ALIBABA CLOUD

Alibaba Cloud

Cloud Firewall

FAQ

Document Version: 20201117

Alibaba Cloud

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**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Protection scope of Cloud Firewall

What cloud assets or traffic can Cloud Firewall protect?

Cloud Firewall can protect the following cloud assets or traffic:

- Internet traffic: traffic from public IP addresses of Elastic Compute Service (ECS) instances, elastic IP addresses (EIPs) of Server Load Balancer (SLB) instances, highly available virtual IP addresses (HAVIPs), EIPs, EIPs of ECS instances, EIPs of Elastic Network Interfaces (ENIs), some public IP addresses of SLB instances, and EIPs of network address translation (NAT) gateways.

  > **Note** Alibaba Cloud provides public and private SLB instances. Some public SLB instances cannot be protected by Cloud Firewall due to network architecture reasons. We recommend that you deploy private SLB instances and associate EIPs with the private SLB instances. For information about how to associate an EIP with an SLB instance, see Associate an EIP with an SLB instance.

- Traffic between VPCs: traffic between VPCs that are connected by using a CEN or Express Connect

Is Cloud Firewall applicable to the classic network?

The Internet firewall and intrusion prevention system (IPS) are applicable to the classic network. Internal firewalls are applicable to VPCs, but are not applicable to the classic network.

Is Cloud Firewall available in regions outside China?

Yes, in addition to regions in mainland China and the China (Hong Kong) region, Cloud Firewall is available in Malaysia (Kuala Lumpur), Singapore (Singapore), Indonesia (Jakarta), and Germany (Frankfurt) regions. For more information, see Editions and regions.

Can Cloud Firewall protect public SLB instances?

Alibaba Cloud provides public and private SLB instances. Some public SLB instances cannot be protected by Cloud Firewall due to network architecture reasons. We recommend that you deploy private SLB instances and associate EIPs with the private SLB instances. For information about how to associate an EIP with an SLB instance, see Associate an EIP with an SLB instance.

> **Note** For a public SLB instance that is in use and is not protected by Cloud Firewall, we recommend that you do not change the network type of the instance by yourself. If you need any help, contact SLB technical support.

After you activate Cloud Firewall, the traffic first goes through the firewall. The destination IP address, which is an elastic IP address (EIP), of the traffic is then translated into an IP address of a private SLB instance by using destination network address translation (DNAT).

Can Cloud Firewall control traffic from private IP addresses to the Internet?

Cloud Firewall controls only traffic to the Internet from EIPs or public IP addresses obtained by using DNAT. It cannot control outbound traffic from private IP addresses.

If you want to control the traffic from a private IP address, bind an EIP to the private IP address and configure access control policies for this EIP.

Can Cloud Firewall control IPsec traffic?

The Internet firewall cannot be used to control decrypted IPsec traffic.

You can use east-west traffic control policies of Cloud Firewall to control decrypted IPsec traffic.

Can Cloud Firewall protect traffic on Express Connect or Cloud Enterprise Network (CEN)?

Yes, Cloud Firewall can protect traffic on Express Connect and CEN.

- Cloud Firewall can protect only traffic between VPCs that are connected by using Express Connect in the same region. It cannot protect traffic between a VPC and a Virtual Border Router (VBR) that are connected by using Express Connect.
- Cloud Firewall can protect traffic between two VPCs in different regions, as well as a VPC and a VBR, that are connected by using a CEN.

> **Note** If you need Cloud Firewall to protect traffic between two VPCs in different regions, or between a VPC and a VBR, migrate the traffic of Express Connect to a CEN. For more information, see Migrate a VPC in a peering connection to a CEN instance.

Why does Cloud Firewall provide three types of firewalls?

Cloud Firewall provides three types of firewalls: Internet firewall, VPC firewall, and internal firewall.

