DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Milan LELIEVRE - 2025/2026

FICHE RÉSEAU ET VLANS

CONTEXTE ET OBJECTIF :

Une entreprise de formation à besoin de configurer un réseau pour ses bureaux et ses salles de classes, l'objectif est donc de séparer et d'isoler deux réseaux dédiés, un pour l'équipe de l'entreprise, l'autre aux étudiants de la formation. Pour ce faire nous utiliserons une technologie utilisée pour séparer des réseaux en plusieurs sous réseaux, les "***Vlans***". Nous mettrons en place d'autres services d'administration et de sécurité.

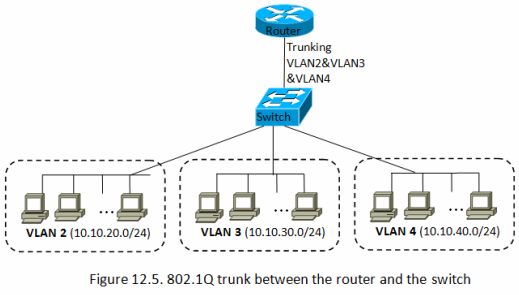


Figure 12.5. 802.1Q trunk between the router and the switch

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

SOMMAIRE :

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

MATÉRIEL ET RESSOURCES :

- Switch **TP-Link TL-SG1024D**

- Switch **TP-Link TL-SG1016PE**

- Ordinateur **Intel Nuc** (Dans notre cas un Intel NUC7i3BNH)

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

- 4 Répéteurs Wi-Fi **Zyxel NWA50AX**

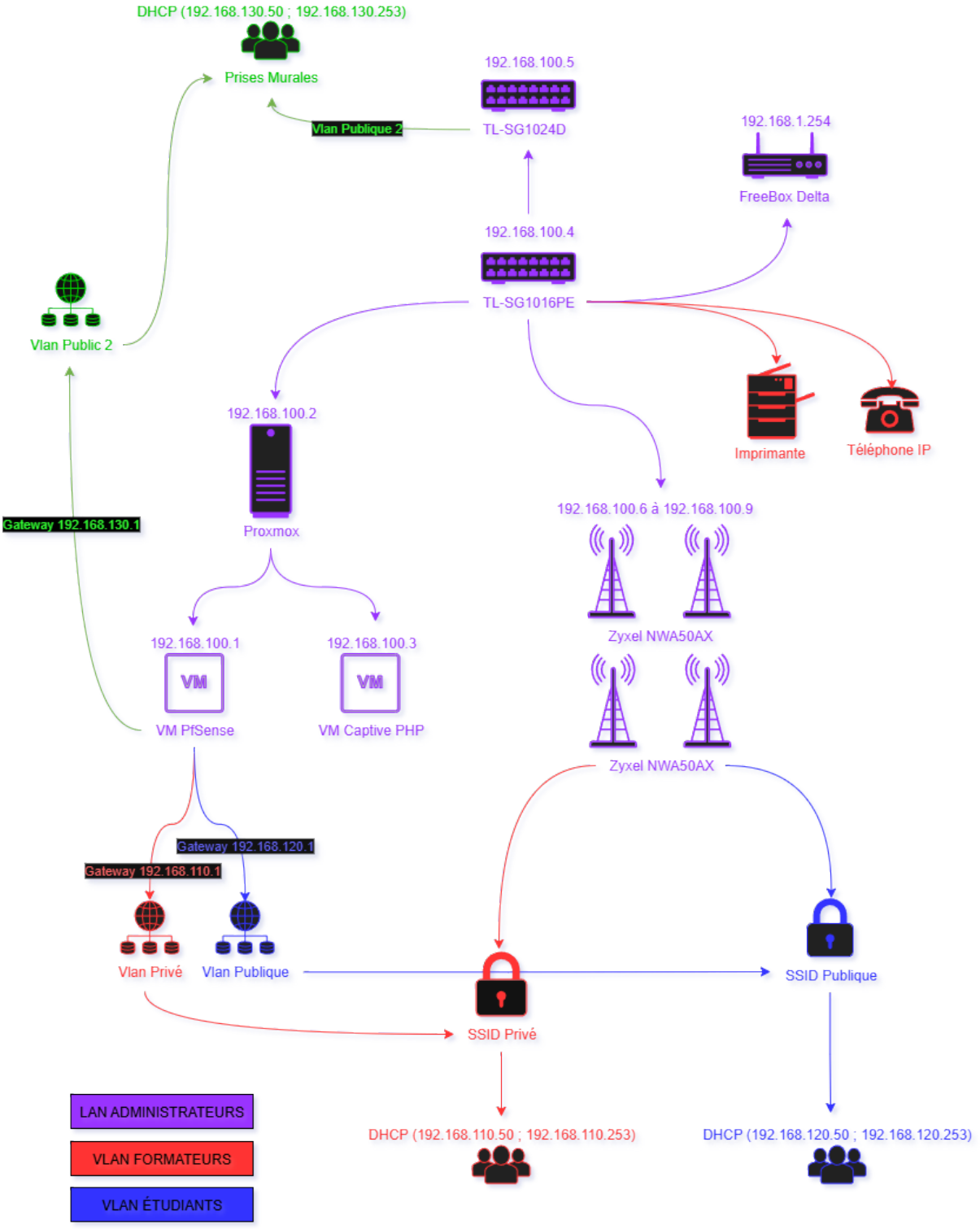
- L'hyperviseur "**Proxmox**" pour le Intel Nuc

PROXMOX

- La distribution **PfSense** en machine virtuel (sur le Intel Nuc) pour faire rôle de routeur

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

SCHÉMA DU RÉSEAU :



DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

🖧 Schéma Réseau - Version Textuelle

🏠 Routeur Principal

- 📡 **FreeBox Delta**
  🆔 IP : 192.168.1.254

🔀 Switchs

🧩 TL-SG1024D

- 🆔 IP : 192.168.100.5

🧩 TL-SG1016PE (connecté au TL-SG1024D)

- 🆔 IP : 192.168.100.4

🖥️ Serveur Proxmox

- 🆔 IP : 192.168.100.2

💻 Machines Virtuelles hébergées :

🔐 **VM PfSense**

- 🆔 IP : 192.168.100.1
- Gère deux VLAN :
  - 🔒 **VLAN Privé**
  - 🌐 **VLAN Public**

- 🛣️ **Gateway VLAN Privé :** `192.168.110.1`

🌐 **VM Captive PHP**

- 🆔 `IP : 192.168.100.3`

📡 Bornes WiFi (Zyxel NWA50AX)

- 🆔 `IPs : 192.168.100.6 → 192.168.100.9`

🔐 **SSID Privé**

- 🛣️ **Gateway :** `192.168.120.1`
- 🧾 **DHCP :** `192.168.110.10 → 192.168.110.250`

🌍 **SSID Publique**

- 🛣️ **Gateway :** `192.168.120.1`
- 🧾 **DHCP :** `192.168.120.10 → 192.168.120.250`

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

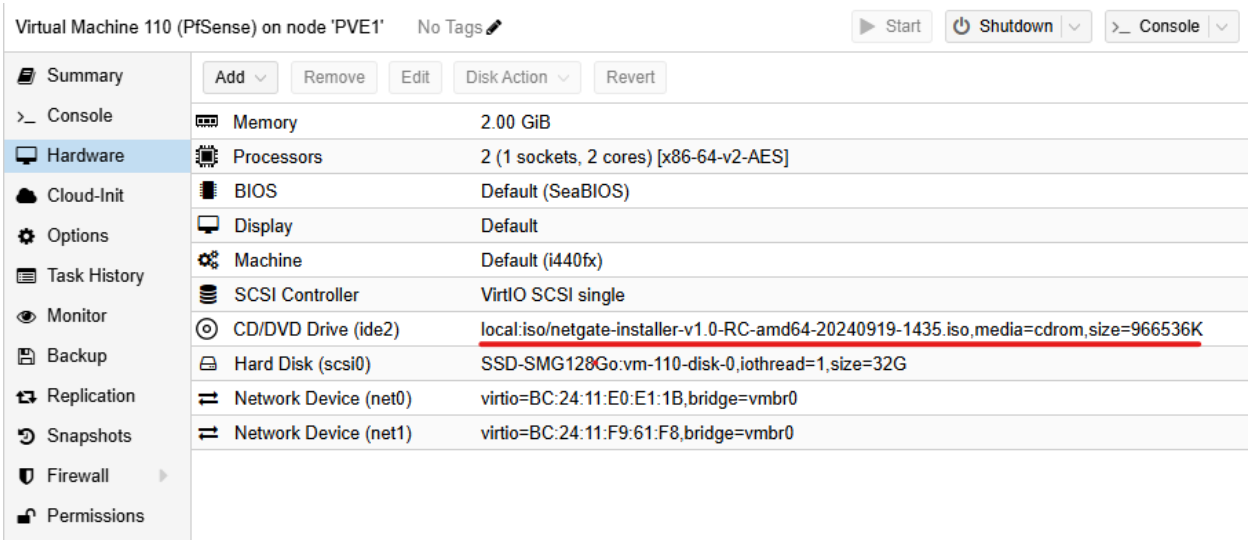
RÉALISATION DE L'INFRASTRUCTURE :

Avant de commencer, les prérequis sont d'avoir un serveur proxmox d'installer et de configurer, puis avoir deux iso dont :

- Un iso de PfSense
- Un iso de Debian 12

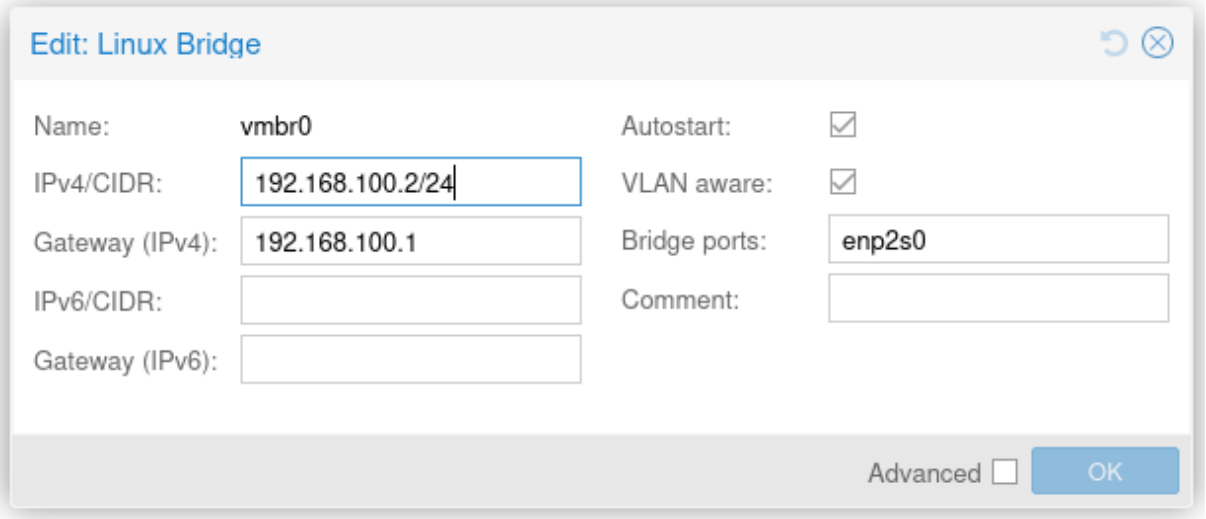
Étant donné que nous utiliserons la range **192.168.100.0** pour notre réseau administrateur, vous pouvez configurer l'ip du serveur proxmox sur **192.168.100.2**. Pour rappel, le port du panel de gestion de proxmox par défaut est **8006**. (Cf. Doc Proxmox)

