# Rapport sur la Mise en Œuvre d'un Pare-feu PfSense

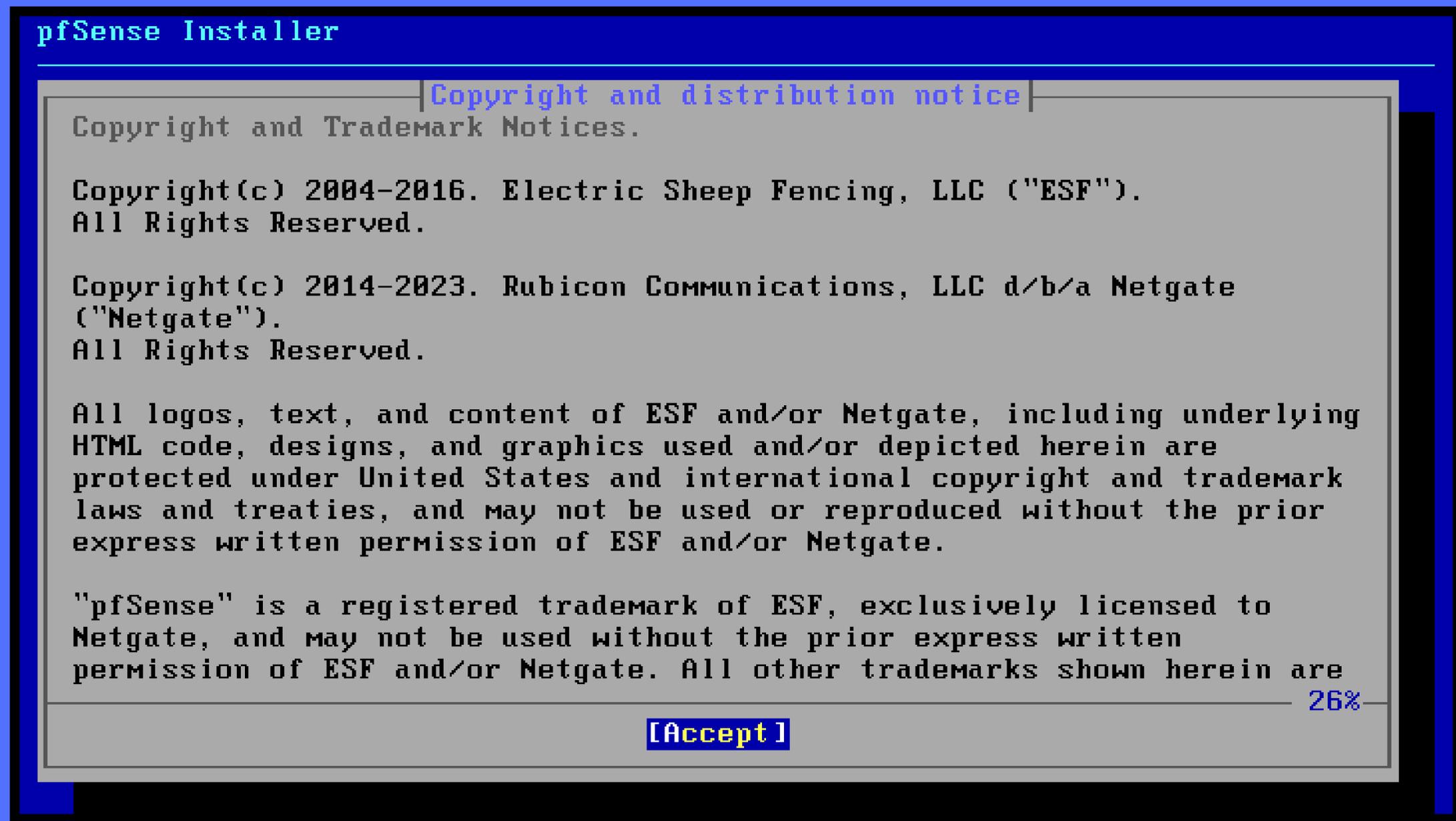**Chater Ahmed**

David Daouda Coulibaly

introduction :

