Anti-DDoS

Troubleshooting

Product Documentation

Contents

Troubleshooting
Business IPs Blocked Due to High-traffic Attacks

Last updated：2024-07-01 11:40:46

Issue

The business suffered high-traffic attacks, causing the IP to be blocked and the business to be inaccessible.

Possible causes

The protection traffic threshold is exceeded, leading to blocking.
The attack is still ongoing, so the IP cannot be automatically unblocked.

Solutions

By default, the IP blocking duration lasts for 2-24 hours (subject to the actual situation). In case of a security emergency, you can apply for Anti-DDoS emergency protection.

Business IPs Blocked When DDoS Attack Traffic Doesn't Reach the Threshold

Last updated：2024-07-01 11:40:46

Issue

The attack traffic did not reach the purchased blocking threshold, but the IP was blocked.

Possible causes

You have purchased Anti-DDoS Pro, and the total attack traffic at all network egresses has not reached the purchased threshold, but the IP was blocked. The calculation method is to compare the attack traffic at all network egresses with the purchased threshold.

1. There are two types of blocking based on the location of the blocked node.

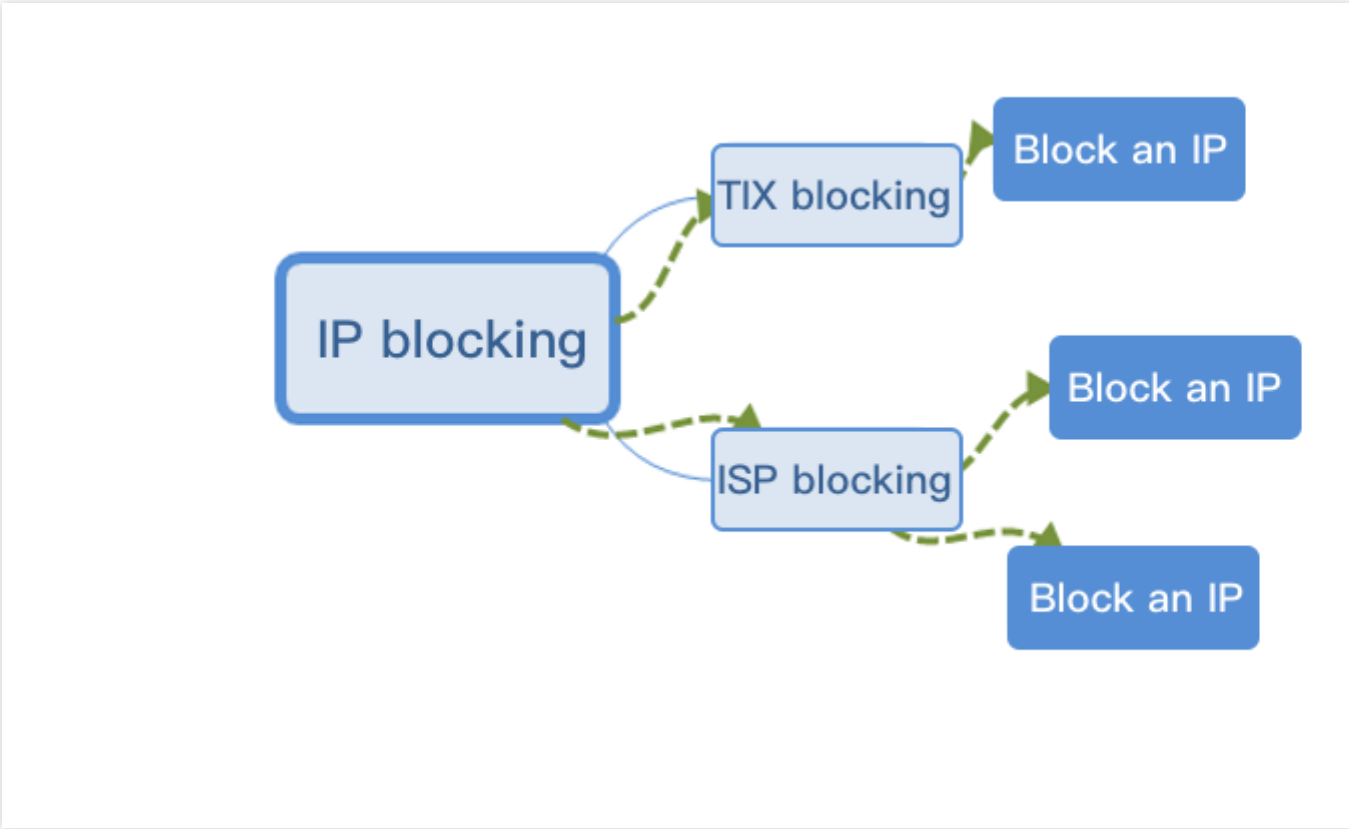
TIX blocking: The IP is blocked by Tencent's egress gateway. The blocking threshold is adjustable.

ISP blocking: The IP is blocked by the ISP. The blocking threshold is basically fixed.

2. In case of ISP blocking, there are two ways of blocking.

Single-IP blocking: When an IP's traffic reaches the single-IP blocking threshold of a certain egress (set according to the egress bandwidth), it will be blocked.

Multi-IP blocking: When the total IDC traffic (attack traffic + business traffic) in a certain detection range exceeds the multi-IP blocking threshold, multi-IP blocking will be triggered.



Solutions

After the attack is over, you can perform manual unblocking or wait for auto unblocking.

Troubleshooting the Issue

1. Log in to the Anti-DDoS console and click **Unblocking Service** on the left sidebar to view the remaining number of times of manual unblocking.
If the remaining number of times of manual unblocking is 0, proceed to Step 5 or wait for auto unblocking.
Otherwise, proceed to Step 2.
Note:
For more information on the auto unblocking time, please see the **Estimated unblocking time** value on the Unblocking Service page in the console.

2.
Check whether the attack has stopped by clicking Overview.

If yes, proceed to Step 3.
If no, continue the unblocking operation and perform Step 3 after the attack is over.

Note:
If the attack persists, you cannot perform unblocking, and you need to wait for the attack to end before manual unblocking or auto unblocking.
3.
On the left sidebar, click **Unblocking Service**.

4. On the **Unblocking Service** page, find the protected IP in the **Auto Unblocking** status and click **Unblock** in the **Operation** column on the right.
5.
The suggestions for users of different Anti-DDoS services are as follows:

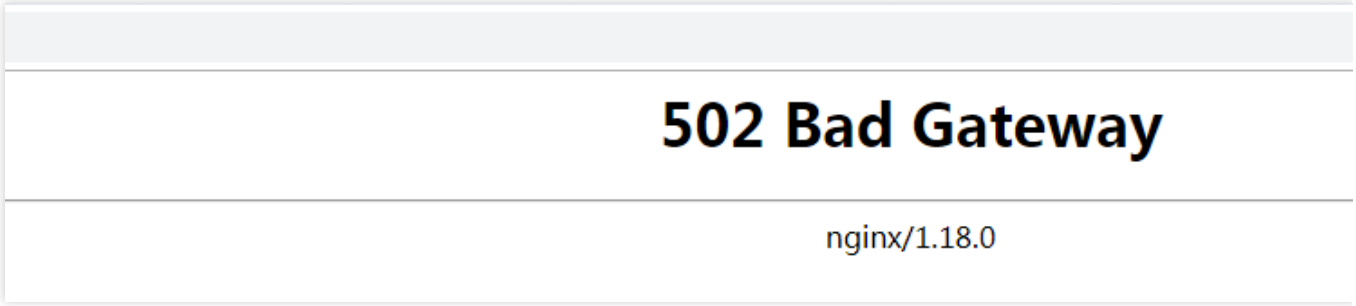
If you use Anti-DDoS Basic, we recommend you purchase Anti-DDoS Pro (available in Guangzhou, Shanghai, and Beijing regions). Then, you can perform unblocking when binding devices for the first time.
If you use Anti-DDoS Pro or Advanced, we recommend you upgrade your protection package so as to increase the number of protected IPs or times of protection and perform unblocking earlier.

