AletheiaVox

COMPRENDRE · ÉCLAIRER · TRANSMETTRE

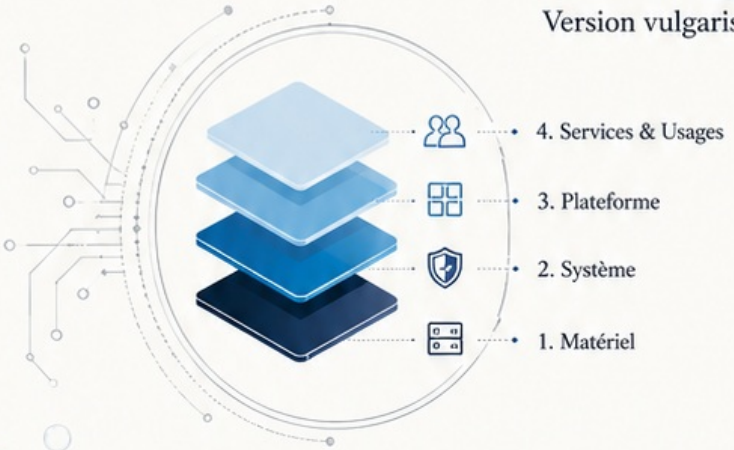
Livret de survie numérique

SecuBox-Deb

Reprendre la main sur son infrastructure,
couche par couche, cas d'usage par cas d'usage.

CyberMind · SecuBox-Deb v2.4.x · Debian bookworm arm64

Version vulgarisée AletheiaVox



- Cas d'usage terrain
- Procédures de survie
- Checklists opérationnelles
- Méthodes claires et reproductibles

7 invariants · 4 couches · 9 cas d'usage · Procédures de survie · Checklists opérationnelles

Comprendre vite. Agir juste. Survivre proprement.

AletheiaVox

COMPRENDRE · ÉCLAIRER · TRANSMETTRE

Les 7 invariants & les 4 couches

Le socle à comprendre avant tout déploiement

Si vous ne retenez que cela, vous avez déjà l'essentiel :
des règles stables, puis une architecture lisible couche par couche.

LES 7 INVARIANTS

1. Le flux descend, la confiance ne remonte jamais.
2. Refus par défaut, dans les deux sens.
3. Une seule porte exposée sur Internet.
4. Rien ne tourne sur l'hôte : tout est isolé.
5. Une sauvegarde non restaurée n'est pas une sauvegarde.
6. Ce qui n'est pas journalisé n'a pas eu lieu.
7. Prévoir la sortie avant l'entrée.

LES 4 COUCHES

C1 — TRANSPORT
Zones, filtrage, routage

C2 — NOMMAGE & IDENTITÉ
DNS, certificats, comptes

C3 — SERVICES
Isolation, proxy, sauvegardes

C4 — ACCÈS DISTANT
Tunnel, révocation, secours

PRINCIPE CLÉ

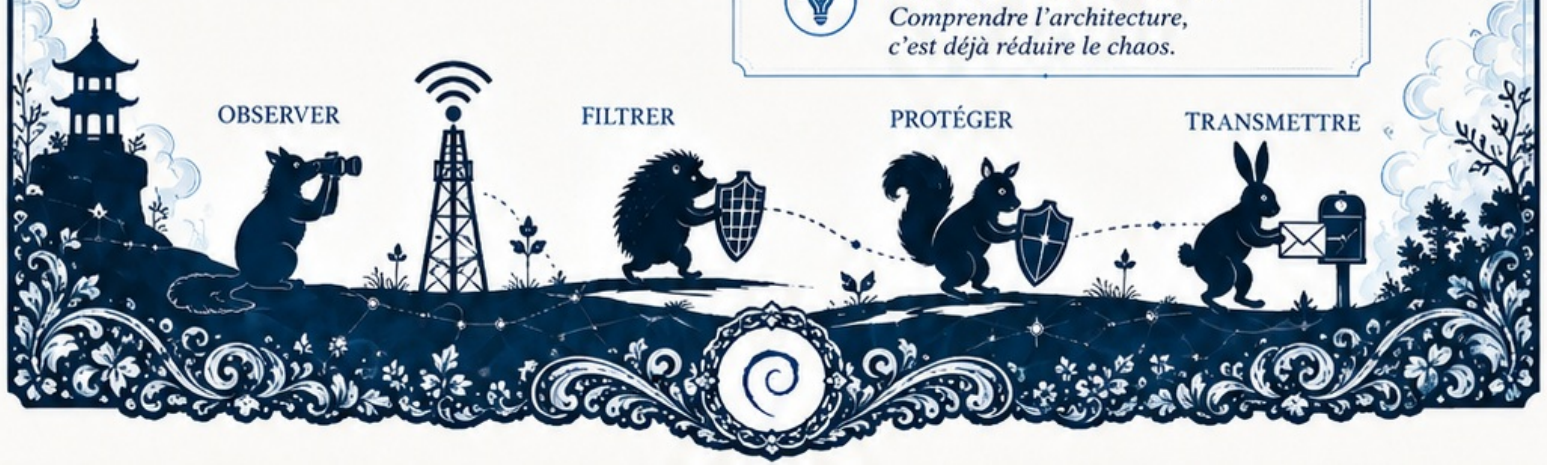
La confiance ne circule que vers le haut.
Une couche s'appuie sur celle qui la porte,
jamais sur celle qu'elle porte.

SYNTHÈSE À RETENIR

Une seule sortie.
Un seul port exposé.
Un seul chemin de secours testé.

NOTE DE VULGARISATION

Comprendre l'architecture,
c'est déjà réduire le chaos.



AletheiaVox

COMPRENDRE · ÉCLAIRER · TRANSMETTRE

Cas d'usage & procédures de survie

Neuf profils, puis les gestes essentiels quand ça casse

Une même architecture, plusieurs réglages selon le terrain.
Puis des réflexes clairs pour survivre aux incidents.

