DOCUMENTATION TP – Sécurisation, Supervision et Services Réseau

I. Mise en place du réseau

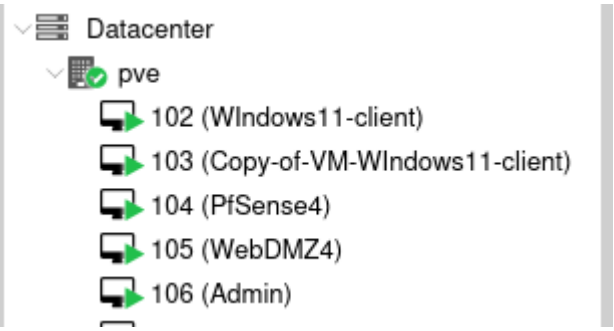
L'objectif est de créer une architecture réseau sécurisée avec pfSense et plusieurs machines virtuelles

Architecture :

```
pfSense connecté à 3 interfaces :

WAN → Internet

LAN → Réseau interne (192.168.1.0/24)

DMZ → Serveur web isolé
```

VMs utilisées :

```
Windows Client (LAN)

Serveur Web Debian (DMZ)

Serveur Logs Debian (LAN)

VM Admin (VLAN Management)
```



II. VLAN Management (VLAN 99 – Management)

Création du VLAN 99

Dans pfSense :

Interfaces → Assignments → VLANs

`VLAN ID : 99`

`Nom : Management`

VM Admin

`VLAN taggé 99`

`IP : 192.168.99.10/24`

`Peut ping : 192.168.99.1 (pfSense Management)`

```
C:\Users\Windows11-client>ping 192.168.99.1

Envoi d'une requête 'Ping'  192.168.99.1 avec 32 octets de données :
Réponse de 192.168.99.1 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
```

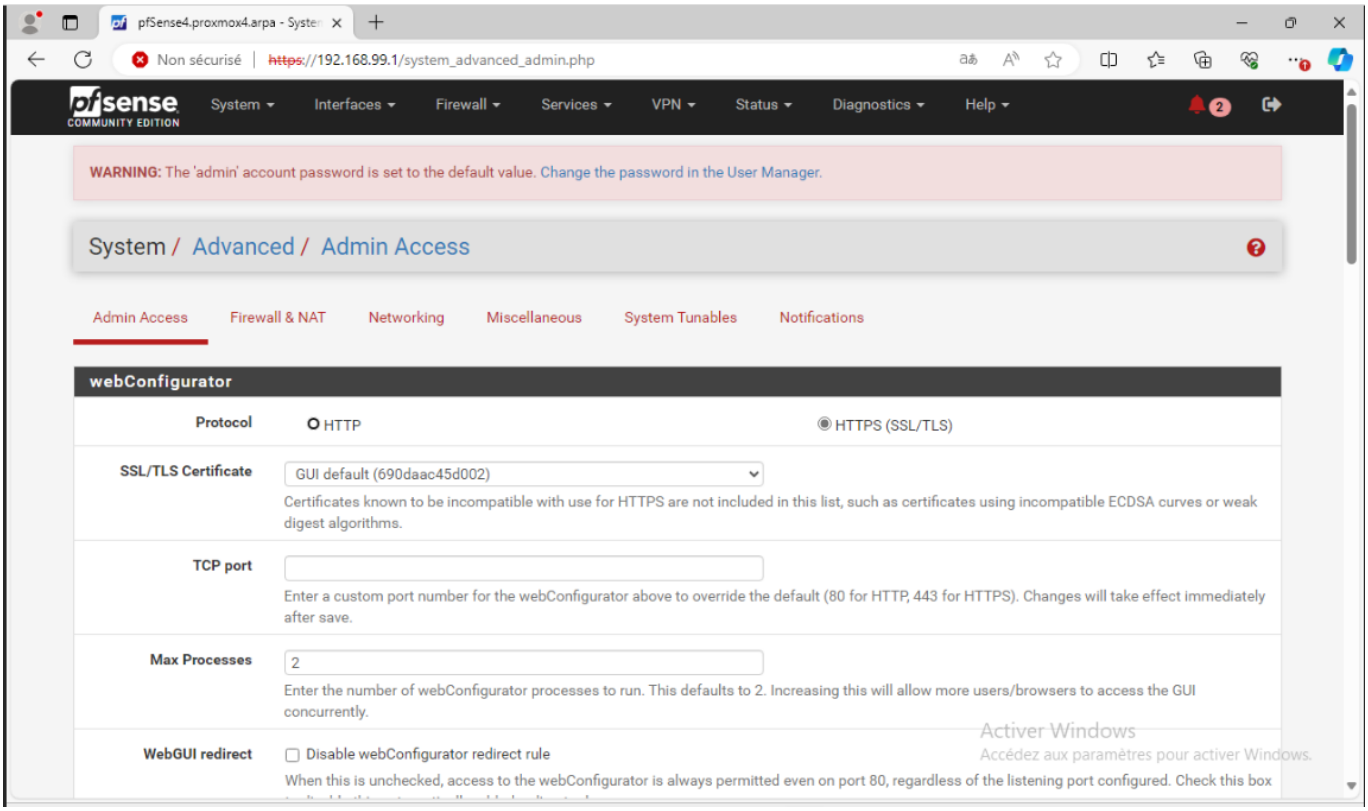
Config

```
C:\Users\Windows11-client>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::3a38:a3bc:44b2:585b%10
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.99.10
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.99.1
```

