

Projet ECKHO

Table des matières

Table des matières	1
Présentation du projet	3
Adressage IP SALAUN TRAVELS	4
Schéma d'architecture réseau.....	5
Création des serveurs Active Directory.....	6
Paramétrage IP de DC2 :	7
Paramétrage IP de DC1 :	8
Nous pouvons donc maintenant configurer le DNS :	9
Configuration du DHCP :	11
Configuration du serveur mail	14
Installation de hMailServer	14
Serveur Web	16
Installation de MariaDB, Apache2, et MySQL.	16
Création base de données Wordpress	17
Installation de Wordpress/ droits / déplacement des fichiers au bon endroit.	17
Configuration Apache	17
Activation du site et du module rewrite	18
Accès site	18
Mot de passe des utilisateurs.....	19
AP4 : Perfectionnement et ajout sur l'infrastructure réseau de Salaun.....	21

Configuration Pfsense	21
Création et installation de Pfsense	21
Acceptation des licences (Copyright and Distribution Notice)	22
Initialisation du réseau (Network Installation)	23
Configuration du mode réseau WAN (vtnet0).....	24
Choisir la version de pfSense à installer.....	25
Configuration des VLANs au premier démarrage	26
Confirmation des interfaces réseau	26
Configuration de l'adresse LAN	27
Fin de l'installation et affichage des interfaces	28
Problème : Impossible d'accéder à l'interface pfSense / pas d'accès Internet	28
Ajout d'utilisateur	29
Création de l'Unité d'Organisation	29
Création de l'utilisateurs	31
Crée un groupe	32
Mettre de droits au groupe.....	34
Réseau Wi-Fi Invités	35
1) Pré-requis (réseau & Wi-Fi).....	35
Installation outil de monitoring.....	39
Installation via Debian.....	39
Ajout d'un serveur	42
Serveur de fichier	47
Sauvegarde Centralisée	48
DMZ	51
Segmentation Réseau — VLANs.....	54

Présentation du projet

Le projet ECKHO consiste à concevoir et déployer une infrastructure informatique complète incluant :

- Un domaine Active Directory,
- Des services réseau (DNS, DHCP),
- Un pare-feu pfSense,
- Un serveur Web (WordPress),
- Un serveur mail,
- Un réseau Wi-Fi Invités isolé,
- Un outil de supervision (Centreon),
- Un serveur de fichiers centralisé.

L'objectif est d'obtenir une infrastructure sécurisée, segmentée et supervisée.

Adressage IP SALAUN TRAVELS

Serveurs (LAN — 10.5.0.0/16)

VM	Rôle	IP	Masque	VLAN
DC1	Contrôleur de domaine principal	10.5.10.0	/16	LAN
DC2	Contrôleur de domaine secondaire	10.5.20.0	/16	LAN
Serveur-mail	Messagerie centralisée	10.5.40.0	/16	LAN
SerFich	Serveur de fichiers	10.5.50.0	/16	LAN
BACKUP	Sauvegarde centralisée	10.5.10.5	/8	LAN
PfSense	Pare-feu / Routeur	10.5.30.1	/16	LAN

DMZ (VLAN 50 — 10.9.0.0/16)

VM	Rôle	IP	Masque	VLAN
DMZ	Passerelle DMZ	10.6.60.1	/24	DMZ
Web	Serveur Web WordPress	10.6.60.10	/24	DMZ

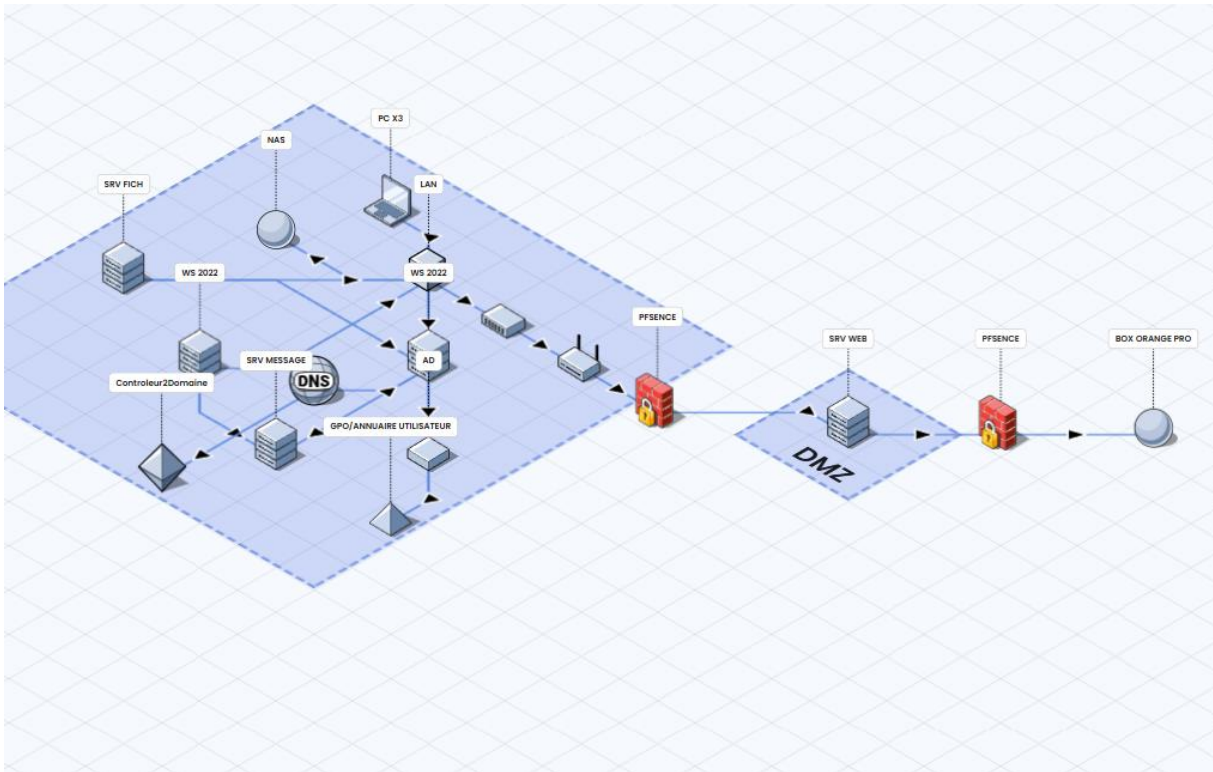
Postes clients

VM	Rôle	IP	VLAN
Client2	Poste utilisateur siège	DHCP (10.7.x.x)	Siège (30)

VLANs PfSense

VLAN	Nom	Gateway	Réseau
LAN	Serveurs	10.5.30.1	10.5.0.0/16
20	WiFi Invité	10.6.0.1	10.6.0.0/16
30	Siège	10.7.0.1	10.7.0.0/16
40	Agences	10.8.0.1	10.8.0.0/16
50	DMZ	10.9.0.1	10.9.0.0/16
60	WiFi Interne	10.10.0.1	10.10.0.0/16

Schéma d'architecture réseau.



Création des serveurs Active Directory

130 (DC2)
131 (DC1)

Création des active directory dans Proxmox.

Paramétrage IP de DC2 :

Propriétés de : Protocole Internet version 4 (TCP/IPv4)



Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP :	<input type="text" value="10 . 5 . 20 . 0"/>
Masque de sous-réseau :	<input type="text" value="255 . 255 . 0 . 0"/>
Passerelle par défaut :	<input type="text" value="10 . 5 . 10 . 0"/>

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :	<input type="text" value="10 . 5 . 10 . 0"/>
Serveur DNS auxiliaire :	<input type="text" value="127 . 0 . 0 . 1"/>

Valider les paramètres en quittant

Avancé...

OK Annuler

Paramétrage IP de DC1 :

Propriétés de : Protocole Internet version 4 (TCP/IPv4) ×

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP :

Masque de sous-réseau :

Passerelle par défaut :

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :


Serveur DNS auxiliaire :

Valider les paramètres en quittant Avancé...

Nous rejoignons le domaine avec DC2 dans notre cas salaun.lan :

Paramètres système avancés Utilisation à distance

Nom de l'ordinateur Matériel

 Windows utilise les informations suivantes pour identifier votre ordinateur sur le réseau.

Description de l'ordinateur :

Par exemple : "Serveur de production IIS" ou "Serveur de gestion".

Nom complet de l'ordinateur : DC2.SALAUN.LAN

Domaine : SALAUN.LAN

Pour renommer cet ordinateur ou changer de domaine ou de groupe de travail, cliquez sur Modifier. Modifier...

Nom	Type	Type de contro...	Site	Description
DC1	Ordinateur	GC	Default-First-Si...	
DC2	Ordinateur	GC	Default-First-Si...	

Nous pouvons donc maintenant configurer le DNS :

The screenshot shows the 'Gestionnaire DNS' (DNS Manager) console. The left pane shows the tree structure: DNS > DC1 > Zones de recherche directe. The right pane displays a table of DNS zones.

Nom	Type	État	État DNSSEC
_msdcs.SALAUN.LAN	Serveur principal intégré à Act...	En cours d'e...	Non signé
SALAUN.LAN	Serveur principal intégré à Act...	En cours d'e...	Non signé

Fichier Action Affichage ?

Nom	Type	Données	Horodate
(identique au dossier parent)	Source de nom (SOA)	[3], dc1.salaun.lan., hostm...	statique
(identique au dossier parent)	Serveur de noms (NS)	dc2.salaun.lan.	statique
(identique au dossier parent)	Serveur de noms (NS)	dc1.salaun.lan.	statique
10.5.10.0	Pointeur (PTR)	DC1.SALAUN.LAN.	statique

Gestionnaire DNS

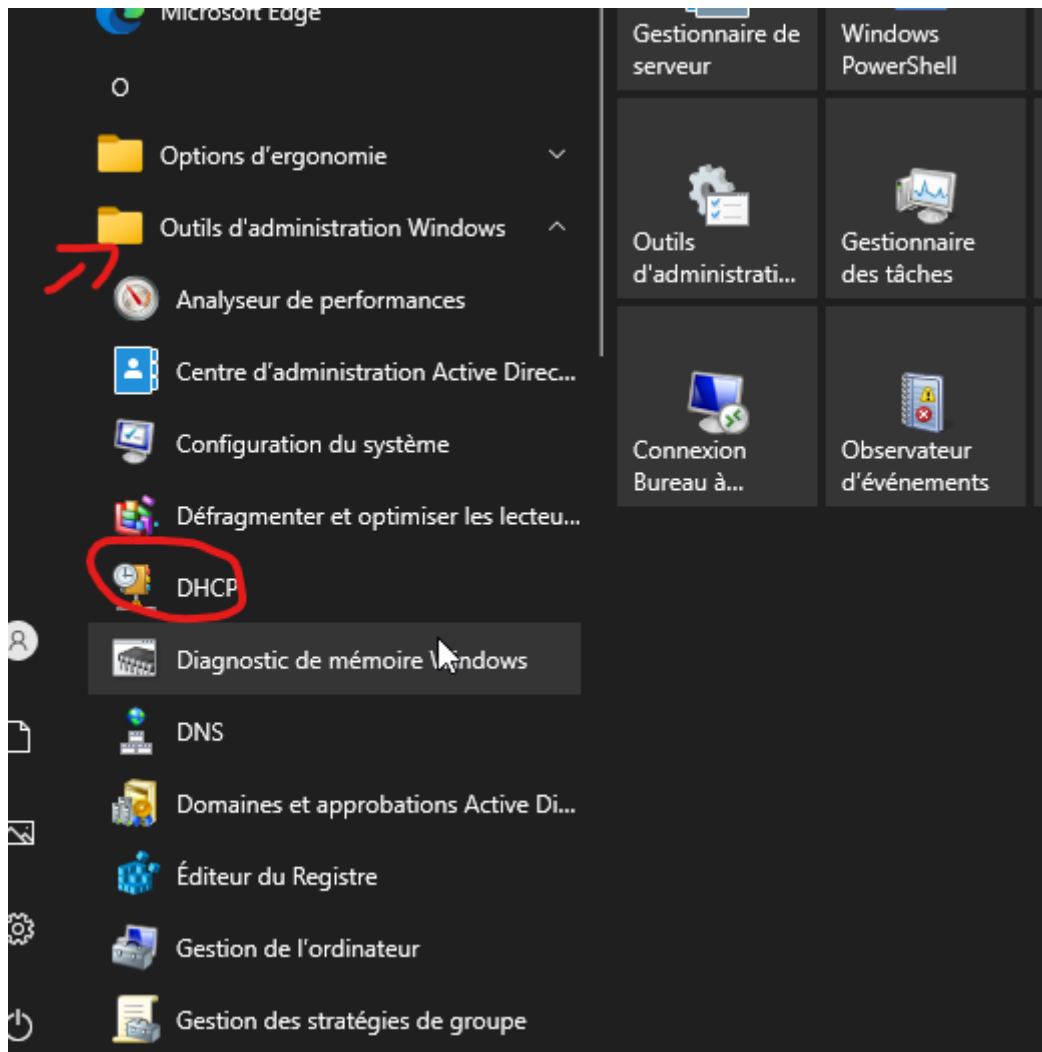
Fichier Action Affichage ?

Nom	Type	Données	Horodate
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(identique au dossier parent)	Source de nom (SOA)	[59], dc1.salaun.lan., host...	statique
(identique au dossier parent)	Serveur de noms (NS)	dc2.salaun.lan.	statique
(identique au dossier parent)	Serveur de noms (NS)	dc1.salaun.lan.	statique
(identique au dossier parent)	Hôte (A)	10.5.10.0	13/10/20:
(identique au dossier parent)	Hôte (A)	10.5.20.0	13/10/20:
dc1	Hôte (A)	10.5.10.0	statique
DC2	Hôte (A)	10.5.20.0	statique
www	Alias (CNAME)	dc1.SALAUN.LAN.	statique

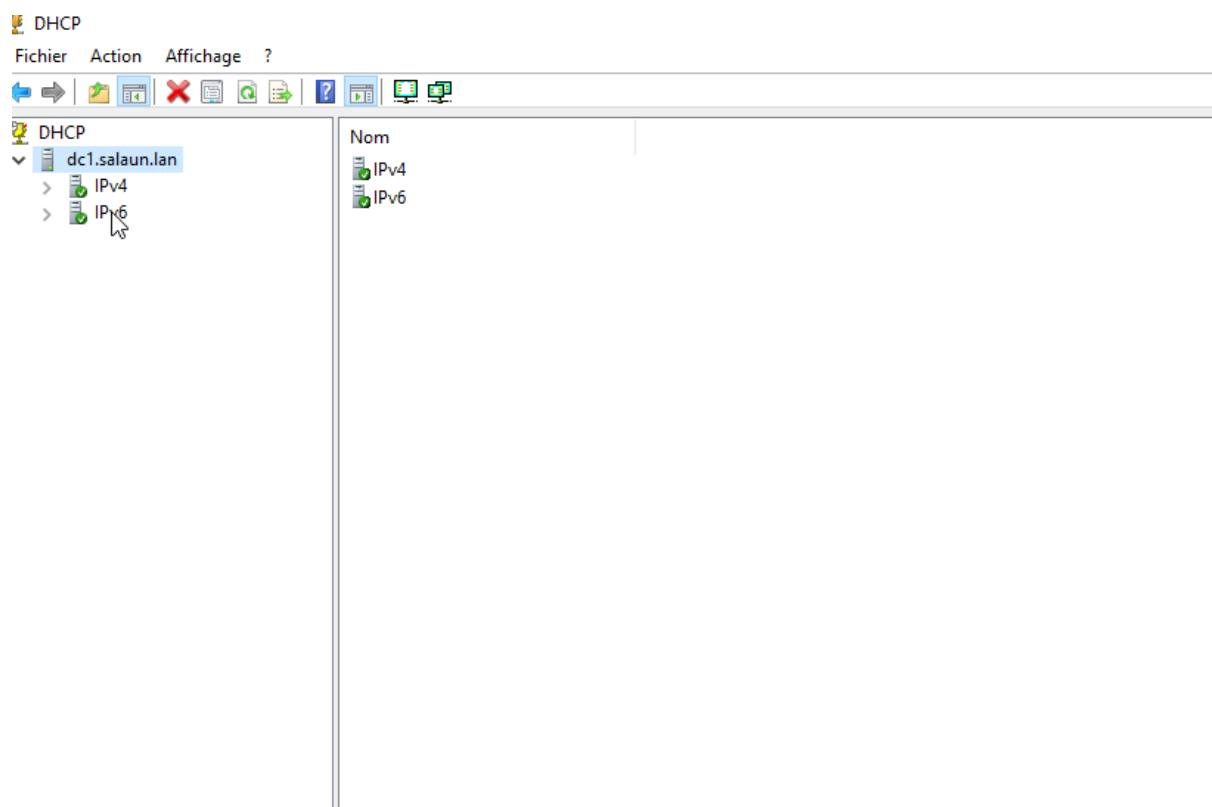
Configuration du DHCP :

On active le DHCP depuis l'assistant d'ajout de rôles et de fonctionnalités.

