

BENZERGUA FARES

AP14 : PFSense & PORTAIL CAPTIF



1. Création d'une VM sous Proxmox

Nous débutons par la création d'une machine virtuelle (VM) sur Proxmox.

Create: Virtual Machine

General

OS

System

Disks

CPU

Memory

Network

Confirm

Node:

pvesio-grp6

Resource Pool:

C420-GRP4

VM ID:

3038

Name:

SrvPfSense

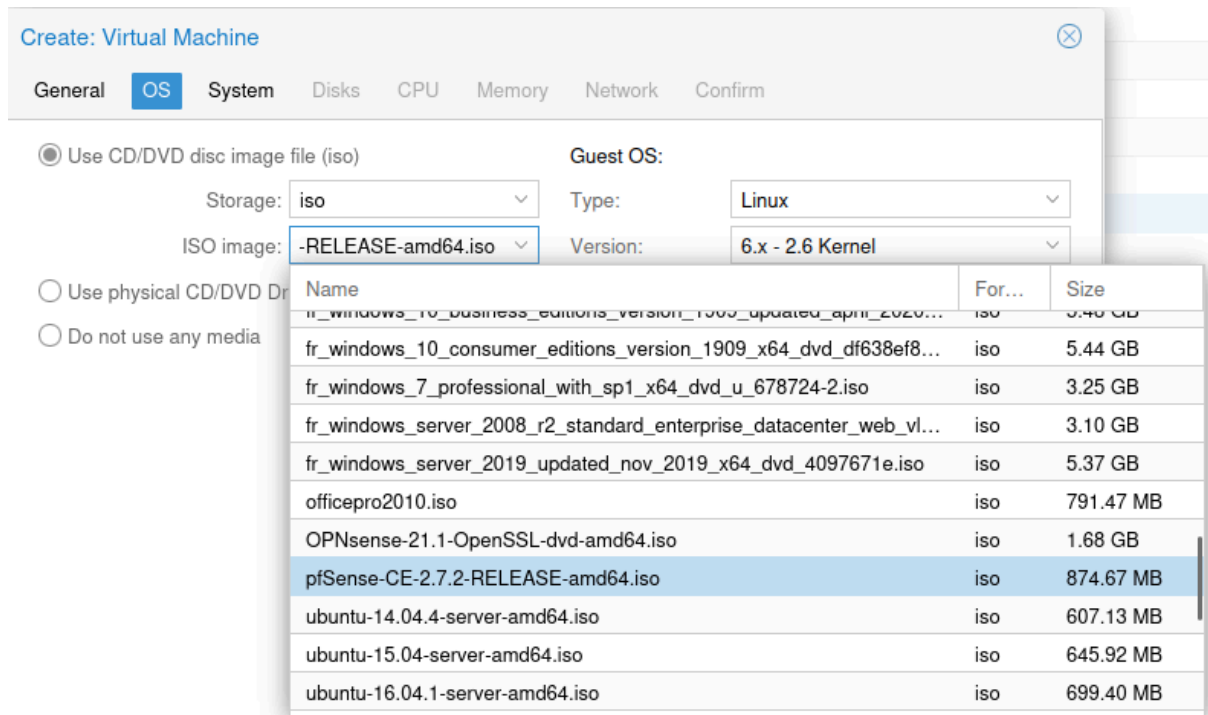
Ensuite, nous procédons à la configuration des cartes réseau en ajoutant une seconde interface. Voici la répartition des interfaces :

- net0 : Interface WAN (connexion vers l'extérieur).

net1 : Interface LAN (réseau interne).

⇄	Network Device (net0)	virtio=BC:24:11:7F:0B:E5,bridge=vmbr1,firewall=1,tag=544
⇄	Network Device (net1)	virtio=BC:24:11:E3:DE:AE,bridge=vmbr1,firewall=1,tag=540

