Mode Opératoire

VLAN PLT et blocage des réseaux étudiants vers la plateforme docker-srv

Code :	MO-NET-009
Version :	1.0
Date :	21 septembre 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	21/09/2026	Création : mise en production du VLAN 250 PLT et blocage des réseaux étudiants (chantier à distance via VPN collègues).

1 Objet

Ce mode opératoire documente la sortie du plan d'administration de la plateforme Docker (`docker-srv`, CT 200) du réseau plat historique vers un **VLAN dédié 250 ń PLT ż** (`172.31.250.0/24`) routé et filtré par OPNsense, et le **blocage effectif des réseaux étudiants** (salles filaires `10.0.232.0/24` et `10.0.230.0/24`, VMs étudiantes `10.0.113.0/24`, Wi-Fi étudiants `10.0.240.0/24`) vers cette plateforme.

Il couvre : l'architecture cible, les règles pare-feu OPNsense et Proxmox, le marquage VLAN des commutateurs, le rebinding des ports Docker, les vérifications et le retour arrière.

2 Contexte et justification

Jusqu'à septembre 2026, la plateforme de services (portail Homer, supervision Grafana/-Prometheus/Kuma, SSO Authentik, Pi-hole, Portainer, Netbox, contrôleur UniFi…) était hébergée sur le réseau plat `10.0.0.0/16` en `10.0.112.20`. Sur un réseau plat, un poste étudiant de salle machine joint la plateforme **en L2 direct, sans traverser le pare-feu** : aucun filtrage OPNsense n'est possible. Le chantier SSO (MO-PLT-025) avait posé une barrière *applicative* (porte Authentik), mais les accès de secours par IP:port (Kuma `:3001`, Pi-hole `:8053`…) restaient joignables **sans aucune authentification** depuis tout le réseau.

Deux exigences du chantier :

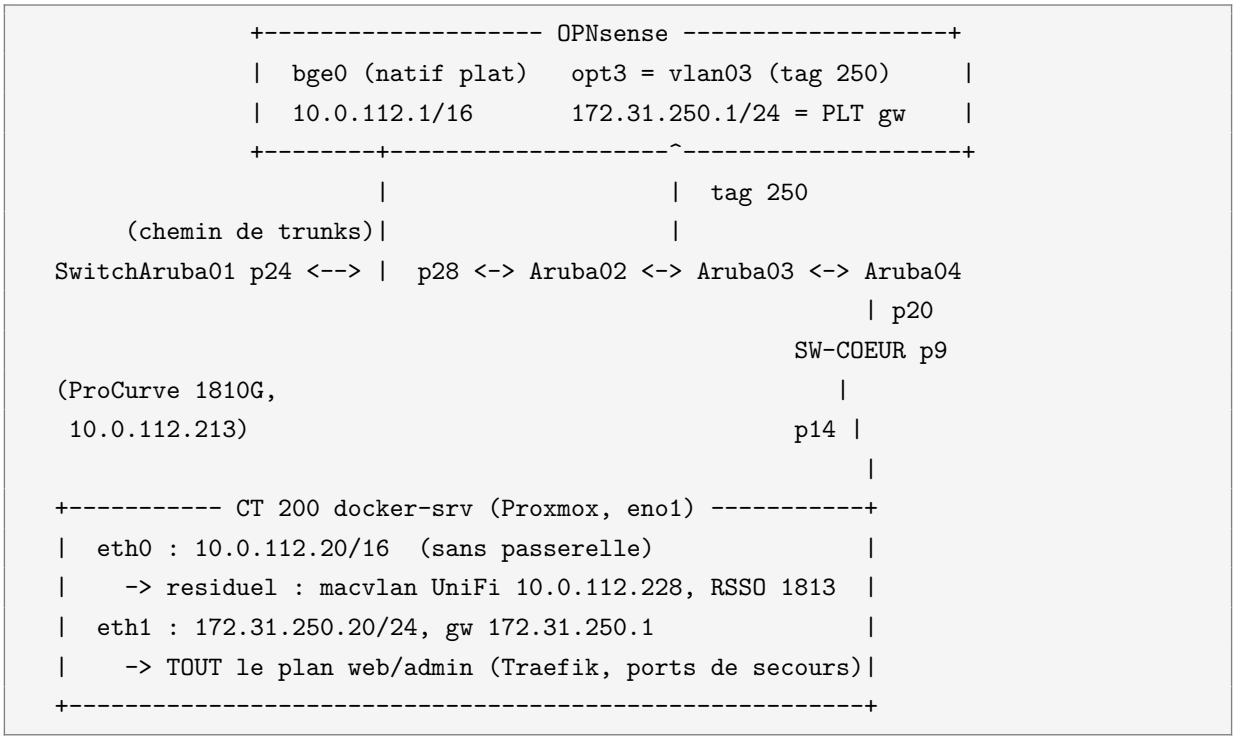
— **blocage réseau réel** des étudiants, pas seulement applicatif ;

— **restriction des accès de secours** sans les supprimer (break-glass conservé pour les admins).

