ALIBABA CLOUD

Alibaba Cloud

Cloud Firewall
Toolbox

Document Version: 20211129

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.Back up and roll back an access control policy

Cloud Firewall allows you to back up and roll back access control policies for both inbound and outbound traffic on the Internet firewall. This topic describes how to back up and roll back an access control policy.

Context

You can roll back access control policies in the Ultimate Edition or Enterprise Edition of Cloud Firewall, but not in the Premium Edition.

Each Alibaba Cloud account can have up to 12 policy backups at a time. If your Alibaba Cloud account has 12 policy backups, you must delete a policy backup before you can create another policy backup. For information about how to delete a policy backup, see Related operations. The number of times you can create policy backups each day is unlimited.

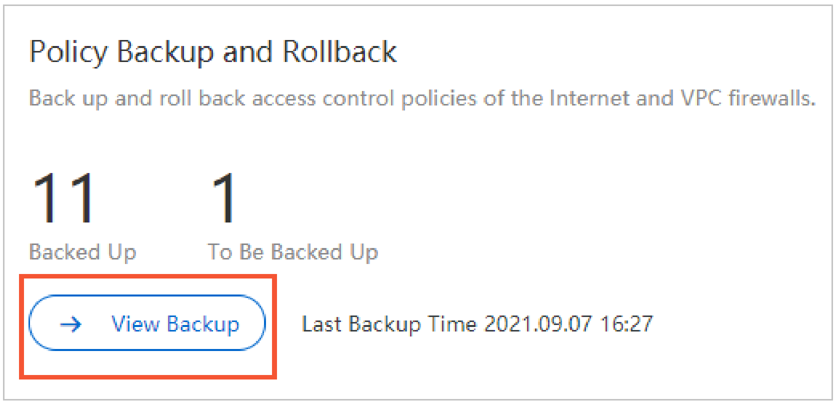
Policy rollback indicates that an in-use policy is replaced with a policy that you have backed up. To ensure that access control policies work normally, we recommend that you perform the following operations to roll back an in-use policy:

1. Back up the policy.
2. During off-peak hours, disable all firewalls.
3. Roll back the policy.
4. After the policy is rolled back, enable the firewalls one by one and verify that access to your services is normal.

> **Note** Only access control policies of the Internet firewall can be rolled back. The access control policies of virtual private cloud (VPC) firewalls and internal firewalls cannot be rolled back.

Back up an access control policy

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Settings** > **Toolbox**.
3. On the **Toolbox** page, click **View Backup**.



Policy Backup and Rollback

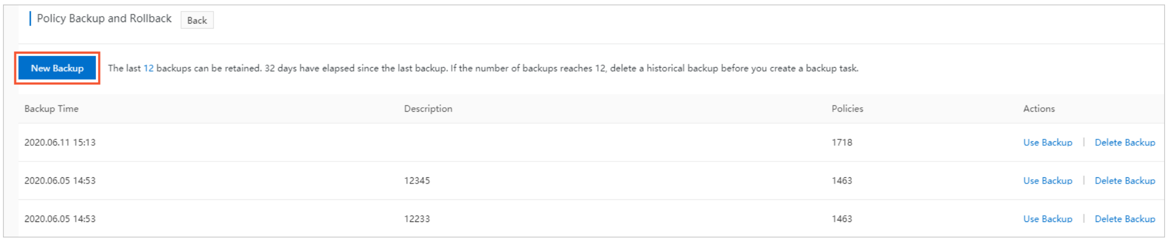
Back up and roll back access control policies of the Internet and VPC firewalls.