The Internet firewall is deployed at the boundary of the Internet to manage public IP addresses. Internal firewalls works in the same way as security groups to manage communications between ECS instances. The following figure shows how the Internet firewall and internal firewalls work and where they are deployed in the network topology.

Internet firewall and internal firewalls

VPC firewalls are used to protect traffic between VPCs and are deployed at the boundaries of VPCs to manage the traffic over Express Connect. The following figure shows how a VPC firewall works and where it is deployed in the network topology.

VPC firewalls

You can use all of the three types of firewalls to refine your network access control strategy and build three protection systems: Internet traffic protection, VPC protection, and instance protection.

- Cloud Firewall provides centralized access control, including inbound and outbound policies, to support more precise control over network traffic. Cloud Firewall also provides application-specific and domain name-specific access control policies for you to centrally manage VPCs and regions. You can use the monitor mode and address books to tune your access control policies.
- For network traffic that requires microsegmentation, Cloud Firewall provides distributed access control. Cloud Firewall is developed based on the capabilities of security groups and offers visualized analysis of internal network traffic, which allows you to tune policies for traffic between ECS instances. The monitor mode, blocked traffic analysis, and threat intelligence features will be soon available.

Cloud Firewall allows you to configure firewalls based on network boundaries to build multiple logical protection systems. This makes your maintenance work much easier. If you only want to detect the Internet traffic, you only need to configure inbound and outbound policies on the Internet firewall. If you want to protect your instances, you can configure access control policies for east-west traffic on internal firewalls.

2.Relationship between Cloud Firewall and Alibaba Cloud products

Cloud Firewall is deployed on Alibaba Cloud.

The following figure shows the logical relationships between Cloud Firewall and some of the Alibaba Cloud products.

Work with other security products such as Web Application Firewall (WAF) and Anti-DDoS Protection

The figure above shows that Cloud Firewall is used to protect the source IP addresses of WAF and Anti-DDoS Protection.

Work with Content Delivery Network (CDN)

Cloud Firewall is used to protect source IP addresses.

Work with Object Storage Service (OSS) and ApsaraDB RDS

Cloud Firewall currently does not support protecting OSS and ApsaraDB RDS instances. This feature will be available in the second half of 2019.

Work with Server Load Balancer (SLB)

SLB instances include internet SLB instances and intranet SLB instances. Cloud Firewall currently does not support protecting internet SLB instances. It only supports protecting intranet SLB instances with EIPs.

3.FAQ about bandwidth supported by Cloud Firewall

What are the protected bandwidth quotas of Cloud Firewall in different editions?

Cloud Firewall can protect your Internet traffic and traffic between VPCs. Cloud Firewall in different editions have different protected bandwidth quotas:

- For Internet traffic, the default protected bandwidth quota per month is 10 Mbit/s in Premium Edition, 50 Mbit/s in Enterprise Edition, and 200 Mbit/s in Ultimate Edition.
- For traffic between VPCs, the default protected bandwidth quota per month is 100 Mbit/s in Enterprise Edition and 1 Gbit/s in Ultimate Edition. No protection is provided in Premium Edition.

For more information, see Features and billing items of each edition.

Which types of traffic consume the protected bandwidth quota of Cloud Firewall?

Internet traffic consumes the protected bandwidth quota of Cloud Firewall. However, the mutual access traffic between VPCs does not consume the quota. For example, if an elastic IP address (EIP) is under a DDoS attack, the traffic to the EIP consumes the protected bandwidth quota no matter whether Cloud Firewall blocks the attack. This is because the traffic is considered Internet traffic.

What do I do if the bandwidth of my business traffic exceeds the protected bandwidth quota of Cloud Firewall?

If the bandwidth of your business traffic exceeds the protected bandwidth quota, Cloud Firewall protects only the traffic within the quota. 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 **VPC Access** page under **Traffic Analysis**. Locate suspicious IP addresses based on Cloud Firewall logs and handle the risks.
- If the bandwidth of your business traffic exceeds the protected bandwidth quota, Cloud Firewall sends a notification email to you. Check emails in time and handle issues based on the information provided in the email.