9 cas d'usage

A. Provider interne indépendant

B. Petite structure multi-postes

C. Nomade en mobilité

D. Site isolé, liaison dégradée

E. Atelier & labo forensic

F. Hébergement de services publics

G. Foyer familial & usage éducatif

H. Continuité en cas de coupure

I. Transmission & succession

En cas de problème

1 Suspicion de compromission

1. Isoler sans éteindre
2. Capturer le volatil
3. Empreinter
4. Analyser depuis l'extérieur
5. Décider : nettoyage ou reconstruction

2 Perte d'accès distant

1. Tunnel de secours
2. 4G hors bande
3. Console série
4. Pair témoin / Meshtastic
5. Déplacement physique

3 Perte de données

1. Arrêter d'écrire
2. Identifier le dernier instantané sain
3. Restaurer vers un emplacement distinct
4. Vérifier
5. Écrire le post-mortem

Ce qui survit n'est pas le plus complexe, mais le plus régulièrement testé.

Note pédagogique
Un cas d'usage n'est pas une autre architecture : c'est une instanciation des quatre couches.

AletheiaVox

COMPRENDRE · ÉCLAIRER · TRANSMETTRE

SecuBox-Deb — version courte terrain

Les réflexes essentiels, en une page

1 Avant de déployer

- Inventorier et supprimer les sorties parallèles
- Définir les zones
- Mettre le filtrage en drop sur input, forward et output
- Activer la journalisation des refus
- Tester le chemin de secours

2 En exploitation

- Lire les refus sortants chaque semaine
- Vérifier les sauvegardes
- Tester une restauration chaque mois
- Revoir comptes, sessions et clés
- Mettre à jour et contrôler les services

3 En urgence

- Ne pas redémarrer
- Isoler sans éteindre
- Capturer le volatil
- Empreinter
- Reconstruire si noyau, boot ou admin sont touchés

4 À retenir

- Une seule porte exposée
- Une clé de tunnel par appareil
- Zone vpn distincte de trust
- Les sauvegardes se testent
- Le WAN se coupe 24 h au moins 2 fois par an

Ports exposés :
51820/udp ;
+ 443/tcp et 25/tcp seulement selon profil.

Comprendre vite. Agir juste. Survivre proprement.

CYBERMIND · DEBIAN BOOKWORM ARM64

Livret de survie numérique

Reprendre la main sur son infrastructure — architecture en quatre couches et neuf cas d'usage SecuBox-Deb.

SecuBox-Deb v2.4.x

Juridiction Cour d'appel de Chambéry

CyberMind — Notre-Dame-du-Cruet, Savoie

Août 2026

Sommaire

Préambule — comment lire ce livret

Ce livret ne se lit pas en entier. Il se traverse.

- **Partie I** pose les invariants. Sept règles. Si vous n'en retenez que ça, vous avez déjà 80 % du bénéfice.
- **Partie II** déroule l'architecture en quatre couches. C'est le squelette commun à tous les déploiements.
- **Partie III** décline neuf cas d'usage. Chacun est une instanciation des quatre couches, pas une architecture différente. Allez directement au vôtre.
- **Partie IV** couvre la survie proprement dite : ce qu'on fait quand ça casse.
- **Partie V** rassemble les checklists opérationnelles.
- **Partie VI** contient les annexes de référence (adressage, matrice de flux, ports).

Convention typographique : `commande` en monospace, `ATTENTION` pour les pièges qui coûtent cher, `CYCLE` pour les points à réévaluer périodiquement.

PARTIE I — Les sept invariants

Ces règles ne se négocient pas au cas par cas. Elles précèdent toute décision de configuration.

I1 — Le flux descend, la confiance ne remonte jamais. Chaque couche fait confiance à celle qui la porte, jamais à celle qu'elle porte. Un service compromis ne doit rien pouvoir affirmer sur son identité auprès de la couche transport.

I2 — Refus par défaut, dans les deux sens. Le filtrage sortant n'est pas une coquetterie. C'est ce qui transforme une compromission en incident contenu plutôt qu'en exfiltration. La règle `policy drop` s'applique à `output` autant qu'à `input` et `forward`.

I3 — Une seule porte. Un port exposé sur Internet. Un seul. Tout le reste passe par le tunnel ou n'existe pas. Chaque service supplémentaire directement exposé multiplie la surface, pas linéairement.

I4 — Rien ne tourne sur l'hôte. L'hôte route, filtre, mesure. Il n'héberge pas. Tout service vit dans son unité isolée, avec son utilisateur, ses capacités réduites, son système de fichiers en lecture seule.

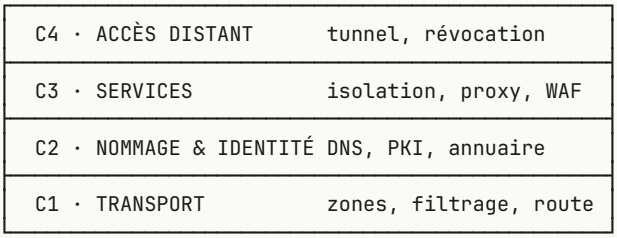
I5 — Une sauvegarde non restaurée n'est pas une sauvegarde. Le test de restauration est planifié, pas improvisé. Il figure au calendrier au même titre que la sauvegarde elle-même.

I6 — Ce qui n'est pas journalisé n'a pas eu lieu. Les refus se journalisent. Les authentifications se journalisent. Le journal est chaîné (BLAKE2b) et répliqué hors de la machine qui le produit.

I7 — Prévoir la sortie avant l'entrée. Avant d'activer un accès distant, on prépare le chemin de secours qui permettra d'y accéder quand cet accès sera tombé. Console série, clé de récupération, pair témoin. Toujours.

ATTENTION **Le piège classique** : appliquer I1 à I6 avec rigueur et oublier I7. Un jour, une règle `nft` mal ordonnée vous verrouille hors de votre propre passerelle, à 400 km de distance.

