ALIBABA CLOUD

Alibaba Cloud

Cloud Firewall
Traffic Analysis

Document Version: 20220425

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
⚠ Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⚠ Danger: Resetting will result in the loss of user configuration data.
🔔 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	🔔 Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
📢 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	📢 Notice: If the weight is set to 0, the server no longer receives new requests.
? Note	A note indicates supplemental instructions, best practices, tips, and other content.	? Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Traffic analysis overview

Traffic analysis of Cloud Firewall provides visualized statistics on intrusion events, network activities, traffic trends, traffic blocked by the intrusion prevention system (IPS), and external connections across the network.

Cloud Firewall analyzes traffic in the following activities:

- External connections
- Internet access
- VPC access
- All access activities

2.Outbound connections

After the Internet firewall is enabled for your network assets, the Outbound Connections page displays real-time information about outbound connections initiated by your servers. This helps you detect suspicious servers. This topic describes the information displayed and operations that you can perform on this page.

Overview

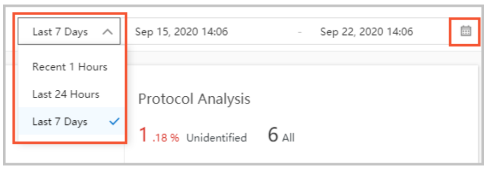
After you enable the Internet firewall for your network assets, you can log on to the Cloud Firewall console and choose **Traffic Analysis > Outbound Connections** in the left-side navigation pane to view traffic analysis data. For more information, see the following sections:

- Outbound connection statistics
- Outbound traffic
- Visualized analysis

> **Notice** The **Outbound Connections** page displays traffic analysis data only after you enable the Internet firewall. For information about how to enable the Internet firewall, see Enable firewalls.

In the upper-right corner of the Outbound Connections page, you can customize a time range from the date and time picker. You can also select **Recent 1 Hours**, **Last 24 Hours**, or **Last 7 Days** from the time drop-down list. You can specify a custom time range that is no more than seven days.

> **Note** Otherwise, the system displays an error message to prompt you that the time range you specify is invalid and you must select a time range within seven days.



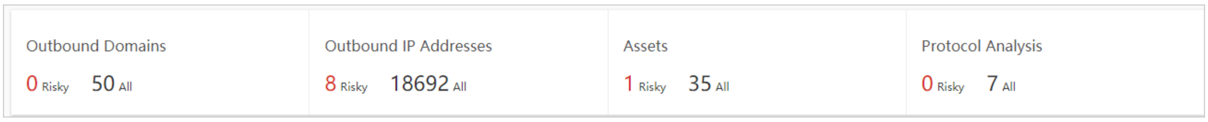
Sep 15, 2020 14:06 - Sep 22, 2020 14:06

Protocol Analysis

1 .18 % Unidentified 6 All

Outbound connection statistics

This section is in the upper part of the **Outbound Connections** page. It provides the following statistics:



Outbound Domains	Outbound IP Addresses	Assets	Protocol Analysis
0 Risky 50 All	8 Risky 18692 All	1 Risky 35 All	0 Risky 7 All

- **Outbound Domains**: the total number of domain names and the number of risky domain names in outbound connections.

  You can click this section to view details about the domain names on the Outbound Domains tab of the **Outbound traffic** tab.

- **Outbound IP Addresses**: the total number of destination IP addresses and the number of risky destination IP addresses in outbound connections.

  You can click this section to view details about the outbound IP addresses on the Outbound IP Addresses tab of the **Outbound traffic** tab.

- **Assets**: the total number of assets that initiate outbound connections and the number of assets that initiate risky outbound connections.

  You can click this section to view details about the assets on the Assets tab of the **Outbound traffic** tab.

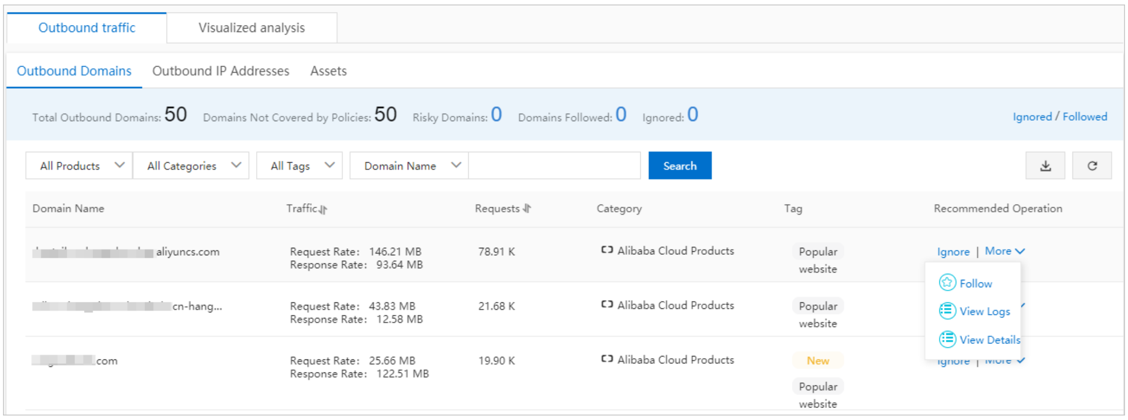
- **Protocol Analysis**: the analysis results of protocols used in outbound connections, including the total number of protocols and the proportion of outbound connections with unidentified protocols.

  You can click this section to view details about the IP address traffic and analysis results of protocols in the **Visualized analysis** tab. This tab displays IP Traffic and Protocol Analysis.

Outbound traffic

The **Outbound traffic** tab displays domain names, destination IP addresses, and assets used in outbound connections. You can click the **Outbound Domains**, **Outbound IP Addresses**, or **Assets** tab to view details.

- **Outbound Domains**

  Outbound traffic | Visualized analysis

  Outbound Domains | Outbound IP Addresses | Assets

  Total Outbound Domains: 50 Domains Not Covered by Policies: 50 Risky Domains: 0 Domains Followed: 0 Ignored: 0 Ignored / Followed

  All Products | All Categories | All Tags | Domain Name | Search

Domain Name	Traffic	Requests	Category	Tag	Recommended Operation
[redacted]aliyuncs.com	Request Rate: 146.21 MB Response Rate: 93.64 MB	78.91 K	Alibaba Cloud Products	Popular website	Ignore | More Follow View Logs View Details
[redacted]cn-hang...	Request Rate: 43.83 MB Response Rate: 12.58 MB	21.68 K	Alibaba Cloud Products	Popular website	
[redacted].com	Request Rate: 25.66 MB Response Rate: 122.51 MB	19.90 K	Alibaba Cloud Products	New Popular website	Ignore | More

  Each record includes the following information: **Domain Name**, **Traffic**, **Requests**, **Category**, **Intelligence Tag**, and **Recommended Operation**. **Category** and **Intelligence Tag** are website attributes that Cloud Firewall adds based on the Internet information of a domain name. For more information about the tags, see FAQ about network traffic analysis.

  You can click the

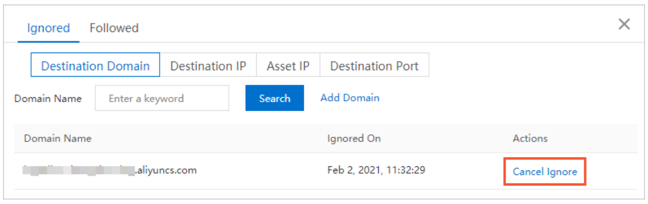
  ⤓

  icon in the upper-right corner above the outbound domain name list to download the list to your computer in the CSV format for check and analysis.

  You can perform the following operations on the outbound domain names:

  - **Ignore**: Find a domain name and click **Ignore** in the Recommended Operation column. The domain name is added to the **Destination Domain** tab of the **Ignored** tab.

