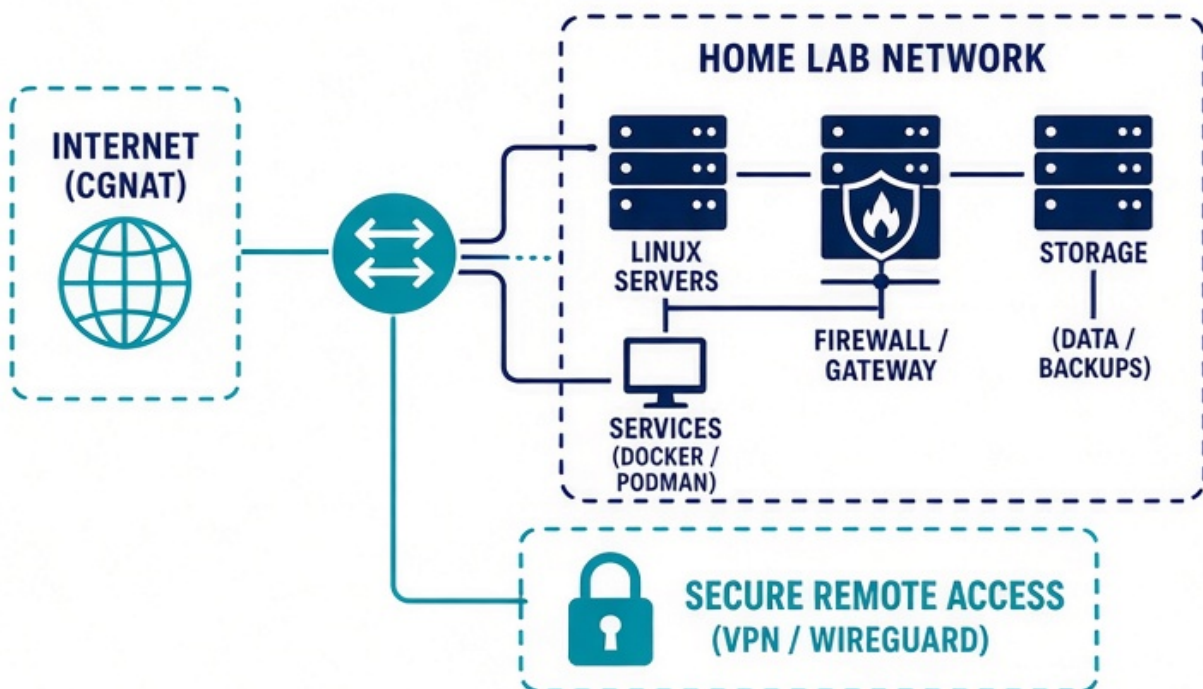


MODERN LINUX HOME LAB FOR SELF-HOSTERS BEHIND CGNAT

DESIGN, IMPLEMENT,
AND TROUBLESHOOT
ROBUST SELF-HOSTED
INFRASTRUCTURE ON THE REAL INTERNET



AMIR HASSAN

Modern Linux Home Lab for Self-Hosters Behind CGNAT

Design, Implement, and Troubleshoot Robust Self-Hosted
Infrastructure on the Real Internet

Steve Publications

This book is available at

<https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>

This version was published on 2026-09-29



This is a [Leanpub](#) book. Leanpub empowers authors and publishers with the Lean Publishing process. [Lean Publishing](#) is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

© 2026 Steve Publications

Contents

Design, Implement, and Troubleshoot Robust Self-Hosted Infrastructure on the Real Internet	1
Introduction: Why Self-Hosting Is a Networking Problem	2
Chapter 1: The Self-Hosting Connectivity Problem	4
The Promise and the Gap: Why Self-Hosting Is Harder Now Than Five Years Ago	4
Residential Internet Topologies: What Your ISP Actually Gives You . .	5
The Three Core Problems: No Inbound IPv4, Unstable IPv6, Broken DNS Assumptions	6
What This Book Will Not Assume	7
How to Use This Book	8
Chapter 2: How the Internet Connects to Your Home	11
The ISP Edge: Broadband Network Gateways, DSLAMs, OLTs, and Cable Modems	11
Customer Premises Equipment: Routers, Modems, and the Home Gateway Problem	12
Your LAN Topology: Single Router, Multiple Routers, and Double NAT	13
Packet Path from Your Server to the Internet and Back	14
Where Restrictions Happen: ISP-Imposed Constraints on Inbound Traffic	15
Identifying Your Actual Topology: Discovery Techniques	16
Chapter 3: IP Addressing, IPv4 Exhaustion, and CGNAT	18
Public vs Private IP Addresses and RFC 1918	18
IPv4 Exhaustion: Timeline, Impact, and Why It Matters to You	18
Carrier-Grade NAT: How It Works and What It Hides	18
CGNAT vs Double NAT: How to Tell the Difference	18
The Self-Hosting Impact: Why Port Forwarding Fails Under CGNAT .	18

Living With CGNAT: Options and Trade-Offs	19
Chapter 4: Linux Networking Fundamentals	20
Network Interfaces: Physical, Virtual, Loopback, and Tunnel Interfaces	20
IP Address Configuration: Interfaces, Addresses, and Scope	20
The Routing Table: How Linux Decides Where to Send Packets	20
Forwarding, Connection Tracking, and the Netfilter Stack	20
Network Namespaces: Isolation, VRFs, and Virtual Routers	21
Inspecting State: ip, ss, route, and the /proc/net Interface	21
Chapter 5: DNS as Infrastructure	22
Recursive vs Authoritative DNS and the Resolution Chain	22
Local DNS Resolution on Linux: systemd-resolved, NetworkManager, and resolv.conf	22
DNS Record Types That Matter: A, AAAA, CNAME, SRV, TXT, PTR	22
Caching, TTLs, and Stale DNS Problems	22
Split-Horizon DNS: Resolving Internally and Externally Differently	22
DNSSEC: Concepts and Practical Reality for Self-Hosters	23
DNS, Certificates, and SNI: The Trust Chain	23
Chapter 6: Firewalls, nftables, and Connection Tracking	24
Netfilter: Hooks, Chains, and the Packet Path Through the Kernel	24
nftables Syntax: Tables, Chains, Sets, Maps, and Rules	24
Connection Tracking: States, Expectations, and Stateful Filtering	24
Default Policies: Deny, Allow, and Reasonable Middle Ground	24
NAT in nftables: SNAT, DNAT, Masquerade, and Hairpin	25
Logging, Rate Limiting, and Detecting Reconnaissance	25
Firewall Design for Self-Hosted Environments	25
Chapter 7: Linux Routing Engineering	26
Route Selection: Longest Prefix Match and Route Metrics	26
Multiple Routing Tables: Main, Local, and Custom Tables	26
Policy-Based Routing: fwmark, Sources, and Destinations	26
Asymmetric Routing: Causes, Symptoms, and Solutions	26
VRFs and Network Namespaces for Traffic Separation	26
Debugging Routing Problems: tracepath, traceroute, and tcpdump Correlation	27
Common Routing Mistakes in Self-Hosting	27
Chapter 8: IPv6 for Self-Hosting	28