PARTIE II — L'architecture en quatre couches



Couche 1 — Transport

1.1 Le principe

La SecuBox est le point de sortie unique. Pas un point de sortie parmi d'autres : **le** point de sortie. S'il existe un chemin qui la contourne — un partage de connexion oublié, un routeur opérateur laissé en mode routeur, un dongle 4G sur un poste — l'ensemble de l'édifice est décoratif.

Premier travail, avant toute configuration : **inventorier les chemins de sortie** et les supprimer. Le routeur opérateur passe en mode pont (bridge). Si l'opérateur ne le permet pas, on le place en DMZ vers la SecuBox et on considère son réseau interne comme hostile.

1.2 Le zonage

Quatre zones minimum. Cinq si vous manipulez des éléments non fiables.

Zone	Rôle	Sortie Internet	Vers services	Entre zones
`trust`	postes de travail, admin	oui	oui	→ toutes
`svc`	conteneurs de services	restreinte	n/a	aucune
`guest`	visiteurs, terminaux tiers	oui	non	aucune
`iot`	objets connectés, domotique	liste blanche	broker seul	aucune
`dirty`	analyse, forensic, quarantaine	aucune	aucune	aucune

Le portage se fait par interfaces physiques distinctes quand c'est possible, par VLAN 802.1Q sinon. Si votre switch ne gère pas les VLAN, remplacez le switch : c'est le meilleur rapport sécurité/euro de tout ce livret.

ATTENTION **VLAN ≠ isolation forte.** Un VLAN protège d'un voisin curieux, pas d'un attaquant déterminé sur le même switch (VLAN hopping, saturation de table CAM). Pour la zone `dirty`, exigez une séparation physique.

1.3 Le filtrage

Squelette `nftables` — la structure importe plus que les lignes.

```
table inet filter {
  chain input {
    type filter hook input priority 0; policy drop;
    ct state established,related accept
    ct state invalid drop
    iif lo accept

    # une seule porte
    udp dport 51820 accept comment "wireguard"

    # administration : depuis trust uniquement
    iifname $trust tcp dport 22 accept

    # DNS et DHCP servis aux zones internes
    iifname { $trust, $guest, $iot } udp dport { 53, 67 } accept
    iifname { $trust, $guest, $iot } tcp dport 53 accept

    log prefix "IN-DROP " level info
  }

  chain forward {
    type filter hook forward priority 0; policy drop;
    ct state established,related accept

    # trust sort librement
    iifname $trust oifname $wan accept

    # guest sort, et rien d'autre
    iifname $guest oifname $wan accept

    # iot : liste blanche stricte
    iifname $iot oifname $wan ip daddr @iot_allow accept

    # accès aux services : par le proxy uniquement
    iifname $trust oifname $svc tcp dport { 443 } accept

    log prefix "FWD-DROP " level info
  }

  chain output {
    type filter hook output priority 0; policy drop;
    ct state established,related accept
    oif lo accept
    # la box elle-même : DNS amont, NTP, dépôts, rien de plus
    meta skuid $resolver udp dport 53 accept
    meta skuid $resolver tcp dport { 53, 853 } accept
    udp dport 123 accept
    meta skuid $apt tcp dport { 80, 443 } accept
    log prefix "OUT-DROP " level info
  }
}
```

Le `set @iot_allow` se remplit **par observation** : on laisse tourner une semaine en mode `log` sans `drop`, on lit les journaux, on liste les destinations légitimes, puis on bascule. Un thermostat qui parle à trois serveurs a trois entrées. S'il en réclame trente, c'est déjà l'information la plus utile que ce livret vous aura apportée.

1.4 Le routage et la sortie

Trois options de sortie, cumulables par zone :

- **Directe** — sortie opérateur nue. Rapide, traçable par l'opérateur.
- **Relais MirrorNet** — sortie par pair distant. Voir couche 4.
- **Tor local** — sortie par le circuit Tor porté par la box. Lente, adaptée aux flux de faible débit et de forte sensibilité.

La politique se décide par zone, pas globalement. Typiquement : `trust` en directe avec bascule manuelle, `dirty` sans sortie du tout.

CYCLE **À réévaluer** : le plan d'adressage à chaque ajout de zone ; les règles `output` à chaque nouveau démon sur l'hôte.

Couche 2 — Nommage et identité

C'est la couche qu'on saute et qu'on regrette. Sans elle, vous n'avez pas une infrastructure : vous avez une pile de services qui se trouvent sur la même machine.

2.1 Résolution DNS

Un résolveur récursif validant DNSSEC, portant votre zone interne, refusant toute requête venue de l'extérieur.

```
# unbound — extrait significatif
server:
    interface: 10.42.0.1
    access-control: 10.42.0.0/16 allow
    access-control: 0.0.0.0/0 refuse

    hide-identity: yes
    hide-version: yes
    qname-minimisation: yes
    aggressive-nsec: yes
    harden-glue: yes
    harden-dnssec-stripped: yes
    val-permissive-mode: no

    # zone interne autoritaire
    local-zone: "sbx.lan." static
    local-data: "nas.sbx.lan. A 10.42.30.10"
    local-data: "mail.sbx.lan. A 10.42.30.20"

forward-zone:
    name: "."
    forward-tls-upstream: yes
    forward-addr: <résolveur amont 1>
    forward-addr: <résolveur amont 2>
```

Deux décisions importantes :

Les noms sont stables, les adresses ne le sont pas. Vous nommez `nas.sbx.lan`, jamais `10.42.30.10` dans une configuration. Le jour où vous déplacez le service, vous changez une ligne de zone au lieu de fouiller quarante fichiers.

Choisissez un suffixe que vous contrôlez. `.lan` et `.home` sont des choix par défaut acceptables mais entrent en collision avec des résolutions publiques dans certains contextes. Un sous-domaine d'un domaine que vous possédez (`int.exemple.fr`) évite toute ambiguïté et permet des certificats publics si besoin.