Sécurisation de l'accès pfSense

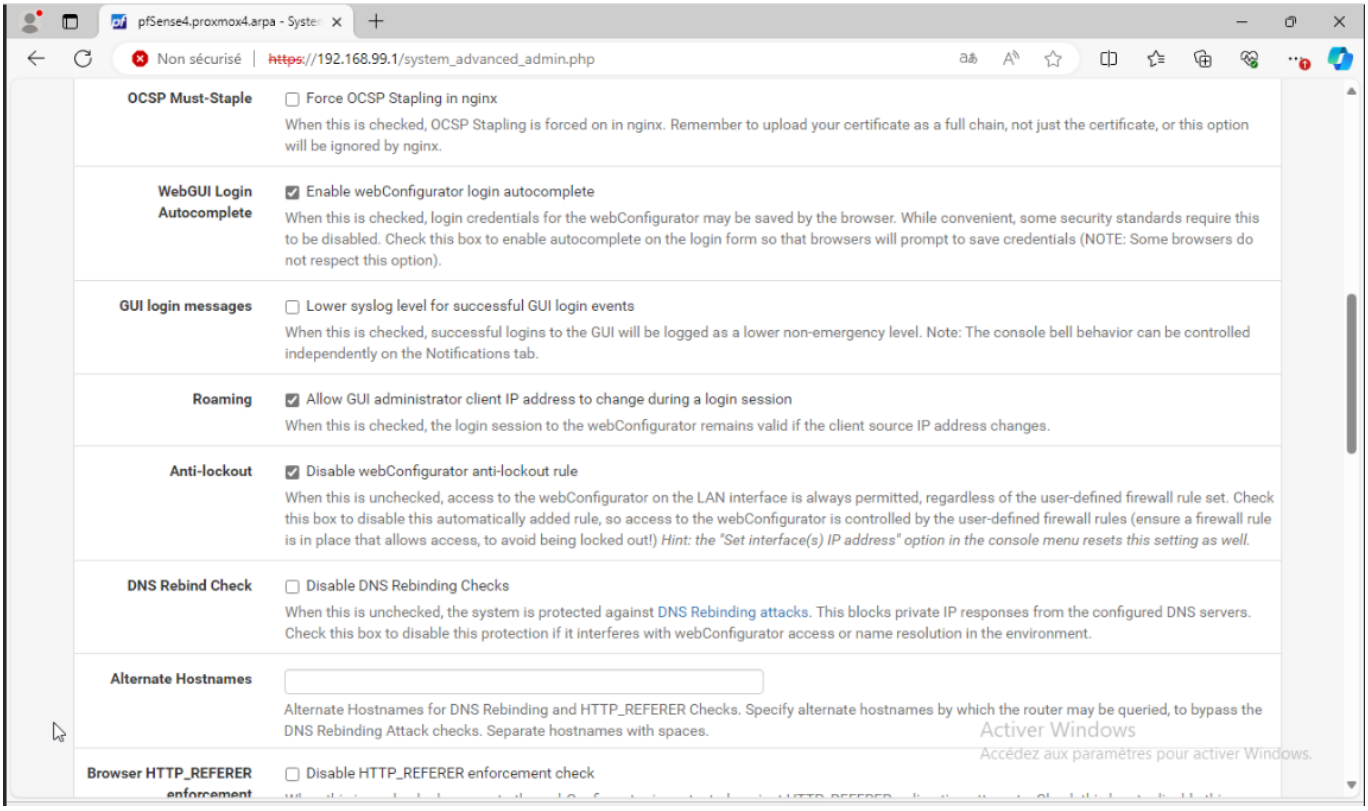
`System → Advanced → Admin Access :`

- Activer HTTPS
- Interface d'écoute : Management
- Désactiver HTTP et SSH ailleurs



