Tailscale + RunPod Workflow (Mac + Docker + Firewall Hardening)

1. OVERVIEW

Goal: Secure private channel between Mac (home) and RunPod instance using Tailscale.
Once linked, both machines appear on the same private network (100.x.x.x range).

2. INSTALL & CONNECT TAILSCALE

A. On Mac (home)

```
brew install tailscale
sudo tailscale up --accept-routes --ssh
tailscale status
```

B. On RunPod VPS

```
curl -fsSL https://tailscale.com/install.sh | sh
sudo tailscale up --ssh --accept-routes
tailscale status
```

3. TEST CONNECTION

From Mac: `ping 100.99.51.22`
From RunPod: `ping 100.88.47.11`

4. USE CASES

A. Access model server on Mac

```
curl http://100.88.47.11:7860
```

B. Access model server on RunPod

```
curl http://100.99.51.22:5000
```

5. MAKE IT PERSISTENT

Mac:

```
sudo tailscale up --accept-routes --ssh
sudo tailscale status
```

RunPod (ephemeral):

```
sudo tailscale up --authkey <ephemeral-key> --ssh --accept-routes
```

6. DOCKER + TAILSCALE INTEGRATION

Docker Compose example:

```
version: "3.9"
services:
  tailscale:
    image: tailscale/tailscale
    hostname: mydocker-node
    environment:
      - TS_AUTHKEY=tskey-<auth-key>
      - TS_STATE_DIR=/var/lib/tailscale
      - TS_EXTRA_ARGS=--accept-routes
    volumes:
      - tailscale-state:/var/lib/tailscale
      - /dev/net/tun:/dev/net/tun
    cap_add:
      - NET_ADMIN
      - NET_RAW
    network_mode: "host"
volumes:
  tailscale-state:
```

```
docker compose up -d
```

7. MACOS FIREWALL + HARDENING

A. Built-in Firewall

System Settings → Network → Firewall → Enable

Enable Stealth Mode

Terminal check:

```
sudo /usr/libexec/ApplicationFirewall/socketfilterfw --getglobalstate
```

B. PF Firewall

Edit /etc/pf.conf:

```
block in all
pass out all
```

Enable:

```
sudo pfctl -f /etc/pf.conf
sudo pfctl -e
```

Disable:

```
sudo pfctl -d
```

C. Harden SSH

Edit /etc/ssh/sshd_config:

```
PermitRootLogin no
PasswordAuthentication no
PubkeyAuthentication yes
AllowUsers yourusername
```

Restart SSH:

```
sudo launchctl unload /System/Library/LaunchDaemons/ssh.plist
sudo launchctl load -w /System/Library/LaunchDaemons/ssh.plist
```

8. AI-ASSISTED FIREWALL OPTIONS

LuLu (free): brew install --cask lulu
Murus: front-end for pf
Little Snitch / Radio Silence: commercial
OpenSnitch (brew): Linux-style outbound firewall

9. MONITORING & SAFETY

```
tailscale status
tailscale logout
tailscale netstat
```

10. OPTIONAL EXTRAS

File sharing: tailscale file cp myfile.txt runpod:~
SSH over Tailscale: ssh runpod
Model syncing: rsync -avzP ./models/ runpod:~/models/

11. SUMMARY

Component	Purpose
Tailscale	Secure private mesh network
Docker	Containerization of models or services
macOS Firewall / LuLu	Control inbound/outbound traffic
RunPod	Remote compute for model execution
SSH via Tailscale	Encrypted admin channel
pf / System Firewall	OS-level network filtering