2.2 Autorité de certification interne

Une AC racine hors ligne, une AC intermédiaire en ligne qui signe à courte durée.

```
racine (10 ans, clé hors ligne, sur support chiffré au coffre)
  └── intermédiaire (2 ans, en ligne, sur la box)
        └── certificats de service (90 jours, renouvellement automatique)
```

La racine se génère une fois, sa clé ne touche jamais une machine connectée. On la sort pour signer une nouvelle intermédiaire, tous les deux ans. Le reste du temps, elle dort.

Le certificat racine se déploie sur **tous** les postes du parc, une bonne fois. Le gain n'est pas cosmétique :

- plus aucun avertissement de sécurité, donc plus d'habitude de cliquer « continuer quand même » ;
- un avertissement qui apparaît devient un **signal**, pas du bruit. C'est votre détection d'interception, gratuite.

ATTENTION Le déploiement de la racine sur les postes Android et iOS est le point qui échoue le plus souvent. Prévoyez la procédure par plateforme avant de généraliser.

2.3 Annuaire et comptes

Un référentiel unique de comptes, consommé par le proxy d'authentification (couche 3). Le point n'est pas la technologie — LDAP, base locale, fournisseur OIDC embarqué — mais la propriété suivante : **un compte se désactive à un seul endroit**.

La gestion service par service garantit qu'un compte oublié traînera quelque part. C'est mathématique : la probabilité qu'aucun ne soit oublié décroît exponentiellement avec le nombre de services. À 20 services, vous en oublierez.

Politique minimale :

- authentification à deux facteurs obligatoire pour tout compte administrateur ;
- comptes de service distincts des comptes humains, non interactifs ;
- revue trimestrielle des comptes actifs (voir Partie V).

Couche 3 — Services

3.1 Isolation

Chaque service tourne dans son unité, avec :

- un utilisateur dédié, non privilégié, sans shell ;
- les capacités réduites au strict nécessaire ;
- un système de fichiers en lecture seule, sauf le volume de données ;

- pas d'accès réseau autre que le réseau interne des services.

Durcissement systemd de référence :

```
[Service]
User=svc-exemple
Group=svc-exemple

ProtectSystem=strict
ProtectHome=yes
PrivateTmp=yes
PrivateDevices=yes
ProtectKernelTunables=yes
ProtectKernelModules=yes
ProtectKernelLogs=yes
ProtectControlGroups=yes
ProtectClock=yes
ProtectHostname=yes
ProtectProc=invisible

NoNewPrivileges=yes
RestrictSUIDSGID=yes
RestrictNamespaces=yes
RestrictRealtime=yes
RestrictAddressFamilies=AF_INET AF_INET6 AF_UNIX
LockPersonality=yes
MemoryDenyWriteExecute=yes

SystemCallFilter=@system-service
SystemCallFilter=~@privileged @resources @obsolete
SystemCallArchitectures=native

CapabilityBoundingSet=
AmbientCapabilities=

ReadWritePaths=/var/lib/exemple
StateDirectory=exemple
```

Vérifiez votre travail : `systemd-analyze security <unité>`. Une note supérieure à 5 sur un service exposé mérite une justification écrite.

3.2 Le point d'entrée unique

Un reverse proxy termine le TLS et porte l'authentification. Les services n'écoutent que sur boucle locale ou réseau interne — jamais sur une interface accessible depuis une zone utilisateur.

Chaîne de référence SecuBox :

```
Internet / tunnel
      │
   HAProxy (TLS 1.3, SNI)
      │
   sbxwaf (inspection, apprentissage, CrowdSec, cache, scale-to-zero)
      │
   ┌──┴──┬──────┬──────┬──────┐
  nas  mail  photo  git  billets…
```

`sbxwaf` apporte quatre choses qui comptent dans un contexte de survie :

- **inspection et blocage** avec apprentissage progressif des motifs de menace ;
- **bans gradués** via CrowdSec, plutôt que le tout-ou-rien ;

- **veille des vhosts** (scale-to-zero) : un service non sollicité s'endort et se réveille à la première requête. Sur une box à 231 vhosts, c'est la différence entre 8 Go saturés et 37 Mo de RSS ;
- **audit de cookies** et injection de bannière en ligne.

3.3 Sauvegarde

La règle 3-2-1 reste valide : trois copies, deux supports, une hors site.

- **Chiffrement avant départ.** La copie hors site est chiffrée localement, avec une clé qui ne quitte jamais votre contrôle. L'hébergeur distant ne doit rien pouvoir lire.
- **Instantanés courts + archives longues.** Instantanés horaires conservés 48 h, quotidiens 30 jours, mensuels 12 mois. Ajustez selon le volume, gardez les trois horizons.
- **Restauration testée.** Voir I5. Une restauration complète par trimestre, une restauration partielle par mois, tracées.

ATTENTION **Le rançongiciel cible les sauvegardes en premier.** Si votre destination de sauvegarde est montée en écriture permanente depuis la machine sauvegardée, vous n'avez pas de sauvegarde. Exigez soit un dépôt en mode ajout seul (append-only), soit une extraction pull depuis la destination, soit un support déconnecté.

Couche 4 — Accès distant

4.1 Le tunnel

Un port UDP. Authentification par clés uniquement — pas de mot de passe, pas d'exception.

Une clé par appareil. Pas une clé par personne : par appareil. C'est ce qui vous permet de révoquer le téléphone perdu sans réémettre pour l'ordinateur portable et la tablette.

```
[Interface]
Address = 10.42.90.1/24
ListenPort = 51820
PrivateKey = <clé serveur>

[Peer]
# tel-gandalf — révoqué séparément
PublicKey = <clé publique appareil>
PresharedKey = <psk par appareil>
AllowedIPs = 10.42.90.11/32
```

La `PresharedKey` par pair ajoute une couche symétrique : elle ne remplace pas la cryptographie du tunnel, mais elle vous protège d'une compromission future des primitives asymétriques sur du trafic capturé aujourd'hui.

4.2 Où atterrit-on ?

Pas en zone `trust`. C'est l'erreur la plus fréquente et la plus coûteuse.