PfSense est une distribution open source de FreeBSD, conçue pour agir comme pare-feu et routeur avec une gestion conviviale via une interface Web. Doté de fonctionnalités telles que le pare-feu, le NAT/PAT, le relais DHCP/DNS, le proxy, le VPN et le hotspot Wi-Fi, PfSense offre une solution complète pour sécuriser et gérer les réseaux.
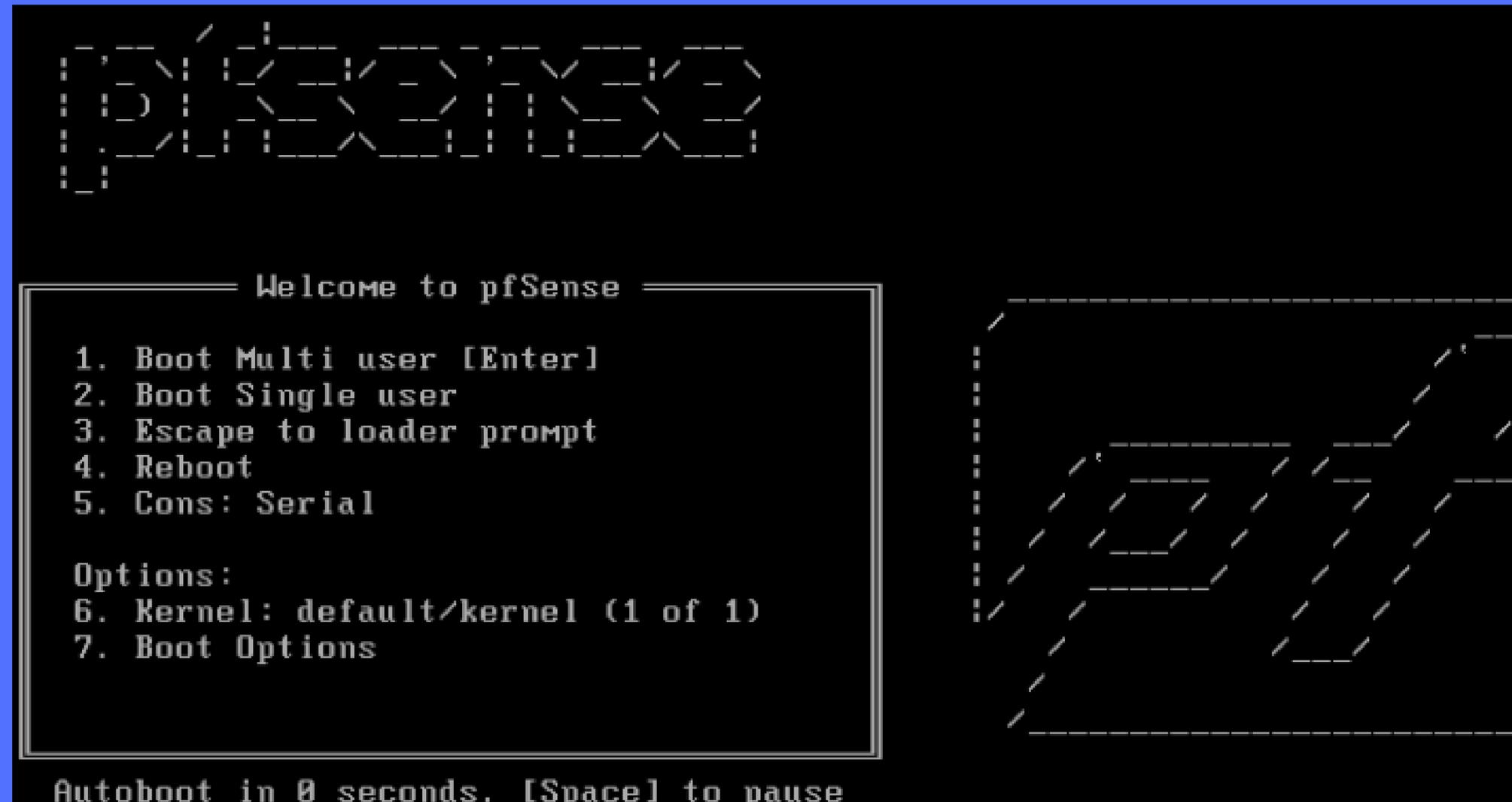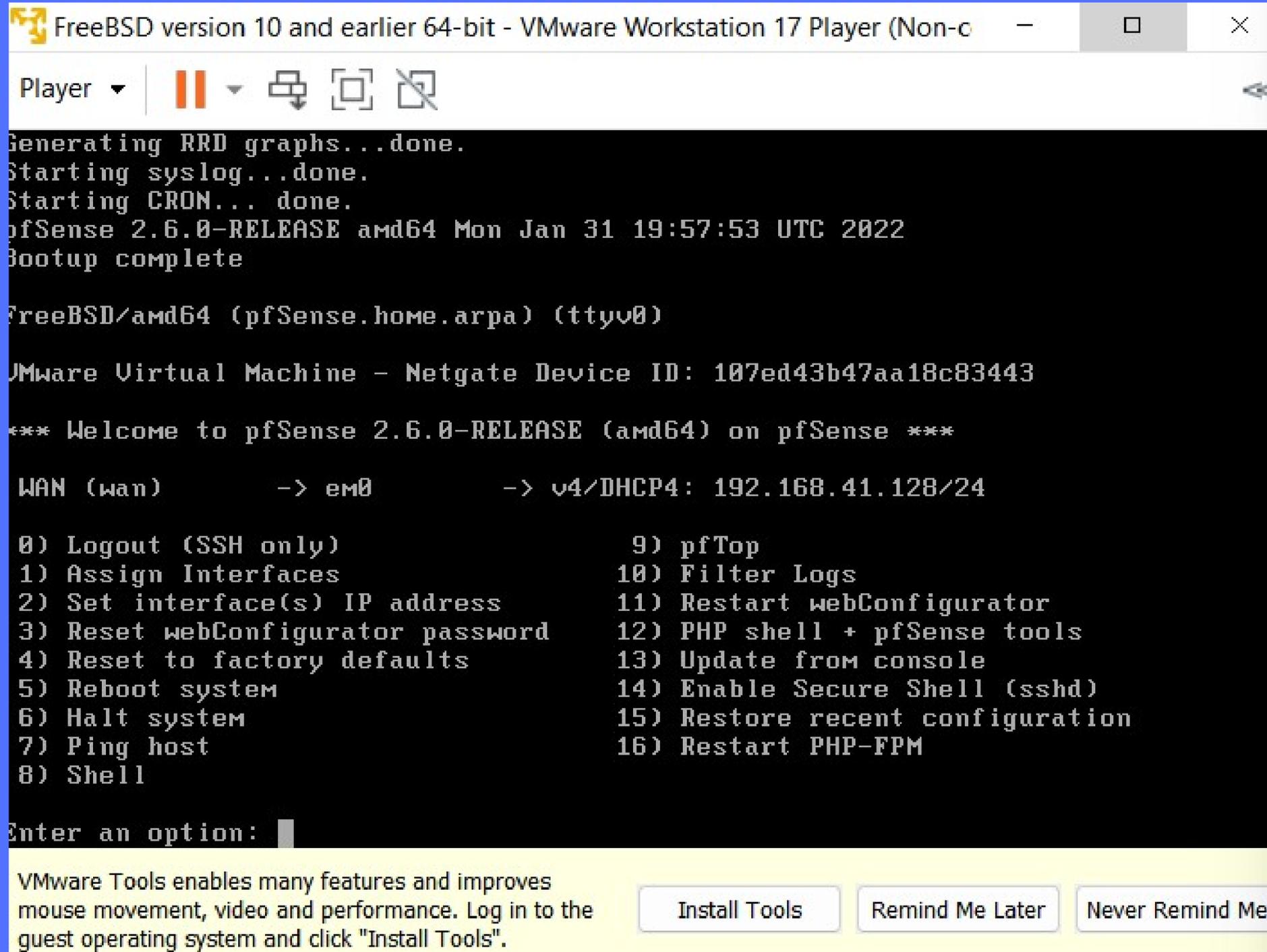
Installation de PfSense :

