Alibaba Cloud
Cloud Firewall

User Guide

Issue: 20190530

Legal disclaimer

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

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `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 Cloud Firewall overview

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

1.1 Authorize Cloud Firewall

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

Background

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

- An Alibaba Cloud primary account
- A RAM user account with the AliyunRAMFullAccess permission

Note:

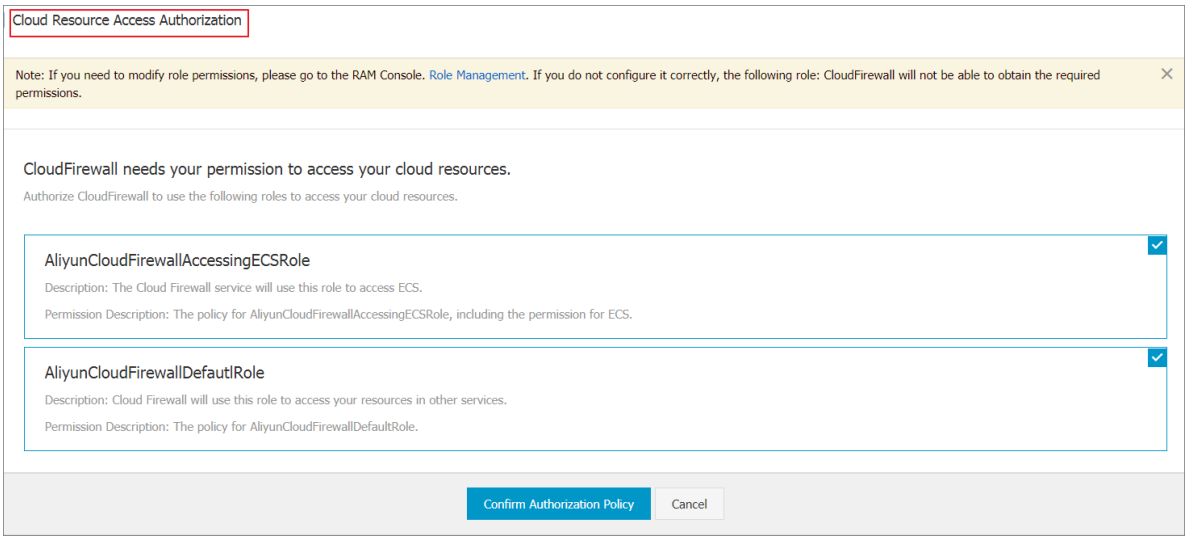
You cannot use a *RAM user account* without the AliyunRAMFullAccess permission to grant Cloud Firewall the access to cloud resources.

Authorization procedure

1. Click Confirm Authorization Policy.

   This grants Cloud Firewall the following permissions:

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



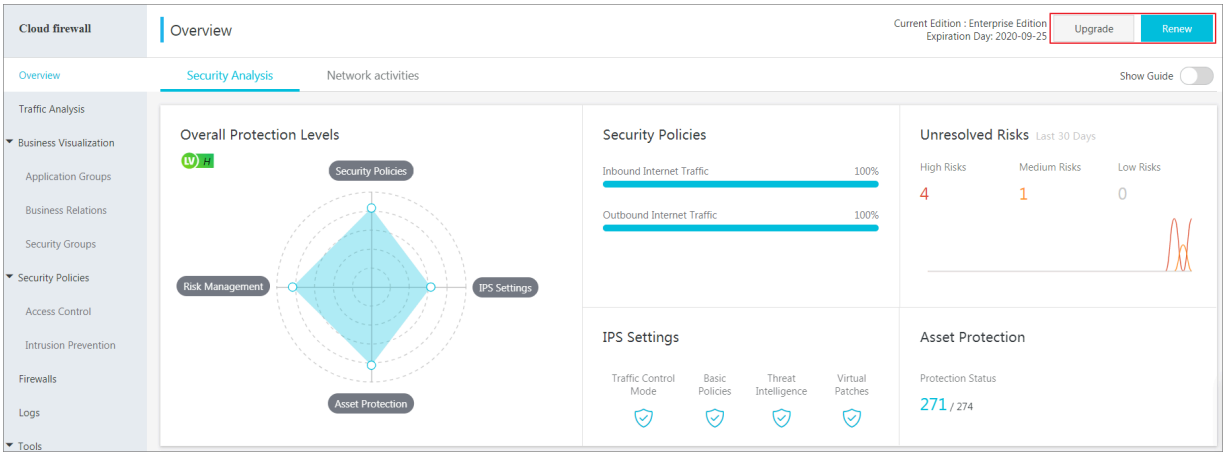
   After the authorization is complete, the system automatically returns to the Cloud Firewall console.

   Note:
   AliyunCloudFirewallAccessingECSRole and AliyunCloudFirewallDefautlRole are default permissions and are both required.

1.2 Upgrade and renewal

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

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



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

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

Note:

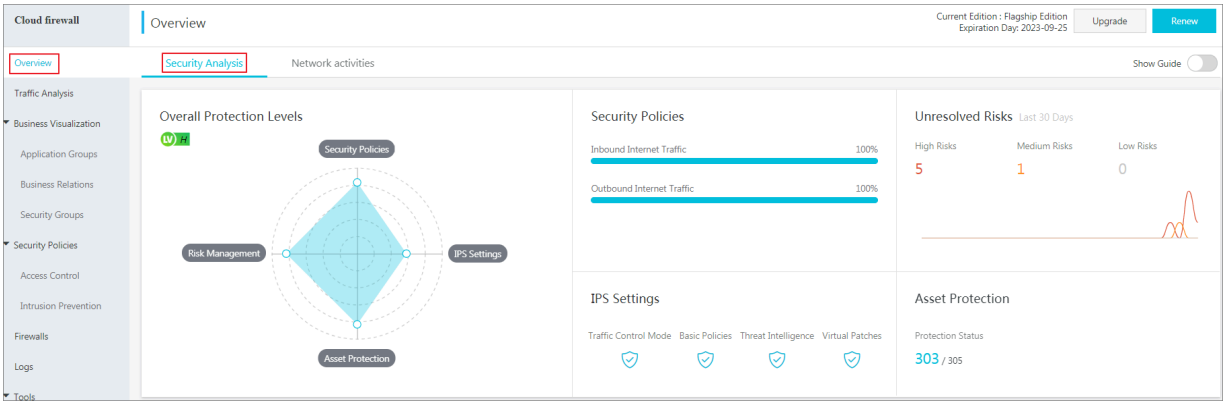
Renew the Cloud Firewall service in a timely manner before it expires to ensure that you can use the service properly.

1.3 Security analysis

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

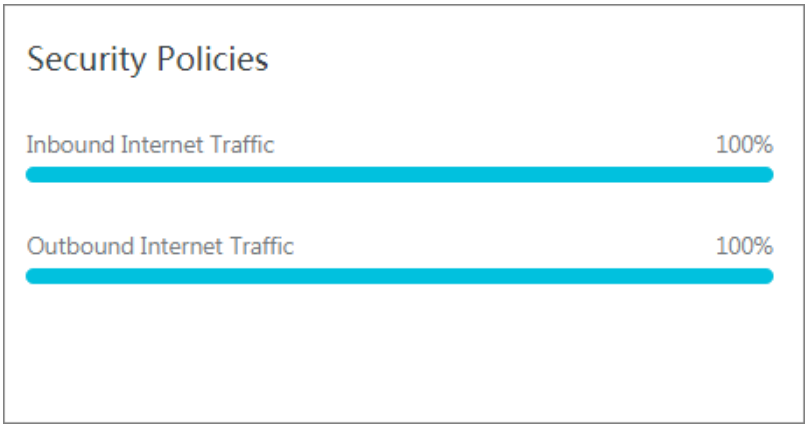
Overall protection levels include high (H), medium (M), and low (L). The four protection items are:

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



Security Policies

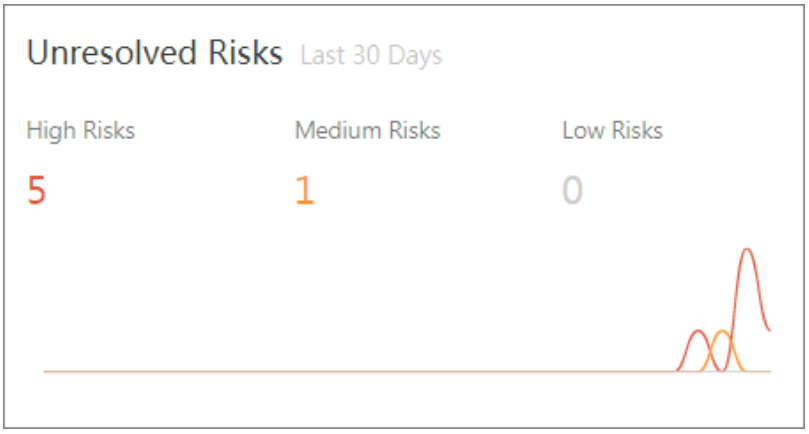
The Security Policies modules displays the percentage of the assets for which access control policies are configured in all your assets. The access control policies include those for outbound traffic to the Internet (in-out traffic) and those for inbound traffic from the Internet (out-in traffic).



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

Unresolved risks

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

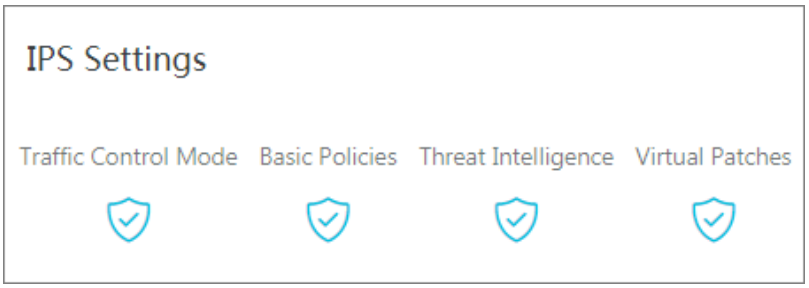


Click in this area to go to the Intrusion Detection tab page of the Network Traffic Analysis page, you can view and process threat activities detected by Cloud Firewall. The earlier the intrusions are handled, the higher the score.

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

IPS features include:

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



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

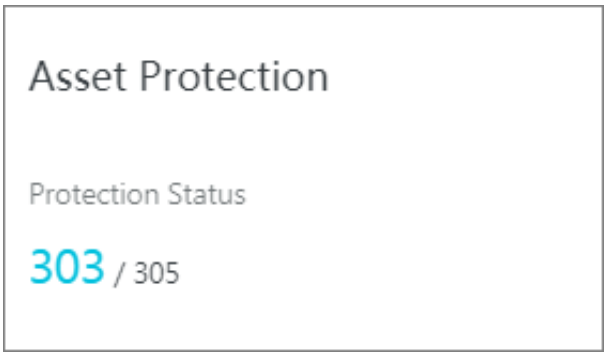
For more information, see *Intrusion prevention policies*.

