**Network-Based Firewall**

**Accessed through web interface /firewall**

OpenWrt

* Uses IPtables

DD-Wrt

* Also uses IPtables

**Features**

Connection warning notifier

Iptables enabling/disabling

Add additional

* Proxies
* Cookies
* Java applets
* ActiveX

WAN blocking

Brute force protection

Logging

^all accessible through IPtables, this is just a web interface GUI to do this

Can also input the Iptables commands into the web interface

**OR**

Enter the commands in the command line via SSH

**Firewall Builder**

* Firewall GUI run on a separate device which will remotely manage the Iptables rules remotely via SSH
* Compatible with Linux, Windows and MacOS
* Works well with routers, especially DD-Wrt

**Dedicated Hardware**

* Old PC/Laptop
* Firewall hardware

Pcengines.ch

* Offer dedicated firewall hardware to set up a firewall to run other devices through
* Designed to be routers and firewalls
* Have multiple different networks cards
  + Allows creation of distinct, different, routable networks
* This would act as a router and firewall
  + Doesn’t include a modem to connect to the internet so would need that on top

Open-Source Hardware

* Novena

**Recommended firewall - PFsense**

Open-source BSD-based

* Installed on computers, not routers
  + Will turn the dedicated hardware into a router and firewall
* Can be used as a DHCP server or a DNS server
* Can install intrusion detection system (IDS) and prevention systems (IPS) e.g. Snort
* Network isolation
* Virtual LANs
* VPN server/client
* Can TORify all traffic

**SmoothWall**

**Vyos**

**Is it worth having a network-based firewall?**

NAT exists so inbound filtering isn’t required

Can install IDS or IPS, block inbound attacks that match certain attack signatures

Outbound filtering

* Lock down just the ports that are going to be used
* Restrict certain devices from using certain ports
* Force DNS over VPN
* Block IPv6 to prevent VPN leakage at the network layer
* Block traffic you don’t want such as torrents
* Limit bandwidth on devices

Network isolation

* Helps with privacy and anonymity

Dedicated firewalls like PFsense have better functionality than a router even though a router can do most of these things aswell

Remember a network firewall cannot protect you from malware already on the network or attempting to enter through an exploit

* The reverse shell will just be executed through a port that is allowed

Application firewall / proxy traffic

* Better results for blocking traffic
* DPI
* Monitoring and logging of traffic
  + See what may or may not be trying to attack