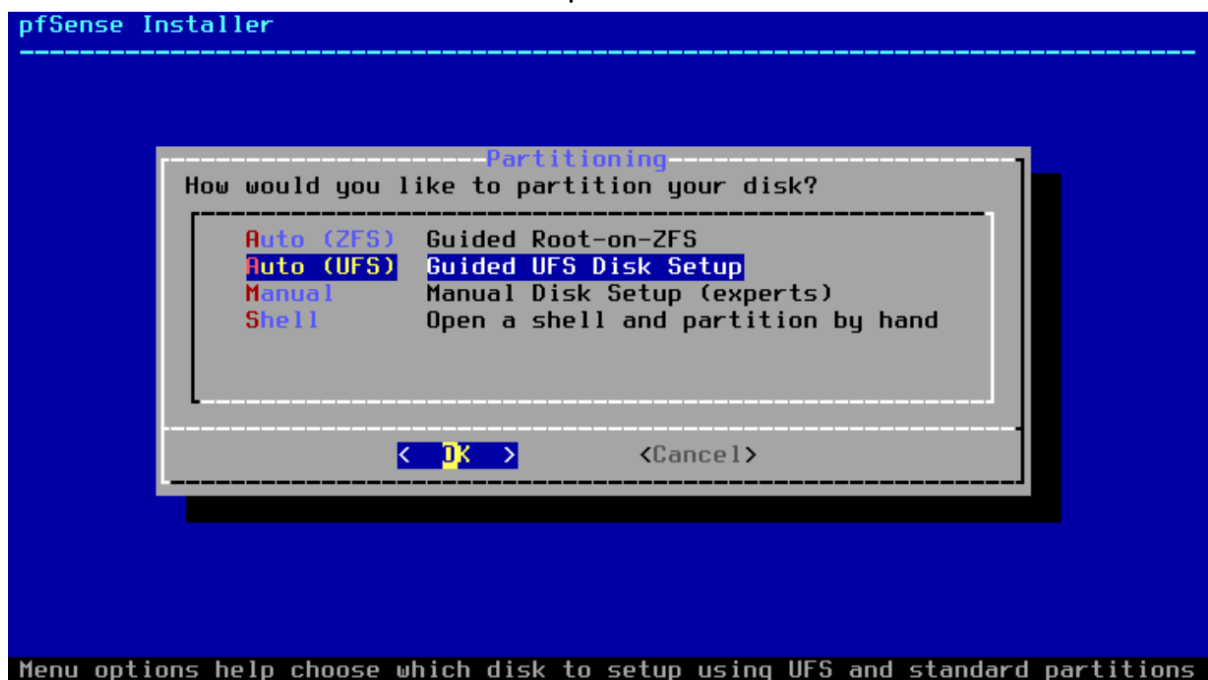
Une fois la VM configurée, nous sélectionnons l'image ISO de Pfsense et lançons l'installation



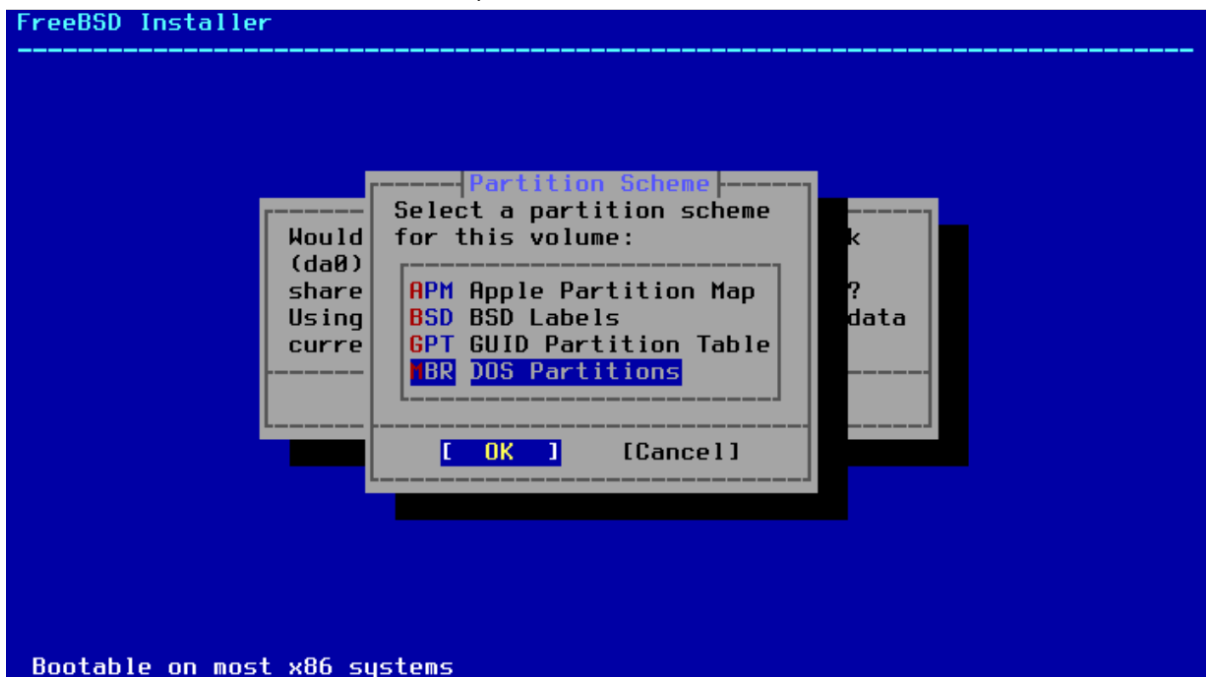
2. Installation de Pfsense

L'installation de Pfsense suit les étapes suivantes :

