ALIBABA CLOUD

Alibaba Cloud

Cloud Firewall

Toolbox

Document Version: 20200929

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 ensures that your access control policies can be restored to a normal status in a timely manner.

Context

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

Each Alibaba Cloud account can have up to 12 policy backups at a time. If you already have 12 policy backups, you must delete a backup before you create another backup. For information about how to delete a backup, see What to do next. There is no limit to the number of times you can create backups in a day.

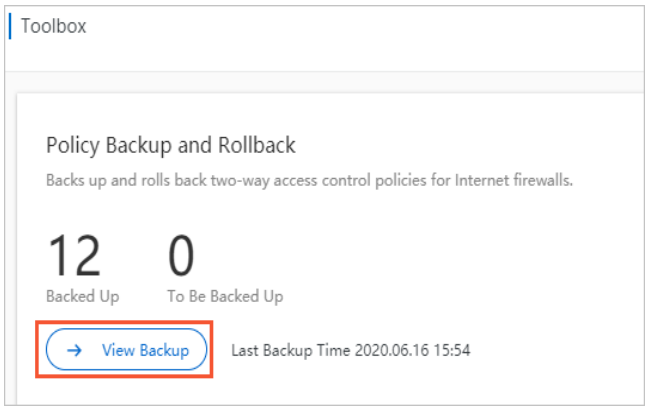
Rolling back an access control policy that is in use replaces it with a policy that you have backed up. To ensure that access control policies function correctly, we recommend that you follow these steps to roll back a policy that is in use:

1. Back up the policy.
2. Roll back the policy during off-peak hours with all firewall switches turned off.
3. After the policy is rolled back, turn on the firewall switches one by one and verify that your business access is normal.

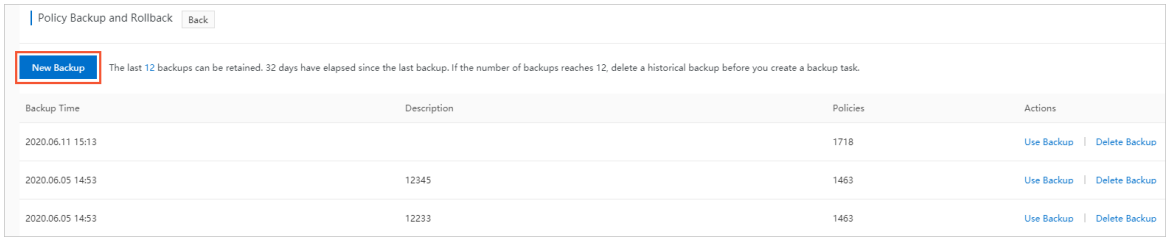
> **Note** Only access control policies of the Internet firewall can be rolled back. Those of VPC firewalls and internal firewalls cannot be rolled back.

Back up an access control policy

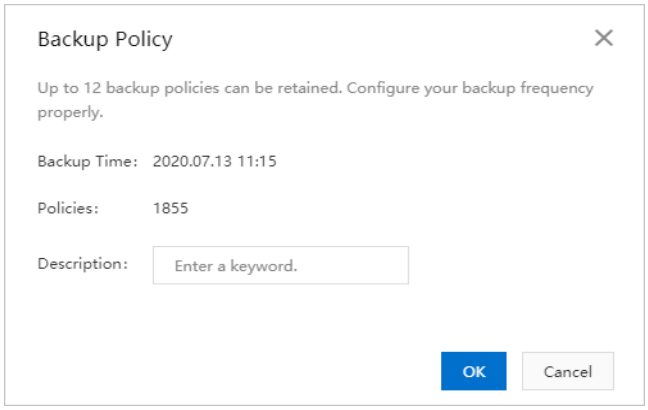
1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, click **Toolbox**.
3. On the **Toolbox** page, click **View Backup**.



