ALIBABA CLOUD

Alibaba Cloud

Cloud Firewall

Quick Start

Document Version: 20220527

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.Use Cloud Firewall

This topic describes the basic operations in the Cloud Firewall console.

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

1. On the **Firewall Settings > Firewall Settings** page, enable firewalls. For more information, see Enable firewalls.
2. On the **Intrusion Prevention > Prevention Configuration** page, configure intrusion prevention policies. For more information, see Enable intrusion prevention.
3. On the **Access Control > Access Control** page, configure access control policies. For more information, see Configure access control policies.
4. On the **Traffic Analysis > Outbound Connections** page, view information about outbound connections. For more information, see View traffic statistics.

2.Enable firewalls

If you enable a firewall but no access control policies are configured for the firewall or the block mode is disabled for the threat detection engine, your service traffic passes through Cloud Firewall but malicious traffic is not blocked. As a result, your assets are not protected. You can enable or disable a firewall for your assets on the **Firewall Settings** page of the Cloud Firewall console. You do not need to perform complex configurations to enable a firewall. After you enable a firewall, the firewall immediately takes effect.

Limits

Cloud Firewall Enterprise Edition and Ultimate Edition support private cloud (VPC) firewalls. The Basic Edition (free of charge) and Premium Edition do not support VPC firewalls. For more information about the features that each edition supports, see Editions and limits.

For more information about the limits that you must bear in mind when you enable VPC firewalls, see VPC firewall limits.

Procedure

1.
2.
3. On the **Firewall Settings** page, enable firewalls.

   Note Only Cloud Firewall Enterprise Edition and Ultimate Edition support VPC firewalls. If you use Basic 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 for your assets.

   - To enable the **Internet firewall**, perform the following steps:

     On the **Internet Firewall** tab, find the asset that you want to protect and click **Enable Firewall** in the **Actions** column. If you want to enable or disable the Internet firewall for multiple assets at a time, select the assets. In the lower-left corner of the page, click **Enable Firewall** or **Disable Firewall**.

   - To enable **VPC firewalls**, perform the following steps:

     On the **VPC Firewall** tab, find the asset that you want to protect and click **Enable Firewall** in the **Actions** column. If you want to enable or disable VPC firewalls for multiple assets at a time, select the assets. In the lower-left corner of the page, click **Enable Firewall** or **Disable Firewall**.

   You can specify filter conditions to search for specific assets and check whether firewalls are enabled for the assets. The filter conditions include **Asset Type**, **Region**, **Protection Status**, and **Account**.

   After the Internet firewall or a VPC firewall is enabled or disabled for your assets, the firewall status changes to Enabled or Disabled in the Firewall Status column. The value Enabled indicates that the firewall takes effect. The value Disabled indicates that the firewall no longer protects your assets. It requires several seconds for the firewall status to be updated.

References

- Enable intrusion prevention
- Configure access control policies

3.Enable intrusion prevention

Cloud Firewall provides an intrusion prevention system (IPS) to defend against intrusions in real time.

Procedure

1.
2.
3. Configure **Threat Engine Mode**.
    - **Monitor Mode**: If you enable this mode, Cloud Firewall monitors traffic and sends alerts when it detects malicious traffic. Cloud Firewall does not block the malicious traffic.
    -
    - You can also configure **Whitelist**, **Threat Intelligence**, **Basic Protection**, **Intelligent Defense**, and **Virtual Patches**. For more information, see Prevention configuration.

What's next

After intrusion prevention is enabled, you can view details about the protection action. For more information about how to view the details, see Intrusion prevention.

4.View traffic statistics

The traffic analysis feature provides real-time traffic statistics, such as the statistics of outbound connections, Internet access activities, virtual private cloud (VPC) access activities, and all access activities. This allows you to control traffic in a visualized manner and identify unusual traffic.

Context

Traffic statistics are essential information for you to configure appropriate access control policies. Before you configure access control policies, we recommend that you view the traffic statistics of your assets.

Outbound connections

The **Outbound Connections** page displays information of the outbound connections that are initiated from your hosts in real time. The information includes Outbound connection statistics, Outbound traffic, and Visualized analysis. This helps you identify suspicious hosts.

You can configure access control policies based on the traffic statistics on the **Outbound Connections** page.

1.
2.
3. On the **Outbound Connections** page, view the details about outbound connections from your assets in the last hour, 24 hours, 7 days, or a custom time range within the last 7 days.

For more information about outbound connections, see Outbound connections.

Internet access

The **Internet Access** page displays information about the capabilities that are provided by Elastic Compute Service (ECS) instances and access to the ECS instances over the Internet. The information includes ports, applications, and IP addresses. The information helps you identify normal traffic and potential intrusions. You can configure access control policies for **outbound traffic** based on the traffic statistics on the Internet Access page.