1. Création de la VM PfSense dans proxmox



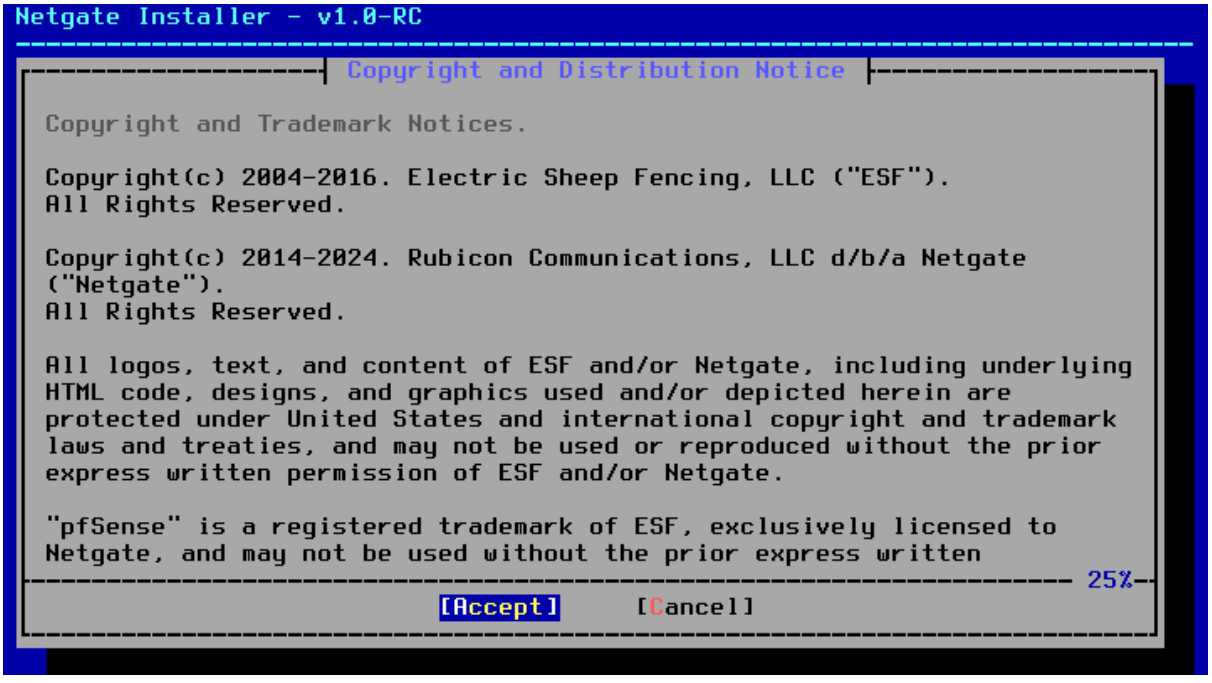
Ajouter une seconde carte réseau qui redirige aussi vers vmbr0 après avoir créé la VM. Modification très importante dans proxmox pour gérer les vlans :

- Désactiver les firewalls sur les cartes réseaux
- Activer "VLAN aware" sur le bridge utilisé par PfSense



Ces modifications permettront à PfSense de pouvoir gérer de lui-même les vlans.

2. Installation basique de PfSense



Configurer **net0** sur WAN et **net1** sur LAN
Identifiant du panel par défaut : admin / pfsense

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

3. Configuration des Vlans

VLAN Interfaces	
Interface	**VLAN tag**
vtnet1 (lan)	55
vtnet1 (lan)	60

Vlan Formateur avec le tag 55 et les élèves avec le tag 60. Le LAN admin est configuré sur le tag 1 (Donc pas de vlan pour gérer le réseau admin). Possibilités d'ajouter d'autres vlans si besoin ou une DMZ pour une potentielle imprimante pour formateurs et étudiants.

4. Montage des interfaces

Interface	Network port
WAN	vtnet0 (bc:24:11:e0:e1:1b)
ADMINISTRATEURS	vtnet1 (bc:24:11:f9:61:f8)
FORMATEURS	VLAN 55 on vtnet1 - lan
ETUDIANTS	VLAN 60 on vtnet1 - lan

Les différentes plages d'ip selon les réseau :

- LAN (Administrateurs) : 192.168.**100**.x
- VLAN 55 (Formateurs) : 192.168.**110**.x
- VLAN 60 (Étudiants) : 192.168.**120**.x
- WAN : 192.168.**2**.x

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Interfaces			
WAN	↑	10Gbase-T <full-duplex>	192.168.2.46
ADMINISTRATEURS	↑	10Gbase-T <full-duplex>	192.168.100.1
FORMATEURS	↑	10Gbase-T <full-duplex>	192.168.110.1
ETUDIANTS	↑	10Gbase-T <full-duplex>	192.168.120.1

5. Configuration des règles de et du pare-feu

- WAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule
☐	✓	1/17.70 MiB	IPv4 UDP	*	*	WAN address	50195	*	none	

Cette règle sert pour l'accès à distance au lan admin grâce à un futur serveur OpenVPN à configurer plus tard.

- Administrateurs

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule
	✓	0/10.34 MiB	*	*	*	ADMINISTRATEURS Address	80	*	*	
☐	✗	0/0 B	IPv4 *	ETUDIANTS address	*	*	*	*	none	
☐	✗	0/0 B	IPv4 *	FORMATEURS address	*	*	*	*	none	
☐	✓	5/18.07 MiB	IPv4 *	ADMINISTRATEURS subnets	*	*	*	*	none	
☐	✓	0/0 B	IPv6 *	ADMINISTRATEURS subnets	*	*	*	*	none	

Règles de base pré-configurées par PfSense. Et blocage de toutes requêtes venant des vlans. La source ne doit pas être ETUDIANTS address mais bien ETUDIANTS subnets. Idem pour les formateurs.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

- Formateurs

Rules (Drag to Change Order)									
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule
☐	✗ 0/4 KiB	IPv4 TCP	*	*	192.168.120.1	80 (HTTP)	*	none	
☐	✗ 0/2 KiB	IPv4 TCP	*	*	192.168.110.1	80 (HTTP)	*	none	
☐	✓ 0/34 KiB	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none	
☐	✓ 0/23.38 MiB	IPv4+6 TCP	*	*	*	80 (HTTP)	*	none	
☐	✓ 0/16.22 MiB	IPv4+6 TCP	*	*	*	443 (HTTPS)	*	none	
☐	✗ 0/312 KiB	IPv4 *	*	*	*	*	*	none	

Les règles des deux vlans sont configurées de sorte à ce que les appareils connectés dessus aient accès limité à internet et aux autres sous réseaux. Possibilité toujours d'ajouter de nouvelles règles aux besoins. Dans notre cas, ils n'ont accès qu'au web, possibilités d'ajouter d'autres autorisation pour les étudiants développeur qui souhaite utiliser des bases de données externes par exemple.

- Étudiants

Rules (Drag to Change Order)									
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule
☐	✓ 0/0 B	IPv4 TCP	*	*	192.168.120.1	8002	*	none	
☐	✗ 0/1 KiB	IPv4 TCP	*	*	192.168.120.1	80 (HTTP)	*	none	
☐	✗ 0/0 B	IPv4 TCP	*	*	192.168.110.1	80 (HTTP)	*	none	
☐	✓ 1/20 KiB	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none	
☐	✓ 0/13 KiB	IPv4+6 TCP	*	*	*	80 (HTTP)	*	none	
☐	✓ 8/5.13 MiB	IPv4+6 TCP	*	*	*	443 (HTTPS)	*	none	
☐	✗ 0/93 KiB	IPv4 *	*	*	*	*	*	none	

Règles globalement assez similaires à celle du vlan pour les formateurs mais ajout d'une règle pour autoriser les paquets pour le captive portal de PfSense. Donc un protocole TCP sur le port 8002 de la gateway du Lan d'administration.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

6. Configuration du switch TP-Link TL-GS1016PE via interface web

TP-Link nous offre une configuration assez rapide et facile pour leurs switch manageables. En récupérant l'adresse ip du switch grâce à leur logiciel qui permet de scanner le réseau et d'identifier les switch TP-Link. Une fois le switch scanner par le logiciel, vous pourrez définir un mot de passe pour y accéder.

Une fois sur l'interface web du switch, l'identifiant pour se connecter est admin et le mot de passe est celui configuré juste dans l'interface web du switch avant.

Une fois la connexion établie, la configuration des ports en vlan peut commencer.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

802.1Q VLAN Configuration

802.1Q VLAN Configuration: (•) Enable ( ) Disable [Apply]

VLAN ID	55 (1-4094)	VLAN Name	Formateurs
Port	Untagged	Tagged	Not Member
Select All	☐	☐	☐
Port 1	○	●	○
Port 2	○	●	○
Port 3	○	●	○
Port 4	○	○	●
Port 5	○	●	○
Port 6	○	○	●
Port 7	○	○	●
Port 8	○	○	●
Port 9	○	○	●
Port 10	○	○	●
Port 11	○	○	●
Port 12	○	○	●
Port 13	○	○	●
Port 14	○	○	●
Port 15	○	○	●
Port 16	○	●	○

[Add/Modify] [Help]

VLAN ID	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Delete
1	Default	1-16		1-16	☐
55	Formateurs	1-3,5,16	1-3,5,16		☐
60	Etudiants	1-3,5,16	1-3,5,16		☐

[Select All] [Delete]

Les ports du switch peuvent varier en fonction des besoins. Les ports des répéteurs doivent être configurés en tagged pour pouvoir envoyer les paquets. Et le serveur avec la machine virtuelle PfSense doit lui aussi être en tagged. Dans notre cas, les ports 1,2,3,5 sont ceux des répéteurs, et le 16 est celui du serveur.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

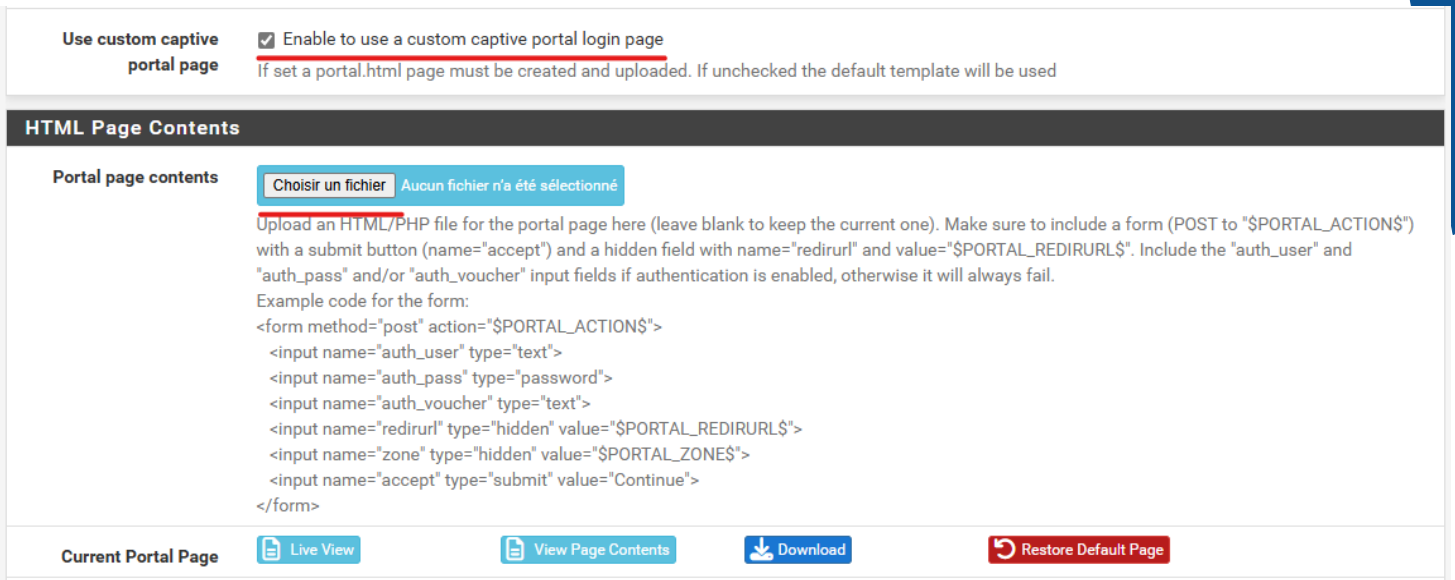
7. Configuration d'un captive portal

Pour le réseau étudiant, il faut donc configurer un captive portal qui renseigne une adresse mail et qui l'enregistre dans un fichier csv en renseignant la date de connexion ainsi que l'ip du poste utilisé.

PfSense ne permet pas de fonctionner comme celà par défaut, il faudra donc faire une page customisé en html ainsi que préparer une vm ou un au serveur sous linux avec un script PHP afin d'enregistrer l'email dans le fichier et de faire une redirection qui permet à pfsense d'accepter le poste en question.

