GANZ EINFACH

Heimnetz und Homelab

Proxmox, VLANs, Pi-hole und Single Sign-on – Schritt für Schritt erklärt



Planen · Einrichten · Vernetzen · Sicher betreiben

Danilo Sieren

Danilo Sieren

Heimnetz und Homelab

Proxmox, VLANs, Pi-hole
und Single Sign-on
Schritt für Schritt erklärt

Erste Auflage 2026
Stand Proxmox VE 9.2 und OPNsense 26.7

Verstehen · Anwenden · Überprüfen

Vorwort

Kennst du das? Im Heimnetz hängen inzwischen mehr Geräte als Menschen im Haushalt. Das Notebook für die Arbeit, die Handys der Familie, der Fernseher, die Spielkonsole, zwei smarte Steckdosen aus dem Sonderangebot, der Saugroboter, die Wetterstation, das Babyfon von früher, das niemand mehr benutzt, aber auch niemand abgemeldet hat. Und alle teilen sich dasselbe Netz. Die billige Steckdose mit der Firmware von 2021 steht im selben Raum wie das Notebook mit den Kundendaten. Jeder Besuch, der das WLAN-Passwort bekommt, sitzt mit im Wohnzimmer deines Netzes.

Dieses Buch zeigt dir, wie du das änderst. Du teilst dein Heimnetz in getrennte Bereiche auf: einen für die Familie, einen für Gäste, einen für smarte Geräte, einen für deine Server. Du filterst Werbung und Tracker für alle Geräte auf einmal. Du betreibst eigene Dienste für Fotos, Passwörter und Dokumente auf einem kleinen, stromsparenden Rechner, statt sie in fremde Clouds zu geben. Du meldest dich bei all diesen Diensten mit einem einzigen, gut geschützten Konto an. Und du erreichst alles von unterwegs, ohne auch nur einen einzigen Port deines Routers ins Internet zu öffnen.

Klingt nach Rechenzentrum und Fachchinesisch? Ist es nicht. Ich erkläre dir alles so, wie ich es einem Freund am Küchentisch erklären würde: in Ruhe, Schritt für Schritt und ohne vorauszusetzen, dass du schon einmal eine Firewall eingerichtet hast. Du brauchst keine Programmierkenntnisse. Ein paar Befehle wirst du in ein Terminal tippen, aber jeder Befehl wird erklärt, und fast alles andere erledigst du mit der Maus in übersichtlichen Weboberflächen.

Durch das ganze Buch begleitet uns Jana Wolff aus Bochum. Jana arbeitet als Fotografin, zum Teil im Homeoffice. Sie lebt mit ihrem Partner Mehmet und ihrem zwölfjährigen Sohn Leo in einer

Altbauwohnung mit einer Fritzbox, einem Dutzend smarter Geräte und einem alten NAS im Keller voller Kundenfotos, von dem es keine Sicherung gibt. Ihr Projekt heißt „Das aufgeräumte Netz“. Am Ende des Buches hat Jana ein sauber getrenntes Heimnetz mit Werbefilter, einen kleinen Server mit ihren eigenen Diensten, eine funktionierende Datensicherung und einen sicheren Zugang von unterwegs. Kapitel 27 fasst den fertigen Aufbau mit Adressplan, Regeln und Diensten zusammen.

Die redaktionelle Prüfung hat den Stand 1. November 2026. Grundlage sind Proxmox VE 9.2, OPNsense 26.7, Pi-hole in Version 6, AdGuard Home, authentik in der Version 2026.5 und die aktuellen Fassungen der übrigen vorgestellten Dienste. Die Anleitungen folgen der offiziellen Dokumentation der jeweiligen Projekte. Anhang F erläutert, welche Angaben wie geprüft wurden und was du vor dem eigenen Nachbau kontrollieren solltest. Die Abbildungen sind bewusst schematisch gehalten: Sie erklären Zusammenhänge und bilden keine Programmoberflächen pixelgenau nach.

Eine Regel begleitet dich durch das ganze Buch: Erst planen, dann umbauen, und immer einen Weg zurück offenhalten. Dein Heimnetz ist kein Testlabor, in dem ein Fehler egal ist. Wenn das Internet ausfällt, merkt es die ganze Familie. Deshalb baust du das neue Netz neben dem alten auf, ziehst die Geräte nacheinander um und hast für jeden Schritt einen Plan, wie du ihn rückgängig machst.