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



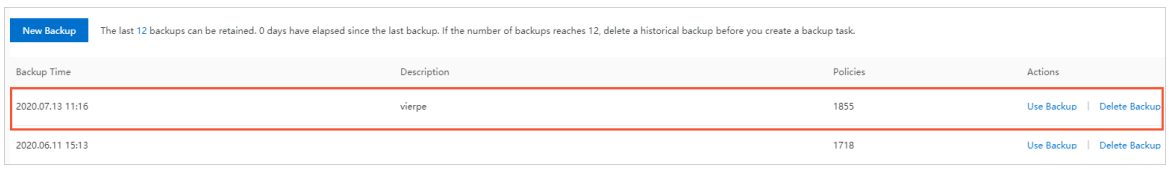
5. In the **Backup Policy** dialog box, enter a description of the policy backup and click **OK**.



The following table describes the parameters for creating a backup.

Parameter	Description
Backup Time	The time the access control policy for both inbound and outbound traffic on the Internet Firewall is backed up.
Description	The description of the policy backup. **Note** You can enter a maximum of 256 characters for the description. You can determine which policy to roll back based on the description and backup time. Therefore, enter an informative description.
Policies	The number of access control policies for both inbound and outbound traffic on the Internet Firewall created by the current Alibaba Cloud account.

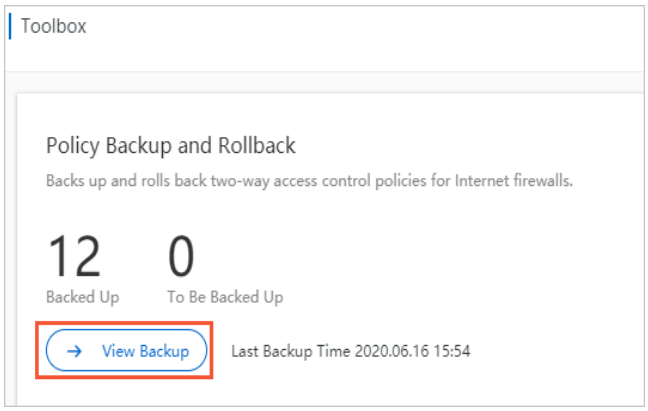
You can view the new backup on the **Policy Backup and Rollback** page.



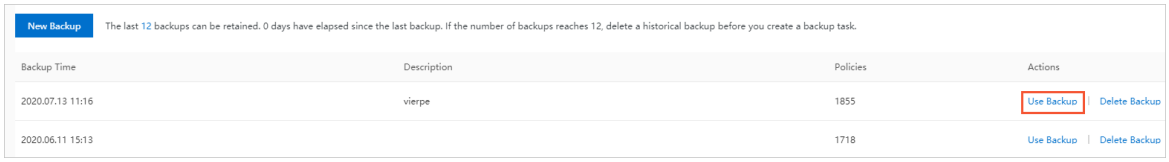
Roll back an access control policy

Before you roll back an access control policy, ensure that a backup file is available for the rollback.

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



4. On the **Policy Backup and Rollback** page, find the policy that you want to roll back and click **Use Backup** in the Actions column.



> **Note**
>
> - The policy is rolled back in seconds.
> - If the number of policies under your Alibaba Cloud account is large or if many users are rolling back policies at the same time, a timeout error may occur. We recommend that you only use your Alibaba Cloud account yourself to roll back policies. If a policy rollback times out, the system displays a message. Follow the prompts to resolve the issue.
> - If a policy rollback fails, the access control policy remains unchanged.

