ALIBABA CLOUD

Alibaba Cloud

Cloud Firewall

Quick Start

Document Version: 20200925

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

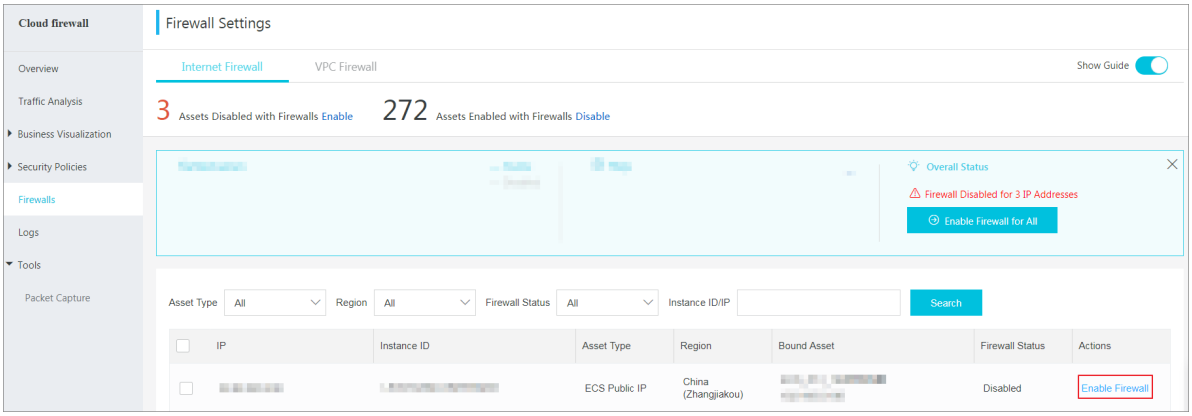
1.Tutorial overview ---- 05
2.Activate Cloud Firewall ---- 07
3.Enable Intrusion Prevention ---- 09
4.View network flow analysis ---- 10
5.Configure access control policies ---- 16

1.Tutorial overview

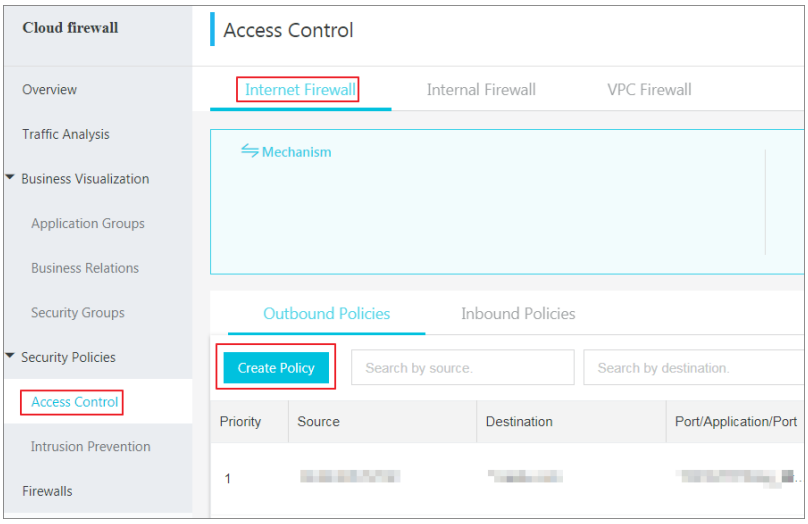
This document introduces how to quickly complete basic operations in the Cloud Firewall console.

