	Not supported. An enterprise policy group requires manual configuration to control both outbound inbound and traffic.

Why is an error returned after I click Apply to allow the traffic of a security group?

The security groups associated with the IP address of the ECS instance do not support the default Allow policy due to the following reasons:

When I apply the default Allow policy, the system prompts a conflict that cannot be resolved. Why?

The priorities of the access control rules that you want to apply to an ECS security group **conflict** with those specified for the rules of another ECS security group in the same virtual private cloud (VPC).

You can click the One-click Apply icon to apply the default Allow policy only when no conflicts exist between the priorities of rules in different ECS security groups in the same VPC.

Why is the One-click Apply icon unavailable?

Conflicts exist between the priorities of rules in different ECS security groups. You can apply the default Allow policy only after you resolve the conflicts between the priorities of rules in the security groups that are associated with the IP address of the ECS instance. For more information, see [Apply default allow policies to security groups](#).

Why is an error returned when I click the One-click Apply icon?

An error is returned because the number of access control rules created for the required security group exceeds the upper limit.

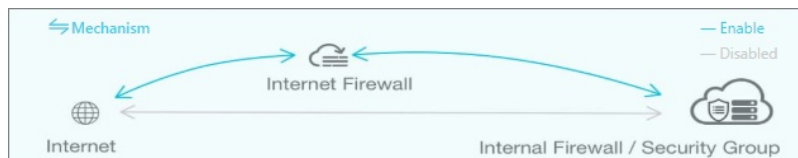
7. FAQ about the Internet firewall

What is the functionality of the Internet firewall?

If you disable the Internet firewall for public IP addresses, the traffic of these public IP addresses is forwarded to internal firewalls or security groups and then to the destination Elastic Compute Service (ECS) instances.

If you enable the Internet firewall for public IP addresses, the traffic of these public IP addresses is monitored and filtered by the Internet firewall. Then, the traffic is forwarded to internal firewalls and then to the destination ECS instances. If you enable the Internet firewall but do not configure access control policies or policies for the intrusion prevention system (IPS), Cloud Firewall monitors traffic and generates alerts for suspicious traffic but does not block the suspicious traffic.

The following figure shows the route of network traffic when the Internet firewall is enabled and the route when the Internet firewall is disabled.



Is network traffic affected if I enable the Internet firewall?

By default, the Internet firewall is enabled after you activate Cloud Firewall. If no policies are configured, the access traffic of your services only passes through Cloud Firewall but Cloud Firewall does not process the traffic.

What happens if I disable the Internet firewall?

The following figure shows the Internet Firewall tab.

If you disable the Internet firewall, the following issues may occur:

- On the Internet Access page, some traffic analysis charts have no data. To go to the Internet Access

page, log on to the Cloud Firewall console and choose **Traffic Analysis > Internet Access** in the left-side navigation pane.

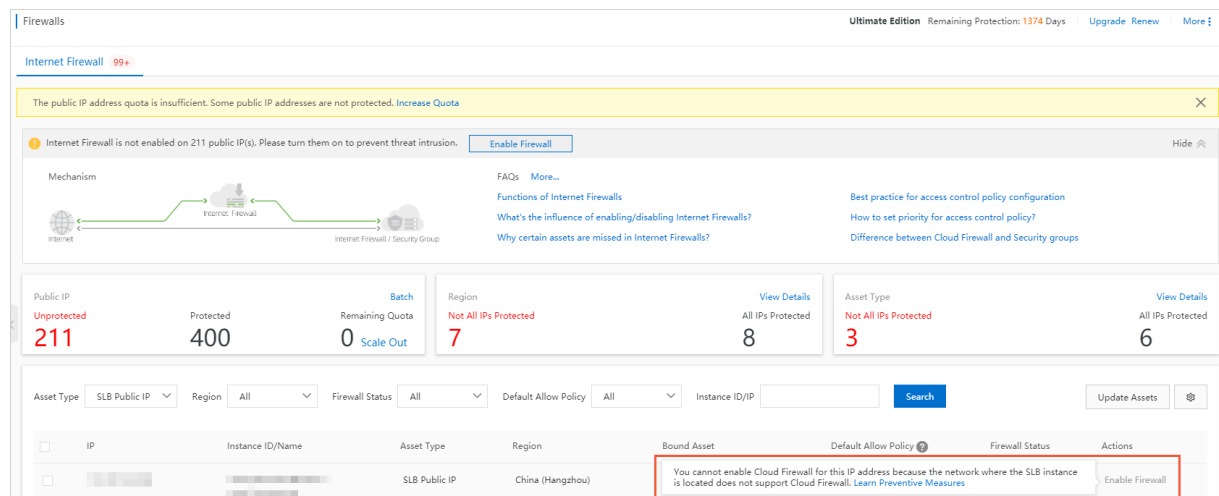
- The **outbound** or **inbound** access control policies that you created for your ECS instances become invalid, and the hits of the policies remain unchanged.
- Network traffic does not pass through Cloud Firewall, and intrusion prevention becomes invalid.
- The **Traffic Logs** tab does not display the traffic data that is generated after you disable the Internet firewall. To go to the Traffic Logs tab, log on to the Cloud Firewall console, choose **Log Analysis > Log Audit** in the left-side navigation pane, and then click the Traffic Logs tab.
- Network traffic does not pass through Cloud Firewall. As a result, traffic data that is generated after you disable the Internet firewall cannot be captured, and the **Packet Capture** section does not show the IP packet information. To go to the Packet Capture section, log on to the Cloud Firewall console and choose **Settings > Toolbox** in the left-side navigation pane. For more information, see [Create a packet capture task](#).

