Alibaba Cloud Cloud Firewall

User Guide

Issue: 20190530

MORE THAN JUST CLOUD | **[-]** Alibaba Cloud

<u>Legal disclaimer</u>

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.
A	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 informatio n, 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 cd / d C :/ windows command to enter the Windows system folder.
Italics	It is used for parameters and variables.	bae log list instanceid Instance_ID
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	ipconfig [-all -t]

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

Contents

Legal disclaimer I
Generic conventionsI
1 Cloud Firewall overview1
1.1 Authorize Cloud Firewall1
1.2 Upgrade and renewal2
1.3 Security analysis3
1.4 Network activities9
2 Network traffic analysis13
2.1 Traffic analysis overview13
2.2 External connections13
2.3 Internet access17
2.4 Intrusion detection21
2.5 IPS analysis23
2.6 All access activities27
3 Log analysis
3.1 Overview
3.2 Log analysis billing method32
3.3 Enable the log analysis service34
3.4 Collect the log
3.5 Fields in the log entry
3.6 Export log entries
3./ Authorize RAM user accounts with Log Analysis function
3.8 Manage log storage 45

1 Cloud Firewall overview

The Overview page provides full security analysis data and network activity information about your assets, and displays your current edition and estimated expiration time. Additionally, you can upgrade or renew the Cloud Firewall service on this page.

1.1 Authorize Cloud Firewall

In the latest version of Cloud Firewall, the Internet access analysis feature is included. To enable this feature, Cloud Firewall has to display your IP addresses and port information. Therefore, you must grant Cloud Firewall the permission to call the SLB API.

Background

To grant Cloud Firewall the access to cloud resources, you must have one of the following accounts:

- An Alibaba Cloud primary account
- $\cdot\,$ A RAM user account with the AliyunRAMFullAccess permission



You cannot use a *RAM user account* without the AliyunRAMFullAccess permission to grant Cloud Firewall the access to cloud resources.

Authorization procedure

1. Click Confirm Authorization Policy.

This grants Cloud Firewall the following permissions:

- AliyunCloudFirewallAccessingECSRole: Allows Cloud Firewall to access ECS instances.
- AliyunCloudFirewallDefautlRole: Allows Cloud Firewall to access other cloud services, such as OSS and SLB.

Cloud Resource Access Authorization			
Note: If you need to modify role permissions, please go to the RAM Console. Role Management. If you do not configure it correctly, the following role: CloudFirewall will not be able to obtain the required permissions.	×		
CloudFirewall needs your permission to access your cloud resources.			
Authorize CloudFirewall to use the following roles to access your cloud resources.			
AliyunCloudFirewallAccessingECSRole	~		
Description: The Cloud Firewall service will use this role to access ECS.			
Permission Description: The policy for AliyunCloudFirewallAccessingECSRole, including the permission for ECS.			
AliyunCloudFirewallDefautIRole	~		
Description: Cloud Firewall will use this role to access your resources in other services.			
Permission Description: The policy for AliyunCloudFirewallDefaultRole.			
Confirm Authorization Policy Cancel			

After the authorization is complete, the system automatically returns to the Cloud Firewall console.



AliyunCloudFirewallAccessingECSRole and AliyunCloudFirewallDefautlRole are default permissions and are both required.

1.2 Upgrade and renewal

Cloud Firewall includes the Pro Edition, Enterprise Edition, and Flagship Edition. You can upgrade Cloud Firewall to the required edition for more features.

Click Upgrade or Renew in the upper-right corner of the Overview page in the Cloud Firewall console to upgrade or renew the Cloud Firewall service.

Cloud firewall	Overview	Current Edition : Enterprise Edition Upgrade Renew Expiration Day: 2020-09-25	
Overview	Security Analysis Network activities		Show Guide
Traffic Analysis			
 Business Visualization 	Overall Protection Levels	Security Policies	Unresolved Risks Last 30 Days
Application Groups	W H	Inbound Internet Traffic 100%	High Risks Medium Risks Low Risks
Business Relations		Outbound Internet Traffic 100%	4 1 0
Security Groups			
 Security Policies 	Risk Management OF Figure 100 (IPS Settings		
Access Control			
Intrusion Prevention		IPS Settings	Asset Protection
Firewalls		Traffic Control Basic Threat Virtual Mode Policies Intelligence Patches	Protection Status
Logs	Asset Protection		271/274
▼ Tools			

For more information on the features available in each edition, see *Features*.

For more information on the upgrade and renewal operations, see Service renewal and upgrade.



Renew the Cloud Firewall service in a timely manner before it expires to ensure that you can use the service properly.

1.3 Security analysis

In Security Analysis page, you can view the Overall protection level of hosts and scores of the four protection items in real time. Stricter configuration of the four protection items means a higher overall protection level and stronger protection for your assets.

Overall protection levels include high (H), medium (M), and low (L). The four protection items are:

- Security Policies
- · Risk Management
- · IPS settings
- Asset protection

Cloud firewall	Overview	Current Edition : Flagship Edition Expiration Day: 2023-09-25	Upgrade Renew	
Overview	Security Analysis Network activities			Show Guide
Traffic Analysis				
 Business Visualization 	Overall Protection Levels	Security Policies	Unresolved Risks Last 30 Days	
Application Groups	(V) H Security Policies	Inbound Internet Traffic 100%	High Risks Medium Risks	Low Risks
Business Relations		Outbound Internet Traffic 100%	5 1	0
Security Groups				
 Security Policies 	Risk Management			
Access Control				
Intrusion Prevention		IPS Settings	Asset Protection	
Firewalls		Traffic Control Mode Basic Policies Threat Intelligence Virtual Patches	Protection Status	
Logs	Asset Protection	$\bigcirc \oslash \oslash \oslash$	303 / 305	
Tools				

Security Policies

The Security Policies modules displays the percentage of the assets for which access control policies are configured in all your assets. The access control policies include those for outbound traffic to the Internet (in-out traffic) and those for inbound traffic from the Internet (out-in traffic).

Security Policies				
Inbound Internet Traffic	100%			
Outbound Internet Traffic	100%			

Click in this area to go to the Access Control page. On the Inbound Traffic and Outbound Traffic tab pages, you can configure access policies. The stricter the access policies are configured, the higher the score of this protection item.

Unresolved risks

The Unresolved Risks area displays the number of abnormal activities that have not been resolved within the last 30 days and the corresponding risk levels.

Unresolved Risks Last 30 Days				
High Risks	Medium Risks	Low Risks		
5	1	0		

Click in this area to go to the Intrusion Detection tab page of the Network Traffic Analysis page, you can view and process threat activities detected by Cloud Firewall. The earlier the intrusions are handled, the higher the score.

The IPS Settings area displays the status of all IPS features on Cloud Firewall.

IPS features include:

- · Interception mode or observation mode
- Basic rules
- · Threat intelligence
- Virtual patching



Click in this area to go to the Intrusion Prevention page. On this page, you can enable or disable the interception mode, basic policies, threat intelligence, and virtual patches features of IPS.

For more information, see Intrusion prevention policies.



You can quickly determine whether an IPS feature is enabled based on the protection status icon displayed in the lower part of the IPS Settings area.

Asset protection

The Asset Protection module displays the number of assets that have been protected by Cloud Firewall.

Asset Protection
Protection Status
303 / 305

Click in this area to go to the Firewall page. On this page, you can enable or disable Cloud Firewall protection for your assets. The more assets are protected by Cloud Firewall, the higher the score of this protection item.

For more information, see Turn on or off the Cloud Firewall switch.

Inbound/Outbound Internet Traffic

The Inbound or Outbound Internet Traffic module displays trend charts for inbound traffic from and outbound traffic after Cloud Firewall protection is enabled. You can view the trends of total sessions and intercepted sessions, and locate the time point when a session is intercepted. Then, you can check whether an abnormal event occurs at the time point on the *IPS Blocking Analysis* or *Operation Logs* page.

After Cloud Firewall protection is enabled, click Yesterday, Today, or Seven Days in the upper-right corner of the Internet Inbound or Outbound Protection Trends area to view data in the specified time range.

Inbound Intern	et Traffic			Yesterday Today Last 7 Days
Average Block Percentage Today 0 .11 %				
Relative Change of Average Blocked Sessions Day on Day Change 7 .99 %	00:00	00:10	00:20	00:30
Outbound Inte	rnet Traffic			
Average Block Percentage Today 5.54 %				
Relative Change of Average Blocked				
Sessions Day on Day Change -23.04 %	00:00	00:10	00:20	00:30

You can view the following protection data for inbound or outbound traffic:

- Average Block Percentage: displays the percentage of the inbound or outbound sessions intercepted by IPS or access control in all sessions in the specified time range.
- Relative Change of Average Blocked Sessions: displays the change rate of the average number of intercepted sessions in the specified time range compared with the average number in the previous time range. The change rate is calculated as follows: (Number of intercepted sessions in the current time range - Number of intercepted sessions in the previous time range)/Number of intercepted sessions in the previous time range
- Click a certain time on the trend chart to view the total number of sessions, number of intercepted sessions, interception percentage, and interception change rate until that time point.

