

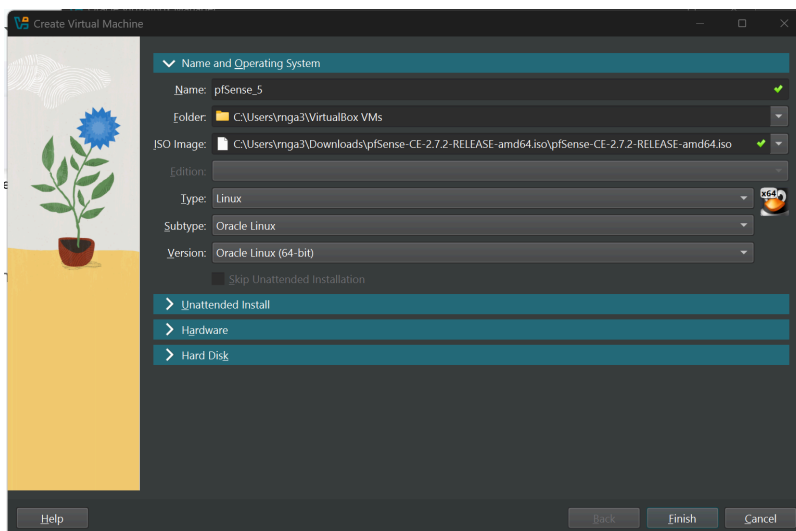
Laboratoire 5 pfSense

Pare-feu Portail Captif - Rôles et Tickets de Connexion

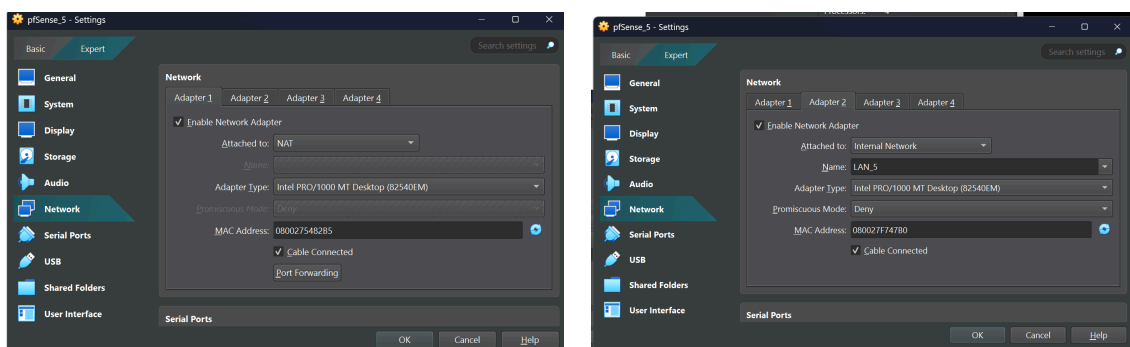
Ce document décrit la configuration complète d'un pare-feu pfSense, depuis son installation initiale et la configuration réseau jusqu'à la mise en place d'un portail captif fonctionnel avec gestion des utilisateurs et des bons de connexion. Le guide couvre également la création des machines clientes dans un environnement virtualisé.

