Alibaba Cloud
Cloud Firewall

Quick Start

Issue: 20190429

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 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.**	`swich` *{stand | slave}*

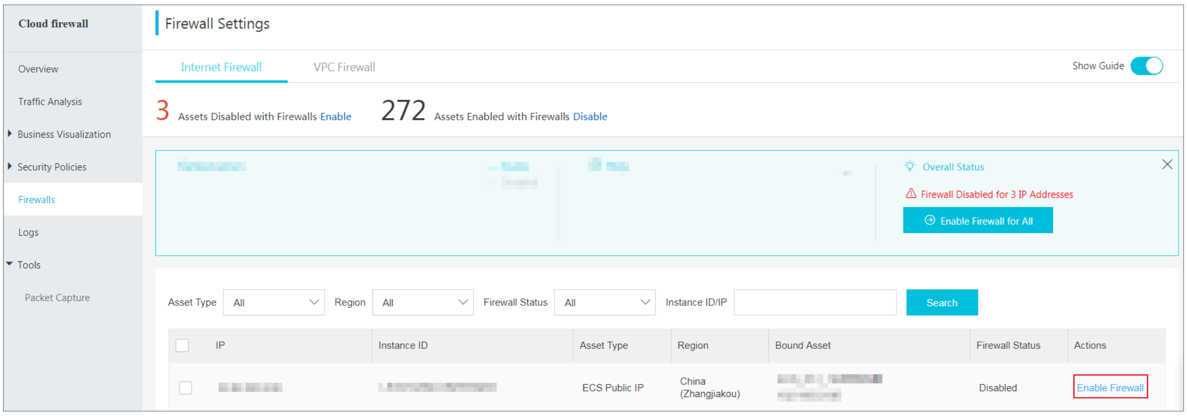
Contents

1 Tutorial overview

This document introduces how to quickly complete basic operations in the Cloud Firewall console.

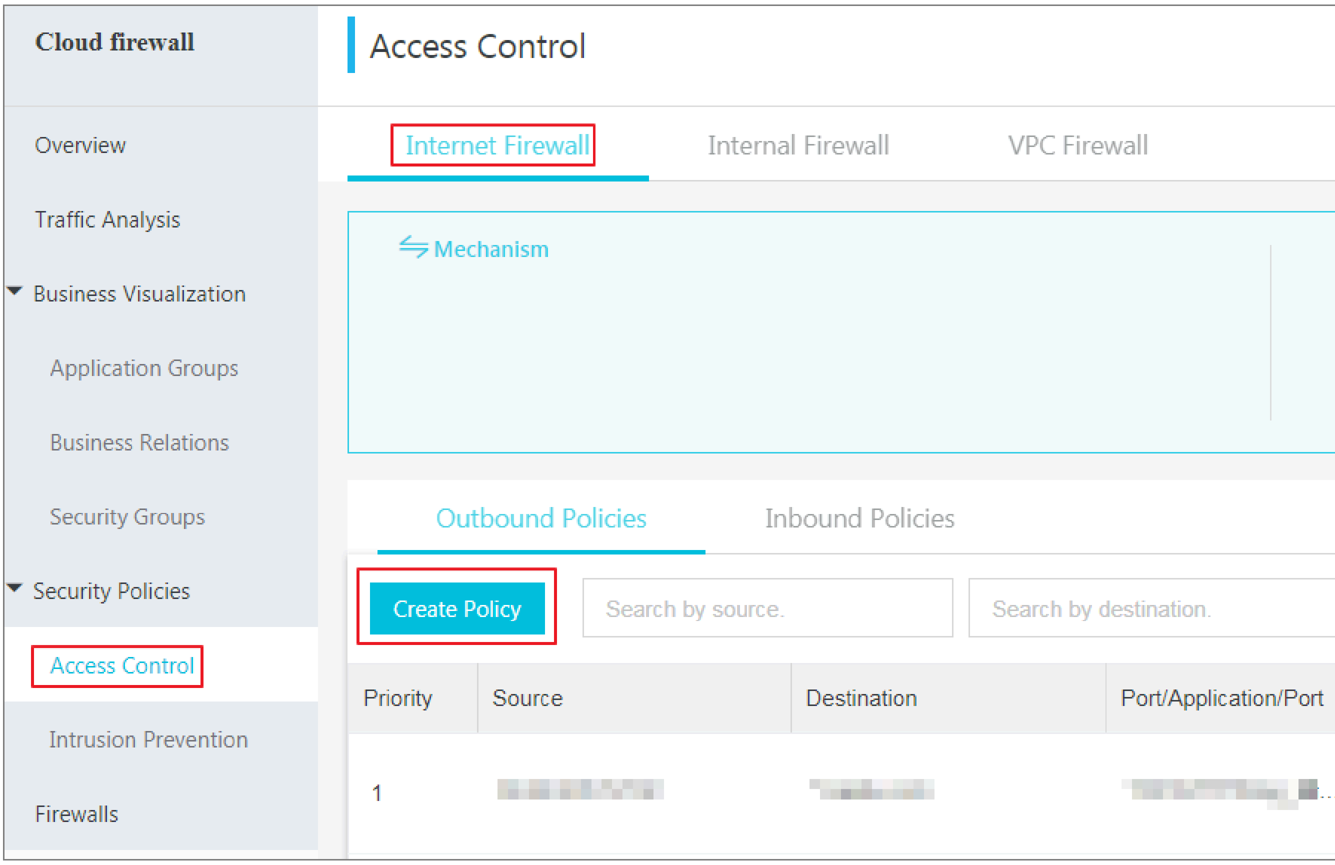
You can perform the following operations in the Cloud Firewall console:

- *Enable the Cloud Firewall service* on the Firewalls page.