So arbeitest du mit diesem Buch

Teil I mit den Kapiteln 1 bis 4 legt die Grundlagen. Du erfährst, was ein Homelab ist und was es dir bringt, lernst die wichtigsten Begriffe rund um Netzwerke kennen, nimmst dein heutiges Netz auf und wählst die passende Hardware aus. Lies diesen Teil vollständig, bevor du etwas kaufst.

Teil II mit den Kapiteln 5 bis 8 dreht sich um Proxmox VE, die Plattform für deinen Server. Du installierst sie, lernst die Oberfläche kennen, legst virtuelle Maschinen und Container an und richtest die Datensicherung ein. Teil III mit den Kapiteln 9 bis 14 ist das Herz des Buches: Du teilst dein Netz mit VLANs auf, richtest den managed Switch ein, installierst die Firewall OPNsense, legst die Netze an, schreibst verständliche Firewallregeln und bringst mehrere Netze ins WLAN.

Teil IV mit den Kapiteln 15 bis 20 füllt das Netz mit Leben: Werbefilter mit Pi-hole oder AdGuard Home, eigene Namen im Heimnetz, Docker, ein Reverse Proxy mit echten Zertifikaten und nützliche Dienste für den Alltag. Teil V mit den Kapiteln 21 bis 28 behandelt die gemeinsame Anmeldung, den Fernzugriff, Überwachung, Wartung, Sicherheit und Fehlersuche, fasst das Lernprojekt zusammen und endet mit der Abnahme.

Jedes Kapitel endet mit einer Werkstatt und häufig mit einer Vertiefung. Die Werkstatt ist eine praktische Übung mit einem Ergebnis, das du überprüfen kannst. Die Vertiefung zeigt Grenzen, Alternativen oder Erweiterungen. Die Anhänge enthalten Einkaufslisten, einen Adressplan zum Ausfüllen, einen Fehlerkatalog, Begriffe, fertige Konfigurationen, den Versionsstand, Vorlagen, Projektideen und eine Übersicht der wichtigsten Befehle.

Befehle und Konfigurationsdateien stehen in Schreibmaschinenschrift in eigenen Blöcken. Befehle tippst du in ein Terminal, also eine Kommandozeile auf dem jeweiligen Rechner. Wo ein Befehl Werte enthält, die du anpassen musst, etwa eine Adresse oder einen Namen, steht das im Text davor. In Konfigurationsdateien im Format YAML entscheidet die Einrückung über die Bedeutung. Verwende dort immer Leerzeichen, niemals Tabulatoren.

Die Adressen in diesem Buch folgen einem festen Plan, den du in Kapitel 12 kennenlernst: Das Netz der Familie heißt 10.10.20.0/24, das der Server 10.10.30.0/24 und so weiter. Du kannst diesen Plan übernehmen oder einen eigenen verwenden. Wichtig ist nur, dass du ihn aufschreibst und dich daran hältst.

> **Tipp:** Leg dir gleich zu Beginn ein Notizheft oder eine Textdatei für dein Netz an. Trage dort jede Adresse, jedes Gerät, jede Entscheidung und jedes Passwort-Versteck ein, also den Hinweis, in welchem Passwortmanager welches Passwort liegt, nie das Passwort selbst. In einem Jahr bist du dir dafür sehr dankbar.

Inhalt

Vorwort 2
So arbeitest du mit diesem Buch 4
Inhalt 6
1 Warum ein eigenes Homelab 9
2 Netzwerkgrundlagen ohne Mathe 16
3 Bestandsaufnahme: dein Netz heute 23
4 Die Hardware 28
5 Proxmox VE installieren 34
6 Die Oberfläche, Paketquellen und Updates 40
7 Virtuelle Maschinen und LXC-Container 46
8 Speicher und Backups 53
9 VLANs verstehen 59
10 Der managed Switch 64
11 OPNsense als Firewall hinter der Fritzbox 69
12 Netze anlegen 76
13 Firewallregeln, die man versteht 82
14 Ein WLAN mit mehreren Netzen 90
15 Pi-hole: Werbung und Tracker filtern 96
16 AdGuard Home als Alternative 103
17 Eigene Namen im Heimnetz 109
18 Docker im Homelab 116
19 Reverse Proxy und echte Zertifikate 124
20 Nützliche Dienste für den Alltag 130
21 Single Sign-on mit authentik 137

