

UNIVERSITÉ CHEIKH ANTA DIOP DE DAKAR

École Supérieure Polytechnique



ECOLE SUPERIEURE
POLYTECHNIQUE

Rapport PfSense avec auth RADIUS/LDAP

Présenté par :

Salif BIAYE

Ndeye Astou DIAGOURAGA

Sous la direction de :

Dr Keba

Enseignant

Année universitaire 2024-2025

Table des Matières

I. Introduction à PfSense

I.1. Présentation de PfSense

I.2. Prérequis matériels et logiciels

II. Architecture du réseau

II.1. Schéma global

II.2. Topologie réseau

III. Installation et configuration de FreeRADIUS et LDAP

III.1. Installation d'Ubuntu Server

III.2. Installation de FreeRADIUS

III.3. Configuration de FreeRADIUS

III.4. Installation et configuration d'OpenLDAP

III.5. Intégration de FreeRADIUS avec LDAP

III.6. Test de configuration

IV. Installation et configuration de PfSense

IV.1. Création des machines virtuelles sur VMware

IV.2. Configuration des commutateurs virtuels

IV.3. Installation de PfSense

IV.4. Configuration initiale des interfaces réseau

IV.5. Configuration des règles de pare-feu

IV.6. Configuration Radius pour l'authentification (BONUS VIDEO)

VII. Conclusion

I. Introduction à PfSense

I.1. Présentation de PfSense

PfSense est une distribution open-source basée sur FreeBSD, spécialisée dans les services de routage et de pare-feu. Elle offre de nombreuses fonctionnalités avancées généralement trouvées dans les pare-feu commerciaux coûteux, comme le filtrage de paquets, le VPN, le portail captif, et bien d'autres.

PfSense est particulièrement apprécié pour :

- Sa stabilité et sa fiabilité
- Son interface web intuitive
- Sa flexibilité grâce aux nombreux packages disponibles
- Sa gratuité et sa communauté active

I.2. Prérequis matériels et logiciels

Pour suivre ce guide, vous aurez besoin de :

Matériel :

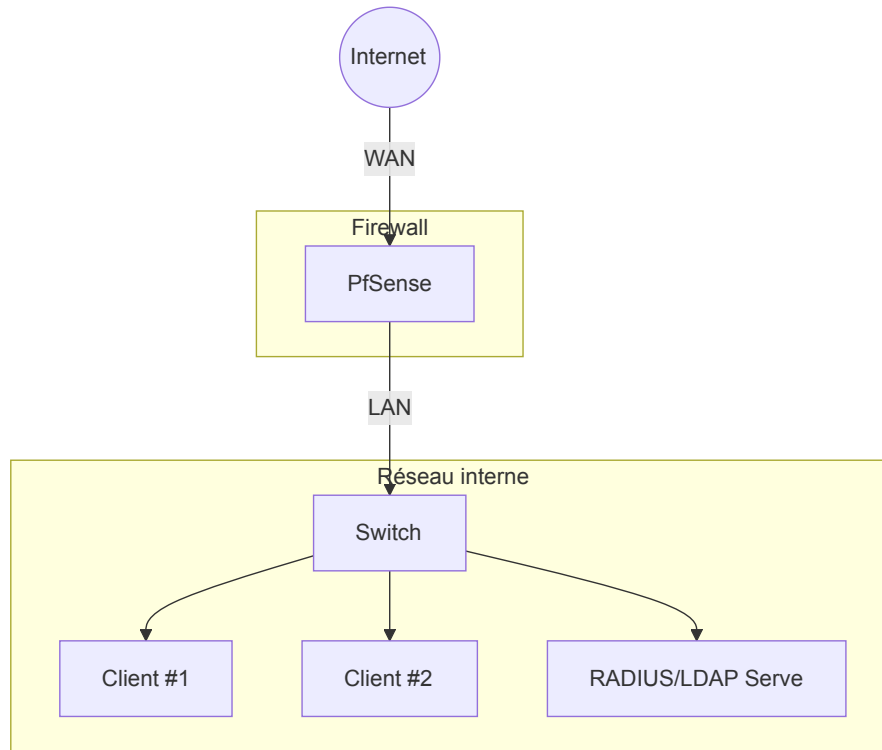
- Un ordinateur hôte avec suffisamment de ressources pour exécuter au moins deux machines virtuelles
- Minimum 8 Go de RAM recommandés
- Espace disque suffisant (au moins 40 Go disponibles)

Logiciels :

