# Alibaba Cloud
# 云防火墙

## Overview

Issue: 20200529

# 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 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 contact Alibaba Cloud directly if you discover any errors in this document.

# Document conventions

| Style | Description | Example |
| --- | --- | --- |
|  | 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. |
|  | 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. |
|  | 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. |
|  | 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]` |

| Style | Description | Example |
| --- | --- | --- |
| {} or {a\|b} | This format is used for a required value, where only one item can be selected. | switch {active\|stand} |

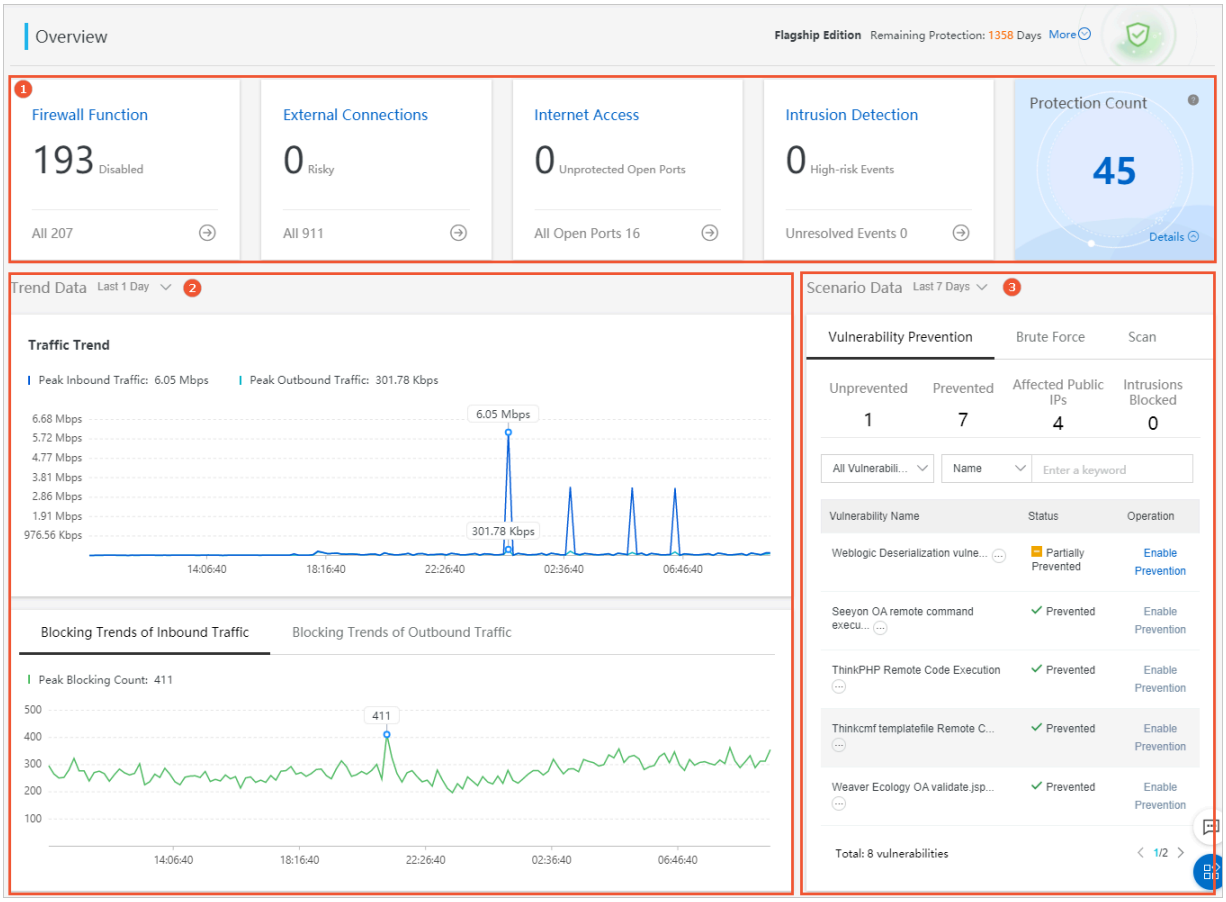
# Contents

# 1 Overview

The Overview page of Cloud Firewall displays the overall protection status of a cloud firewall in terms of protection statistics, traffic trends, and protection scenarios. This topic describes the data displayed on the Overview page, helping you understand the security status of your network assets.

### Access the Overview page

Log on to the Cloud Firewall console. The **Overview** page appears.