11 Backed Up

1 To Be Backed Up

Last Backup Time 2021.09.07 16:27

4. On the **Policy Backup and Rollback** page, click **New Backup**.

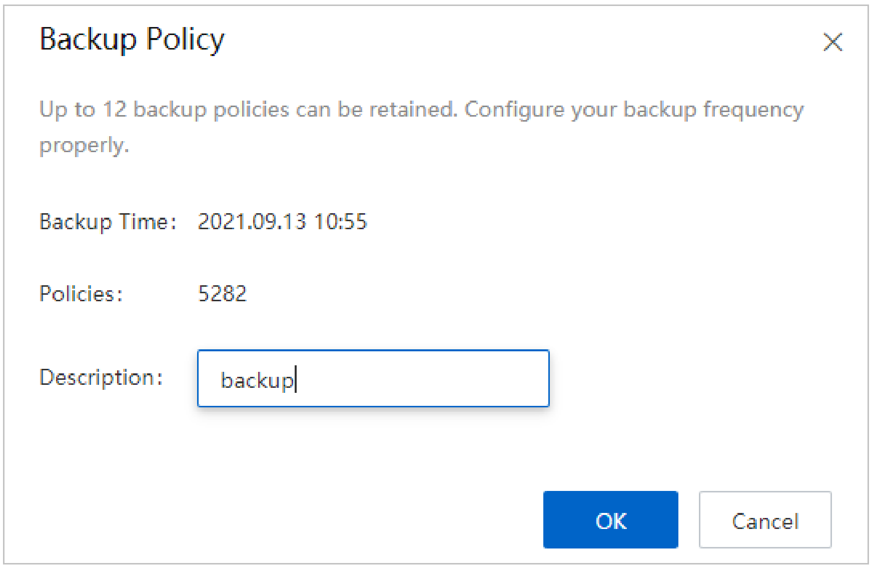


Policy Backup and Rollback

The last 12 backups can be retained. 32 days have elapsed since the last backup. If the number of backups reaches 12, delete a historical backup before you create a backup task.

Backup Time	Description	Policies	Actions
2020.06.11 15:13		1718	Use Backup | Delete Backup
2020.06.05 14:53	12345	1463	Use Backup | Delete Backup
2020.06.05 14:53	12233	1463	Use Backup | Delete Backup

5. In the **Backup Policy** dialog box, enter the description of the policy backup and click **OK**.



Backup Policy

Up to 12 backup policies can be retained. Configure your backup frequency properly.

Backup Time: 2021.09.13 10:55

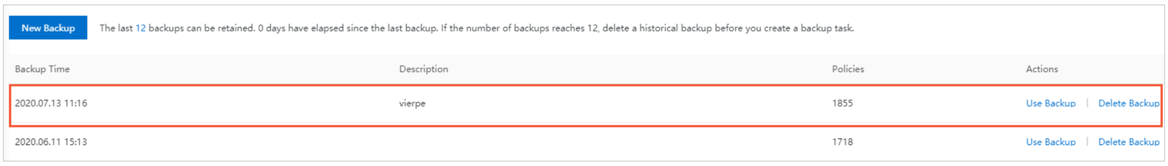
Policies: 5282

Description: backup

The following table describes the parameters in the Backup Policy dialog box.

Parameter	Description
Backup Time	The time when the access control policy for both inbound and outbound traffic on the Internet firewall is backed up.
Policies	The number of access control policies for both inbound and outbound traffic on the Internet firewall. The policies are created within the current Alibaba Cloud account.
Description	The description of the policy backup that you want to create. **Note** You can enter up to 256 characters for Description. You can determine which policy backup to use for rollback based on the description and backup time. To help identify the backup, enter an informative description.

You can view the new policy backup on the **Policy Backup and Rollback** page.



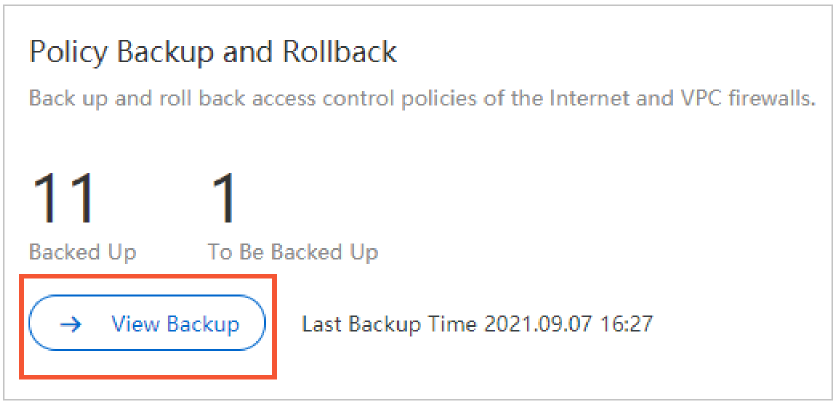
New Backup The last 12 backups can be retained. 0 days have elapsed since the last backup. If the number of backups reaches 12, delete a historical backup before you create a backup task.