Désactiver la règle anti-lockout

Permet d'empêcher le LAN d'accéder à pfSense



II. Durcissement LAN / DMZ

Objectif : limiter les communications entre réseaux

Supprimer la règle LAN → any

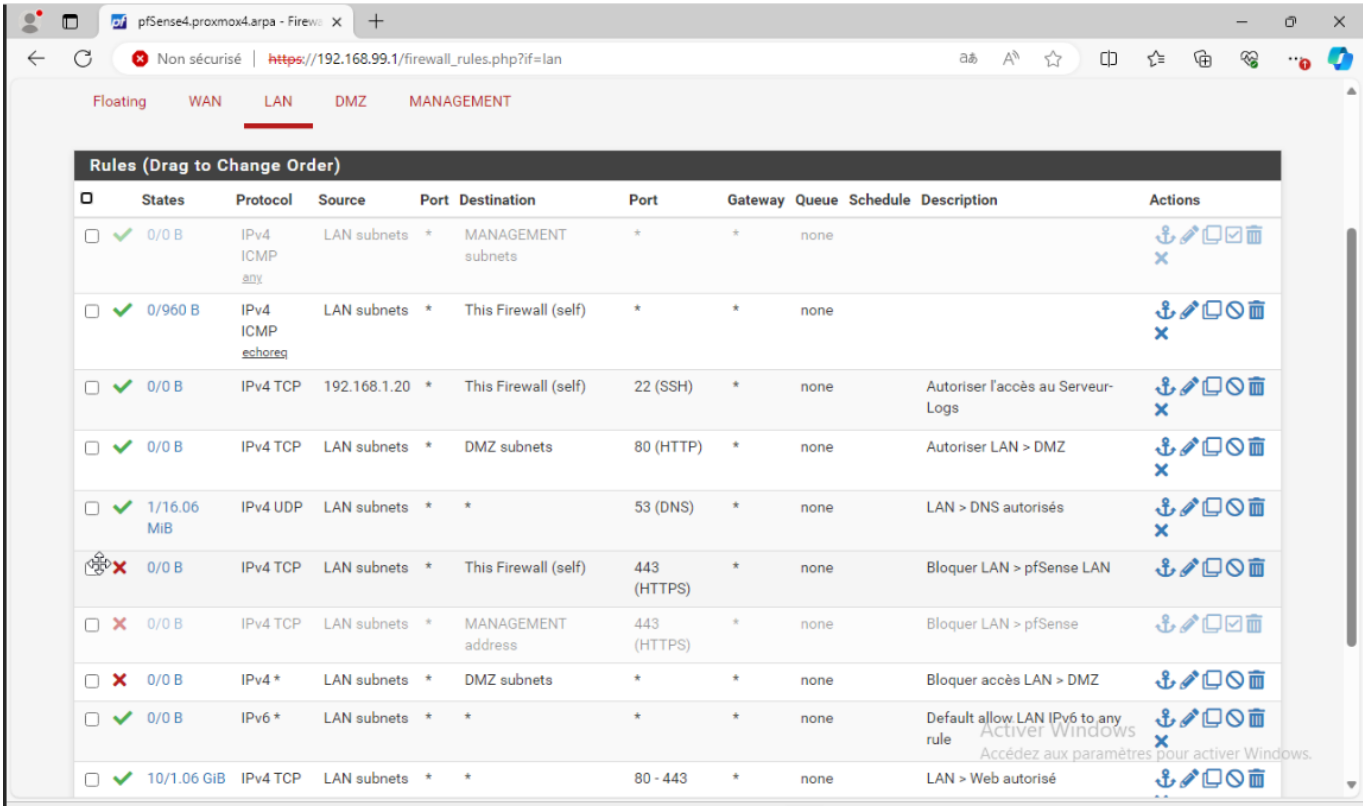
Ajouter les règles nécessaires

- LAN → Internet : ports 80, 443, 53
- LAN → DMZ : port 80
- DMZ → Internet : ports autorisés seulement
- DMZ → LAN : tout bloqué