Inbound Interne Average Block Percentage Today 0.11 % Relative Change of	et Traffic		2019 To Bid In Block Relati	04-29 00:20:00 tal Sessions 23 ccked Sessions cccess Control ntrusion Preventior Percentage (ve Change 47	iay 3.21 K 25 0 1 25 0.10% 7.05%	Last 7 Days
Average Blocked Sessions Day on Day Change 7.99 %	00:00	00:10	00:20 0	00:	30	
Note:						

The Internet Inbound or Outbound Protection Trends area can display traffic protection trends only after Cloud Firewall protection is enabled. We recommend that you click Protect All on the Firewall page to enable Cloud Firewall protection for all assets.

News

The News area displays latest news about Cloud Firewall, such as updates of security intelligence, virtual patches, and IPS rules.

You can click Learn More in the upper-right corner of the Product News area to view all news about Cloud Firewall.



1.4 Network activities

The Traffic Analysis page displays network activities of your assets in real time. With traffic analysis, you can monitor the intrusion events, networks activities, trend of the traffic and your assets' external connection activities.

Cloud Firewall monitors the following network activities in real time:

- External connections
- Internet access
- VPC access
- · Intrusion detection
- · IPS analysis
- · All access activities

Network Traffic

In Network Traffic module, you can monitor the average and peak traffic of both inbound and outbound traffic.

Network Traffic		— Inbound — Outbound
Average Traffic Today	Peak Traffic Today	
Inbound 13.98 Mbps	Inbound 29.30 Mbps	
Outbound 13.97 Mbps	Outbound 29.21 Mbps	
	02:20 04:40 05:50 07:00 02:10 00:20 10:20 11:40 12	250 1400 1510 1620 1720 1840 1950 2100
00:00 01:10 02:20	03:30 04:40 05:50 07:00 08:10 09:20 10:30 11:40 12:	2:50 14:00 15:10 16:20 17:30 18:40 19:50 21:00

Click a certain time on the timeline of Network Traffic, you can view the specified inbound/outbound traffic.

Inbound and outbound traffic trend is displayed.

Inbound Traffic Trend	- Inbound - Outbound
Later Marin	philipt
Outbound Traffic Trend	— Inbound — Outbound
L. M. M. M. M. M.	phinnh

External Connections and Rankings

External Connections and Rankings module provides you with the top 5 unauthorized domains, assets and sessions for external connections.

External Connections and Rankings Learn More		
Unauthorized Domains External Connections (Total Traffic)	Assets External Connections (Total Traffic)	Sessions Destination IP
	36.39 K(38.43 MB)	25.05 K(54.40 MB
1	5.13 K(1.22 MB) = ECS	32.37 K(6.79 MB)
	4.77 K(1.63 MB) (======ECS)	21.85 K(10.24 MB
No data available	+ 2.50 K(537.54 KB) ECS	15.66 K(5.23 MB)
	■ ■ ■ 2.41 K(517.56 KB) ECS	5.87 K(5.43 MB)

Click Learn More to go to the External Connections for details of the external connection activities.

Intrusion Detection and Risk Levels

Intrusion Detection and Risk Levels module displays the proportion in percentage of the three risk levels (High, Medium, Low), and intrusion event list with the events details.

Intrusion Detection and Risk	k Levels	Intrusion	Events Learn More	e			
		Risk Level	Event Name	Asset Type	Instance ID/Name	Affected Asset IP	Occurred At
	High 83%	High	400 (Y 11)	ECS	2000	Public:	2019-04-28 23:42
	Medium 16%	High	and the state of t	ECS	2000	Public: Private:	2019-04-28 16:03
	Low 1%	High	4000	ECS		Public:	2019-04-28 16:02
		High	1000	ECS		Public: Private:	2019-04-28 11:30

Click Learn More to go to the Intrusion Inspection for details of internet traffic.

IPS Analysis

IPS Analysis module displays the traffic blocked by IPS functions of Cloud Firewall. You can view the proportion in percentage of the traffic blocked by different IPS strategies (Basic Protection and Virtual Patches), the top 5 most blocked source IP and destination IP.

	The Most Blocked Source IP Addresses Count	The Most Blocked Destination IP Addresses Count
	335	ECS Public IP
asic Protection 98.66%	······································	ECS Public IP
rtual Patches 1.33%	···· 45	ECS Public IP
	33	ECS Public IP
		ECS Public IP
	asic Protection 98.66% irtual Patches 1.33%	• The Most Blocked Source IP Addresses Count 335 335 107 107 133 33 33 107 1

Click Learn More to go to the IPS Analysis for details of the blocked traffic.

Internet Access Activities

In Internet Access Activities module, you can view the proportion on percentage of the normal/bot traffic and the top 5 most visited assets with the location and IP address.

Internet Access A	Activities I	earn More								
		Bot Traffi	ic		App	lications		The Most Visited Ass	sets	
Normal Traffic 99.36 %								10.000 33	ECS Public IP	42.59%
Bot Traffic								warmer like	SLB EP	13.73%
0.64 %		CDN 0.36%			45	SIP 5.38%		second int	ECS Public IP	4.08%
									ECS Public IP	3.62%
	CDN	Search Engine	Malicious Crawler	SIP	Unknown	HTTP	NetBIOS		ECS Public IP	3.00%
				QUIC						

Click Learn More to go to the Internet Access for details of the internet access activities.

VPC Access Activities

VPC Access Activities module display the traffic ranking of the VPC firewalls, the top 5 most blocked source IP and destination IP of VPC firewall.

Click Learn More to go to the VPC Access for details of the traffic between VPCs.

2 Network traffic analysis

2.1 Traffic analysis overview

Using traffic analysis, you can view intrusion events, network activities, traffic trends, access traffic blocked by IPS features, and external connection activities of hosts in real time. This provides visibility to traffic on the entire network.

Cloud Firewall monitors the following network activities in real time:

- External connections
- Internet access
- VPC access
- · Intrusion detection
- · IPS analysis
- · All access activities

2.2 External connections

The External Connections page displays the details on your assets' external connections, including the connected domain names, external IP addresses, the applied protocols and your assets' info. This helps you identify the suspicious assets activities in a timely manner.

Procedure

1. Log on to the Cloud Firewall console.

2. In the left-side navigation pane, go to Network Flow Analysis > External Connections to check your assets' external connection activities.

You can perform the follows operations on External Connections page:

• Monitor the overview of external connection data, including the amounts of external domains, external IP addresses, assets request for external connections and the relevant protocols.

Cloud firewall	Network flow analysi	S							
Overview	External Connections	Internet Access	VPC Access	Intrusion Detection 🕖	IPS Analysis	All Access / Recent 1 hou	rs 🗸 2019-04-27 20:59	- 2019-04-27 21:59 🛗	
Traffic Analysis Business Visualization	External Domains		External IP Ad	External IP Addresses			Protocol Analysis		
Application Groups	÷	•	+		÷		+		
Business Relations	0 Risky	10 AII	0 Risky	14 AII	1 Risky	261 AII	19.97 % Unidentified	3 All	

In the overview area of external connection data, risky event number and total number of each item are displayed.

Click the Risky or All button to go to the detailed external connection list.

• Monitor the outbound traffic analysis, including the average traffic and peak traffic.



In Outbound Traffic module, you can monitor traffic rate within the selected time range.

Click the time on the timeline, you can see the corresponding rankings for the most visited IPs of the outbound traffic. You can choose to display top 10, 20 or

50 outbound IPs by clicking the Rankings of IP Addresses by Traffic drop-down list.

