IT-Infrastruktur des Ortsverbandes X50 („auf dem Berg“)

- Vorschlag -

Stand: 03.2026 (M. Hopf)

Überblick
Die gesamte Infrastruktur basiert auf einem einzelnen leistungsfähigen Hostrechner mit einer modernen Intel- oder AMD-CPU, 16 bis 32 GB RAM und ausreichend Speicherplatz. Auf diesem Hostrechner läuft **Proxmox** als Virtualisierungsplattform, die alle weiteren Dienste als virtuelle Maschinen (VMs) oder Docker-Container bereitstellt. Der Hostrechner steht an einem entfernten Standort. Bei geeigneter Auswahl der Hardwarekomponenten benötigt er nur eine Gleichspannung von 12V. Der Rechner ist ausschließlich über das Internet erreichbar (es sei denn, man kraxelt auf den Berg 😉).

Netzwerkstruktur
Am Hostrechner ist ein einzelner physischer Ethernet-Port angeschlossen, der mit einem **VLAN-fähigen Switch** verbunden ist. Dieser Switch teilt das Netzwerk in mindestens drei logische Segmente (VLANs) auf. Im ersten Segment (VLAN 10) befinden sich alle VMs des Proxmox-Hosts. Im zweiten Segment (VLAN 20) sind alle externen Hardware-Komponenten wie der Kiwi-SDR-Empfänger, die schaltbare Steckdosenleiste und mögliche weitere Geräte angeschlossen. Das dritte Segment (VLAN 30) ist ausschließlich für die Verwaltung reserviert, also für den Zugriff auf die Proxmox-Weboberfläche und die OPNsense-Verwaltungsoberfläche.
Bei geeigneter Auswahl des Switches benötigt er nur eine Gleichspannung von 12V.

Firewall und Sicherheit
Als erste VM in Proxmox läuft **OPNsense**, eine vollständig quelloffene Firewall-Distribution auf FreeBSD-Basis. OPNsense übernimmt die Rolle des zentralen Gateways und schützt die **gesamte** Infrastruktur vor unerwünschten Zugriffen aus dem Internet. Es verfügt über ein WAN-Interface zur Außenwelt und ein LAN-Interface zum internen Netzwerk. Zusätzlich ist das Intrusion Detection und Prevention System **Suricata** in OPNsense integriert, das den Datenverkehr aktiv auf Angriffsmuster überwacht. Vom Internet aus sind über den vorgelagerten Router nur die Ports 80 (HTTP), 443 (HTTPS) und der WireGuard-VPN-Port (UDP 51820) erreichbar.

Zwei klar getrennte Zugangswege
Die Infrastruktur unterscheidet grundsätzlich zwischen zwei Benutzergruppen mit völlig unterschiedlichen Zugangswegen:

Öffentliche Benutzer – also alle, die die SDR-Empfänger (OpenWebRx-Plus, Kiwi-SDR) oder andere veröffentlichte Webdienste nutzen möchten – greifen ausschließlich über **HTTPS via Reverse Proxy** zu. Sie benötigen kein VPN und erhalten auch keinen Zugriff auf interne Systeme. Für sie ist die Infrastruktur unsichtbar – sie sehen nur die jeweilige Webanwendung hinter einer offiziellen Domain mit gültigem Zertifikat.

Administratoren und Betreiber – also Personen, die die Infrastruktur warten, konfigurieren oder überwachen – nutzen ausschließlich den **WireGuard-VPN-Tunnel**. Nur über diesen Tunnel sind die Proxmox-Weboberfläche, die OPNsense-Verwaltung, SSH-Zugänge und alle internen Dienste erreichbar. Ohne aktive VPN-Verbindung sind diese Verwaltungszugänge von außen vollständig unsichtbar und nicht erreichbar.

Diese strikte Trennung stellt sicher, dass öffentliche Nutzer niemals mit der Verwaltungsebene in Berührung kommen – weder versehentlich noch durch einen Angriff.

Reverse Proxy
Eine eigene Linux-VM mit Docker betreibt den **nginx Proxy Manager** als Reverse-Proxy-Container. Alle eingehenden HTTPS-Anfragen öffentlicher Nutzer laufen über diesen Proxy, der sie an den jeweiligen Zieldienst weiterleitet. Dabei werden **Let's Encrypt-Zertifikate** automatisch geholt und erneuert. Der Reverse Proxy kann sowohl VMs als auch externe Hardware-Komponenten wie den Kiwi-SDR als Ziele ansprechen.

SDR-Empfang mit OpenWebRx-Plus
Für den Kurzwellen- und Breitbandempfang laufen mehrere VMs mit Docker, auf denen jeweils ein **OpenWebRx-Plus**-Container betrieben wird. Die dazugehörigen SDR-USB-Empfänger werden per USB-Passthrough direkt an die jeweilige VM durchgereicht. OpenWebRx-Plus ist für alle Benutzer öffentlich über HTTPS erreichbar – die Verwaltung der VMs selbst erfolgt jedoch ausschließlich über VPN.

Kiwi-SDR und externe Hardware
Der **Kiwi-SDR**-Empfänger ist ein eigenständiges Gerät mit Ethernet-Anschluss und hängt direkt am VLAN-Switch im isolierten VLAN 20. Er ist über den Reverse Proxy ebenfalls öffentlich per HTTPS erreichbar. Gleiches gilt für die **schaltbare Steckdosenleiste**, wobei deren Web-Interface aus Sicherheitsgründen nur über VPN zugänglich sein sollte, da es sich um eine sicherheitsrelevante Steuerkomponente handelt. Die Isolierung im eigenen VLAN stellt sicher, dass ein potenziell unsicheres Gerät keinen Zugriff auf die VMs oder die Verwaltungsebene hat.

