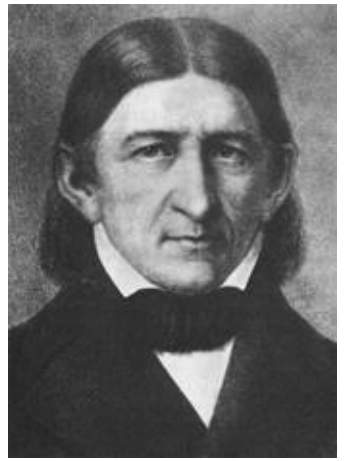
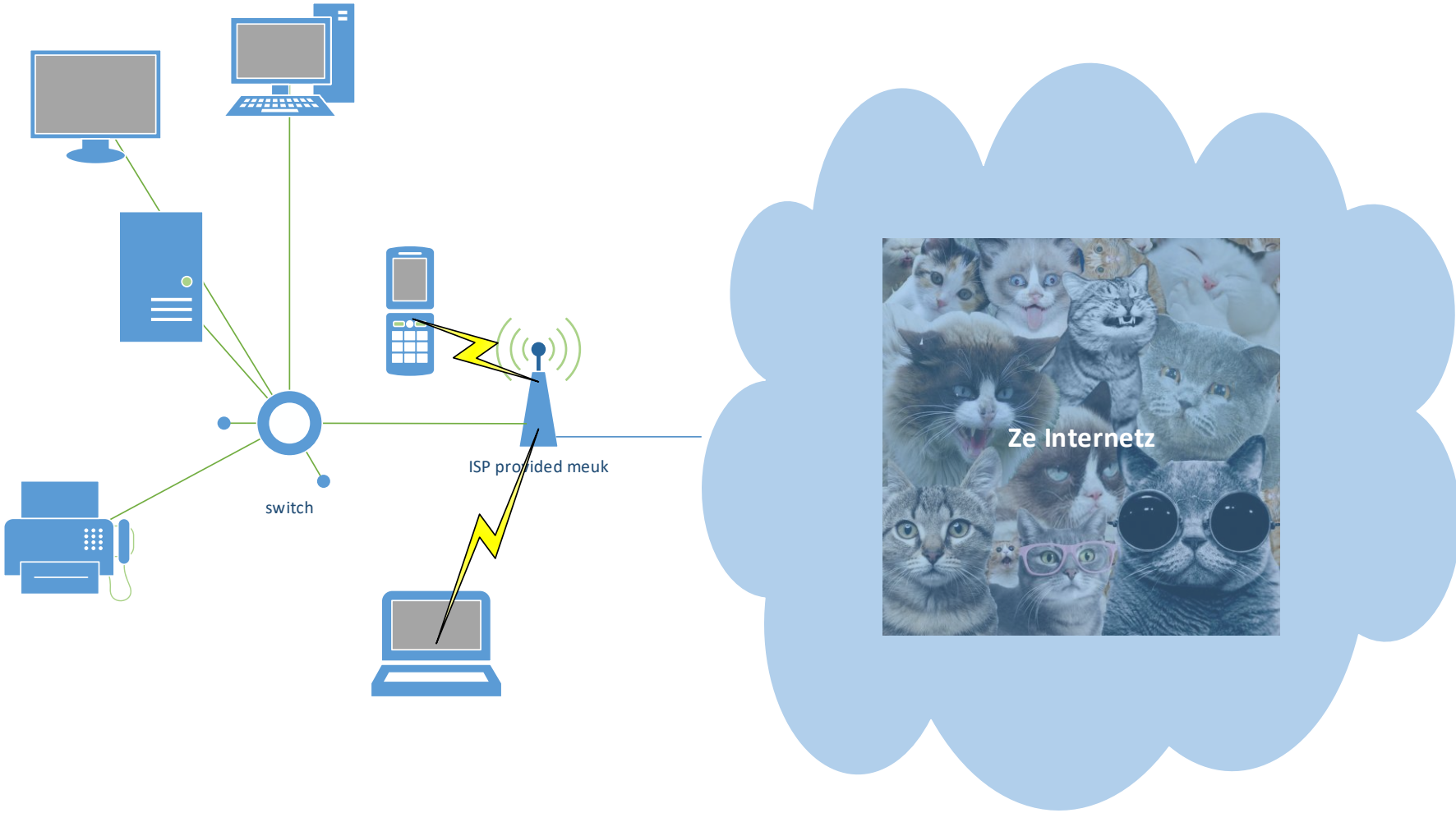
Packet Freubelen

Wikipedia: fröbelen - "vrijblijvend creatief bezig zijn“

(met een licht denigrerende ondertoon)