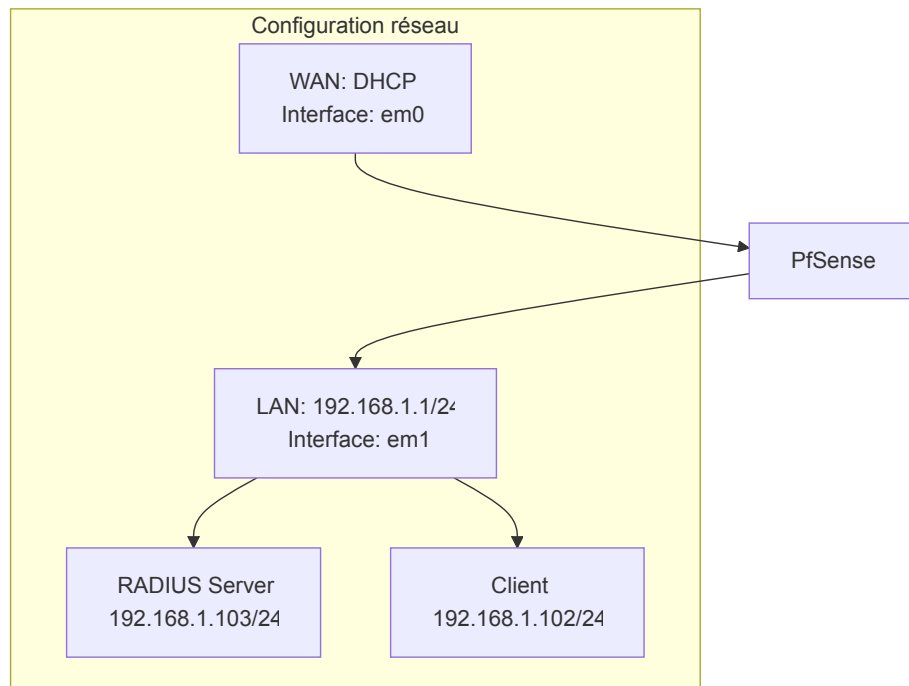
- VmWare (inclus dans Windows 10/11 Pro, Enterprise ou Education)
- Image ISO de PfSense (téléchargeable sur
pfsense.org
)
- Image ISO d'Ubuntu Server (téléchargeable sur
ubuntu.com
)

II. Architecture du réseau

II.1. Schéma global



II.2. Topologie réseau



III. Installation et configuration de FreeRADIUS et LDAP

III.1. Installation d'Ubuntu Server

1. Démarrez la VM Ubuntu-RADIUS
2. Suivez les étapes d'installation d'Ubuntu Server :
 - Sélectionnez la langue et la disposition du clavier
 - Configurez le réseau :
 - Interface réseau : ens33 (ou l'interface détectée)
 - Configuration IP : Statique
 - Adresse IP : 192.168.1.103
 - Masque : 255.255.255.0
 - Passerelle : 192.168.1.1
 - Serveurs DNS : 192.168.1.1
 - Configurez le nom d'hôte : radius-server
 - Créez un utilisateur administrateur
 - Installez OpenSSH Server pour l'accès à distance
3. Finalisez l'installation et redémarrez

III.2. Installation de FreeRADIUS

1. Connectez-vous à la VM Ubuntu à l'aide de SSH ou directement dans la console
2. Mettez à jour les paquets système :

```
sudo apt update  
sudo apt upgrade -y
```

3. Installez FreeRADIUS et les outils associés :

```
sudo apt install freeradius freeradius-ldap freeradius-utils -y
```

III.3. Configuration de FreeRADIUS

1. Arrêtez le service FreeRADIUS :

```
sudo systemctl stop freeradius
```

2. Configurez le fichier clients.conf pour autoriser PfSense à communiquer avec FreeRADIUS :

```
sudo nano /etc/freeradius/3.0/clients.conf
```

3. Ajoutez la configuration suivante à la fin du fichier :

```
client pfsense {
    ipaddr = 192.168.1.1
    secret = testing123
    require_message_authenticator = no
    nas_type = other
}

client kdc {
    ipaddr = 192.168.1.103
    secret = testing123
    shortname = kdc
}
```

4. Configurez le fichier users pour créer un utilisateur de test :

```
sudo nano /etc/freeradius/3.0/users
```

5. Ajoutez l'utilisateur suivant pour les tests (avant le bloc "DEFAULT") :

```
testuser Cleartext-Password := "password123"
    Reply-Message := "Hello, %{User-Name}"
```

6. Démarrez FreeRADIUS en mode debug pour vérifier la configuration :

```
sudo freeradius -X
```

7. Si aucune erreur n'apparaît, arrêtez FreeRADIUS (Ctrl+C) et démarrez le service :

```
sudo systemctl start freeradius
sudo systemctl enable freeradius
```