Outbound Traffic	Ranking of IP	\sim	2019-04-24 15:00		
٩	IP	Туре	Request Rate ↓	Response Rate ↓	Actions
Peak Traffic Request Rate 2.17 Mbps Response Rate 50.97 Mbps		ECS Public IP	435.58 Kbps	8.72 Mbps	View Logs
Average Traffic Request Kate 575.78 Kbps Response Kate 14.45 Mbps		ECS Public IP	294.80 Kbps	8.45 Mbps	View Logs
57 Mbps 48 Mbps		ECS Public IP	45.57 Kbps	17.69 Kbps	View Logs
38 Mbps 04/24 15:04		ECS Public IP	4 Kbps	16.53 Kbps	View Logs
29 Mbps 18 Mbps 19 Mbps Mar Mar Mar Mar Mar Mar Mar Mar Mar Mar		ECS Public IP	3.96 Kbps	16.53 Kbps	View Logs
10 Mbps	10.00.00	ECS Public IP	3.99 Kbps	16.41 Kbps	View Logs
04/23 00:04	1.10.00	ECS Public IP	3.71 Kbps	15.11 Kbps	View Logs

• Monitor the Top 10/20/50 traffic of external connections, with the relevant IP address, request/response rate, and logs recorded by Cloud Firewall.

Ranking of IP	Addresses by T	raffic Top 50	^	2019-04-27 21:54
IP	Туре	Reque Top 50	sponse Rate √∖	Actions
	ECS Public IP	261.0 Top 10	43 Mbps	View Logs
	ECS Public IP	149.82 Kops	5.13 Mbps	View Logs
10.01	ECS Public IP	2.41 Kbps	8.46 Kbps	View Logs
4.10.01.01	ECS Public IP	42.63 Kbps	7 Kbps	View Logs
	ECS Public IP	2.40 Kbps	2.27 Kbps	View Logs
1.0	ECS Public IP	2.38 Kbps	1.11 Kbps	View Logs
	ECS Public IP	191 bps	641 bps	View Logs

Click View Logs, Logs > Access Log is displayed, and automatically filtered with Outbound direction. You can check the details on the Outbound traffic,

•

including the time of access, source/destination IP and port, access application, protocol, bytes/packets of the access traffic, and applied access control policy. Monitor the protocol analysis for external connections, including the information on applications, ports and corresponding connection numbers.



If you need to monitor certain ports for external connections, click Follow to add the ports to the Protocol Details list. Details of the ports are displayed in the list.

Protocol Analysis	Protocol Details					Follow / Ignore
Applications	Application	Port	Requests	Responses	Visits	Actions
	HTTPS	443	20.76 MB	14.73 MB	2.57 K	More 🗸
HTTPS 22.91%	HTTP	80	1.67 MB	1.76 MB	1.22 K	More 🗸
		3333	164.72 MB	3.61 GB	111	
HTTPS Unknown HTTP		4343	606.54 KB	0B	1.26 K	Unfollow Ignore
Ports Used by Applications Conr Unfollow		65283	56.23 KB	28.36 KB	55	E View Logs
2.57 K 🗙 🖉		43	16.68 KB	36.60 KB	36	More V
		33479	94 B	0B	1	More 🗸
		33490	94 B	0B	1	More V
	- Onknown	33474	94 B	0B	1	More 🗸

- View the protocol details, and Follow/Ignore or View the Logs of the specified protocols.
- Monitor the detailed outbound traffic list, including external domains, IP addresses and assets.

External Domains Ext	ternal IP Addresses	Assets			Recent 1	h ∨ 2019-04-28 13:15	5 - 2019-04	28 14:15 🛗
Total External Domains : 10	Domains Not Covered	by Policies : 🛛 📄 Risky	Domains : 0 🔳 Doma	ins Followed : 1 🔳 Do	mains Ignored : 3			Follow / Ignore
All Products 🗸 All Categories	✓ All Tags	All Suggesti V	Policy Coverage \checkmark	ECS Public IP \checkmark		Search		
Domain Name	Traffic	Requests√	Category	Tag	Suggestion	Policy Coverage	Actions	
	Request Rate : 572.02 KB Response Rate : 254.26 KB	404	CJ Alibaba Cloud Products	-	🏀 Allow	Full Coverage	View Details	More 💛
	Request Rate : 15.34 MB Response Rate : 2.43 MB	199	reputation website	Popular website	🏀 Allow	Full Coverage	View Details	More 🔨
-	Request Rate : 111.91 KB Response Rate : 587.39 KB	152	-	-	🔞 Monitor	Full Coverage	View Details	More 🔨
2010.00	Request Rate : 142.14 MB Response Rate : 3 GB	98	-	-	🔞 Monitor	Full Coverage	View Details	More 🔨

In the Action column, you can view details or logs, follow/unfollow or ignore the specified external domain/IP address.

Click View Details to open the details page of external domain/IPs.

Cloud firewall						External IP Address	es				>	
						Basic Information						
Traffic Analysis	Total External IP Addresses : 12 A IP Addresses Not Covered by Policies : 3 A Risky IP Ad				A Risky IP Ade	Destinati on Informati		 Status 			 Suggesti on 	
 Business Visualization 	All Products V	All Categories 🗸	All Tags 🗸 🗸	All Suggesti 🗸	Policy Cove	Destination IP:115.28.1	22.198	Category : All Alib	aba Cloud		۲	
Application Groups					-	Location : Qingdao		And a second second			Allow	
Business Relations	Destination IP	Applications/Ports	Traffic	Sessions↓↑	Categ	ISP : Alibaba Cloud		Tag : -				
Security Groups	120.25.115.20 🌸	NTP/123 1个	Request Rate : 61.34 KB Response Rate : 61.34 KB	571	cə /							
Access Control	115.28.122.198 ★	NTP/123 1个	Request Rate : 990 B Response Rate : 0B	9	сэ ⁴	Applications/Ports 共1组 NTP/123					Show ~	
Firewalls	120.25.108.11 👻	NTP/123 1个	Request Rate : 330 B Response Rate : 330 B	3	co A	GAffected Assets	Duble D V		Comt			
▼ Tools	203.107.6.88	NTP/123 1个	Request Rate : 165.75 KB Response Rate :	1.54 K	c3 ^A	ECS IP	Occurred At	Traffic	Requests√	Policy Coverage	Actions	
Packet Capture	47 92 219 128	Unknown/ 1个	Request Rate :	4.24 1/			13:37 Last Time:2019-04-28	Request Rate : 990 B Response Rate : 0B	9	Full Coverage	View Logs	

2.3 Internet access

The Internet access tab page in the Cloud Firewall console provides an overview of normal and abnormal inbound traffic details of your assets.

You can view the open applications, ports, public IP addresses, cloud products info, inbound internet traffic, and the internet access list with details.

Cloud firewall	Network flow analysis												
Overview	External Connections Internet Access	VPC Access Int	trusion Detection 🕖 IPS Anal	lysis All Access Activities						L	ast 7 D 🗸 201	9-04-21 00:1 - 20	19-04-28 00:1 10
Traffic Analysis	Open Applications		Open Ports			Open Public IP 4	Addresses			Cloud Produ	icts		
 Business Visualiza 	open appreciations					open r ubite ir y	-uuresses			ciouurrout			
Application Groups	• • •					•				Public SLB			
Business Relations	6 Risky 11 All		79 Risky	159 All		141 Risky 267 All O Public				0 Public IP		0 Open Ports	
Security Groups													
 Security Policies 	Inbound Internet Traffic								Ranking of IP	Addresses by Tr	affic Top 50	~	2019-04-27 23:00
Access Control		Q							IP	Туре	Request Rate	Response Rate	Actions
Intrusion Filtewalitzion	Peak Traffic Request Rate 3.75 Mbps Re Average Traffic Request Rate 585.73 Kbps	wak Traffic Request Rate 3/3 Mbps Response Rate 44.07 Mbps werage Traffic Request Rate 555/3 Kbps Response Rate 34.69 Mbps										21 Mbps	View Logs
Logs	48 Mbps						Response Rate	Request Rate		ECS Public IP	561.31 Kbps	0	View Logs
 Tools Packet Capture 	29 Mbps 19 Mbps	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Am				$\sim M \sim M$	·~~		ECS Public IP	69.53 Kbps	139.39 Kbps	View Logs
	10 Mbps					$\sim \sim$	v·· · ·	VV.		ECS Public IP	7.12 Kbps	20 bps	View Logs
Technical Support	04/21 00:04	04/23 00.04	4	04/25 00:04			04/27 00:04			ECS Public IP	5.08 Kbps	49 bos	View
	Open Applications Open Ports	Open Public IP Addresses	Details Cloud Produc	ts									
	All Risk L V All Sugge V All A	pplic V Search by port	2. Search										
	Application Protocol	Port	Public IP Addresses	Total Ports	Percenta	ge (7 Days)	Risk Level		Threat	Suggestic	n	Actions	
	FTP_DATA tcp	9046 ③	1	1	<0.1 %	9	High		BruteForce,S niffing,Over	💫 Chec	ĸ	View Details	
	Unknown tcp	22,80 121A ③	153	4970	99.9 %)	Low			🚳 Unkr	own	View Details	

Procedure

1. Log on to the Cloud Firewall console.

2. In the left-side navigation pane, go to Traffic Analysis > Internet Access to check your assets' internet access activities.