Pourquoi un sous-réseau hors de 10.0.0.0/16. Les hôtes du plat ont un masque /16 : si la plateforme avait reçu une IP en `10.0.250.x`, ils l'auraient crue joignable en direct et auraient ARPé dans le vide. En choisissant `172.31.250.0/24`, tout trafic vers la plateforme passe obligatoirement par la passerelle OPNsense, qui filtre 100 % des flux. Effet secondaire utile : le blocage RFC1918 existant du VLAN 240 couvre déjà `172.16.0.0/12` — le Wi-Fi étudiants reste bloqué sans retouche.

Pourquoi ne pas réutiliser le VLAN 240 ou 241. Le 240 est le segment *à bloquer* (y loger la plateforme la rendrait injoignable par OPNsense, car intra-sous-réseau = non filtrable) ; le 241 (profs) est un segment d'accès clients avec DHCP et portail captif — un serveur n'y a pas sa place, et les profs y atteindraient les ports de secours en L2 direct sans pouvoir être limités au portail.

3 Architecture cible



Principes :

— **Dual-homing** : le CT conserve une jambe flat *uniquement* pour les flux de production des bornes (UniFi inform 8080, STUN 3478/udp, découverte 10001/udp, accounting RSSO 1813/udp) — ces flux sont L2 par nature et leur migration est une phase ultérieure (section 12).

— **Filtrage en deux couches** : OPNsense filtre tout ce qui entre/sort du VLAN 250 (routage obligé) ; le pare-feu Proxmox filtre ce qui reste sur la jambe flat (net0).

— **Routage par source (connmark)** dans le CT : chaque connexion est marquée à l'entrée (0x64 si eth0, 0x65 si eth1) et les réponses empruntent la table de routage de la jambe d'origine — indispensable, sinon les réponses aux clients du plat repartiraient par le VLAN (asymétrie).

— **Transition douce** : Traefik écoute encore sur `10.0.112.20:443` en plus de `172.31.250.20:443` tant que le DNS n'a pas basculé (les collègues VPN n'ont pas encore le sous-réseau PLT dans leur configuration).

4 Règles OPNsense

4.1 Interface

VLAN 250 sur `bge0` (`vlan03`), assigné en `opt3` ń PLT ż, IPv4 statique `172.31.250.1/24`, pas de passerelle, pas de DHCP (adressage statique uniquement).

4.2 Alias

— `Ports_Plateforme_Admin` (ports) : 22, 443, 8088, 9443, 3000, 3001, 8080, 8053, 9000 — SSH, Traefik et accès de secours web.

— `Reseaux_Etudiants` (réseaux) : `10.0.232.0/24` (salles filaires), `10.0.113.0/24` (VMs étudiantes), `10.0.240.0/24` (Wi-Fi étudiants).

4.3 Règles de filtrage (ordre d'évaluation)

Le trafic *vers* PLT entre dans OPNsense par d'autres interfaces (wireguard, lan, opt2…) : les règles sont donc **flottantes** (direction *in*, quick) — pattern éprouvé au chantier UniFi du 20/09. S'y ajoutent les règles d'interface opt3 (egress du CT) et une règle explicite dans le groupe wireguard (auto-documentation du cantonnement).

Flottantes (in, quick)	
150 PASS tcp	VPN collègues `10.10.30.0/24` → `172.31.250.20` ports `Ports_Plateforme_Admin`
151 PASS	VLAN admin `10.0.112.0/24` → `172.31.250.0/24`
152 PASS tcp	Wi-Fi profs `10.0.241.0/24` → `172.31.250.20:443` (portail seul)
153 BLOCK+log	`Reseaux_Etudiants` → `172.31.250.0/24`
Interface opt3	
10 BLOCK+log	`172.31.250.20` → `Reseaux_Etudiants` (pas d'initiation)
20 PASS	`172.31.250.20` → any (egress docker-srv)
Groupe wireguard	
250 PASS tcp	`10.10.30.0/24` → `172.31.250.20` ports `Ports_Plateforme_Admin` — insérée entre le PASS de cantonnement (200) et le BLOCK (300)

Le Wi-Fi étudiants (VLAN 240) était déjà bloqué vers tout RFC1918 (opt1, MO-NET-008) : le bloc couvre `172.16.0.0/12`, donc le VLAN PLT sans retouche. Le journal de cette règle a été activé à cette occasion (référence ğ10).

