

The Sovereign Operator's Guide: OpSec + Passport Burner Identity

Version 2.0 • El Salvador Edition

"Never do anything illegal — and always upbuild society."

What Changed in v2.0

IPsec is a tool; OpSec is the discipline:

- Promotes OpSec to the organizing principle of the entire guide.
 - Demotes IPsec to one of three optional network tools, alongside Tailscale and Nym Mixnet.
 - Adds honest trade-offs for each tool so you can choose based on your actual threat model.
 - Keeps the Passport workflow but reframes it as one layer in a broader compartmentalization strategy.
-

Table of Contents

1. Introduction: OpSec Is the Point
 2. Part I: The OpSec Mindset
 3. Part II: Network Privacy Tools (Choose One or Stack)
 4. Part III: Passport — Forging Your Burner Identity
 5. Part IV: Plugging into Nostr Clients
 6. Part V: Plugging into Bitcoin Wallets
 7. Part VI: The Full Compartmentalization Workflow
 8. Part VII: Maintenance, Recovery & Emergencies
 9. Appendix: Quick Reference
-

1. OpSec Is the Point

Operational Security (OpSec) is the process of identifying what information you are trying to protect, who you are protecting it from, and what actions you take to prevent that information from being discovered. It is not a product you install. It is not a VPN you connect to. It is a practice — a set of habits, decisions, and procedures that you follow consistently.

The cryptographic tools in this guide — Passport, Nostr clients, Bitcoin wallets — are only as strong as the OpSec surrounding them. A perfect Ed25519 seed is worthless if you paste your nsec into a compromised website. A pristine BIP84 wallet is worthless if you fund it directly from a KYC exchange. A clean Nostr identity is worthless if you connect to the same relays as your main identity from the same IP address.

The core principle of OpSec for burner identities is compartmentalization. Every identity gets its own:

- Keys — no reuse across identities
- Network path — separate VPN user, separate exit node, or separate mixnet client
- Device or VM — separate browser profile, separate OS user, or separate physical device
- Behavioral pattern — separate writing style, separate posting times, separate relay set
- Financial trail — no direct on-chain links between main and burner wallets

This guide gives you the tools and the procedures to build that compartmentalization.

Part I: The OpSec Mindset

2.1 Threat Modeling: Who Are You Hiding From?

Before you choose tools, you must answer: who is the adversary?

Adversary Capabilities What You Need

Data brokers / advertisers Passive tracking, cookie correlation, fingerprinting Browser separation, no reuse of identifiers

ISP / local network Traffic inspection, DNS logging, bandwidth analysis Encrypted tunnel (IPsec, Tailscale, or Nym)

Relay operators See which npubs connect from which IPs, timing of events Separate network path per identity, separate relay sets

Chain analysts Full blockchain graph analysis, clustering heuristics No direct on-chain links, use P2P or Lightning swaps

State-level adversary Global passive observation, endpoint compromise, legal coercion Full stack: Nym mixnet, airgapped devices, no digital trace

You do not need the full stack unless you are facing the full adversary. Match your tools to your threat model.

2.2 The Golden Rules of Burner OpSec

1. Never cross the streams. Main identity and burner identity never share a device, a network path, a browser profile, or a relay set.
 2. Never reuse identifiers. No shared avatars, usernames, bios, writing styles, or timestamps.
 3. Never link in content. Do not mention your main identity in burner posts, and vice versa.
 4. Never transact directly. No on-chain Bitcoin transaction from main wallet to burner wallet.
 5. Never trust a single layer. If your network path is the only thing protecting you, you have no protection. Stack layers: network + device + behavioral + financial.
 6. Assume metadata leaks. Nostr relays see your IP and timing. Bitcoin nodes see your transactions. Design for the assumption that metadata is public, and minimize what metadata you produce.
-

Part II: Network Privacy Tools (Choose One or Stack)

You need some network privacy layer to prevent relay operators, ISPs, and chain analysts from correlating your burner identity with your main identity by IP address. Here are three options, from simplest to strongest.

3.1 IPsec — The Classic Tunnel

What it is: A protocol suite that encrypts individual IP packets between your device and a VPN server you control.