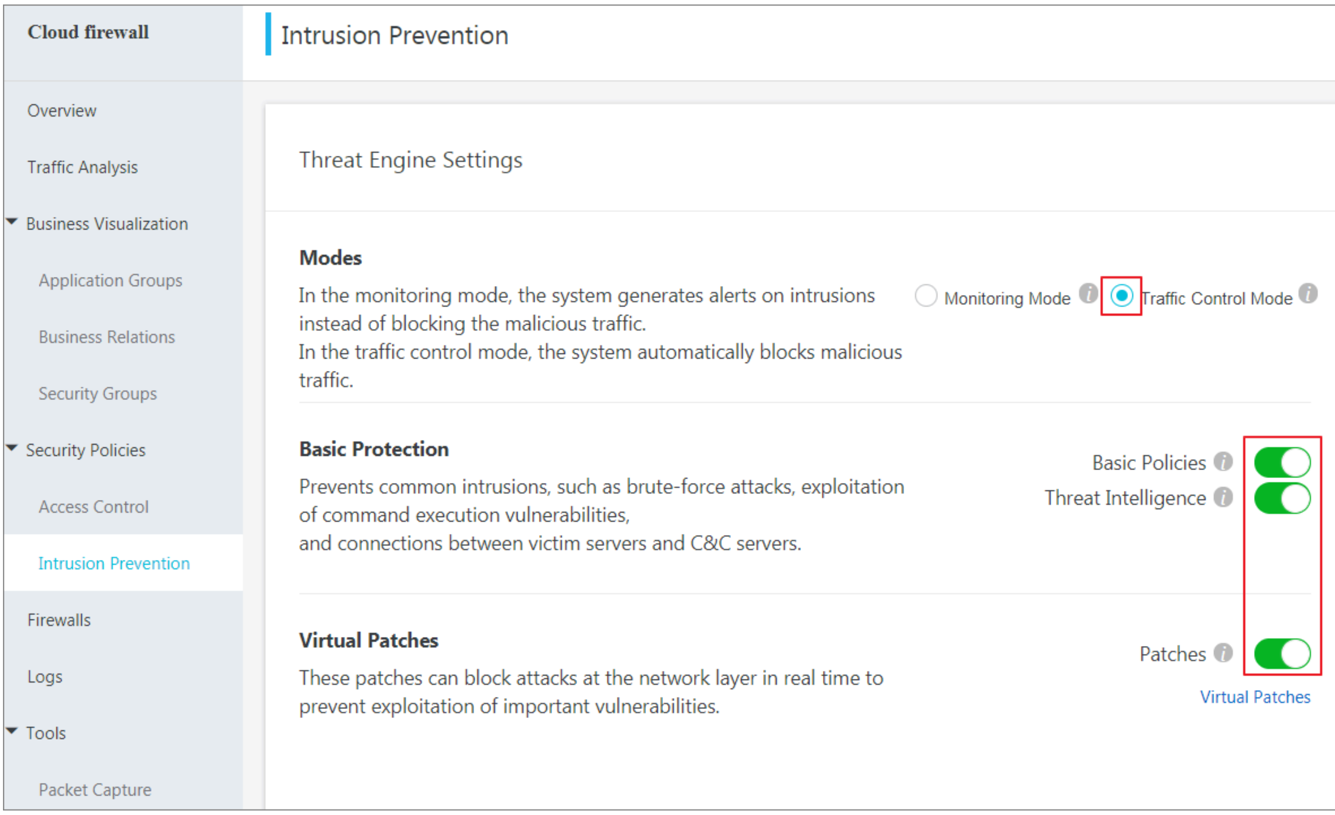
IP	Instance ID	Asset Type	Region	Bound Asset	Firewall Status	Actions
		ECS Public IP	China (Zhangjiakou)		Disabled	Enable Firewall

- Click Add Policy in the upper-right corner of the Access Control page to *Configure access control policies*.



Priority	Source	Destination	Port/Application/Port
1			

- *Configure intrusion prevention policies* on the Intrusion Prevention page.



Cloud firewall

Intrusion Prevention

Threat Engine Settings

Modes

In the monitoring mode, the system generates alerts on intrusions instead of blocking the malicious traffic.
In the traffic control mode, the system automatically blocks malicious traffic.

○ Monitoring Mode ● Traffic Control Mode

Basic Protection

Prevents common intrusions, such as brute-force attacks, exploitation of command execution vulnerabilities,
and connections between victim servers and C&C servers.

Basic Policies: on
Threat Intelligence: on

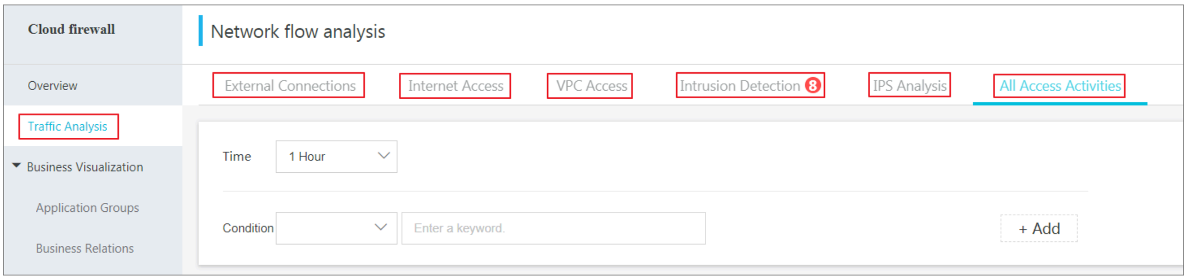
Virtual Patches

These patches can block attacks at the network layer in real time to prevent exploitation of important vulnerabilities.

Patches: on

Virtual Patches

- *View traffic analysis* on the Traffic Analysis page. You can check traffic analysis on external connections, internet access, VPC access, intrusion detection, IPS analysis and all access activities.



Cloud firewall

Network flow analysis

Time: 1 Hour

Condition: Enter a keyword.