How to Fix a 502 Bad Gateway Error

Last updated：2024-07-01 11:40:46

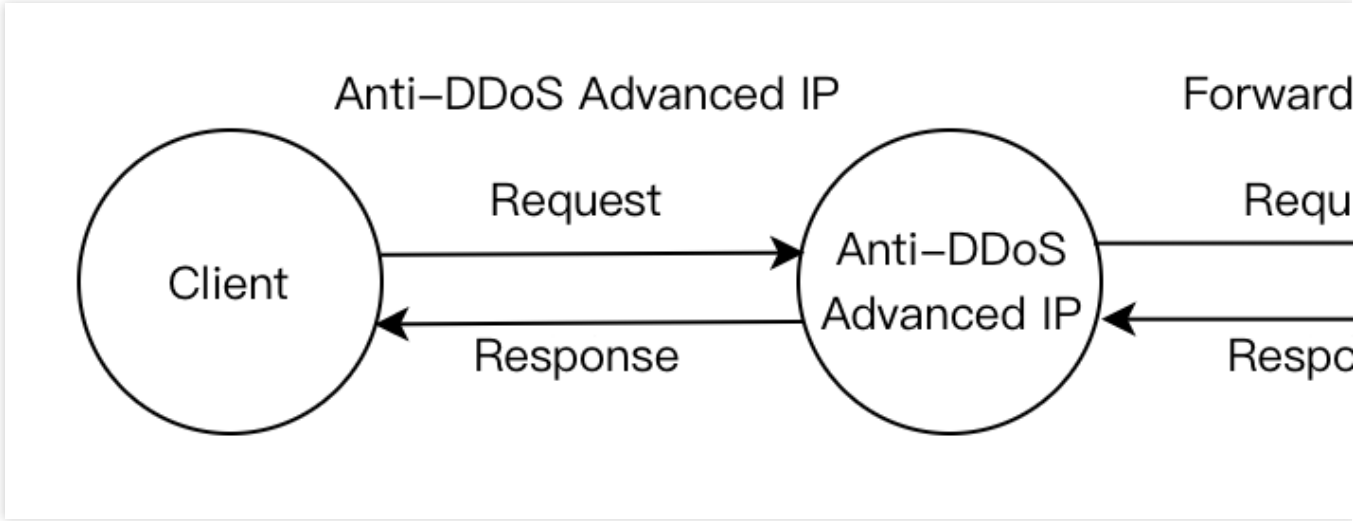
Issue

A 502 Bad Gateway error occurs when you are using Anti-DDoS Advanced, as shown below:



Possible causes

The following figure shows how the business traffic flows:



Cause 1: The forwarding IP is blocked by the real server or limited to a specific rate.

After you connect to Anti-DDoS Advanced, Anti-DDoS Advanced will process access requests as a proxy for the real server and send received requests to the real server using the forwarding IP instead of the client IP. Thus, the real server IP becomes invisible to the client. However, the number of forwarding IPs is insufficient to handle volumes of access requests.

If the real server is configured with protection policies, it is possible to trigger corresponding policies to limit the rate of the forwarding IP and even block it.

Cause 2: The real server works abnormally, causing a response timeout.

Possible reasons:

1. The real server IP is not connected to Anti-DDoS Advanced and crippled by malicious attacks.
2. A failure occurs to the data center of the real server.
3. High memory and CPU usage lead to weakening performance.
4. Web programs such as Apache and Nginx are abnormal.
5. The forwarding linkage between the public network and the real server is faulty.

Cause 3: There is network jitter or faulty linkage.

The poor public network quality affects the stability of business access and a 502 error is returned.

Solutions

Solution to cause 1

Test whether access to the real server IP and the Anti-DDoS Advanced forwarding IP is normal through the Cloud Automated Testing (CAT) platform. For the testing method, see here.
If only the real server IP works normally, the forwarding IP is blocked by the real server or is rate-limited. We recommend you add the forwarding IP to your allowlist.

For more details, see Instructions for cause 1.

Solution to cause 2

Modify the local host resolution result to the real server to check whether the real server works normally. Firstly, edit the `hosts` file and ensure that the binding in the file has taken effect. Then use your domain name to check whether the real server can be accessed normally. If the access fails, perform the following steps:

1. Protect the real server IP, as instructed in Measure 1.
2. Ask for technical support to troubleshoot the data center, as instructed in Measure 2.
3. Check whether the web service is normal and restore it if it works abnormally, as instructed in Measure 3.
4. Check whether performance metrics such as the server process occupancy and memory usage are normal, and restore them to normal, as instructed in Measure 4.
5. Check the network layer. Alternatively, check the linkage status or change to another linkage. You can refer to Measure 5.

For more details, see Instructions for cause 2.

Solution to cause 3

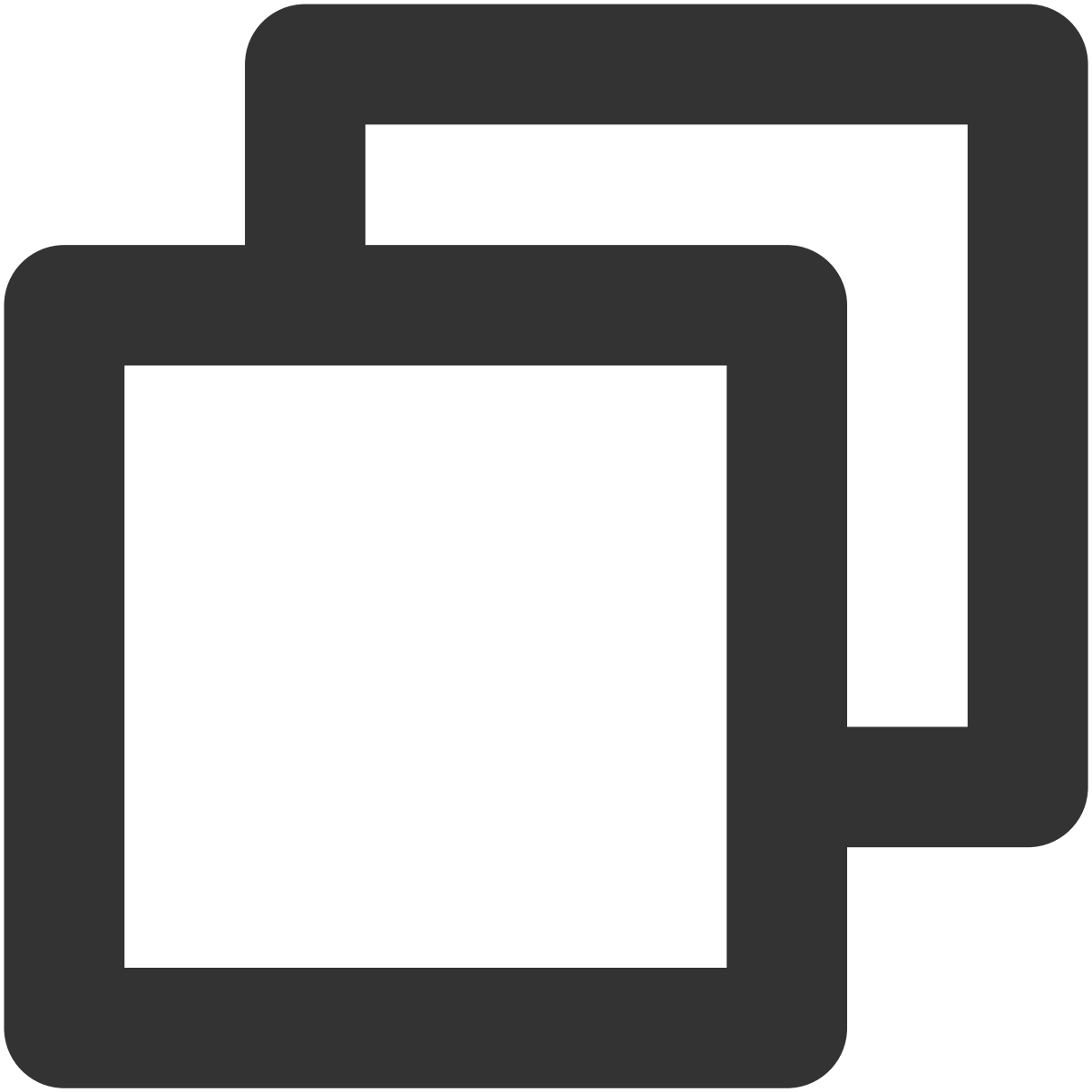
Check whether there is a linkage failure and contact the ISP for repair.