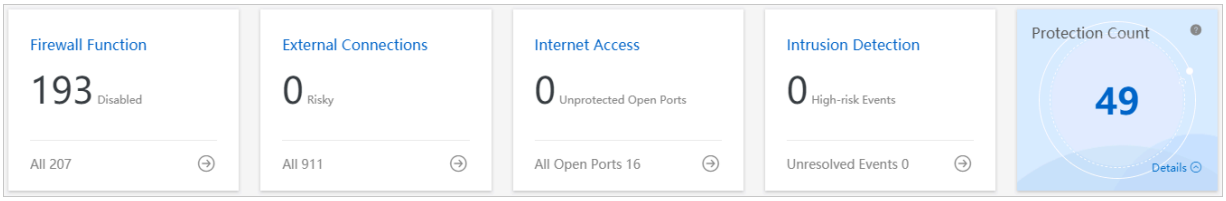

The **Overview** page consists of three parts. You can click the following links to view the individual parts.

- Protection statistics (marked by ①)
- Trend data (marked by ②)
- Scenario data (marked by ③)

In the upper-right corner of the **Overview** page, you can view the version and the valid days of the Cloud Firewall instance that remain. You can click **Upgrade** or **Renew** based on

your business requirements. For more information, see Upgrade and renewal. You can click **More** to view instance details, including the bandwidth specification, peak bandwidth in the last week, number of supported regions, number of current regions, public IP address quota, and storage space for log analysis.

**Protection statistics**



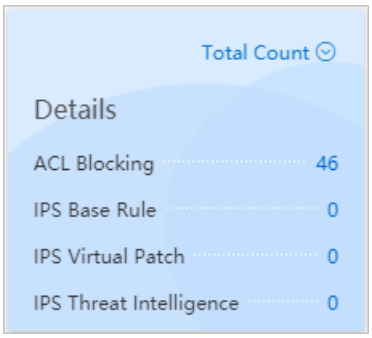

Protection statistics include the following information:

- **Firewall Function**: displays the number of network assets for which you have not enabled Internet firewall. You can click the number or the icon to go to the **Firewall Settings** page to enable or disable the firewall. For more information, see #unique_5.
- **External Connections**: displays the number of risky external connections detected by Cloud Firewall. You can click the number or the icon to go to the **External Connections** page to view details. For more information, see #unique_6.
- **Internet Access**: displays the number of risky open ports on network assets. You can click the number or the icon to go to the **Internet Access** page to view details. For more information, see #unique_7.
- **Intrusion Detection**: displays the number of unhandled intrusion events on network assets. You can click the number or the icon to go to the **Intrusion Detection** page and handle the intrusion events. For more information, see #unique_8.
- **Protection Count**: displays the number of abnormal sessions blocked by Cloud Firewall in real time.

**Note:**

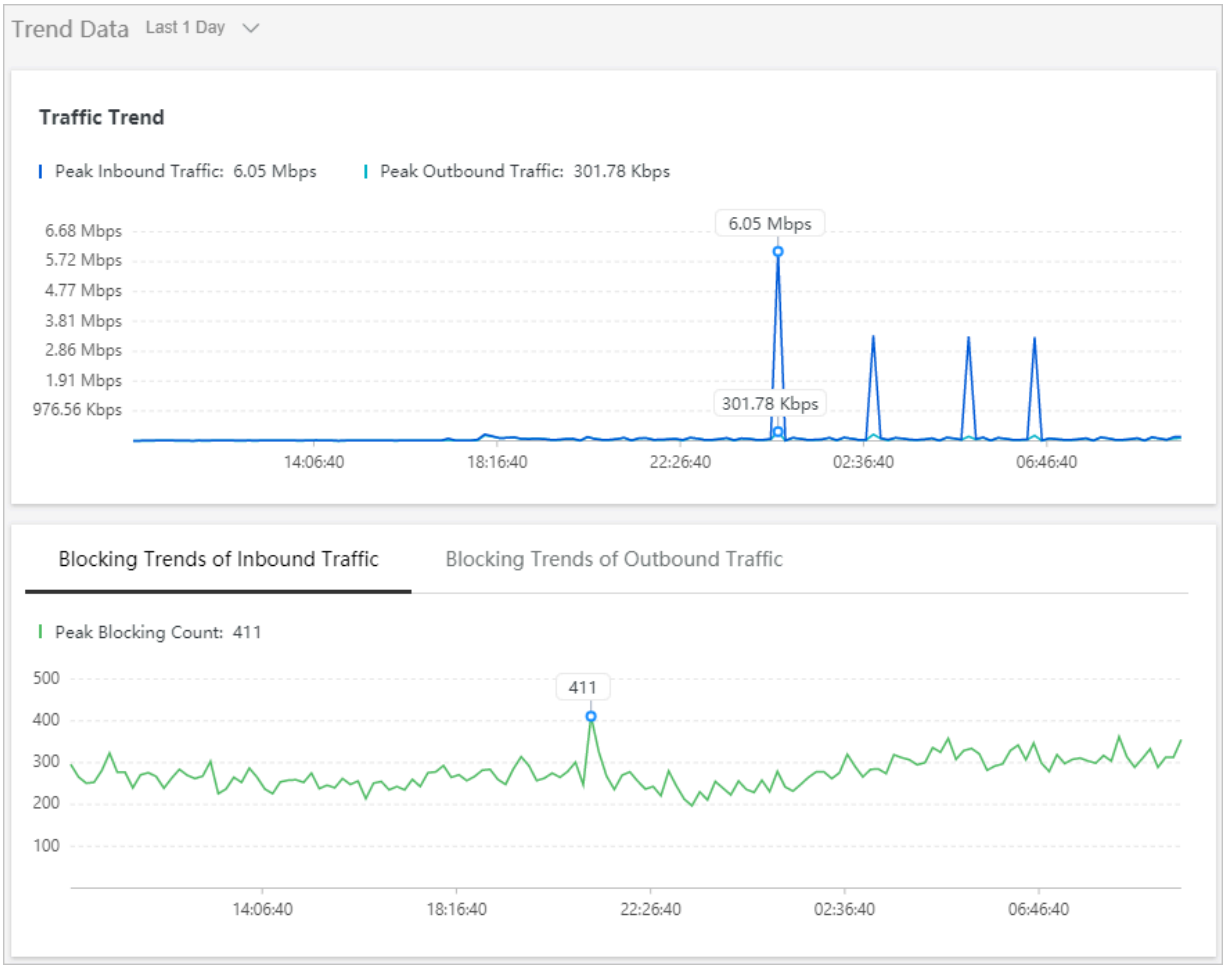
The number of abnormal sessions updates with a delay of several minutes.