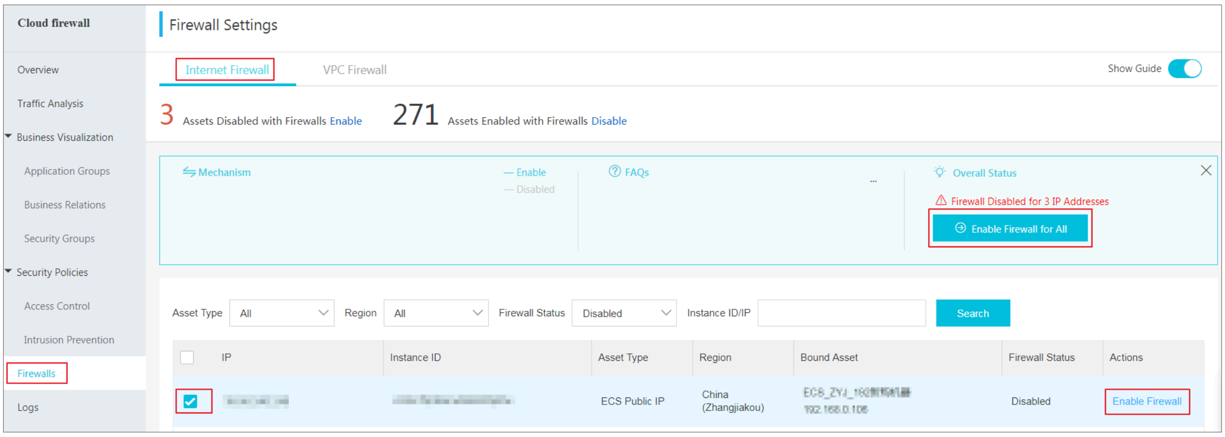
+ Add

2 Enable the firewall settings

After you subscribe Cloud Firewall service, the firewall setting is disabled by default. On the Firewallpage, you can enable the firewall service for the assets in specified Internet/VPC networks. Once enabled, the Cloud Firewall service starts to monitor the Internet/VPC traffic without requiring network configurations.

Internet Firewall

On the Firewalls > Internet Firewallpage of Cloud Firewall console, click Enable Firewall for All to enable the service for all assets protected by Internet Firewall, or select assets and click Enable Firewall to enable the service for specified assets.



3 Assets Disabled with Firewalls Enable   271 Assets Enabled with Firewalls Disable

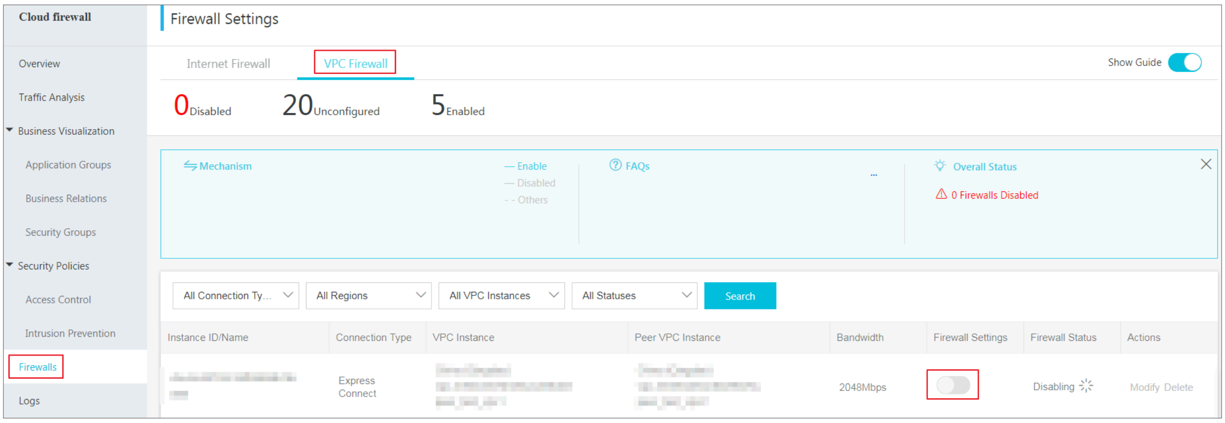
Firewall Disabled for 3 IP Addresses

Asset Type: All   Region: All   Firewall Status: Disabled   Instance ID/IP:

□	IP	Instance ID	Asset Type	Region	Bound Asset	Firewall Status	Actions
☑	[redacted]	[redacted]	ECS Public IP	China (Zhangjiakou)	[redacted]	Disabled	Enable Firewall

VPC Firewall

On the Firewalls > VPC Firewall page of Cloud Firewall console, select the assets you need to monitor and click the Firewall Settings switch to enable the service for specified assets.



0 Disabled   20 Unconfigured   5 Enabled

0 Firewalls Disabled

All Connection Ty...   All Regions   All VPC Instances   All Statuses

Instance ID/Name	Connection Type	VPC Instance	Peer VPC Instance	Bandwidth	Firewall Settings	Firewall Status	Actions
[redacted]	Express Connect	[redacted]	[redacted]	2048Mbps	○	Disabling	Modify Delete

3 Enable Intrusion Prevention

Cloud Firewall is embedded with IPS to defend against intrusions in real time.

Procedure

1. Select the Intrusion Prevention Mode.
    - Monitoring Mode: Enable monitoring mode to monitor malicious traffic and generate alarms.
    - Traffic Control Mode: Enable traffic control mode to block the malicious traffic.

    Note:

    After you subscribe to the Cloud Firewall service, Monitoring Mode is enabled for IPS by default.
2. In the Basic Protection module, turn on or off the Basic Policies switch to enable or disable the built-in basic intrusion prevention rules. The basic rules can intercept intrusions such as password cracking and command execution vulnerability.
3. Turn on or off the Threat Intelligence switch to enable or disable the function of collecting network-wide threat intelligence.
4. In the Virtual Patches Module, turn on or off the Patches switch to enable or disable the installation-free virtual patch function for preventing exploitation of high-risk vulnerabilities.

Note:

After the configuration, you can view the details on different intrusion prevention activities in the IPS Analysis area on Traffic Analysis page.

4 View network flow analysis

Network flow analysis provides you with full visibility of flows across the entire network. You can view real-time activities in your assets, including threat events, network activities, traffic trends, access traffic blocked by IPS, and external connection activities.

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.

