

Tencent Cloud Firewall

Troubleshooting

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Troubleshooting

Solution for False Alarms and False Positives

Troubleshooting

Solution for False Alarms and False Positives

Last updated : 2024-01-24 16:23:02

This topic describes how to deal with a large number of firewall false positives and an abnormal drop in traffic due to improper strategy changes.

Problem

A large number of legitimate requests from certain IPs are blocked due to false positives of intrusion defense, or an abnormal drop in traffic is caused by improper strategy changes.

Solution

If these requests are blocked by Cloud Firewall, you can disable the blocking feature, allow requests from the blocked IPs, or request support from the product security team.

Steps

Step 1: disable the blocking feature

1. Log in to the [Cloud Firewall console](#), and then click **Intrusion Protection System** in the left navigation pane.
2. Select **Observe** for the protection mode on the intrusion defense page.

Protection mode



Observe 4



Block 13



Strict 0

3. Disable "Enable blocklist" above the blocklist.

The screenshot shows the 'Block List' tab in the Tencent Cloud Firewall console. At the top, there are three tabs: 'Block List', 'Allowed list', and 'Quarantined list'. Below the tabs, there are several controls: a blue 'Add address' button, a 'Delete address' button, a dropdown menu for 'All directions', a dropdown menu for 'Sort by valid date in reverse', and a red-bordered toggle switch labeled 'Enable blocklist' which is currently turned on. To the right of the toggle is a 'Separate keywords' input field. Below these controls is a table with columns: 'IP address', 'Severity...', 'Location', 'Blocked dir...', 'Event source', and 'Effective period'. Two rows of data are visible, both with 'Unknown' severity and 'Edge outbo...' as the blocked direction.

Step 2: manual troubleshooting

1. Log in to the [Cloud Firewall console](#), and then click **Alert Management** in the left navigation pane to enter the Alert Management page.
2. On the Alert Management page, select **Blocked statistics -> Inbound**.
3. On the Inbound tab, select **Sort by blocking statistics** to find the IP address that is falsely blocked.

The screenshot shows the 'Inbound' tab in the Tencent Cloud Firewall console. At the top, there are three tabs: 'Inbound', 'Lateral movements', and 'Outbound'. Below the tabs, there are several controls: a blue 'Open all' button, a 'Block' button, an 'Ignore' button, a dropdown menu for 'All policies', a dropdown menu for 'All statuses', and a 'Separate keywords with "|"; press Enter to' input field. Below these controls is a table with columns: 'Access source', 'Access destination', 'Real-time blocking statistics', 'Location', 'Destination port', 'Last blocked', and 'Avg. blocked frequency'. Two rows of data are visible, both with 'Moscow, Russia' as the location and 'Real-time blocking statistics1' and 'Real-time blocking statistics42' as the statistics.

4. Add the IP address to the allowlist.

Method 1: Click **Allow** on the right side of the falsely blocked IP address to add it to the allowlist (ignore list) and allow access from the IP address.

Method 2: On the [Intrusion Defense](#) page, select **Ignore list -> Add addresses** to add the falsely blocked IP addresses in batches.

The screenshot displays the 'Allowed list' management interface. At the top, there are tabs for 'Block List', 'Allowed list' (which is selected and highlighted with a red box), and 'Quarantined list'. Below the tabs, there are several controls: a blue 'Add address' button (also highlighted with a red box), a 'Delete address' button, a dropdown menu for 'All directions', a dropdown menu for 'Sort by valid date in reverse', and a 'Separate keywords' button. The main area contains a table with the following columns: 'IP/Do...', 'Severity...', 'Locati...', 'Allowed dir...', 'Event source', 'Reason', and 'Effective period'. Two rows of data are visible:

<input type="checkbox"/>	IP/Do...	Severity...	Locati...	Allowed dir...	Event source	Reason	Effective period
<input type="checkbox"/>		Prompt	Issy-le...		Add manually	Others	2022-11-09 15:18:52 to Permanent
<input type="checkbox"/>		Unknown	United...		Add manually	Others	2022-11-09 15:18:52 to Permanent

5. After the above procedures, restore the configuration in [Step 1](#) and observe if the traffic volume returns to normal.

Step 3: submit a ticket to report false positives

1. If the traffic volume is still abnormal after manual troubleshooting, enter the [Submit ticket](#) page and provide your AppID and the falsely blocked IP addresses to the security team.
2. After the feedback is received, the security team will respond within the specified time period and adjust the detection rules.