Standaard setup



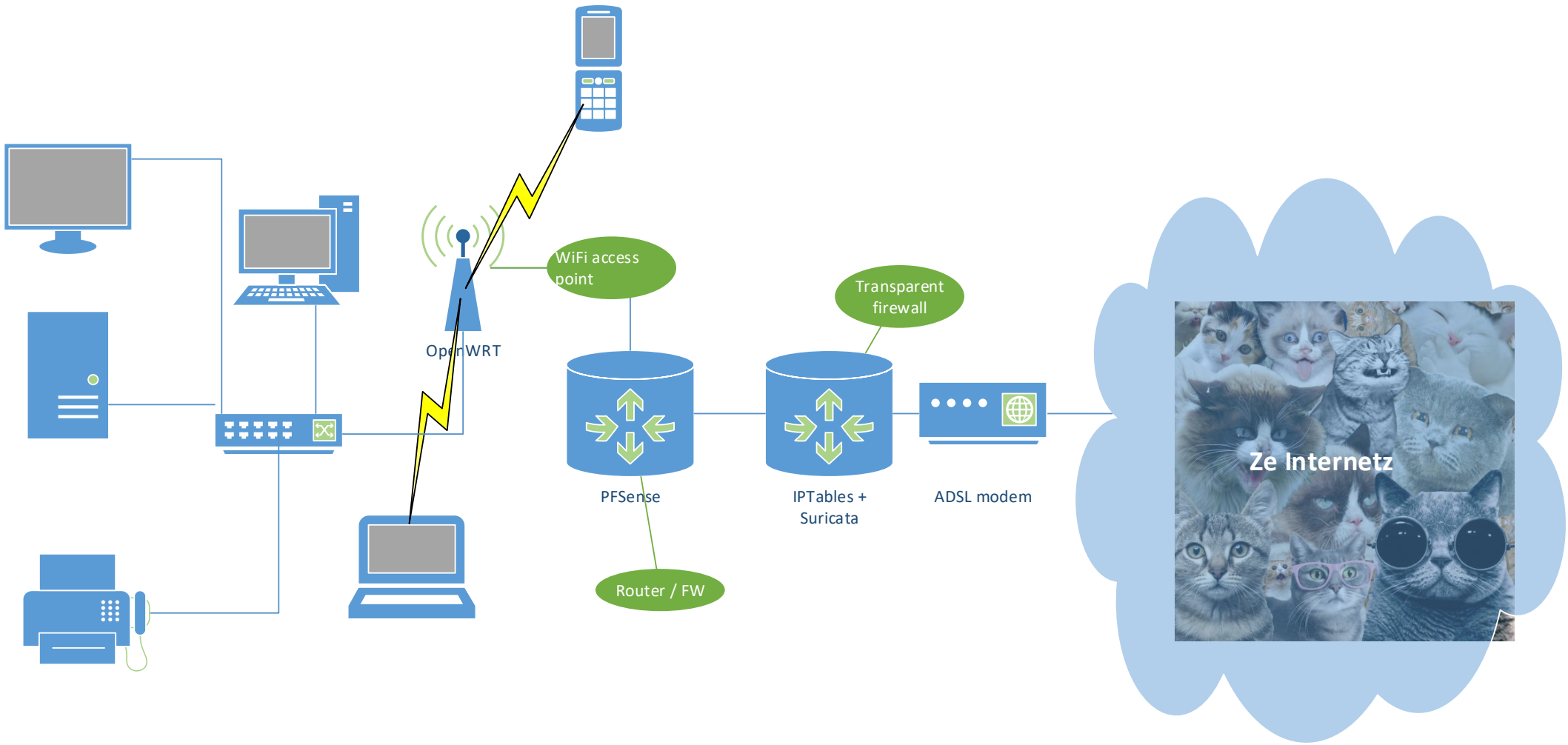
Standaard setup eigenschappen

- COTS
  - Nauwelijks logging
  - El-cheapo (voor de fabrikant)
- Meerdere taken op 1 apparaat
  - Voor beveiligings taak ongewenst

Mini-tinfoil-mad-hatter setup

Want ontheffing van Murphy gekregen…

Mini-tinfoil mad-hatter setup



Mini-tinfoil mad-hatter setup router

- PFSense
  - BSD gebaseerd
  - Meerdere taken:
    - SNAT Firewall
    - DNS → Unbound
    - DHCP → ISC DHCPD
    - VPN → OpenVPN
  - IF internal: intern netwerk
  - IF external: ISP (internet)

Mini-tinfoil mad-hatter setup router

- Unbound
  - DNS server, alternatief voor BIND (*funny guys ☺)
  - Focus op security
  - Resolver voor lokale domeinen
  - Forwarder
  - Blackholing van ongewenste domeinen
  - DNSSec (uiteraard…)

Mini-tinfoil mad-hatter setup Transp. FW

- Arch Linux
- 3 IF’s
  - IF-groen → LAN kant (router ←→ FW), bridge mode naar IF-rood
  - IF-rood → WAN kant, bridge mode naar IF-groen
  - IF-mgt → management
- IPTables
  - Default DROP
- Suricata IDS
  - In inline IPS mode (iptables: –j NFQUEUE)
- IPSet white / black list
  - DNS / malware

Mini-tinfoil mad-hatter setup Transp. FW - Suricata

- Intrusion Detection System
  - Maar kan ook als IPS acteren
  - Regel gebaseerd (ala YARA) (en slikt SNORT definities)
  - Regels:
    - Van simpel (alert als dst ip == 42.0.0.0/8)
    - Tot complex (alert als hdr == 0x4ebbce && mark1 == set …)
  - Modus:
    - IDS: b.v. op SPAN port switch, tap of router
    - IPS: acteer bij waarnemen fout gedrag (b.v. DROP actie ipv ALERT)
  - Regels dagelijks bijgewerkt m.b.v. barnyard2