  > **Note** The notification email is sent no later than the day after your business traffic exceeds the protected bandwidth quota.

- Upgrade the Cloud Firewall edition to increase the protected bandwidth quota. For more information, see Renewal and upgrade.

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

A security group is a virtual internal firewall 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, VPC firewalls to control the traffic between VPCs, and internal firewalls to control the traffic between ECS instances.

Internal firewalls 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*.
- Address books. You can add multiple IP addresses, ports, or ECS instances with the same tag to an address book for centralized management.
- Intrusion prevention. Cloud Firewall provides preemptive measures 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 in a policy group is set to allow, 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.

- You can publish multiple policies at a time.
- The number of policies configured for internal firewalls (rules in ECS security groups) is limited. You can configure access control policies for VPC firewalls to ensure security. You can submit a ticket to increase the quota of access control policies for VPC firewalls.

5.Why does Cloud Firewall require authorization?

With Cloud Firewall, you can view your assets' requests and responses transmitted through the Internet. You can also view your assets' network traffic within the internal network. You can analyze these statistics and create policies to for access control. Therefore, after you purchase Cloud Firewall, you need to authorize it to access your cloud assets.

You must authorize Cloud Firewall to access your ECS instance list, VPC network list, and SLB instance list.

Your Alibaba Cloud account must meet one of the following requirements for granting Cloud Firewall the authorization:

- Your account is an Alibaba Cloud account.
- Your account is a RAM account that has AliyunRAMFullAccess permission.

For more information about authorization, see Authorize Cloud Firewall.

6.FAQ about network traffic analysis

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

Possible causes:

- A large amount of traffic is generated from the Internet and the traffic does not comply with standard protocols. Therefore, Cloud Firewall cannot identify the traffic type.
- The destination server blocks network traffic and returns a large number of RST packets. These packets are carried in the inbound or outbound traffic, which causes a large proportion of traffic from unknown applications.

> **Note** You can choose **Log Audit > Traffic Logs** or **Log Audit > Event Logs** in the left-side navigation pane to check the source and purpose of the traffic with unknown applications, and determine whether the traffic is normal.

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

- Unknown application types on the **Internet Access** page

  

- Unknown applications in the **Rankings of Visits by Traffic** section on the **All Access Activities** page

  

Why is there a large proportion of traffic with unknown ISPs on the All Access Activities page under Traffic Analysis?

This occurs because a large amount of inbound traffic comes from regions outside China. Cloud Firewall marks the ISPs of such traffic as unknown. To view the regions and ISPs of specific IP addresses, choose **Log Audit > Traffic Logs** in the left-side navigation pane.

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

The tags are automatically added by Cloud Firewall based on the Internet information in domain names or destination IP addresses. The tags include **New**, **Periodic**, **Malicious download**, **Popular website**, **Ore pooled**, and **Threat Intelligence**.

- **New**: Cloud Firewall identifies a domain name for the first time.
- **Periodic**: Your assets periodically communicate with a domain name or destination IP address.
- **Malicious download**, **Ore pooled**, or **Threat Intelligence**: Cloud Firewall considers the outbound connection risky. Check whether the risk exists. If the risk exists, we recommend that you configure an access control policy. For more information, see Outbound and inbound traffic control on the Internet firewall.

- **Popular website**: A domain name is frequently accessed by your server or business.

7.FAQ about access control policies

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

The priorities of access control policies determine the order of the policies to be matched against network traffic.

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

  The traffic that arrives at **Cloud Firewall** is matched against policies with priorities 1 to 8 in sequence. If the traffic hits an allow policy, the traffic is allowed. If the traffic hits a deny policy, the traffic is denied. The priority for each access control policy must be unique.

  For more information, see Change the priority of an access control policy.

- For access control policies of internal firewalls, a small value indicates a high priority, which is the same as security group rules.