For more information, see [互联网边界防火墙](#).

Why do I fail to enable the Internet firewall?

Problem description

When you click **Enable Firewall** in the Actions column for some assets on the Internet Firewall tab of the Firewall Settings page, the following message appears: **You cannot enable Cloud Firewall for this IP address because the network where the SLB instance is located does not support Cloud Firewall.**



Cause

The Server Load Balancer (SLB) instance has only private IP addresses and does not support the Internet firewall.

Solution

If your assets are deployed only on an internal-facing SLB instance, associate an elastic IP address (EIP) with the internal-facing SLB instance to redirect the traffic to Cloud Firewall. For more information, see [Associate an EIP with a CLB instance](#).

What types of public IP addresses can be protected by the Internet firewall?

The Internet firewall can protect the following types of public IP addresses:

- EIPs of Elastic Network Interfaces (ENIs). The EIPs can be associated with ECS instances of the VPC type, internal-facing SLB instances of the VPC type, ENIs, and Network Address Translation (NAT) gateways
- Public IP addresses of ECS instances
- EIPs associated with SLB instances of the VPC type
- Public IP addresses of bastion hosts

8. FAQ about VPC Firewall

Is network traffic affected after firewalls are enabled?

Are the rules of ECS security groups affected after VPC Firewall is enabled?

No, the rules of ECS security groups are not affected after VPC Firewall is enabled.

After VPC Firewall is enabled, a security group named `Cloud_Firewall_Security_Group` is automatically added and an access control policy is created to allow traffic to the VPC firewall.

The security group applies only to the traffic between VPCs. The existing rules of ECS security groups are not affected. You do not need to migrate or modify the rules of the ECS security groups.

What are the limits of VPC Firewall?

For more information, see [VPC firewall limits](#).

9. FAQ about Cloud Firewall logs

This topic provides answers to some commonly asked questions about Cloud Firewall logs.

Can traffic logs on Cloud Firewall be exported to a third-party system?

Yes. Cloud Firewall Premium Edition, Enterprise Edition, and Ultimate Edition provides the log analysis feature that can be used with Alibaba Cloud Log Service, also known as Simple Log Service (SLS). The log analysis feature allows you to view and export **Internet traffic logs**.

You can use this feature to export traffic logs to your business system, such as your security O&M center.

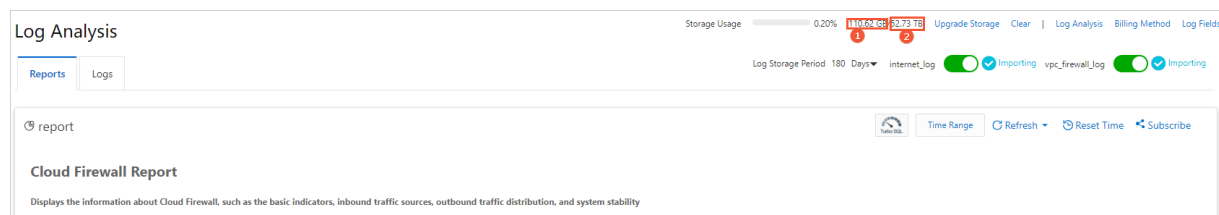


Note

For information about how to export logs, see [Import the traffic logs of Cloud Firewall to a third-party system](#).

How do I know the remaining log storage capacity of Cloud Firewall?

