BTS Services Informatiques aux Organisations

Option Solutions d'Infrastructure, Systèmes et Réseaux (S.I.S.R)

Documentation Technique | Épreuve E6 - Situation 1

DANIEL NASSIM SIO2-SISR

SOMMAIRE

DOCUMENTATION TECHNIQUE — OPNsense

Partie 1 — Installation initiale

1.1 Prérequis matériels

OPNsense est un pare-feu open source basé sur FreeBSD. Pour fonctionner correctement dans le cadre de l'infrastructure du Pamandzi Hotel, la machine hébergeant OPNsense doit disposer des caractéristiques suivantes :

Élément	Caractéristiques minimales	Caractéristiques recommandées
Processeur	64 bits, 1 GHz	64 bits, 1.5 GHz dual-core
Mémoire RAM	2 Go	4 Go
Stockage	8 Go	SSD 40 Go
Interfaces réseau	2 minimum (WAN + LAN)	2 ou plus

Dans notre cas, OPNsense a été déployé sur une machine physique dédiée disposant de deux interfaces réseau Ethernet :

- eth0 (re0) : connectée au réseau SIO (interface WAN), IP 172.18.153.208/21
- eth1 (em0) : connectée au port 23 du switch HP31 en mode trunk (interface LAN supportant les VLAN 1, 31, 32 et 33)

1.2 Téléchargement de l'image ISO

L'image d'installation est disponible sur le site officiel : https://opnsense.org/download/

Choisir :

- Architecture : amd64
- Type : DVD (image ISO complète) ou USB selon le support utilisé
- Mirror : choisir le miroir le plus proche géographiquement

Une fois l'image téléchargée, vérifier son intégrité avec le checksum SHA256 fourni sur le site avant de la graver sur un support bootable.

1.3 Installation sur la machine physique

L'installation se déroule en plusieurs étapes :

1. Insérer le support d'installation (USB ou DVD) et démarrer la machine dessus (modifier l'ordre de boot dans le BIOS si nécessaire).

2. Au boot, OPNsense charge un environnement de démonstration (live). Se connecter avec les identifiants par défaut :
    - Login : **installer**
    - Mot de passe : **opnsense**
    -

3. L'assistant d'installation se lance automatiquement. Suivre les étapes :
    - Keymap : sélectionner fr (clavier français)
    - Type d'installation : Install (UFS) pour une installation simple
    - Disque cible : sélectionner le disque de destination
    - Partitionnement : Auto (par défaut)

4. À la fin de l'installation, définir un mot de passe root robuste (à conserver précieusement).

5. Redémarrer la machine en retirant le support d'installation.

1.4 Configuration initiale (assignation des interfaces)

Au premier démarrage, OPNsense affiche une console de configuration. Il faut assigner les interfaces réseau :
1. Choisir l'option 1) Assign interfaces

2. Répondre aux questions :
- Configure VLANs now? → n (on les configurera via l'interface web)
- Enter the WAN interface name → re0 (selon le nom détecté par OPNsense)
- Enter the LAN interface name → em0
- Enter the Optional 1 interface name → laisser vide et appuyer sur Entrée

3. Confirmer avec y

4. Configurer l'IP de l'interface LAN (utile pour accéder à l'interface web depuis un poste admin) :
- Choisir l'option 2) Set interface IP address
- Sélectionner l'interface LAN
- Configurer une IP statique (exemple : 192.168.3.254/26 pour la passerelle VLAN1_ADMIN)

1.5 Premier accès à l'interface web

Pour accéder à l'interface d'administration d'OPNsense, il faut configurer un poste d'administration (PC admin) avec une adresse IP appartenant au même sous-réseau que l'interface LAN d'OPNsense (VLAN1_ADMIN — 192.168.3.192/26).

<u>Configuration IP du PC d'administration</u>

Le PC d'administration doit être branché sur un port du switch HP31 affecté au VLAN 1 (Admin) — par exemple le port 1. Ensuite, configurer ses paramètres réseau de la manière suivante :

Paramètre	Valeur
Adresse IP	192.168.3.200
Masque de sous-réseau	255.255.255.192 (équivalent /26)
Passerelle par défaut	192.168.3.254 (interface LAN d'OPNsense)
Serveur DNS préféré	192.168.3.254

Sur Windows, la configuration se fait via : Panneau de configuration > Réseau et Internet > Centre Réseau et partage > Modifier les paramètres de la carte > clic droit sur la carte Ethernet > Propriétés > Protocole Internet version 4 (TCP/IPv4) > Propriétés

Cocher "Utiliser l'adresse IP suivante" et "Utiliser l'adresse de serveur DNS suivante", puis renseigner les valeurs ci-dessus.

[CAPTURE 2] : Fenêtre des propriétés TCP/IPv4 du PC admin avec l'adresse 192.168.3.200/26 configurée

Vérification de la connectivité

Avant d'ouvrir le navigateur, vérifier que le PC admin peut joindre OPNsense en ouvrant une invite de commande (Windows : cmd) et en tapant :

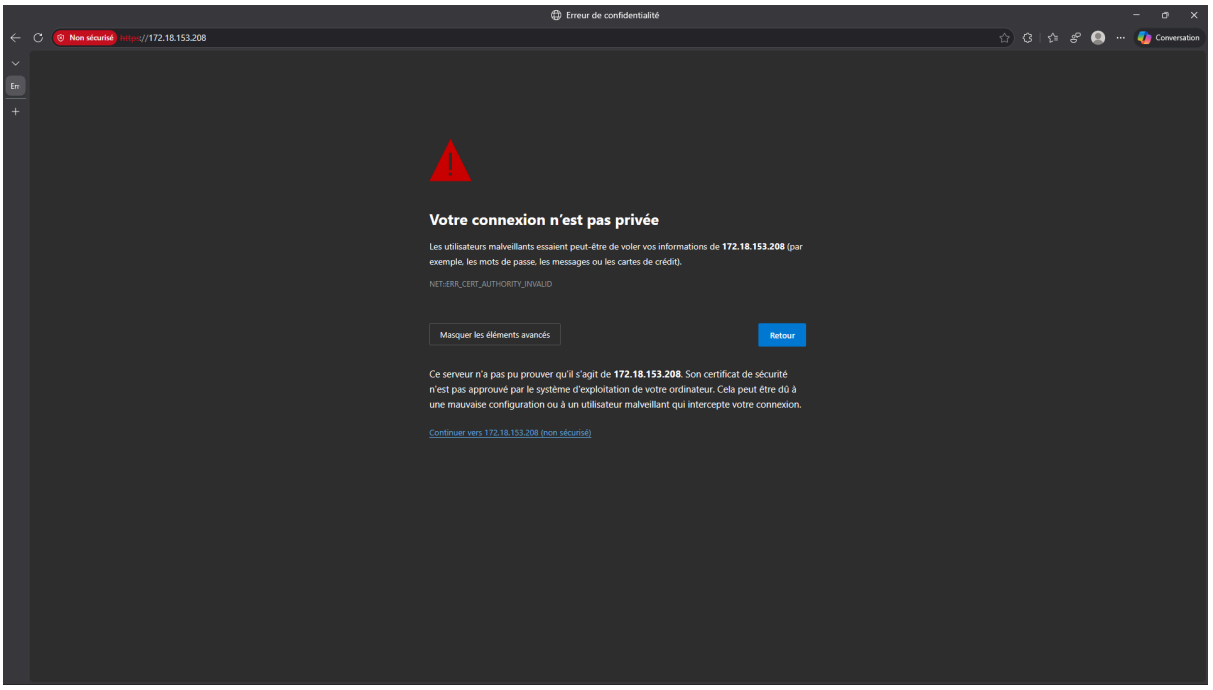
ping 192.168.3.254

Si OPNsense répond, la configuration réseau est correcte.
[CAPTURE 3] : Résultat du ping vers 192.168.3.254 depuis le PC admin (réponses positives)

Accès à l'interface web

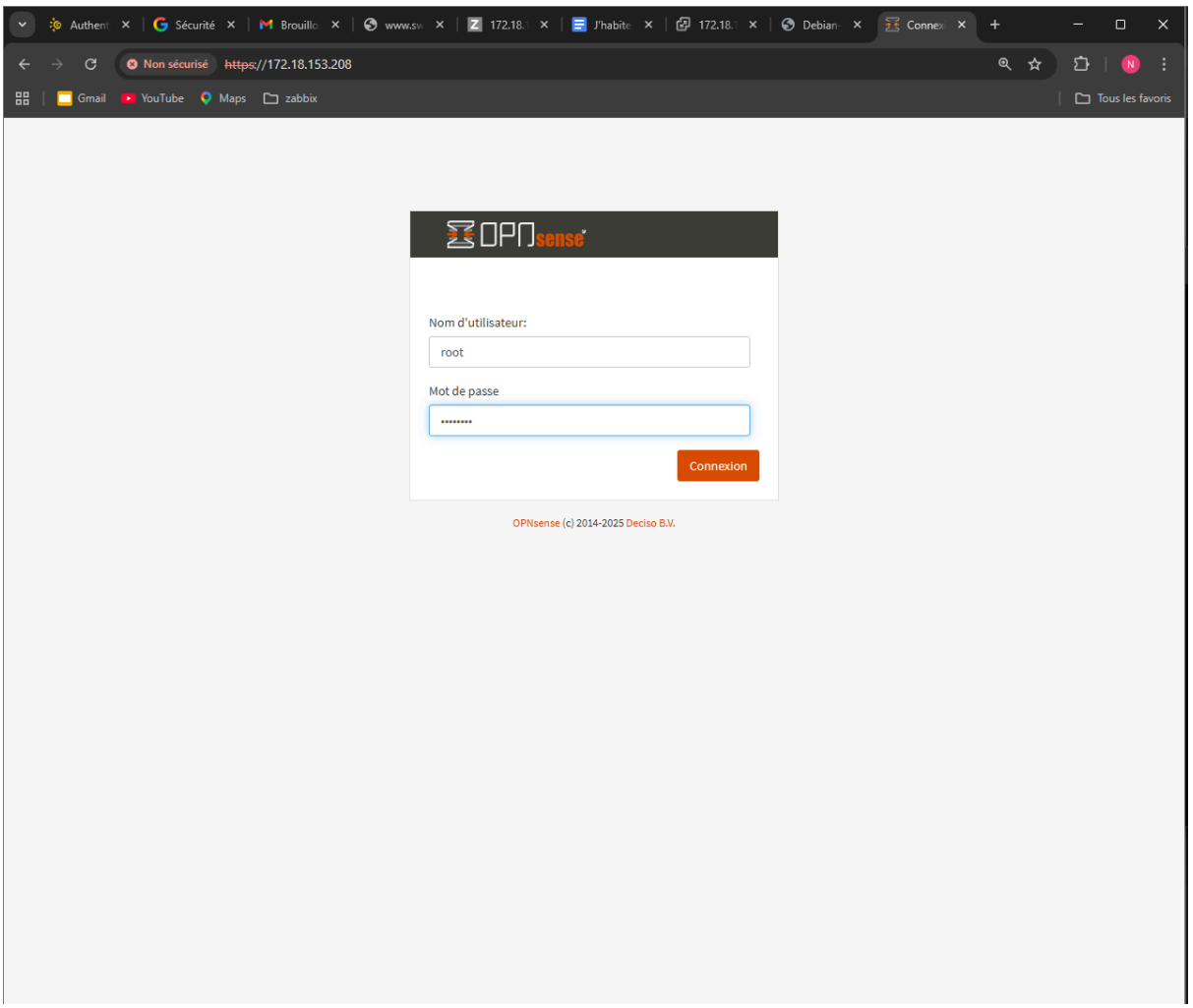
Ouvrir un navigateur (Edge, Chrome, Firefox) et accéder à l'URL : https://192.168.3.254

Le navigateur affichera un avertissement de certificat (auto-signé par OPNsense lors de l'installation) — c'est normal lors du premier accès. Cliquer sur "Avancé" puis "Continuer vers le site (non sécurisé)".

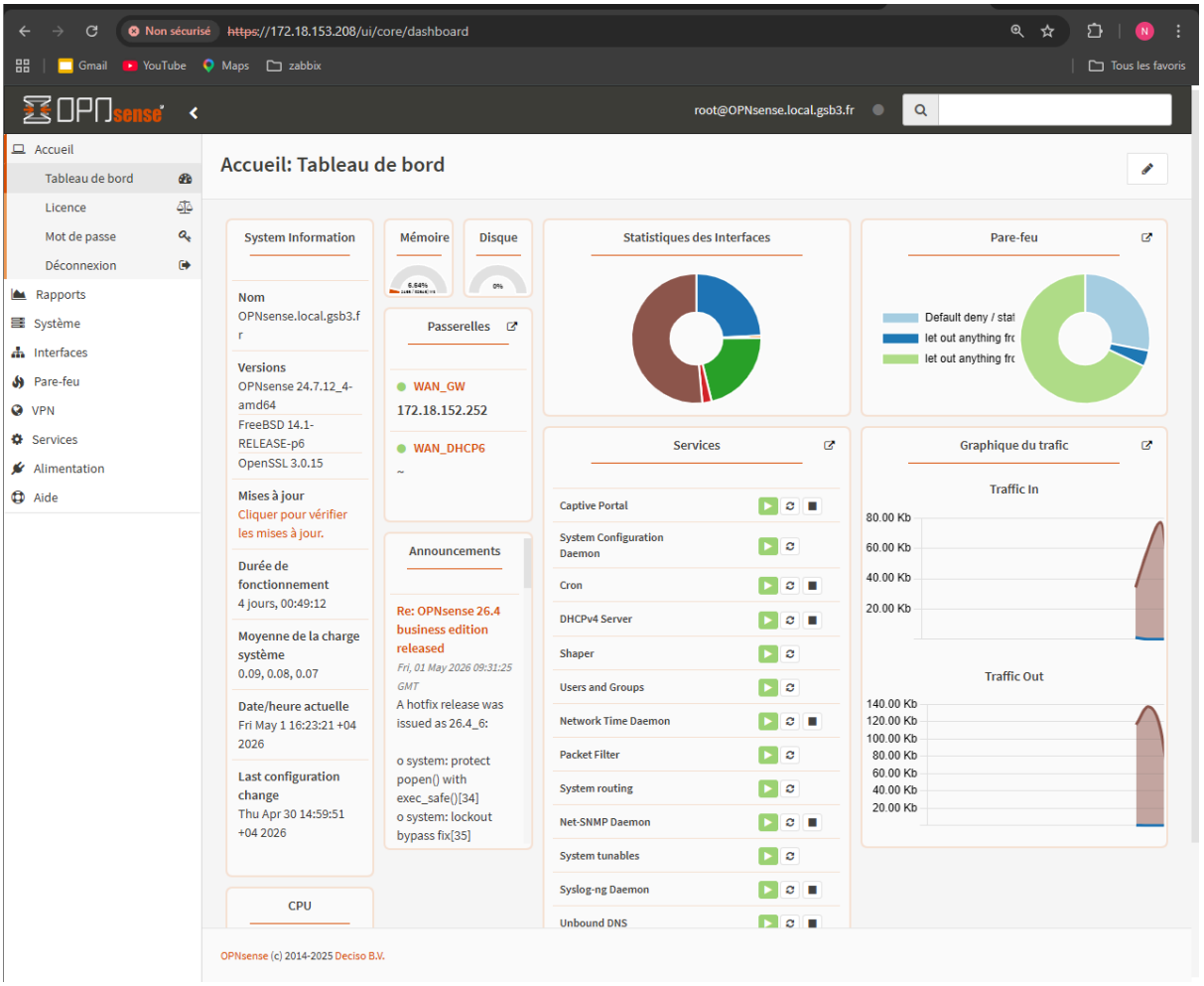


S'authentifier avec :

- Login : root
- Mot de passe : celui défini lors de l'installation



Au premier accès, OPNsense propose un assistant de configuration (Setup Wizard). Il est recommandé de le suivre pour configurer les paramètres de base (hostname, DNS, fuseau horaire), bien que ces paramètres puissent être modifiés ultérieurement.

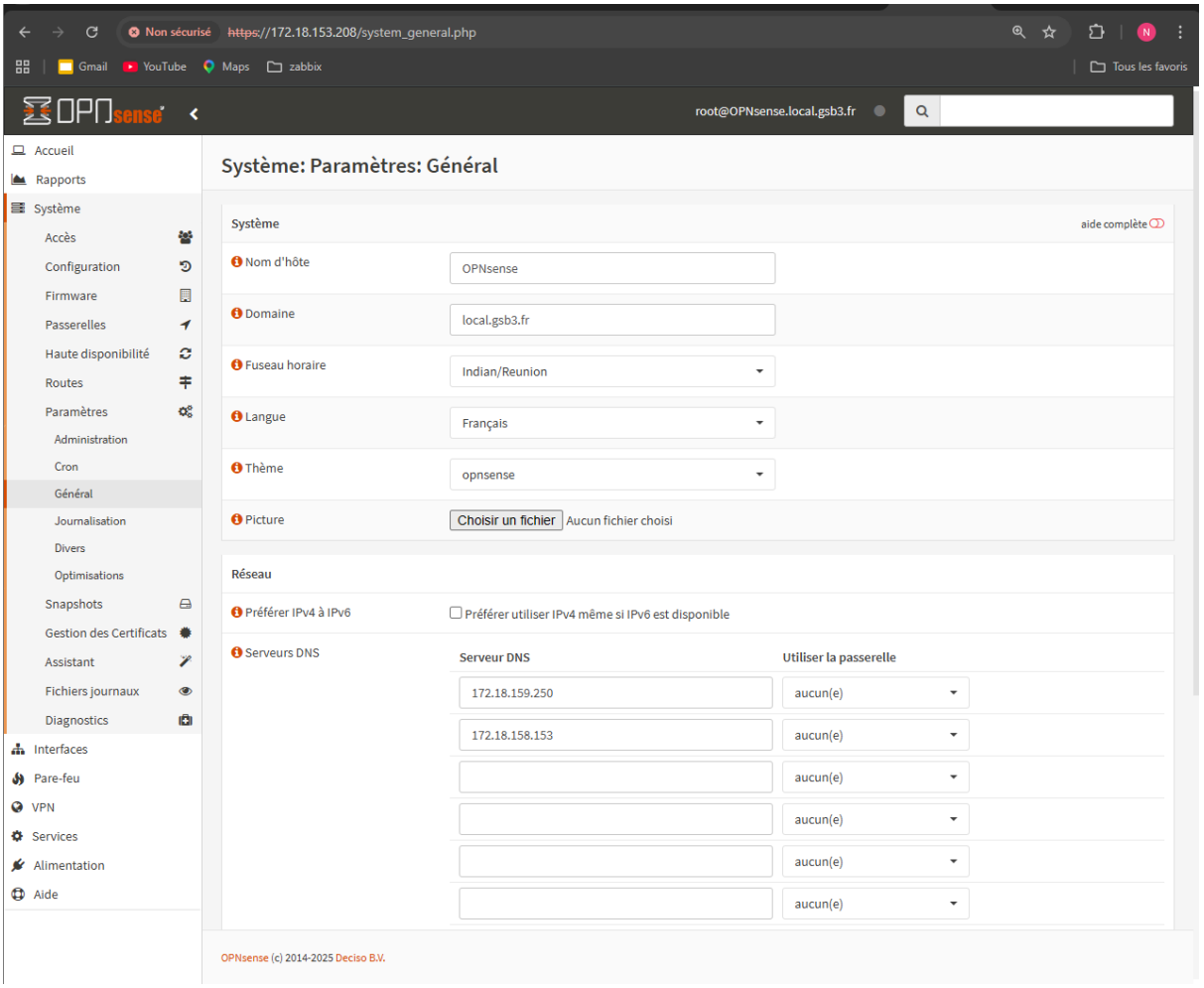


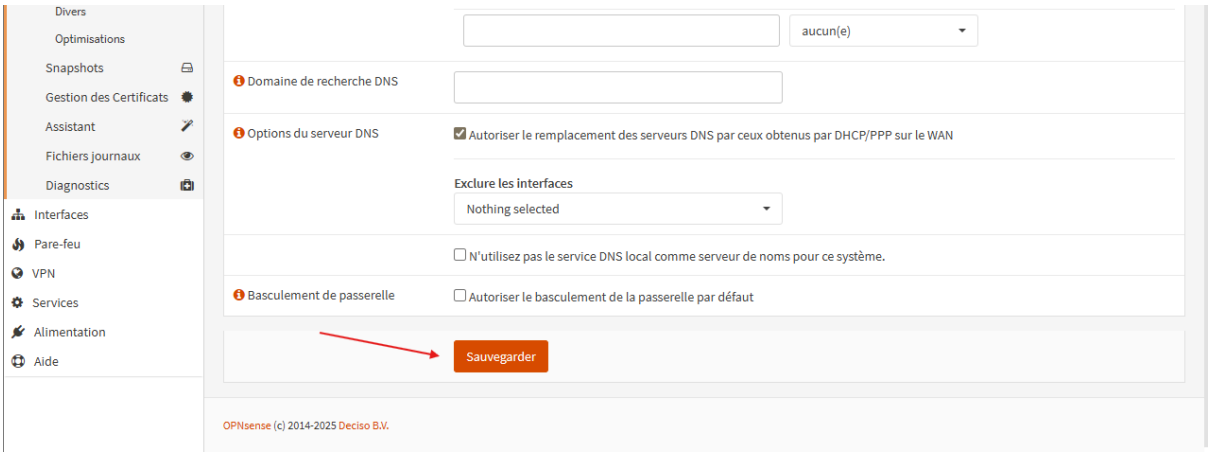
1.6 Configuration générale (hostname, DNS, fuseau horaire)

Aller dans Système > Paramètres > Général.

Configurer les paramètres suivants :

Paramètre	Valeur
Hostname	OPNsense
Domain	local.gsb3.fr
Serveurs DNS	8.8.8.8 (Google), 1.1.1.1 (Cloudflare)
Override DNS	Coché (autorise OPNsense à utiliser les DNS du WAN si dispo)
Time zone	Indian/Reunion (ou la zone géographique appropriée)
Language	French
Theme	(au choix)





Cliquer sur Sauvegarder en bas de page.

L'hostname complet sera donc OPNsense.local.gsb3.fr. Il sera utilisé notamment pour les certificats internes et pour identifier la machine sur le réseau.

Partie 2 — Configuration des VLAN

2.1 Introduction aux VLAN

Un VLAN (Virtual Local Area Network) permet de segmenter logiquement un réseau physique en plusieurs sous-réseaux indépendants. Cette segmentation présente plusieurs avantages :

- Sécurité : isolation des flux entre groupes d'utilisateurs (ex : invités et employés ne sont pas sur le même réseau)
- Performance : limitation du trafic broadcast à chaque VLAN
- Organisation : adressage IP cohérent par usage (admin, employés, visiteurs, équipements)
- Souplesse : un changement d'affectation se fait par configuration logique, sans recâblage

Dans le cadre du Pamandzi Hotel, l'infrastructure est segmentée en quatre VLAN :

VLAN	Nom	Usage	Sous-réseau	Passerelle (OPNsense)
1	VLAN1_ADMIN	Administration des équipements (postes admin, switches HP31/HP32)	192.168.3.192/26	192.168.3.254
31	VLAN31_PERSONNEL	Personnel et clients HallInclusive (Wi-Fi avec accès DMZ)	192.168.3.0/26	192.168.3.60
32	VLAN32_VISITEURS	Visiteurs classiques (Wi-Fi Internet uniquement)	192.168.3.64/26	192.168.3.124
33	VLAN_MANAGEMENT	Plan de gestion du WAP3 (séparé du plan de données)	192.168.3.128/26	192.168.3.190

Tous les VLAN sont transportés via un seul lien physique (port 23 du switch HP31 vers l'interface eth1 d'OPNsense) configuré en mode trunk 802.1Q (étiquetage des trames par VLAN).

