Mode Opératoire

Routage inter-VLAN et filtrage sur OPNsense

Code :	MO-NET-004
Version :	1.2
Date :	10 septembre 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	06/05/2026	Création initiale
1.1	26/06/2026	Harmonisation de la présentation des étapes et des encadrés.
1.2	10/09/2026	Mise en production effective pour le Wi-Fi pédagogique : interfaces VLAN 240/241 (opt1/opt2) avec adressage statique, DHCP Kea sur les deux sous-réseaux, filtrage (isolation 240) et zone de portail captif. Architecture complète et règles exactes dans le MO-NET-008.

1 Objet

Ce mode opératoire décrit la procédure de création d'interfaces VLAN sur le pare-feu OPNsense, leur assignation, la configuration du routage inter-VLAN et la mise en place des règles de filtrage associées. Il s'inscrit dans la segmentation réseau de l'infrastructure BTS SIO du Lycée Jean Lurçat.

L'architecture retenue est de type *router-on-a-stick* : les sous-interfaces VLAN sont portées par l'interface physique LAN (`bge0`), qui assure à la fois le routage et le filtrage entre les différents segments. Le switch connecté au pare-feu transporte l'ensemble des VLANs sur un trunk 802.1Q.

La procédure utilise le VLAN 100 « Serveurs » (`10.0.100.0/24`) comme exemple fil conducteur, mais elle est reproductible pour tout VLAN supplémentaire.

2 Champ d'application

Public concerné	Administrateurs de l'infrastructure BTS SIO
Système	Pare-feu OPNsense 26.1.5 (`10.0.112.1`, FreeBSD 14.3)
Protocole	HTTP (`http://10.0.112.1`)
Authentification	Compte administrateur nominatif
Durée estimée	30–45 minutes par VLAN (hors tests bout en bout)

Interface	Rôle actuel	Adressage
bge0 (LAN)	Lien trunk vers le switch	`10.0.112.1/16` → `/24` après déploiement
bge1 (WAN)	Lien vers la box Orange	`192.168.1.69/24`
em0–em3	Non utilisées	—

3 Prérequis

Prérequis

— **Accès réseau au pare-feu : `http://10.0.112.1` (câble RJ45 sur site ou tunnel VPN WireGuard)**

— **Compte administrateur OPNsense (identifiants dans le gestionnaire de**

mots de passe)
- **Plan d'adressage validé : identifiant VLAN, sous-réseau, passerelle**
- **Trunk 802.1Q configuré côté switch (cf. MO-NET-003)**
- **Accès physique à la console du pare-feu ou management hors-bande (iLO), en cas de perte de connectivité**

Accès console indispensable

Avant toute modification de l'interface LAN ou des règles de filtrage, s'assurer de disposer d'un accès physique à la console du pare-feu. Une erreur d'adressage ou de filtrage peut rendre l'interface web inaccessible ; la console permet alors de rétablir la configuration.

Masque du LAN actuel

Le LAN est actuellement configuré en `10.0.112.1/16`. Ce masque large englobe tous les sous-réseaux `10.0.x.x` dans le même domaine de diffusion, ce qui rend la segmentation VLAN inopérante. Lors du déploiement des VLANs, le masque du LAN doit être réduit à `/24` (`10.0.112.0/24`) pour que le routage inter-VLAN fonctionne correctement.