IPv6 Addressing: Global Unicast, Link-Local, Unique Local, and Special Ranges	28
SLAAC, Router Advertisements, and Stateless Address Assignment . .	28
DHCPv6 and Stateful IPv6 Configuration	28
IPv6 Prefix Delegation: How It Works and Why It Matters	28
Stable Addresses: DHCPv6-PD with Static Lease, Stable SLAAC, and Trade-Offs	28
Firewalling IPv6: Common Mistakes and Complete Policies	29
IPv6, DNS, and Certificates: AAAA Records and SNI	29
When Your ISP Changes the Prefix: Detection, Reaction, and Automation	29
Chapter 9: NAT and Port Forwarding Mechanics	30
How NAT Works: Packet Rewriting, State Tables, and Port Mapping .	30
Port Forwarding: Configuration, Topology, and Packet Flow	30
Hairpin NAT and NAT Loopback: Why It Fails by Default	30
NAT Traversal Assumptions: Cone NAT, Symmetric NAT, and Endpoint Independence	30
When Port Forwarding Fails: CGNAT, ISP Blocking, and Port Conflicts	31
NAT and IPv6: The Fundamental Incompatibility	31
Chapter 10: WireGuard Fundamentals	32
WireGuard Protocol: Noise Framework, Encryption, and Handshake .	32
Key Generation and Identity: The Public-Key Model	32
Configuration Semantics: ListenPort, Endpoint, and AllowedIPs	32
How AllowedIPs Works: Routing Decisions and Traffic Selection	32
WireGuard and the Linux Kernel: Tunnel Interfaces and Routing	32
Persistent Keepalives: Why They Exist and When You Need Them . .	33
Common Configuration Mistakes and Their Symptoms	33
WireGuard Monitoring with wg and wg-queue	33
Chapter 11: VPN Architectures for Self-Hosting	34
Road-Warrior Access: Remote Client to Home Network	34
Full-Tunnel vs Split-Tunnel: Security, Performance, and Convenience	34
Site-to-Site VPNs: Connecting Segments and Branches	34
Hub-and-Spoke vs Mesh Topologies	34
Subnet Routing Through WireGuard: AllowedIPs as Route Control . .	34
WireGuard with NAT Behind the VPN: Client and Server Considerations	35
Comparing WireGuard, IPsec, and OpenVPN for Self-Hosting	35

Chapter 12: Reverse Tunnels and Outbound-Only Connectivity 36

 The Outbound-Only Strategy: Why Tunnel Out Instead of Waiting
 Inbound 36

 SSH Reverse Tunnels: Local Port Forwarding in Reverse 36

 Reverse WireGuard: Client-Initiated Connections to a VPS Server . . . 36

 Relay Architectures: VPS as Public Ingress, Tunnel Back Home 36

 Rendezvous and Hole Punching: When and Why They Work 37

 Managed Reverse Tunnel Services: Tailscale, ZeroTier, Cloudflare
 Tunnel, and Alternatives 37

 Designing a CGNAT-Safe Architecture Using Reverse Tunnels 37

Chapter 13: Dynamic DNS and Name Resolution for Self-Hosters 38

 Dynamic DNS: How It Works and Provider Options 38

 Self-Hosted Authoritative DNS: BIND, CoreDNS, and dnsmasq 38

 Split-Horizon DNS Implementations: Internal vs External Records . . 38

 Service Discovery in Homelabs: mDNS, DNS-SD, and Simple DNS-
 Based Approaches 38

 Wildcard Certificates and Dynamic DNS: Combining Them 39

 Handling IPv6 Prefix Changes with DNS: Automation and Scripting . . 39

 DNS over TLS and DNS over HTTPS for Resolver Privacy 39

Chapter 14: Reverse Proxies as Internet Ingress 40

 The Reverse Proxy Role: Ingress Control, TLS Termination, and Back-
 end Routing 40

 HTTP Reverse Proxying: Host Headers, Paths, and Upstream Routing 40

 TCP Proxying: Exposing Non-HTTP Services Through a Single Ingress 40

 SNI and Multi-Domain TLS Termination 40

 TLS Certificates: ACME, Certbot, Let’s Encrypt, and Automation . . . 41

 Authentication, Headers, and Trust: Forwarding Auth and Preserving
 Client Info 41

 Rate Limiting, Access Control, and Protection at the Edge 41

 Comparing nginx, Caddy, and HAProxy for Self-Hosting Ingress 41

Chapter 15: Container Networking for Self-Hosted Services 42

 Docker Networking Drivers: Bridge, Host, None, and Overlay 42

 Docker Bridge Networks: NAT, Port Publishing, and Packet Flow . . . 42

 Container-to-Host Communication and Host Firewall Interactions . . 42

 Docker Compose Networking: Services, Internal Networks, and DNS . 42

 Network Policies and Container Isolation 43

Running WireGuard and Tunnels in Containers	43
Container Networking Best Practices for Self-Hosting	43
Chapter 16: Reference Architecture One: Single Machine Home Server	44
Requirements and Design Decisions	44
Network Topology and Addressing	44
Base System: Interfaces, Routing, and nftables Firewall	44
DNS Configuration: Domain, Records, and Resolution	44
Reverse Proxy: nginx or Caddy with TLS Automation	44
Service Deployment: Example Services and Exposure	45
Security Hardening: SSH, User Accounts, and Least Privilege	45
Operational Checklist and Troubleshooting Hints	45
Chapter 17: Reference Architecture Two: Multi-Host Homelab with VPN Access	46
Requirements: Segmentation, Remote Access, and Internal Communication	46
Network Topology: Subnets, Gateways, and Addressing Plan	46
WireGuard VPN: Road-Warrior and Hub-and-Spoke Configuration	46
Internal DNS: Authoritative Resolution Across Subnets	46
Inter-Subnet Routing and Firewall Policy	47
Reverse Proxy Across Multiple Backend Servers	47
Container Host Integration: Docker on the Homelab Network	47
Complete Working Configuration: All Components Integrated	47
Chapter 18: Reference Architecture Three: CGNAT Survival With VPS Relay	48
Requirements: No Inbound IPv4, Unreliable IPv6, Full Public Access	48
VPS Selection and Cost Considerations	48
Reverse WireGuard Tunnel: Server on VPS, Client at Home	48
Route Propagation: Which Traffic Goes Through the Tunnel	48
DNS and Dynamic DNS With the VPS as Authoritative Edge	49
Reverse Proxy on VPS: Terminating TLS and Forwarding Through Tunnel	49
IPv6 as Primary When Available: Failover and Dual-Stack Strategy	49
Security Model: Trust Boundaries, Tunnel as Perimeter, and Risk Assessment	49
Complete Working Configuration	49
Chapter 19: Reference Architecture Four: IPv6-Enabled Homelab With Dynamic Prefix	51