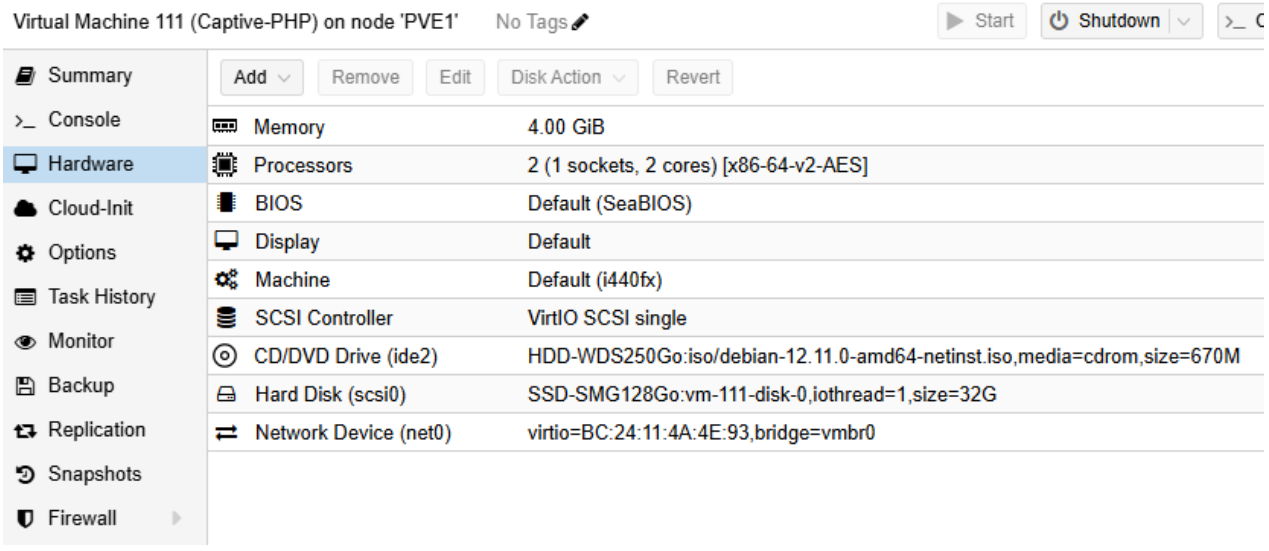
**Voici un aperçu de la page d'accueil, en html.*

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE



Dans notre cas, il faut activer l'option pour pouvoir utiliser une custom captive page login. Puis téléverser le fichier html dans le serveur.

Ensuite, mise en place de la machine virtuelle qui s'occupera du captive portal. Elle sera donc sous debian 12 sans interface graphique



Configurer une IP dans le lan Administrateur (dans notre cas : **192.168.100.3**)

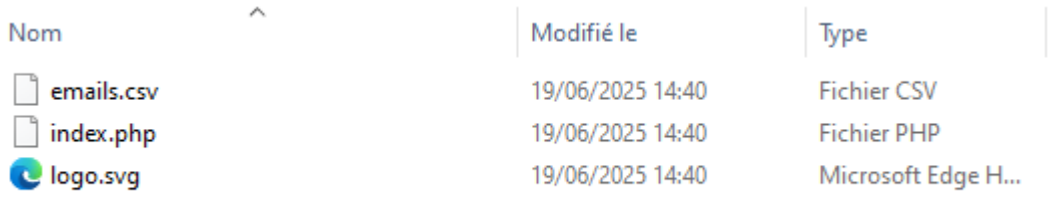
DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Sur cette machine virtuelle, il est nécessaire d'installer PhP et toute ses dépendances, avec la commande "**sudo apt install php libapache2-mod-php php-mbstring php-curl php-xml php-cli php-common php-gd apache2**", après avoir effectué "**sudo apt update**" dans un premier temps.

Vous pouvez redémarrer apache2 si besoin.

Une fois tout installé, il ne manque maintenant plus qu'à importer sur votre VM le script en PHP pour le captive portal, puis créer un fichier csv avec le même nom inscrit dans le script dans le même dossier que votre script. Pour faciliter les choses, il est préférable de déposer tout ça dans /var/www/html/Captive (le dossier Captive doit être créé avant).

Pour importer vos fichiers plusieurs méthodes s'offrent à vous, le sftp, le scp, le wget et d'autres encore. La plus rapide et facile dans le contexte est la mieux adapté.



DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

```php
<?php
$file = 'emails.csv';

$email = $_POST['auth_user'] ?? '';
$ip = $_SERVER['REMOTE_ADDR'] ?? 'unknown';

if (filter_var($email, FILTER_VALIDATE_EMAIL)) {
    $handle = fopen($file, 'a');
    if ($handle !== false) {
        fputcsv($handle, [date('Y-m-d H:i:s'), $email, $ip]);
        fclose($handle);
    }
    header('Location: http://192.168.120.1:8002/index.php?accept=true');
    exit;
} else {
    echo "Adresse e-mail invalide. <a href='javascript:history.back()'>Retour</a>";
}
?>
```

**Exemple de script en php pour faire la redirection*

```html
<!DOCTYPE html>
<html lang="fr">
<head>
  <meta charset="UTF-8">
  <title>
    Connexion Wi-Fi - [redacted]
  </title>
  <link rel="stylesheet" type="text/css" href="./styles.css">
</head>
<body onselectstart="return false">
  <div class="container">
    <img src="./logo.svg" alt="Logo [redacted]" class="logo">
    <h2>
      Bienvenue à [redacted]
    </h2>
    <p>
      Pour accéder au Wi-Fi invité, veuillez renseigner votre adresse e-mail :
    </p>
    <form method="post" action="$PORTAL_ACTION$">
      <input type="email" name="auth_user" placeholder="email@example.com" required>
      <input type="hidden" name="auth_pass" value="dummy">
      <button type="submit">Se connecter</button>
    </form>
    <div class="footer">
      <p>
        © 2025 [redacted] - <a href="https://[redacted]">[redacted]</a>
      </p>
    </div>
  </div>
</body>
</html>
```

**Exemple de code en html pour la page d'accueil du portail (non stylisé)*

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Pour les redirections des liens hypertext, la page html sur le PfSense doit redirigé vers le script PhP sur la machine virtuelle pour le captive portal, et le script du captive portal doit redirigé vers le portail du PfSense avec comme argument "?accept=true" dans le fichier index.php.

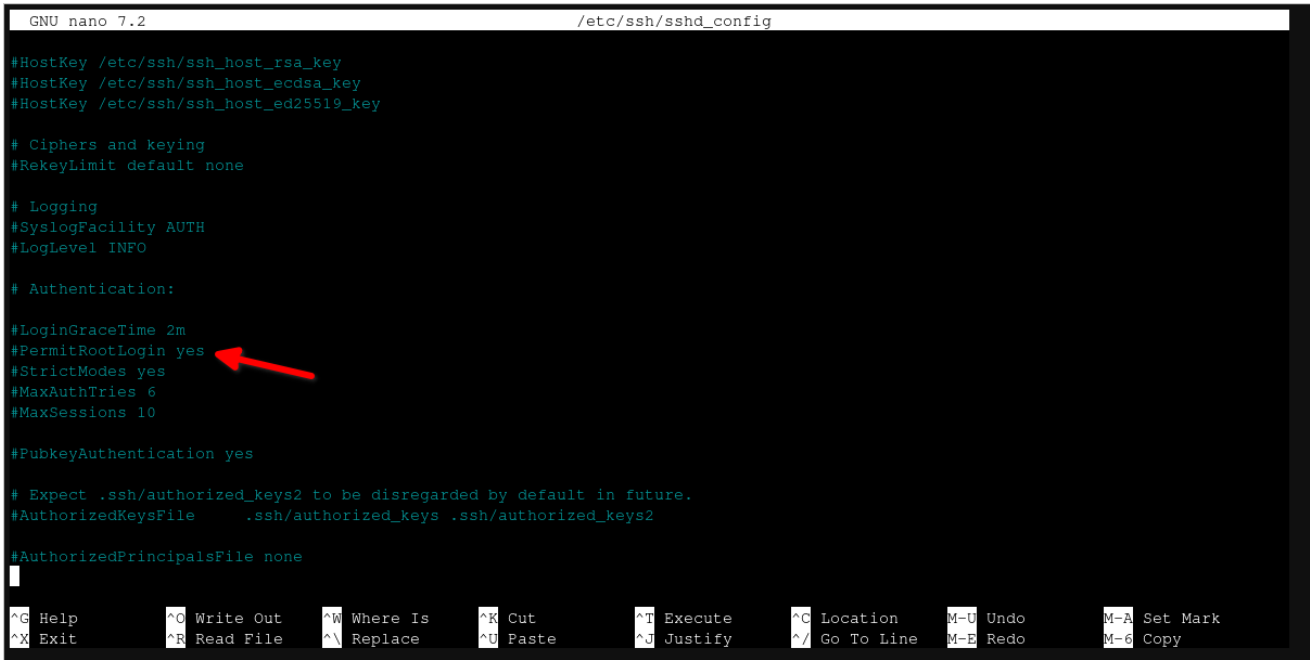
8. Sécurisation de l'infrastructure

Plusieurs paramètres sont à prendre en comptes pour sécuriser l'infrastructure :

- Empêcher le login root en ssh sur tout les serveur
- Changer le port de SSH
- Interdire la connexion avec mot de passe
- Authentification via clé publique

Pour ce faire, vous devez donc modifier plusieurs paramètres dans le fichier de configuration ssh, avec "**sudo nano /etc/ssh/sshd_config**" :

- Port 22022 *Changement du port ssh.
- PermitRootLogin no *interdire la connection directement en root
- PasswordAuthentication no *interdire la connection avec MDP
- ChallengeResponseAuthentication no ***
- AuthenticationMethods publickey *authentication via clé publique



**Un exemple de modification dans le fichier /etc/ssh/sshd_config : PermitRootLogin*

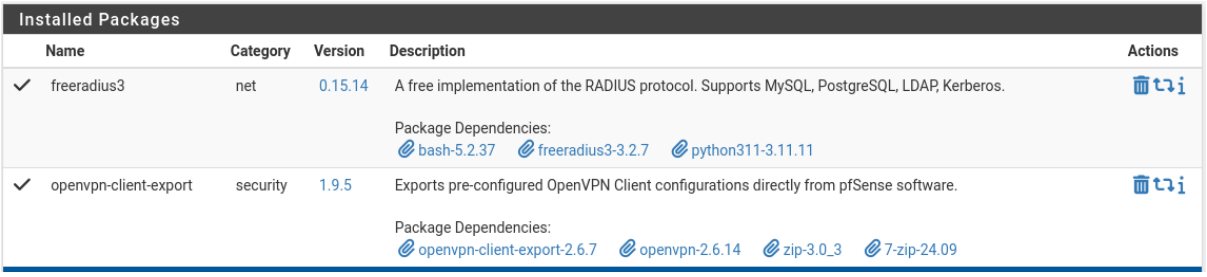
DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Pour que les paramètres se mettent à jour, il faut tout d'abord enlever l'en-tête de commentaire (en enlevant le #). Puis il faut relancer le service ssh, soit en redémarrant la machine après avoir fait d'autres modifications, soit en effectuant "**sudo systemctl restart sshd**".

9. Mise en place d'un openVPN via PfSense via radius authentification

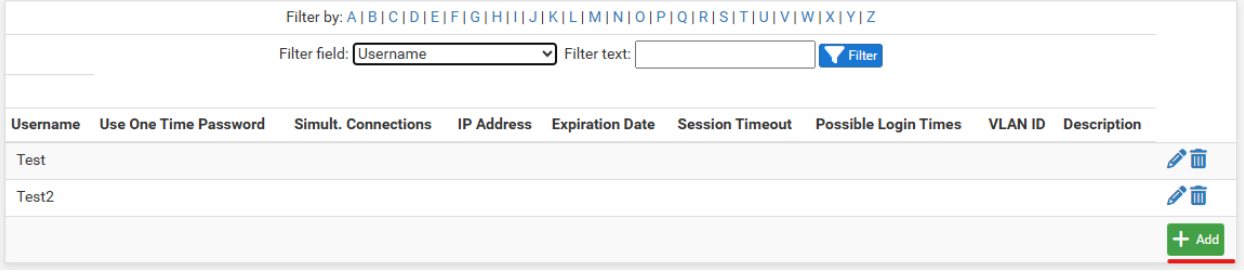
Pour mettre en place un VPN via radius authentification, il faut installer deux dépendances nécessaires :