Note:

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

Asset protection

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



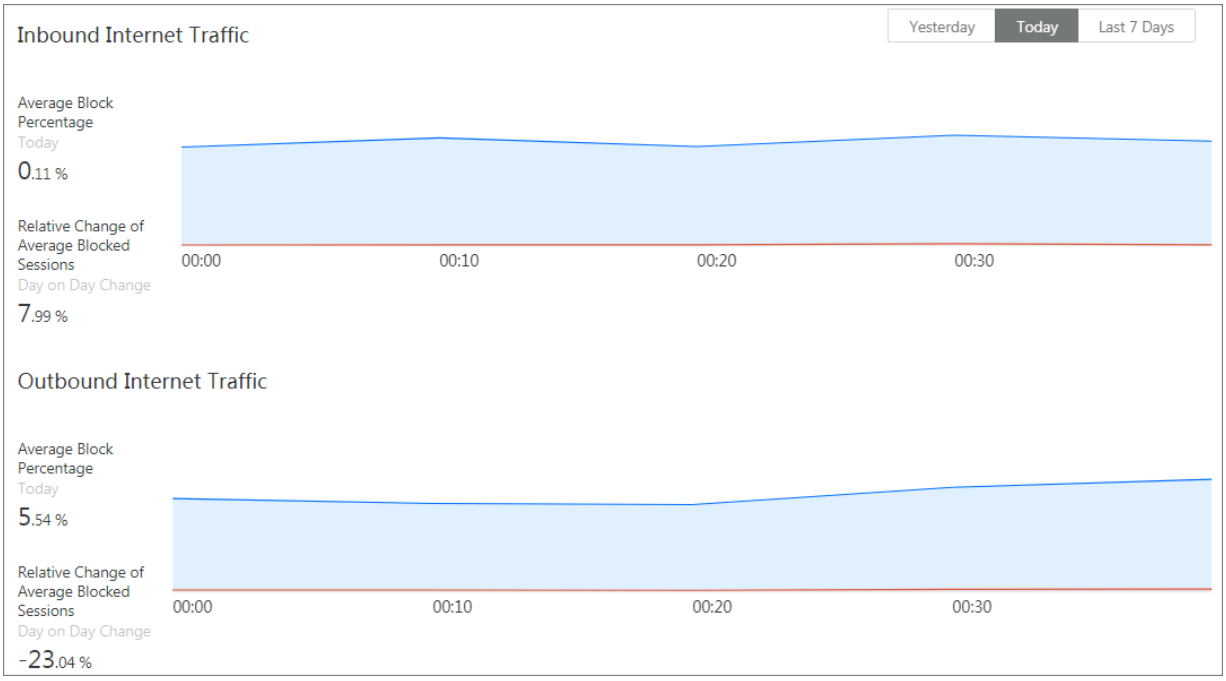
Click in this area to go to the Firewall page. On this page, you can enable or disable Cloud Firewall protection for your assets. The more assets are protected by Cloud Firewall, the higher the score of this protection item.

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

Inbound/Outbound Internet Traffic

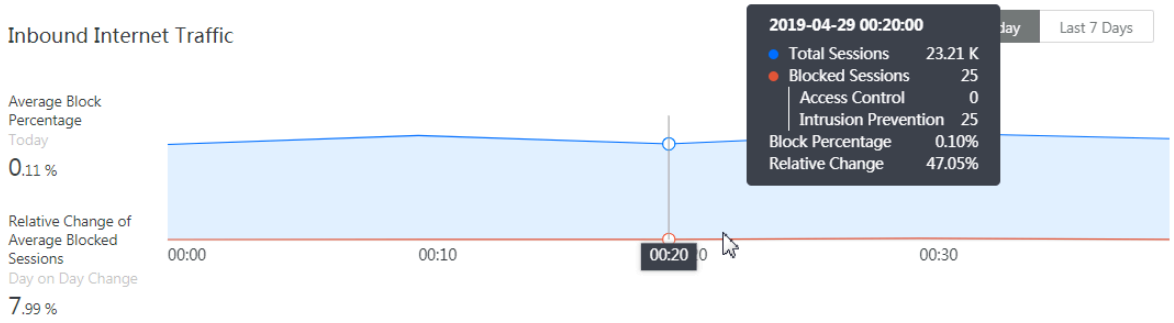
The Inbound or Outbound Internet Traffic module displays trend charts for inbound traffic from and outbound traffic after Cloud Firewall protection is enabled. You can view the trends of total sessions and intercepted sessions, and locate the time point when a session is intercepted. Then, you can check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

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



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

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



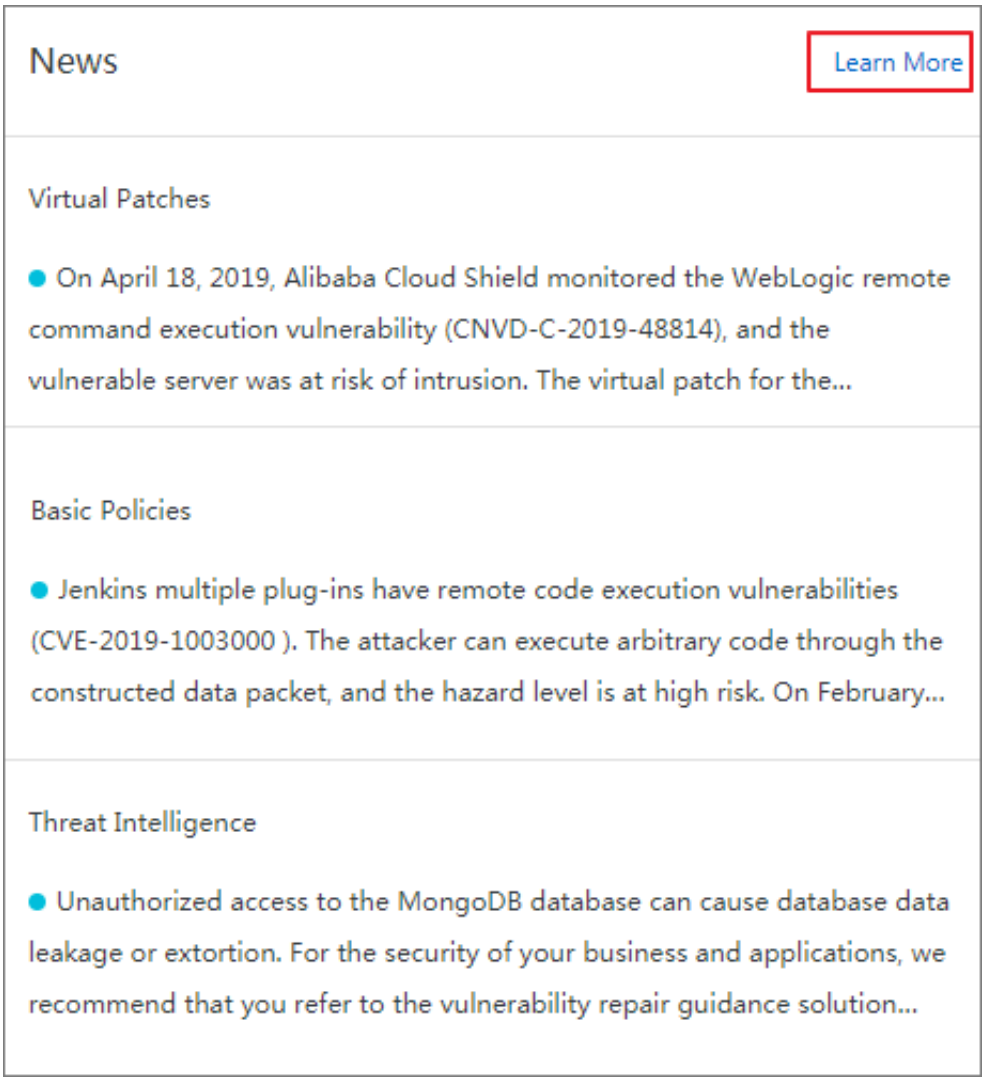
Note:

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

News

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

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



1.4 Network activities

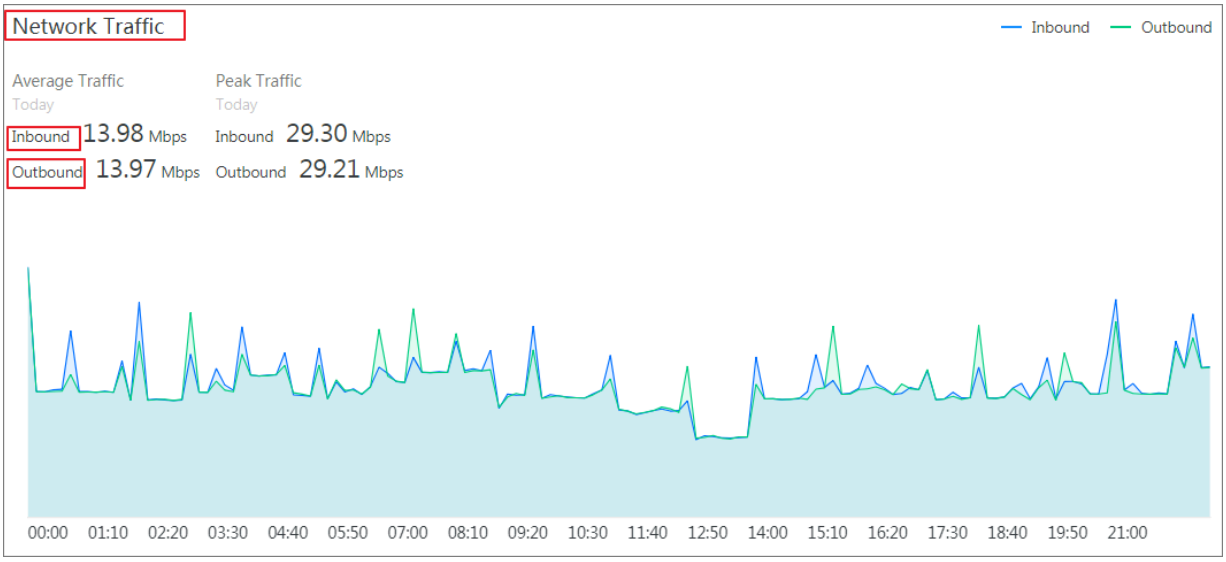
The Traffic Analysis page displays network activities of your assets in real time. With traffic analysis, you can monitor the intrusion events, networks activities, trend of the traffic and your assets' external connection activities.

Cloud Firewall monitors the following network activities in real time:

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

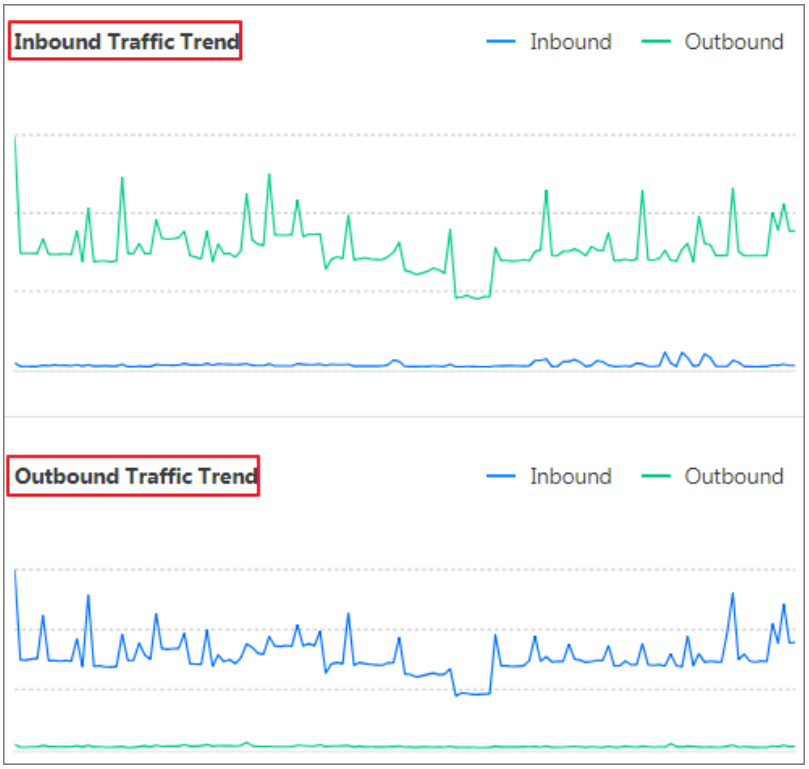
Network Traffic

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



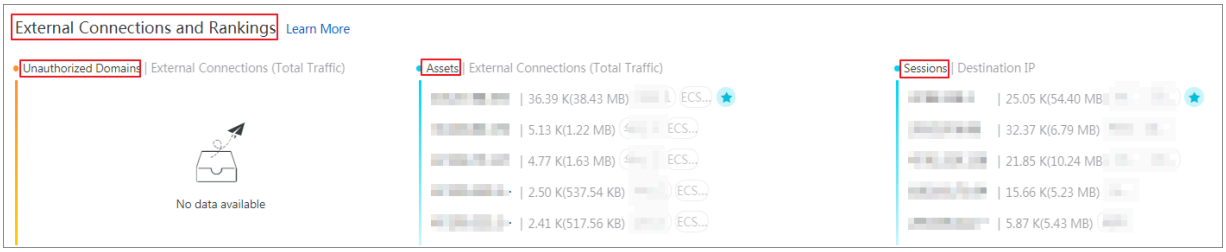
Click a certain time on the timeline of Network Traffic, you can view the specified inbound/outbound traffic.