Dans « Outils d'administration Windows » cliquez sur DHCP.

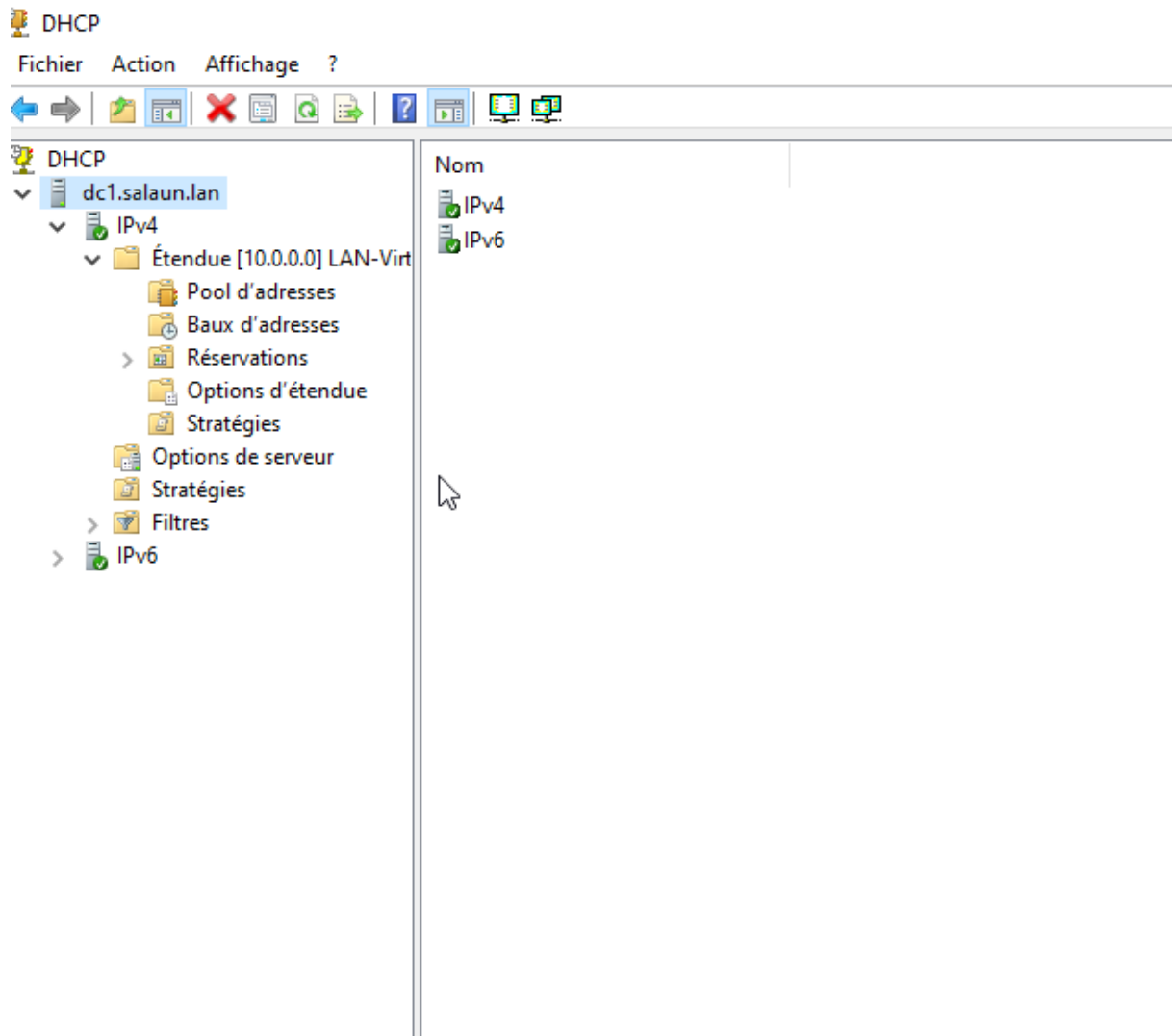


Vous arriverez sur cette page :

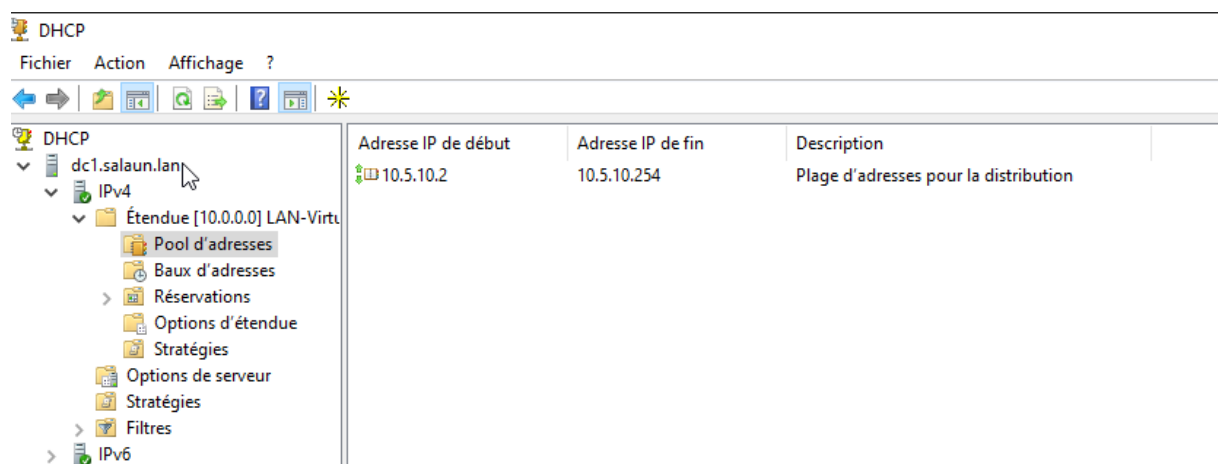


En effectuant un clic droit sur IPv4 puis « nouvelle étendue » et suivre les différentes étapes.

Vous devriez obtenir ce résultat :

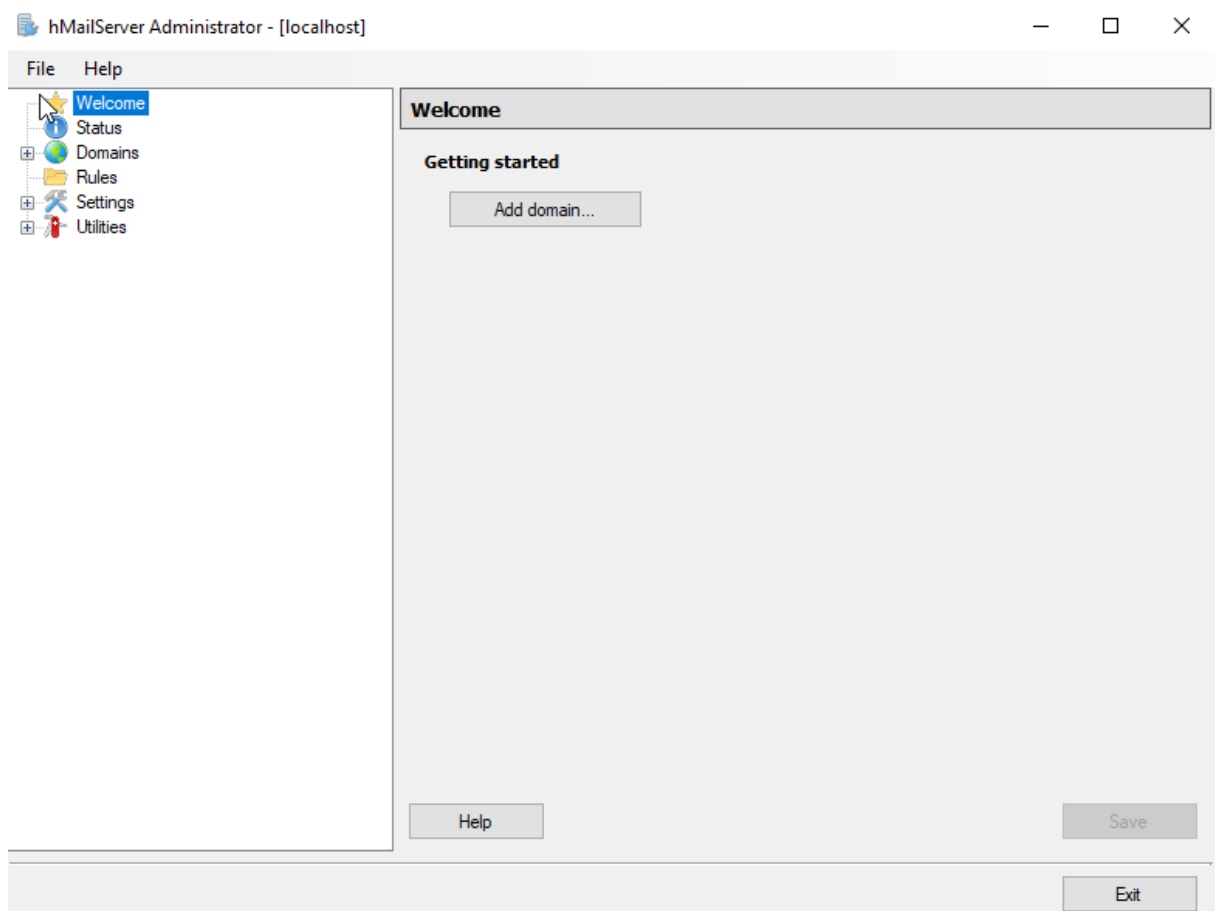


Une fois sur cette page allez dans pool d'adresses pour pouvoir ajouter notre etendue d'adresses que les différents clients recevront :



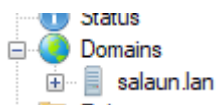
Configuration du serveur mail

Installation de hMailServer

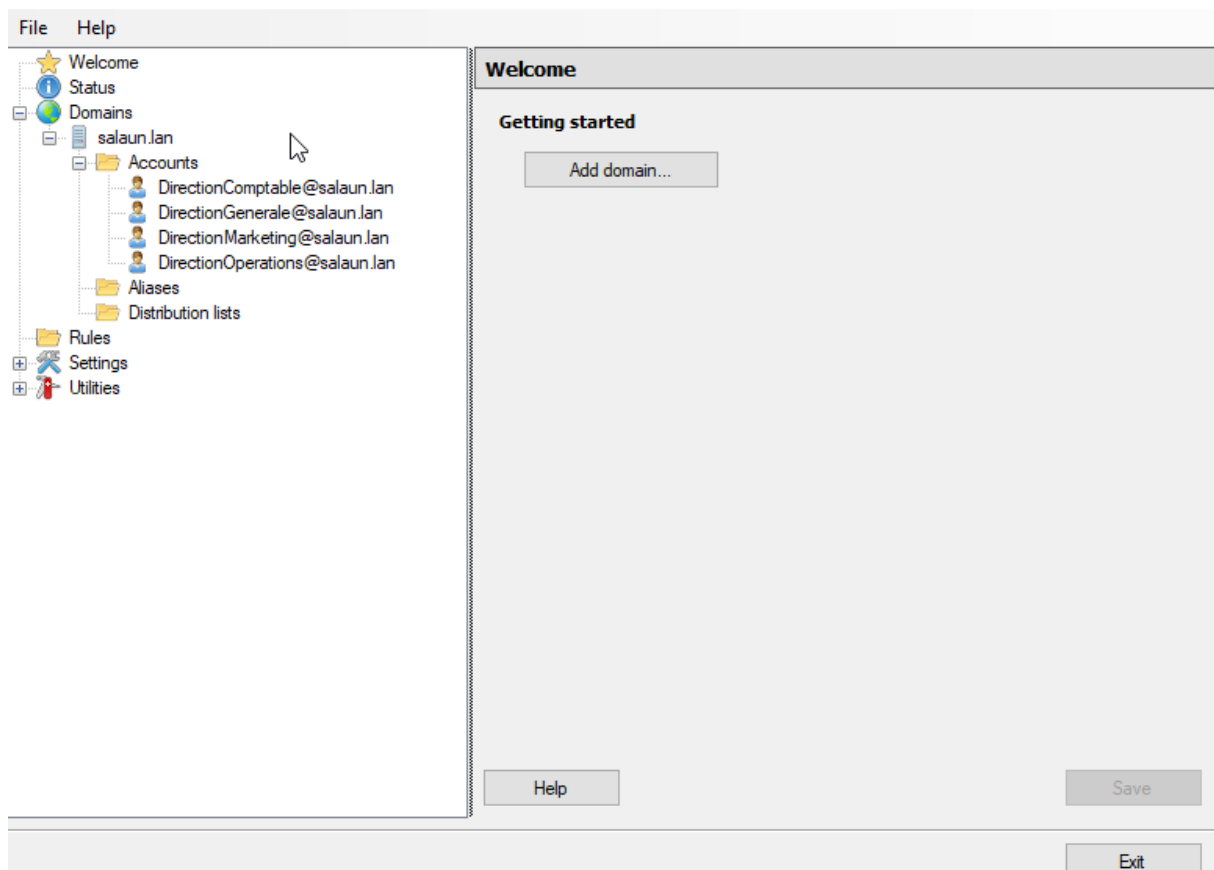


Après l'installation on arrive sur cette page et on ajoute un domaine.