Backup Time	Description	Policies	Actions
2020.07.13 11:16	vierpe	1855	Use Backup | Delete Backup
2020.06.11 15:13		1718	Use Backup | Delete Backup

Roll back an access control policy

After you create backups of a policy, you can roll back the policy to restore one of the policy backups.

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Settings > Toolbox**.
3. On the **Toolbox** page, click **View Backup**.



Policy Backup and Rollback

Back up and roll back access control policies of the Internet and VPC firewalls.

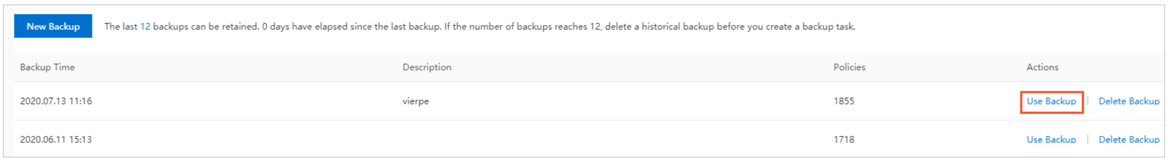
11 Backed Up

1 To Be Backed Up

→ View Backup

Last Backup Time 2021.09.07 16:27

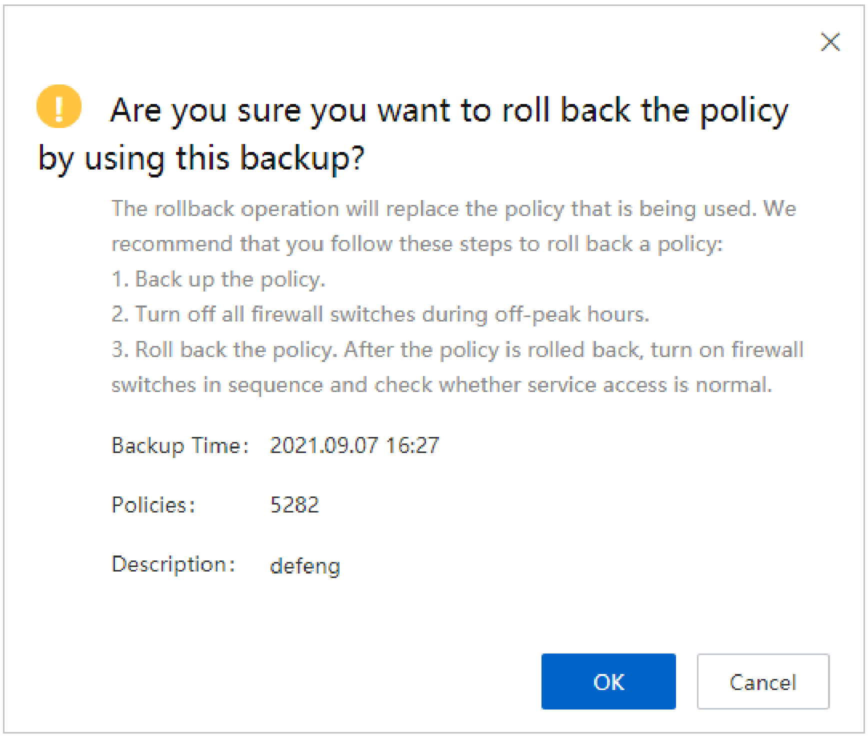
4. On the **Policy Backup and Rollback** page, find the backup that you want to use for the policy rollback and click **Use Backup** in the Actions column.



New Backup The last 12 backups can be retained. 0 days have elapsed since the last backup. If the number of backups reaches 12, delete a historical backup before you create a backup task.

Backup Time	Description	Policies	Actions
2020.07.13 11:16	vierpe	1855	Use Backup | Delete Backup
2020.06.11 15:13		1718	Use Backup | Delete Backup

5. In the **Are you sure you want to roll back the policy by using this backup?** message, click **OK**.



Are you sure you want to roll back the policy by using this backup?