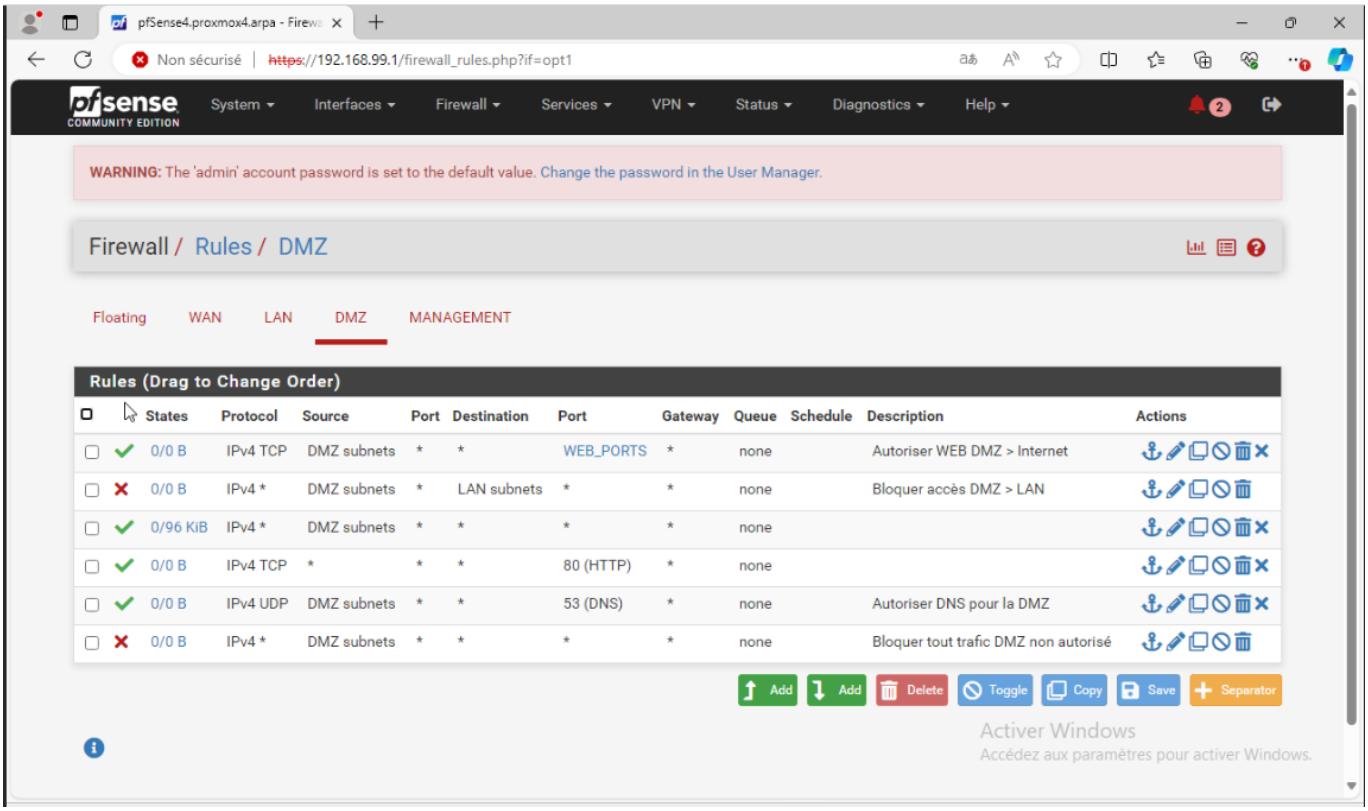
Alias WEB_PORTS

- Contient : 80, 443, 53

Rules LAN



Rules DMZ



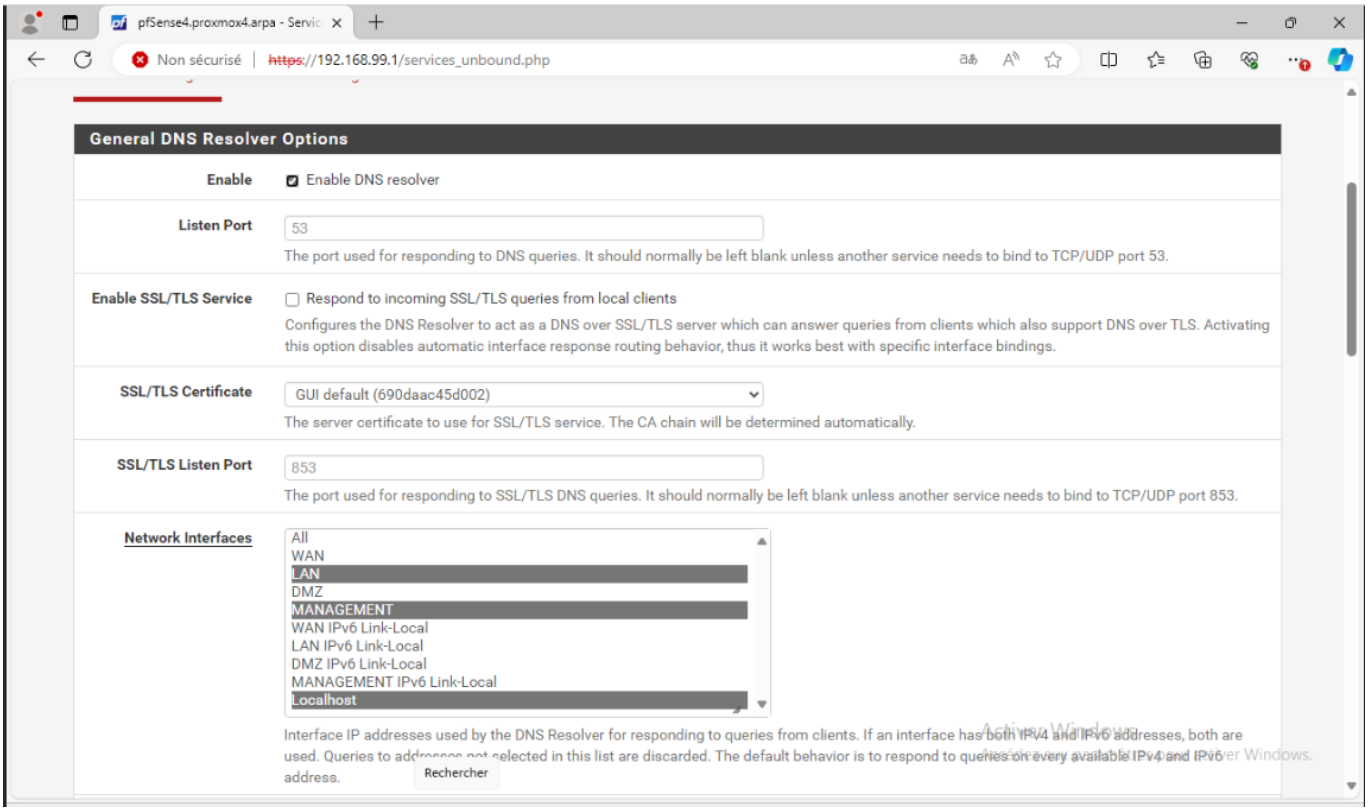
IV. DNS local (DNS Resolver)

Objectif : utiliser pfSense comme serveur DNS interne

Activer DNS Resolver

Services → DNS Resolver

- Activer
- Interfaces : LAN + Management + Localhost
- Enregistrer DHCP leases → ✔



Ajouter des enregistrements internes

- webdmz.local → IP serveur DMZ
- pfsense.local → 192.168.99.1

Host Overrides

Host	Parent domain of host	IP to return for host	Description	Actions
pfsense	local	192.168.99.1	pfSense Management	
webdmz	local	192.168.2.10	Serveur web DMZ	
www	facebook.com	127.0.0.1		

Configurer les clients

- VM LAN → DNS : 192.168.1.1
- VM Admin → DNS : 192.168.99.1

Tests

- ping pfsense.local → OK

```
C:\Users\Windows11-client>ping pfsense.local

Envoi d'une requête 'ping' sur pfsense.local [192.168.99.1] avec 32 octets de données :
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
```

- nslookup webdmz.local → OK

```
C:\Users\Windows11-client>nslookup webdmz.local
Serveur :   UnKnown
Address:  192.168.1.5

Réponse ne faisant pas autorité :
Nom :    webdmz.local
Address:  192.168.2.10
```