Requirements: Stable Self-Hosting With a Changing Delegated Prefix	51
Prefix Delegation Configuration: systemd-networkd, radvd, and DHCPv6	51
Stable Address Assignment: DHCPv6-PD With Static Leases	51
DNS Automation: Updating Records When the Prefix Changes	51
nftables Policies for IPv6: Matching Both Families	52
Reverse Proxy With IPv6 and AAAA Records	52
IPv6 Firewalling Mistakes to Avoid	52
Complete Working Configuration	52
Chapter 20: Security Architecture for Self-Hosted Infrastructure . . .	53
Threat Modeling for Self-Hosters: What You Are Protecting Against .	53
Attack Surfaces: Internet-Facing Services, VPNs, and Internal Services	53
Network Segmentation as Defense: Isolating Critical Services	53
Least Privilege: Services, Users, Containers, and Tunnels	53
SSH Hardening: Keys, Configuration, and Access Patterns	54
VPN Key Management: Rotation, Revocation, and Multi-Peer Policies	54
TLS Lifecycle: Certificate Renewal, Revocation, and Monitoring	54
Secrets Management in Self-Hosting: Avoiding Hardcoded Credentials	54
Logging, Monitoring, and Intrusion Detection	54
IPv6 Exposure: The Forgotten Attack Surface	55
Supply Chain and Container Image Security	55
The Difference Between Being Reachable and Being Secure	55
Chapter 21: Observability and Systematic Troubleshooting	56
Troubleshooting Methodology: From Symptom to Packet Path	56
Essential Tools: ip, ss, tcpdump, dig, nft, conntrack, traceroute, curl, openssl	56
Reading tcpdump Output: Filtering, Decoding, and Following Connections	56
Diagnosing DNS Problems: dig, resolvectl, and Cache Issues	56
Diagnosing Firewall Blocks: nft Logs, conntrack State, and Rule Tracing	57
Diagnosing Routing Problems: ip route, Policy Routing Checks, and Asymmetry	57
Diagnosing WireGuard Problems: wg Show, Endpoint Reachability, and AllowedIPs	57
Diagnosing Reverse Proxy Issues: Upstream Failures, SNI, and Protocol Mismatch	57
Common Failure Scenarios and Their Diagnoses	57

Building Observability: Logging, Metrics, and Alerting for Self-Hosted Networks	58
Chapter 22: Operations, Reliability, and Future-Proofing	59
System Updates: Patching Without Downtime for Critical Services . .	59
Configuration Management: Git, Ansible, or Script-Based Approaches	59
Backups: Configuration, Data, Keys, and Recovery Procedures	59
Monitoring: Uptime Checks, Service Health, and Alerting	59
Handling ISP Changes: Address Changes, Prefix Changes, and Topol- ogy Changes	60
Disaster Recovery: When the Home Server Is Unreachable	60
Documentation: Documenting Your Architecture While It Is Fresh . .	60
Future Trends: What Self-Hosters Should Watch	60
Conclusion	61
References	62

Design, Implement, and Troubleshoot Robust Self-Hosted Infrastructure on the Real Internet

This book explains how to design, build, and run self-hosted services on Linux that are accessible from anywhere on the Internet despite the constraints of modern residential broadband: carrier-grade NAT, missing inbound IPv4 connectivity, changing IPv6 prefixes, ISP firewalling, and double NAT. It treats networking as engineering rather than configuration: you will learn how packets move through interfaces, bridges, tunnels, firewalls, and reverse proxies; how Linux makes routing decisions; how WireGuard selects and encrypts traffic; how DNS interacts with routing and service discovery; and how to build architectures that survive real-world connectivity problems using outbound-only tunnels, VPS relays, IPv6 when stable, VPNs for secure access, and reverse proxies as ingress control planes. The book provides complete, internally consistent reference architectures with full working configurations for WireGuard, nftables, systemd-networkd, BIND and CoreDNS, nginx and Caddy, Docker, and SSH, plus systematic troubleshooting methods based on packet-path analysis rather than guesswork.

Introduction: Why Self-Hosting Is a Networking Problem

Five years ago, self-hosting was simple: you got a public IPv4 address from your ISP, you opened a port on your router, and your services were reachable. That model is dying. IPv4 exhaustion has forced ISPs to deploy carrier-grade NAT on residential connections, hiding thousands of customers behind a handful of public addresses. IPv6 brings a return to end-to-end connectivity but introduces its own problems with unstable delegated prefixes and incomplete ISP support. The tutorials that tell you to forward ports and point DNS at your home IP assume conditions that most residential connections no longer provide.

This book exists because modern self-hosting has become fundamentally a connectivity engineering problem. You are not just running services. You are building an architecture that must survive upstream constraints you cannot control: an ISP that changes your IPv6 prefix without warning, a CGNAT device that blocks all inbound IPv4 traffic, a residential gateway that you cannot fully configure, or a double-NAT topology that makes traditional port forwarding impossible. Success requires understanding the underlying mechanisms well enough to design around those constraints rather than fighting them.

The central thesis of this book is straightforward: when inbound connectivity is unreliable or unavailable, you must design architectures that work from the inside out. Outbound connections are almost universally permitted on residential networks. Inbound connections are increasingly blocked. Therefore robust self-hosting uses outbound tunnels, reverse proxies on public relay servers, encrypted VPNs initiated from your own network, and IPv6 when the ISP provides it stably. These techniques are not workarounds. They are the correct architectural response to the reality of modern Internet infrastructure.

This book is written for people who already understand basic Linux and networking. It assumes you can SSH into a server, edit configuration files, and understand that an IP address identifies a network interface. What it does not assume is that you understand how packets flow through a Linux kernel, how connection tracking enables stateful firewalls, how WireGuard uses AllowedIPs

to make routing decisions, how IPv6 prefix delegation interacts with router advertisements, or how to systematically diagnose why a connection fails across a complex network topology. Those are the gaps this book fills.

The structure builds progressively from foundations to complete architectures. The first few chapters establish the networking concepts and constraints that make self-hosting difficult. The middle chapters go deep into the core technologies: Linux routing and firewalls, IPv6, WireGuard, DNS, reverse proxies, and container networking. The later chapters combine those pieces into complete reference architectures for real-world scenarios: a single-machine home server, a multi-host homelab with VPN access, a CGNAT-constrained setup using a VPS relay, and an IPv6-first homelab with dynamic prefix handling. Throughout, security and observability are treated as integral parts of the design, not afterthoughts.

By the end of this book you will be able to reason about your self-hosting network from first principles. You will understand the packet path from an Internet client to your service under various topologies. You will know which architectural pattern works for your connectivity constraints and why. You will have complete working configurations you can adapt. And when things break, which they will, you will have the diagnostic toolkit to find the exact point of failure without guesswork.

The book focuses on open-source, self-managed technologies because that is what self-hosting means. Where managed services like Tailscale, Cloudflare Tunnel, or managed DNS are relevant, they are discussed as architectural options, not as replacements for understanding. You should be able to use those tools without depending on them.