  The priorities range from 1 to 100. Different access control policies can have the same priority. For policies with the same priority, **deny** policies take precedence over allow policies.

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

By default, you can create up to 100 policy groups and 100 policies in each group. The policies include those synchronized from ECS security groups to Cloud Firewall and those created in the Cloud Firewall console. If you need more policies, we recommend that you delete unnecessary policies or submit a ticket for Alibaba Cloud technical support.

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

Policy groups for an internal firewall that controls the traffic between ECS instances are classified into common policy groups and enterprise policy groups.

- A common policy group is equivalent to an ECS security group. A common policy group functions as a virtual firewall to detect the connection status and filter data packets. It can be used to divide security zones on the cloud. You can configure access control policies to allow or deny inbound and outbound traffic between ECS instances in a common policy group.
- An enterprise policy group is equivalent to an advanced ECS security group. An enterprise policy group 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 features of common and enterprise policy groups.

Feature	Common policy group	Enterprise policy group
VPC	Supported.	Supported.
Policy priority configuration	Supported.	Not supported.

Feature	Common policy group	Enterprise policy group
Authorization to other policy groups	Supported.	Not supported.
Custom allow policy	Supported.	Supported.
Custom deny policy	Supported.	Not supported. Enterprise policy groups deny all traffic by default.
Number of private IP addresses allowed	2,000	65,536
Communication between ECS instances in the same policy group	Supported.	Not supported. You must add access control policies for the ECS instances to the policy group.

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

The security group associated with the public IP address does not support the default allow policy due to the following reasons:

- Advanced security groups do not support default allow policies. For more information, see Advanced security group. If a VPC contains an advanced security group, default allow policies are also not supported for other security groups in the VPC.
- Default allow policies can be configured only for security groups associated with public IP addresses or EIPs of ECS instances. They cannot be configured for Internet SLB instances.
- To better protect your assets, we recommend that you do not apply default allow policies to IP addresses with the Internet firewall disabled. You must enable the firewall for IP addresses to which you have applied default allow policies. Otherwise, these IP addresses may be exposed to the Internet.

Why am I unable to handle the configuration conflict that occurred when the default allow policy is applied?

The priorities of the access control rules you want to apply to an ECS security group conflict with the rules for another ECS security group in the same VPC.

You can apply the default allow policy with one click only if priorities of access control rules for all ECS security groups in the VPC do not have conflicts.

Why is the One-click Apply icon unavailable?

ECS security groups have rule priority conflicts. You can apply the default allow policy only after the priority conflicts between the access control rules for ECS security groups are handled. For more information, see Default allow policies for security groups.

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

The cause is that the number of access control rules created for a security group exceeds the upper limit.

By default, you can create up to 100 policy groups and 100 policies in each group. The policies include those synchronized from ECS security groups to Cloud Firewall and those created in the Cloud Firewall console. If you need more policies, we recommend that you delete unnecessary policies or submit a ticket for Alibaba Cloud technical support.

8.FAQ about the Internet firewall

What is the function of the Internet firewall?

If the Internet firewall is disabled, the traffic of public IP addresses is forwarded to internal firewalls or security groups and then to the destination ECS instances.

If the Internet firewall is enabled, the traffic of public IP addresses is redirected to the Internet firewall before it is forwarded to internal firewalls or security groups and then to the destination ECS instances. If you enable the Internet firewall but do not configure access control policies for Cloud Firewall or policies for the intrusion prevention system (IPS), Cloud Firewall detects traffic and generates alerts for suspicious traffic but does not block any traffic.

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

Is network traffic affected when you enable the Internet firewall?

Enabling Internet Firewall or VPC Firewall has no impact on network traffic.

What are the impacts of disabling the Internet firewall?

The following figure shows the Internet Firewall tab.