Installation dans une VM dédiée : L'image est installée dans une machine virtuelle (VM) dédiée, où le processus de configuration démarre automatiquement.

```
pfSense Installer

                    ┤Copyright and distribution notice├
 Copyright and Trademark Notices.

 Copyright(c) 2004-2016. Electric Sheep Fencing, LLC ("ESF").
 All Rights Reserved.

 Copyright(c) 2014-2023. Rubicon Communications, LLC d/b/a Netgate
 ("Netgate").
 All Rights Reserved.

 All logos, text, and content of ESF and/or Netgate, including underlying
 HTML code, designs, and graphics used and/or depicted herein are
 protected under United States and international copyright and trademark
 laws and treaties, and may not be used or reproduced without the prior
 express written permission of ESF and/or Netgate.

 "pfSense" is a registered trademark of ESF, exclusively licensed to
 Netgate, and may not be used without the prior express written
 permission of ESF and/or Netgate. All other trademarks shown herein are
                                                                   26%
                         [Accept]
```

Installation de PfSense :

Pendant l'installation, les interfaces réseau sont configurées, avec une identification du WAN (Wide Area Network) et du LAN (Local Area Network).
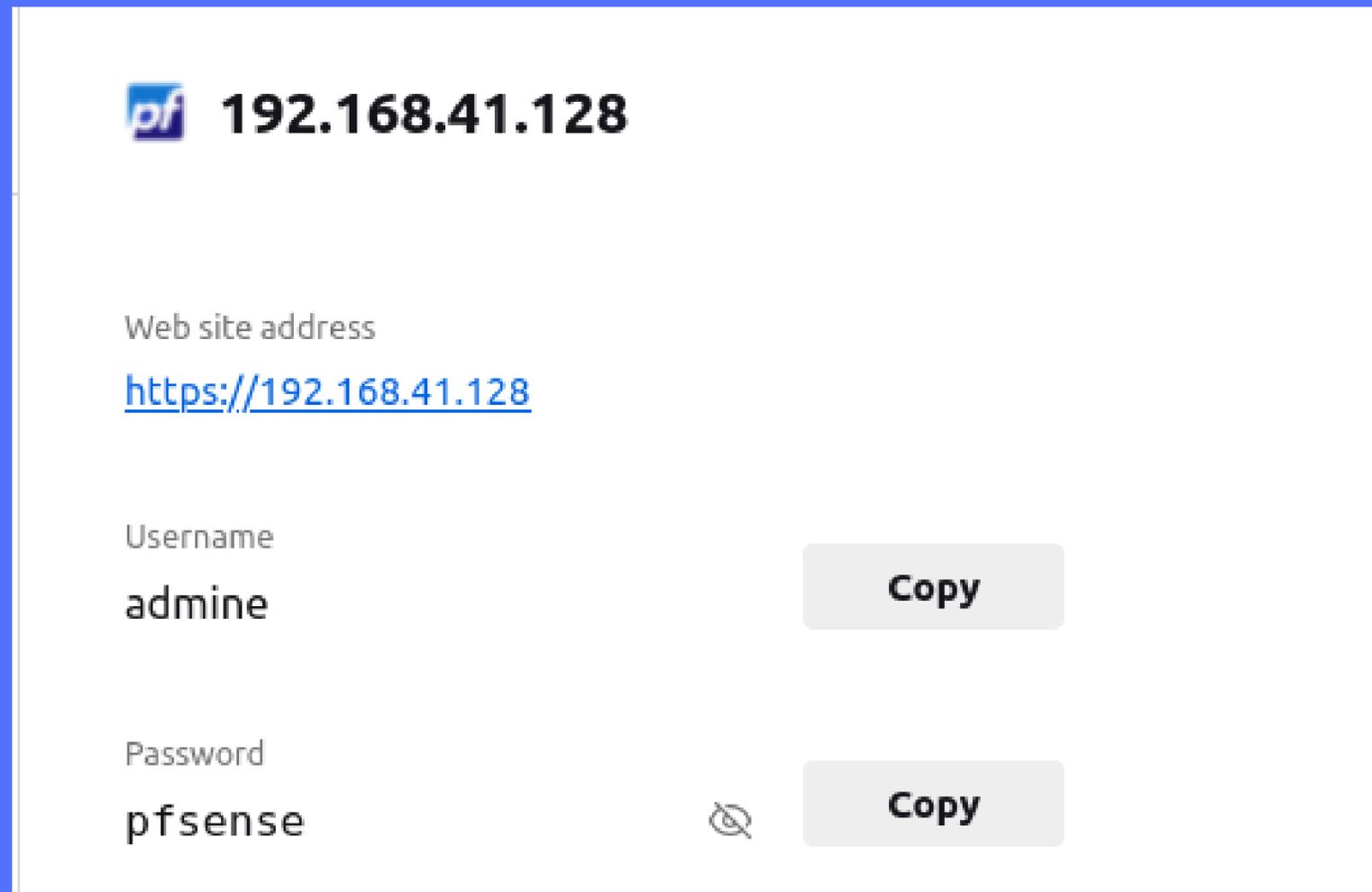
Configuration de pfsense :
Configuration des informations générales : L'utilisateur peut modifier le nom
du pare-feu, déclarer un nom de domaine et sélectionner le fuseau horaire.
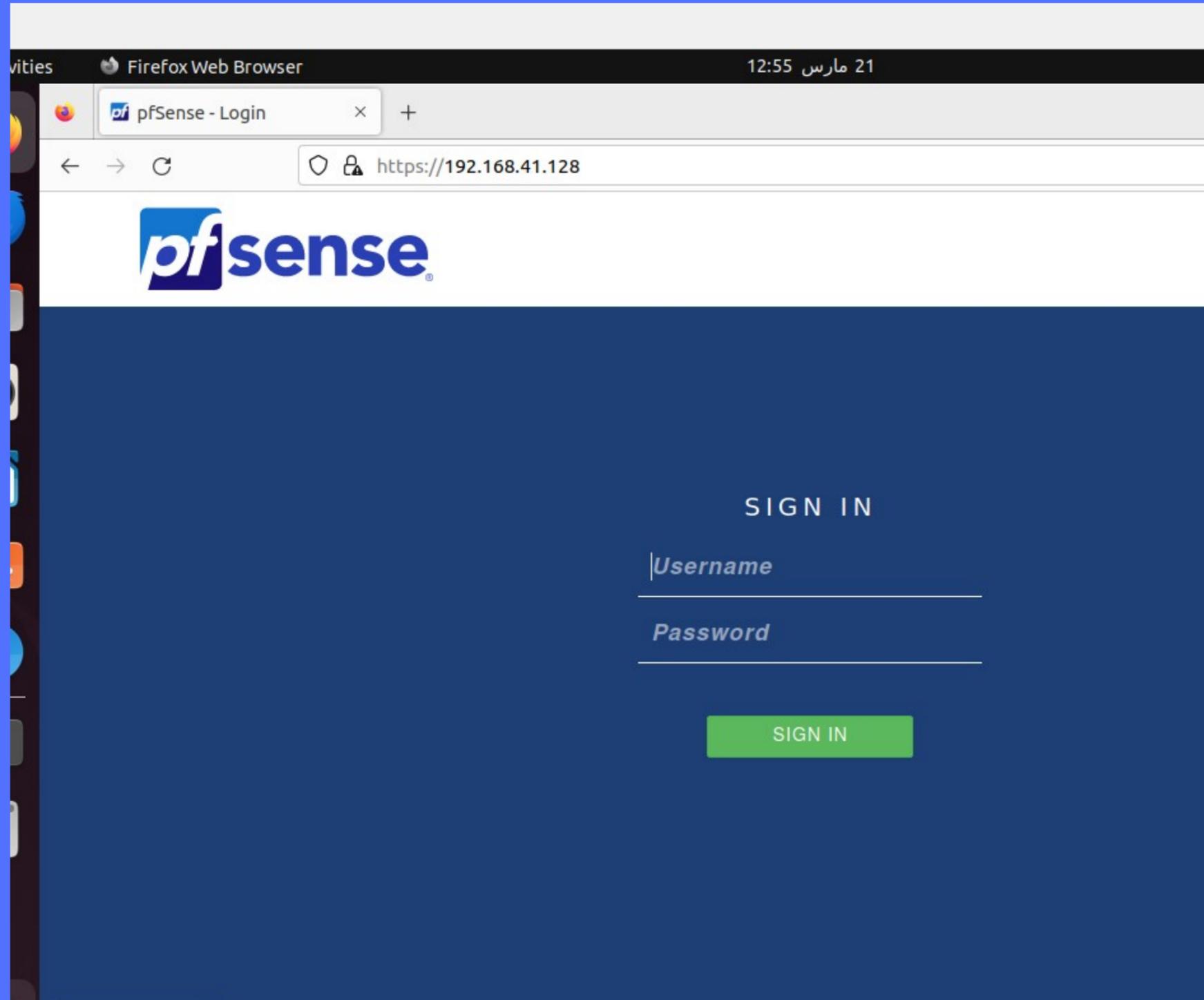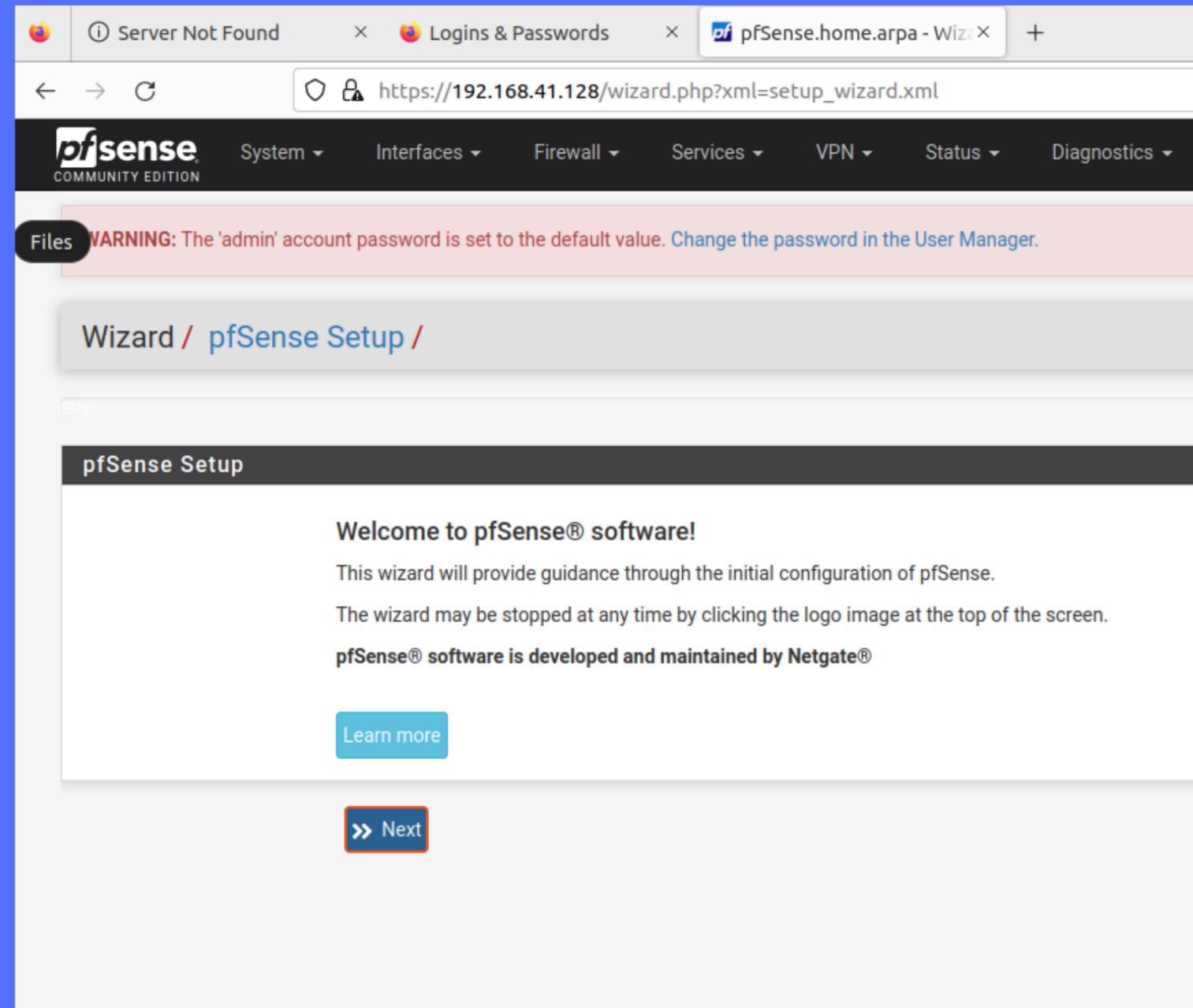
Assistant de configuration :
À travers l'interface utilisateur Web, l'assistant de configuration guide l'utilisateur pour finaliser l'installation du pare-feu.

