Refonte et sécurisation de l’infrastructure réseau – Mise en place VLAN, pfSense et services associés

---

Analyse du besoin

Contexte général

Je travaille pour l'ESN WildCorp, nouvellement choisie pour accompagner EcoSolar Solutions dans la modernisation de son système d'information. Cette entreprise toulousaine fabrique des panneaux solaires haute performance et connaît une croissance importante, ce qui met en évidence les limites de son infrastructure informatique actuelle, vieillissante, peu sécurisée et majoritairement hébergée sur site.

Ma mission consiste à participer à la refonte complète de cette infrastructure : améliorer la sécurité, moderniser le réseau, faciliter les accès distants, renforcer la protection des

données sensibles et préparer l'hébergement des services dans une baie nouvellement louée dans un datacenter à Marseille.

Dans ce projet mené en mode Agile/Scrum, je dois concevoir, tester et documenter des solutions techniques adaptées, tout en respectant les bonnes pratiques de sécurité et les besoins stratégiques d'EcoSolar Solutions.

Contexte technique initial

Actuellement, l'entreprise ne possède aucune solution de redondance au sein de son infrastructure : elle fonctionne uniquement avec des points de défaillance uniques (SPOF). Cette situation rend toute panne potentielle extrêmement critique pour la production. L'objectif est donc de mettre en place une redondance au niveau de Proxmox, des firewalls et des switches, afin d'assurer la continuité des services essentiels et de garantir un fonctionnement stable même en cas d'incident.

État initial du réseau

Élément	Description
Adresse réseau	192.168.128.0/24 (classe C unique)
Switch principal	Cisco 3560 – VLAN par défaut – aucun routage inter-VLAN - Switch Manageable mais accès non sécurisé
Firewall	pfSense SG-2440 – politique permissive « any any »
Wi-Fi	WPA2, un seul SSID pour tous les utilisateurs
Hyperviseur	Proxmox VE – plusieurs VM critiques : AD, ERP, GLPI, mail, téléphonie
Serveurs	Aucun cluster, stockage non redondé, pas d'onduleur
Datacenter	Baie 42U vide, IPv4 /30 fournie, prêt pour PRA
Problèmes constatés	Absence totale de segmentation, risque cyber élevé, single point of failure, performances limitées, aucune supervision

Identification du besoin

EcoSolarSolutions souhaite moderniser son infrastructure réseau afin d'accompagner sa croissance et de renforcer la sécurité de ses données sensibles.
Actuellement, l'ensemble des équipements de l'entreprise — postes utilisateurs, serveurs, tablettes industrielles, smartphones, imprimantes — fonctionne sur un **seul réseau local non segmenté (192.168.128.0/24)**, connecté à un **unique switch Cisco 3560** configuré avec le VLAN par défaut.

Le Wi-Fi interne utilise également ce même réseau, et le firewall pfSense laisse sortir et entrer le trafic sans filtrage spécifique ("permit all").
Cette architecture provoque un manque de sécurité, une absence d'isolation entre les

services sensibles (production, administratif, R&D), ainsi qu'une difficulté à absorber la montée en charge prévue.

La direction souhaite donc engager une refonte complète : **création de VLAN**, durcissement des accès, modernisation de l'infrastructure, et mise en place d'un schéma directeur réseau cohérent.
Une étude d'impact doit être menée afin d'anticiper les conséquences sur la connectivité, la sécurité, la performance et la maintenance globale du SI.

Objectifs de la réorganisation

Objectif	Description
Renforcer la sécurité globale	Segmenter le réseau afin d'isoler les services sensibles (R&D, Direction, SI) et limiter les risques d'accès non autorisés.
Sécuriser les accès distants	Mettre en place des solutions d'accès VPN chiffrées pour les commerciaux et collaborateurs itinérants.
Optimiser les performances du réseau	Réduire le trafic de broadcast et améliorer la qualité de service des applications critiques (ERP, messagerie, fichiers).
Préparer l'intégration du datacenter	Adapter la structure réseau pour faciliter l'interconnexion sécurisée entre le site de Toulouse et la baie du datacenter de Marseille.
Faciliter la maintenance et la supervision	Clarifier l'architecture via des VLAN dédiés, améliorer la visibilité des équipements et intégrer une supervision centralisée.
Améliorer la résilience et la disponibilité	Mettre en place une politique de sauvegarde, un début de PRA/PCA et sécuriser l'alimentation via onduleurs.
Préparer l'évolution des services	Prévoir l'ajout futur de nouveaux serveurs, d'un hébergement web interne, et d'un réseau Wi-Fi invité isolé.

Rapport d'étude d'impact réseau

Équipements concernés

- Cisco 3560 → configuration VLAN + trunk + routage inter-VLAN (si L3 activé).
- pfSense → création des interfaces logiques + ACL + VPN.
- Proxmox → réorganisation du bridge réseau + séparation trafic management / VM.
- Point d'accès Cisco C9136I → mise en place de plusieurs SSID + VLAN associés.
- Baie Datacenter → préparation de l'interconnexion future (VPN IPsec / tunnel GRE).

Impacts identifiés

Domaine	Impact principal	Détails / Recommandations
Adressage IP	Refonte complète	Changement d’adresses sur toutes les VM et les équipements.
Routage	Ajout inter-VLAN	Configuration des sous-interfaces ou routage L3 du switch.
DHCP	Plusieurs pools	Un pool par VLAN, réservations pour serveurs & téléphonie.
Wi-Fi	Séparation flux	3 SSID : corporate, prod, guest. Filtrage par pfSense.
Sécurité	Durcissement	ACL inter-VLAN, firewall restrictif, suppression règle any-any.
Accès distants	Mise en place VPN	Accès sécurisés pour commerciaux → OpenVPN/IPsec.
Datacenter	Préparation PRA	Nécessite un routeur, tunnel VPN, réplication future.
Production	Risque coupure	Planification migration hors production (soir / week-end).