Le tunnel débouche sur une zone dédiée `vpn` (10.42.90.0/24) qui a accès à ce dont vous avez besoin à distance — le proxy de services, peut-être l'administration — et rien d'autre. Un ordinateur portable compromis dans un aéroport ne doit pas devenir un poste de la zone de confiance.

```
# depuis vpn : le proxy, et l'admin depuis les appareils de confiance
iifname $vpn oifname $svc tcp dport 443 accept
iifname $vpn ip saddr @vpn_admin tcp dport 22 accept
```

4.3 Le chemin de secours

Invariant I7. Trois niveaux, du plus simple au plus robuste :

1. **Console série** — un adaptateur USB-série sur l'en-tête UART de la box, un poste dédié à côté. Fonctionne quand le réseau est mort. Indispensable pour un déploiement à domicile.
2. **Accès de secours hors bande** — modem 4G en veille, activable, sur une interface strictement filtrée. Pour les déploiements distants.
3. **Pair témoin MirrorNet / Meshtastic** — une balise LoRa qui remonte un état de santé et peut porter un ordre de réinitialisation signé. Fonctionne sans Internet, sans opérateur, sur batterie. C'est le dernier recours, et sur un site isolé c'est le recours.

ATTENTION Testez le chemin de secours **avant** d'en avoir besoin. Un chemin de secours non testé est une croyance, pas un plan.

PARTIE III — Les cas d'usage

Neuf profils. Chacun est un réglage des quatre couches, pas une autre architecture. La colonne « delta » indique ce qui change par rapport au socle.

A — Provider interne indépendant

Contexte : un foyer ou une structure autonome qui cesse de dépendre du cloud. La box devient passerelle, résolveur, relais mail, stockage, sortie chiffrée.

Delta par couche

Couche	Réglage
C1	Cinq zones complètes. Sortie directe par défaut, bascule MirrorNet manuelle. Filtrage sortant strict sur `iot`.
C2	Zone interne autoritaire complète. AC racine hors ligne obligatoire. Annuaire pour tous les membres du foyer.
C3	Pile complète : Nextcloud, mail + webmail, PhotoPrism, PeerTube, blog RSS, forge. Tous derrière sbxwaf.
C4	Tunnel + console série. Pas de 4G nécessaire (accès physique possible).

Le point dur : le mail. C'est le service qui décide si vous êtes réellement indépendant ou seulement hébergé chez vous. Trois obstacles :

1. **La réputation IP.** Une IP résidentielle est très largement rejetée. Solution réaliste : relais sortant chez un opérateur SMTP tiers, réception en direct chez vous. Vous gardez la souveraineté sur le contenu et le stockage, vous concédez le transport sortant.
2. **SPF / DKIM / DMARC.** Non négociables. `DMARC` en `p=quarantine` puis `p=reject` après deux semaines de rapports propres.
3. **La disponibilité.** Un MX secondaire qui met en file d'attente pendant vos coupures. Sans ça, une panne de 48 h vous fait perdre du courrier définitivement.

Ordre de déploiement recommandé — ne les inversez pas :

1. Zonage + filtrage (C1), validé une semaine en observation
2. DNS + AC + déploiement de la racine sur les postes (C2)
3. Tunnel + chemin de secours (C4) — avant les services, pour pouvoir intervenir
4. Stockage et sauvegarde (C3)
5. Le reste des services, un par semaine
6. Le mail en dernier, quand tout le reste est stable

Coût matériel de référence (BOM août 2026) : MOCHAbin 400 € + SSD 100 € + clé wifi 40 € + module Mesh 40 € + Zigbee 40 € = **620 €**.

B — Bureaux, petite structure multi-postes

Contexte : 5 à 30 postes, du personnel non technique, une obligation de continuité de service.

Delta par couche

Couche	Réglage
C1	Zone `trust` scindée par métier si les besoins divergent (compta / production / direction). VLAN obligatoires.
C2	Annuaire central non négociable. 2FA obligatoire pour tous, pas seulement les admins.
C3	Partage de fichiers + messagerie + sauvegarde postes. Journalisation renforcée.
C4	Tunnel pour le télétravail, une clé par appareil professionnel. 4G de secours.

Ce qui change vraiment par rapport au cas A : ce n'est pas la technique, c'est l'humain.

- **Documentez ou ça ne tiendra pas.** Un runbook par procédure courante : ajouter un poste, révoquer un départ, restaurer un fichier supprimé. Écrit pour quelqu'un qui n'est pas vous.
- **Le facteur bus.** Si vous êtes le seul à pouvoir intervenir, la structure a un point de défaillance unique qui s'appelle vous. Une seconde personne doit savoir accéder au coffre de clés et exécuter une restauration.
- **La procédure de départ.** Elle se déclenche le jour du départ, pas la semaine suivante. Compte désactivé, clés d'appareil révoquées, sessions invalidées, accès physique repris. Checklist en Partie V.

ATTENTION **Contexte réglementaire** : dès que vous traitez des données personnelles de salariés ou de clients, le RGPD s'applique — registre des traitements, information des personnes, sécurité proportionnée. L'auto-hébergement ne vous en dispense pas ; il vous en rend au contraire pleinement responsable.

C — Nomade, poste unique en mobilité

Contexte : un seul opérateur, un portable, des réseaux hostiles par défaut (hôtel, aéroport, coworking).

Delta par couche

Couche	Réglage
C1	La box est restée à la maison. Le poste applique son propre filtrage local, `drop` sortant sauf tunnel.
C2	Racine AC embarquée sur le poste. La résolution passe par le tunnel, jamais par le DHCP local.
C3	Aucun service local. Tout est distant.
C4	Tunnel permanent, remontée automatique, kill switch.

Le kill switch est le cœur du profil. Si le tunnel tombe, le trafic ne doit pas basculer en clair : il doit s'arrêter.

```
chain output {
  type filter hook output priority 0; policy drop;
  oif lo accept
  oifname $wg accept
  # uniquement le nécessaire pour monter le tunnel
  udp dport 51820 ip daddr <endpoint> accept
  udp dport 53 ip daddr <résolveur DHCP> accept comment "résolution endpoint seule"
}
```

Résolution DNS captive : le point de friction récurrent. Les portails captifs exigent une résolution en clair avant authentification. Procédure : autoriser temporairement la résolution locale, s'authentifier au portail, monter le tunnel, **refermer**. Ne laissez pas la règle temporaire devenir permanente.