    To remove a domain name from the Ignored tab, click **Ignored** in the upper-right corner. On the **Destination Domain** tab, find the domain name and click **Cancel Ignore** in the Actions column.

    Ignored | Followed

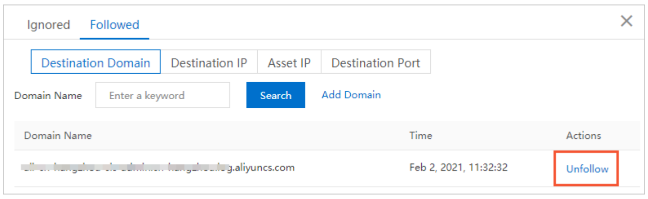
    Destination Domain | Destination IP | Asset IP | Destination Port

    Domain Name: Enter a keyword | Search | Add Domain

Domain Name	Ignored On	Actions
[redacted].aliyuncs.com	Feb 2, 2021, 11:32:29	Cancel Ignore

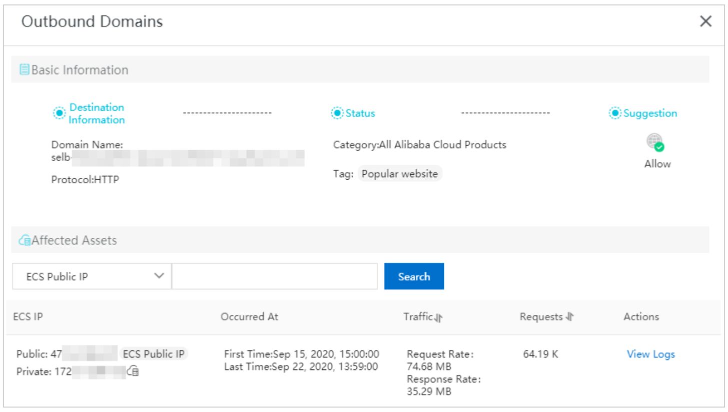
- **Follow**: Find a domain name and choose **More > Follow** in the Recommended Operation column. The domain name is added to the **Destination Domain** tab of the **Followed** tab.

  To unfollow a domain name, click **Followed** in the upper-right corner. On the **Destination Domain** tab, find the domain name and click **Unfollow** in the Actions column.

Domain Name	Time	Actions
[redacted]g.aliyuncs.com	Feb 2, 2021, 11:32:32	Unfollow

- **View Logs**: Find a domain name and choose **More > View Logs** in the Recommended Operation column. On the **Traffic Logs** tab of the **Log Audit** page, view the traffic information about the domain name. For more information, see Log audit.
- **View Details**: Find a domain name and choose **More > View Details** in the Recommended Operation column. In the Outbound Domains panel, view the access details of the domain name. The details include the IP addresses of ECS instances that access the domain name, the time when the outbound connections are initiated, the transmission rates of request and response traffic, and the number of requests. The following figure shows the access details of a domain name.

  Domain Name: selb[redacted]

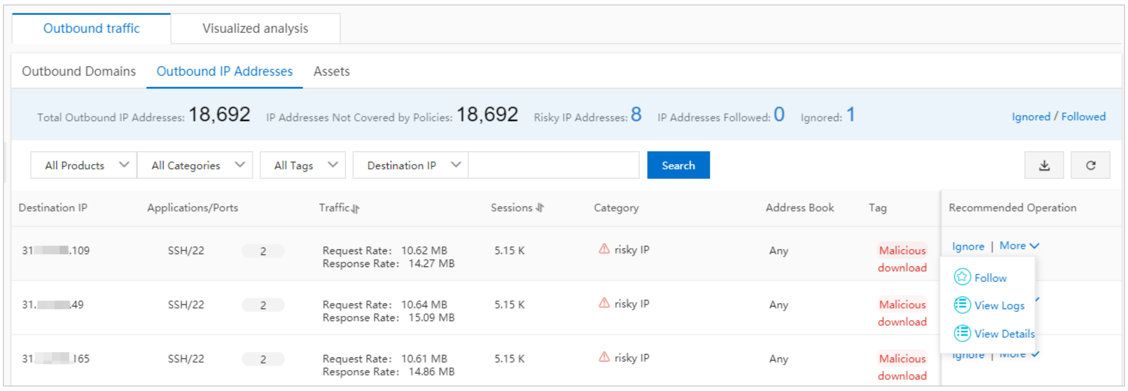
  Protocol:HTTP

  Category:All Alibaba Cloud Products

  Tag: Popular website

ECS IP	Occurred At	Traffic	Requests	Actions
Public: 47[redacted] ECS Public IP Private: 172[redacted]	First Time:Sep 15, 2020, 15:00:00 Last Time:Sep 22, 2020, 13:59:00	Request Rate: 74.68 MB Response Rate: 35.29 MB	64.19 K	View Logs

- **Outbound IP Addresses**



Total Outbound IP Addresses: 18,692 IP Addresses Not Covered by Policies: 18,692 Risky IP Addresses: 8 IP Addresses Followed: 0 Ignored: 1

Destination IP	Applications/Ports		Traffic	Sessions	Category	Address Book	Tag	Recommended Operation
31[redacted].109	SSH/22	2	Request Rate: 10.62 MB Response Rate: 14.27 MB	5.15 K	⚠ risky IP	Any	Malicious download	Ignore | More
31.[redacted].49	SSH/22	2	Request Rate: 10.64 MB Response Rate: 15.09 MB	5.15 K	⚠ risky IP	Any	Malicious download	
31[redacted].165	SSH/22	2	Request Rate: 10.61 MB Response Rate: 14.86 MB	5.15 K	⚠ risky IP	Any	Malicious download	Ignore | More

Each record includes the following information: **Destination IP**, **Applications/Ports**, **Traffic**, **Sessions**, **Category**, **Address Book**, **Intelligence Tag**, and **Recommended Operation**. **Category** and **Intelligence Tag** are website attributes that Cloud Firewall adds based on the Internet information of a domain name. For more information about the tags, see FAQ about network traffic analysis.**Address Book** indicates the address book that stores the destination IP address.

You can click the

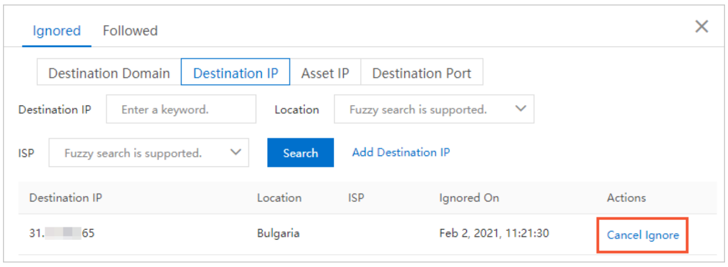
⤓

icon in the upper-right corner above the outbound IP address list to download the list to your computer in the CSV format for check and analysis.

You can perform the following operations on the outbound IP addresses:

- **Ignore**: Find an IP address and click **Ignore** in the Recommended Operation column. The IP address is added to the **Destination IP** tab of the **Ignored** tab.

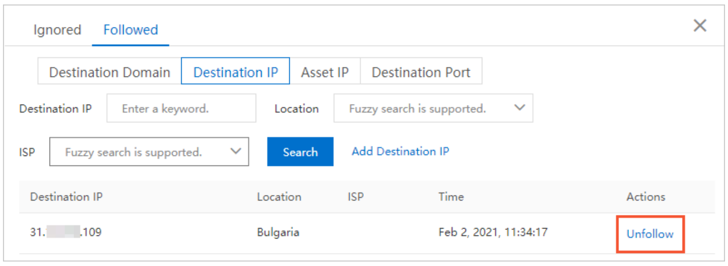
  To remove an IP address from the Ignored tab, click **Ignored** in the upper-right corner. On the **Destination IP** tab, find the IP address and click **Cancel Ignore** in the Actions column.