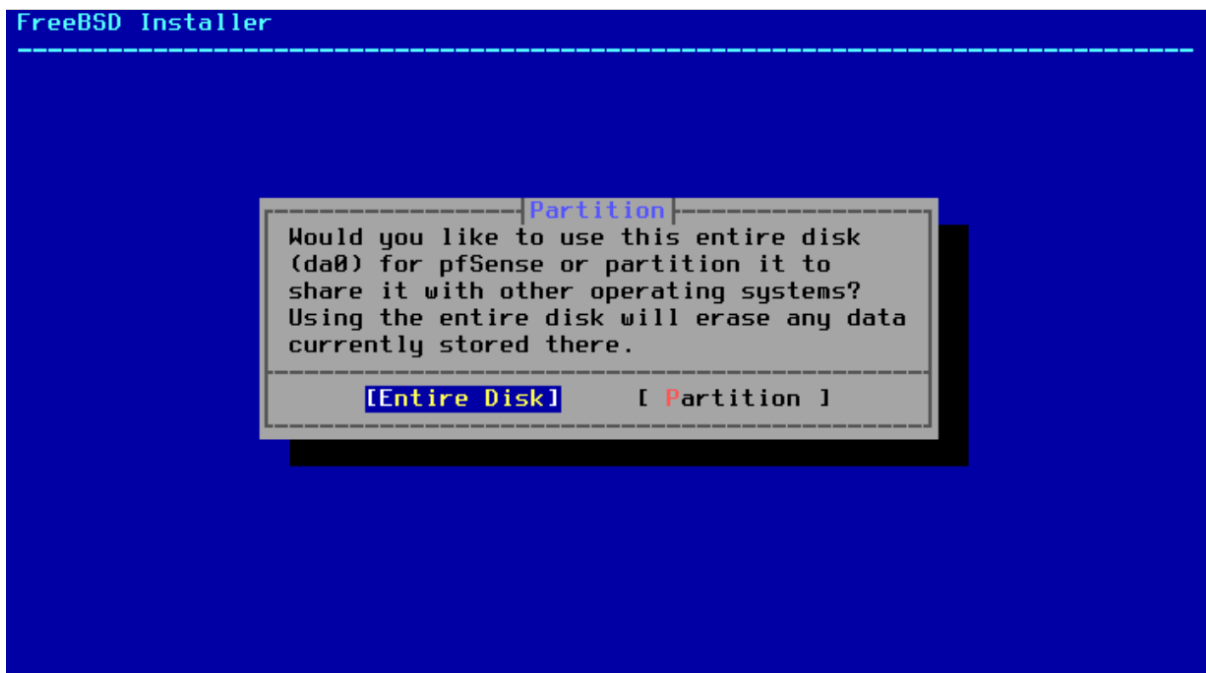
Partitionnement automatique du disque : Nous choisissons l'option de partitionnement automatique pour utiliser la totalité de l'espace disque disponible.



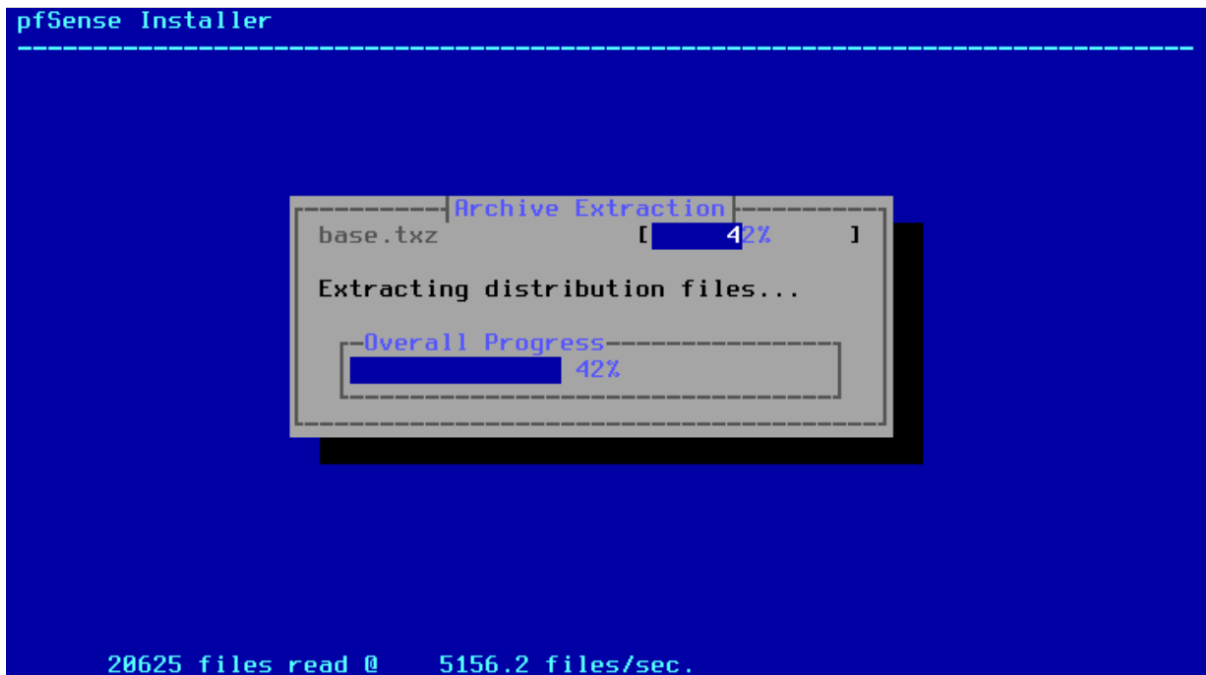
Méthode MBR (Master Boot Record) : Nous utilisons ce mode de partitionnement.