Dans notre cas salaun.lan

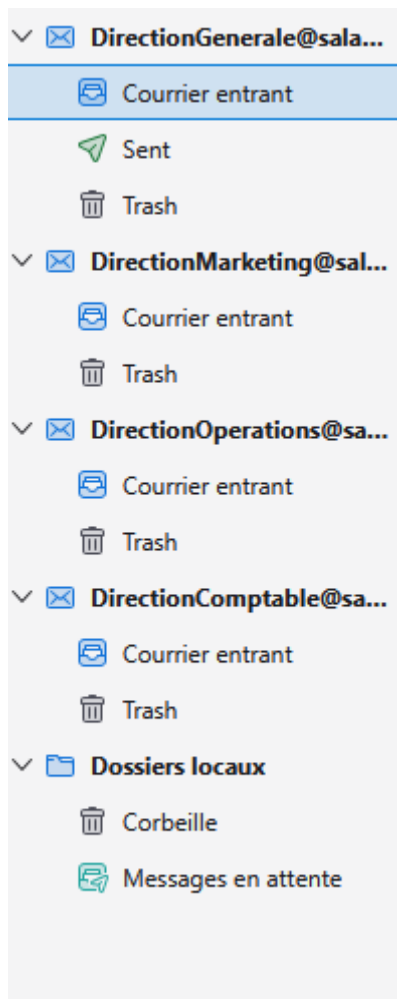


Puis dans « Accounts » nous ajoutons les comptes.



Nous choisissons un client mail ici Mozilla Thunderbird

Dans « Paramètres des comptes nous ajoutons les comptes déjà renseignés dans hMailServer »



Serveur Web

Mise en place d'une machine Debian 12.

|-> Ip fixe : 10.5.60.0

```
root@Web:/etc/apache2/sites-available# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0@if451: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether bc:24:11:0d:ed:9b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.5.60.0/24 brd 10.5.60.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe0d:ed9b/64 scope link
        valid_lft forever preferred_lft forever
root@Web:/etc/apache2/sites-available#
```

Installation de MariaDB, Apache2, et MySQL.

|-> apt install apache2 -y

```
|->apt install mariadb-server -y
```

```
|-> sudo apt install php php-mysql php-curl php-gd php-mbstring php-xml php-xmlrpc  
php-soap php-intl php-zip libapache2-mod-php -y
```

Création base de données Wordpress

```
|->CREATE DATABASE wordpress_db;
```

```
CREATE USER 'wordpress_user'@'localhost' IDENTIFIED BY 'MDP';
```

```
GRANT ALL PRIVILEGES ON wordpress_db.* TO 'wordpress_user'@'localhost';
```

```
FLUSH PRIVILEGES;
```

```
EXIT;
```

Installation de Wordpress/ droits / déplacement des fichiers au bon endroit.

```
|->wget https://wordpress.org/latest.tar.gz tar -xvzf latest.tar.gz sudo mv wordpress  
/var/www/html/ sudo chown -R www-data:www-data /var/www/html/wordpress sudo  
chmod -R 755 /var/www/html/wordpress
```

Configuration Apache

```
|->nano /etc/apache2/sites-available/wordpress.conf
```

Y ajouter :

```
<VirtualHost *:80>
```

```
    ServerAdmin admin@example.com
```

```
    DocumentRoot /var/www/html/wordpress
```

```
    ServerName votre-domaine.com
```

```
<Directory /var/www/html/wordpress/>
```

```
    Options FollowSymlinks
```

```
    AllowOverride All
```

```
    Require all granted
```

```
</Directory>
```

```
    ErrorLog ${APACHE_LOG_DIR}/error.log
```

```
    CustomLog ${APACHE_LOG_DIR}/access.log combined
```

```
</VirtualHost>
```

Activation du site et du module rewrite

```
|->a2ensite wordpress.conf
```

```
|->a2enmod rewrite
```

```
|->systemctl restart apache2
```

Accès site

```
http://10.5.60.10
```

Erreur à éviter en créant le serveur WordPress éviter de mettre une adresse IP de réseau comme 10.5.60.0 le zéro à la fin signifie adresse de réseau il faut mettre une adresse de machine comme exemple : 10.5.60.10 . car le pfSense bloque l'accès avec l'adresse 10.5.60.0

Pourquoi pfSense bloque l'accès avec 10.5.60.0

10.5.60.0 = adresse réseau

Dans un réseau /16, .0 identifie tout le réseau, pas une machine.

Une machine ne peut pas utiliser cette IP.

NAT / Redirection pfSense

pfSense doit savoir vers quelle machine envoyer le trafic WAN.

Avec .0, il ne sait pas quelle machine réelle doit recevoir le paquet.

Résultat : la redirection ne fonctionne pas → site inaccessible.

Passerelle .1

.1 est généralement pfSense lui-même, donc pas utilisable par le serveur.

Solution : donner au serveur une IP valide comme 10.5.60.10

PfSense peut maintenant rediriger correctement le trafic WAN → serveur → WordPress accessible.

Mot de passe des utilisateurs

Nom	Prenom	Role	MDP
PODER	VALY	Compta fournisseur	3cz3LDgJt
PHILON	VALERIE	Compta fournisseur frais généraux	6Co?zLxrDs
AUTRET	FRANCK	Directeur de réseau	H@!6bCP!gm
MARCHAND	FREDERIC	Directeur	L5JVOrW
COURSIER	STEFAN	Informatique	SdxWW23
DEMAY	ROSELINE	Compta clients	o@6a84Nxx\$
ALIX	PASCALE	Compta générale	SRsKRE6@Lg
JEAGLE	MARIE	Commercial	t4pSr9M\$gs
BERTHEL	ANAIS	Accueil	T5i5?NiH\$3
PENPENY	HUGUES	Administrateur réseaux et systemes	Sz!ecygP4o
LEMEN	MANON	Exploitation	7Xdi?rdBdy
PERRON	AURELIE	Formalités	hm46d@Gftf
COLLET	AUDE	Gestion des produits Autocar France et étrangers	9Bp\$HDCMt4
JUSTAL	JULIE	Gestion des voyages	QdT!rNtb9S
ROCHEFORT	ISABELLE	Maquettiste	bx&NGTF43R
PANIS	OLIVIER	Pilote amateur	zBK6QpTe3
LOEB	SEBASTIEN	Pilote pro	DimAqFK8\$L
GUINARD	PATRICIA	Prod	9D!i@zGFMX
THOUROUDE	ERIC	Production avion	PfRdYj&q7E

ROLLAND	ANGELIQUE	Qualité	\$kXrph?K4\$
LEBEC	FLORENCE	Responsable Agence	h&bRToxax7
SALAUN	HUGO	Service web	t4\$JpN8x7s!
PAULI	PHILIPPE	Transport	\$p7jtaKz6x

SQL Server 2022
😊 — ✕

Express Edition

L'installation s'est correctement terminée.

NOM D'INSTANCE
SQLEXPRESS

ADMINISTRATEURS SQL
WIN-GD3EK34UIMN\Administrateur

FONCTIONNALITÉS INSTALLÉES
SQLENGINE

VERSION
16.0.1000.6, RTM

CHAÎNE DE CONNEXION
Server=localhost\SQLEXPRESS;Database=master;Trusted_Connection=True

DOSSIER DU JOURNAL D'INSTALLATION SQL SERVER
C:\Program Files\Microsoft SQL Server\160\Setup Bootstrap\Log\2025121

DOSSIER DU SUPPORT D'INSTALLATION
C:\SQL2022\Express_FRA

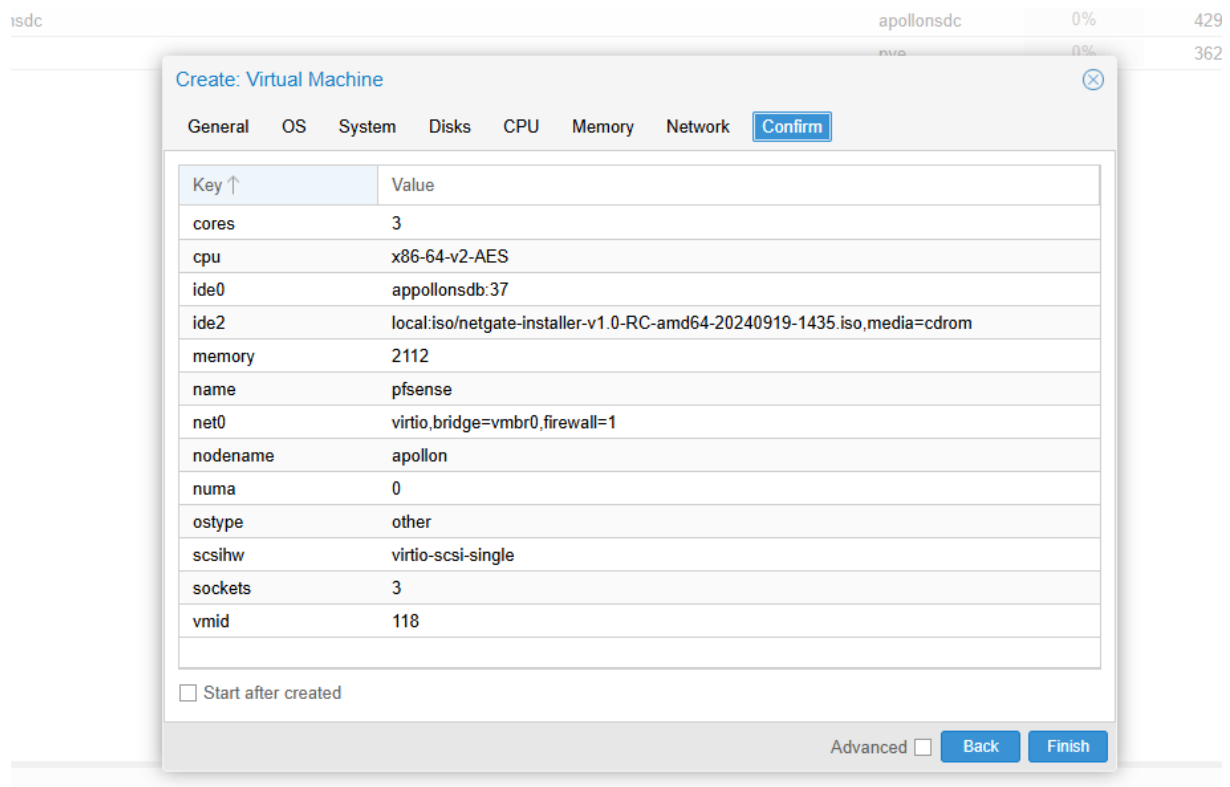
DOSSIER DES RESSOURCES D'INSTALLATION
C:\Program Files\Microsoft SQL Server\160\SSE\Resources

🔑 Se connecter maintenant
Personnaliser
Installer SSMS
Fermer

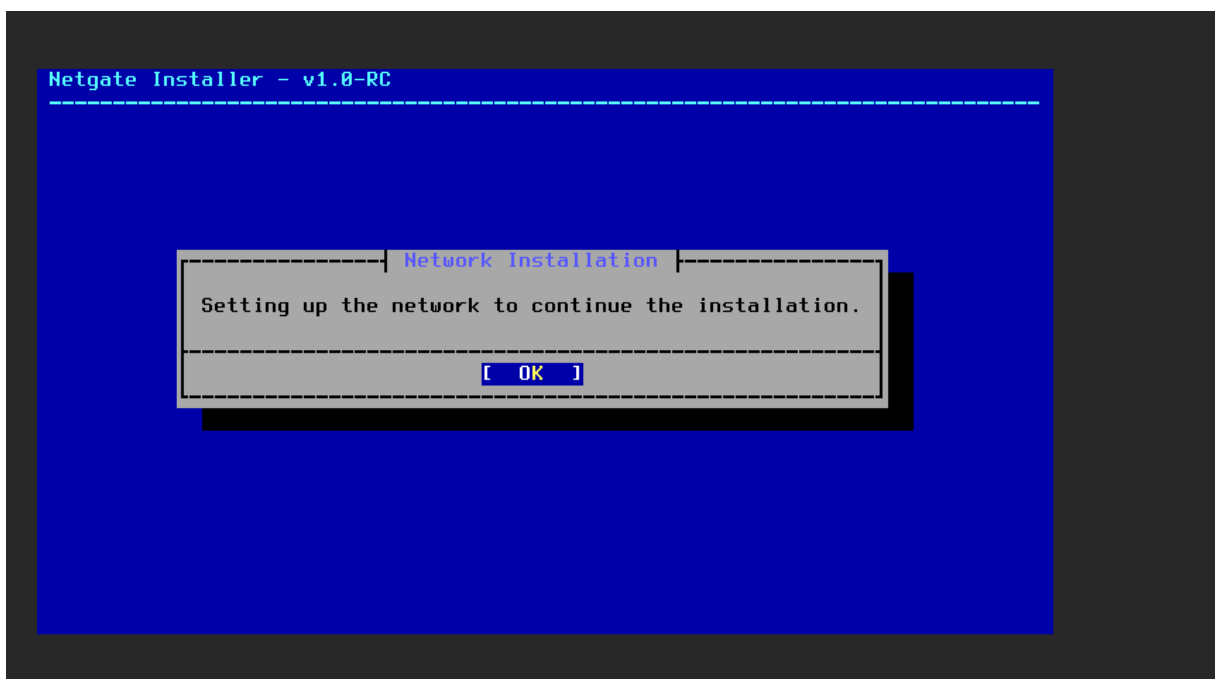
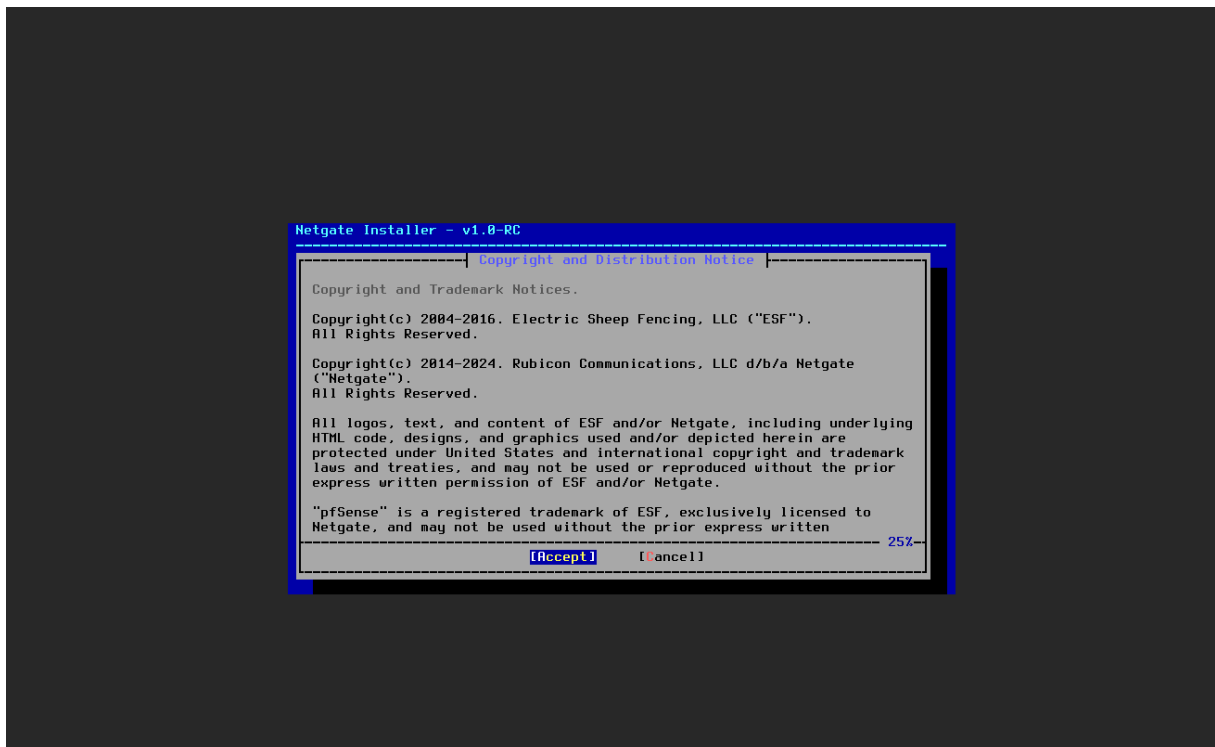
AP4 : Perfectionnement et ajout sur l'infrastructure réseau de Salaun.

