

PROJET INFRASTRUCTURE ET SYSTÈME **D'INFORMATION**

Antoine PIZZETTA
Pierre ROY
Margot TOMATIS

B1 INFORMATIQUE
02/05/2022

Sommaire

I.	INTRODUCTION	3
	1.1 <i>Objet du document</i>	3
	1.2 <i>Domaine d'application</i>	3
	1.3 <i>Acteurs du projet</i>	3
II.	CADRE DU PROJET	4
	2.1 <i>Présentation du projet</i>	4
	2.2 <i>Contexte du projet</i>	4
	2.3 <i>Enoncé du besoin</i>	4
	2.4 <i>Contraintes du projet</i>	4
	2.5 <i>Objectifs et enjeux</i>	4
	2.6 <i>Livrables</i>	5
III.	MACHINES	6
	3.1 <i>Création</i>	6
	3.2 <i>Configuration du réseau</i>	6
IV.	PFSENSE	7
	4.1 <i>Installation</i>	7
	4.2 <i>Configuration</i>	7
	4.3 <i>Configuration du réseau</i>	7
V.	BACKUP	9
	5.1 <i>Installation de RSync</i>	9
	5.2 <i>Configuration de la VM backup</i>	9
	5.3 <i>Configuration de la VM serveur</i>	9
	5.4 <i>Automatisation</i>	10
VI.	NGINX	11
	6.1 <i>Installation</i>	11
	6.2 <i>Configuration</i>	11
VII.	DÉPLOIEMENT	12
	7.1 <i>Configuration des machines</i>	12
	7.2 <i>Règle de PFSense</i>	12
VIII.	ORGANISATION	13

CONCLUSION	14
GLOSSAIRE	15
ANNEXE	17

1 INTRODUCTION

1.1 *Objet du document*

Ce document représente le compte rendu du projet infrastructure et système d'information : c'est à dire, un document qui fait état d'un rapport, exposé, et relation de certains faits particuliers.

1.2 *Domaine d'application*

Le compte rendu est un document que l'on utilise dans le cadre du développement d'un projet. Sa rédaction suit en général des normes assez fixes. Il sert à définir la finalité d'un projet, les étapes pour sa réalisation et les éléments nécessaires pour le mener à bien.

1.3 *Acteurs du projet*

Les chefs de projets PIZZETTA Antoine, ROY Pierre & TOMATIS Margot se chargent du déploiement du réseau local afin de laisser communiquer une entreprise. Cela facilitera l'utilisation du réseau pour les utilisateurs dans l'entreprise.

2 CADRE DU PROJET

2.1 Présentation du projet

Déploiement d'un système d'informations et d'un réseau pour une petite entreprise pour l'aider à communiquer et envoyer des données plus facilement. Cette structure permettra aux personnels un système pratique et le site aidera à se documenter sur la nouvelle infrastructure plus rapidement.

L'infrastructure sera composée d'un parefeu PFSense, deux clients (Windows et Linux), un serveur web Linux, un serveur de backup Linux.

L'accès au serveur linux de sauvegarde peut se faire seulement via le réseau interne de la société (soit les deux clients et le serveur web).

L'accès au site web peut se faire du réseau internet ou externe.

2.2 Contexte du projet

Le projet a été entrepris dans un cadre universitaire dont le sujet était de créer un réseau local d'une entreprise et mettre en ligne un site web en utilisant divers langages et outils de notre choix (VMWare, PFSense, NginX, HTML, CSS) Durant la phase de recherche, l'idée de créer un site regroupant les informations nécessaires à la création et l'organisation du projet nous paraissait important. Les utilisateurs pourront donc se documenter plus facilement.

2.3 Enoncé du besoin

Les visiteurs susceptibles de se rendre sur le site seront sûrement ceux cherchant une documentation approfondie du réseau local de l'entreprise. Celui-ci ayant été créé dans un cadre universitaire.

2.4 Contraintes du projet

Le projet se devait de respecter quelques points primordiaux. Tout d'abord les informations nécessaires à la création entière du réseau devaient se trouver sur le site. Ces informations devront être concises et précises pour ne pas déstabiliser l'utilisateur.

De plus, en tant que projet dans un cadre universitaire, la durée définie pour livrer le projet est limitée. Nous devons donc avoir un rythme de travail régulier et autonome, ainsi qu'un programme précis.

2.5 Objectifs et enjeux

Aider les utilisateurs à comprendre le réseau établi et permettre à l'entreprise de pouvoir avoir un réseau sécurisé et efficace pour répondre à leurs besoins.

Accorder des renseignements clairs et rapides aux utilisateurs, rendre le site le plus compréhensible possible était une nécessité dont nous ne pouvions nous passer. Chacun de nos utilisateurs doit pouvoir y trouver ce qui l'intéresse.

Les objectifs principaux que nous cherchons à répondre sont avant tout : un système d'informations fonctionnel, une infrastructure efficace et un site web accessible à tous.

2.6 Livrables

Le projet doit être terminé pour le 2 mai 2022 à 23h59 maximum. Il y aura également une version orale de la présentation du projet le 4 mai 2022.

3 MACHINES

3.1 Création

La création des machines virtuelles suit plusieurs étapes relativement simples. Pour commencer, nous allons initialiser notre première machine grâce au logiciel [VMware Workstation](#). Pour ce faire, effectuer clic droit et naviguer sur “New Virtual Machine...” ([cf annexe 1](#)).

Ensuite, sélectionner le type de configuration recommandé ([cf annexe 2](#)).

La machine a besoin d'un iso, trouvable sur internet, il est préférable de l'importer directement ([cf annexe 3](#)).

Pour que l'utilisateur s'y retrouve parmi toutes les machines virtuelles, on peut attribuer un nom à celles-ci ([cf annexe 4](#)).

Nous pouvons ensuite nommer la machine ([cf annexe 6](#)).

Ensuite, il faut attribuer la taille du disque que l'on souhaite ([cf annexe 7](#)).

Désormais, nous accédons au paramètres ([cf annexe 8](#)) pour y modifier la RAM ([cf annexe 9](#)) puis changer les paramètres réseaux en **Host-Only** ([cf annexe 13](#)).

3.2 Configuration du réseau

Créer un réseau local (LAN, Local Area Network) est nécessaire pour permettre à l'entreprise de communiquer en interne et se partager des données, mais aussi d'avoir une connexion avec le WAN (Wide Area Network) pour donner l'accès au site par d'autres utilisateurs.

Des plans ont donc été imaginés afin de structurer ce réseau ([cf annexe 11](#)).

Dans notre situation, l'entreprise ne possède que deux clients, deux serveurs et un pare-feu (soit 5 connexions différentes). L'utilisation d'un masque de sous-réseau /29 nous paraissait donc le plus efficace pour répondre à ses besoins (rend possible 6 connexions). Il faudra cependant prendre en compte le fait que le nombre de connexions d'une vraie entreprise pourra augmenter dans le temps en optant pour un autre CIDR (mais cela ne reste que théorique dans notre cas) ([cf annexe 12](#)).

Il est important de changer le réseau des VMs, dans les paramètres de ces dernières, en **Host-Only** (et non **NAT**) afin de réaliser un réseau local entre les VMs, soit une représentation du réseau interne de l'entreprise ([cf annexe 13](#)).

Enfin, il faut changer les IPs des VMs à ceux correspondant au plan prévus. Les modifications en linux et windows peuvent se faire manuellement depuis les paramètres ([cf annexe 14](#) et [15](#)). Les informations ont donc normalement été modifiées ([cf annexe 16](#) et [17](#)).

Pour vérifier si le réseau fonctionne correctement, il est utile de tester les pings entre les VMs. Cependant pour permettre le ping sur Windows il faut activer la règle Partage de fichiers et imprimantes Demande d'échos Trafic entrant ICMPv4 ([cf annexe 18](#)).

4 PFSense

4.1 Installation

PFSense est un outil de surveillance de la sécurité du réseau. Il permet de surveiller les connexions et les déconnexions des utilisateurs.

Le principe d'installation de la VM PFSense est le même que pour les autres VMs. Il faut simplement choisir un ISO différent, soit celui correspondant à PFSense ([cf annexe 19](#)).

Il faut donc ensuite choisir le nom de la VM ainsi que son emplacement sur le PC host ([cf annexe 20](#)) et choisir sa taille, ici 20go par défaut ([cf annexe 21](#)).

4.2 Configuration

Une fois installé, il faut le configurer.

Il faut accepter le copyright pour faire apparaître un menu d'installation ([cf annexe 22 et 23](#)). PFSense demande ensuite de choisir un clavier et un groupe de raccourcis à utiliser, nous utilisons celui de base ([cf annexe 24](#)). Il faut donc configurer les partitions du disque dur ([cf annexe 25](#)) et les valider ([cf annexe 26](#)). Il demande enfin de choisir un type d'utilisation de disque dur à plusieurs partitions, nous utilisons le type de disque dur par défaut ([cf annexe 27](#)) et la valider ([cf annexe 28](#)).

La machine demande de formater les partitions, il faut appuyer sur * pour les sélectionner toutes ([cf annexe 29](#)). PFSense s'installe finalement après le formatage des partitions ([cf annexe 30](#)). Il est donc finalement configuré et avertis qu'il va redémarrer ([cf annexe 32](#)). Le projet n'ayant pas besoin de configuration en plus le terminal de PFSense se lance ([cf annexe 33](#)).

4.3 Configuration du réseau

Une fois configuré, PFSense nous renvoie une IP em0. En mettant celle-ci dans le navigateur, nous arrivons sur la page de configuration du réseau de PFSense ([cf annexe 34](#)).

Le pare feu va bloquer le rafraîchissement de notre page donc taper la commande **pfctl -d** dans le terminal du PFSense ([cf annexe 35](#)). Cela va désactiver le pare feu pour nous permettre d'affecter nos changements.

Pour instaurer une nouvelle règle pour le pare feu, il faut aller sur le navigateur de PFSense.

Aller dans la catégorie **rules** puis appuyer sur **add** ([cf annexe 36](#)). Rentrer les paramètres souhaités, dans notre situation, nous rentrons les critères de notre port 80 (notre site étant en HTTP) ([cf annexe 37](#)).

Dans le cas où notre site serait en HTTPS, il faudrait travailler avec le port 443 ([cf annexe 38](#)).

Une fois les règles écrites, nous pouvons les retrouver dans la liste des règles sur PFSense ([cf annexe 39](#)). Il faut ensuite refaire la commande **pctfl -d** dans le terminal.

Il ne reste qu'à faire des tests de ping pour vérifier la connexion à internet et entre les VMs et le pare feu.

D'une part le serveur PFSense au client Windows ([cf annexe 40](#)) et inversement ([cf annexe 41](#)).

5 BACKUP

5.1 Installation de RSync

Pour mettre en place le système de backup (sauvegarde), nous avons utilisé RSync. Remote Synchronization à distance est un logiciel de synchronisation de fichiers. Il est fréquemment utilisé pour mettre en place des systèmes de sauvegarde distance ou des points de restauration du système (via l'interface Timeshift).

Pour ce faire il faut deux serveurs linux (ici le serveur web et le serveur backup).

Commençant par l'installation de rsync ([cf annexe 42](#)) avec la commande **sudo apt-get install rsync -y** sur les deux serveurs puis lancer et autoriser le service ([cf annexe 43](#)) avec les deux commandes **sudo systemctl start rsync** et **sudo systemctl enable rsync**.