- freeradius
- openvpn-client-export



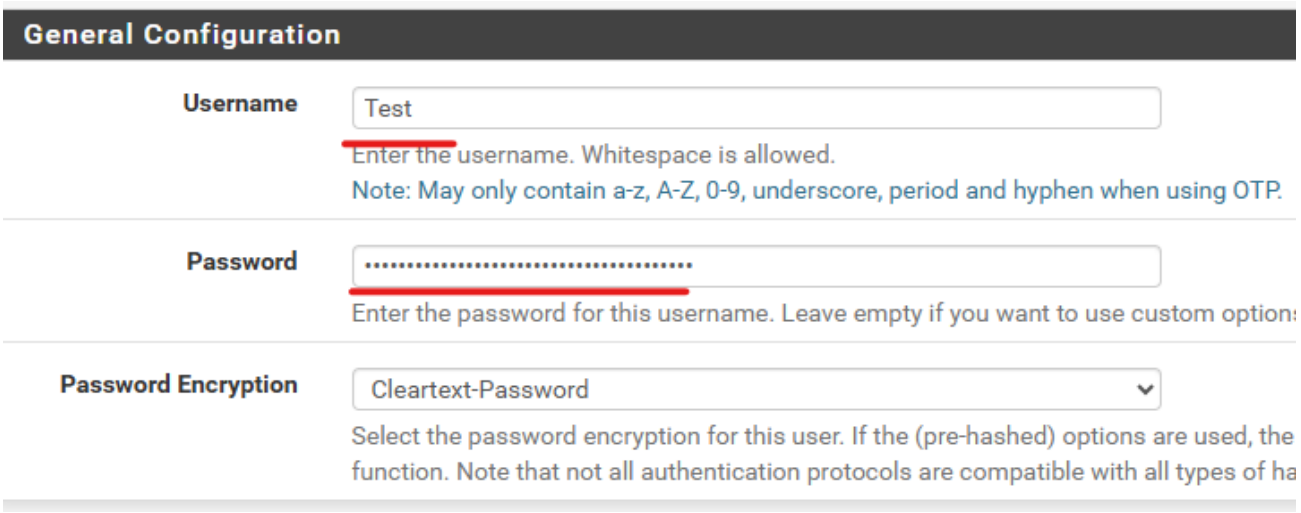
Puis il faut configurer le serveur radius sur le PfSense :

Premièrement; il faut d'abord créer des utilisateurs pour pouvoir se connecter grâce à eux au serveur Open VPN :

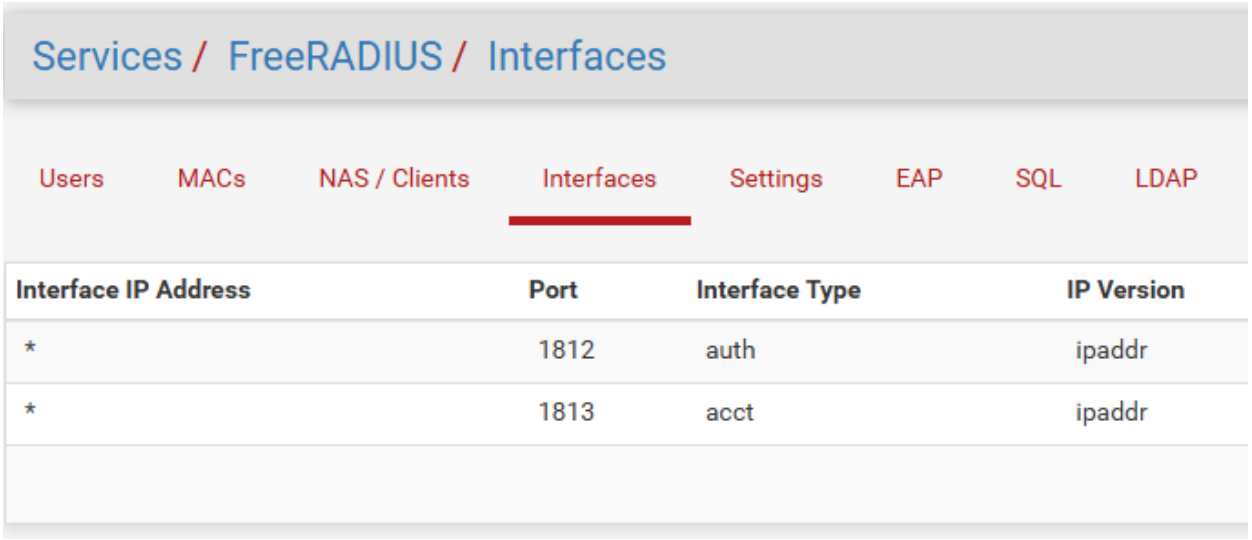


DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

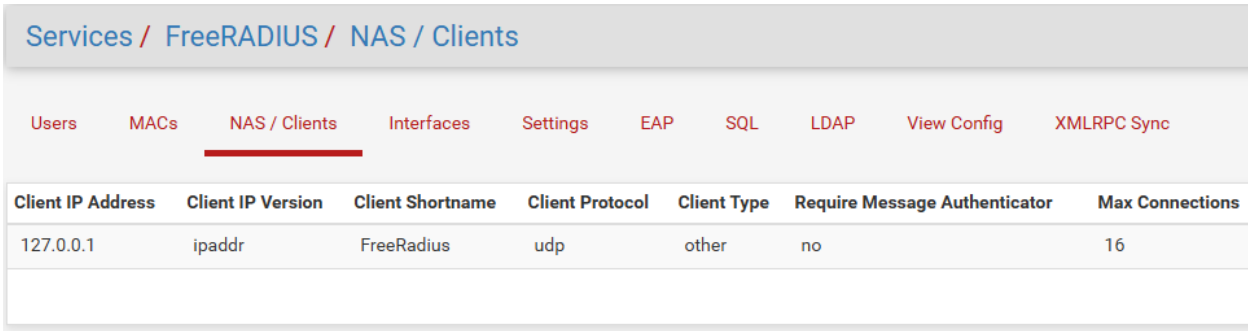
Il suffira de cliquer sur add puis simplement d'ajouter un username et un mot de passe.



Il faudra ensuite créer deux interfaces dans le service FreeRadius pour l'authentification.

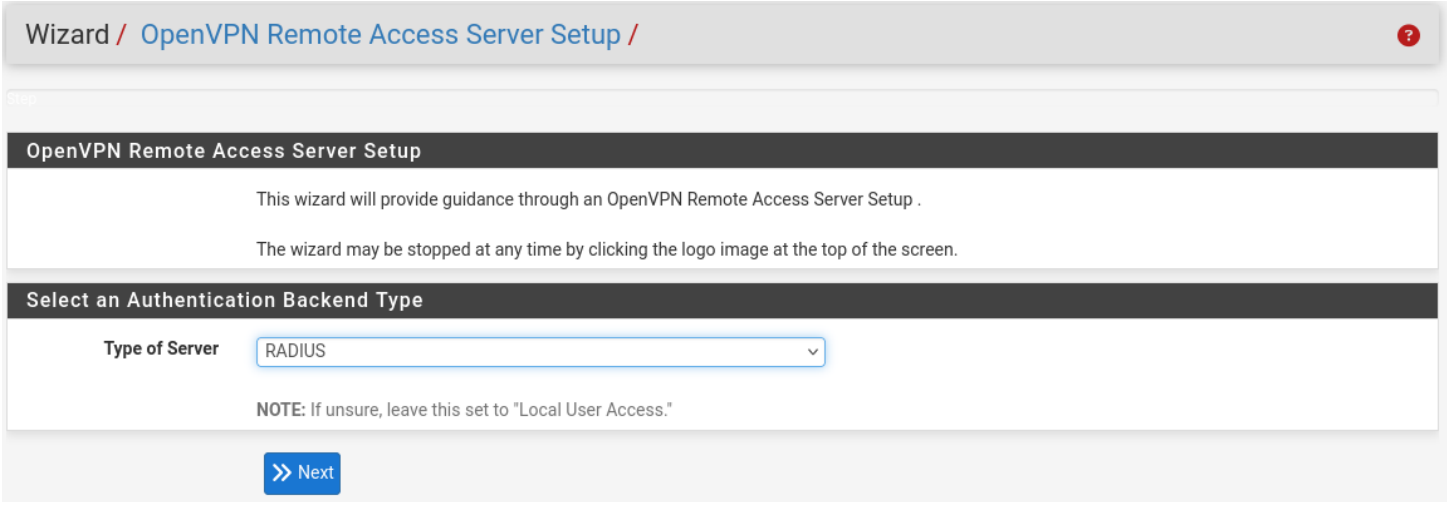


DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

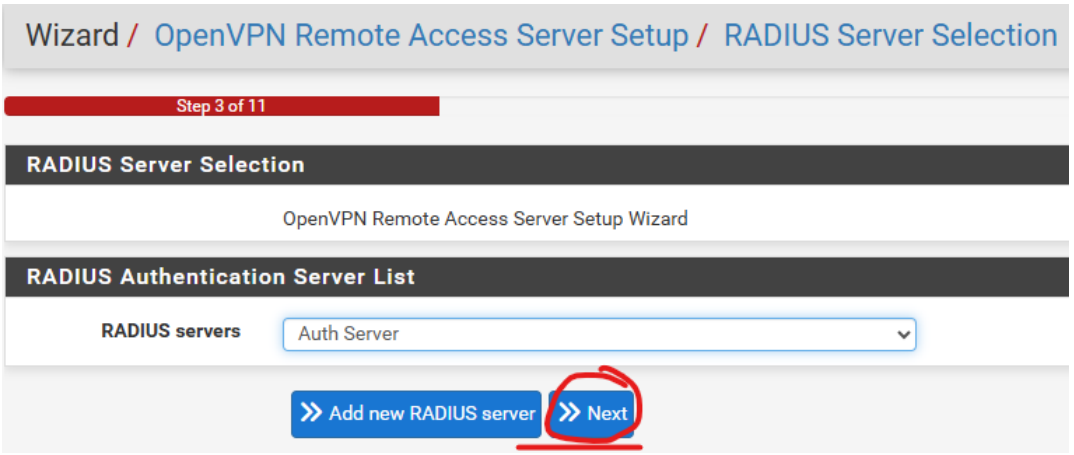


Puis créer un espace pour que les clients puissent se connecter et accéder au lan d'administration.

Enfin, PfSense propose un setup automatique du serveur Open VPN, Nous pouvons donc le configurer en sélectionnant RADIUS comme type de serveur et le rediriger vers le serveur radius configuré juste avant.

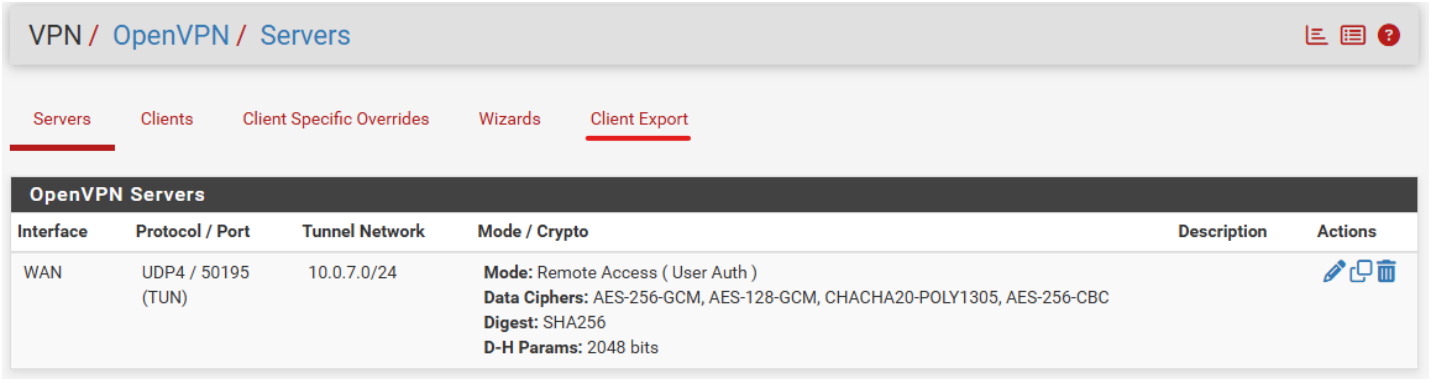


DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

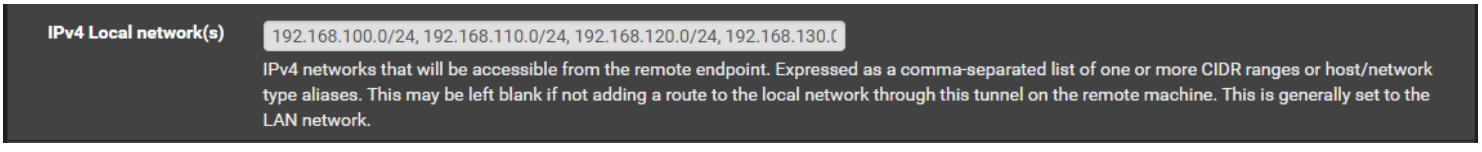


⚠️: Attention à bien cliquer sur Next lors de ses étapes de configuration (toujours en sélectionnant à chaque étape le serveur radius que vous venez de configurer)

Pour se connecter au VPN avec notre authentification radius, il faut aller dans client-export dans notre VPN

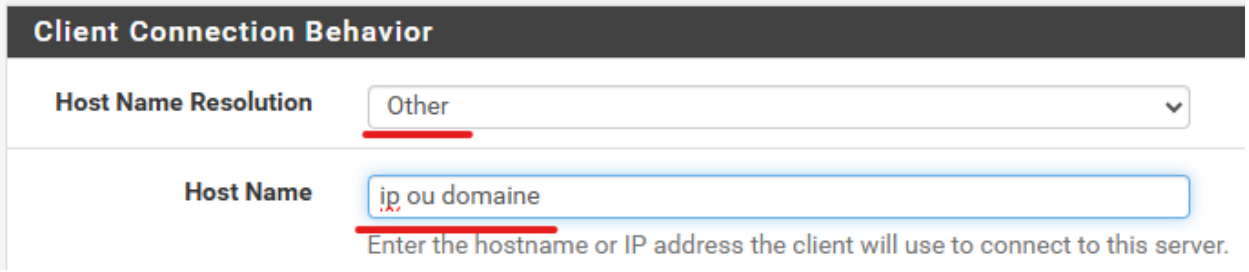


Dans notre cas, le port utilisé est 50195 mais le port de base est 1194. De plus, pour accéder à tous les réseaux, il faut préciser dans la configuration du serveur OpenVPN sur quelle(s) passerelle(s) le serveur nous redirige.