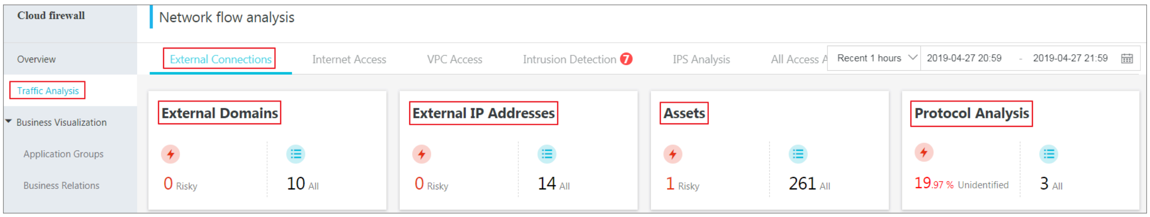
Procedure

1. Log on to the *Cloud Firewall console*.

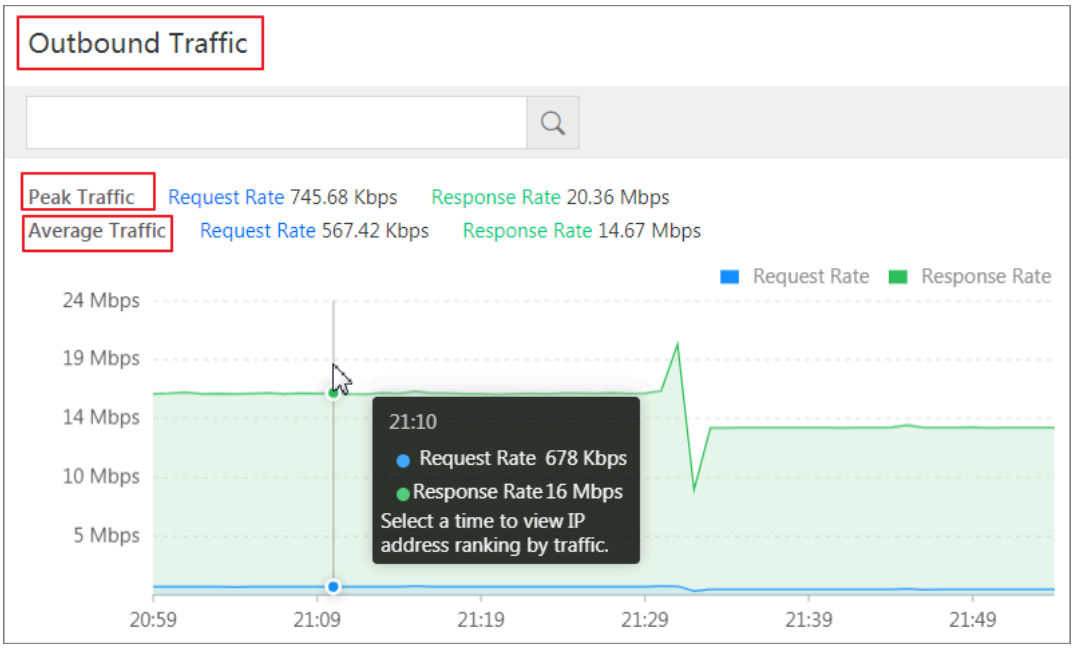
2. In the left-side navigation pane, go to Network Flow Analysis > External Connections to check your assets' external connection activities.

   You can perform the follows operations on External Connections page:

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



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

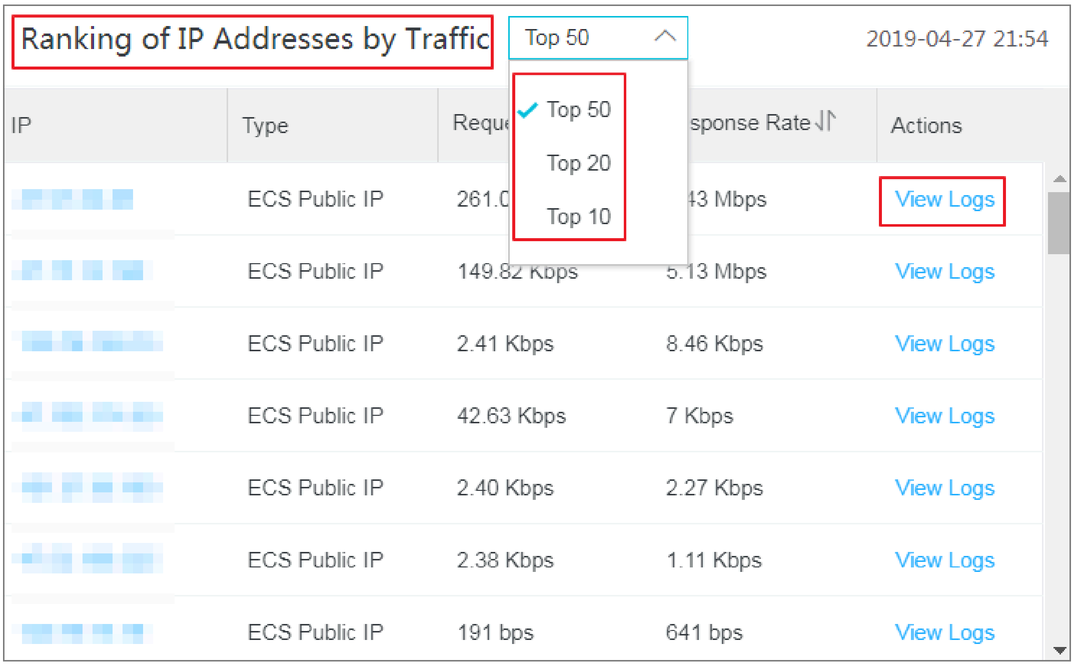

Outbound Traffic

Peak Traffic Request Rate 745.68 Kbps Response Rate 20.36 Mbps

Average Traffic Request Rate 567.42 Kbps Response Rate 14.67 Mbps

21:10
● Request Rate 678 Kbps
● Response Rate 16 Mbps
Select a time to view IP address ranking by traffic.

   - 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 Traffic

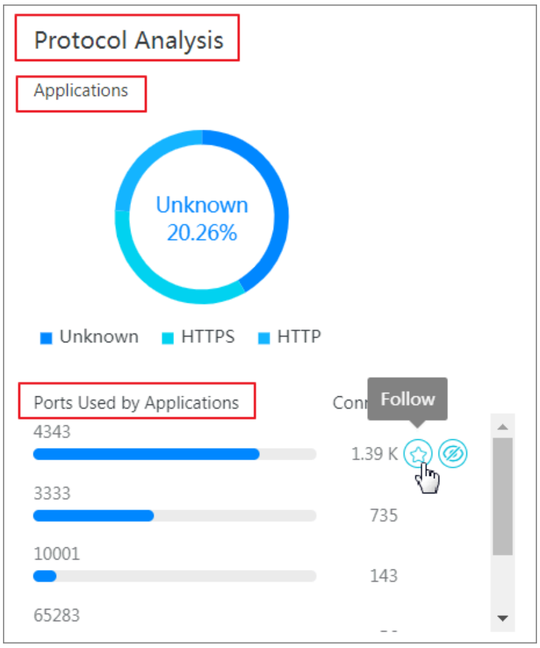
Top 50

2019-04-27 21:54

✓ Top 50
Top 20
Top 10

IP	Type	Reque	sponse Rate	Actions
[redacted]	ECS Public IP	261.0	43 Mbps	View Logs
[redacted]	ECS Public IP	149.82 Kbps	5.13 Mbps	View Logs
[redacted]	ECS Public IP	2.41 Kbps	8.46 Kbps	View Logs
[redacted]	ECS Public IP	42.63 Kbps	7 Kbps	View Logs
[redacted]	ECS Public IP	2.40 Kbps	2.27 Kbps	View Logs
[redacted]	ECS Public IP	2.38 Kbps	1.11 Kbps	View Logs
[redacted]	ECS Public IP	191 bps	641 bps	View Logs

- Monitor the protocol analysis for external connections, including the information on applications, ports and corresponding connection numbers.