5.2 Configuration de la VM backup

Aller dans le fichier de configuration de RSync avec **sudo nano /etc/rsync.conf** ([cf annexe 44](#)), et rentrer les paramètres pour gérer les arrivées d'information ([cf annexe 45](#)) avec :

[backup]

path=/home/backuo/backup (donne le chemin de destination des fichiers, soit le lieu de stockage dans la backup)

hosts allow = 10.0.0.1 (IP du serveur qui envoie les données. Le partage se faisant dans un réseau local, nous y mettons une IP locale)

hosts deny = * (empêcher l'envoi de fichiers venant de n'importe qui pour sécuriser)

list = true

uid = root

gid = root

read only = false (gestion des permissions users et groupes)

sudo systemctl restart rsync permet de relancer le logiciel et appliquer les changements.

5.3 Configuration de la VM serveur

Dans le dossier du serveur, qui sera sauvegardé dans la backup de notre autre système, crée un fichier rsync ([cf annexe 46](#)) avec la commande **nano rsync** qui nous permettra également d'entrer directement dans le fichier.

Ecrire la commande **rsync -avz /var/www/html/Infra-Website/ 10.0.0.2::backup** ([cf annexe 47](#)) dans ce fichier. **/var/www/html/Infra-Website/** représente le fichier depuis lequel nous voulons "extraire" des données et **10.0.0.2** l'IP vers laquelle elles seront envoyées.

Il faut ensuite donner les permissions d'exécution du user au fichier avec la commande **chmod u+x rsync** ([cf annexe 48](#))

5.4 Automatisation

Automatiser le système de sauvegarde est nécessaire pour avoir un système fiable à l'entreprise. Pour ce faire, nous avons donc choisis d'utiliser l'outil planificateur de tâches régulières dans linux, le Cron, qui est très pratique pour un serveur pour y lancer des scripts de sauvegardes.

La commande **crontab -e** permet d'y accéder ([cf annexe 49](#)).

Il faut donc ensuite écrire la tâche à exécuter.

Dans un premier cas, il a été planifié toutes les minutes afin de vérifier le fonctionnement ([cf annexe 50](#)) avec la commande `* * * * * /var/www/html/Infra-Website/rsync` (* * * * * indique toutes les minutes et `/var/.../rsync` le fichier à exécuter).

Nous pouvons ainsi vérifier que le fichier (**test**) a bien été envoyé dans le backup ([cf annexe 51](#) et [52](#)) mais aussi que le cron c'est bien exécuté via le syslog ([cf annexe 53](#)).

Le délai est ensuite remis à 24 heures, en indiquant au planificateur d'exécuter la tâche chaque jour à minuit ([cf annexe 54](#)).

Ayant pu constater le fonctionnement de la sauvegarde dans le cas d'ajout de fichier dans le dossier du serveur web, un nouveau test a été exécuté en modifiant cette fois-ci le contenu du fichier **test** depuis le système du serveur web ([cf annexe 55](#)).

6 NGINX

6.1 Installation

Pour installer Nginx, il faut simplement exécuter la commande “**sudo apt-get install nginx**” ([cf annexe 56](#)). Une fois ceci fait, le serveur sera en place et disponible en réseau local (nous pouvons le vérifier avec la commande “**service nginx status**” ([cf annexe 57](#))).

6.2 Configuration

Le site est accessible via l’URL “**localhost**” ou grâce à l’IP locale de la machine sur laquelle le serveur est hébergé (dans notre cas *10.0.0.1*).

Lorsqu’on se rend sur la page, le contenu sera donc la page HTML par défaut proposée par Nginx ([cf annexe 63](#)).

Si l’on veut modifier la page par défaut, il suffit de naviguer dans le dossier où se situe la page ([cf annexe 58](#)), le fichier par défaut se nomme `index.nginx-debian.html` ([cf annexe 59](#)).

Dans notre cas, nous ne toucherons pas à ce fichier mais modifierons la page HTML que prendra Nginx par défaut. Pour ce faire, il faut se rendre dans le dossier de configuration de Nginx nommé “**sites-enabled**” ([cf annexe 60](#)), puis l’éditer ([cf annexe 61](#)) en y plaçant le chemin d’accès que l’on souhaite ([cf annexe 62](#)).

7 DÉPLOIEMENT

7.1 Configuration des machines

Il est possible d'accéder au site depuis un autre ordinateur sous de précises conditions. Il faut tout d'abord changer le réseau externe de la VM PFSense en **bridged** (laissant le réseau interne en **Host-Only**) ([cf annexe 70](#)).

Le pare-feu de Ynov étant limité, il faut mettre le PC host en partage de connexion depuis un téléphone. Cela aura cependant comme conséquence de changer l'IP WAN du pare-feu ([cf annexe 71](#)).

7.2 Règle de PFSense

Il faut donc créer une règle qui autorise les autres ordinateurs du réseau à se connecter par bridge au port du site ([cf annexe 72](#)). Nous pouvons ensuite constater que le site peut être accéder par un autre PC ([cf annexe 73](#)).

8 ORGANISATION DU PROJET

Tout d'abord, nous avons pris quelques heures pour réaliser un brainstorming des idées primaires, nous permettant d'émettre des plans qui nous orienteront plus précisément.

Grâce à ces idées, de nombreux schémas du réseau ont été réalisés en mélangeant toutes les idées reçues jusqu'à en perfectionner un que nous trouvions plus pratique, plus simple et plus adapté au besoin de l'entreprise.

Nos idées étaient claires, nous avons commencé à suivre nos croquis pour avoir une base concrète sur laquelle travailler. De ce fait, les créations des VMs ont été commencées et le réseau local a été implémenté.

Nous avons ensuite pu entreprendre la réalisation de la backup, puis de la mise en ligne du serveur web.

Une fois la globalité du système créée, nous avons pu reprendre la documentation ainsi que l'amélioration du site web.

Nous avons finalement terminé par la réalisation des supports pour la présentation orale.

CONCLUSION

Ainsi l'infrastructure et le système d'informations sont adaptés au besoin de l'entreprise. Le site web détaille l'implémentation de toutes les fonctionnalités et peut être accessible sur d'autres PC, ce qui reste idéal pour comprendre plus efficacement le réseau mis en place.

Les solutions pour l'entreprise ont donc été exposées et pourront être adaptées en fonction des nouveaux besoins de celle-ci.

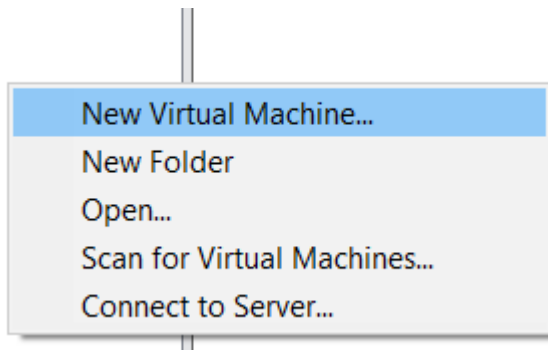
GLOSSAIRE

- Infrastructure : Ensemble d'installations, d'équipements nécessaires à une collectivité.
- Système d'informations : Ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information, en général grâce à un réseau d'ordinateurs.
- Pare feu : Dispositif qui protège un système informatique connecté à Internet des tentatives d'intrusion qui pourraient en provenir.
- PFSense : système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD.
- FreeBSD : Système d'exploitation UNIX libre.
- NginX : Serveur web open-source qui, depuis son succès initial en tant que serveur web, est maintenant aussi utilisé comme reverse proxy, cache HTTP, et load balancer.
- Reverse proxy : Type de serveur, habituellement placé en frontal de serveurs web.
- Clients : Logiciel capable d'envoyer des requêtes HTTP à un serveur web et d'afficher les résultats. Les navigateurs web sont les clients web les plus répandus.
- Serveur Web : Logiciel capable de répondre à des requêtes HTTP, c'est à dire de renvoyer des données (par exemple une page HTML), en réponse à des demandes écrites en HTTP (par exemple une requête GET).
- Windows : Système d'exploitation conçu pour les micro-ordinateurs de la famille PC.
- Linux : Système d'exploitation Open Source.
- Système d'exploitation : Ensemble de programmes permettant de faire fonctionner et contrôler un appareil informatique.
- Backup : Sauvegardes qui vont permettre de capturer et de synchroniser un » point-in-time snapshot « , qu'il sera possible de restaurer en cas de problème pour récupérer les données perdues.
- IP : Numéro unique attribué de manière provisoire ou durable à un ordinateur connecté à un réseau informatique qui utilise l'internet protocole.
- DNS : Les serveurs DNS traduisent des demandes de noms en adresses IP, en contrôlant à quel serveur un utilisateur final va se connecter quand il tapera un nom de domaine dans son navigateur.
- Switch : Boîtier doté de quatre à plusieurs centaines de ports Ethernet, et qui sert à relier en réseau différents éléments du système informatique.
- Routeurs : Équipement matériel informatique dont la fonction principale consiste à orienter les données à travers un réseau.
- Disques : Matériel informatique utilisé pour stocker du contenu et des données numériques sur les ordinateurs.

- HTML : HyperText Markup Language, désigne un type de langage informatique descriptif. Il s'agit plus précisément d'un format de données utilisé dans l'univers d'Internet pour la mise en forme des pages Web.
- CSS : Règles de styles destinées à des éléments ou des groupes d'éléments particuliers dans la page.
- Machine Virtuelle : Environnement entièrement virtualisé qui fonctionne sur une machine physique. Elle exécute son propre système d'exploitation (OS) et bénéficie des mêmes équipements qu'une machine physique.
- VMWare : Plate-forme de virtualisation leader pour la création d'infrastructures de Cloud Computing.
- ISO : International Organization for Standardization, est un fichier "image" d'un disque optique (CD, DVD, blu-ray, etc.). Il reprend l'ensemble des secteurs de données présents sur le disque, son contenu est strictement identique à celui présent sur le disque (dossiers, fichiers, arborescence).
- RAM : Random Access Memory, est une mémoire vive présente dans tous les ordinateurs. Elle permet de stocker provisoirement des données.
- LAN : Local Area Network, réseau informatique physique et/ou virtuel. Il permet d'interconnecter par Wi-Fi ou câbles Ethernet des terminaux entre eux.
- WAN : Wide Area Network, désigne un type de réseau de télécommunications.
- Masque de sous-réseau : Nombre qui définit une plage d'adresses IP disponible dans un réseau.
- CIDR : "*Classless Inter-Domain Routing*". Une adresse IP unique peut être utilisée pour désigner de nombreuses adresses IP uniques avec CIDR.
- Ping : Composante du protocole de connexion Internet TCP/IP. Sa mission principale consiste à vérifier les connexions établies entre un ou plusieurs hôtes distants.
- Partitions : Partie d'un disque dur destinée à accueillir un système de fichiers.
- Cron : Cron est un programme pour exécuter automatiquement des scripts, des commandes ou des logiciels à une date et une heure spécifiée précise, ou selon un cycle défini à l'avance.

ANNEXES

Annexe 1 : Création d'une machine virtuelle



Annexe 2 : Type de configuration



Annexe 3 : Installer l'iso

New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?


Install from:

☐ Installer disc:

No drives available

☒ Installer disc image file (iso):

C:\iso\ubuntu-20.04.2.0-desktop-amd64.iso Browse...

 Ubuntu 64-bit 20.04.2.0 detected.
This operating system will use Easy Install. [\(What's this?\)](#)

☐ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Help < Back Next > Cancel

Annexe 4 : Personnalisation des informations

New Virtual Machine Wizard

Easy Install Information

This is used to install Ubuntu 64-bit.