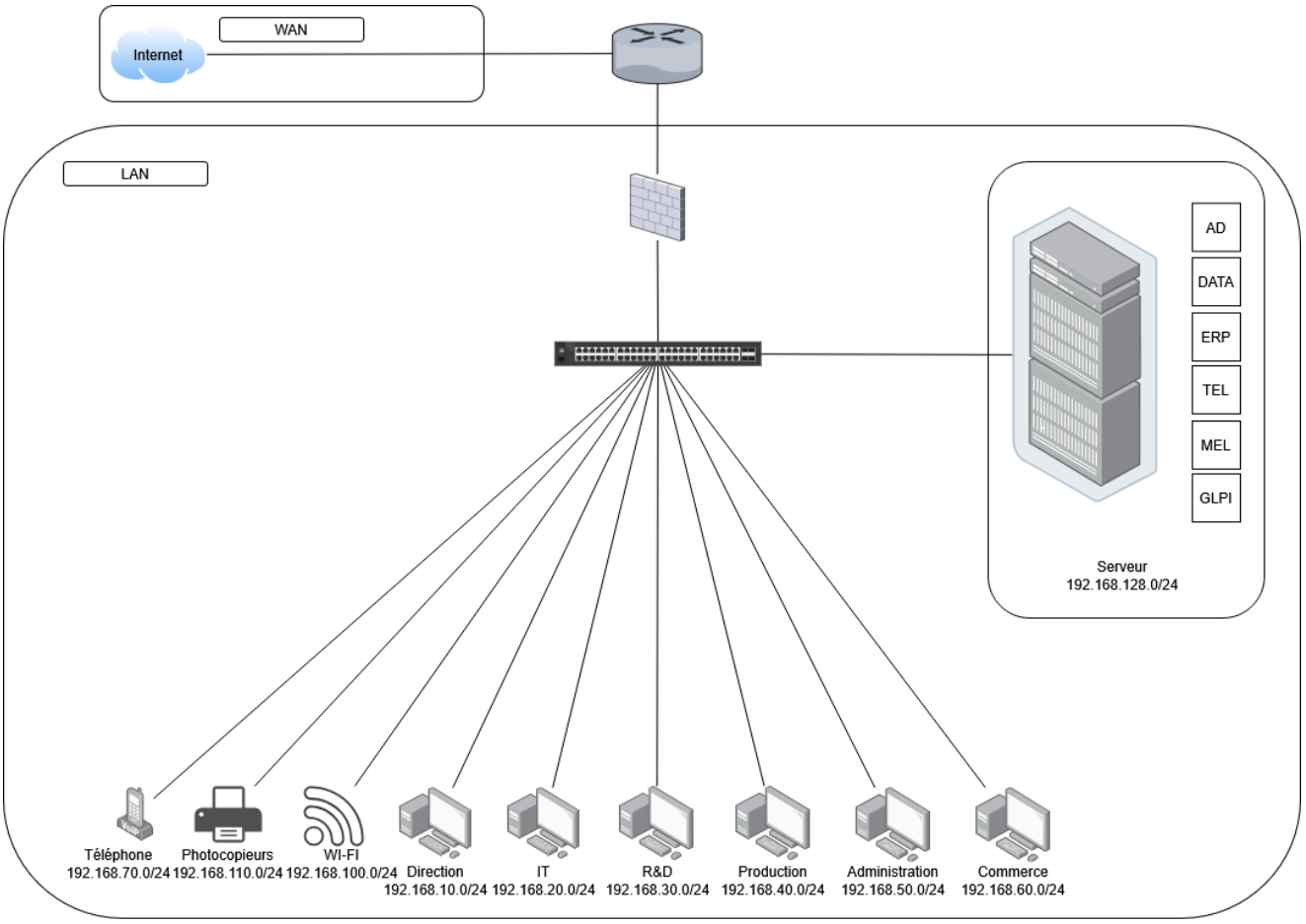
Bénéfices attendus

Domaine	Bénéfice
Performance	Isolement des flux, stabilité accrue.
Sécurité	Réduction drastique de la surface d’attaque.
Disponibilité	Préparation PRA/PCA → réduction temps d'arrêt.
Maintenance	Diagnostic facilité par segmentation cohérente.
Évolutivité	Ajout futur de serveurs, VLAN et services simplifié.
Conformité	Alignement avec les bonnes pratiques ANSSI & RGPD.

Conception

---

4. Architecture cible proposée



Nouveau plan d’adressage

VLAN	USAGE	Sous-réseau	Passerelle	nombre de poste	Description
1	Par défaut	192.168.1.0/24	192.168.1.254	/	Réseau principal nor segmenté
10	Direction	192.168.10.0/24	192.168.10.254/24	2	Accès réserv à la directior
20	IT	192.168.20.0/24	192.168.20.254/24	2	Gestion du parc informatique
30	R&D	192.168.30.0/24	192.168.30.254/24	3	Environnem de tests et développem
40	Production	192.168.40.0/24	192.168.40.254/24	7	Réseau déd aux postes d production
50	Administration	192.168.50.0/24	192.168.50.254/24	5	Services administratif
60	Commerce	192.168.60.0/24	192.168.60.254/24	7	Postes du service

VLAN	USAGE	Sous-réseau	Passerelle	nombre de poste	Description
					commercial
70	Téléphone	192.168.70.0/24	192.168.70.254/24	/	Réseau VoIP dédié
80	Sauvegarde	192.168.80.0/24	192.168.80.254/24	3	Système de sauvegarde NAS
90	Monitoring	192.168.90.0/24	192.168.90.254/24	/	Supervision surveillance réseau
100	Wifi	192.168.100.0/24	192.168.100.254/24	/	Réseau sans fil pour utilisateurs
110	Photocopieurs	192.168.110.0/24	192.168.110.254/24	2	Réseau déd aux imprimantes salles
128	Serveur	192.168.128.0/24	192.168.128.254/24	2	Hébergemer des serveurs internes

Organisation des VLAN

VLAN	USAGE	Sous-réseau	Passerelle	nombre de poste	Des
1	Par défaut	192.168.1.0/24	192.168.1.254	/	Rés prin segr
10	Direction	192.168.10.0/24	192.168.10.254/24	2	Acc à la
20	IT	192.168.20.0/24	192.168.20.254/24	2	Ges parc infor
30	R&D	192.168.30.0/24	192.168.30.254/24	3	Envi de te déve
40	Production	192.168.40.0/24	192.168.40.254/24	7	Rés aux proc

VLAN	USAGE	Sous-réseau	Passerelle	nombre de poste	Des
50	Administration	192.168.50.0/24	192.168.50.254/24	5	Serv adm
60	Commerce/Accueil	192.168.60.0/24	192.168.60.254/24	7	Post serv com
70	Téléphone	192.168.70.0/24	192.168.70.254/24	/	Rés dédi
80	Sauvegarde	192.168.80.0/24	192.168.80.254/24	3	Syst sauv NAS
90	Monitoring	192.168.90.0/24	192.168.90.254/24	/	Sup surv rése
100	Wifi	192.168.100.0/24	192.168.100.254/24	/	Rés fil pc utilis
110	Photocopieurs/réunion	192.168.110.0/24	192.168.110.254/24	2	Rés aux impr salle
128	Serveur	192.168.128.0/24	192.168.128.254/24	2	Héb des inter

Serveur : on change rien pour éviter le changement d'IP des VM installé sur le serveur.

Ports	Etat	Mode	VLAN	Description
G0/0		Trunk	120	VERS_FIREWALL
G0/1			50	ADMIN
G0/2			10	DIRECTION
G0/3			20	IT
G1/0			30	R&D
G1/1			40	PRODUCTION
G1/2			60	COMMERCE
G1/3	Shutdown			
G2/0	Shutdown			
G2/1	Shutdown			

Ports	Etat	Mode	VLAN	Description
G2/2	Shutdown			
G2/3	Shutdown			
G3/0	Shutdown			
G3/1	Shutdown			
G3/2				PROXMOX
G3/3				WI-FI

Mise en œuvre

Configuration du switch

1. Renommage du switch

Je renomme le switch.

Switch>en
Switch#conf t

Puis je change le nom :

```
Switch(config)#hostname SW1
SW1(config)#
```

À chaque étape :

- `exit`
- `wr` pour enregistrer

---

2. Création des VLAN

Création des VLAN d'après mon tableau :

```
SW1(config-vlan)#
SW1(config-vlan)#vlan 70
SW1(config-vlan)#
SW1(config-vlan)#name TELEPHONE
SW1(config-vlan)#
SW1(config-vlan)#vlan 80
SW1(config-vlan)#
SW1(config-vlan)#name  SAUVEGARDE
SW1(config-vlan)#
SW1(config-vlan)#vlan 90
SW1(config-vlan)#
SW1(config-vlan)#name MONITORING
SW1(config-vlan)#
SW1(config-vlan)#vlan 100
SW1(config-vlan)#
SW1(config-vlan)#name WIFI
SW1(config-vlan)#
SW1(config-vlan)#vlan 110
SW1(config-vlan)#
SW1(config-vlan)#name PHOTOCOPIEUR
SW1(config-vlan)#
SW1(config-vlan)#vlan 128
SW1(config-vlan)#
SW1(config-vlan)#name  SERVEUR
SW1(config-vlan)#
SW1(config-vlan)#exit
```

