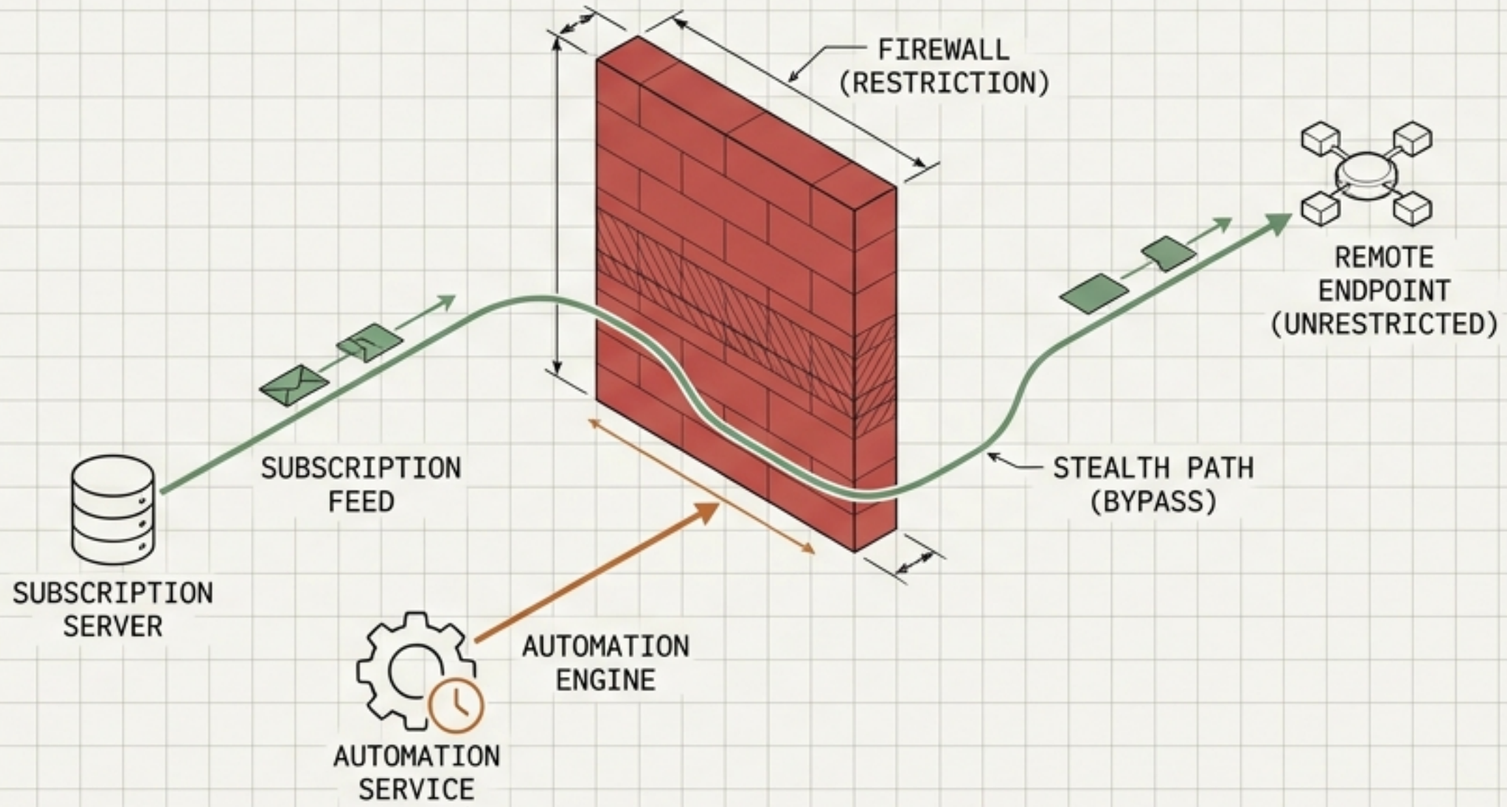
Self-Hosted Proxy Runbook

Full-Stack sing-box Deployment, Subscriptions & Automation



REV: 1.0	
DATE: OCT 2024	
ENGINEER: SYSTEM_ARCHITECT	
APPROVED: NET_OPS	

The Anatomy of a Block

Step 1

The Connection

Processors to data slinor
unV active packet

Step 2

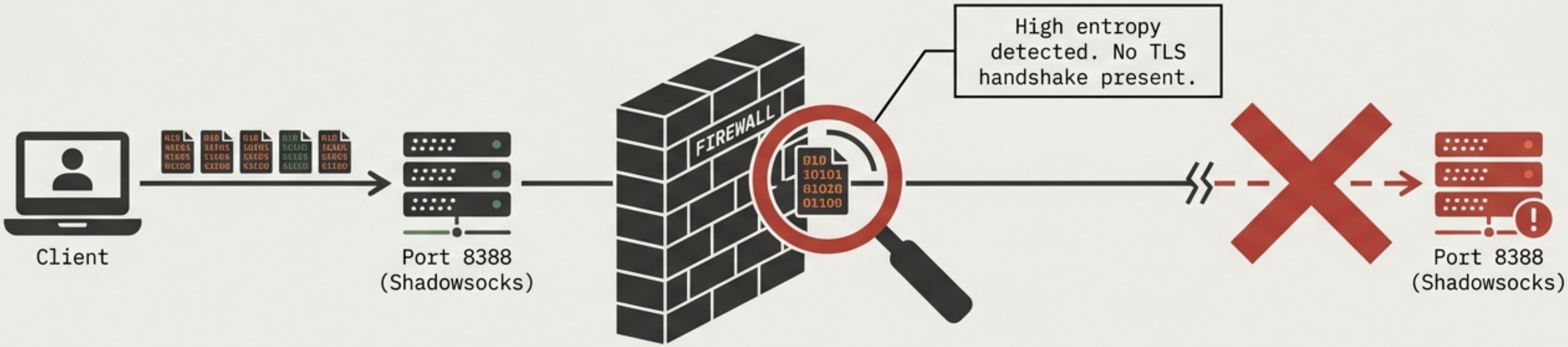
The Active Probe

Intercepted by loon wall,
inspection firewall

Step 3

The Drop

Connection data templated
with that connected



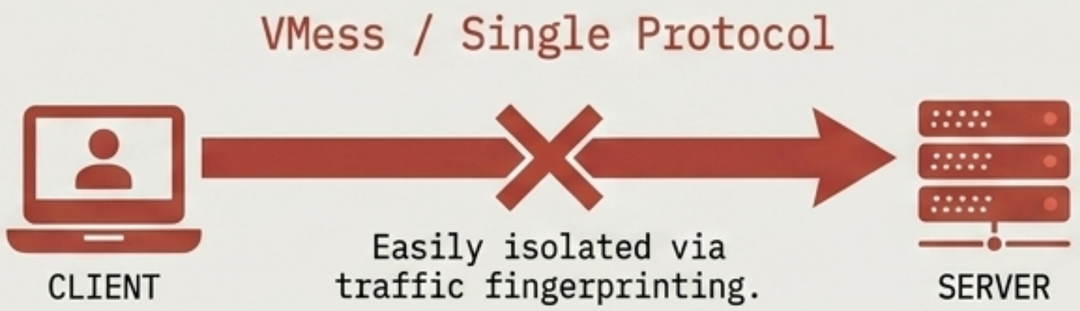
For IPs serving mainland China, SS/VMess/Socks5 without obfuscation is a dead end. Bare protocols fail within hours.