III.4. Installation et configuration d'OpenLDAP

1. Installez OpenLDAP et les outils associés :

```
sudo apt install slapd ldap-utils -y
```

2. Lors de l'installation, vous serez invité à définir un mot de passe administrateur pour LDAP
3. Reconfigurez slapd pour des paramètres supplémentaires :

```
sudo dpkg-reconfigure slapd
```

4. Répondez aux questions comme suit :
 - Omettre la configuration d'OpenLDAP ? Non

- Nom de domaine DNS : ldap.local
 - Nom d'organisation : MonOrganisation
 - Mot de passe administrateur : (entrez un mot de passe fort)
 - Confirmer le mot de passe : (répétez le mot de passe)
 - Moteur de base de données : MDB
 - Supprimer la base lors de la purge ? Non
 - Déplacer l'ancienne base de données ? Oui
5. Vérifiez que le service LDAP fonctionne :

```
sudo systemctl status slapd
```

III.5. Intégration de FreeRADIUS avec LDAP

1. Créez un fichier racine LDIF :

```
nano ~/racine.ldif
```

2. Ajoutez le contenu suivant :

```
# racine.ldif
dn: dc=smarttech,dc=sn
objectClass: dcObject
objectClass: organization
dc: smarttech
o: smarttech.sn
```

3. Exécutez la commande suivante pour ajouter la racine LDAP :

```
ldapadd -x -D "cn=admin,dc=smarttech,dc=sn" -W -f racine.ldif
```

4. Créez un fichier info.ldif :

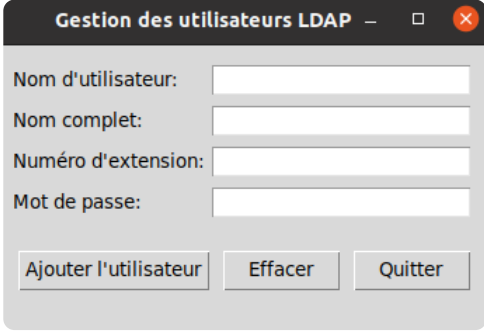
```
# OU freeradius
dn: ou=freeradius,dc=smarttech,dc=sn
objectClass: top
objectClass: organizationalUnit
ou: asterisk
# OU users
dn: ou=users,ou=freeradius,dc=smarttech,dc=sn
objectClass: top
objectClass: organizationalUnit
ou: users
# OU extensions
dn: ou=extensions,ou=freeradius,dc=smarttech,dc=sn
objectClass: top
objectClass: organizationalUnit
ou: extensions
```

5. Ajoutez les informations LDAP :

```
ldapadd -x -D "cn=admin,dc=smarttech,dc=sn" -W -f info.ldif
```

6. a l'aide d'un script python on automatise maintenant la creation des utilisateurs via une interface graphique voici le script

`user.py`



7. Configurez FreeRADIUS pour utiliser LDAP :

```
sudo nano /etc/freeradius/3.0/mods-available/ldap
```

8. Modifiez les paramètres suivants :

```
server = 'localhost'
identity = 'cn=admin,dc=smarttech,dc=sn'
password = 'passer'
base_dn = 'dc=smarttech,dc=sn'
user {
    base_dn = "ou=users,${..base_dn}"
    filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
}
```

9. Activez le module LDAP :

```
sudo ln -s /etc/freeradius/3.0/mods-available/ldap /etc/freeradius/3.0/mods-enabled
```

10. Modifiez le fichier de sites pour utiliser LDAP :

```
sudo nano /etc/freeradius/3.0/sites-available/default
```

11. Dans la section `authorize`, assurez-vous que `ldap` est décommenté

12. Redémarrez FreeRADIUS :

```
sudo systemctl restart freeradius
```

III.6. Test de configuration

1. Testez l'authentification RADIUS avec l'utilisateur local :

```
radtest testuser password123 localhost 0 MonSecretPartage
```

2. Testez l'authentification RADIUS avec l'utilisateur LDAP :

```
radtest user1 [mot_de_passe] localhost 0 MonSecretPartage
```