Création des machines clientes et pfSense dans VMWare

pfSense + Setup

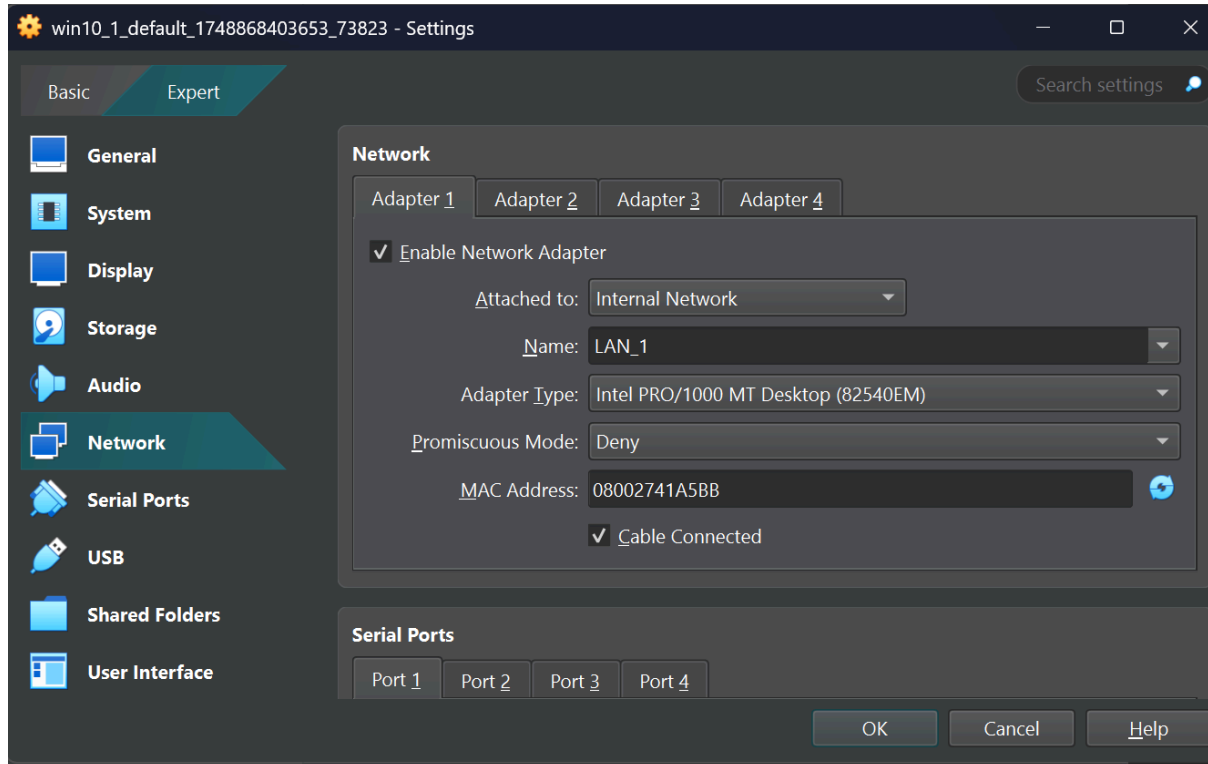


Configuration des cartes réseaux pfSense (NAT Adapter 1 et LAN Adapter 2)



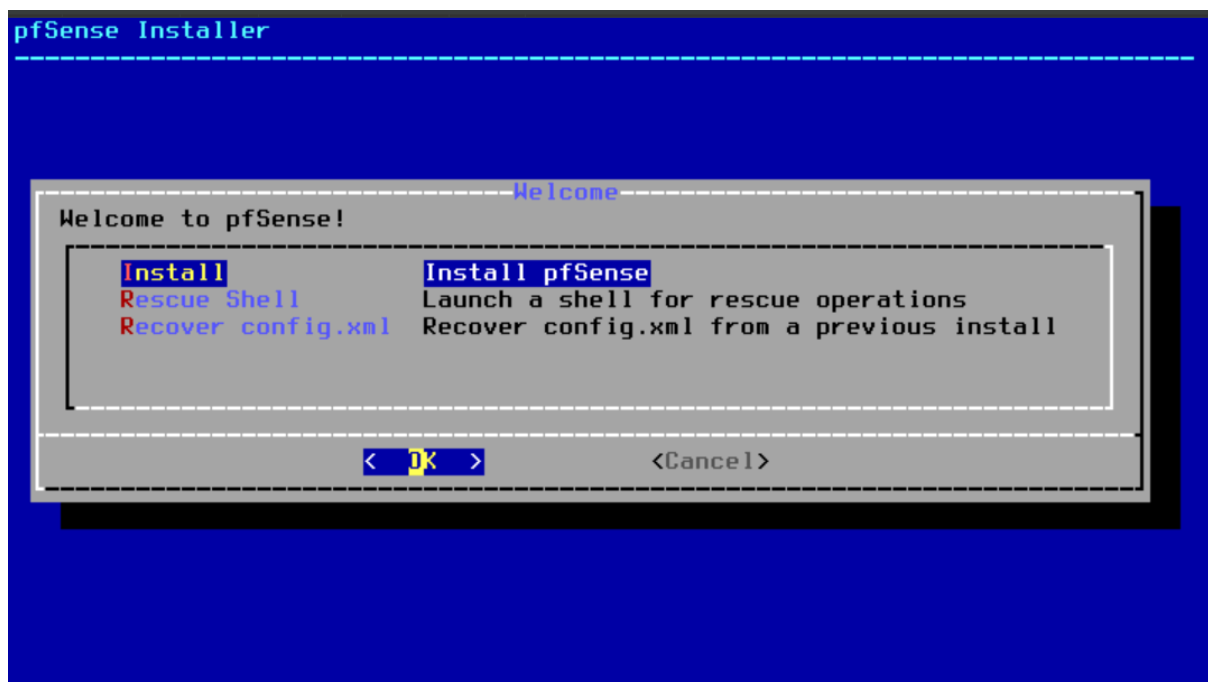
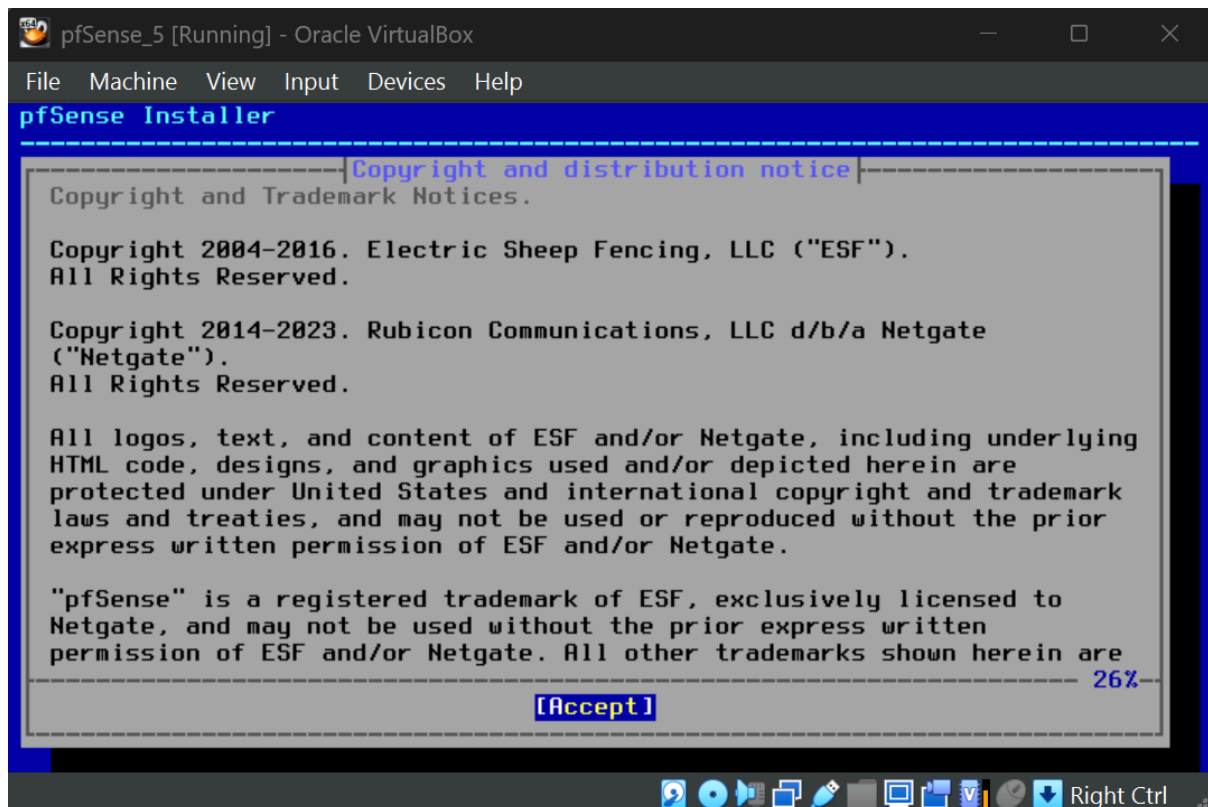
Création des machines clientes (avec Vagrant; L'installation va prendre quelques minutes). Répéter pour chaque client (deux dans mon cas), et ensuite, configurer leurs cartes réseaux vers le LAN_5 dans VB (Seulement LAN).

```
PS C:\Users\rnga3\OneDrive\Documents\VMs\lab5> cd win10_1
PS C:\Users\rnga3\OneDrive\Documents\VMs\lab5\win10_1> vagrant init gusztavvargadr/windows-10
A 'Vagrantfile' has been placed in this directory. You are now
ready to 'vagrant up' your first virtual environment! Please read
the comments in the Vagrantfile as well as documentation on
'vagrantup.com' for more information on using Vagrant.
PS C:\Users\rnga3\OneDrive\Documents\VMs\lab5\win10_1> vagrant up
```