Inbound and outbound traffic trend is displayed.



External Connections and Rankings

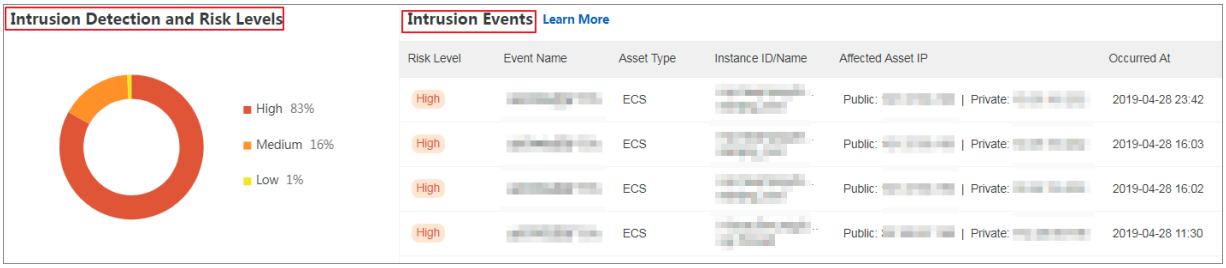
External Connections and Rankings module provides you with the top 5 unauthorized domains, assets and sessions for external connections.



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

Intrusion Detection and Risk Levels

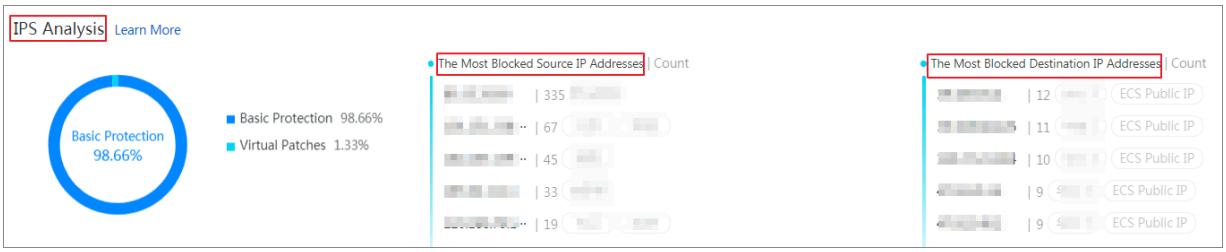
Intrusion Detection and Risk Levels module displays the proportion in percentage of the three risk levels (High, Medium, Low), and intrusion event list with the events details.



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

IPS Analysis

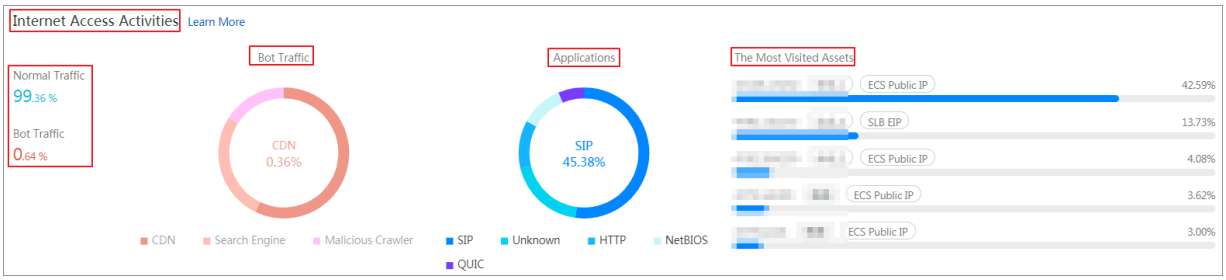
IPS Analysis module displays the traffic blocked by IPS funtions of Cloud Firewall. You can view the proportion in percentage of the traffic blocked by different IPS strategies (Basic Protection and Virtual Patches), the top 5 most blocked source IP and destination IP.



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

Internet Access Activities

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



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

VPC Access Activities

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

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

2 Network traffic analysis

2.1 Traffic analysis overview

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

Cloud Firewall monitors the following network activities in real time:

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

2.2 External connections

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

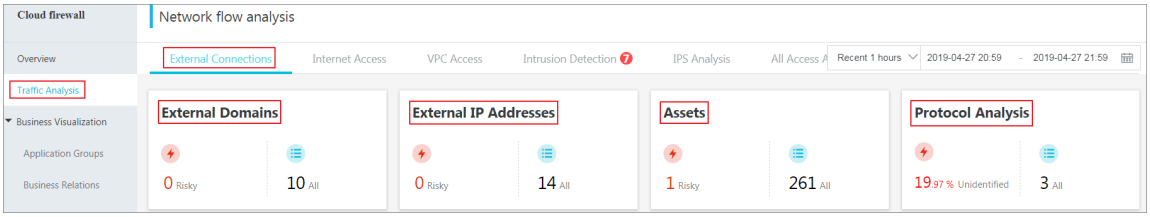
Procedure

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

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

   You can perform the follows operations on External Connections page:

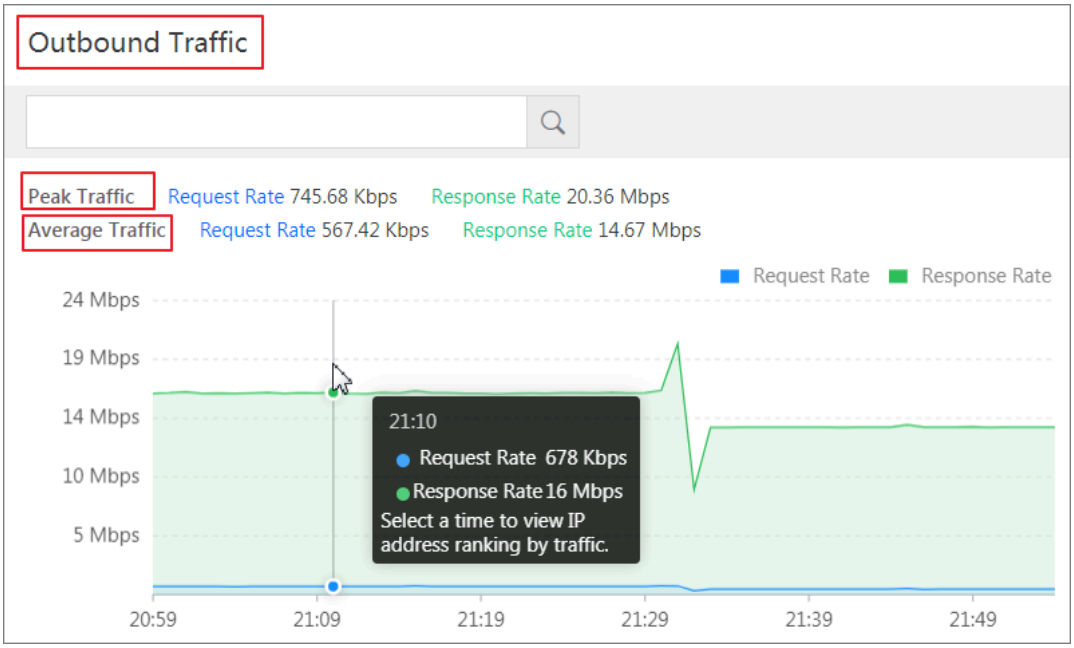
   · Monitor the overview of external connection data, including the amounts of external domains, external IP addresses, assets request for external connections and the relevant protocols.



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

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

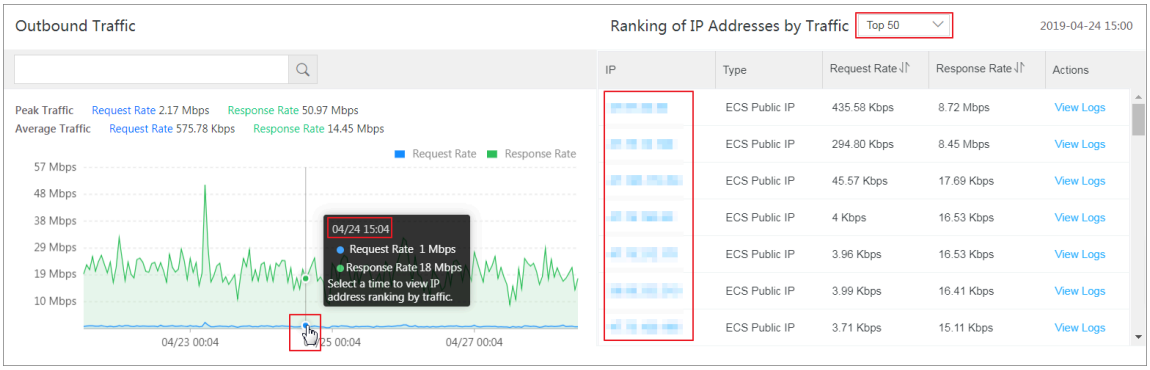
   · Monitor the outbound traffic analysis, including the average traffic and peak traffic.



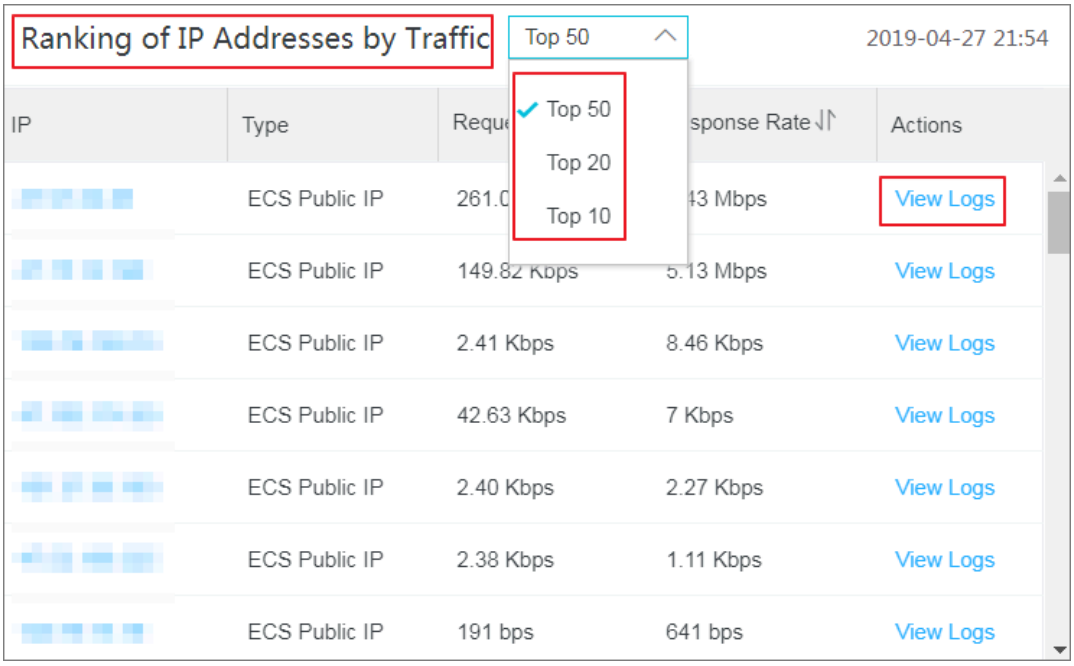
   In Outbound Traffic module, you can monitor traffic rate within the selected time range.