192.168.41.128

Web site address

https://192.168.41.128

Username

admine | **Copy**

Password

pfsense | **Copy**

Assistant de configuration :

L'interface WAN est généralement configurée automatiquement par DHCP, mais peut être configurée manuellement si nécessaire.

VMware Workstation 17 Player ✕

Error while powering on: The process cannot access the file because another process has locked a portion of the file

Cannot open the disk 'C:\Users\USUARIO \Documents\Virtual Machines\FreeBSD version 10 and earlier 64-bit\FreeBSD version 10 and earlier 64-bit.vmdk' or one of the snapshot disks it depends on.

Module 'Disk' power on failed.

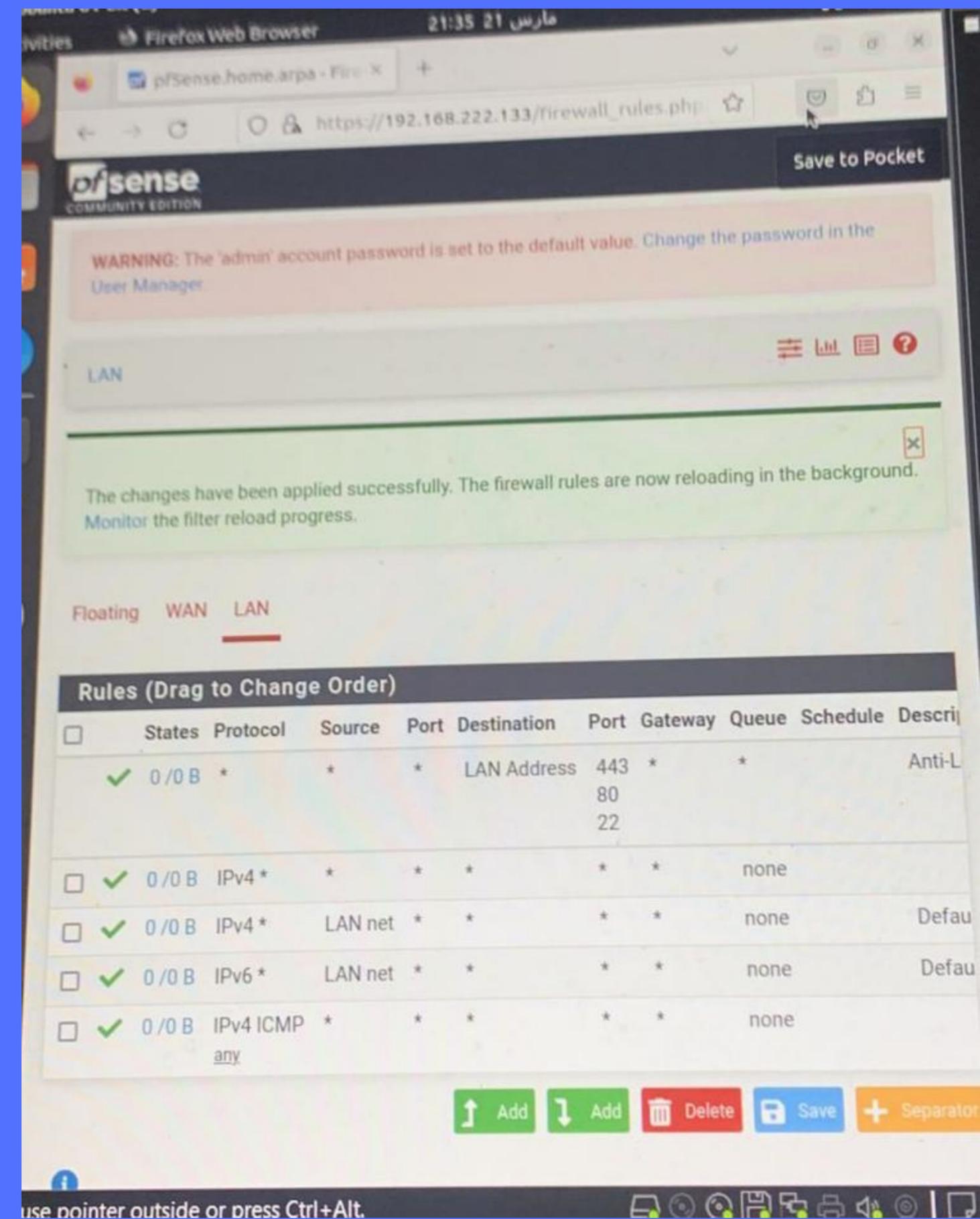Failed to start the virtual machine.

OK

Configuration de l'interface WAN :

 L'utilisateur peut modifier l'adresse IP de l'interface LAN et changer les identifiants par défaut du compte admin de PfSense.

Configuration des règles :

L'utilisateur peut définir des règles en fonction de divers critères tels que l'interface, le protocole, l'adresse source et de destination.

Configuration de l'interface LAN :

L'utilisateur peut modifier l'adresse IP de l'interface LAN et changer les identifiants par défaut du compte admin de PfSense.

Configuration de l'interface LAN :
L'utilisateur peut modifier l'adresse IP de l'interface LAN et changer les identifiants par défaut du compte admin de PfSense.

Configuration de l'interface LAN :

L'utilisateur peut modifier l'adresse IP de l'interface LAN et changer les identifiants par défaut du compte admin de PfSense.

Configuration de l'interface LAN :
L'utilisateur peut modifier l'adresse IP de l'interface LAN et changer les identifiants par défaut du compte admin de PfSense.

Configuration de l'interface LAN :
L'utilisateur peut modifier l'adresse IP de l'interface LAN et changer les identifiants par défaut du compte admin de PfSense.

Règles LAN -> WAN :