Destination IP	Location	ISP	Ignored On	Actions
31.[redacted]65	Bulgaria		Feb 2, 2021, 11:21:30	Cancel Ignore

- **Follow**: Find an IP address and choose **More > Follow** in the Recommended Operation column. The IP address is added to the **Destination IP** tab of the **Followed** tab.

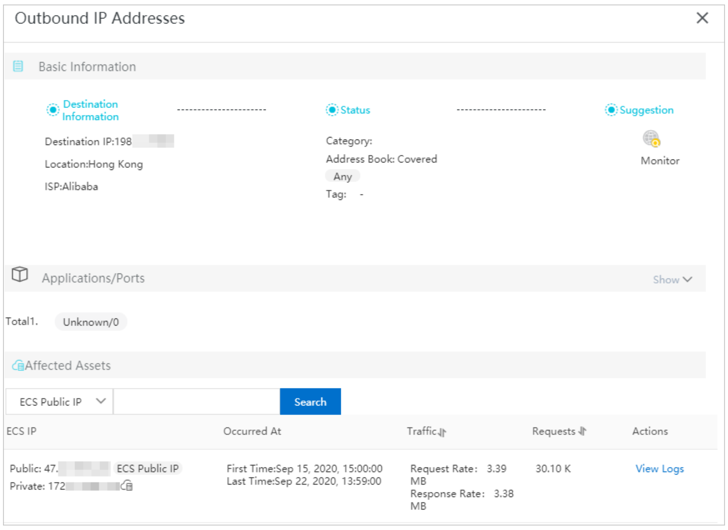
  To unfollow an IP address, click **Followed** in the upper-right corner. On the **Destination IP** tab, find the IP address and click **Unfollow** in the Actions column.

Destination IP	Location	ISP	Time	Actions
31.[redacted].109	Bulgaria		Feb 2, 2021, 11:34:17	Unfollow

- **View Logs**: Find an IP address and choose **More > View Logs** in the Recommended Operation column. On the **Traffic Logs** tab of the **Log Audit** page, view the traffic information about the IP address. For more information, see Log audit.

- ○ **View Details**: Find a domain name and choose **More > View Details** in the Recommended Operation column. In the Outbound IP Addresses panel, view the access details of the IP address. The details include the IP address of ECS instances that access this IP address, the time when outbound connections are initiated, transmission rates of request and response traffic, and the number of requests. The following figure shows the access details of a destination IP address.



Outbound IP Addresses

Basic Information

Destination Information

Destination IP:198[redacted]

Location:Hong Kong

ISP:Alibaba

Status

Category:

Address Book: Covered

Any

Tag: -

Suggestion

Monitor

Applications/Ports

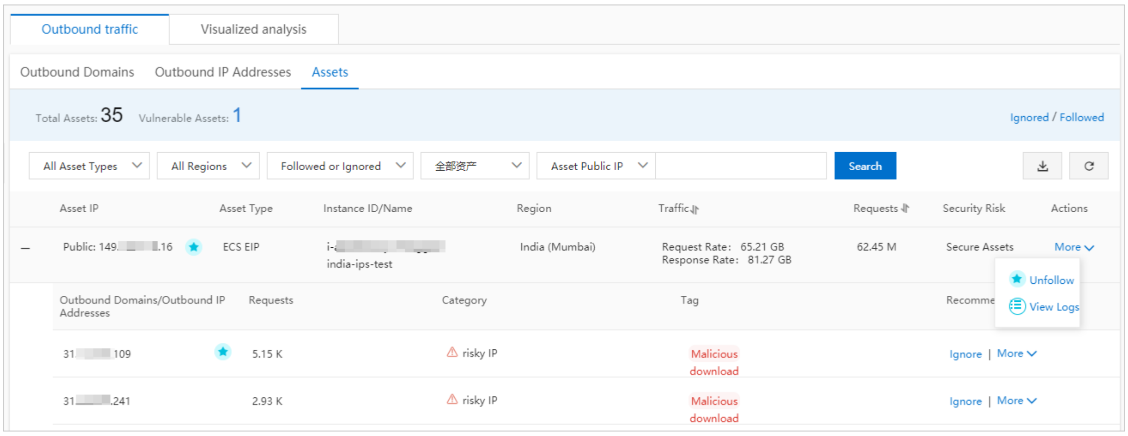
Total1. Unknown/0

Affected Assets

ECS Public IP | Search

ECS IP	Occurred At	Traffic	Requests	Actions
Public: 47.[redacted] ECS Public IP Private: 172[redacted]	First Time:Sep 15, 2020, 15:00:00 Last Time:Sep 22, 2020, 13:59:00	Request Rate: 3.39 MB Response Rate: 3.38 MB	30.10 K	View Logs

- **Assets**



Outbound traffic | Visualized analysis

Outbound Domains | Outbound IP Addresses | Assets

Total Assets: 35 Vulnerable Assets: 1 Ignored / Followed

All Asset Types | All Regions | Followed or Ignored | 全部资产 | Asset Public IP | Search

Asset IP	Asset Type	Instance ID/Name	Region	Traffic	Requests	Security Risk	Actions
Public: 149.[redacted].16	ECS EIP	i-[redacted] india-ips-test	India (Mumbai)	Request Rate: 65.21 GB Response Rate: 81.27 GB	62.45 M	Secure Assets	More Unfollow View Logs

Outbound Domains/Outbound IP Addresses	Requests	Category	Tag	Recomme
31[redacted]109	5.15 K	⚠ risky IP	Malicious download	Ignore | More
31[redacted].241	2.93 K	⚠ risky IP	Malicious download	Ignore | More

Each record includes the following information: **Asset IP**, **Asset Type**, **Instance ID/Name**, **Region**, **Traffic**, **Requests**, **Security Risk**, and **Actions**. **Security Risk** indicates the status that Cloud Firewall sets for an asset based on outbound connection records.

You can click the

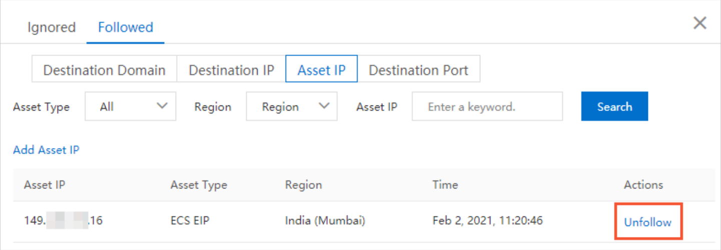
⤓

icon in the upper-right corner above the asset list to download the list to your computer in the CSV format for check and analysis.

You can perform the following operations on the asset IP addresses:

- **Follow**: Find an asset IP address and choose **More > Follow** in the Actions column. The IP address is added to the **Asset IP** tab of the **Followed** tab.

  To unfollow an asset IP address, click **Followed** in the upper-right corner. On the **Asset IP** tab, find the IP address and click **Unfollow** in the Actions column.

Asset IP	Asset Type	Region	Time	Actions
149.[redacted].16	ECS EIP	India (Mumbai)	Feb 2, 2021, 11:20:46	Unfollow

- **View Logs**: Find an asset IP address and choose **More > View Logs** in the Actions column. On the **Traffic Logs** tab of the **Log Audit** page, view the traffic information about the asset IP address, which indicates the source IP address of an outbound connection. For more information, see Log audit.
- To view more details about an asset IP address, click the

  +

  icon next to the asset IP address.

  The details include **Outbound Domains/Outbound IP Addresses**, **Requests**, **Category**, **Tag**, and **Recommended Operation**. **Category** and **Intelligence Tag** are website attributes that Cloud Firewall adds based on the Internet information of a domain name. For more information about the tags, see FAQ about network traffic analysis.

  You can perform the following operations on an outbound domain name or IP address that is displayed in the details:

  - **Ignore**: Find an outbound domain name or IP address and click **Ignore** in the Recommended Operation column. The domain name or IP address is added to the **Destination Domain** or **Destination IP** tab of the **Ignored** tab.