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

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



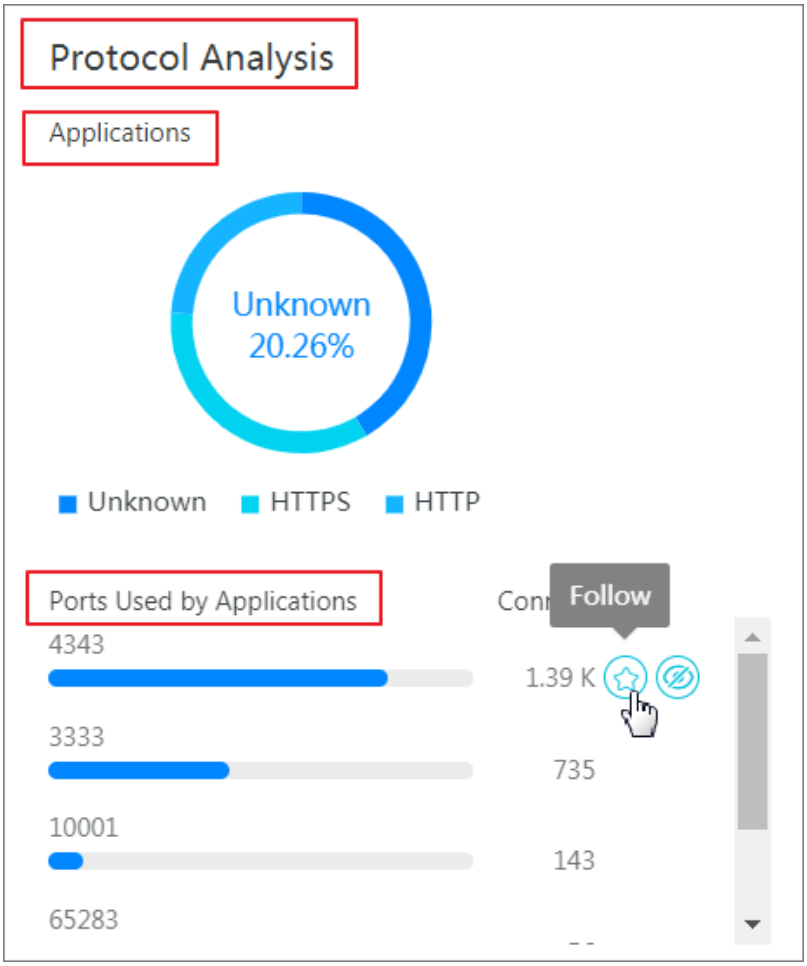
- Monitor the Top 10/20/50 traffic of external connections, with the relevant IP address, request/response rate, and logs recorded by Cloud Firewall.



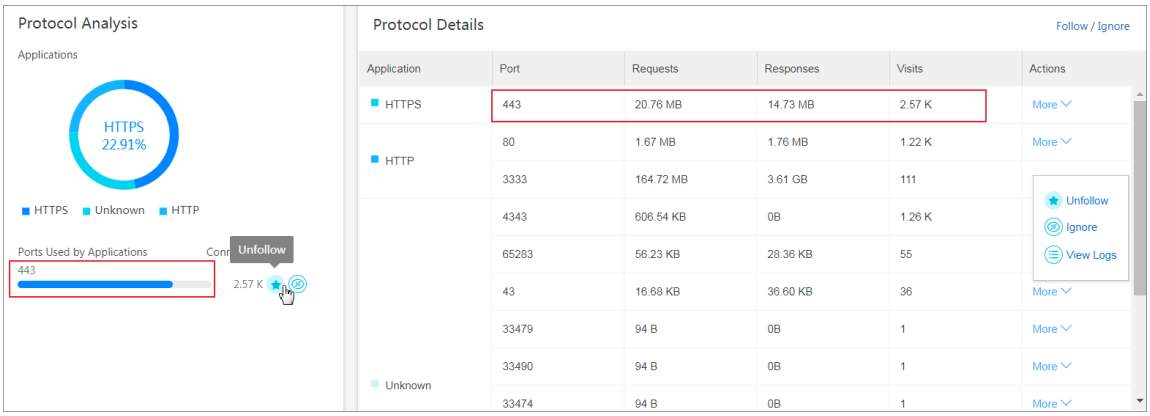
Click View Logs, Logs > Access Log is displayed, and automatically filtered with Outbound direction. You can check the details on the Outbound traffic,

including the time of access, source/destination IP and port, access application, protocol, bytes/packets of the access traffic, and applied access control policy.

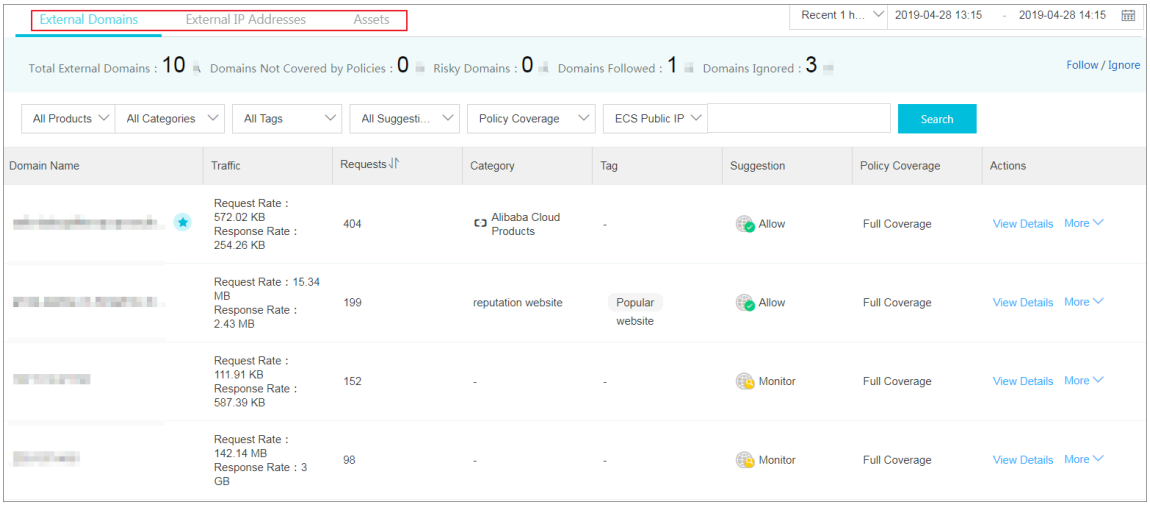
- Monitor the protocol analysis for external connections, including the information on applications, ports and corresponding connection numbers.



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

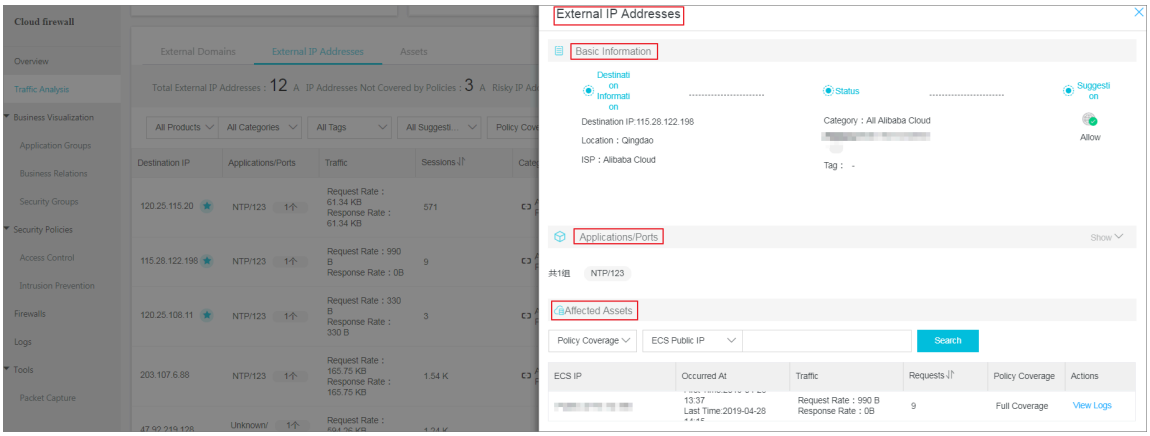


- View the protocol details, and Follow/Ignore or View the Logs of the specified protocols.
- Monitor the detailed outbound traffic list, including external domains, IP addresses and assets.



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

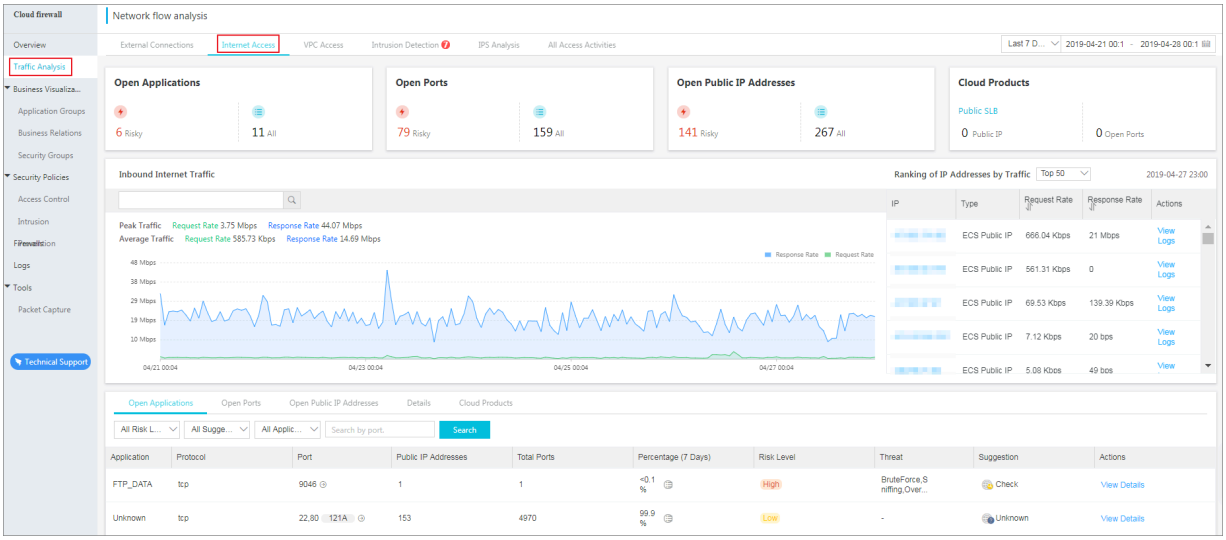
Click View Details to open the details page of external domain/IPs.