Personalize Linux

Full name: server-ubuntu

User name: server

Password: ●●●

Confirm: ●●●

Help < Back Next > Cancel

Annexe 5 : Personnalisation des informations (bis)

New Virtual Machine Wizard ✕

Easy Install Information
This is used to install Ubuntu 64-bit.

Personalize Linux

Full name:

User name:

Password:

Confirm:

Annexe 6 : Nommage de la machine

New Virtual Machine Wizard ✕

Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:

Location:

The default location can be changed at Edit > Preferences.

Annexe 7 : Allocation de la taille du disque

New Virtual Machine Wizard

×

Specify Disk Capacity
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB):

Recommended size for Ubuntu 64-bit: 20 GB

☐ Store virtual disk as a single file

☒ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.


Help


< Back


Next >

Cancel












Annexe 8 : Paramètres

 CLIENT LINUX

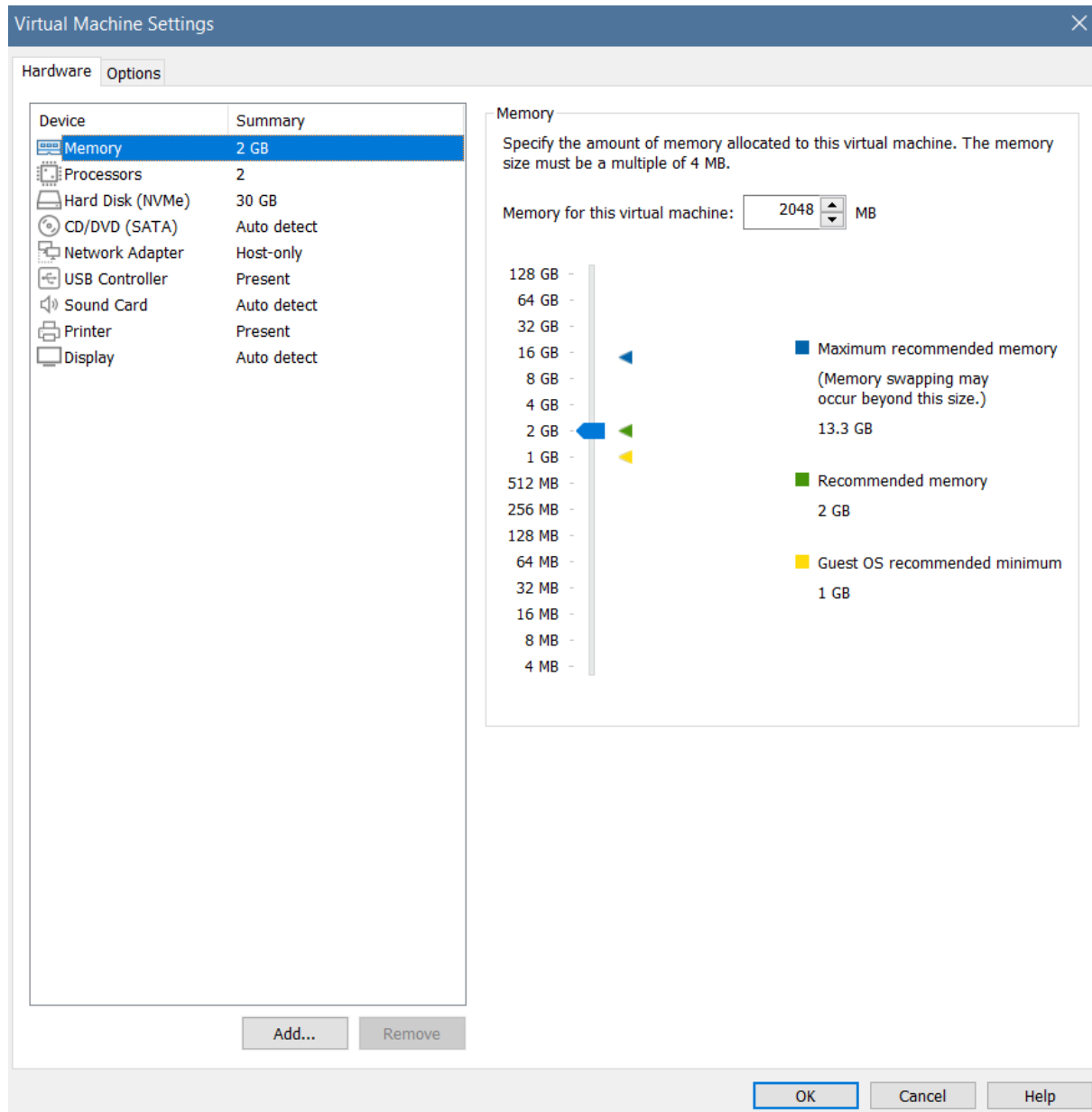
 Power on this virtual machine

 Edit virtual machine settings

▼ Devices


 Memory	2 GB
 Processors	2
 Hard Disk (SCSI)	20 GB
 CD/DVD 2 (SATA)	Using file C:\iso\...
 CD/DVD (SATA)	Using file autoin...
 Floppy	Using file autoin...
 Network Adapter	Host-only
 USB Controller	Present
 Sound Card	Auto detect
 Printer	Present
 Display	Auto detect


Annexe 9 : Attribution de la RAM














Server-ubuntu

 [Power on this virtual machine](#)


 [Edit virtual machine settings](#)


▼ Devices

 Memory	4 GB
 Processors	2
 Hard Disk (SCSI)	20 GB
 Hard Disk 2 (SCSI)	102 MB
 CD/DVD (SATA)	Using file C:\iso\...
 Network Adapter	Host-only
 USB Controller	Present
 Sound Card	Auto detect
 Printer	Present
 Display	Auto detect











PFSENSE

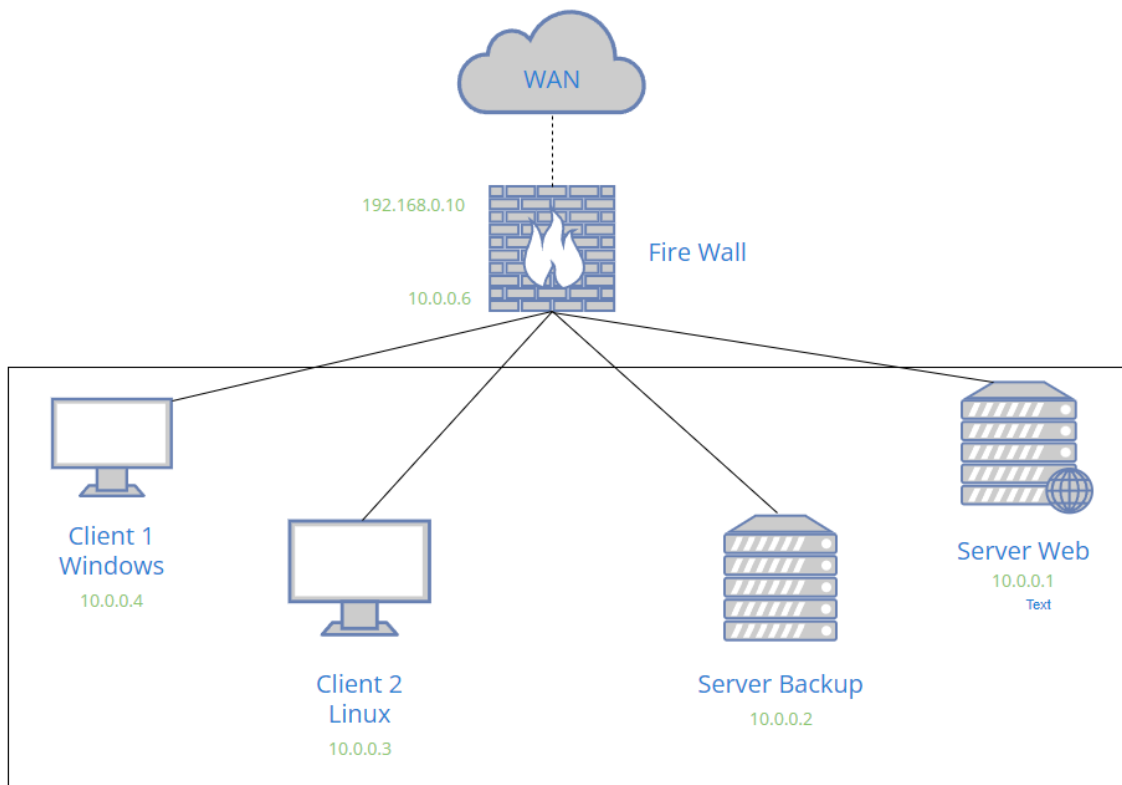
 [Power on this virtual machine](#)

 [Edit virtual machine settings](#)

▼ Devices

 Memory	256 MB
 Processors	1
 Hard Disk (SCSI)	20 GB
 CD/DVD (IDE)	Using file C:\iso\...
 Network Adapter	NAT
 Network Adapter 2	Host-only
 USB Controller	Present
 Sound Card	Auto detect
 Display	Auto detect

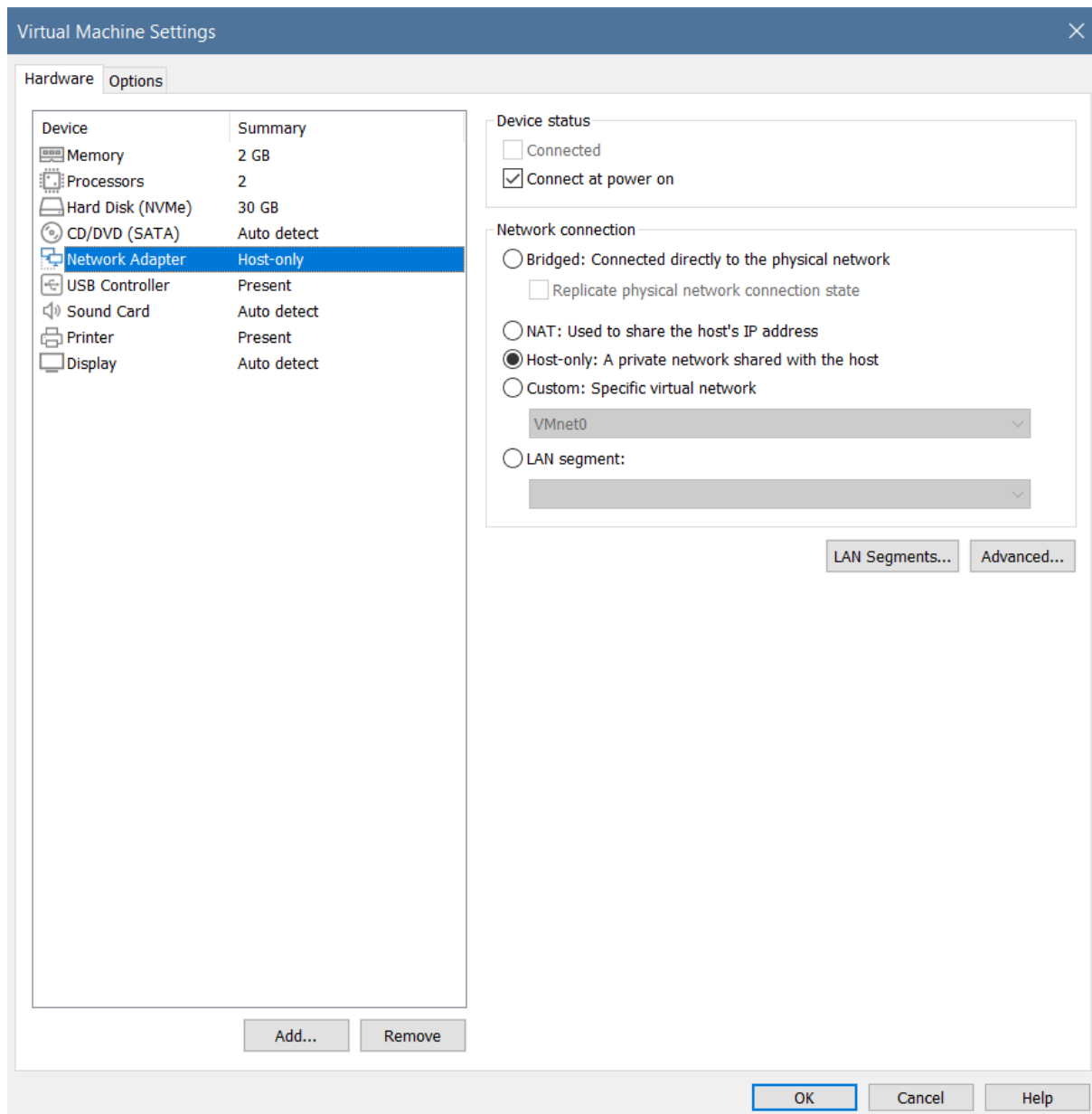
Annexe 11 : Schéma du réseau interne et externe.



