Role B: firewall

*assumes you have already set up the server

Ideally the attacker and the server should be different devices (VM-to-VM, or host-to-VM), but same VM is probably okay as well

UFW install

Enable universe repository (tbh idk what this does none of the guides tell me)

```
sudo add-apt-repository universe

sudo apt update -y
```

Install gufw

```
sudo apt install gufw -y
```

UFW setup

sudo ufw logging level

```
sudo ufw logging medium
```

* higher levels are unnecessary for this sim

Import rules

Open gufw's UI, click File > Import profile, find the profile and import

Export rules

Open gufw's UI, click File > Export this profile, find a place to export to

Install hping3 (attack tool)

```
sudo apt install hping3
```

before test:

1. (optional) clear ufw log so exporting it doesn't kill your computer
   * to export before purging, see test step 5 first
   ```
   cat /dev/null | sudo tee /var/log/ufw.log
   ```

test:

1. Enable/disable ufw
   server: sudo ufw <enable/disable>

2. Live monitor cpu usage & logs
   server (terminal 1): sudo top

   -> monitor cpu et al usage

   server (terminal 2): sudo tail -f /var/log/ufw.log

   -> live follow ufw logs (if ufw enabled)

3. Run attack
   attacker: sudo hping3 **<your host ip>** -S --flood -p 443

4. Watch logs or cpu usage or try accessing website in private browser
5. (optional) export logs for ref
   sudo cat /var/log/ufw.log > /whichever/dir/you/like

   export w/ filtering:

   sudo grep <FILTER WORD> /var/log/ufw.log > /whichever/dir/you/like

6. Repeat for enable/disable ufw

Expected results

No firewall: cpu usage occasionally spikes, usually to >50%, sometimes almost 100%, browser access really laggy

*sometimes cpu falls back down to normal level, or takes time to spike. idk why.

With firewall: cpu still spikes, but only to around 30%, browser access should be less terrible, ufw logs show tcp syn requests blocked/limit blocked

Logging

Filter keywords (case sensitive):

UFW LIMIT BLOCK/UFW BLOCK: blocked by ufw rules

UFW LIMIT ACCEPT: not blocked

UFW LIMIT AUDIT: honestly idk what this is and google isn’t helping me so far

PROTO=TCP: TCP packets

SYN: syn packets

SRC=<ip addr>: packet src ip

*etc these are the ones i used to filter