ATTENTION **Le poste nomade est le maillon faible de tout le dispositif.** Chiffrement intégral du disque, verrouillage automatique court, aucune clé de tunnel non protégée par phrase de passe. Un portable volé déverrouillé, c'est votre infrastructure entière.

D — Site isolé, liaison dégradée

Contexte : montagne, satellite, liaison intermittente. Coupures mesurées en jours, pas en minutes.

Delta par couche

Couche	Réglage
C1	Fonctionnement nominal **hors ligne**. Toute dépendance à Internet pour un service local est un défaut de conception.
C2	Résolveur autoritaire complet en local, sans dépendance amont pour la zone interne. AC locale indispensable (pas de Let's Encrypt sans connectivité).
C3	Services conçus pour la réconciliation différée. Files d'attente persistantes.
C4	Meshtastic / MirrorNet comme canal de secours principal.

La règle d'or : hors ligne d'abord.

Testez le déploiement **câble WAN débranché.** Ce qui ne fonctionne pas dans ce mode ne fonctionnera pas pendant la tempête de février. Cela élimine d'office : toute authentification qui dépend d'un fournisseur externe, tout service qui valide sa licence en ligne, tout certificat public à renouvellement automatique.

Synchronisation opportuniste. Quand la liaison remonte, l'ordre de priorité est fixé à l'avance :

1. journaux d'incident et empreintes ALERTE·DÉPÔT
2. sauvegardes différentielles
3. courrier en file d'attente
4. mises à jour de paquets
5. le reste

Ne laissez pas `apt` saturer une liaison satellite pendant que vos journaux d'incident attendent.

La couche Meshtastic porte les balises d'empreintes et les ancres de notarisation. Débit dérisoire, portée considérable, indépendance opérateur totale. Ce n'est pas un canal de données : c'est un canal de **preuve et de commande**.

E — Atelier et labo forensic

Contexte : manipulation de matériel non fiable, analyse d'échantillons, rétro-ingénierie.

Delta par couche

Couche	Réglage
C1	Zone `dirty` **physiquement** séparée. Switch distinct, câblage distinct, pas de VLAN. Aucune route sortante.
C2	Aucune. La zone `dirty` n'a ni DNS interne ni AC. Elle ne doit rien pouvoir résoudre ni valider.
C3	Services d'analyse dans la zone, sans passerelle vers `svc`.
C4	Aucun accès distant vers `dirty`. Jamais.

Le transfert entre zones se fait par sas manuel. Support physique, empreinte calculée des deux côtés, jamais de partage réseau monté simultanément dans les deux zones. C'est fastidieux. C'est le prix.

`ATTENTION` **Les canaux auxiliaires** : USB, alimentation, Bluetooth, écran partagé, presse-papier d'hyperviseur. L'isolation réseau ne vaut rien si un échantillon peut sortir par une clé USB montée automatiquement. Désactivez le montage automatique. Physiquement, si possible.

Notarisation : toute pièce entrante est empreinte (BLAKE2b) et ancrée dans le journal chaîné **avant** analyse. Sinon vous ne pourrez rien affirmer sur l'intégrité de ce que vous avez examiné.

F — Hébergement de services publics

Contexte : vitrine, blog, PeerTube, forge — des services délibérément exposés à Internet.

Delta par couche

Couche	Réglage
C1	Zone `pub` distincte de `svc`. Aucune route de `pub` vers `trust` ni vers `svc`.
C2	Certificats publics pour les vhosts exposés (AC interne pour l'administration seulement).
C3	sbxwaf en première ligne, apprentissage actif, CrowdSec en bans gradués.
C4	Administration **exclusivement** par le tunnel. L'interface d'admin n'est jamais exposée.

La double interface est le motif structurant : `<svc>.domaine` en public, `admin.domaine/<svc>` accessible depuis le tunnel uniquement. Deux vhosts, deux politiques, jamais de mélange.

Ordres de grandeur observés (instance Armada 4 cœurs / 8 Go, 24 h) : 59 414 requêtes légitimes, 2 028 menaces bloquées, 138 services réveillés depuis la veille, 37 Mo de RSS, ~4 % CPU sur 231 vhosts. Le scale-to-zero est ce qui rend ces chiffres possibles sur ce matériel.

Ce qu'il faut accepter : exposer, c'est être attaqué en continu. Le but n'est pas zéro tentative — c'est zéro tentative réussie, et une visibilité complète sur ce qui est tenté. D'où l'importance du regroupement des attaquants par séquence-type de sondes : vous ne suivez pas des IP, vous suivez des campagnes.

G — Foyer familial et usage éducatif

Contexte : cohabitation de profils très inégaux en compétence, dont des mineurs.

Delta par couche

Couche	Réglage
C1	Zone `family` avec politique de sortie propre. Plages horaires portées au niveau réseau, pas au niveau des appareils.
C2	Comptes nominatifs pour chacun, y compris les enfants.
C3	Stockage familial partagé + espaces privés. Photos, médias.
C4	Tunnel pour les membres majeurs uniquement.

Le filtrage au niveau réseau est contournable et c'est normal. Un adolescent motivé passera. L'objectif n'est pas la coercition technique — c'est de rendre le fonctionnement visible et de servir de sup-

port de conversation. Un filtrage annoncé et expliqué a plus d'effet qu'un filtrage subi et découvert.

Bénéfice sous-estimé : un foyer où chacun a un compte nominatif sur une infrastructure locale est un foyer où l'on apprend ce qu'est une donnée personnelle. C'est de la pédagogie par l'architecture.

H — Continuité en cas de coupure ou de restriction

Contexte : coupure opérateur prolongée, filtrage amont, restriction d'accès.