Chapter 1: The Self-Hosting Connectivity Problem

The Promise and the Gap: Why Self-Hosting Is Harder Now Than Five Years Ago

Self-hosting began as an act of independence: instead of paying a monthly fee for hosted software, you run it on your own hardware. You control the data, the configuration, the updates. That promise has not changed, but the network conditions under which self-hosting operates have become significantly harder.

Ten years ago, most residential broadband connections came with a public IPv4 address assigned directly to your home router. You could log into that router, configure a port forward from port 80 or 443 to your internal server, set up dynamic DNS to handle address changes, and your services were globally reachable. That topology was not ideal, but it worked, and a vast body of tutorials assumed it existed.

Today that topology is increasingly rare. IPv4 address exhaustion has forced ISPs to conserve their public address pools by deploying carrier-grade NAT on residential connections. Your home router now receives a private address from the ISP instead of a public one. The public address belongs to the ISP's equipment, not to you, and you have no control over its port mappings. Port forwarding on your router does nothing useful because the upstream ISP NAT device has no idea what ports you want open.

IPv6 was meant to solve this problem by restoring end-to-end connectivity, but in residential deployments it has introduced a different set of problems. ISPs typically delegate IPv6 prefixes to residential customers dynamically, and they can change those prefixes periodically, after router reboots, or at arbitrary intervals. A service that was reachable yesterday at 2001:db8:1234::10 may be unreachable today because the ISP changed the prefix to 2001:db8:efgh:5678::. Dynamic DNS and DNS automation can handle this, but only if the ISP supports

stable prefix delegation or if you build automation to update records on every change, and only if the client actually uses IPv6.

Beyond addressing, ISPs frequently impose restrictions that further complicate self-hosting. Residential plans often block common server ports like 80 and 443 entirely, or implement aggressive ingress filtering that drops unsolicited incoming connections. Some ISPs run firewalls that block protocols associated with self-hosting, such as WireGuard's UDP port or SSH on unusual ports. Mobile broadband, satellite internet, and some cable providers deploy particularly restrictive NAT configurations that make inbound connectivity effectively impossible.

The gap between promise and reality is now substantial. You want a globally reachable service. The network conditions available to you are designed for outbound consumption, not inbound hosting. The tutorials tell you to open ports. Your ISP's equipment prevents it. This book addresses that gap directly.

Residential Internet Topologies: What Your ISP Actually Gives You

To design a working self-hosting architecture, you need to understand exactly what network conditions you have. This starts with identifying your actual topology from the ISP to your LAN. The common patterns fall into a small number of categories, each with different implications for connectivity.

The simplest and most favorable topology is a direct public IP assignment. Your ISP's network terminates at your home with a single public IPv4 address on your router's WAN interface, and your router has full control over NAT and port forwarding. This is becoming rare but still exists on many business plans and some residential connections. If your router's WAN IPv4 address matches the public IP reported by external services like whatismyip.com, and that address is not in the RFC 6598 CGNAT range (100.64.0.0/10), you likely have this topology.

The next common pattern is carrier-grade NAT without ISP-supplied routing equipment. The ISP assigns your router a private address, typically from the 100.64.0.0/10 range reserved for CGNAT or sometimes from an RFC 1918 range, and the ISP's upstream equipment performs NAT to a shared pool of public addresses. In this topology, your router can configure NAT and port forwarding, but those settings affect only the translation between your LAN

and the ISP's private network. The upstream CGNAT device does not expose your ports to the Internet. This is increasingly common on residential plans.

A third pattern involves ISP-supplied gateway equipment running its own NAT, combined with your own router. The ISP provides a modem-router combo or optical network terminal with built-in routing. You connect your own router to it in router mode rather than bridge mode. Both devices perform NAT independently, creating a double-NAT topology. Your internal router's port forwards affect only the inner NAT, but the ISP's gateway controls the outer NAT and usually does not expose configuration for port forwarding. This pattern produces symptoms similar to CGNAT but is fundamentally different because the NAT layer is within your home, not at the ISP, and it can often be resolved by placing the ISP equipment in bridge mode.

Mobile broadband and satellite connections often implement the most restrictive topology. The ISP's equipment is entirely outside your control, the NAT is carrier-grade and symmetric, and there is typically no mechanism for port forwarding or PCP-based port control. Some mobile providers offer a small public IPv6 prefix that can enable inbound connectivity on IPv6, but the IPv4 path is effectively outbound-only.

Each of these topologies requires different architectural responses. With a direct public IP, traditional port forwarding and DNS work fine. With CGNAT, you must use reverse tunnels, VPS relays, or IPv6 if available. With double NAT, you can often resolve the problem by reconfiguring your home topology. With mobile broadband, you generally need to accept outbound-only connectivity and build accordingly. Identifying which topology you have is the first practical step, which we will address in detail in Chapter 2.

The Three Core Problems: No Inbound IPv4, Unstable IPv6, Broken DNS Assumptions

Modern residential self-hosting faces three fundamental connectivity problems that every architecture must address.

The first is the lack of inbound IPv4 connectivity. Under CGNAT, the ISP's NAT device has no static mapping from a public port to your private address and port. When an Internet client attempts to connect to the ISP's public IP on port 443, the CGNAT device has no record of an existing connection initiated by your server to that client, so it drops the packet. You cannot create that

mapping from inside your network because you do not control the CGNAT device. RFC 6888, which defines requirements for CGNAT, recommends supporting the Port Control Protocol so subscribers can create their own port mappings, but in practice very few ISPs have deployed PCP support on their CGNAT equipment. The practical result is that inbound IPv4 is effectively unavailable on most residential CGNAT connections, and any architecture that assumes you can receive inbound IPv4 connections will fail.

The second problem is IPv6 prefix instability. When an ISP delegates an IPv6 prefix to a residential customer via DHCPv6-PD or static assignment, that prefix is typically dynamic. The ISP may change it after a router reboot, on a scheduled cycle, when network infrastructure is reconfigured, or for reasons you cannot predict. Each global unicast IPv6 address for your services is constructed from the delegated prefix plus a subnet identifier plus a host identifier. When the prefix changes, all those addresses become invalid. DNS records pointing to the old prefix stop working until they are updated. The problem is compounded by the fact that many ISPs provide only a /60 or /56 prefix for residential customers, and some even change the prefix more aggressively than others. If you want stable IPv6-based self-hosting, you need either a provider that offers a static or long-term prefix, or automation that detects prefix changes and updates DNS records promptly.

The third problem is the breakdown of DNS assumptions. Traditional self-hosting tutorials assume a simple DNS setup: you have a domain name, you point its A record at your public IPv4 address, and clients resolve that address to reach you. This model fails when your IPv4 address changes frequently, when you have no public IPv4 address at all, when your IPv6 address changes periodically, or when you need different DNS answers for clients inside your network versus clients on the Internet. Dynamic DNS helps with changing addresses but requires that addresses be reachable in the first place. Split-horizon DNS solves the internal versus external problem but requires managing two sets of records and configuring internal clients to use your own DNS resolver. DNSSEC adds security but introduces complexity with key management and can interfere with split-horizon setups if not configured carefully. And all of this assumes that the client can actually route to the address DNS returns, which brings us back to the connectivity problem.