Protocol Analysis

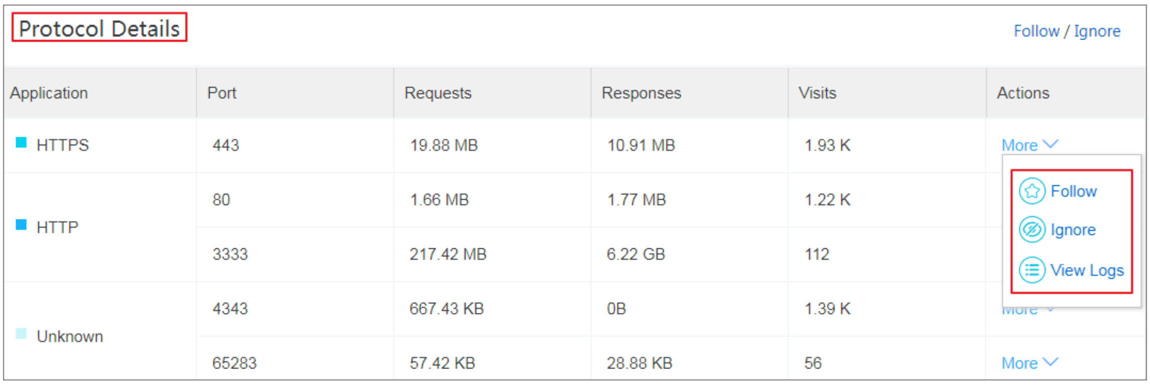
Applications

Ports Used by Applications

Conn Follow

Ports Used by Applications	Conn
4343	1.39 K
3333	735
10001	143
65283	--

- View the protocol details, and follow or ignore the specified protocols.



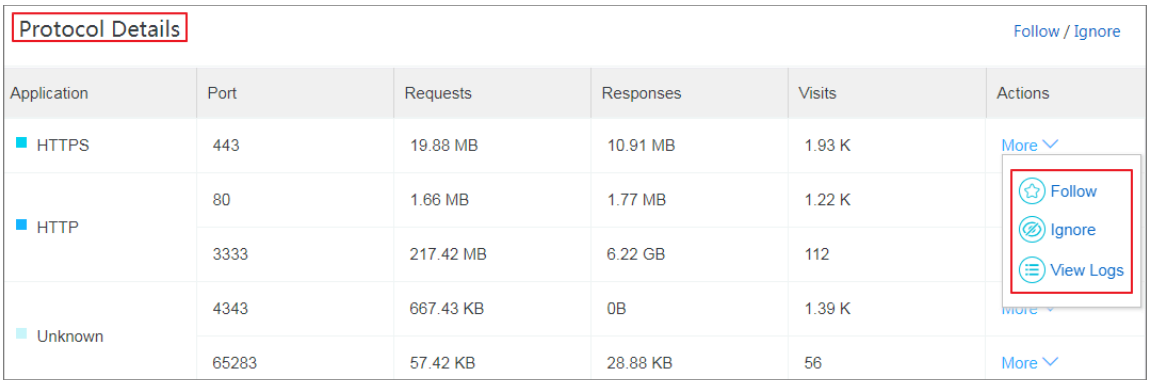
Protocol Details

Follow / Ignore

Application	Port	Requests	Responses	Visits	Actions
HTTPS	443	19.88 MB	10.91 MB	1.93 K	More
HTTP	80	1.66 MB	1.77 MB	1.22 K	
	3333	217.42 MB	6.22 GB	112	
Unknown	4343	667.43 KB	0B	1.39 K	More
	65283	57.42 KB	28.88 KB	56	More

Follow
Ignore
View Logs

- View the protocol details, and follow or ignore the specified protocols.



Protocol Details

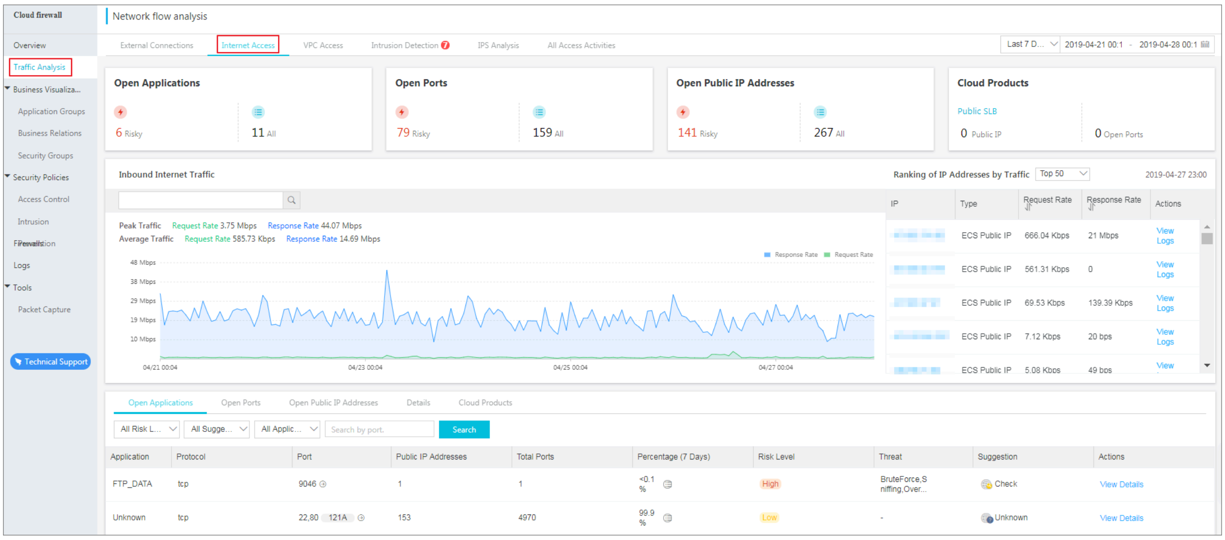
Follow / Ignore

Application	Port	Requests	Responses	Visits	Actions
HTTPS	443	19.88 MB	10.91 MB	1.93 K	More
HTTP	80	1.66 MB	1.77 MB	1.22 K	
	3333	217.42 MB	6.22 GB	112	
Unknown	4343	667.43 KB	0B	1.39 K	More
	65283	57.42 KB	28.88 KB	56	More

Follow
Ignore
View Logs

Internet Access

The Internet Access page displays the details on the internet access traffic, including the open applications/ports/internet IP and the correlated cloud products.