3. Les deux tests devraient retourner "Access-Accept", confirmant que l'authentification fonctionne.

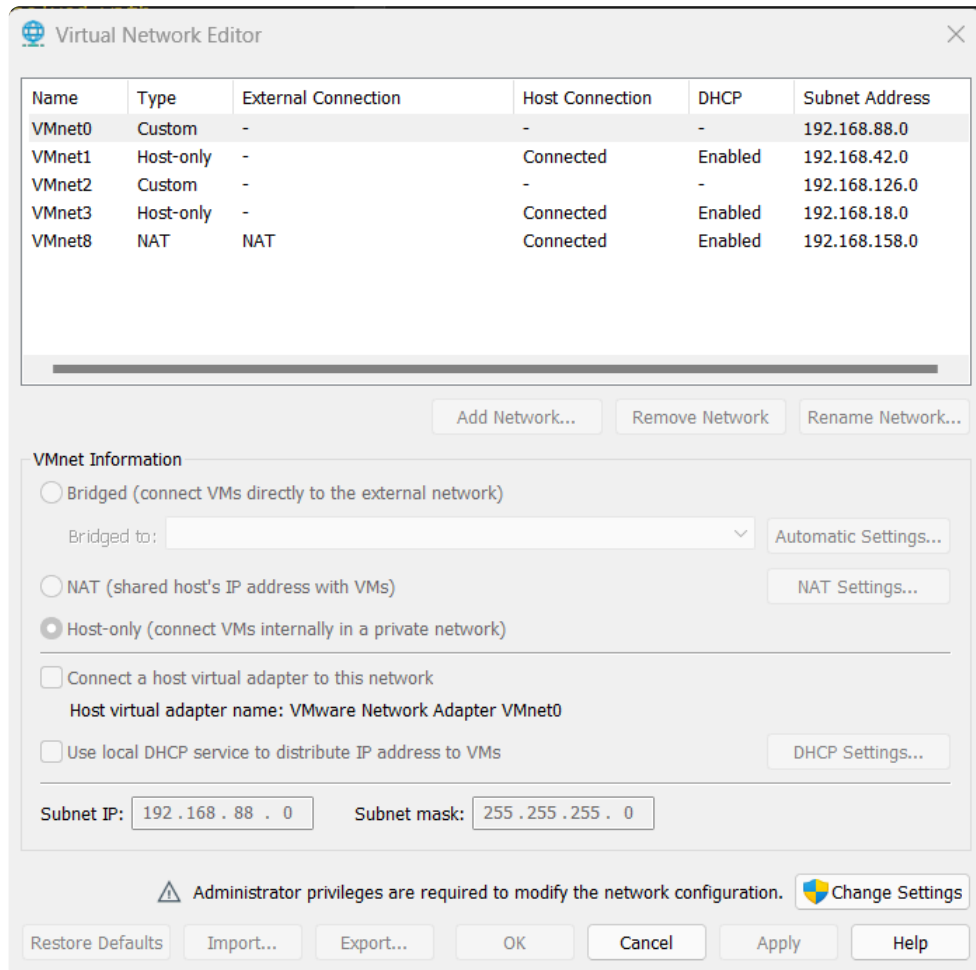
IV. Installation et configuration de PfSense

IV.1. Création des machines virtuelles sur VMware

1. Ouvrez le [Gestionnaire VMware](#)
2. Créez une nouvelle machine virtuelle pour PfSense :
 - Nom : PfSense
 - Génération : Génération 1 (pour une meilleure compatibilité)
 - Mémoire : 2048 Mo minimum
 - Configuration réseau : Non connecté (nous configurerons les réseaux ultérieurement)
 - Disque dur virtuel : 20 Go
 - Options d'installation : Installer un système d'exploitation à partir d'un fichier image de démarrage (.iso)
 - Sélectionnez l'image ISO de PfSense
3. Créez une seconde machine virtuelle pour Ubuntu Server (RADIUS/LDAP) :
 - Nom : Ubuntu-RADIUS
 - Génération : Génération 1
 - Mémoire : 2048 Mo minimum
 - Configuration réseau : Non connecté (nous configurerons le réseau ultérieurement)
 - Disque dur virtuel : 20 Go
 - Options d'installation : Installer un système d'exploitation à partir d'un fichier image de démarrage (.iso)
 - Sélectionnez l'image ISO d'Ubuntu Server


IV.2. Configuration des commutateurs virtuels

1. Dans le **Virtual network editor**, cliquez sur **Change settings** dans le panneau d'actions



2. Créez deux commutateurs virtuels :

- **Réseau NAT** :
 - Nom : VMnet8
 - Type de connexion : Externe
 - Sélectionnez votre carte réseau physique qui a accès à Internet

 Virtual Network Editor
 ✕

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Custom	-	-	-	192.168.88.0
VMnet1	Host-only	-	Connected	Enabled	192.168.42.0
VMnet2	Custom	-	-	-	192.168.126.0
VMnet3	Host-only	-	Connected	Enabled	192.168.18.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.158.0

Add Network...
Remove Network
Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)

Bridged to:
Automatic Settings...

☒ NAT (shared host's IP address with VMs)
 NAT Settings...