For more details, see Instructions for cause 3.

Troubleshooting

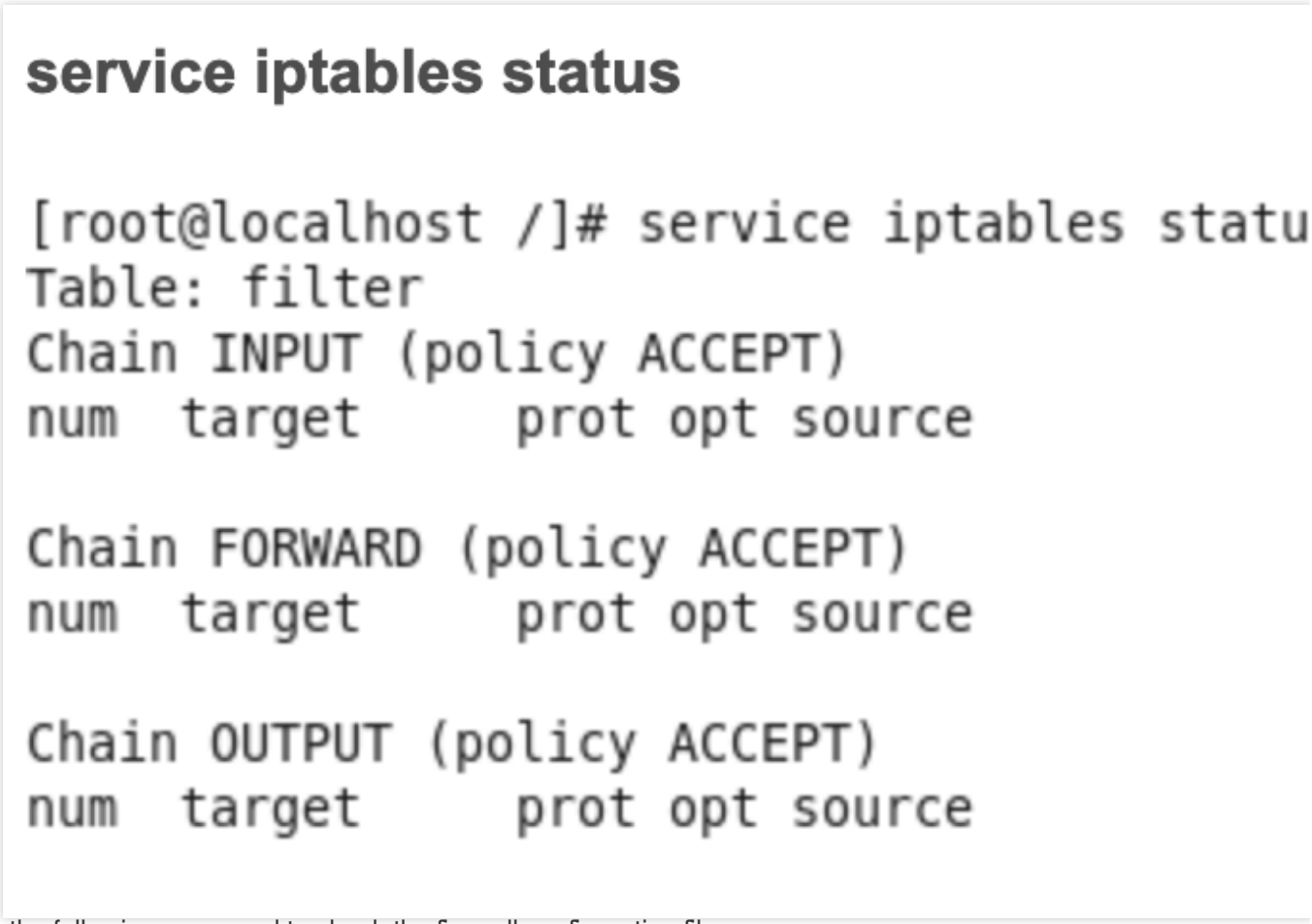
Instructions for cause 1

Add the forwarding IP range of Anti-DDoS Advanced to the firewall and host security software allowlists. Here, let's take the firewall of CentOS 6.5 as an example:
1. Run the following command to check the Linux firewall status.

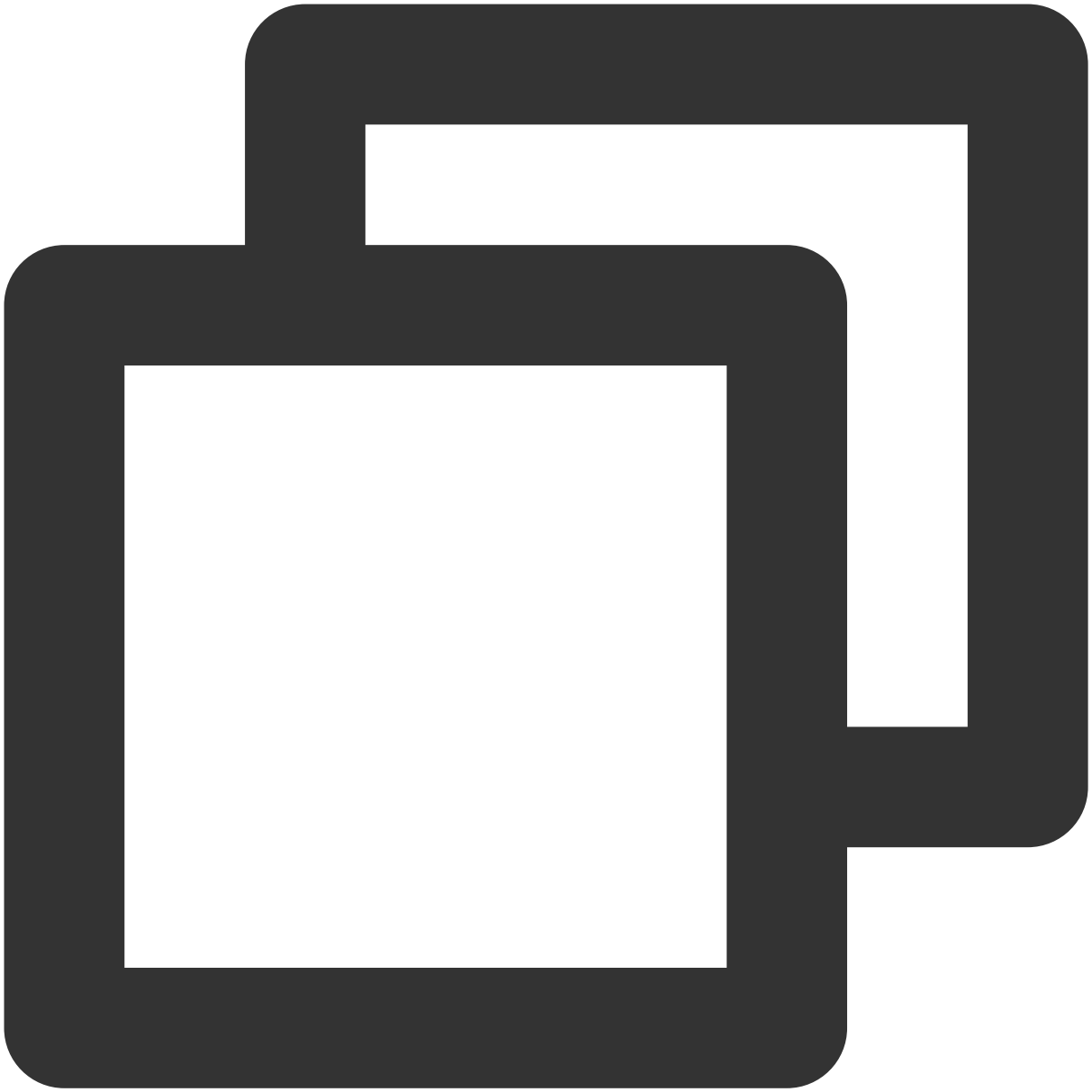


```
service iptables status
```

If there are no rules for Chain INPUT, Chain FORWARD, and Chain OUTPUT displayed in the console, the firewall is not yet started.