Open Applications: 6 Risky, 11 All

Open Ports: 79 Risky, 159 All

Open Public IP Addresses: 141 Risky, 267 All

Cloud Products: Public SLB, 0 Public IP, 0 Open Ports

Inbound Internet Traffic

Peak Traffic Request Rate 3.75 Mbps Response Rate 44.07 Mbps
Average Traffic Request Rate 585.73 Kbps Response Rate 14.69 Mbps

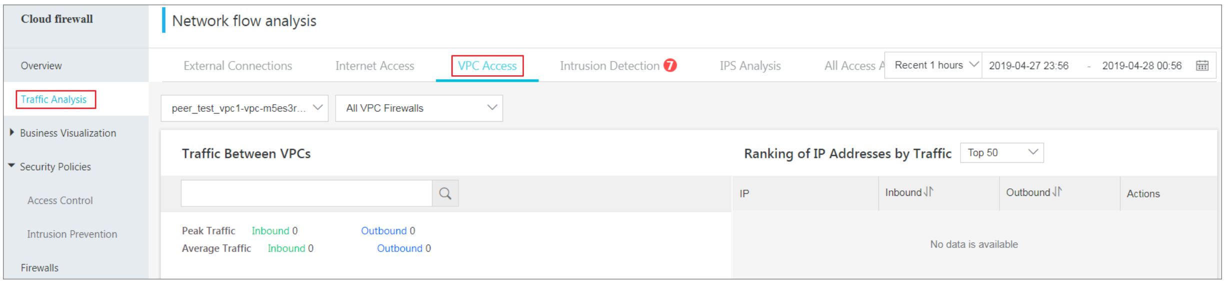
Ranking of IP Addresses by Traffic Top 50 2019-04-27 23:00

IP	Type	Request Rate	Response Rate	Actions
[redacted]	ECS Public IP	666.04 Kbps	21 Mbps	View Logs
[redacted]	ECS Public IP	561.31 Kbps	0	View Logs
[redacted]	ECS Public IP	69.53 Kbps	139.39 Kbps	View Logs
[redacted]	ECS Public IP	7.12 Kbps	20 bps	View Logs
[redacted]	ECS Public IP	5.08 Kbps	49 bps	View

Application	Protocol	Port	Public IP Addresses	Total Ports	Percentage (7 Days)	Risk Level	Threat	Suggestion	Actions
FTP_DATA	tcp	9046	1	1	<0.1 %	High	BruteForce,Sniffing,Over...	Check	View Details
Unknown	tcp	22,80 121A	153	4970	99.9 %	Low	-	Unknown	View Details

VPC Access

The VPC Access page displays the details on the traffic in VPC networks, including the traffic between VPCs, ranking of the sessions between VPCs, and the open ports and assets in VPC firewall.

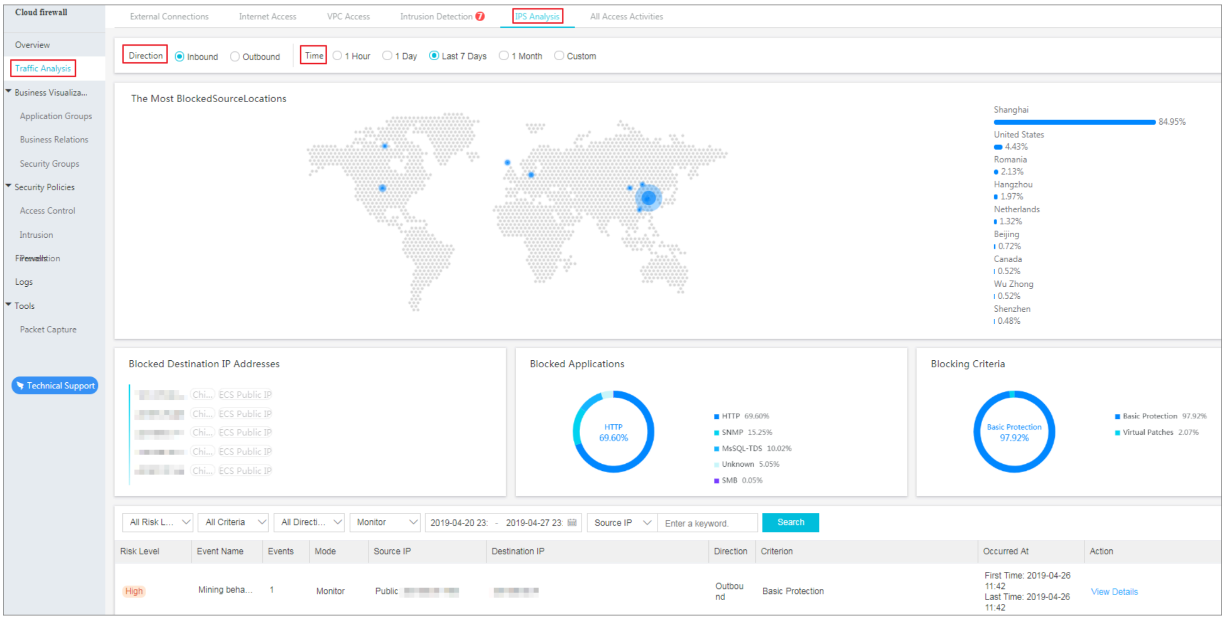


Peak Traffic Inbound 0 Outbound 0
Average Traffic Inbound 0 Outbound 0

No data is available

IPS Analysis

The IPS Analysis page displays the details on blocked traffic in real time.