The Multi-Protocol Evasion Strategy

ARCHITECTURAL COMPARISON: LEGACY VS. MODERN EVASION

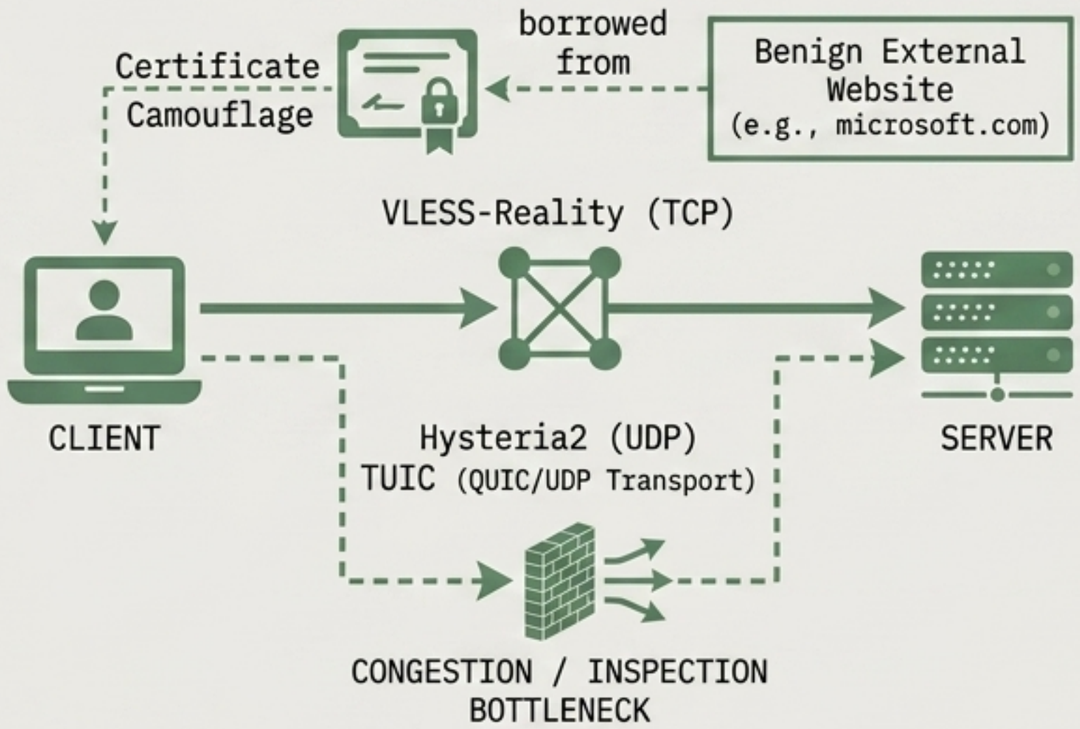
Legacy Architecture

SINGLE-CHANNEL VULNERABILITY

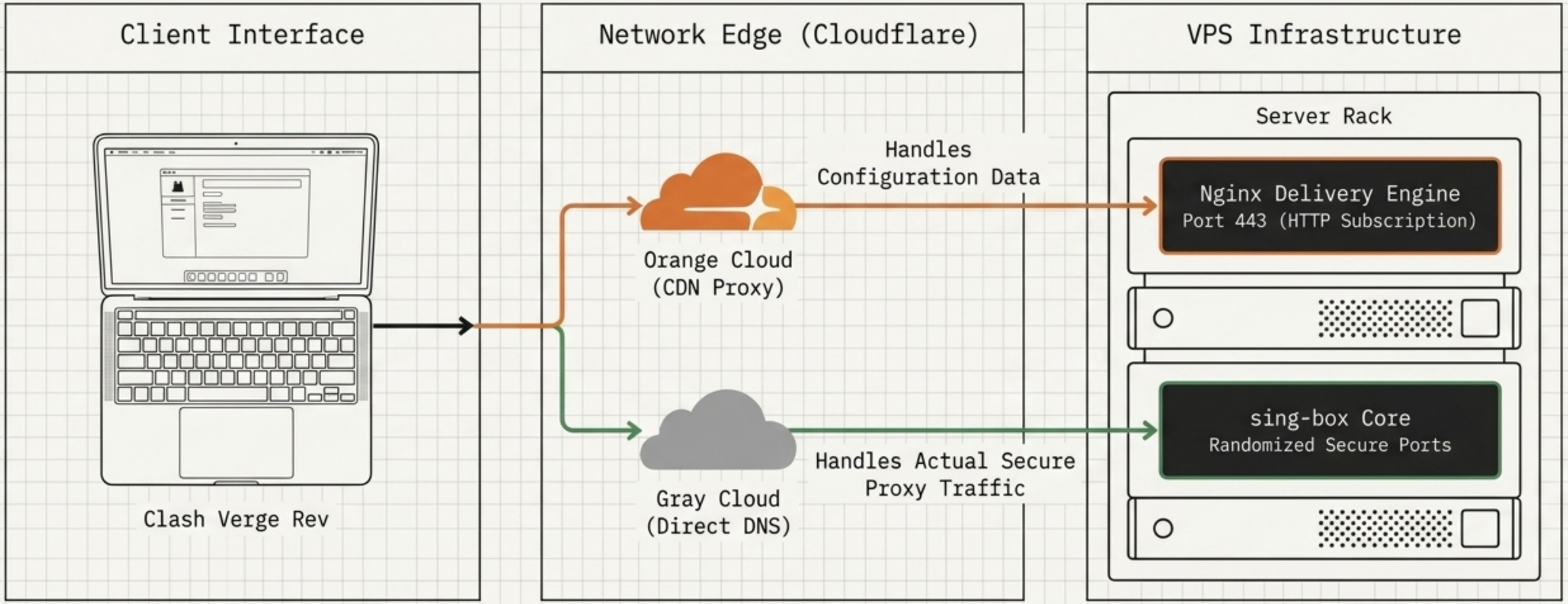


Modern sing-box Architecture

MULTI-CHANNEL DYNAMIC TOPOLOGY



Target Architecture Blueprint



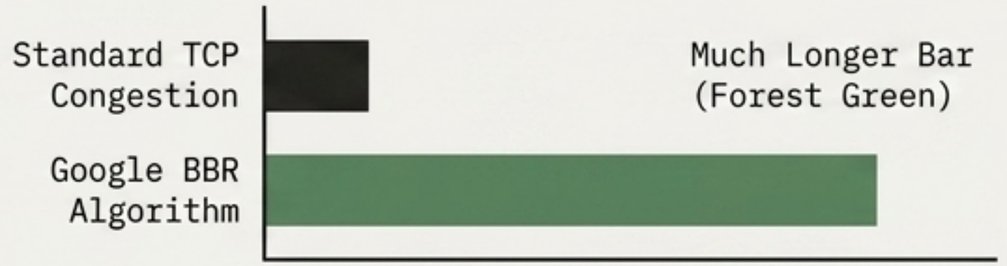
Infrastructure & Provisioning Criteria

The Hardware Matrix

Provider:	Atlas Networks
Routing:	AS9929 / CN2 GIA (Bypasses AS4837 congestion)
IP Type:	Static Residential
Bandwidth:	100Mbps+ Minimum
OS:	Ubuntu 24.04.1 LTS

Network & Security Configuration

Throughput Optimization



Security Warning

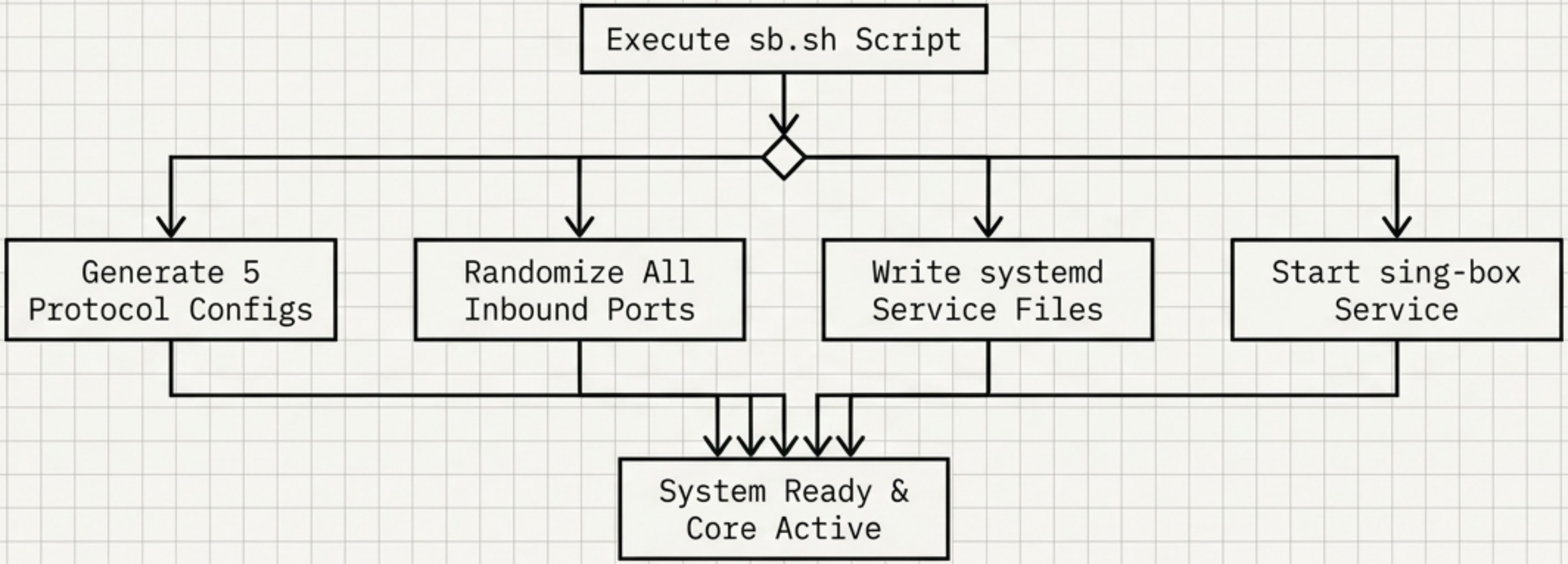
Check sshd_config for PubkeyAuthentication no on new instances to avoid SSH lockout.