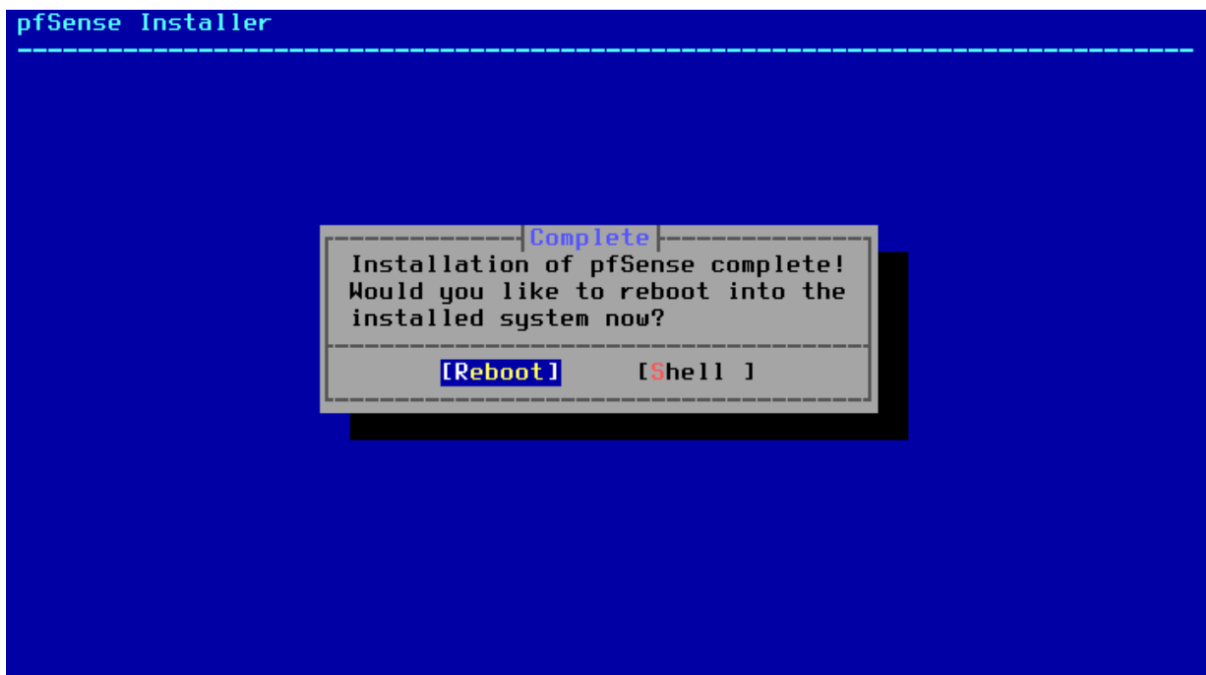
Réinitialisation du disque dur : Cette étape est nécessaire avant de poursuivre l'installation.



Installation en cours : Pfsense s'installe sur notre VM.



Redémarrage de la machine : Une fois l'installation terminée, nous redémarrons la VM.



3. Configuration de Pfsense

Après le redémarrage, nous attribuons les interfaces réseau comme suit :