    To remove a domain name or IP address from the Ignored tab, click **Ignored** in the upper-right corner. On the **Destination Domain** tab, find the domain name or IP address and click **Cancel Ignore** in the Actions column.

  - **Follow**: Find an outbound domain name or IP address and choose **More > Follow** in the Recommended Operation column. The domain name or IP address is added to the **Destination Domain** or **Destination IP** tab of the **Followed** tab.

    To unfollow a domain name or IP address, click **Followed** in the upper-right corner. On the **Destination Domain** or **Destination IP** tab, find the domain name or IP address and click **Unfollow** in the Actions column.

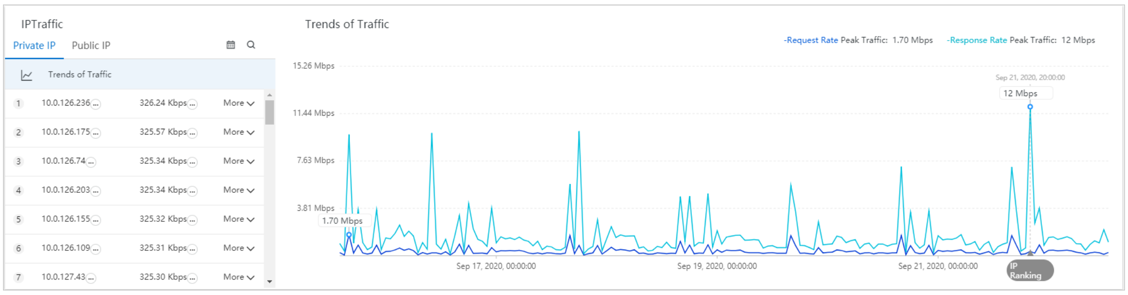
  - **View Logs**: Find an outbound domain name or IP address and choose **More > View Logs** in the Recommended Operation column. On the **Traffic Logs** tab of the **Log Audit** page, view the traffic information about the domain name or IP address. For more information, see Log audit.

Visualized analysis

The **Visualized analysis** tab displays the **IP traffic statistics** and **protocol analysis** modules.

- **IP traffic statistics**

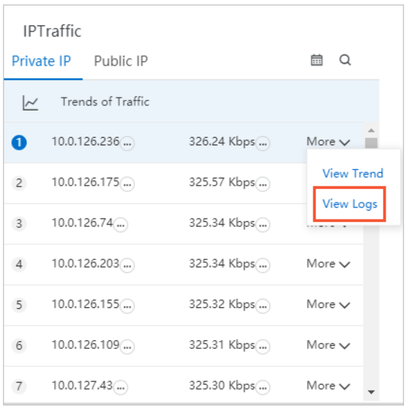
This module provides IP address lists in the **IP Traffic** section and traffic trends of IP addresses in the **Trends of Traffic** section. You can click an IP address in the lists to view its traffic trend.



1	10.0.126.236 ...	326.24 Kbps ...	More
2	10.0.126.175 ...	325.57 Kbps ...	More
3	10.0.126.74 ...	325.34 Kbps ...	More
4	10.0.126.203 ...	325.34 Kbps ...	More
5	10.0.126.155 ...	325.32 Kbps ...	More
6	10.0.126.109 ...	325.31 Kbps ...	More
7	10.0.127.43 ...	325.30 Kbps ...	More

IP Traffic: lists private and public IP addresses in descending order based on their response traffic at a specific point in time.

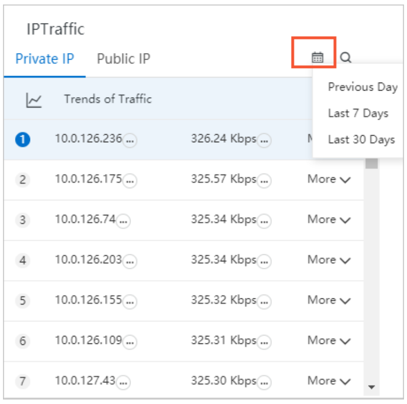
- Click the **Private IP** or **Public IP** tab to check the traffic of IP addresses.
- In the **Trends of Traffic** section, click a point in time on the x-axis to refresh the traffic rankings in the IP Traffic section.
- Find an IP address and choose **More > View Logs**. On the **Traffic Logs** tab of the **Log Audit** page, view the traffic information about the IP address. For more information, see Log audit.



1	10.0.126.236 ...	326.24 Kbps ...	More
2	10.0.126.175 ...	325.57 Kbps ...	
3	10.0.126.74 ...	325.34 Kbps ...	
4	10.0.126.203 ...	325.34 Kbps ...	More
5	10.0.126.155 ...	325.32 Kbps ...	More
6	10.0.126.109 ...	325.31 Kbps ...	More
7	10.0.127.43 ...	325.30 Kbps ...	More

Trends of Traffic: displays the peak transmission rates of request and response traffic of specified or all network assets in real time. You can move the pointer over a position in the trend chart to view the peak transmission rates at the point in time that corresponds to the position.

- Specify a time range. By default, data of the last seven days is displayed. You can select a time range in the **IP Traffic** section.

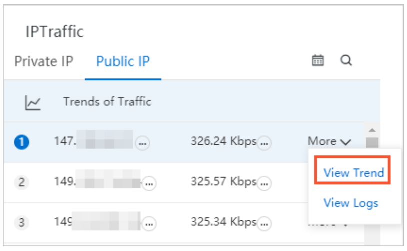
  

1	10.0.126.236 ...	326.24 Kbps ...	M
2	10.0.126.175 ...	325.57 Kbps ...	More
3	10.0.126.74 ...	325.34 Kbps ...	More
4	10.0.126.203 ...	325.34 Kbps ...	More
5	10.0.126.155 ...	325.32 Kbps ...	More
6	10.0.126.109 ...	325.31 Kbps ...	More
7	10.0.127.43 ...	325.30 Kbps ...	More

  The following time ranges are available:

  - **Previous Day**
  - **Last 7 Days**
  - **Last 30 Days**

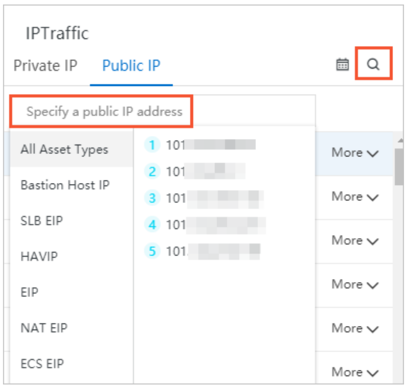
- Specify a data range. By default, the traffic trends of all protected network assets are displayed. In the **IP Traffic** section, you can specify an IP address to view its trends by using one of the following methods:
  - Click an IP address, or find an IP address and choose **More > View Trend**.



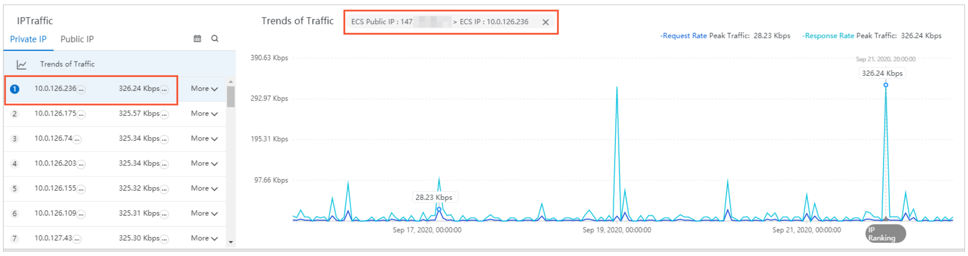
1	147.[redacted]	326.24 Kbps	More
2	149.[redacted]	325.57 Kbps	
3	14[redacted]	325.34 Kbps	

  - Click the search icon in the upper-right corner and enter a public or private IP address.