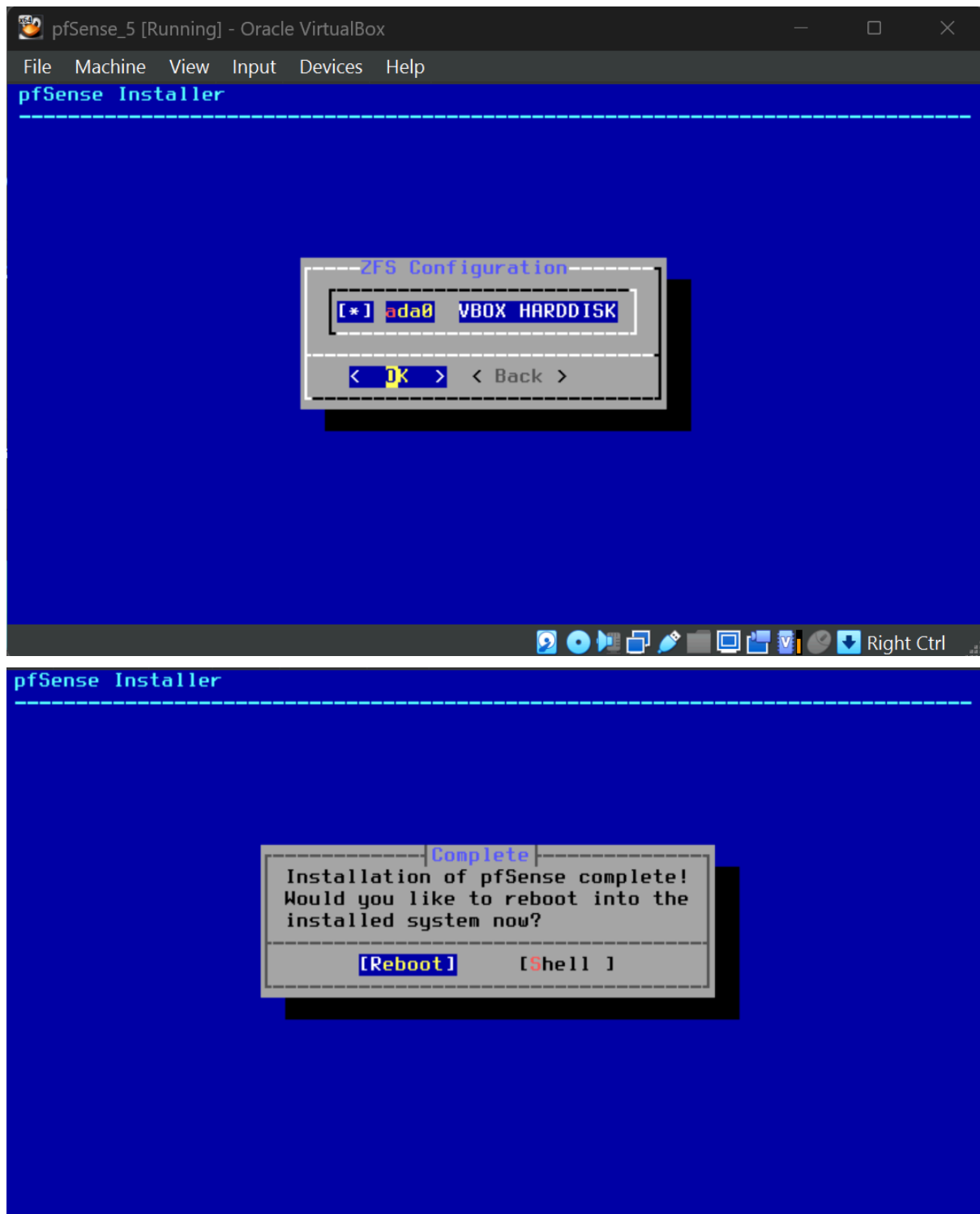


Installation et configuration de base de pfSense

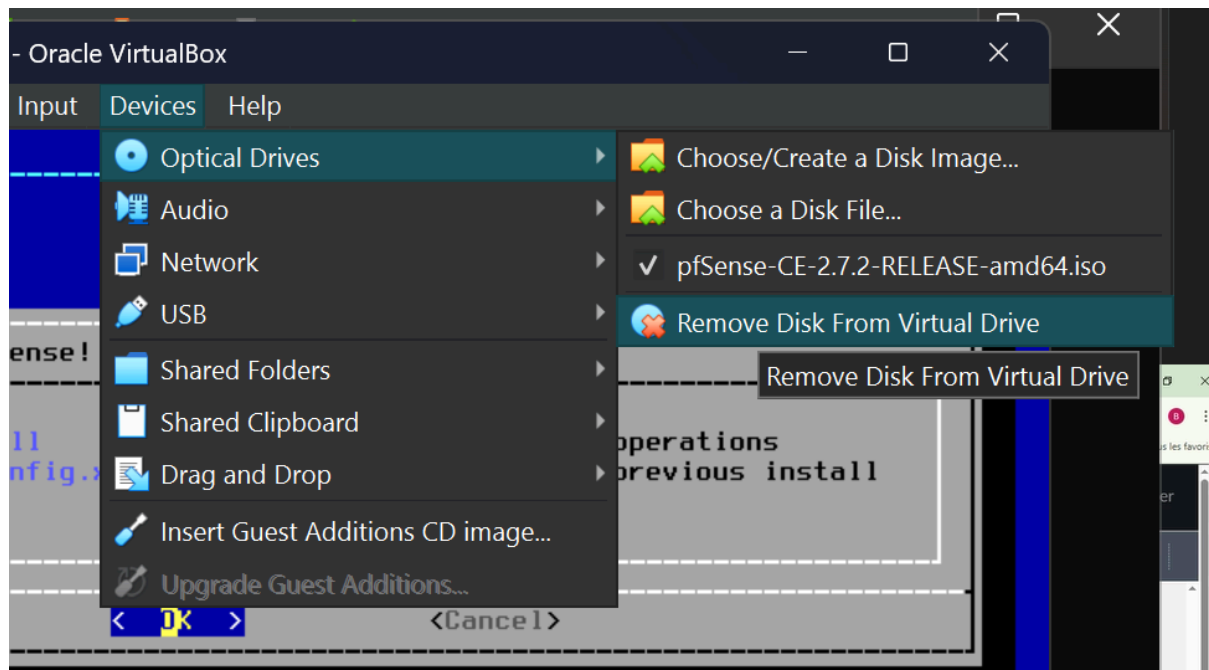
Installation



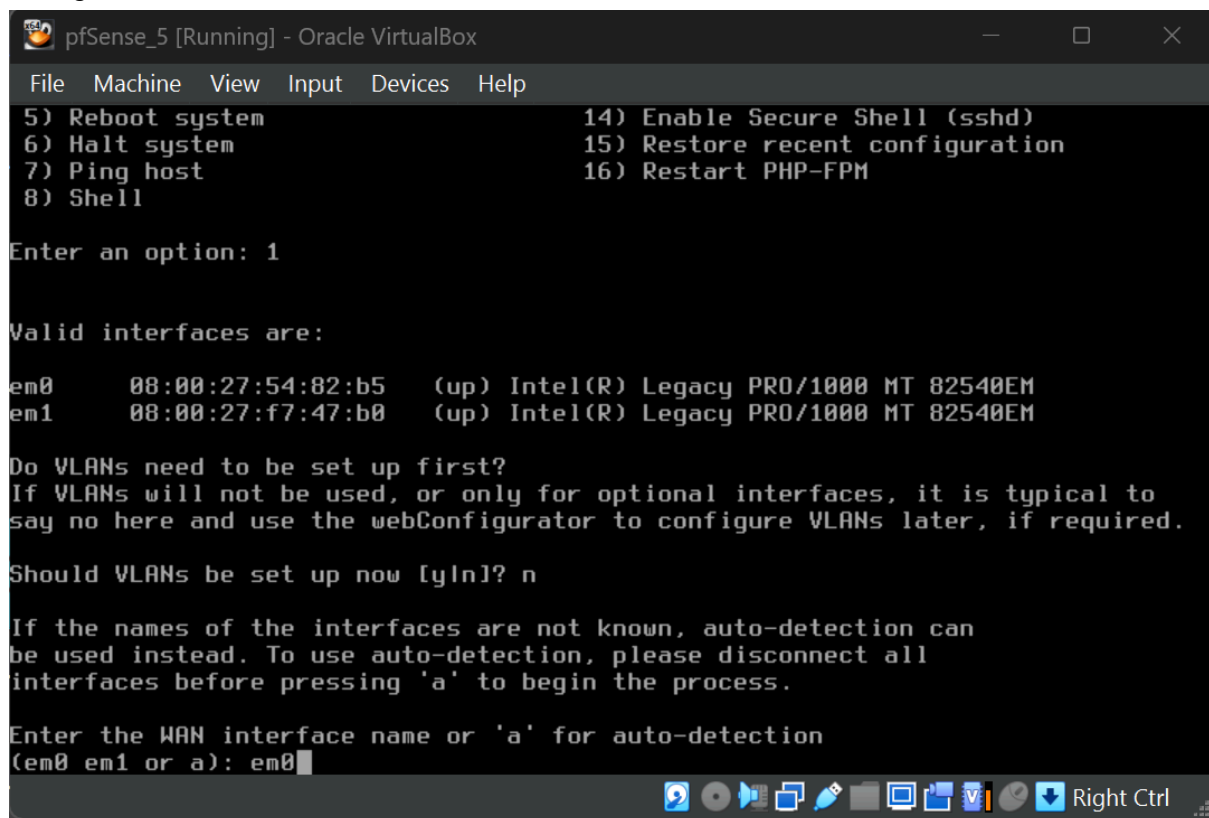
Space+Enter



Retirer le média d'installation et reboot



Configuration de base



```
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1

Do you want to proceed [y|n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