Vérification de la création :

```
SW1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gi0/0, Gi0/1, Gi0/2, Gi0/3
                                                 Gi1/0, Gi1/1, Gi1/2, Gi1/3
                                                 Gi2/0, Gi2/1, Gi2/2, Gi2/3
                                                 Gi3/0, Gi3/1, Gi3/2, Gi3/3
10   DIRECTION                         active
20   IT                                active
30   R&D                               active
40   PRODUCTION                        active
60   COMMERCE                          active
70   TELEPHONE                         active
80   SAUVEGARDE                        active
90   MONITORING                        active
100  WIFI                              active
110  PHOTOCOPIEUR                      active
128  SERVEUR                           active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

---

3. Attribution des ports aux VLAN

Configuration du trunk (vers firewall)

Je mets l'interface `g0/0` en mode trunk :

```
SW1(config)#interface g0/0
SW1(config-if)#
SW1(config-if)#swi
SW1(config-if)#switchport mode t
SW1(config-if)#switchport mode trunk
```

SW1(config-if)#switchport trunk allowed vlan 1,10,20,30,40,50,60,120

Vérification :

```
SW1#show interfaces g0/0 switchport
Name: Gi0/0
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 1,10,20,30,40,50,60,70,80,90,100,110,120,128
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

Accès PROXMOX

Même configuration :

```
SW1(config)#
SW1(config)#interf
SW1(config)#interface g3/2
SW1(config-if)#
SW1(config-if)#swit
SW1(config-if)#switchport tr
SW1(config-if)#switchport trunk
SW1(config-if)#switchport en
SW1(config-if)#switchport enc
SW1(config-if)#switchport t
SW1(config-if)#switchport trunk e
SW1(config-if)#switchport trunk encapsulation do
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#
SW1(config-if)#switchport mode t
SW1(config-if)#switchport mode trunk
SW1(config-if)#
SW1(config-if)#switchport mode trunk am
SW1(config-if)#switchport mode trunk al
SW1(config-if)#switchport t
SW1(config-if)#switchport trunk a
SW1(config-if)#switchport trunk allowed vla
SW1(config-if)#switchport trunk allowed vlan 50,70,80,90,128
```

Ports en accès

Configuration type :

interface g0/1
switchport mode acces
switchport acces vlan 10
description DIRECTION

```
SW1#show interfaces g3/2 switchport
Name: Gi3/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 50,70,80,90,128
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/3, Gi2/0, Gi2/1, Gi2/2
                                                Gi2/3, Gi3/0, Gi3/1, Gi3/2
                                                Gi3/3
10   DIRECTION                        active    Gi0/2
20   IT                               active    Gi0/3
30   R&D                              active    Gi1/0
40   PRODUCTION                       active    Gi1/1
50   ADMINISTRATION                   active    Gi0/1
60   COMMERCE                         active    Gi1/2
```

Sécurisation des ports inutilisés

SW1(config)#interface g3/1
SW1(config-if)#shutdown
SW1(config-if)#exit

---

4. Sécurisation des accès

Mot de passe

SW1(config)#enable password ChangeMe123!
SW1(config)#service password-encryption

Accès SSH

SW1(config)#username admin password ChangeMe123!
SW1(config)#line vty 0 4
SW1(config-line)#login local

Adresse IP de gestion

SW1(config)#interface g0/1
SW1(config-if)#ip adresse 192.168.50.10 255.255.255.0

Mise en place de SSH sur le switch

Configuration de base

Mot de passe privilégié

(config)# enable password ChangeMe123!
(config)# enable password-encryption

Interface VLAN

(config)# interface vlan 1
(config-if)# ip address 192.168.128.250 255.255.255.0
(config-if)# no shutdown

Hostname

(config)# hostname SW01

Nom de domaine

(config)# ip domain-name exosolarsolutions.local

Configuration SSH

Génération clé RSA

(config)# crypto key generate rsa

Version SSH

(config)# ip ssh version 2

Utilisateur

(config)# username admin password ChangeMe123!

Accès distants (VTY)

(config)# line vty 0 4
(config-line)# transport input ssh
(config-line)# login local
(config-line)# exec-timeout 5 0
(config-line)# logging synchronous

Sécurisation

Blocage après échecs

(config)# login block-for 120 attempts 3 within 60

Paramètre	Signification
block-for 120	Bloque les connexions pendant 120 secondes
attempts 3	Après 3 échecs
within 60	Sur une période de 60 secondes

Timeout SSH

(config)# ip ssh time-out 60

Problème d'algorithmes SSH

Certaines versions IOS utilisent des algorithmes obsolètes → échec de négociation.

Vérification côté client

ssh -vvv admin@192.168.128.250

Script de connexion SSH

Création

nano Bureau/ssh_SW01.sh

Contenu

#!/bin/bash

ssh \
-oKexAlgorithms=+diffie-hellman-group14-sha1 \
-oHostKeyAlgorithms=+ssh-rsa \
-oPubkeyAcceptedAlgorithms=+ssh-rsa \
admin@192.168.128.250