What to do next

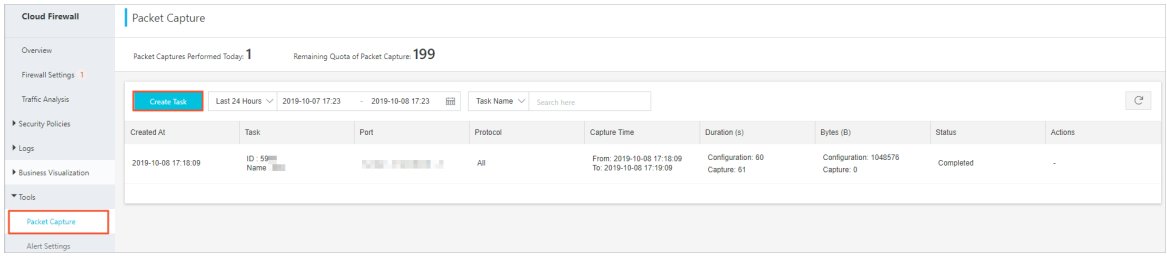
To delete a policy backup, follow these steps: Navigate to the **Policy Backup and Rollback** page, find the target policy, and click **Delete Backup** in the Actions column.

2.Packet capture

This topic describes how to create a packet capture task. You can use the packet capture function to analyze the security of data packets sent by a specific source and identify network security risks.

Procedure

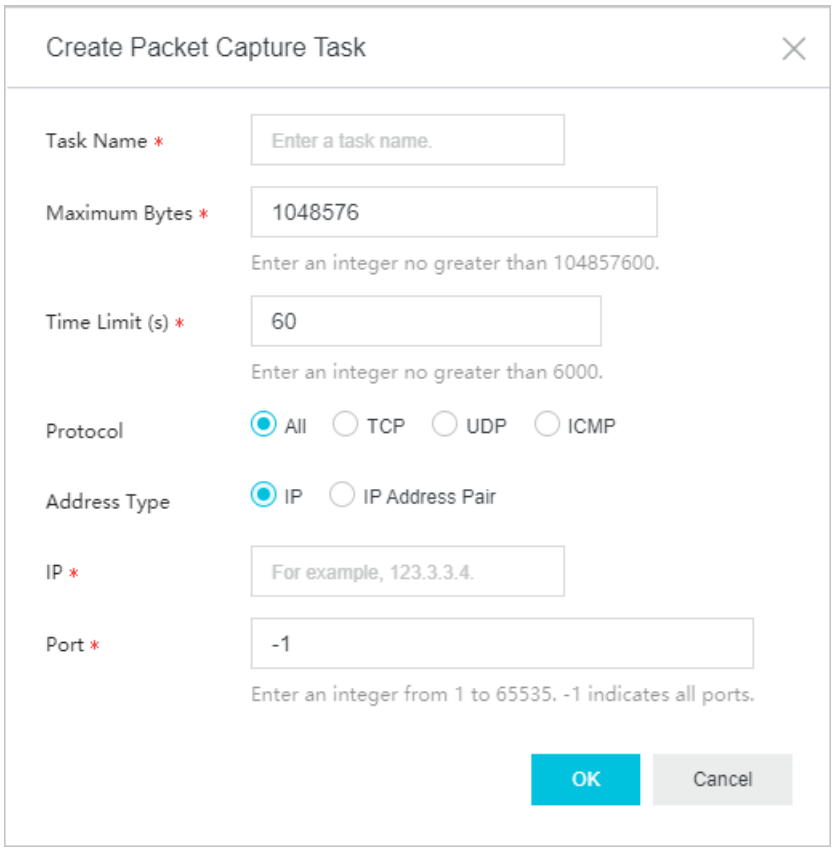
1. Log on to the Cloud Firewall console.
2. Choose **Tools** > **Packet Capture**.
3. Click **Create Task**.