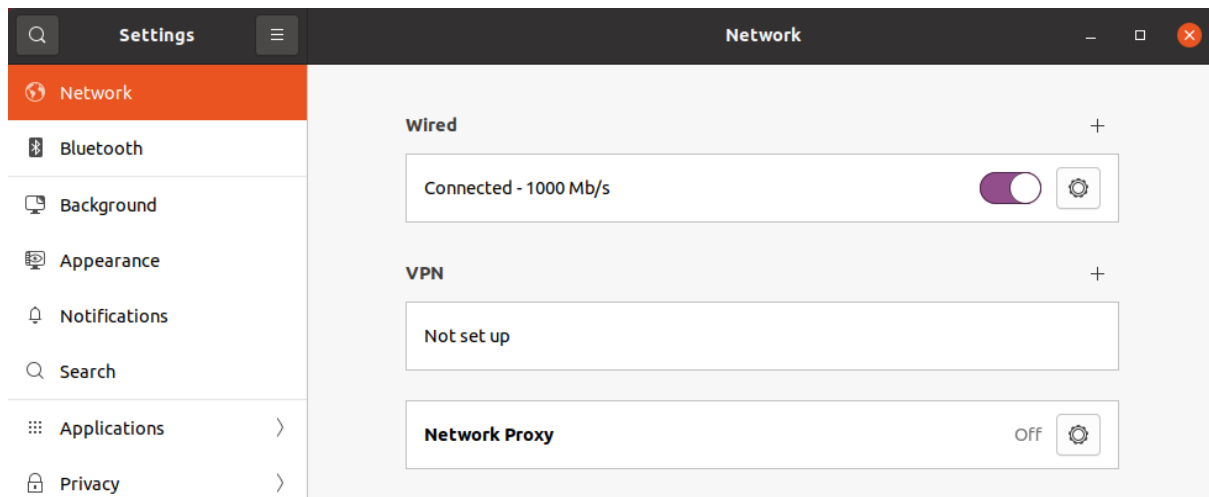
Annexe 12 : Plan d'adressage du réseau.

Nom	Adresse Ip	CIDR	Default Gateway	VLAN
Client Linux	10.0.0.3	/29	10.0.0.6	
Client Windows	10.0.0.4	/29	10.0.0.6	
Backup	10.0.0.2	/29	10.0.0.6	
Serveur Web	10.0.0.1	/29	10.0.0.6	
Pare Feu Lan	10.0.0.6	/29		
Pare Feu Wan	192.168.0.10	/29		

Annexe 13 : Paramétrage du réseau (network) dans une VMs.



Annexe 14 : Changement des IPs en Linux.



- ☒ Connect automatically
- ☐ Make available to other users
- ☐ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.

Cancel

Wired

Apply

Details

Identity

IPv4

IPv6

Security

IPv4 Method

☐ Automatic (DHCP)

☒ Manual

☐ Shared to other computers

☐ Link-Local Only

☐ Disable

Addresses

Address	Netmask	Gateway	
10.0.0.2	255.255.255.248	10.0.0.6	

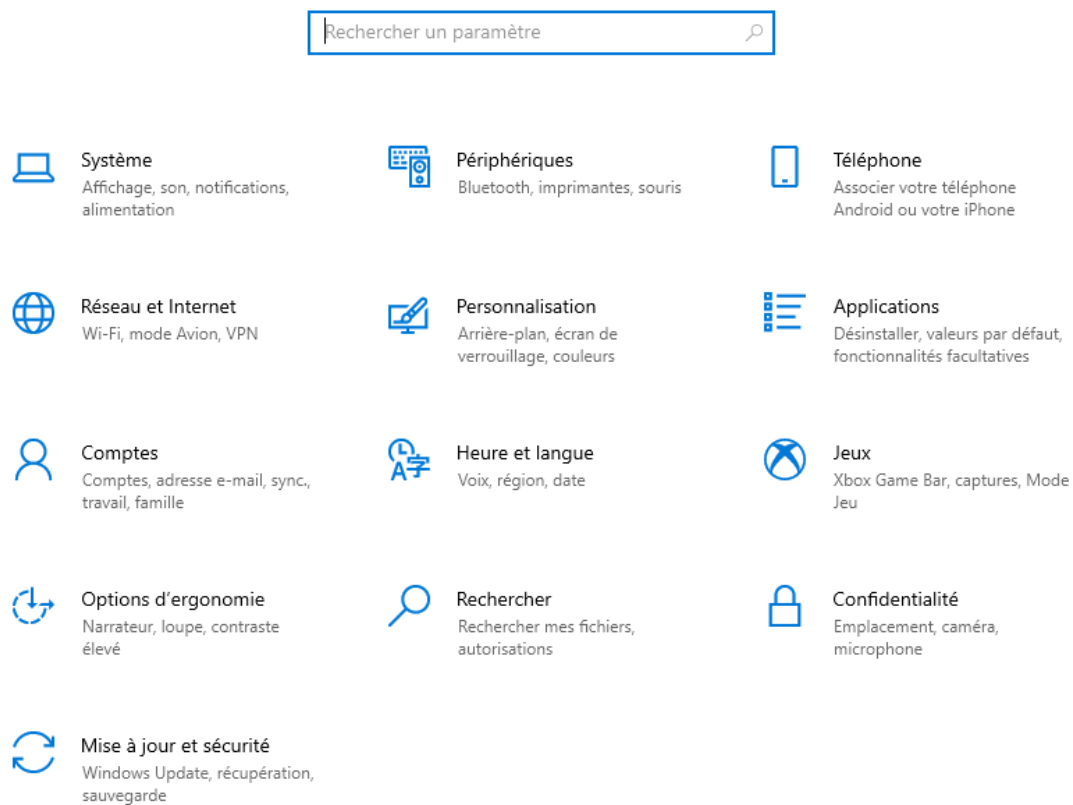
DNS

Automatic



1.1.1.1

Separate IP addresses with commas

Annexe 15 : Changement des IPs sur Windows.



Paramètres réseau avancés

-  **Modifier les options d'adaptateur**
Affichez les cartes réseau et modifiez les paramètres de connexion.
-  **Centre Réseau et partage**
Décidez des contenus que vous souhaitez partager sur les réseaux auxquels vous vous connectez.

[Afficher les propriétés du matériel et de la connexion](#)

[Pare-feu Windows](#)

[Réinitialisation du réseau](#)

Connexions réseau

← → ↕ > Panneau de configuration > Réseau et Internet > Connexions réseau

Organiser ▾

Désactiver ce périphérique réseau

Diagnostiquer cette connexion

Renommer cette connexion

Aff



Connexion réseau Bluetooth
Non connecté
Bluetooth Device (Personal Area ...



Ethernet0

Rése
Intel

Désactiver

Statut

Diagnostiquer

Connexions de pont

Créer un raccourci

Supprimer

Renommer

Propriétés

Propriétés de Ethernet0



Gestion de réseau

Connexion en utilisant :

Intel(R) 82574L Gigabit Network Connection

Configurer...

Cette connexion utilise les éléments suivants :

- ☒ Client pour les réseaux Microsoft
- ☒ Partage de fichiers et imprimantes Réseaux Microsoft
- ☒ Planificateur de paquets QoS
- ☒ Protocole Internet version 4 (TCP/IPv4)
- ☐ Protocole de multiplexage de carte réseau Microsoft
- ☒ Pilote de protocole LLDP Microsoft
- ☒ Protocole Internet version 6 (TCP/IPv6)

Installer...

Désinstaller

Propriétés

Description

Protocole TCP/IP (Transmission Control Protocol/Internet Protocol). Protocole de réseau étendu par défaut permettant la communication entre différents réseaux interconnectés.

OK

Annuler

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...

OK Annuler

Annexe 16 : IP d'une VM linux modifiée par celle prévue.

Cancel Wired Apply

Details Identity IPv4 IPv6 Security

Link speed 1000 Mb/s

IPv4 Address 10.0.0.2

IPv6 Address fe80::4ced:a344:c478:6e79

Hardware Address 00:0C:29:E6:BA:C1

Default Route 10.0.0.6

DNS 1.1.1.1

☒ Connect automatically

☐ Make available to other users

☐ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.