4 Procédure

4.1 Création de l'interface VLAN

1

Créer le périphérique VLAN

1. **Se connecter à l'interface d'administration : `http://10.0.112.1`**

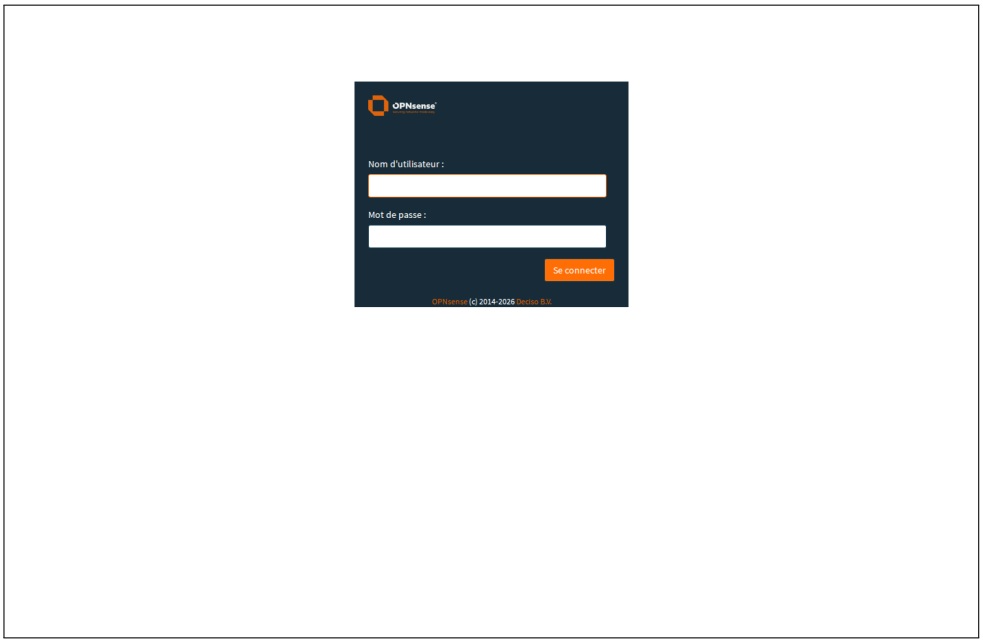


Figure 1 : Page de connexion de l'interface web OPNsense : saisir le nom d'utilisateur et le mot de passe du compte administrateur nominatif.

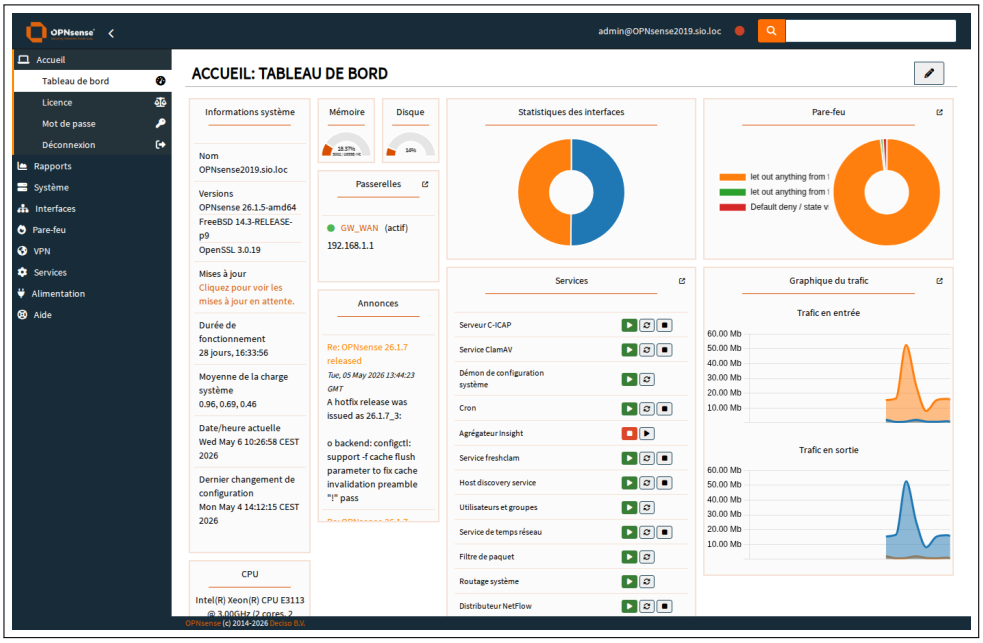


Figure 2 : Tableau de bord OPNsense après connexion : informations système, statistiques des interfaces, état des services et du pare-feu.