Mini-tinfoil mad-hatter setup Transp. FW - ipset

- Efficiente lookup van ip hosts EN netwerken
- Duizenden entries in iptables –j DROP
  - == oldskool (als in 14k4 baud….)
- Duizenden entries in ipset list met –m set
  - == nauwelijks merkbare performance hit
- Aantal lijsten, b.v.:
  - allowed_dns: toegestane uitgaande DNS queries
  - wan_blocks / lan_blocks
- Dagelijks geupdate (wan_blocks) middels python script

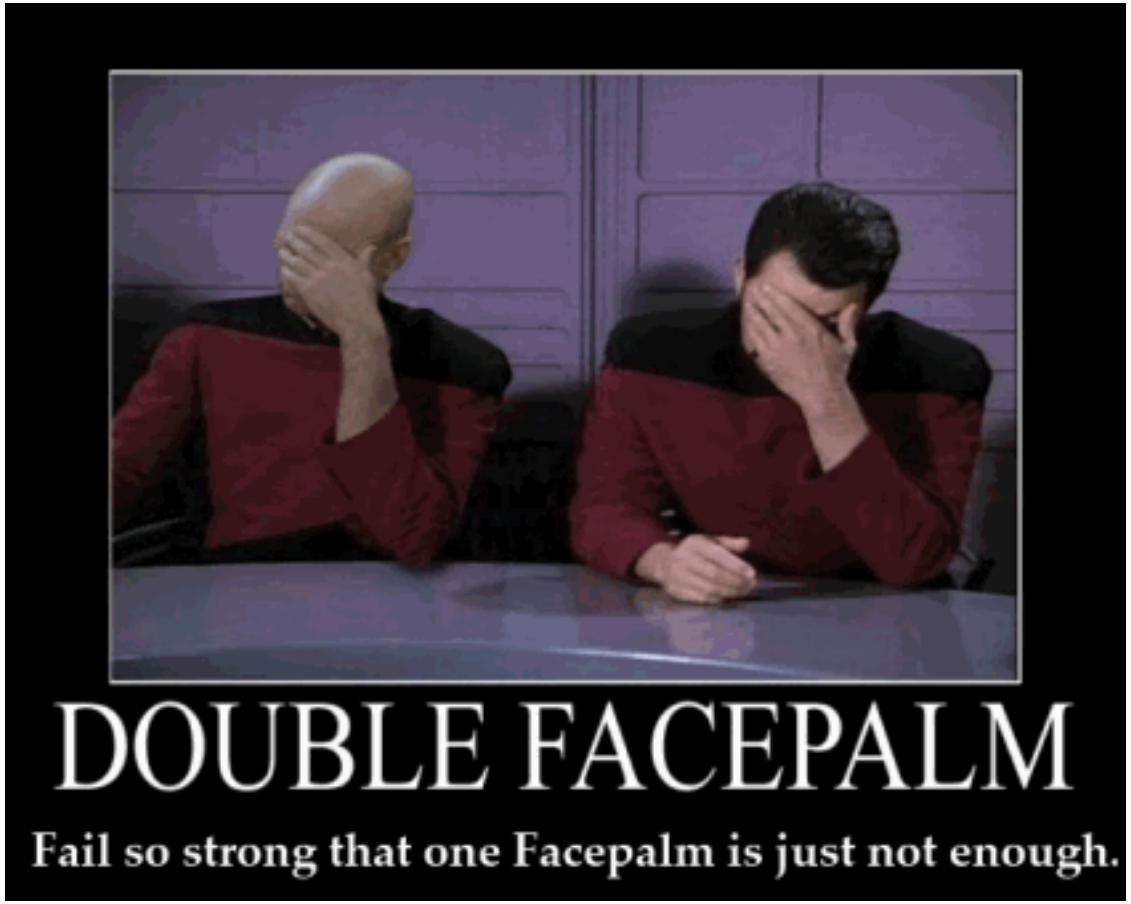
Mini-tinfoil mad-hatter setup Transp. FW - logging

- Log daemon bij voorkeur onzichtbaar
  - Minder kans sporen wissen
  - Sniffen rsyslog via promiscious mode

- ULOGD
  - Kernel logs → user space
  - IPTables meldingen, maar ook bv AppArmor, SELINUX meldingen
  - Verschillende bestemmingen mogelijk
    - Remote syslog
    - MySQL (remote)
    - …

Mini-tinfoil mad-hatter setup Transp. FW - gotcha

- Niet doorgedacht:
  - FDE m.b.v. LUKS
  - Maar:
  - Reboot / crash betekend on-site
- Toekomst:
  - Migratie naar NFTables



Mini-tinfoil mad-hatter setup scripts & config

- https://github.com/mgdegroot/dipshit
  - Defender of IP based Streams Hosted In Python
- util_ids.py
- iptables.rules
- unbound
- ulogd