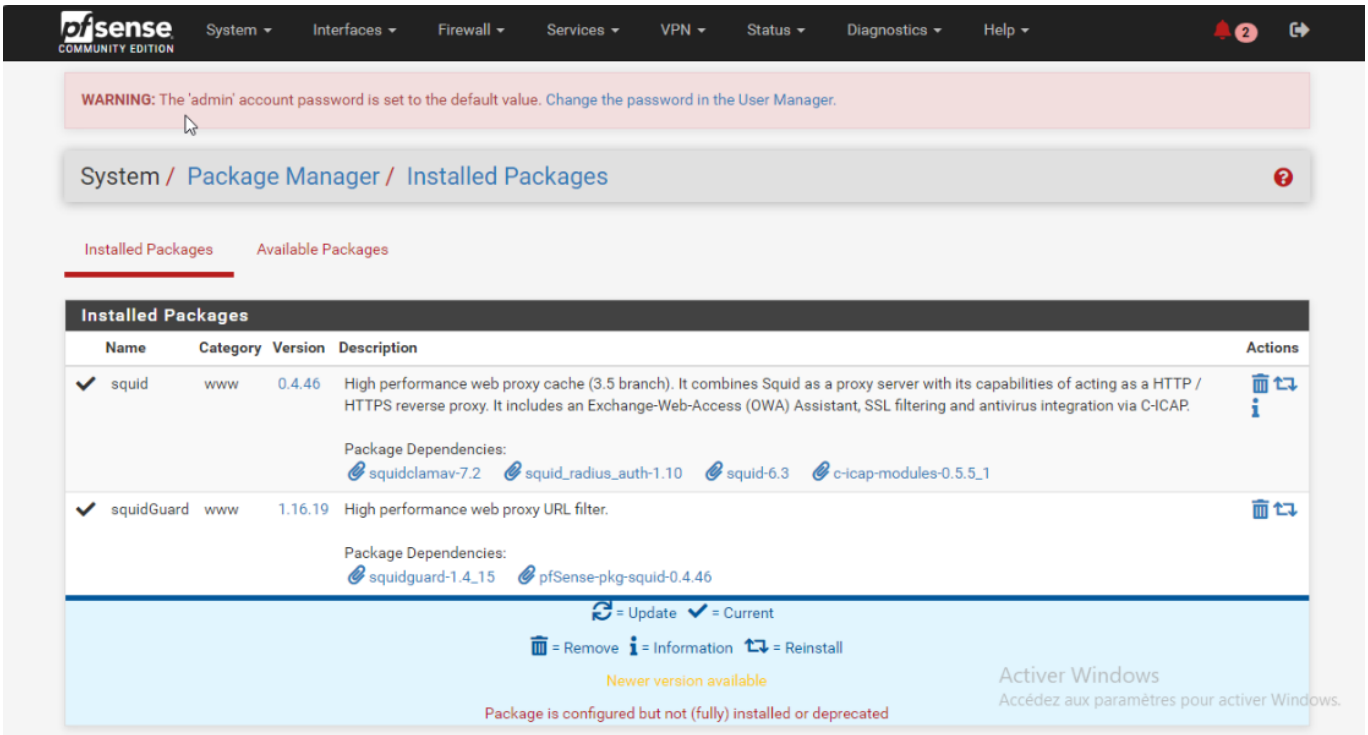
- ping webdmz.local → BLOQUÉ (pare-feu)

```
C:\Users\Windows11-client>ping webdmz.local

Envoi d'une requête 'ping' sur webdmz.local [192.168.2.10] avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
```

V. Proxy HTTP + Filtrage (Squid / SquidGuard)

Objectif : filtrer certains sites web

- Installer Squid & SquidGuard



Depuis Package Manager

Configurer Squid

- Activer
- Transparent Proxy
- Interface : LAN

Configurer SquidGuard

- Activer
- Télécharger une blacklist

Dans Common ACL :

- Bloquer : social_networks, adult, malware
- Autoriser le reste

Problème HTTPS

HTTPS ne peut pas être filtré en proxy transparent → Facebook n'est pas bloqué

Solution simple (DNS)

Ajouter dans DNS Resolver :

- Host : www
- Domain : facebook.com
- IP : 127.0.0.1

Désactiver DNS sécurisé dans le navigateur

VI. Serveur de Logs (rsyslog)

But : centraliser les logs de pfSense

VM Logs

- Debian
- IP : 192.168.1.20

Activer rsyslog

Modifier /etc/rsyslog.conf :

```
module(load="imudp")
input(type="imudp" port="514")
module(load="imtcp")
input(type="imtcp" port="514")
```