22 Fernzugriff ohne offene Ports 145
23 Überwachung und Benachrichtigungen 152
24 Updates und Wartung 158
25 Sicherheit und Härtung 164
26 Fehler eingrenzen 170
27 Janas fertiges Heimnetz 175
28 Abnahme und Ausbauideen 182
Anhang A Einkaufslisten 188
Anhang B Adressplan und VLAN-Vorlage 193
Anhang C Fehlerkatalog 197
Anhang D Begriffe für die tägliche Arbeit 203
Anhang E Fertige Konfigurationen 207
Anhang F Versionsstand und Grenzen der Überprüfung 216
Anhang G Vorlagen zum Abschreiben 219
Anhang H Projektideen zum Weiterbauen 224
Anhang I Befehle auf einen Blick 227
Quellen und offizielle Dokumentation 234
Ausführliches Inhaltsverzeichnis 238
Stichwortverzeichnis 248
Impressum 252

1 Warum ein eigenes Homelab

1.1 Ein Netz, in dem alles mit allem spricht

Ein typisches Heimnetz in Deutschland sieht so aus: Ein Router, meist eine Fritzbox, verbindet die Wohnung mit dem Internet. Er verteilt Adressen an alle Geräte, stellt ein WLAN bereit und vielleicht noch ein Gäste-WLAN. Alles, was im normalen WLAN oder am Netzwerkkabel hängt, kann mit allem anderen sprechen. Das Notebook sieht den Drucker, der Drucker sieht den Fernseher, der Fernseher sieht die smarte Steckdose, und die smarte Steckdose sieht das Notebook.

Für den Alltag ist das bequem. Für die Sicherheit ist es ein Problem. Jedes Gerät im Netz ist so sicher wie seine Software, und die Software vieler smarter Geräte wird nach ein, zwei Jahren nicht mehr aktualisiert. Eine Kamera mit bekannter Sicherheitslücke, die jemand aus dem Internet übernommen hat, steht dann mitten in deinem Netz, direkt neben dem Rechner mit deinen Bankunterlagen. Fachleute sprechen von einem flachen Netz: eine einzige Ebene ohne Trennwände.

Jana kennt das Problem aus eigener Erfahrung. Vor einem Jahr hat sich herausgestellt, dass eine billige WLAN-Kamera, die Mehmet für den Balkon gekauft hatte, ständig Verbindungen zu Servern in aller Welt aufbaute. Niemand wusste, warum. Die Kamera kam weg, aber die Frage blieb: Was machen eigentlich die anderen Geräte?

1.2 Was ein Homelab ist

Ein Homelab ist, ganz wörtlich, ein Labor zu Hause. Der Begriff kommt aus der IT-Welt, wo Fachleute zu Hause mit Servern und Netzwerktechnik experimentieren, um Neues zu lernen. Im Laufe der Jahre ist daraus mehr geworden. Heute versteht man unter einem Homelab meist einen oder mehrere kleine Rechner, die zu Hause eigene Dienste bereitstellen: einen Werbefilter, eine

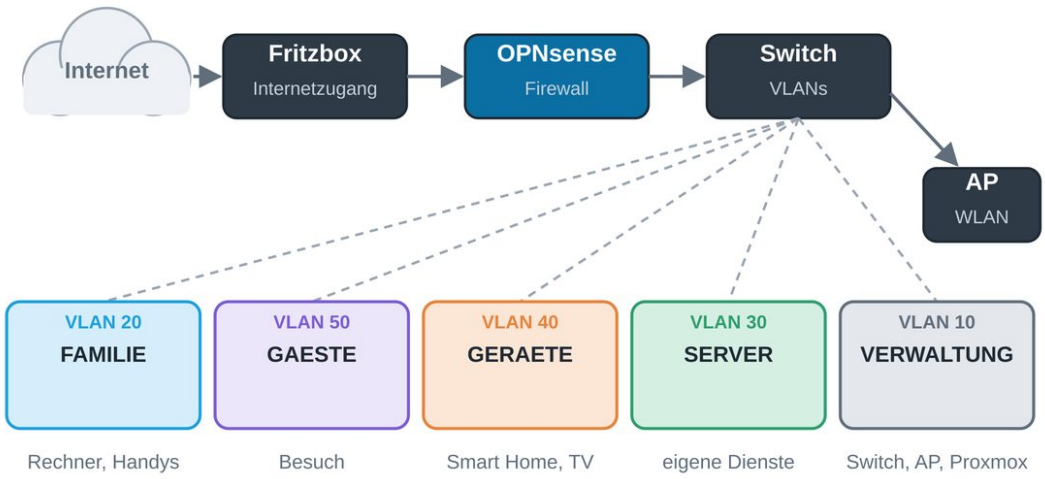
Fotoverwaltung, einen Passwortmanager, eine Hausautomation, einen Speicher für Dokumente.