5 Marquage VLAN 250 sur les commutateurs

Marquage **tagged** additif (VLAN 1 natif préservé partout, continuité du plat) ; procédure générique MO-NET-003.

Commutateur	IP	Ports tagués 250 (rôle)
SwitchAruba01	`10.0.112.221`	p24 (vers OPNsense), p28 (vers Aruba02)
SwitchAruba02	`10.0.112.222`	p26 (vers Aruba03), p27 (vers Aruba01)
SwitchAruba03	`10.0.112.223`	p26 (vers Aruba04), p27 (vers Aruba02)
SwitchAruba04	`10.0.112.224`	p20 (vers cœur), p27 (vers Aruba03)
SW-COEUR (ProCurve 1810G)	`10.0.112.213`	p9 (vers Aruba04), p14 (vers Proxmox)

Correction d'inventaire

Le ń cœur ż est un HP ProCurve 1810G-24 (J9450A), pas un HP 1920G comme indiqué par erreur dans le MO-NET-008 (la notation GE1/0/9 y correspond au port 9). La reconnaissance du 21/09/2026 (LLDP sur Proxmox + SNMP) a établi : Proxmox `eno1` ↔ 1810G port 14. Le device NetBox a été corrigé en conséquence.

6 Proxmox et CT 200

1. `vmbr0` passé en VLAN-aware (`bridge-vlan-aware yes`) + `ifreload -a`, sous watchdog de restauration automatique (annulé après validation).
2. `bridge vlan add vid 250 dev eno1` — le bridge VLAN-aware n'autorise pas le VLAN sur l'uplink physique automatiquement au premier ajout d'un tag invité.
3. CT 200 : `net1` (tag 250, `172.31.250.20/24`, gw `172.31.250.1`) ajouté ; passerelle retirée de `net0` ; redémarrage.
4. **Routage par source** : unité systemd `flat-policy-routing.service` (`/root/flat-policy-routing.sh` dans le CT) — marquage connmark à l'ingrès (0x64/0x65), tables 100/101 (défaut via `10.0.112.1` / `172.31.250.1` + routes liées vers tous les bridges Docker + loopback), règles `from` pour `10.0.112.20/32` et `10.0.112.228/32`. Persistance prouvée par redémarrage du CT.

Pièges rencontrés (à connaître)

— **Après recréation avec bindings par IP, la chaîne filter `DOCKER` peut perdre l'ACCEPT FORWARD d'un port (443 Traefik) → timeout ; corriger par `docker compose down && up -d` et vérifier `iptables -L DOCKER -n`.**

— **Le conteneur UniFi (macvlan) route son trafic hors-/16 via la table *main* du CT (sa passerelle est le bridge Docker) : d'où la règle `from 10.0.112.228` vers la table flat.**

— **Le réseau macvlan UniFi a pour sous-réseau `10.0.0.0/16` : ne jamais créer de règle `from` globale sur cette plage (elle détournerait les flux forwardés après DNAT — testé et cassé puis corrigé).**

7 Rebinding des ports Docker

Service
Traefik 443/80
Portainer 9443, Grafana 3000, Kuma 3001, Netbox 8080, Pi-hole admin 8053, Authentik 9000, Homer
Pi-hole DNS 53 tcp/udp
RSSO 1813/udp
UniFi (macvlan `10.0.112.228`)

Conséquence immédiate : les accès de secours web **n'écoutent plus du tout sur le réseau plat** — structurellement invisibles pour les étudiants, joignables par les admins via le VLAN PLT (VPN collègues inclus).

8 Pare-feu Proxmox sur net0

Pare-feu PVE activé de manière ciblée : datacenter `enable=1` avec `policy_in ACCEPT` (l'hôte et les autres CT ne changent pas), puis option firewall du CT 200 et règles sur `net0` uniquement. Règles IN (ordre d'évaluation) :

0–3	ACCEPT bornes `10.0.230.0/24` → UniFi inform 8080, STUN 3478/udp, discovery 10001/udp, RSSO 1813/udp
4–5	ACCEPT DNS Pi-hole 53 tcp+udp (toute source — DNS de production des salles)
6	ACCEPT `10.0.112.0/24` (VLAN admin)
7	ACCEPT `10.10.30.0/24` (VPN collègues)
8	ACCEPT `10.0.241.0/24` (Wi-Fi profs)
9–12	DROP logué : salles filaires 232, VMs étudiantes 113, Wi-Fi étudiants 240, salles S112 (230, hors flux bornes)
13	DROP logué final (fail-closed)

Pièges PVE (à connaître)