2.3 Internet access

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

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



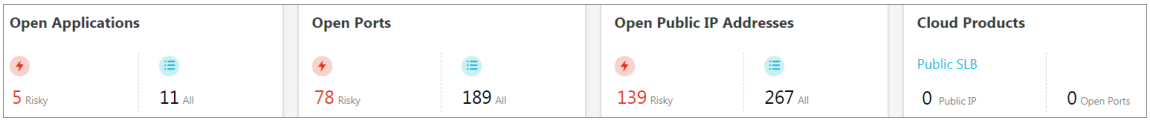
Procedure

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

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

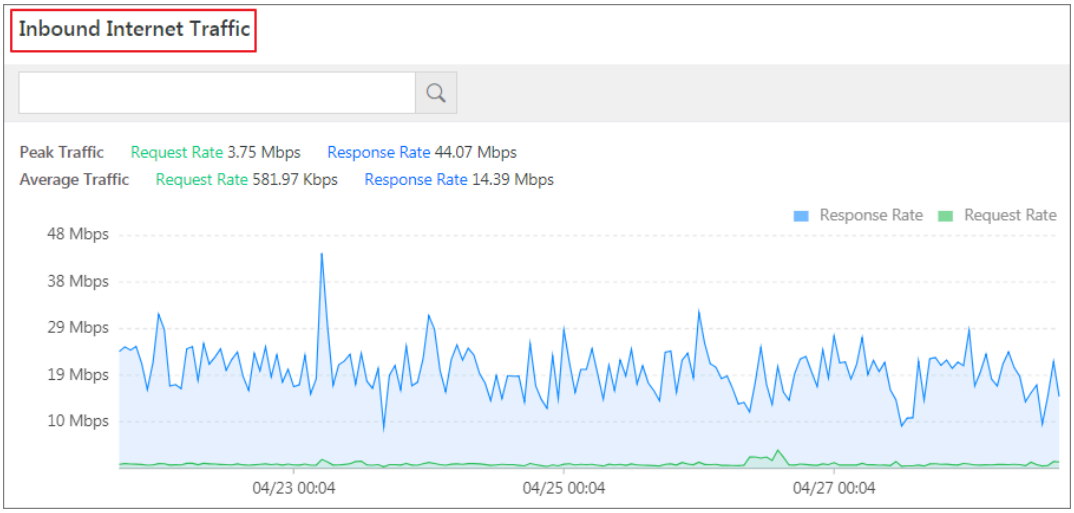
   You can perform the follows operations on Internet Access page:

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



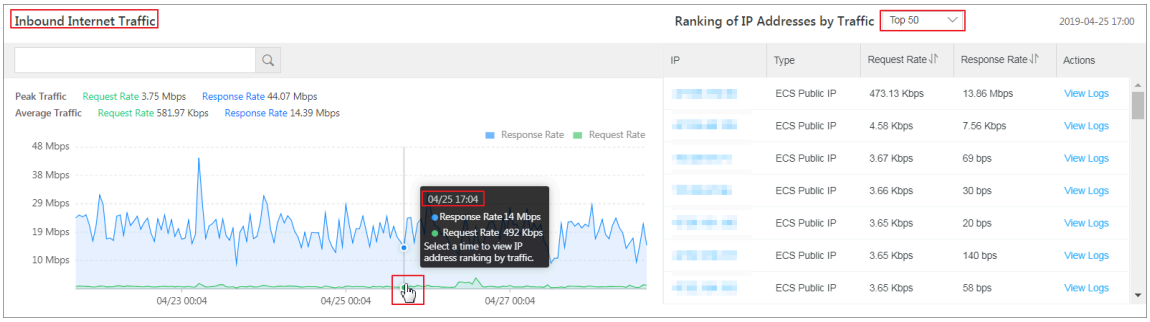
     In the overview area of internet access, risky event number and total number of each item are displayed. Click the Risky or All button to go to the detailed internet access list.

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

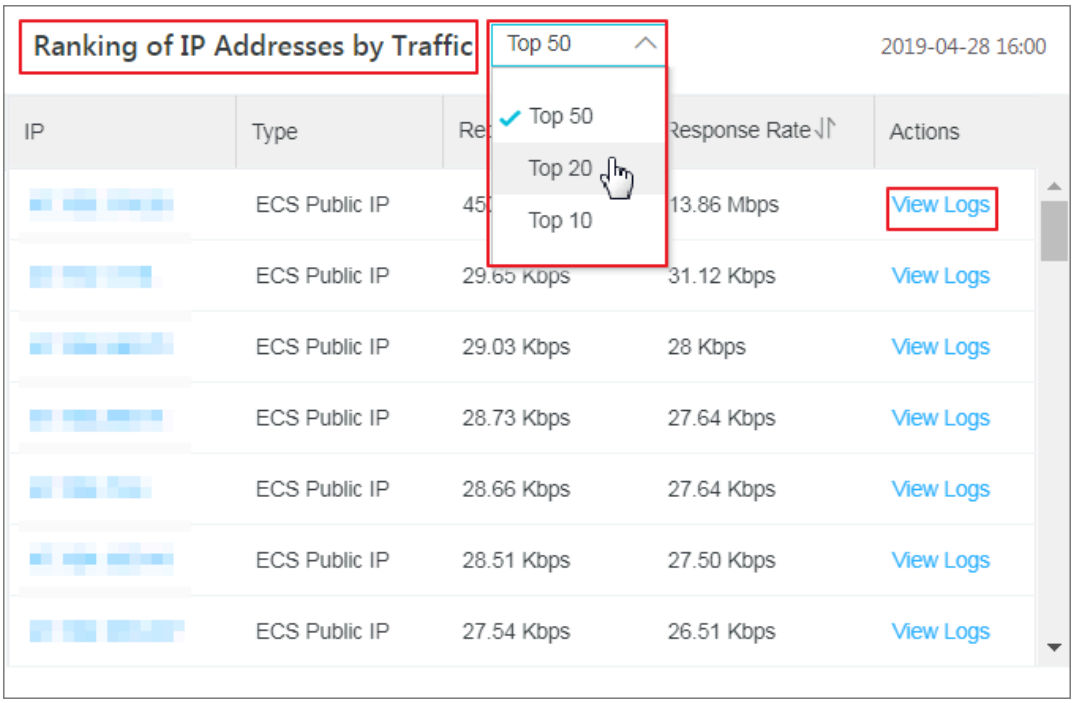


     In Inbound Internet Traffic module, you can monitor traffic rate within the selected time range.

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



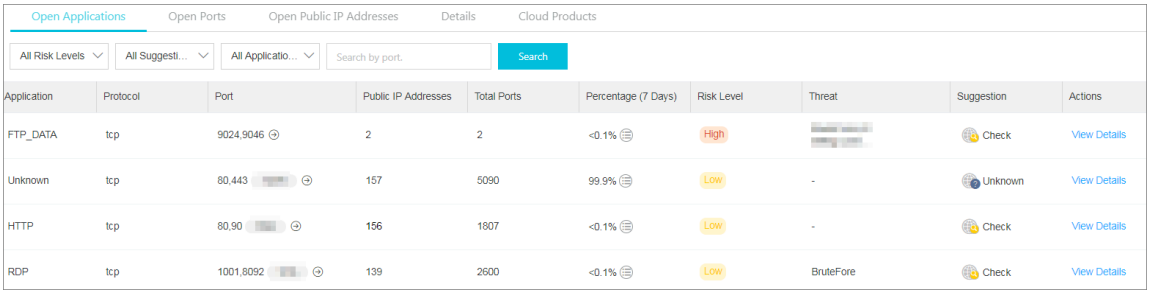
- **Monitor the Top 10/20/50 internet access traffic with the relevant IP address, request/response rate, and logs recorded by Cloud Firewall.**



Click View Logs, Access Log in Logsis displayed, and automatically filtered with Inbound direction. You can check the details on the inbound traffic, including

the time of access, source/destination IP and port, access application, protocol, bytes/packets of the access traffic, and applied access control policy.

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



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

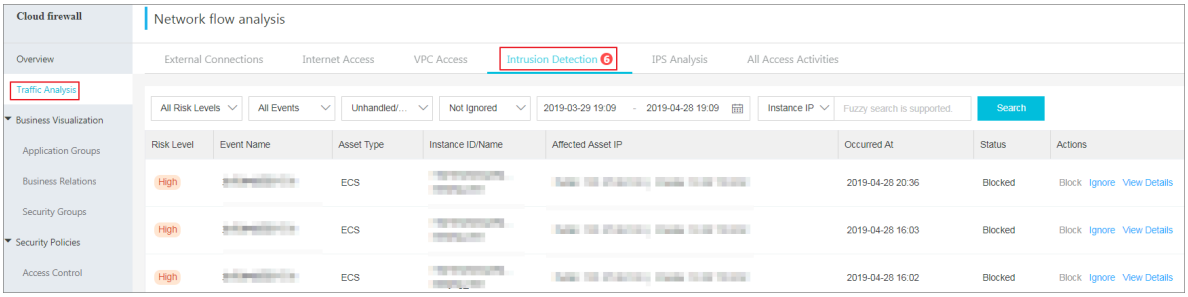
2.4 Intrusion detection

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

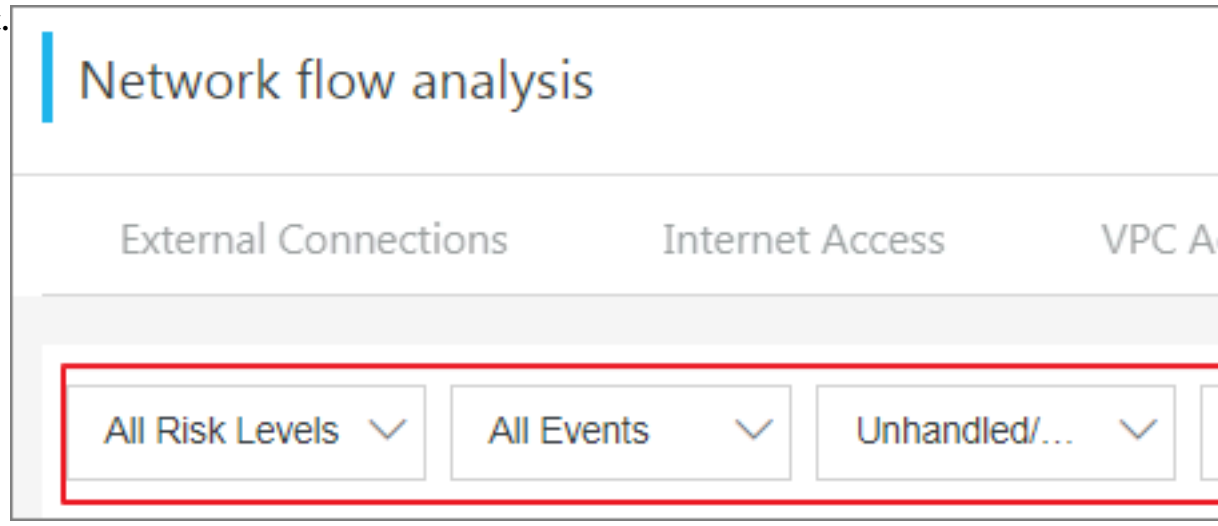
Procedure

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

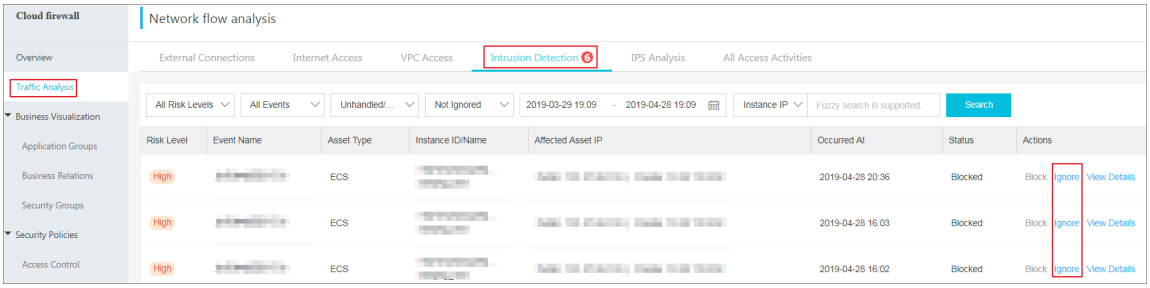
3. Click Intrusion Detection and view the intrusion event list.



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



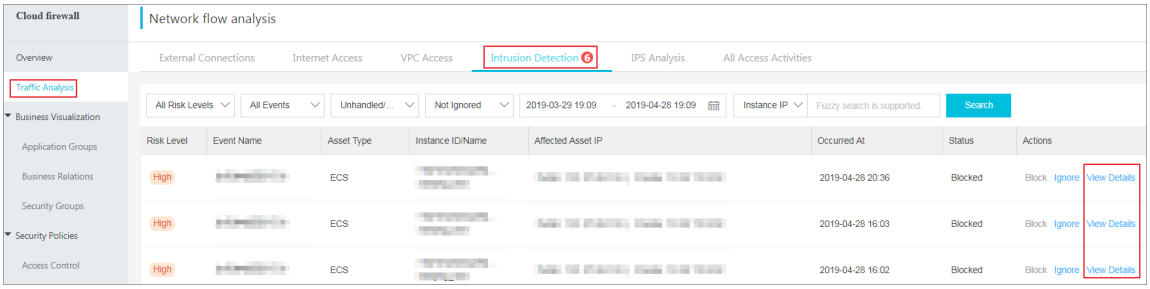
- If you determine that an intrusion event is a normal activity, click Ignore in the Action column to ignore the event.