You can perform the follows operations on Internet Access page:

• Monitor the overview on internet access traffic, including the amounts of open applications, open ports, open public IP addresses, and cloud products.



In the overview area of internet access, risky event number and total number of



detailed internet access list.

Monitor the inbound internet traffic, including the average traffic and peak traffic.



In Inbound Internet Traffic module, you can monitor traffic rate within the selected time range.

Click the time on the timeline, you can see the corresponding rankings for the most visited IPs of the inbound traffic. You can choose to display top 10, 20 or 50 inbound IPs by clicking the Rankings of IP Addresses by Traffic drop-down list.

Inbound Internet Traffic	Ranking of IP Addresses by Traffic Top 50 V				2019-04-25 17:00
Q	IP	Туре	Request Rate ↓	Response Rate ↓↑	Actions
Peak Traffic Request Rate 3.75 Mbps Response Rate 44.07 Mbps		ECS Public IP	473.13 Kbps	13.86 Mbps	View Logs
Average Traffic Kequest Rate 581.97 Kbps Kesponse Rate 14.39 Mbps Response Rate Response Rate Rate Response Rate Response Rate Rate Rate Rate Rate Rate Rate Rat	100.00	ECS Public IP	4.58 Kbps	7.56 Kbps	View Logs
48 Mbps		ECS Public IP	3.67 Kbps	69 bps	View Logs
29 Mbps 04/25 17/04	10.00	ECS Public IP	3.66 Kbps	30 bps	View Logs
19 Mipps Windows Rate 14 Mipps		ECS Public IP	3.65 Kbps	20 bps	View Logs
10 Mbps	1000	ECS Public IP 3.65 Kbps 14	140 bps	View Logs	
04/23 00:04 04/25 00:04 04/27 00:04	10.00	ECS Public IP	3.65 Kbps	58 bps	View Logs

• Monitor the Top 10/20/50 internet access traffic with the relevant IP address, request/response rate, and logs recorded by Cloud Firewall.

Ranking of IP A	ddresses by Traf	fic Top 50 /		2019-04-28 16:00
IP	Туре	Re: Top 50 Top 20	Response Rate√	Actions
	ECS Public IP	45. Top 10	13.86 Mbps	View Logs
	ECS Public IP	29.65 Kbps	31.12 Kbps	View Logs
11 Mar 10	ECS Public IP	29.03 Kbps	28 Kbps	View Logs
	ECS Public IP	28.73 Kbps	27.64 Kbps	View Logs
	ECS Public IP	28.66 Kbps	27.64 Kbps	View Logs
	ECS Public IP	28.51 Kbps	27.50 Kbps	View Logs
	ECS Public IP	27.54 Kbps	26.51 Kbps	View Logs

Click View Logs, Access Log in Logsis displayed, and automatically filtered with Inbound direction. You can check the details on the inbound traffic, including the time of access, source/destination IP and port, access application, protocol, bytes/packets of the access traffic, and applied access control policy.

Monitor the detailed inbound traffic list, including the open applications, protocols, open ports, open public IP addresses and inbound traffic of the cloud products.

Open Applic	Open Applications Open Ports Open Public IP Addresses Details Cloud Products								
All Risk Levels	✓ All Suggesti ∖	All Applicatio V Sea	rch by port.	Search					
Application	Protocol	Port	Public IP Addresses	Total Ports	Percentage (7 Days)	Risk Level	Threat	Suggestion	Actions
FTP_DATA	tcp	9024,9046 ④	2	2	<0.1% 🗐	High	State and a	Check	View Details
Unknown	tcp	80,443 💮 🕀	157	5090	99.9% 🗎	Low	-	Unknown	View Details
HTTP	tcp	80,90	156	1807	<0.1%	Low		Check	View Details
RDP	tcp	1001,8092	139	2600	<0.1%	Low	BruteFore	Check	View Details

In Action column, click View Details to open the details page of internet access traffic.

2.4 Intrusion detection

The Intrusion Detection page displays the intrusions and details detected by IPS.

Procedure

- 1. Log on to the Cloud Firewall console.
- 2. In the left-side navigation pane, click Traffic Analysis to go to the network flow analysis page.

3. Click Intrusion Detection and view the intrusion event list.

Cloud firewall	Network	Network flow analysis								
Overview	External	External Connections Internet Access VPC Access Intrusion Detection 3 IPS Analysis All Access Activities								
Traffic Analysis Business Visualization	All Risk Le	vels 🗸 All Events	V Unhandled/	✓ Not Ignored ✓	2019-03-29 19:09 - 2019-04-28 19:09 🛗 Ins	stance IP V Fuzzy search is supported.	Search			
Application Groups	Risk Level	Event Name	Asset Type	Instance ID/Name	Affected Asset IP	Occurred At	Status	Actions		
Business Relations	High	1000000	ECS		No. 10 (1971), Talk 110 (1971)	2019-04-28 20:36	Blocked	Block Ignore View Details		
Security Groups Security Policies	High		ECS		No. 12 (1971), Talk 112 (1972)	2019-04-28 16:03	Blocked	Block Ignore View Details		
Access Control	High	10000000	ECS		NAME OF ADDRESS OF ADD	2019-04-28 16:02	Blocked	Block Ignore View Details		

- In the intrusion event list, you can view the details about all intrusion events. The details include the risk level, IP address of the affected asset, and event processing status.
- You can specify conditions such as the risk level, processing status, detection time range, and instance IP address to search for a single intrusion

event.	Network flow analysis	
	External Connections Internet Access	VPC A
	All Risk Levels V All Events V Unhandled/	~

• If you determine that an intrusion event is a normal activity, click Ignore in the Action column to ignore the event.

Cloud firewall	Network	Network flow analysis							
Overview	External	Connections Inter	net Access	VPC Access Intrusi	on Detection 🗿 IPS Analysis Al	Access Activities			
Traffic Analysis	All Risk Lev	rels 🗸 🛛 All Events	Vunhandled/	✓ Not Ignored ✓	2019-03-29 19:09 - 2019-04-28 19:09 🛗	Instance IP ∨ Fuzzy search is supported.	Search		
 Business Visualization Application Groups 	Risk Level	Event Name	Asset Type	Instance ID/Name	Affected Asset IP	Occurred At	Status	Actions	
Business Relations	High	1000000	ECS		148 (1.167) (188 (1.177))	2019-04-28 20:36	Blocked	Block Ignore View Details	
Security Groups Security Policies	High	10000000	ECS		No. 10 (1976) (No. 110 (1976)	2019-04-28 16:03	Blocked	Block Ignore View Details	
Access Control	High		ECS	10000000	NUMBER OF STREET, STRE	2019-04-28 16:02	Blocked	Block Ignore View Details	
	ote:								

An ignored intrusion event is removed from the intrusion event list. Cloud Firewall no longer reports alarms for this event.

 Click View Details in the Action column to go to the details page of an intrusion event and view the event details and security suggestions. You can also enable or disable IPS features on the Event Details page.

Cloud firewall	Network	Network flow analysis								
Overview	External 0	External Connections Internet Access VPC Access Intrusion Detection 3 IPS Analysis All Access Activities								
Traffic Analysis Business Visualization	All Risk Lev	vels V All Events V	/ Unhandled/	✓ Not Ignored ✓	2019-03-29 19:09 - 2019-04-28 19:09 📾 🗌 Instance IP 🗸	Fuzzy search is supported.	Search			
Application Groups	Risk Level	Event Name	Asset Type	Instance ID/Name	Affected Asset IP	Occurred At	Status	Actions		
Business Relations	High	1000000	ECS	10000	NAME OF PARTY AND ADDRESS OF	2019-04-28 20:36	Blocked	Block Ignore View Details		
Security Groups Security Policies	High	1000000	ECS		NUMBER OF STREET	2019-04-28 16:03	Blocked	Block Ignore View Details		
Access Control	High	10000000	ECS		NAME OF A DESCRIPTION O	2019-04-28 16:02	Blocked	Block Ignore View Details		

Click Block to enable the Threat Engine of IPS.

2.5 IPS analysis

The IPS analysis tab page displays the threats detected by IPS, including details on the blocked events, blocked destination IP and application.

Cloud Firewall can detect the IPS blocking events that occurred in the last one hour, one day, seven days, and one month. You can also select and display the blocked events in the customized time range.



The blocked traffic in IPS Analysis is blocked by the IPS treat engines. Mare sure you've selected Traffic Control Mode and enabled the Basic Protections and the Patches in Intrusion Prevention page.