☐ Host-only (connect VMs internally in a private network)

☒ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet8


☒ Use local DHCP service to distribute IP address to VMs
 DHCP Settings...

Subnet IP: 192.168.158.0
 Subnet mask: 255.255.255.0

 Administrator privileges are required to modify the network configuration.
 Change Settings

Restore Defaults
Import...
Export...
OK
Cancel
Apply
Help

- **Réseau Host-only** :
 - Nom : VMnet3
 - Type de connexion : Interne
 - Ce commutateur sera utilisé pour le réseau interne

 Virtual Network Editor
 ✕

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Custom	-	-	-	192.168.88.0
VMnet1	Host-only	-	Connected	Enabled	192.168.42.0
VMnet2	Custom	-	-	-	192.168.126.0
VMnet3	Host-only	-	Connected	Enabled	192.168.18.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.158.0

Add Network...
Remove Network
Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)
 Bridged to: Automatic Settings...

☐ NAT (shared host's IP address with VMs) NAT Settings...

☒ Host-only (connect VMs internally in a private network)

☒ Connect a host virtual adapter to this network
 Host virtual adapter name: VMware Network Adapter VMnet3

☒ Use local DHCP service to distribute IP address to VMs DHCP Settings...

Subnet IP: 192 . 168 . 18 . 0 Subnet mask: 255 . 255 . 255 . 0

⚠ Administrator privileges are required to modify the network configuration. Change Settings

Restore Defaults
Import...
Export...
OK
Cancel
Apply
Help

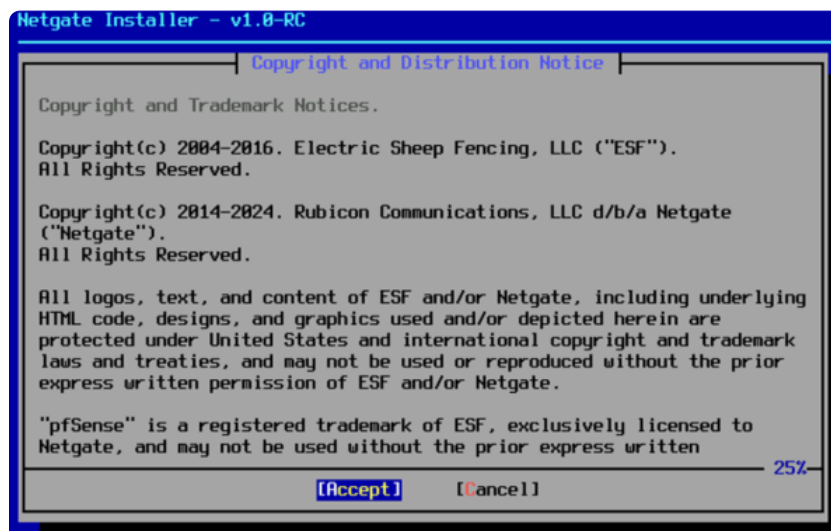
3. Configurez les cartes réseaux de la VM PfSense :
 - Accédez aux Paramètres de la VM PfSense
 - Ajoutez deux cartes réseau :
 - Adaptateur réseau 1 : Connecté au commutateur virtuel WAN
 - Adaptateur réseau 2 : Connecté au commutateur virtuel LAN
4. Configurez la carte réseau de la VM Ubuntu-RADIUS :
 - Accédez aux Paramètres de la VM Ubuntu-RADIUS
 - Configurez l'adaptateur réseau : Connecté au commutateur virtuel LAN

IV.3. Installation de PfSense

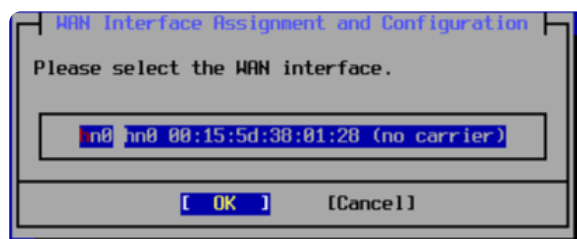
1. Démarrez la VM PfSense
2. Lorsque le menu d'installation apparaît, appuyez sur Entrée pour lancer l'installation



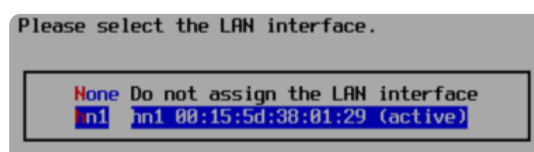
3. Sélectionnez [Accept](#) pour accepter les termes de la licence