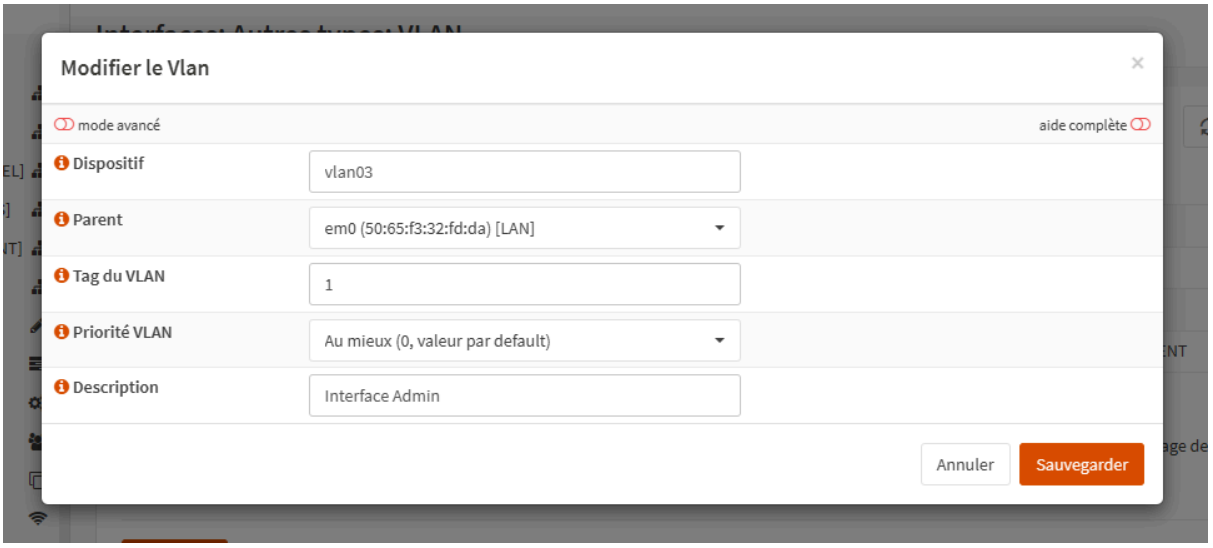
2.2 Création des VLAN dans OPNsense

Aller dans Interfaces > Autres types > VLAN.
Cliquez sur le bouton + Ajouter en haut à droite pour créer chaque VLAN.

VLAN 1 (Admin)

Paramètre	**Valeur**
Interface parent	em0 (interface LAN physique)
Tag VLAN	1
Priorité VLAN	0 (priorité par défaut)
Description	Interface Admin

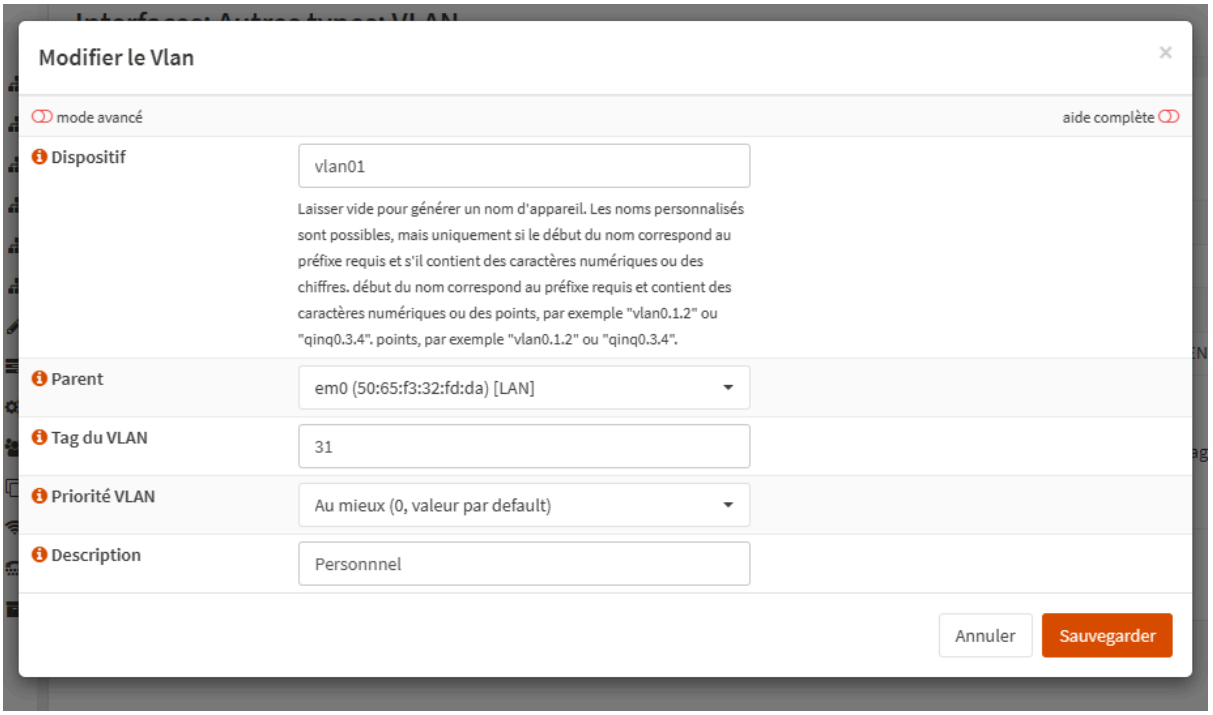
Cliquer sur Sauvegarder.



Dispositif : Laisser vide pour générer un nom d'appareil

VLAN 31 (Personnel)

Paramètre	**Valeur**
Interface parent	em0
Tag VLAN	31
Priorité VLAN	0
Description	Personnnel

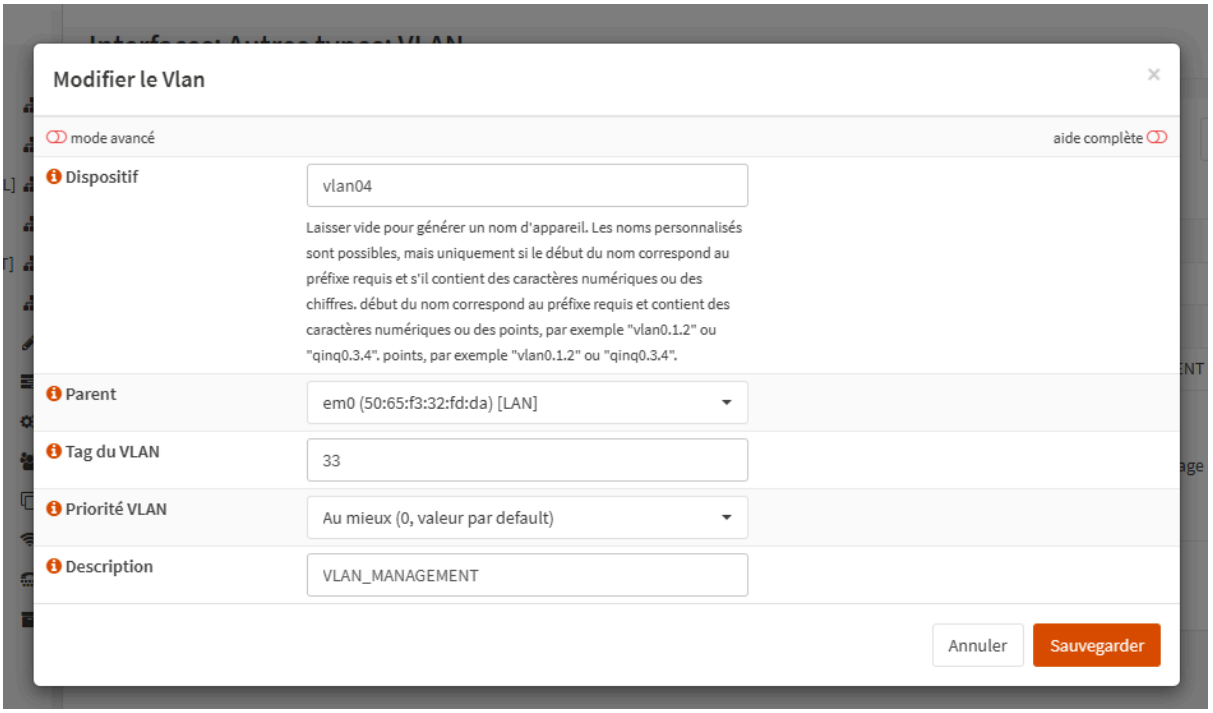


VLAN 32 (Visiteurs)

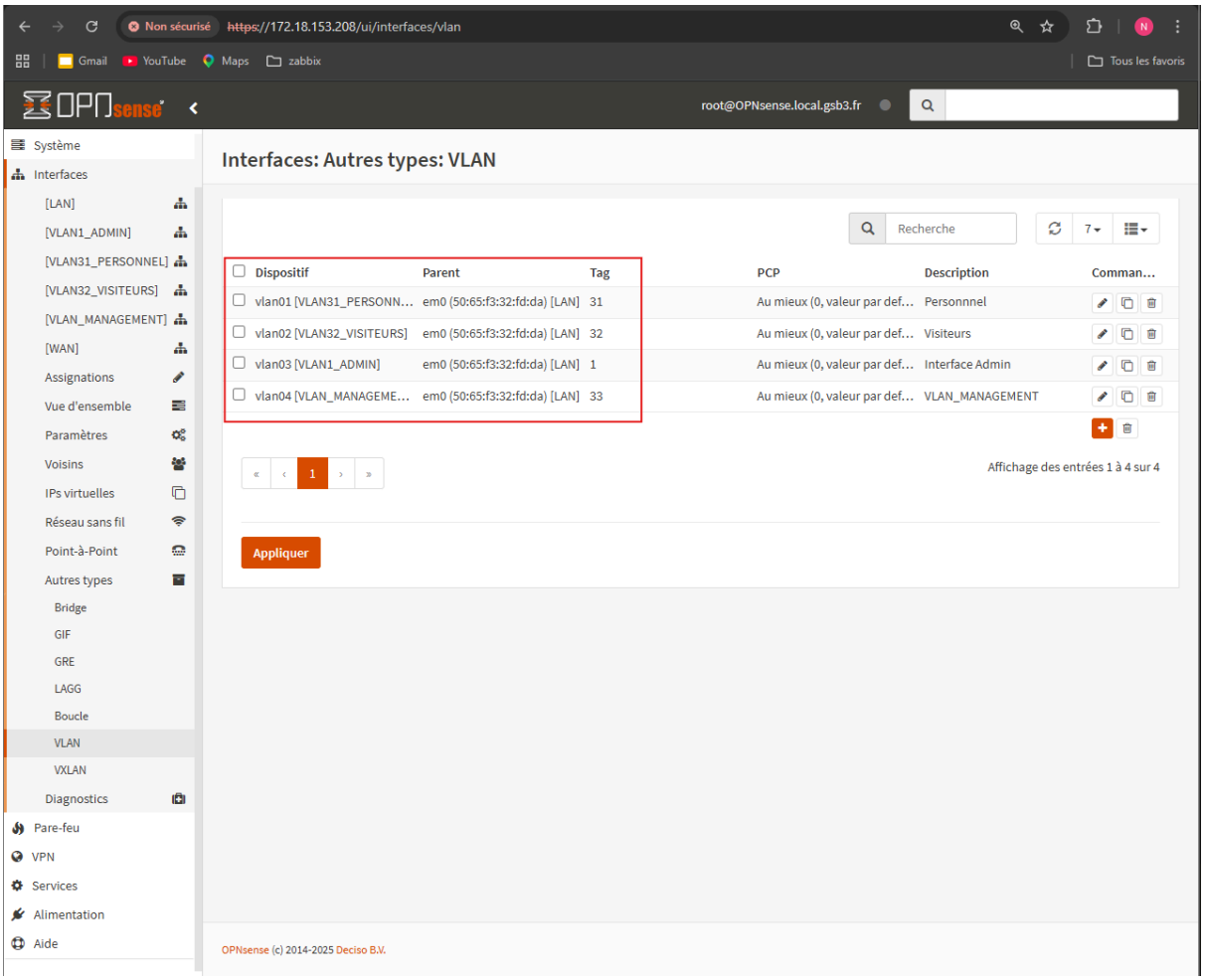
Paramètre	**Valeur**
Interface parent	em0
Tag VLAN	32
Priorité VLAN	0
Description	Visiteurs

VLAN 33 (Management)

Paramètre	**Valeur**
Interface parent	em0
Tag VLAN	33
Priorité VLAN	0
Description	VLAN_MANAGEMENT



Une fois les 4 VLAN créés, ils apparaissent dans la liste avec les noms de dispositifs vlan01, vlan02, vlan03, vlan04 (numérotation automatique d'OPNsense).



2.3 Assignation des VLAN aux interfaces

Une fois les VLAN créés, il faut les assigner comme interfaces logiques pour pouvoir les configurer (IP, DHCP, règles de pare-feu, etc.).

Aller dans Interfaces > Assignations.

Pour chaque VLAN, dans la liste déroulante en bas de la page, sélectionner le VLAN puis cliquer sur **+ Ajouter** :

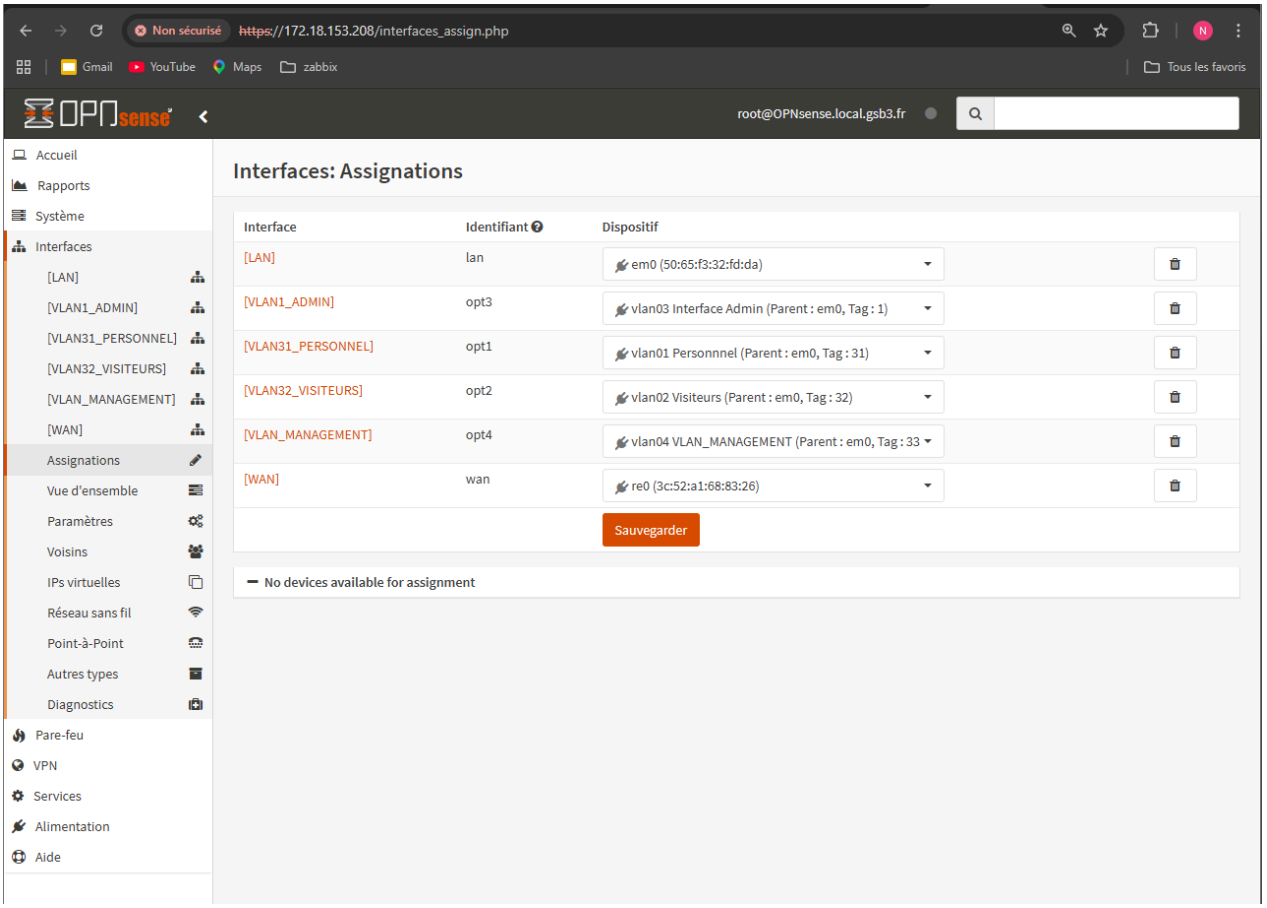
Pour chaque VLAN, dans la liste déroulante en bas de la page, sélectionner le VLAN puis cliquer sur + Ajouter :

- Sélectionner vlan03 (VLAN 1, parent: em0) → Ajouter
- Sélectionner vlan01 (VLAN 31, parent: em0) → Ajouter
- Sélectionner vlan02 (VLAN 32, parent: em0) → Ajouter
- Sélectionner vlan04 (VLAN 33, parent: em0) → Ajouter

Une fois ajoutés, les VLAN apparaissent comme interfaces avec des noms par défaut (OPT1, OPT2, OPT3, OPT4).

Renommer chaque interface pour qu'elle soit identifiable :

Identifiant	**Nom à attribuer**
OPT3 (vlan03)	VLAN1_ADMIN
OPT1 (vlan01)	VLAN31_PERSONNEL
OPT2 (vlan02)	VLAN32_VISITEURS
OPT4 (vlan04)	VLAN_MANAGEMENT



Cliquer sur Sauvegarder après chaque modification.

2.4 Configuration IP de chaque interface VLAN

Pour chaque interface VLAN, il faut activer l'interface et lui attribuer une adresse IP qui servira de passerelle par défaut pour les équipements de ce VLAN.

Procédure générique :

Aller dans Interfaces > [VLAN1_ADMIN] (ou autre VLAN selon le cas).

Cocher "Activer l'interface".

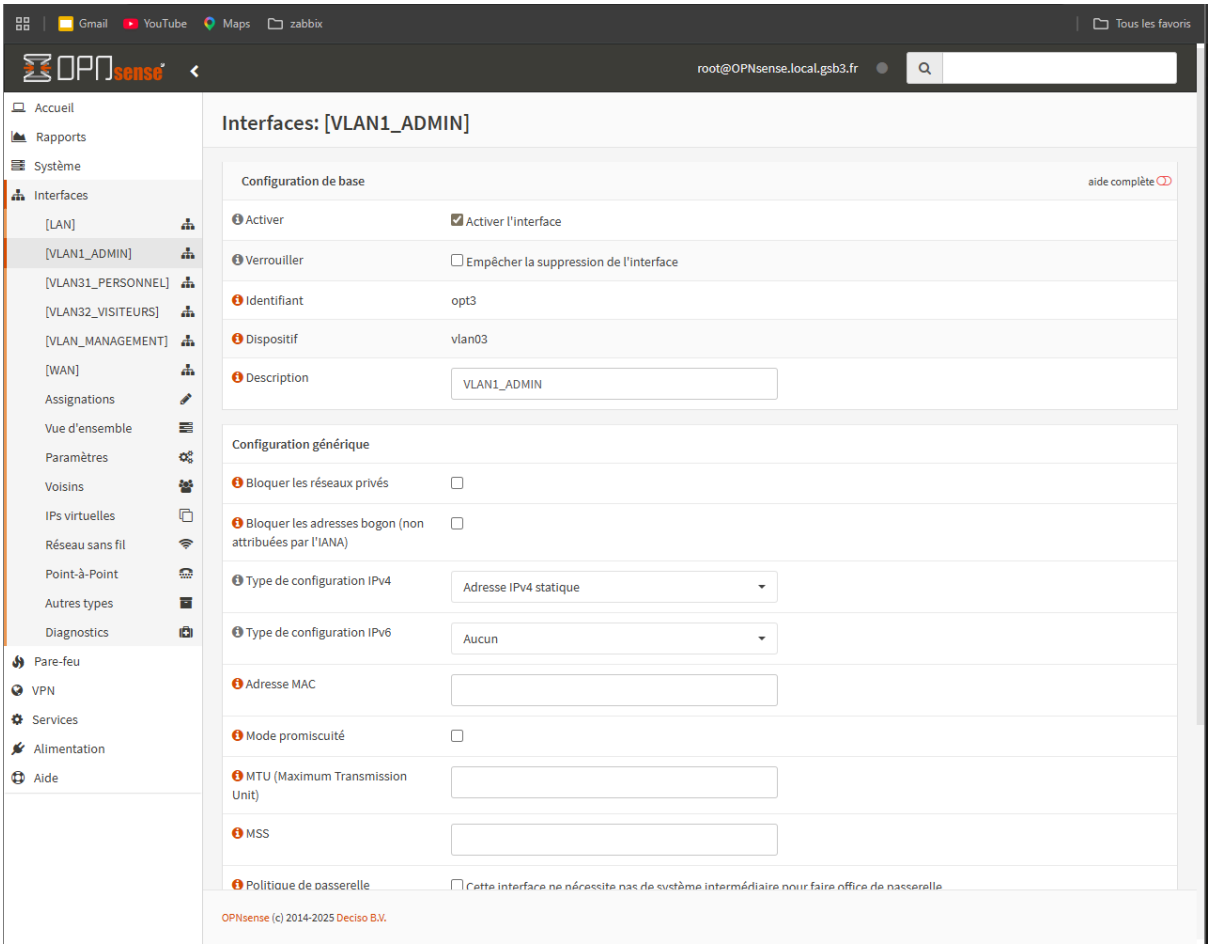
Dans Type de configuration IPv4, sélectionner "Adresse IPv4 statique".

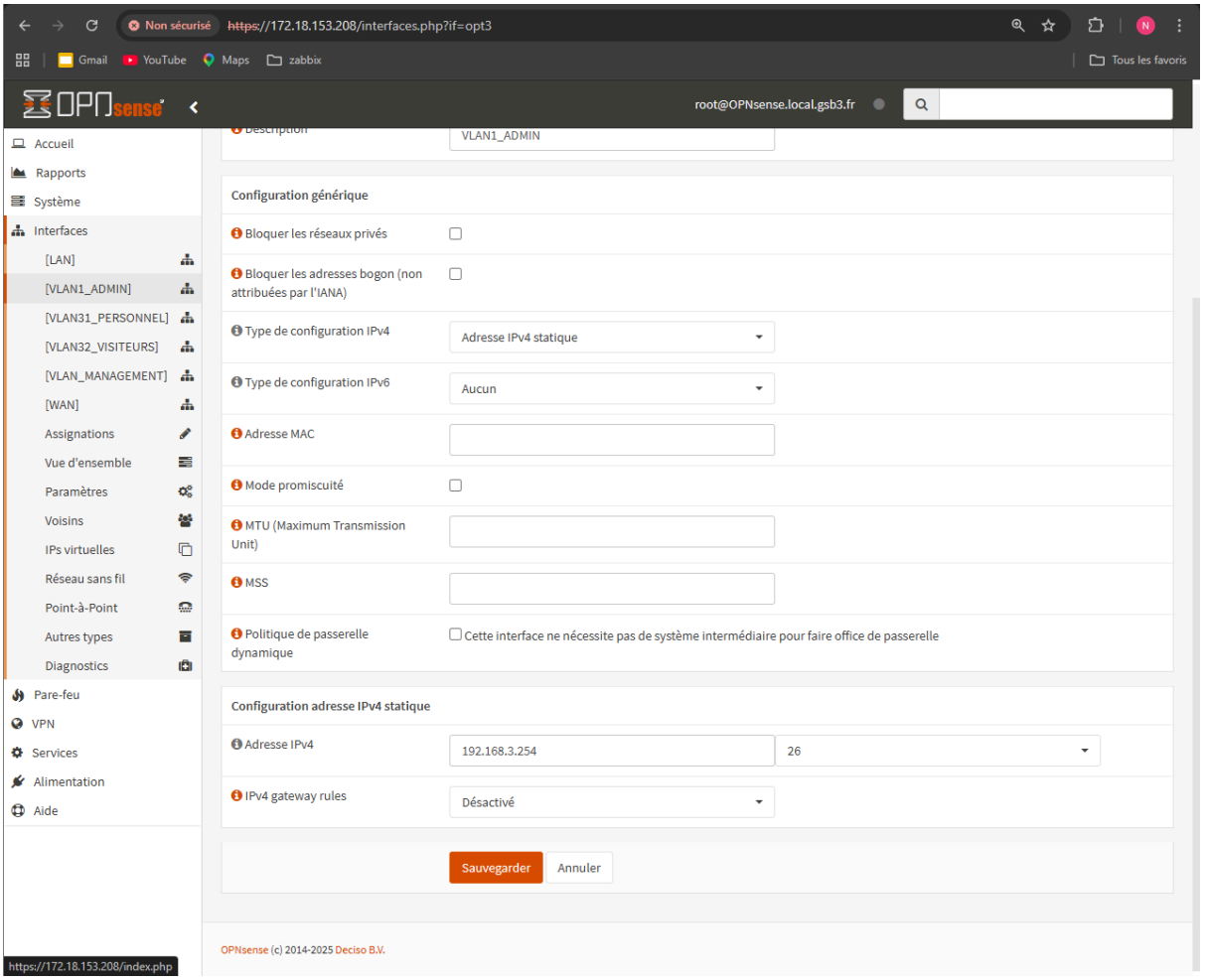
Dans Type de configuration IPv6, sélectionner "Aucun" (l'IPv6 n'est pas utilisé dans cette infrastructure).