Core Inbound Protocol Matrix

Protocol Name	Transport Type	Block Resistance	Description/Notes
VLESS-Reality-Vision	TCP	★★★★★	Primary: Disguises as HTTPS
Hysteria2	UDP	★★★★	High-Speed: Requires UDP testing
TUIC-v5	UDP	★★★★	Low Latency
Anytls	TCP	★★★★	TLS Mimicry
Vmess-WebSocket	TCP	★★	Deprecated: Target for removal

[PORTS RANDOMIZED ON DEPLOYMENT]

Automated Core Execution (sb.sh)

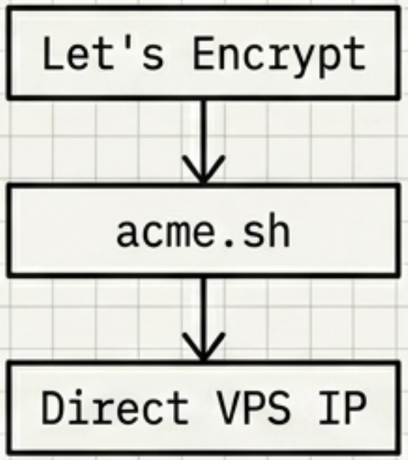


WARNING: ufw may be uninstalled during setup. Default iptables policy is ACCEPT.

The Cloudflare DNS State Machine

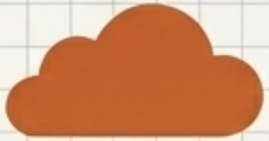
Phase 1: Gray Cloud

DNS ONLY

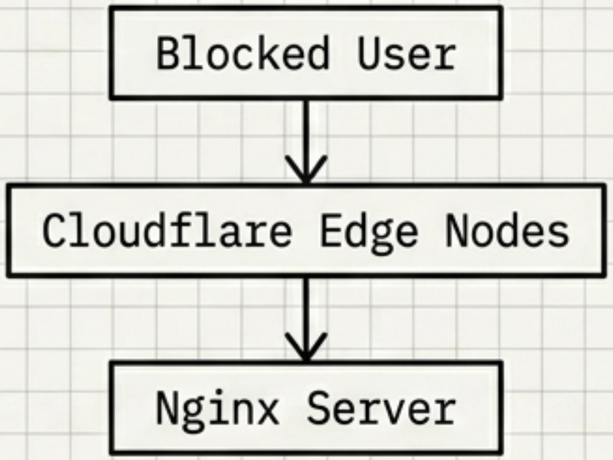


Use case: Initial SSL validation and establishing direct proxy connections.

