

Alibaba Cloud Cloud Firewall

FAQ

Issue: 20190516

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK.
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Cloud Firewall trial and pre-sales consulting.....	1
2 FAQs.....	2
3 Relationship between Cloud Firewall and Alibaba Cloud products.....	4
4 Differences between Cloud Firewall and Security groups.....	5
5 How to set priority for access control policy?.....	8
6 How to troubleshoot network connection failures.....	9
7 Functions of Internet Firewalls.....	15
8 What's the influence of enabling/disabling Internet Firewall?.....	16
9 Why certain assets are missing in Internet Firewalls?.....	18
10 Why does Cloud Firewall require authorization?.....	19
11 Differences between Cloud Firewall Basic for Finance Cloud and other editions.....	20

1 Cloud Firewall trial and pre-sales consulting

If you have issues related to the functions, price, purchase, trial or product selection of Cloud Firewall, please contact us on DingTalk. By scanning the QR code below, you can receive advice from experts in Cloud Firewall from Alibaba Cloud.



2 FAQs

Does Cloud Firewall apply to classic networks?

The north-south access control and IPS features of Cloud Firewall apply to classic networks. However, its micro-isolation feature oriented for east-west access applies only to VPCs, but not classic networks.

Does Cloud Firewall apply to international sites outside China?

The current version applies only to sites in Mainland China and Hong Kong, but not international sites outside China.

Can Cloud Firewall control the access traffic tunneled through Internet SLBs?

Cloud Firewall temporarily cannot protect the inbound traffic tunneled through Internet SLBs due to a certain network architecture issue. To work around this issue, we recommend that you deploy Destination Network Address Translation (DNAT) and intranet SLBs. In this way, the inbound traffic flows through Cloud Firewall, DNAT (or EIP), and intranet SLBs in sequence.

Can Cloud Firewall control outbound access from private addresses to the Internet?

Cloud Firewall only controls outbound access for public IP addresses DNATed from private IP addresses or for EIP addresses bound to private IP addresses. It cannot directly control outbound access from private IP addresses.

Recommended workaround: Bind an independent EIP to the private IP address for which you want to control outbound access. Then configure access control policies on this EIP.

Can Cloud Firewall control IPsec traffic?

North-south traffic control policies of Cloud Firewall cannot be used to control decrypted IPsec traffic.

Recommended workaround: Regard the decrypted IPsec traffic as east-west traffic, and use east-west traffic control policies of Cloud Firewall to control the traffic.

Can Cloud Firewall control the access traffic tunneled through Express Connect?

Currently, Cloud Firewall does not support this function. You can configure [security groups](#) to control the access traffic tunneled through Express Connect.

Can Cloud Firewall control the access traffic tunneled through bastion hosts?

Currently, Cloud Firewall does not support this function.

The traffic of the Unknown application type accounts for a large proportion of all inbound network traffic. Is this because Cloud Firewall cannot identify specific requests from the Internet?

There is a large amount of inbound scanning traffic from the Internet, most of which does not comply with any standard protocol. Cloud Firewall cannot identify this type of traffic and marks the traffic as unknown.

You can view logs under Logs > Access Log or Logs > Event Log to determine the specific sources and uses of such unknown traffic.

On the Full Activity Search tab of the Network Traffic Analysis page, why is there a large percentage of traffic with unknown carriers in the Top Access Traffic area?

For inbound traffic from and outbound traffic to carriers outside China, Cloud Firewall only identifies the countries to which the carriers belong and marks the carriers as unknown. You can view logs under Logs > Access Logs to determine the regions and carriers to which the specific IP addresses belong.