Descendre jusqu'à la section Configuration adresse IPv4 statique et renseigner:

Pour VLAN1_ADMIN :

Adresse IPv4 : 192.168.3.254
Masque : /26
IPv4 gateway rules : Désactivé

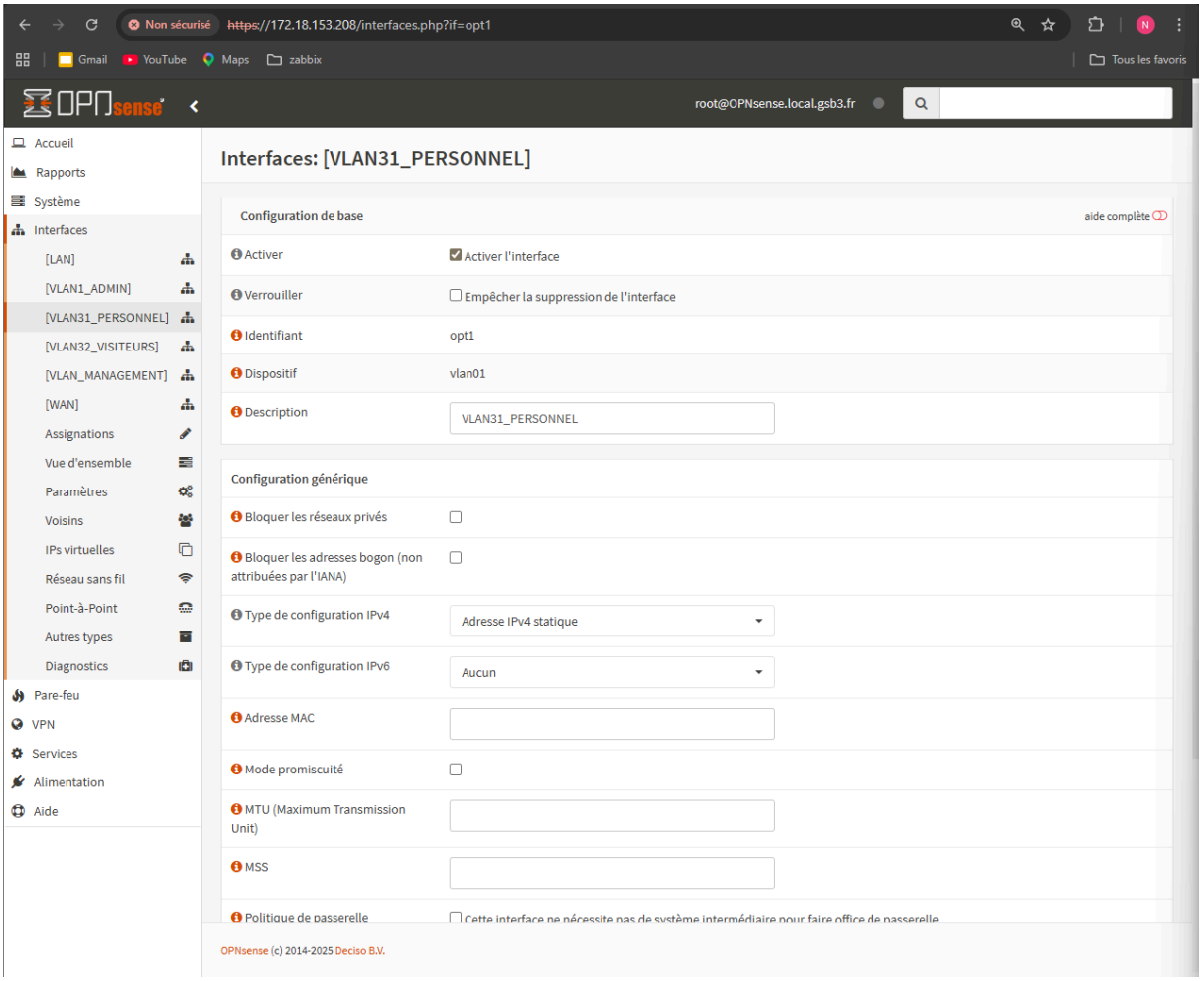


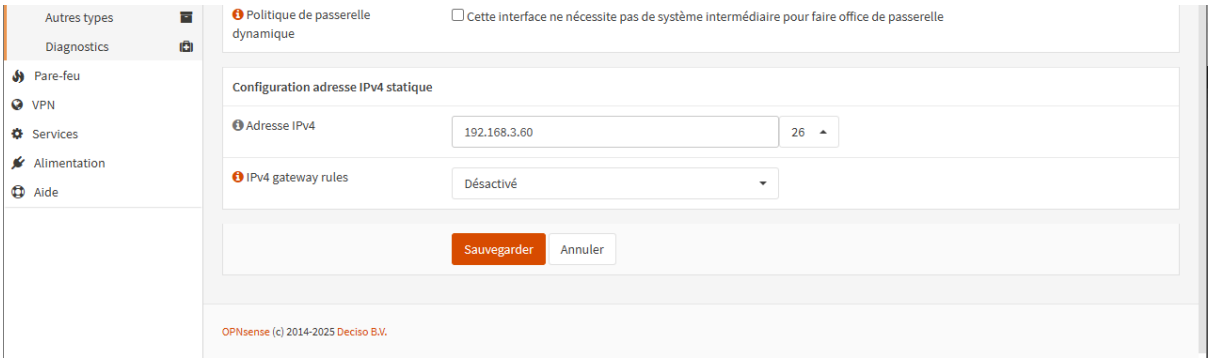


Cliquer sur Sauvegarder puis Appliquer les modifications en haut de la page.

Pour VLAN31_PERSONNEL :

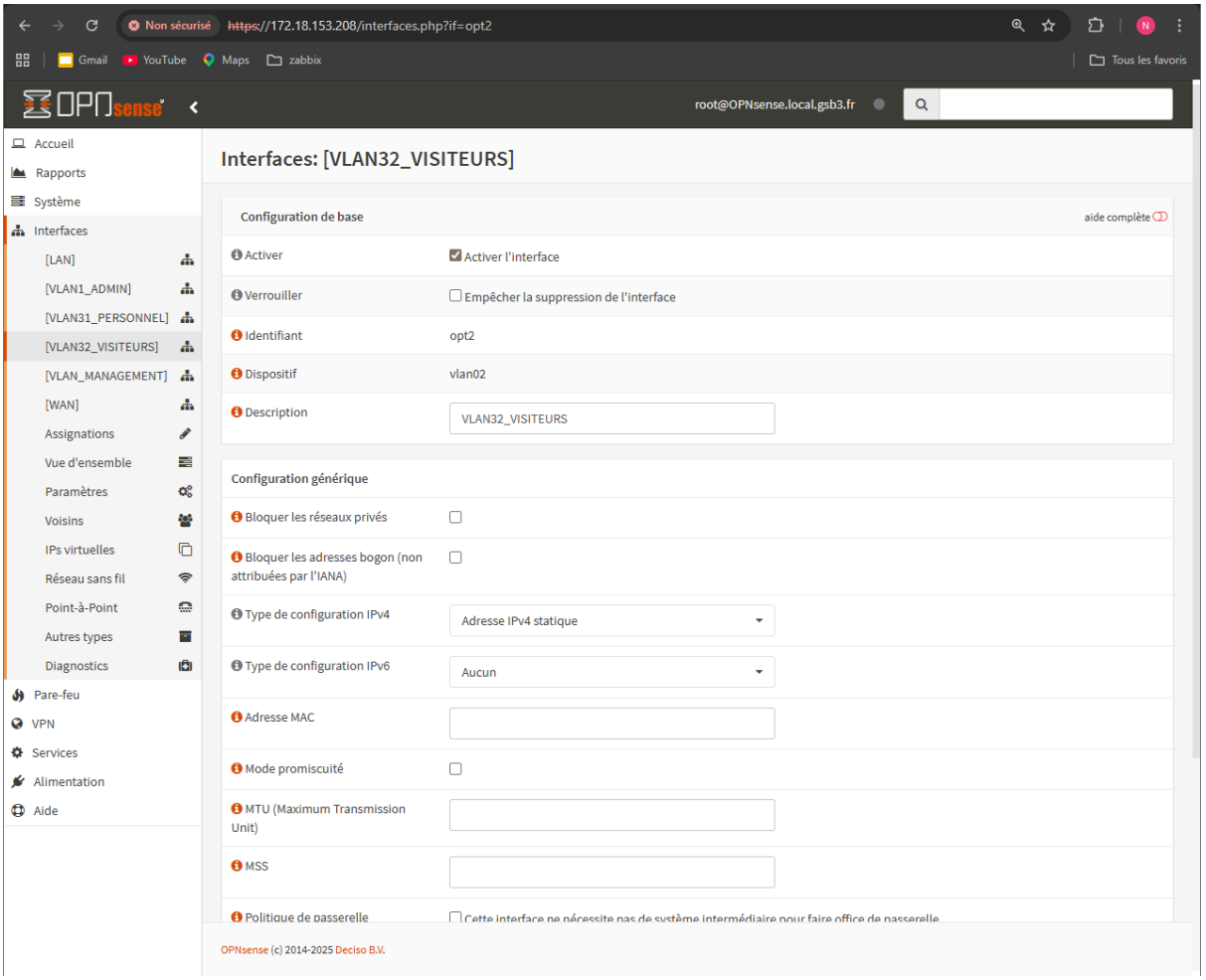
- Adresse IPv4 : 192.168.3.60
- Masque : /26
- IPv4 gateway rules : Désactivé

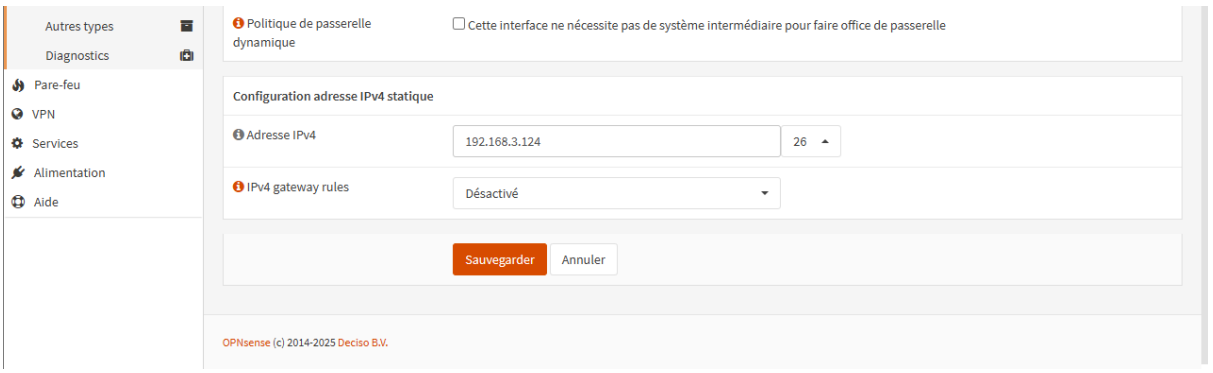




Pour VLAN32_VISITEURS :

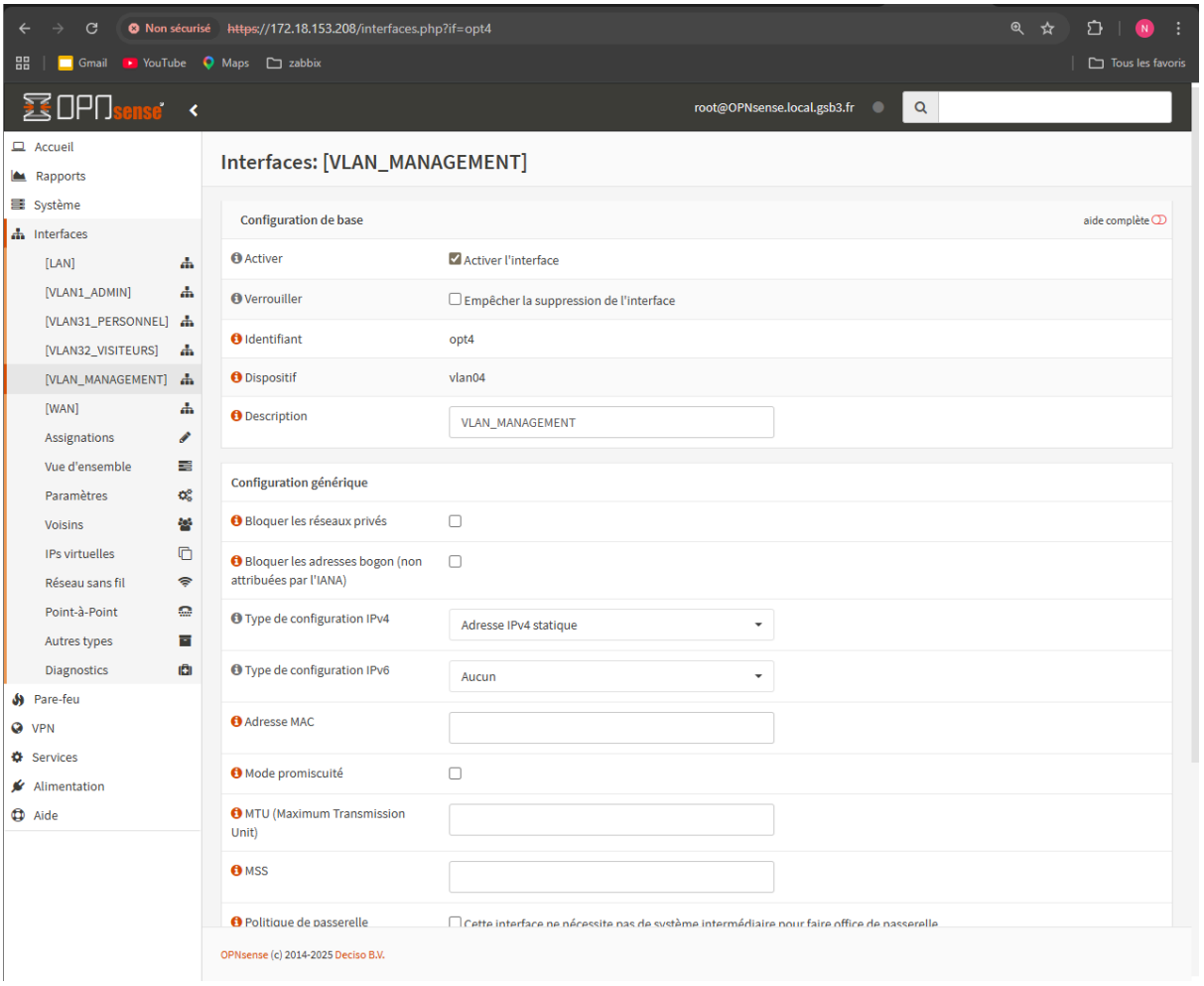
- Adresse IPv4 : 192.168.3.124
- Masque : /26
- IPv4 gateway rules : Désactivé

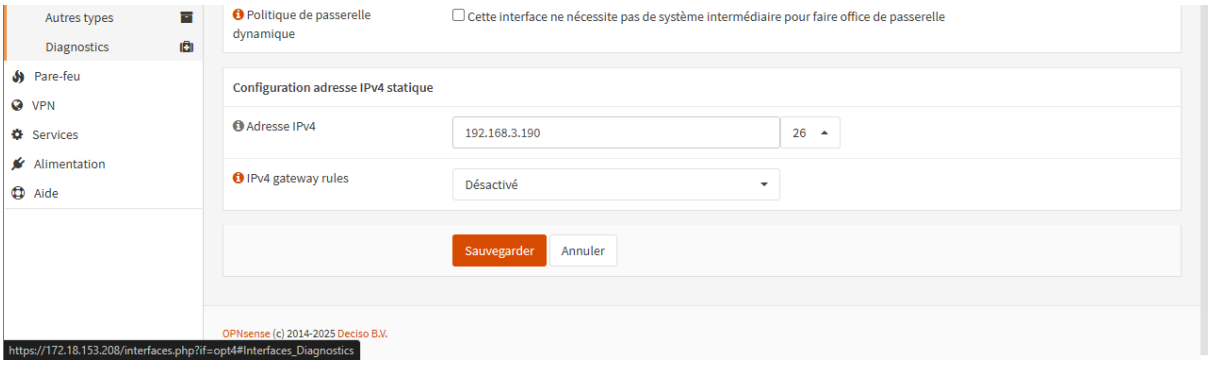




Pour VLAN_MANAGEMENT :

- Adresse IPv4 : 192.168.3.190
- Masque : /26
- IPv4 gateway rules : Désactivé



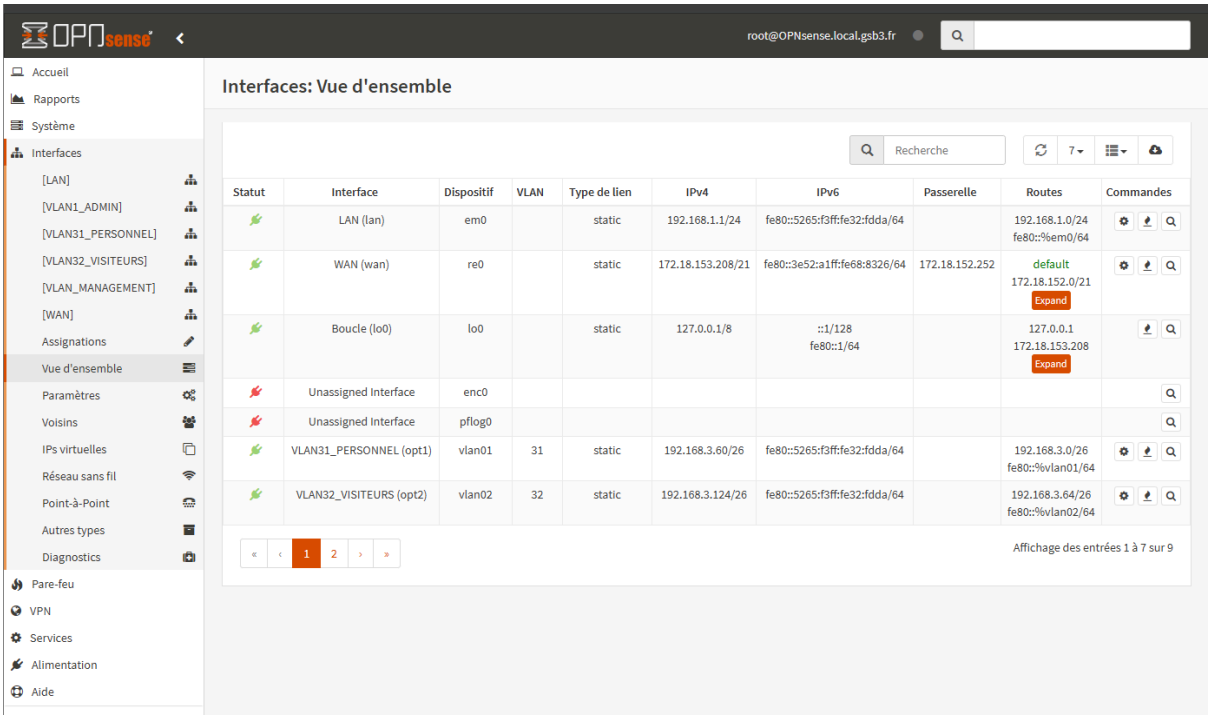


2.5 Vérification de la configuration

Aller dans Interfaces > Vue d'ensemble pour vérifier que toutes les interfaces sont correctement configurées et actives (icône verte).

La vue d'ensemble doit afficher :

Interface	Dispositif	VLAN	IPv4	Statut
LAN	em0	-	(non utilisé directement)	Actif
WAN	re0	-	`172.18.153.208/21`	Actif
VLAN1_ADMIN	vlan03	1	`192.168.3.254/26`	Actif
VLAN31_PERSONNEL	vlan01	31	`192.168.3.0/26` (IF: 192.168.3.60)	Actif
VLAN32_VISITEURS	vlan02	32	`192.168.3.64/26` (IF: 192.168.3.124)	Actif
VLAN_MANAGEMENT	vlan04	33	`192.168.3.128/26` (IF: 192.168.3.190)	Actif



Partie 3 — Services réseau

3.1 Configuration DHCP par VLAN

Le serveur DHCP intégré à OPNsense permet de distribuer automatiquement des adresses IP aux équipements connectés sur chaque VLAN. Cette automatisation est indispensable pour les Wi-Fi clients (VLAN 31 et VLAN 32) qui accueillent un grand nombre d'appareils différents.

L'infrastructure du Pamandzi Hotel utilise une stratégie d'adressage hybride :

VLAN	**Mode d'adressage**	**Justification**
VLAN1_ADMIN	Statique uniquement	VLAN sensible. Les équipements (OPNsense, switches HP31/HP32, PC admin) doivent toujours conserver la même IP pour être joignables et identifiables sans ambiguïté. Aucun DHCP n'est activé.
VLAN31_PERSONNEL	DHCP	VLAN Wi-Fi destiné au personnel et aux clients HallInclusive. Le nombre de clients est variable et imprévisible, le DHCP est donc indispensable.
VLAN32_VISITEURS	DHCP	VLAN Wi-Fi pour les visiteurs classiques. Même logique que VLAN31.
VLAN_MANAGEMENT	Statique uniquement	Un seul équipement présent (le WAP3 en 192.168.3.130). Pas besoin de DHCP.

Plan d'adressage statique (VLAN1_ADMIN et VLAN_MANAGEMENT) :

Équipement	**IP**	**VLAN**
OPNsense (interface VLAN1_ADMIN)	192.168.3.254	VLAN 1
Switch HP31	192.168.3.251	VLAN 1
Switch HP32	192.168.3.252	VLAN 1
PC administrateur	192.168.3.200	VLAN 1
OPNsense (interface VLAN_MANAGEMENT)	192.168.3.190	VLAN 33
WAP3 (Cisco WAP121)	192.168.3.130	VLAN 33

Plages DHCP retenues (VLAN31 et VLAN32) :

VLAN	**Plage DHCP**	**Passerelle**	**DNS distribué**
VLAN31_PERSONNEL	192.168.3.1 – 192.168.3.59	192.168.3.60	172.18.159.250
VLAN32_VISITEURS	192.168.3.65 – 192.168.3.123	192.168.3.124	172.18.159.250

Note sur le serveur **DNS distribué** : le DNS 172.18.159.250 correspond au serveur DNS du réseau SIO du lycée. Ce choix permet aux clients connectés en Wi-Fi de bénéficier directement d'une résolution DNS fonctionnelle sans dépendance à un service DNS local. La résolution Internet est ainsi assurée pour les clients du Pamandzi Hotel via cette infrastructure existante.