Note:

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

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

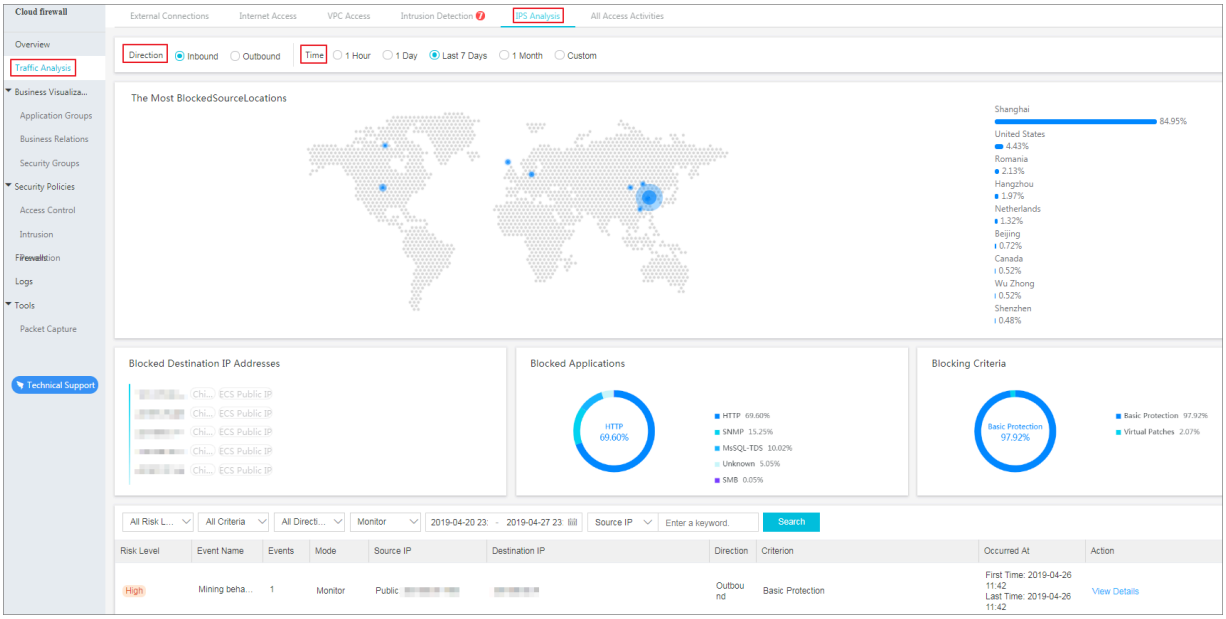


Click Block to enable the Threat Engine of IPS.

2.5 IPS analysis

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

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

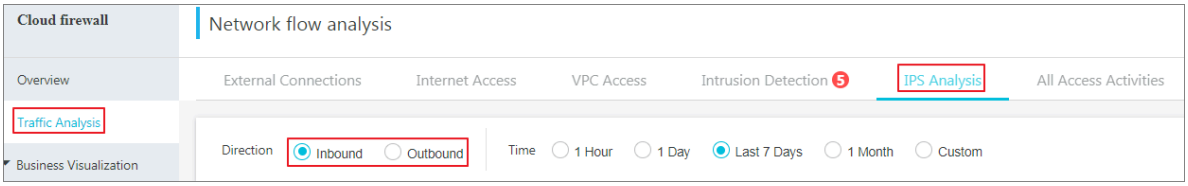


Note:

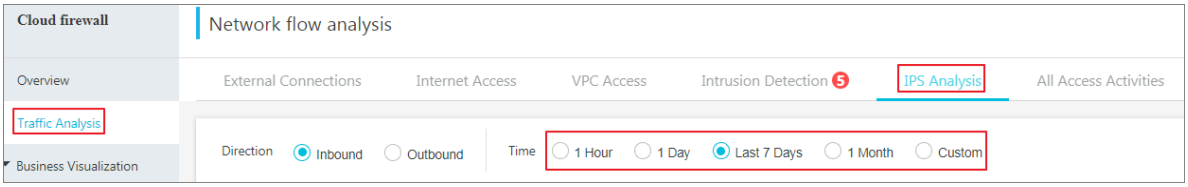
The blocked traffic in IPS Analysis is blocked by the IPS treat engines. Mare sure you've selected Traffic Control Mode and enabled the Basic Protections and the Patches in Intrusion Prevention page.

Procedure

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

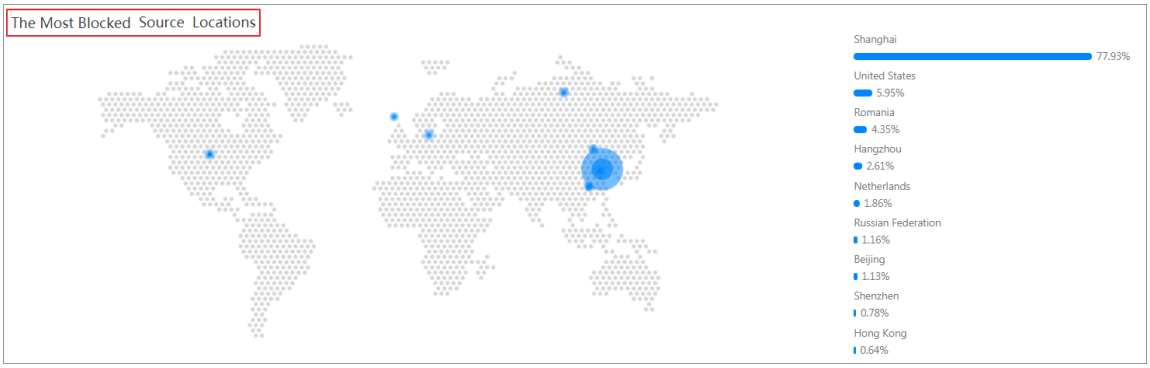


4. Select Time by one hour, one day, last seven days, one month, or a custom time range to display the required blocking traffic.

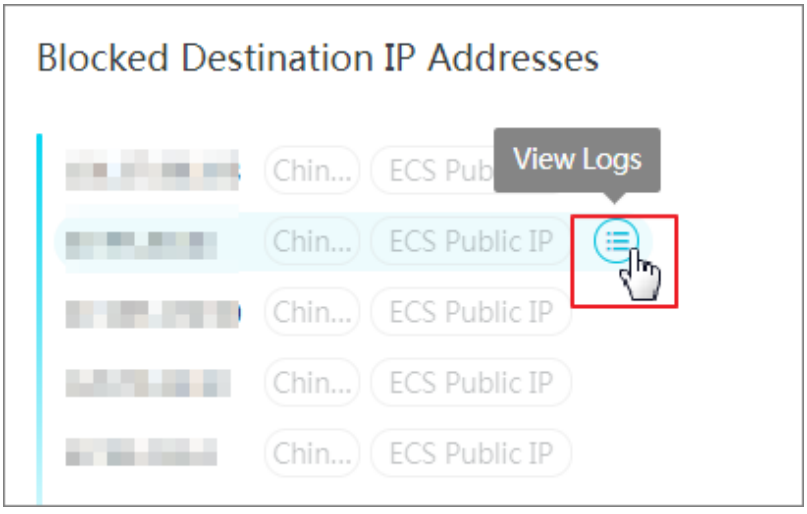


You could monitor the following information on the blocked traffic:

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

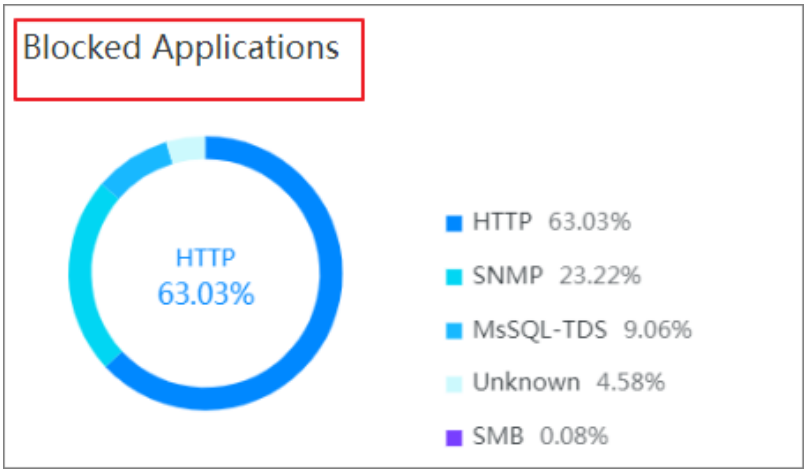


- Blocked destination IP addresses with IP type and location.

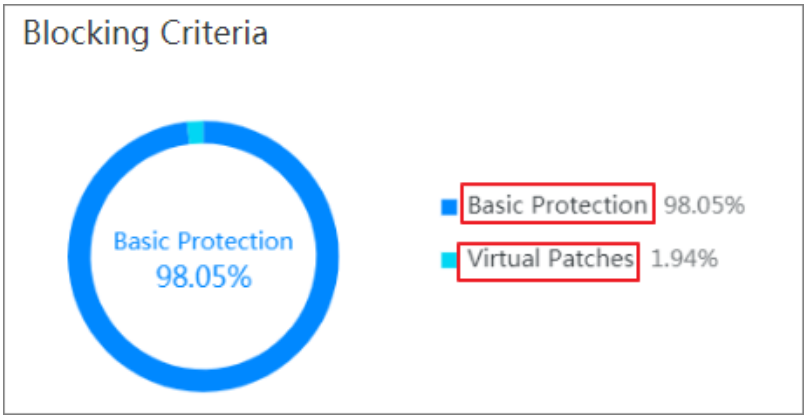


If you want to view the details of a certain blocked destination IP, click View Logs to open the Access Log.

- Blocked application with its proportion in percentage.

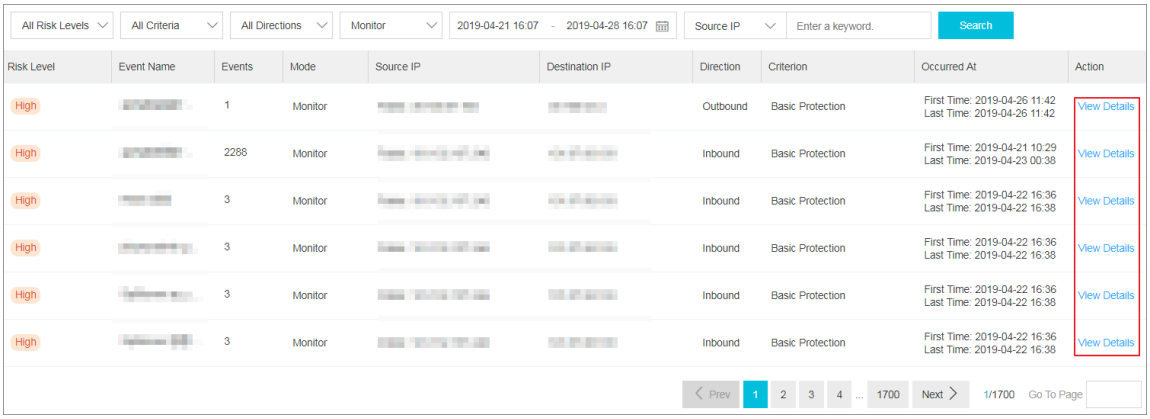


- IPS threat engines that block the traffic.