```

Configuration du IPv4 DHCP Service

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - dhcp)

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:
> 192.168.1.1

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):
> 24

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

```
>
Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.5
Enter the end address of the IPv4 client address range: 192.168.1.15
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

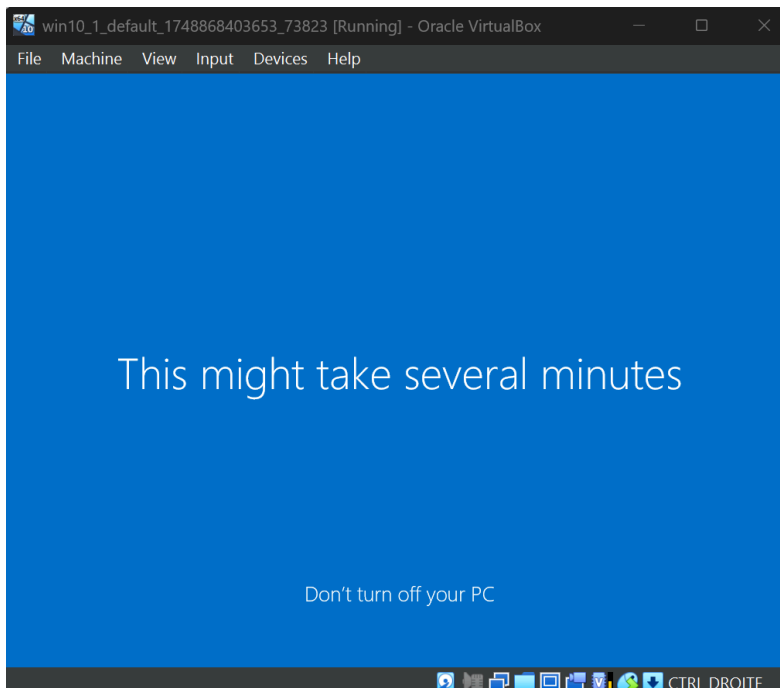
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

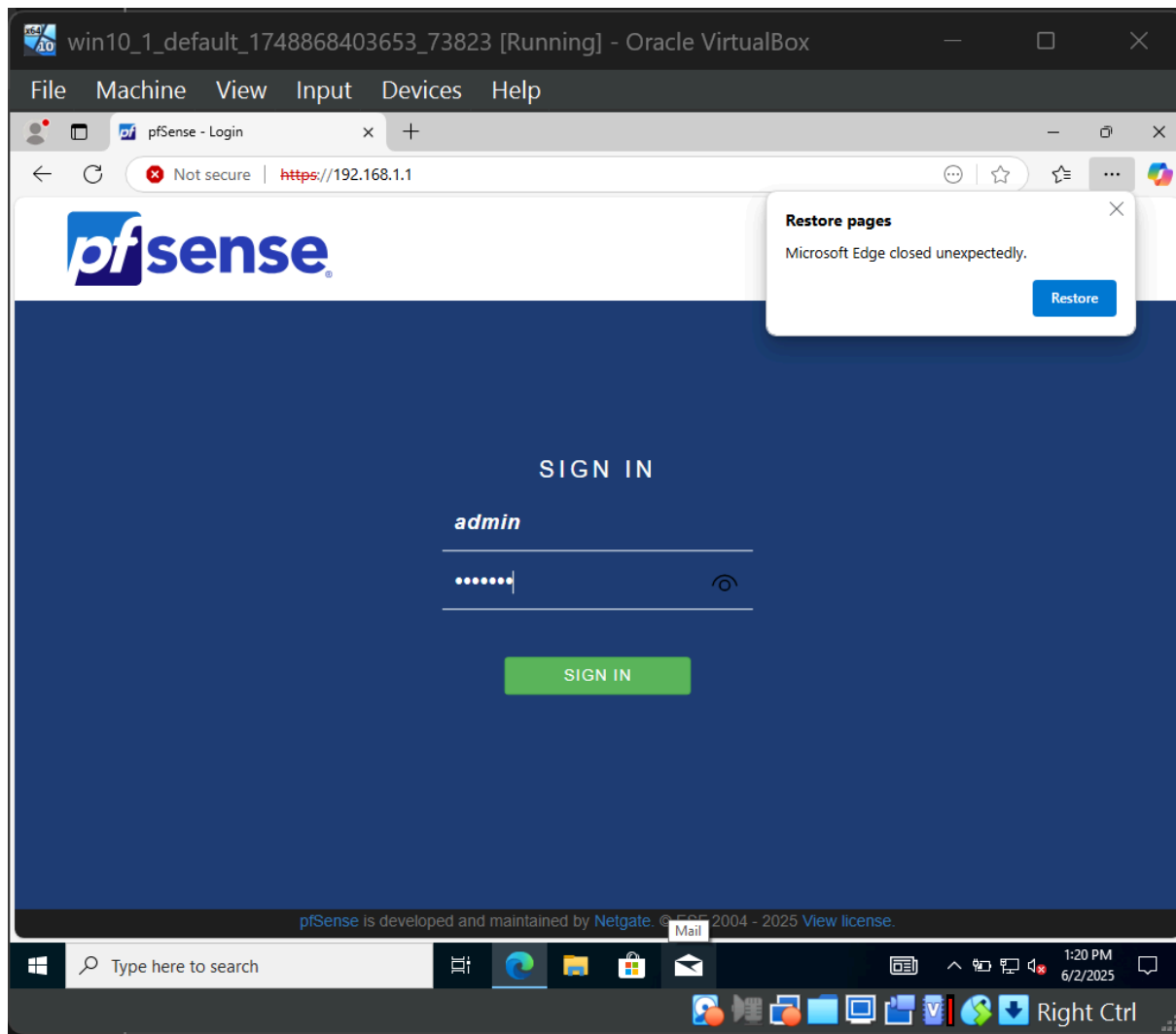
The IPv4 LAN address has been set to 192.168.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
        https://192.168.1.1/

Press <ENTER> to continue.
```