3.2 Configuration du DHCP sur OPNsense

OPNsense intègre deux moteurs DHCP :

- ISC DHCPv4 : moteur historique, stable, présent dans toutes les versions d'OPNsense
- Kea DHCP : moteur plus récent, utilisé en remplacement progressif d'ISC

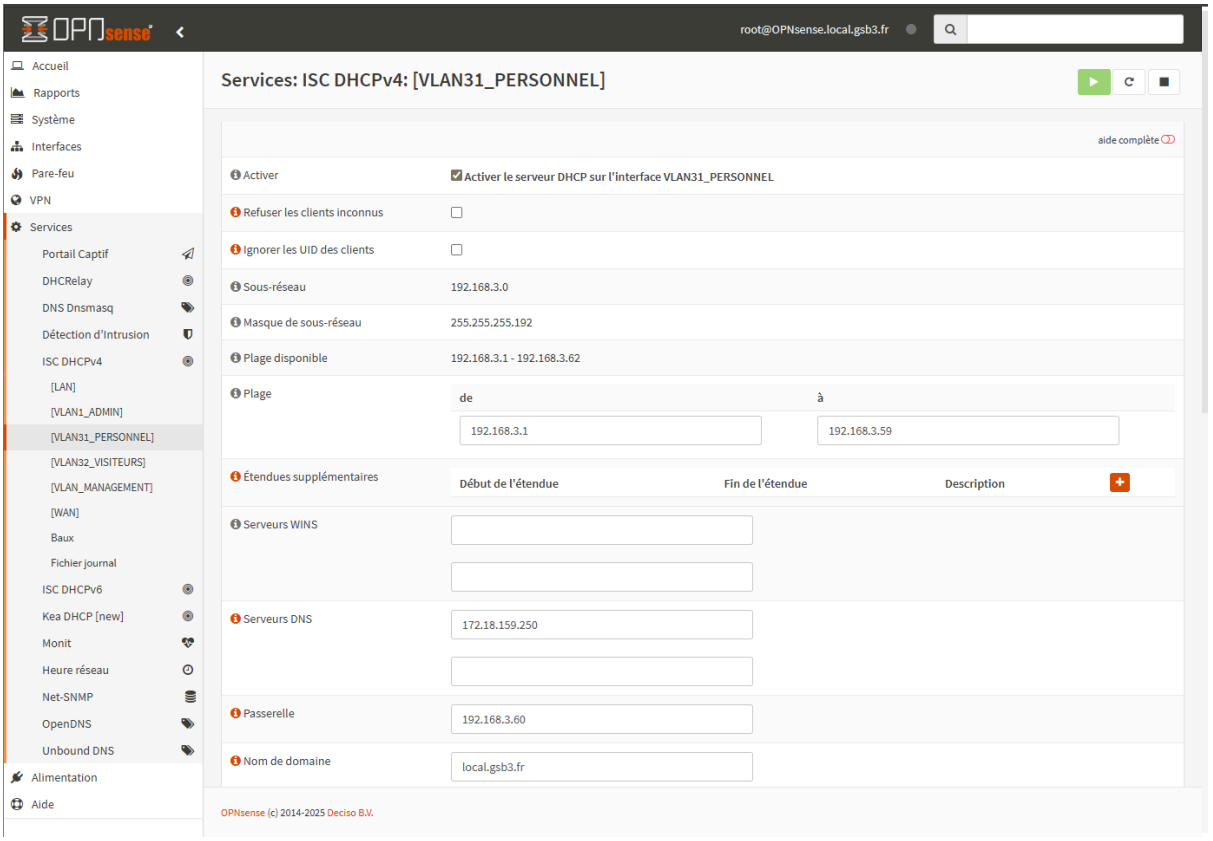
Dans le cadre de cette infrastructure, le service utilisé est ISC DHCPv4 pour sa stabilité éprouvée et sa configuration simplifiée.

Procédure de configuration (à répéter pour chaque VLAN) :

Aller dans Services > ISC DHCPv4 > [VLAN31_PERSONNEL].

Configuration pour VLAN31_PERSONNEL :

Paramètre	Valeur	Explication
Activer	Cocher "Activer le serveur DHCP sur l'interface VLAN31_PERSONNEL"	Active le service DHCP pour ce VLAN
Refuser les clients inconnus	Décoché	Permet à tout client du VLAN d'obtenir une IP
Sous-réseau	192.168.3.0 (auto-rempli)	Découle du masque /26 de l'interface VLAN
Masque sous-réseau	255.255.255.192 (auto-rempli)	Équivalent /26
Plage disponible	192.168.3.1 - 192.168.3.62 (auto-rempli)	IPs réellement utilisables sur le sous-réseau
Plage (de / à)	192.168.3.1 à 192.168.3.59	Plage distribuable par le DHCP
Serveurs DNS	172.18.159.250	DNS du réseau SIO
Passerelle	192.168.3.60	Interface OPNsense sur ce VLAN
Nom de domaine	local.gsb3.fr	Nom de domaine de l'infrastructure

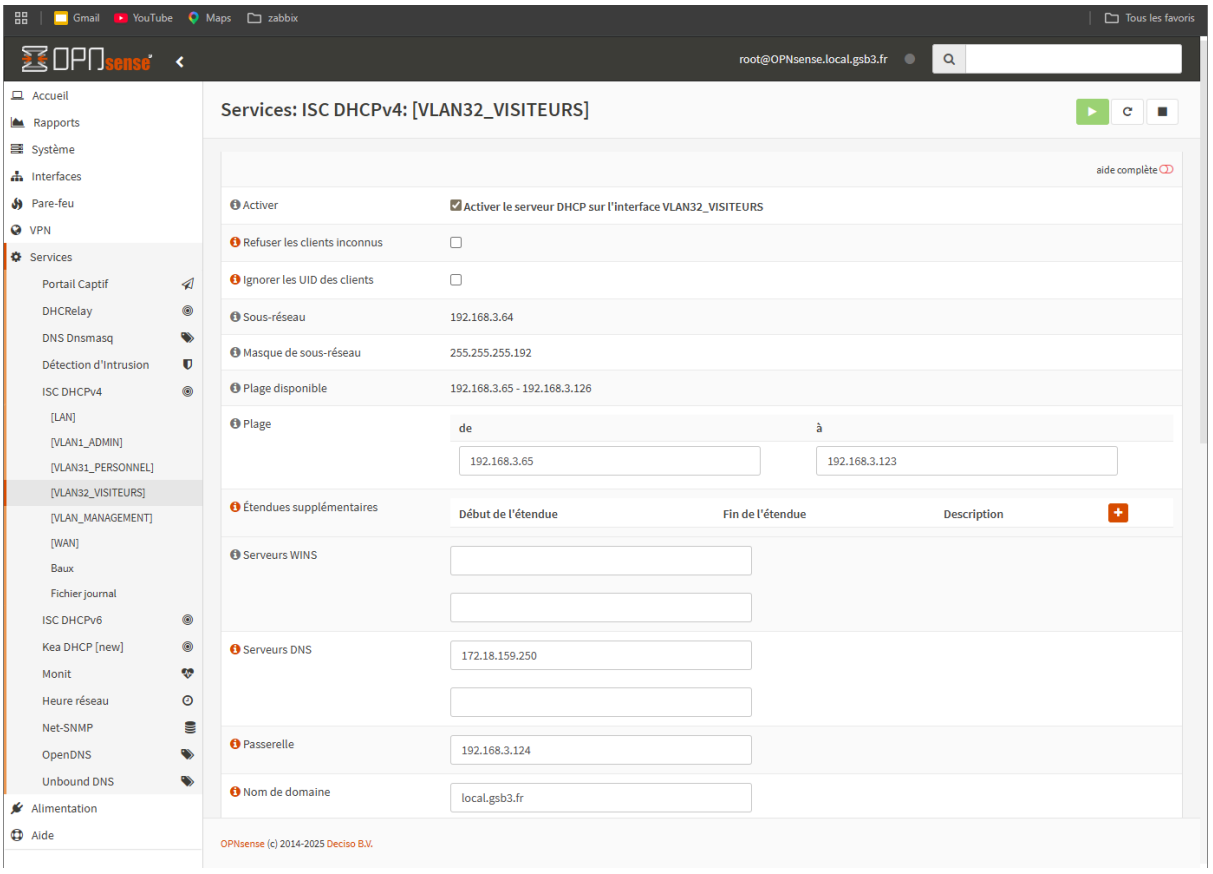


Cliquer sur Sauvegarder en bas de page.

Configuration pour VLAN32_VISITEURS :

Aller dans Services > ISC DHCPv4 > [VLAN32_VISITEURS] et appliquer la même procédure avec les valeurs suivantes :

Paramètre	Valeur
Activer	Cocher
Plage (de / à)	192.168.3.65 à 192.168.3.123
Serveurs DNS	172.18.159.250
Passerelle	192.168.3.124
Nom de domaine	local.gsb3.fr

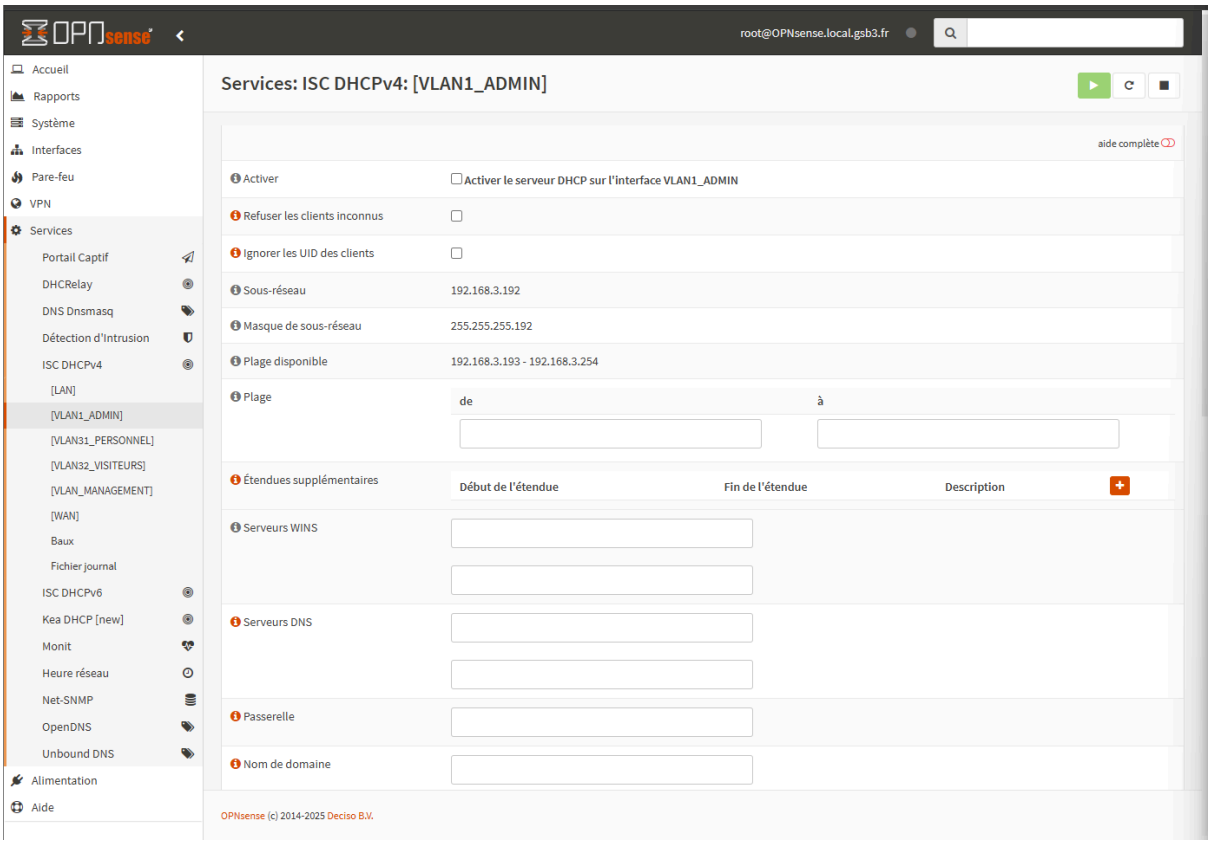


Cliquer sur Sauvegarder en bas de page.

Cas du VLAN1_ADMIN et VLAN_MANAGEMENT :

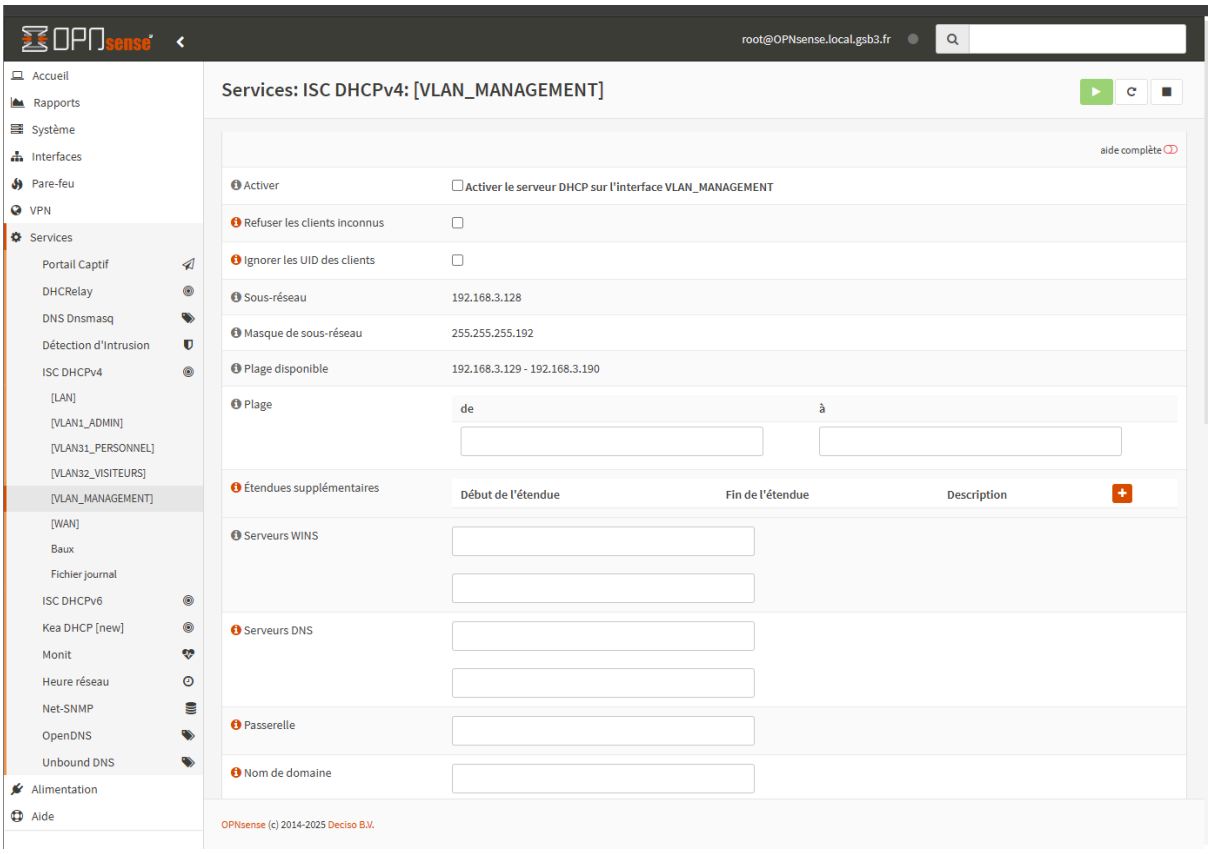
Pour ces deux VLAN, le DHCP reste désactivé (case "Activer le serveur DHCP" non cochée). Aucune configuration supplémentaire n'est nécessaire : les équipements sont configurés en IP statique manuellement.

VLAN1_ADMIN



Cliquer sur Sauvegarder en bas de page.

VLAN_MANAGEMENT



Cliquer sur Sauvegarder en bas de page.

3.3 Vérification du fonctionnement DHCP

Test côté client :

Connecter un terminal mobile (smartphone, tablette) ou un ordinateur portable au Wi-Fi (SSID destiné au VLAN 31 ou VLAN 32). Le client doit recevoir automatiquement :

- Une adresse IP dans la plage du VLAN
- Le masque correspondant (255.255.255.192)
- La passerelle (interface OPNsense du VLAN)
- Le DNS (172.18.159.250)

Sur Windows, vérifier avec une invite de commande :
ipconfig /all

Sur macOS/Linux :
ip a

Vérification côté OPNsense (liste des baux DHCP en cours) :
Aller dans Services > ISC DHCPv4 > Baux.

Cette page affiche tous les clients qui ont obtenu une adresse IP via DHCP, avec :

- Adresse IP attribuée
- Adresse MAC du client
- Nom d'hôte (si fourni par le client)
- Date de fin du bail
- État (actif / expiré)

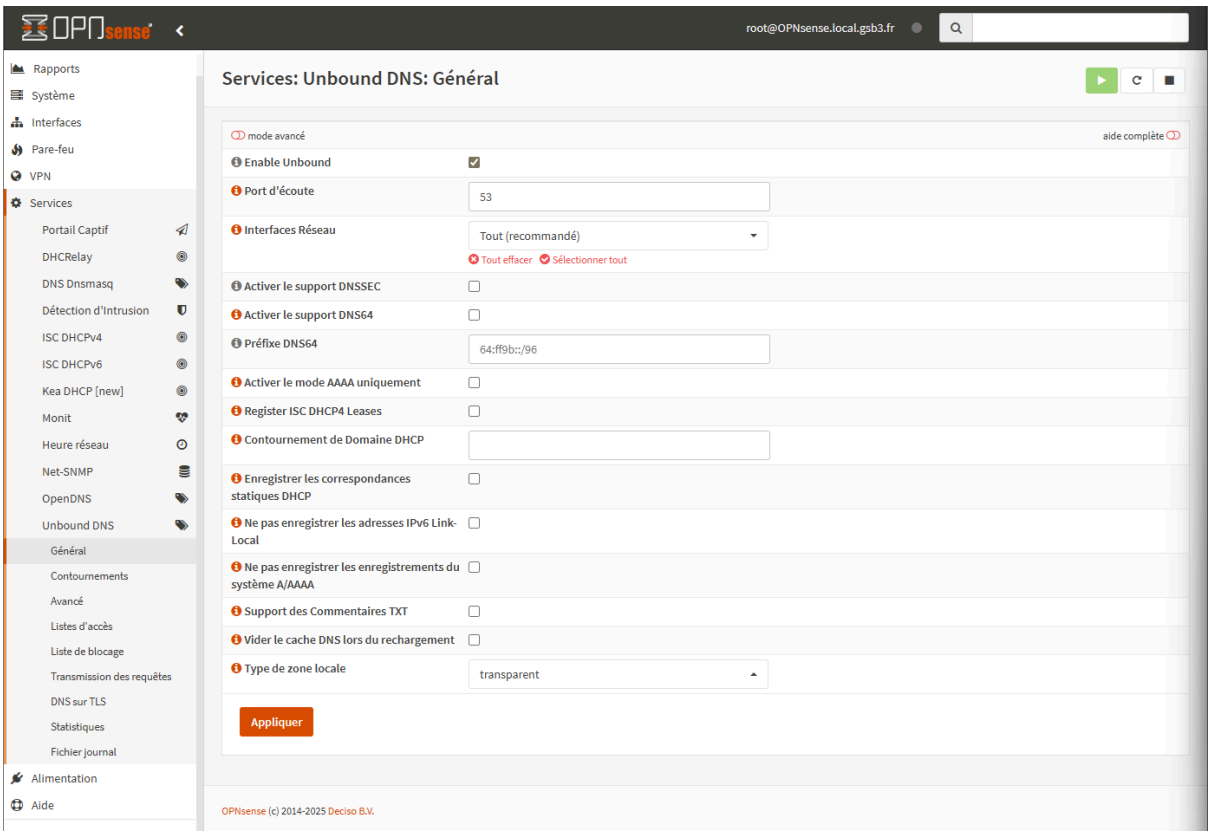
3.4 Configuration DNS Unbound

OPNsense intègre Unbound DNS, un serveur DNS résolveur. Dans cette infrastructure, Unbound est conservé dans sa configuration par défaut : il est utilisé en interne par OPNsense pour ses propres résolutions et pour les services intégrés (portail captif, etc.). Les clients connectés en Wi-Fi reçoivent quant à eux directement le DNS du réseau SIO (172.18.159.250) via le DHCP, sans passer par Unbound.

Aller dans Services > Unbound DNS > Général.

Configuration retenue :

Paramètre	Valeur	Explication
Enable Unbound	Coché	Active le service Unbound
Port d'écoute	53	Port DNS standard
Interfaces Réseau	Tout (recommandé)	Unbound écoute sur toutes les interfaces
Activer le support DNSSEC	Décoché	Non utilisé en lab
Activer le support DNS64	Décoché	Non utilisé (pas d'IPv6)
Activer le mode AAAA uniquement	Décoché	Non utilisé
Register ISC DHCP4 Leases	Décoché	Non utilisé
Enregistrer les correspondances statiques DHCP	Décoché	Non utilisé
Ne pas enregistrer les adresses IPv6 Link-Local	Décoché	-
Ne pas enregistrer les enregistrements du système A/AAAA	Décoché	-
Support des Commentaires TXT	Décoché	-
Vider le cache DNS lors du rechargement	Décoché	-
Type de zone locale	transparent	Mode standard



Cliquer sur Sauvegarder en bas de page.

Note : la configuration d'Unbound est volontairement minimale dans cette infrastructure car les clients utilisent directement le DNS du réseau SIO (172.18.159.250) distribué par DHCP. Unbound reste actif pour le bon fonctionnement interne d'OPNsense.

3.5 Configuration NAT (sortie Internet) (à remplacer dans la doc)

Pour que les équipements internes (VLAN 31 et VLAN 32) puissent accéder à Internet via le réseau SIO, OPNsense doit faire de la traduction d'adresses (NAT) : remplacer leur IP source privée (192.168.3.x) par son IP WAN (172.18.153.208).

Modes de NAT disponibles dans OPNsense :

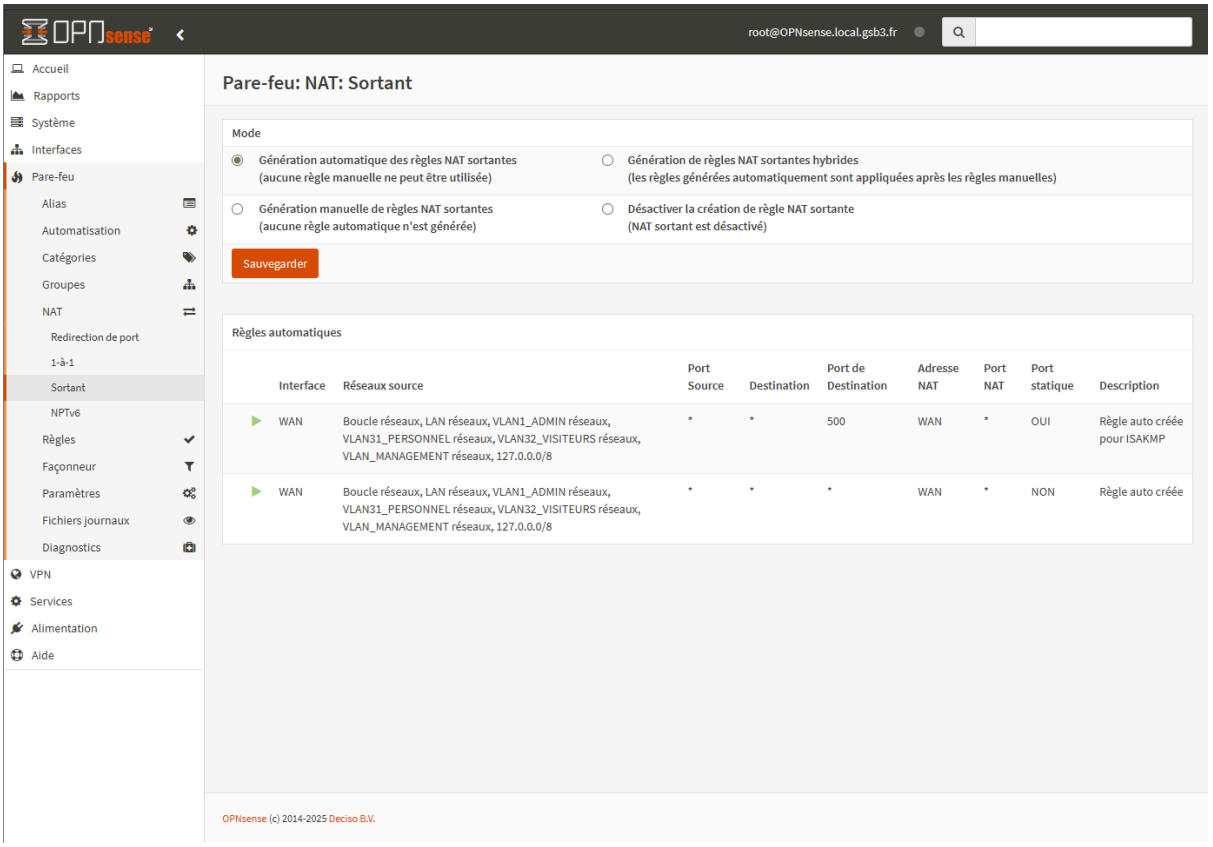
Mode	Description
Génération automatique des règles NAT sortantes	OPNsense crée automatiquement des règles NAT pour tous les sous-réseaux internes connectés à ses interfaces. Recommandé pour une configuration simple.
Génération de règles NAT sortantes hybrides	Les règles automatiques sont appliquées après les règles manuelles éventuelles.
Génération manuelle de règles NAT sortantes	Aucune règle automatique : toutes les règles doivent être définies manuellement.
Désactiver la création de règle NAT sortante	NAT sortant complètement désactivé.