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

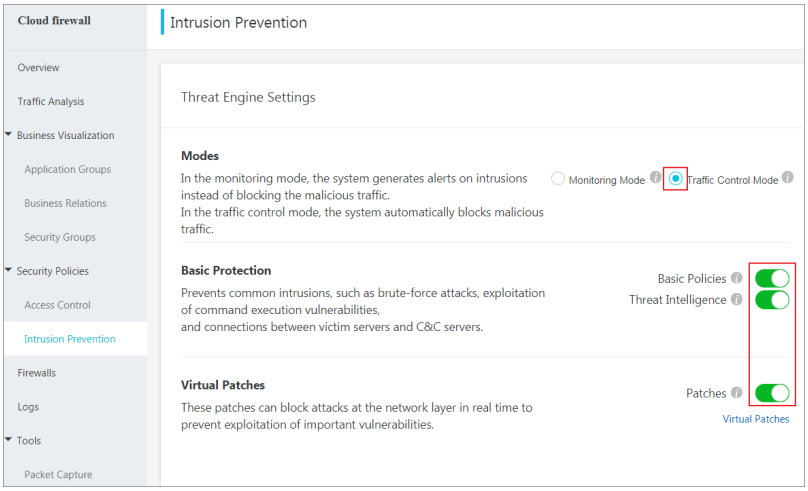
- Enable the Cloud Firewall service on the Firewalls page.



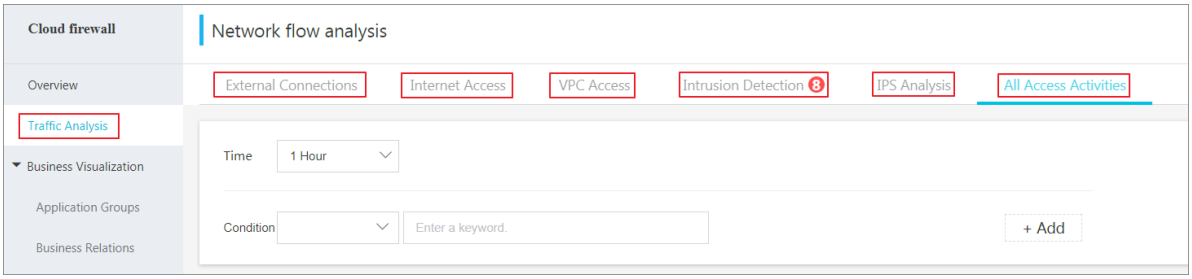
- Click Add Policy in the upper-right corner of the Access Control page to Configure access control policies.



- Configure intrusion prevention policies on the Intrusion Prevention page.



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



2.Activate Cloud Firewall

After you purchase Cloud Firewall, it does not automatically start protection. You can activate or deactivate this service on the **Firewall Settings** page. After you activate this service, you can use it without the need to perform complex configurations.