Procedure

- 1. Log on to the Cloud Firewall console.
- 2. In the left-side navigation pane, go to Traffic Analysis > IPS Analysis.
- 3. In the Direction area, click Inbound or Outbound to view the corresponding blocked inbound or outbound traffic.

Cloud firewall	Network flow analysis	
Overview	External Connections Internet Access VPC Access Intrusion Detection (3	All Access Activities
Traffic Analysis		
 Business Visualization 	Direction Inbound Outbound Time 1 Hour 1 Day Last 7 Days 1 Month Custo)m

4. Select Time by one hour, one day, last seven days, one month, or a custom time range to display the required blocking traffic.

Cloud firewall	Network flow analysis	
Overview	External Connections Internet Access VPC Access Intrusion Detection S IPS Analysis	All Access Activities
Traffic Analysis		
Business Visualization	Direction Inbound Outbound Time 1 Hour 1 Day Last 7 Days 1 Month Custom	

You could monitor the following information on the blocked traffic:

• The most blocked source locations with the corresponding proportion in percentage.



• Blocked destination IP addresses with IP type and location.



If you want to view the details of a certain blocked destination IP, click View Logs to open the Access Log.

Blocked application with its proportion in percentage.



• IPS threat engines that block the traffic.



• Blocked event list with the events details.

In the blocked event list, specify the blocking source, direction, defense status, detection time, or source IP address to search for blocking events and to view details.

All Risk Levels $$	All Criteria	✓ All Direc	tions 🗸 Mor	nitor V 2019-04-21 16:07	7 - 2019-04-28 16:07 🛗	Source IP	✓ Enter a keyword.	Search	
Risk Level	Event Name	Events	Mode	Source IP	Destination IP	Direction	Criterion	Occurred At	Action
High	1000	1	Monitor	No		Outbound	Basic Protection	First Time: 2019-04-26 11:42 Last Time: 2019-04-26 11:42	View Details
High	erentier.	2288	Monitor	http://www.clinical.com/article/	0.0100.00	Inbound	Basic Protection	First Time: 2019-04-21 10:29 Last Time: 2019-04-23 00:38	View Details
High		3	Monitor	1000-00103-07-04	0.040	Inbound	Basic Protection	First Time: 2019-04-22 16:36 Last Time: 2019-04-22 16:38	View Details
High	*****	3	Monitor	100.000	10.01.0010	Inbound	Basic Protection	First Time: 2019-04-22 16:36 Last Time: 2019-04-22 16:38	View Details
High	later as	3	Monitor	100.000	10.0100	Inbound	Basic Protection	First Time: 2019-04-22 16:36 Last Time: 2019-04-22 16:38	View Details
High	14000 B	3	Monitor	100.000	10.000	Inbound	Basic Protection	First Time: 2019-04-22 16:36 Last Time: 2019-04-22 16:38	View Details
						< Prev 1	2 3 4 1700	Next > 1/1700 Go To Pa	age

Click View Details to open the detailed page of the specified blocked event. You can view the event description on the Details page.

Cloud firewall	In page 1	ECS Public	c IP					Details	
Overview	6.0,000						HTTP 62.93%	Event Name	a history and history
Traffic Analysis	1.00.000				нттр 62.93%		SNMP 23.35%	Mode	Monitor
	10000						MsSQL-TDS 9.049	First Detected A	t 2019-04-27 11:51
 Business Visualization 							SMB 0.09%	Last Detected A	1 2019-04-27 11:51
Application Groups								Events	8
Business Relations		All Criteria				7 . 2019-04-		e in	5
Security Groups								Source IP	10.00.00
 Security Policies 	Risk Level	Event Name	Events	Mode	Source IP	Destination IF	Dire	Destination IP	100.000
Access Control		10000	1	Monitor	10.00		Int	Direction	Inbound
Intrusion Prevention			8					Criterion	Basic Protection
Firewalls			Ŭ					Event Description	Contraction Contract, 1983
		-	1	Monitor	Trans. In success	-	Int		
Logs									
▼ Tools			3	Monitor	NAME OF TAXABLE PARTY.		Int		
Packet Capture	Medium	-	11	Monitor	THE REAL OF	-	Int		

2.6 All access activities

The All access activities page displays activity data about all hosts protected by Cloud Firewall in real time.

In All access activities page, you can see the historical trend of the traffic both inbound and outbound, the ranking of visits by inbound/outbound traffic, the top traffic's source location and destination location with corresponding proportion in percentage.

Cloud firewall	Network flow analysis
Overview	External Connections Internet Access VPC Access Intrusion Detection 🚱 IPS Analysis All Access Activities
Traffic Analysis	
 Business Visualization 	Time 1 Day ^
Application Groups	15 Minutes
Business Relations	4 Hours
Security Groups	✓ 1 Day
 Security Policies 	Histori 1 week
Access Control	Traffic Ussum pncurent Industry
Intrusion Prevention	And a second and a second and a second
Firewalls	9 Mbps
Logs	
▼ Tools	21:30 22:20 23:10 00:00 00:50 01:40 02:30 03:20 04:10 05:00 05:50 06:40 07:30 08:20 09:10 10:00 10:50 11:40 12:30 13:20 14:10 15:00 15:50 16:40 17:30 18:20 19:10 20:00 20:50
Packet Capture	 Public Inbound Traffic Public Outbound Traffic

Procedure

- 1. Log on to the Cloud Firewall console.
- 2. In the left-side navigation pane, click Traffic Analysis to go to the network traffic analysis page.

3. Click All Access Activities. View all the normal and abnormal activities, the trend charts and the rankings of visits by both inbound and outbound traffic in the last 15 minutes, 1 hour, 4 hours, 1 day, 7 days, or a custom time range.



You can specify any time range without limitations.

 Select a search condition from the Condition drop-down list and enter or select the condition details. Click Query to filter the historical traffic trends based on the condition. To clear the search condition, click Reset.

Cloud firewall	Network	flow analys	is				
Overview	External C	Connections	Internet Access	VPC Access	Intrusion Detection 🜀	IPS Analysis	All Access Activities
Traffic Analysis							
 Business Visualization 	Time	1 Day	\sim				
Application Groups	Condition		Enter a keyword.				+ Add
Business Relations		THP					
Security Groups		Location ISP					
 Security Policies 	Histori	Asset IP					
Access Control	19 Mbp	Asset Region	oncurrent				
Intrusion Prevention		Application			~~~~~	\sim	
Firewalls	9 Mbp	Destinatio n Port					m
Logs		IP Address Type	-				

• In the Historical Trends area, you can view trend charts about the inbound and outbound traffic, the number of new connections, and the number of concurrent connections.

Click Traffic, New, or Concurrent to switch to the trend chart about the inbound and outbound traffic, the number of new connections, or the number of concurrent connections.



A trend chart displays traffic data in the last 15 minutes, 1 hour, 4 hours, 1 day, 7 days, or a custom time range. You can specify any time range without limitations.

- In the Rankings of Visits by Traffic area, you can view the top 10 inbound or outbound traffic with the percentage of each source region or application type.
- Click View Details in the Rankings of Visits by Traffic area to view the details on the inbound or outbound traffic, including the source ISP, sessions, bytes received or sent and packets sent.

Traffic Analysis	21:00 03:00 09:00	View Details						>	< .:00	0 03:00	09:00 15:00	21:00	03:00	09:00 1	.5:00
 Business Visualization 															
Application Groups		Application Protocol	Sessions↓↑	Bytes Received √1	Bytes Sent √↑	Packets Received ↓]^	Packets Sent ↓↑	Actions							
Business Relations	Rankings of Visits by Tra	HTTP	64641	34135800023	972479159458	414749762	637446769	Add to Condition							
Security Policies	Inbound Traffic	Unknown	36191846	3504596412	782893208	43149293	9695580	Add to Condition							
Access Control	Application Protocol	SSH	180640	487837561	621969769	3196823	2986767	Add to Condition	Pc	ort				V	iew Details
Firewalls	/	SIP	330155	158865625	1594829	367592	2111	Add to Condition		_					9.86%
Logs ▼ Tools	(VNC	46283	29440827	35508152	368928	423096	Add to Condition	-	_					8.30%
Packet Capture		HTTPS	44469	8326358	8796078	72105	57767	Add to Condition							7.38%
	VNC HTTPS							< 1/4 >							6.37%
Technical Support															4.35%

• Click Add to Condition to automatically fill the full activity search box with the current condition. Trend charts are displayed in the Historical Trends and Top Access Traffic areas based on the added conditions.