Configuration retenue : Génération automatique

Aller dans Pare-feu > NAT > Sortant.

Sélectionner "Génération automatique des règles NAT sortantes (aucune règle manuelle ne peut être utilisée)" puis cliquer sur Sauvegarder.

OPNsense génère automatiquement deux règles NAT visibles dans la section **Règles automatiques :**



Explication :

- La première règle gère le NAT pour le protocole ISAKMP (port UDP 500), utilisé pour les négociations IPsec/VPN. C'est une règle générée automatiquement par OPNsense par précaution même si aucun VPN n'est configuré.

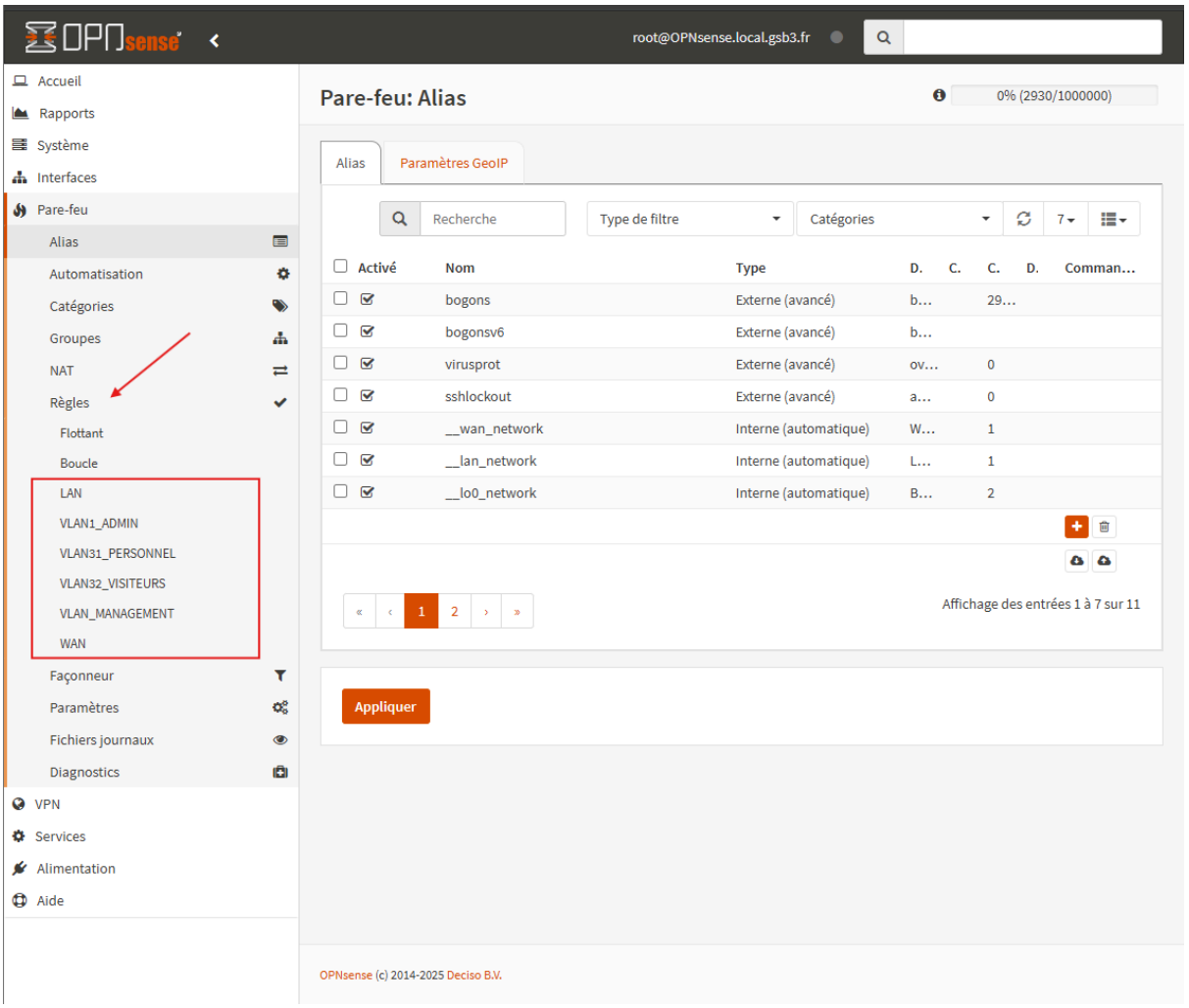
- La deuxième règle gère le NAT pour tout le reste du trafic sortant. Elle s'applique à tous les sous-réseaux internes (VLAN 1, 31, 32, 33, ainsi que LAN et boucle locale) et masque leur IP source avec l'IP WAN d'OPNsense.

Partie 4—Configuration du pare-feu OPNsense

La configuration du pare-feu repose sur deux principes fondamentaux d'OPNsense :

- Politique « deny by default » : tout trafic non explicitement autorisé est bloqué. Aucune règle de blocage générique n'est donc nécessaire.
- Pare-feu à états (stateful) : OPNsense mémorise les connexions initiées depuis l'intérieur dans une table d'états. Les paquets de retour sont automatiquement autorisés sans qu'aucune règle entrante ne soit nécessaire sur le WAN. Cela permet de limiter au strict minimum les règles WAN entrantes.

Les règles sont organisées par interface. L'évaluation se fait dans l'ordre, première correspondance gagne.



4.1 Règles sur l'interface WAN

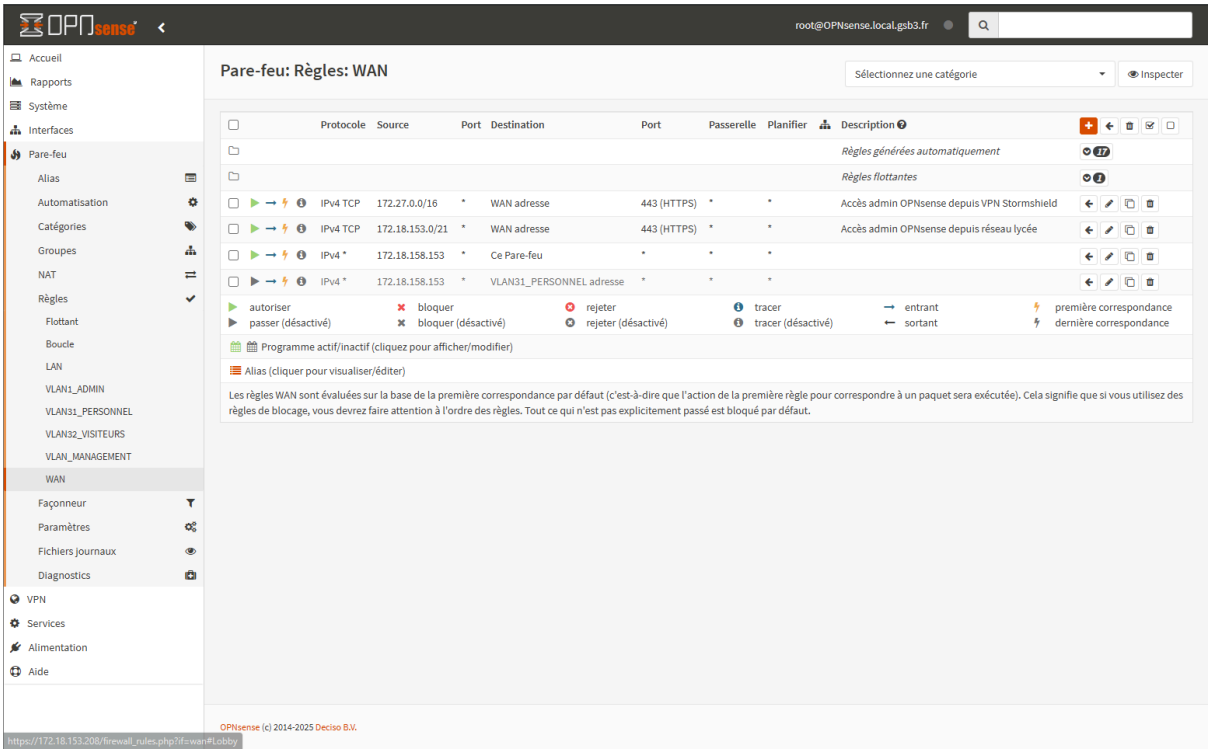
L'interface WAN reçoit le trafic en provenance du réseau SIO du lycée (172.18.152.0/21). Conformément au principe du moindre privilège, seuls les flux entrants strictement nécessaires sont autorisés.

#	Action	Source	Destination	Port	Description
1	Autoriser	172.27.0.0/16 (VPN Stormshield)	WAN adresse	HTTPS (443)	Accès admin OPNsense depuis VPN Stormshield
2	Autoriser	172.18.153.0/21 (réseau SIO)	WAN adresse	HTTPS (443)	Accès admin OPNsense depuis réseau lycée
3	Autoriser	172.18.158.153 (serveur Samba)	Ce Pare-feu	*	Diagnostic réseau réciproque avec serveur Samba camarade

Justification de la configuration :

- La règle 1 autorise l'administration distante via le VPN Stormshield depuis le poste de l'administrateur, en HTTPS uniquement pour garantir le chiffrement des sessions.
- La règle 2 restreint l'accès à l'interface d'administration au seul réseau SIO du lycée, ce qui permet l'administration depuis les postes pédagogiques tout en bloquant tout autre accès.
- La règle 3 autorise le serveur Samba du camarade à dialoguer avec OPNsense pour les besoins de diagnostic réseau (ICMP, tests de connectivité). Cette règle est volontairement maintenue dans le cadre de l'environnement de laboratoire mutualisé.

Note importante sur les flux entrants : aucune autre règle WAN entrante n'est nécessaire pour le fonctionnement des services. Lorsqu'un client interne (VLAN31, VLAN32) initie une connexion vers un serveur du réseau SIO (serveur web, Samba, Zabbix), le retour des paquets est automatiquement autorisé par la table d'états du pare-feu. C'est une application directe du principe du stateful firewall.

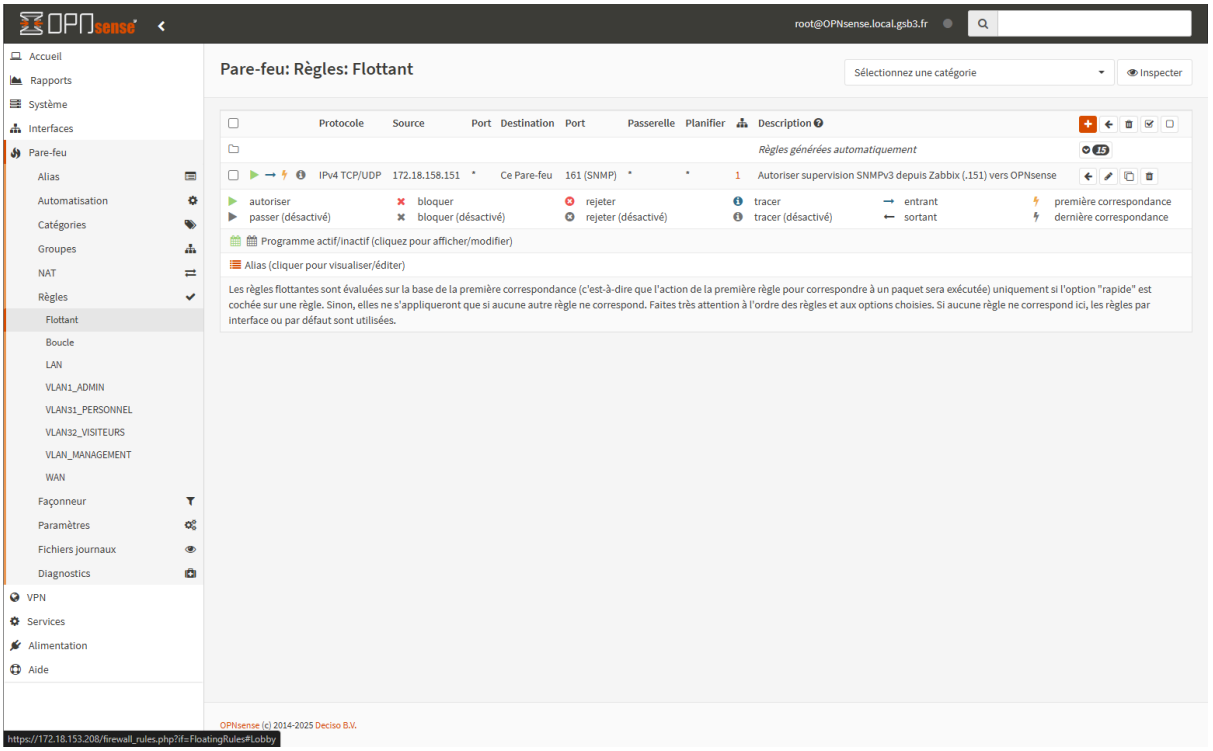

root@OPNsense.local.gsb3.fr
Accueil
Rapports
Système
Interfaces
Pare-feu
Alias
Automatisation
Catégories
Groupes
NAT
Règles
Flottant
Boucle
LAN
VLAN1_ADMIN
VLAN31_PERSONNEL
VLAN32_VISITEURS
VLAN_MANAGEMENT
WAN
Façonneur
Paramètres
Fichiers journaux
Diagnostics
VPN
Services
Alimentation
Aide
Pare-feu: Règles: WAN
Sélectionnez une catégorie
Inspecter
Protocole Source Port Destination Port Passerelle Planifier Description
Règles générées automatiquement
Règles flottantes
IPv4 TCP 172.27.0.0/16 * WAN adresse 443 (HTTPS) * * Accès admin OPNsense depuis VPN Stormshield
IPv4 TCP 172.18.153.0/21 * WAN adresse 443 (HTTPS) * * Accès admin OPNsense depuis réseau lycée
IPv4 * 172.18.158.153 * Ce Pare-feu * * *
IPv4 * 172.18.158.153 * VLAN31_PERSONNEL adresse * * *
autoriser
passer (désactivé)
bloquer
bloquer (désactivé)
rejeter
rejeter (désactivé)
tracer
tracer (désactivé)
entrant
sortant
première correspondance
dernière correspondance
Programme actif/inactif (cliquez pour afficher/modifier)
Alias (cliquer pour visualiser/éditer)
Les règles WAN sont évaluées sur la base de la première correspondance par défaut (c'est-à-dire que l'action de la première règle pour correspondre à un paquet sera exécutée). Cela signifie que si vous utilisez des règles de blocage, vous devrez faire attention à l'ordre des règles. Tout ce qui n'est pas explicitement passé est bloqué par défaut.
OPNsense (c) 2014-2025 Deciso B.V.
https://172.18.153.208/firewall_rules.php?if=wan#Lobby

4.2 Règle flottante : supervision SNMPv3

Une règle flottante a été créée pour autoriser le serveur Zabbix à interroger OPNsense via SNMPv3. Les règles flottantes s'appliquent à toutes les interfaces et sont évaluées avant les règles d'interface, ce qui permet de centraliser des règles transverses.

Action	Source	Destination	Protocole	Port	Description
Autoriser	172.18.158.151 (Zabbix)	Ce Pare-feu	TCP/UDP	SNMP (161)	Autoriser supervision SNMPv3 depuis Zabbix vers OPNsense

Justification : la supervision SNMPv3 est essentielle pour assurer la disponibilité du pare-feu (CPU, mémoire, état des interfaces, sessions actives). L'utilisation de SNMPv3 avec authentification SHA et chiffrement AES garantit la confidentialité et l'intégrité des données de supervision, contrairement à SNMPv1/v2c qui transitent en clair.

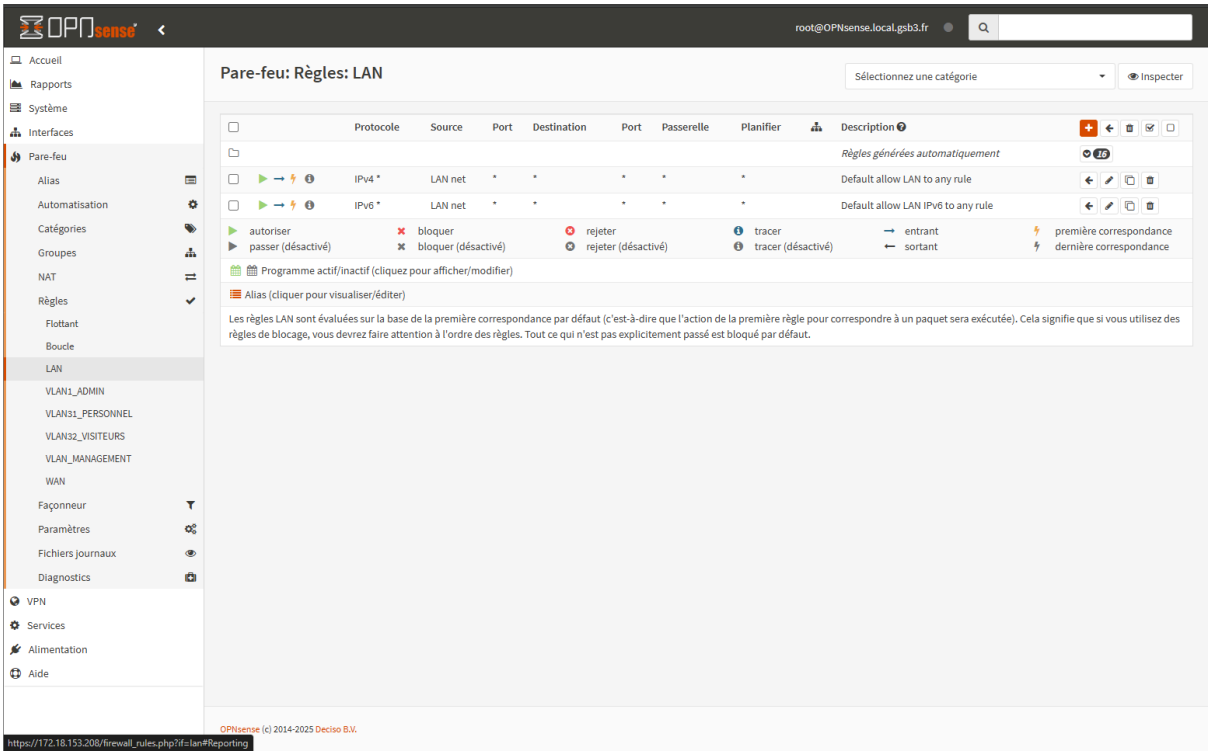


4.3 Règles sur l'interface LAN

L'interface LAN (em0, 192.168.1.1/24) est l'interface physique « neutre » qui sert uniquement de support aux interfaces VLAN taggées. Aucun équipement n'est directement raccordé au LAN natif. Les règles par défaut générées par OPNsense sont conservées en l'état.

Action	Source	Destination	Description
Autoriser	LAN net	*	Default allow LAN to any rule (IPv4)
Autoriser	LAN net	*	Default allow LAN IPv6 to any rule

Justification : ces règles n'ont aucun impact opérationnel puisque aucun client n'est physiquement présent dans le réseau LAN natif (192.168.1.0/24). Elles sont conservées par sécurité au cas où un équipement de maintenance serait branché temporairement.



4.4 Règles sur l'interface VLAN1_ADMIN

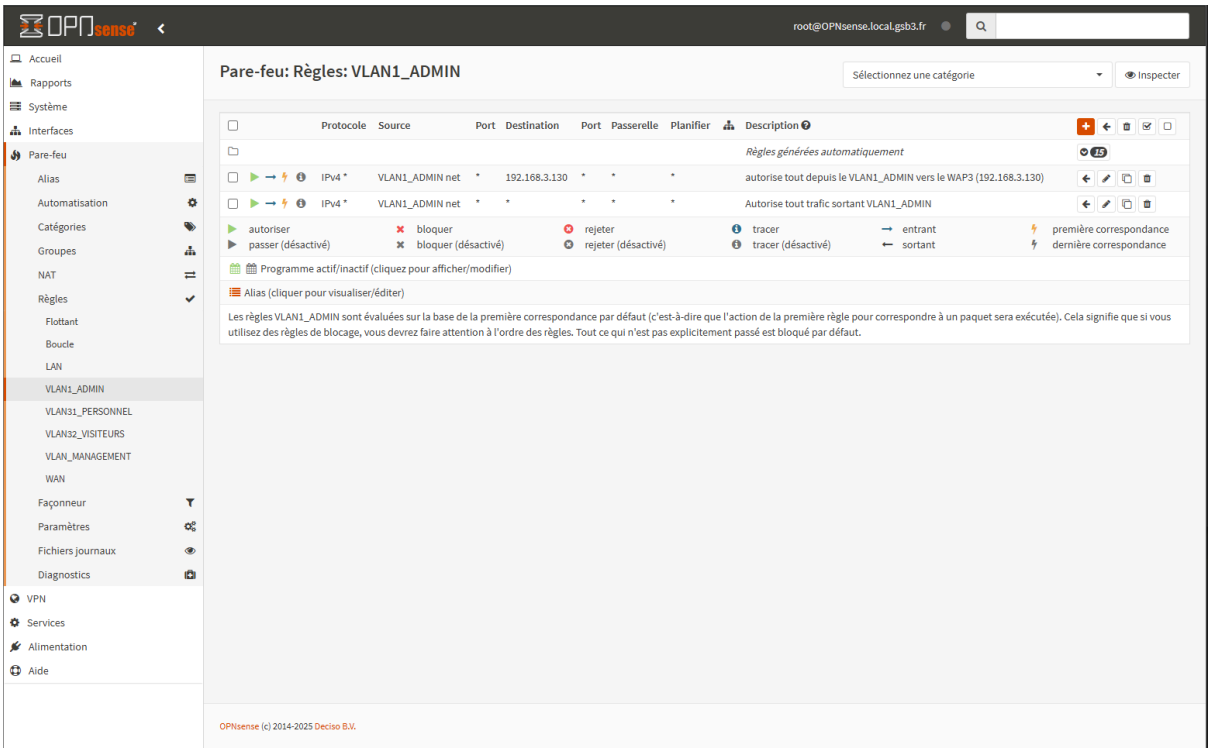
Le VLAN1_ADMIN est dédié à l'administration de l'infrastructure. Il accueille le poste administrateur (192.168.3.200) et a pour rôle d'accéder à l'ensemble des équipements de gestion.

#	Action	Source	Destination	Description
1	Autoriser	VLAN1_ADMIN net	192.168.3.130 (WAP3)	Autorise tout depuis VLAN1_ADMIN vers WAP3
2	Autoriser	VLAN1_ADMIN net	*	Autorise tout trafic sortant VLAN1_ADMIN

Justification :

- La règle 1 autorise explicitement l'administrateur à accéder à l'interface de gestion du WAP3, qui est isolé dans le VLAN_MANAGEMENT (192.168.3.128/26). Sans cette règle, le blocage par défaut empêcherait l'admin de configurer le WAP.
- La règle 2 donne un accès complet à l'administrateur vers toutes les autres destinations (autres VLAN, réseau SIO, Internet) pour permettre les tâches de configuration, supervision et diagnostic.

Ce niveau de privilège est justifié par le rôle d'administration de ce VLAN, et l'accès au VLAN1_ADMIN est lui-même restreint physiquement (port 24 du HP31, IP statique 192.168.3.200).



4.5 Règles sur l'interface VLAN31_PERSONNEL

Le VLAN31 est destiné au personnel de l'hôtel Pamandzi (gamme HallInclusive). Les utilisateurs ont besoin d'accéder aux services métiers (serveur web interne, partage de fichiers Samba) et à Internet, mais ne doivent en aucun cas pouvoir accéder aux interfaces d'administration.