2. **Naviguer vers Interfaces → Périphériques → VLAN (`/ui/interfaces/vlan`)**
3. **Cliquer sur le bouton + pour ajouter un VLAN**
4. **Remplir les champs :**
   - ***Dispositif* : laisser la valeur générée automatiquement (`vlan0100`)**
   - ***Parent* : `bge0` (interface LAN physique)**
   - ***Tag du VLAN* : `100`**
   - ***Priorité VLAN* : laisser par défaut (0 — *Best Effort*)**
   - ***Description* : `VLAN Serveurs`**
5. **Laisser le protocole sur Auto (défaut 802.1Q)**
6. **Cliquer sur Sauvegarder**

Le périphérique `vlan0100` apparaît dans la liste des VLANs.

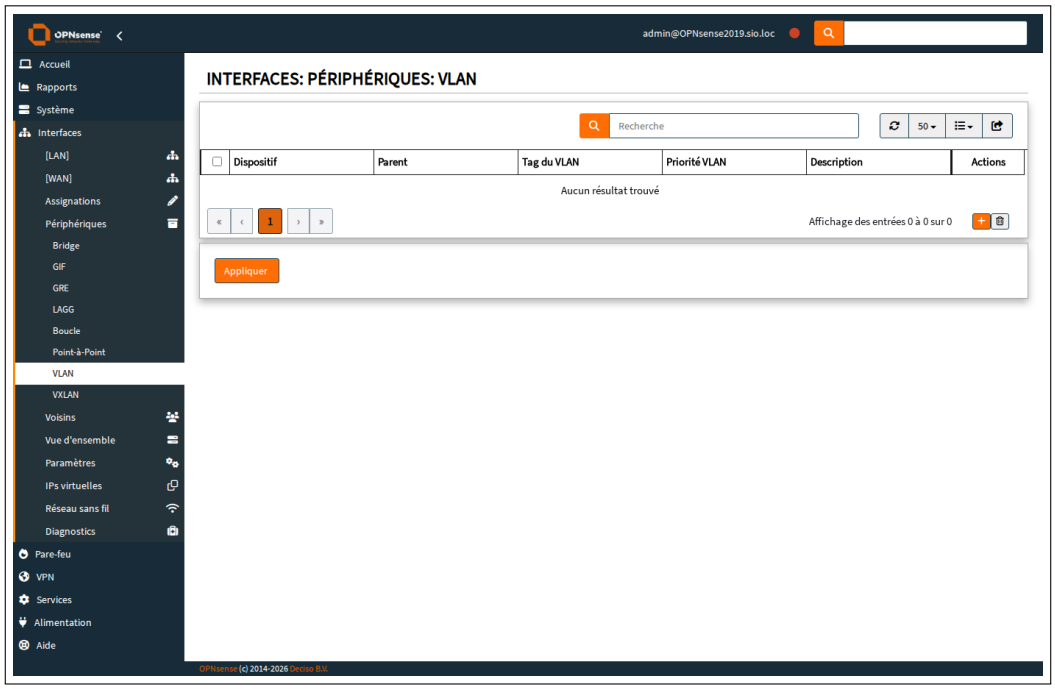


Figure 3 : Page **Interfaces → Périphériques → VLAN** : liste des VLANs avant création (aucune entrée).