Configuration Pfsense

Création et installation de Pfsense



Voici une capture de la configuration de la machine virtuelle. Si tous les paramètres sont corrects, cliquer sur Finish pour lancer la création de la machine virtuelle.



Acceptation des licences (Copyright and Distribution Notice)

Lorsque l'installateur PfSense démarre, la première fenêtre affichée contient les informations de copyright et de licences d'utilisation.

Cet écran rappelle que PfSense et ses composants sont protégés par les droits d'auteur et que leur utilisation est soumise aux conditions de Netgate.

Action à effectuer :

1. Lire les informations affichées.
2. Sélectionner l'option Accepte à l'aide des flèches du clavier.
3. Valider avec Entrée pour poursuivre l'installation.

Initialisation du réseau (Network Installation)

Après avoir accepté les licences, une fenêtre intitulée "Network Installation" apparaît. Cette fenêtre informe que PfSense procède à la configuration réseau minimale nécessaire pour continuer l'installation.

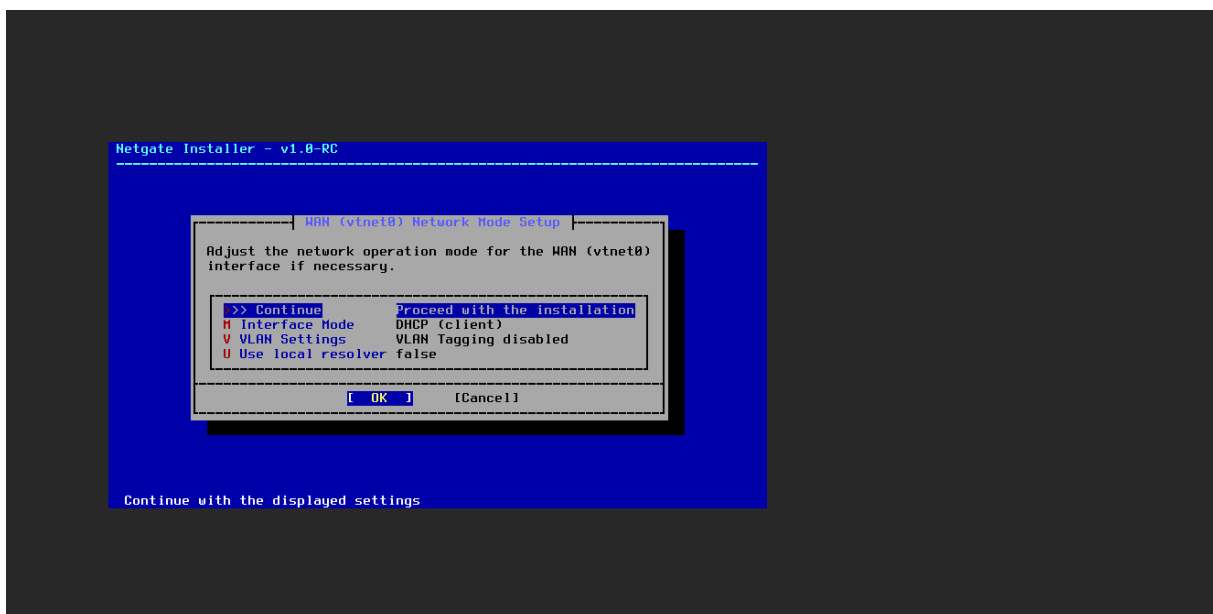
Le message affiché est :

"Setting up the network to continue the installation."

Action à effectuer :

- Appuyer sur Entrée pour valider l'option OK.

Une fois cette étape validée, l'installateur passe automatiquement à la configuration suivante.



Configuration du mode réseau WAN (vtnet0)

Après l'initialisation du réseau, l'installateur affiche la fenêtre « WAN (vtnet0) Network Mode Setup ».

Cette étape permet de choisir le mode de fonctionnement de l'interface WAN de PfSense (ici vtnet0) avant de poursuivre l'installation.

La fenêtre présente plusieurs paramètres configurés par défaut :

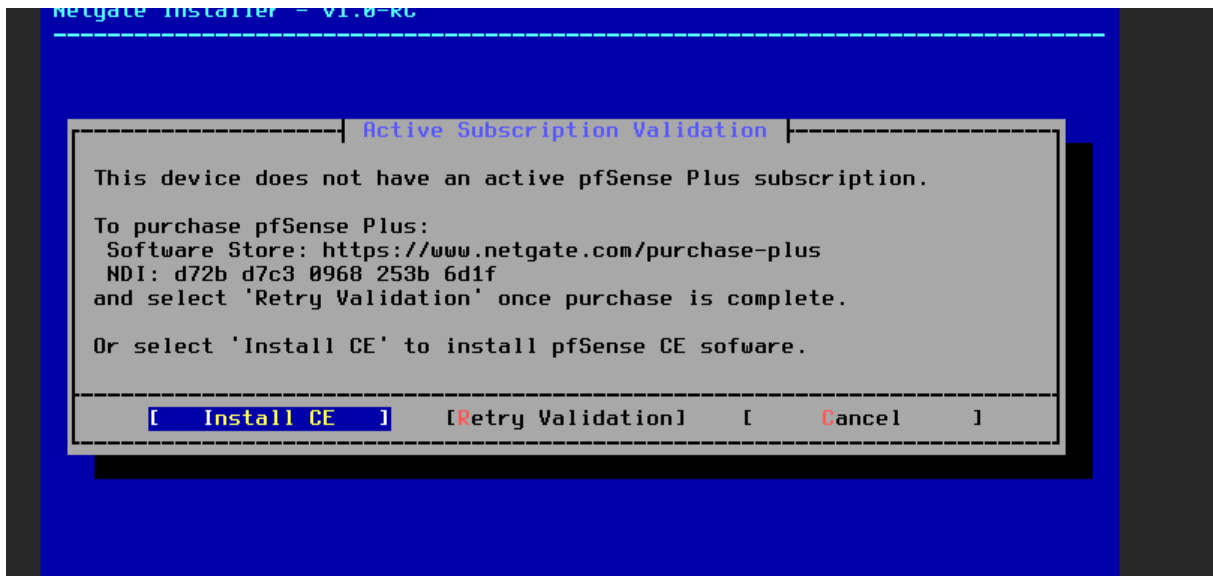
Paramètres affichés :

- Continue : Proceed with the installation
→ Permet de continuer vers la prochaine étape.
- Interface Mode : DHCP (client)
→ L'interface WAN sera configurée en DHCP, c'est-à-dire qu'elle recevra automatiquement une adresse IP du réseau amont.
- VLAN Settings : VLAN Tagging disabled
→ Aucun VLAN n'est activé sur l'interface WAN.
- Use local resolver : false
→ Le résolveur DNS local n'est pas utilisé pendant l'installation.

Action à effectuer :

1. Laisser les paramètres par défaut (sauf cas particulier de configuration réseau spécifique).
2. Sélectionner Continue si ce n'est pas déjà le cas.
3. Valider avec la touche Entrée.
4. Puis choisir OK pour continuer.

L'installation passe ensuite à la configuration suivante.



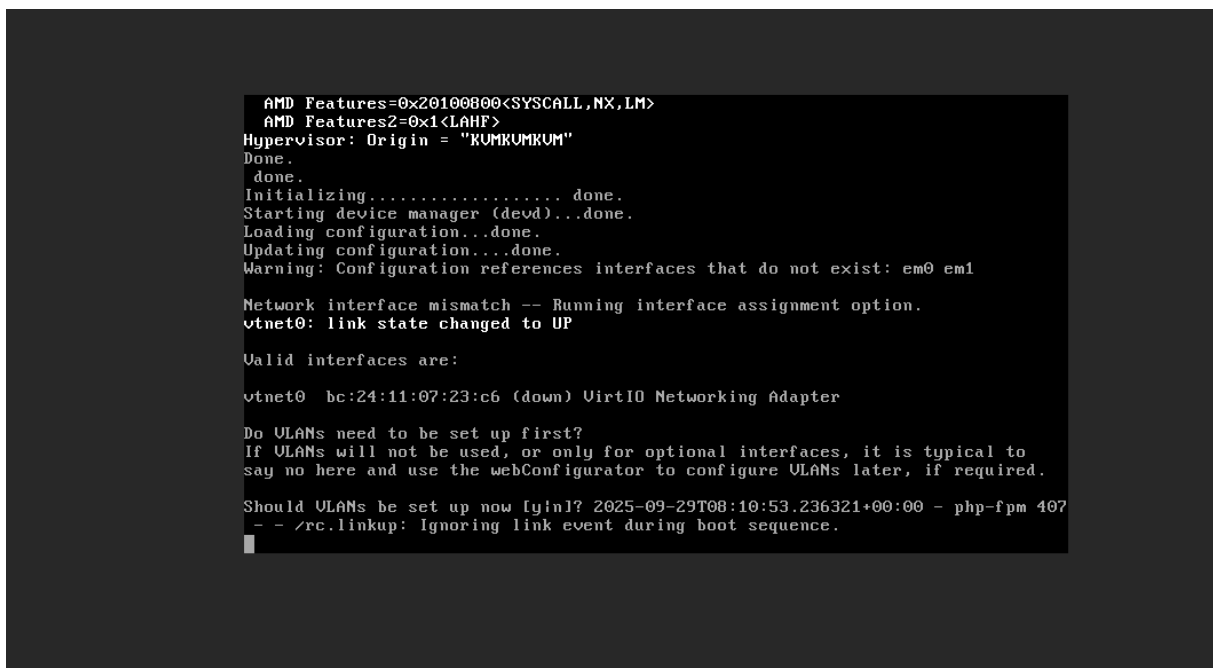
Choisir la version de pfSense à installer

L'installateur indique qu'aucune licence PfSense Plus n'est active sur la machine. Pour continuer gratuitement, il faut installer la version pfSense CE (Community Edition).

Action à faire :

- Sélectionner Install CE
- Valider avec Entrée

Cela lance l'installation de la version gratuite et open-source de pfSense.



Configuration des VLANs au premier démarrage

Au premier démarrage, PfSense détecte les interfaces réseau et demande si des VLANs doivent être configurés maintenant.

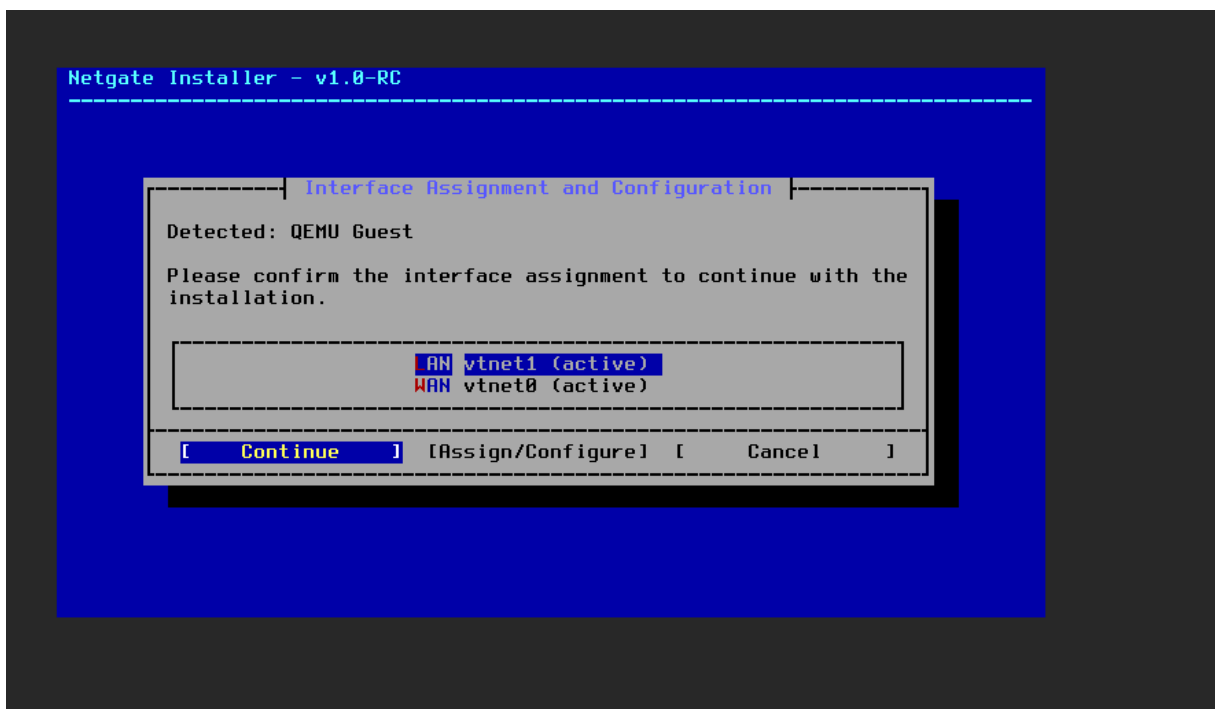
L'écran indique les interfaces disponibles (ex : vtnet0) et pose la question :

“Should VLANs be set up now [y/n]?”

Action à faire :

- Taper n (non)
- Valider avec Entrée

Les VLANs pourront être configurés plus tard via l'interface web si nécessaire.



Confirmation des interfaces réseau

L'installateur affiche les interfaces détectées pour PfSense :

- LAN : vtnet1 (active)
- WAN : vtnet0 (active)

Il s'agit des bonnes interfaces détectées automatiquement.

Action à faire :

- Laisser les interfaces telles quelles

- Sélectionner Continue
- Valider avec Entrée

Cela confirme l'affectation des interfaces et poursuit l'installation

```

Available interfaces:

1 - WAN (em0 - static)
2 - LAN (em1 - static)
3 - VLAN10INFRA (em1.10 - static)
4 - OPT2 (em1.20)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.5.30.0

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 16

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 10.5.255.254

```

Configuration de l'adresse LAN

Dans cette étape, PfSense demande de configurer l'interface LAN manuellement.

Actions réalisées dans la capture :

1. Choix de l'interface à configurer :
→ Saisie : 2 (interface LAN)
2. Adresse LAN via DHCP
→ Réponse : n (configuration manuelle)
3. Nouvelle adresse IPv4 LAN
→ Saisie : 10.5.30.0
4. Masque de sous-réseau (CIDR)
→ Saisie : 16
(équivalent à 255.255.0.0)
5. Gateway IPv4 pour le LAN :
→ Rien à mettre → appuyer sur Entrée
(le LAN n'a pas de passerelle)

```
pfctl: pf not enabled
[2.8.1-RELEASE][root@pfSense.home.arpal/root]: pfctl -d
pfctl: pf not enabled
[2.8.1-RELEASE][root@pfSense.home.arpal/root]: exit
exit
QEMU Guest - Netgate Device ID: a7af53ccf6ed3237ec8c

*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

WAN (wan)          -> em0      -> v4: 10.5.30.254/16
LAN (lan)          -> em1      -> v4: 10.5.30.0/16
```

Fin de l'installation et affichage des interfaces

PfSense a terminé son installation et affiche maintenant un résumé des interfaces réseau configurées.