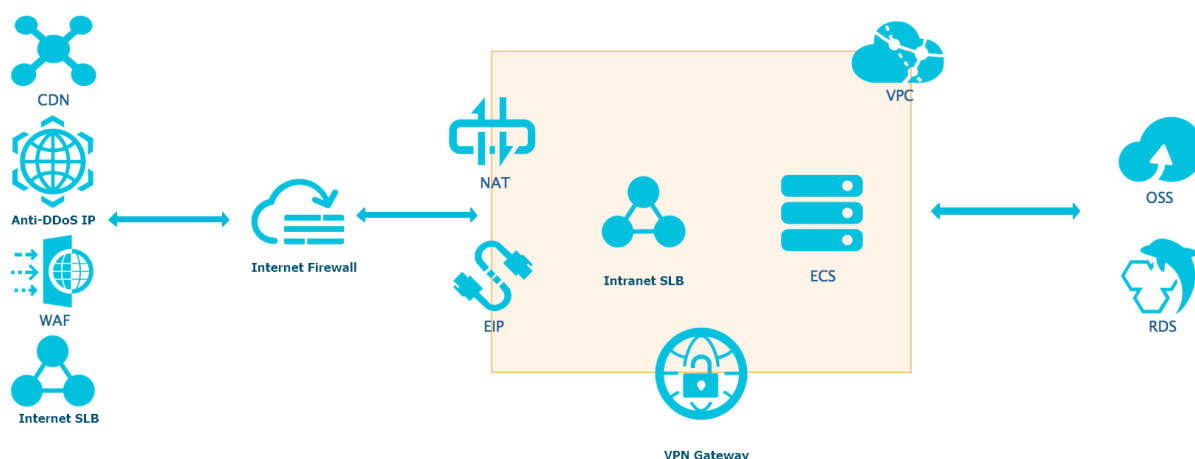
The traffic of the Unknown application type accounts for a large proportion of all outbound network traffic. Is this because Cloud Firewall cannot identify this type of traffic?

Outbound traffic may be blocked by destination servers, which then send back RST packets. These packets are recorded as outbound traffic. If there are a large number of RST packets, the traffic of the Unknown application type accounts for a large proportion of all outbound traffic. You can view logs under Logs > Traffic Logs to determine whether exceptions occur in outbound traffic.

3 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.

4 Differences between Cloud Firewall and Security groups

This topic describes the major differences between Cloud Firewall and Security groups of ECS.

A security group is a distributed virtual firewall provided by ECS. It controls the traffic between ECS instances.

Cloud Firewall consists of the Internet firewall, VPC firewall, and internal firewall. These firewalls are used to provide protection for the Internet traffic, VPC networks, and ECS instances.

Unique features of Cloud Firewall

Compared with security groups, Cloud Firewall supports the following unique features:

- Supports access control on applications. For example, you can set HTTP as Allow in access control policy configuration, so that HTTP services can run on any port.
- Supports access control based on domain names. For example, you can allow all ECS instances to send requests to *. aliyun . com only.
- Support address books. You can add multiple IP addresses, ports, or ECS instances with the same tags to an address book and use this address book in access control configuration. This simplifies your configuration.
- Supports intrusion prevention system (IPS). You can use IPS to detect and fix common system vulnerabilities.
- Prevents brute force password cracking.
- Monitor and overall logs for blocked traffic analysis.

Enhanced features of Cloud Firewall

Compared with Security groups of ECS, certain features have been enhanced in Cloud Firewall. The internal firewall is based on the capabilities of security groups. You can go to the Access Control -> Internal Firewall tab page to create policies or go to the security group page in ECS console to create rules. The policies and rules in both Cloud Firewall and ECS Security groups are automatically synchronized.

The following features of Cloud Firewall are enhanced:

- You can release multiple policies at the same time.
- Policy group templates are supported.
- Security groups can be automatically created based on application groups.
- By default, ECS instances in the same security group cannot communicate with each other.