> **Note** After you perform this operation, the IP Traffic section does not display traffic rankings.



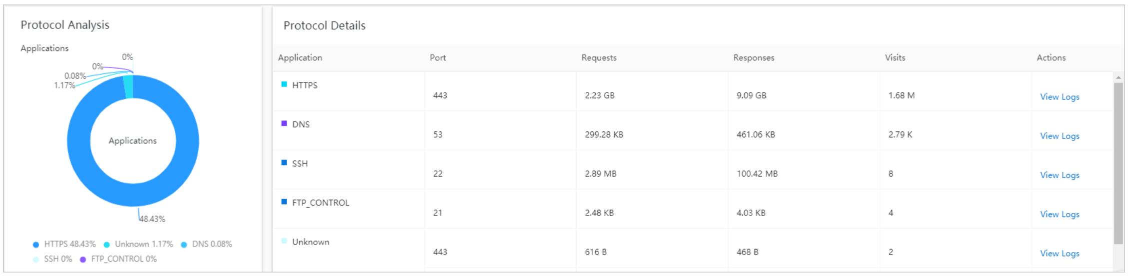
The filter condition you specified is displayed above the chart.



1	10.0.126.236	326.24 Kbps	More
2	10.0.126.175	325.57 Kbps	More
3	10.0.126.74	325.34 Kbps	More
4	10.0.126.203	325.34 Kbps	More
5	10.0.126.155	325.32 Kbps	More
6	10.0.126.109	325.31 Kbps	More
7	10.0.127.43	325.30 Kbps	More

- **Protocol analysis**

  This module contains the Protocol Analysis and **Protocol Details** sections. The Protocol Analysis section provides a pie chart of **Applications**.



Protocol Details

Application	Port	Requests	Responses	Visits	Actions
HTTPS	443	2.23 GB	9.09 GB	1.68 M	View Logs
DNS	53	299.28 KB	461.06 KB	2.79 K	View Logs
SSH	22	2.89 MB	100.42 MB	8	View Logs
FTP_CONTROL	21	2.48 KB	4.03 KB	4	View Logs
Unknown	443	616 B	468 B	2	View Logs

  Applications: displays the proportion of each application protocol used in outbound connections.

Protocol Details: displays the details about application protocols used in outbound connections. You can find an application and click **View Logs** in the **Actions** column. On the **Traffic Logs** tab of the Log Audit page, you can view the traffic information about the application.

References

- Enable firewalls
- FAQ about network traffic analysis
- Intelligent policies
- Manage address books

3.Internet access

The Internet Access page of the Cloud Firewall console provides an overview of the normal and abnormal inbound traffic of your assets, including the information about open applications, open ports, open public IP addresses, and cloud services to which inbound traffic flows.

Prerequisites

The Internet firewall is enabled. Otherwise, the **Internet Access** page does not provide traffic analysis data.

For more information about how to enable the Internet firewall, see Enable firewalls.

Procedure

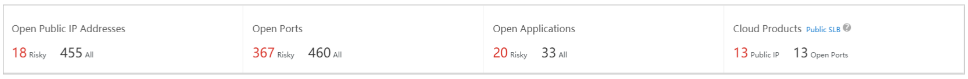
1.
2.
3. In the upper-right corner of the **Internet Access** page, specify a time range for query.

   You can select the following time ranges from the time drop-down list: **Last 1 Hour**, **Last 24 Hours**, and **Last 7 Days**. You can also customize a time range within the last seven days by using the date and time picker.国际站截图和中国站不一致，需更新中文

4. View the data about access over the Internet.

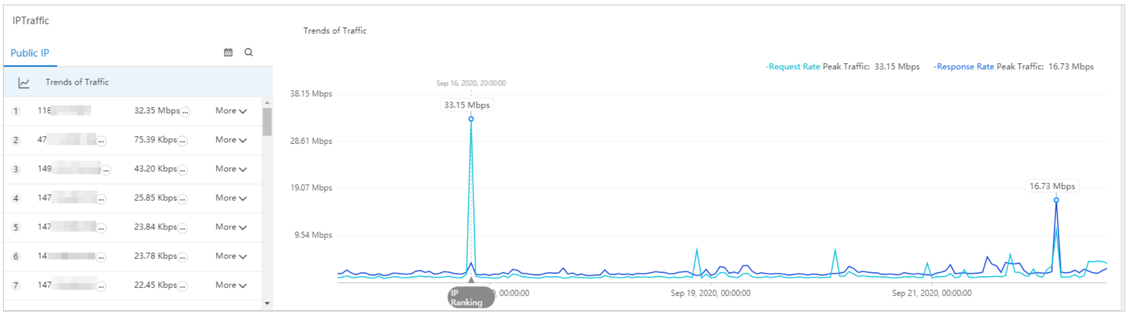
   You can view the following data:

   - Overview of Internet access activities: You can view the numbers of total and risky items below **Open Public IP Addresses**, **Open Ports**, and **Open Applications**. You can also view the number of risky public IP addresses specified by **Public IP** and the total number of open ports specified by **Open ports** below **Cloud Products**.



Open Public IP Addresses	Open Ports	Open Applications	Cloud Products Public SLB
18 Risky 455 All	367 Risky 460 All	20 Risky 33 All	13 Public IP 13 Open Ports

   - **IP Traffic** and **Trends of Traffic**



IPTraffic

Public IP

Trends of Traffic

1	118[redacted]	32.35 Mbps...	More
2	47[redacted]...	75.39 Kbps...	More
3	149[redacted]...	43.20 Kbps...	More
4	147[redacted]...	25.85 Kbps...	More
5	147[redacted]...	23.84 Kbps...	More
6	14[redacted]...	23.78 Kbps...	More
7	147[redacted]...	22.45 Kbps...	More

- **IP Traffic**: You can view public IP addresses in descending order based on their transmission rates at a specific point in time. The point is represented by **IP Ranking** in the x-axis of the chart in the **Trends of Traffic** section.

  You can perform the following operations in the **IP Traffic** ranking list:

  - Find a public IP address and choose **More > View Trend**. Then, you can view the traffic trend of the public IP address in the **Trends of Traffic** section.
  - Find a public IP address and choose **More > View Logs**. Then, the **Traffic Logs** tab of the **Log Audit** page appears. You can view the inbound traffic of the public IP address. For more information, see Log audit.

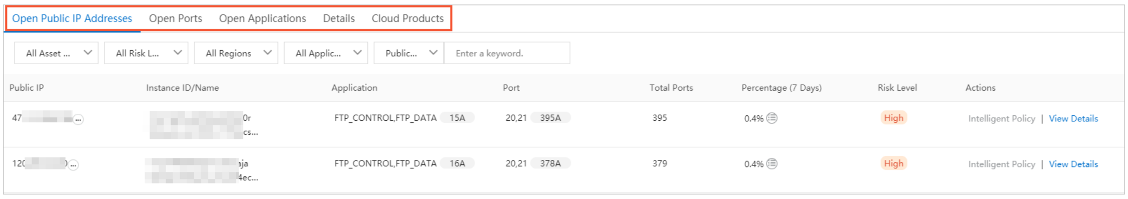
- **Trends of Traffic**: You can view the peak transmission rates of request and response traffic on all assets.

- Details of Internet access activities: You can view **Open Public IP Addresses**, **Open Ports**, **Open Applications**, **Details**, and **Cloud Products**.

  You can click the

  ⤓

  icon in the upper-right corner above each list to download the data to a CSV file to your computer for check and analysis.