Permissions

chmod +x Bureau/ssh_SW01.sh

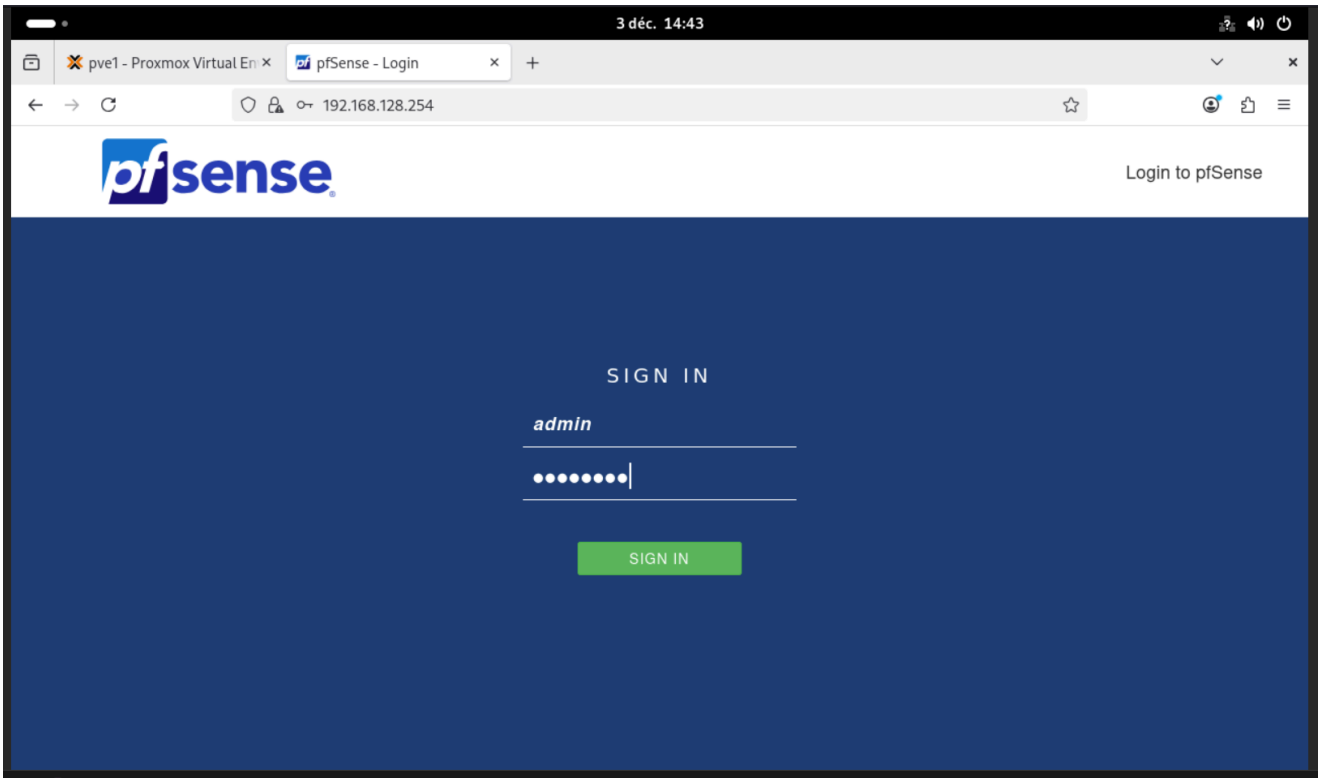
Exécution

./Bureau/ssh_SW01.sh

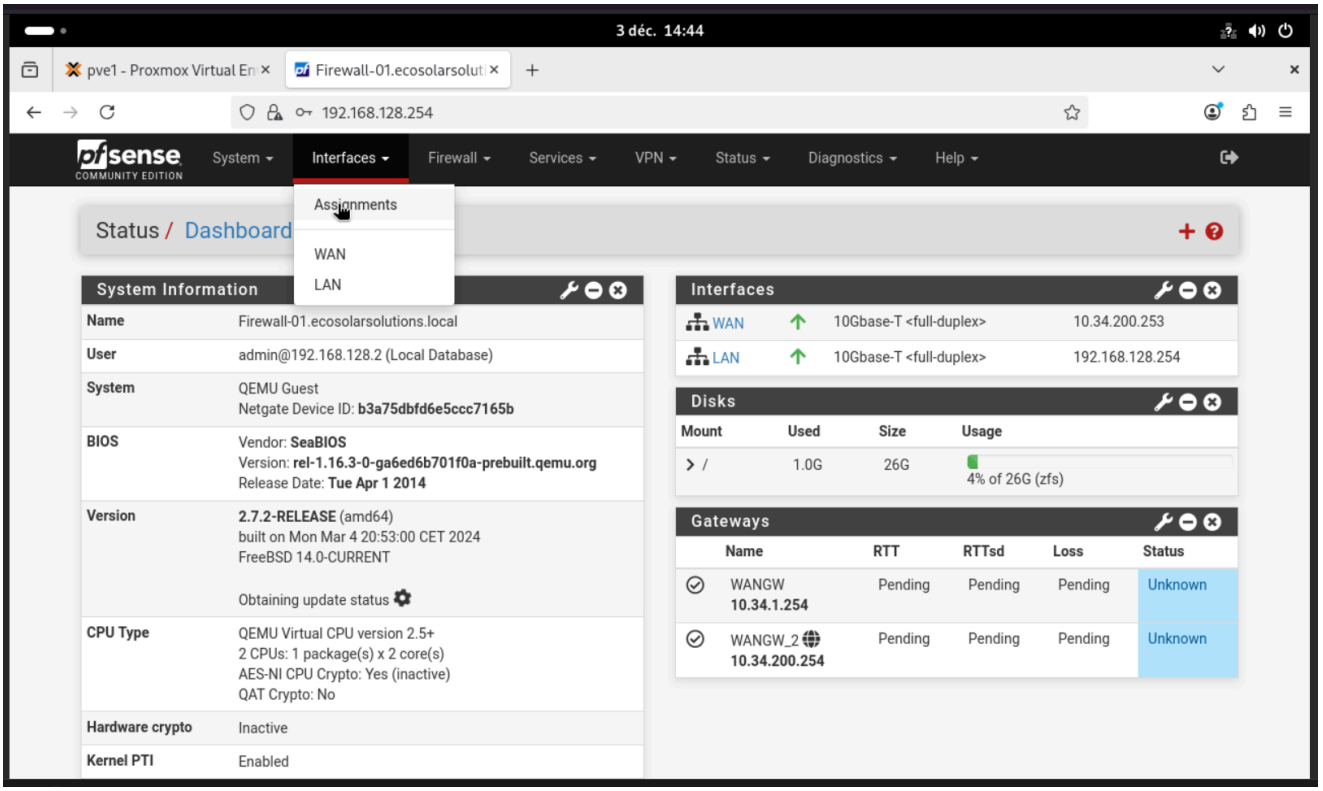
Firewall

Préparation VLAN

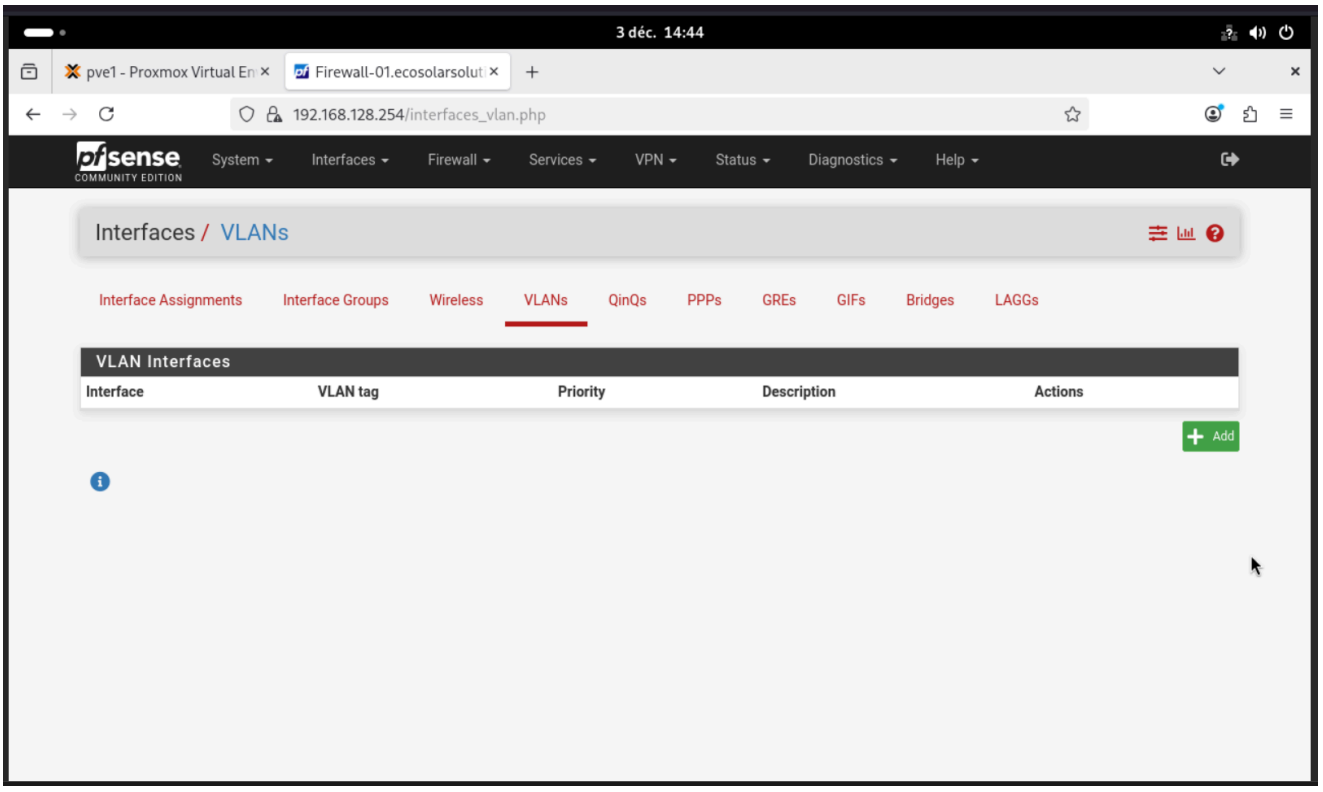
Connexion à Proxmox puis PFsense :