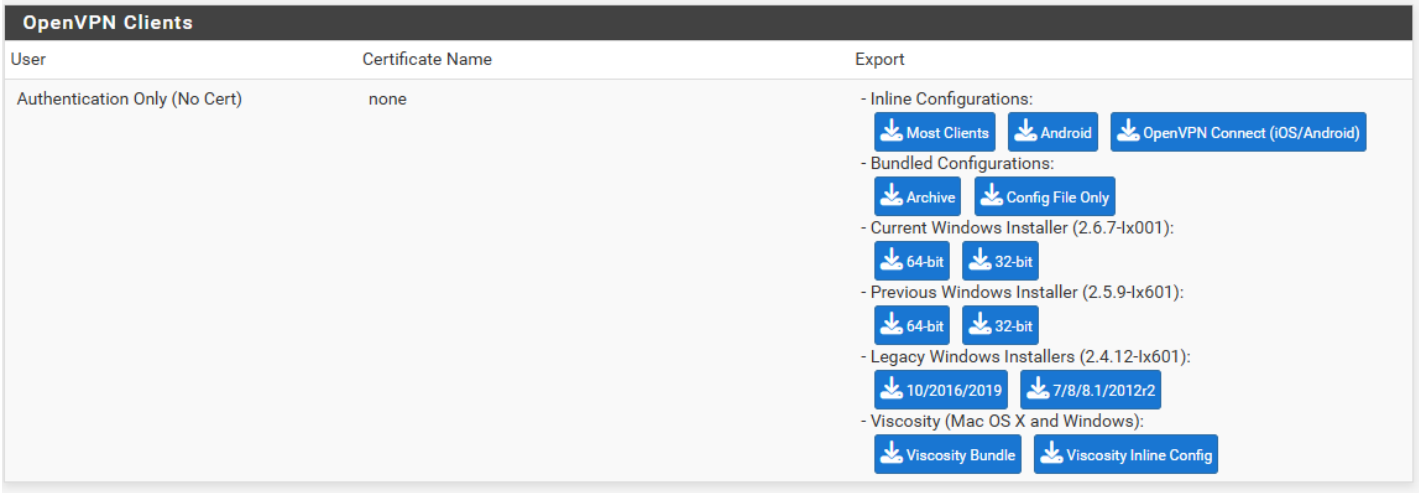


Vous trouverez cette option dans “Tunnel Settings”.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE



Dans cette catégorie, il est nécessaire de modifier l'"host name resolution" si le but de ce serveur est d'y accéder via un autre réseau que le nôtre. Pour ce faire, il faut modifier "Host Name Resolution", sélectionné "Other" puis dans "Host Name" indiqué l'adresse IP de votre box ou un nom de domaine si vous en possédez un.

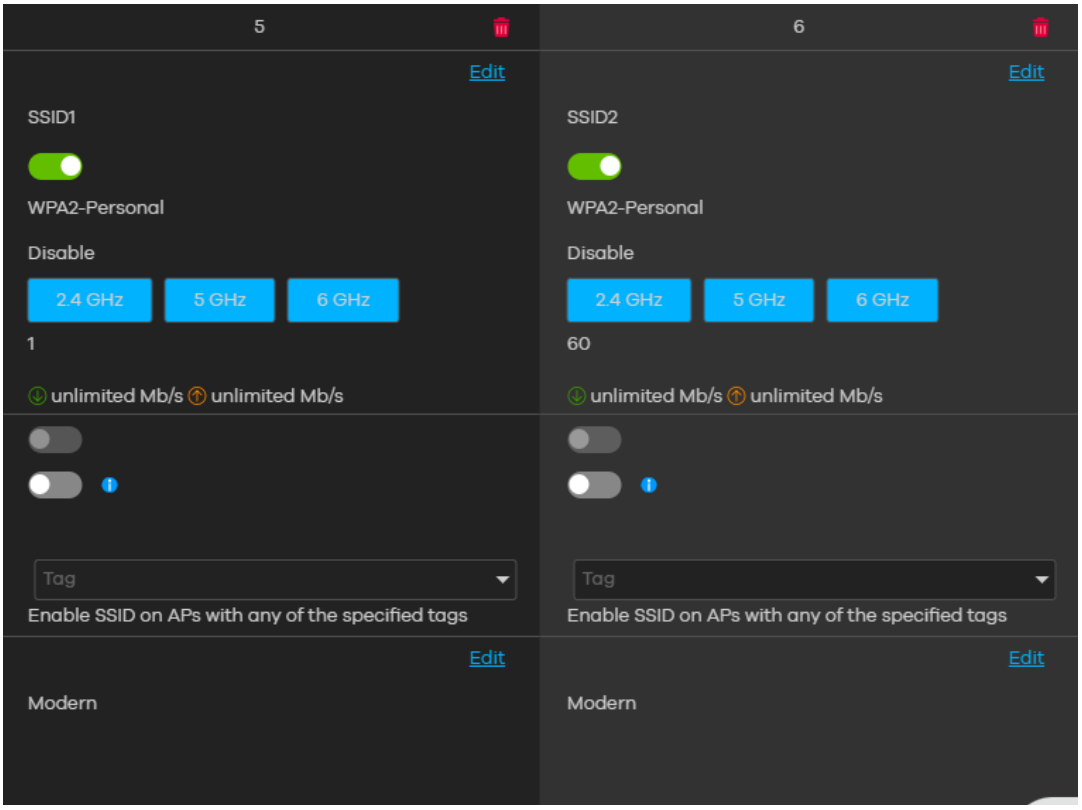


Enfin, pour se connecter au VPN, vous avez besoin d'une des installations clients correspondant à votre plateforme / version plus bas dans la page "Client Export".

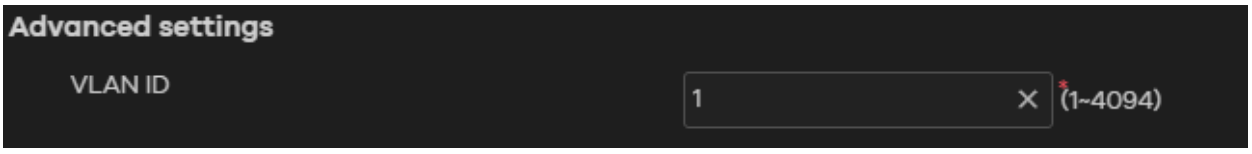
DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

10. Configuration des répéteurs Wi-Fi (via nebula)

Par défaut, les 4 répéteurs ont chacun leur propre SSID de configurés, il faut donc ajouter deux SSID supplémentaires pour faire en sorte que les 4 répéteurs utilisent tous ces deux SSID.



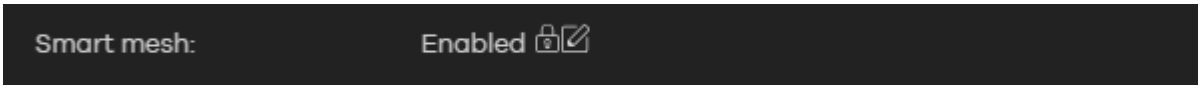
Sur le site web de Nebula (par Zyxel), dans la catégorie "configure", rendez vous dans "SSID Settings", dans "Access Point". C'est ici que nous pouvons ajouter et configurer les SSID sur site.



DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

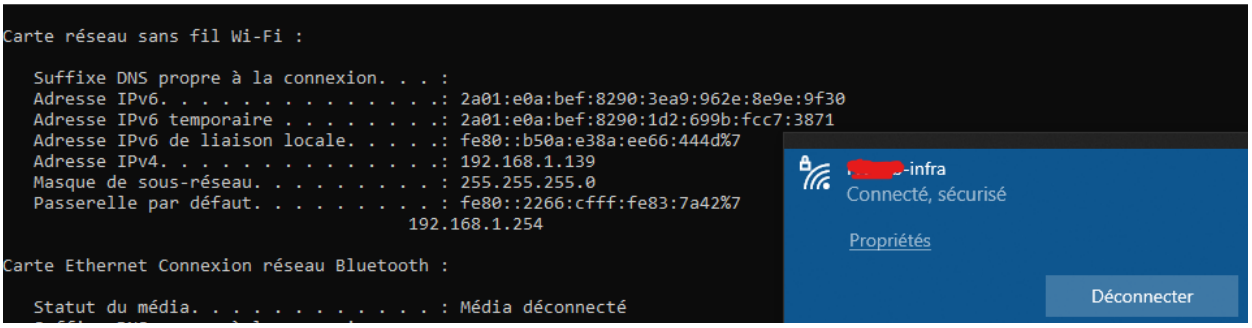
Dans “Advanced settings” la première option concerne la VLAN ID, ce qui nous intéresse donc pour la réalisation de notre projet. Configurer deux Vlans différentes pour le SSID Public et Privé.

Une fois vos deux SSID créées et configurées, elles devraient fonctionner simultanément sur les 4 répéteurs. Zyxel propose si besoin une option “Smart mesh” pour mailler les répéteurs.

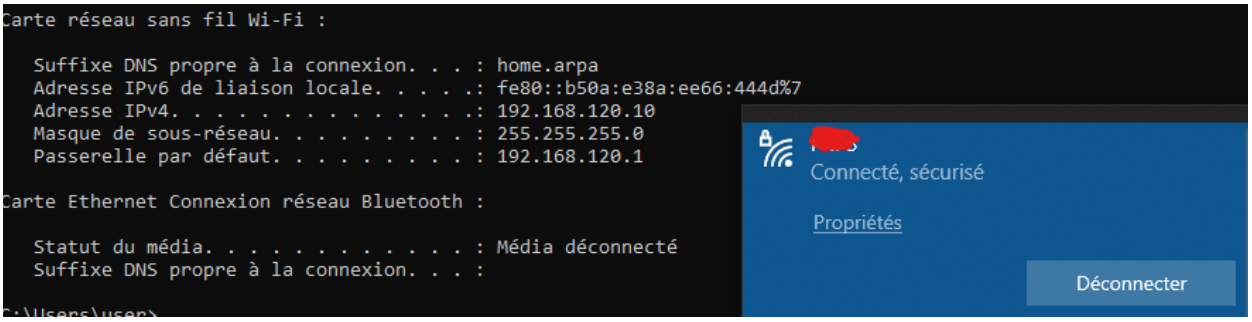


Cette option se trouve dans “Device”, puis “Access points”. Elle se situe dans “Status” après avoir sélectionné un répéteur.

Une fois que les deux SSID sont créés il ne manque plus qu'à les tester.



Je me connecte donc sur le wifi de base d'un des répéteurs Wi-Fi, je remarque que, n'étant pas configuré, j'accède bien au réseau mais en lan 1. Donc avec l'ip de mon routeur.



DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

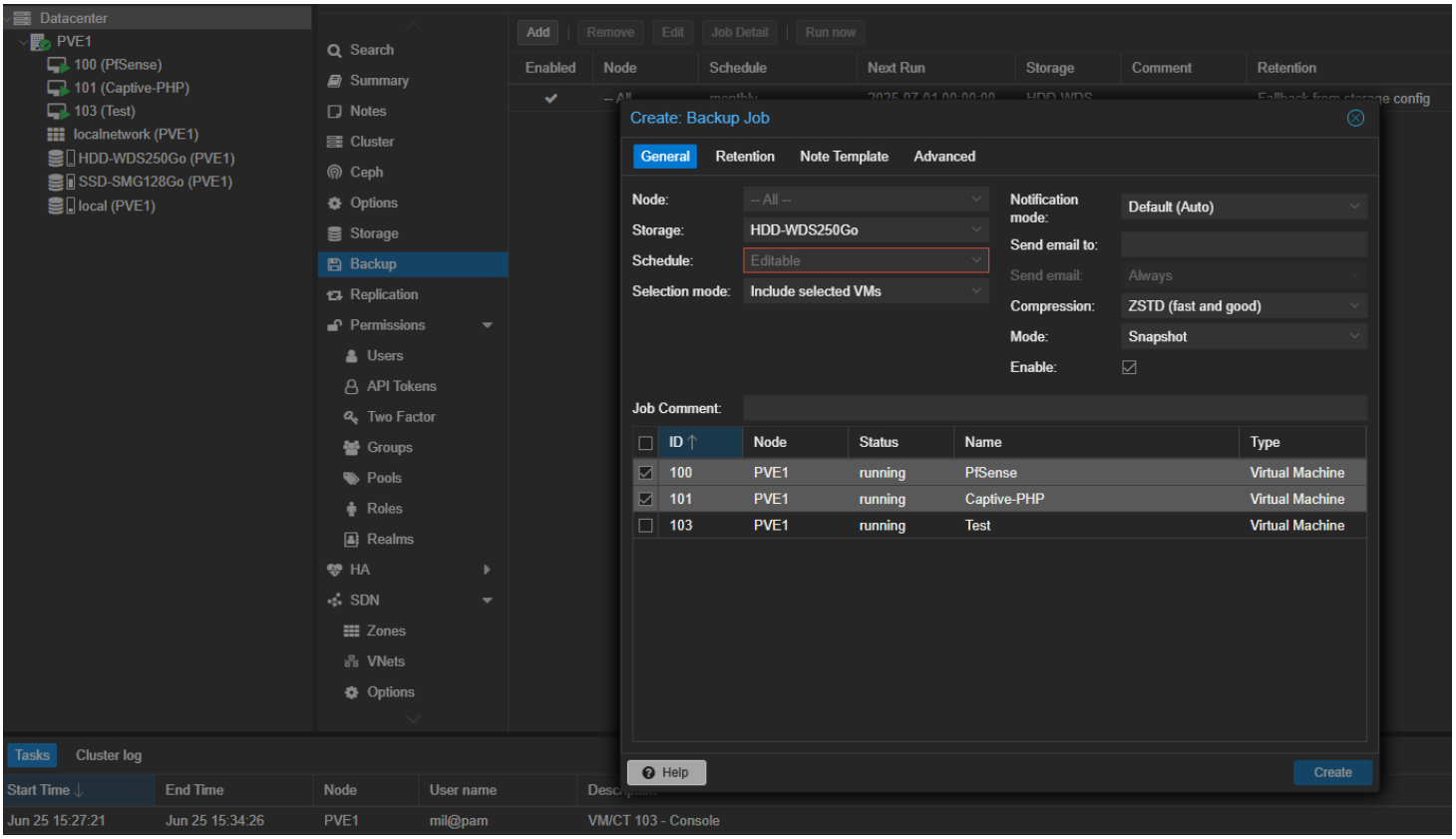
Je change ensuite de réseau et constate que mon SSID ainsi que mon vlan fonctionne bel est bien. Pour terminer je lancer une requête ICMP si j'ai une règle dans mon réseau qui me l'autorise, ou bien je navigue sur internet pour vérifier la connexion réseau.

Il ne reste plus qu'à essayer avec les SSID restants et à ensuite déployer le réseau dans l'entreprise.

⚠️: Si votre routeur possède un Wi-Fi, s'il ne sert pas, pensez à le désactiver afin d'éviter toute faille de sécurité dans votre réseau.

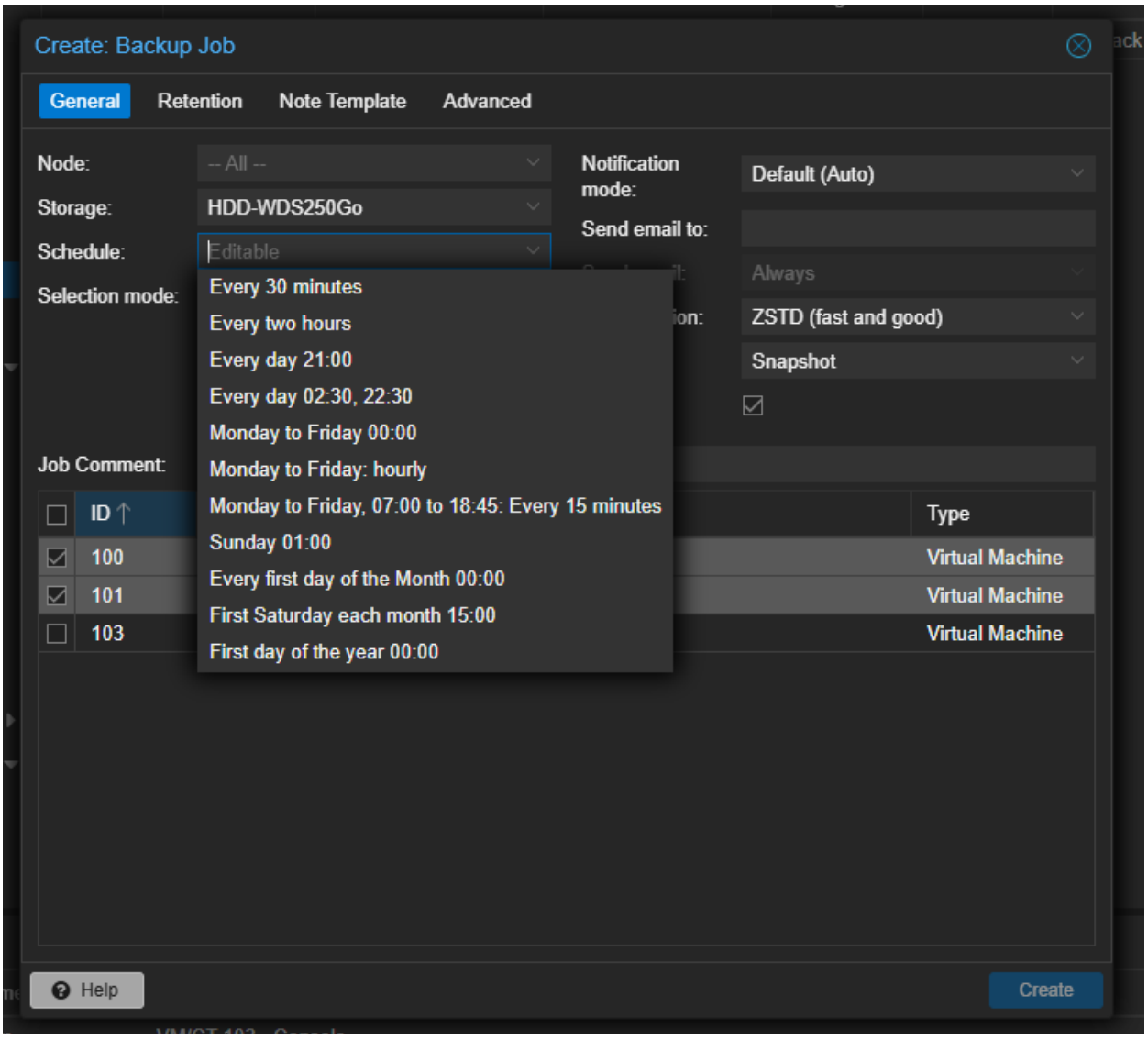
11. Mise en place d'un système de backup

Pour éviter toutes pertes de données importantes, pertes de configuration ou encore de VM, Proxmox propose un système de backup automatique pour sauvegarder vos machines virtuelles. Celà sécurise vos machines virtuelles au cas où une ou plusieurs serait à devenir corrompue où hors service. Pour ce faire rien de plus simple, tout est dans la catégorie "backup" dans datacenter.



DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Vous pouvez sélectionner les machines virtuelles que vous souhaitez à tout prix sauvegarder et vous pouvez choisir le disque auquel les backups seront stockés. Dans notre cas, nous choisissons de sauvegarder nos machines virtuelles critiques (donc la PfSense et la VM debian 12 qui sert de portail captif et de scan réseau).

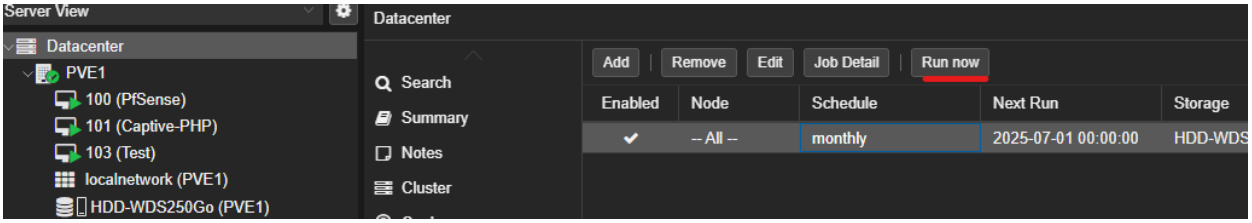


Par défaut. Proxmox vous propose déjà certains horaires pour effectuer vos sauvegardes.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Vous pouvez choisir de faire vos backup automatique :

- Toutes les 30 minutes.
- Toutes les deux heures.
- Tous les jours à 21 heures.
- Tous les jours à 2 heure 30 et 22 heures 30.
- Tous les jours du lundi au vendredi à minuit.
- Tous les jours du lundi au vendredi à l'heure à laquelle vous créer la backup.
- Tous les jours du lundi au vendredi toutes les 15 minutes mais seulement entre 7 heures et 18 heures 45.
- Tous les dimanches à minuit.
- Tous les premier du mois à minuit.
- Tous les premier samedi de chaque mois à 15 heures.
- Tous les premier de l'année à minuit.

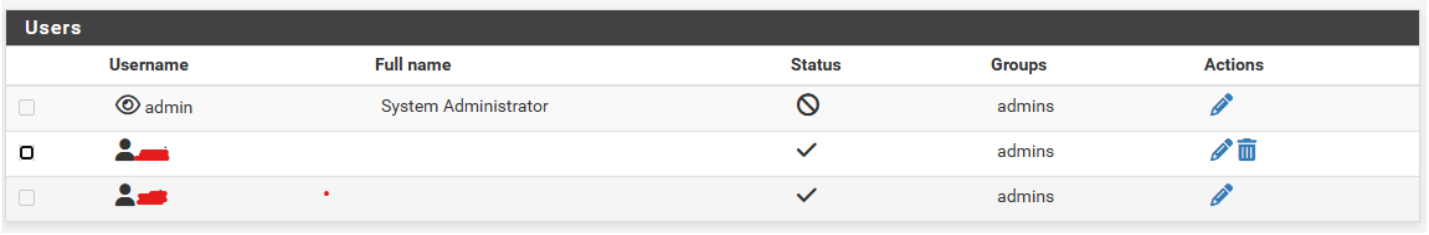


Si la backup automatique ne se lance que dans un moment, le bouton "Run now" sert à démarrer la backup automatique manuellement pour déjà sauvegarder les machines virtuelles.

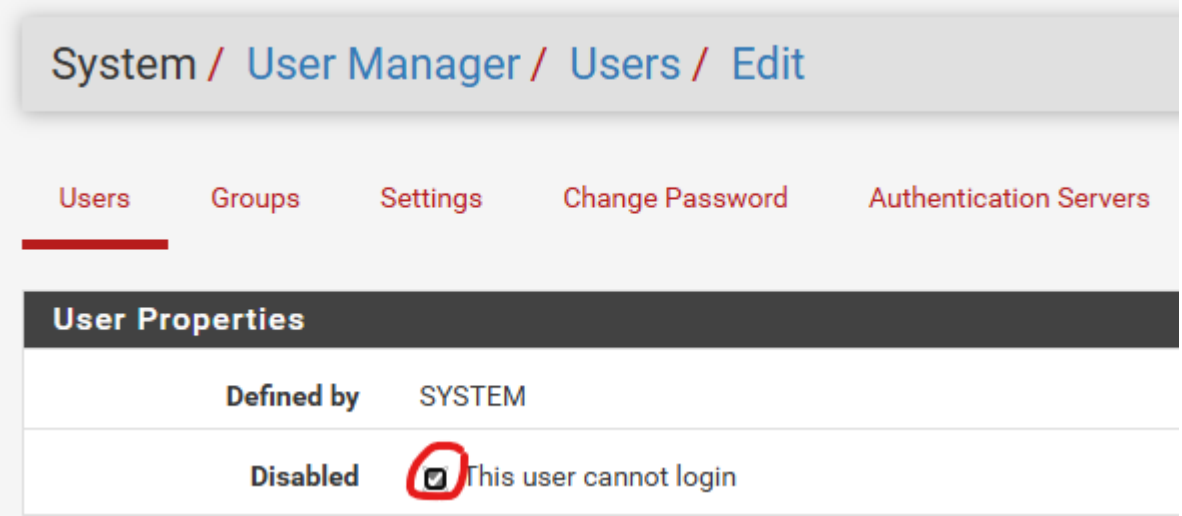
DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