Phase 2: Orange Cloud

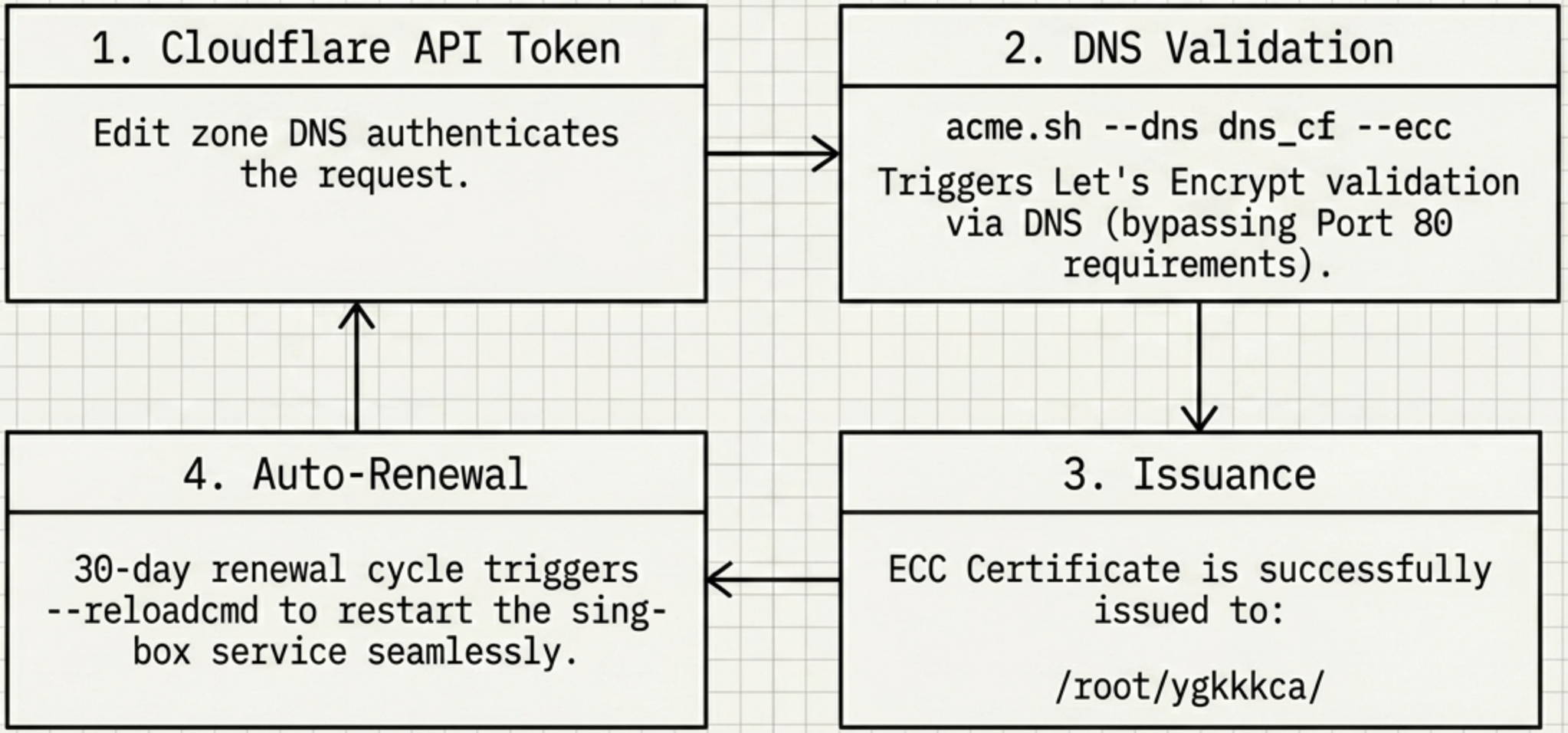


CDN PROXY



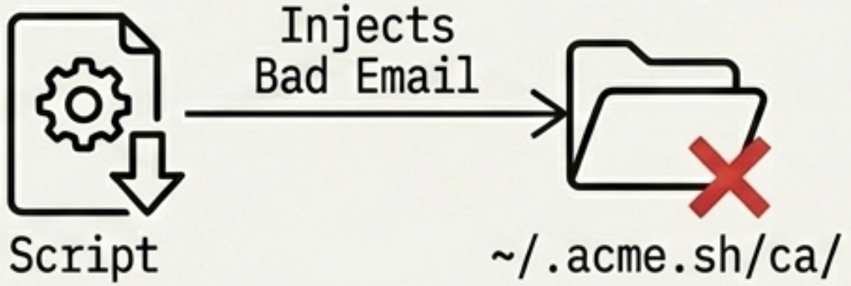
Use case: Ensuring secure, reliable delivery of the configuration subscription URL.

SSL Certificate Automation Engine



Critical SSL Sync Interventions

Alert 1: The Cache Corruption

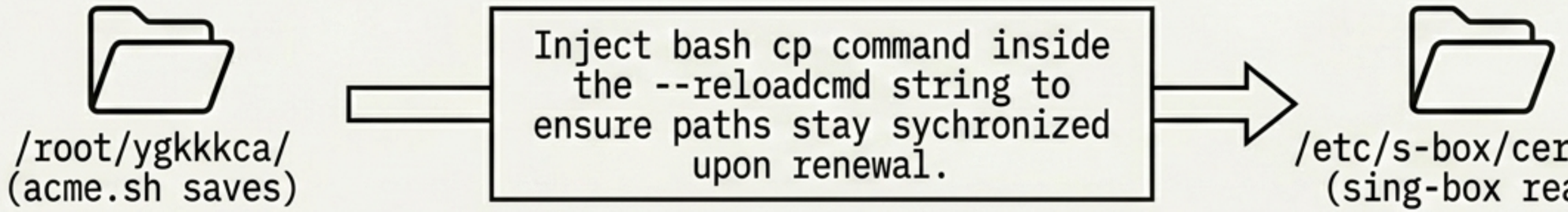


Resolution

`rm -rf ~/.acme.sh/ca/`

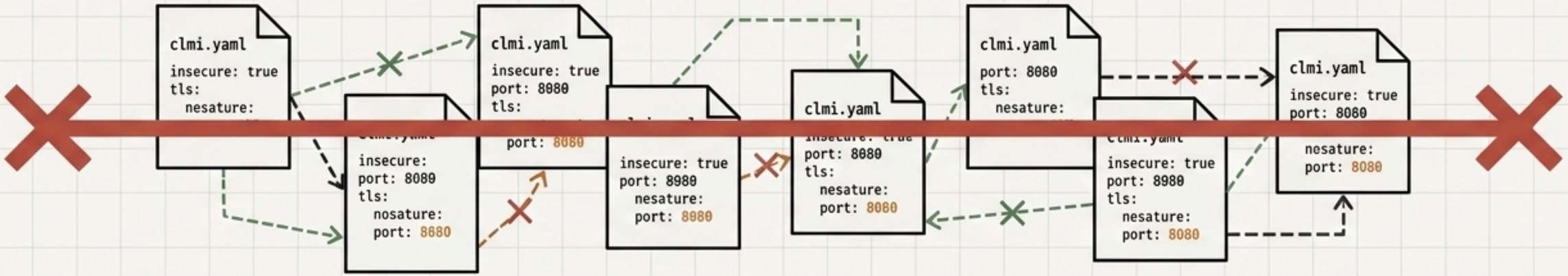
Run manual acme.sh with `--accountemail` and `--force`