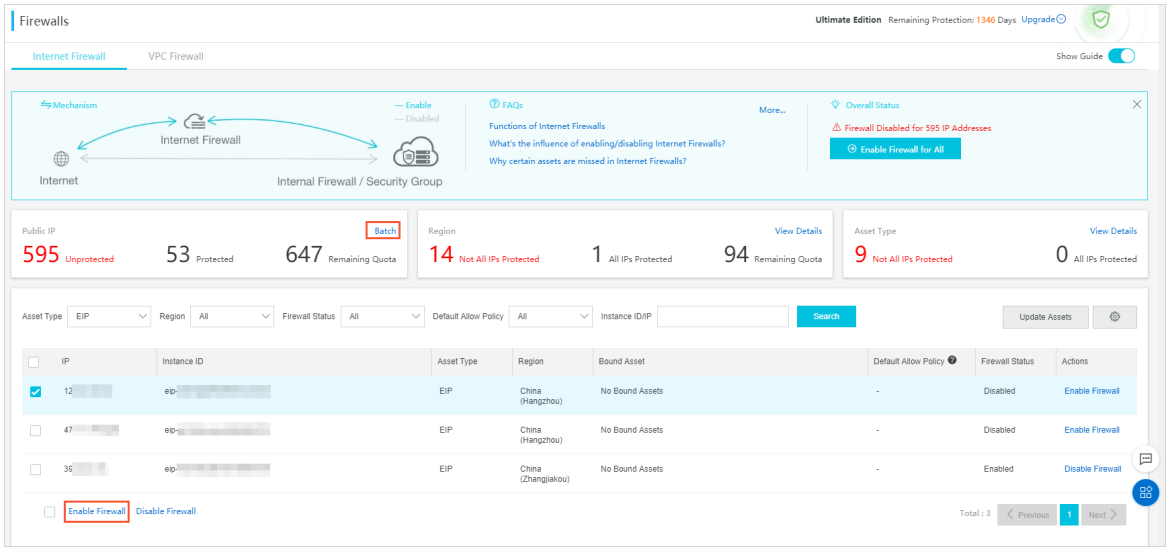
Limits

Cloud Firewall Enterprise Edition and Ultimate Edition support VPC firewalls. The free trial edition and Premium Edition do not support VPC firewalls. For more information, see Editions and regions.

For the items that you must pay attention to when you enable VPC firewalls, see VPC firewall limits.

Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, click **Firewall Settings**.
3. On the **Firewall Settings** page, activate Cloud Firewall.



> **Note** Only Cloud Firewall Enterprise Edition and Ultimate Edition support VPC firewalls. If you are using the free trial edition or Premium Edition, the **VPC Firewall** tab does not appear on the **Firewall Settings** page.

You can enable the **Internet firewall** or **VPC firewalls**.

- To enable the **Internet firewall**, perform the following steps:
  a. On the **Firewall Settings** page, click the **Internet Firewall** tab.
  b. On the **Internet Firewall** tab, perform the following operations:
     - Click **Batch**. In the dialog box that appears, select Enable Protection and click **Enable** to enable the Internet firewall for all assets.
     - Select the assets for which you want to enable the Internet firewall and click **Enable Firewall** in the lower-left corner.

- To enable **VPC firewalls**, perform the following steps:
  a. On the **Firewall Settings** page, click the **VPC Firewall** tab.
  b. On the **VPC Firewall** tab, find the asset for which you want to enable VPC firewalls and turn on the switch in the **Firewall Settings** column.

You can view the firewall status of assets by specifying **Asset Type**, **Region**, and **Firewall Status**.

3.Enable Intrusion Prevention

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

Procedure

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

   > Note After you subscribe to the Cloud Firewall service, **Monitoring Mode** is enabled for IPS by default.

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

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

4.View network flow analysis

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

External Connections

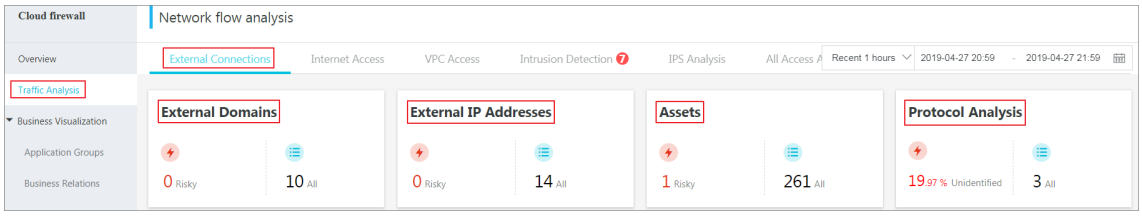
The **External Connections** page displays the details on your assets' external connections, including the connected domain names, external IP addresses, the applied protocols and your assets' info. This helps you identify the suspicious assets activities in a timely manner.

Procedure

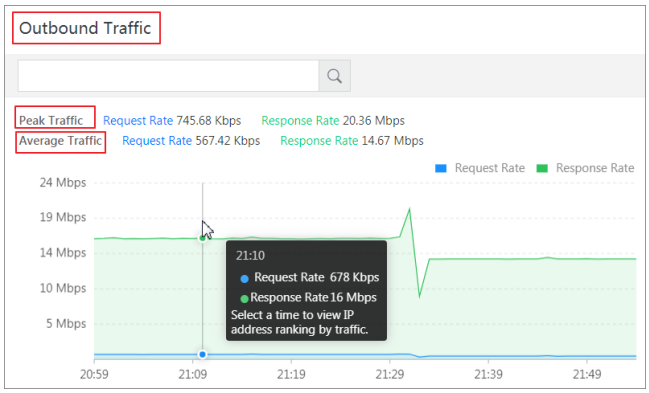
1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, go to **Network Flow Analysis > External Connections** to check your assets' external connection activities.