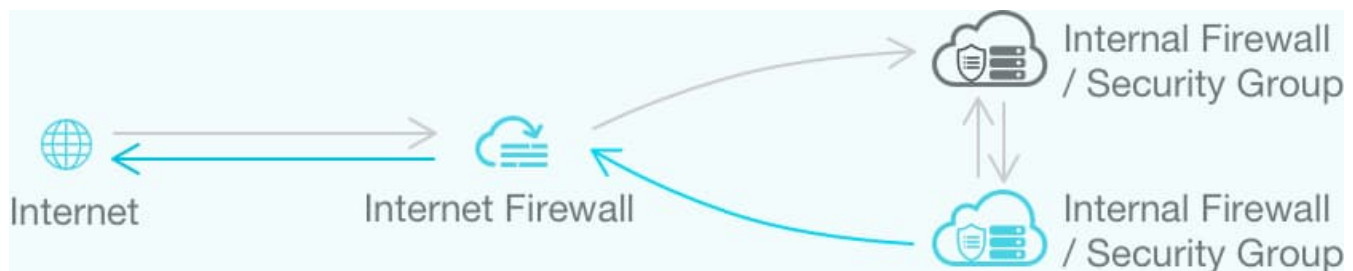
Internet firewall, VPC firewall, and internal firewall

Cloud Firewall consists of the Internet firewall, VPC firewall, and internal firewall. These firewalls are used to provide protection for the Internet traffic, VPC networks, and ECS instances.

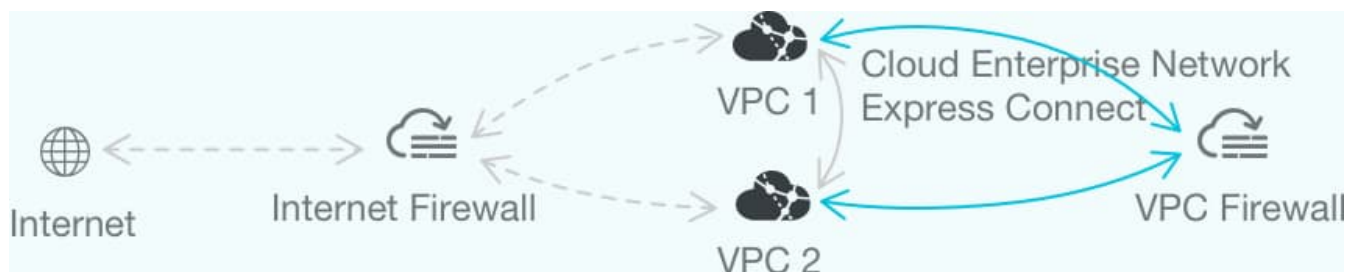
The Internet firewall is deployed at the border between Internet and internal network, and monitors the traffic with public IP addresses.

The internal firewall works in the same way as security groups to manage the traffic between ECS instances.

The following figure shows how the Internet firewall and internal firewall work and where they are deployed in the network topology:



The VPC firewall is deployed at the border of the VPC networks to manage the traffic forwarded through Express Connect. The following figure shows how the VPC firewall works and where it is deployed in the network topology:



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

- Cloud Firewall provides centralized access control, including inbound and outbound policies, to support more precise control of 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 micro-segmentation, Cloud Firewall provides distributed access control. Currently, Cloud Firewall is based on the capabilities of security groups. It offers visualized analysis of internal network traffic, allowing you to tune internal policies. The monitor mode, blocked network traffic analysis, and threat intelligence features will be soon available.

Cloud Firewall allows you to configure firewalls based on network borders to build multiple logical protection systems. This makes your maintenance work much easier. If you only need to protect the external traffic, then you can configure Internet border firewall policies (inbound and outbound policies) in the south-north direction. If you need to protect your ECS instances, you can configure internal firewall policies (internal policies) for ECS instances.

5 How to set priority for access control policy?

The priority of access control policies determines the order of the policies to be validated against the network traffic.

- Internet Firewall

For inbound and outbound policies of the Internet Firewall, the greater the value, the lower the priority.