You can click **Details** to view detailed information. The following figure shows the details.



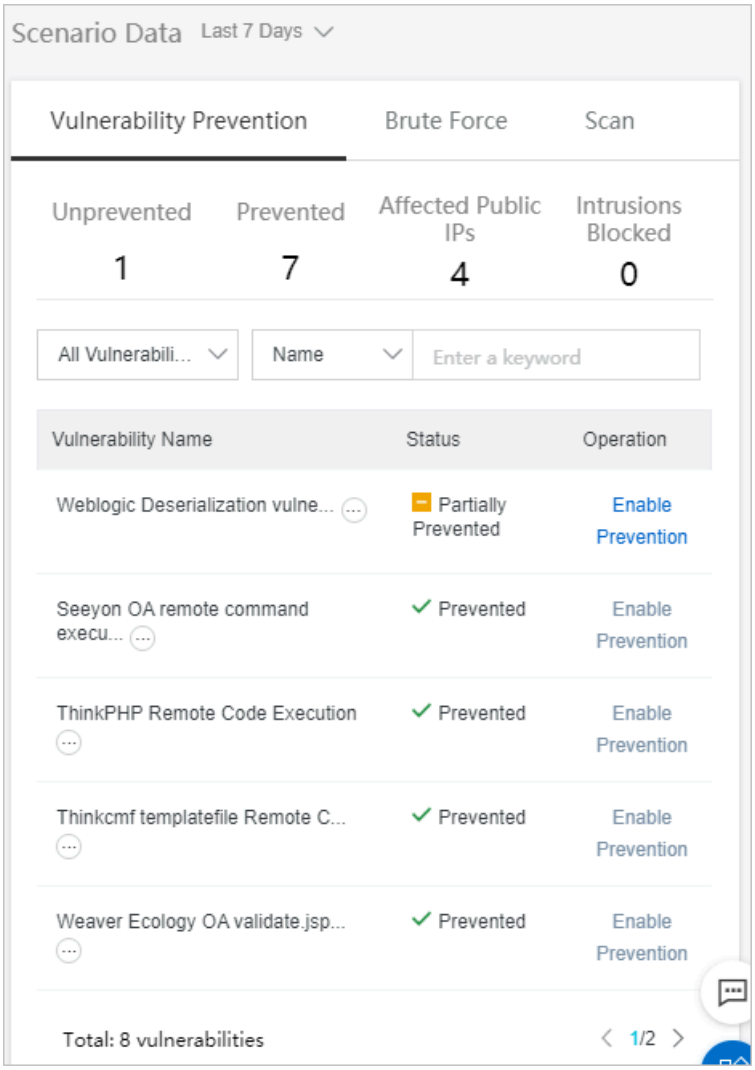

### Trend data

Trend data displays the overall traffic trend of protected network assets and the number of both inbound and outbound sessions blocked by Cloud Firewall within a specified period. You can click the drop-down arrow next to **Trend Data** and select a time range. The options include **Last 1 Hour**, **Last 1 Day**, and **Last 7 Days**.



### Scenario data

Scenario data shows vulnerability prevention, brute-force attacks, and risks identified by scanning on the protected network assets within a specified period. You can click the drop-down arrow next to **Scenario Data** and select a time range. The options include **Last 1 Hour**, **Last 1 Day**, and **Last 7 Days**. You can also click the **Vulnerability Prevention**, **Brute Force**, or **Scan** tab to view data of these types.