Ein Homelab muss weder laut noch groß noch teuer sein. Ein moderner Mini-PC von der Größe eines Buches, der weniger Strom braucht als eine Energiesparlampe, reicht für alles, was in diesem Buch vorkommt. Du brauchst keinen Serverschrank, keine Klimaanlage und keinen Keller. Janas Homelab steht im Flurschrank neben der Fritzbox.

Wichtig ist dabei der Unterschied zwischen Labor und Betrieb. In einem Labor darf etwas kaputtgehen; man lernt daraus. Im Betrieb dagegen sollen Dinge zuverlässig laufen. Dein Heimnetz und die Dienste, auf die sich deine Familie verlässt, gehören zum Betrieb. Dieses Buch hilft dir, beides zu trennen: Du lernst und probierst, ohne dass das Internet der Familie davon abhängt.

1.3 Was du am Ende hast

Am Ende dieses Buches hast du ein Heimnetz, das in mehrere getrennte Bereiche aufgeteilt ist. Jeder Bereich ist ein eigenes Netz mit eigenen Regeln. Die Familie kann ins Internet und auf die eigenen Dienste zugreifen. Gäste kommen nur ins Internet. Smarte Geräte dürfen nur das, was sie unbedingt brauchen. Deine Server sind von den übrigen Geräten abgeschirmt und nur über die vorgesehenen Wege erreichbar.



Das Ziel: ein aufgeräumtes Heimnetz mit getrennten Bereichen

Dazu kommen zentrale Dienste, die allen zugutekommen. Ein Werbefilter blockiert Werbung und Tracker für jedes Gerät im Haus, auch für den Fernseher und die Spielkonsole, auf denen sich kein Werbeblocker installieren lässt. Eigene Namen im Netz ersetzen kryptische Adressen: Statt 10.10.30.20 tippst du `fotos.deine-domain.de` in den Browser, und die Seite hat sogar ein gültiges Zertifikat. Eine gemeinsame Anmeldung sorgt dafür, dass du nicht für jeden Dienst ein eigenes Passwort brauchst. Eine Datensicherung schützt vor dem Verlust, und ein sicherer Fernzugang bringt all das auf dein Handy, wenn du unterwegs bist.

1.4 Die Bausteine im Überblick

Die Technik hinter diesem Ziel besteht aus wenigen Bausteinen, die du in den folgenden Kapiteln nacheinander kennenlernst.

Baustein	Aufgabe	Kapitel
Fritzbox	Verbindung zum Internet, wie bisher	3, 11
OPNsense	Firewall, trennt die Netze und regelt den Verkehr	11 bis 13

Baustein	Aufgabe	Kapitel
Managed Switch	verteilt die getrennten Netze über Kabel	10
Access Point	verteilt die getrennten Netze per WLAN	14
Proxmox VE	Plattform für virtuelle Maschinen und Container	5 bis 8
Pi-hole oder AdGuard Home	Werbefilter und Namensauflösung	15 bis 17
Docker	einfacher Betrieb vieler kleiner Dienste	18
Reverse Proxy	schöne Namen und echte Zertifikate	19
authentik	gemeinsame Anmeldung für alle Dienste	21
WireGuard oder Tailscale	sicherer Fernzugang ohne offene Ports	22

Das sieht nach viel aus, aber du baust es nicht auf einmal. Jedes Kapitel fügt einen Baustein hinzu, und nach jedem Kapitel funktioniert dein Netz. Wenn du nach Kapitel 15 aufhörst, hast du bereits ein getrenntes Netz mit Werbefilter, und das ist mehr, als die meisten Haushalte je haben werden.

1.5 Was ein Homelab kostet

Ein Homelab kostet Geld, Strom und Zeit. Ehrlicherweise solltest du alle drei Posten kennen, bevor du anfängst.

Für die Hardware rechnest du mit 500 bis 900 Euro: eine kleine Firewall-Box, ein Mini-PC als Server, ein managed Switch, ein Access Point mit mehreren WLAN-Netzen und eine externe Festplatte für die Datensicherung. Kapitel 4 und Anhang A nennen Preisspannen für jedes Teil. Wer schon einen alten Rechner hat, kann klein anfangen und später aufrüsten.