Cloud firewall	Network flow analysis	
Overview	External Connections Internet Access VPC Access Intrusion Detection 😚 IPS Analysis All Access Activities	
Traffic Analysis		
 Business Visualization 	Time 1 Week V	
Application Groups		
Rusiness Relations	Condition Direction V Inbound V - Delete	
Security Groups	AND Application V HTTP V - Delete + Add	Query Reset

3 Log analysis

3.1 Overview

The Log Analysis service of Cloud Firewall provides internet traffic logs and real-time log analysis.

The Log Analysis service of Cloud Firewall can automatically collect and store realtime log of both inbound and outbound traffic. It outputs query analysis, reports, alarms, and downstream computing interconnection and provide you with detailed analysis result.

Cloud firewall	Log Analysis					Storage Usage	0.03% 34.47 G	8/97.66 TB Upgrade Storage	Clear Log Ana	ysis Billing Method	Log Fields
Overview	internet_log	~								Status	5
Traffic Analysis											
Business Visualization	🗟 cloudfirewall-log	store							© 15Minutes(Rela	tive) 🔽 Saved as	Alarm
	1 log_type:interne	t_log							0	Search & A	nalysis
 Security Policies 	SOk										
Firewalls	25k										- 1
Logs	0 16:38:52	16:40:15	16:41:45	16:43:15 16:44:45	16:46:15	16:47:45	16:49:15	16:50:45	16:52:15	16	53:37
▶ Tools				Log Entries:429,	725 Search Status: The result	ts are accurate.					
TAN AND A CANADA	Raw Logs	Graph						Display	Content Column	Column Settings	(†
	Quick Analysis	<	Time 🛋 🔻	Content							
Log Analysis	topic		May 20, 16:53:42	source: log_service topic: cloudfrewall_access_log							
	aliuid	۲		aliuid : 1832006554254177 app_name : Unknown							
	app_name	•		direction : in domain :							
	direction	۲		encije 47 (10:77.106 encijent 0 encijent 0 encijent: 1458542420 likbes: 944							
	domain	•									
	dst_ip	۲		in_packet_bytes: 118 in_packet_count: 1							
	dst_port	•		in_pps : 1 ip_protocol : icmp							

Benefits

The Log Analysis service of Cloud Firewall has the following benefits:

- Classified Protection compliance: Log Analysis provides log storage duration of six months to help your website meet the requirements of classified protection compliance.
- Easy configuration: Easy configuration allows you to collect Internet traffic logs in real time.
- Real-time analysis: Integrated with the Simple Log Service (SLS), the Log Analysis service provides the real-time log analysis service and report center. With the help of log analysis, you can view all the traffic and user's visits going through Cloud Firewall.
- Real-time alarms: Log Analysis supports you to customize real-time monitoring and alerts based on specific indicators. This ensures you receive real-time alerts when there is any threats detected in the critical business.

Prerequisites

Before you begin to use the service of Log Analysis, the following prerequisite must be available:

• You have purchased and activated the Log Analysis service of Cloud Firewall (Log Analysis is available in Pro, Enterprise, and Flagship editions). For details, refer to *Enable the log analysis service*.

Restrictions

The logstore of Cloud Firewall is an exclusive logstore with the following restrictions:

• You cannot write data into logstore with APIs or SDKs, or modify the attributes of the logstore (such as the storage cycle).

Note:

Other general logstore features (such as query, statistics, alarms, and stream consumption) are supported, and there is no difference with the general logstore.

- Alibaba Cloud's Log Service (SLS) does not charge for the exclusive logstore of Cloud Firewall, but SLS itself must be available (not overdue).
- Built-in reports provided by Log Analysis of Cloud Firewall may be updated and upgraded automatically.

Scenarios

- Track Internet traffic logs to trace security threats.
- Allow you to view Internet request activities in real time, and check the security status and trend of your assets.
- Provide you with quick understanding of security operation efficiency and handling the risks in a timely manner.
- Output logs to your self-built data and computing centers.

3.2 Log analysis billing method

Cloud Firewall Log Analysis service charges fees based on the selected log storage duration and log storage capacity. Log Analysis is charged by monthly and annual subscription.

Enable Activate Log Service and select the log storage period and the log storage size. Then, the price is automatically calculated based on the log store specification of your choice.

Log storage specification

Log storage duration	Log storage size	Applicable bandwidth	Recommer d version	Monthly subscription fee	Annual subscripti on fee
180 days	1TB	Applicable to business scenarios with monthly bandwidth not higher than 10 Mbps	Pro Edition	To be released.	To be released.
	5TB	Applicable to business scenarios with monthly bandwidth not higher than 50 Mbps	Enterprise Edition	To be released.	To be released.
	20TB	Applicable to business scenarios with monthly bandwidth not higher than Mbps	Flagship Edition	To be released.	To be released.

Different log storage specifications of Cloud Firewall are charged as follows:



To increase the bandwidth, we recommend that you expand with 1TB log storage for every 10 Mbps increase.

Upgrade storage capacity

If you have no log storage left, a notification appears to remind you to expand the storage size. You can click Upgrade on the console to expand the storage size.

Cloud firewall	Overview		Current Edition : Flagship Edition Upgrade Renew Expiration Day: 2023-09-25
Overview	Security Analysis Network activities		Show Guide
Traffic Analysis			
 Business Visualization 	Overall Protection Levels	Security Policies	Unresolved Risks Last 30 Days
Application Groups	Security Policies	Inbound Internet Traffic 100%	High Risks Medium Risks Low Risks
Business Relations		Outbound Internet Traffic 100%	1 0 0
Security Groups Security Policies	(175 Setting) Control (186 Manugement)		/
Access Control		IPS Settings	Asset Protection
Firewalls		Traffic Control Mode Basic Policies Threat Intelligence Virtual Patches	Protection Status
Logs	Asset Protection		247/249
 Tools 			

UNotice:

If you fail to upgrade the log storage capacity when the storage capacity is full, Cloud Firewall will stop writing new log data to the exclusive logstore of log analysis service, the stored log data in the logstore is retained. Log data is deleted automatically if it is stored for more than 180 days or is not renewed after the Log Analysis service expires for 7 days. Once the log data is deleted, it cannot be recovered.

Duration

The purchase duration of Cloud Firewall log service is bound to the subscription instance of the Cloud Firewall you purchased.

- Buy: When you buy a Cloud Firewall subscription and enable Log Analysis, the price of Log Service is calculated based on the validity of the subscription.
- Upgrade: When you enable Log Service by upgrading an existing Cloud Firewall subscription, the price of Log Service is calculated based on the log storage size.

Service expiration

If the purchased Cloud Firewall instance is about to expire, Log Analysis service will also expire.

• When the service expires, Cloud Firewall stops writing log entries to the exclusive logstore in Log Service.

• The log entries recorded by Cloud Firewall Log Analysis are retained within seven days after the service expires. If you renew the service within seven days after the service expires, you can continue to use Log Analysis service. Otherwise, all stored log entries are deleted.

3.3 Enable the log analysis service

After you activate Cloud Firewall, you can enable the Log Analysis service in the Cloud Firewall console. Log Analysis provides you with the real-time log search and analysis features.

Features

After the Log Analysis service is activated, real-time logs of the internet traffic through Cloud Firewall can be collected automatically. You can also perform realtime log search and analysis with Log Analysis service, and check the results in log dashboards. You need to set the storage duration and storage capacity when you enable the Cloud Firewall log analysis service.

Note:

The log analysis service is available in the Cloud Firewall Pro, Enterprise, and Flagship editions.

Enable the Log Analysis service of Cloud Firewall

- 1. Log on to the Cloud Firewall console.
- 2. In the left-side navigation pane, select Advanced Features > Log Analysis.
- 3. Click Activate Now on the Log Analysis page.

Cloud firewall	
Overview	Log Analysis
Traffic Analysis	Log Analysis supports real-time log search and analysis, and provides a flexible report center. You
Security Policies	can use a variety of SQL statements to analyze log data, create custom reports, and set alarms based on your needs.
Firewalls	Activate Now Learn More
Logs	
▶ Tools	
Advanced Features	
Log Analysis	

4. Select your log storage capacity, and then click Pay to complete the payment.



For more information about log analysis pricing, refer to Log analysis billing method.

- 5. Go back to Log Analysis page in Cloud Firewall console.
- 6. Click the Status switch on the right side to enable the Log Analysis service.