What This Book Will Not Assume

This book assumes technical competence but does not assume specialized networking knowledge. Specifically:

You are expected to be comfortable with a Linux command line. You can edit configuration files, restart services with `systemctl`, read log output with `journalctl`, and follow multi-step instructions without hand-holding. You understand that a shell prompt is your primary interface to the system.

You understand basic networking vocabulary. You know what an IP address, subnet mask, default gateway, and DNS server are. You have used commands like `ping` and `curl`. You understand that a router forwards packets between networks and that a firewall filters packets based on rules.

You understand the basics of configuration management for your own systems. You know that changes to configuration files typically require restarting the affected service. You understand that some systems manage networking through `systemd-networkd`, some through `NetworkManager`, and some through distribution-specific tools like `Netplan`.

You do NOT need to understand routing protocols like OSPF or BGP. This book covers static routing, policy routing, and the routing decisions Linux makes by default. Dynamic routing protocols are important in large networks but are rarely necessary for self-hosting at the residential scale.

You do NOT need deep experience with `iptables` or complex firewall configurations. We will build firewall configurations from the ground up using `nftables`, explaining every rule and its purpose.

You do NOT need to understand the internals of `WireGuard`, TCP/IP stacks, or DNS protocol specifications in detail before reading this book. Those topics are explained in the chapters where they are needed.

You do NOT need any specific hardware or infrastructure. The architectures in this book work with commodity hardware: a Raspberry Pi, an old laptop repurposed as a server, a mid-range mini-PC, a used server blade. A VPS costs as little as five dollars per month. The principles apply regardless of whether your network has one host or a dozen.

How to Use This Book

The book is structured as a progressive learning path. Read it in order. Each chapter introduces concepts that later chapters rely upon. The early chapters are not filler. They establish the mental model and terminology you need to understand the architectures in later chapters.

Chapters 1 through 3 establish the context: why self-hosting is harder today than it used to be, how residential Internet connections are structured, and why IPv4 addressing constraints matter. Read these chapters even if you think you already understand the material. The specific framing and terminology used here appear throughout the rest of the book.

Chapters 4 through 8 cover the core technologies that make modern self-hosting possible: Linux networking fundamentals, DNS as infrastructure, nftables firewalls, Linux routing engineering, and IPv6 in depth. These chapters are technical and detailed. They are the foundation. If you are already comfortable with these topics, you can skim the sections you know and focus on the areas where your knowledge is incomplete. But do not skip them entirely, because later chapters assume this knowledge.

Chapters 9 through 15 go deep into specific mechanisms and technologies: NAT mechanics, WireGuard fundamentals and architecture, reverse tunnels, DNS for self-hosters, reverse proxies, and container networking. Each of these chapters could be a standalone technical reference. Together they provide the complete toolkit.

Chapters 16 through 19 are complete reference architectures. Each one describes a specific scenario, walks through the requirements and design decisions, and provides complete working configurations for all components: addressing, routing, DNS, firewalls, tunnels, reverse proxies, and services. These chapters integrate everything from the earlier chapters into coherent systems. You can use these architectures as templates for your own setup, adapting them to your specific constraints and requirements.

Chapter 20 covers security architecture for self-hosted environments, and Chapter 21 covers systematic troubleshooting. Both chapters are substantial. Treat them as essential reading, not optional appendices. A self-hosted network that is not secure is not a network you can rely on, and a network you cannot troubleshoot systematically is a network you will eventually lose access to.

Chapter 22 covers operations and long-term reliability: updates, backups, monitoring, disaster recovery, and documentation. These topics are boring until you need them, which is exactly why you should read this chapter.

Throughout the book, configurations use specific IP addresses, domain names, and identifiers for clarity. These values are not arbitrary recommendations. They are concrete examples that form internally consistent networks. When you adapt them for your own use, you must change the values to match your actual network, but the relationships between those values must be preserved. Where a value must be changed, the text explicitly says so.

Every configuration in this book has been designed to work as written within its described architecture. If you follow the instructions and your system behaves differently, there is almost certainly a configuration mismatch, a topology difference, or a distribution-specific behavior that needs investigation. The troubleshooting chapter will help you find it.

Chapter 2: How the Internet Connects to Your Home

The ISP Edge: Broadband Network Gateways, DSLAMs, OLTs, and Cable Modems

To understand your home network, you need to understand how the Internet reaches it. The physical and logical path from the global Internet to your self-hosted server passes through multiple layers of infrastructure, each with its own characteristics and constraints.

For fiber-to-the-home connections, your ISP terminates fiber in an optical line terminal at the central office or neighborhood node. The fiber extends to your home where an optical network terminal converts optical signals to electrical Ethernet. The OLT is the ISP's routing endpoint for your connection. It assigns you an IP address, terminates authentication protocols like PPPoE or TR-069, and forwards your traffic to the ISP's core network. Some ISPs integrate CGNAT directly into the OLT, meaning your entire connection terminates inside a NAT device that the ISP controls.

For cable modem connections, the path runs from the ISP headend through hybrid fiber-coaxial plant to a node in your neighborhood, then to your cable modem via coaxial cable. The cable modem terminates in the ISP's cable modem termination system, which authenticates your device by MAC address and assigns an IP address. Cable ISPs have been deploying CGNAT extensively due to IPv4 exhaustion on shared cable networks. Your cable modem may receive a CGNAT private address instead of a public address.

For DSL connections, a DSLAM at the central office terminates your DSL line and connects to the ISP's network. DSLAMs typically provide PPPoE authentication and address assignment. The ISP's broadband network gateway handles routing and often NAT. DSL users are also increasingly behind CGNAT as ISPs run out of public IPv4 addresses.

Regardless of the physical medium, the logical structure is similar: your connection terminates at the ISP's access network equipment, which authen-

ticates your device, assigns an address, and forwards traffic. That access equipment connects to the ISP's core network, which routes traffic to the broader Internet. Somewhere in this path, the constraints that affect self-hosting are applied: CGNAT that hides your address, ingress filtering that drops inbound packets, port blocking that prevents server services, and DHCP configurations that change addresses periodically.

Customer Premises Equipment: Routers, Modems, and the Home Gateway Problem

At your home, the ISP's infrastructure connects to customer premises equipment that your ISP typically provides. This is where the home gateway problem begins. ISPs ship combined modem-router-WiFi-appliance devices designed for general consumers, not for self-hosting. These devices have limited configuration options, locked-down firmware, and interfaces optimized for casual use rather than network engineering.

The ISP gateway often performs routing, NAT, DHCP, WiFi access point functions, and sometimes firewalling and content filtering. When you connect your own Linux server to this gateway, your server is on the gateway's LAN with a private IP address. The gateway performs NAT between your LAN and the ISP's network. If the gateway receives a public IP from the ISP, this is a single-NAT topology that works for traditional port forwarding. If the gateway receives a CGNAT private address, your port forwards are pointless because the ISP's upstream NAT device controls external connectivity.