Beim Strom liegen moderne Mini-PCs mit sparsamen Prozessoren im Leerlauf bei etwa 8 bis 15 Watt. Zusammen mit Switch und Access Points kommst du auf etwa 30 bis 50 Watt im Dauerbetrieb. Das sind im Jahr rund 260 bis 440 Kilowattstunden, bei einem Strompreis von 35 Cent je Kilowattstunde also etwa 90 bis 150 Euro. Ein alter Bürorechner aus dem Gebrauchtmarkt kann dagegen schnell das Dreifache verbrauchen.

Die Zeit ist der größte Posten. Plane für den Aufbau mehrere Wochenenden ein. Danach brauchst du etwa eine Stunde im Monat für Updates und Kontrolle. Dafür sparst du an anderer Stelle: Abos für Cloudspeicher, Passwortmanager und Fotodienste können wegfallen, und du verstehst dein Netz so gut, dass dich Probleme nicht mehr ratlos zurücklassen.

> **Hinweis:** Software kostet in diesem Buch nichts. Alle vorgestellten Programme sind Open Source und kostenlos nutzbar. Manche Projekte bieten kostenpflichtige Abos für Unterstützung oder Zusatzfunktionen an; für ein Heimnetz brauchst du sie nicht. Wenn dir ein Projekt gefällt, ist eine Spende trotzdem eine gute Idee.

1.6 Die drei Grundregeln

Bevor es losgeht, drei Regeln, die sich durch das ganze Buch ziehen.

Erstens: Kein offener Port ins Internet. In diesem Buch öffnest du an deinem Router keine einzige Portfreigabe für deine Dienste. Was aus dem Internet erreichbar ist, wird auch angegriffen, rund um die Uhr, von automatisierten Programmen. Für den Zugriff von unterwegs verwendest du ein VPN, das in Kapitel 22 eingerichtet wird. So bleiben deine Dienste für Fremde unsichtbar.

Zweitens: Immer einen Weg zurück. Bevor du etwas umbaust, überlegst du, wie du es rückgängig machst. Die Fritzbox bleibt zunächst unverändert und kann jederzeit wieder die ganze Arbeit übernehmen. Von jeder Konfiguration gibt es eine Sicherung. Und es gibt ein Notfallblatt, auf dem steht, wie die Familie wieder ins Internet kommt, falls du gerade nicht da bist.

Drittens: Aufschreiben. Jede Adresse, jedes Gerät, jede Regel und jede Entscheidung gehört in deine Dokumentation. Ein Netz, das nur in deinem Kopf existiert, ist ein Netz, das niemand außer dir reparieren kann, und auch du nur, solange du dich erinnerst.

1.7 Werkstatt: Deine Ziele aufschreiben

Bevor du ein einziges Gerät kaufst, schreib auf, was du erreichen willst. Nimm dein Notizheft oder eine Textdatei und beantworte vier Fragen. Welche Probleme hat dein Netz heute? Welche Dienste möchtest du selbst betreiben? Wer in deinem Haushalt ist von Änderungen betroffen? Wie viel Zeit und Geld willst du investieren?

Jana hat ihre Antworten auf eine Seite geschrieben. Probleme: zu viele unbekannte Geräte im Netz, keine Datensicherung der Kundenfotos, Werbung auf dem Fernseher, ständig vergessene Passwörter. Wunschdienste: Werbefilter, Fotoverwaltung, Passwortmanager, Dokumentenarchiv. Betroffene: Mehmet arbeitet ebenfalls von zu Hause und braucht stabiles Internet für Videokonferenzen, Leo braucht WLAN für Schule und Spiele. Budget: etwa 800 Euro, verteilt auf zwei Monate, und zwei Wochenenden im Monat.

Bewahre diese Seite auf. In Kapitel 28 nimmst du sie wieder zur Hand und prüfst, was du erreicht hast.

1.8 Vertiefung: Wann ein Homelab nicht die richtige Wahl ist

Ein Homelab ist nicht für jeden die beste Lösung. Wenn du keine Lust hast, dich um Updates zu kümmern, ist ein gepflegter Clouddienst sicherer als ein vergessener Server im Schrank. Wenn deine Familie auf ständig verfügbares Internet angewiesen ist und niemand außer dir die Technik versteht, brauchst du einen sehr klaren Notfallplan. Und wenn du nur einen Werbefilter willst, reicht ein Raspberry Pi mit Pi-hole an der Fritzbox; dafür musst du nicht das ganze Netz umbauen.

Sei ehrlich zu dir selbst. Die beste Technik ist die, die du auch in zwei Jahren noch pflegst. Dieses Buch ist so aufgebaut, dass du an vielen Stellen aufhören kannst und trotzdem ein besseres Netz hast als vorher. Du entscheidest, wie weit du gehst.