   You can perform the follows operations on **External Connections** page:

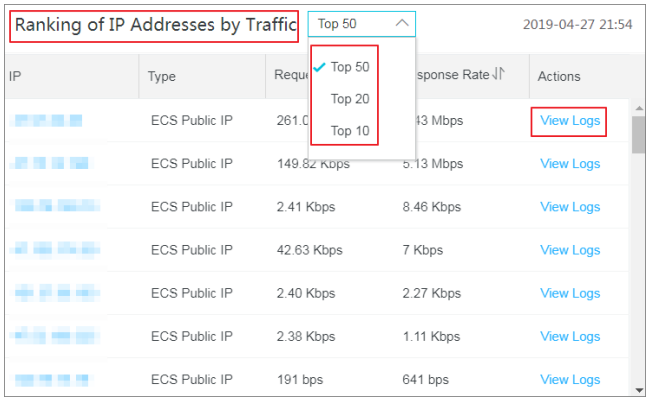
   - Monitor the summaries on external connection data, including the amounts of external domains, external IP addresses, assets request for external connections and the relevant protocols.



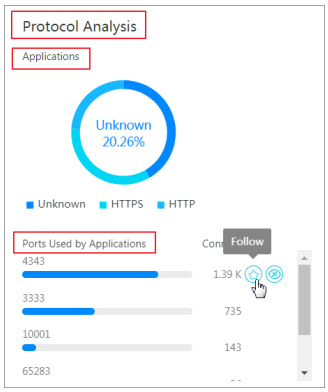
   - Monitor the outbound traffic analysis, including the average traffic and peak traffic.



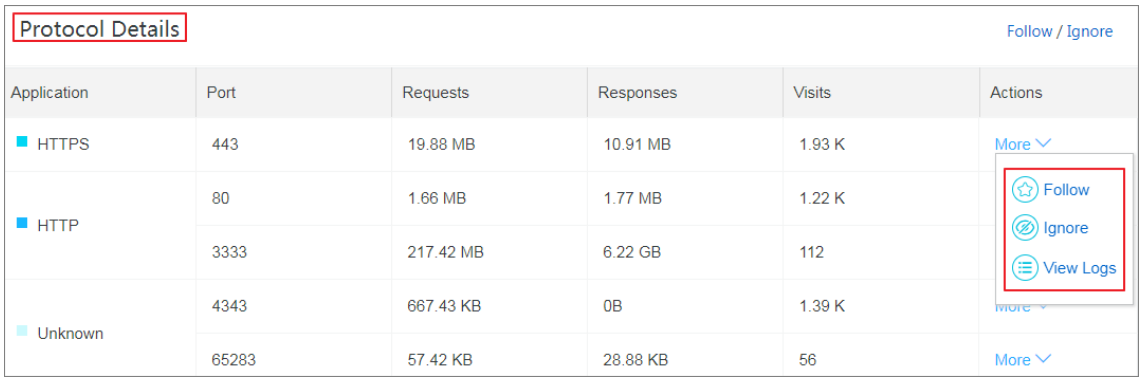
   - Monitor the Top 10/20/50 traffic of external connections, with the relevant IP address, request/response rate, and logs recorded by Cloud Firewall.