Public IP	Instance ID/Name	Application	Port	Total Ports	Percentage (7 Days)	Risk Level	Actions
47[redacted]...	[redacted]0r cs...	FTP_CONTROL,FTP_DATA 15A	20,21 395A	395	0.4%	High	Intelligent Policy | View Details
12[redacted]...	[redacted]ja 4ec...	FTP_CONTROL,FTP_DATA 16A	20,21 378A	379	0.4%	High	Intelligent Policy | View Details

4.VPC access

The VPC Access page of the Cloud Firewall console provides real-time information about traffic between virtual private clouds (VPCs). This way, you can detect suspicious traffic and mitigate risks at the earliest opportunity. The VPC Access page provides statistics on the traffic, IP addresses, sessions, ports, and assets involved in communications between VPCs.

Prerequisites

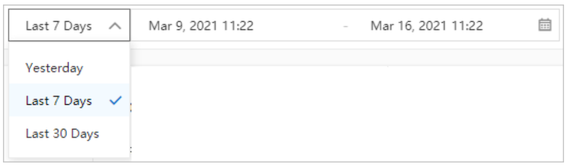
The required VPC firewall is enabled. Otherwise, the **VPC Access** page does not provide traffic analysis data.

For more information about how to enable a VPC firewall, see Enable firewalls.

Procedure

1.
2.
3. In the upper-right corner of the **VPC Access** page, specify a time range for query.

   You can select the following time ranges from the time drop-down list: **Recent 1 Hours**, **Last 24 Hours**, and **Last 7 Days**. You can also customize a time range within the last seven days by using the date and time picker.

4. In the upper part of the **VPC Access** page, select the required VPC and VPC firewalls.
5. View the data about access of the selected VPC.

   You can view the following data:

   - **Traffic Between VPCs**: You can view the peak and average volumes of both inbound and outbound traffic of the VPC. You can also view the trends in both inbound and outbound traffic.
   - **Ranking of IP Addresses by Traffic**: You can view the top 10, 20, or 50 IP addresses with the highest traffic. You can also view the details of inbound and outbound traffic for each IP address.
   - **Ranking of Sessions Between VPCs by Visits and Traffic**: You can view the ranking of sessions between VPCs. You can also view the traffic volume, session type, number of sessions, and ports for each type of session.

     In the **Rankings of Sessions Between VPCs by Visits and Traffic** section, you can click **View** in the **Ratio** column to view the proportions of ports in a specific type of session.
   - **Open Ports by Traffic**: You can view the proportions of all open ports.
   - **Open Ports** and **Assets**: You can view the details of traffic between VPCs. The details include basic information about open ports and your assets.

You can click the ⤓ icon in the upper-right corner above the port or asset list to download the open ports or assets to a CSV file to your computer for check and analysis.

5.All access activities

The All Access Activities page displays real-time activity information about all hosts protected by Cloud Firewall. Such information includes traffic trends, as well as source locations and sessions of inbound and outbound traffic.

Prerequisites

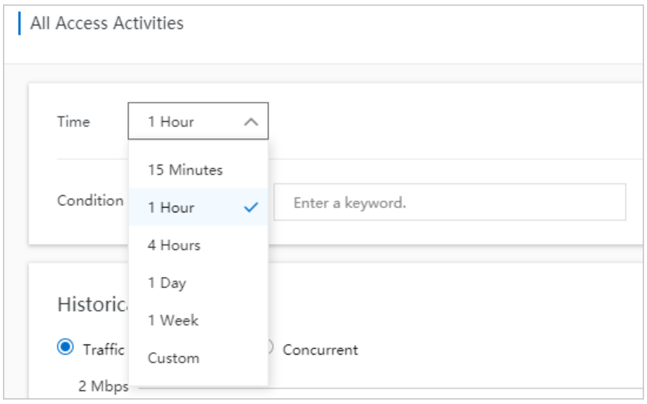
The **All Access Activities** page displays the analysis data only after you activate Cloud Firewall. For information about how to activate Cloud Firewall, see Enable firewalls.

Procedure

1.

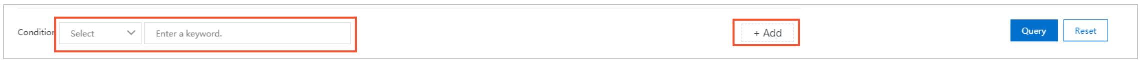
2.

3. On the **All Access Activities** page, view the threat activities and trend charts in the last 15 minutes, 1 hour, 4 hours, 1 day, 1 Week, or a specified time range.



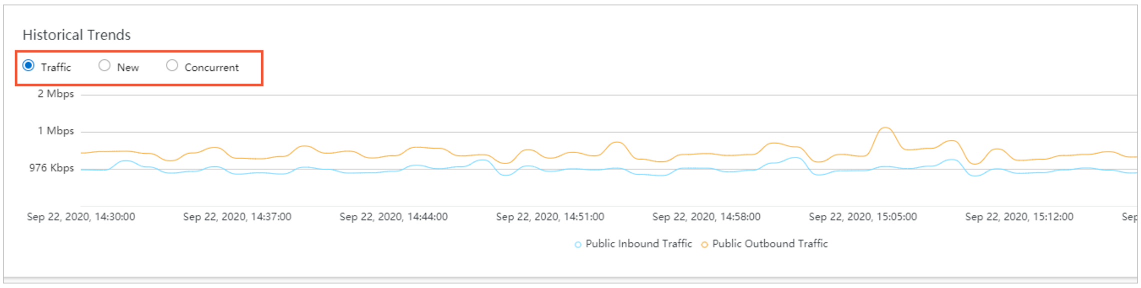
Note You can specify a time range as required.

- Select a search condition from the **Condition** drop-down list and enter or select the condition details. Click **Query** to query historical traffic trends that meet the condition. To delete the search condition, click **Reset** .



Note You can click **Add** to add search conditions. All conditions take effect at the same time when you click Query. You can configure a maximum of three conditions.

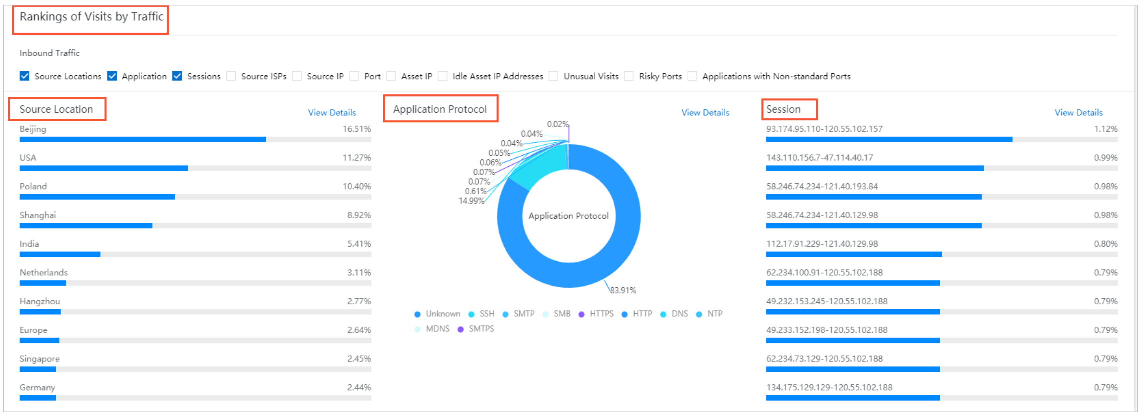
- In the **Historical Trends** section, view the trend charts of inbound and outbound traffic, the number of new connections, and concurrent traffic.



You can select **Traffic**, **New**, or **Concurrent** to switch between the trend charts of inbound and outbound traffic, the number of new connections, and the inbound and outbound concurrent traffic.

> **Note** A trend chart displays traffic data in the last 15 minutes, 1 hour, 4 hours, 1 day, 7 days, or a specified time range. You can specify a time range as required.

- In the **Rankings of Visits by Traffic** section, you can view top 10 source locations and applications of inbound and outbound traffic, as well as the percentages of traffic for each source location and application.