4. In the **Create Packet Capture Task** dialog box that appears, configure the task parameters.

Parameter	Description
Task Name	The name of the packet capture task. We recommend that you use information such as the task purpose to facilitate task management.
Maximum Bytes	The maximum size of a captured data packet in bytes. If the data packet size exceeds the specified value, the packet is discarded.
Time Limit (s)	The maximum time for capturing packets. Unit: seconds.
Protocol	The type of the protocol used to capture packets. Valid values: *All*, *TCP*, *UDP*, and *ICMP*.
Address Type	The IP address type. ○ *IP*: The IP address to be filtered. Only data packets that contain the IP address are captured. ○ *IP Address Pair*: The IP address pair to be filtered. Only data packets that contain the IP address pair are captured.
IP	The IP address to be filtered.
Port	The port number to be filtered.
Peer IP	The peer IP address. **Note** This parameter is specified only when **Address Type** is set to *IP Address Pair*.

Parameter	Description
Peer Port	The peer port number. Note This parameter is specified only when Address Type is set to *IP Address Pair*.



5. Click **OK**.

Result

Choose **Tools** > **Packet Capture**. On the page that appears, you can view the created packet capture task and the task status.

3.Check security group rules

Improper configuration of security group rules may bring security risks. The security check function of Cloud Firewall allows you to check risky security group rules for your ECS instances and provides troubleshooting suggestions. This improves security and efficiency of security groups. This topic describes how to use the security check function in the Cloud Firewall console.

Context

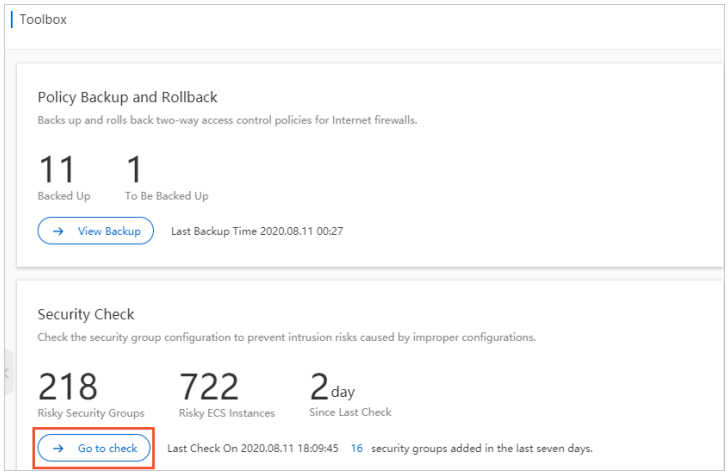
The Premium Edition, Enterprise Edition, and Ultimate Edition of Cloud Firewall support the security check function.

A security group is a virtual firewall that is used to protect ECS instances in Alibaba Cloud. The security check function supports both basic and advanced security groups. For more information, see Overview.

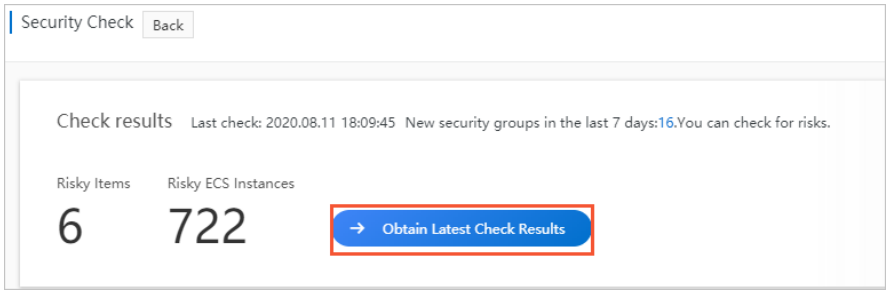
For information about the check items, see Security group checks.

Procedure

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, click **Toolbox**.
3. In the left-side navigation page, click **Toolbox**. In the **Security Check** section, click **Go to check**.



4. (Optional)On the **Security Check** page, click **Obtain Latest Check Results**.The check may take 1 to 5 minutes.