Informations visibles :

- WAN (em0) → IPv4 : 10.5.30.254/16
- LAN (em1) → IPv4 : 10.5.30.1/16

Cela confirme que pfSense est installé et que les interfaces sont opérationnelles.

Prochaine étape :

Vous pouvez maintenant accéder à l'interface web de pfSense via :

<https://10.5.30.1>

Problème : Impossible d'accéder à l'interface pfSense / pas d'accès Internet

Après l'installation de pfSense, nous avons constaté deux problèmes :

- Impossible d'accéder à l'interface web de pfSense
- Les machines du réseau ne pouvaient pas naviguer sur Internet

Ces problèmes étaient causés par le pare-feu pfSense, qui bloquait le trafic par défaut sur certaines interfaces.

Solution temporaire : Désactivation du pare-feu

Pour vérifier l'origine du problème, nous avons désactivé temporairement le pare-feu PfSense.

Une fois le pare-feu désactivé :

- L'accès à l'interface web de pfSense a immédiatement fonctionné
- L'accès Internet a été rétabli

Cela confirme que le blocage provenait des règles du pare-feu.

Conclusion

La désactivation du pare-feu a permis d'identifier l'origine du problème.

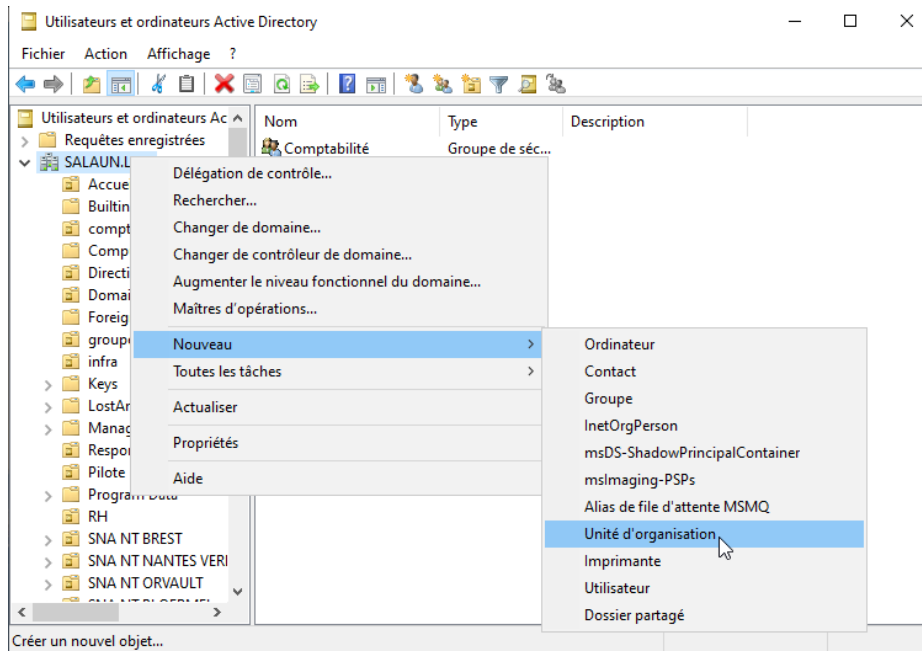
Ensuite, des règles de pare-feu adaptées devront être configurées pour permettre :

- L'accès à l'interface web depuis le LAN
- Le trafic Internet sortant
- Le routage entre réseaux si nécessaire

Ajout d'utilisateur

Création de l'Unité d'Organisation

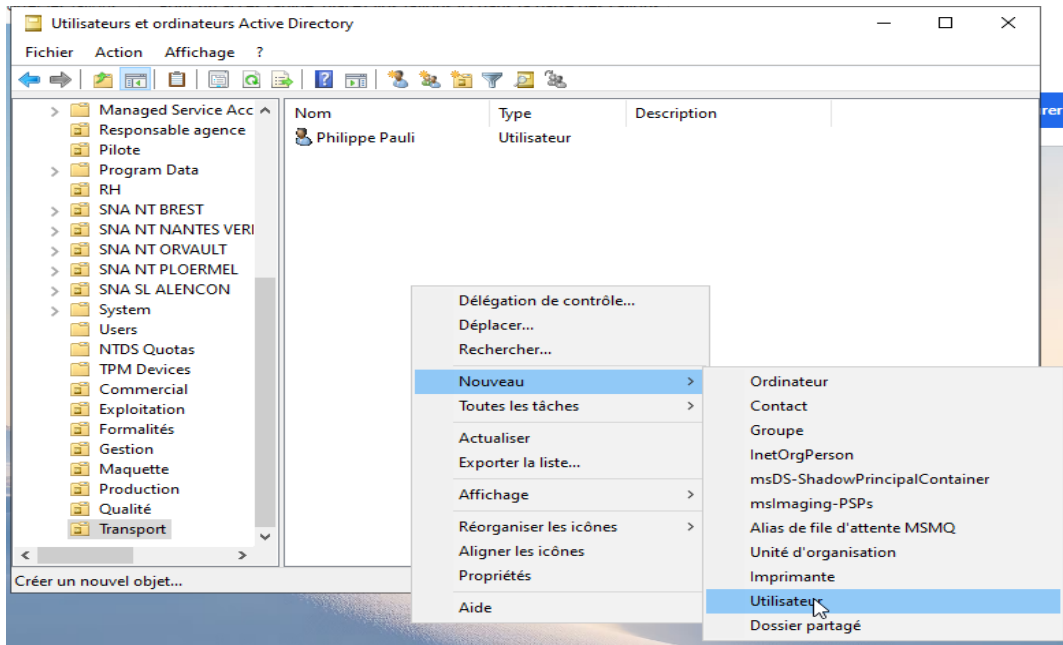
Une unité d'organisation (UO) est un conteneur logique qui sert à organiser les objets du réseau.



Dans Utilisateur et ordinateurs Active Directory effectuer :

- Un clic droit sur votre domaine.
- Positionner sa souris sur nouveau et attendre que le menu déroulant apparaisse.
- Puis choisir Unité d'organisation.

Création de l'utilisateurs



Dans votre UO faire le même cheminement que pour crée une UO mais dans ce cas la vous allez choisir Utilisateur

Nouvel objet - Utilisateur ×

Créer dans : SALAUN.LAN/Transport

Prénom : Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur : @SALAUN.LAN ▼

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : SALAUN\

< Précédent Suivant > Annuler

Vous arriverez donc sur cette page :

-Renseignez donc le prénom, le nom et le nom d'ouverture de session.

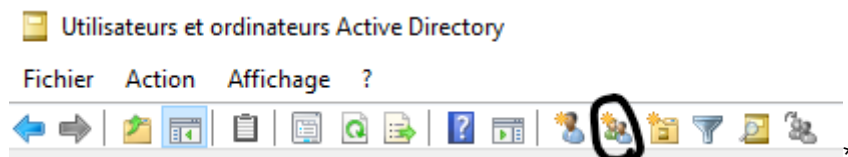
-Puis cliquez sur Suivant.

Une page va donc apparaître :

-Renseignez le mot de passe de cette session puis effectuer les paramètres de votre choix en cochant ou décochant les carrés à gauche des informations.*

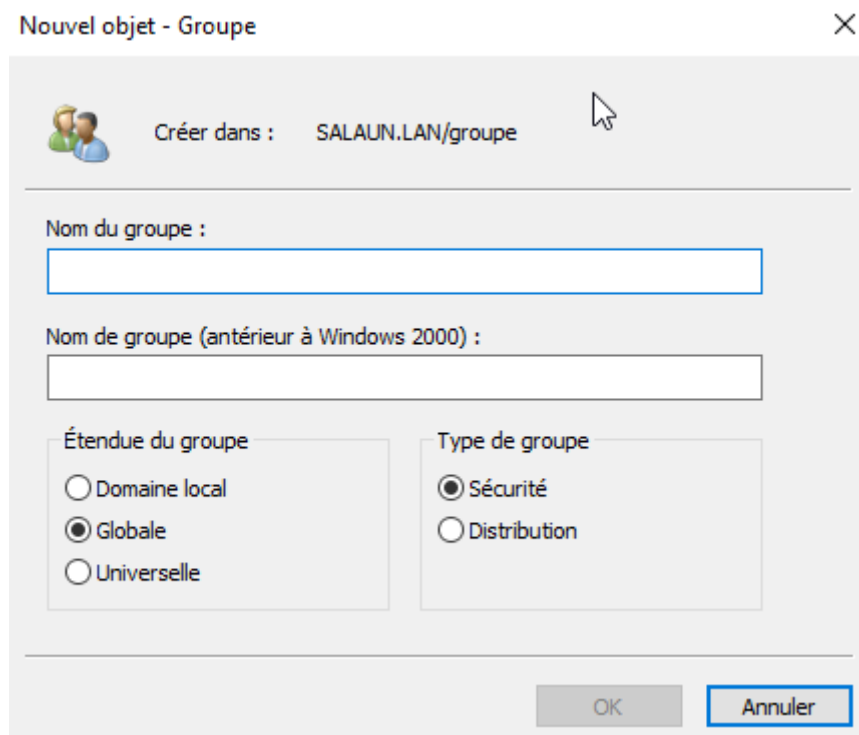
Votre utilisateur est Maintenant créé

Crée un groupe

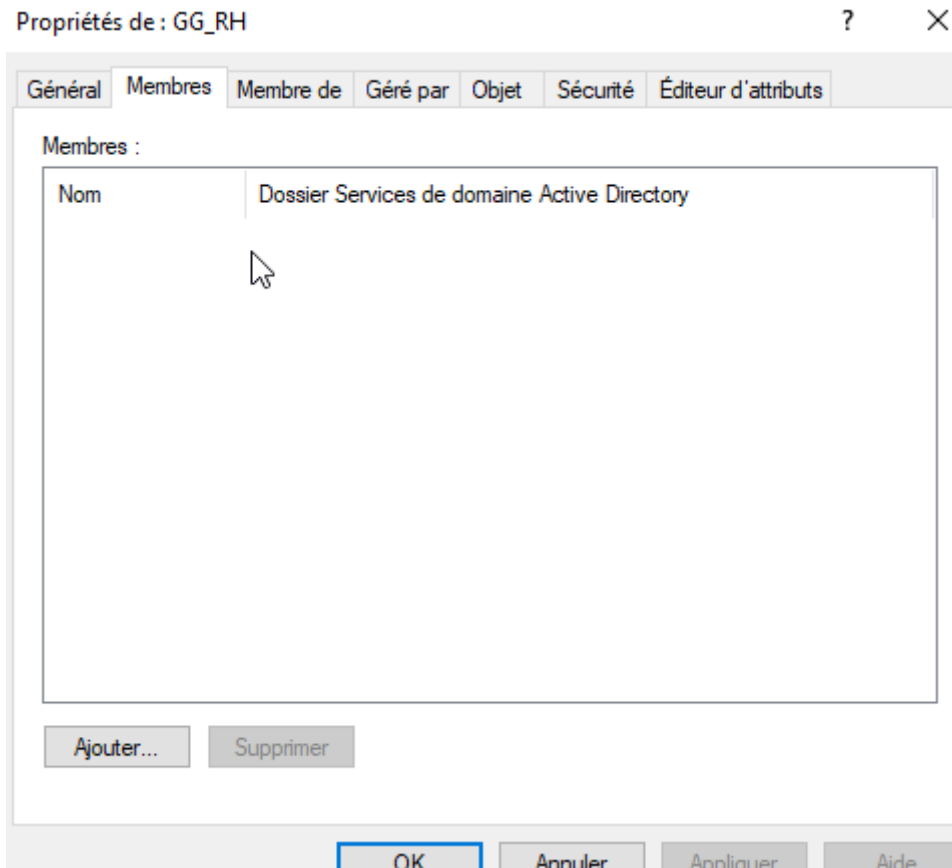


-Sélectionner ce bouton pour crée un groupe.

Vous arriverez sur cette page.

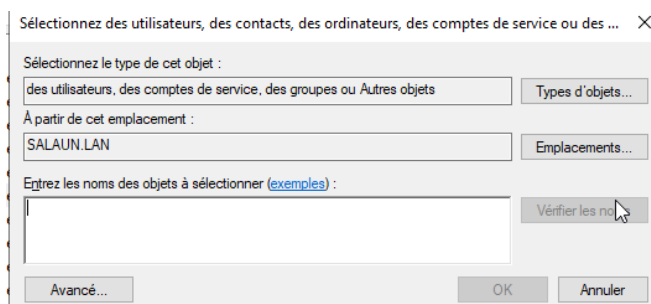
The image shows a screenshot of the 'Nouvel objet - Groupe' (New Object - Group) dialog box. The title bar reads 'Nouvel objet - Groupe' with a close button (X) on the right. Below the title bar, there is a group icon and the text 'Créer dans : SALAUN.LAN/groupe'. The main area contains two text input fields: 'Nom du groupe :' and 'Nom de groupe (antérieur à Windows 2000) :'. Below these fields are two sections: 'Étendue du groupe' (Group Scope) with radio buttons for 'Domaine local', 'Globale' (selected), and 'Universelle'; and 'Type de groupe' (Group Type) with radio buttons for 'Sécurité' (selected) and 'Distribution'. At the bottom, there are 'OK' and 'Annuler' buttons.

Après avoir créé le groupe vous pouvez effectuer un double clic sur le groupe créé pour arriver sur cette page.



Cette page permet d'ajouter des membres au groupe.

-Cliquer donc sur ajouter.

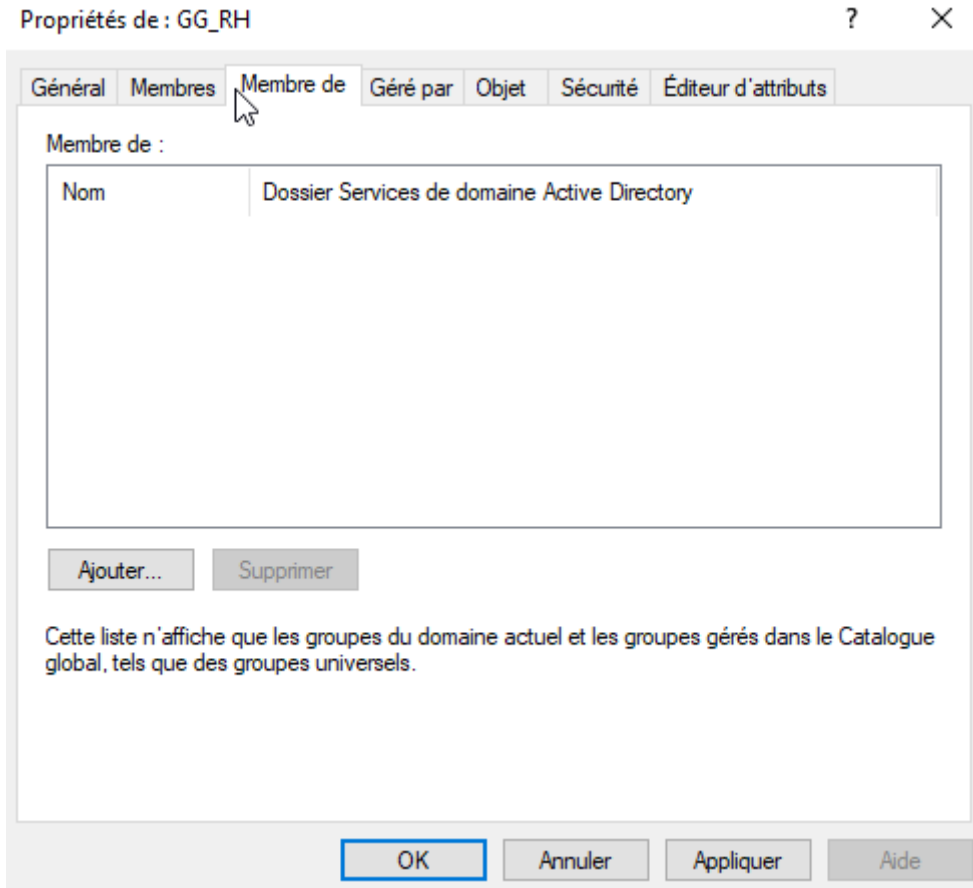


-Entrer le nom du compte à ajouter puis cliquer sur « Vérifier les noms » puis sur ok (vous pouvez ajouter plusieurs utilisateurs à la fois).