- net0:WAN
- net1:LAN

```

vtnet1  bc:24:11:e3:de:ae (down) VirtIO Networking Adapter

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [yln]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(vtnet0 vtnet1 or a): vtnet1

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet0 a or nothing if finished): vtnet0

The interfaces will be assigned as follows:

WAN  -> vtnet1
LAN  -> vtnet0

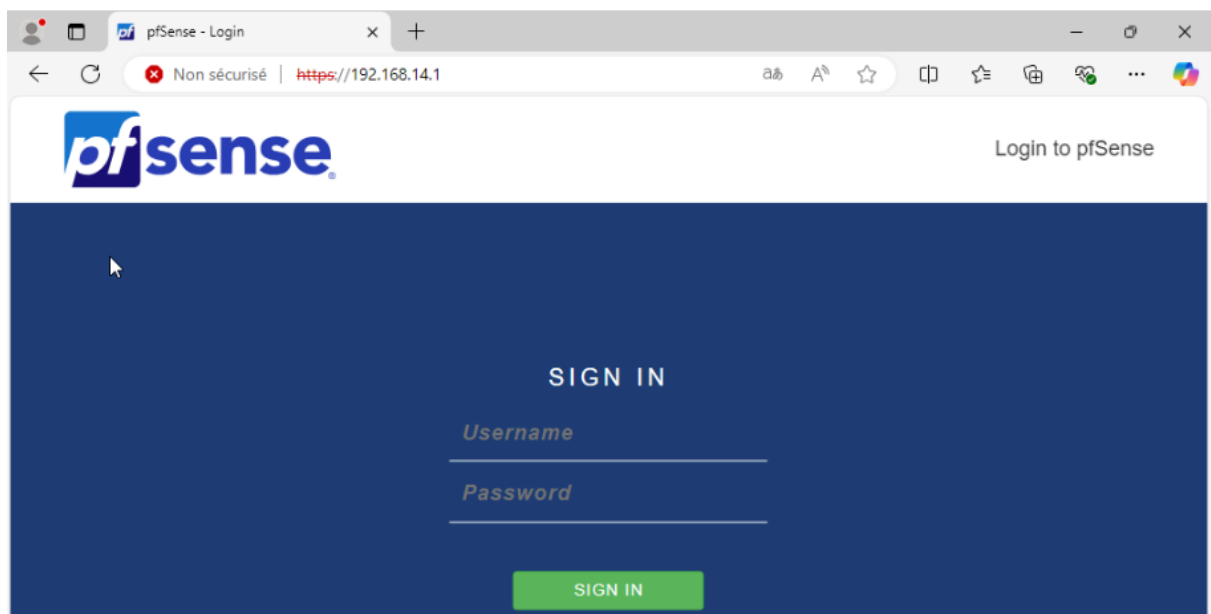
Do you want to proceed [yln]?
Enter an option:
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from 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:

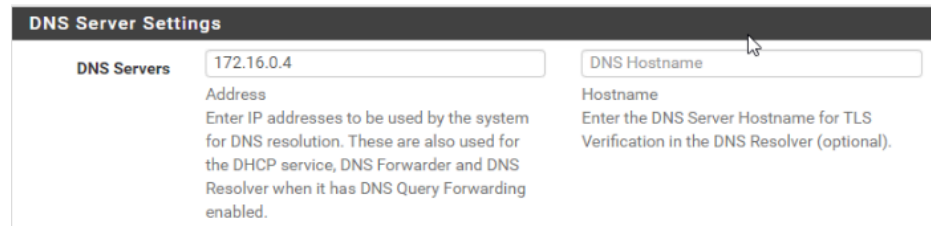
```

4. Mise en place du portail captif

1. Connexion à l'interface d'administration de Pfsense via l'URL :
<https://192.168.14.1/>.
2. Identification avec les identifiants par défaut :
 - Login : **admin**
 - Mot de passe : **pfsense**



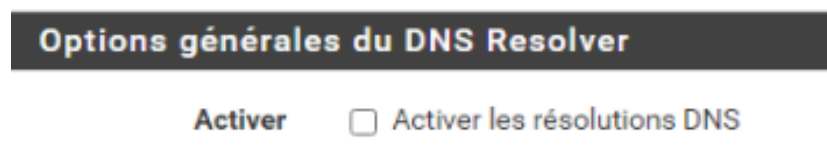
3. Configuration du serveur DNS avec les adresses DNS du lycée : **172.16.0.4**.



DNS Server Settings

DNS Servers	<input type="text" value="172.16.0.4"/>	<input type="text" value="DNS Hostname"/>
Address	Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.	Hostname Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).

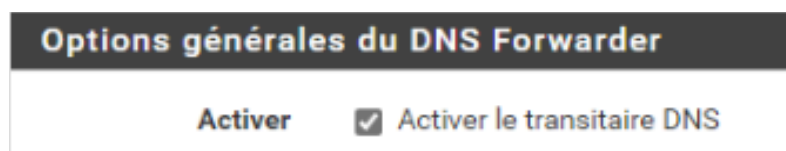
4. Désactivation du service DNS Resolver (menu **Services -> DNS Resolver**).



Options générales du DNS Resolver

Activer ☐ Activer les résolutions DNS

5. Activation du service DNS Forwarder (**Services -> DNS Forwarder**).



Options générales du DNS Forwarder

Activer ☒ Activer le transitaire DNS

Ensuite, nous effectuons une série de tests depuis un client Windows :