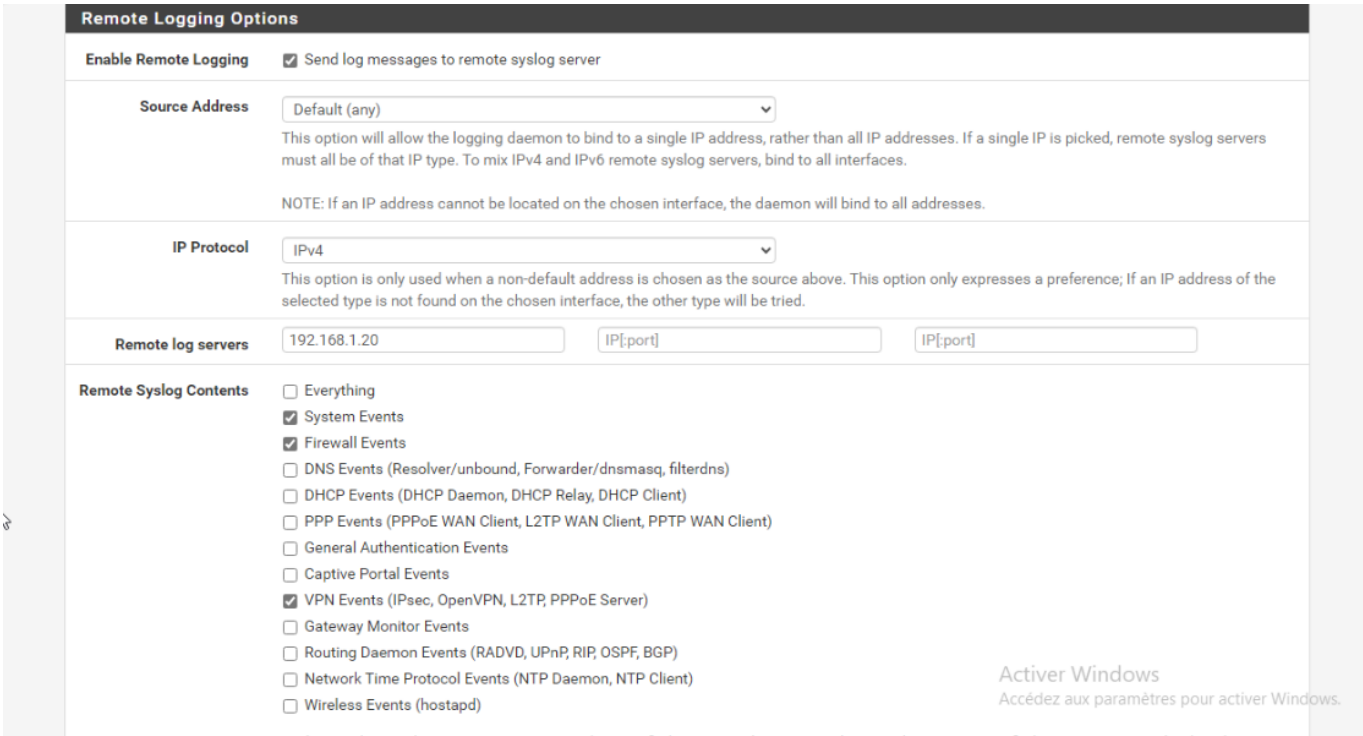
Puis redémarrer :

```
systemctl restart rsyslog
```

pfSense → envoi des logs

Status → System Logs → Settings :

- Enable Remote Logging
- Serveur : 192.168.1.20



Vérification

```
tail -f /var/log/syslog
```

VII. Supervision avec ntopng

Installation sur le serveur logs

```
wget https://packages.ntop.org/apt/bullseye/all/apt-ntop.deb
apt install ./apt-ntop.deb
apt update
apt install ntopng
```

Accès depuis le LAN

Naviguer vers : `http://192.168.1.20:3000`

Vérification

Les machines du LAN doivent apparaître dans “Hosts”

VIII. Sauvegardes

Sauvegarde automatique pfSense

- Activer SSH sur pfSense
- Sur serveur logs :

```
ssh-keygen
ssh-copy-id admin@192.168.1.1
```

Cron :

```
0 20 * * * scp admin@192.168.1.1:/cf/conf/config.xml /backup/pfsense-$(date +\%F).xml
```