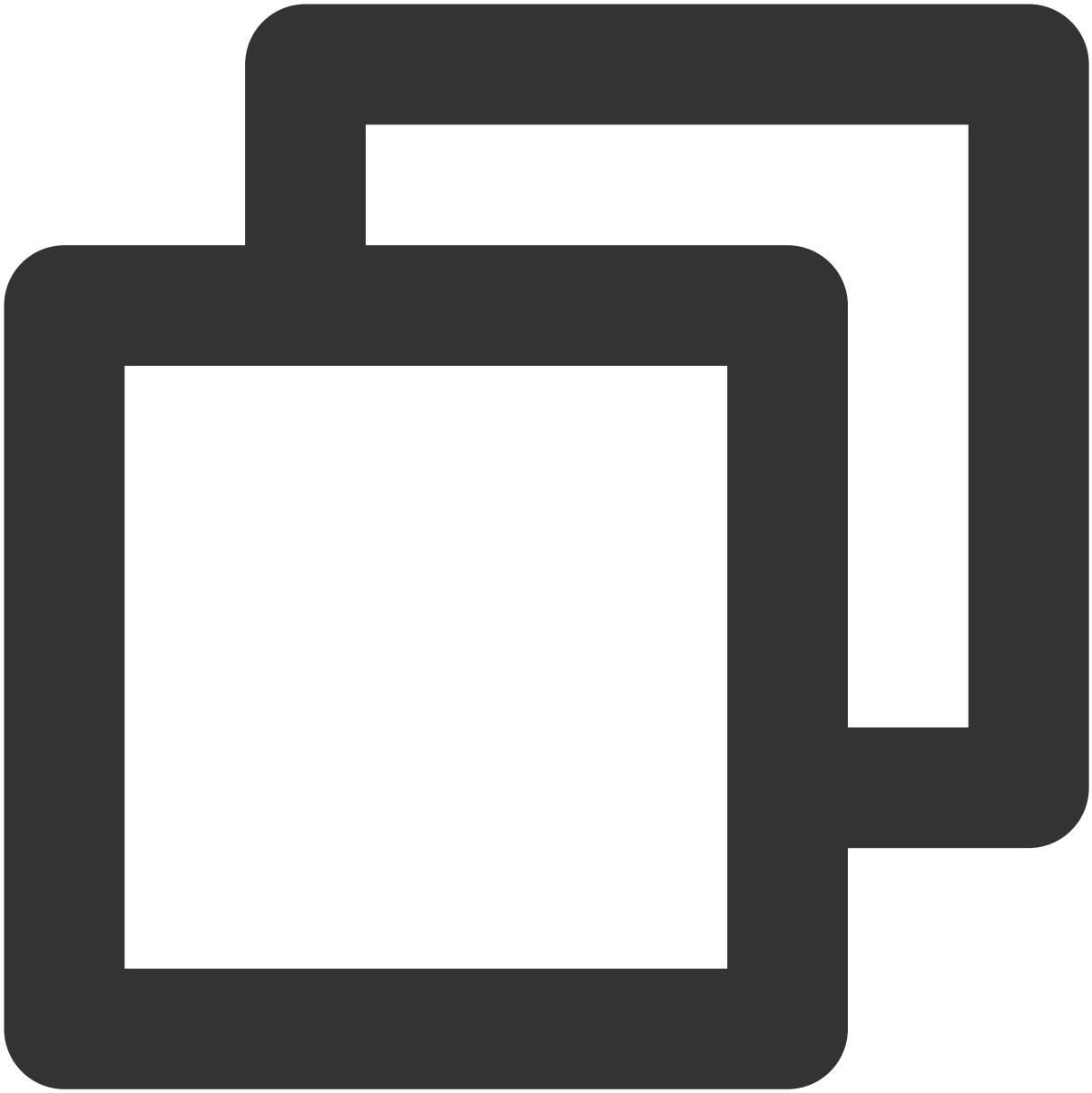
2. Run the following command to check the firewall configuration file.



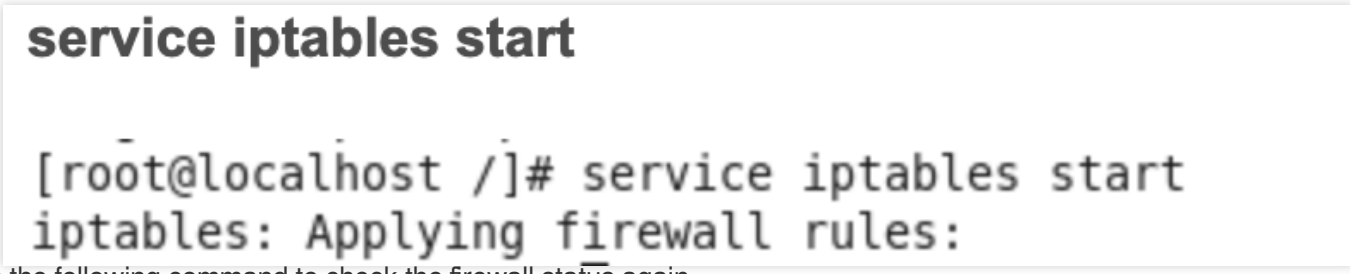
```
cat /etc/sysconfig/iptables
```

Make sure that you have completed the blocklist and allowlist configuration before you start the firewall.

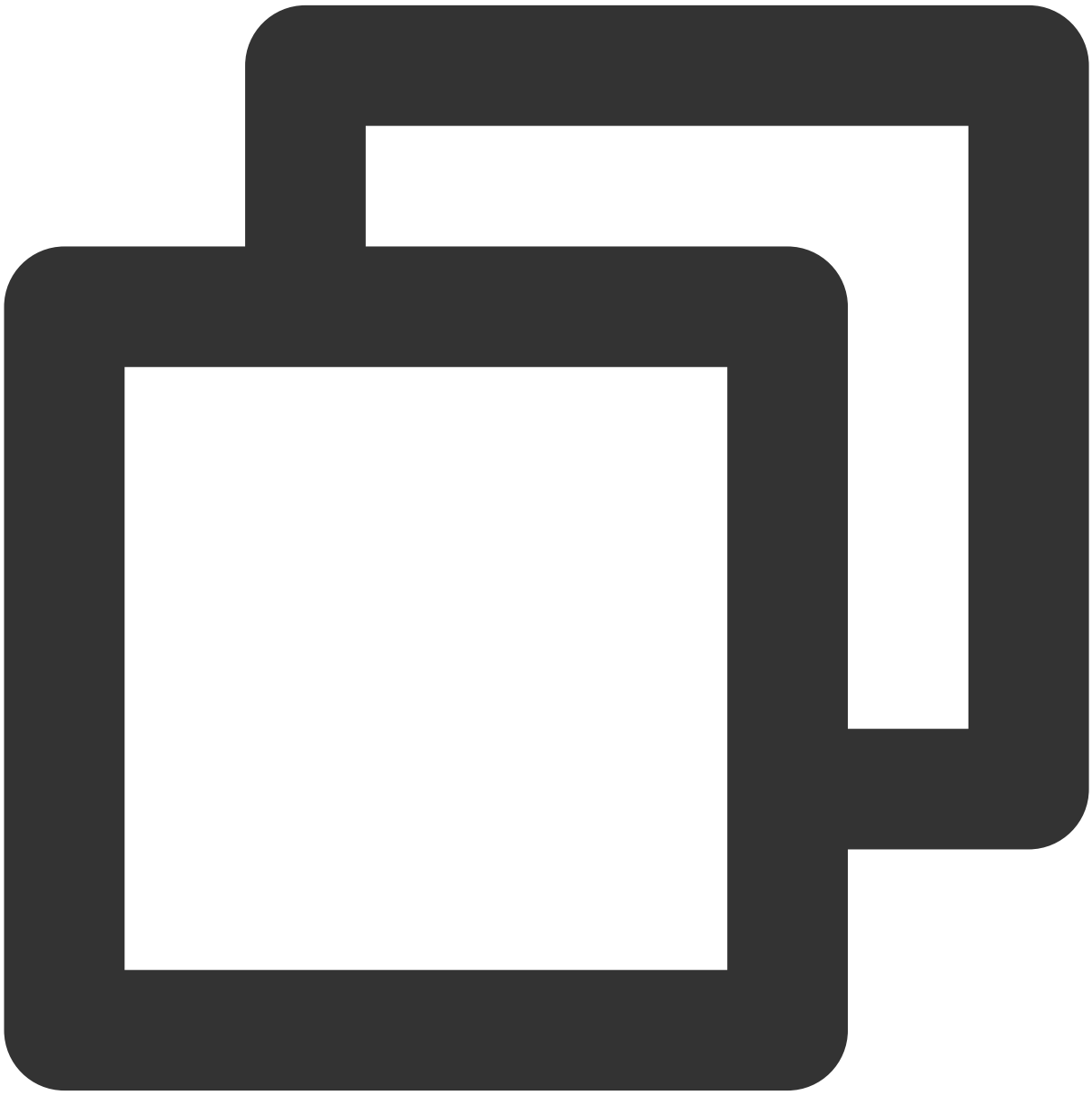
3. Run the following command to start the firewall.



```
service iptables start
```