What it protects against:

- ISP-level traffic inspection
- DNS logging by your local network
- Eavesdropping on untrusted networks (coffee shops, hotels)

What it does NOT protect against:

- The VPN server operator (you, if you self-host — that is the point)
- A global passive adversary who can observe both your ingress and egress traffic
- Correlation if you use the same VPN user account for main and burner identities

Best for: Users who want a simple, self-hosted tunnel and who trust their own server.

How to set it up (Linode StackScript):

1. Deploy the StackScript at <https://cloud.linode.com/stackscripts/37239>
2. Choose a region far from your physical location

3. Select the \$5 Nanode plan
4. Set a strong IPsec PSK and server password
5. After deployment, use LISH console to retrieve the .mobileconfig or .p12 file
6. Import the certificate into your device's VPN settings
7. Create a separate VPN user for your burner identity:

```
sudo addvpuser burner-main  
# Enter a strong, unique password
```

Critical OpSec rule: Your main identity connects as main-user. Your burner connects as burner-main. Never use the same credentials.

3.2 Tailscale — Mesh VPN with Exit Nodes

What it is: A WireGuard-based mesh VPN that creates a private network between your devices. Tailscale also offers exit nodes (via Mullvad integration) that route your public internet traffic through a chosen location.

What it protects against:

- ISP-level traffic inspection (when using an exit node)
- Device-to-device traffic snooping on untrusted networks
- Some metadata correlation (if you use separate tailnets per identity)

What it does NOT protect against:

- No kill switch. Tailscale does not block traffic if the exit node becomes unreachable — it falls back to direct routing, exposing your real IP. This makes it unsuitable as a privacy-critical always-on solution without additional firewall rules.
- Identity-aware by default. Tailscale does not support anonymous tailnets. Your tailnet is tied to an identity provider (Google, GitHub, etc.). If that identity is linked to your main identity, the tailnet is too.
- DNS leaks. The Mullvad exit node integration does not always set the correct DNS servers, meaning your DNS queries may still go to your local DNS server.
- Tailscale can see which exit node you use. If you opt out of client logging, Tailscale does not have visibility into which Mullvad exit node a device uses, but this is an opt-out, not the default.

Best for: Users who want easy mesh networking between their own devices and who are willing to add a kill switch (e.g., pf firewall rules on macOS) to prevent leaks. Not recommended as your only privacy layer.

How to set it up:

1. Create a Tailscale account with an email address that is not linked to your main identity
2. Install Tailscale on your burner device
3. Enable Mullvad exit node in the Tailscale admin panel
4. Configure your DNS settings in Tailscale to use Mullvad's DNS servers
5. Add a kill switch (example for macOS):

```
# Block all traffic except through the Tailscale exit node
# (This is a simplified example; test thoroughly before relying on it)
sudo pfctl -e
# Add pf rules to block non-Tailscale traffic
```

Critical OpSec rule: Use a separate Tailscale tailnet for your burner identity. Do not add your burner device to the same tailnet as your main devices.

3.3 Nym Mixnet — The Strongest Anonymity Layer

What it is: A mixnet that routes traffic through 5 hops (Entry Gateway, three Mix Node layers, Exit Gateway), each adding random delays and mixing packets with those of other users. Every packet is the same size, and a constant stream of dummy packets hides when real communication is occurring.

What it protects against:

- Global passive adversaries who can observe the entire internet. Nym adds cover traffic and timing obfuscation that Tor and VPNs do not.
- Traffic analysis — an adversary cannot tell when you are communicating or with whom.
- IP address correlation — the exit gateway sees your destination, but not your origin.

What it does NOT protect against:

- The exit gateway can inspect your raw IP packets. The mixnet anonymizes the pipe, not what you put through it. If you visit an HTTP site, the exit gateway sees the content.

- Performance degradation. The delays and cover traffic add latency. Nym is not suitable for real-time applications like video calls or gaming.

Best for: Users who face a global passive adversary and who need the strongest available anonymity layer. The gold standard for burner identity network privacy.