The rollback operation will replace the policy that is being used. We recommend that you follow these steps to roll back a policy:

1. Back up the policy.
2. Turn off all firewall switches during off-peak hours.
3. Roll back the policy. After the policy is rolled back, turn on firewall switches in sequence and check whether service access is normal.

Backup Time: 2021.09.07 16:27

Policies: 5282

Description: defeng

Note

- The policy is rolled back in seconds.
- If a large number of access control policies exist within your Alibaba Cloud account, or a large number of users are performing policy rollback at the same time, a timeout error can occur. If a timeout error occurs, the system displays prompts for you to address the issue.
- If the rollback fails, the access control policy that is in use remains unchanged.

Related operations

To delete the backups of a policy, go to the **Policy Backup and Rollback** page, find the backup that you want to delete, and then click **Delete Backup** in the Actions column.

2.Create a packet capture task

This topic describes how to create a packet capture task. You can use the packet capture feature to capture network data packets for specific IP addresses and ports, and analyze the packets. This feature allows you to identify exceptions that occur on your network, analyze attacks, and identify the security risks of network communications.

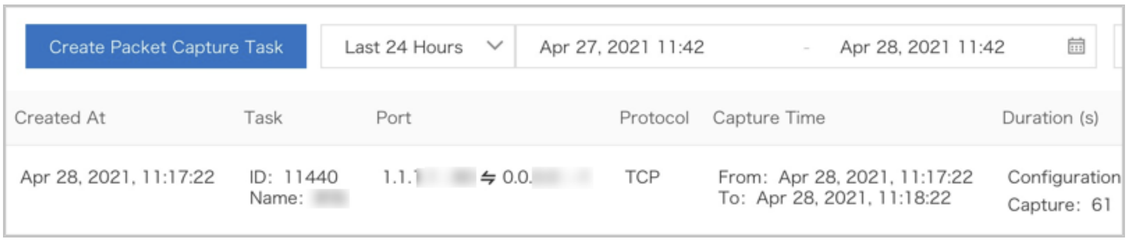
Limits

Enterprise Edition and Ultimate Edition of Cloud Firewall support the packet capture feature. Basic Edition and Premium Edition of Cloud Firewall do not support this feature. The following list describes the quota of packet capture tasks per Alibaba Cloud account:

- If you use Enterprise Edition of Cloud Firewall, the quota is 20 per day.
- If you use Ultimate Edition of Cloud Firewall, the quota is 50 per day.

Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Settings > Toolbox**.
3. On the **Toolbox** page, click **Capture Now** in the Packet Capture section.
4. On the **Packet Capture** page, click **Create Packet Capture Task**.


Create Packet Capture Task
Last 24 Hours
Apr 27, 2021 11:42 - Apr 28, 2021 11:42

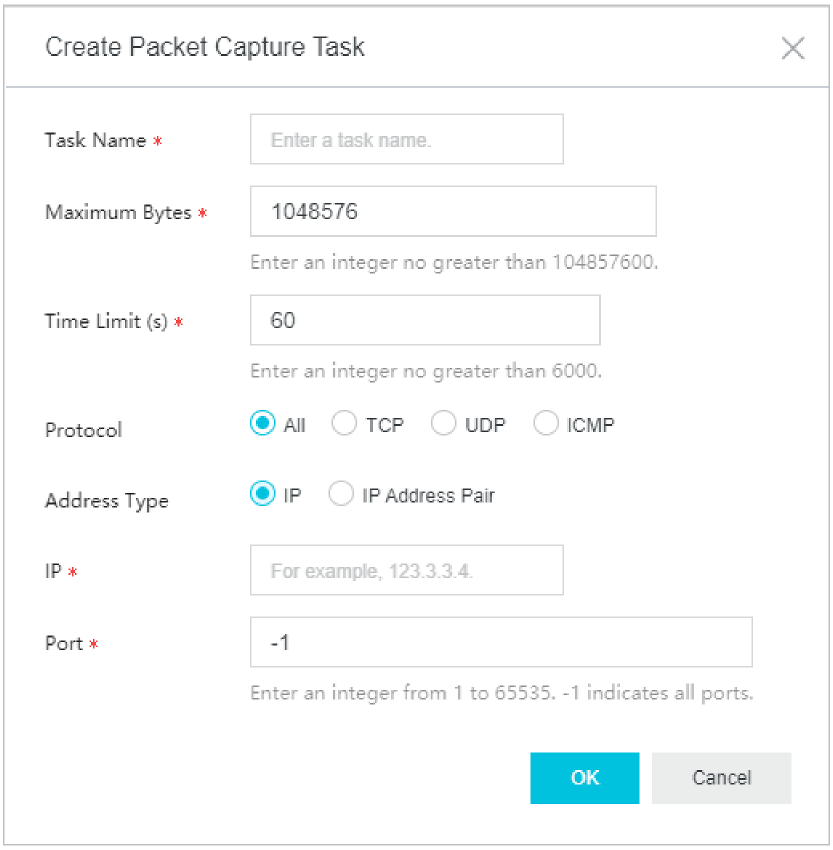
Created At	Task	Port	Protocol	Capture Time	Duration (s)
Apr 28, 2021, 11:17:22	ID: 11440 Name: [redacted]	1.1.1[redacted] ⇋ 0.0.[redacted]	TCP	From: Apr 28, 2021, 11:17:22 To: Apr 28, 2021, 11:18:22	Configuration Capture: 61