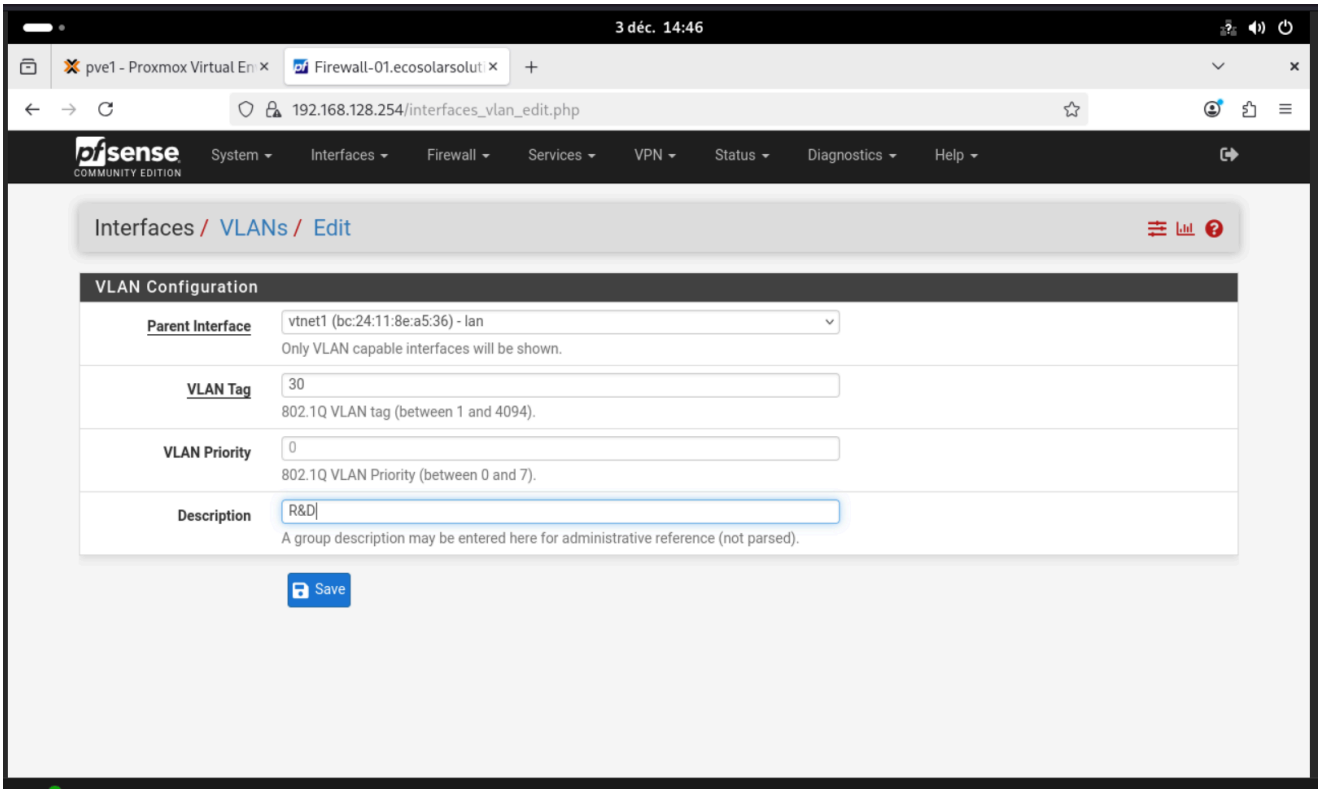
Assignation des interfaces



Création VLAN



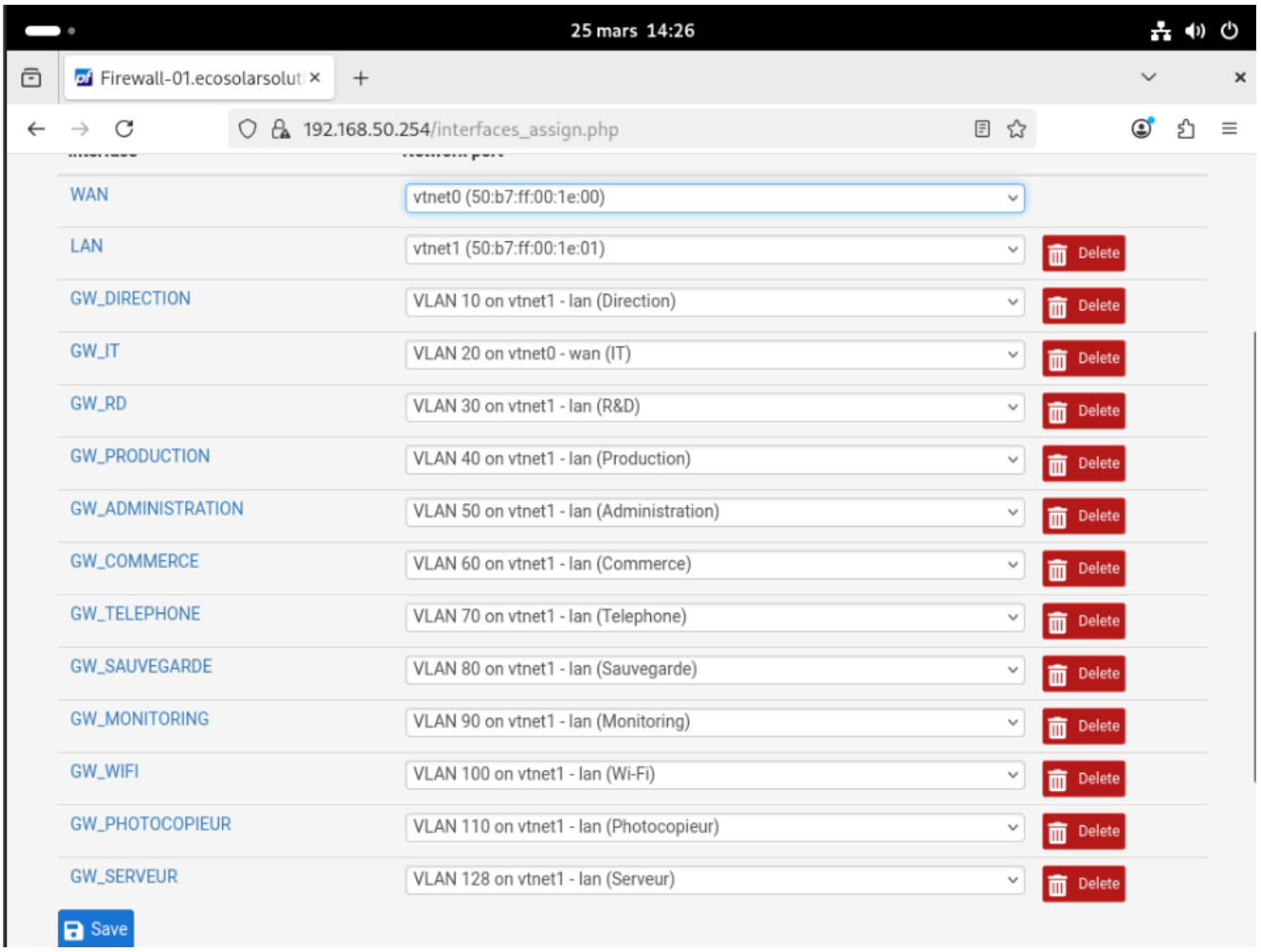
Configuration :



Nommage des interfaces

Convention :

GW_"Nom du réseau"