How to set it up:

1. Download the NymVPN client from <https://nym.com>
2. Choose Mixnet mode (not dVPN mode) for maximum anonymity
3. Connect. Your traffic is now routed through 5 hops with cover traffic.
4. Verify your IP address has changed (use ipleak.net)

Critical OpSec rule: Nym is a network layer tool. It does not protect your device from compromise, and it does not protect you from behavioral correlation (e.g., posting at the same times as your main identity). It is one layer in a stack.

3.4 Comparison Table

Feature	IPsec (Self-Hosted)	Tailscale	+ Mullvad	Nym	Mixnet
---------	---------------------	-----------	-----------	-----	--------

Ease of setup	Medium	Easy	Easy	Easy	Easy
---------------	--------	------	------	------	------

Self-hosted	Yes	No	(Mullvad exit)	No	(decentralized)
-------------	-----	----	----------------	----	-----------------

Anonymous	tailnet	N/A	No	Yes	Yes
-----------	---------	-----	----	-----	-----

Kill switch	Yes (manual)	No	(needs pf rules)	Yes	Yes
-------------	--------------	----	------------------	-----	-----

Resistant to global adversary	No	No	Yes	Yes	Yes
-------------------------------	----	----	-----	-----	-----

Latency	Low	Low	High	High	High
---------	-----	-----	------	------	------

Best for	Self-hosted simplicity	Mesh networking	Maximum anonymity	Maximum anonymity	Maximum anonymity
----------	------------------------	-----------------	-------------------	-------------------	-------------------

Recommendation: If you are just starting, use IPsec with a separate burner VPN user. If you need mesh networking, use Tailscale but add a kill switch. If your threat model includes a global passive adversary, use Nym Mixnet.

Part III: Passport — Forging Your Burner Identity

4.1 What Passport Generates

Passport is a single-file HTML application that deterministically derives six outputs from two inputs — an alias and a password:

Output Type Purpose

Alias Public Your burner handle

Persona ID Public A unique serial (SIF-XXXX-XXXX-XXXX)

PVK (Ed25519 Seed) Secret Root signing identity

Nostr npub Public Your burner public identity

Nostr nsec Secret Your burner private key

Bitcoin Seed (12 words) Secret BIP39 mnemonic

Bitcoin Address (BIP84) Public Native SegWit receive address

Account zpub Sensitive Watch-only key

The security model: Your password is stretched with PBKDF2-HMAC-SHA256 at 1,000,000 iterations, producing a 512-bit root. Each output is separated with HKDF-SHA256 under a distinct domain label. The Ed25519, secp256k1, and BIP39 outputs are cryptographically independent. The security boundary is your password.

4.2 Step-by-Step: Forging a Burner Identity

Step 1: Airgap (Recommended)

1. Download the Passport HTML file.
2. Disconnect from the internet.
3. Open the file in a browser. Confirm "Self-test: PASS (10/10)" in green.
4. If the self-test fails, do not proceed.

Step 2: Choose Your Alias

Your alias should be:

- Memorable to you
- Meaningful to you
- Not linked to your main identity (no real name, no main handle, no email prefix)
- Not a word that appears in your main identity's vocabulary

Step 3: Choose Your Password

This is the most important step.

- Minimum 12 characters (enforced)
- Mix of character types (lowercase, uppercase, numbers, symbols)
- Not used anywhere else
- Memorable to you without being written down in a place linked to your main identity

Recommended: Use a diceware-style passphrase — 5–6 random words separated by symbols. Example: correct-horse-battery-staple-42!

Write this password on paper. Store it separately from your main password manager.

Step 4: Forge

1. Enter your alias and password.
2. Aim for "Strong" entropy (100+ bits).
3. Click Forge Identity.
4. Wait 1–3 seconds while PBKDF2 runs.
5. The output card appears.

Step 5: Record Your Outputs

Tap Reveal to show each secret.

Write down or copy:

- Alias, Persona ID, Nostr npub, Bitcoin Address (public)

Do NOT write down or copy until you have a secure storage plan:

- PVK, Nostr nsec, Bitcoin Seed, Account zpub (secrets)

Step 6: Secure the Secrets

For each secret:

Option A: Paper backup (recommended for beginners)

1. Tap Reveal.
2. Write the value on paper.
3. Store in a physically secure location.
4. Do not photograph. Do not store in a cloud-synced note.