Alert 2: The Path Discrepancy

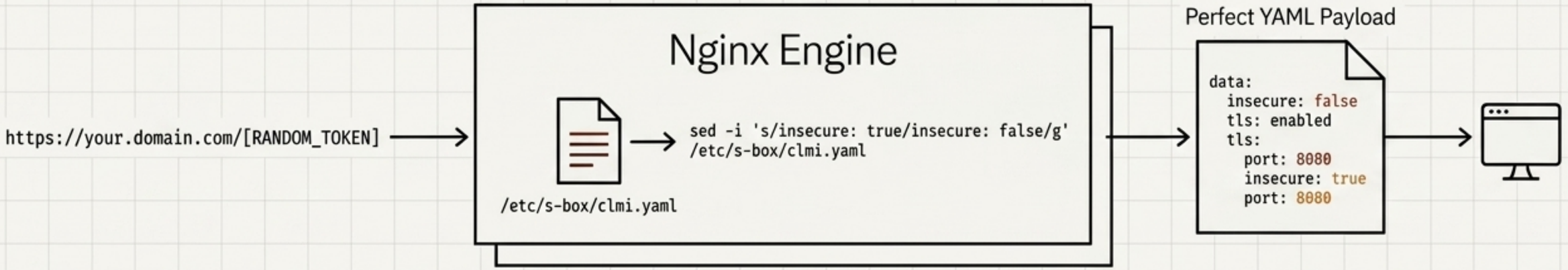


The Configuration Delivery Engine (Nginx)

