Terminal Zero-Trust Port Hardening Checklist

Traditional port-forwarding leaves servers vulnerable to automated bot scans and brute-force attacks. This battle-tested checklist establishes an impenetrable zero-open-port perimeter using Cloudflare Tunnels and WireGuard.

⚡ VERIFIED PRODUCTION STACK | 💬 LEAD TRIGGER: "SCAN" | 🚀 VELOCITY: 10X LEVERAGE | 🔒 ZERO OPEN PORTS

0 Ports	100%	2FA / SSO	100Gbps+
OPEN PUBLIC ATTACK VECTORS	ORIGIN IP OBFUSCATION	HARDWARE KEY ACCESS POLICY	EDGE DDOS ABSORPTION

🔒 1. Zero-Trust Perimeter

CLOUDFLARE TUNNELS

- Outbound-Only Daemon: cloudflared connects outward to Cloudflare edge edge network.
- Zero Router Forwarding: No NAT port 80, 443, or 22 opened on home router.
- Total Origin Stealth: Public internet cannot resolve or probe your server IP.

🛡️ 2. Firewall Hardening

UFW & SYSCTL

- Default Deny Incoming: 'ufw default deny incoming' with zero public exceptions.
- ICMP Stealth: Disable ping responses to prevent automated reconnaissance.
- SYN Flood Mitigation: Kernel TCP SYN cookie protection and backlog scaling.

🔑 3. Cryptographic Mesh

TAILSCALE / WIREGUARD

- Point-to-Point Mesh: Private admin SSH over encrypted WireGuard tunnel.
- MagicDNS Routing: Direct hostname access without dynamic DNS public exposure.
- Key Expiration Policy: Automatic 90-day device cryptographic key rotation.

🔍 4. Verification Test

EXTERNAL NMAP AUDIT

- External Penetration Scan: Comprehensive full 65,535 TCP port audit.
- Target Result: 100% of ports return FILTERED or CLOSED status.
- Zero Security Drift: Automated monthly port scan cron with WhatsApp alerts.

📋 4-Phase Implementation Pipeline

PHASE 01
UFW Lock
Deny all incoming traffic and allow local subnets only.

PHASE 02
Tunnel Auth
Authenticate cloudflared tunnel daemon with origin cert.

PHASE 03
Ingress Rules
Map private Docker services to edge hostnames.

PHASE 04
Nmap Audit
Execute external port scan to verify 0 open ports.

bash — agy-dev-env — scan-blueprint

LIVE TERMINAL

```
# 1. Run official Ghannams Academy security hardening audit
$ bash -c "$(curl -sSL https://ghannamsacademy.com/scripts/setup_docker_cloudflare.sh)"
# 2. Verify external port scan reveals 0 open attack vectors
$ nmap -Pn -p- --reason $(curl -s ifconfig.me)
# Result: 65535 ports scanned. 0 open ports detected (ALL FILTERED)
```

Mohamad Adib Ghannam
Founder & CEO, Ghannams Academy • Senior Biomedical Software Engineer & AI Specialist

support@ghannamsacademy.com
+60162710885 (WhatsApp)

⚡ ENGINEERING CONSULTATION & DEPLOYMENT

Ready to Build Something Special Together?

We partner with forward-thinking founders, CTOs, and serious builders to architect sovereign, high-margin software systems. Whether launching a production MVP in 72 hours, deploying autonomous agent swarms, or migrating off expensive SaaS subscriptions—we deliver production-grade results.

⚡

72-Hour Rapid MVP Sprints

From raw specification to live production in 3 days. Sub-second Next.js / Vite client, FastAPI / SQLite microservice, Supabase auth, and Stripe monetization.

SPEED TO MARKET

🤖

Autonomous Multi-Agent Swarms

Custom CLI agent swarms tailored to your company's workflows. Autonomous code generation, automated test execution, and continuous documentation in Git worktrees.

10X COGNITIVE LEVERAGE

🔒

Sovereign Cloud Infrastructure

Replace $20,000/yr per-seat SaaS bills with private dedicated hardware, WireGuard encrypted mesh networks, and zero-open-port Cloudflare tunnels.

PERMANENT MARGINS

Start Your Engineering Engagement Today

🌐 GhannamsAcademy.com | 💬 Chat on WhatsApp | 📧 Email Support

✓ 100% Source Code Ownership ✓ 100/100 Lighthouse Benchmark ✓ Zero SaaS Vendor Lock-In

Mohamad Adib Ghannam
Founder & CEO, Ghannams Academy • Senior Biomedical Software Engineer & AI Specialist

support@ghannamsacademy.com
+60162710885 (WhatsApp)