- **`pvesh create .../firewall/rules` insère chaque règle en tête : créer dans l'ordre inverse de l'évaluation voulue.**
- **L'activation du pare-feu implique un filtre MAC de sortie par défaut (DROP si MAC ≠ celle du CT) — casse les conteneurs macvlan (UniFi) : poser `macfilter 0` et `ipfilter 0` dans les options firewall du CT.**
- **Le fichier de règles est `/etc/pve/lxc/200.fw` ; après édition directe, repasser par l'API pour forcer la recompilation (la vue pmxcfs peut rester périmée).**

Le blocage est **effectif dès maintenant** pour le filaire/VMs/Wi-Fi étudiants (testé par amputation : une règle DROP temporaire sur la source VPN du demandeur a produit le timeout attendu, puis retour au vert après suppression). Il deviendra **structurel** (résistant au spoofing d'IP) à la finalisation, quand l'écoute Traefik flat sera retirée.

9 Certificat

Le wildcard `*.docker.bts.sio` a été réémis par l'ADCS ń BTS SIO Root CA ż (gabarit `BTSSIOWebServer1an`, Request ID 13) avec SANs : `docker.bts.sio`, `*.docker.bts.sio`, IP `10.0.112.20` **et** `172.31.250.20`. Déployé dans Traefik (`/opt/docker/traefik/certs/`, couple wildcard remplacé, ancien conservé en `.bak-20260921`). La configuration CSR versionnée est `openssl-wildcard.cnf` (MO-SEC-005) mise à jour.

10 Vérifications

1. **Batterie HTTPS** (`check_https.sh`, validation par la racine ADCS, sans `-k`) : les 12 URLs au vert — porte Authentik (302 vers `auth.docker.bts.sio`) sur les services protégés, 200 Homer, page de login Portainer (200, OIDC natif).
2. **Négatif par amputation** : règle DROP temporaire sur la source VPN → timeout constaté, suppression → retour au vert.
3. **Non-régression production** : bornes UniFi en ligne (console 8443 OK), collecteur RSSO joignant l'API OPNsense, DNS Pi-hole résolvant depuis les salles, Prometheus et exporters joignables depuis le CT, Vaultwarden/Wazuh inchangés.
4. **VLAN 240** (re-vérification) : règles opt1 relues (ordre DNS → portail → BLOCK RFC1918 → Internet, quick) ; l'alias RFC1918 couvre `172.16.0.0/12` donc le VLAN PLT ; journal activé sur le bloc ; aucun client `10.0.240.x` n'interroge Pi-hole (indice de cloisonnement effectif). Test depuis un client Wi-Fi étudiant : à faire sur place (finalisation).
5. **Chemin VLAN de bout en bout** : `ping 172.31.250.1` depuis le CT et accès `172.31.250.20` depuis le VPN — validés après le marquage des commutateurs (voir ğ5).

11 Retour arrière

— **OPNsense** : supprimer les 7 règles (uuids notés au journal), les 2 alias, désassigner opt3, supprimer vlan03. Export XML pré-chantier : `opn_config_backup_2026-09-21.xml`.
— **Switches** : repasser les ports du VLAN 250 en ń non membre ż (le VLAN peut rester créé, inerte).
— **CT 200** : `pct set 200 -delete net1` + remettre `gw=10.0.112.1` sur net0 + reboot ; désactiver `flat-policy-routing.service` ; snapshot vzdump du 21/09 (18:29) disponible.
— **Docker** : archive `/root/docker-composes.bak-250.tgz` (hôte) — restaurer les composes et recréer.
— **Pare-feu PVE** : `pvesh set /nodes/pve/lxc/200/firewall/options -enable 0` (règles conservées pour réanalyse) ; datacenter `enable 0`.
— **Certificat** : restaurer le couple `wildcard.crt.bak-20260921` / `.key` si besoin.

12 Phase de finalisation (présentiel ou après coordination)

1. Bascule DNS `docker.bts.sio` + `*.docker.bts.sio` → `172.31.250.20` (zone DC1), puis retrait de l'écoute Traefik flat `10.0.112.20:443/80` — blocage alors structurel, y compris contre le spoofing d'IP.
2. Regénération + distribution des configurations VPN des collègues (`AllowedIPs` incluant `172.31.250.0/24` — script `opnsense_wg_peer.py`).
3. Migration des flux bornes vers le VLAN (inform par FQDN, macvlan UniFi sur le VLAN, RSSO 1813 via OPNsense) puis retrait complet de la jambe flat du CT 200.
4. Test terrain du VLAN 240 depuis un client Wi-Fi étudiant.
5. Extensions tracées : Postfix du CT 200 en loopback-only (actuellement `0.0.0.0:25` — recouvert par le DROP final net0) ; extension du filtrage aux CT Vaultwarden (127) et Wazuh (103) ; bascule du Zabbix restant.