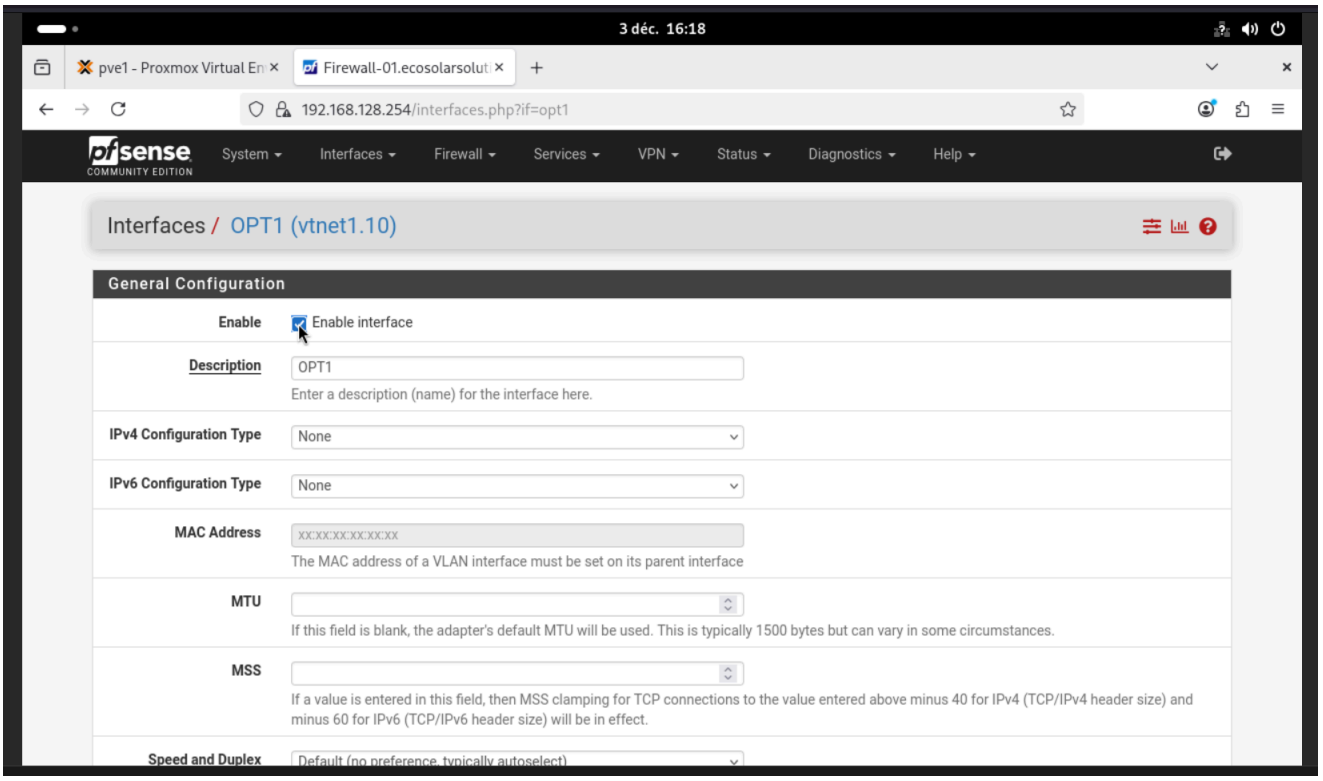


Résultat final

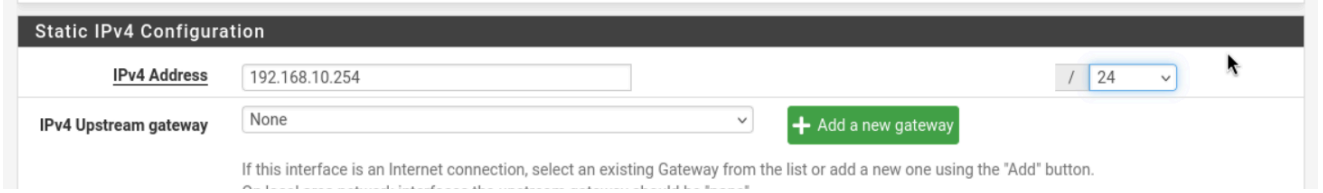
VLAN Interfaces

Interface	VLAN tag	Priority	Description	Actions
vtnet1 (lan)	10		Direction	
vtnet1 (lan)	20		IT	
vtnet1 (lan)	30		R&D	
vtnet1 (lan)	40		Production	
vtnet1 (lan)	50		Administration	
vtnet1 (lan)	60		Commerce	
vtnet1 (lan)	128		Serveurs	
vtnet1 (lan)	70		Tel	
vtnet1 (lan)	80		Sauvegarde	
vtnet1 (lan)	90		Monitoring	
vtnet1 (lan)	100		Wifi	
vtnet1 (lan)	110		Copieurs	