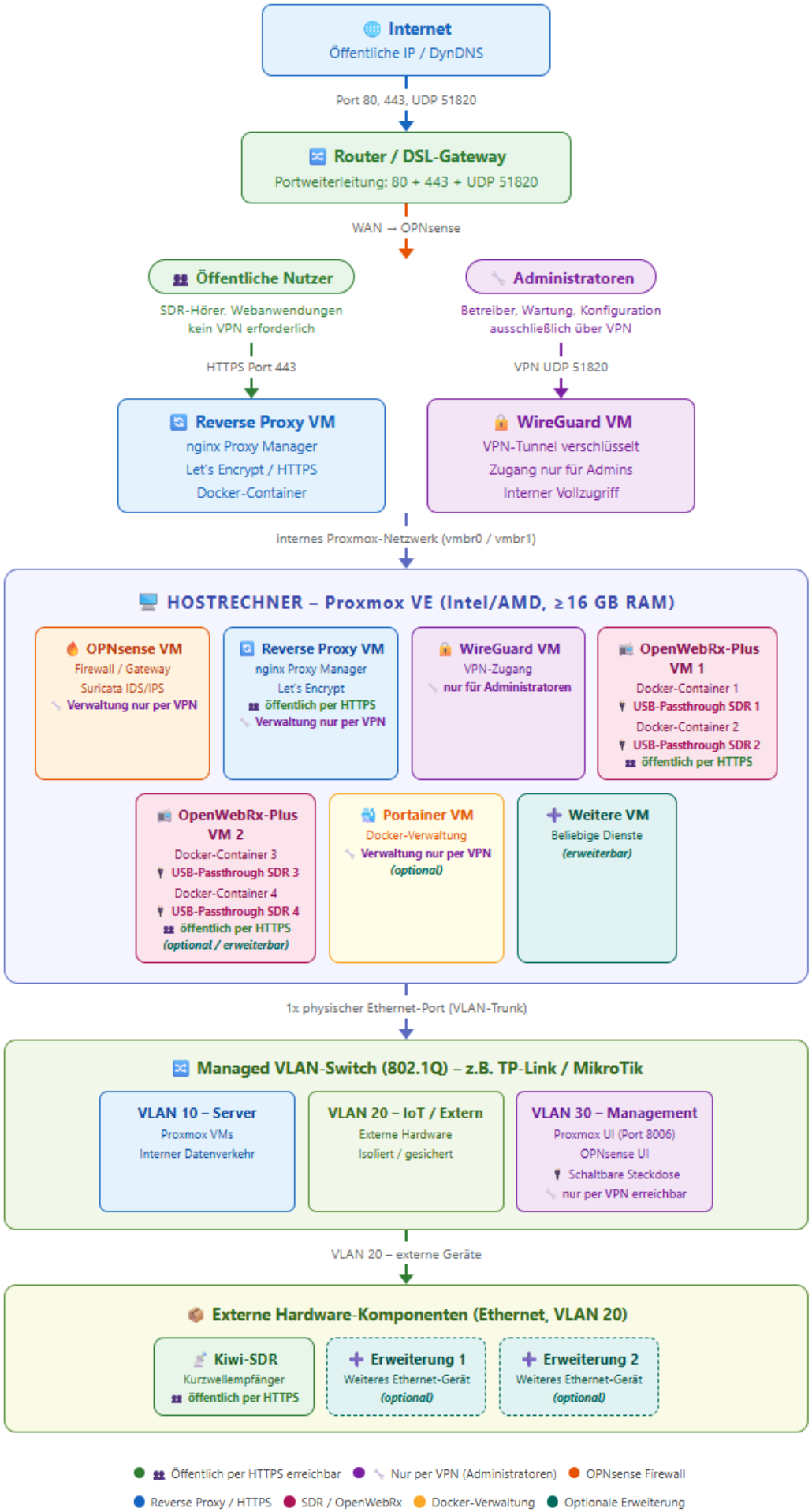
Erweiterbarkeit
Die Infrastruktur ist sehr gut erweiterbar. Weitere VMs oder Docker-Container können jederzeit in Proxmox hinzugefügt werden. Neue externe Hardware-Komponenten werden einfach am Switch in VLAN 20 angeschlossen und im Reverse Proxy eingetragen. Eine optionale **Portainer-VM** zur komfortablen Verwaltung aller Docker-Container ist ebenfalls vorgesehen.

Stromverbrauch
Bei geeigneter Auswahl der Hardwarekomponenten (Rechner, Switch) und Einsatz einer stromsparenden CPU, sollte der Stromverbrauch, je nach Auslastung (Anzahl der gleichzeitigen OpenWebRx-Hörer) zwischen 30 und 60 W liegen.

Übersicht siehe nächste Seite…

IT-Infrastruktur Übersicht – Proxmox / OPNsense / VLAN

Zwei getrennte Zugangswege: 👥 Öffentliche Nutzer via HTTPS · 🔧 Administratoren via VPN



🟢 👥 Öffentlich per HTTPS erreichbar 🟣 🔧 Nur per VPN (Administratoren) 🟠 OPNsense Firewall

🔵 Reverse Proxy / HTTPS 🔴 SDR / OpenWebRx 🟡 Docker-Verwaltung 🟢 Optionale Erweiterung