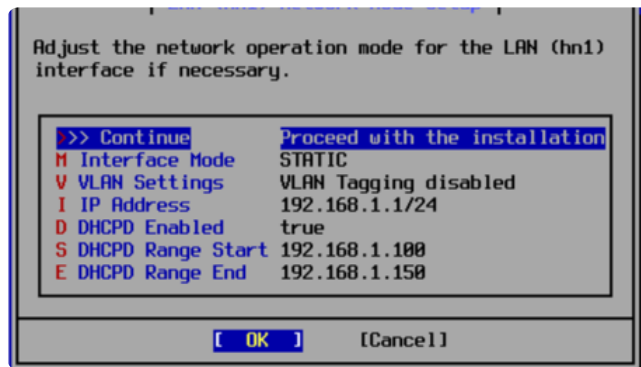


4. Suivez les étapes d'installation jusqu'à la configuration des interfaces réseau
5. pfSense va détecter les interfaces :
 - [Attribuer l'interface WAN](#) → Sélectionner la carte connectée au commutateur [WAN](#)

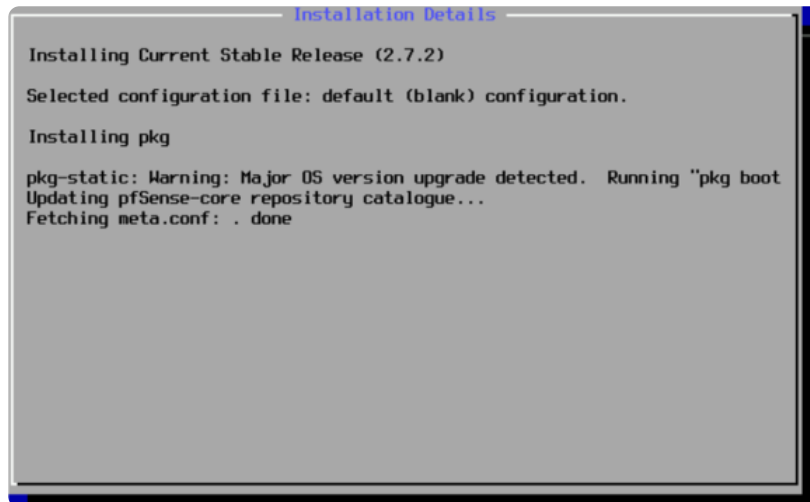


- [Attribuer l'interface LAN](#) → Sélectionner la carte connectée au commutateur [LAN](#)





