ALIBABA CLOUD

Alibaba Cloud

Cloud Firewall

Traffic Analysis

Document Version: 20201019

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
- Breach awareness
- Traffic blocked by IPS
- All access activities

2.Outbound connections

After Cloud Firewall is activated for network assets, the Outbound Connections page displays information about outbound connections initiated by your servers in real time, which helps you detect suspicious servers. This topic describes the information on this page and operations that you can perform on this page.

Overview

The Outbound Connections page consists of the following four modules. You can click a module name to view its details and perform required operations. To go to the Outbound Connections page, log on to the Cloud Firewall console, and choose **Traffic Analysis** > **Outbound Connections** in the left-side navigation pane.

- Outbound connection statistics
- IP traffic statistics
- Protocol analysis
- Outbound connections

> **Note** The **Outbound Connections** page displays traffic analysis data only after you activate Cloud Firewall. For information about how to activate Cloud Firewall, see Activate Cloud Firewall.

In the upper-right corner, click the date and time picker to specify a time range. You can select **Recent 1 Hours**, **Last 24 Hours**, **Last 7 Days**, or specify a time range that spans seven days. If you specify a time range that spans more than seven days, an error message appears.

Outbound connection statistics

This module provides statistics on outbound connections.

- **Outbound Domains**: the total number of outbound domain names and the number of risky outbound domain names. You can click this section to view details about the outbound domain names.
- **Outbound IP Addresses**: the total number of outbound IP addresses and the number of risky outbound IP addresses. You can click this section to view details about the outbound IP addresses.
- **Assets**: the total number of assets that initiate outbound connections and the number of risky assets. You can click this section to view details about the assets.
- **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 protocols.

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.

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

- Click the **Private IP** or **Public IP** tab to check the traffic of IP addresses.
- In the **Trends of Traffic** section, click a time point on the horizontal axis to refresh the traffic rankings in the IP Traffic section.
- Find the IP address that you want to query, click the drop-down arrow next to **More** in the Actions column, and then click **View Logs**. The **Traffic Logs** tab appears, and you can view traffic logs of the IP address on this tab.

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 to any position in the chart to view the peak transmission rates at the time point that corresponds to the position.

- Specify the time range. By default, data of the last seven days is displayed. You can use the date picker in the upper-right corner of the **IP Traffic** section to specify a time range.

  

  The following time ranges are available:

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

- Specify the data range. By default, the overall 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 following methods:
  - Click the IP address or find the IP address, click the drop-down arrow next to **More** in the Actions column, and then click **View Trend**.

    

  - 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 on top of the chart.

  

Protocol analysis

This module displays a pie chart in the **Applications** section and a table in the **Protocol Details** section.

Applications: displays the proportions of application protocols used in outbound connections.

Protocol Details: displays the details about the application protocols used in outbound connections. You can follow or ignore a specific application or view its logs.

- Follow an application: Find the application that you want to follow, click **More** in the Actions column, and then click **Follow**. The port of the followed application is added to the Destination Port tab on the Followed tab. You can click **Followed** in the upper-right corner, click the **Destination Port** tab, find the port, and then click **Unfollow** in the Actions column to unfollow it.
- Ignore an application: Find the application that you want to ignore, click **More** in the Actions column, and click **Ignore**. The port of the ignored application is added to the Destination Port tab on the Ignored tab. The ignored application is removed from the Protocol Analysis section. You can click **Ignored** in the upper-right corner, click the **Destination Port** tab, find the port, and then click **Cancel Ignore** in the Actions column to unignore it.
- View logs of an application: Find the application whose logs you want to view, click **More** in the Actions column, and then click **View Logs**. The **Traffic Logs** tab appears. You can view traffic logs of this application on this tab.

Outbound connections

This module displays domain names, destination IP addresses, and assets used in outbound connections. Click the **Outbound Domains**, **Outbound IP Addresses**, or **Assets** tab to view details.

- **Outbound Domains**

  

  Each record includes the following information: **Domain Name**, **Traffic**, **Requests**, **Category**, **Tag**, and **Recommended Operation**.