4. Run the following command to check the firewall status again.

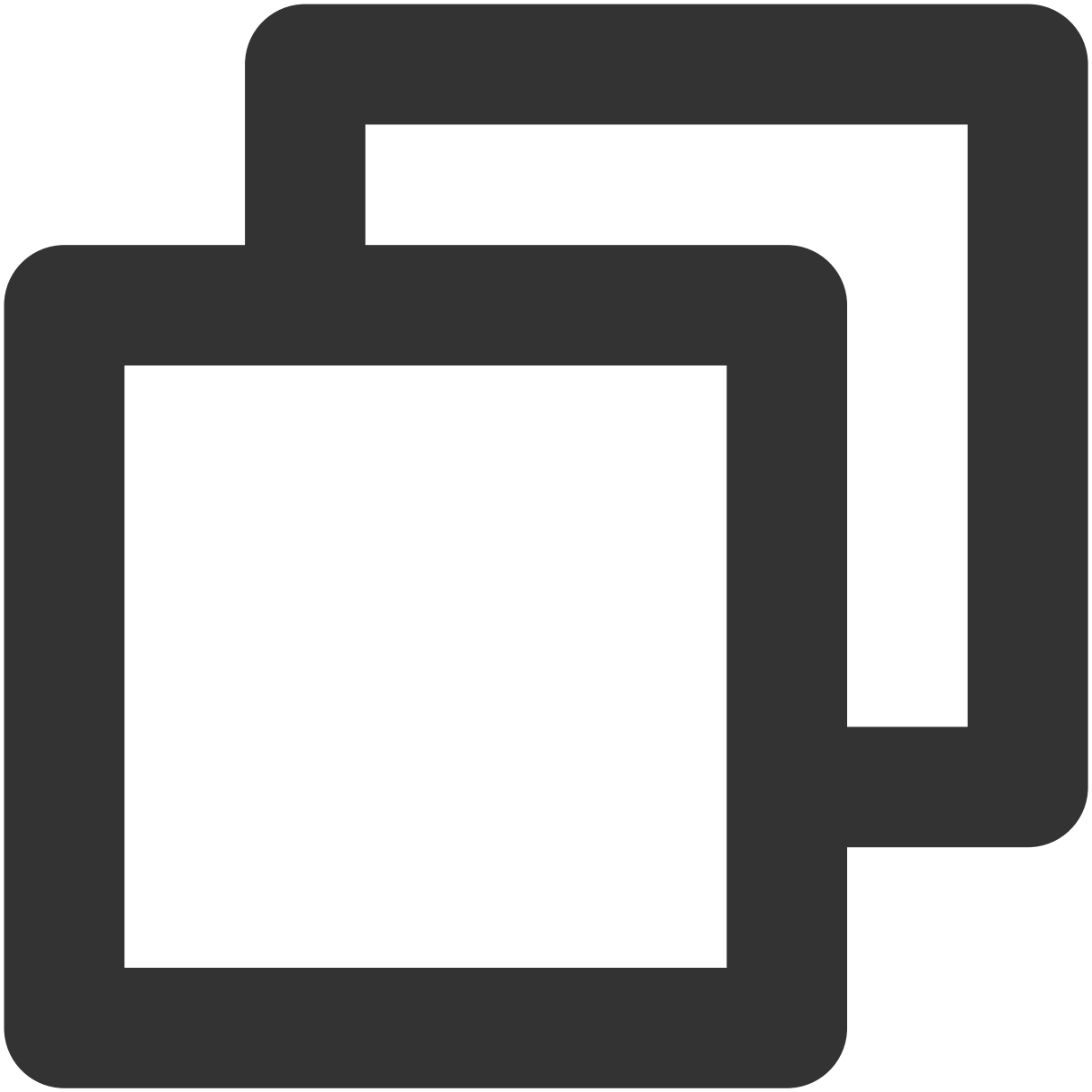


```
service iptables status
```

If any rules for Chain INPUT, Chain FORWARD, and Chain OUTPUT are displayed in the console, the firewall is started successfully.

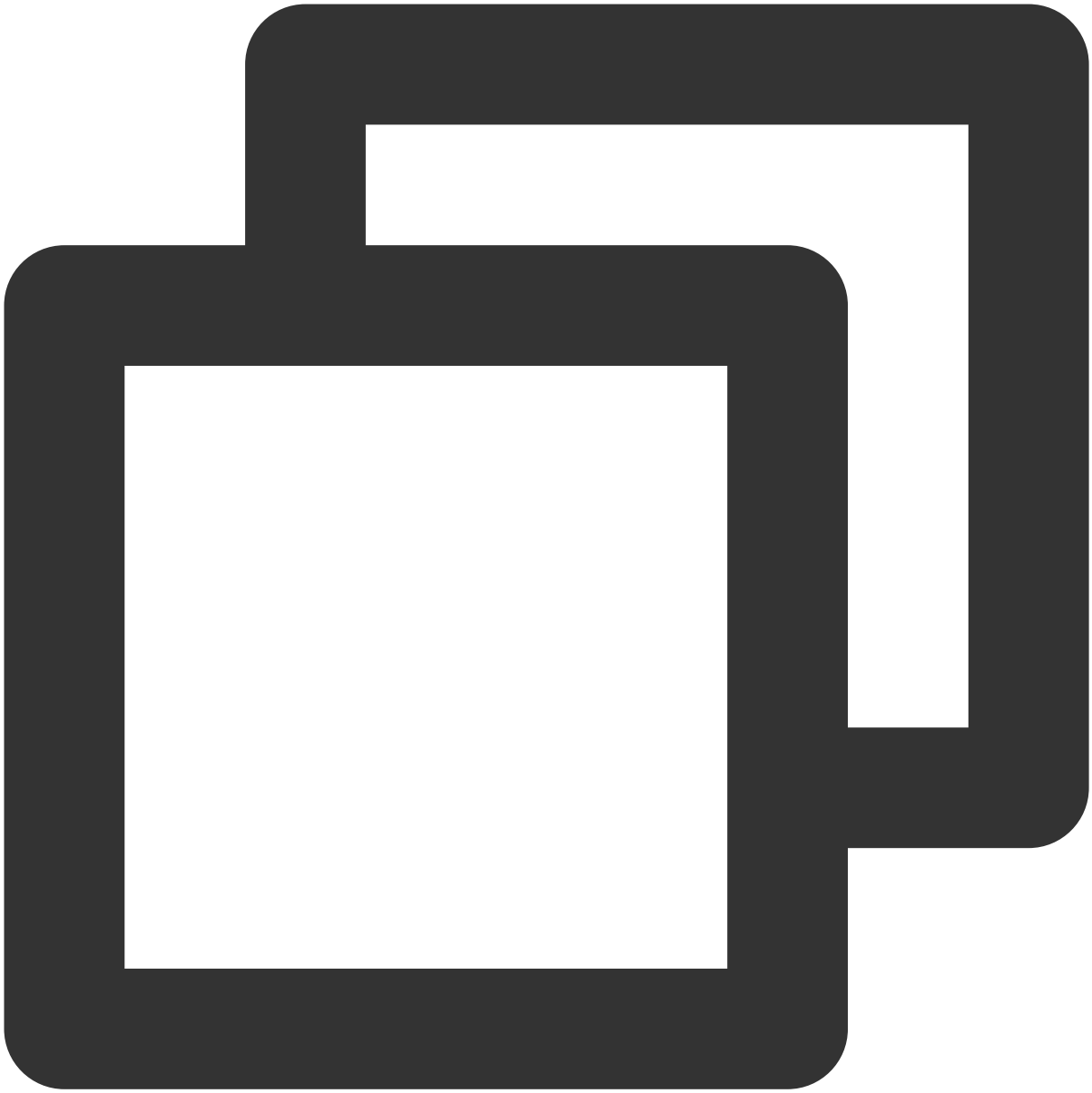
```
[root@localhost /]# service iptables status
Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ESTABLISHED
2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
3    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
4    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0
dpt:22
5    REJECT     all  --  0.0.0.0/0            0.0.0.0/0
mp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     all  --  0.0.0.0/0            0.0.0.0/0
mp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
```