6. Attendez la fin de l'installation, puis redémarrez lorsque vous y êtes invité



7. Une fois pfSense installé et redémarré, vous verrez un menu avec :

- WAN (par défaut en **DHCP**)
- LAN (par défaut en **192.168.1.1/24**)

```
Enter a host name or IP address: 192.168.1.103

PING 192.168.1.103 (192.168.1.103): 56 data bytes
64 bytes from 192.168.1.103: icmp_seq=0 ttl=64 time=0.648 ms
64 bytes from 192.168.1.103: icmp_seq=1 ttl=64 time=0.451 ms
^CUMware Virtual Machine - Netgate Device ID: 1e54b46610e47b2e8b10

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

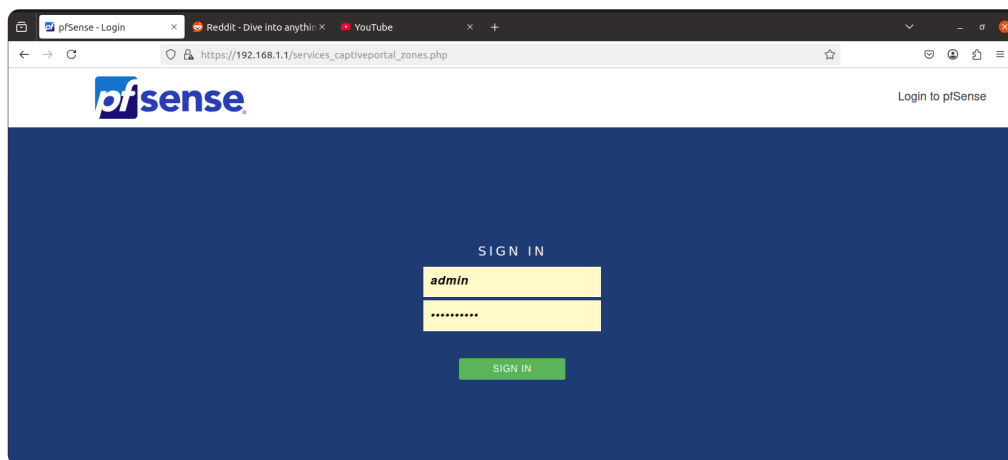
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.158.135/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

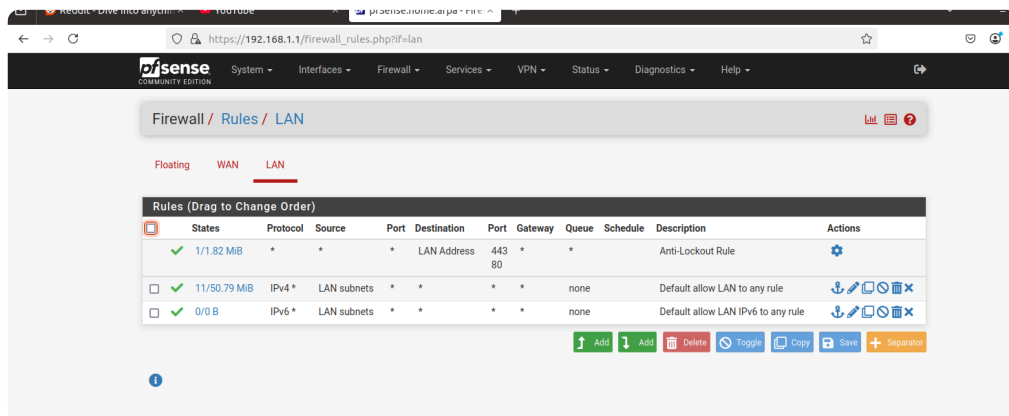

IV.4. Configuration initiale des interfaces réseau

1. Sur votre ordinateur hôte, configurez une adresse IP statique dans le même sous-réseau que l'interface LAN de PfSense :
 - Adresse IP : 192.168.1.102
 - Masque de sous-réseau : 255.255.255.0
 - Passerelle par défaut : 192.168.1.1
2. Ouvrez un navigateur web et accédez à l'adresse <https://192.168.1.1>
3. Ignorez les avertissements de sécurité du navigateur concernant le certificat
4. Connectez-vous avec les identifiants par défaut :
 - Nom d'utilisateur : [admin](#)
 - Mot de passe : [pfsense](#)



IV.5. Configuration des règles de pare-feu

1. Dans l'interface web de PfSense, allez dans [Firewall](#) > [Rules](#)
2. Sélectionnez l'onglet [LAN](#)
3. Par défaut, une règle permettant tout le trafic sortant depuis LAN devrait exister
4. Si ce n'est pas le cas, ajoutez une règle :
 - Action : [Pass](#)
 - Interface : [LAN](#)
 - Adresse source : [LAN net](#)
 - Adresse de destination : [Any](#)
 - Description : "Allow LAN to Internet"
5. Cliquez sur [Save](#) puis sur [Apply Changes](#)



Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
 Set this option to disable this rule without removing it from the list.

Interface LAN
 Choose the interface from which packets must come to match this rule.

Address Family IPv4
 Select the Internet Protocol version this rule applies to.

Protocol Any
 Choose which IP protocol this rule should match.

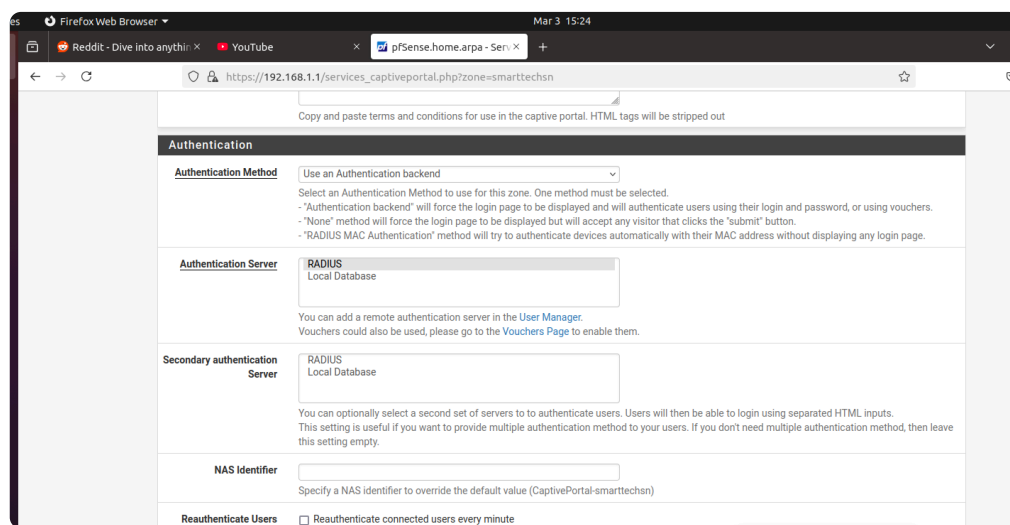
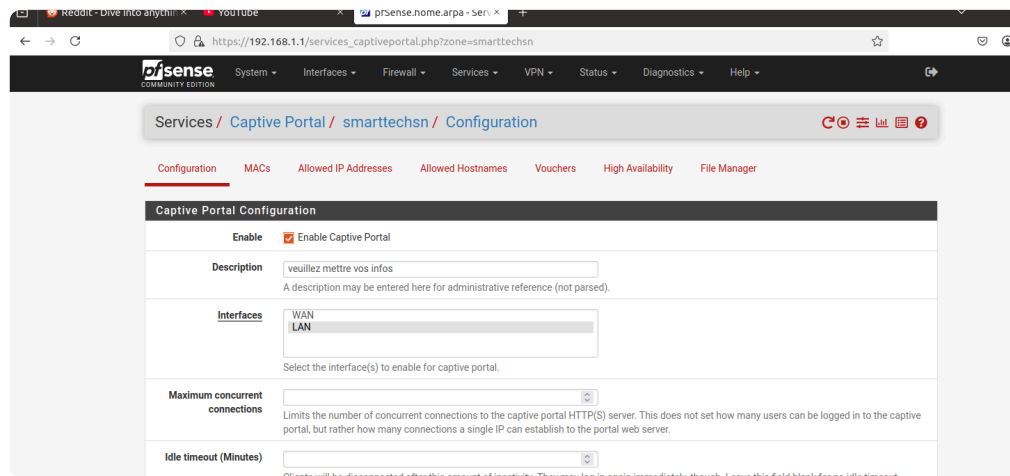
Source

Source ☐ Invert match LAN subnets Source Address /

IV.6. Configuration Radius pour l'authentification

1. Activer et Configurer le Captive Portal sur pfSense

1. Connectez-vous à [pfSense](#)
2. Va dans [Services](#) → [Captive Portal](#)