Rankings of Visits by Traffic

Inbound Traffic

☑ Source Locations ☑ Application ☑ Sessions □ Source ISPs □ Source IP □ Port □ Asset IP □ Idle Asset IP Addresses □ Unusual Visits □ Risky Ports □ Applications with Non-standard Ports

Source Location	View Details
Beijing	16.51%
USA	11.27%
Poland	10.40%
Shanghai	8.92%
India	5.41%
Netherlands	3.11%
Hangzhou	2.77%
Europe	2.64%
Singapore	2.45%
Germany	2.44%

Session	View Details
93.174.95.110-120.55.102.157	1.12%
143.110.156.7-47.114.40.17	0.99%
58.246.74.234-121.40.193.84	0.98%
58.246.74.234-121.40.129.98	0.98%
112.17.91.229-121.40.129.98	0.80%
62.234.100.91-120.55.102.188	0.79%
49.232.153.245-120.55.102.188	0.79%
49.233.152.198-120.55.102.188	0.79%
62.234.73.129-120.55.102.188	0.79%
134.175.129.129-120.55.102.188	0.79%

- Click **View Details** to check the statistics on source or destination locations or application protocols.
- Click **Add to Condition** to add the condition to the query condition setting section. After you click Query, the **Historical Trends** and **Rankings of Visits by Traffic** sections display trend charts of access activities that meet the condition.

References

Protection scope of Cloud Firewall

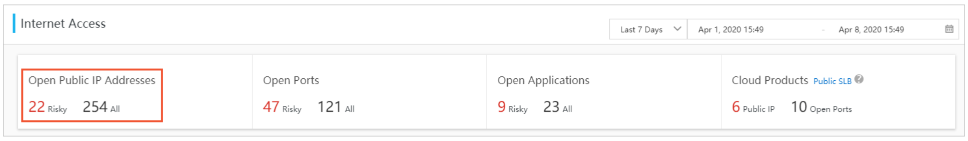
6.Intelligent policies

Cloud Firewall provides intelligent ACL policies for Internet access and external connections. These policies isolate high-risk services for inbound traffic, prevent the spread of worm viruses in outbound traffic, and defend your networks and hosts against security threats.

Isolate high-risk services

Intelligent policies provide you with optimal ACL policies based on security threats detected in Internet access traffic. For example, if high-risk services, such as SSH and RDP, are enabled for IP addresses exposed to the Internet, the recommended policies only allow Internet requests sent by hosts that exhibits normal logon status and from common source locations. This reduces risks of network attacks.

1.
2.
3. On the **Internet Access** page, click **Open Public IP Addresses**.

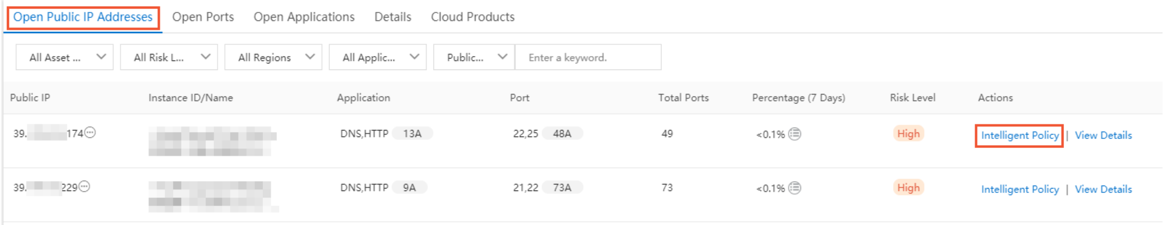


Internet Access

Last 7 Days | Apr 1, 2020 15:49 - Apr 8, 2020 15:49

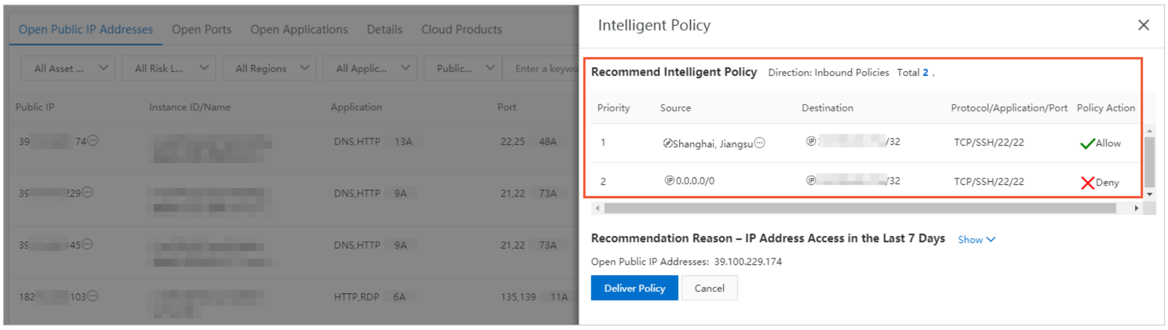
Open Public IP Addresses	Open Ports	Open Applications	Cloud Products Public SLB
22 Risky 254 All	47 Risky 121 All	9 Risky 23 All	6 Public IP 10 Open Ports

4. Find the target public IP address and click **Intelligent Policy** in the **Actions** column.



Public IP	Instance ID/Name	Application	Port	Total Ports	Percentage (7 Days)	Risk Level	Actions
39.[redacted]174	[redacted]	DNS,HTTP 13A	22,25 48A	49	<0.1%	High	Intelligent Policy | View Details
39.[redacted]229	[redacted]	DNS,HTTP 9A	21,22 73A	73	<0.1%	High	Intelligent Policy | View Details

The **Intelligent Policy** page displays policies recommended for the public IP address, including both **Allow** and **Deny** policies.



Public IP	Instance ID/Name	Application	Port
39[redacted]74	[redacted]	DNS,HTTP 13A	22,25 48A
39[redacted]229	[redacted]	DNS,HTTP 9A	21,22 73A
39[redacted]45	[redacted]	DNS,HTTP 9A	21,22 73A
182[redacted]103	[redacted]	HTTP,RDP 6A	135,139 11A

Intelligent Policy

Recommend Intelligent Policy Direction: Inbound Policies Total 2 ,

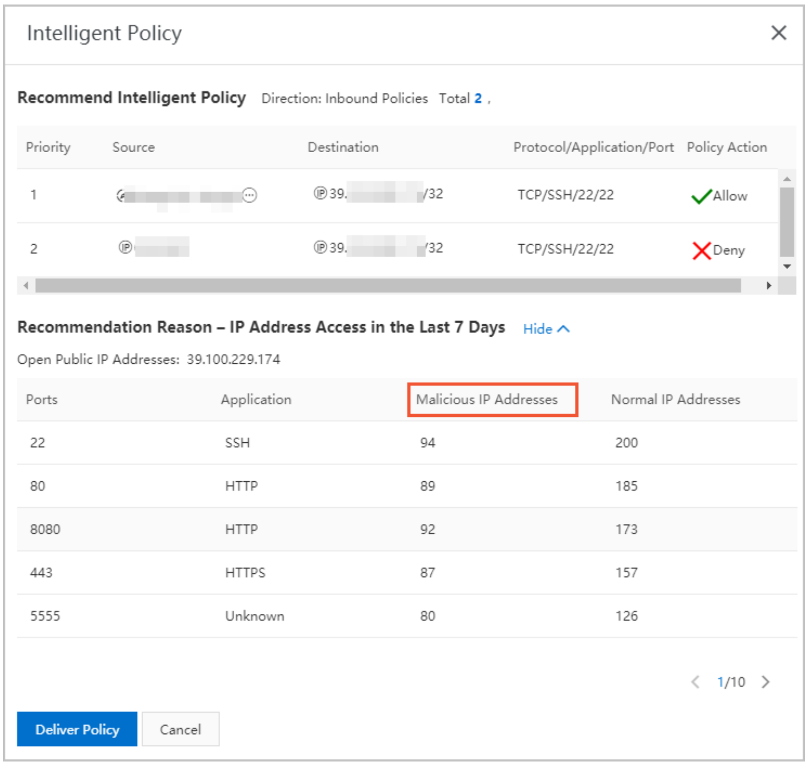
Priority	Source	Destination	Protocol/Application/Port	Policy Action
1	Shanghai, Jiangsu	[redacted]/32	TCP/SSH/22/22	✓ Allow
2	0.0.0.0/0	[redacted]/32	TCP/SSH/22/22	✗ Deny

Recommendation Reason – IP Address Access in the Last 7 Days Show

Open Public IP Addresses: 39.100.229.174

5. On the **Intelligent Policy** page, you can perform the following operations:
   - Click **Show** to view the reason why a policy is recommended.