Cloud firewall	Log Analysis						Storage Usage	0.03% 34.47 G	8/97.66 TB Upgrade Storag	e Clear Log Analy	sis Billing Method Log Fields
Overview	internet_log ~										Status 🚺
Traffic Analysis											_
Business Visualization	cloudfirewall-logstore									© 15Minutes(Relati	ve) 🔽 Saved as Alarm
Security Policies	1 log_type:internet_log									۲	Search & Analysis
Firewalls	25k										_
Logs	17:00:26	17:01:45	17:03:15	17:04:45	17:06:15	17:07:45	17:09:15	17:10:45	17:12:15	17:13:45	17:15:11
▶ Tools					Log Entries:403,98	8 Search Status:The results are	e accurate.				
-	Raw Logs Grap	h							Display	Content Column	Column Settings [🕹
 Advanced Features 	Quick Analysis	<	Time 🛋 🔻	Content							
Log Analysis	topic	1	May 20, 17:15:20	source: log_: topic: cloudfi	service rewail_access_log						
	aliuid 💿			alluid : app_name : Unkno	own						
	app_name 💿			direction : out domain :							
	direction ③			dst_ip: dst_port: 0							
	domain 💿			end_time: 155834 in_bps: 944	13719						
	dst_ip 💿			in_packet_bytes : in_packet_count :	118						

Log Analysis service retrieves records of both inbound and outbound Internet traffic flowing through Cloud Firewall. You can use the retrieved records to detect threats in real time.

3.4 Collect the log

You can enable the log collector function for Cloud Firewall in the Cloud Firewall console.

Prerequisites

- You have activated Cloud Firewall.
- · You have activated Alibaba Cloud Log Service.

Context

The log collector function retrieves log data of inbound and outbound Internet traffic for Alibaba Cloud Firewall in real time. The retrieved log data can be searched and analyzed in real time, and the returned results are displayed in dashboards. Based on the log data, you can analyze visits to and attacks on your websites and help the security engineers develop protection strategies.

After you enable the Cloud Firewall log analysis function, the log analysis function automatically creates a dedicated Logstore named cloudfirewall-logstore under your account. Cloud Firewall automatically imports log entries to this dedicated Logstore in real time. For more information about the default configuration of the dedicated Logstore, see *Default configuration*.

Procedure

- 1. In the left-side navigation pane, locate Log Analysis.
- 2. Click the Status switch on the right side to enable the log collector function.

Cloud firewall	Log Analysis				Storage Usage	0.09% 85.93 GB/97.66 TB Upg	ade Storage Clear Log Analys	is Billing Method Lo	g Fields
Overview	internet_log \sim							Status	
Traffic Analysis	-							_	
Business Visualization	logstore						© 15Minutes(Relation	e) Saved as Ala	.rm
Security Policies	1 log_type:internet_log 50k						0	Search & Analy	sis
Firewalls	25k								- 1
Logs	0 19:57:16 19:58:45	20:00:15	20:01:45 20:03:15	20:04:45	20:06:15	20:07:45 20:09:1	\$ 20:10:45	20:12:	:01
▶ Tools			Log Entries:428,80	IO Search Status: The results are acc	curate.				
▼ Advanced Features	Raw Logs Graph Quick Analysis <	Time ▲▼	Content				Display Content Column	Column Settings [1
Log Analysis	topic ① 1	May 30, 20:12:01	source: log_service topic: cloudfirewall_access_log						
	aliuid		aluid: 1 app_name: Unknown						

Default configuration item	Description
Project	The log analysis project created by Cloud Firewall. The project name is determined according to the region of your Cloud Firewall instance.
	 If the Cloud Firewall instance is deployed in a Mainland China region, the project name is: cloudfirewall-project-Alibaba Cloud account
	 If the Cloud Firewall instance is deployed in the Finance Cloud (Hangzhou) region, the project name is: cloudfirewall-project-Alibaba Cloud
	 <i>account</i> ID-cn-hangzhou-finance. If the Cloud Firewall instance is deployed in other regions, the project name is: cloudfirewall-project-Alibaba Cloud account ID-ap-southeast-1.
Logstore	The default Logstore is cloudfirew all - logstore. All log data retrieved by Cloud Firewall is stored in this Logstore.

Default configuration item	Description
Region	 If the Cloud Firewall instance is deployed in a Mainland China region, the project is saved in the China (Hangzhou) region by default. If the Cloud Firewall instance is deployed in other regions, the project is saved in the Singapore region by default.
Shard	By default, two shards are created and the <i>Automatic shard splitting</i> function is enabled.
Dashboards	A dashboard is created by default.



Note:

The default log analysis configuration items cannot be modified.

Restrictions and guidelines

- After you enable the Log Analysis function, the system automatically creates a Logstore named cloudfirewall-logstore in the Log Service console. The Logstore is dedicated to Cloud Firewall and stores all log entries of Cloud Firewall. Do not delete this Logstore.
- · Other data cannot be written into the dedicated Logstore.

Log entries generated by Cloud Firewall are stored in the dedicated Logstore. You cannot write other data into this Logstore by using the API, SDK, or other methods.

Note:

The dedicated Logstore has no restrictions in search, statistics, alerts, streaming consumption, and other functions.

- Basic configurations, such as the log storage period, cannot be modified.
- The dedicated Logstore is not billed.

To use the dedicated Logstore, you must activate Log Service for your account.



When your Log Service is overdue, the Cloud Firewall log collector function is suspended until you pay the bills.

- Do not delete or modify the configurations of the default project, Logstore, index, and dashboards created by Log Service. Log Service will update the Cloud Firewall log analysis function. The index of the dedicated Logstore and the default report are also updated.
- If you want to use the Cloud Firewall log analysis function with a RAM user account, you must grant the required Log Service permissions to the RAM user account. For more information, see*Authorize RAM user accounts with Log Analysis function*.

3.5 Fields in the log entry

Cloud firewall records the inbound and outbound traffic logs, including multiple log fields. You can perform query and analysis based on specific fields.

Field Name	Description	Example	Comments	
time	Time of the operation in Cloud Firewall	2018-02-27 11:58:15	-	
topic	Log topic	cloudfirewall_access _log	Log topic is unique, which is cloudfirew for Cloud Firewall.	
Log_type	Log types	Internet_log	Internet_l og refers to the Internet Traffic Log.	
aliuid	User's Alibaba Cloud UID	12333333333333	-	
app_name	Protocol of the access traffic	HTTPS	Possible values include HTTPS , NTP, SIP, SMB , NFS, and DNS. Unknown values are Unknown.	

Field Name	Description	Example	Comments
direction	Traffic direction	in	 in: traffic goes to the ENI out: traffic goes from the ENI
domain	Domain name	www.aliyun.com	-
dst_ip	Destination IP	1.1.1.1	-
dst_port	Destination port	443	-
end_time	Session end time	1555399260	Unit: Seconds (Unix timestamp)
In_bps	Bps of inbound traffic	11428	Unit: bps
In_packet_bytes	Total number of bytes of inbound traffic	2857	-
In_packet_ count	Total number of packet of inbound traffic	18	-
In_pps	Pps of inbound traffic	9	Unit: pps
Ip_protocol	IP protocol type	ТСР	Protocol name . TCP and UDP protocol are supported.
Out_bps	Bps of outbound traffic	27488	Unit: bps
Out_packet _bytes	Total number of bytes of outbound traffic	6872	-
Out_packet _count	Total number of packet of outbound traffic	15	-
Out_pps	Pps of outbound traffic	7	Unit: pps
region_id	Region to which the access traffic belongs	cn-beijing	-

Field Name	Description	Example	Comments		
Rule_result	Result of matching with the rules	pass23	The result of matching with the rules. The values are: • Pass: The traffic is allowed to pass through Cloud Firewall. • Alert: Cloud		
			Firewall detects threats in the traffic. • Discard: The traffic is not		
			allowed to pass through Cloud Firewall.		
src_ip	Source IP	1.1.1.1	-		
src_port	The port of the host from which traffic data is sent	47915	-		
start_time	Session start time	1555399258	Unit: Seconds (Unix timestamp)		
Start_time_min	Session start time, which is an integer in minutes	1555406460	Unit: Seconds (Unix timestamp)		
Tcp_seq	TCP serial number	3883676672	-		
Total_bps	Total bps of both inbound and outbound traffic	38916	Unit: bps		
Total_pack et_bytes	Total number of bytes of both inbound and outbound traffic	9729	Unite: byte		

Field Name	Description	Example	Comments		
Total_pack et_count	Total number of packets of both inbound and outbound traffic	33	-		
Total_pps	Total number of pps of both inbound and outbound traffic	16	Unit: pps		
Src_private_ip	Private IP of the source host	1.1.1.1			
Vul_level	Vulnerability Risk level	High	Vulnerability Risk level: • 1: Low • 2: Moderate • 3: High		

3.6 Export log entries

The Log Analysis function of Cloud Firewall allows you to export log entries to your local device.