1.
2.
3. On the **Internet Access** page, view the open public IP addresses, ports, and applications of your assets.

For more information about Internet access, see Internet access.

VPC access

The **VPC Access** page displays information about the traffic between VPCs. The information helps you identify unusual traffic and potential attacks.

1.
2.
3. On the **VPC Access** page, view information about the traffic between VPCs, rankings of sessions, open ports, and assets.

For more information about VPC access, see VPC access.

All access activities

The **All Access Activities** page displays real-time traffic information about external IP addresses and IP addresses of your assets.

1.
2.
3. On the **All Access Activities** page, specify a time range and search conditions to view traffic trends of all hosts that are protected by Cloud Firewall. You can perform the following operations:
    - Configure the **Time** parameter to view all access activities and trend charts over the last 15 minutes, 1 hour, 4 hours, 1 day, 1 week, or a custom time range.

      > ⓘ **Note** The time range that you can specify is not limited.

    - Click the ⌄ icon next to **Condition**, select a search condition, and then enter or select the condition details. Then, Cloud Firewall displays historical traffic trends based on the condition.
    - In the **Rankings of Visits by Traffic** section, view information such as the top 10 traffic source locations, application protocols and percentages, and the top 10 session addresses.

For more information about all access activities, see All access activities.

5.Configure access control policies

Cloud Firewall allows you to configure access control policies for inbound, outbound, and internal traffic. This can reduce the risk of intrusion into your assets.

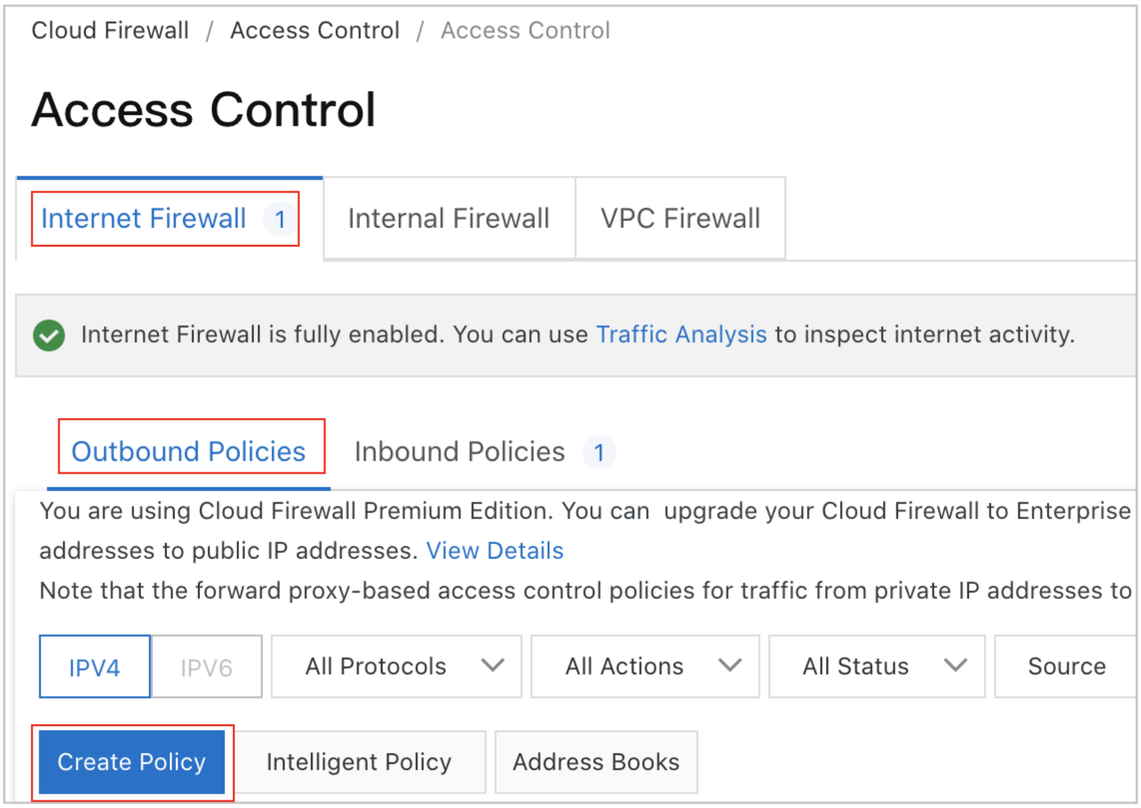
Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Access Control > Access Control**.
3. On the **Access Control** page, configure access control policies for the Internet firewall, an internal firewall, or a virtual private cloud (VPC) firewall.

   You can add multiple IP addresses to an address book. This simplifies the procedure to configure access control policies. You can also click **Address Books** to add, modify, or delete IP addresses. For more information, see Manage address books.

   - If you want to control outbound traffic, click the **Internet Firewall** tab to create **outbound policies**.