As shown in the following figure, when a request reaches the Cloud Firewall, it is matched against the policies with priorities from 1 to 8. If the request matches an Allow policy, then it is allowed to pass through. If it matches a Deny policy, then this request/traffic is blocked.



Note:

The priorities of the Internet firewall policies must be unique.

Cloud firewall		Access Control						
		Internet Firewall Internal Firewall VPC Firewall						
		Show Guide Address Books						
		Outbound Policies Inbound Policies						
		Create Policy Search by source Search by destination Enter a description Protocol Policy Action Search						
		Priority	Source	Destination	Port/Application/Port	Policy Action	Description	Hits
		1			TCP/HTTP/8080	Deny		4
		2			TCP/SMTP/25443	Allow		6
		3			TCP/HTTP/8080	Monitor		0
		4			TCP/HTTPS/443	Allow		0
		5			TCP/SSH/2222	Deny		0
		6			TCP/HTTP/8080	Deny		0
		7			ICMP/ANY	Deny		25
		8			TCP/HTTP/8080	Monitor		3

- Internal Firewall

The priority of Internal Firewall policies are similar to that of security groups. The greater the value, the lower the priority. For internal firewall policies, valid priority values are from 1 to 100. Different policies can be assigned with the same priority. For policies assigned with the same priority, Deny policies are applied first.