  - **Category** and **Tag** are website attributes of an outbound domain name.
  - **Recommended Operation**includes the following options: Intelligent policy delivery
    - **Follow**: Add the current outbound domain name to the followed list. You can click **Followed** in the upper-right corner, click the **Destination Domain** tab, find the domain name, and then click **Unfollow** to unfollow it.
    - **Ignore**: Add the current outbound domain name to the ignored list. You can click **Ignored** in the upper-right corner, click the **Destination Domain** tab, find the domain name, and then click **Cancel Ignore** to unignore it.
    - **View Logs**: View the detailed traffic information of an outbound domain name on the **Traffic Logs** tab.
    - **View Details**: View the access details of an outbound domain name. The details include ECS instance IP addresses that are mapped to this domain name, the time outbound connections are initiated, transmission rates of request and response traffic, and the number of requests. The following figure shows the access details of an outbound domain name.

      

- **Outbound IP Addresses**

  

  Each record includes the following information: **Destination IP**, **Applications/Ports**, **Traffic**, **Sessions**, **Category**, **Address Book**, **Tag**, and **Recommended Operation**.

  - **Category** and **Tag** are website attributes of an outbound IP address.
  - **Address Book** indicates the address book that stores an outbound IP address.

- **Recommended Operation** includes the following options: Intelligent policy delivery
  - **Follow**: Add the current outbound IP address to the followed list. You can click **Followed** in the upper-right corner, click the **Destination IP** tab, find the IP address, and then click **Unfollow** to unfollow it.
  - **Ignore**: Add the current outbound IP address to the ignored list. You can click **Ignored** in the upper-right corner, click the **Destination IP** tab, find the IP address, and then click **Cancel Ignore** to unignore it.
  - **View Logs**: View the detailed traffic information of an outbound IP address on the **Traffic Logs** tab.
  - **View Details**: View the access details of an outbound IP address. The details include ECS instances bound to this IP address, the time outbound connections are initiated, transmission rates of request and response traffic, and the number of requests. The following figure shows the access details of an outbound IP address.

    

- **Assets**

  

  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 Cloud Firewall sets for an asset based on outbound connection records.
  - Supported operations in the **Actions** column include:
    - **Follow**: Add the current asset IP address to the followed list. You can click **Followed** in the upper-right corner, click the **Asset IP** tab, find the asset IP address, and then click **Unfollow** to unfollow it.
    - **Ignore**: Add the current asset IP address to the ignored list. You can click **Ignored** in the upper-right corner, click the **Asset IP** tab, find the asset IP address, and then click **Cancel Ignore** to unignore it.
    - **View Logs**: View the detailed traffic information of an asset IP address (the source IP address of an outbound connection) on the **Traffic Logs** tab.

  Click the plus sign next to an asset to view more details about its outbound connections, including **Outbound Domains/Outbound IP Addresses**, **Requests**, **Category**, **Tag**, and **Recommended Operation**.

  - **Category** and **Tag** are website attributes of an outbound IP address or domain name.
  - **Recommended Operation** includes the following options: Intelligent policy delivery
    - **Follow**: Add the current outbound IP address or domain name to the followed list. You can click **Followed** in the upper-right corner, click the **Destination IP** or **Destination Domain** tab, find the IP address or domain name, and then click **Unfollow** to unfollow it.
    - **Ignore**: Add the current outbound IP address or domain name to the ignored list. You can click **Ignored** in the upper-right corner, click the **Destination IP** or **Destination Domain** tab, find the IP address or domain name, and then click **Cancel Ignore** to unignore it.
    - **View Logs**: View the detailed traffic information of an outbound IP address or domain name on the **Traffic Logs** tab.

3.Internet access

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

Prerequisites

The **Internet Access** page displays traffic analysis data only after you activate Cloud Firewall. For information about how to activate Cloud Firewall, see Activate Cloud Firewall.

Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Traffic Analysis > Internet Access**.
3. On the **Internet Access** page, perform the following operations:
   - View overall information about Internet access activities, including the number of total and risky open applications, open ports, and open public IP addresses, as well as the number of public IP addresses and open ports of the cloud products.

     
   - View information in the **IP Traffic** and **Trends of Traffic** sections. The **IP Traffic** section lists public IP addresses in descending order based on their transmission rates at a specified time point. The time point is represented by **IP Ranking** in the horizontal axis in the chart in the **Trends of Traffic** section. The **Trends of Traffic** section displays the peak transmission rates of request and response traffic on all assets.