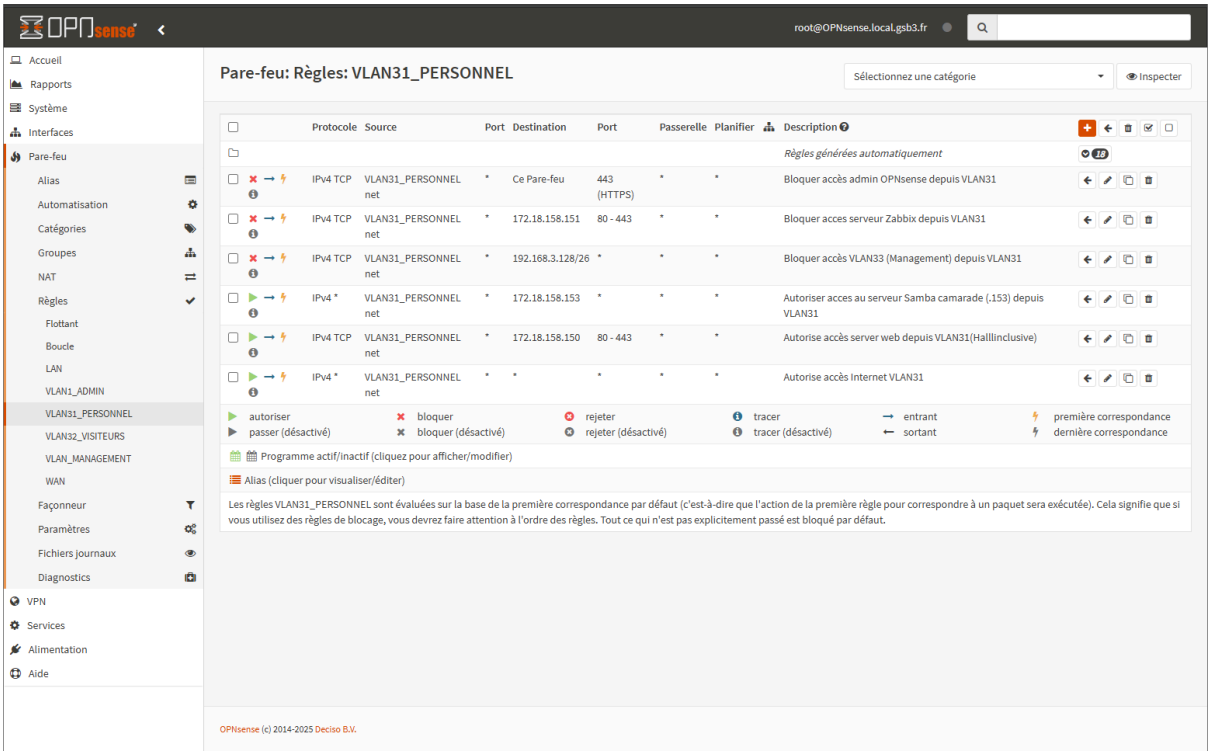
L'ordre des règles est crucial : les règles spécifiques de blocage sont placées en premier, puis les règles spécifiques d'autorisation, et enfin la règle générale d'accès Internet en dernier.

#	Action	Source	Destination	Port	Description
1	Bloquer	VLAN31_PERSONNEL net	Ce Pare-feu	HTTPS (443)	Bloquer accès admin OPNsense depuis VLAN31
2	Bloquer	VLAN31_PERSONNEL net	172.18.158.151 (Zabbix)	80-443	Bloquer accès serveur Zabbix depuis VLAN31
3	Bloquer	VLAN31_PERSONNEL net	192.168.3.128/26 (VLAN33)	*	Bloquer accès VLAN33 (Management) depuis VLAN31
4	Autoriser	VLAN31_PERSONNEL net	172.18.158.153 (Samba)	*	Autoriser accès au serveur Samba camarade (.153) depuis VLAN31
5	Autoriser	VLAN31_PERSONNEL net	172.18.158.150 (Web)	80-443	Autorise accès server web depuis VLAN31 (HallInclusive)
6	Autoriser	VLAN31_PERSONNEL net	*	*	Autorise accès Internet VLAN31

Justification de l'ordre des règles :

1. Règles 1, 2, 3 : blocages explicites pour empêcher le personnel d'atteindre les services d'administration (interface OPNsense, supervision Zabbix) et le VLAN de management du WAP. Le blocage du VLAN33 est essentiel pour empêcher tout accès au plan de gestion (management plane).
2. Règles 4, 5 : autorisations spécifiques vers les services métiers nécessaires.
3. Règle 6 : règle générique d'accès à Internet, placée en dernier pour ne pas masquer les règles spécifiques.

Note pédagogique : si la règle 6 (« autoriser any ») était placée avant les règles 4 et 5, ces dernières seraient mortes — jamais évaluées. L'ordre traduit donc une réflexion explicite sur la politique de sécurité : on autorise précisément ce qui doit l'être, puis on autorise le reste.



4.6 Règles sur l'interface VLAN32_VISITEURS

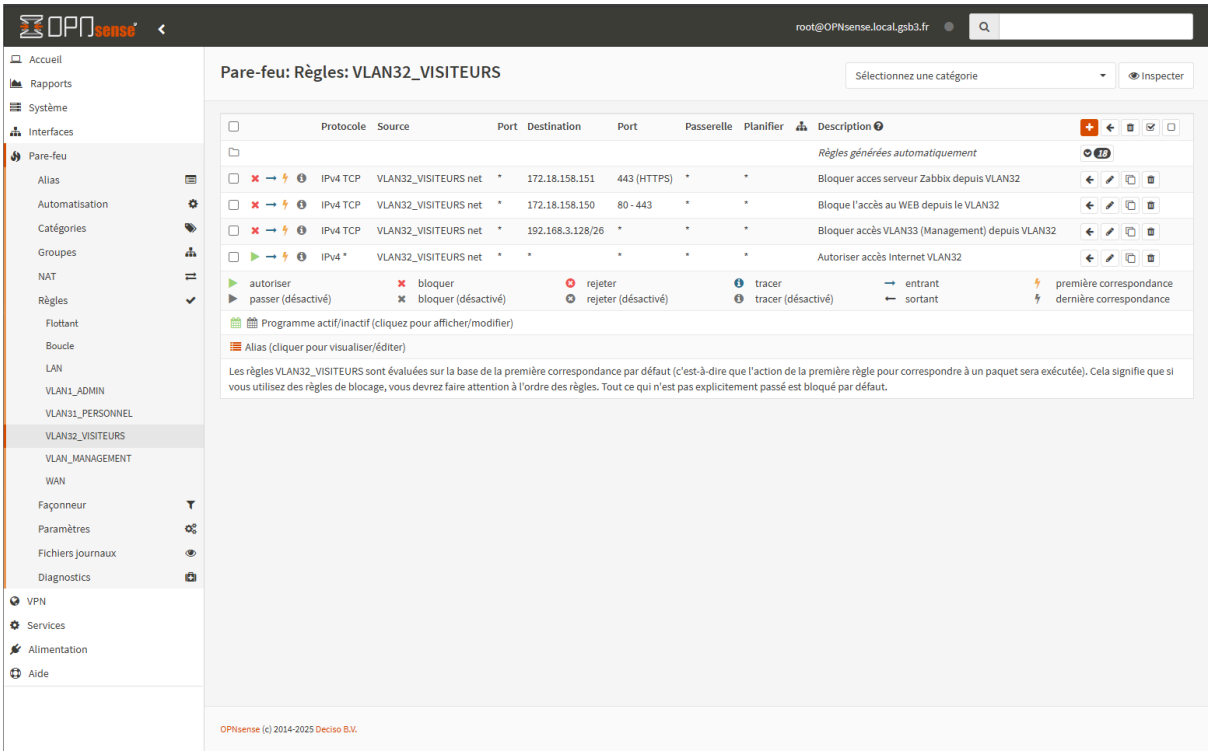
Le VLAN32 est destiné aux clients de l'hôtel et aux visiteurs. La politique de sécurité y est nettement plus restrictive : ils ne doivent accéder ni aux services internes de l'établissement, ni aux interfaces d'administration. Seul l'accès à Internet leur est autorisé.

#	Action	Source	Destination	Port	Description
1	Bloquer	VLAN32_VISITEURS net	172.18.158.151 (Zabbix)	HTTPS (443)	Bloquer accès serveur Zabbix depuis VLAN32
2	Bloquer	VLAN32_VISITEURS net	172.18.158.150 (Web)	80-443	Bloquer l'accès au serveur web depuis VLAN32
3	Bloquer	VLAN32_VISITEURS net	192.168.3.128/26 (VLAN33)	*	Bloquer accès VLAN33 (Management) depuis VLAN32
4	Autoriser	VLAN32_VISITEURS net	*	*	Autoriser accès Internet VLAN32

Justification :

- Les règles 1 et 2 isolent les visiteurs des services internes hébergés sur le réseau SIO : ils n'ont aucune raison légitime d'accéder à la supervision ou au serveur web métier.
- La règle 3 bloque l'accès au VLAN de management, dans la même logique que pour le VLAN31.
- La règle 4 autorise uniquement la sortie vers Internet, ce qui correspond à l'usage attendu d'un visiteur d'hôtel (consultation web, messagerie).

Sécurité supplémentaire : l'accès au VLAN32 est en outre conditionné par l'authentification via le portail captif (vouchers d'accès). Les visiteurs doivent saisir un voucher avant de pouvoir générer du trafic.


root@OPNsense.local.gsb3.fr
Accueil
Rapports
Système
Interfaces
Pare-feu
Alias
Automatisation
Catégories
Groupes
NAT
Règles
Flottant
Boucle
LAN
VLAN1_ADMIN
VLAN31_PERSONNEL
VLAN32_VISITEURS
VLAN_MANAGEMENT
WAN
Façonneur
Paramètres
Fichiers journaux
Diagnostics
VPN
Services
Alimentation
Aide
Pare-feu: Règles: VLAN32_VISITEURS
Sélectionnez une catégorie
Inspecter
Protocole Source Port Destination Port Passerelle Planifier Description
Règles générées automatiquement
IPv4 TCP VLAN32_VISITEURS net * 172.18.158.151 443 (HTTPS) * * Bloquer acces serveur Zabbix depuis VLAN32
IPv4 TCP VLAN32_VISITEURS net * 172.18.158.150 80 - 443 * * Bloque l'accès au WEB depuis le VLAN32
IPv4 TCP VLAN32_VISITEURS net * 192.168.3.128/26 * * * Bloquer accès VLAN33 (Management) depuis VLAN32
IPv4 * VLAN32_VISITEURS net * * * * * Autoriser accès Internet VLAN32
autoriser
passer (désactivé)
bloquer
bloquer (désactivé)
rejeter
rejeter (désactivé)
tracer
tracer (désactivé)
entrant
sortant
première correspondance
dernière correspondance
Programme actif/inactif (cliquez pour afficher/modifier)
Alias (cliquer pour visualiser/éditer)
Les règles VLAN32_VISITEURS sont évaluées sur la base de la première correspondance par défaut (c'est-à-dire que l'action de la première règle pour correspondre à un paquet sera exécutée). Cela signifie que si vous utilisez des règles de blocage, vous devrez faire attention à l'ordre des règles. Tout ce qui n'est pas explicitement passé est bloqué par défaut.
OPNsense (c) 2014-2025 Deciso B.V.

4.7 Règles sur l'interface VLAN_MANAGEMENT (VLAN33)

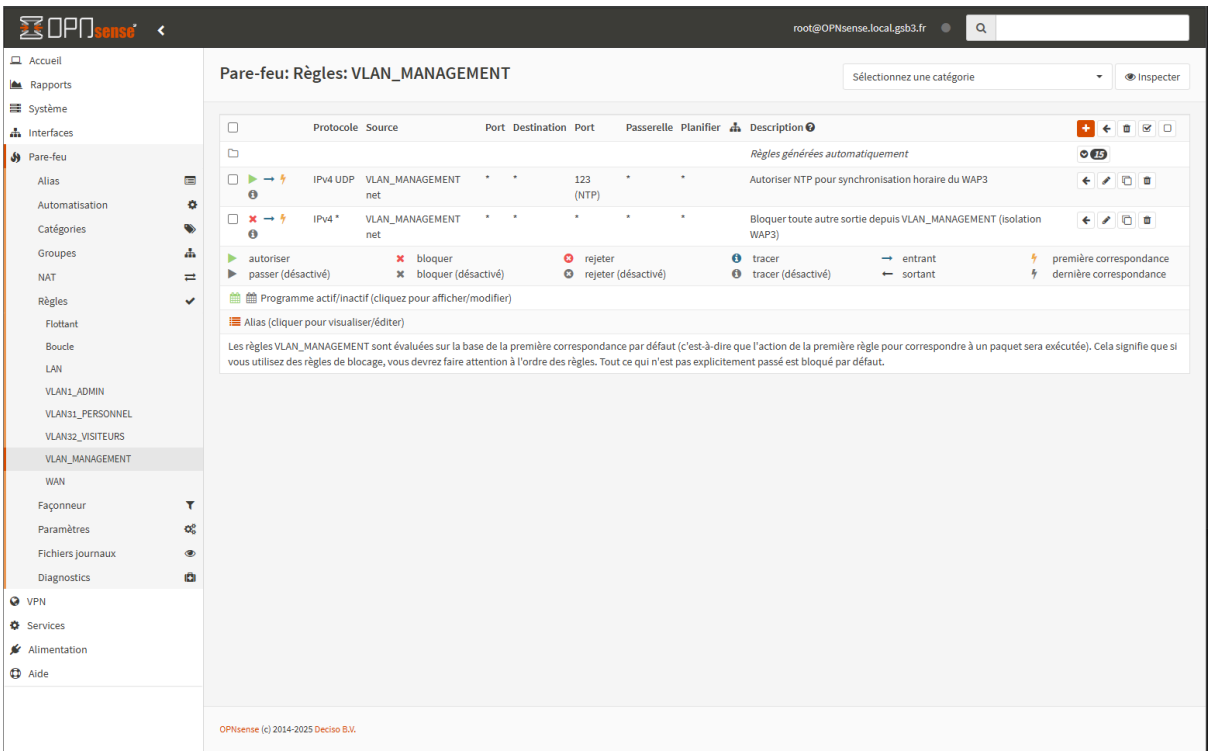
Le VLAN_MANAGEMENT héberge uniquement le WAP3 (192.168.3.130) en tant qu'équipement à administrer. Conformément aux bonnes pratiques de segmentation entre plan de données et plan de gestion, ce VLAN est strictement isolé.

#	Action	Source	Destination	Port	Description
1	Autoriser	VLAN_MANAGEMENT net	*	NTP (123) UDP	Autoriser NTP pour synchronisation horaire du WAP3
2	Bloquer	VLAN_MANAGEMENT net	*	*	Bloquer toute autre sortie depuis VLAN_MANAGEMENT (isolation WAP3)

Justification :

- La règle 1 autorise spécifiquement le protocole NTP pour permettre au WAP3 de maintenir une horloge synchronisée. Une horloge fiable est indispensable pour l'horodatage des journaux et la corrélation d'événements en cas d'incident de sécurité.
- La règle 2 bloque explicitement tout autre trafic sortant. Cette règle de blocage explicite, bien qu'elle fasse doublon avec la politique « deny by default », a une vocation documentaire et défensive : elle traduit dans la configuration la volonté délibérée d'isoler le WAP3 et empêche qu'une règle supplémentaire ajoutée en haut de la liste vienne accidentellement ouvrir le VLAN.

Principe de défense en profondeur : en cas de compromission du WAP3 (vulnérabilité firmware, attaque du protocole 802.11), un attaquant se retrouverait confiné dans le VLAN33, sans possibilité de rebond vers les autres VLAN ou le réseau SIO. Les flux d'administration entrants (PC admin → WAP3) restent possibles grâce à la règle 1 du VLAN1_ADMIN, et leurs paquets de retour passent par la table d'états.


root@OPNsense.local.gsb3.fr
Accueil
Rapports
Système
Interfaces
Pare-feu
Alias
Automatisation
Catégories
Groupes
NAT
Règles
Flottant
Boucle
LAN
VLAN1_ADMIN
VLAN31_PERSONNEL
VLAN32_VISITEURS
VLAN_MANAGEMENT
WAN
Façonneur
Paramètres
Fichiers journaux
Diagnostics
VPN
Services
Alimentation
Aide
Pare-feu: Règles: VLAN_MANAGEMENT
Sélectionnez une catégorie
Inspecter
Protocole Source Port Destination Port Passerelle Planifier Description
Règles générées automatiquement
IPv4 UDP VLAN_MANAGEMENT net * * 123 (NTP) * * Autoriser NTP pour synchronisation horaire du WAP3
IPv4 * VLAN_MANAGEMENT net * * * * * Bloquer toute autre sortie depuis VLAN_MANAGEMENT (isolation WAP3)
autoriser
passer (désactivé)
bloquer
bloquer (désactivé)
rejeter
rejeter (désactivé)
tracer
tracer (désactivé)
entrant
sortant
première correspondance
dernière correspondance
Programme actif/inactif (cliquez pour afficher/modifier)
Alias (cliquer pour visualiser/éditer)
Les règles VLAN_MANAGEMENT sont évaluées sur la base de la première correspondance par défaut (c'est-à-dire que l'action de la première règle pour correspondre à un paquet sera exécutée). Cela signifie que si vous utilisez des règles de blocage, vous devrez faire attention à l'ordre des règles. Tout ce qui n'est pas explicitement passé est bloqué par défaut.
OPNsense (c) 2014-2025 Deciso B.V.

4.8 Synthèse de la matrice de flux

Le tableau ci-dessous synthétise la politique de sécurité appliquée :

Source ↓ / Destination →	**OPNsense (admin)**	**Zabbix (.151)**	**Web (.150)**	**Samba (.153)**	**VLAN33 (mgmt)**	**Internet**
VLAN1_ADMIN	oui	oui	oui	oui	oui	oui
VLAN31_PERSONNEL	non	non	oui	oui	non	oui
VLAN32_VISITEURS	non	non	non	non	no	oui
VLAN_MANAGEMENT	non	non	non	non	—	NTP uniquement

Cette matrice illustre l'application stricte du principe de moindre privilège : chaque VLAN ne dispose que des accès strictement nécessaires à son rôle métier.

Partie 5–Configuration du portail captif

Le portail captif est un dispositif d'authentification placé entre les clients Wi-Fi et l'accès à Internet. Conformément au cahier des charges du Pamandzi Hotel, deux portails distincts ont été déployés :

- Un portail pour le personnel (VLAN31) — accès professionnel aux services internes et à Internet, durée de session adaptée à une journée de travail.
- Un portail pour les visiteurs (VLAN32) — accès Internet uniquement, durée de session adaptée à un séjour touristique.

L'authentification s'appuie sur le système de vouchers natif d'OPNsense : des bons d'échange à usage unique générés à l'avance et distribués physiquement à la réception de l'hôtel (mode « cybercafé »).

5.1 Présentation et choix techniques

Justification du choix des vouchers

Plusieurs méthodes d'authentification étaient envisageables (RADIUS, LDAP, base locale, vouchers). Le choix s'est porté sur les vouchers pour les raisons suivantes :

Critère	**Vouchers**	**RADIUS / LDAP**
Complexité de mise en œuvre	Simple	Élevée (serveur dédié)
Adapté à des comptes à durée limitée	Oui (codes à péremption)	Nécessite gestion manuelle
Distribution physique en réception	Oui (impression)	Non adapté
Indépendance vis-à-vis d'un annuaire externe	Oui	Non
Coût	Aucun (intégré OPNsense)	Serveur supplémentaire

Le système de vouchers est parfaitement adapté à un usage hôtelier : la réception remet un bon d'échange au client lors du check-in, le client se connecte avec, et la session expire automatiquement à la fin du séjour.

Architecture du portail captif:

[Client Wi-Fi]
↓ (HTTP/HTTPS)
[OPNsense - Portail captif]
↓ vérification du voucher
[Serveur de bons d'échange (interne OPNsense)]
↓ si voucher valide
[Internet / Réseau SIO]

Le portail intercepte toute requête HTTP/HTTPS, redirige le client vers une page d'authentification, et n'ouvre l'accès qu'après validation du voucher saisi.

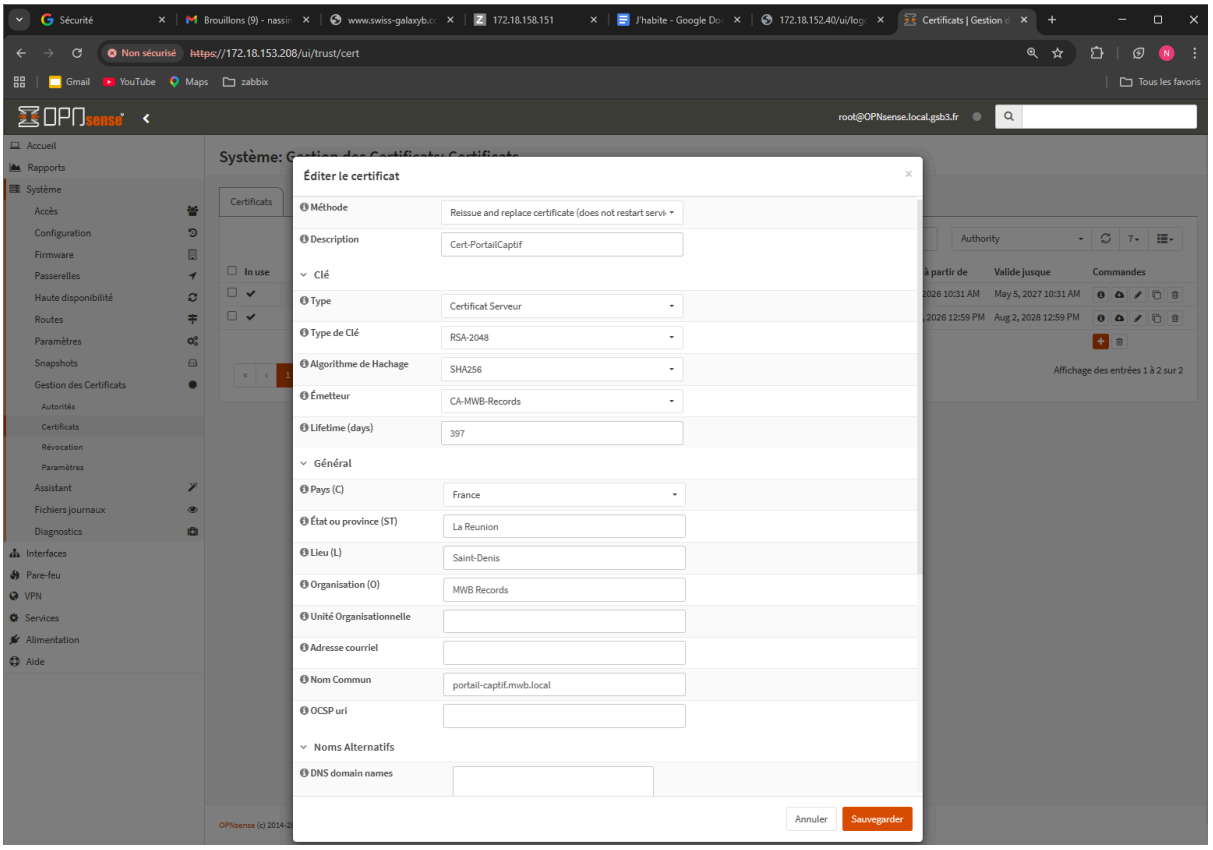
5.2 Création du certificat SSL

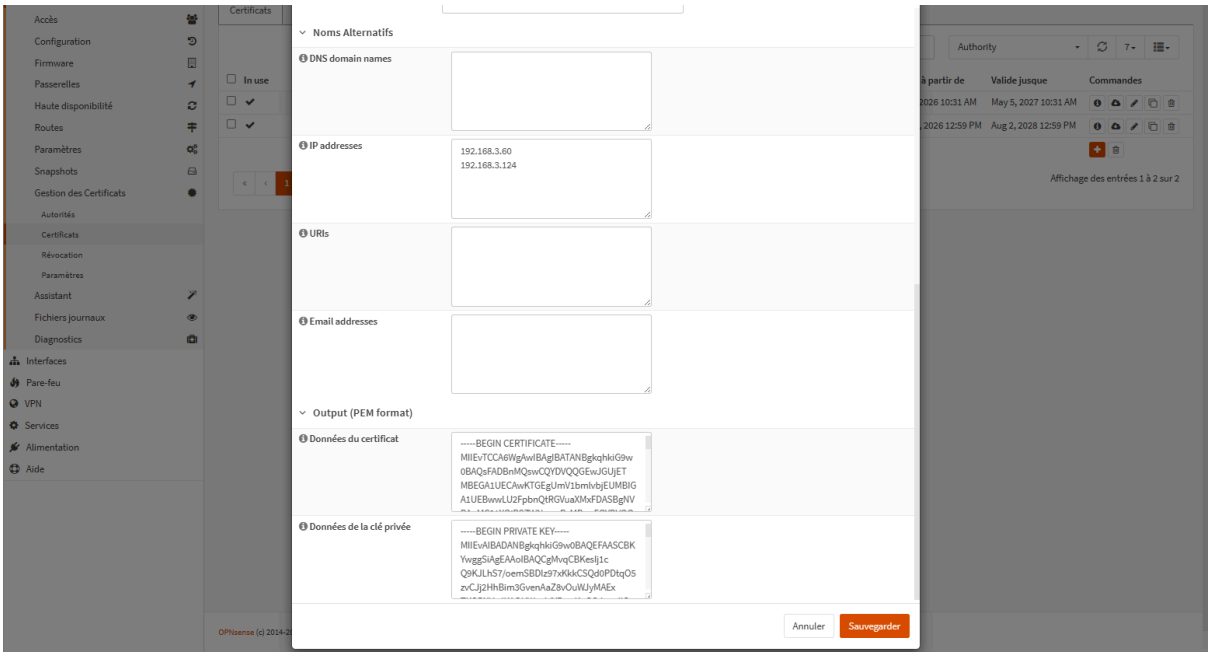
Pour garantir la confidentialité des informations transmises lors de l'authentification (saisie du voucher), le portail captif est servi en HTTPS. Un certificat auto-signé Cert-PortailCaptif a été généré dans OPNsense.