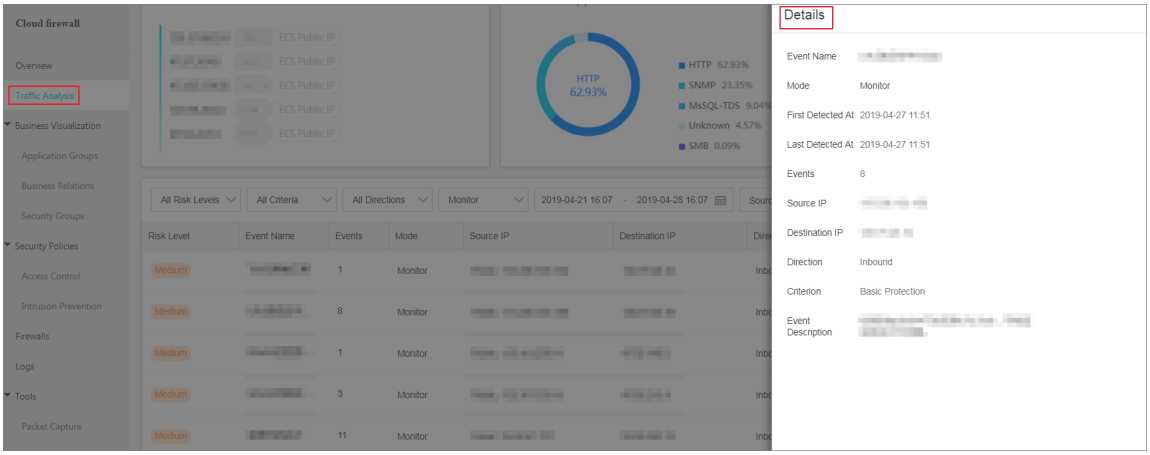


- Blocked event list with the events details.

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



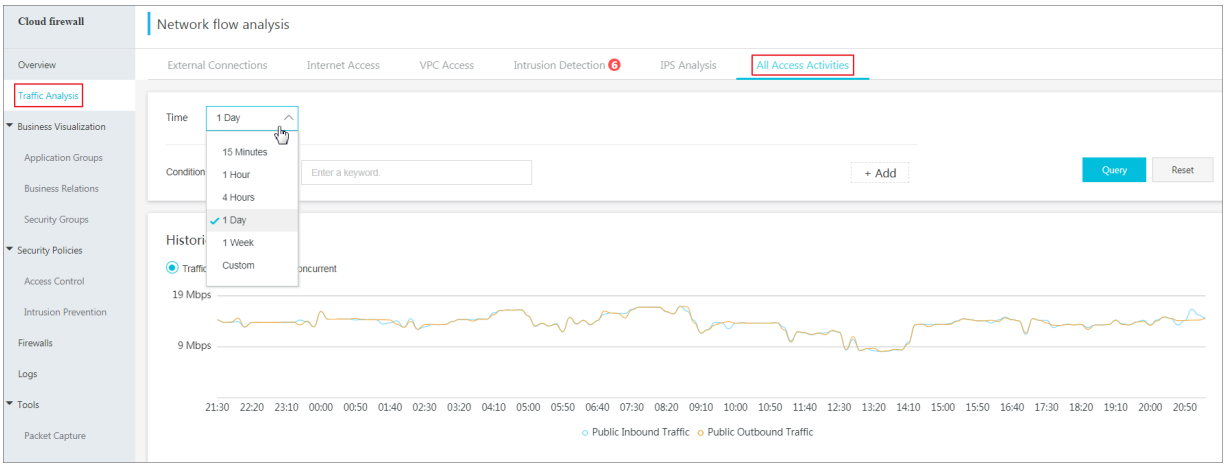
  Click View Details to open the detailed page of the specified blocked event. You can view the event description on the Details page.



2.6 All access activities

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

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



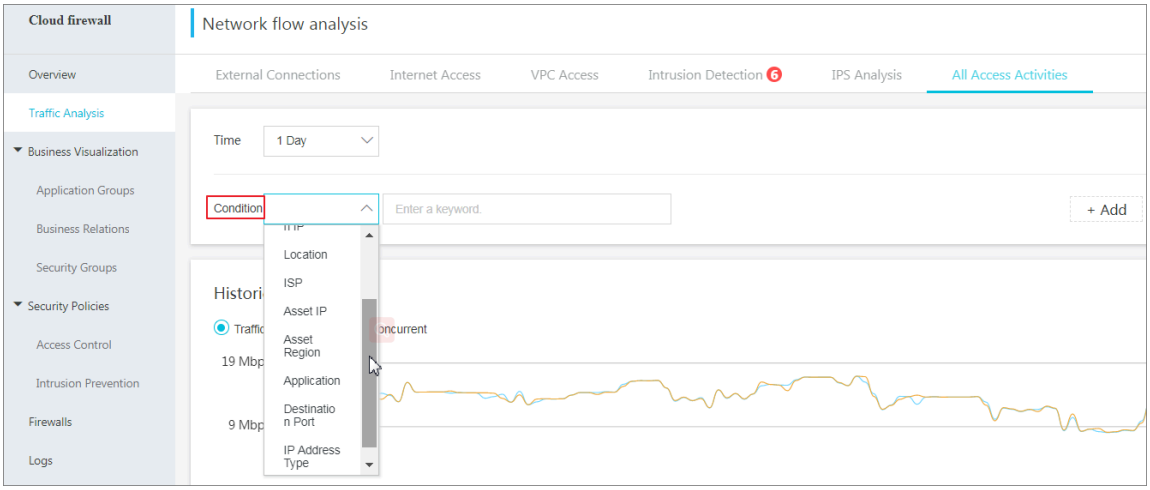
Procedure

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

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

> **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 Query to filter the historical traffic trends based on the condition. To clear the search condition, click Reset.



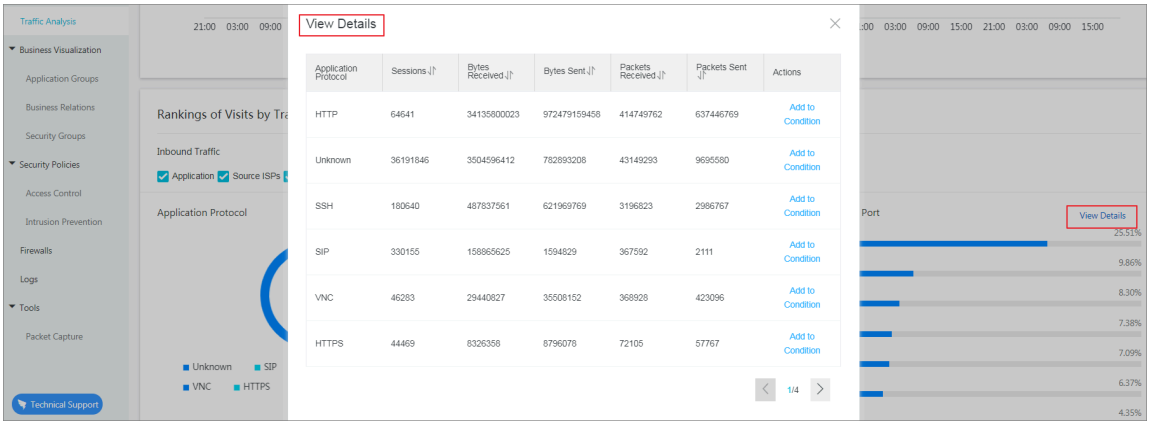
- In the Historical Trends area, you can view trend charts about the inbound and outbound traffic, the number of new connections, and the number of concurrent connections.

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

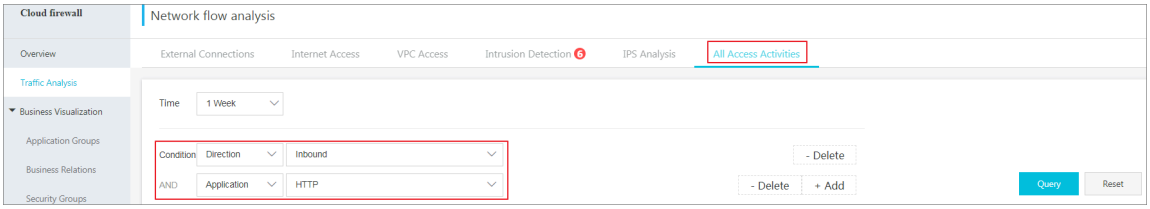
> **Note:**

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

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



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

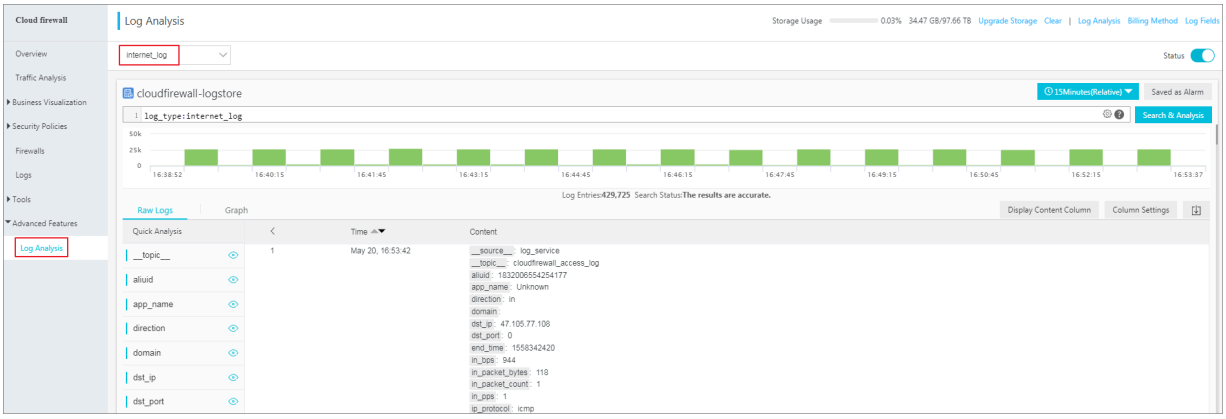


3 Log analysis

3.1 Overview

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

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



Benefits

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

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

Prerequisites

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

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

Restrictions

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

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

   Note:
  Other general logstore features (such as query, statistics, alarms, and stream consumption) are supported, and there is no difference with the general logstore.
- Alibaba Cloud's Log Service (SLS) does not charge for the exclusive logstore of Cloud Firewall, but SLS itself must be available (not overdue).
- Built-in reports provided by Log Analysis of Cloud Firewall may be updated and upgraded automatically.