Par défaut, toutes les connexions sont autorisées, mais l'utilisateur peut ajouter des règles pour contrôler le trafic. Les règles définissent des actions telles que Pass (autoriser), Block (bloquer) ou Reject (rejeter).
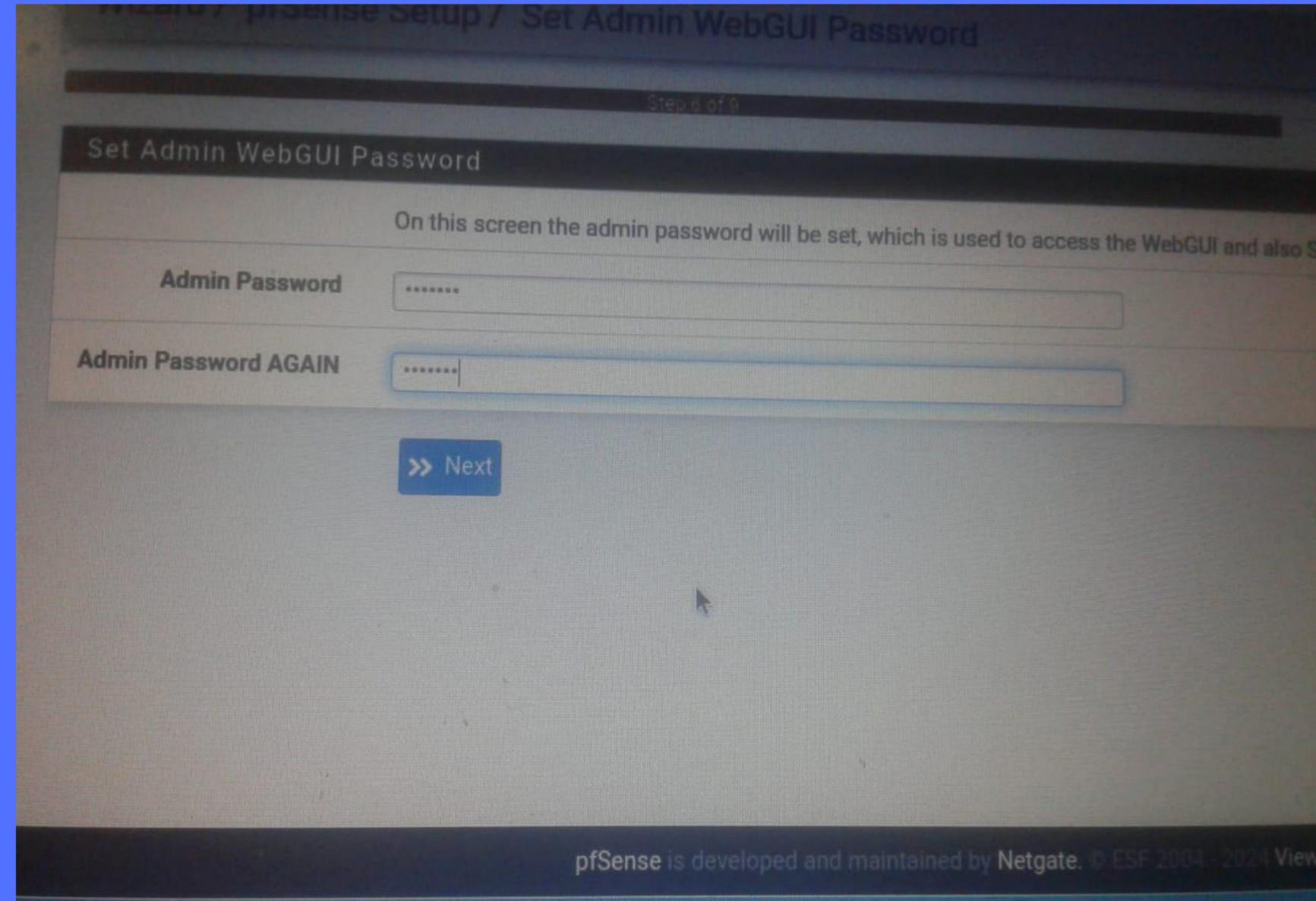
Name	chater.coulibaly.arpa
User	admin@192.168.41.130 (Local Database)
System	VMware Virtual Machine Netgate Device ID: **107ed43b47aa18c83443**
BIOS	Vendor: **Phoenix Technologies LTD** Version: **6.00** Release Date: **Thu Nov 12 2020**
Version	**2.6.0-RELEASE** (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE *Unable to check for updates*
CPU Type	11th Gen Intel(R) Core(TM) i7-1195G7 @ 2.90GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Disabled
MDS Mitigation	Inactive

🖧 WAN

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 return
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

WAN

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

TCP

Choose which IP protocol this rule should match.

Source ☐ Invert match   any   Source Address

🔧 Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this
its default value, any.

Destination   ☐ Invert match   any

Protocol   TCP

Choose which IP protocol this rule should match.

Source

| Source | ☐ Invert match | Network ⌄ | Source Address |

⚙ Hide Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases its default value, **any**.

| Source Port Range | FTP (21) ⌄ | | FTP (21) ⌄ | |
| | From | Custom | To | Custom |

Specify the source port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Destination

| Destination | ☐ Invert match | Network ⌄ | Destination Address |

| Destination Port Range | FTP (21) ⌄ | | FTP (21) ⌄ | |
| | From | Custom | To | Custom |

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

| Log | ☐ Log packets that are handled by this rule |

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider usi the Status: System Logs: Settings page).

Description

Conclusion :

La mise en œuvre d'un pare-feu PfSense offre une solution complète et conviviale pour sécuriser et gérer les réseaux. À travers des étapes d'installation et de configuration bien définies, les utilisateurs peuvent bénéficier de fonctionnalités avancées tout en maintenant un niveau élevé de sécurité.