Remove Connection Profile

Annexe 17 : IP d'une VM windows modifiée par celle prévue.

```
C:\Users\antap>ipconfig

Configuration IP de Windows

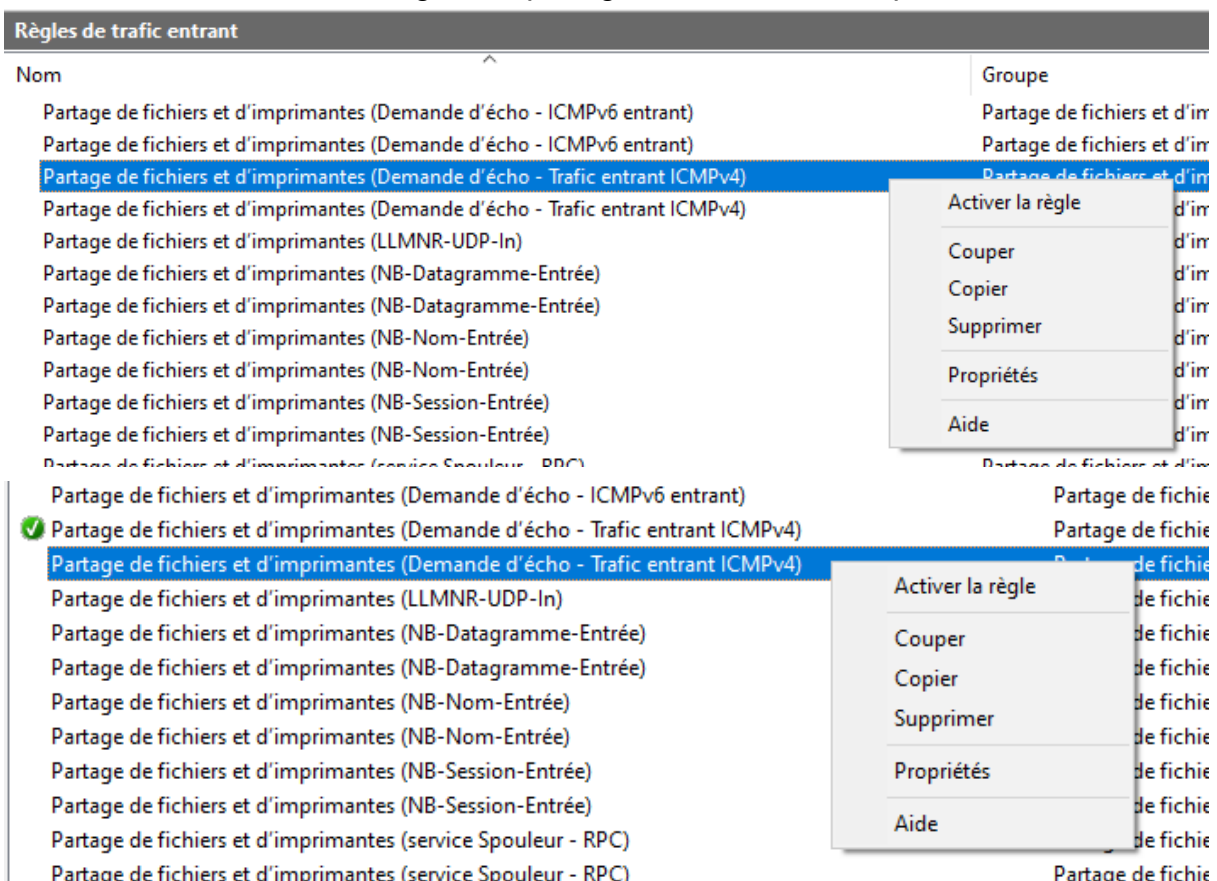
Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . : home.arpa
    Adresse IPv6 de liaison locale. . . . . : fe80::90b0:897:e4ad:d130%7
    Adresse IPv4. . . . . : 10.0.0.4
    Masque de sous-réseau. . . . . : 255.255.255.248
    Passerelle par défaut. . . . . : fe80::20c:29ff:fe55:d0a7%7
                                   10.0.0.6

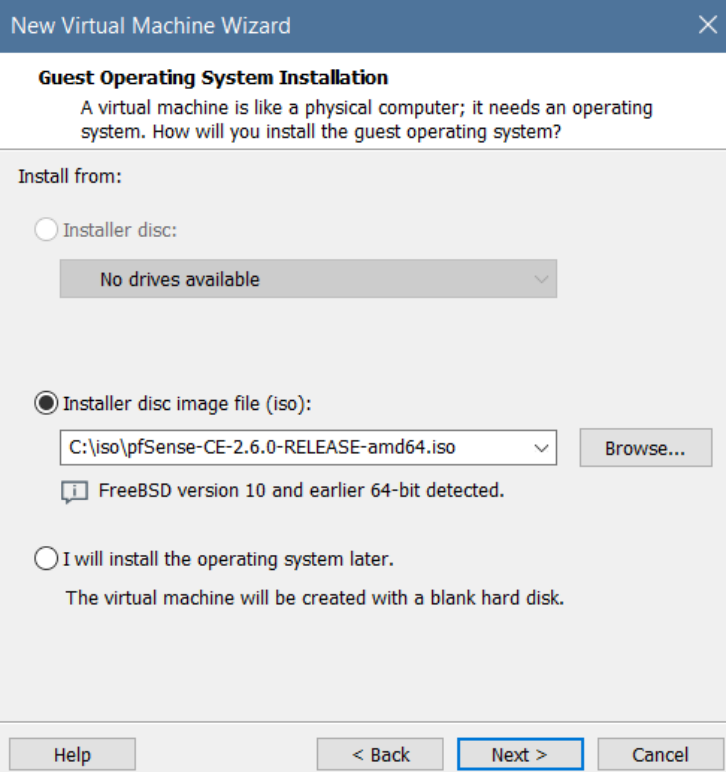
Carte Ethernet Connexion réseau Bluetooth :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :
```

Annexe 18 : Activation des règles de partage de fichiers et d'imprimantes.



Annexe 19 : Choix de l'ISO de PFSense.



New Virtual Machine Wizard

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?


Install from:

☐ Installer disc:

No drives available

☒ Installer disc image file (iso):

C:\iso\pfSense-CE-2.6.0-RELEASE-amd64.iso Browse...

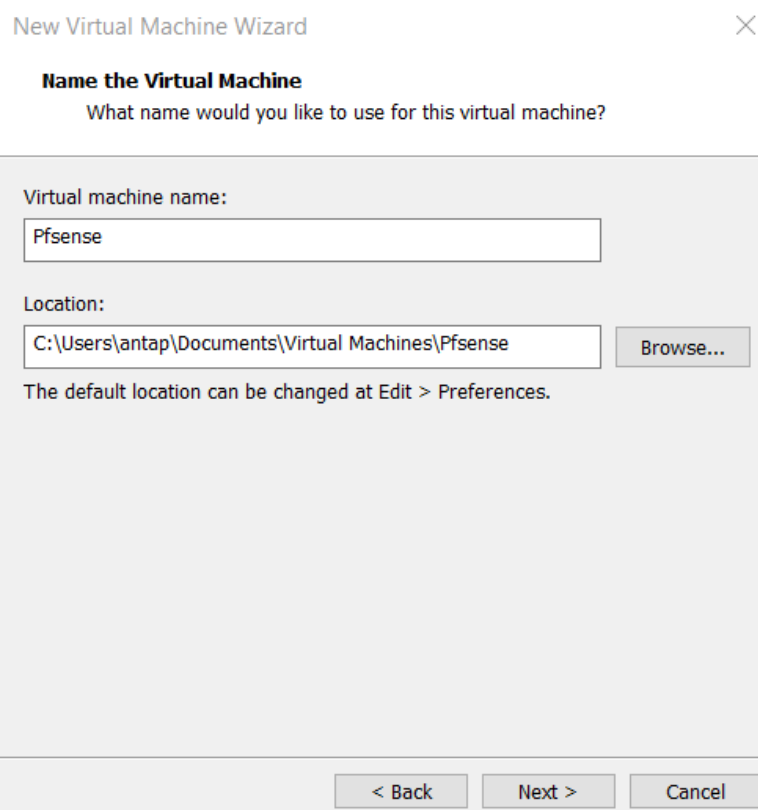
 FreeBSD version 10 and earlier 64-bit detected.

☐ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Help < Back Next > Cancel

Annexe 20 : Choix du nom et de l'emplacement de la VM PFSense.



New Virtual Machine Wizard

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name:

Pfsense

Location:

C:\Users\antap\Documents\Virtual Machines\Pfsense Browse...

The default location can be changed at Edit > Preferences.

< Back Next > Cancel

Annexe 21 : Choix de la taille de la VM PFSense.

New Virtual Machine Wizard ✕

Specify Disk Capacity
How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB):

Recommended size for FreeBSD version 10 and earlier 64-bit: 20 GB

☐ Store virtual disk as a single file
☒ Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Annexe 22 : Copyright de PFSense.

Copyright and distribution notice

Copyright and Trademark Notices.

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

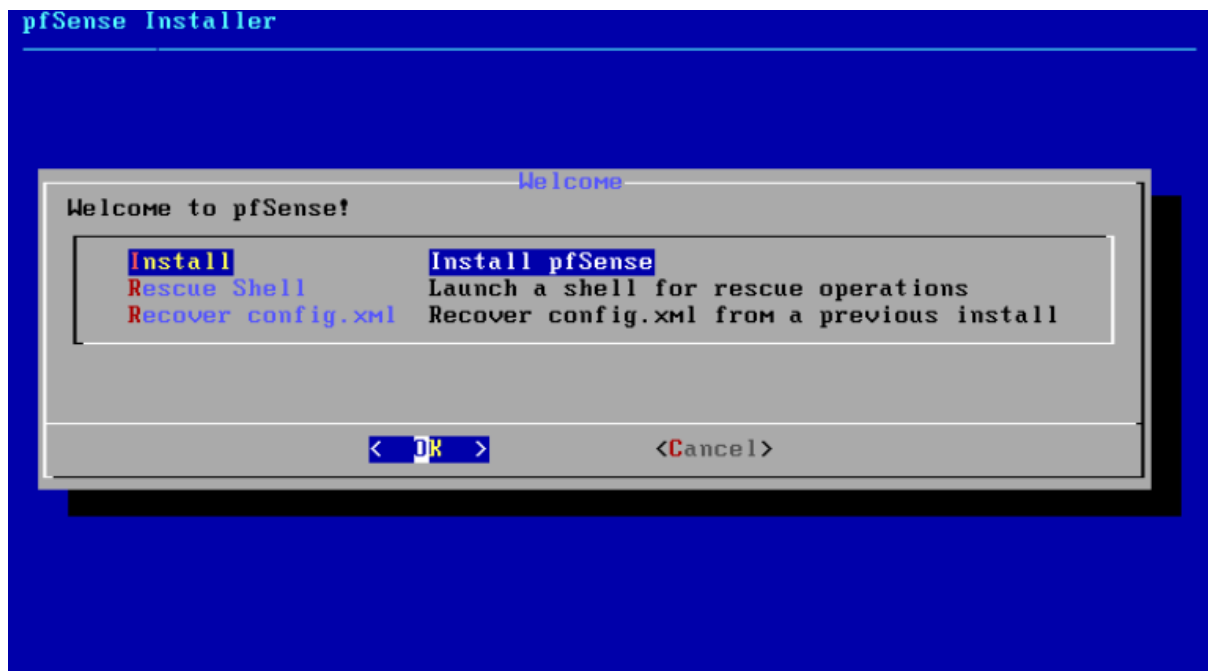
Copyright(c) 2014-2022. Rubicon Communications, LLC d/b/a Netgate
("Netgate").
All Rights Reserved.

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.

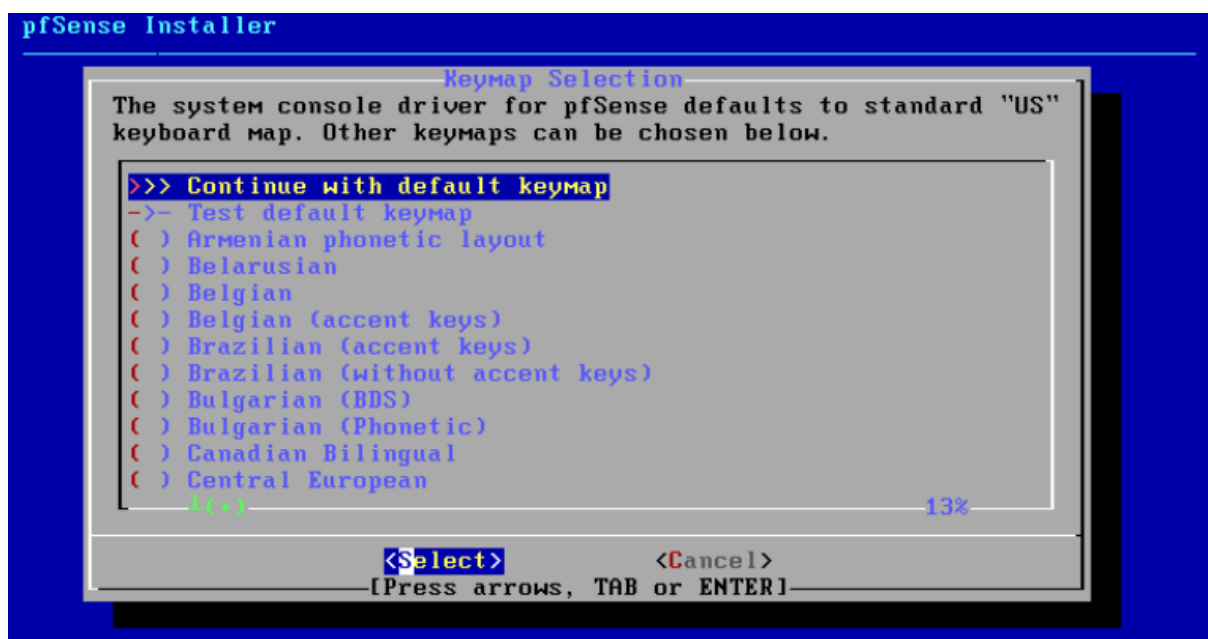
"pfSense" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are owned by the respective companies or persons indicated.

