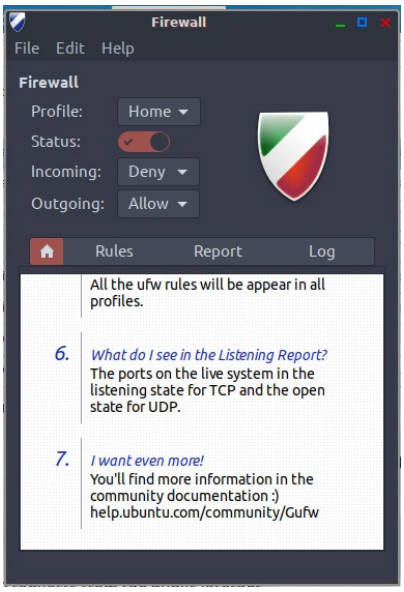
Ubuntu-MD February 27, 2021 Meeting

Firewall on Ubuntu Desktop
Antivirus Program

First question is do we need a firewall
Uncomplicated Fire Wall (ufw) and iptables
UFW is is a front-end to iptables that is much more easy to configure.
Iptables is much more capable for creating and managing enterprise level firewalls.
GUI interface for ufw is gufw (sudo apt install gufw)



1. Setup if not installed by default (whereis ufw returns several paths to app if it is already installed)
   if not installed, sudo apt install ufw
   Once installed the default setting denies all incoming connections and allow all outgoing
   sudo ufw default deny incoming | sudo ufw default allow outgoing (restore defaults)
   Status: sudo ufw status | return active or inactive
2. Activate: sudo ufw enable (make sure you have opened any critical port like ssh before enabling)
3. Add rule for ssh to your desktop to allow access from another machine on the same network
   sudo ufw allow ssh or sudo ufw allow 22 (if port assigned to ssh is 22)
4. Add rule for openvpn client on desktop
   sudo ufw allow openvpn or sudo ufw allow 1194
5. Add rule for hosting webserver
   sudo ufw allow http(s) (port 80/443)
6. Add rule to allow file transfer protocal (ftp)
   sudo ufw allow ftp or sudo ufw allow 21
7. Add rule to allow multiple port ranges
   sudo ufw allow 6000:6007/tcp (must include port protocol type tcp or udp)
8. Add rule to allow to any port from a specific ip
   sudo ufw allow from 10.1.10.56
   sudo ufw allow from 192.168.0.25 to any port 22 (only allow ssh access on port 22 from machine with 192.168.0.25 ip)
9. Add rule to allow a specific network interface
   sudo ip addr to see your network device
   sudo ufw allow in on eth1 any port 3306 (MySQL)
10. Deny connection rules
    sudo ufw deny http (port 80)
    sudo ufw deny from 96.87.23.128 (block access from a malicious site)
11. Delete rules
    sudo ufw status numbered
    sudo ufw delete {rule number}

sudo ufw delete allow openvpn

12. Disable ufw
sudo ufw disable
13. Reset ufw: sudo ufw reset

Fail2ban Program ….

Antivirus Programs

Do you need one?
Free Linux programs: Clamav and Bitdefender.
Clamav :

sudo apt install clamav clamav-daemon	
clamscan --version	Version number should appear if installed correctly
sudo systemctl stop clamav-freshclam	Stop the service to update database
sudo freshclam	Update the database and if it doesn't work may need to download the lastest build https://database.clamav.net/daily.cvd
sudo systemctl start clamav-freshclam	Restart the daemon
clamscan --infected --remove --recursive /*home*/you/Desktop	Do a test scan of your Desktop files. Output results will appear after it completes
sudo apt install clamtk	Install the GUI