- Ping vers le serveur Pfsense.

```
C:\Users\sio>ping 192.168.14.1

Envoi d'une requête 'Ping' 192.168.14.1 avec 32 octets de données :
Réponse de 192.168.14.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.14.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.14.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.14.1:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
Ctrl+C
^C
C:\Users\sio>ping 192.168.11.71

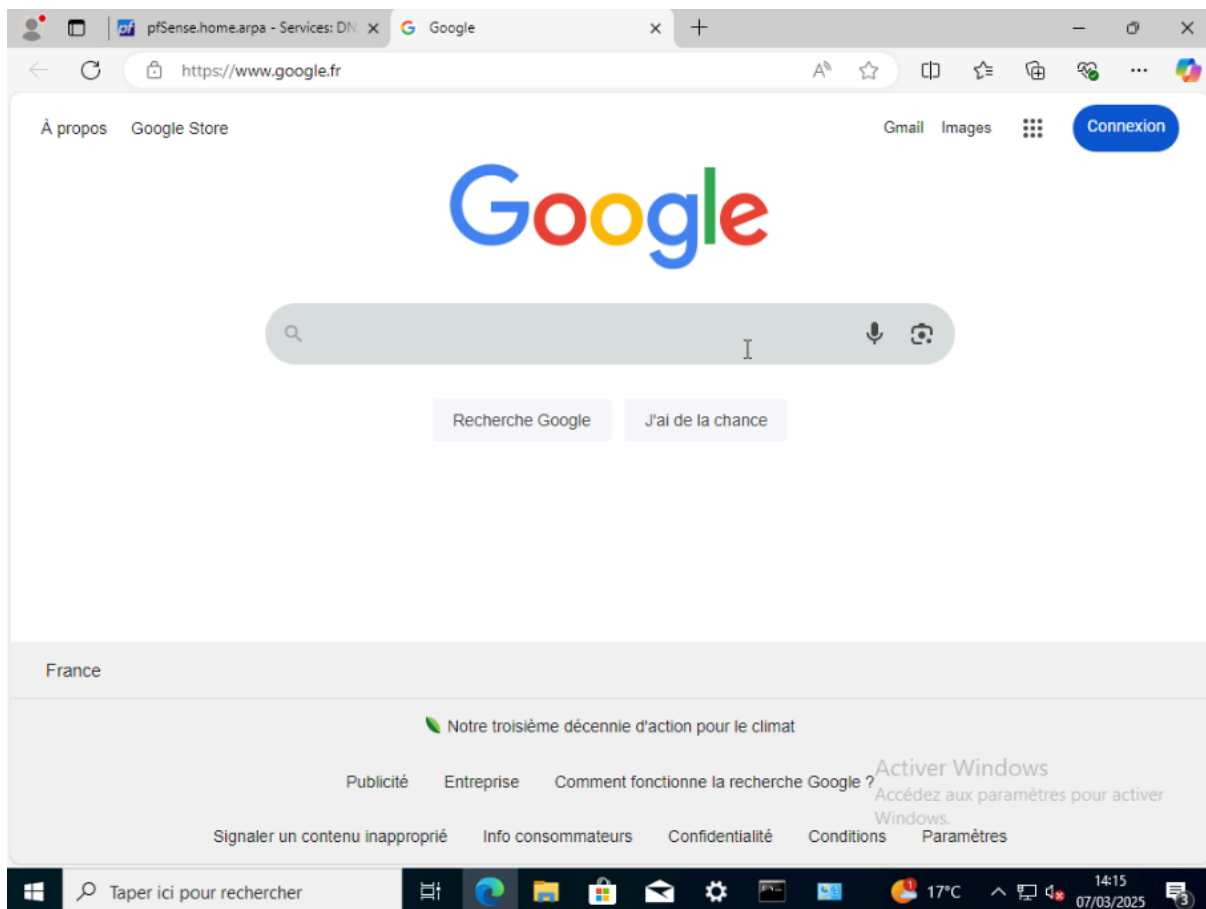
Envoi d'une requête 'Ping' 192.168.11.71 avec 32 octets de données :
Réponse de 192.168.11.71 : octets=32 temps<1ms TTL=64
Réponse de 192.168.11.71 : octets=32 temps<1ms TTL=64
Réponse de 192.168.11.71 : octets=32 temps<1ms TTL=64
```

- Test **nslookup** avec le serveur DNS.

```
C:\Users\sio>nslookup google.fr
Serveur : pfsense.home.arpa
Address: 192.168.14.1

Réponse ne faisant pas autorité :
Nom : google.fr
Addresses: 2a00:1450:4007:80e::2003
216.58.214.163
```

- Accès à **google.fr** via un navigateur web.



Activation du portail captif

1. Création du portail captif nommé PortailCaptif.
2. Activation du portail sur l'interface LAN.

Services / Captive Portal / PortailCaptif / Configuration

Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers High

Captive Portal Configuration

Enable ☒ Enable Captive Portal

Description
A description may be entered here for administrative reference (not

Interfaces

Select the interface(s) to enable for captive portal.

3. Sélection d'une authentification de type "Authentication backend".

Authentication

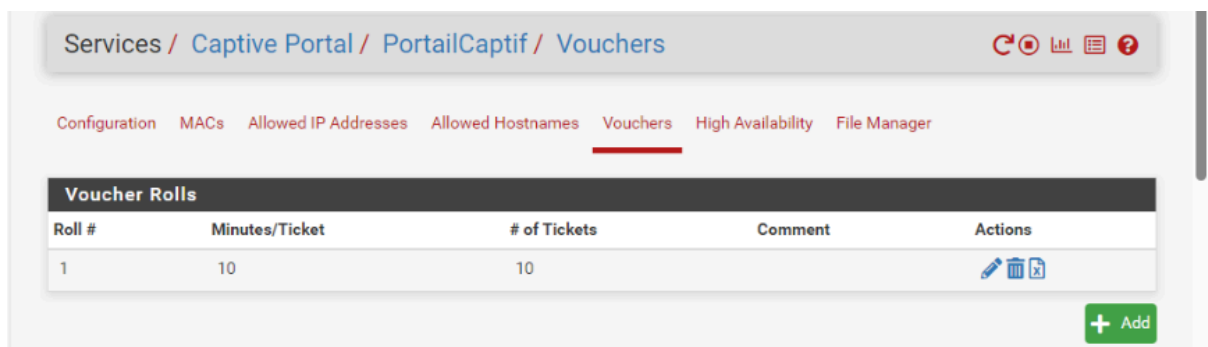
Authentication Method

Select an Authentication Method to use for this zone. One method must be selected.