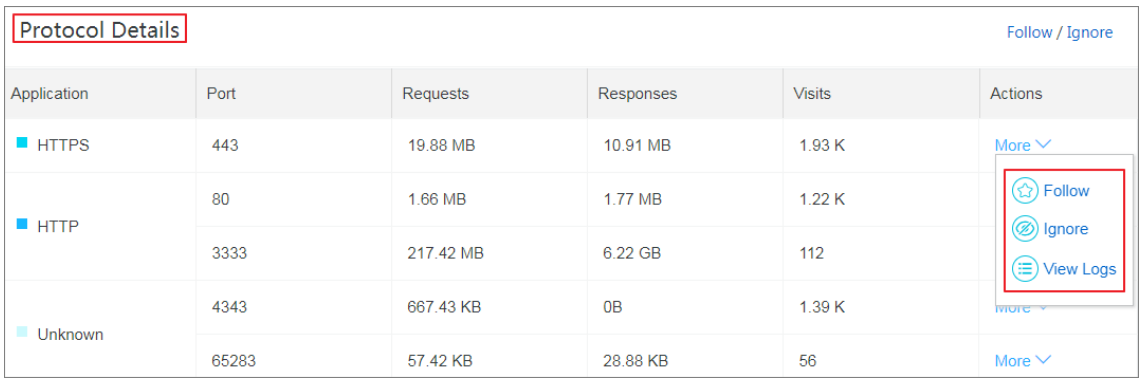
- Monitor the protocol analysis for external connections, including the information on applications, ports and corresponding connection numbers.



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

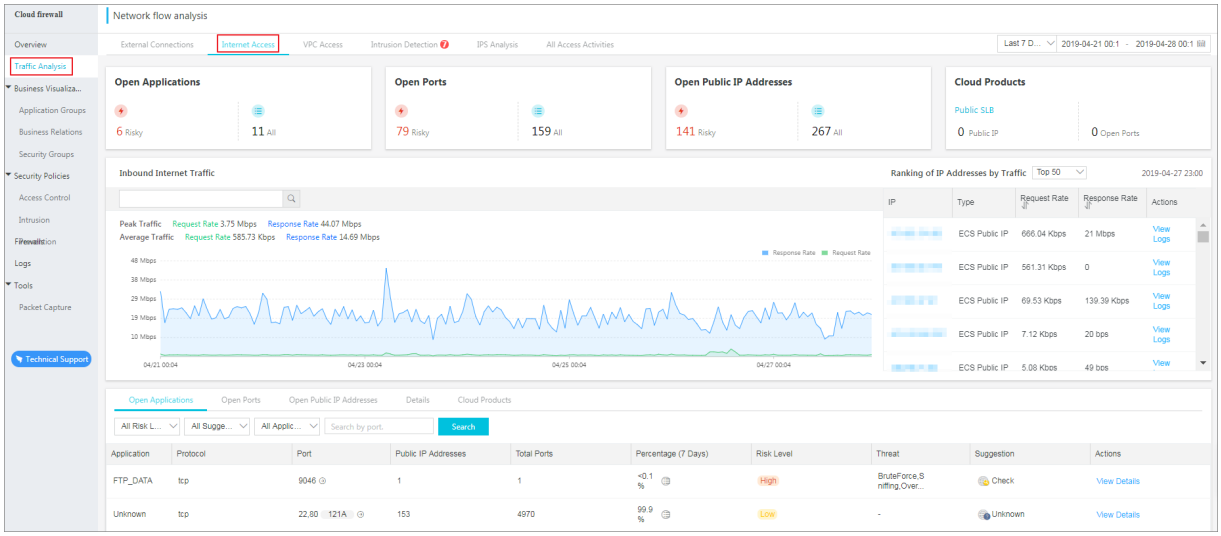


- View the protocol details, and follow or ignore the specified protocols.