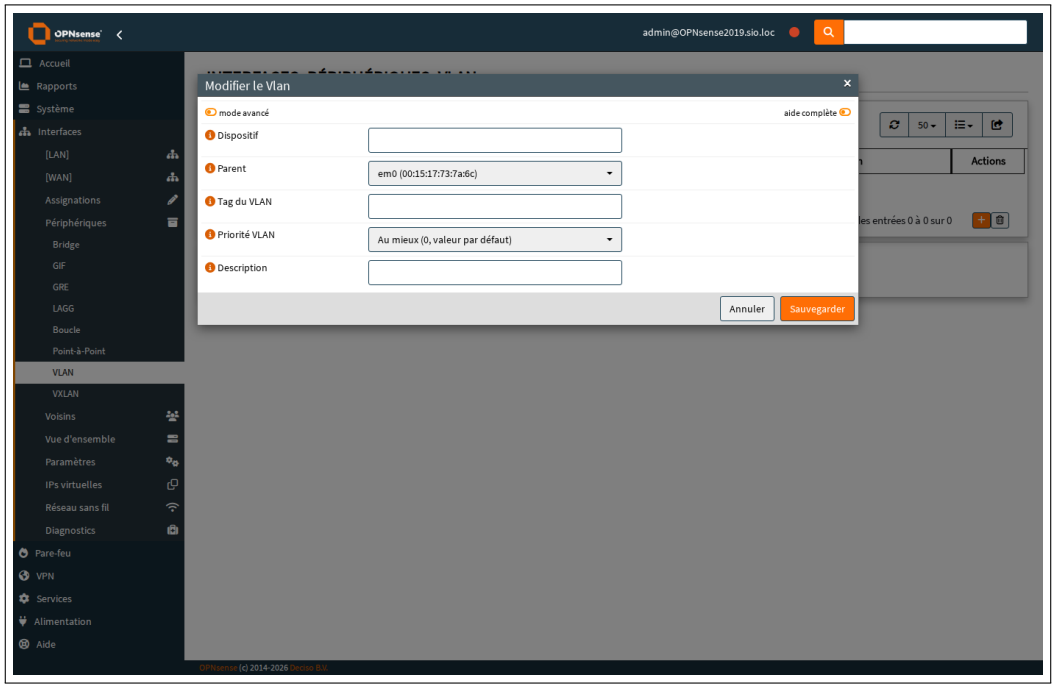


Figure 4 : Boîte de dialogue de création d'un VLAN : champs *Parent*, *Tag du VLAN* et *Description*.

4.2 Assignation de l'interface

2 **Assigner le VLAN à une interface logique**

1. **Naviguer vers Interfaces → Assignations (`/interfaces_assign.php`)**
2. **Dans la section *Assigner une nouvelle interface*, sélectionner le périphérique VLAN créé : `vlan0100 (VLAN Serveurs sur bge0)`**
3. **Saisir une description (par exemple `SERVERS`)**
4. **Cliquer sur Ajouter**

L'interface apparaît dans la liste des assignations sous le nom `[OPTx]` (par ex. `[OPT1]`).