Accès à WebConfigurator d'une machine cliente

Sans fermer pfSense, lancer une machine cliente, et accéder à sa default gateway/l'adresse IP de pfSense sur un navigateur, soit <https://192.168.1.1> dans ce cas.





pfSense = default password

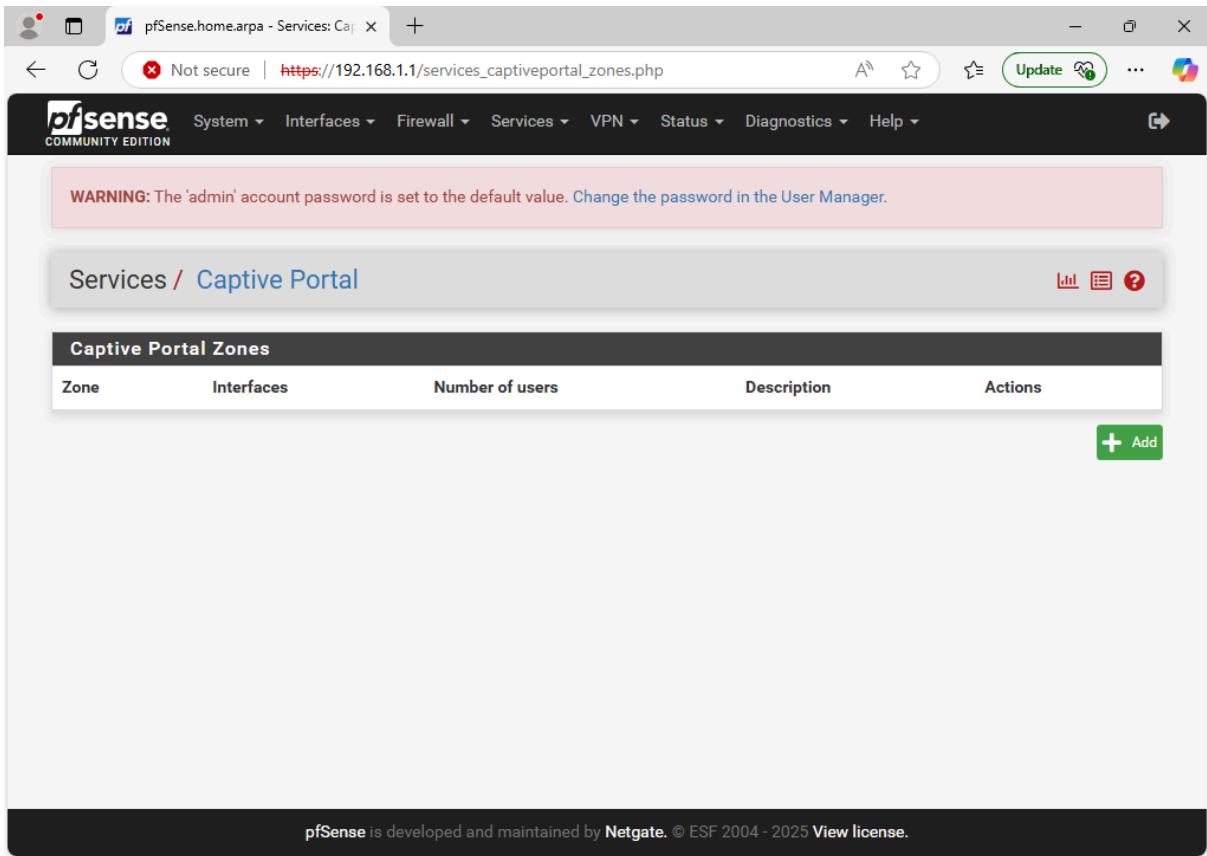
Configuration du portal captif

Naviguez vers Services > Captive Portal.