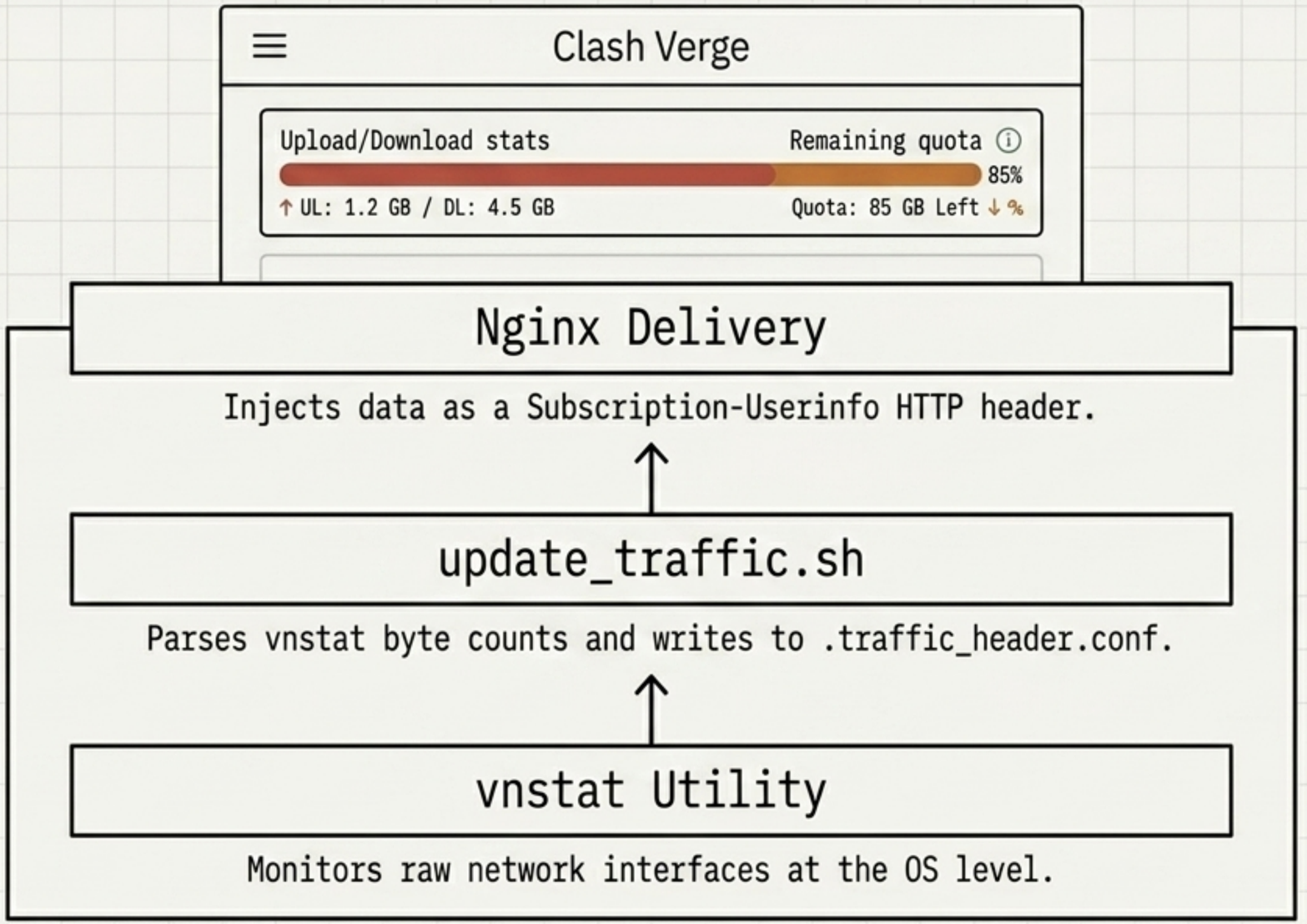
Manual Edits



Subscription URL Pipeline



Real-Time Traffic Tracking Architecture



Pre-Flight Configuration Optimization

Action 1: Aesthetic Cleanup

Before:
VLESS-Reality-Vision-5[illegible]b

Regex pattern

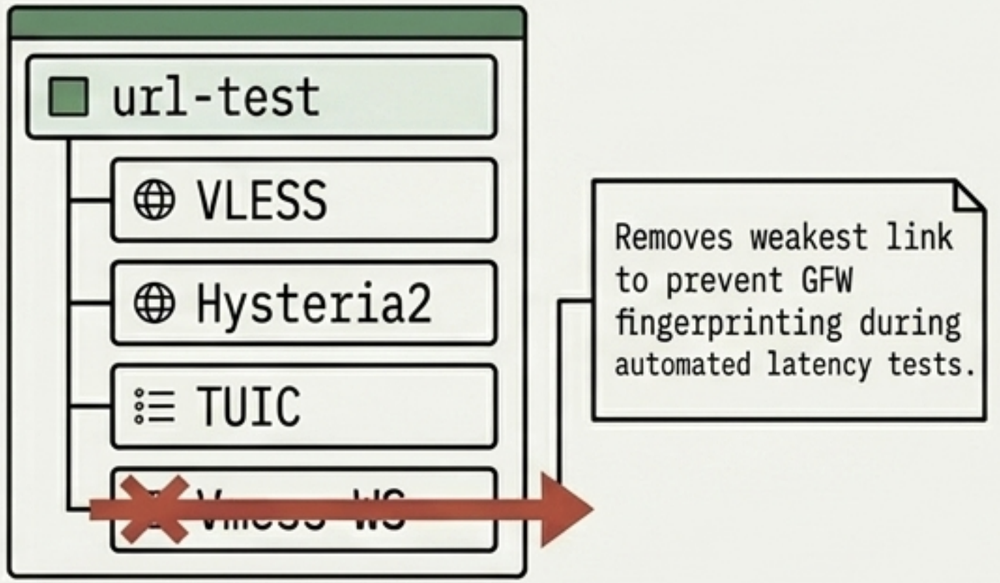
⇨ Regex: s/-[a-f0-9]{4}$//g

Regex configuration operation

Regex: -[a-f0-9]{4}$//g

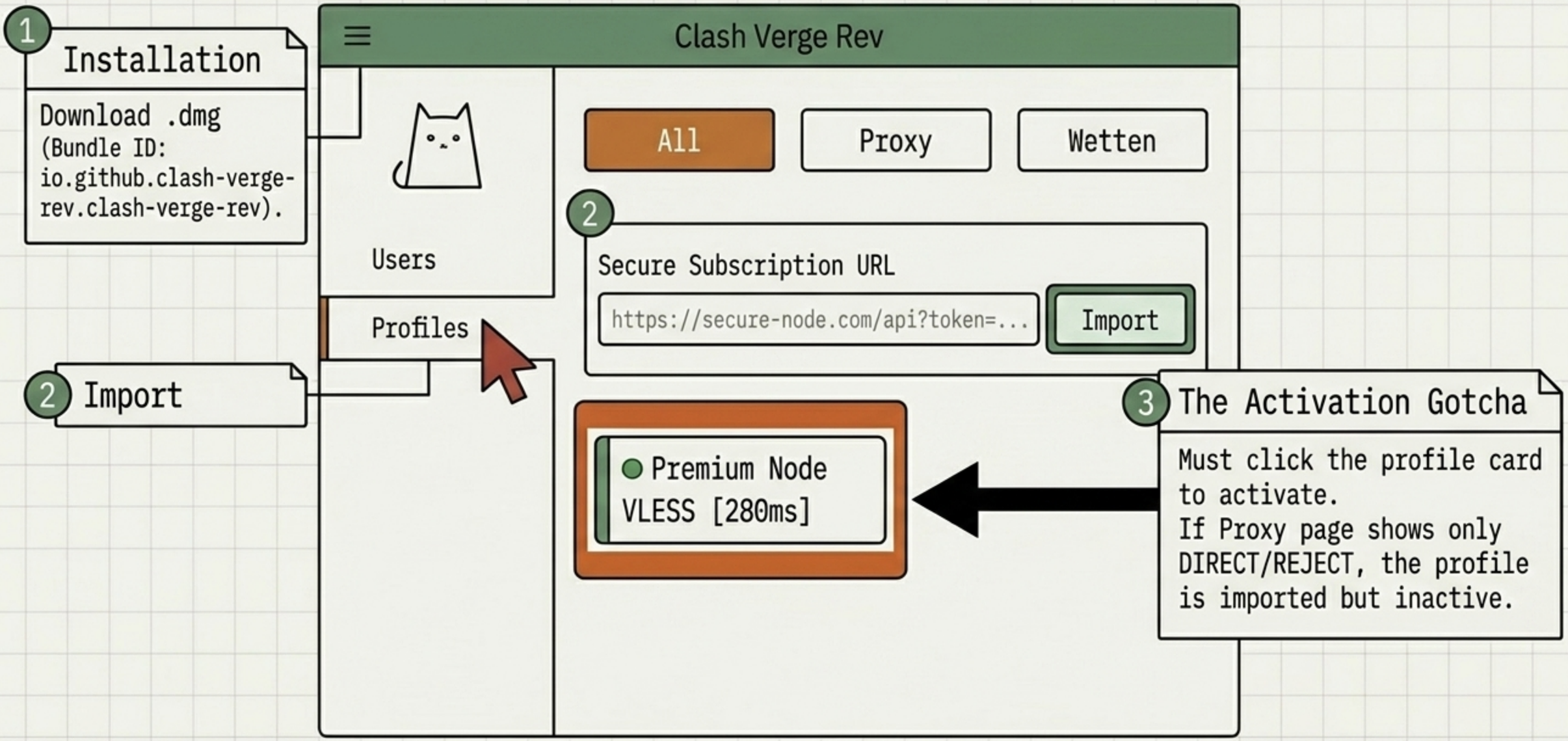
After:
VLESS-Reality-Vision

Action 2: Security Hardening

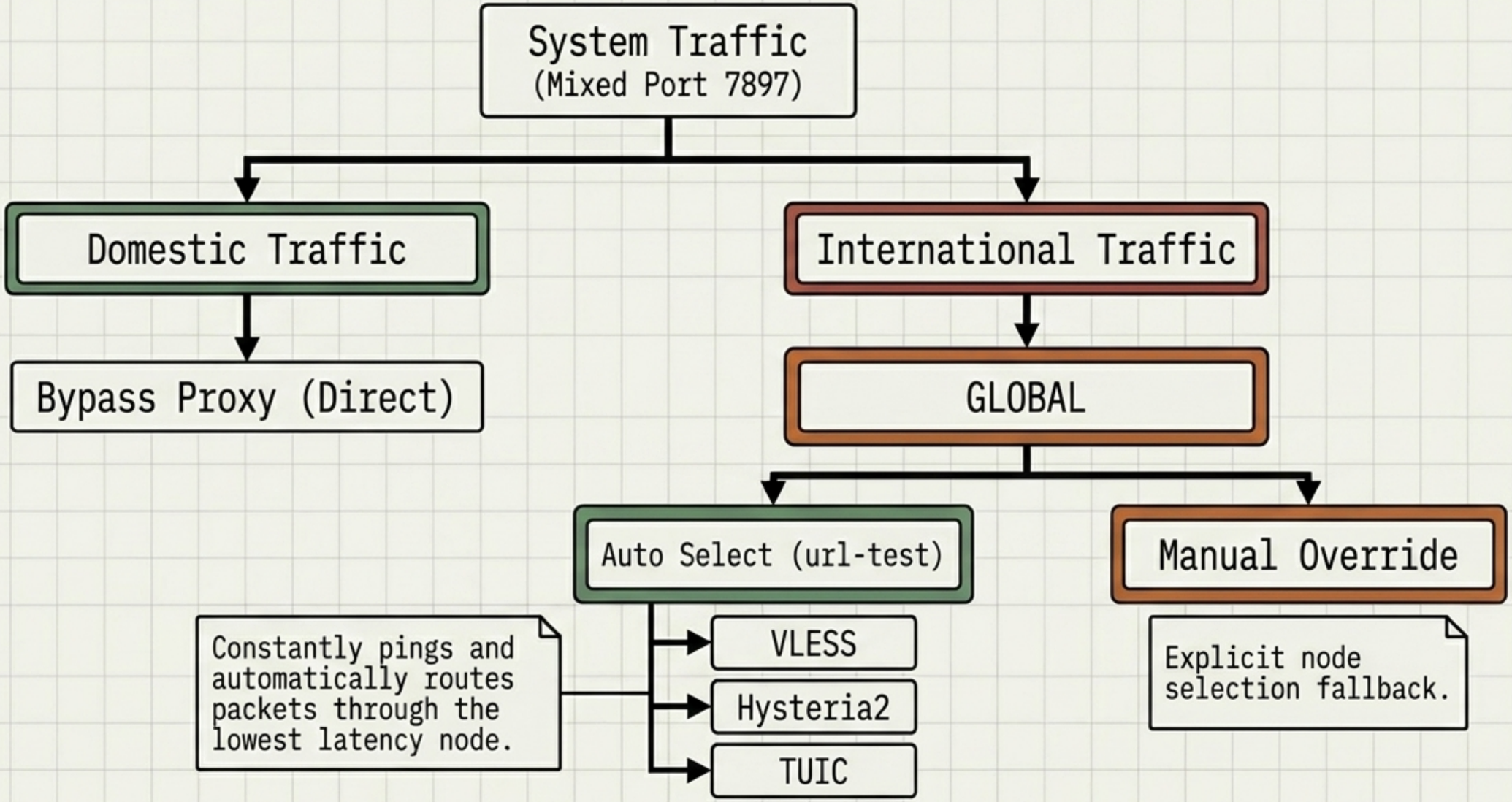


RULE: Make all changes in the server-side YAML.
Local client edits will be overwritten on the next update.

macOS Client Integration (Clash Verge Rev)



Proxy Group Routing Logic



Diagnostic Matrix: Network & Transport

Symptom	Root Cause	Fix
