ZAKON NETWORK EGRESS — 3-Source Public IP Verification

ZAKON NETWORK EGRESS — Verification Protocol

> **Public IP za CF whitelist / firewall rules MORA biti verified iz 3 nezavisna izvora.** `curl ifconfig.me` **SAM nije dovoljan — vraća VPN exit ako je VPN klijent aktivan.**

Date: 2026-04-28 **Origin:** ANVIL CF whitelist incident. John napravio 4 reverzalne tvrdnje o ANVIL public IP-u u jednoj sesiji. Memory imala stale `46.46.247.60`. curl iz Studio sesije vratio `46.46.247.96` (VPN exit). Stvarni LAN egress = `92.221.168.61` (Tailscale peer connections confirmed). Tri nezavisna izvora bi rezultat dali odmah, bez 30 min iteracija.

Rule

Svaki task koji uključuje **public IP whitelist, firewall rule, CF Configuration Rule, ili IP-based access policy** MORA proći ovaj 3-source verification PRIJE dispatch-a:

Source 1 — Outbound HTTP (curl)

```
curl -s https://api.ipify.org
curl -s https://ifconfig.me
curl -s https://ipinfo.io/ip
```

WARNING: Ako VPN klijent aktivan, ovo daje VPN exit, ne ISP egress.

Source 2 — DNS-based (bypassuje HTTP routing)

```
dig +short myip.opendns.com @resolver1.opendns.com
dig +short TXT o-o.myaddr.l.google.com @ns1.google.com
```

DNS upit obično ide kroz drugačiji routing nego HTTP, otkriva VPN.

Source 3 — Peer connection address (ground truth)

```
tailscale status | grep "direct"
# Vidi peer connections — `direct PEER_IP:PORT` = stvarni egress IP koji peers vide
```

Authoritative za LAN egress — to je IP koji eksterni endpoints VIDE.

VPN detection (mandatory check)

```
ifconfig | grep -c "^utun"
```

Ako > 1 (Tailscale je 1) → **VPN klijent aktivan**. curl rezultat se NE smije koristiti bez Source 2/3 confirmation.

Reconciliation matrix

Source 1 (curl)	Source 2 (DNS)	Source 3 (Tailscale)	Conclusion
same	same	same	✅ Verified, safe to whitelist
different	same Source 3	matches Source 3	⚠ VPN aktivan — koristi Source 3
different	different	different	🛑 Pita CEO, ne dispatchuj

When to apply

- Bilo koji MC task sa keyword "whitelist", "IP rule", "firewall", "CF Access policy", "BIC rule"

- Mehanik gate MORA pozvati ovaj check pre `CLEAR TO DISPATCH` za network tasks
- Validation (Proveo): post-deploy curl iz svake whitelistovane mašine + iz non-whitelistovane → expected behavior

---

Anti-patterns (explicit, observed 2026-04-28)

1. **"curl ifconfig.me kaže X, znači X"** — false ako VPN aktivan
2. **"Memory kaže X, znači X"** — false, memory može biti stale (DHCP rotation, VPN exit rotation)
3. **"Studio i ANVIL su na istom LAN-u, dijele IP"** — false ako VPN drugačije routes outbound vs LAN
4. **"Pretpostavljam dvije mašine, X i Y"** — provjeri jesu li alias/ista mašina prije diskusije

---

Related rules

- `cf-proxied-api-bic-whitelist.md` — primjenjuje ovaj rule na CF specifically
- `claim-verification-protocol.md` — opšti verification standard
- `zakon-feasibility-check.md` — Mehanik feasibility gate

Revision #2
Created 2026-04-28 10:31:45 UTC by John
Updated 2026-05-31 20:06:42 UTC by John