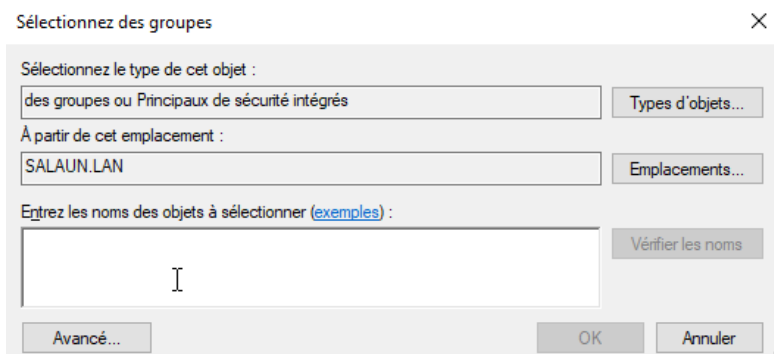
-Une fois ajouter l'utilisateur apparaîtra dans la liste des membres.

Mettre de droits au groupe.

Toujours dans le même onglet, mais nous allons sélectionner « Membre de »



-Nous allons cliquer sur « ajouter ». Cette page apparaîtra.



Dans cette page vous aller choisir le rôle des utilisateurs présents dans le groupe (dans notre cas « utilisateurs »

Noms multiples trouvés



Plusieurs objets correspondent au nom ut. Sélectionnez un ou plusieurs noms dans la liste, ou retapez le nom.

Noms correspondants :

Nom	Description	Dossier
Utilisateurs		SALAUN.LAN/Builtin
Utilisateurs de gestion à dista...		SALAUN.LAN/Builtin
Utilisateurs de l'Analyseur de...		SALAUN.LAN/Builtin
Utilisateurs DHCP	Les membres qui ont un accès ...	SALAUN.LAN/Users
Utilisateurs du Bureau à dista...		SALAUN.LAN/Builtin
Utilisateurs du domaine	Tous les utilisateurs du domaine	SALAUN.LAN/Users
Utilisateurs du journal de perf...		SALAUN.LAN/Builtin
Utilisateurs du modèle COM ...		SALAUN.LAN/Builtin

OK

Annuler

Sélectionner le premier choix puis « Ok » « Ok » et enfin « appliquer » et « ok ».

Réseau Wi-Fi Invités

Mettre en place un réseau Wi-Fi Invités isolé du réseau interne, avec :

- attribution automatique d'adresse IP par DHCP pfSense,
- Portail captif avec acceptation des CGU (Option A),
- accès Internet uniquement (blocage des réseaux privés internes),
- gestion par segmentation (VLAN + sous-réseau dédié).

Le Captive Portal pfSense force les utilisateurs à passer par une page web d'acceptation/connexion avant d'accéder au réseau, selon le mode choisi.

1) Pré-requis (réseau & Wi-Fi)

1.1 Matériel / VM

- pfSense avec 2 interfaces : WAN (em0) et LAN (em1) → OK.
- Switch/Point d'accès Wi-Fi capable de tagger un SSID sur un VLAN.

1.2 VLAN

- VLAN Invités : VLAN 20
 - Le port switch vers l'AP doit transporter ce VLAN (trunk/tagged).
 - Le SSID "Invités" doit être associé au VLAN 20.
-

2) Plan d'adressage (Portail captif)

2.1 Réseau invités

- Sous-réseau : 10.6.20.0/24
- Passerelle (pfSense GUEST) : 10.6.20.1
- DHCP : 10.6.20.50 → 10.6.20.200
- DNS : 10.6.20.1 (pfSense)

Remarque : le Captive Portal s'applique sur une interface non-WAN (LAN/VLAN) ayant une IP.

3) Création du VLAN "Invités" sur pfSense (em1)

Étape 3.1 — Créer le VLAN

1. Aller dans Interfaces → Assignments
2. Onglet VLANs
3. Cliquer Add
4. Renseigner :
 - Parent interface : em1 (LAN)
 - VLAN Tag : 20
 - Description : VLAN_GUEST
5. Save

Étape 3.2 — Assigner le VLAN comme interface OPT

1. Revenir sur Interface Assignments
2. Dans la liste des ports disponibles, sélectionner VLAN 20 on em1
3. Ajouter bouton "Add" ou apparition d'OPT1 après sélection
4. Tu obtiens OPT1

Étape 3.3 — Configurer l'interface OPT1 (GUEST)

1. Aller dans Interfaces → OPT1
 2. Cocher Enable
 3. Description : GUEST ou INVITES
 4. IPv4 Configuration Type : *Static IPv4*
 5. IPv4 Address : 10.6.20.1/24
 6. Save puis Apply Changes
-

4) DHCP sur pfSense (réseau invités)

1. Aller dans Services → DHCP Server → GUEST
2. Cocher Enable DHCP server on GUEST
3. Configurer :
 - Range : 10.6.20.50 à 10.6.20.200
 - (Optionnel) Default lease time : ex 7200 sec (2h) ou 14400 sec (4h)
4. DNS :
 - Soit 10.6.20.1 (pfSense)
 - Soit DNS public (si tu ne veux pas que les invités utilisent le DNS interne)

À ce stade, un client invité doit déjà obtenir une IP en 10.6.20.x.

5) Règles Firewall (Invités = Internet uniquement)

5.1 Pourquoi bloquer RFC1918 ?

Pour empêcher l'accès aux réseaux internes privés, on bloque les plages RFC1918 :

- 10.0.0.0/8
- 172.16.0.0/12

- 192.168.0.0/16

C'est parfait dans ton cas : ton LAN est en 10.5.x.x, donc il est inclus dans 10.0.0.0/8 → les invités ne pourront pas toucher ton SI.

5.2 Créer un alias RFC1918

1. Firewall → Aliases
2. Add
3. Type : Network(s)
4. Name : RFC1918
5. Ajouter :
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16
6. Save

5.3 Créer les règles sur l'interface GUEST

Aller dans Firewall → Rules → GUEST et mettre dans cet ordre :

Règle 1 — Autoriser DNS (si DNS = pfSense)

- Action : Pass
- Protocol : TCP/UDP
- Source : GUEST net
- Destination : This Firewall (GUEST address) (donc 10.6.20.1)
- Port : 53
- Description : "DNS invités vers pfSense"

Règle 2 — Bloquer accès aux réseaux internes (RFC1918)

- Action : Block
- Source : GUEST net
- Destination : RFC1918
- Description : "Blocage réseaux privés (RFC1918)"

Règle 3 — Autoriser Internet

- Action : Pass
- Protocol : Any (ou TCP 80/443 + UDP 123)
- Source : GUEST net
- Destination : any
- Description : “Accès Internet invités”
- Résultat : les invités ont Internet mais ne peuvent pas joindre 10.5.x.x ni aucun réseau privé RFC1918.

4) Page captive “click-through” : simple OU personnalisée

Installation outil de monitoring

Nous avons choisi Centreon pour sa facilité de prise en main et nous le trouvons cohérent avec le projet.

Services actifs

-Centengine

-Cbd (broker)

-Apache2

-Mariadb

Installation via Debian

Etape 1 : Installation

apt update && apt upgrade

```
apt install lsb-release ca-certificates apt-transport-https software-properties-common
wget gnupg2 curl
```

```
echo "deb https://packages.sury.org/php/ $(lsb_release -sc) main" | tee
/etc/apt/sources.list.d/sury-php.list
```

```
wget -O- https://packages.sury.org/php/apt.gpg | gpg --dearmor | tee
/etc/apt/trusted.gpg.d/php.gpg > /dev/null 2>&1
```

```
apt update
```

```
Hit:1 https://download.docker.com/linux/debian bookworm InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libglib2.0-0 libglib2.0-data libislirp0 pigs shared-mime-info slurp4netns xdg-user-dirs
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@centreonclary:~# apt install lsb-release ca-certificates apt-transport-https software-properties-common wget gnupg2 curl
echo "deb https://packages.sury.org/php/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/sury-php.list
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
lsb-release is already the newest version (12.0-1).
ca-certificates is already the newest version (20230311deb12u1).
wget is already the newest version (1.21.3-1+deb12u1).
curl is already the newest version (7.88.1-10+deb12u4).
The following packages were automatically installed and are no longer required:
  libislirp0 pigs slurp4netns
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  appstream gir1.2-glib-2.0 gir1.2-packagekit-glib-1.0 iso-codes libappstream4 libduktape207 libdwl libgirepository-1.0-1 libglib2.0-bin libgstreamer1.0-0 libpackagekit-glib2-18 libpolkit-agent-1.0
  libpolkit-gobject-1-0 libstemmer0d libunwind8 libxmlb2 packagekit packagekit-tools polkitd python3-blinker python3-ffi-backend python3-cryptography python3-dbus python3-gi python3-jwt
  python3-lazr.restfulclient python3-lazr.uri python3-ouathlib python3-software-properties python3-wadllib xml-core
Suggested packages:
  apt-config-icons isoquery gstreamer1.0-tools polkitd-pkla python-blinker-doc python-cryptography-doc python3-cryptography-vectors python-dbus-doc python3-crypto debhelper
The following NEW packages will be installed:
  appstream apt-transport-https gir1.2-glib-2.0 gir1.2-packagekit-glib-1.0 gnupg2 iso-codes libappstream4 libduktape207 libdwl libgirepository-1.0-1 libglib2.0-bin libgstreamer1.0-0 libpackagekit-gli
  libpolkit-agent-1.0 libpolkit-gobject-1-0 libstemmer0d libunwind8 libxmlb2 packagekit packagekit-tools polkitd python3-blinker python3-ffi-backend python3-cryptography python3-dbus python3-gi pyt
  python3-lazr.restfulclient python3-lazr.uri python3-ouathlib python3-software-properties python3-wadllib software-properties-common xml-core
0 upgraded, 34 newly installed, 0 to remove and 0 not upgraded.
Need to get 8503 kB of archives.
After this operation, 43.4 MB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://deb.debian.org/debian bookworm/main amd64 libstemmer0d amd64 2.2.0-2 [118 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 libxmlb2 amd64 0.3.10-2 [60.2 kB]
Get:3 http://deb.debian.org/debian bookworm/main amd64 libappstream4 amd64 0.16.1-2 [199 kB]
Get:4 http://deb.debian.org/debian bookworm/main amd64 appstream amd64 0.16.1-2 [407 kB]
Get:5 http://deb.debian.org/debian bookworm/main amd64 apt-transport-https all 2.6.1 [25.2 kB]
Get:6 http://deb.debian.org/debian bookworm/main amd64 libgirepository-1.0-1 amd64 1.74.0-3 [101 kB]
Get:7 http://deb.debian.org/debian bookworm/main amd64 gir1.2-glib-2.0 amd64 1.74.0-3 [159 kB]
Get:8 http://deb.debian.org/debian bookworm/main amd64 libpackagekit-glib2-18 amd64 1.2.6-5 [113 kB]
Get:9 http://deb.debian.org/debian bookworm/main amd64 gir1.2-packagekit-glib-1.0 amd64 1.2.6-5 [25.9 kB]
Get:10 http://deb.debian.org/debian bookworm/main amd64 gnupg2 all 2.2.40-1.1+deb12u1 [446 kB]
Get:11 http://deb.debian.org/debian bookworm/main amd64 iso-codes all 4.15.0-1 [2906 kB]
Get:12 http://deb.debian.org/debian bookworm/main amd64 libduktape207 amd64 2.7.0-2 [134 kB]
Get:13 http://deb.debian.org/debian bookworm/main amd64 libdwl amd64 0.130-2.1 [25 kB]
Get:14 http://deb.debian.org/debian bookworm/main amd64 libglib2.0-bin amd64 2.74.6-2+deb12u7 [112 kB]
Get:15 http://deb.debian.org/debian bookworm/main amd64 libunwind8 amd64 1.6.2-3 [51.2 kB]
Get:16 http://deb.debian.org/debian bookworm/main amd64 libgstreamer1.0-0 amd64 1.22.0-2+deb12u1 [1170 kB]
Get:17 http://deb.debian.org/debian bookworm/main amd64 libpolkit-gobject-1-0 amd64 122-1 [43.9 kB]
```

Installation de la base de données :

```
curl -Ls https://r.mariadb.com/downloads/mariadb_repo_setup | bash -s -- --os-
type=debian --os-version=12 --mariadb-server-version="mariadb-10.11"
```

```
# [Info] Skipping OS detection and using OS type 'debian' and version '12' as given on the command line
# [Info] Checking for script prerequisites.
# [Info] MariaDB Server version 10.11 is valid
# [Info] Repository file successfully written to /etc/apt/sources.list.d/mariadb.list
# [Info] Adding trusted package signing keys...
# [Info] Running apt-get update...
# [Info] https://packages.sury.org/php/dist/bookworm/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in a
# [Info] t-key(8) for details.
# [Info] Done adding trusted package signing keys.
```

Installation des dépôts :

```
echo "deb https://packages.centreon.com/apt-standard-24.10-stable/ $(lsb_release -
sc) main" | tee /etc/apt/sources.list.d/centreon.list
```

```
echo "deb https://packages.centreon.com/apt-plugins-stable/ $(lsb_release -sc) main" |  
tee /etc/apt/sources.list.d/centreon-plugins.list
```

```
wget -O- https://apt-key.centreon.com | gpg --dearmor | tee  
/etc/apt/trusted.gpg.d/centreon.gpg > /dev/null 2>&1
```

```
root@Centreon:~# wget -O- https://apt-key.centreon.com | gpg --dearmor | tee /etc/apt/trusted.gpg.d/centreon.gpg > /dev/null 2>&1  
--2025-04-15 12:50:19-- https://apt-key.centreon.com/  
Résolution de apt-key.centreon.com (apt-key.centreon.com)... 3.165.136.3, 3.165.136.45, 3.165.136.40, ...  
Connexion à apt-key.centreon.com (apt-key.centreon.com) [3.165.136.3]:443... connecté.  
requête HTTP transmise, en attente de la réponse... 200 OK  
Taille : 4276 (4,2K) [binary/octet-stream]  
Sauvegarde en : « STDOUT »  
  
100%[=====] 4,18K --.-KB/s ds 0s  
  
2025-04-15 12:50:19 (28,5 MB/s) - envoi vers sortie standard [4276/4276]  
root@Centreon:~#
```

```
apt update && apt install -y centreon-mariadb centreon
```

```
systemctl daemon-reload
```

```
systemctl restart mariadb
```

