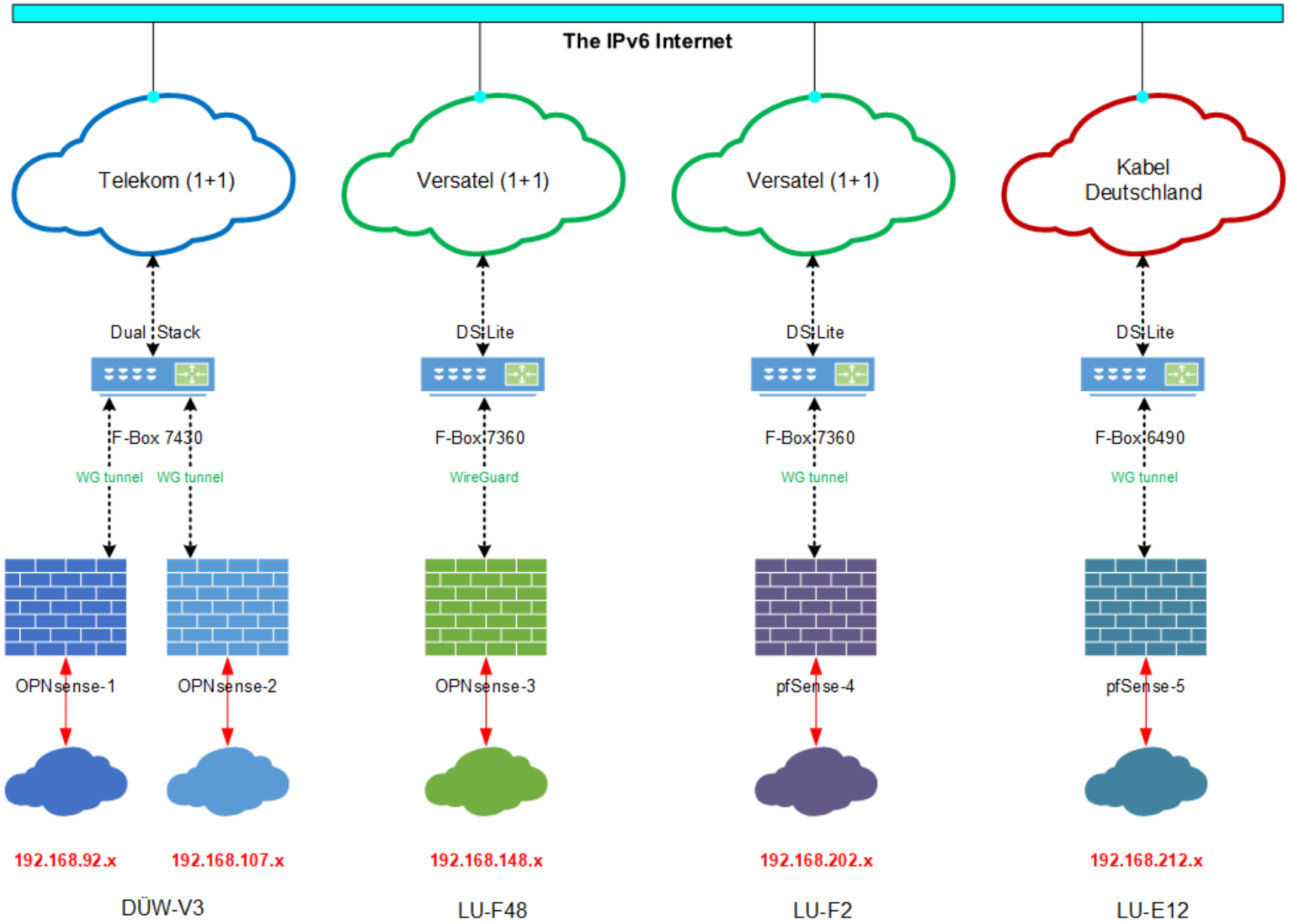
Secure Site-to-Site VPNs, using WireGuard and IPv6

Additional ingredients:
FritzBox routers, DS-Lite,
OPNsense firewalls,
and dynv6.com

Motivation

- I am running several small networks at a few different sites.
- These sites have non-overlapping private IPv4 address ranges.
- All sites are connected to the Internet via different ISPs.
- Most of these ISPs do no longer provide a publicly routable IPv4 address for the CPE (**C**ustomer **P**remise **E**quipment).
- All ISPs do provide the CPEs with IPv6 (DS-Lite or Dual-Stack).
- I want to have easy and transparent connectivity between the application networks. I.e. all complexity should be confined to the OPNsense firewalls that are behind the Fritz!Box CPEs.

Network diagram



Use Cases

- Ability to manage all systems remotely,
  regardless of my current location.
- Learning about IPv6 and WireGuard technologies.
- Implementation of the 3-2-1 backup scheme:
  3 copies at 2 different locations, 1 of them off-site
- Connecting smart IoT devices at different sites
  to local home automation systems and
  sending aggregated events to a centralized controller.
- Learning to use cloud-native technologies at home.

Agenda

- Part 1:
  - “A whirlwind tour of IPv6”
- Part 2:
  - “Implementation details of a modern, secure site-to-site VPN”
- Part 3:
  - “Lessons learned”

Lessons learned

- End-to-End networking is cool!
- Do not fear IPv6: use host firewalls
- Watch out for PMTU + ICMP6 !!
- Use RADVD; instead of DHCP6 !!
- Debugging: Log-Files and Online Tests (and Google ☺)
  - What is my IP?
  - Test-IPv6, IPv6-Test

Ressources

- Websites and books in German:
  - Excellent book by Dan Lüdtke: “IPv6 Workshop”
  - “Elektronik-Kompendium.de” has lots of good content
- Open-Source Firewalls:
  - OPNsense
  - pfSense
- IP connectivity test sites:
  - ipv6-test.com
  - test-ipv6.com
  - kame.net
  - whatismyip.host
  - heise.de
- DynDNS providers:
  - spdyn.de
  - twodns.de
  - dynv6.com