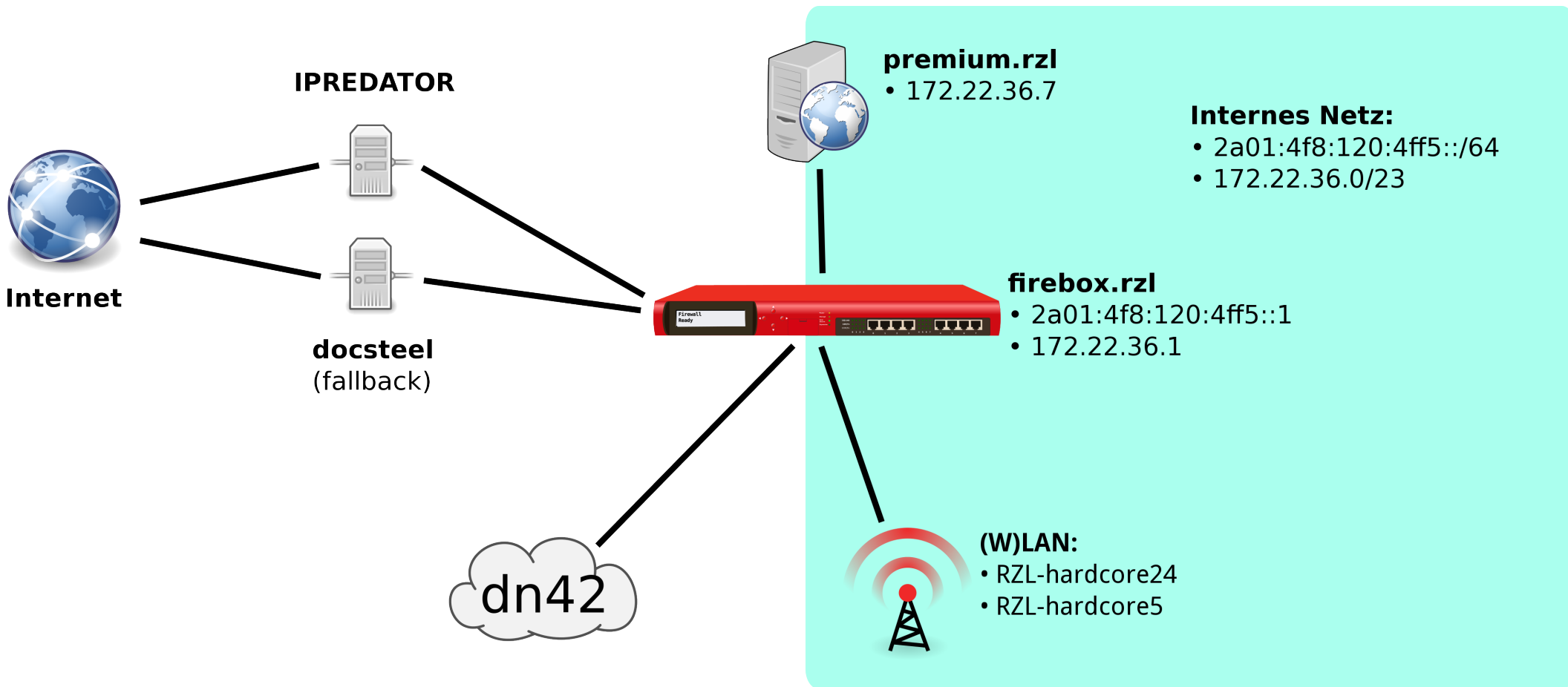


Das RZL-Netzwerk

(speziell: OpenVPN Failover)

RaumZeitLabor e.V.
Else und hax404

Unser Setup



(Bild Courtesy of hax404. All rights reserved. KTHXBYE)

OpenVPN Gateways

- Standardmäßig vergibt OpenVPN im Client-Server Modus folgende Routen:
 - 0.0.0.0/1 → \$GATEWAY
 - 128.0.0.1/1 → \$GATEWAY
 - Route zum \$GATEWAY Netz.
- bei zwei Tunneln funktioniert das natürlich nicht

OpenVPN Failover

- OpenVPN kann Liste von Servern nutzen
 - nützt uns nichts (verschiedene Configs)
- Failover gibts so direkt nicht, selber basteln
 - OpenVPN ist skriptbar über up / down Direktive
 - Routen müssen dann manuell gesetzt werden
- Idee: eigene Routingtabelle pro Tunnel
 - flexibler als „Longest Matching Prefix“ ...
 - wird von Skript gesetzt

Unser Setup

- Gegeben: Routingtabelle
 - docsteel: default via \$DOCSTEEL_GW
 - ipredator: default via \$IPREDATOR_GW
- Traffic „flaggen“:
 - `-A PREROUTING -s 172.22.36.0/23 ! -d 172.22.0.0/15 -j MARK --set-mark 0x1337`
- Policy-based Routing:
 - `ip rule add fwmark 0x1337 prio 100 table ipredator`
 - `ip rule add fwmark 0x1337 prio 200 table docsteel`

Demo

Bye.