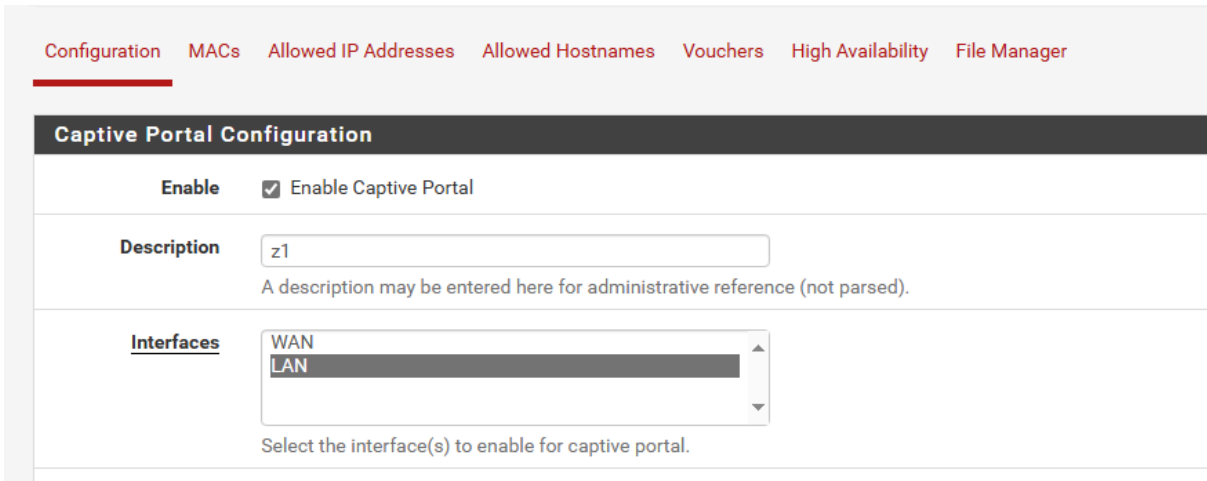
Cliquez sur Add pour créer une nouvelle zone.

Entrez zone1 comme "Zone name" et z1 comme "Zone description".

Cliquez sur Save & Continue.



Cochez *Enable Captive Portal*.
Sous "*Interfaces*", sélectionnez *LAN*.
Sous "*Authentication*", choisissez *Local Database* comme "*Method*".
Considérez l'option *Reauthenticate connected users every minute* si nécessaire.



System / [User Manager](#) / [Users](#)

[Users](#) [Groups](#) [Settings](#) [Authentication Servers](#)

Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	user1		✓	groupe_a	

[+ Add](#) [Delete](#)

Authentication

Authentication Method Use an Authentication backend

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

- "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

Authentication Server Local Database

You can add a remote authentication server in the [User Manager](#).
Vouchers could also be used, please go to the [Vouchers Page](#) to enable them.

Secondary authentication Server Local Database

You can optionally select a second set of servers to to authenticate users. Users will then be able to login using se HTML inputs.
This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.

Reauthenticate Users ☐ Reauthenticate connected users every minute

If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requi

Nouveau Groupe et nouvel utilisateur

Naviguez vers [System](#) > [User Manager](#) > [Groups](#) pour gérer les groupes d'utilisateurs.

Naviguez vers [System](#) > [User Manager](#) > [Users](#) pour gérer les utilisateurs.

Ajoutez un nouvel utilisateur (par exemple, [user1](#)) et assignez-le à un groupe (par exemple, [groupe_a](#)).

Il faut aussi faire sur de donner au groupe les autorisations et privilèges nécessaires pour accéder au portail captif.





not secure | https://192.168.1.1/system_groupmanager.php

pfsense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

System / User Manager / Groups ?

Users Groups Settings Authentication Servers

Groups			
Group name	Description	Member Count	Actions
all	All Users	1	 
admins	System Administrators	1	 

[+ Add](#)

Vouchers

Services / Captive Portal / zone1 / Vouchers ?

Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

Voucher Rolls				
Roll #	Minutes/Ticket	# of Tickets	Comment	Actions

Create, Generate and Activate Rolls with Vouchers

Enable ☒ Enable the creation, generation and activation of rolls with vouchers

Create, Generate and Activate Rolls with Vouchers

Voucher Public Key

Services / Captive Portal / zone1 / Vouchers / Edit

Voucher Rolls

Roll #

12

Enter the Roll# (0..65535) found on top of the generated/printed vouchers

Minutes per ticket

60

Defines the time in minutes that a user is allowed access. The clock starts ticking the first time a voucher is used for authentication.