Option B: Metal backup (recommended for long-term)

1. Use a metal seed backup plate.
2. Stamp or engrave the mnemonic words.
3. Store in a fireproof safe.

Option C: Encrypted digital backup (advanced)

1. Encrypt the secrets with age or gpg.
2. Store on an offline USB drive.
3. Store the decryption passphrase separately.

Step 7: Burn the Session

1. Click Burn Session.
2. Confirm the form is cleared.
3. Close the browser tab.
4. For maximum security, reboot before doing anything else.

4.3 Regenerating Your Identity

Because Passport is deterministic, you can regenerate at any time by entering the same alias and password.

- You do not need to store the derived keys if you trust your memory.
- You must remember the alias and password exactly (NFKC normalization, lowercase, trimmed).
- If you forget either, the identity is lost forever.

Recommendation: Store the alias and password on paper in a location separate from your derived secrets.

Part IV: Plugging into Nostr Clients

5.1 Understanding the Nostr Key Model

- npub — your public key. Safe to share.
- nsec — your private key. Never share.

Your identity is the keypair. You can use the same nsec across multiple clients.

5.2 Importing Your Burner nsec

Client Platform Login Method

Damus iOS/macOS "I have an account" → paste nsec

Amethyst Android "Login with nsec" → paste nsec

Primal Web/Mobile "Login" → "Private Key" → paste nsec

Snort Web "Login" → "Private Key" → paste nsec

Coracle Web "Add Account" → "Private Key" → paste nsec

Important: Log out of your main identity before logging in with your burner nsec.

5.3 Setting Up Your Burner Profile

Publish a kind 0 event with:

- Name: your alias
- Display Name: a human-readable name
- About: a short bio. Do not link to your main identity.
- Picture: a fresh avatar. Do not reuse your main avatar.
- NIP-05 (optional): see below

5.4 NIP-05 Verification (Optional)

NIP-05 maps your npub to a DNS-based identifier like you@yourdomain.com.

Option A: Free provider

1. Register with a NIP-05 provider (e.g., nost.vip).
2. Enter your burner npub.
3. In your client's profile settings, enter the NIP-05 identifier.
4. Save.

Option B: Self-host

1. Create <https://yourdomain.com/.well-known/nostr.json>:

```
{
  "names": {
    "volcan-satoshi": "your_burner_npub_hex"
  }
}
```

2. Serve with Access-Control-Allow-Origin: *.
3. Enter volcan-satoshi@yourdomain.com in your client.

Important: Do not use a domain linked to your main identity.

5.5 Configuring Relays

- Use 3–5 relays for redundancy.
- Prefer relays that do not require KYC.

- Prefer relays that support AUTH (NIP-42).
- Do not use the same relay set as your main identity.

Relay operators can observe metadata. They see which npubs publish adverts, to whom offers are sent, and the timing of that traffic. Using separate relays for your burner identity reduces the correlation surface.

Recommended relays (as of this writing):

- wss://relay.damus.io
- wss://nos.lol
- wss://relay.nostr.band
- wss://nostr.wine (paid)
- wss://relay.snort.social

5.6 Nostr OpSec Notes

- Use NIP-59 gift wrap for private messaging. It hides not just content but most metadata, including sender, timestamp, and event kind.
 - Use private zaps to hide tipping details. Public zaps can leak your on-chain identity.
 - Back up keys offline. Regularly.
 - Verify identities with NIP-05 only if you trust the domain operator.
-

Part V: Plugging into Bitcoin Wallets

6.1 Understanding the Bitcoin Seed

Your Passport generates a BIP39 mnemonic (12 words) and derives a BIP84 wallet (native SegWit, bc1q...).

- Anyone who learns the mnemonic can spend all funds.
- Anyone who learns the zpub can see your entire wallet history.