     

     In the **IP Traffic** section, find the IP address that you want to query, click the drop-down arrow next to **More** in the Actions column, and then click **View Logs**. On the **Traffic Logs** tab, view the inbound traffic of the IP address.

     In the **IP Traffic** section, find the IP address that you want to query, click the drop-down arrow next to **More** in the Actions column, and then click **View Trend**. In the **Trends of Traffic** section, view traffic trends of the IP address.
   - View the details of Internet access activities, including open public IP addresses, open ports, open applications, assets, and cloud products.

     

References

Protection scope of Cloud Firewall

4.VPC access

The VPC Access page provides real-time information about traffic between VPCs. It helps you promptly detect suspicious traffic and mitigate risks. You can view the statistics of traffic, sessions, ports, and assets involved in communications between VPCs.

Context

Cloud Firewall provides VPC firewalls to detect suspicious traffic between VPCs. All traffic information is displayed on the VPC Access page.

> Note The VPC Access page displays traffic analysis data only after you enable the VPC Firewall feature. For information about how to enable the VPC Firewall feature, see Activate Cloud Firewall.

Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose Traffic Analysis > VPC Access.
3. Select a VPC to view its traffic information.

   

   On the VPC Access page, perform the following operations:

   - View the peak and average traffic rates in both the inbound and outbound directions over a specific time range.
   - View the top 10, 20, or 50 IP addresses with the highest traffic rates, including their inbound and outbound traffic rates.
   - View the rankings of sessions between VPCs, including the number of sessions, traffic volumes, and ports.

     In the Rankings of Sessions Between VPCs by Visits and Traffic section, click View in the Ratio column to view the proportions of ports in a session.
   - View the proportions of all ports.
   - View the details of traffic between VPCs, including ports and assets.

     

5.Breach awareness

The Breach Awareness page displays intrusion events detected by the intrusion prevention system (IPS).

Prerequisites

The **Breach Awareness** page displays the detected intrusion events only after you enable Internet Firewall. For information about how to enable Internet Firewall, see Activate Cloud Firewall.

Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Traffic Analysis > Breach Awareness.**
3. On the **Breach Awareness** page, view the details of intrusion events.

   

   You can perform the following operations on the **Breach Awareness** page as required:

   - In the intrusion event list, view the event details, such as risk levels, IP addresses of the affected assets, and the event status.
   - Specify a filter condition. such as a risk level, status, or time range, or enter an instance IP address, and then click **Search** to search for intrusion events that meet the condition.
   - If an intrusion event is a normal activity, click **Ignore** in the **Actions** column to ignore this event.

     > **Note** After you click **Ignore**, the intrusion event is removed from the list, and Cloud Firewall no longer reports alerts for this event.

   - View details of an event. Find the intrusion event that you want to view details and click **View Details** in the **Actions** column. In the Details pane, you can view the details of the intrusion event and the security tips.

     > **Note** The **Block** function does not take effect on single events. You can enable this function to enable the Intrusion Prevention feature provided by Cloud Firewall.

6.Traffic blocked by IPS

The Traffic Blocked by IPS page displays real-time data of traffic blocked by the intrusion prevention system (IPS) of Cloud Firewall. The data includes source locations, destination IP addresses, and applications of the traffic, IPS modules used to block the traffic, and the traffic blocking event details. This topic describes data that is displayed on the Traffic Blocked by IPS page and the operations that you can perform on this page.

Prerequisites

Basic Policies on the **Intrusion Prevention** page is turned on.

Overview

The Traffic Blocked by IPS page displays data of traffic blocked by the Internet firewall and VPC firewalls. You can view details on the **Internet Traffic Blocking** or **VPC Traffic Blocking** tab. To go to the Traffic Blocked by IPS page, choose **Traffic Analysis > Traffic Blocked by IPS** in the left-side navigation pane.

Traffic blocked by IPS

Internet Traffic Blocking

On the **Internet Traffic Blocking** tab, you can view the inbound or outbound traffic that is blocked in the last one hour, one day, seven days, one month, or a custom time range within the last three months.

Traffic Blocked by IPS

The Internet Traffic Blocking tab contains the following sections:

- **The Most Blocked Source Locations** section displays the source and destination locations of inbound and outbound traffic blocked by the Cloud Firewall IPS.