Scenarios

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

3.2 Log analysis billing method

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

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

Log storage specification

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

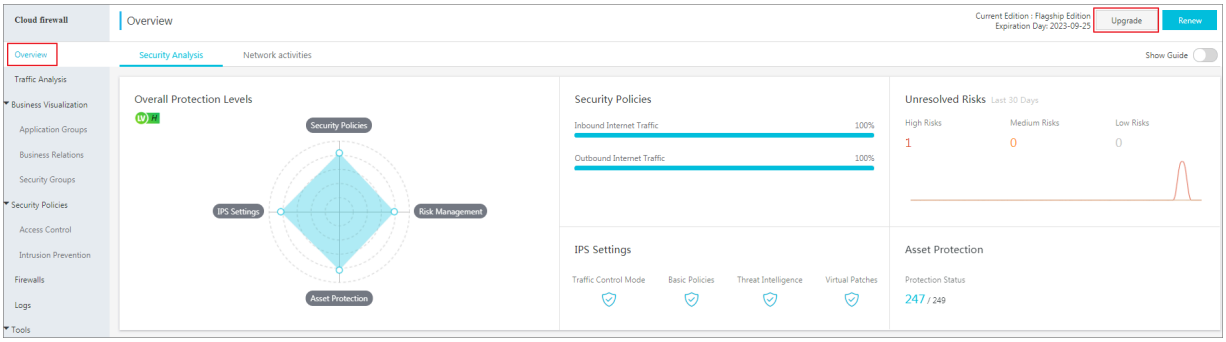
Log storage duration	Log storage size	Applicable bandwidth	Recommend version	Monthly subscription fee	Annual subscription fee
180 days	1TB	Applicable to business scenarios with monthly bandwidth not higher than 10 Mbps	Pro Edition	To be released.	To be released.
	5TB	Applicable to business scenarios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

Note:

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

Upgrade storage capacity

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



Notice:

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

Duration

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

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

Service expiration

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

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

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

3.3 Enable the log analysis service

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

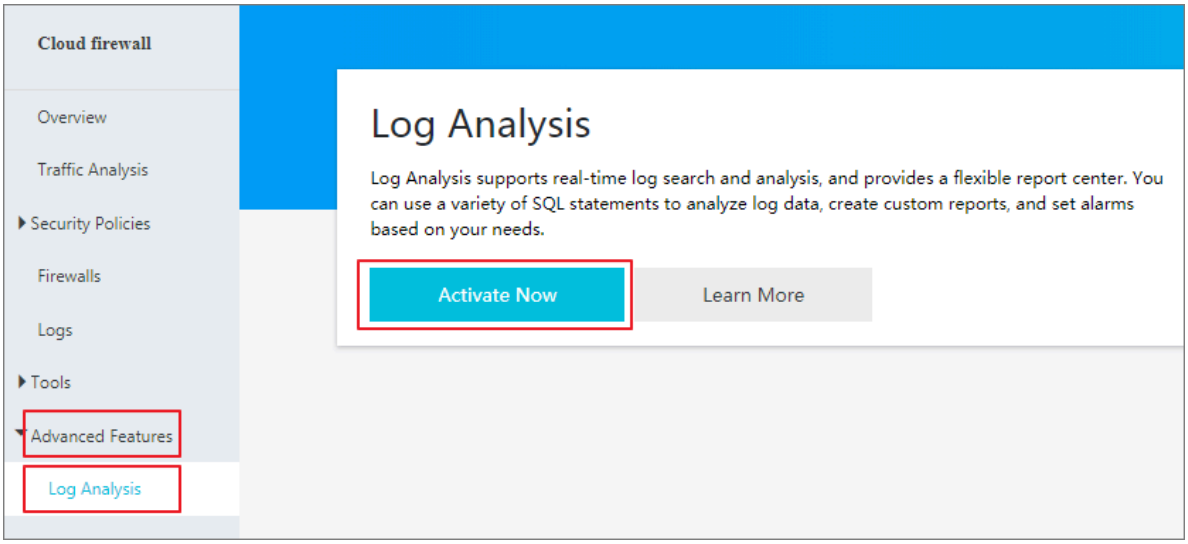
Features

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

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

Enable the Log Analysis service of Cloud Firewall

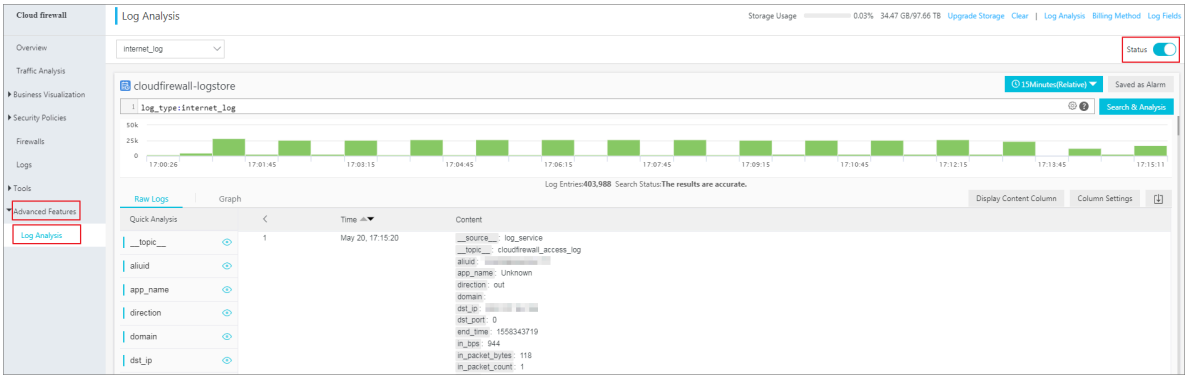
1. Log on to the *Cloud Firewall console*.
2. In the left-side navigation pane, select Advanced Features > Log Analysis.
3. Click Activate Now on the Log Analysis page.



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

> Note:
> For more information about log analysis pricing, refer to *Log analysis billing method*.

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



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

3.4 Collect the log

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

Prerequisites

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

Context

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

After you enable the Cloud Firewall log analysis function, the log analysis function automatically creates a dedicated Logstore named cloudfirewall-logstore under your account. Cloud Firewall automatically imports log entries to this dedicated Logstore

in real time. For more information about the default configuration of the dedicated Logstore, see *Default configuration*.

Procedure

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

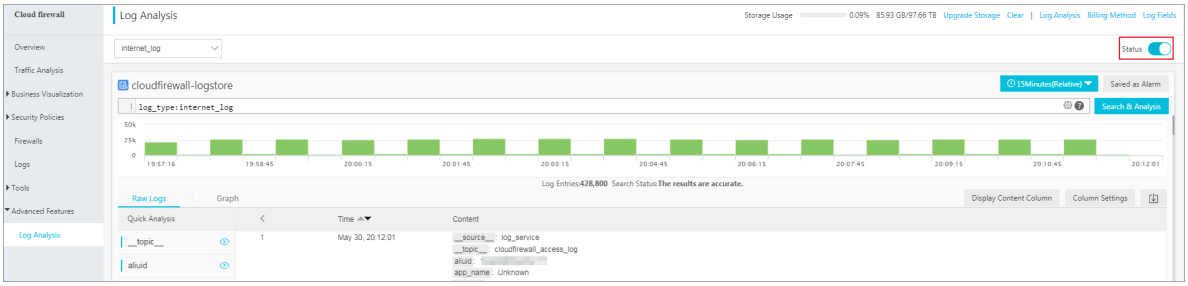


Table 3-1: Default log analysis configuration

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

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

Note:
The default log analysis configuration items cannot be modified.

Restrictions and guidelines

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

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

  Note:
  The dedicated Logstore has no restrictions in search, statistics, alerts, streaming consumption, and other functions.
- Basic configurations, such as the log storage period, cannot be modified.
- The dedicated Logstore is not billed.

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

  Note:

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

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

3.5 Fields in the log entry

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

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

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

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

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

3.6 Export log entries

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

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

Procedure

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

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

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

   - Download logs in current page:

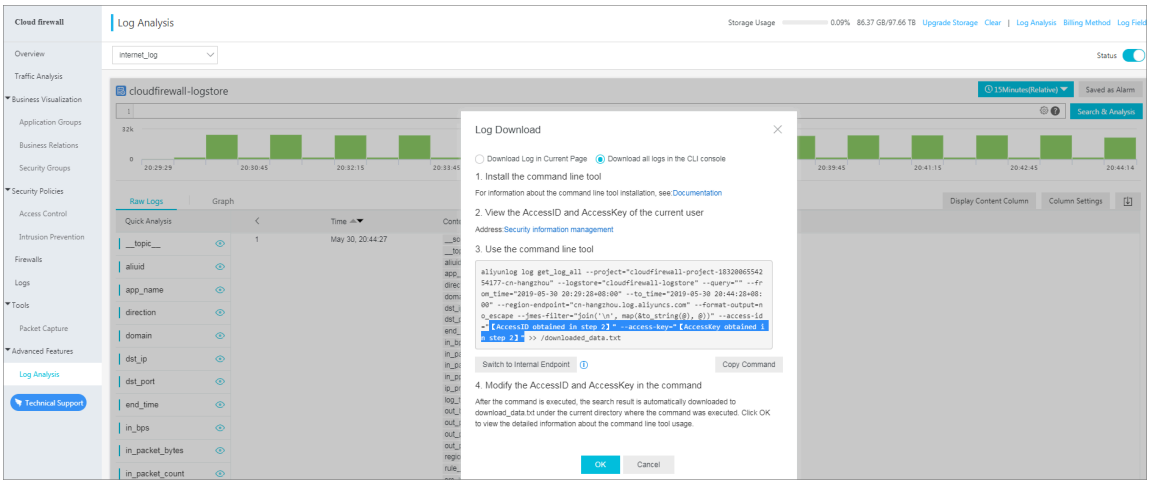
     Click OK to export the raw log entries on the current page to a CSV file.

   - Download all logs by CLI:

     a. For more information about installing the CLI, see *CLI guide*.

     b. Click *Security Information Management Link* to view and record the AccessKey ID and AccessKey Secret of the current user.

     c. Click Copy Command and paste the command into CLI, replace the `AccessID obtained in step 2` and `AccessKey Secret obtained in step 2` with the AccessKey ID and AccessKey Secret of the current user, and run the command.



After you run the command, all raw log entries created by Cloud Firewall are automatically exported and saved to the file `download_data.txt`.

3.7 Authorize RAM user accounts with Log Analysis function

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

Context

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

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

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

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

Procedure

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

Note:

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

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

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

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

3.8 Manage log storage

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

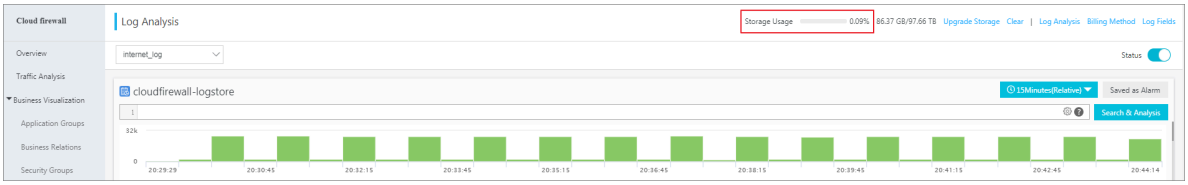
Chethe log storage

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

 **Note:**

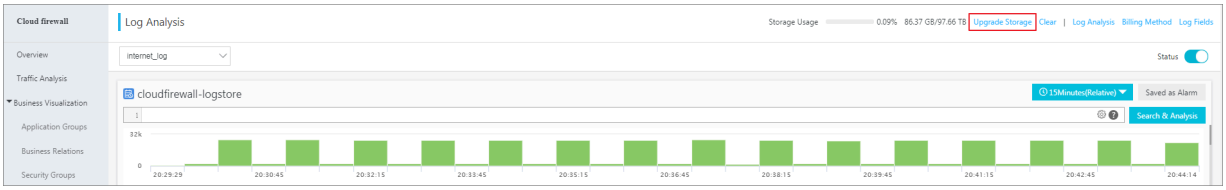
The log storage information in the console is not updated in real time. It takes up to two hours to update the actual storage information to the console. We recommend that you expand the log storage space before it is exhausted.

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



Expand log storage

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

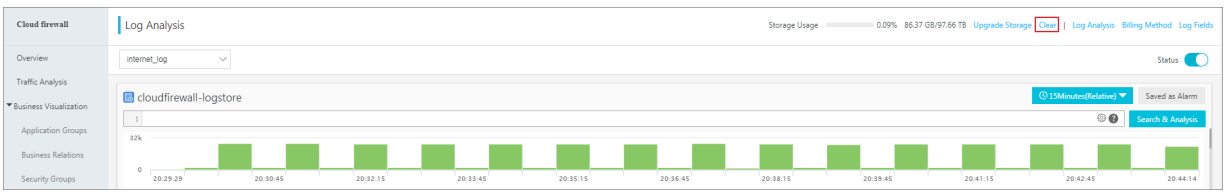


Note:
We recommend that you expand the log storage space before it is exhausted. If no storage space is available, then the new log data cannot be written into the dedicated Logstore.

Clear log storage

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

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



 **Notice:**

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

 **Note:**

You only have limited times for clearing the log storage.