28%

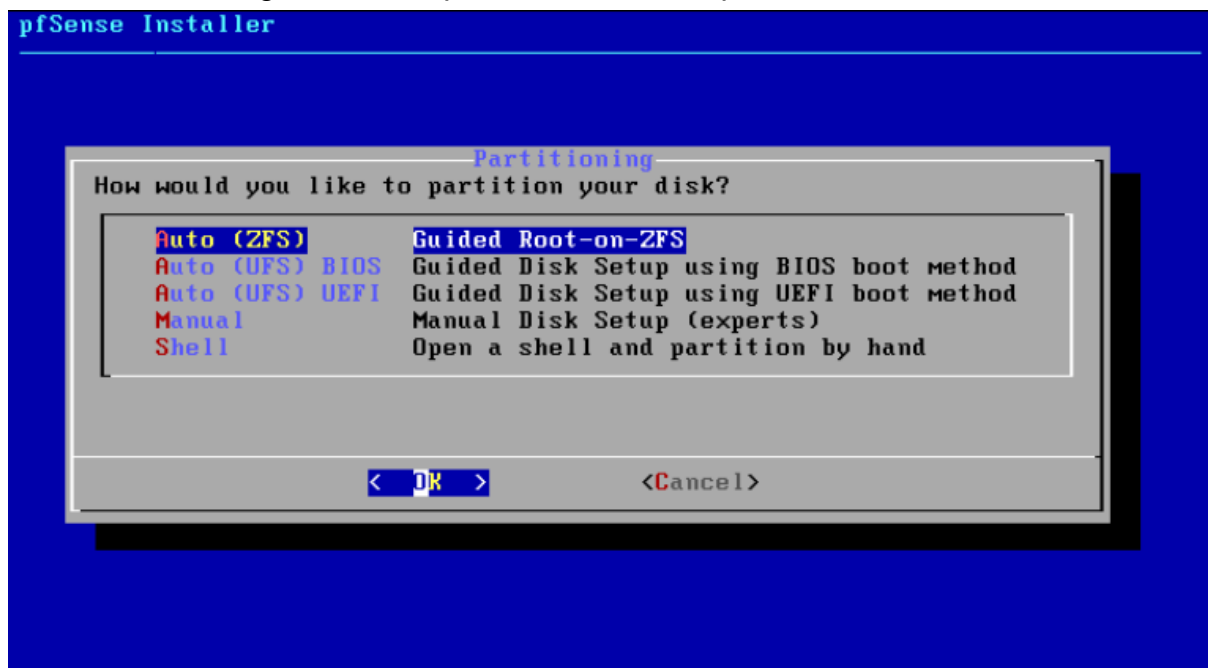
Annexe 23 : Menu d'installation de PFSense.



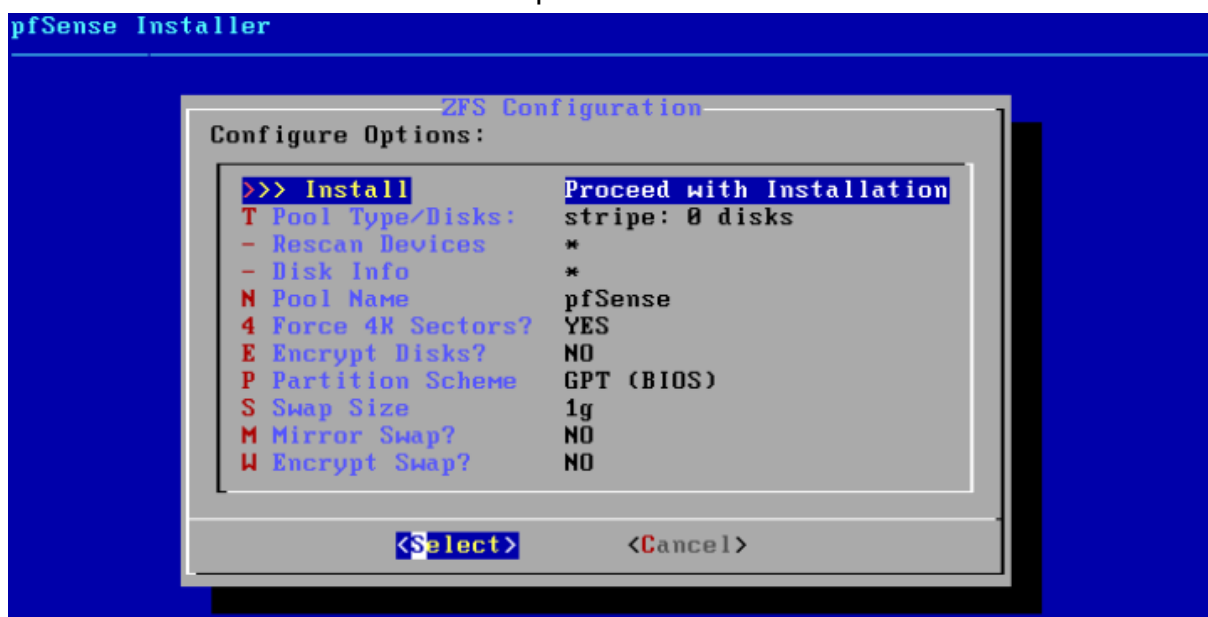
Annexe 24 : Choix du clavier et des raccourcis de PFSense.



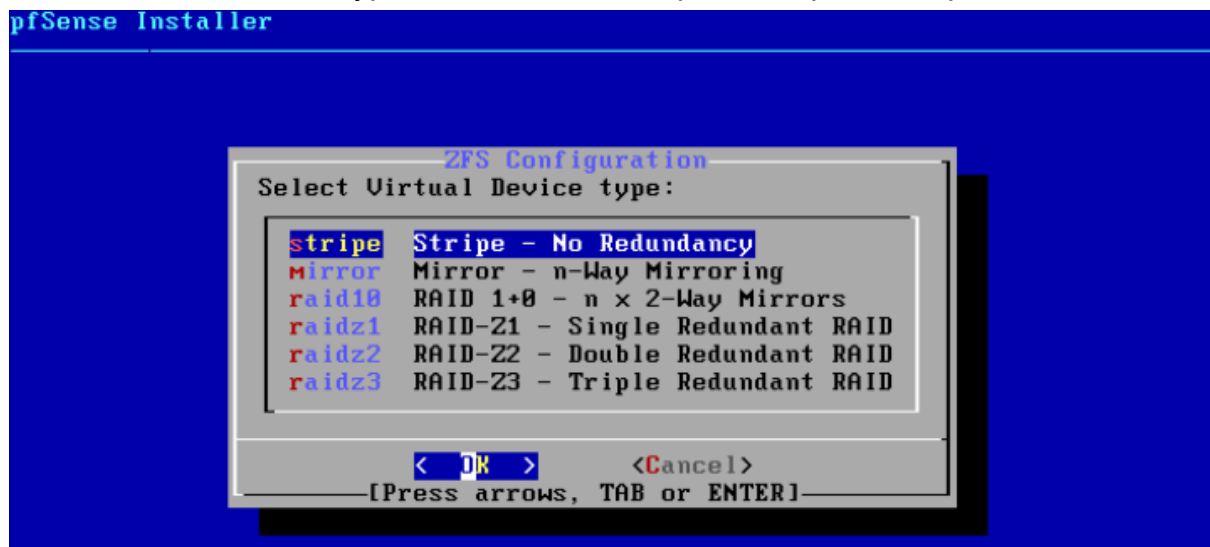
Annexe 25 : Configuration des partitions sur le disque dur.



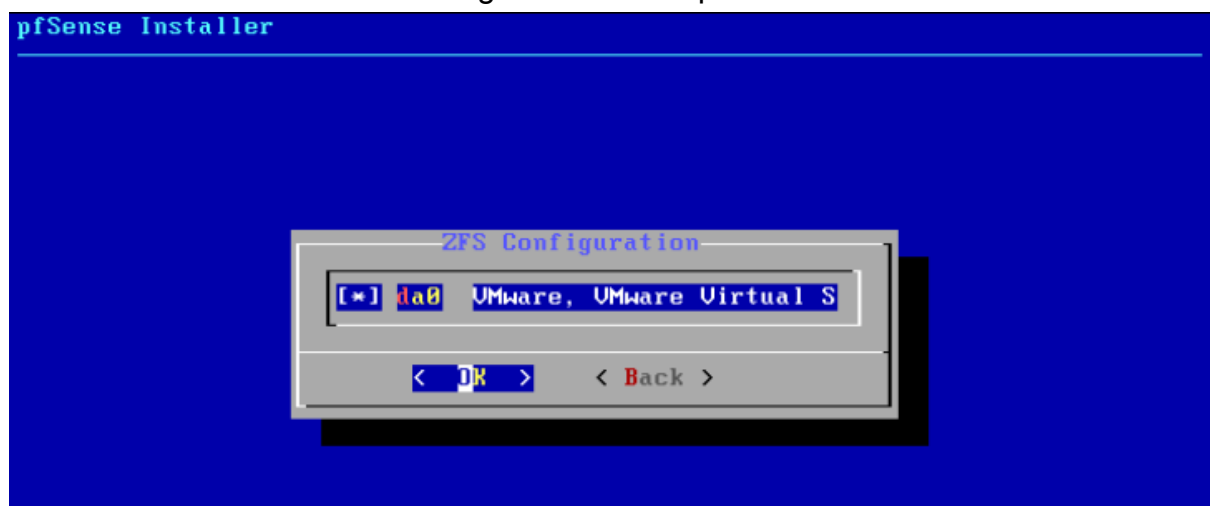
Annexe 26 : Validation des choix des partitions.



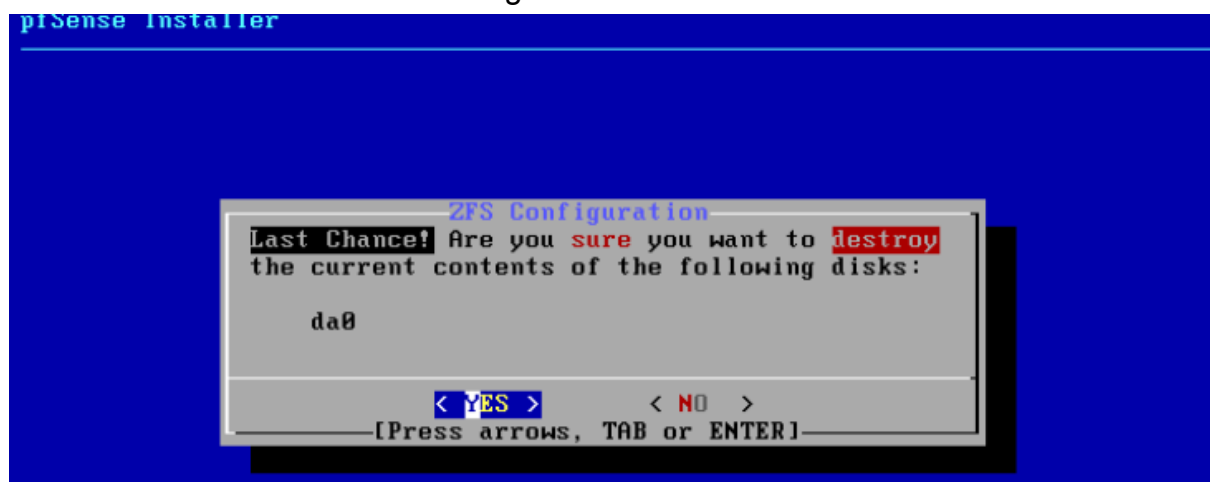
Annexe 27 : Choix d'un type d'utilisation du disque dur à plusieurs partitions.