5. Run the following command to add the forwarding IP range to the firewall allowlist.



```
Iptables -A INPUT -s Forwarding IP -j ACCEPT
```

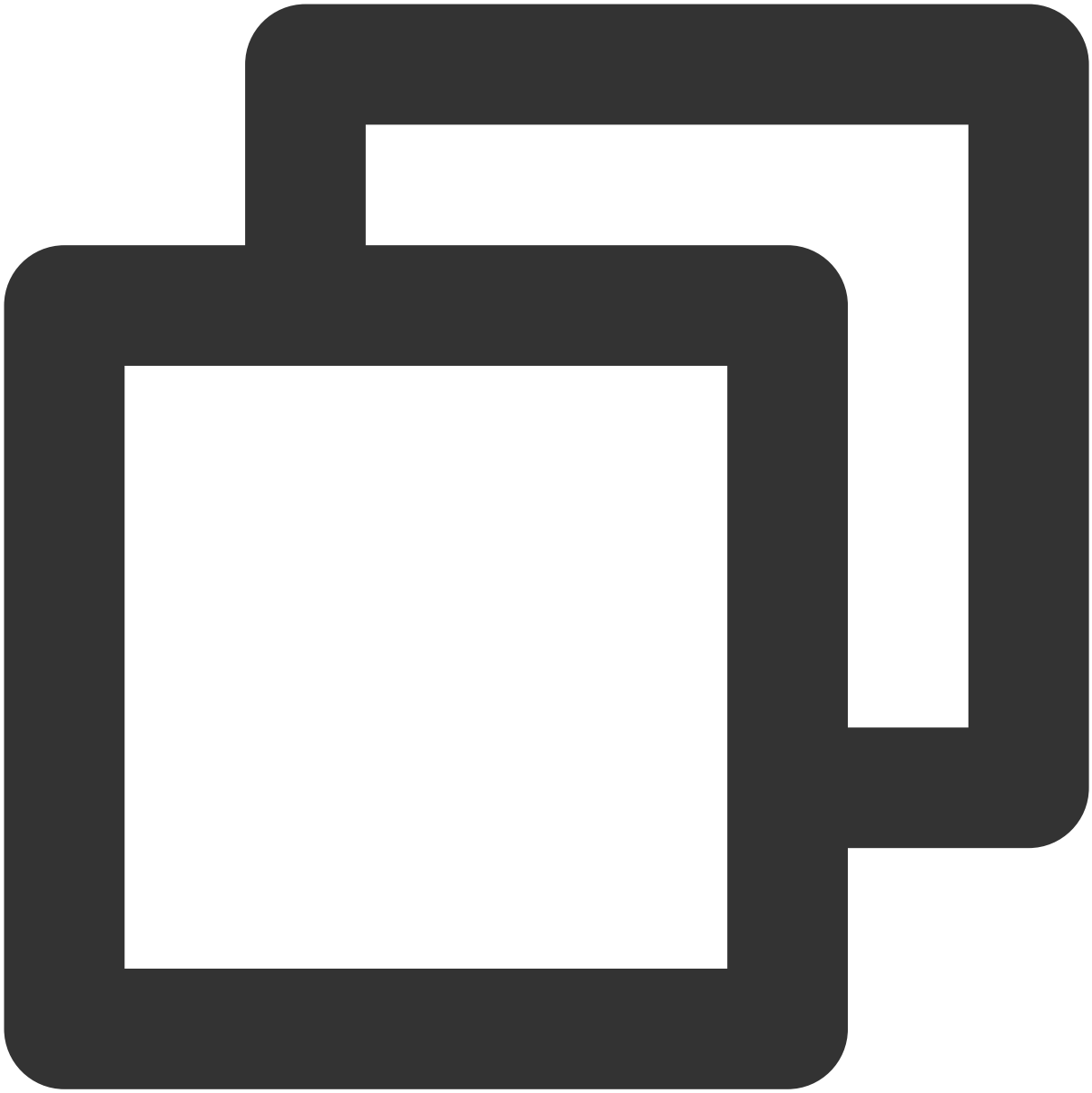
6. Run the following command to check whether the configured allowlist policy is added to the firewall settings.



```
iptables -nL --line-number
```

The allowlist policy is added successfully if there are firewall rules in the output.

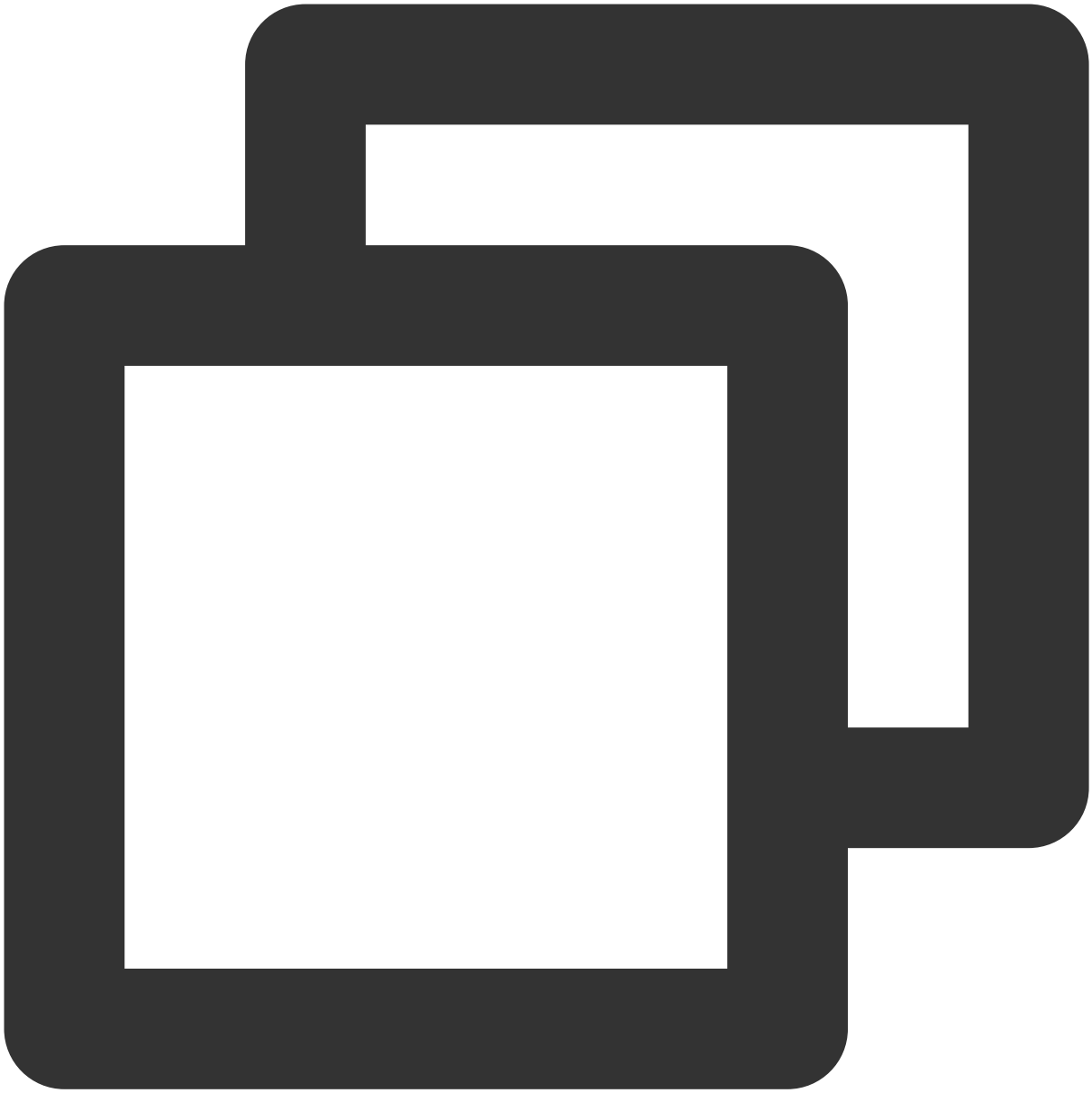
7. Run the following command to save the firewall settings.



```
service iptables save
```

```
[root@localhost /]# service iptables save
iptables: Saving firewall rules to /etc/sysconf
```