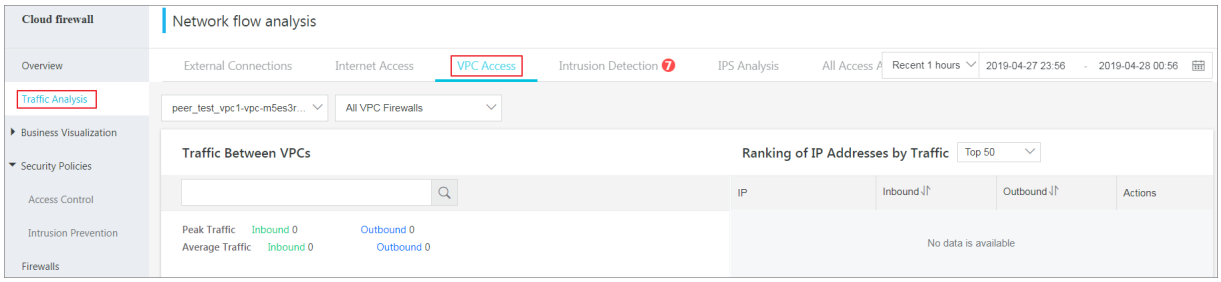
Internet Access

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



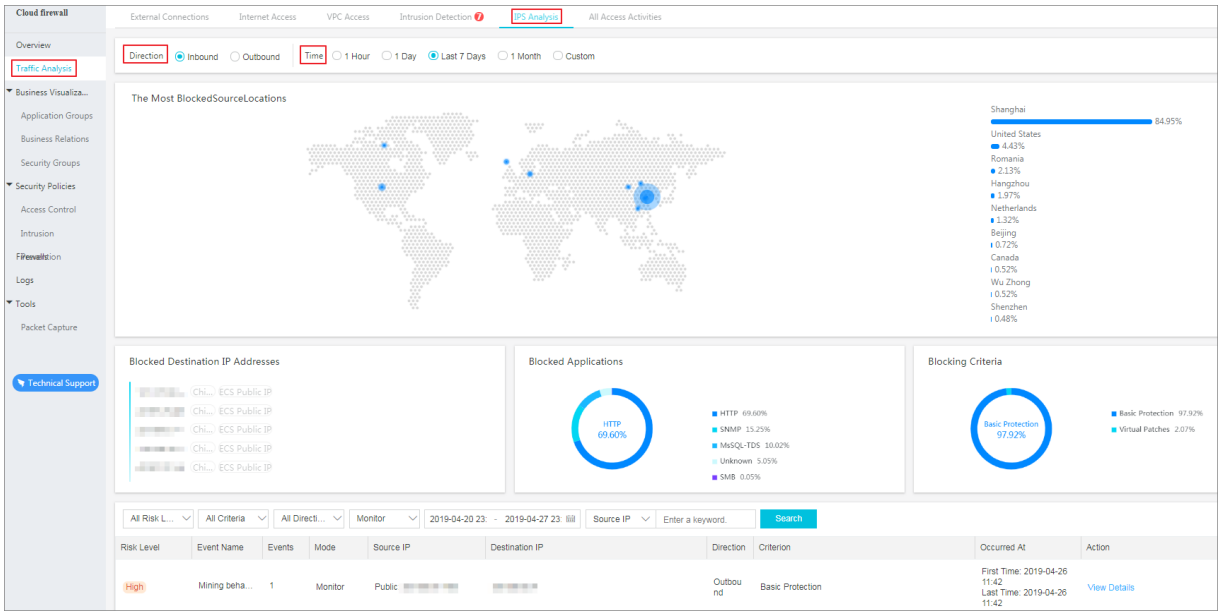
VPC Access

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



IPS Analysis

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



Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, go to **Traffic Analysis > IPS Analysis**.
3. In the **Direction** area, click **Inbound** or **Outbound** to view the corresponding blocked inbound or outbound traffic.
4. Select **Time** by one hour, one day, last seven days, one month, or a custom time range to display the required blocking traffic.