Étape 2 : Configuration

Lancement de Centreon au démarrage

```
systemctl enable php8.2-fpm apache2 centreon cbd centengine gorgoned  
centreontrapd snmpd snmptrapd mariadb
```

```
systemctl restart mariadb apache2
```

Sécurisation de la base de données :

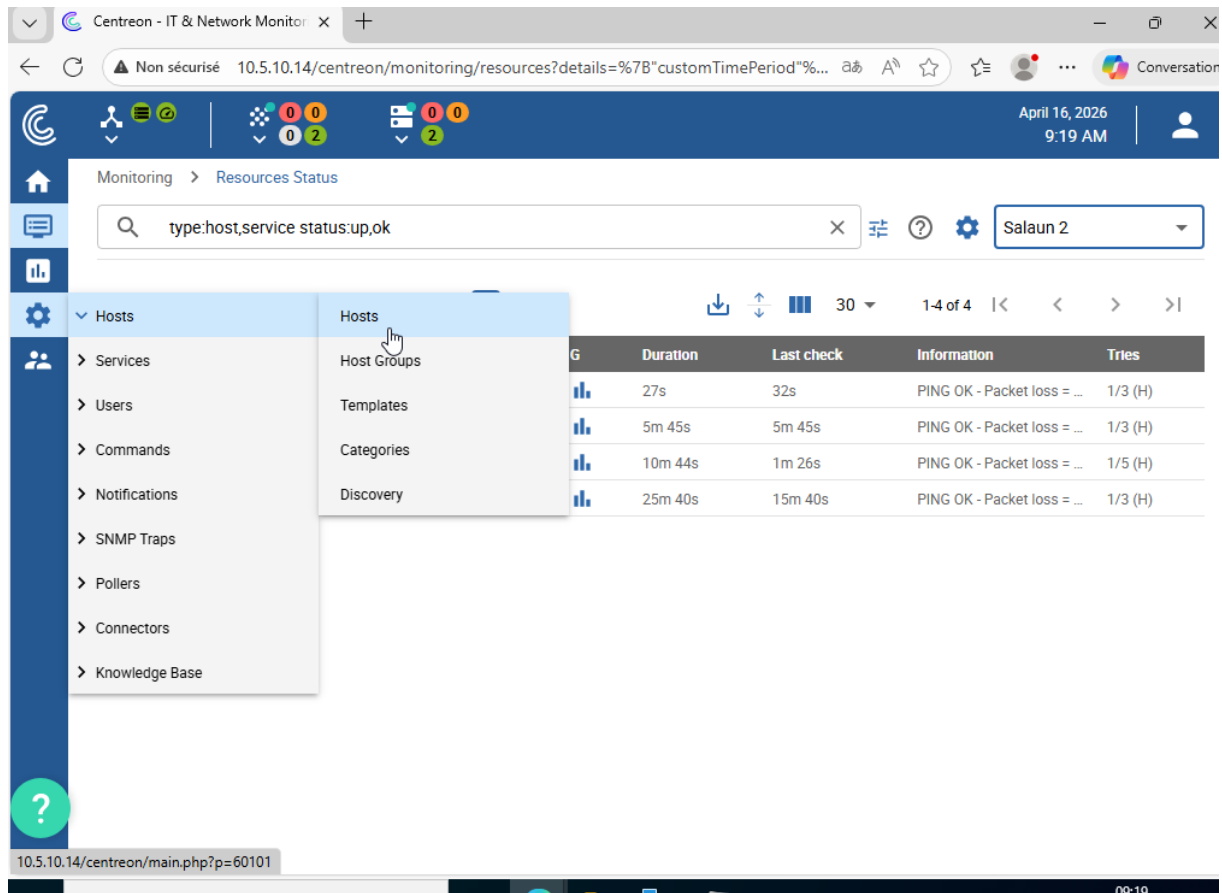
```
mariadb-secure-installation
```

Étape 3 : Interface web

<http://10.5.10.14>

Ajout d'un serveur

Une fois sur centreon il faut se rendre sur la roulette puis Hosts et encore une fois Hosts.



The screenshot shows the Centreon web interface. The top navigation bar includes the Centreon logo, a search bar with the query "type:host,service status:up,ok", and the user "Salaun 2". The main navigation menu on the left is expanded to show the "Hosts" section, which includes options like Host Groups, Templates, Categories, and Discovery. The main content area displays a table of host resources with the following data:

G	Duration	Last check	Information	Tries
	27s	32s	PING OK - Packet loss = ...	1/3 (H)
	5m 45s	5m 45s	PING OK - Packet loss = ...	1/3 (H)
	10m 44s	1m 26s	PING OK - Packet loss = ...	1/5 (H)
	25m 40s	15m 40s	PING OK - Packet loss = ...	1/3 (H)

Une fois sur la page cliquer sur add.

<input type="checkbox"/>	Name	Alias	IP Address / DNS	Poller	Templates	Status	Options
<input type="checkbox"/>	DC1	DomainController1	10.5.10.0	Central		ENABLED	1
<input type="checkbox"/>	DC2	DomainContreoller2	10.5.20.0	Central		ENABLED	1
<input type="checkbox"/>	ServeurDeFichier	Servfich	10.5.50.0	Central		ENABLED	1

Après avoir cliqué sur add. Renseigner les différentes informations demander. Puis Save.

| Add a HOST

Host basic information

Name *

Alias

Address * [Resolve](#)

SNMP Community & Version

Monitoring server

Timezone

Templates

Nothing here, use the "Add" button

Yes No Create Services linked to the Template too

Host check options

Check Command

Args

Custom macros

Nothing here, use the "Add" button

Scheduling options

Check Period	24x7	
Max Check Attempts		
Normal Check Interval		* 60 seconds
Retry Check Interval		* 60 seconds
Active Checks Enabled	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Default	
Passive Checks Enabled	<input type="radio"/> Yes <input checked="" type="radio"/> No <input type="radio"/> Default	

Une fois l'host crée nous allons faire de même dans les services by host.

The screenshot shows the Centreon web interface. On the left, there is a vertical navigation menu with icons for a dashboard, settings, and users. The 'Services' menu item is expanded, showing a list of options: Hosts, Users, Commands, Notifications, SNMP Traps, Pollers, Connectors, and Knowledge Base. A secondary menu is open over the 'Services' menu, listing: Services by host (highlighted with a mouse cursor), Services by host group, Service Groups, Templates, Categories, Meta Services, Auto Discovery, Scan, Rules, and Overview. The URL at the bottom of the browser is 10.5.10.14/centreon/main.php?p=60201.

Une fois sur la page cliquer sur add et remplir de la même manière.

Hosts *

Template

Service Check Options

Check Command *

Custom macros

- Template inheritance
- Command inheritance

+ Add a new entry
Nothing here, use the "Add" button

Args	Argument	Value	Example
	No argument found for this command		

Service Scheduling Options

Check Period

Max Check Attempts

Normal Check Interval * 60 seconds

Retry Check Interval * 60 seconds

Active Checks Enabled Yes No Default

Passive Checks Enabled Yes No Default

Is Volatile Yes No Default

Une fois ces deux choses faites se rendre dans Pollers pour pouvoir enregistrer la configuration. Sélectionner votre serveur et cliquer sur export configuration.

Configuration > Pollers

Poller Filters

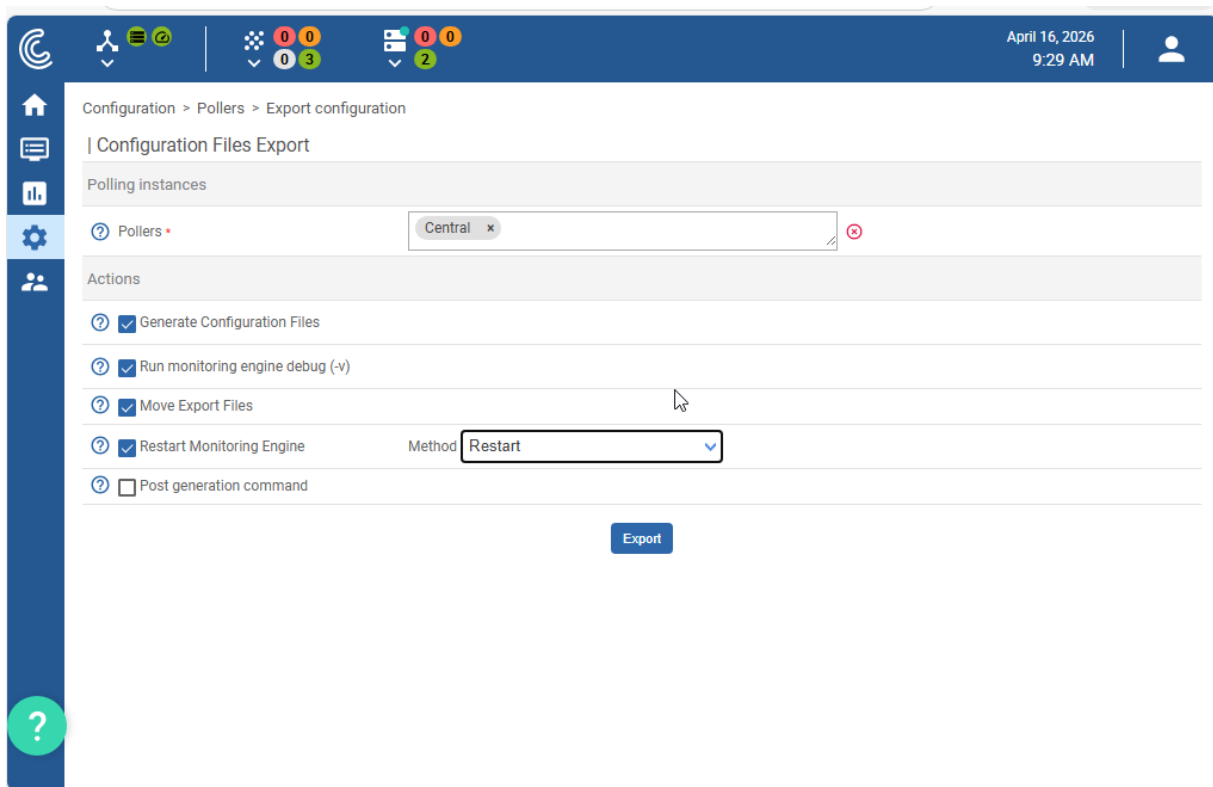
30

<input type="checkbox"/>	Name	Address	Server type	Is running?	Conf Changed *	PID	Uptime	Last Update	Version	Default	Status	Actions	Options
<input checked="" type="checkbox"/>	Central	127.0.0.1	Central	YES	YES	51003	9 minutes 30 seconds	April 16, 2026 9:28:42 AM	Centreon Engine 24.10.17	Yes	ENABLED		<input type="text" value="1"/>

30

* Only services, servicegroups, hosts and hostgroups are taken in account in order to calculate this status. If you modify a template, it won't tell you the configuration had changed.

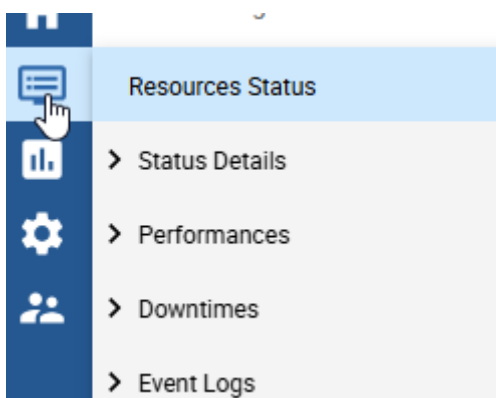
Sélectionner les mêmes paramètres que sur l'image ci-dessous. Puis cliquer sur Export.



Une fois tout cela terminer se rendre sur le serveur ssh centreon pour redémarrer les différents services avec ces commandes dans cet ordre.

```
root@Centreon:~# systemctl restart cbd
root@Centreon:~# systemctl restart centengine
root@Centreon:~#
```

Après avoir terminer tout cela le serveur devrait apparaitre. Dans Ressources Status.



Serveur de fichier

Un disque de données dédié a été ajouté à la machine virtuelle via Proxmox afin de séparer le système d'exploitation des données utilisateurs.

Le volume D:\DATA est utilisé pour le stockage des fichiers partagés, facilitant la maintenance, la sauvegarde et la sécurité.

. Architecture mise en place

Élément	Valeur
Système	Windows Server
Rôle	Serveur de fichiers
Domaine	SALAUN.LAN
Serveur	SERFICH
Partage principal	\\SERFICH\Dossier-de-partage
Volume données	E:\DATA

Organisation des données

Les données sont stockées sur un disque dédié (E:), distinct du système d'exploitation.

Arborescence du volume

Plain Text

E:\DATA

├─ dossier-de-partage

├─ adminSYS

├─ COMMERCIAL

├─ Commun

├─ Comptabilite

├─ Direction

├─ PRODUCTION

├─ QUALITE

Groupes Active Directory utilisés

Les accès aux dossiers sont contrôlés par des groupes de sécurité globaux.

Exemples de groupes

Dossier	Groupe AD
Commun	GG_Tous
Comptabilite	GG_Compta
RH	GG_RH
Direction	GG_Direction
Commercial	GG_Commercial
Production	GG_Production
Qualité	GG_Qualite
Transport	GG_Transport
Admin système	GG_AdminSYS

Les utilisateurs sont ajoutés aux groupes correspondant à leur service.

Sauvegarde Centralisée

1. Présentation

Dans le cadre du projet, une solution de sauvegarde centralisée a été mise en place via Proxmox Backup Server (PBS) 4.2. Elle permet de sauvegarder automatiquement toutes les VMs de l'infrastructure SALAUN .

2. Caractéristiques techniques

Élément	Détail
Solution	Proxmox Backup Server 4.2

Élément	Détail
Hostname	pbs.SALAUN.LAN
IP du serveur	10.5.10.5/8
Gateway	10.5.30.1
DNS	10.5.10.0
Port d'administration	8007 (HTTPS)
Filesystem	ext4
Disque système	/dev/sda
Datastore	backup-store
Chemin du datastore	/mnt/datastore/backup-store
Compression	ZSTD
Mode de sauvegarde	Snapshot
GC Schedule	Daily
Prune Schedule	Daily
Fréquence	Toutes les nuits à 00h00
Périmètre	Toutes les VMs

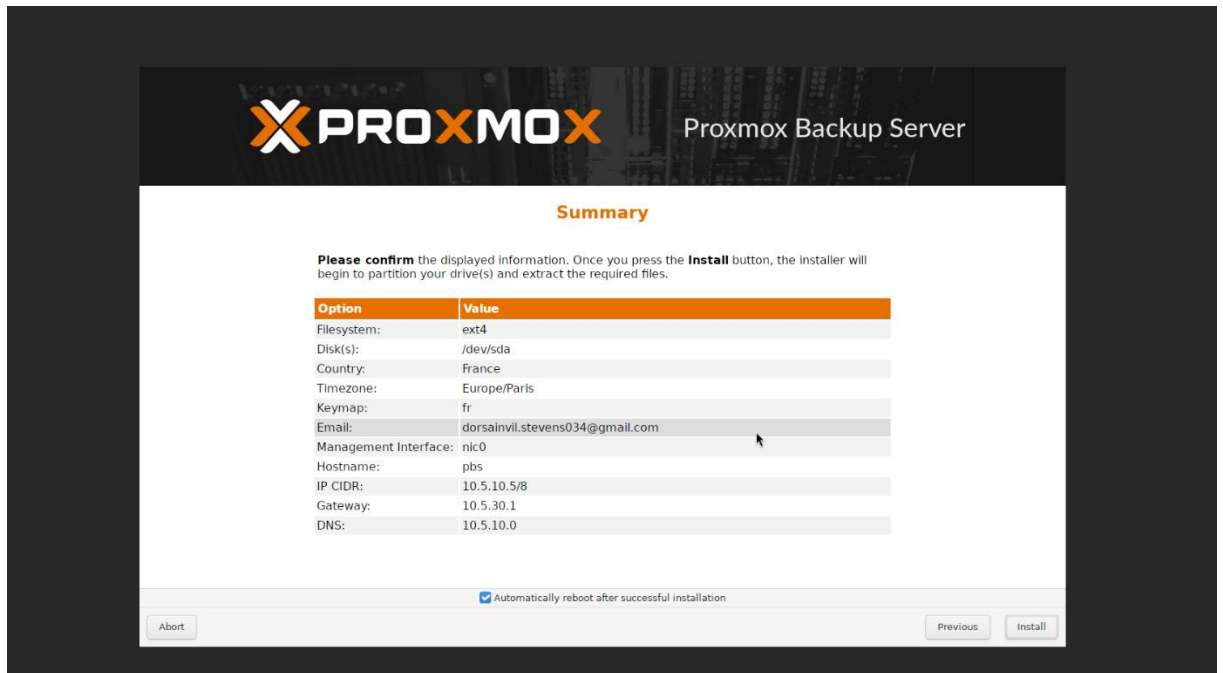
3. Étapes d'installation

Étape 1 — Boot sur l'ISO Démarrage sur l'ISO PBS 4.2, sélection de Install Proxmox Backup Server (Graphical).