Procédure : Système > Gestion des Certificats > Certificats > Ajouter

Paramètre	**Valeur**
Méthode	Créer un certificat interne
Nom descriptif	Cert-PortailCaptif
Type	Certificat serveur
Algorithme de clé	RSA 2048 bits
Algorithme de signature	SHA-256
Durée de vie	825 jours
Common Name	portail.pamandzi.local

Note de sécurité : un certificat auto-signé entraîne un avertissement dans le navigateur du client. Dans un déploiement en production, ce certificat serait remplacé par un certificat signé par une autorité de certification reconnue (Let's Encrypt ou autorité interne). Dans le cadre de ce projet pédagogique, le certificat auto-signé est acceptable.


Éditer le certificat
Méthode
Reissue and replace certificate (does not restart servi
Description
Cert-PortailCaptif
Clé
Type
Certificat Serveur
Type de Clé
RSA-2048
Algorithme de Hachage
SHA256
Émetteur
CA-MWB-Records
Lifetime (days)
397
Général
Pays (C)
France
État ou province (ST)
La Reunion
Lieu (L)
Saint-Denis
Organisation (O)
MWB Records
Unité Organisationnelle
Adresse courriel
Nom Commun
portail-captif.mwb.local
OCSP uri
Noms Alternatifs
DNS domain names
Annuler
Sauvegarder


Noms Alternatifs
DNS domain names
IP addresses
192.168.3.60
192.168.3.124
URIs
Email addresses
Output (PEM format)
Données du certificat
-----BEGIN CERTIFICATE-----
MIIEvTCCA6WgAwIBAgIBATANBgkqhkiG9w
0BAQsFADBnMQswCQYDVQQGEwJGUjET
MBEGA1UECAwKTGEgUmV1bmlvbjEUMBIG
A1UEBwwLU2FpbnQtRGVuaXMxFDASBgNV
Données de la clé privée
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBK
YwggSiAgEAAoIBAQCgMvqCBKesIj1c
Q9KJLhS7/oemSBDIz97xKkkCSQd0PDtqO5
zvCJj2HhBim3GvenAaZ8vOuWJyMAEx
Annuler
Sauvegarder

5.3 Création des serveurs de bons d'échange

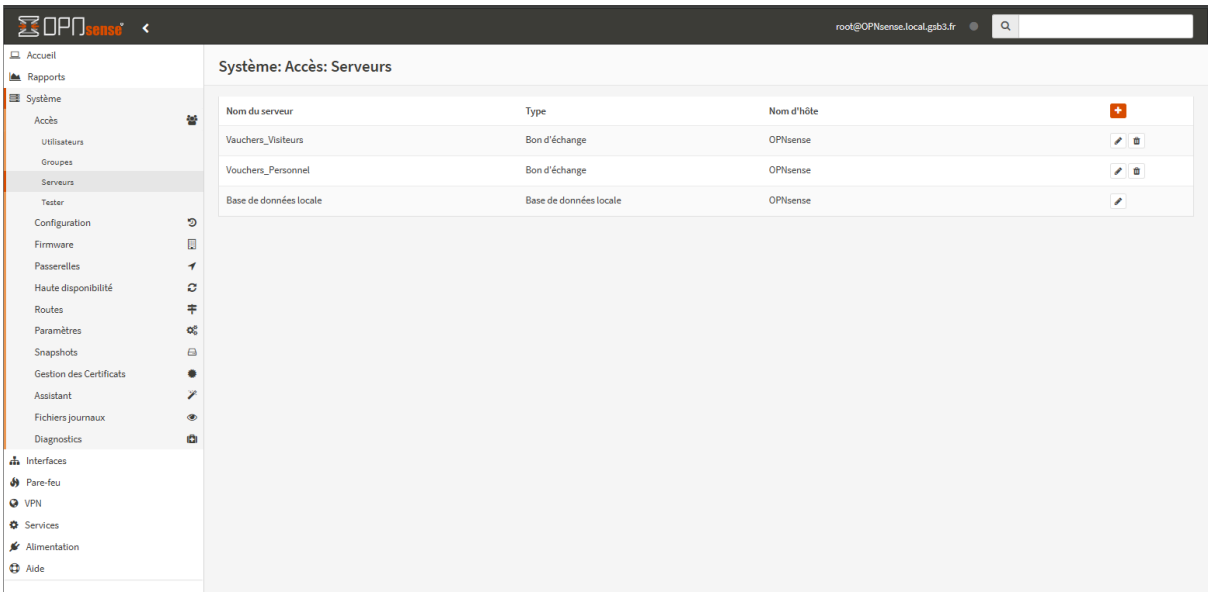
Les serveurs de bons d'échange sont les bases de données qui stockent les vouchers générés et leurs paramètres de validité. Deux serveurs distincts ont été créés pour séparer les codes du personnel de ceux des visiteurs.

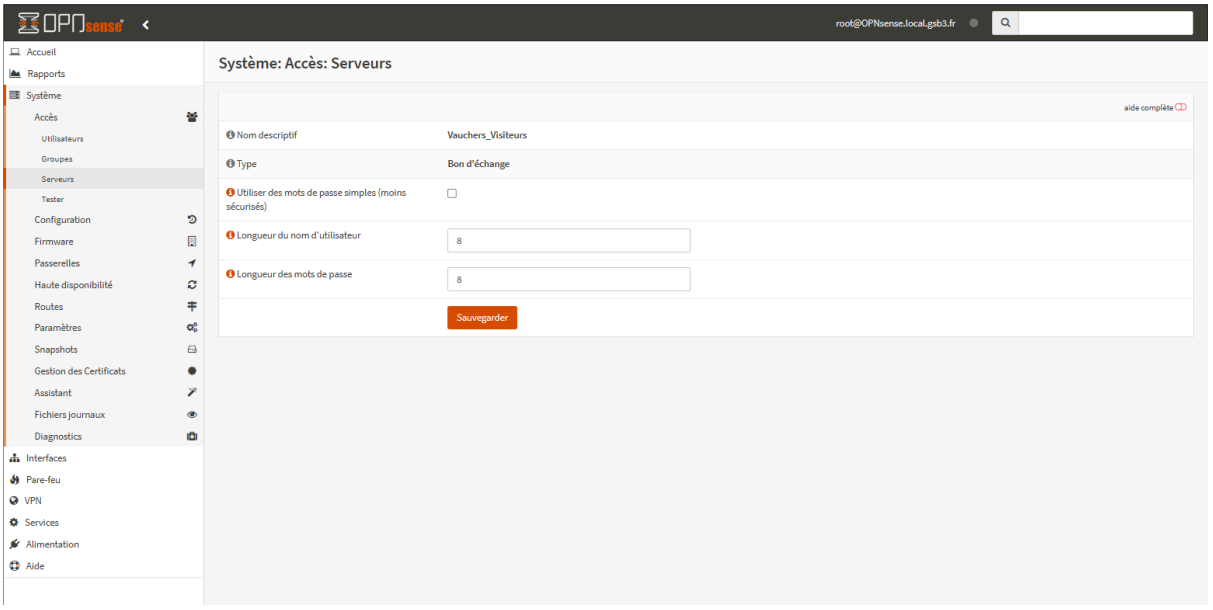
Procédure : Système > Accès > Serveurs > Ajouter

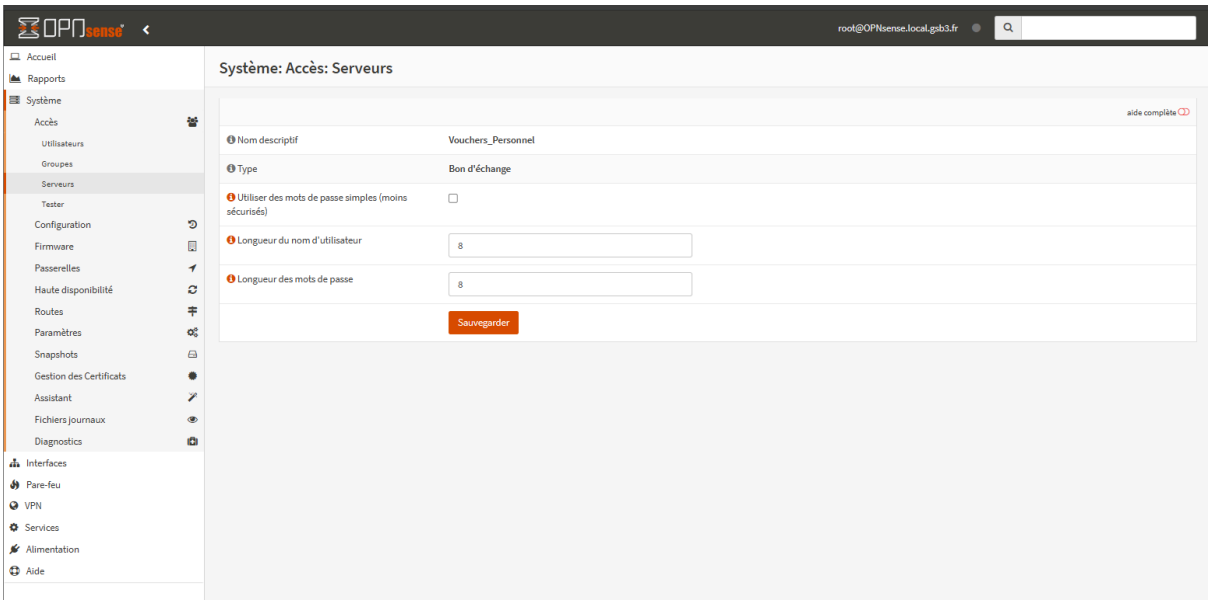
Paramètre	**Vouchers_Personnel**	**Vouchers_Visiteurs**
Type	Bon d'échange	Bon d'échange
Nom descriptif	Vouchers_Personnel	Vouchers_Visiteurs
Longueur du nom d'utilisateur	8 caractères	8 caractères
Longueur du mot de passe	8 caractères	8 caractères
Mots de passe simples	Désactivé	Désactivé

Justification du choix de la longueur :
8 caractères permettent une combinatoire suffisante pour empêcher les attaques par force brute, tout en restant lisibles et saisissables sans erreur depuis un téléphone mobile (4-5 caractères seraient devinables, 12+ seraient pénibles à saisir).

Justification du refus des mots de passe simples :
OPNsense propose une option « mots de passe simples » qui exclut les caractères ambigus (1/l, 0/O). Elle a été désactivée pour augmenter l'entropie des codes générés et donc renforcer la sécurité contre les attaques par devinette.




root@OPNsense.local.gsb3.fr
Accueil
Rapports
Système
Accès
Utilisateurs
Groupes
Serveurs
Tester
Configuration
Firmware
Passerelles
Haute disponibilité
Routes
Paramètres
Snapshots
Gestion des Certificats
Assistant
Fichiers journaux
Diagnostics
Interfaces
Pare-feu
VPN
Services
Alimentation
Aide
Système: Accès: Serveurs
aide complète
Nom descriptif
Vauchers_Visiteurs
Type
Bon d'échange
Utiliser des mots de passe simples (moins sécurisés)
Longueur du nom d'utilisateur
8
Longueur des mots de passe
8
Sauvegarder


root@OPNsense.local.gsb3.fr
Accueil
Rapports
Système
Accès
Utilisateurs
Groupes
Serveurs
Tester
Configuration
Firmware
Passerelles
Haute disponibilité
Routes
Paramètres
Snapshots
Gestion des Certificats
Assistant
Fichiers journaux
Diagnostics
Interfaces
Pare-feu
VPN
Services
Alimentation
Aide
Système: Accès: Serveurs
aide complète
Nom descriptif
Vouchers_Personnel
Type
Bon d'échange
Utiliser des mots de passe simples (moins sécurisés)
Longueur du nom d'utilisateur
8
Longueur des mots de passe
8
Sauvegarder

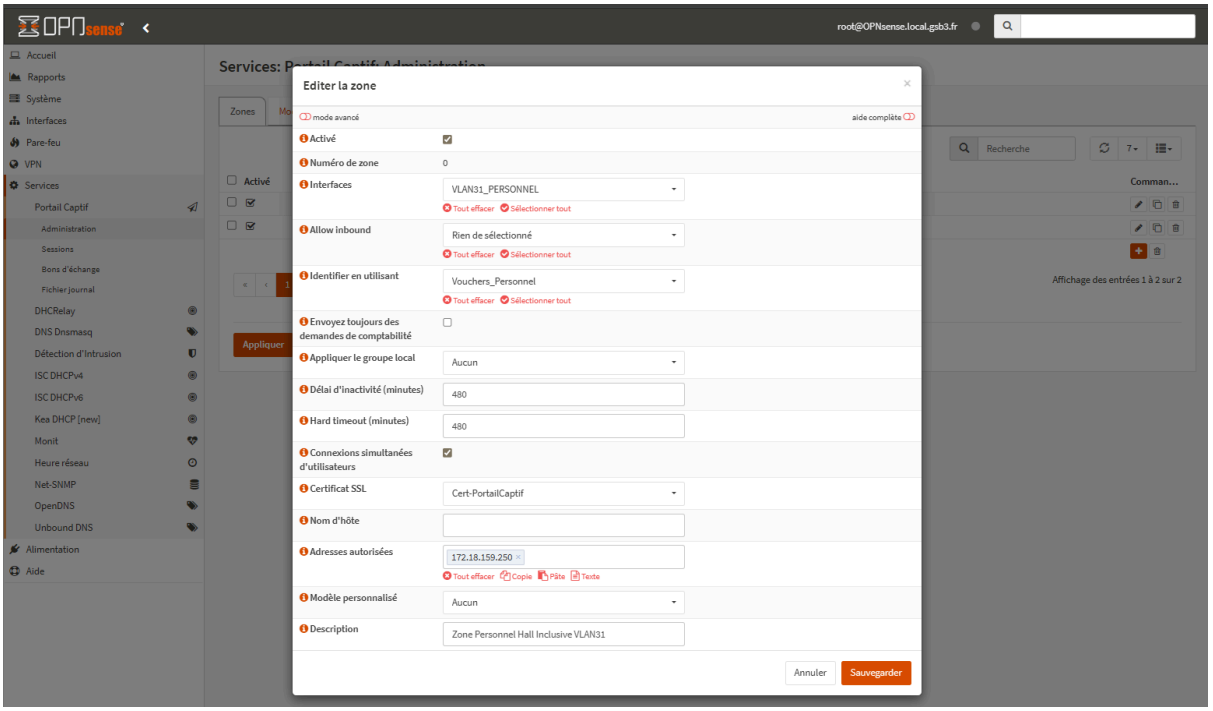
5.4 Configuration des zones du portail captif

Une zone du portail captif définit sur quelle interface le portail s'applique et quels paramètres d'authentification il utilise. Deux zones ont été créées : une par VLAN.

Procédure : Services > Portail Captif > Administration > Onglet Zones > Ajouter

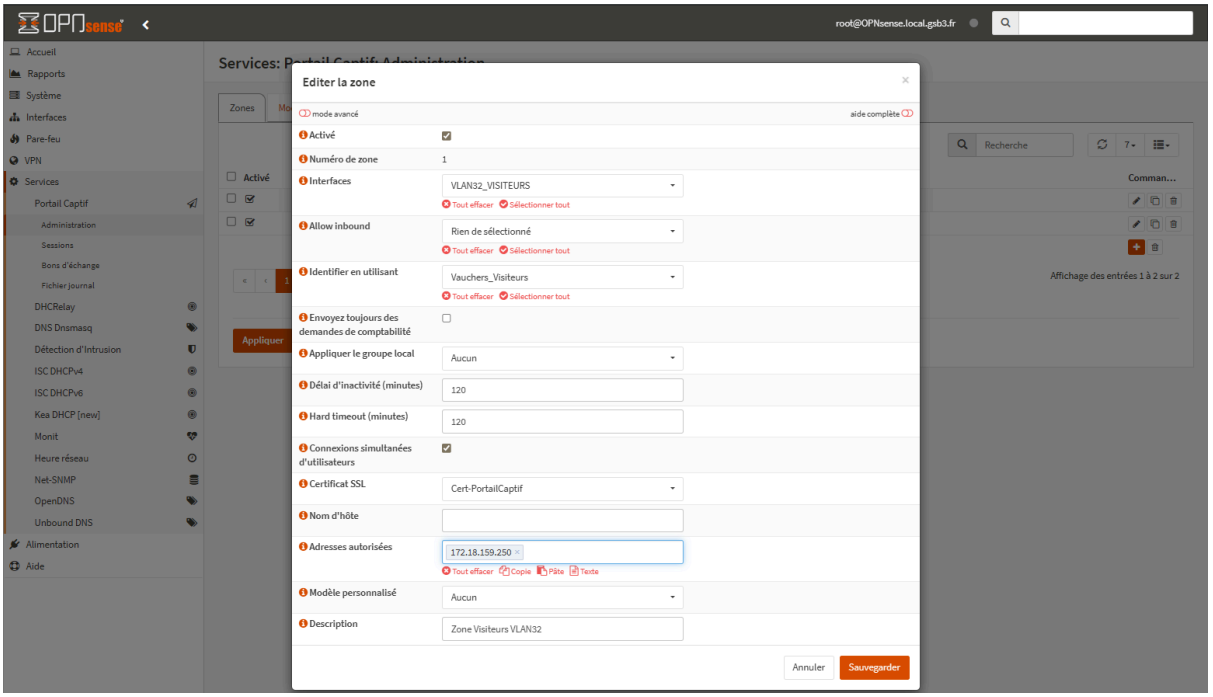
5.4.1 Zone Personnel Hall Inclusive (VLAN31)

Paramètre	**Valeur**	**Justification**
Activé	Oui	Activation de la zone
Numéro de zone	0	Identifiant interne (auto)
Interfaces	VLAN31_PERSONNEL	Portail appliqué uniquement sur ce VLAN
Identifier en utilisant	Vouchers_Personnel	Serveur d'authentification associé
Délai d'inactivité	480 min (8h)	Déconnexion après 8h d'inactivité
Hard timeout	480 min (8h)	Durée maximale d'une session = journée de travail
Connexions simultanées	Autorisées	Permet à un même utilisateur d'utiliser téléphone + ordinateur
Certificat SSL	Cert-PortailCaptif	Chiffrement HTTPS de la page d'authentification
Adresses autorisées	172.18.159.250	DNS du SIO accessible avant authentification
Description	Zone Personnel Hall Inclusive VLAN31	Identification claire dans l'admin


Editer la zone
mode avancé
aide complète
Activé
Numéro de zone
0
Interfaces
VLAN31_PERSONNEL
Tout effacer
Sélectionner tout
Allow inbound
Rien de sélectionné
Identifier en utilisant
Vouchers_Personnel
Envoyez toujours des demandes de comptabilité
Appliquer le groupe local
Aucun
Délai d'inactivité (minutes)
480
Hard timeout (minutes)
480
Connexions simultanées d'utilisateurs
Certificat SSL
Cert-PortailCaptif
Nom d'hôte
Adresses autorisées
172.18.159.250
Modèle personnalisé
Description
Zone Personnel Hall Inclusive VLAN31
Annuler
Sauvegarder

5.4.2 Zone Visiteurs (VLAN32)

Paramètre	Valeur	Justification
Activé	Oui	Activation de la zone
Numéro de zone	1	Identifiant interne (auto)
Interfaces	VLAN32_VISITEURS	Portail appliqué uniquement sur ce VLAN
Identifier en utilisant	Vouchers_Visiteurs	Serveur d'authentification associé
Délai d'inactivité	120 min (2h)	Déconnexion après 2h d'inactivité
Hard timeout	120 min (2h)	Durée maximale d'une session = créneau de visite typique
Connexions simultanées	Autorisées	Permet l'utilisation multi-appareils
Certificat SSL	Cert-PortailCaptif	Chiffrement HTTPS de la page d'authentification
Adresses autorisées	172.18.159.250	DNS du SIO accessible avant authentification
Description	Zone Visiteurs VLAN32	Identification claire dans l'admin

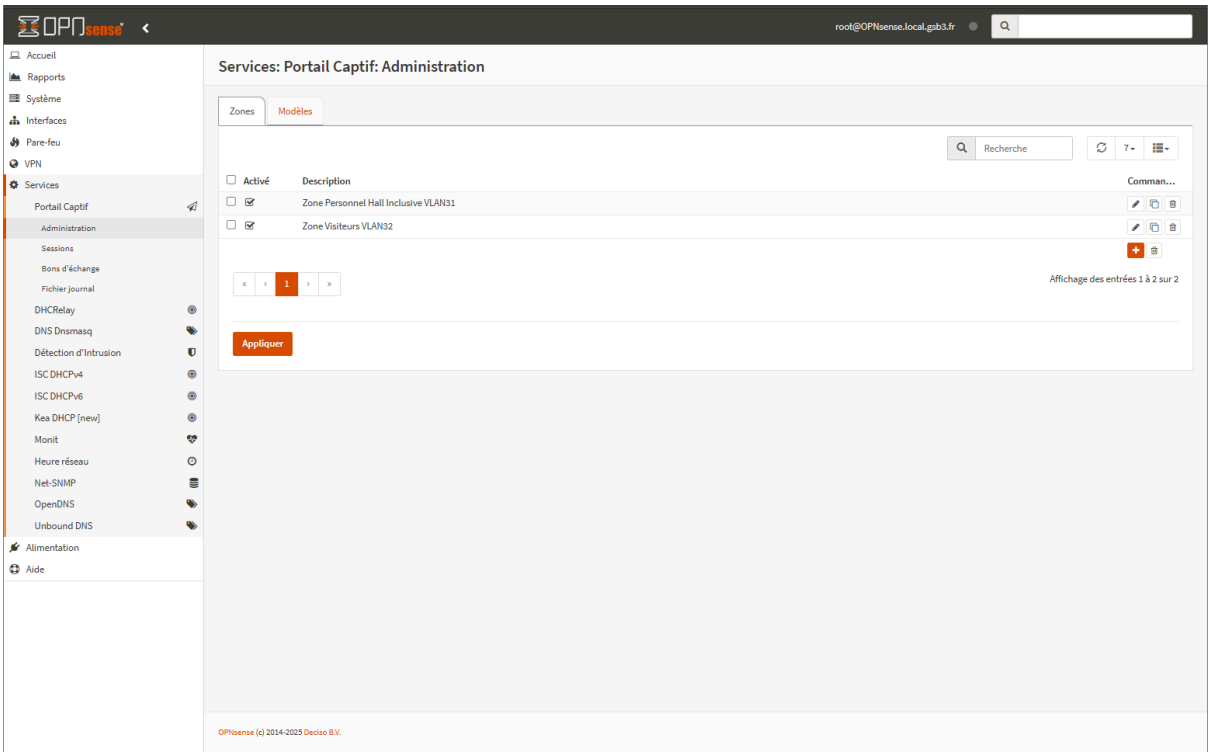


5.4.3 Justification des paramètres communs

Pourquoi autoriser le DNS (172.18.159.250) avant authentification ?
La résolution DNS doit fonctionner avant que le portail captif ne redirige le client. Sinon, le navigateur du client ne peut résoudre aucun nom de domaine, et la redirection vers la page d'authentification échoue. C'est un cas classique de configuration des portails captifs.

Pourquoi des durées différentes entre Personnel et Visiteurs ?
Le personnel travaille sur des sessions longues (journée complète), tandis que les visiteurs ont des usages ponctuels (consultation de mails, recherche d'info). Une durée plus courte pour les visiteurs limite l'occupation des sessions inutiles et le partage de vouchers entre clients (le voucher expire avant qu'un client ne puisse le repasser à un autre).