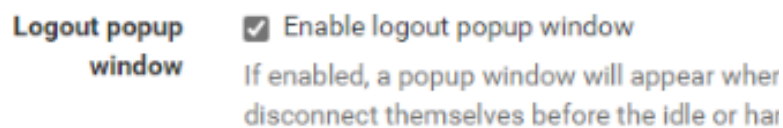
- "Authentication backend" will force the login page to be displayed a password, or using vouchers.
- "None" method will force the login page to be displayed but will not authenticate.
- "RADIUS MAC Authentication" method will try to authenticate device without displaying any login page.

4. Configuration du mode d'authentification par vouchers avec les paramètres suivants :

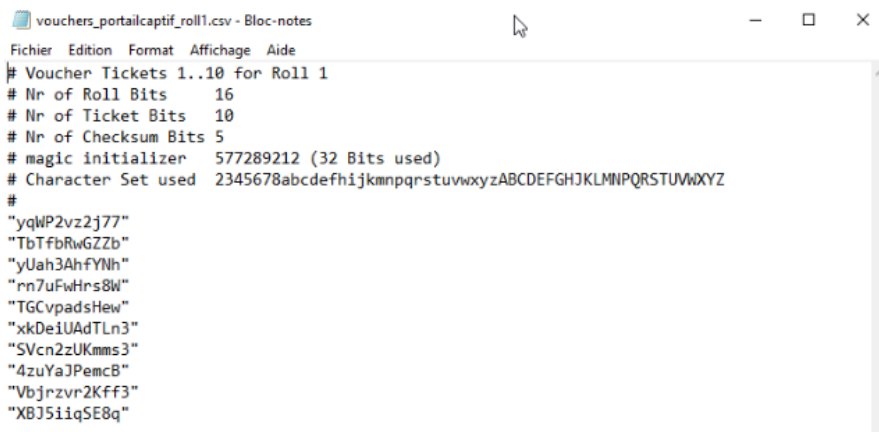
- Nombre maximal de bons d'échange : 10
- Durée de connexion par bon : 10 minutes



5. Activation de l'option "Enable logout popup window" pour permettre aux utilisateurs de se déconnecter.



6. Récupération du fichier .csv contenant les bons d'échange.



5. Configuration du DHCP

1. Activation du service DHCP sur l'interface LAN.

General DHCP Options	
DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface

2. Définition d'une plage d'adresses IP en excluant :
 - L'IP de PfSense.
 - L'IP du routeur.
 - L'IP future de la borne WiFi.

Primary Address Pool	
Subnet	192.168.14.0/24
Subnet Range	192.168.14.1 - 192.168.14.254
Address Pool Range	<div>192.168.14.150</div> <div>From</div> <div>192.168.1.225</div> <div>To</div>

Vérification du service DHCP

Pour vérifier le bon fonctionnement du DHCP, nous utilisons une machine Windows 10 qui reçoit bien une adresse IP automatiquement attribuée.