Count

10

Enter the number of vouchers (1..1023) found on top of the generated/printed vouchers. WARNING: Changing this number for an existing Roll will mark all vouchers as unused again

Comment


test

Can be used to further identify this roll. Ignored by the system.

Save

Captive Portal Login

Not secure | 192.168.1.1:8002/index.php?zone=zone1&redirecturl=http%3A%2F%2Fedge-http.microso...



First Authentication Method

User

Password

Second Authentication Method

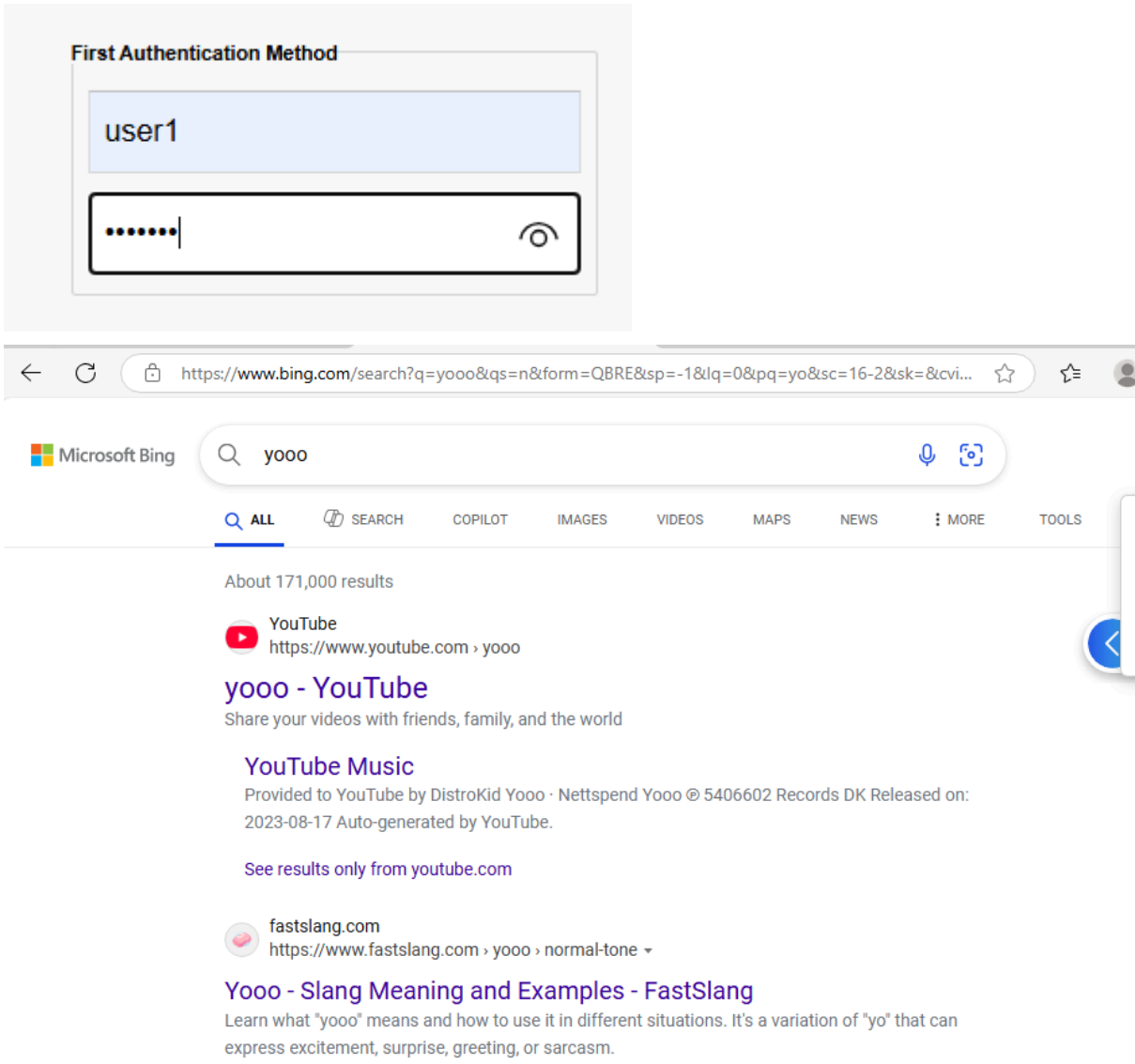
User

Password

Voucher Code

Login

Tune here to search 2:14 PM



Monitoring

Naviguez vers *Status > Captive Portal > zone1 > Active Users* pour voir les utilisateurs connectés, leur adresse IP, adresse MAC, nom d'utilisateur et l'heure de début de session.

Users Logged In (1)

IP address	MAC address	Username	Session start	Actions
192.168.1.5	08:00:27:41:a5:bb	user1	06/03/2025 14:17:39	

Show Last Activity

Disconnect All Users

Status / Captive Portal / zone1 / Voucher Rolls

Active Users

Active Vouchers

Voucher Rolls

Test Vouchers

Expire Vouchers

Roll#	Minutes/Ticket	# of Tickets	Comment	used	active	ready
5	60	10		0	0	10

Conclusion

Ces étapes guident l'utilisateur à travers la configuration complète d'un pare-feu pfSense, depuis son installation initiale et la configuration réseau jusqu'à la mise en place d'un portail captif fonctionnel avec gestion des utilisateurs et des bons de connexion.