Bare SS/VMess port blocked	High entropy, GFW active probe	Migrate to VLESS-Reality TLS mimicry.
nc -zv or telnet timeouts on ports 18877/31227	Hysteria2/TUIC are UDP protocols; TCP probes will fail	Use UDP-specific verification tools.
Subscription URL times out from China	Direct IP blocked	Enable Cloudflare CDN proxy (Orange Cloud) for HTTP delivery.

Diagnostic Matrix: SSL & Configuration

Symptom	Root Cause	Fix
acme.sh email mismatch error	sb.sh script cache pollution	Clear ~/.acme.sh/ca/ and force --accountemail.
Cert renewed but Hysteria throws TLS error	Certificate paths out of sync	Inject copy command into --reloadcmd.
Custom client settings lost on reboot	Local edits in Clash Verge overwritten	Centralize edits in Nginx-served YAML only.
Auto-select group suffers high latency	Vmess-WS being chosen	Manually delete Vmess-WS from url-test group.

System Verification Gates

Server-Side

- `systemctl status sing-box` is active.
- Nginx responds to token URL with YAML payload.

Client UI

- Profile card border is highlighted.
- System Proxy is enabled.
- Proxy Mode is set to "Rule".

Network Validations

- Proxy node list populates with latency data (no timeouts).
- Browsing to https://ip.me displays the Atlas Networks VPS IP.

Master System Reference Architecture

Port Topology	
Service	Port/Protocol
SSH (Custom)	TCP (random)
Nginx HTTP	TCP (80)
Nginx HTTPS	TCP (443)
VLESS	TCP (random)
Hysteria2	UDP (random)
TUIC-v5	UDP (random)
Anytls	TCP (random)

Critical Paths
/etc/s-box/sb.json ——— Core Config
/etc/s-box/clmi.yaml ——— Client Sub
/root/ygkkkca/fullchain.crt — SSL Target
/etc/s-box/update_traffic.sh - Traffic Script
/etc/s-box/.sub_token ——— Token Secret