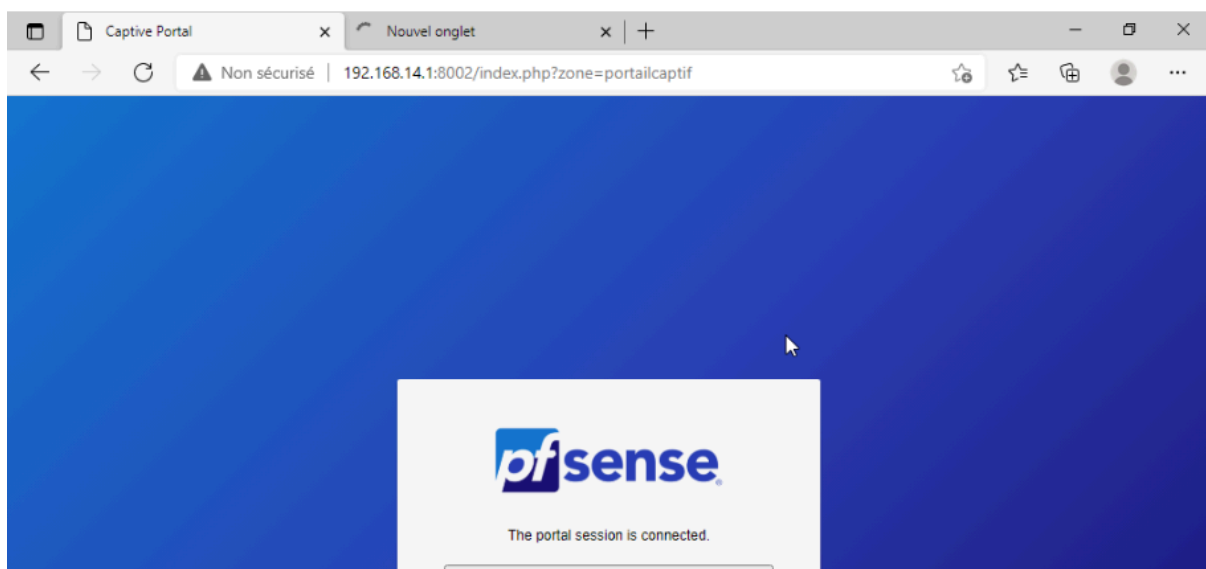
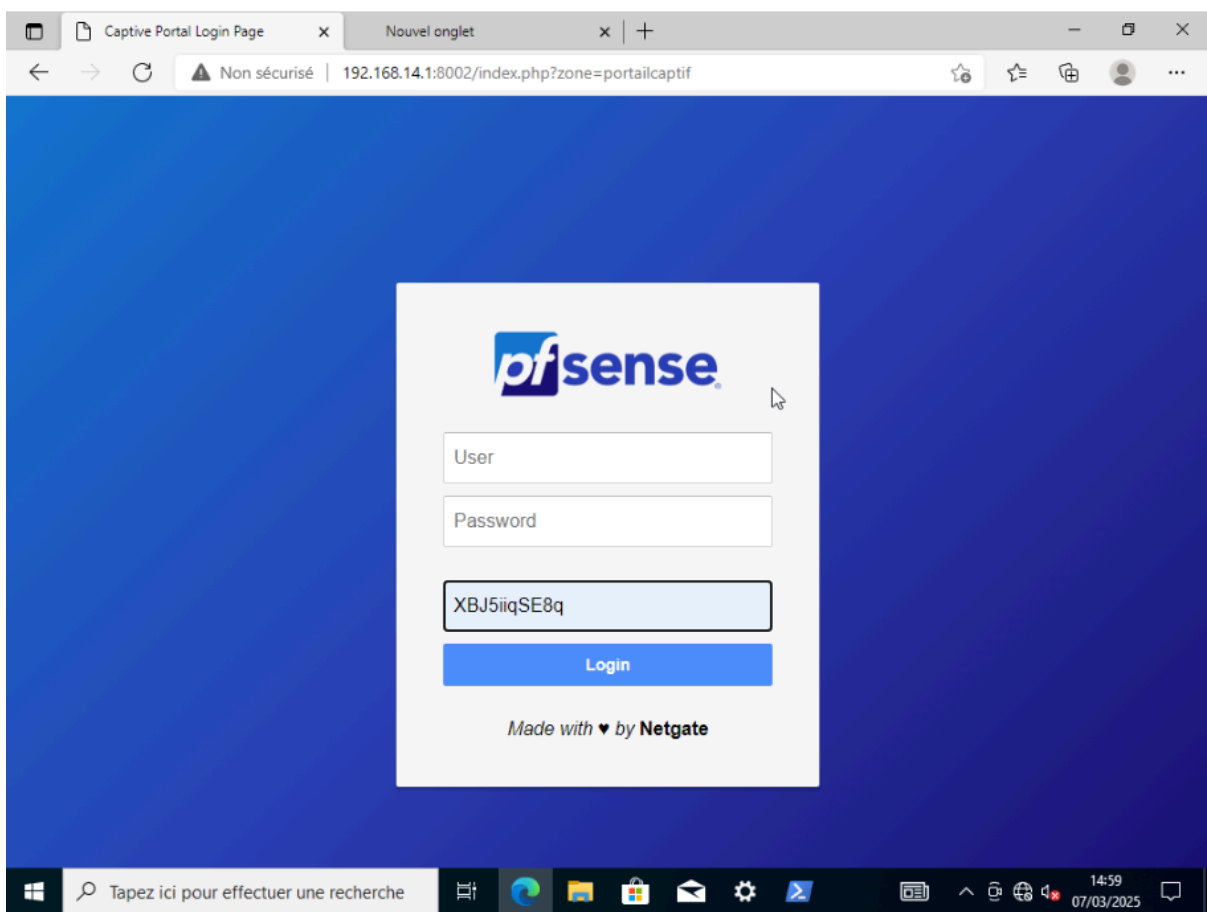
```
PS C:\Users\sio> ipconfig /renew

Configuration IP de Windows

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . : home.arpa
    Adresse IPv6 de liaison locale. . . . . : fe80::3749:30df:514d:a895%7
    Adresse IPv4. . . . . : 192.168.14.200
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.14.1
```

Ensuite, nous testons l'accès à un serveur HTTPS interne. Lors de la connexion, une page d'authentification apparaît. Après identification avec un bon d'échange valide, une page de confirmation s'affiche.



k

6. Validation finale

Enfin, nous testons l'accès à [google.fr](https://www.google.fr) pour s'assurer du bon fonctionnement du réseau. Tous les paramètres sont opérationnels.