Direction ● Inbound ○ Outbound Time ○ 1 Hour ○ 1 Day ● Last 7 Days ○ 1 Month ○ Custom

Shanghai 84.95%
United States 4.43%
Romania 2.13%
Hangzhou 1.97%
Netherlands 1.32%
Beijing 0.72%
Canada 0.52%
Wu Zhong 0.52%
Shenzhen 0.48%

[redacted] Chi... ECS Public IP
[redacted] Chi... ECS Public IP
[redacted] Chi... ECS Public IP
[redacted] Chi... ECS Public IP
[redacted] Chi... ECS Public IP

HTTP 69.60%
HTTP 69.60%
SNMP 15.25%
MsSQL-TDS 10.02%
Unknown 5.05%
SMB 0.05%

Basic Protection 97.92%
Basic Protection 97.92%
Virtual Patches 2.07%

All Risk L... All Criteria All Directi... Monitor 2019-04-20 23: - 2019-04-27 23: Source IP Enter a keyword.

Risk Level	Event Name	Events	Mode	Source IP	Destination IP	Direction	Criterion	Occurred At	Action
High	Mining beha...	1	Monitor	Public [redacted]	[redacted]	Outbound	Basic Protection	First Time: 2019-04-26 11:42 Last Time: 2019-04-26 11:42	View Details

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.

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

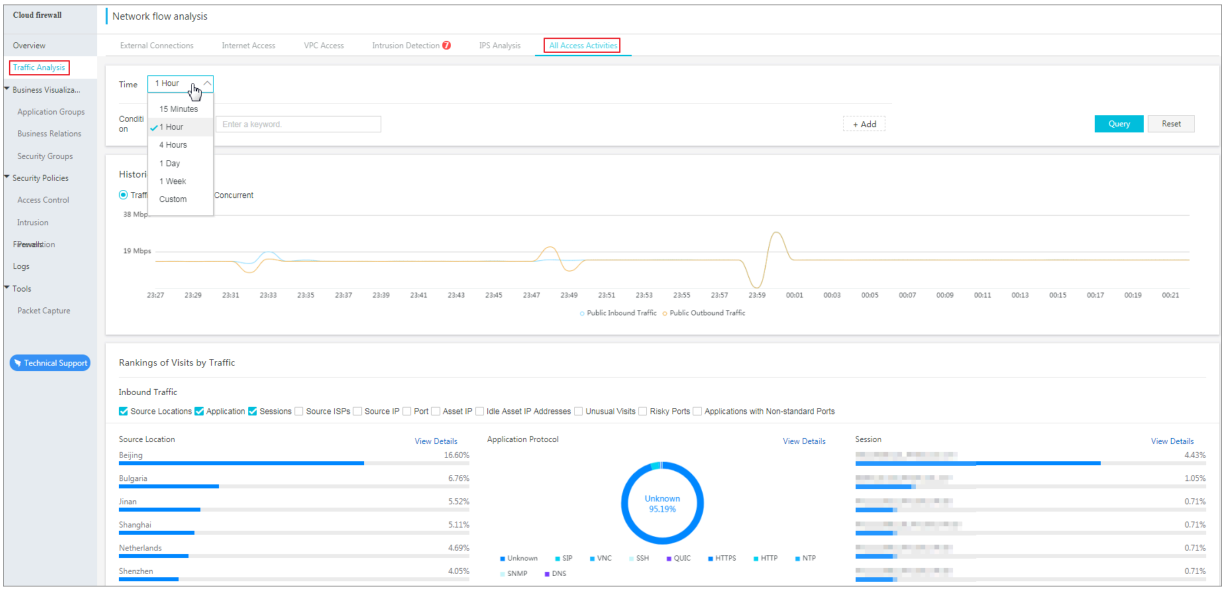
   You could monitor the following information on the blocked traffic:

   - the most blocked source locations
   - blocked destination IP addresses
   - blocked applications
   - IPS settings
   - blocked event list

     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 Access Activities

The All Access Activities page displays the details on activity data about all hosts protected by Cloud Firewall in real time. The data includes all traffic trends, top N source regions of inbound and outbound application access, the percentage of each region, top N session addresses, and the percentage of each address.



Procedure

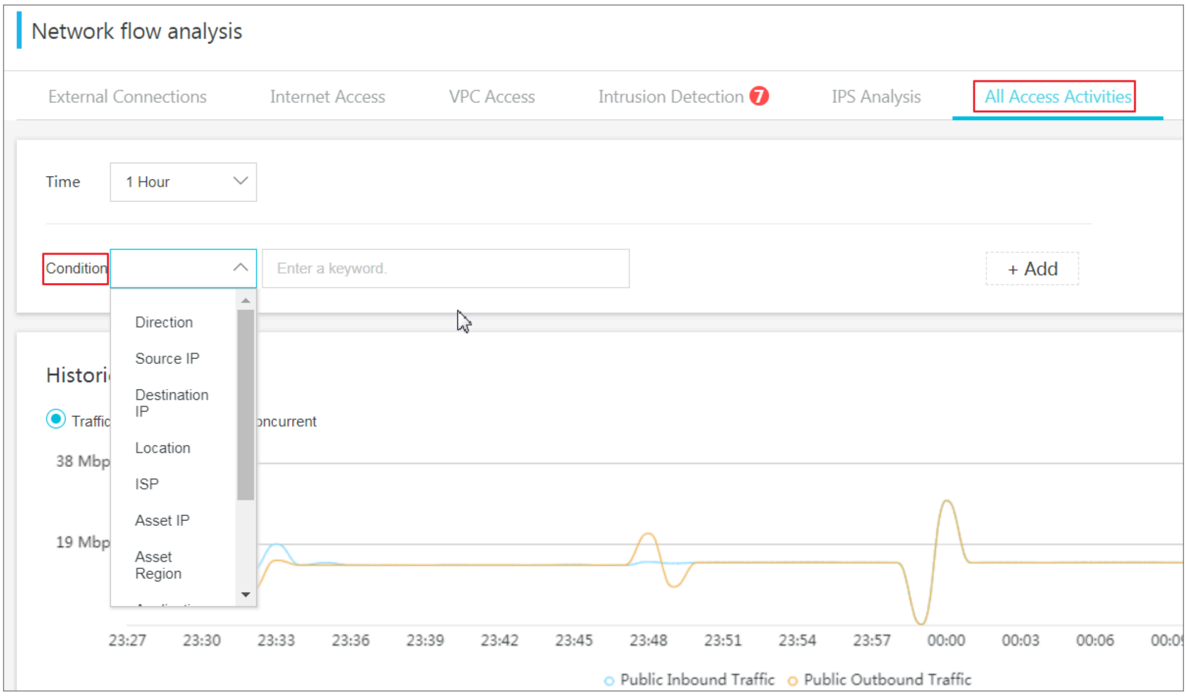
1. Log on to the *Cloud Firewall console*.