6 How to troubleshoot network connection failures

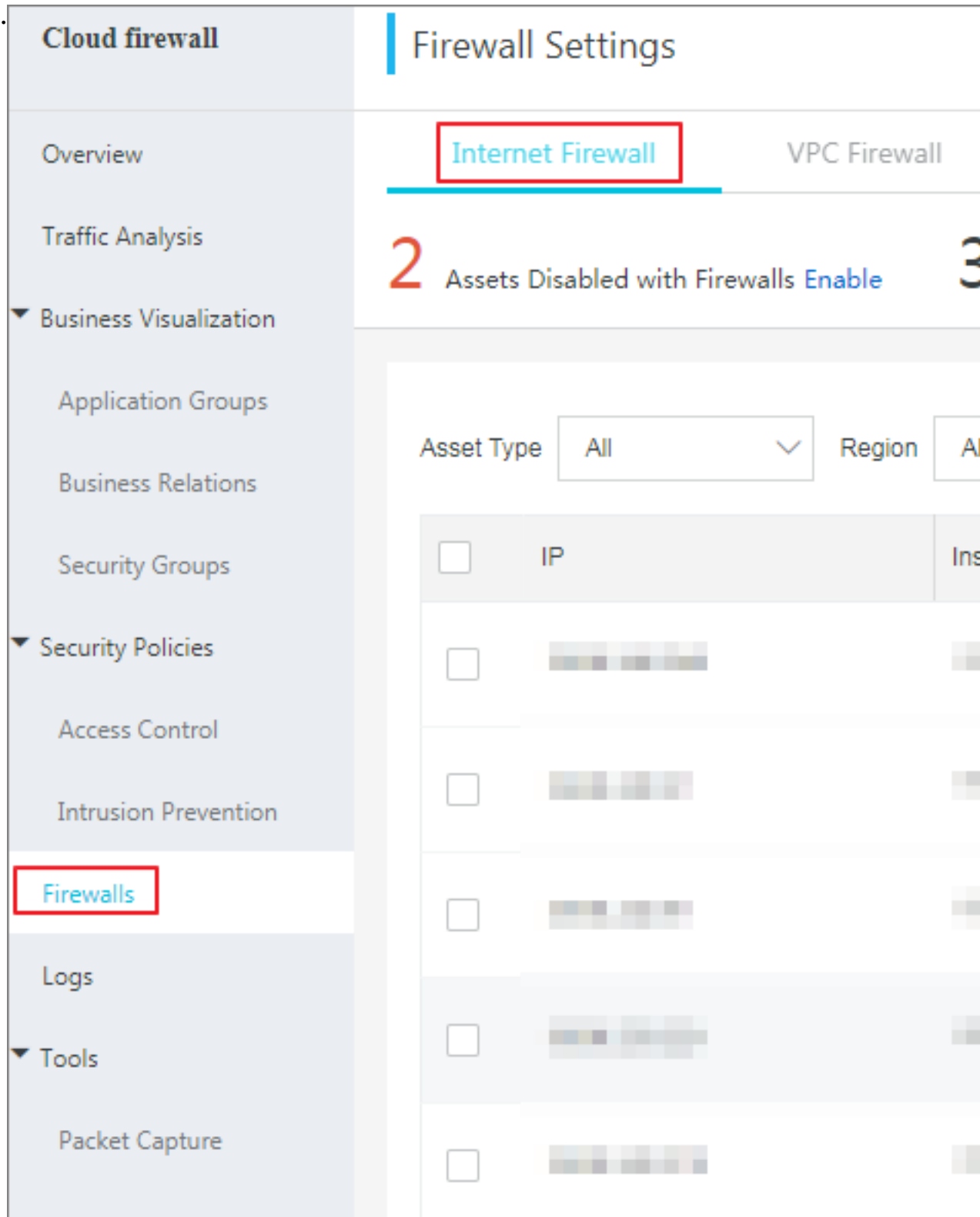
Symptom

After you enable the Cloud 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.

The screenshot displays the Cloud Firewall management console. On the left is a navigation sidebar with the following menu items: Cloud firewall, Overview, Traffic Analysis, Business Visualization (expanded), Application Groups, Business Relations, Security Groups, Security Policies (expanded), Access Control, Intrusion Prevention, Firewalls, Logs (highlighted with a red box), Tools (expanded), and Packet Capture. The main content area is titled 'Logs' and features two tabs: 'Event Log' and 'Access Log' (highlighted with a red box). Below the tabs, there are filters for 'Internet boundary ...' and 'Source IP'. A date range selector shows '2019-04-29 10:08' to '2019-04-29 11:08'. A table lists log entries with columns for 'Time' and 'Source IP'. Each entry shows a time range (e.g., 'From : 2019-04-29 11:08 To : 2019-04-29 11:10') and a corresponding source IP address, with a circular icon to the right of each IP.

Time	Source IP
From : 2019-04-29 11:08 To : 2019-04-29 11:10	[Redacted IP] ...
From : 2019-04-29 11:08 To : 2019-04-29 11:10	[Redacted IP] ...
From : 2019-04-29 11:08 To : 2019-04-29 11:09	[Redacted IP] ...
From : 2019-04-29 11:08 To : 2019-04-29 11:09	[Redacted IP] ...
From : 2019-04-29 11:08 To : 2019-04-29 11:09	[Redacted IP] ...
From : 2019-04-29 11:08 To : 2019-04-29 11:10	[Redacted IP] ...

- 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 Discardaction according to the information in the Criterion column.

The screenshot displays the Cloud Firewall management interface. On the left, a sidebar contains navigation options: Overview, Traffic Analysis, Business Visualization (with sub-items Application Groups, Business Relations, Security Groups), Security Policies (with sub-items Access Control, Intrusion Prevention, Firewalls), Logs (highlighted with a red box), and Tools (with sub-item Packet Capture). The main panel shows the 'Logs' section with the 'Event Log' tab selected (also highlighted with a red box). Below the tab is a search bar for 'Source IP' with the placeholder text 'Enter a source IP.'. A table of log entries follows, with columns 'Received At' and 'Type'.