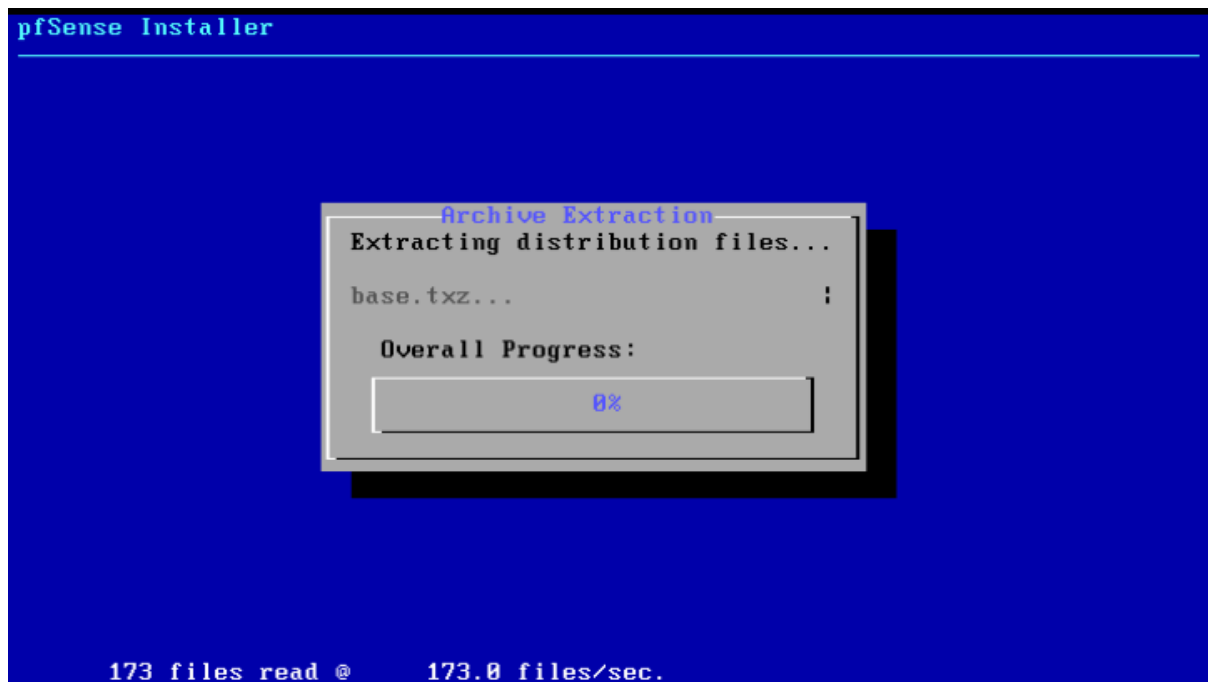
Annexe 28 : Validation de la configuration du disque dur.



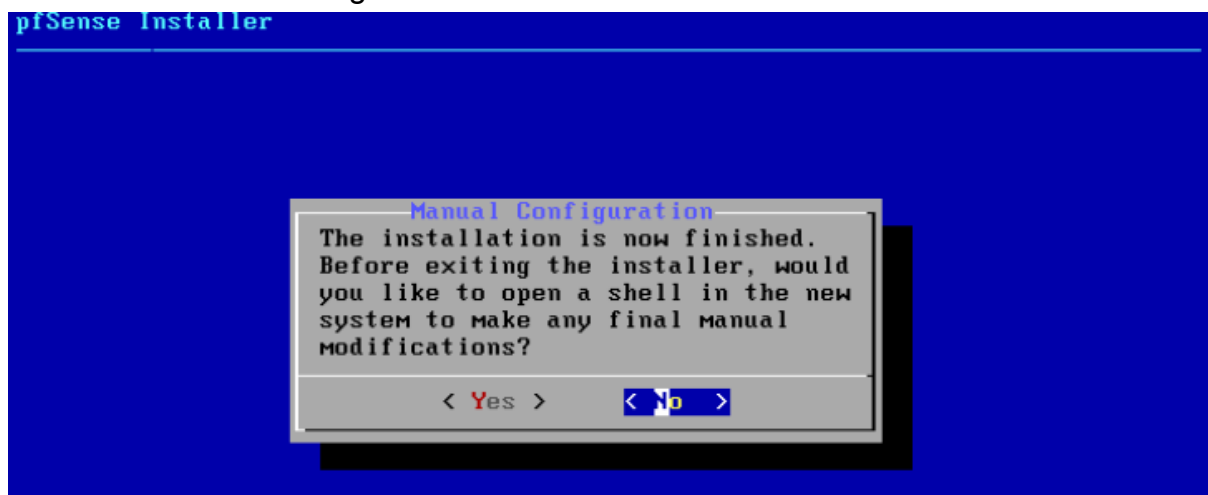
Annexe 29 : Vérification du formatage.



Annexe 30 : PFSense s'installe après le formatage des partitions.



Annexe 31 : Fin de configuration de PFSense.



Annexe 32 : PFSense configuré avertis qu'il va redémarrer.



Annexe 33 : Terminal de PFSense.

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv00)

VMware Virtual Machine - Netgate Device ID: 1c2b434219dc41f2ba29

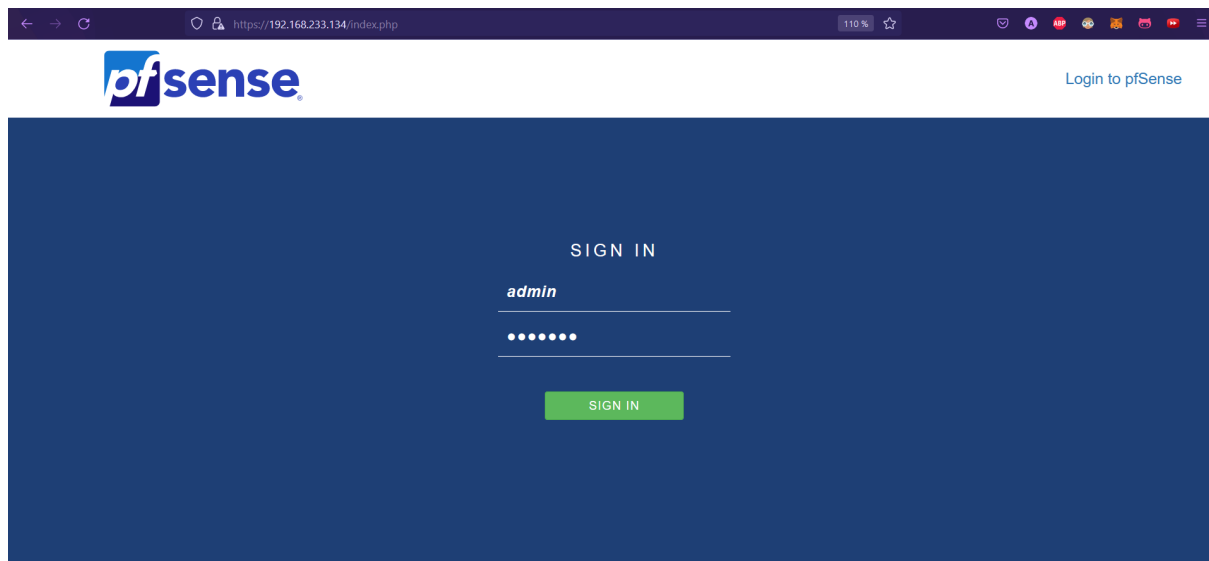
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.233.134/24
LAN (lan)      -> em1      -> v4: 10.0.0.6/29

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: █
```

Annexe 34 : Page de PFSense sur le navigateur.



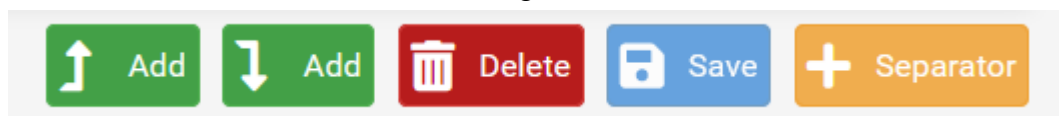
Annexe 35 : Commande **pfctl -d** dans le terminal de PFSense.

```
7) Ping host          16) Restart PHP-FPM
8) Shell

Enter an option:
Message from syslogd@pfSense at May  2 07:07:48 ...
php-fpm[913631]: /index.php: Successful login for user 'admin' from: 192.168.233.
1 (Local Database)
8

[2.6.0-RELEASE][root@pfSense.home.arpal/root: pfctl -d
```

Annexe 36 : Barre d'outils de la catégorie rules du PFSense.



Annexe 37 : Page d'une règle de PFSense pour du HTTP.

Firewall / Rules / 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

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

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 setting must remain at its default value, any.

Destination

Destination

☐ Invert match

WAN address

Destination Address

/

Destination Port Range

HTTP (80)

From

Custom

HTTP (80)

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 using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Rule Information

Tracking ID

1646661857

Created

3/7/22 14:04:17 by admin@192.168.233.1 (Local Database)

Updated

3/7/22 14:04:17 by admin@192.168.233.1 (Local Database)

Save

Annexe 38 : Page d'une règle de PFSense pour du HTTPS.

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

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

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 setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match

WAN address

Destination Address

/

Destination Port Range

HTTPS (443)

From

Custom

HTTPS (443)

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 using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Rule Information

Tracking ID

1646661435

Created











3/7/22 13:57:15 by admin@192.168.233.1 (Local Database)

Updated

3/7/22 14:01:28 by admin@192.168.233.1 (Local Database)

Save

Annexe 39 : Liste des règles de PFSense.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1 / 257 KiB	IPv4 TCP	*	*	WAN address	443 (HTTPS)	*	none			    
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	WAN address	80 (HTTP)	*	none			    

Annexe 40 : Ping du PFSense vers le serveur Windows.

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.233.134/24
LAN (lan)      -> em1      -> v4: 10.0.0.6/29

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: 8

[2.6.0-RELEASE][root@pfSense.home.arpal]/root: ping 10.0.0.4
PING 10.0.0.4 (10.0.0.4): 56 data bytes
64 bytes from 10.0.0.4: icmp_seq=0 ttl=128 time=0.510 ms
64 bytes from 10.0.0.4: icmp_seq=1 ttl=128 time=0.430 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=128 time=0.293 ms
64 bytes from 10.0.0.4: icmp_seq=3 ttl=128 time=0.365 ms
64 bytes from 10.0.0.4: icmp_seq=4 ttl=128 time=0.395 ms
█
```

Annexe 41 : Ping du client Windows vers le PFSense.

```
C:\Users\antap>ping 10.0.0.6

Envoi d'une requête 'Ping' 10.0.0.6 avec 32 octets de données :
Réponse de 10.0.0.6 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.6 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.6 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.6 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.0.0.6:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Annexe 42 : Commande pour installer RSync.