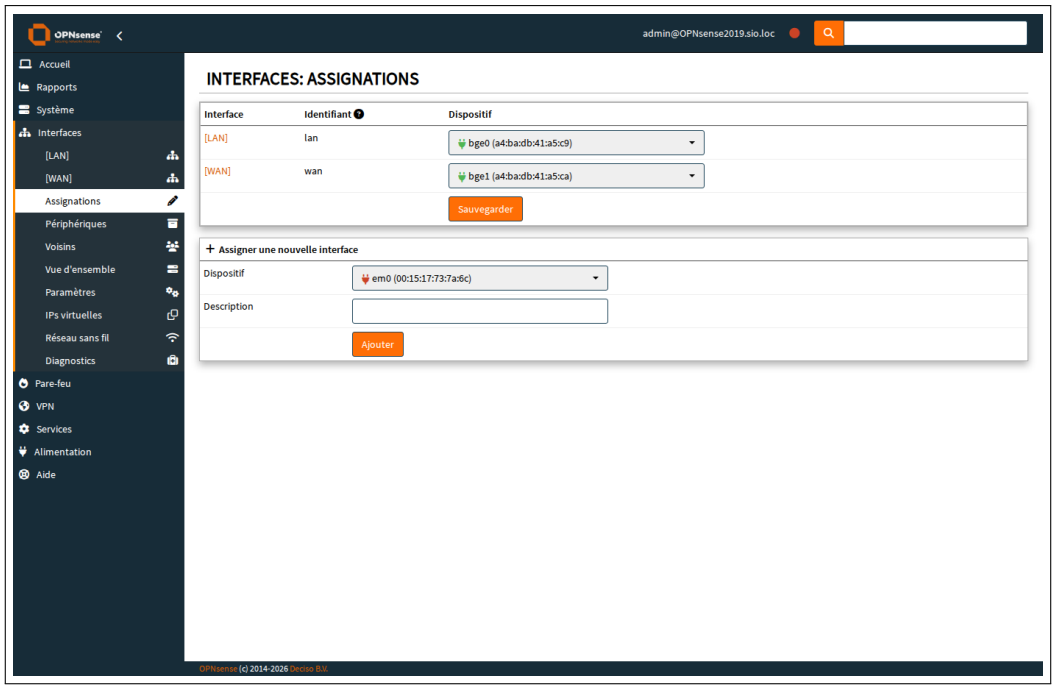


Figure 5 : Page **Interfaces → Assignations** : interfaces actuelles (LAN, WAN) et menu déroulant pour assigner une nouvelle interface.

4.3 Configuration de l'interface

3 Activer et configurer l'interface VLAN

1. Naviguer vers Interfaces → [OPTx] (cliquer sur le nom de l'interface nouvellement créée)
2. Cocher *Activer l'interface*
3. Dans *Description*, remplacer `OPTx` par un nom explicite : `SERVERS`
4. Dans *Type de configuration IPv4*, sélectionner Statique IPv4
5. Dans la section *Configuration statique IPv4* :
   - *Adresse IPv4* : `10.0.100.1`
   - *Masque* : `/24` (soit `255.255.255.0`)
6. Cliquer sur Sauvegarder
7. Cliquer sur Appliquer les modifications dans le bandeau jaune

L'adresse `10.0.100.1` devient la passerelle par défaut du VLAN 100 pour les équipements de ce segment.

Convention de nommage

Adopter un nommage court et cohérent pour les interfaces : `SERVERS`, `STUDENTS`, `WIFI`, `MGMT`. OPNsense affiche ces noms dans les menus de règles de filtrage ; un nom parlant facilite la lecture et la maintenance des règles.

4.4 Configuration DHCP (optionnel)

4 Configurer le service DHCP pour le VLAN

Le choix dépend de l'architecture DHCP en place :

Option A — OPNsense sert le DHCP pour ce VLAN :

1. **Naviguer vers Services → DHCPv4 → [SERVERS]**
2. **Cocher *Activer le serveur DHCP sur l'interface SERVERS***
3. **Configurer la plage d'adresses :**
   — ***Début*** **:** `10.0.100.10`
   — ***Fin*** **:** `10.0.100.250`
4. **Renseigner la passerelle :** `10.0.100.1`
5. **Renseigner le(s) serveur(s) DNS :** `10.0.112.10` **(DC1),** `10.0.112.11` **(DC2)**
6. **Cliquer sur** Sauvegarder

Option B — Windows Server (DC1/DC2) gère le DHCP :

Dans l'infrastructure BTS SIO, le DHCP est géré par les contrôleurs de domaine. Il faut alors configurer un relai DHCP sur OPNsense pour que les requêtes DHCP provenant du VLAN soient transmises aux DCs :

1. **Naviguer vers Services → DHCPv4 → Relai**
2. **Cocher *Activer le relai DHCP***
3. **Dans *Interfaces du relai*, sélectionner l'interface du VLAN (**`SERVERS`**)**
4. **Dans *Serveurs de destination*, saisir les adresses des DCs :** `10.0.112.10`, `10.0.112.11`
5. **Cliquer sur** Sauvegarder

