Table of Contents

Firewall

The cPanel servers make use of various firewalling features

`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.

Do not forget to update the firewall by running the script:
`/etc/cron.daily/update_firewall.sh`

The script runs daily, but running it now will immediately update the firewall.

Do not forget to add the IP to each of the 2 accounts, master on chost and beacontechnology on kingscpw01.

Click here to learn more

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”

Troubleshooting

It may be the case that sometimes the script gives an error for various reasons, here are some steps to try to fix it:

1. Try rebooting server
2. Try making a change in cpHulk like adding/removing an IP and trying again
3. Try this command: `nft flush set inet filter ccblockset` and try again
4. try this command: WARNING, may result in getting locked out, add your IP to `/etc/sysconfig/nftables.conf` before proceeding... `nft flush set inet filter adminwhitelist`

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`.

update_firewall.sh

This script help managing nftables

update_firewall.sh

```
#!/bin/bash

# this script extends cpHulk to assist managing nftables.

# country codes selected in CPhulk will be banned at the IP level
# whitelisted ips will be included as administratively allowed

set -e
trap 'catch $? $LINENO' EXIT

catch() {
  if [ "$1" != "0" ]; then
    echo failed to update firewall rules
    echo "Error $1 occurred on $2"
  fi
}

geoipdir='/usr/local/cpanel/3rdparty/share/geoipfree/country-cidrs'

whitelist=$(mktemp)
blacklist=$(mktemp)

# get list of CCs that are blocked
cclist=$( whmapi1 --output=json load_cphulk_config |
          jq -r '.data.cphulk_config.country_blacklist' )

# loop over list and concat all subnets from cpanel free geoip
for i in ${cclist//,/ }; do
  grep -oP '(\d+\.){3}\d+/\d+' $geoipdir/$i | tr '\n' ',' >> $blacklist
done

# write list of whitelist ips to temp file
whmapi1 --output=json read_cphulk_records list_name='white' |
        jq -r '.data.ips_in_list | keys[]' | grep -oP '(\d+\.){3}\d+' >
$whitelist

# generate new rules for nftables
{
  echo 'flush set inet filter ccblockset'
  echo 'flush set inet filter adminwhitelist'

  # create whitelist set
  echo -n 'add element inet filter adminwhitelist { '
  cat $whitelist | tr '\n' ','
```

```
  echo ' }'

  # create blacklist set
  echo -n 'add element inet filter ccblockset { '
  cat $blacklist | tr '\n' ','
  echo ' }'
} | nft -f -

echo firewall was successfully updated
```

Allowing IPs to locked down cpanel accounts

On some accounts, there is htaccess that whitelists IPs for extra security.

The htaccess is normally at: `/home/username/public_html/.htaccess`

The area you are looking for looks something like this:

```
order allow,deny
allow from xxx.xxx.xxx.xxx
allow from xxx.xxx.xxx.xxx
allow from xxx.xxx.xxx.xxx
allow from xxx.xxx.xxx.xxx
```

Just add a similar new entry below the last one in the list