3. Clique sur [Ajouter une Zone](#) et donne-lui un nom (ex: Portail_Reseau)
4. Active la zone et choisis l'interface sur laquelle tu veux appliquer le portail captif (ex: [LAN](#) ou [WIFI](#))
5. Clique sur [Save & Continue](#)



2. Configurer l'Authentification via FreeRADIUS

1. Dans **pfSense**, va dans **System** → **User Manager** → **Authentication Servers**
2. Clique sur **Add** et remplis :
 - **Descriptive Name** : FreeRADIUS
 - **Type** : RADIUS
 - **Hostname or IP Address** : 192.168.1.103 (ton serveur FreeRADIUS)
 - **Shared Secret** : (mets le même secret que dans FreeRADIUS)
 - **Services Offered** : coche Authentication and Accounting
 - **Authentication Port** : 1812
 - **Accounting Port** : 1813
3. Clique sur **Save & Test** pour voir si la connexion est OK

Users Groups Settings **Authentication Servers**

Server Settings

Descriptive name

Type

RADIUS Server Settings

Protocol

Hostname or IP address

Shared Secret

Services offered

Authentication port

Accounting port

Authentication Timeout
 This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. NOTE: If using an interactive two-factor authentication system, increase this timeout to at least 30 seconds and enter a token.

RADIUS NAS IP Attribute
 Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests. Please note that this choice won't change the interface used for contacting the RADIUS server.

4. Vous pouvez voir le nombre d'utilisateurs connectés dans l'interface

Services / Captive Portal

Zone	Interfaces	Number of users	Description	Actions
smarttechnsn	LAN	2	veuillez mettre vos infos	Edit Delete

[+ Add](#)

voici une [video](#) demo

VII. Conclusion

Félicitations ! Vous avez maintenant un système complet avec PfSense, un portail captif, et une authentification via RADIUS et LDAP. Cette configuration vous permet de :

- Gérer votre réseau avec un pare-feu robuste
- Sécuriser l'accès à Internet via un portail d'authentification
- Centraliser la gestion des utilisateurs via LDAP
- Auditer les connexions grâce aux journaux RADIUS

Cette configuration est adaptée à de nombreux environnements, notamment :

- Les petites et moyennes entreprises
- Les établissements éducatifs
- Les hôtels et espaces publics offrant un accès Wi-Fi
- Les environnements de test et de développement

Pour aller plus loin, vous pourriez explorer :

- La mise en place d'un VPN pour l'accès à distance
- La configuration de VLAN pour segmenter davantage votre réseau
- L'implémentation de règles de filtrage par utilisateur
- La supervision du réseau avec des outils comme Nagios ou Zabbix