     > **Notice**
     >
     > We recommend that you configure the actions of outbound policies to **Deny**. This does not apply if the policies are used to allow necessary outbound connections.

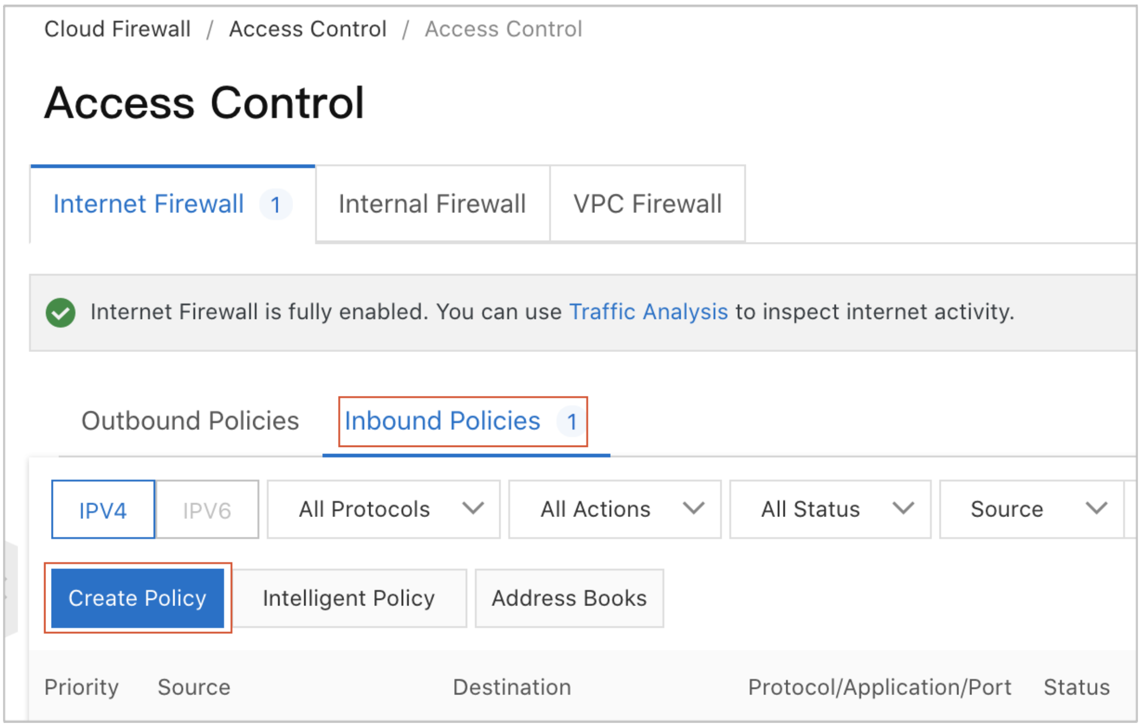
     

     Internet Firewall is fully enabled. You can use Traffic Analysis to inspect internet activity.

     You are using Cloud Firewall Premium Edition. You can upgrade your Cloud Firewall to Enterprise addresses to public IP addresses. View Details

     Note that the forward proxy-based access control policies for traffic from private IP addresses to

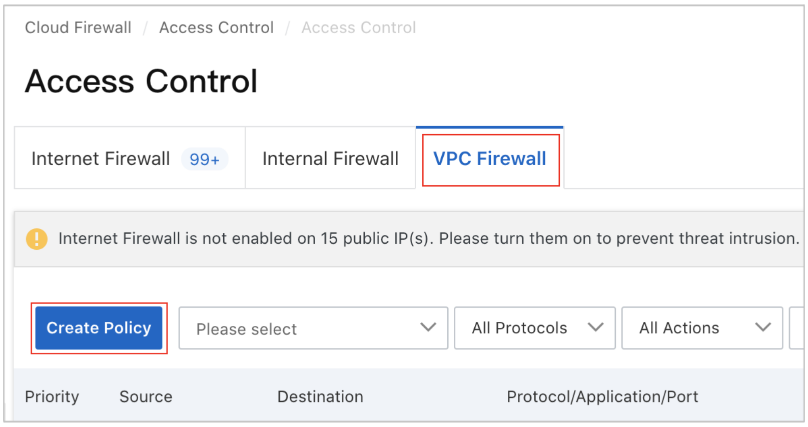
   - If you want to control inbound traffic, click the **Internet Firewall** tab to create **inbound policies**.



Internet Firewall is fully enabled. You can use Traffic Analysis to inspect internet activity.

- If you want to control traffic between VPCs, click the **VPC Firewall** tab to create access control policies for **VPC firewalls**.

> **Notice** The VPC Firewall feature is supported only for Cloud Firewall Enterprise Edition and Ultimate Edition.



Internet Firewall is not enabled on 15 public IP(s). Please turn them on to prevent threat intrusion.