     The following figure shows that a large number of malicious IP addresses have tried to access the SSH service of your IP address.



Intelligent Policy

Recommend Intelligent Policy Direction: Inbound Policies Total 2 ,

Priority	Source	Destination	Protocol/Application/Port	Policy Action
1	[redacted]	39.[redacted]/32	TCP/SSH/22/22	✓Allow
2	[redacted]	39.[redacted]/32	TCP/SSH/22/22	✗Deny

Recommendation Reason – IP Address Access in the Last 7 Days Hide

Open Public IP Addresses: 39.100.229.174

Ports	Application	Malicious IP Addresses	Normal IP Addresses
22	SSH	94	200
80	HTTP	89	185
8080	HTTP	92	173
443	HTTPS	87	157
5555	Unknown	80	126

- Choose **Deliver Policy** > **Submit**. The recommended policy takes effect immediately. You can view delivered policies by choosing **Security Policies** > **Access Control** > **Internet Firewall** > **Inbound Policies**.

> **Note** Before you click **Deliver Policy** to deliver a recommended policy, make that you understand its content and possible service impacts.

You can perform **Modify**, **Delete**, **Insert**, and **Move** operations on a delivered policy.

Prevent worm attacks

Worm attacks control your host by using malicious code and cause it to send requests to the domain name of a malicious website. After Cloud Firewall detects that your host has initiated an external connection request, a recommended policy takes effect to prevent access to malicious domain name, downloads of malicious programs, virus-control over the host, and attacks by using cryptocurrency mining malware.

1.
2.
3. On the **External Connections** page, click **External Domains**.

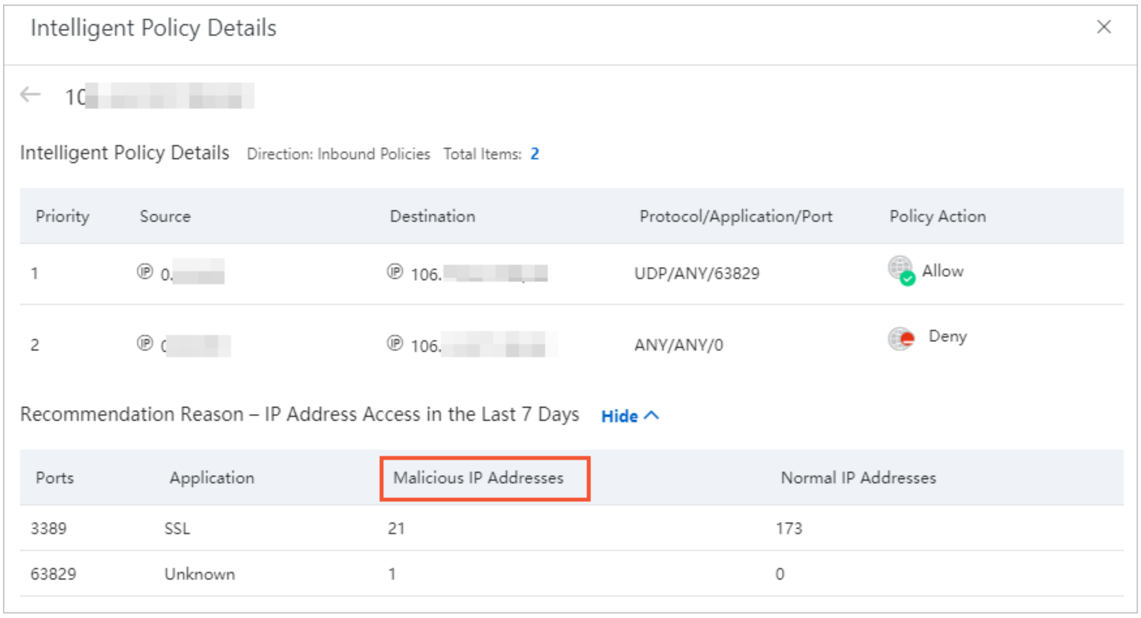
   The page displays the external domain name list.

4. Find the target external domain name and click **Intelligent Policy** in the **Recommended Operation** column.

   The **Intelligent Policy** page displays **Deny** policies recommended by Cloud Firewall for an IP address based on its external connections.

5. On the **Intelligent Policy** page, you can perform the following operations:
   - Click **Show** to view the reason why an intelligent policy is recommended.

The following figure shows that the host has sent many requests to malicious destinations.



Intelligent Policy Details

10[redacted]

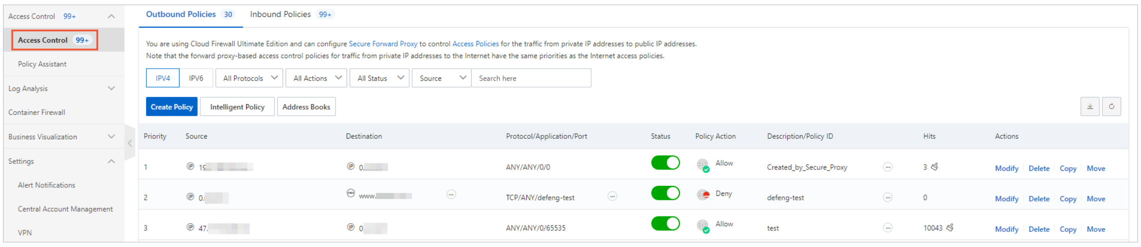
Intelligent Policy Details Direction: Inbound Policies Total Items: 2

Priority	Source	Destination	Protocol/Application/Port	Policy Action
1	0.[redacted]	106.[redacted]	UDP/ANY/63829	Allow
2	([redacted]	106.[redacted]	ANY/ANY/0	Deny

Recommendation Reason – IP Address Access in the Last 7 Days Hide

Ports	Application	Malicious IP Addresses	Normal IP Addresses
3389	SSL	21	173
63829	Unknown	1	0

- Choose **Deliver Policy** > **Submit**. The recommended policy takes effect immediately. You can view delivered policies by choosing **Security Policies** > **Access Control** > **Internet Firewall** > **Outbound Policies**.



You are using Cloud Firewall Ultimate Edition and can configure Secure Forward Proxy to control Access Policies for the traffic from private IP addresses to public IP addresses.
Note that the forward proxy-based access control policies for traffic from private IP addresses to the Internet have the same priorities as the Internet access policies.

Priority	Source	Destination	Protocol/Application/Port	Status	Policy Action	Description/Policy ID	Hits	Actions
1	19[redacted]	0.[redacted]	ANY/ANY/0/0		Allow	Created_by_Secure_Proxy	3	Modify Delete Copy Move
2	0.[redacted]	www.[redacted]	TCP/ANY/defeng-test		Deny	defeng-test	0	Modify Delete Copy Move
3	47.[redacted]	0[redacted]	ANY/ANY/0/65535		Allow	test	10043	Modify Delete Copy Move

Note Before you click **Deliver Policy** to deliver a recommended policy, make sure that you understand its content and possible service impacts.

You can perform the **Modify**, **Delete**, **Insert**, and **Move** operations on a delivered policy.