Pourquoi autoriser les connexions simultanées ?
Un même utilisateur peut souhaiter connecter son téléphone et son ordinateur portable avec le même voucher. Refuser les connexions simultanées créerait une mauvaise expérience utilisateur sans réel gain de sécurité (le voucher est déjà à durée limitée).



5.5 Génération et export des vouchers

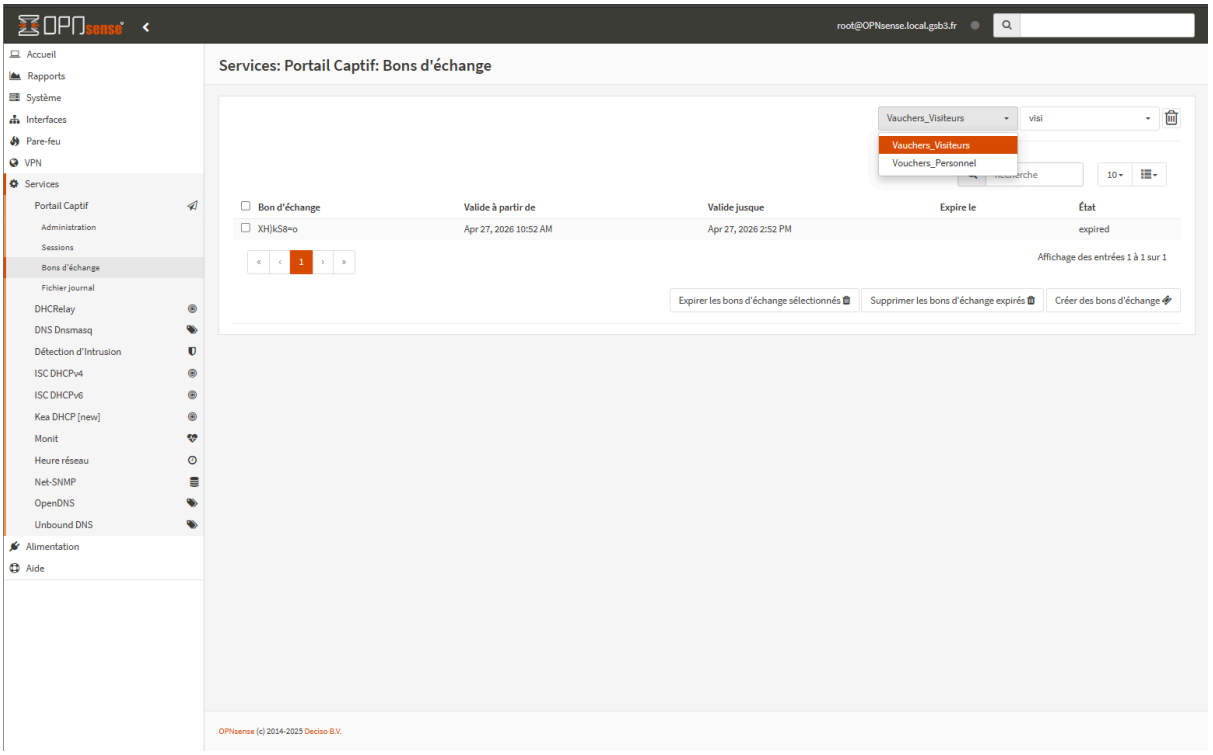
Les vouchers sont générés par lots depuis l'interface d'administration et distribués physiquement à la réception de l'hôtel.

Procédure : Services > Portail Captif > Bons d'échange > Créer des bons d'échange

Paramètre	Valeur
Serveur	Vouchers_Visiteurs (ou Vouchers_Personnel)
Nom du lot	Date du jour (ex: visi-2026-04-27)
Nombre de vouchers	25
Validité	120 minutes pour les visiteurs / 480 minutes pour le personnel
Délai d'expiration	30 jours après génération

Une fois générés, les vouchers sont exportés au format CSV pour impression. Chaque voucher comporte un nom d'utilisateur et un mot de passe à 8 caractères.

Cycle de vie d'un voucher :
[Création]
↓ (lot de 25 généré et exporté en CSV)
[Impression / découpe]
↓ (remis à la réception de l'hôtel)
[Distribution au client lors du check-in]
↓ (le client saisit son code sur le portail)
[Activation à la première utilisation]
↓ (le compteur de validité démarre)
[Expiration]
↓ (selon la durée définie : 2h ou 8h)
[Statut « expired »]



Note : un voucher non utilisé reste en statut « unused » et peut être recyclé. Un voucher utilisé puis expiré ne peut plus être réutilisé. Un job de nettoyage peut être configuré pour supprimer automatiquement les vouchers expirés.

5.6 Limitation de bande passante (Traffic Shaping)

Pour garantir une qualité de service équitable et empêcher qu'un seul utilisateur ne sature la connexion partagée, une politique de traffic shaping a été mise en place via le façonneur OPNsense.

5.6.1 Principe

Le façonneur d'OPNsense fonctionne en deux temps :

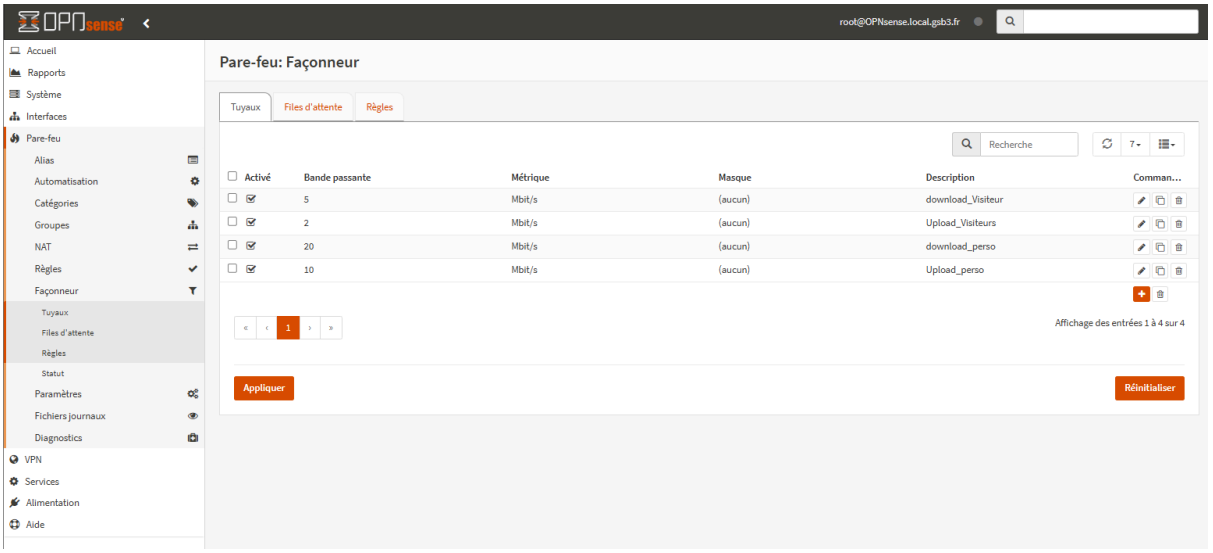
1. Tuyaux (pipes) : définissent un débit maximum (en Mbit/s).
2. Règles : associent un VLAN ou un type de trafic à un tuyau, avec une direction précise (entrant/sortant).

Les files d'attente (queues) ne sont pas configurées : elles servent à introduire des sous-priorités au sein d'un même tuyau (ex : VoIP prioritaire sur téléchargements). Pour ce projet, une simple limitation de débit global par VLAN est suffisante au regard du besoin métier.

5.6.2 Configuration des tuyaux

Procédure : Pare-feu > Façonneur > Tuyaux

#	Description	Bande passante	Métrique	Usage
1	download_Visiteur	5	Mbit/s	Trafic descendant vers les visiteurs
2	Upload_Visiteurs	2	Mbit/s	Trafic montant depuis les visiteurs
3	download_perso	20	Mbit/s	Trafic descendant vers le personnel
4	Upload_perso	10	Mbit/s	Trafic montant depuis le personnel



5.6.3 Justification des débits

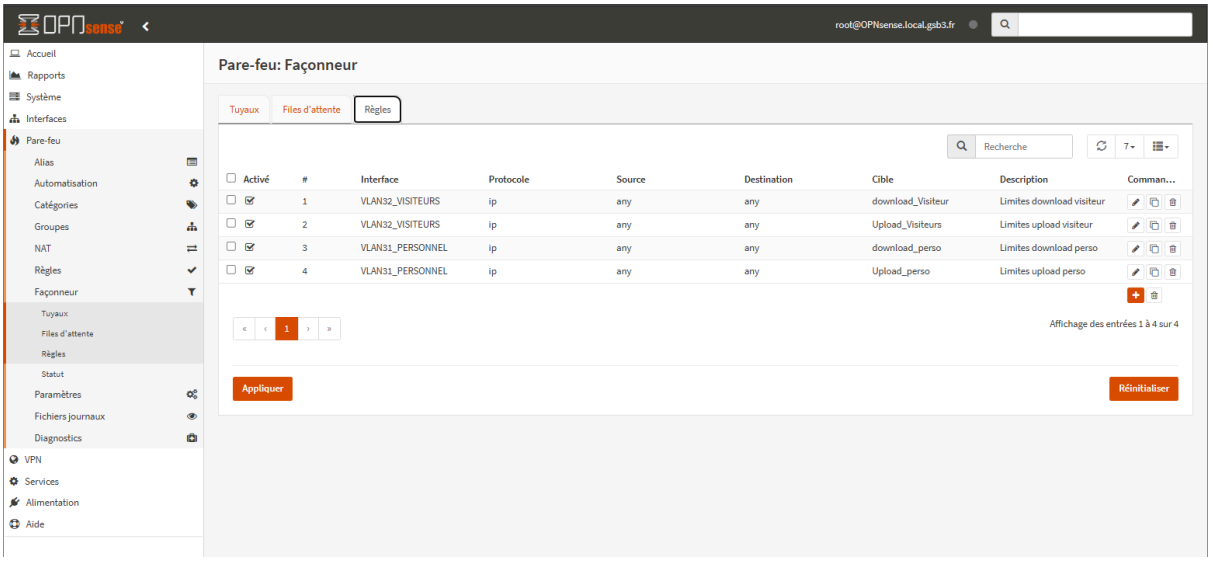
VLAN	**Download**	**Upload**	**Justification**
VLAN31 Personnel	20 Mbit/s	10 Mbit/s	Débits suffisants pour les usages métiers : visioconférence, transferts de fichiers, accès aux applications cloud
VLAN32 Visiteurs	5 Mbit/s	2 Mbit/s	Débits suffisants pour la consultation web et le streaming vidéo standard, mais insuffisants pour la saturation par téléchargement intensif

L'asymétrie download/upload reflète l'usage réel :
la majorité du trafic Internet est descendant (consultation, streaming). L'upload est volontairement plus restreint pour empêcher l'usage du réseau hôtelier comme passerelle de partage de fichiers volumineux.

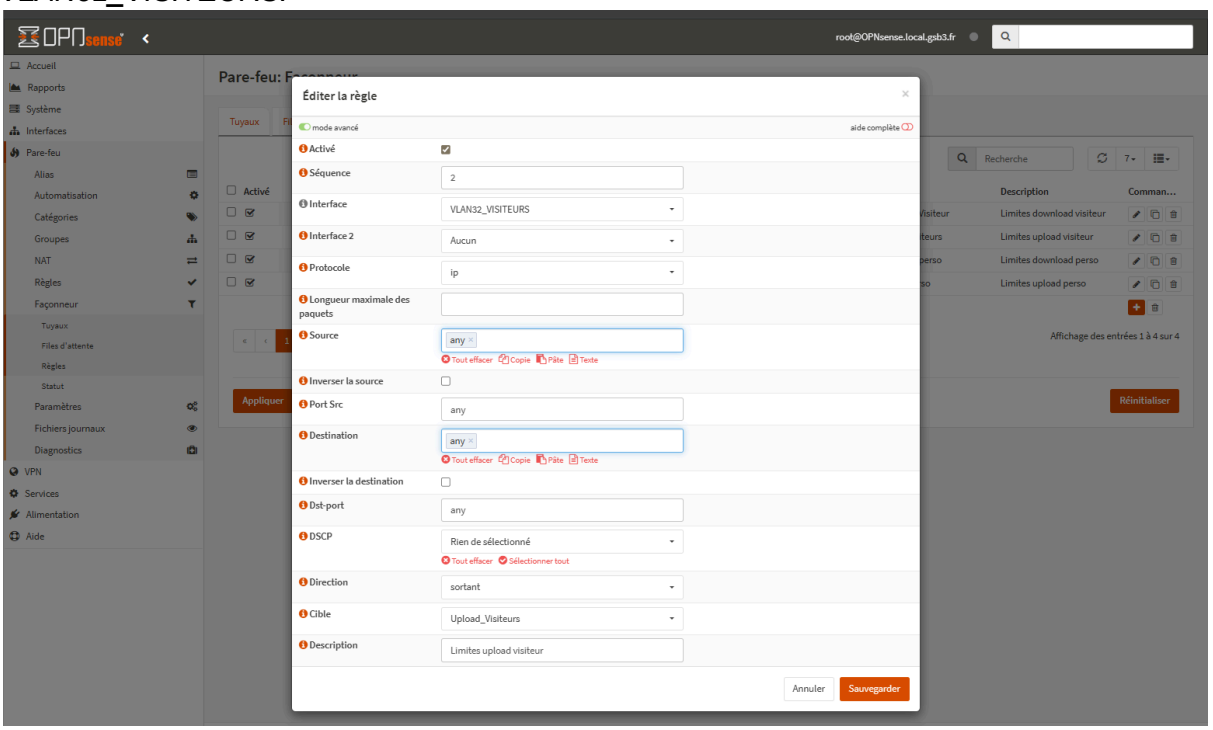
5.6.4 Configuration des règles du façonneur

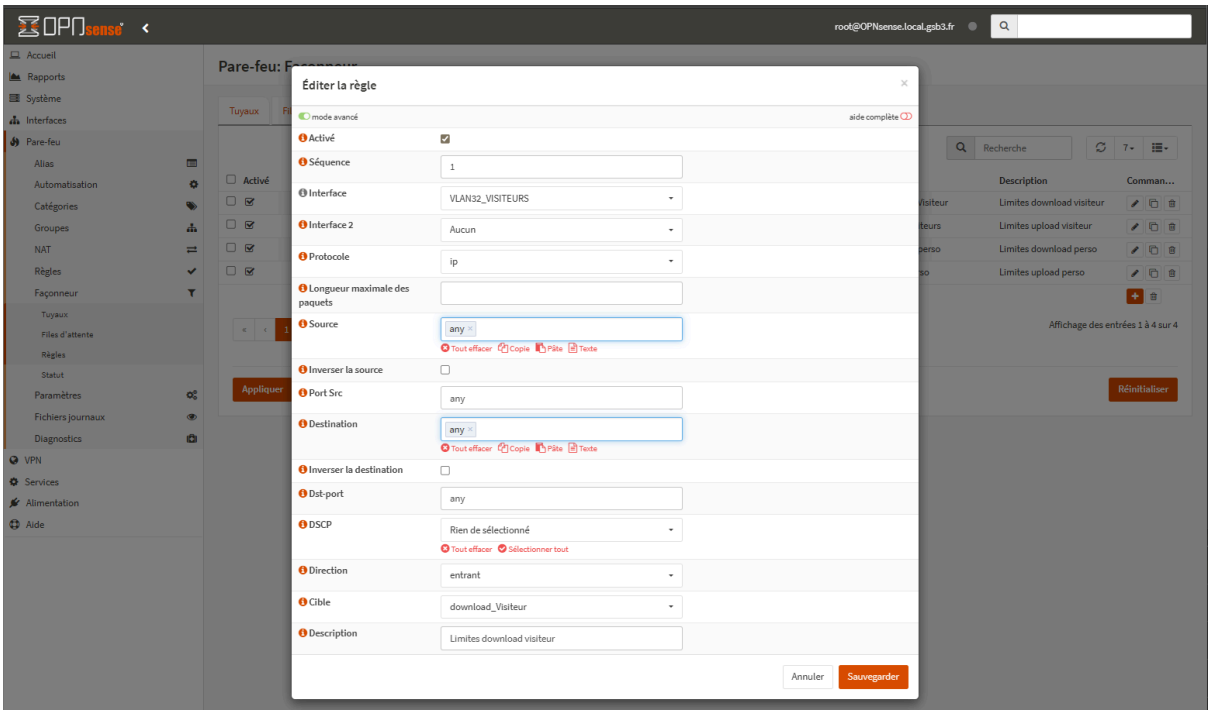
Procédure : Pare-feu > Façonneur > Règles

#	Interface	Protocole	Direction	Cible	Description
1	VLAN32_VISITEURS	IP	entrant	download_Visiteur	Limites download visiteur
2	VLAN32_VISITEURS	IP	sortant	Upload_Visiteurs	Limites upload visiteur
3	VLAN31_PERSONNEL	IP	entrant	download_perso	Limites download perso
4	VLAN31_PERSONNEL	IP	sortant	Upload_perso	Limites upload perso

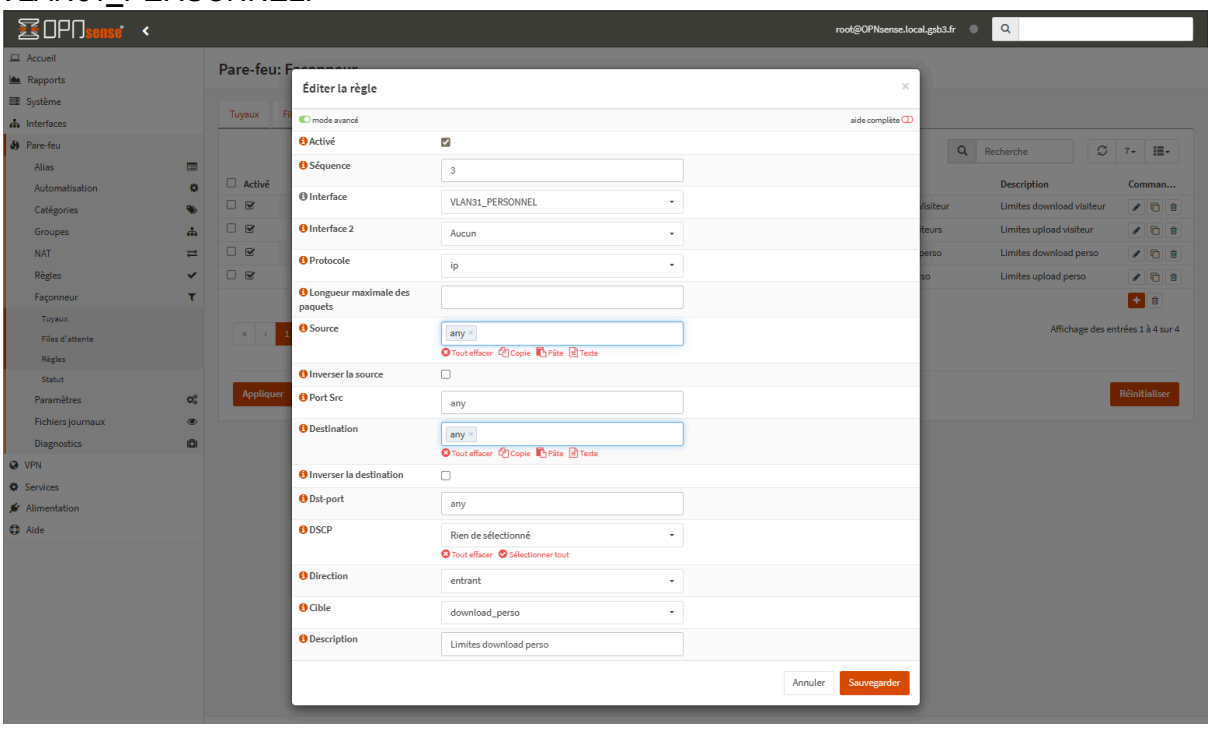


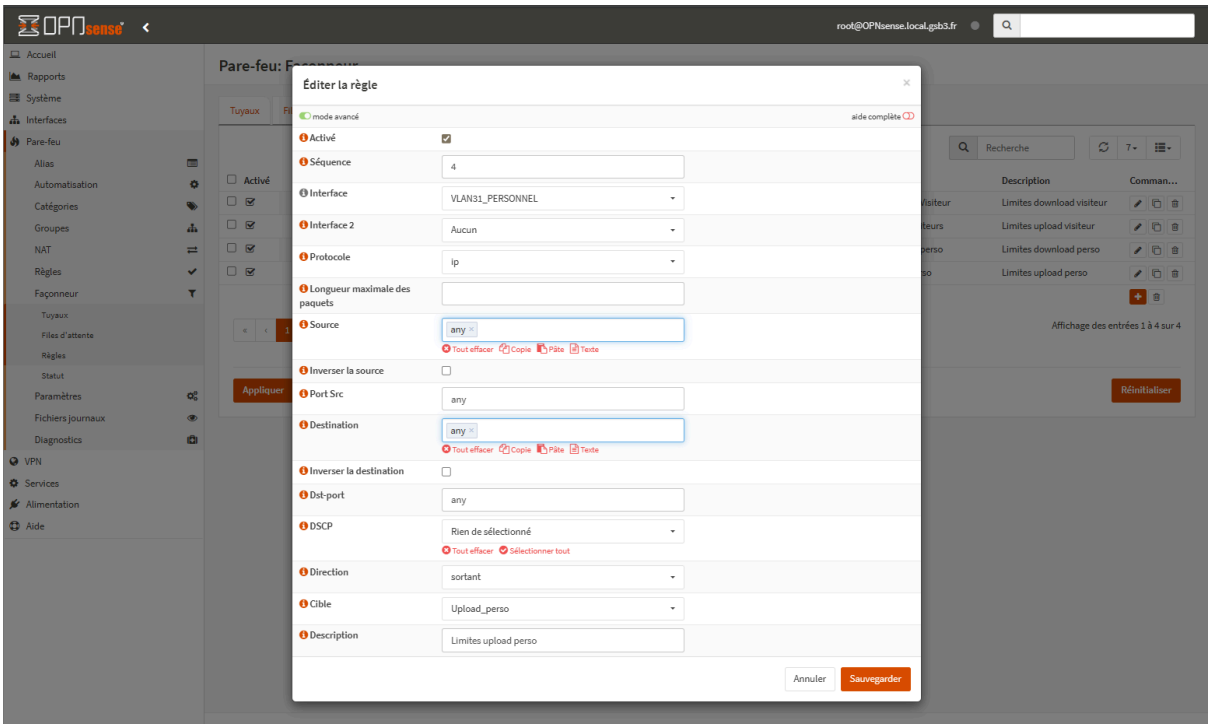
VLAN32_VISITEURS:





VLAN31_PERSONNEL:





5.6.5 Justification du choix des directions

La direction (entrant/sortant) est définie du point de vue de l'interface VLAN et non du point de vue du client. Cette distinction est cruciale pour que le shaping s'applique au bon sens du flux :

- Direction entrant (in) : paquets qui arrivent sur l'interface VLAN. Pour un client interne, cela correspond au trafic descendant (download) — les paquets proviennent du WAN et entrent dans le VLAN pour atteindre le client.
- Direction sortant (out) : paquets qui quittent l'interface VLAN. Pour un client interne, cela correspond au trafic montant (upload) — les paquets proviennent du client, sortent du VLAN et partent vers le WAN.

Cette configuration permet d'appliquer des débits asymétriques (download ≠ upload) de manière cohérente avec le sens réel des flux de données.

5.7 Synthèse de la configuration

Composant	Personnel (VLAN31)	Visiteurs (VLAN32)
Serveur d'authentification	Vouchers_Personnel	Vouchers_Visiteurs
Longueur du voucher	8 caractères	8 caractères
Délai d'inactivité	8 heures	2 heures
Hard timeout	8 heures	2 heures
Download max	20 Mbit/s	5 Mbit/s
Upload max	10 Mbit/s	2 Mbit/s
Connexions simultanées	Autorisées	Autorisées
Certificat SSL	Cert-PortailCaptif	Cert-PortailCaptif

Cette configuration applique une politique différenciée selon le profil utilisateur : le personnel bénéficie de sessions longues et de débits confortables pour son activité professionnelle, tandis que les visiteurs disposent d'un accès limité dans la durée et le débit, cohérent avec un usage de loisir ponctuel.