2. In the left-side navigation pane, go to Traffic Analysis > All Access Activities.

   You can view the historical trends for all the access activities in the last 15 minutes, 1 hour, 4 hours, 1 day, 7 days, or a custom time range.

   > Note:
   > 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 Search to query the historical traffic trend based on the selected condition.

   Time: 1 Hour

   In the Rankings of Visits by Traffic area, view the top 10 source regions and application types with the most requested inbound/outbound traffic and top N session addresses. You can also view the percentage of each source location, application protocol, or session address.

5 Configure access control policies

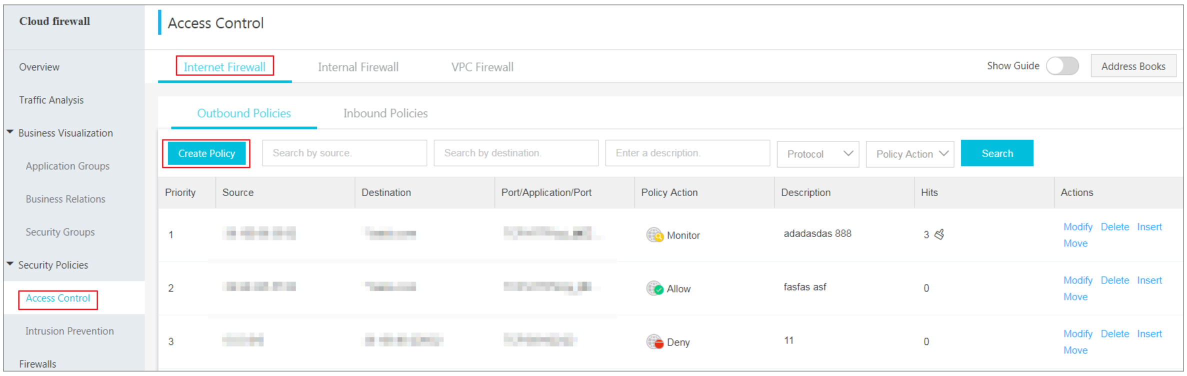
Cloud Firewall allows you to configure access control policies to specify the accessible ports on your assets and control the access from your assets to the Internet. You can use access control policies to control inbound and outbound traffic.

You could add a group of IP addresses or ports to the Address Books. With this Address Book, you can quickly configure the control policy with multiple IP or addresses.

Procedure

1. Log on to the *Cloud Firewall console*.

2. On the Access Control > Internet firewall page of the console, click Create Policy to configure an access control policy.

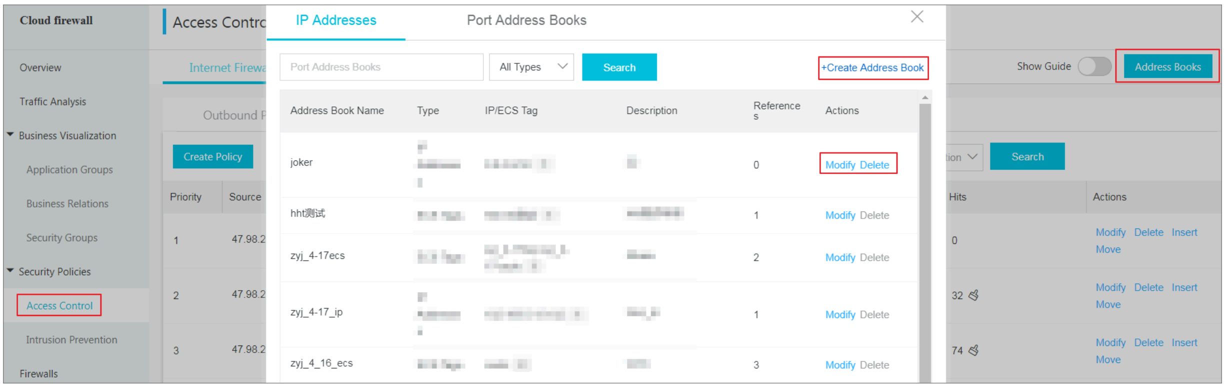


Priority	Source	Destination	Port/Application/Port	Policy Action	Description	Hits	Actions
1	[redacted]	[redacted]	[redacted]	Monitor	adadasdas 888	3	Modify Delete Insert Move
2	[redacted]	[redacted]	[redacted]	Allow	fasfas asf	0	Modify Delete Insert Move
3	[redacted]	[redacted]	[redacted]	Deny	11	0	Modify Delete Insert Move

Configurations are as follows:

- Source Type: The data sender type. Select IP or Address book.
- Source: The address of data sender. If you select IP for Source Type, you must enter an IP address or CIDR block in Access Source.
- Destination Type: The type of the data's destination. You can select IP, Address Book or Domian Name.
- Destination: The data's destination address.
- Protocol: The protocol of the data. The supported protocols include TCP, UDP, and ICMP.
- Port Type: The type of the port, including Ports and Address Book.
- Destination Port: The port of the data's recipient.
- Application: The application to which the access control policy applies in the specified protocol.
- Policy Action: The action on the access traffic. You can select Allow, Monitor or Deny.
- Description: The remarks on the access control policy.

Click Address books on the Internet Firewall page, you can create new address books, or modify/delete existing address books.



Priority	Source	Hits	Actions
1	47.98.2	0	Modify Delete Insert Move
2	47.98.2	32	Modify Delete Insert Move
3	47.98.2	74	Modify Delete Insert Move

Address Book Name	Type	IP/ECS Tag	Description	References	Actions
joker	[redacted]	[redacted]	[redacted]	0	Modify Delete
hht测试	[redacted]	[redacted]	[redacted]	1	Modify Delete
zyj_4-17ecs	[redacted]	[redacted]	[redacted]	2	Modify Delete
zyj_4-17_ip	[redacted]	[redacted]	[redacted]	1	Modify Delete
zyj_4_16_ecs	[redacted]	[redacted]	[redacted]	3	Modify Delete

Note:

Except for certain necessary/safe external connection activities, we recommend that you select Deny for all the other outbound access to the Internet .