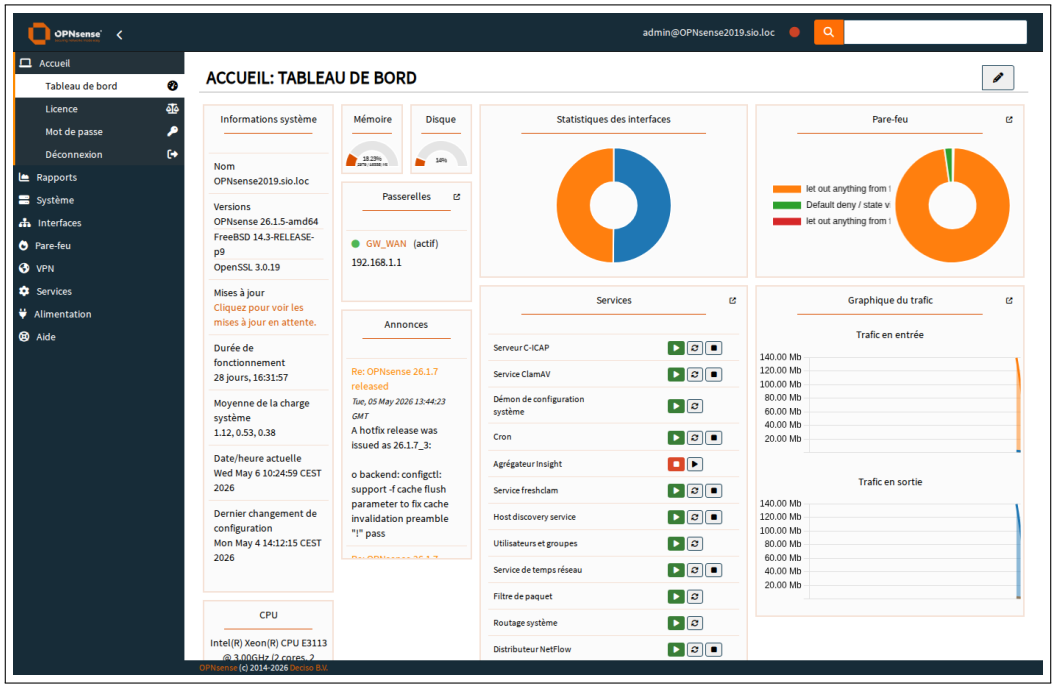


Figure 6 : Page **Services** → **DHCPv4** : configuration du serveur DHCP pour une interface.

Relai et serveur DHCP

OPNsense ne permet pas d'activer simultanément le serveur DHCP et le relai DHCP sur la même interface. Si le DHCP est centralisé sur les DCs pour le domaine Active Directory, privilégier systématiquement le relai : cela évite de maintenir deux périmètres DHCP indépendants.

4.5 Création des règles de filtrage inter-VLAN

5 Définir la politique de filtrage du VLAN

Par défaut, OPNsense bloque tout le trafic sur les interfaces nouvellement créées. Les règles doivent être ajoutées explicitement selon le principe du *deny by default*.

1. **Naviguer vers Pare-feu → Règles → [SERVERS]**
2. **Créer les règles nécessaires en cliquant sur +**

Exemples de règles pour le VLAN Serveurs :

#	Action	Source	Destination	Port	Description
1	Pass	SERVERS net	DC1, DC2	53, 88, 389, 636	DNS, Kerberos, LDAP(S)
2	Pass	SERVERS net	DC1, DC2	445	Partages SYSVOL/NETLOGON
3	Pass	SERVERS net	WAN net	*	Accès Internet
4	Block	SERVERS net	LAN net	*	Blocage vers le VLAN admin
5	Block	SERVERS net	*	*	Rejet par défaut (im-

Chaque règle doit comporter une description claire pour faciliter la relecture ultérieure. L'ordre des règles est déterminant : OPNsense évalue les règles de haut en bas, la première correspondance l'emporte.

Après création de l'ensemble des règles, cliquer sur Appliquer les modifications.