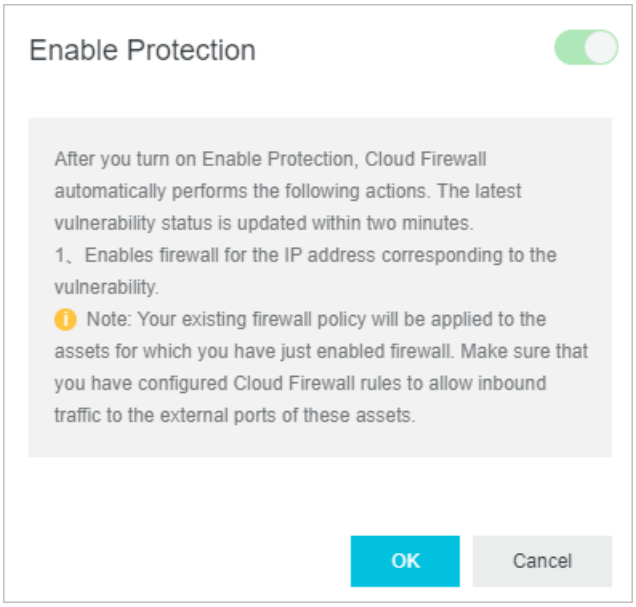

- **Vulnerability Prevention**: displays vulnerability statistics and a vulnerability list. Vulnerability statistics include the numbers of unprevented vulnerabilities, prevented vulnerabilities, affected public IP addresses, and blocked intrusions. To enable prevention for a specific vulnerability, follow these steps:

  1. Find the vulnerability you want to prevent and click **Enable Prevention**.

     **Note:**

Prevention can be enabled only for vulnerabilities whose status is **Unprevented** or **Partially Prevented**.

2. In the **Enable Prevention** dialog box that appears, confirm the information, and click **OK**.




Then, **Status** of the vulnerability changes to **Prevented**.

- **Brute Force**: displays statistics of brute-force attacks and details about attacked applications and assets. Statistics of brute-force attacks include the numbers of attacks, blocked attacks, attacked applications, and attacked assets.
- **Scan**: displays risk statistics and details about scanned applications and assets. Risk statistics include the numbers of attacks, blocked attacks, attacked applications, and attacked assets.

# 2 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:**

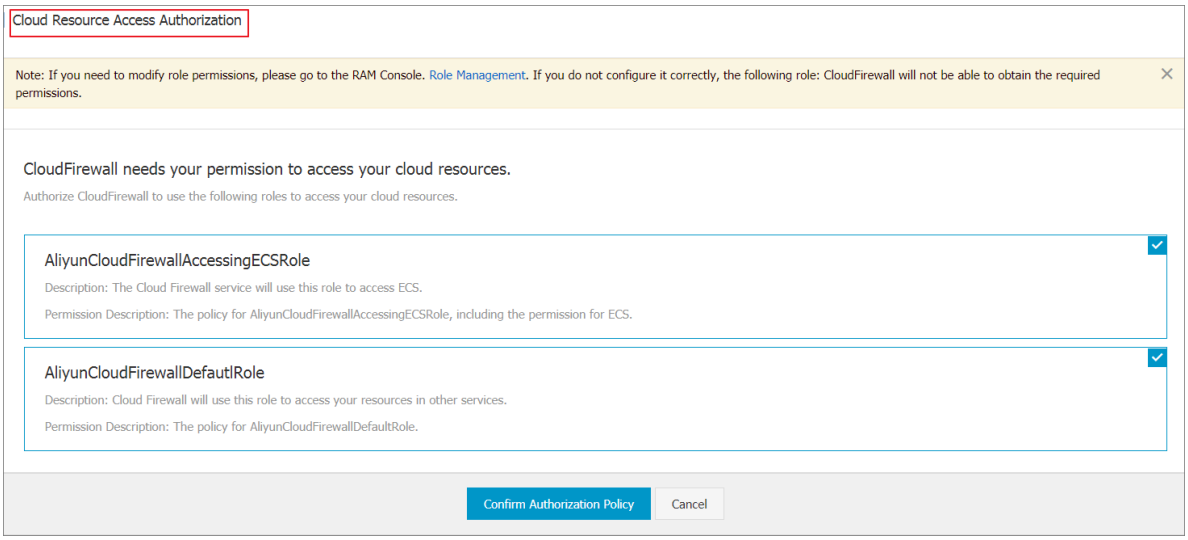
You cannot use a RAM user account without the AliyunRAMFullAccess permission to grant Cloud Firewall the access to cloud resources.

### 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.

# 3 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** or 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.