8. Run the following command to restart the firewall to have the configuration take effect.



```
service iptables restart
```

```
[root@localhost /]# service iptables restart
iptables: Setting chains to policy ACCEPT: filt
iptables: Flushing firewall rules:
iptables: Unloading modules:
iptables: Applying firewall rules:
```

Instructions for cause 2

Modify the local host resolution result to the real server to check whether the real server is normal. Firstly, modify the local `hosts` file. The specific steps are as follows:

1. Edit the local `hosts` file to allow local requests to the protected business domain name to reach the real server. The following uses the Windows OS as an example to configure the local `hosts` file:

Open the `hosts` file in `C:\\Windows\\System32\\drivers\\etc` , and add the following content at the end of the file:

```
<源站 IP 地址> <被防护网站的域名>
```

For example, if the real server IP is `10.1.1.1` and the domain name is `www.qqq.com` , add:

```
10.1.1.1        www.qqq.com
```

Save the `hosts` file. Run the ping command to ping the protected domain name on the local computer.

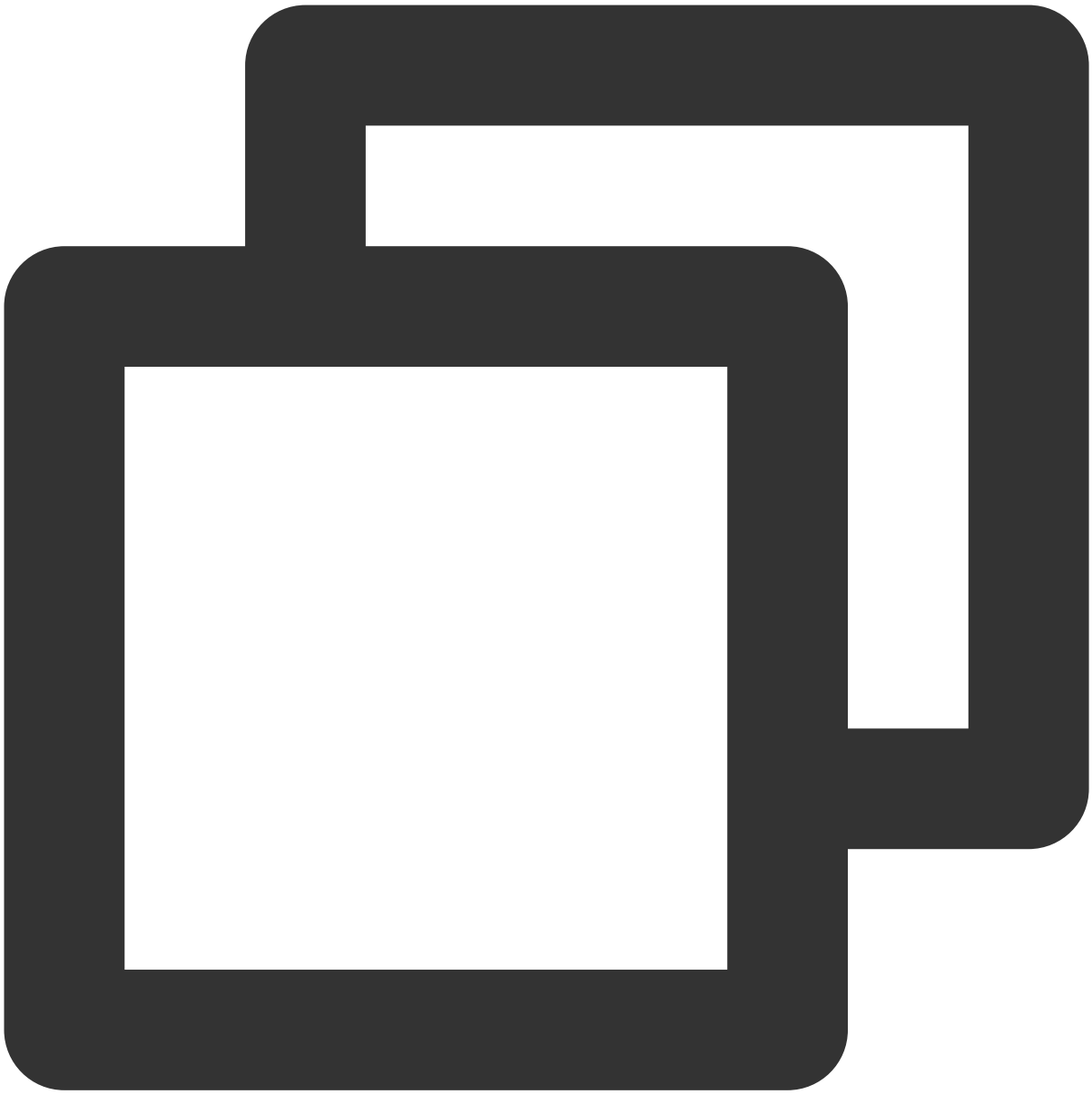
If the resolved IP address is the real server IP address bound in the `hosts` file, the file has taken effect. Otherwise, run `ipconfig /flushdns` in the Windows command prompt to refresh the local DNS cache.

2. After confirming the binding in the 'hosts' file has taken effect, check whether access to the real server is normal using the domain name. If the real server cannot be accessed normally, the following measures can be taken.

Measure 1: Protect the real server IP.