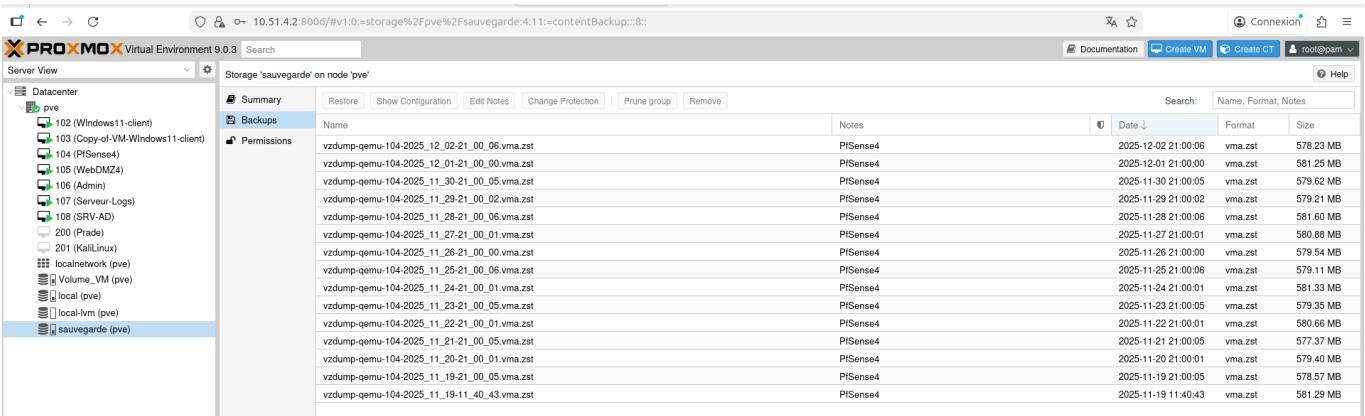
Sauvegarde Proxmox

Créer dossier `/var/lib/vz/backups`

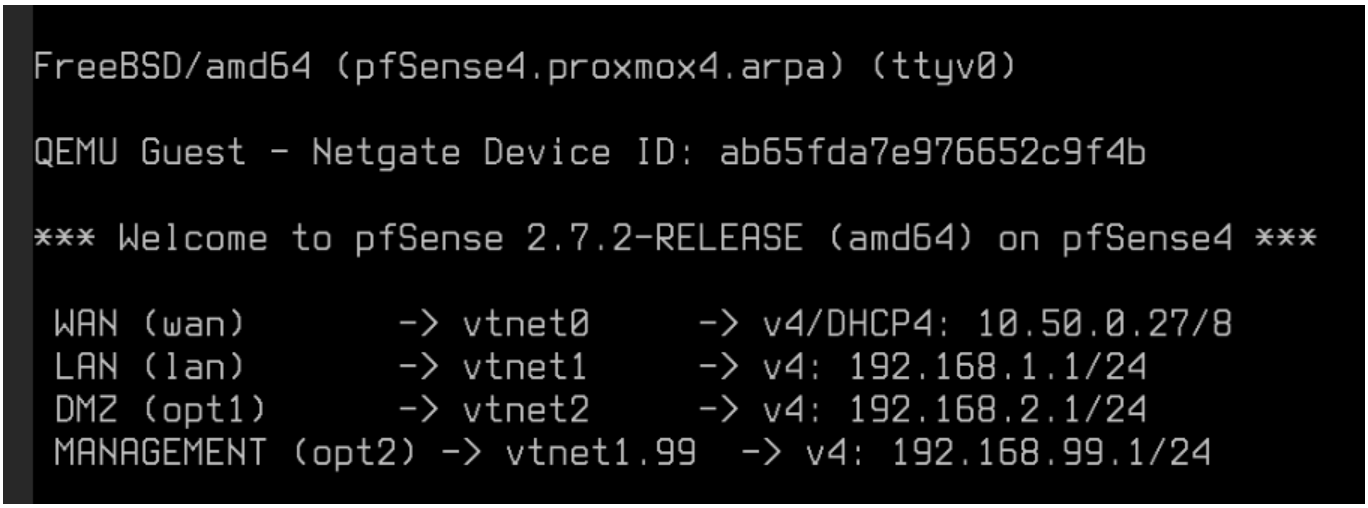
Sauvegarder pfSense vers ce dossier

Restauration

- Supprimer la VM pfSense
- Restaurer à partir du backup précédent



- Vérifier que la configuration réseau est identique


FreeBSD/amd64 (pfSense4.proxmox4.arpa) (ttyv0)
QEMU Guest - Netgate Device ID: ab65fda7e976652c9f4b
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense4 ***
WAN (wan) -> vtnet0 -> v4/DHCP4: 10.50.0.27/8
LAN (lan) -> vtnet1 -> v4: 192.168.1.1/24
DMZ (opt1) -> vtnet2 -> v4: 192.168.2.1/24
MANAGEMENT (opt2) -> vtnet1.99 -> v4: 192.168.99.1/24