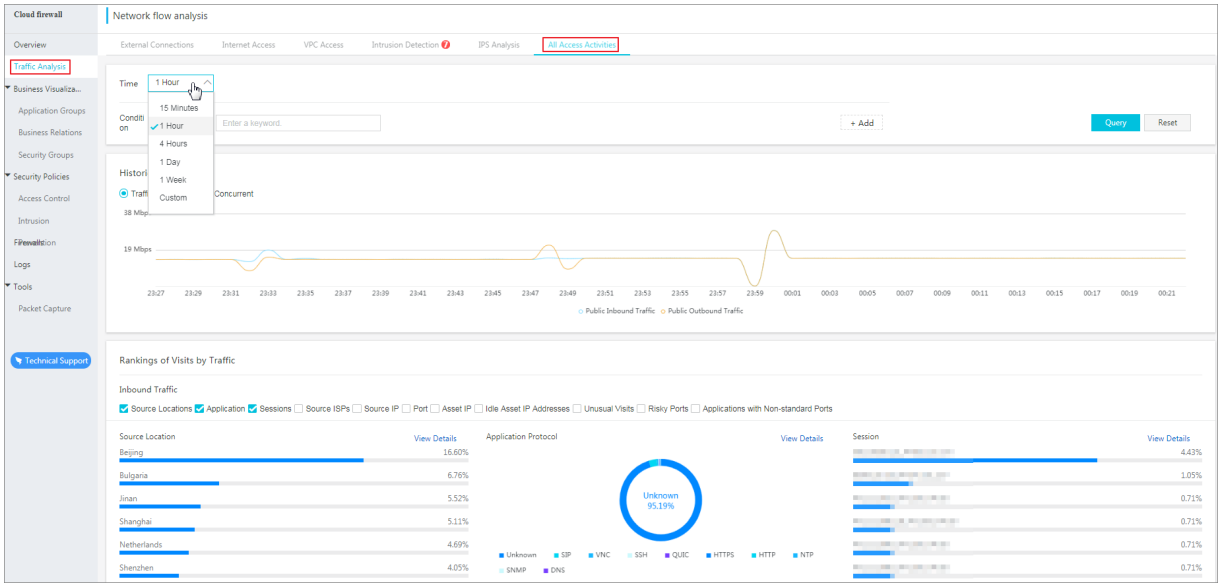
   You could monitor the following information on the blocked traffic:

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

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

All Access Activities

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



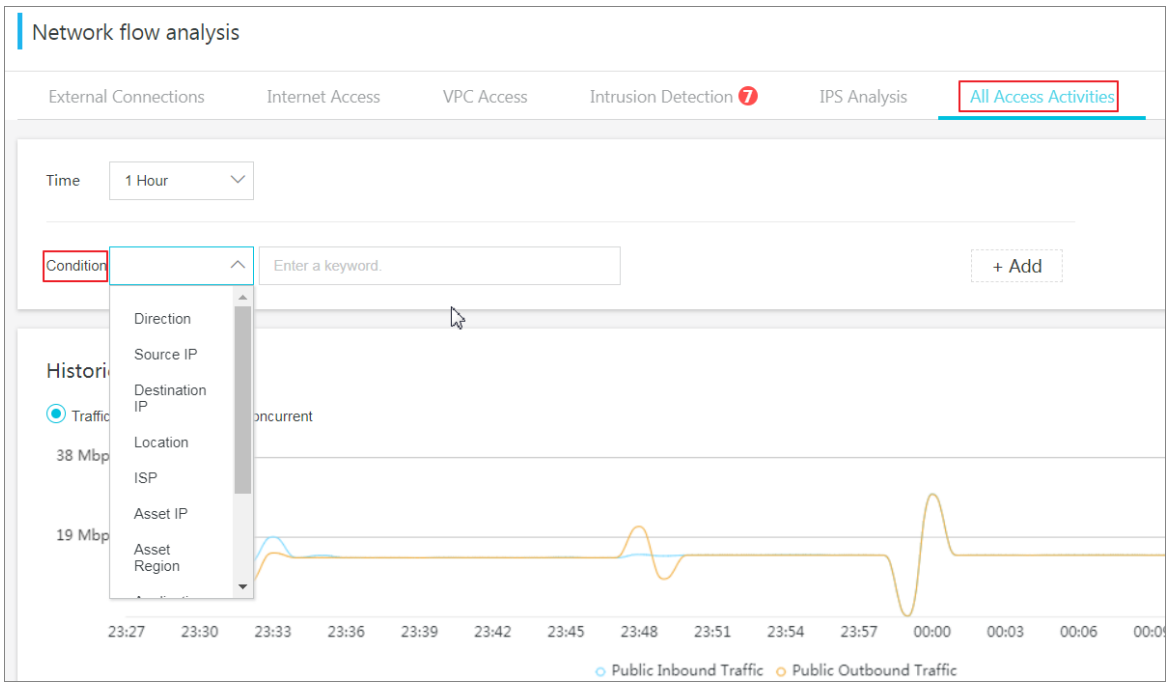
Procedure

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

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

   > **Note** You can specify any time range without limitations.

