Tencent Cloud Firewall

Troubleshooting

Product Documentation

Copyright Notice

©2013-2025 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

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by the Tencent corporate group, including its parent, subsidiaries and affiliated companies, as the case may be. 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

©2013-2025 Tencent Cloud International Pte. Ltd.

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.

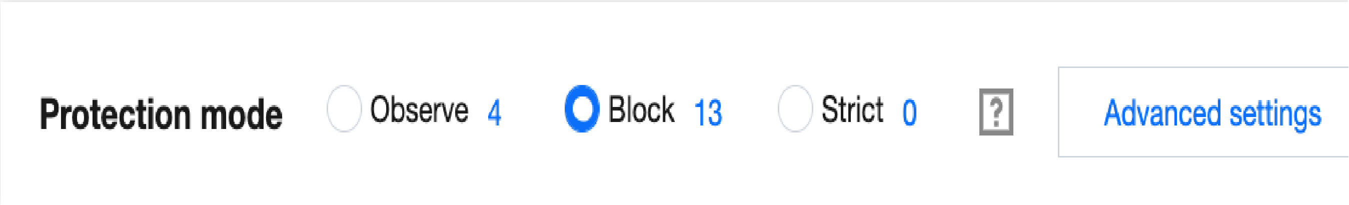
Solution

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

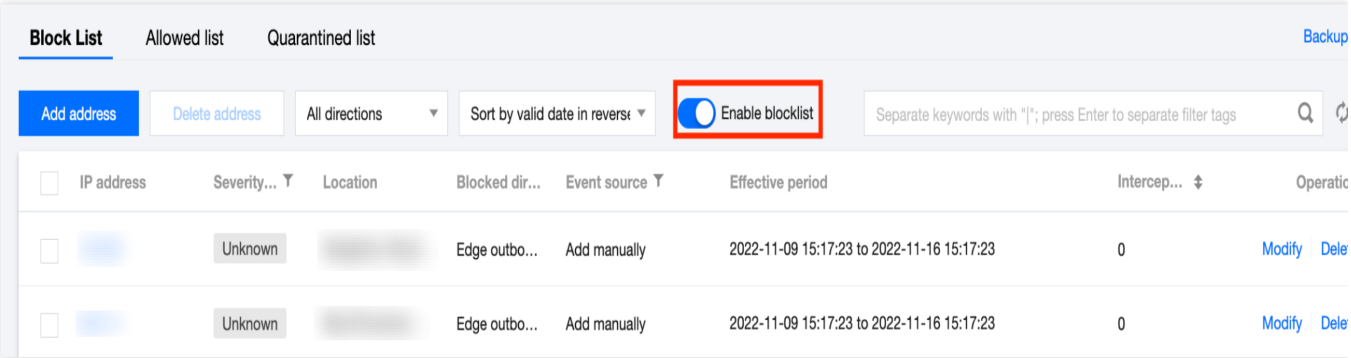
1. Log in to the Cloud Firewall console, and then click **Intrusion Protection System** in the left navigation pane.
2. Select **Observe** for the protection mode on the intrusion defense page.



Protection mode ○ Observe 4 ● Block 13 ○ Strict 0

3. Disable "Enable blocklist" above the blocklist.

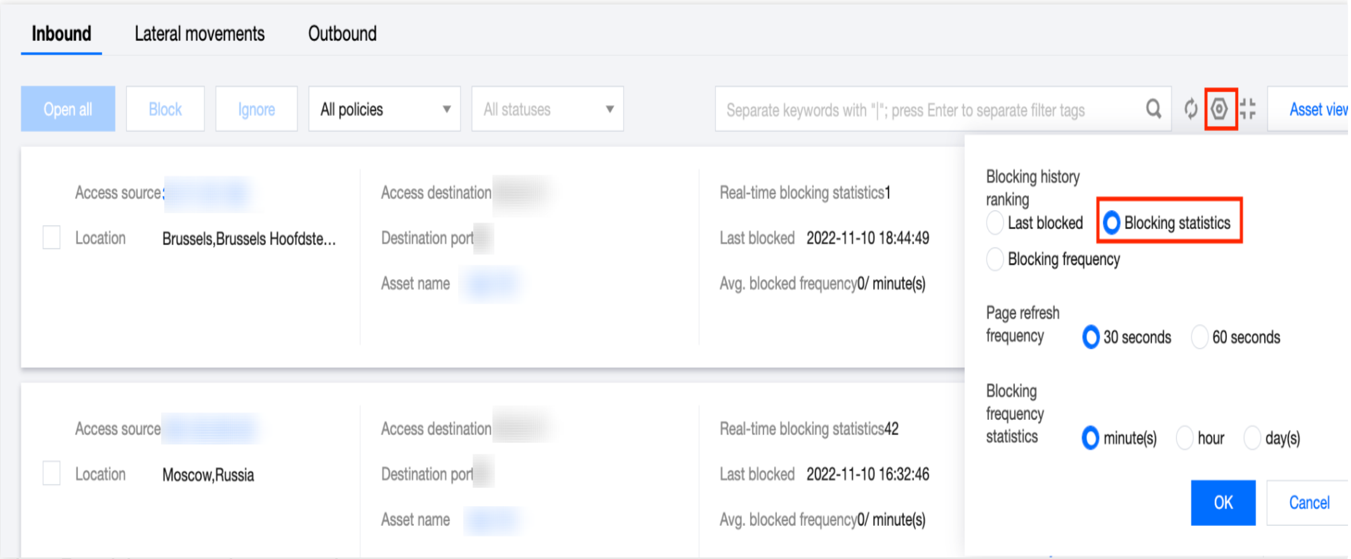
©2013-2025 Tencent Cloud International Pte. Ltd.