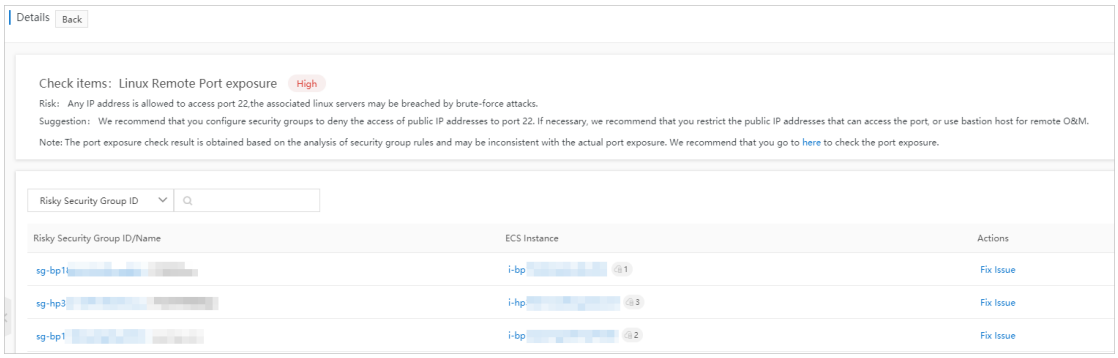
> **Note** The latest check results are obtained based on the static analysis of security group rules and may not cover all port risks. You can view complete check results about port exposure on the Internet access page.

5. In the **Check Result Details** section, view the details of detected security group risks.

You can view the **Risk Level**, **Check Item**, **Risky Security Groups/Servers**, and **Check Item Status** of a security group.

> **Note** You can turn on or off **Check Item Status**.

6. Fix the issue of a check item.
   i. Find the target check item, and click **View Details** in the Actions column.You can also click the number in the **Risky Security Groups/Servers** column to go to the **Details** page.
   ii. On the **Details** page, find the target security group, and click **Fix Issue** in the Actions column.

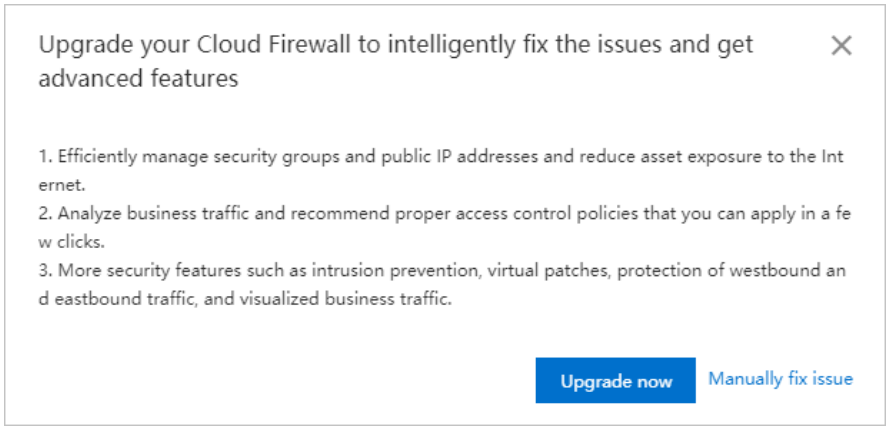


You can also click the security group ID in the **Risky Security Group ID/Name** column to go to the **Security Groups** page of the ECS console and fix the issue.

> **Note** Improper configuration of security group rules may bring severe risks. The **Details** page provides suggestions to fix the issue. We recommend that you modify the risky security group rules based on the suggestions.

Related operations

If you use the Free Edition of Cloud Firewall, after you click **Fix Issue**, you can select **Upgrade now** or **Manually fix issue**.



- **Upgrade now**: You can purchase the Premium Edition or a higher edition and use the **Security Check** function to fix risky security group rules. We recommend that you select this option. You can use Cloud Firewall to centrally manage access control policies of security groups and public IP addresses. This reduces assets exposure and improves efficiency of security management.
- **Manually fix issue**: You are redirected to the **Security Groups** page of the ECS console. You can manually fix the risky security group rules. For more information, see Modify security group rules.