If you have purchased Cloud Firewall Premium Edition, Enterprise Edition, or Ultimate Edition, and have enabled the log analysis feature, you can view the used and remaining log storage capacity in the upper-right corner of the Log Analysis page. To go to this page, choose **Log Analysis > Log Analysis** in the left-side navigation pane.



Note The free trial edition of Cloud Firewall does not support the log analysis feature, so the log storage capacity is not displayed.

Why is the log storage capacity not displayed in the Cloud Firewall console?

The free trial edition of Cloud Firewall does not support the log analysis feature. If you are using the free trial edition of Cloud Firewall, the log storage capacity is not displayed. For information about how to enable the log analysis feature, see [Enable the log analysis feature](#).

10.How do I troubleshoot network connection failures?

Problem description


After you enable a firewall, the following issues may occur:

- You cannot log on to your server.
- You cannot access the services that run on your server.
- Your server cannot connect to the Internet.

Troubleshooting for the Internet firewall

1. Check whether the Internet firewall is enabled for your asset.

After you enable the Internet firewall, traffic can pass through Cloud Firewall. For more information about how to enable the Internet firewall, see [互联网边界防火墙](#).

 **Note** If the Internet firewall is not enabled for your asset, traffic does not pass through Cloud Firewall. In this case, you must check whether other issues such as network connection failures occur.

2. Check whether traffic logs are generated on the **Traffic Logs** tab.
 - If no traffic logs are found, the traffic is discarded before it reaches the Internet firewall.
 - If traffic logs are found and the action is **Discard**, the traffic is discarded by the Internet firewall. In this case, you can find the relevant event on the **Event Logs** tab and confirm the module that performs the Discard action based on the information in the **Module** column.
 - If the Discard action is performed by the **Access Control** module, the traffic is discarded based on the access control policies that you configure. We recommend that you check the access control policies and modify them based on your business requirements.
 - If the Discard action is performed by the **Basic Protection**, **Virtual Patches**, or **Threat Intelligence** module, the traffic is discarded based on the intrusion prevention policies that you configure. In this case, you can choose **Intrusion Prevention > Intrusion Prevention** in the left-side navigation pane to disable the intrusion prevention policies.
 - If traffic logs are found and the action is **Allow** or **Monitor**, the traffic is not discarded by the Internet firewall. You must check security groups.

Troubleshooting for security groups


Log on to the [ECS console](#). In the left-side navigation pane, choose **Instances & Images > Instances**. On the page that appears, click the name of the Elastic Compute Service (ECS) instance on which the network connection failure occurs. On the **Security Groups** tab of the **Security Groups** tab, make sure that the value in the **Action** column of the required security group rule is **Allow**.

If the issue persists after you perform the preceding troubleshooting operations, submit a .


11. What are the priorities of rules that are used by Cloud Firewall to protect traffic?

Cloud Firewall matches traffic against rules based on the following priorities of rules:

- If no access control policies are enabled, or if access control policies are enabled but the traffic does not match access control policies, Cloud Firewall matches the traffic first against the rules of **Threat Intelligence**, and then against the rules of **Basic Protection**, **Intelligent Defense**, and **Virtual Patches**.

 **Notice** If the traffic is blocked by the rules of **Threat Intelligence**, Cloud Firewall no longer matches the traffic against other rules.

- If access control policies are enabled and the traffic matches an Allow policy or a Monitor policy, Cloud Firewall does not match the traffic against the rules of **Threat Intelligence**, but matches the traffic against the rules of **Basic Protection**, **Intelligent Defense**, and **Virtual Patches**.
- If access control policies are enabled and the traffic matches a Deny policy, Cloud Firewall no longer matches the traffic against other rules.

 **Notice** Cloud Firewall matches all traffic against the rules of **Basic Protection**, **Intelligent Defense**, and **Virtual Patches**, and these rules have no priorities.

12. Why am I unable to activate Cloud Firewall for my account?

Problem description

When I log on to the Cloud Firewall console by using my Alibaba Cloud account, the message "Your account cannot be used to activate Cloud Firewall." appears.

Causes


This issue can be caused by one of the following reasons:

- Your account is an Alibaba Cloud account and is added as a member by another Alibaba Cloud account for centralized management.
- Your account is a Resource Access Management (RAM) user and does not have the required permissions.

Solution

You can move the pointer over the profile picture in the upper-right corner of the Cloud Firewall console to view the value of **Account ID**.