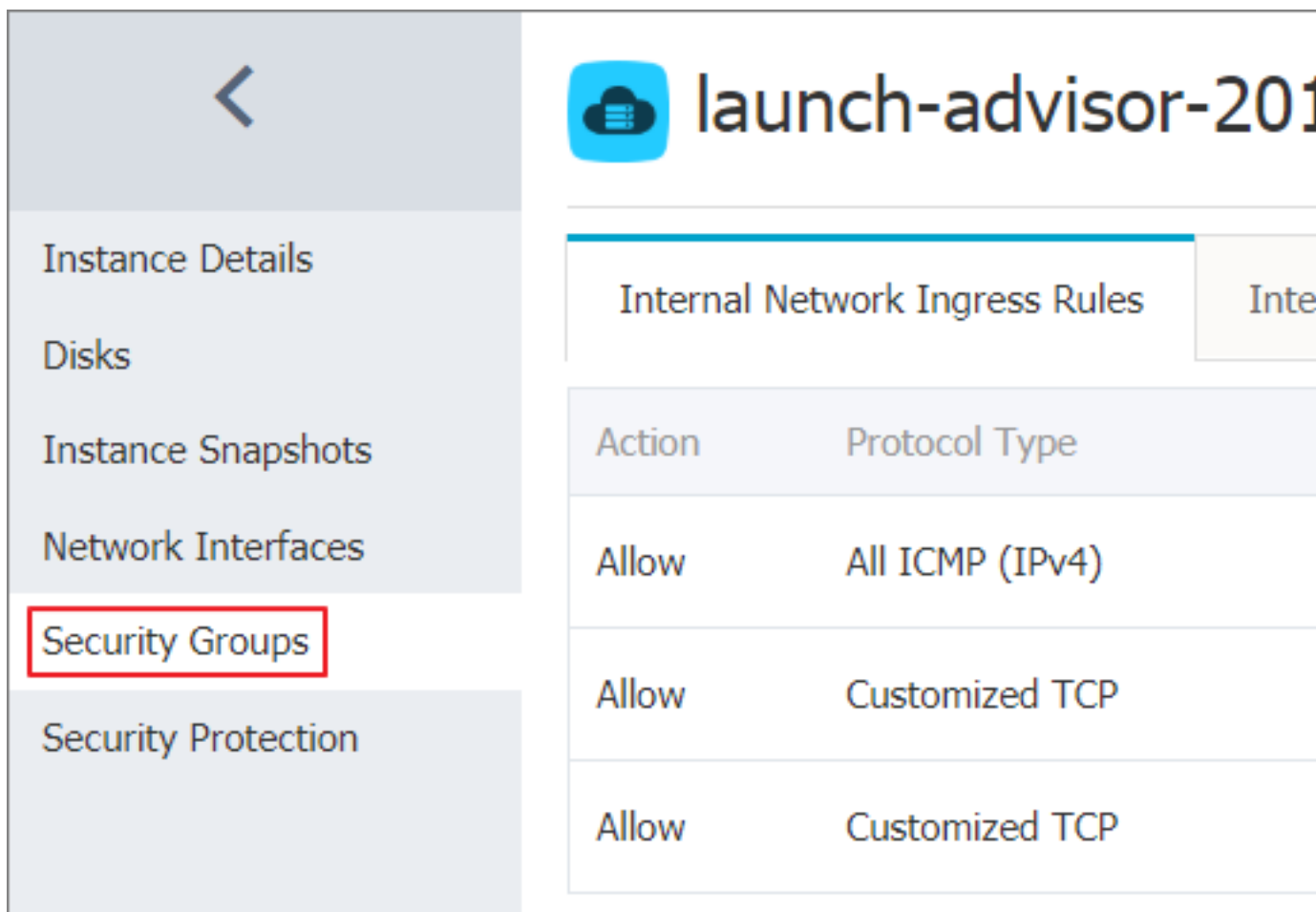
Received At	Type
2019-04-29 11:55	Scan
2019-04-29 11:54	Scan
2019-04-29 11:53	Mining Behavior
2019-04-29 11:53	Mining Behavior
2019-04-29 11:53	Mining Behavior
2019-04-29 11:53	Mining Behavior
2019-04-29 11:53	Mining Behavior
2019-04-29 11:52	Mining Behavior
2019-04-29 11:52	Mining Behavior
2019-04-29 11:52	Mining Behavior

- 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](#).