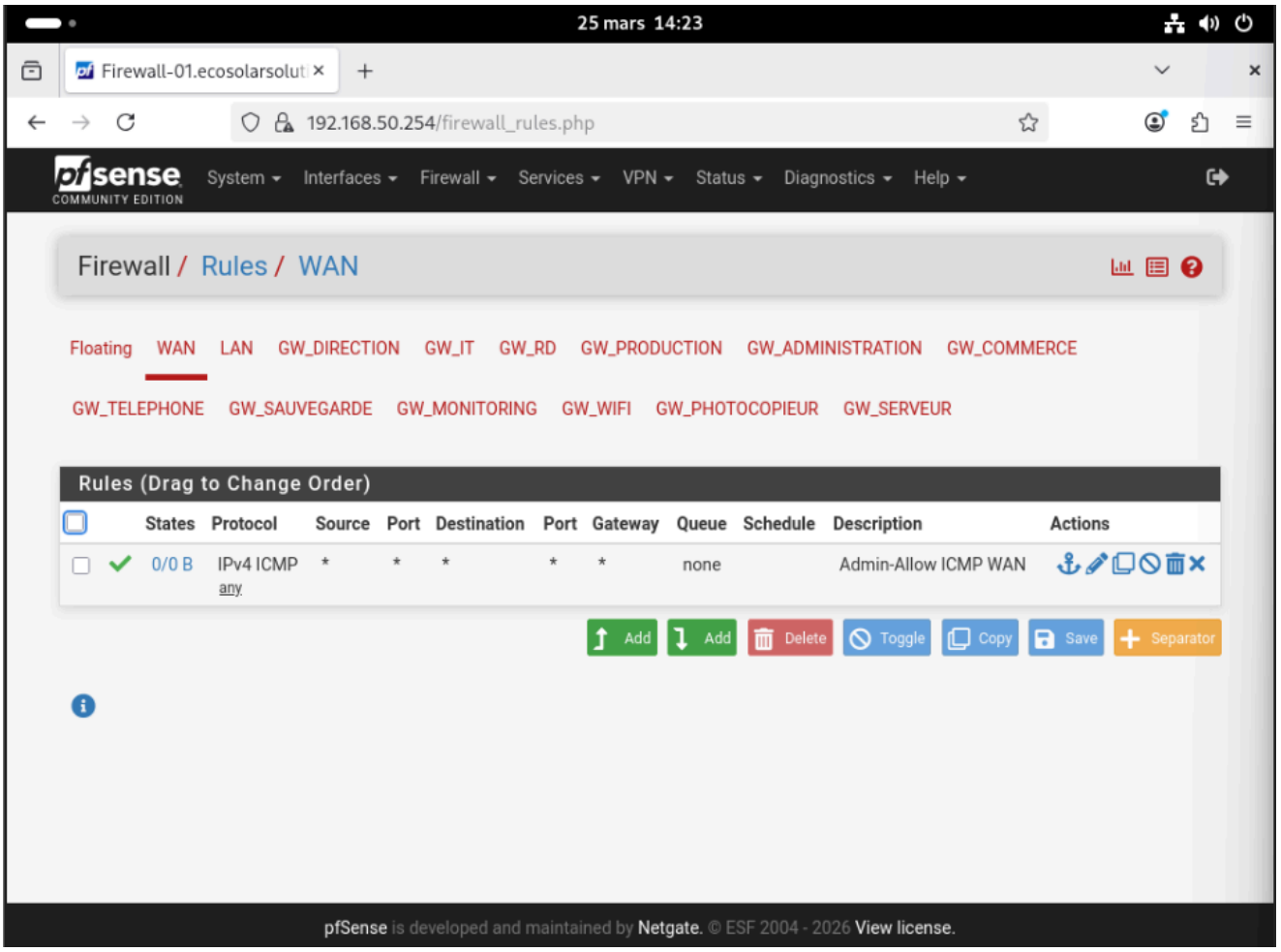
Activation des interfaces



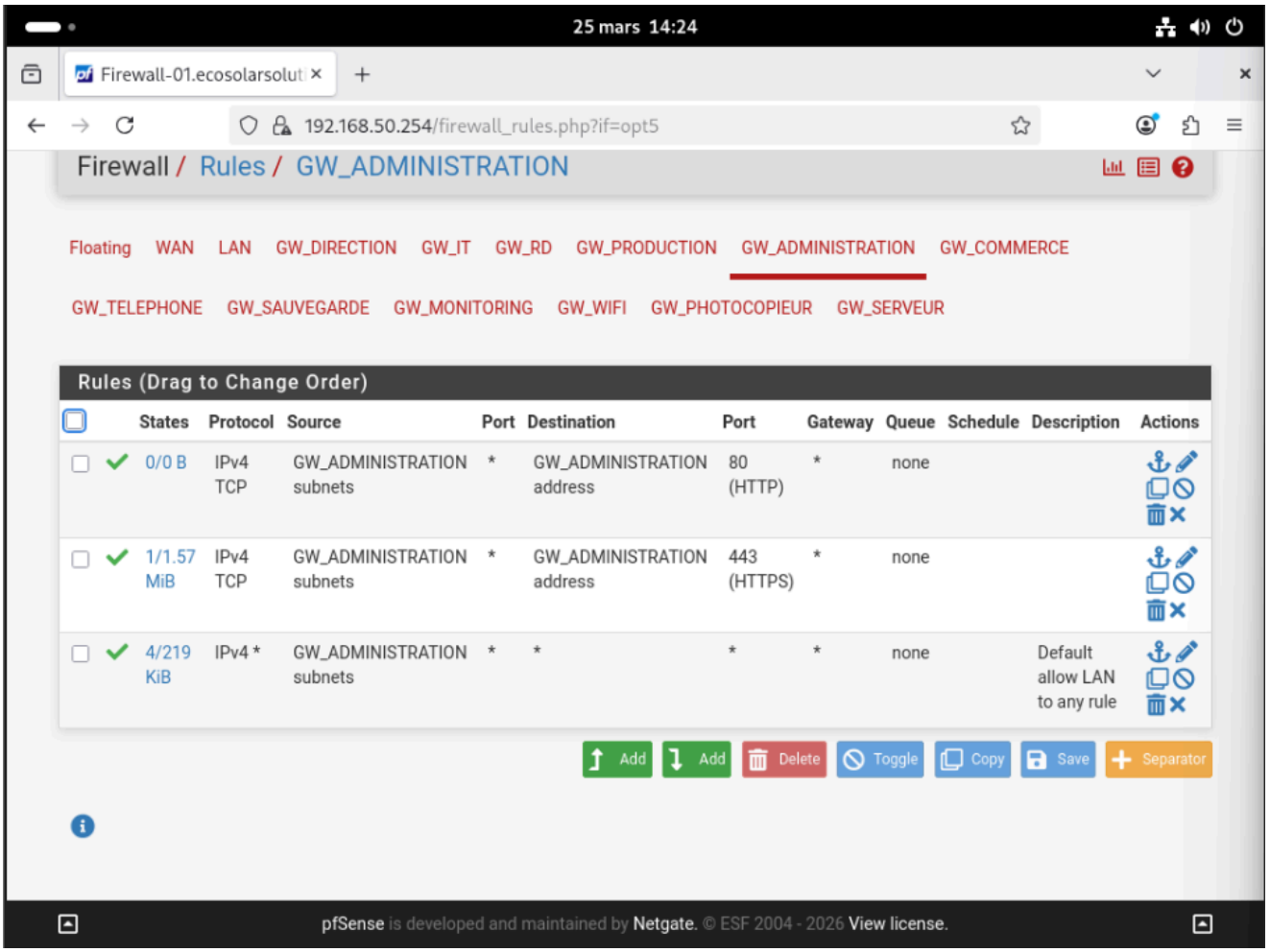
Attribution IP



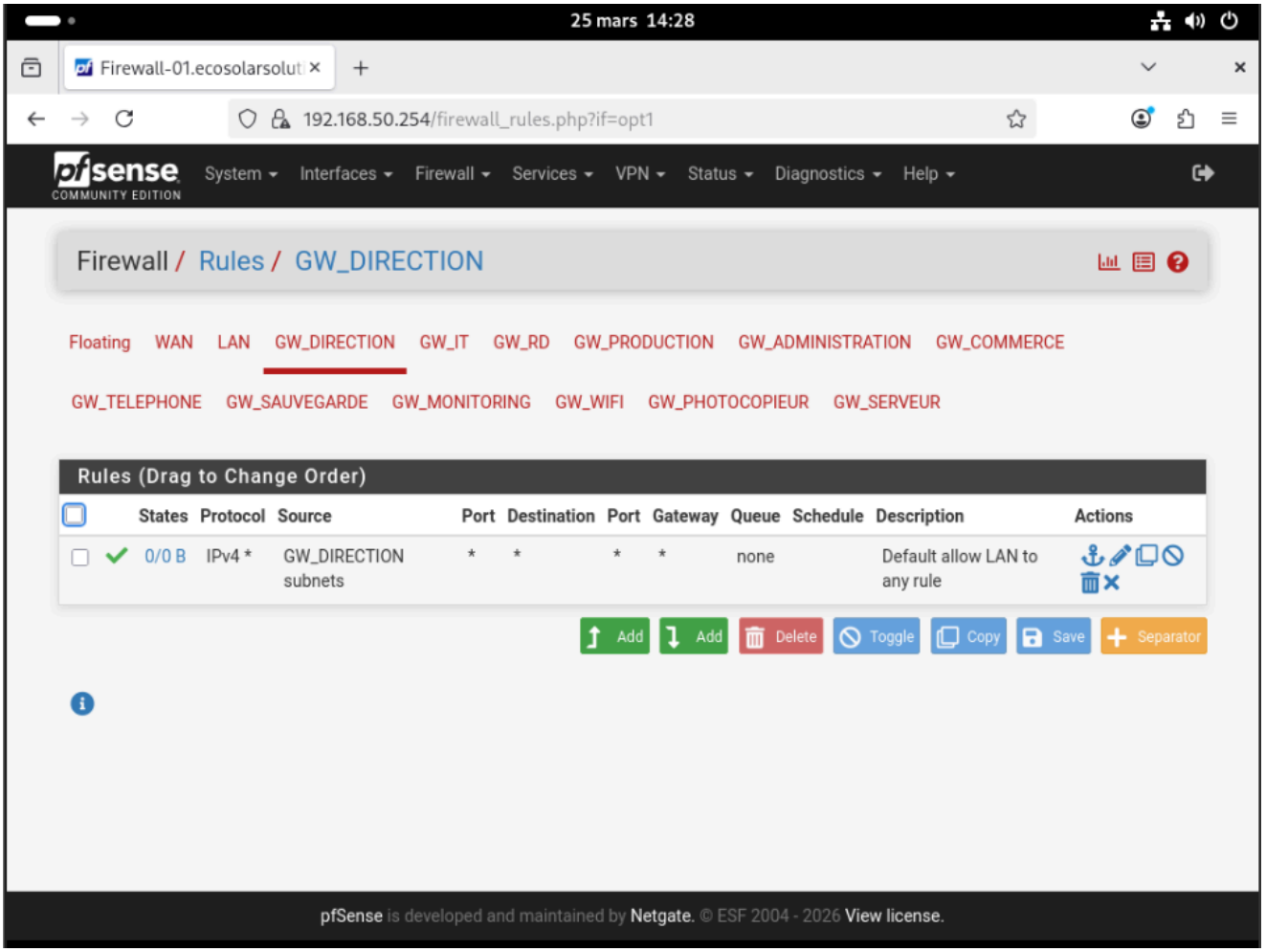
Vérification règles firewall



Règle administration



Configuration temporaire en `any` pour tests :



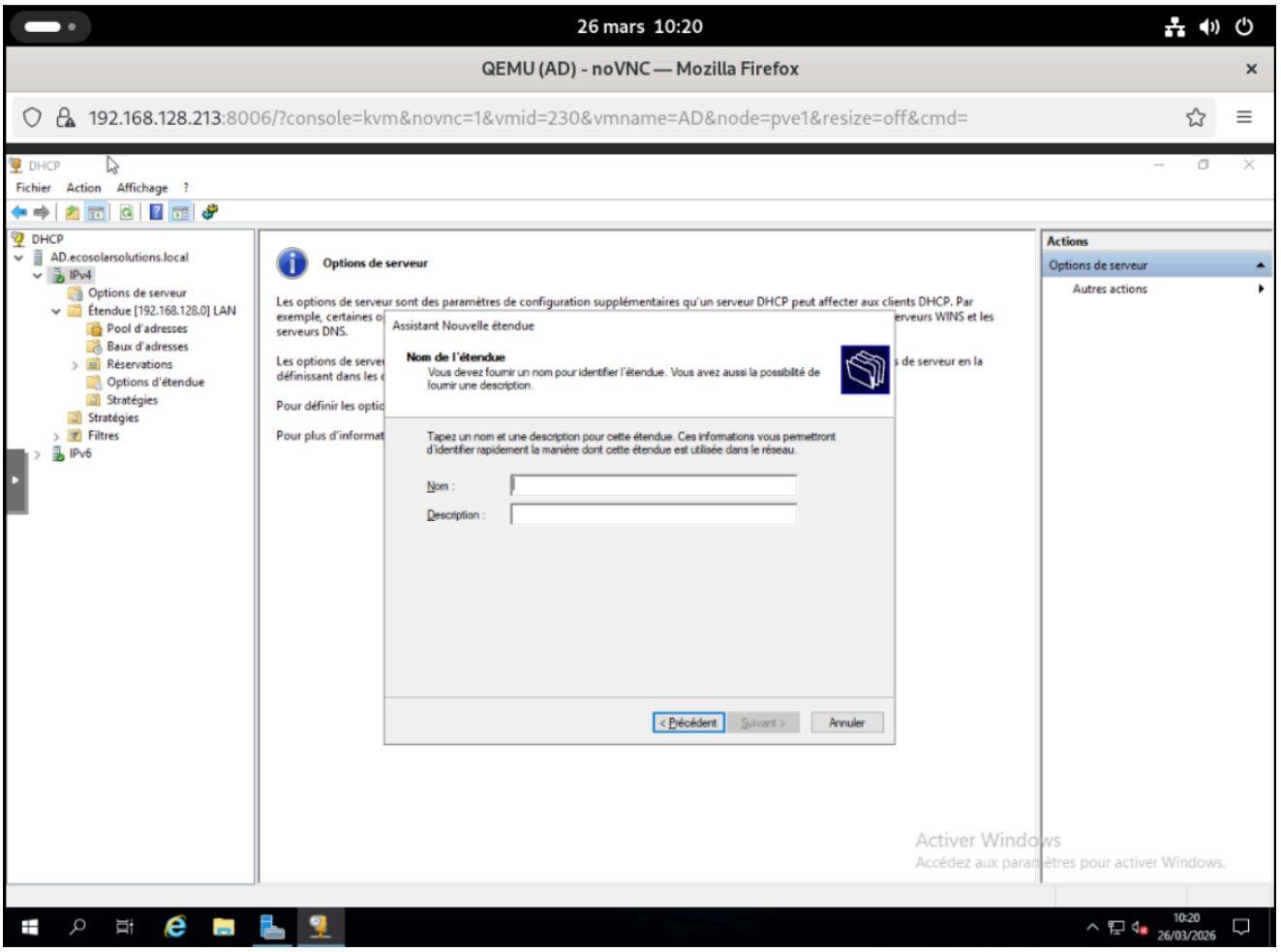
Configuration du DHCP

Configuration des étendues par VLAN :

VLAN	Usage	Étendue
10	Direction	192.168.10.50 - 192.168.10.200
20	IT	192.168.20.50 - 192.168.20.200
30	R&D	192.168.30.50 - 192.168.30.200
40	Production	192.168.40.50 - 192.168.40.200
50	Administration	192.168.50.50 - 192.168.50.200
60	Commerce/Accueil	192.168.60.50 - 192.168.60.200
70	Téléphone	192.168.70.50 - 192.168.70.200
100	Wifi	192.168.100.50 - 192.168.100.200

Configuration côté AD

Connexion à l’AD via Proxmox, puis configuration des étendues en fonction de mon plan d'adressage initial :



Conclusion

La refonte de l'infrastructure réseau réalisée répond directement aux problématiques initiales identifiées, notamment l'absence de segmentation, les failles de sécurité et le manque de résilience.

La mise en place des VLAN a permis de structurer le réseau en isolant les différents services (Direction, IT, Production, Administration, etc.), réduisant ainsi les risques de propagation d'incidents et améliorant la lisibilité globale de l'architecture. Cette segmentation, couplée à la configuration du firewall pfSense, constitue une première étape solide vers un contrôle plus fin des flux réseau.

La sécurisation des équipements, notamment via l'activation du SSH, le chiffrement des mots de passe et le durcissement des accès, corrige des vulnérabilités critiques présentes dans l'infrastructure initiale. Toutefois, certaines configurations, comme les règles firewall en « any », restent volontairement permissives à ce stade pour les phases de test et devront être restreintes en production.

L'intégration du DHCP par VLAN permet également une gestion plus propre et automatisée de l'adressage IP, facilitant l'administration quotidienne et limitant les erreurs humaines.

Malgré ces améliorations significatives, l'infrastructure reste perfectible. Des points importants restent à traiter pour atteindre un niveau de maturité plus élevé :

- mise en place de règles firewall strictes (principe du moindre privilège),
- ajout de mécanismes de redondance (switch, firewall, stockage),
- déploiement d’une supervision réseau,
- sécurisation avancée des accès distants (VPN),
- préparation effective du PRA/PCA.

En l’état, la solution est fonctionnelle, cohérente et nettement plus sécurisée qu’à l’origine, mais elle constitue surtout une base technique solide sur laquelle construire une infrastructure réellement robuste, scalable et conforme aux bonnes pratiques professionnelles.