6.2 Importing the Seed

Wallet Platform Import Method

BlueWallet iOS/Android Add Wallet → Import Wallet → Mnemonic → Custom path
m/84'/0'/0'

Sparrow Desktop File → New Wallet → Mnemonic → Native SegWit (BIP84)

Electrum Desktop File → New/Restore → Standard Wallet → I have a seed → Native SegWit

Verify: The first bc1q... address should match the one generated by Passport.

6.3 Setting Up a Watch-Only Wallet

A watch-only wallet lets you monitor balances without exposing spending keys.

- BlueWallet: Add Wallet → Import Wallet → Watch-only → paste zpub
- Sparrow: File → New Wallet → Watch Only → paste zpub
- Electrum: File → New/Restore → Standard Wallet → Use a master key → paste zpub

6.4 Bitcoin OpSec for Burner Identities

Funding your burner wallet:

1. Do not send directly from your main wallet. This creates a permanent on-chain link.
2. Use a peer-to-peer exchange (RoboSats, Bisq, Hodl Hodl) to buy Bitcoin with fiat, then withdraw to your burner address.
3. Use a Lightning swap (Boltz, Loop) to convert Lightning funds to on-chain funds in your burner wallet.
4. Use a mixer (CoinJoin via JoinMarket, Whirlpool) if you need to break the link. Note legal implications.

Critical: You cannot fund a burner identity using Bitcoin bought on Coinbase, Kraken, or any centralized exchange. Every fraction purchased on a regulated exchange is permanently tethered to your government ID, biometric scan, and physical address.

Spending:

- Spend small amounts.
- Do not consolidate burner funds with main funds.
- Use P2P exchanges, not KYC exchanges, to convert back to fiat.

Airgap for large amounts:

- For significant holdings, use an air-gapped hardware wallet (ColdCard, SeedSigner).
- Private keys never touch an internet-connected device.

Part VI: The Full Compartmentalization Workflow

7.1 The Complete Sequence

Phase 0: Preparation

1. Choose your network privacy tool (IPsec, Tailscale, or Nym).

2. Set up a dedicated network path for your burner identity.
3. Prepare a separate device, VM, or browser profile.
4. Have a secure way to store secrets (paper, metal, encrypted USB).

Phase 1: Forge the Identity

1. Airgap your machine.
2. Open Passport. Confirm self-test passes.
3. Enter alias and password.
4. Click Forge Identity.
5. Record public outputs.
6. Securely record secret outputs.
7. Click Burn Session.
8. Close browser. Reconnect.

Phase 2: Set Up the Burner Environment

1. Connect to your network privacy tool using the burner credentials.
2. Verify your IP address has changed.
3. Open your burner browser profile or device.
4. Ensure no main-identity accounts are logged in.

Phase 3: Configure Nostr

1. Open a Nostr client.
2. Log out of any existing identity.
3. Import your burner nsec.
4. Publish your burner profile.
5. Configure your relays (3–5 privacy-respecting relays, separate from main).
6. Optionally set up NIP-05.
7. Publish a test note.

Phase 4: Configure Bitcoin

1. Open a Bitcoin wallet.
2. Import your burner mnemonic with BIP84 derivation.
3. Verify the first address matches Passport.
4. Set up a watch-only wallet on a separate device using zpub.

5. Fund via P2P or Lightning swap.

Phase 5: Operationalize

1. Use burner identity only from the burner environment.
2. Use main identity only from the main environment.
3. Never cross the streams.
4. Monitor burner wallet via watch-only wallet.
5. Periodically verify decoupling (IP leaks, relay connections, cross-links).

7.2 Timeline

Day Task

Day 1 Set up network privacy tool, create burner credentials

Day 2 Forge identity in Passport, record secrets

Day 3 Set up Nostr client, publish profile, test posting

Day 4 Set up Bitcoin wallet, verify address, set up watch-only

Day 5 Fund wallet via P2P or Lightning swap

Day 6 Operational testing — post, zap, receive, spend small amount

Day 7 Review, adjust OpSec, document procedures

Part VII: Maintenance, Recovery & Emergencies

8.1 Backup Strategy

What to back up:

Item Storage

Alias + Password Paper, stored separately from derived secrets

Nostr nsec Paper or metal

Bitcoin mnemonic Paper or metal. Do not store digitally.