Delta par couche

Couche	Réglage
C1	Politique de sortie multiple préconfigurée : directe / MirrorNet / Tor, bascule sans reconfiguration.
C2	Zone interne pleinement fonctionnelle sans amont.
C3	Tous services opérationnels en local.
C4	Relais multiples préappairés, Meshtastic actif.

Ce qui se prépare avant, pas pendant :

- les pairs MirrorNet **préappairés** — l'appairage est impossible quand le canal est déjà coupé ;
- les profils de bascule testés (générateur de profil partagé du module MESH : profil → systemd-networkd / wg-quick / babeld) ;
- une copie hors ligne de la documentation d'exploitation — sur papier ou sur support local. Un runbook qui n'est consultable que sur un service en ligne est inutile exactement quand il devient nécessaire.

Test semestriel `CYCLE` : coupez le WAN pendant 24 h. Notez tout ce qui casse. C'est votre feuille de route.

I — Transmission et succession

Contexte : que se passe-t-il si l'opérateur de la box disparaît, part, ou devient indisponible ?

C'est le cas d'usage que personne ne prépare et qui finit par arriver.

Le dossier de transmission, sur support chiffré, avec la procédure d'accès confiée séparément :

1. schéma d'architecture à jour (les quatre couches, votre instanciation)
2. plan d'adressage et matrice de flux
3. inventaire matériel et emplacements physiques
4. procédure d'accès au coffre de clés
5. procédure de restauration complète, testée et datée
6. liste des services, de leur criticité, et de ce qu'on peut éteindre
7. contacts : opérateur, registrar, hébergeur de sauvegarde

8. **procédure d'extinction propre** — comment arrêter tout ça sans perte de données, si personne ne veut reprendre

Le point 8 est le plus difficile à écrire et le plus utile. Une infrastructure dont on ne sait pas sortir est un piège pour ceux qui restent.

CYCLE **Revue annuelle.** Un dossier de transmission de trois ans est de la fiction.

PARTIE IV — Procédures de survie

4.1 Suspicion de compromission

Ne redémarrez pas. Le premier réflexe détruit l'essentiel des preuves en mémoire.

Ordre d'intervention :

1. **Isoler sans éteindre** — débrancher le lien WAN, laisser la machine alimentée et en fonctionnement.
2. **Capturer le volatil** — mémoire, connexions établies, processus, modules chargés, tables de filtrage. Vers un support externe, jamais sur la machine analysée.
3. **Empreinter** — BLAKE2b sur les captures, ancrage dans le journal chaîné. Vous datez et scellez avant de toucher à quoi que ce soit.
4. **Analyser depuis l'extérieur** — support en lecture seule, depuis la zone `dirty`, jamais depuis la machine elle-même.
5. **Décider** : nettoyage ou reconstruction.

Le critère de décision est simple : si la compromission a touché le noyau, l'amorçage, ou un compte privilégié — **reconstruction**. Pas de nettoyage. Un système dont on n'est pas certain n'est pas un système : c'est une source d'angoisse permanente et de décisions dégradées.

4.2 Reconstruction

Ordre imposé — chaque étape valide la précédente :

1. Réinstallation depuis un support vérifié (empreinte contrôlée sur une machine saine)
2. **Nouvelles clés partout.** Toutes. Tunnel, AC intermédiaire, comptes de service. On suppose tout ce qui était sur la machine comme connu de l'attaquant.
3. Restauration des **données** uniquement — jamais des configurations ni des binaires
4. Rejeu de la configuration depuis la source de vérité versionnée
5. Remise en service progressive, service par service, avec observation entre chaque

`ATTENTION` **Restaurer une configuration est la façon la plus fiable de restaurer la compromission.** La configuration se rejoue depuis git, pas depuis la sauvegarde.

4.3 Perte d'accès distant

Escalade dans l'ordre :

1. Tunnel de secours sur port alternatif (préconfiguré, jamais improvisé)
2. Accès hors bande 4G
3. Console série
4. Commande signée par pair Meshtastic
5. Déplacement physique

Si vous atteignez régulièrement le niveau 5, votre invariant I7 est mal appliqué. Corrigez le dispositif, pas l'incident.

4.4 Perte de données

1. **Arrêter d'écrire.** Immédiatement. Sur tout ce qui touche le volume concerné.
2. Identifier le dernier instantané sain — par date et par contrôle de contenu, pas par date seule.
3. Restaurer **vers un emplacement distinct**, jamais par écrasement.
4. Vérifier avant de basculer.
5. **Écrire le post-mortem** — cause, détection, correction, prévention. Sans ça, l'incident se reproduira à l'identique.

4.5 Compromission d'un appareil client

1. Révoquer la clé de tunnel **de cet appareil** (d'où : une clé par appareil)
2. Invalider les sessions du compte associé
3. Changer le mot de passe et régénérer les facteurs 2FA
4. Examiner les journaux du proxy pour cet appareil sur 30 jours
5. Évaluer ce à quoi il avait accès — et traiter ces données comme exposées

PARTIE V — Checklists

Mise en service

- ☐ Chemins de sortie parallèles inventoriés et supprimés
- ☐ Routeur opérateur en pont ou en DMZ
- ☐ Zones définies, VLAN configurés, séparation physique pour `dirty`
- ☐ Filtrage en `drop` par défaut sur `input`, `forward` **et** `output`
- ☐ Journalisation des refus active et vérifiée
- ☐ Semaine d'observation effectuée, `@iot_allow` constitué
- ☐ Résolveur opérationnel, DNSSEC validé, zone interne servie
- ☐ AC racine générée **hors ligne**, clé au coffre
- ☐ AC intermédiaire en service, renouvellement automatique testé
- ☐ Racine déployée sur 100 % des postes, y compris mobiles
- ☐ Annuaire opérationnel, 2FA sur les comptes admin
- ☐ Tunnel monté, une clé par appareil, `AllowedIPs` en /32
- ☐ Zone `vpn` distincte de `trust`, filtrage vérifié
- ☐ **Chemin de secours testé** (I7)
- ☐ Sauvegarde configurée, chiffrée, avec copie hors site
- ☐ **Restauration complète testée et datée** (I5)
- ☐ Configuration versionnée dans git
- ☐ Runbooks rédigés
- ☐ Dossier de transmission constitué

