Table of Contents

Firewall

The cPanel servers make use of various firewalling features

`dev.beacontechnology.com` uses CSF to manage the Linux firewall (iptables).

`chost.beacontechnology` uses `Host Access Control` to manage the Linux firewall (nftables).

cPHulk

`cPHulk` is part of cPanel and will ban IPs that log too many login failures. `cPHulk` does not normally completely firewall off blocked IPs, and instead only blocks them from logging in. This is fixed by a custom script that imports these rules into nftables on a schedule.

`cPHulk` has a whitelist, blacklist and country management feature. These are managed by the user.

The script that dumps the whitelist and country blacklist, and imports them into `nftables`.

`/etc/cron.daily/update_firewall.sh`

Whitelist Management

In general it is a good idea to whitelist administrative IPs to avoid getting banned.

To do so:

1. Go to WHM > cPHulk Brute Force Protection
2. Click on Whitelist Management tab
3. If logging in from an IP not on the list, there might be a popup with a button that can be pressed to add the current IP to the list.
4. If not, add the IP to the box and put a comment with # character if needed.
5. When done, click “Add”

To remove an IP from the whitelist, just click delete from the same interface.

Additionally, IPs added to the whitelist may be included as administratively allowed IPs in nftables by the `/etc/cron.daily/update_firewall.sh` script.

Blacklist Management

Sometimes the user might be banned, or can't connect to a specific service for some unknown reason. It could be cPHulk blocking them.

To unblock:

1. Go to WHM > cPHulk Brute Force Protection

2. Click on Blacklist Management tab
3. Search for the IP in question, if the IP is unknown, ask the user to go to: ipecho.net and read the IP back.
4. When the record is located, click “Delete”

Host Access Control

New instructions:

CSF is no longer necessary, a basic firewall solution now comes with cPanel and is called `Host Access Control`.

`Host Access Control` provides a basic firewall interface that integrates with Linux nftables.

The current rules can be viewed by going to WHM > Host Access Control

Host Access Control is very basic and does not natively handle expressions like “any port”, and so some rules say “undefined” for certain parts. This just means that the rule was manually added to `/etc/sysconfig/nftables.conf`

To Add new rules:

1. edit: `/etc/sysconfig/nftables.conf`
2. Scroll the sections where it says `chain cPanel-HostAccessControl`
3. Please copy an existing rule and edit it to what is needed.
4. When done, save and exit
5. run the command: `systemctl restart nftables.service`
6. When the WHM Host Access Control page is reloaded, the changes should now be reflected.

Also note that rules are dynamically loaded into nftables by `update_firewall.sh`.

CSF

chost does not use CSF

chost does not use CSF

chost does not use CSF

CSF is a third party addon for cPanel.

Whitelisting IPs

IPs can be whitelisted two different ways, either via the web interface or SSH

If using the web interface:

1. Go to WHM > ConfigServer Security & Firewall

2. Click “csf” tab near the top, under the banners
3. Under “csf - ConfigServer Firewall” click “Firewall Allow IPs”
4. Add IP and comment to list how the rest are
5. Click Change
6. Click Restart csf+lfd

If using shell/ssh

1. Edit `/etc/csf/csf.allow`
2. Add entries like the others and save the file
3. Run: `csf -ra` to restart/reload CSF

Removing Banned IPs

CSF

While the server only allows whitelisted IPs to connect, it might be possible that the server can ban someone that is on the list if they try to log in too many times.

1. Under WHM > ConfigServer Security & Firewall
2. Go to: csf - ConfigServer Firewall
3. Where it says: Search for IP, type in their IP and click Search.
4. If something comes back, click Return
5. Go to: csf - Quick Actions
6. Type in the IP to Quick Unblock and click the button

cPHulk

cPHulk can also block IPs for various reasons.

To find blacklisted IPs:

Go to: WHM > cPHulk Brute Force Protection Click “Blacklist Management” You should see all IPs block by cPHulk on this page If you want to remove an IP from the list, just click Delete and Continue

You can also whitelist in cPHulk as well by going to the “Whitelist Management page”. If you are whitelisting yourself from your current machine, you can just click “Add to Whitelist” on the red box.

Installation General Information

Two main things need to be set up

1. CSF needs to be configured to not allow any ports
2. IPs need to be added to the `csf.allow` list

Installation

The administrative security policy requires that only specified Ips are allow to connect to the dev server. CSF is one of the most popular cPanel plugins to somewhat easily control the linux firewall.

Click Here for the documentation to set up CSF.

Otherwise, run these commands:

```
cd /root
wget https://download.configserver.com/csf.tgz
tar -xzf csf.tgz
cd csf
./install.cpanel.sh

# reboot server

sed -ibak 's/^TESTING = "1"/TESTING = "0"/'
sed -r -ibak 's/^TCP_IN = "[0-9,]+"/TCP_IN = ""/' /etc/csf/csf.conf

sync; csf -ra
```

From:
https://wiki.beacontechnology.com/ - **Guide**

Permanent link:
https://wiki.beacontechnology.com/doku.php?id=wiki:firewall&rev=1690237248

Last update: **2023/07/24 22:20**