Étape 2 — Configuration réseau

- Hostname : pbs.SALAUN.LAN
- IP : 10.5.10.5/8
- Gateway : 10.5.30.1

- DNS : 10.5.10.0



Étape 3 — Configuration du stockage Création d'un Directory sur le 2ème disque puis d'un Datastore backup-store dans /mnt/datastore/backup-store.

Étape 4 — Connexion à Proxmox sur l'interface <https://10.5.10.5:8007> Ajout du stockage PBS dans Datacenter → Storage → Add → Proxmox Backup Server avec le fingerprint SSL du certificat.

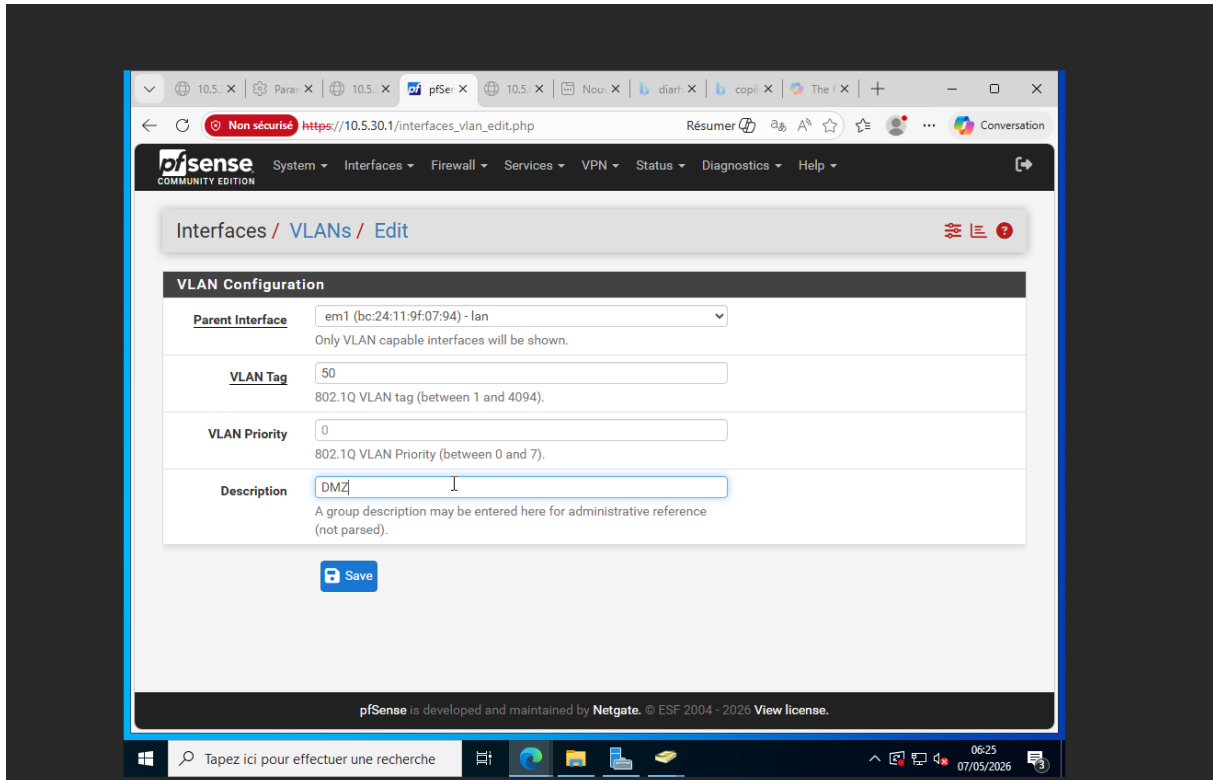
Étape 5 — Job de sauvegarde Création d'un job automatique dans Datacenter → Backup planifié à 00h00 chaque nuit pour toutes les VMs.

4. Procédure de restauration

1. Se connecter à Proxmox (<https://10.5.40.100:8006>)
2. Sélectionner la VM → Backup
3. Choisir le point de restauration
4. Cliquer sur Restore

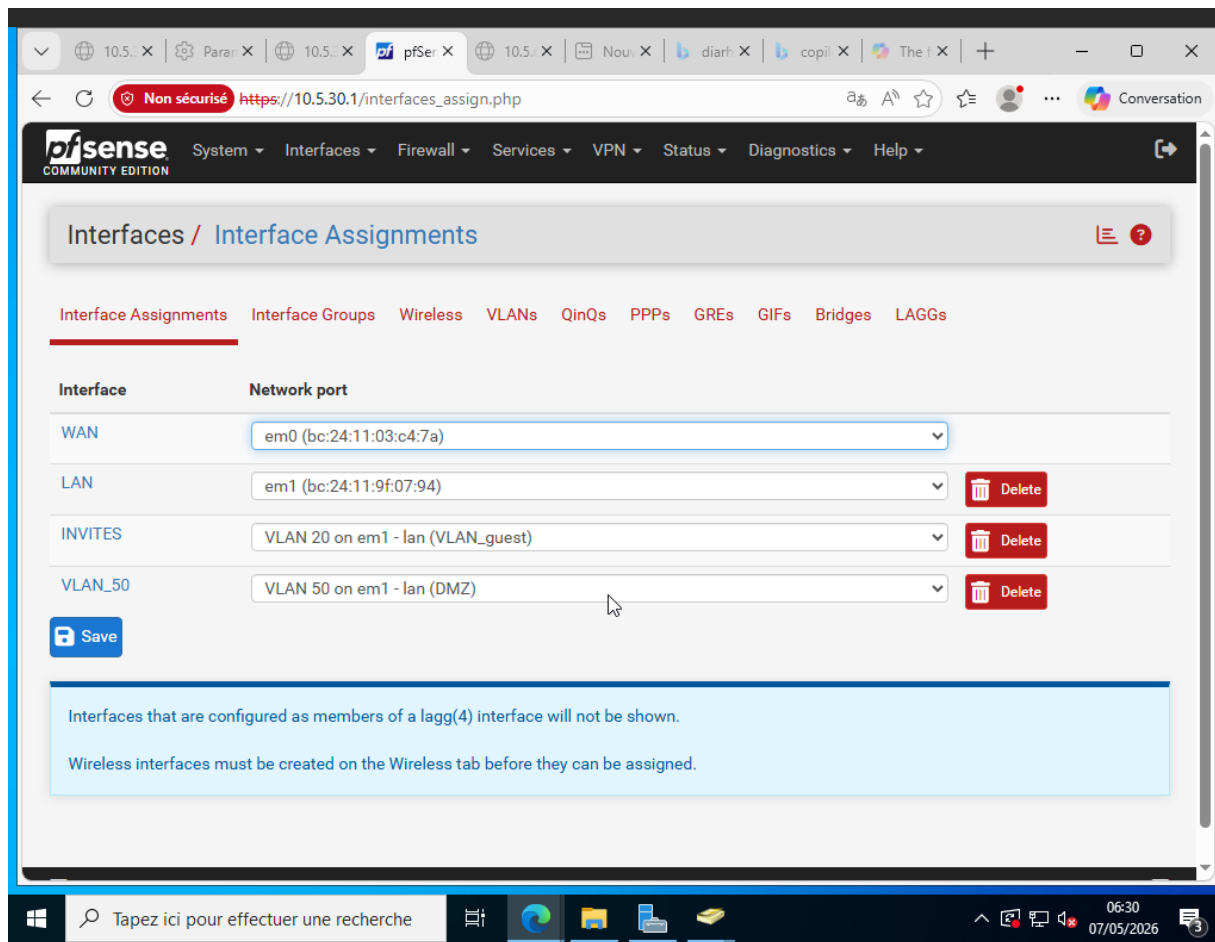
Interface web <https://10.5.10.5:8007>

DMZ



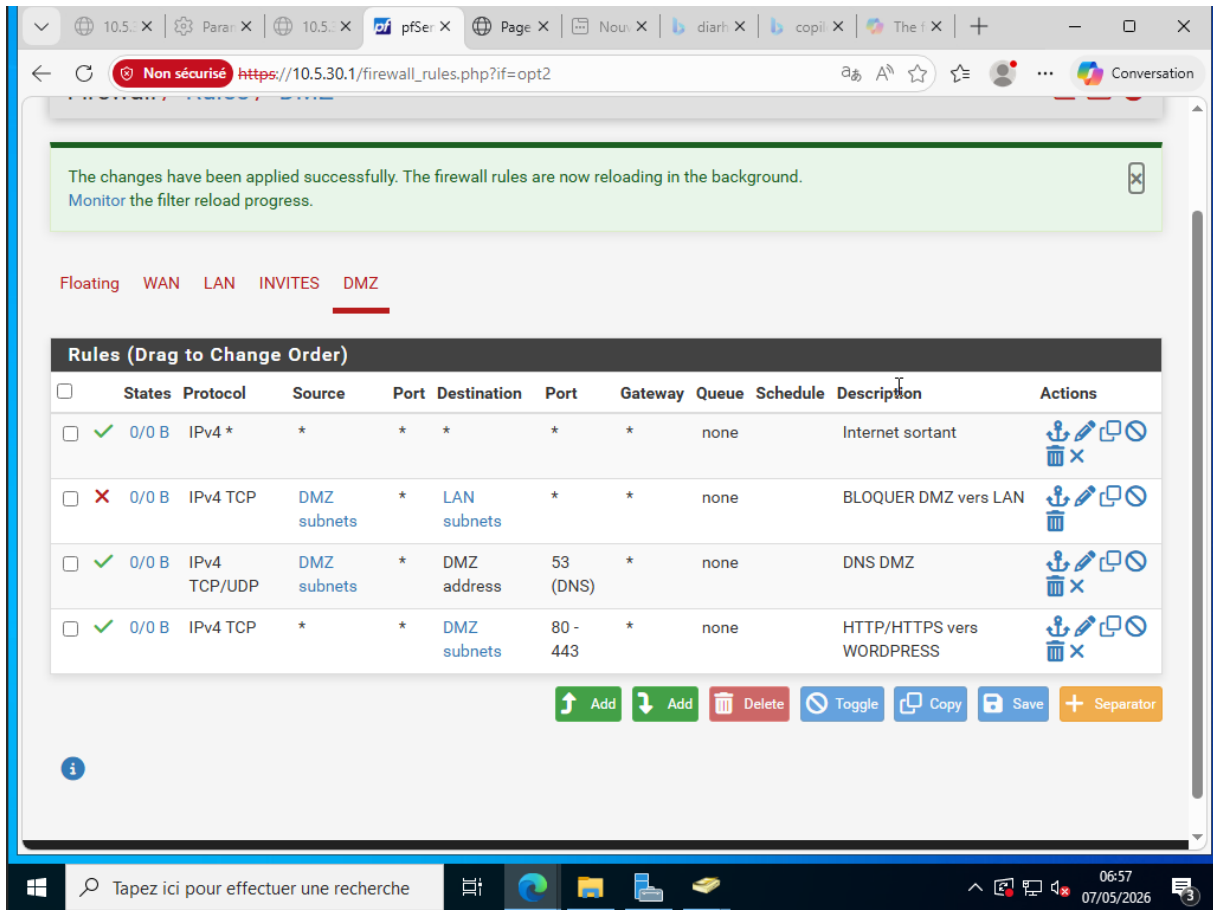
Étape 1 : Créer le VLAN 50

1. Accède à pfSense → Interfaces → Assignments → onglet VLANs
2. Clique Add
3. Remplis :
 - Parent Interface : em1
 - VLAN Tag : 50
 - Description : DMZ
4. Save



Étape 2 : Assigner comme interface

1. Dans Interfaces → Assignments, onglet Interface Assignments
2. Dans la dropdown, sélectionne "VLAN 50 on em1"
3. Clique Add
4. Save



Étape 4 : Créer les règles firewall DMZ

Va dans pfSense → Firewall → Rules → DMZ

Ajoute ces 4 règles (dans cet ordre) :

Règle 1 - HTTP/HTTPS (Internet → DMZ)

Action: Pass

Protocol: TCP

Source: any

Destination: DMZ net

Destination Port: 80, 443

Description: "HTTP/HTTPS vers WordPress"

Règle 2 - Bloquer accès LAN (DMZ → LAN)

Action: Block

Source: DMZ net

Destination: LAN net

Description: "Bloquer DMZ vers LAN"

Règle 3 - DNS (DMZ → pfSense)

Action: Pass

Protocol: TCP/UDP

Source: DMZ net

Destination: This Firewall (DMZ address)

Port: 53

Description: "DNS DMZ"

Règle 4 - Internet sortant (DMZ → WAN)

Action: Pass

Protocol: Any

Source: DMZ net

Destination: any

Description: "Internet sortant DMZ"

Segmentation Réseau — VLANS

Pour sécuriser et isoler les différents services de SALAUN TRAVELS, nous avons mis en place des VLANs sur PfSense.

Plan d'adressage

VLAN	Nom	Réseau	Gateway
LAN	Serveurs	10.5.0.0/16	10.5.30.1
20	WiFi Invité	10.6.0.0/24	10.6.0.1
30	Siège	10.7.0.0/24	10.7.0.1
40	Agences	10.8.0.0/24	10.8.0.1
50	DMZ	10.9.0.0/24	10.9.0.1

VLAN	Nom	Réseau	Gateway
60	WiFi Interne	10.10.0.0/24	10.10.0.1

Ce qu'on a fait

On a créé les VLANs sur l'interface em1 de PfSense, assigné chaque interface, configuré les IPs et activé le DHCP sur chaque VLAN avec le DNS pointant vers le DC1 (10.5.10.0). Des règles firewall ont été ajoutées pour autoriser le trafic sur chaque VLAN.

Le WiFi invité et la DMZ sont isolés du reste du réseau interne.