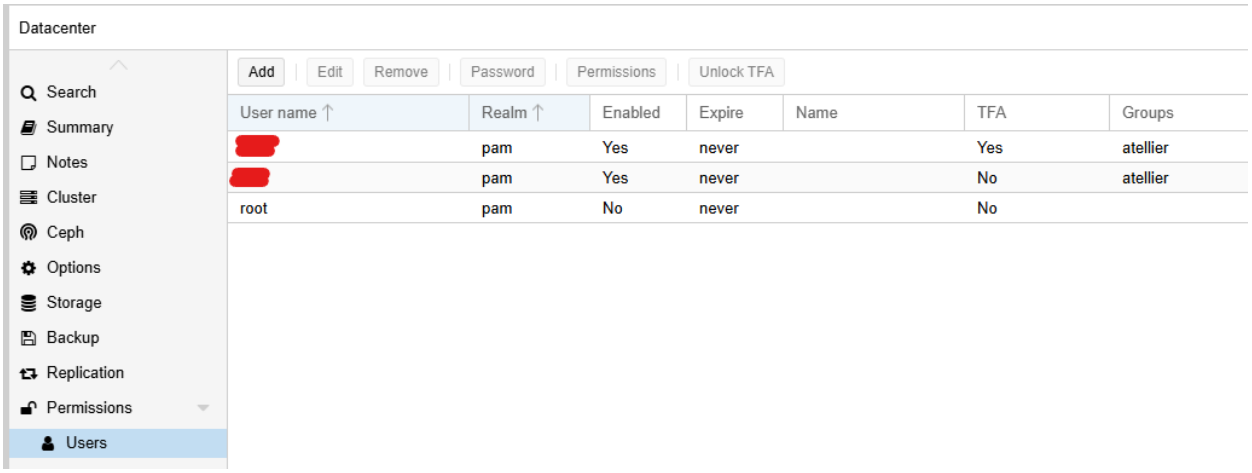
12. Changement des comptes utilisateurs par défaut

Pour une meilleure sécurité, il est recommandé de désactiver les comptes utilisateurs créés par défauts afin d'en créer des seconds avec un nom d'utilisateurs méconnu afin d'éviter toute éventuelle attaque.



Il suffit donc de désactiver la permission de login des utilisateurs créé par défaut. Dans notre premier cas ici, PfSense, grâce à l'option présente ci-dessous dans le "User Manager".





Dans un second cas, désactiver également l'utilisateur par défaut sur le serveur proxmox.

13. Mise en place de NetAlert

NetAlertX est un outil de scan réseau. Il référence tous les appareils connectés au réseau et permet de scanner et de notifier en cas de faille détectée. Pour se faire nous utiliserons d'abord un outil pour faire en sorte que ce services puisse s'installer et fonctionner sur un debian 12 (Brok..). Pour cela, il est nécessaire d'installer docker ou un service similaire.

Premièrement, la première étape est d'installer docker. Après avoir mis la liste des paquets à jour, installer les dépendances à docker avec
"sudo apt-get install apt-transport-https ca-certificates curl gnupg2 software-properties-common".

Ensuite, il est nécessaire d'ajouter le dépôt officiel de Docker, pour ce faire deux commandes sont nécessaires :
"sudo curl -fsSL https://download.docker.com/linux/debian/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg"

"sudo echo "deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/debian $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list"

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Nous pouvons ensuite mettre à nouveau à jour les paquets avec **"sudo apt-get update"** puis installer les paquets pour docker avec **"sudo apt-get install docker-ce docker-ce-cli containerd.io"**

Puis si besoin, le faire lancer par défaut avec **"sudo systemctl enable docker"**

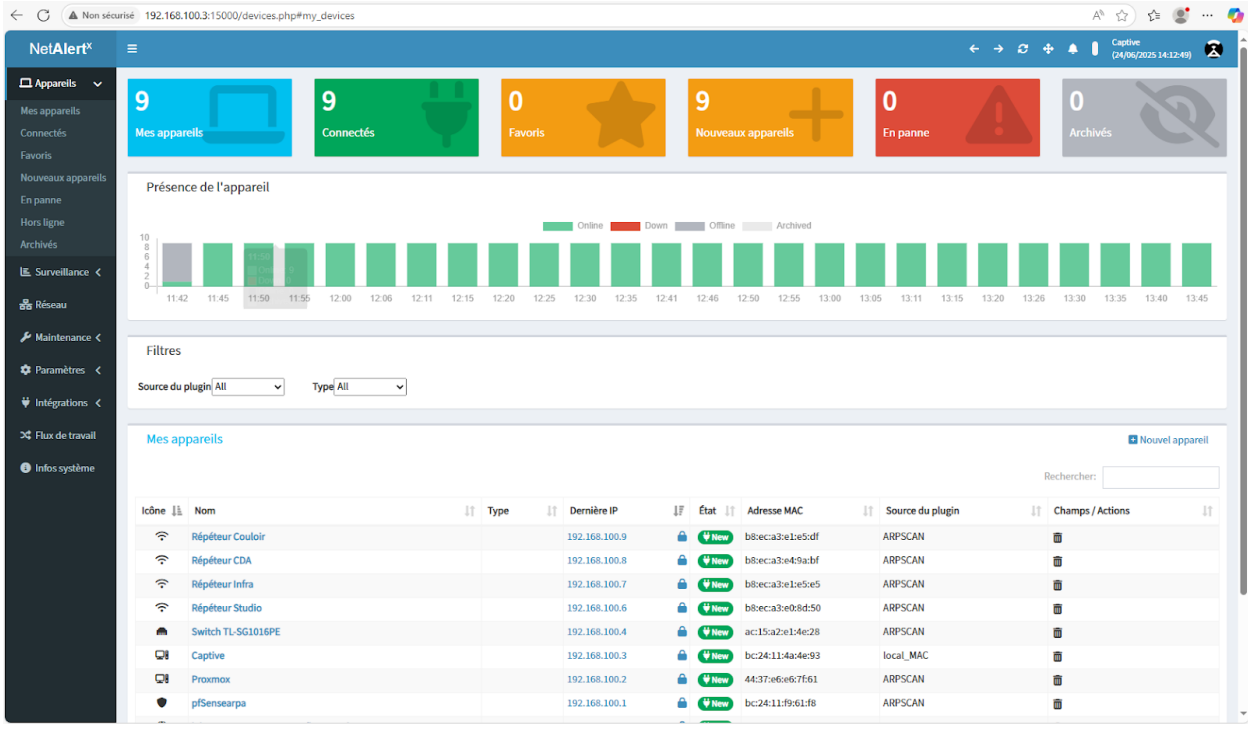
Une fois fait, un emplacement doit être créé et définis pour NetAlertX, donc créer un dossier en le mettant dans le répertoire "/opt/docker-compose". Ensuite, pour faire fonctionner NetAlertX, nous devons créer et éditer un fichier (par exemple "**docker-compose.yml**", avec la configuration suivante :

```
services:
  netalertx:
    image: jokobsk/netalertx:latest   # Nom de l'image Docker à utiliser
    container_name: netalertx        # Nom du conteneur Docker
     healthcheck:                    # Vérifier état de santé du conteneur (attention au port)
      test: curl -f http://127.0.0.1:15000/ || exit 1
    mem_limit: 1g                    # Limite RAM pour le conteneur
    security_opt:
        - no-new-privileges:true            # Option de sécurité contre l'élévation de privilèges
    volumes:
     - config:/app/config:rw         # Volume pour "config" (configuration)
     - db:/app/db:rw                 # Volume pour "db" (base de données)
     - log:/app/front/log:rw         # Volume pour "log" (journaux)
    environment:
     TZ: Europe/Paris                # Fuseau horaire
      PORT: 15000                    # Port à utiliser sur la machine locale (adapter le healthcheck en fonction)
      # ALWAYS_FRESH_INSTALL: true    # Réinitialise l'application (effacer toutes les données)
    network_mode: host               # Mode "host" obligatoire pour cette application
     restart: on-failure:5           # Restart en cas de problème avec le conteneur ; 5 tentatives pour relancer
volumes:                             # Créer automatiquement les volumes nécessaires
  config:
  db:
  log:
```

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Pour lancer le conteneur, rendez vous dans le dossier ou se situe le fichier yml et entrer la commande **"docker compose up -d"**.

Le panel d'administration et de configuration de NetAlertX devrait maintenant être disponible à l'adresse de la VM avec le port configuré dans le fichier ci-dessus. Dans notre cas **192.168.100.3:15000**



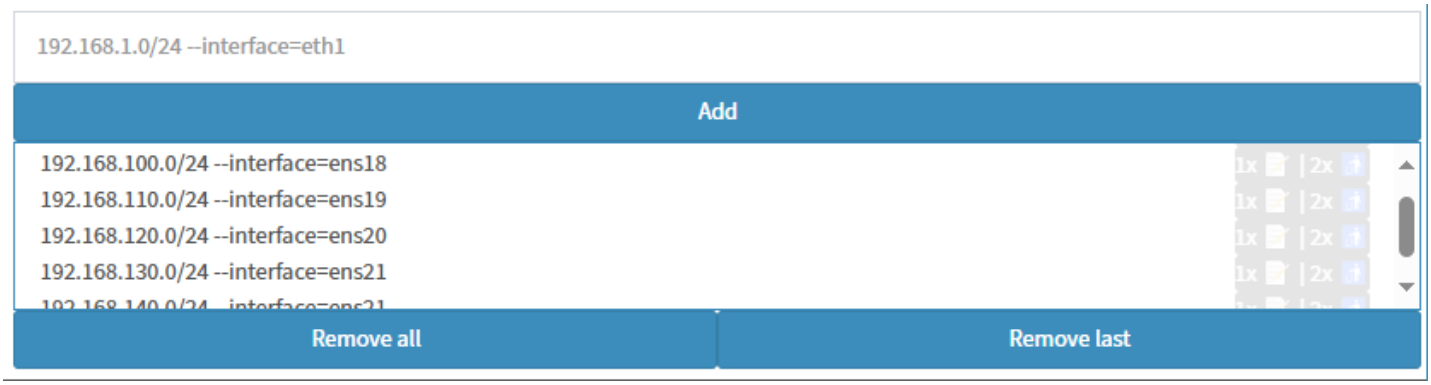
Une fois dans le panel, pour que le service scan toutes les vlans, des cartes réseaux doivent être créer et configurer dans proxmox.

Network Device (net0)	virtio=BC:24:11:4A:4E:93,bridge=vmbr0
Network Device (net1)	virtio=BC:24:11:9A:16:31,bridge=vmbr0,tag=55
Network Device (net2)	virtio=BC:24:11:BF:D2:20,bridge=vmbr0,tag=60
Network Device (net3)	virtio=BC:24:11:1F:B9:2F,bridge=vmbr0,tag=65
Network Device (net4)	virtio=BC:24:11:76:A4:12,bridge=vmbr0,tag=70
Network Device (net5)	virtio=BC:24:11:32:F4:94,bridge=vmbr0

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Les cartes doivent avoir leur tag respectif. Attention à décocher le firewall dans proxmox.

Ensuite, il ne reste plus qu'à ajouter les scan réseau dans NetAlertX dans la catégorie "settings" puis "core". C'est le paramètre nommé "Network to scan".