Select a search condition from the **Condition** drop-down list and enter or select the condition details. Click **Search** to query the historical traffic trend based on the selected condition.



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

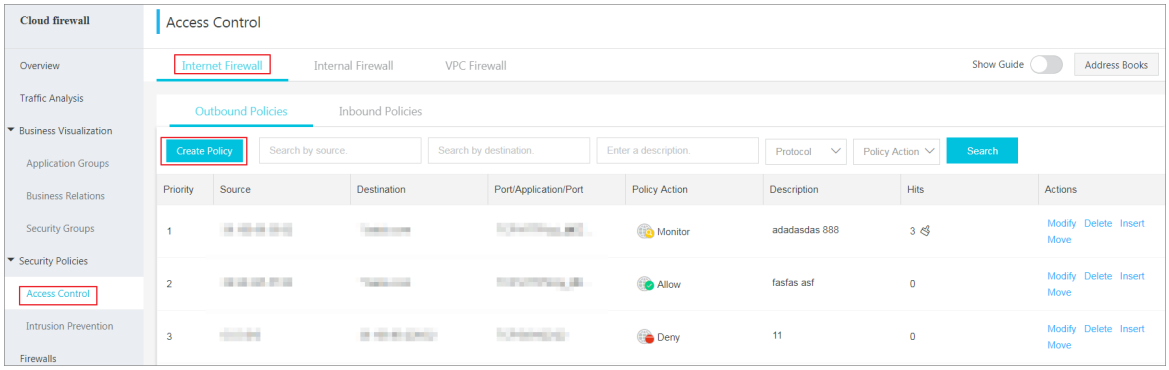
5.Configure access control policies

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

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

Procedure

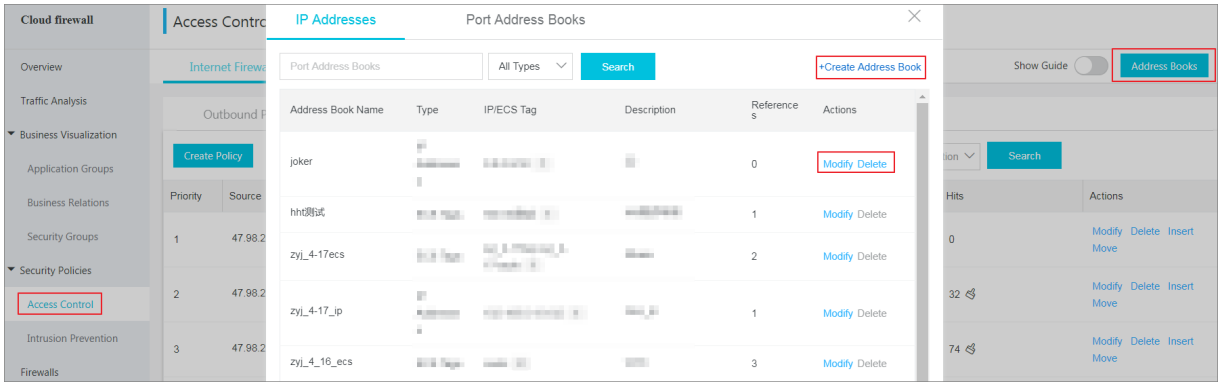
1. Log on to the Cloud Firewall console.
2. On the **Access Control > Internet firewall** page of the console, click **Create Policy** to configure an access control policy.



Configurations are as follows:

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

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



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