Disabling the Internet firewall may have the following impacts:

- On the Internet Access page, some traffic analysis charts have no data. To go to this page, choose **Traffic Analysis > Internet Access** in the left-side navigation pane.
- If you have created **outbound** or **inbound** access control policies, these policies become invalid. The **hits** of these policies remain unchanged.
- Network traffic does not pass Cloud Firewall. Intrusion prevention is not implemented.

  Even if Intrusion Prevention Mode is set to **Monitoring Mode**, the IPS no longer detects network traffic on the server. **Traffic Control Mode** is also invalid.
- The Traffic Logs tab does not display the traffic data generated after the Internet firewall is disabled. To go to this tab, choose **Logs > Log Audit** in the left-side navigation pane, and click the Traffic Logs tab.
- Network traffic does not pass Cloud Firewall, so traffic data cannot be captured. The Packet Capture page does not display the IP packet information. To go to this page, choose **Tools > Packet Capture** in the left-side navigation pane. For more information, see Packet capture.

For information about how to enable or disable the Internet firewall, see Enable or disable Internet Firewall.

Why do I fail to enable the Internet firewall?

Symptom

On the Internet Firewall tab of the Firewalls page, when you click **Enable Firewall** in the Actions column for some assets, the system prompts a message **You cannot enable Cloud Firewall for this IP address because the network where the SLB instance is located does not support Cloud Firewall.**

Causes

The Internet firewall cannot be enabled because the network where the Server Load Balancer (SLB) instance is located does not support the Internet firewall. The specific cause is one of the following reasons:

- A limit is imposed on the network architecture of the SLB instance.
- The assets do not have public IP addresses.

Solution

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

Which 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). EIPs can be associated with ECS instances of the VPC type, private SLB instances in the VPC type, ENIs, and Network Address Translation (NAT) gateways.
- Public IP addresses of ECS instances
- EIPs of SLB instances of the VPC type
- Public IP addresses of bastion hosts

9.FAQ about VPC Firewall

Is network traffic affected after firewalls are enabled?

Enabling Internet Firewall or VPC Firewall has no impact on network traffic.

However, when you enable or disable VPC Firewall, persistent connections are reset. Consider this limit before you enable VPC Firewall. If your VPC uses a private SLB instance, make sure that your applications support automatic TCP retransmission before you enable VPC Firewall. You must also pay attention to the application connection status and prevent disconnections caused by the retransmission mechanism not configured.

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.

10.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** Internet traffic logs contain data such as the vulnerability priorities and hit results of access control rules.

For information about how to export logs, see Import Cloud Firewall Internet logs 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 Cloud Firewall console**Logs > 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.

11.How to troubleshoot network connection failures

Symptom

After you enable the Clouf Firewall, the following issues may occur:

1. You cannot log on to your ECS instance.
2. You cannot access the service running on your instance.
3. Your ECS instances cannot access external networks.

Troubleshoot the Internet firewall

- Verify the Internet firewall is enabled for your asset. If it is disabled, skip this step.
- Check the access records on the **Logs > Access Log** tab page.
  - If no relevant record is found, this means that the request is dropped before it reaches the firewall.
  - If you find the record of the request and the action is **Discard**, this means that the request is blocked by the internal firewall. Find the relevant event on the **Logs > Event Log** tab page, and then confirm the module that performs the **Discard** action according to the information in the **Criterion** column.
    - If the **Criterion** shows **Access Control**, then you must check the configuration of the relevant access control policy.
    - If the column shows **Basic Protection**, **Virtual Patches**, or **Threat Intelligence**, then you must go to the **Security Policies > Intrusion Prevention** tab page to disable the relevant module.
  - If you find the record of the request and the action is **Allow** or **Monitor**, this means that the request is not blocked by the Internet firewall. You must troubleshoot the internal firewall and security groups.

Troubleshoot the internal firewall and security group

Log on to the ECS console, click the ECS instance where the connection failure occurs, and click **Security Groups** in the left-side navigation pane. Verify the **Action** of the rules in the security group is set to **Allow**.

If the issue still exists, submit a ticket.

12.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.