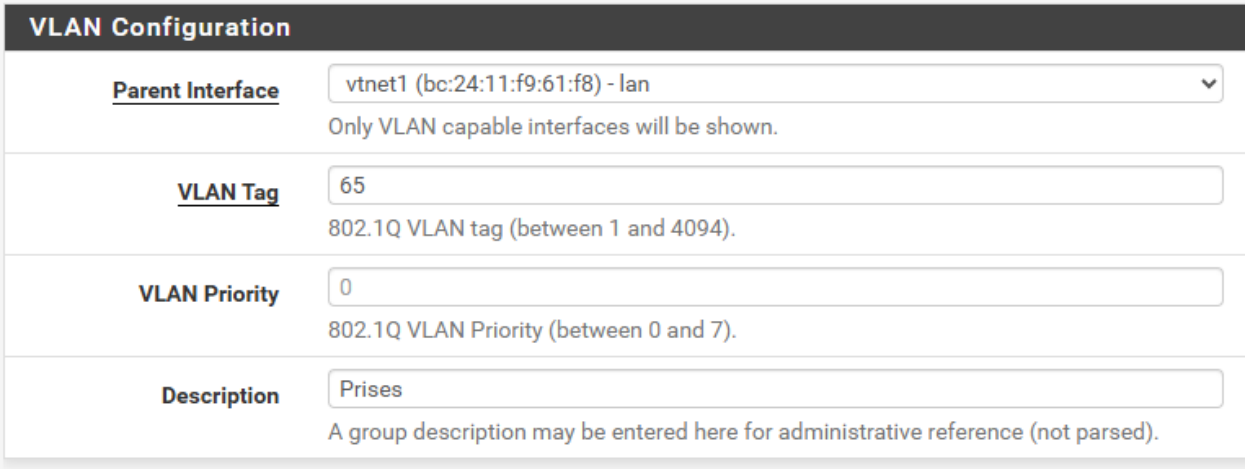
Chaque carte réseau doit correspondre à sa vlan tag. N'oubliez pas de config le fichier **interfaces**, vous pouvez soit définir une IP fixe, soit définir l'ip en DHCP.

```
  GNU nano 7.2
# This file describes the network interfa
# and how to activate them. For more info

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens18
iface ens18 inet static
        address 192.168.100.3/24
        gateway 192.168.100.1

allow-hotplug ens19
iface ens19 inet dhcp

allow-hotplug ens20
iface ens20 inet dhcp

allow-hotplug ens21
iface ens21 inet dhcp

allow-hotplug ens22
iface ens22 inet dhcp
```

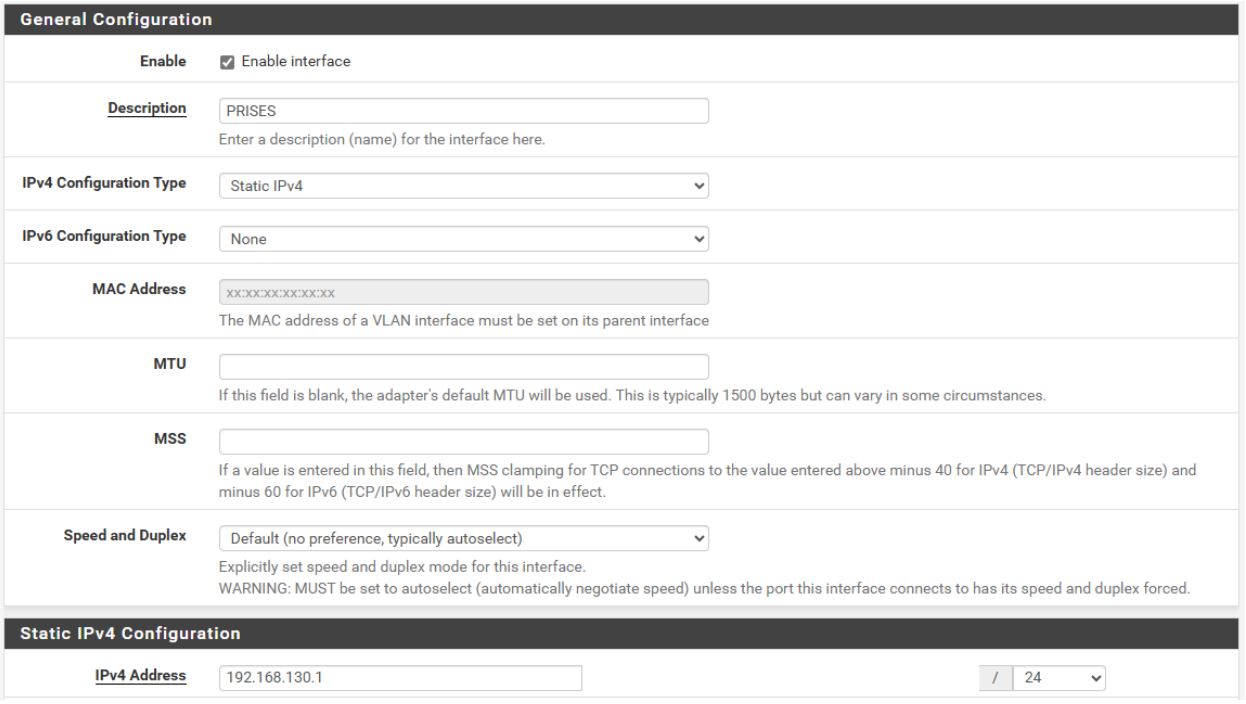
DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

14. Bonus : Configurer imprimantes, téléphonie, prise murales

Nous allons commencer par créer une nouvelle vlan pour les prises murales. Globalement la procédure est la même, créer une vlan dans PfSense.



Également créer une interface pour un réseau séparé, avec une autre plage d'adresse IP.



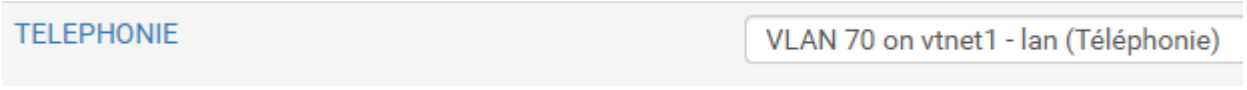
Pour cette interface, les règles seront exactement les mêmes que pour les étudiants. Il ne manquera plus qu'à configurer le port du switch pe dans la vlan nécessaire pour qu'elle tag toutes les paquets venant du switch qui possèdes toutes les connexions aux prises murales.

Pour attribuer les IP aux clients, toujours activer le serveur DHCP et définir la plage d'IP à attribuer aux postes.

Il faut ensuite configurer le port du switch sur la nouvelle vlan, le switch 24 ports sera donc entièrement configuré sur la vlan des prises murales.

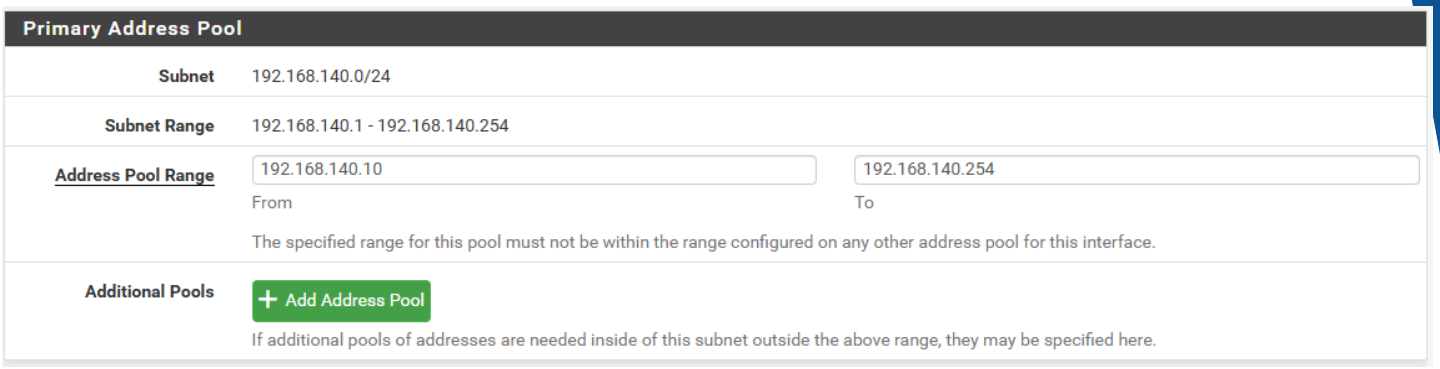
Pour l'imprimante, dans le contexte actuel, il suffit juste de la mettre dans le réseau de l'équipe de l'entreprise.

Enfin, le téléphone nécessite d'être isolé dans un sous réseau, pour éviter toutes interférences. Il faut donc créer une dernière vlan accès pour la téléphonie. Il est donc nécessaire d'ajouter une nouvelle interface avec une nouvelle vlan et de lui attribuer une adresse IP pour la passerelle.

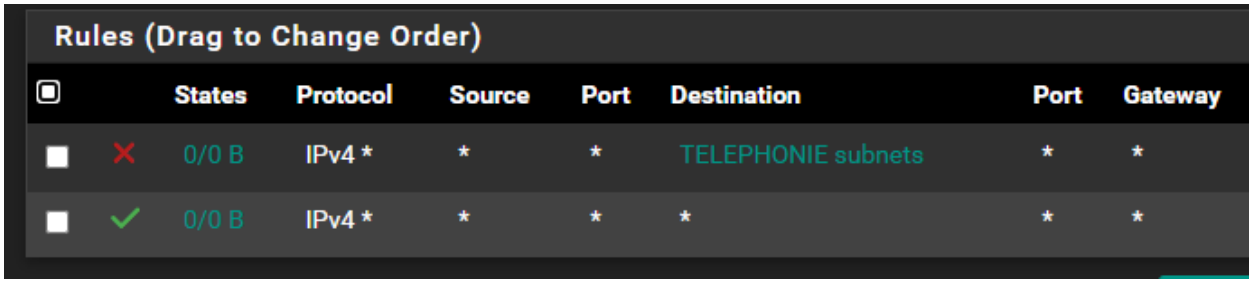


A ne pas oublier qu'il faut également configurer un autre serveur DHCP sur cette interface réseau.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE



Pour ce qui est des règles pour l'interface réservée à la téléphonie, la configuration ne nécessite pas de règles particulières. Vous pouvez laisser passer tous les paquets en autorisant tous les protocoles vers n'importe quelle direction.



N'oubliez pas de configurer votre téléphone, de le mettre dans la vlan correspondante.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

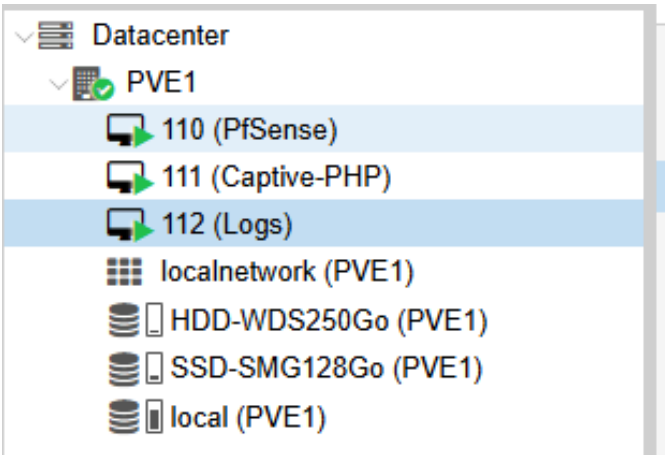
RÉCAP DE L'INFRASTRUCTURE :

Interface	Network port
WAN	vtnet0 (bc:24:11:e0:e1:1b)
ADMINISTRATEURS	vtnet1 (bc:24:11:f9:61:f8)
FORMATEURS	VLAN 55 on vtnet1 - lan (Équipe)
ETUDIANTS	VLAN 60 on vtnet1 - lan (Étudiants)
PRISES	VLAN 65 on vtnet1 - lan (Prises)
TELEPHONIE	VLAN 70 on vtnet1 - lan (Téléphonie)

5 sous réseaux sont donc gérer par PfSense, 4 d'entre eux sont donc configurés en vlans par PfSense.

- Le lan Administrateur est donc utilisé par le VPN pour administrer et gérer tous les sous réseaux.
- La vlan 55 est donc celle utilisée par l'équipe de l'entreprise et à pour but de séparer les appareils des formateurs de ceux des étudiants.
- La vlan 60 est donc celle que les étudiants devront utiliser pour accéder à internet dans les salles de classes.
- La vlan 65 est adapté pour les étudiants qui souhaitent si besoin utiliser une des prises murales ethernet pour se connecter au réseau.
- La vlan 70 est utilisé pour isoler toute la téléphonie IP afin d'éviter tous troubles et tous problèmes technique lié aux transferts de paquet.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE



3 Machines virtuelles sont en ligne sur le serveur proxmox.

- La machine **110** est donc notre VM PfSense, servant de routeur pour nos sous réseaux.
- La machine **111** va gérer le captive portal et va donc enregistrer les emails et les IP des utilisateurs connectés sur le réseau étudiants.
- Enfin, la machine **112** va enregistrer les logs de tous les appareils de l'infrastructure.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

LAN (PfSense)	
PfSense	192.168.100.1
Proxmox	192.168.100.2
Captive portal (VM Debian)	192.168.100.3
Switch PoE	192.168.100.4
Switch 52 Port	192.168.100.5
Répéteur Studio	192.168.100.6
Répéteur Infra	192.168.100.7
Répéteur CDA	192.168.100.8
Répéteur Couloir	192.168.100.9

LAN (FreeBox)	
FreeBox Delta	192.168.1.254
PfSense	192.168.1.185 (DHCP static)

VLAN 55 (PfSense) Équipe	
PfSense	192.168.110.1
Imprimante	192.168.110.x (DHCP)

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

VLAN 70 (PfSense) Téléphonie	
PfSense	192.168.110.1
Téléphone	192.168.140.x (DHCP)

VLAN 60 (PfSense) Étudiants	
PfSense	192.168.120.1

VLAN 65 (PfSense) Prises murales	
PfSense	192.168.130.1