Hebdomadaire

- ☐ Lecture des refus sortants — toute nouveauté s'explique ou s'investigue
- ☐ Tableau de bord WAF : menaces, campagnes, nouveaux motifs
- ☐ Sauvegardes réussies sur les 7 derniers jours
- ☐ Espace disque et santé SSD
- ☐ Mises à jour de sécurité appliquées

Mensuel

- ☐ Restauration partielle testée (un fichier, un service)
- ☐ Revue des comptes actifs et des sessions ouvertes
- ☐ Revue des clés de tunnel — un appareil non utilisé depuis 90 jours se révoque
- ☐ Vérification des dates d'expiration de certificats
- ☐ `systemd-analyze security` sur les services modifiés

Trimestriel

- ☐ **Restauration complète** vers matériel de test
- ☐ Revue de la matrice de flux face à la configuration réelle
- ☐ Revue des comptes de service et de leurs privilèges
- ☐ Test du chemin de secours (les trois niveaux)
- ☐ Revue du plan d'adressage

Semestriel

- ☐ **Exercice de coupure WAN 24 h** — noter tout ce qui casse
- ☐ Test de bascule des sorties (directe / MirrorNet / Tor)
- ☐ Vérification de l'appairage des pairs MirrorNet
- ☐ Test de la liaison Meshtastic

Annuel

- ☐ Revue du dossier de transmission
- ☐ Revue des sept invariants face à la réalité du déploiement
- ☐ Renouvellement de l'AC intermédiaire (tous les 2 ans)
- ☐ Inventaire matériel et évaluation du vieillissement
- ☐ Exercice de reconstruction complète sur matériel de test

Départ d'un utilisateur

- ☐ Compte désactivé (jour J, pas J+1)
- ☐ Toutes les clés de tunnel de ses appareils révoquées
- ☐ Sessions actives invalidées sur tous les services
- ☐ Accès physique repris (badges, clés, matériel)
- ☐ Données personnelles traitées selon la politique de conservation
- ☐ Comptes de service dont il était le seul détenteur : transférés

PARTIE VI — Annexes

A6.1 Plan d'adressage de référence

Zone	Sous-réseau	VLAN	Usage
`wan`	—	—	liaison opérateur
`trust`	10.42.10.0/24	10	postes de travail, admin
`svc`	10.42.30.0/24	30	conteneurs de services
`pub`	10.42.40.0/24	40	services exposés
`guest`	10.42.50.0/24	50	visiteurs
`iot`	10.42.60.0/24	60	objets connectés
`dirty`	10.42.70.0/24	phys.	analyse, quarantaine
`vpn`	10.42.90.0/24	—	pairs de tunnel
`mesh`	10.42.100.0/24	—	relais MirrorNet

Le /16 laisse de la place. Vous en aurez besoin plus vite que prévu.

A6.2 Matrice de flux

Lecture : ligne = source, colonne = destination.

↓ vers →	wan	trust	svc	pub	guest	iot	dirty	vpn
trust	OUI	—	443	443	NON	admin	NON	NON
svc	LB	NON	—	NON	NON	NON	NON	NON
pub	LB	NON	NON	—	NON	NON	NON	NON
guest	OUI	NON	NON	NON	—	NON	NON	NON
iot	LB	NON	broker	NON	NON	—	NON	NON
dirty	NON	NON	NON	NON	NON	NON	—	NON
vpn	NON	NON	443	NON	NON	NON	NON	—

`OUI` libre · `NON` interdit · `LB` liste blanche · nombre = port autorisé

Cette matrice est la **source de vérité**. La configuration `nftables` en découle, pas l'inverse. En cas de divergence, c'est la configuration qui a tort.

A6.3 Ports exposés

Sur Internet : `51820/udp` (tunnel). Plus `443/tcp` et `25/tcp` en profil F ou A avec mail entrant.

C'est tout. Toute ligne supplémentaire dans ce tableau exige une justification écrite dans votre documentation.

En interne : voir la matrice A6.2.

A6.4 Ordre de démarrage des services

En cas de redémarrage complet, l'ordre compte :

1. réseau et filtrage
2. résolveur DNS
3. AC intermédiaire et distribution de certificats
4. annuaire
5. bases de données
6. tunnel
7. reverse proxy et WAF
8. services applicatifs
9. tâches de sauvegarde

Un service qui démarre avant sa dépendance échoue ou, pire, démarre dans un état dégradé silencieux.

A6.5 Modèle de post-mortem

```
INCIDENT — <identifiant> — <date>

Détection      : quand, par quel moyen, par qui
Chronologie    : horodatage des faits établis
Impact         : services, données, utilisateurs concernés
Cause racine   : le « pourquoi » derrière le « quoi »
Correction     : ce qui a été fait pour rétablir
Prévention     : ce qui change pour que ça ne se reproduise pas
Détection future: comment on le verra plus tôt la prochaine fois
```

Le post-mortem est **sans blâme**. Il porte sur le système, jamais sur la personne. Un post-mortem accusatoire garantit que le prochain incident sera dissimulé.

Pour finir

Ce livret décrit une pratique, pas un produit. Les quatre couches et les sept invariants tiennent quelle que soit la technologie que vous mettez dessous.

Ce qui distingue un déploiement qui survit d'un déploiement qui s'écroule, ce n'est jamais la sophistication : c'est la régularité des checklists, la sincérité des tests de restauration, et l'honnêteté du chemin de secours.

> Quand le réseau se ferme et que les datacenters brûlent des mégawatts, SecuBox fait l'inverse : un boîtier chez vous, sobre, sécurisé, qui vous rend la maîtrise de votre vie numérique.

CyberMind · Notre-Dame-du-Cruet, Savoie Licence CMSD-1.0 · Juridiction : Cour d’appel de Chambéry