  The Most Blocked Source Locations

- The **Blocked Destination IP Addresses** section displays the destination IP addresses of inbound or outbound traffic blocked by the Cloud Firewall IPS.

  Blocked Destination IP Addresses

  If you want to view details about a blocked destination IP address, click the **View Logs** icon to go to the **Log Audit** page. In the log list, you can view the destination port and application of the IP address, and the actions that you can perform on the IP address.

- The **Blocked Applications** section displays the top five applications whose inbound and outbound traffic is blocked by the Cloud Firewall IPS.

  Blocked Applications

- The **Blocking Criteria** section displays the percentage of traffic blocked by each IPS module.

  Blocking Criteria

- The **Detailed Data** section displays details about each traffic blocking event, including the risk level, number of times the event occurred, source IP address, and destination IP address.

In the **Detailed Data** section, you can perform the following operations:

- Search for events based on the risk level, module, traffic direction, or time range.
- Click **View Details** in the **Action** column to check details about a traffic blocking event.

  Event details

References

- Protection scope of Cloud Firewall
- Intrusion prevention

7.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 Activate Cloud Firewall.

Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Traffic Analysis > All Access Activities**.
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, 7 days, 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.

     

   - 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

8.Intelligent policy delivery

Cloud Firewall provides the intelligent policy feature targeted at Internet access and external connections. With this feature, Cloud Firewall provides security policies to isolate high-risk services (inbound traffic) and prevent worms from spreading (outbound traffic), and recommends ACL policies to help you defend against security threats to networks and hosts.

Isolation of high-risk services

The **intelligent policy** feature of Cloud Firewall provides you with the optimal ACL policy based on detected security threats in Internet access traffic. For example, if high-risk services such as SSH and RDP are enabled on IP address assets that are exposed to the Internet and are at risk of being cracked or intruded, the **intelligent policy** feature will recommend a policy. This policy allows only Internet requests sent by users in normal logon status and in commonly used logon areas, and rejects requests from other logon areas to reduce the risk of network attacks.

1. Log on to the Cloud Firewall console.
2. Choose **Traffic Analysis** > **Internet Access** > **Open Public IP Addresses**.
3. Find the target public IP address and click **Intelligent Policy** in the **Actions** column corresponding to the public IP address.

   On the **Intelligent Policy** page that appears, the **Recommended Intelligent Policy** section is displayed. The recommended intelligent policy specifies the **allow** or **deny** action on user IP addresses and ports.
4. On the **Intelligent Policy** page, perform the following operations.
   - Click **Show** to view the reason for recommending the intelligent policy.

     For example, you can see that a large number of malicious IP addresses have tried to access the SSH service of the user IP address.
   - Click **Deliver Policy**. Choose **Security Policies** > **Access Control** > **Internet Firewall** > **Inbound Policies** to view the configured defense policy.

     > **Note** Before clicking **Deliver Policy**, make sure that you understand the meaning of the recommended policy and the possible impact of this policy on your business.

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

Worm prevention

When your host suffers from worm attacks, it will be controlled by the malicious code of the worm and send requests to domain names of malicious websites. If Cloud Firewall detects that your host has initiated an external connection request, Cloud Firewall recommends a policy to you to prevent the host from accessing malicious domain names, downloading malicious programs, being controlled, and being attacked by cryptocurrency mining malware.

1. Log on to the Cloud Firewall console.
2. Choose **Traffic Analysis** > **External Connections** > **External Domains**.
3. Find the target external domain name, and click **Intelligent Policy** in the **Recommended Operation** column corresponding to the external domain name.

On the **Intelligent Policy** page that appears, the **Recommended Intelligent Policy** section is displayed. The recommended intelligent policy specifies the allow or deny action on external connections.

4. On the **Intelligent Policy** page, perform the following operations.
   - Click **Show** to view the reason for recommending the intelligent policy.

     For example, you can see that your host has sent many malicious requests.
   - Click **Deliver Policy**. Choose **Security Policies > Access Control > Internet Firewall > Inbound Policies** to view the configured defense policy.

     > **Note** Before clicking **Deliver Policy**, make sure that you understand the meaning of the recommended policy and the possible impact of this policy on your business.

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