7 Functions of Internet Firewalls

You can enable the Internet Firewall for a single or multiple public IP addresses.

The following figure shows the routes of the network traffic when the Internet Firewall is enabled and disabled.



- When the Internet Firewall is disabled, the internet traffic with public IP is forwarded to the Internal Firewall or Security Group and then to the target ECS instances, without the need to pass through the Internet Firewall.
- When the Internet Firewall is enabled, the internet traffic with public IP is forwarded to the Internet Firewall for monitoring and filtering, then passed through Internal Firewall or Security Group and finally to the target ECS instances.

8 What's the influence of enabling/disabling Internet Firewall?

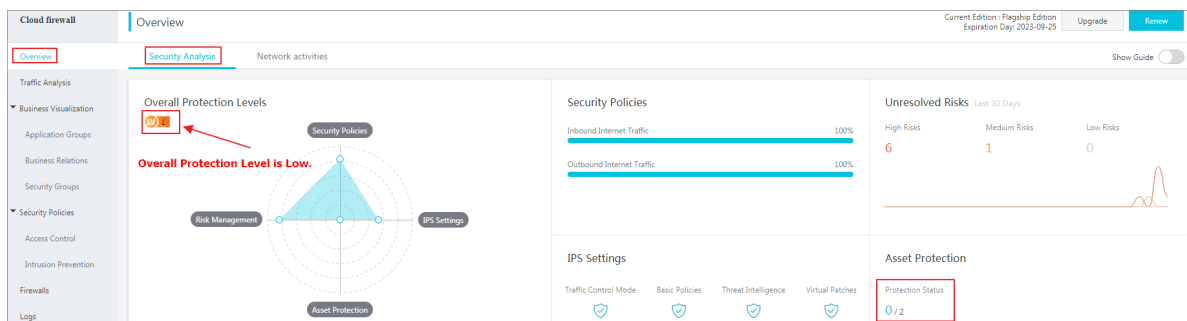
This topic describes the impacts of enabling and disabling the Internet Firewall.

The following figure shows the configuration of Internet Firewall.

Asset Type	Instance ID	Asset Type	Region	Bound Asset	Firewall Status	Actions
IP		ECS Public IP	China (Zhangjiakou)		Enabled	Disable Firewall
		ECS Public IP	China (Zhangjiakou)		Enabled	Disable Firewall
		ECS Public IP	China (Zhangjiakou)		Enabled	Disable Firewall
		ECS Public IP	China (Zhangjiakou)		Enabled	Disable Firewall

Disabling the Internet Firewall may have the following impacts:

- On the Overview > Security Analysis tab page, the Overall Protection Levels of your assets may be changed to Low. Less assets are protected, as shown under Asset Protection.



- On the Overview > Network Activities tab page, some network traffic analysis charts may fail to display the data.
- If you have configured inbound or outbound policies, these policies will become invalid after the Internet Firewall is disabled. You can find the policy hits of the affected server stays unchanged. This means the policy no longer takes effect.

- After you disable the Internet Firewall, network traffic no longer pass through the Cloud Firewall to reach its destination. This means that the intrusion prevention function no longer takes effect.

Even if the IPS is set to the Monitor mode, IPS no longer detects network traffic on the instance, and the Traffic Control mode of IPS is invalid then.

- After the Internet Firewall is disabled, Network traffic statistics generated are not displayed on the Logs > Access Log tab page.

For more information, see [Enable or disable the Cloud Firewall service](#).

9 Why certain assets are missing in Internet Firewalls?

For those cloud products don't support enable Cloud Firewall, or the asset is only assigned with a private IP, then the Internet Firewall is unavailable to these asset, and you cannot find them in Internet Firewall setting list.