- If the value of **Account ID** is a string of digits that start with 1, your account is an Alibaba Cloud account. Log on to the Cloud Firewall console by using the Alibaba Cloud account that manages your account. Then, activate Cloud Firewall for your account.
- If the value of **Account ID** is a string of digits that start with 2, your account is a RAM user. Perform the following operations to grant permissions to your account:
 - i. Log on to the [RAM console](#). For more information, see [Log on to the Alibaba Cloud Management Console as a RAM user](#).
 - ii. In the left-side navigation pane, choose **Identities > Users**.
 - iii. On the **Users** page, find the RAM user to which you want to grant permissions and click **Add Permissions** in the **Actions** column.
 - iv. In the **Add Permissions** panel, select the **createSlr**, **AliyunYundunCloudFirewallReadOnlyAccess**, and **AliyunYundunCloudFirewallFullAccess** policies.

 **Notice** createSlr is a custom policy. For more information, see [Create a policy](#).

- v. Click **OK**.

Create a policy

- Log on to the [RAM console](#).
- In the left-side navigation pane, choose **Permissions > Policies**.
- On the **Policies** page, click **Create Policy**.
- On the **Create Policy** page, click the **JSON** tab.
- On the **JSON** tab, enter the policy document based on the following example and click **Next Step**. On the page that appears, set **Name** to **createSlr**.

```
{
  "Statement": [
    {
      "Action": [
        "ram:CreateServiceLinkedRole"
      ],
      "Resource": "acs:ram:*:166032244439****:role/*",
      "Effect": "Deny",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": [
            "cloudfw.aliyuncs.com"
          ]
        }
      }
    }
  ],
  "Version": "1"
}
```



Notice You must set the value of Resource in the following format: `acs:ram*:UID of the Alibaba Cloud account:role/*`. The UID indicates the UID of the Alibaba Cloud account to which your RAM user belongs.

- Click **OK**. The policy is created.

13. Why are ICMP detection packets periodically sent by Cloud Firewall?

To ensure the quality of service, Cloud Firewall periodically sends ICMP packets for network error detection. The detection is not a scanning attack and does not affect services.

You can click **Source address for SLA monitoring** on the Cloud Address Books tab to view the source IP address and can click the value in the Hits column in the Inbound Policies tab on the Access Control page to view detailed logs.

14.FAQ about firewall protection for some public IP addresses of an SLB instance that is deployed in the classic network

Problem description

A Server Load Balancer (SLB) instance is deployed in the classic network and is assigned public IP addresses. Firewalls are enabled for the public IP addresses on which routing upgrade is not performed. In this case, the protection engine of Cloud Firewall cannot provide full protection capabilities for the traffic of the IP addresses. Some protection features do not work. Cloud Firewall is upgraded at 00:00 on June 23, 2022 to provide better protection and resolve the issue that full protection capabilities fail to be provided for the traffic of the IP addresses.

After the upgrade, Cloud Firewall automatically checks whether routing upgrade is performed on a public IP address for which you want to enable firewalls.

- If the routing upgrade is performed, Cloud Firewall allows you to enable firewalls.
- If the routing upgrade is not performed, Cloud Firewall does not allow you to enable firewalls for the IP address.

If you want to enable a firewall due to urgent service requirements but you cannot enable a firewall, we recommend that you submit a . The Cloud Firewall team can help you complete the routing upgrade for the public IP address in a more efficient manner. After the routing upgrade is performed, you can enable firewalls in Cloud Firewall with a few clicks.

Solutions

If you have enabled a firewall for one of the preceding IP addresses before Cloud Firewall is upgraded, you can check the results of the routing upgrade for the IP address in the **Firewall Status** column on the **Internet Firewall** tab.

- If the routing upgrade is performed, you can upgrade Cloud Firewall with a few clicks to obtain the full protection capabilities of Cloud Firewall. Before the upgrade, we recommend that you add the public IP address to a whitelist or make sure that a security policy allows the public IP address of the SLB instance.

If the public IP address is added to a whitelist before Cloud Firewall is upgraded, the upgrade does not pose risks in theory. If an exception occurs due to the upgrade, you can click **Disable Firewall** in the Actions column of the IP address to restore the IP address to the state before the upgrade. We recommend that you perform the upgrade during off-peak hours.

- If the routing upgrade is not performed, you cannot upgrade Cloud Firewall for the preceding IP addresses. We recommend that you disable the firewall for the public IP address to avoid potential risks caused by incomplete protection capabilities.

If you want to enable a firewall due to urgent service requirements but you cannot enable a firewall, we recommend that you submit a . The Cloud Firewall team can help you complete the routing upgrade for the public IP address in a more efficient manner. After the routing upgrade is performed, you can enable firewalls in Cloud Firewall with a few clicks.