The most common mistake self-hosters make is accepting the ISP gateway in its default mode and trying to build a self-hosting network behind it. This creates unnecessary complexity and limitations. The correct approach in most cases is to place the ISP gateway in bridge mode if possible, which disables its routing and NAT functions and turns it into a simple modem. You then use your own router between the bridged modem and your LAN. This gives you full control over routing, NAT, DHCP, firewalling, and port forwarding. It also makes it easier to diagnose problems because you know exactly how the network is configured.

If the ISP gateway cannot be bridged, some ISPs offer IP passthrough, which assigns the public IP directly to your connected router's MAC address while the gateway remains in routing mode. This works similarly to bridge mode but

keeps the ISP gateway's basic routing active. It is less ideal than true bridge mode but better than running both routers in full routing mode.

When you have both an ISP gateway and your own router running in routing mode, you create a double-NAT topology. Your internal router's NAT operates on top of the ISP gateway's NAT. Port forwards on your router affect only the inner NAT translation. The ISP gateway still controls whether traffic reaches your router's WAN interface. If the gateway has its own firewall blocking inbound connections on common server ports, your port forwards never work regardless of how they are configured.

Your LAN Topology: Single Router, Multiple Routers, and Double NAT

Inside your home, the LAN topology can range from a single router connecting all devices to a complex multi-router setup with multiple subnets. For self-hosting, the simplest and most manageable topology is a single router with one LAN subnet, unless you specifically need segmentation for security or organizational reasons.

A single router topology means all your devices, including your server, connect to the same Layer 2 network, typically on the same 192.168.x.0/24 or 10.x.x.x/24 subnet. The router provides a single NAT between the LAN and the WAN. Port forwards on this router map external ports to internal IP addresses and ports. DNS queries from LAN devices are forwarded to external resolvers unless you run your own DNS server. This is simple to configure, simple to understand, and simple to troubleshoot.

Multiple router topologies appear when you extend coverage with additional WiFi access points that are actually routers, or when you deliberately segment your network into separate subnets. If you connect one router's LAN port to another router's WAN port, both routers perform NAT independently. A device behind the second router must cross two NAT layers to reach the Internet. This is double NAT. For self-hosting, double NAT is problematic because port forwarding must work on both routers in sequence, and most ISP gateways do not expose configuration for port forwarding.

Double NAT also breaks many features that self-hosters rely on. UPnP and NAT-PMP port mapping requests from your server reach only the inner router, not the outer one. P2P applications that depend on hole punching may fail

because symmetric NAT behavior at one of the NAT layers prevents direct connections. IPv6 prefix delegation may not propagate correctly through multiple routers. Some gaming consoles and smart home devices refuse to work properly behind double NAT.

The solution to unintentional double NAT is straightforward: use the second router as an access point or switch rather than as a router. Disable DHCP on the second device. Connect its LAN ports to the first router. Give the second device a management IP on the first router's subnet. Now both devices operate on the same Layer 2 network with a single NAT layer at the edge. This preserves WiFi coverage while eliminating the double NAT problem.

Intentional network segmentation is a different matter. For advanced self-hosting setups, you may want separate subnets for different trust levels: one for Internet-facing services, one for internal infrastructure, one for guest WiFi. This requires multiple subnets and routing between them. Later chapters cover how to implement this correctly with a single router or with multiple routers in a controlled configuration that does not create accidental double NAT.

Packet Path from Your Server to the Internet and Back

Understanding the packet path through your network is essential for both design and troubleshooting. Let me trace what happens when a client on the Internet attempts to reach a web service on your self-hosted server.

The client sends a TCP SYN packet to your server's public IP address and port 443. This packet traverses the Internet via the client's ISP, transit providers, and routing infrastructure until it reaches your ISP's edge router. Your ISP's router examines the destination IP address. If you have a direct public IP, the ISP routes the packet toward your home gateway. If you are behind CGNAT, the ISP's CGNAT device checks its translation table for a mapping from that public IP and port to a specific customer and port. If no mapping exists, which it will not for unsolicited inbound traffic, the CGNAT device drops the packet. This is the fundamental barrier to inbound connectivity under CGNAT.

If the packet reaches your home gateway and you have configured port forwarding, the gateway examines the destination port. If port 443 is forwarded to your server's internal IP address and port 443, the gateway rewrites the packet's destination IP address from its own WAN IP to your server's LAN IP,

and rewrites the destination port if you are mapping to a different internal port. The gateway records this translation in its NAT state table so it can rewrite return traffic. The packet then reaches your server on the LAN.

Your server's operating system receives the packet on its network interface. The kernel checks the destination IP and port against listening sockets. If a service is listening on port 443, the kernel delivers the packet to that service. The service responds with a TCP SYN-ACK packet. The response travels back through the same path in reverse: your server sends the response to the gateway, the gateway uses its NAT state table to rewrite the source address and port back to the public IP, and the response traverses the Internet back to the client.

This path assumes every device along the way allows the packet. Your ISP's network may have ingress filtering that drops packets destined for non-standard ports. Your home gateway may have a firewall blocking inbound connections. Your server may have a local firewall dropping packets that do not match its rules. Each potential drop point is a troubleshooting target. When a connection fails, you must determine which device along the path is responsible, which requires understanding the complete packet flow and checking each segment.

Where Restrictions Happen: ISP-Imposed Constraints on Inbound Traffic

Modern ISPs impose constraints on residential connections that directly limit self-hosting capability. These restrictions exist for legitimate reasons such as abuse prevention, network management, and protecting consumers from accidentally exposing vulnerable services. They also exist because ISPs have no incentive to make residential self-hosting easy.

The most common restriction is CGNAT, which we have already discussed. CGNAT eliminates inbound IPv4 connectivity by design. The ISP's NAT device has no mechanism for unsolicited inbound connections to reach your server because the translation table is populated only by outbound connections from your network.

Port blocking is another common restriction. Many ISPs block inbound connections on ports 80, 443, 25, and sometimes other commonly used server ports on residential plans. This prevents residential customers from running

web servers, mail servers, and other services that could generate abuse complaints or compete with the ISP's services. Even if you have a public IP address, your ISP's edge equipment may simply drop inbound packets on these ports.

Ingress filtering, sometimes called Unicast Reverse Path Forwarding, is a technique that drops packets with source addresses that cannot be routed back through the receiving interface. While primarily designed to prevent spoofing, aggressive ingress filtering can also affect NAT translations and complex routing setups. Some ISPs implement policies that drop any inbound packet that is not a response to an outbound connection, effectively making inbound connectivity impossible.

Asymmetric routing restrictions can also affect self-hosting. Some ISPs expect all traffic for a given subscriber to enter and leave through the same access point. If your network has multiple paths to the Internet, such as a bonded connection or a failover configuration, the ISP may drop return traffic that arrives on a different interface than the original outbound traffic left.

To determine what restrictions your ISP imposes, you need to test. The detection techniques in the next section will help you identify CGNAT, port blocking, and other constraints. Understanding your actual connectivity limits is essential for choosing the right architecture.

Identifying Your Actual Topology: Discovery Techniques

Before you can design a self-hosting architecture, you must know exactly what network conditions you have. Here are systematic techniques for identifying your topology.