	IP address	Severity...	Location	Blocked dir...	Event source	Effective period	Intercep...	Operatio
□	[redacted]	Unknown	[redacted]	Edge outbo...	Add manually	2022-11-09 15:17:23 to 2022-11-16 15:17:23	0	Modify | Dele
□	[redacted]	Unknown	[redacted]	Edge outbo...	Add manually	2022-11-09 15:17:23 to 2022-11-16 15:17:23	0	Modify | Dele

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.



□ Access source [redacted]
Location Brussels,Brussels Hoofdste...
Access destination [redacted]
Destination port [redacted]
Asset name [redacted]
Real-time blocking statistics1
Last blocked 2022-11-10 18:44:49
Avg. blocked frequency0/ minute(s)

□ Access source [redacted]
Location Moscow,Russia
Access destination [redacted]
Destination port [redacted]
Asset name [redacted]
Real-time blocking statistics42
Last blocked 2022-11-10 16:32:46
Avg. blocked frequency0/ minute(s)

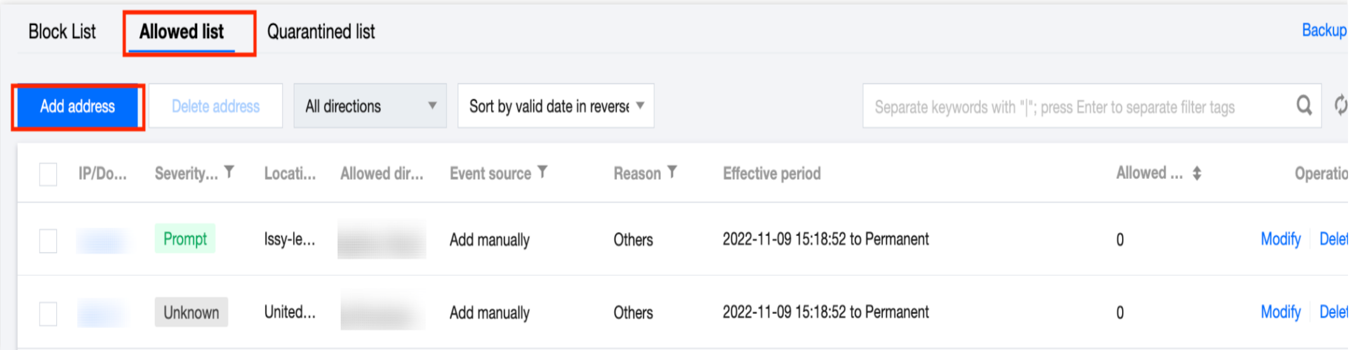
Blocking history ranking: ○ Last blocked ● Blocking statistics ○ Blocking frequency
Page refresh frequency: ● 30 seconds ○ 60 seconds
Blocking frequency statistics: ● minute(s) ○ hour ○ day(s)

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.

©2013-2025 Tencent Cloud International Pte. Ltd.


Block List
Allowed list
Quarantined list
Backup
Add address
Delete address
All directions
Sort by valid date in reverse
Separate keywords with "|"; press Enter to separate filter tags

	IP/Do...	Severity...	Locati...	Allowed dir...	Event source	Reason	Effective period	Allowed ...	Operatio
□	[redacted]	Prompt	Issy-le...	[redacted]	Add manually	Others	2022-11-09 15:18:52 to Permanent	0	Modify Delet
□	[redacted]	Unknown	United...	[redacted]	Add manually	Others	2022-11-09 15:18:52 to Permanent	0	Modify Delet

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.

©2013-2025 Tencent Cloud International Pte. Ltd.