4.Strict mode of the Internet firewall

The strict mode of the Internet firewall blocks traffic that matches an access control policy but contains an application unknown to Cloud Firewall. Cloud Firewall identifies applications based on packet characteristics. If Cloud Firewall fails to identify the application in the traffic, it allows the traffic by default. If you want to discard traffic with unknown applications, you can enable the strict mode.

Context

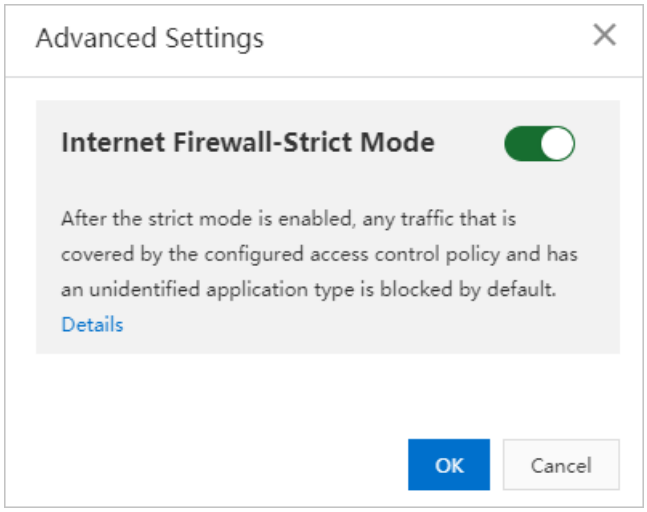
The strict mode only takes effect on traffic that matches an access control policy, regardless of whether the policy action is allow, deny, or monitor. If the traffic does not match any access control policy, the traffic is allowed even if its application is unknown.

Before you enable the strict mode on the Internet firewall, we recommend that you configure access control policies. For more information, see Outbound and inbound traffic control on the Internet firewall.

Enable or disable the strict mode

1. Log on to the Cloud Firewall console.
2. In the left-side navigation pane, choose **Security Policies** > **Access Control**.
3. In the upper-right corner of the **Internet Firewall** tab, click **Advanced Settings**.

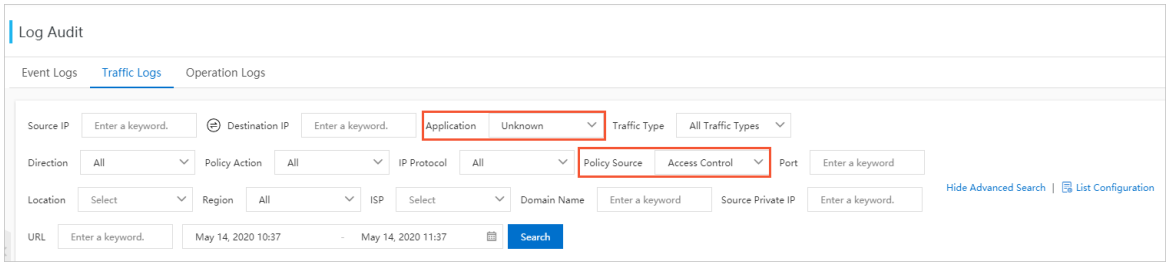
4. In the **Advanced Settings** dialog box that appears, enable or disable **Internet Firewall-Strict Mode** and click **OK**.



After the strict mode is enabled, all traffic that matches an access control policy and contains unknown applications is discarded. You can view 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 **Logs > Log Audit**.
3. Navigate to **Traffic Logs > Internet Firewall** and click **Show Advanced Search**. Then, set **Application** to **Unknown** and **Policy Source** to **Access Control** and click **Search**.



4. View the logs of traffic discarded in strict mode. The policy names of these logs are **unknown_app_deny_all**. You can view the time, source IP addresses, destination IP addresses, and destination ports of the discarded traffic. If normal traffic is discarded, we recommend that you add the application information to the request packets or disable the strict mode.