PVK Paper or metal

zpub Can be stored digitally (not a spending key)

Backup locations:

- Paper: physically secure location (safe, locked drawer, trusted person)
- Metal: fireproof safe or safety deposit box
- Encrypted digital: offline USB drive, encrypted with strong passphrase

Do not:

- Photograph mnemonic or nsec
- Store in cloud-synced notes
- Store in cloud-synced password managers
- Email to yourself

8.2 Recovery Scenarios

Scenario Recovery

Forgot alias Use paper backup of derived secrets (nsec, mnemonic, PVK). Cannot regenerate from scratch.

Forgot password Same as above.

Lost nsec Regenerate in Passport with alias + password. Or use paper backup.

Lost mnemonic Regenerate in Passport with alias + password. Or use paper backup.

New device Install client, log in with nsec or import mnemonic.

8.3 Periodic Verification

Monthly:

- Verify burner network path works and IP is not leaking.
- Verify burner Nostr identity still posts and receives.
- Verify burner wallet balance via watch-only.

Quarterly:

- Review relay list. Remove non-operational or privacy-hostile relays.
- Review backup locations. Ensure secure and accessible.
- Review OpSec. Have you accidentally crossed streams?

Annually:

- Consider rotating network exit node.
- Consider rotating burner identity if suspicion of compromise.
- Review threat model.

8.4 Emergency Checklist

If you believe your burner identity is compromised:

1. Stop using it immediately.
2. Move funds from burner wallet to a new burner wallet (generate new identity with new alias and password).

3. Publish a final note on burner Nostr: "This identity is compromised. Do not trust messages from it."
 4. Do not delete the identity — you may need evidence.
 5. Investigate how the compromise happened.
 6. Rotate network credentials, relay list, backup locations.
 7. Document what happened and what you learned.
-

Appendix: Quick Reference

A.1 Passport Outputs

Output Format Storage

Alias String Public

Persona ID SIF-XXXX-XXXX-XXXX Public

PVK 64 hex chars Secret — paper/metal

Nostr npub npub1... Public

Nostr nsec nsec1... Secret — paper/metal

Bitcoin Seed 12 words Secret — paper/metal

Bitcoin Address bc1q... Public

Account zpub zpub... Sensitive — encrypted digital

A.2 Network Tools Quick Comparison

Tool	Setup	Kill Switch	Anonymous	Global Adversary	Best For
IPsec (self-hosted)	Medium	Yes	N/A	No	Self-hosted simplicity
Tailscale + Mullvad	Easy	No*	No	No	Mesh networking
Nym Mixnet	Easy	Yes	Yes	Yes	Maximum anonymity

*Tailscale requires manual pf firewall rules for kill switch.

A.3 Nostr Client Login

Client Platform Login Method

Damus iOS/macOS "I have an account" → paste nsec

Amethyst Android "Login with nsec" → paste nsec

Primal Web/Mobile "Login" → "Private Key" → paste nsec

Snort Web "Login" → "Private Key" → paste nsec

Coracle Web "Add Account" → "Private Key" → paste nsec

A.4 Bitcoin Wallet Import

Wallet Platform Import Method

BlueWallet iOS/Android Add Wallet → Import Wallet → Mnemonic → Custom path
m/84'/0'/0'

Sparrow Desktop File → New Wallet → Mnemonic → Native SegWit

Electrum Desktop File → New/Restore → Standard Wallet → I have a seed → Native SegWit

A.5 The Six Golden Rules

1. Never cross the streams.
2. Never reuse identifiers.
3. Never link in content.
4. Never transact directly.
5. Never trust a single layer.
6. Assume metadata leaks.

Final Word

"Never do anything illegal — and always upbuild society."

OpSec is not about paranoia. It is about intentionality — deciding what you share, with whom, and why. The tools in this guide — Passport, Nostr clients, Bitcoin wallets, and network privacy layers — give you the technical means to compartmentalize your digital life. But the discipline is yours.

Use these tools to build, to teach, to connect, and to uplift. Not to hide from accountability, but to protect the space you need to do good work.

Nunca hagas nada ilegal • Siempre edifica la sociedad.