First, determine whether your connection has a public IPv4 address or is behind CGNAT. Log into your home router and find its WAN or Internet IPv4 address. Compare this address to what external services report as your public IP. Use a command from any internal device:

```
1 dig +short myip.opendns.com @resolver1.opendns.com
```

This queries a public resolver that returns the source IP of the query, which is your external public IP. If your router's WAN IP matches the returned address and is not in the 100.64.0.0/10 range, you have a public IPv4 address. If your router's WAN IP is in the 100.64.0.0/10 range, you are behind CGNAT using the

standard shared address space. If your router's WAN IP is an RFC 1918 private address (192.168.x.x, 10.x.x.x, or 172.16-31.x.x) but differs from the external IP, you have some form of upstream NAT, which could be CGNAT or double NAT.

Second, use traceroute to see the path from your network to the Internet and identify NAT or routing layers:

```
1 traceroute -n 8.8.8.8
```

The first hop is your router. If the second hop is a private IP address that is not your router, you likely have double NAT with another router between you and the ISP's network. If you see addresses in the 100.64.0.0/10 range as an early hop, CGNAT is present in the ISP's network.

Third, test port forwarding capability. Configure your router to forward an uncommon port like 50080 to a device running a simple server. From an external network, use a port checking service or a simple connection test to verify whether the forwarded port is reachable. If the port is not reachable despite correct configuration, and you confirmed you have a public IP, your ISP may be blocking inbound connections on certain ports or at the edge.

Fourth, check IPv6 connectivity and prefix delegation status. On your Linux server, check for IPv6 addresses:

```
1 ip -6 addr show
```

Look for addresses beginning with 2000::/3, which indicates global unicast addresses from your ISP. Check for router advertisements and DHCPv6 activity with:

```
1 ip -6 neigh show
2 ip -6 route show
```

If you have global IPv6 addresses but they start with fe80::, you only have link-local addresses and no IPv6 Internet connectivity. If you have 2000::/3 addresses, you have IPv6 connectivity. To check for prefix delegation, look at your router's IPv6 configuration page or run a test with a DHCPv6 client to see if a prefix is delegated to you.

These discovery techniques establish your baseline connectivity. The rest of this book builds architectures that work within whatever constraints you find.

Chapter 3: IP Addressing, IPv4 Exhaustion, and CGNAT

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Public vs Private IP Addresses and RFC 1918

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

IPv4 Exhaustion: Timeline, Impact, and Why It Matters to You

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Carrier-Grade NAT: How It Works and What It Hides

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

CGNAT vs Double NAT: How to Tell the Difference

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

The Self-Hosting Impact: Why Port Forwarding Fails Under CGNAT

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Living With CGNAT: Options and Trade-Offs

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 4: Linux Networking

Fundamentals

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Network Interfaces: Physical, Virtual, Loopback, and Tunnel Interfaces

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

IP Address Configuration: Interfaces, Addresses, and Scope

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

The Routing Table: How Linux Decides Where to Send Packets

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Forwarding, Connection Tracking, and the Netfilter Stack

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Network Namespaces: Isolation, VRFs, and Virtual Routers

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Inspecting State: ip, ss, route, and the /proc/net Interface

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 5: DNS as Infrastructure

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Recursive vs Authoritative DNS and the Resolution Chain

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Local DNS Resolution on Linux: systemd-resolved, NetworkManager, and resolv.conf

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

DNS Record Types That Matter: A, AAAA, CNAME, SRV, TXT, PTR

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Caching, TTLs, and Stale DNS Problems

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Split-Horizon DNS: Resolving Internally and Externally Differently

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

DNSSEC: Concepts and Practical Reality for Self-Hosters

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

DNS, Certificates, and SNI: The Trust Chain

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 6: Firewalls, nftables, and Connection Tracking

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Netfilter: Hooks, Chains, and the Packet Path Through the Kernel

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

nftables Syntax: Tables, Chains, Sets, Maps, and Rules

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Connection Tracking: States, Expectations, and Stateful Filtering

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Default Policies: Deny, Allow, and Reasonable Middle Ground

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

NAT in nftables: SNAT, DNAT, Masquerade, and Hairpin

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Logging, Rate Limiting, and Detecting Reconnaissance

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Firewall Design for Self-Hosted Environments

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 7: Linux Routing Engineering

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Route Selection: Longest Prefix Match and Route Metrics

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Multiple Routing Tables: Main, Local, and Custom Tables

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Policy-Based Routing: fwmark, Sources, and Destinations

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Asymmetric Routing: Causes, Symptoms, and Solutions

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

VRFs and Network Namespaces for Traffic Separation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Debugging Routing Problems: tracepath, traceroute, and tcpdump Correlation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Common Routing Mistakes in Self-Hosting

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 8: IPv6 for Self-Hosting

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

IPv6 Addressing: Global Unicast, Link-Local, Unique Local, and Special Ranges

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

SLAAC, Router Advertisements, and Stateless Address Assignment

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

DHCPv6 and Stateful IPv6 Configuration

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

IPv6 Prefix Delegation: How It Works and Why It Matters

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Stable Addresses: DHCPv6-PD with Static Lease, Stable SLAAC, and Trade-Offs

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Firewalling IPv6: Common Mistakes and Complete Policies

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

IPv6, DNS, and Certificates: AAAA Records and SNI

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

When Your ISP Changes the Prefix: Detection, Reaction, and Automation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 9: NAT and Port Forwarding Mechanics

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

How NAT Works: Packet Rewriting, State Tables, and Port Mapping

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Port Forwarding: Configuration, Topology, and Packet Flow

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Hairpin NAT and NAT Loopback: Why It Fails by Default

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

NAT Traversal Assumptions: Cone NAT, Symmetric NAT, and Endpoint Independence

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

When Port Forwarding Fails: CGNAT, ISP Blocking, and Port Conflicts

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

NAT and IPv6: The Fundamental Incompatibility

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 10: WireGuard Fundamentals

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

WireGuard Protocol: Noise Framework, Encryption, and Handshake

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Key Generation and Identity: The Public-Key Model

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Configuration Semantics: ListenPort, Endpoint, and AllowedIPs

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

How AllowedIPs Works: Routing Decisions and Traffic Selection

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

WireGuard and the Linux Kernel: Tunnel Interfaces and Routing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Persistent Keepalives: Why They Exist and When You Need Them

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Common Configuration Mistakes and Their Symptoms

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

WireGuard Monitoring with wg and wg-queue

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 11: VPN Architectures for Self-Hosting

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Road-Warrior Access: Remote Client to Home Network

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Full-Tunnel vs Split-Tunnel: Security, Performance, and Convenience

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Site-to-Site VPNs: Connecting Segments and Branches

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Hub-and-Spoke vs Mesh Topologies

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Subnet Routing Through WireGuard: AllowedIPs as Route Control

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

WireGuard with NAT Behind the VPN: Client and Server Considerations

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Comparing WireGuard, IPsec, and OpenVPN for Self-Hosting