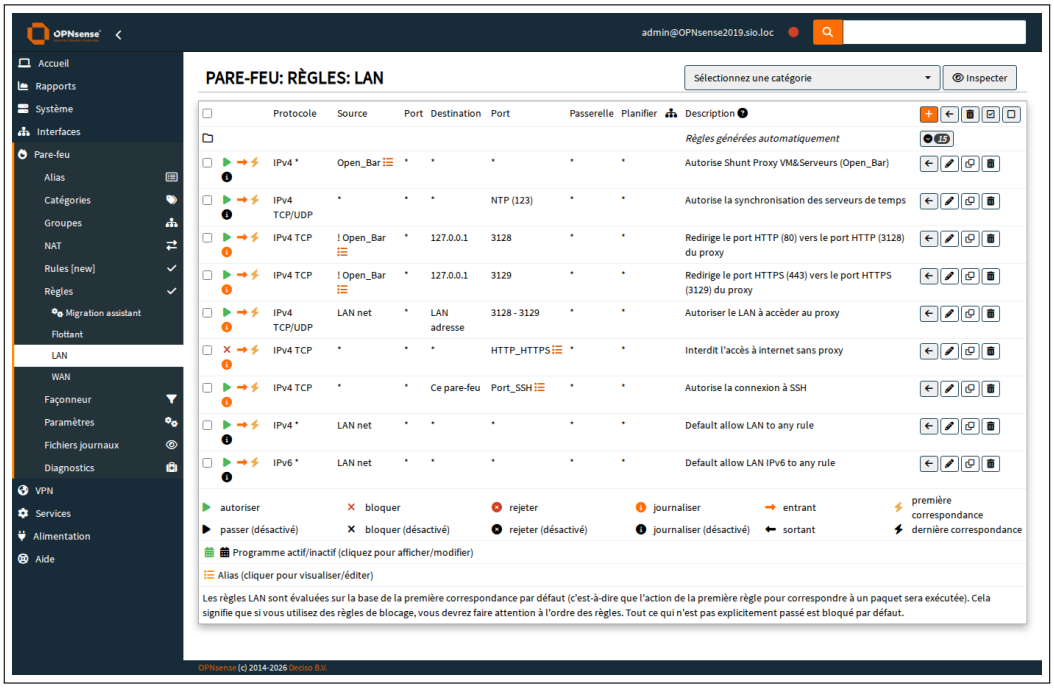


Figure 7 : Page **Pare-feu** → **Règles** → **LAN** : règles de filtrage actuelles sur l'interface LAN.

Alias Open_Bar

L'alias `Open_Bar` (`10.0.0.0/16`) autorise actuellement l'ensemble du trafic interne sans restriction. Lors du déploiement des VLANs, cet alias doit être restreint au seul VLAN d'administration (`10.0.112.0/24`) ou supprimé, sous peine de rendre le cloisonnement VLAN inopérant. Cf. constat F-SEC-001 et tâche T33.

Utiliser des alias

Pour simplifier la gestion des règles, créer des alias dans Pare-feu → Alias pour regrouper les adresses récurrentes : `DC_Servers` (`10.0.112.10`, `10.0.112.11`), `AD_Ports` (53, 88, 389, 445, 636), etc. Les règles deviennent alors lisibles et plus faciles à maintenir.

4.6 Vérification du trunk côté switch

6

S'assurer que le trunk transporte le VLAN

Le port du switch connecté à l'interface `bge0` d'OPNsense doit être configuré en trunk 802.1Q et transporter le VLAN nouvellement créé.