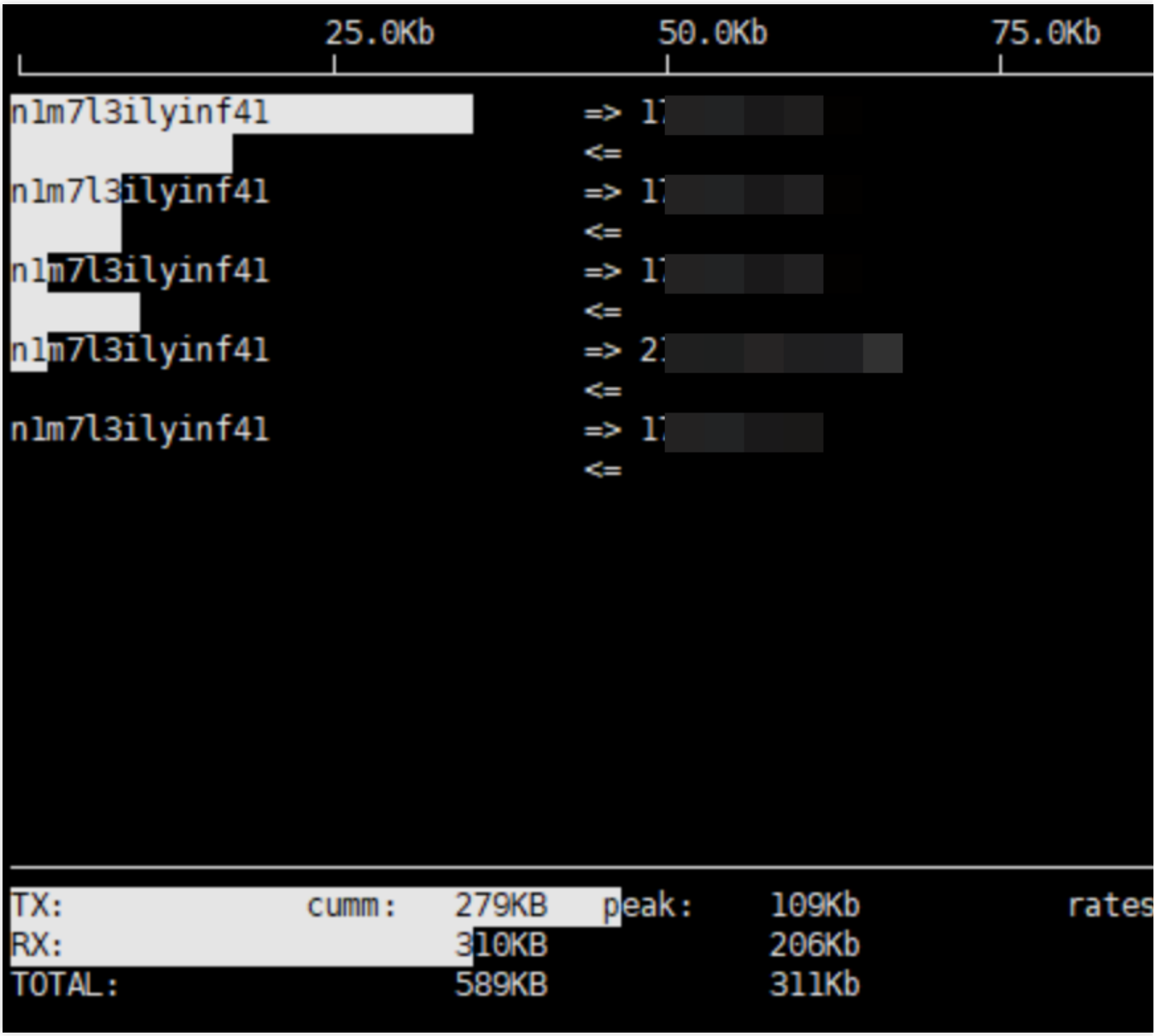
Check whether the real server has a significant increase in traffic and request volume, and the monitoring data from the Anti-DDoS Advanced console. The following describes how to check the real server traffic volume when the OS is CentOS.

1. Check the traffic usage of a Linux server using iftop:



```
Run the command `iftop [-i interface]`. The parameter `interface` indicates the API
```

The output is as follows:



Output description:

The bandwidth usage is displayed at the top.

The external connection list is in the middle. The list records IPs that are connecting to the local network.

On the right of the list is the real-time traffic information, which is the average traffic of 2 seconds, 10 seconds, and 40 seconds when the real server is accessed.

`=>` means sending data and `<=` means receiving data.

The bottom three lines:

In the first column, `TX` stands for sending traffic, `RX` for receiving traffic, and `TOTAL` for total traffic.

In the second column, `cumm` stands for the total traffic in the first column.

In the third column, `peak` stands for the peak traffic in the first column.

In the fourth column, `rates` stands for the average traffic for each period of 2 seconds, 10 seconds, and 40 seconds.

2. For instructions on how to view business traffic in the Anti-DDoS Advanced console, see Protection Overview.
If the real server is attacked by a large amount of traffic without any exceptions displayed in the Anti-DDoS Advanced console, the attacks might have bypassed Anti-DDoS Advanced. You can refer to **In Case of Real Server IP Exposed** to deal with this situation.

Measure 2: Ask for technical support to troubleshoot the data center.

You can check whether the data center has physical hardware failures, such as failures with power, network interface card, drive, memory, and wiring.

Measure 3: Check the web service.

Check the monitoring data of the real server, such as CPU usage, memory usage, and bandwidth usage.
Note:
Normally, if the usage of CPU or memory exceeds 90% for a long time, the web service is in abnormal status.
You need to compare the bandwidth usage with business process occupancy during normal periods to see if there is a significant increase. For more details, see **CVM Bandwidth Utilization Is Too High**.
If there is an exception, please contact technical support for further troubleshooting.

Measure 4: Check server performance parameters such as server process occupancy and memory usage.

Check the web program status. Run the `ps -C nginx -o pid` command to check whether the server's nginx process is running normally.
If there is an exception, please contact technical support for further troubleshooting.

Measure 5: Check the network layer or the linkage status.

Run a check on the linkage quality, linkage connectivity, and forwarding status of the intermediate network equipment between the public network and the real server. You can also verify and avoid the issue by changing to another linkage.

Instructions for cause 3

Check and monitor the public network quality of the real server IP and the Anti-DDoS Advanced forwarding IP through the CAT platform. For the monitoring method, see here.
If the public network is not working well, contact the ISP for assistance.

"No ICP filing" Prompted During Domain Name Connection

Last updated：2024-07-01 11:40:46

Issue

The system prompted that my domain name had no ICP filing when I tried to connect it to Anti-DDoS Advanced.

Possible causes

The domain name does not have an ICP filing from the MIIT

Pursuant to the State Council Decree No.292 "Administrative Measures for Internet Information Services" and the "Measures for the Archival Administration of Non-operational Internet Information Services", China implements a licensing system for operational internet information services and filing system for non-operational internet information services. Internet information services shall not be provided before the license or filing is obtained; otherwise, it would be illegal.

Therefore, any website providing services in the Chinese mainland must first apply for ICP filing, and the website can be launched for access only after the ICP filing number is obtained from the competent communications administration.

The ICP filing information was not synced in time

If your domain name has been successfully filed with the MIIT, but the system prompted that the domain name has no ICP filing, it may be because that the ICP filing information of the MIIT has not been synced to the Tencent Cloud website ICP filing system.

Troubleshooting

The domain name does not have an ICP filing from the MIIT

You can use the Tencent Cloud website ICP filing service to submit an application. After the application is successful and the ICP filing number is obtained from the competent communications administration, your domain name can be

connected to Anti-DDoS Advanced.

Note:

If you have already applied for an ICP filing at another service provider, please consult the provider accordingly.

The ICP filing information was not synced in time

After you get your ICP filing, it takes some time to sync the information from the MIIT to the Tencent Cloud ICP filing management system. Please wait 24 hours and try again.

A public IP suffered DDoS attacks

Last updated：2024-07-01 11:40:46

Problem

DDoS attacks overwhelm your business with massive amounts of traffic, exhausting the server performance and network bandwidth and thus crashing down the server.

Common Cause

Tencent Cloud's free basic protection capability (2 Gbps) is not enough to defeat the DDoS attacks.

Solutions

Replace a public IP (expedient)
When attackers start DDoS attacks against your specific business IP, you can avoid the blocking trouble temporarily by replacing the attacked IP with a new one. However, the new IP is still exposed to DDoS attacks, causing potential business interruptions.
Get an Anti-DDos product (recommended)
By getting an Anti-DDoS instance, you can improve IP protection capability to defend against large traffic attacks. If the Anti-DDoS Pro instance of the region is unable to defeat massive attack traffic, you can use an Anti-DDoS Advanced instance with greater protection capability as needed.

Directions

Replace a public IP (expedient)
The use limits are as follows:
Each account can change public IP addresses in the same region a maximum of 3 times per day.
Each instance can only change its public IP once.
The old public IP will be released after it is replaced.
For details, see Changing Public IP Addresses.
Get and set an Anti-DDoS product (recommended)
To learn more about purchasing and configuring an Anti-DDoS Pro instance, see Purchase Directions and Getting Started.

To learn more about purchasing and configuring an Anti-DDoS Advanced instance, see Purchase Directions and Getting Started.

For details on differences between Anti-DDoS Pro and Anti-DDoS Advanced instances, see Comparison of Anti-DDoS Protection Schemes.