The Internet Firewall is unavailable to the cloud assets in the following situations:

- The asset is assigned with the public IP which is not supported by Internet Firewall , such as an SLB public IP address.
- The asset is assigned with only the private IP address.
- The asset is not owned by the account that has purchased Cloud Firewall.

The public IP supported by Internet Firewall are as follows:

- EIPs. You can bind EIPs to your ECS instances in VPC network, SLB instances in VPC network, ENIs, and NAT gateways.
- ECS public IP addresses (NatPublicIP).

10 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](#).

11 Differences between Cloud Firewall Basic for Finance Cloud and other editions

You can upgrade Cloud Firewall Basic to Cloud Firewall Pro or Enterprise in the following situations:

- You want to know the EIPs and ports that are enabled for your businesses in the cloud, and the risks of enabling these IP addresses and ports.
- You need to save a log that contains records over the last six months for security regulation and compliance requirements.
- You need to control network access based on domain names. You want to control requests sent from your instances to the Internet and only allow requests destined for the specified domain names and IP addresses.
- You need to control network access based on the applications that use the FTP and MQTT protocols.
- In addition to Finance Cloud in the China (Hangzhou) region, you also need to use Cloud Firewall to protect resources in other regions.

Differences between Cloud Firewall Basic for Finance Cloud and other editions

Basic for Finance Cloud

in

for

Finance

Cloud

in

the

China

(

Hangzhou

)

region

Firewall

control

based

on

IP

addresses

and

ports

.

Describe

n
for

Finance

Cloud

in

the

China

(

Hangzhou

)

region

Access

.

control

based

on

applicatio

ns

.

Describe

n
for

Finance

Cloud

in

the

China

(
Hangzhou
)

region

Access

.
control

based

on

domain

names

.
External

.
connection

detection

.

Basic

n

for

Finance

Cloud

in

the

China

(

Hangzhou

)

region

Basic

Prevention

•

detection

•

Virtual

patches

•

Threat

intelligen

ce

•

Network

•

access

activities

•

~~Describe~~

n
for

Finance

Cloud

in

the

China

(
Hangzhou
)

region

~~External~~

.
connection
s

.
~~Intrusion~~
. prevention

activities

~~IPS~~
. analysis
.

~~All~~

access

activities

.

Basic for Finance Cloud

n
for

Finance

Cloud

in

the

China

(

Hangzhou

)

region

Logs

.

include

the

security

log

,

access

log

,

and

operation

log

.

Newly

created

Describe

n
for

Finance

Cloud

in

the

China

(

Hangzhou

)

region

Network

:

segmentation

on

visualizat

ion

and

business

topology

visualizat

ion

.

Describe

n
for

Finance

Cloud

in

the

China

(
Hangzhou
)

region

Micro

segmentati
on

(
access

control

in

the

east

-
west

direction
).

Basic for Finance Cloud

in
for

Finance

Cloud

in

the

China

(

Hangzhou

)

region

Supported

.

regions

(

Hangzhou

)

regions

supported

.

Supported

.

Cloud

.

Basic for Finance Cloud

n
for

Finance

Cloud

in

the

China

(

Hangzhou

)

region

Basic for Finance Cloud

é

Internet

Writer

/

firewall

.

Upgradable

).

Basic for Finance Cloud

n
for

Finance

Cloud

in

the

China

(
Hangzhou
)

region

Basic for Finance Cloud

÷
segmentati
on

ECS

is

instances

not

Upgradable

supported

supported

by

micro

-

segmentati

on

.

Describe

n
for

Finance

Cloud

in

the

China

(

Hangzhou

)

region

Maximum

EIPs

.

of

EIPs

supported

by

each

firewall

.

Basic for

n
for

Finance

Cloud

in

the

China

(
Hangzhou
)

region

Maximum

,
policies

•
policies

•
policies

•