You can export log entries on the current page to a CSV file, or export all log entries to a TXT file.

Procedure

- 1. Log on to the Cloud Firewall console.
- 2. In the left-side navigation pane, select Advanced Features > Log Analysis.
- 3. On the Raw Logs tab page, click the Download icon

on the right side.



The download icon does not appear if there's no search result.

- 4. In the Log Download dialog box, select Download Log in Current Page or Download all logs by the CLI console.
 - Download logs in current page:

Click OK to export the raw log entries on the current page to a CSV file.

- Download all logs by CLI:
 - a. For more information about installing the CLI, see CLI guide.
 - b. Click Security Information Management Link to view and record the AccessKey ID and AccessKey Secret of the current user.
 - c. Click Copy Command and paste the command into CLI, replace the AccessID obtained in step 2 and AccessKey Secret

obtained in step 2 with the AccessKey ID and AccessKey Secret of the current user, and run the command.



After you run the command, all raw log entries created by Cloud Firewall are automatically exported and saved to the file $download_d$ at a. $t \times t$.

3.7 Authorize RAM user accounts with Log Analysis function

If you want to use Cloud Firewall's Log Analysis function with a RAM user account, you must first use your Alibaba Cloud account to authorize this RAM user account with the Log Analysis functions of Cloud Firewall.

Context

The following permissions are required for enabling and using Cloud Firewall's Log Analysis function.

Operations	Required account
Enable the Log Analysis function. You only need to perform this operation once.	Alibaba Cloud account
Authorize Cloud Firewall to write the log data into the dedicated Logstore of Log Analysis in real time. You only need to perform this operation once.	 Alibaba Cloud account A RAM user account with AliyunLogF ullAccess permission A RAM user account with the customized permission of log writing
Use the Log Analysis function.	 Alibaba Cloud account A RAM user account with AliyunLogF ullAccess permission A RAM user account with the customized permission s

You can grant permissions to a RAM user account as needed.

Scenarios	Grant a RAM user account permissions	Procedure
Grant a RAM user account full permission to Log Service.	The AliyunLogF ullAccess policy specifies full permission to Log Service.	For more information, see <i>RAM user management</i> .
After you use your Alibaba Cloud account to enable the Cloud Firewall log analysis function and complete the authorizat ion, grant the RAM user account the permission to view logs.	The AliyunLogR eadOnlyAcc ess policy specifies the read-only permission.	For more information, see RAM user management.
Grant the RAM user account the permission s to enable and use the Cloud Firewall log analysis function. Do not grant other permissions to Log Service.	Create a custom authorizat ion policy, and apply the policy to the RAM user account.	For more information, see the following procedure.

Procedure

- 1. Log on to the RAM console.
- 2. Open the Create Custom Policy tab page on the Policies page.
- 3. In the upper-right corner of the page, click Create Authorization Policy.
- 4. Click Blank Template, enter the Policy Name and the following Policy Content into this template.

Note:

Replace \${ Project } and \${ Logstore } in the following policy with the Log Service Project name and Logstore name dedicated for Cloud Firewall, respectively.

```
{
  " Version ": " 1 ",
  " Statement ": [
      " Action ": " log : GetProject ",
      " Resource ": " acs : log :*:*: project /${ Project }",
      " Effect ": " Allow "
    },
      " Action ": " log : CreateProj ect ",
" Resource ": " acs : log :*:*: project /*",
      " Effect ": " Allow "
    },
      " Action ": " log : ListLogSto res ",
      " Resource ": " acs : log :*:*: project /${ Project }/
logstore /*",
      " Effect ": " Allow "
    },
    {
      " Action ": " log : CreateLogS tore ",
      " Resource ": " acs : log :*:*: project /${ Project }/
logstore /*",
      " Effect ": " Allow "
    },
      " Action ": " log : GetIndex ",
      " Resource ": " acs : log :*:*: project /${ Project }/
logstore /${ Logstore }",
          " Effect ": " Allow "
    },
{
      " Action ": " log : CreateInde x ",
      " Resource ": " acs : log :*:*: project /${ Project }/
logstore /${ Logstore }",
          " Effect ": " Allow "
    },
    {
      " Action ": " log : UpdateInde x ",
```

```
" Resource ": " acs : log :*:*: project /${ Project }/
 logstore /${ Logstore }",
       " Effect ": " Allow "
    },
    {
       " Action ": " log : CreateDash board ",
       " Resource ": " acs : log :*:*: project /${ Project }/
 dashboard /*"
       " Effect ": " Allow "
    },
    {
       " Action ": " log : UpdateDash board ",
       " Resource ": " acs : log :*:*: project /${ Project }/
 dashboard /*"
       " Effect ": " Allow "
    },
{
       " Action ": " log : CreateSave dSearch ",
" Resource ": " acs : log :*:*: project /${ Project }/
 savedsearc h /*",
" Effect ": " Allow "
    },
{
       " Action ": " log : UpdateSave dSearch ",
       " Resource ": " acs : log :*:*: project /${ Project }/
 savedsearc h /*",
    " Effect ": " Allow "
    }
  ]
}
```

- 5. Click Create Authorization Policy.
- 6. Go to the Users page, locate the RAM user account, and click Authorize.
- 7. Select the custom authorization policy that you created, and then click OK. The authorized RAM user account then can enable and use the Log Analysis function. However, this RAM user account is not authorized to use other functions of Log Service.

3.8 Manage log storage

After you enable the Log Analysis function of Cloud Firewall, the log storage space is allocated based on your specified log storage size. You can view the usage of the log storage space on the Log Analysis page in the Cloud Firewall console.

Chethe log storage

You can view the log storage in the Cloud Firewall console at any time.



The log storage information in the console is not updated in real time. It takes up to two hours to update the actual storage information to the console. We recommend that you expand the log storage space before it is exhausted.

- 1. Log on to the Cloud Firewall console.
- 2. In the left-side navigation pane, select Advanced Features > Log Analysis.
- 3. View the log storage information in the upper-right corner of the Log Analysis

page.

Cloud firewall	Log Analysis		Storage Usage 0.09% 86.37 GB/97.66	T8 Upgrade Storage Clear Log Analysis Billing Method Log Fields
Overview	internet_log V			Status 🔵
Traffic Analysis				
▼ Rusiness Visualization	Cloudfirewall-logstore			© 15Minutes(Relative) ▼ Saved as Alarm
	1			Search & Analysis
Application Groups	82k			
Business Relations				
Security Groups	20:29:29 20:30:45 20:32:15 20:33:45	20:35:15 20:36:45	20:38:15 20:39:45	20:41:15 20:42:45 20:44:14

Expand log storage

To expand the log storage, click Upgrade Storage at the top of the Log Analysis page.

Cloud firewall	Log Analysis	Storage Usage 009% 86.37 GB/97.66 T6 Upgrade Storage Clear Log Analysis Billing Method Log Fields
Overview	Internet_Jog \checkmark	Status 🔵
Traffic Analysis		
Rusiness Visualization	cloudfirewall-logstore	①15Minutes[Relative) ➤ Saved as Alarm
	1	© 🕜 Search & Analysis
Application Groups	32k	
Business Relations		
Security Groups	0 20:29:29 20:30:45 20:32:15 20:33:45	20:35:15 20:36:45 20:38:15 20:39:45 20:41:15 20:42:45 20:44:14

Note:

We recommend that you expand the log storage space before it is exhausted. If no storage space is available, then the new log data cannot be written into the dedicated Logstore.

Clear log storage

You can delete all log entries stored in the Logstore. For example, you can delete the log entries generated during the testing phase and use the log storage space to store log entries that are generated during the production phase only.

Click Clear at the top of the Log Analysis page, and confirm to delete all stored log entries.

Cloud firewall	Log Analysis					Storage Usage	0.09% 86.37 GB/97	7.66 TB Upgrade Storage	Clear Log Analysis Billin	ng Method Log Fields
Overview	internet_log \checkmark									Status 🚺
Traffic Analysis								_		
 Business Visualization 	cloudfirewall-logstore								③ 15Minutes(Relative) ▼	Saved as Alarm
									© 🕜	Search & Analysis
Application Groups	32k									
Business Relations										
Security Groups	0 20:29:29 20:30:45	20:32:15	20:33:45	20:35:15	20:36:45	20:38:15	20:39:45	20:41:15	20:42:45	20:44:14

I Notice:

You cannot recover the deleted log entries. This operation is irreversible.

Note:

You only have limited times for clearing the log storage.