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 12: Reverse Tunnels and Outbound-Only Connectivity

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

The Outbound-Only Strategy: Why Tunnel Out Instead of Waiting Inbound

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

SSH Reverse Tunnels: Local Port Forwarding in Reverse

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Reverse WireGuard: Client-Initiated Connections to a VPS Server

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Relay Architectures: VPS as Public Ingress, Tunnel Back Home

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Rendezvous and Hole Punching: When and Why They Work

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Managed Reverse Tunnel Services: Tailscale, ZeroTier, Cloudflare Tunnel, and Alternatives

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Designing a CGNAT-Safe Architecture Using Reverse Tunnels

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 13: Dynamic DNS and Name Resolution for Self-Hosters

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Dynamic DNS: How It Works and Provider Options

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Self-Hosted Authoritative DNS: BIND, CoreDNS, and dnsmasq

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Split-Horizon DNS Implementations: Internal vs External Records

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Service Discovery in Homelabs: mDNS, DNS-SD, and Simple DNS-Based Approaches

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Wildcard Certificates and Dynamic DNS: Combining Them

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Handling IPv6 Prefix Changes with DNS: Automation and Scripting

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

DNS over TLS and DNS over HTTPS for Resolver Privacy

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 14: Reverse Proxies as Internet Ingress

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

The Reverse Proxy Role: Ingress Control, TLS Termination, and Backend Routing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

HTTP Reverse Proxying: Host Headers, Paths, and Upstream Routing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

TCP Proxying: Exposing Non-HTTP Services Through a Single Ingress

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

SNI and Multi-Domain TLS Termination

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

TLS Certificates: ACME, Certbot, Let's Encrypt, and Automation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Authentication, Headers, and Trust: Forwarding Auth and Preserving Client Info

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Rate Limiting, Access Control, and Protection at the Edge

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Comparing nginx, Caddy, and HAProxy for Self-Hosting Ingress

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 15: Container Networking for Self-Hosted Services

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Docker Networking Drivers: Bridge, Host, None, and Overlay

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Docker Bridge Networks: NAT, Port Publishing, and Packet Flow

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Container-to-Host Communication and Host Firewall Interactions

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Docker Compose Networking: Services, Internal Networks, and DNS

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Network Policies and Container Isolation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Running WireGuard and Tunnels in Containers

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Container Networking Best Practices for Self-Hosting

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 16: Reference Architecture

One: Single Machine Home Server

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Requirements and Design Decisions

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Network Topology and Addressing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Base System: Interfaces, Routing, and nftables Firewall

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

DNS Configuration: Domain, Records, and Resolution

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Reverse Proxy: nginx or Caddy with TLS Automation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Service Deployment: Example Services and Exposure

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Security Hardening: SSH, User Accounts, and Least Privilege

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Operational Checklist and Troubleshooting Hints

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 17: Reference Architecture

Two: Multi-Host Homelab with VPN Access

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Requirements: Segmentation, Remote Access, and Internal Communication

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Network Topology: Subnets, Gateways, and Addressing Plan

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

WireGuard VPN: Road-Warrior and Hub-and-Spoke Configuration

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Internal DNS: Authoritative Resolution Across Subnets

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Inter-Subnet Routing and Firewall Policy

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Reverse Proxy Across Multiple Backend Servers

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Container Host Integration: Docker on the Homelab Network

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Complete Working Configuration: All Components Integrated

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 18: Reference Architecture

Three: CGNAT Survival With VPS Relay

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Requirements: No Inbound IPv4, Unreliable IPv6, Full Public Access

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

VPS Selection and Cost Considerations

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Reverse WireGuard Tunnel: Server on VPS, Client at Home

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Route Propagation: Which Traffic Goes Through the Tunnel

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

DNS and Dynamic DNS With the VPS as Authoritative Edge

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Reverse Proxy on VPS: Terminating TLS and Forwarding Through Tunnel

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

IPv6 as Primary When Available: Failover and Dual-Stack Strategy

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Security Model: Trust Boundaries, Tunnel as Perimeter, and Risk Assessment

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Complete Working Configuration

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcnat>.

Chapter 19: Reference Architecture

Four: IPv6-Enabled Homelab With Dynamic Prefix

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Requirements: Stable Self-Hosting With a Changing Delegated Prefix

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Prefix Delegation Configuration: systemd-networkd, radvd, and DHCPv6

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Stable Address Assignment: DHCPv6-PD With Static Leases

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

DNS Automation: Updating Records When the Prefix Changes

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

nftables Policies for IPv6: Matching Both Families

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Reverse Proxy With IPv6 and AAAA Records

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

IPv6 Firewalling Mistakes to Avoid

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Complete Working Configuration

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 20: Security Architecture for Self-Hosted Infrastructure

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Threat Modeling for Self-Hosters: What You Are Protecting Against

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Attack Surfaces: Internet-Facing Services, VPNs, and Internal Services

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Network Segmentation as Defense: Isolating Critical Services

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Least Privilege: Services, Users, Containers, and Tunnels

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

SSH Hardening: Keys, Configuration, and Access Patterns

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

VPN Key Management: Rotation, Revocation, and Multi-Peer Policies

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

TLS Lifecycle: Certificate Renewal, Revocation, and Monitoring

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Secrets Management in Self-Hosting: Avoiding Hardcoded Credentials

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Logging, Monitoring, and Intrusion Detection

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

IPv6 Exposure: The Forgotten Attack Surface

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Supply Chain and Container Image Security

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

The Difference Between Being Reachable and Being Secure

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 21: Observability and Systematic Troubleshooting

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Troubleshooting Methodology: From Symptom to Packet Path

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Essential Tools: ip, ss, tcpdump, dig, nft, conntrack, traceroute, curl, openssl

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Reading tcpdump Output: Filtering, Decoding, and Following Connections

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Diagnosing DNS Problems: dig, resolvectl, and Cache Issues

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Diagnosing Firewall Blocks: nft Logs, conntrack State, and Rule Tracing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Diagnosing Routing Problems: ip route, Policy Routing Checks, and Asymmetry

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Diagnosing WireGuard Problems: wg Show, Endpoint Reachability, and AllowedIPs

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Diagnosing Reverse Proxy Issues: Upstream Failures, SNI, and Protocol Mismatch

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Common Failure Scenarios and Their Diagnoses

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Building Observability: Logging, Metrics, and Alerting for Self-Hosted Networks

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Chapter 22: Operations, Reliability, and Future-Proofing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

System Updates: Patching Without Downtime for Critical Services

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Configuration Management: Git, Ansible, or Script-Based Approaches

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Backups: Configuration, Data, Keys, and Recovery Procedures

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Monitoring: Uptime Checks, Service Health, and Alerting

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Handling ISP Changes: Address Changes, Prefix Changes, and Topology Changes

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Disaster Recovery: When the Home Server Is Unreachable

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Documentation: Documenting Your Architecture While It Is Fresh

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Future Trends: What Self-Hosters Should Watch

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

Conclusion

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.

References

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/modernlinuxhomelabforself-hostersbehindcgnat>.