5. In the **Create Packet Capture Task** dialog box, configure the parameters.

Parameter	Description
Task Name	The name of the packet capture task. We recommend that you enter an informative name, such as a name that indicates the purpose of the task.
Maximum Bytes	The maximum number of bytes in a packet that can be captured. If the number of bytes in a packet exceeds this number, the packet is discarded.
Duration (s)	The maximum duration for the packet capture task. Unit: seconds.
Protocol	The protocol type for packet capture. Valid values: ○ *All* ○ *TCP* ○ *UDP* ○ *ICMP*

Parameter	Description
Address Type	The type of the IP address configuration. ○ *IP*: Only the packets that are sent to or from a specific IP address are captured. You can enter only one IP address. ○ *IP Address Pair*: Only the packets that are transmitted between a specific IP address and its peer IP address are captured. You can enter only one IP address and its peer IP address.
IP	The IP address based on which packets are captured.
Port	The port based on which packets are captured.
Peer IP	The peer IP address based on which packets are captured. **Note** This parameter is required only when Address Type is set to IP Address Pair.
Peer Port	The peer port based on which packets are captured. **Note** This parameter is required only when Address Type is set to IP Address Pair.

6. Click **OK**.



Create Packet Capture Task

Task Name * Enter a task name.

Maximum Bytes * 1048576

Enter an integer no greater than 104857600.

Time Limit (s) * 60

Enter an integer no greater than 6000.

Protocol ● All ○ TCP ○ UDP ○ ICMP

Address Type ● IP ○ IP Address Pair

IP * For example, 123.3.3.4.

Port * -1

Enter an integer from 1 to 65535. -1 indicates all ports.

Result

You can go to the **Packet Capture** page to view the newly created task and the status of the task. If the status of the task changes to **Completed** in the **Status** column, the packet capture task is complete.

3.Strict mode of the Internet firewall

After you enable the strict mode of the Internet firewall, the Internet firewall directly blocks traffic that meets the following conditions: The traffic matches an access control policy, and the application type of the traffic is identified Unknown by Cloud Firewall. Cloud Firewall identifies application types based on packet characteristics. If Cloud Firewall fails to identify the application type of the traffic, Cloud Firewall automatically allows the traffic. If you want to discard traffic with unknown application types, we recommend that you enable the strict mode.

Prerequisites

Access control policies are configured for the Internet firewall. For more information, see Create access control policies for outbound and inbound traffic on the Internet firewall.