1. **Vérifier la configuration trunk sur le switch : le VLAN 100 doit apparaître dans la liste des VLANs *tagged* du port**
2. **Le VLAN d'administration (112) doit rester comme VLAN *untagged* (natif) pour préserver la compatibilité avec la configuration actuelle**
3. **Se référer au MO-NET-003 pour la procédure complète de configuration des VLANs sur les switches Aruba 1930**

```
# Verification du trunk depuis OPNsense (console ou SSH)
ifconfig vlan0100
# Doit afficher : vlan: 100 parent interface: bge0
# et l'adresse 10.0.100.1/24

# Test de connectivite layer 2
tcpdump -i vlan0100 -c 5
```

VLAN natif

Le VLAN 112 (administration) est conservé comme VLAN natif (*untagged*) sur le trunk. Les trames du VLAN 112 circulent donc sans tag 802.1Q, ce qui assure la rétrocompatibilité : les postes et équipements non reconfigurés continuent d'accéder au réseau sans interruption.

5 Vérification

Vérification

Après création de chaque VLAN, vérifier systématiquement :

Interface et adressage

- ☐ **Le VLAN apparaît dans Interfaces → Périphériques → VLAN**
- ☐ **L'interface est assignée et activée (`Status : up`)**
- ☐ **L'adresse IP de la passerelle est correcte (`10.0.100.1/24`)**
- ☐ **Le masque du LAN a été réduit de `/16` à `/24`**

Connectivité

- ☐ **Depuis un poste du VLAN, `ping 10.0.100.1` répond (passerelle)**
- ☐ **La résolution DNS fonctionne (`nslookup bts.sio 10.0.112.10`)**
- ☐ **L'accès Internet fonctionne si autorisé par les règles**

Filtrage

- ☐ **Le trafic autorisé par les règles passe effectivement**
- ☐ **Le trafic non autorisé est bien bloqué (tester avec `telnet` ou `Test-NetConnection`)**
- ☐ **Les logs du pare-feu (Pare-feu → Journal → Temps réel) confirment les blocages attendus**
- ☐ **L'alias `Open_Bar` ne contourne pas le cloisonnement**

DHCP

- ☐ **Un poste du VLAN obtient une adresse dans la plage configurée**
- ☐ **La passerelle et les serveurs DNS reçus sont corrects**

6 Dépannage

Problème	Solution
Pas de connectivité dans le VLAN	Vérifier que l'interface est activée (**Interfaces** → [**nom**]). Contrôler la configuration trunk du switch (le VLAN doit être *tagged* sur le port). S'assurer que le masque LAN a été réduit à `/24`.
Ping vers la passerelle OK, mais pas de routage inter-VLAN	Vérifier les règles de filtrage sur l'interface source : par défaut tout est bloqué. Consulter le journal temps réel (**Pare-feu** → **Journal**) pour identifier la règle qui bloque.
DHCP ne distribue pas d'adresses	Si relai DHCP : vérifier que le serveur DHCP Windows possède un scope pour le sous-réseau du VLAN. Vérifier que les règles de filtrage autorisent le trafic DHCP (ports 67/68 UDP) entre le VLAN et les DCs.
Perte d'accès à l'interface web après modification du masque LAN	Accéder à la console physique du pare-feu. Utiliser l'option 2 du menu console (*Set interface(s) IP address*) pour reconfigurer l'adresse LAN.
Le trafic inter-VLAN passe malgré les règles de blocage	Vérifier que l'alias `Open_Bar` n'autorise pas un trafic non souhaité. Contrôler l'ordre des règles : une règle PASS placée avant un BLOCK prend le dessus.

7 Voir aussi

— **MO-NET-001** — Vérification post-hardening OPNsense (contrôle après intervention)
— **MO-NET-002** — Mise à jour du firmware OPNsense (maintenir le pare-feu à jour)
— **MO-NET-003** — Configuration des VLANs sur switches Aruba 1930 (complément indispensable : la création des VLANs et la configuration des trunks 802.1Q côté switches, préalable à la présente procédure)
— **MO-AD-001** — Administration distante des contrôleurs de domaine (accès WinRM pour le DHCP)
— Documentation OPNsense : *Virtual LANs* (`https://docs.opnsense.org/manual/vlans.html`)