Context

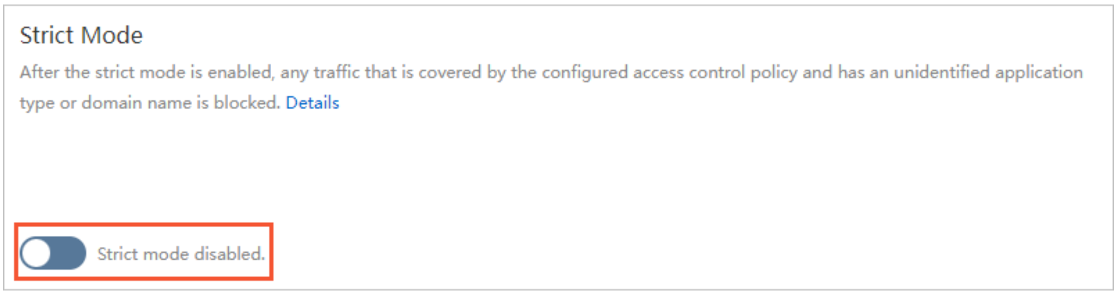
The strict mode takes effect only on traffic that matches an access control policy, regardless of whether the policy action is allow, deny, or monitor. If traffic does not match an access control policy, the traffic is allowed even if its application type is unknown.

Enable or disable the strict mode

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Settings > Toolbox**.
3. On the **Toolbox** page, enable or disable the switch in the **Strict Mode** section.

   The following steps describe how to enable **Strict Mode**:

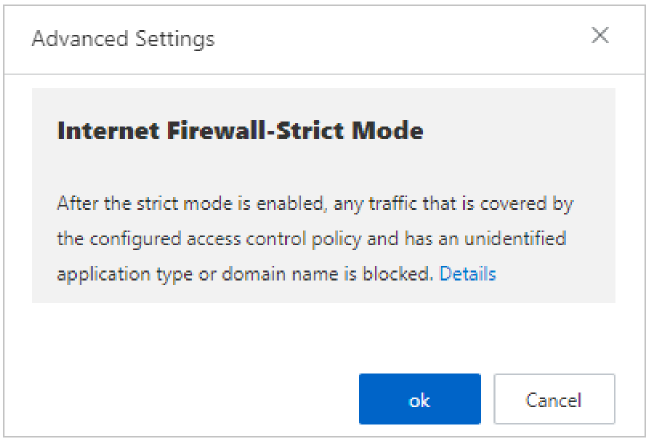
   i. In the **Strict Mode** section, turn on Strict Mode.



Strict Mode

After the strict mode is enabled, any traffic that is covered by the configured access control policy and has an unidentified application type or domain name is blocked. Details

ii. In the **Advanced Settings** message, click **OK**.



Advanced Settings

Internet Firewall-Strict Mode

After the strict mode is enabled, any traffic that is covered by the configured access control policy and has an unidentified application type or domain name is blocked. Details

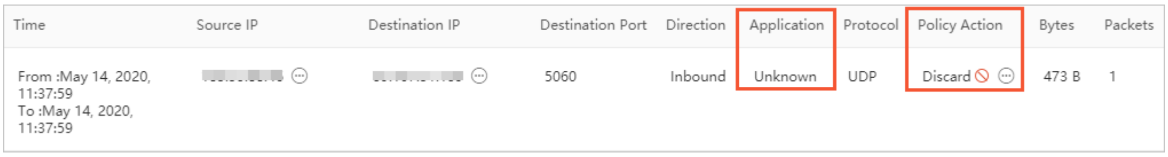
After the strict mode is enabled, the Internet firewall blocks traffic that meets the following conditions: The traffic matches an access control policy, and the application type of the traffic is identified Unknown. You can view the logs of discarded traffic on the **Log Audit** page.

View logs of discarded traffic

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Log Analysis > Log Audit**.
3. On the **Traffic Logs** tab of the **Log Audit** page, find the **Internet Firewall** tab.
4. On the **Internet Firewall** tab, click **Show Advanced Search**. Then, set **Application** to **Unknown** and **Policy Source** to **Access Control** and click **Search**.
5. View the logs of traffic that is discarded in strict mode. For example, you can view the time, source IP addresses, destination IP addresses, and destination ports of the discarded traffic.

   The **policy names** in these logs are **unknown_app_deny_all**.

   Notice If normal traffic is discarded, we recommend that you add the application protocol information to the request packets or disable the strict mode.



Time	Source IP	Destination IP	Destination Port	Direction	Application	Protocol	Policy Action	Bytes	Packets
From :May 14, 2020, 11:37:59 To :May 14, 2020, 11:37:59	[redacted]	[redacted]	5060	Inbound	Unknown	UDP	Discard	473 B	1