```
Terminal
R19:16:33 qqnqq@virtual-machine:~$
sudo apt-get install rsync -y
```

Annexe 43 : Commande pour lancer et autoriser RSync.

```
19:16:33 qqnq@q-virtual-machiqne:~$ sudo systemctl start rsync
19:16:33 qqnq@q-virtual-machiqne:~$ sudo systemctl enable rsync
```

Annexe 44 : Commande pour aller dans le fichier de configuration de RSync.

```
backuo@ubuntu: ~
backuo@ubuntu:~$ sudo nano /etc/rsyncd.conf
[sudo] password for backuo:
backuo@ubuntu:~$
```

Annexe 45 : Ligne de configuration pour le fichier de configuration de RSync.

```
GNU nano 4.8 /etc/rsyncd.conf
[backup]
path=/home/backuo/backup
hosts allow = 10.0.0.1
hosts deny = *
list = true
uid = root
gid = root
read only = false
```

Annexe 46 : Création du fichier rsync.

```
19:04:34 qqnq@q-virtual-machiqne:~$ cd /var/www/html/Infra-Website/
19:04:39 qqnq@q-virtual-machiqne:/var/www/html/Infra-Website$ nano rsync
```

Annexe 47 : Commande à mettre dans le fichier rsync.

```
Ordinateur  var  www  html  Infra-Website
js  pages  style  LICENSE  README.md  rsync  test

Terminal
GNU nano 4.8 rsync Modifié
rsync -avz /var/www/html/Infra-Website/ 10.0.0.2::backup
```

Annexe 48 : Changement des permissions du fichier rsync.

```
19:04:39 qqnq@q-virtual-machiqne:/var/www/html/Infra-Website$ chmod u+x rsync
```

Annexe 49 : Commande pour entrer dans le fichier cron.

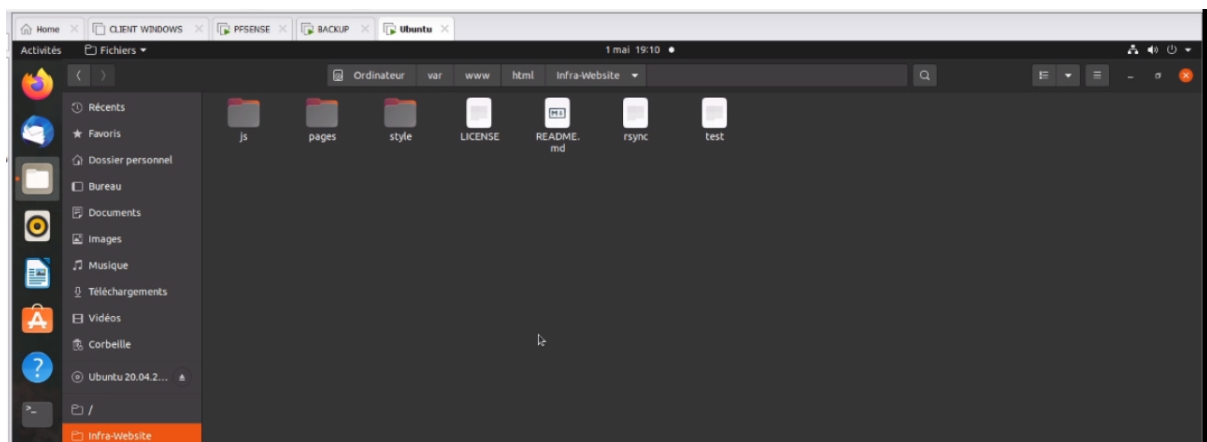
```
19:04:39 qqng@q-virtual-machine:/var/www/html/Infra-Website$ crontab -e
```

Annexe 50 : Contenu du fichier cron.

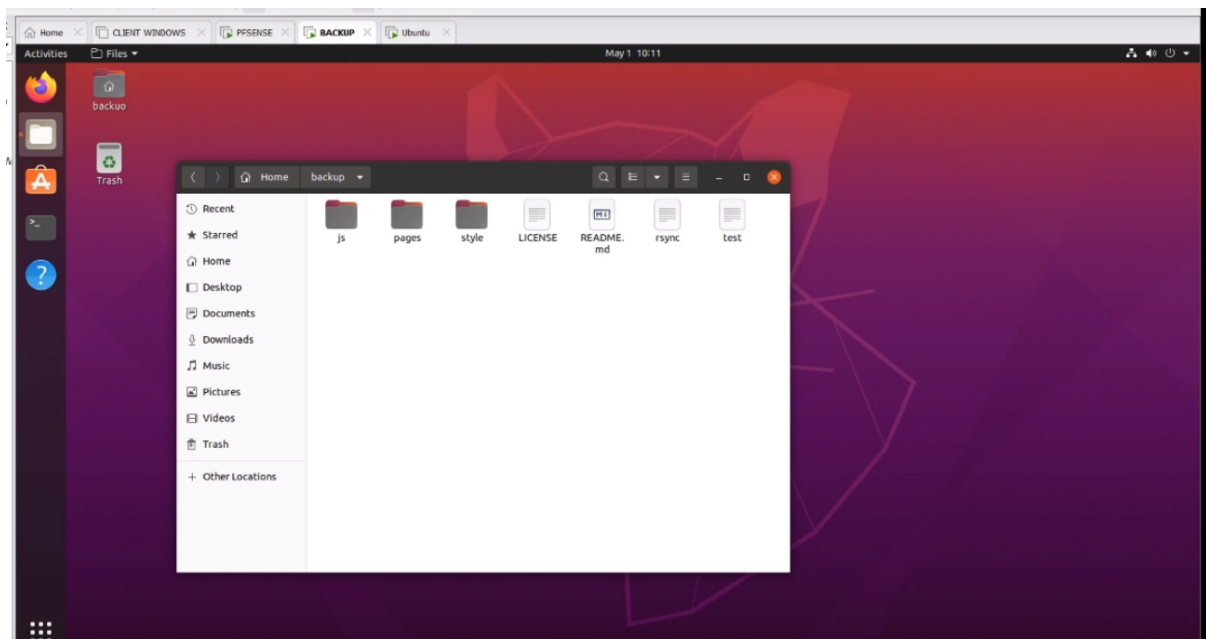
```
GNU nano 4.8 /tmp/crontab.W39ZWf/crontab
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
* * * * * /var/www/html/Infra-Website/rsync

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^J Justifier
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^T Orthograp.
```

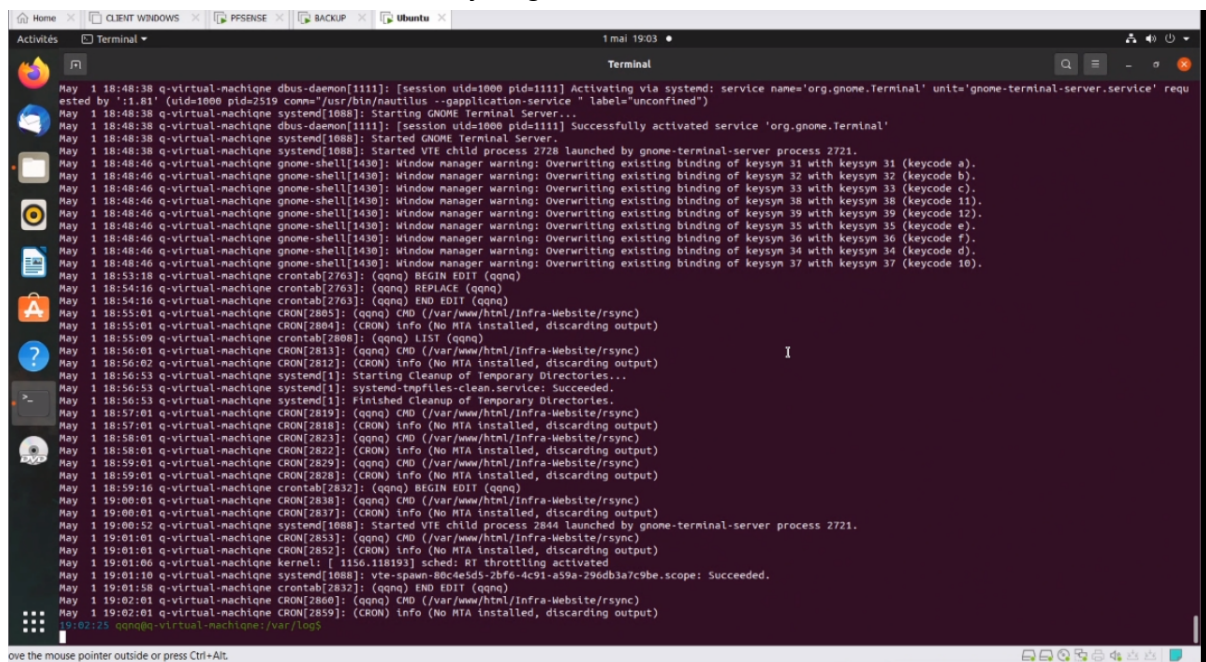
Annexe 51 : Contenu du dossier Infra-Website dans le serveur web.



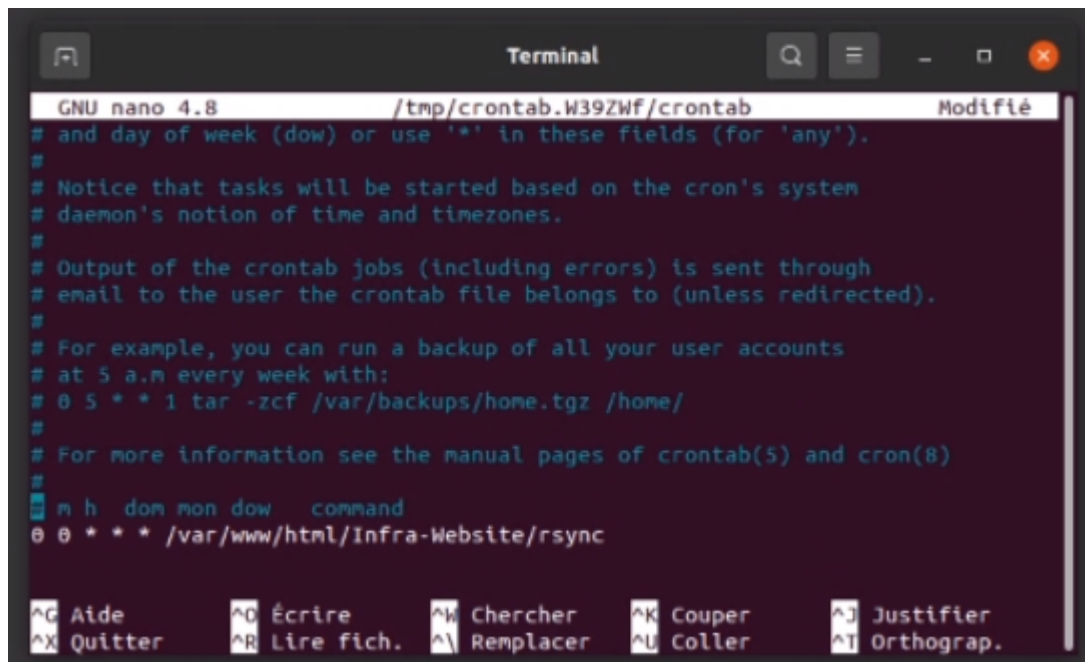
Annexe 52 : Contenu du dossier backup dans le serveur backup



Annexe 53 : Contenu du fichier syslog.

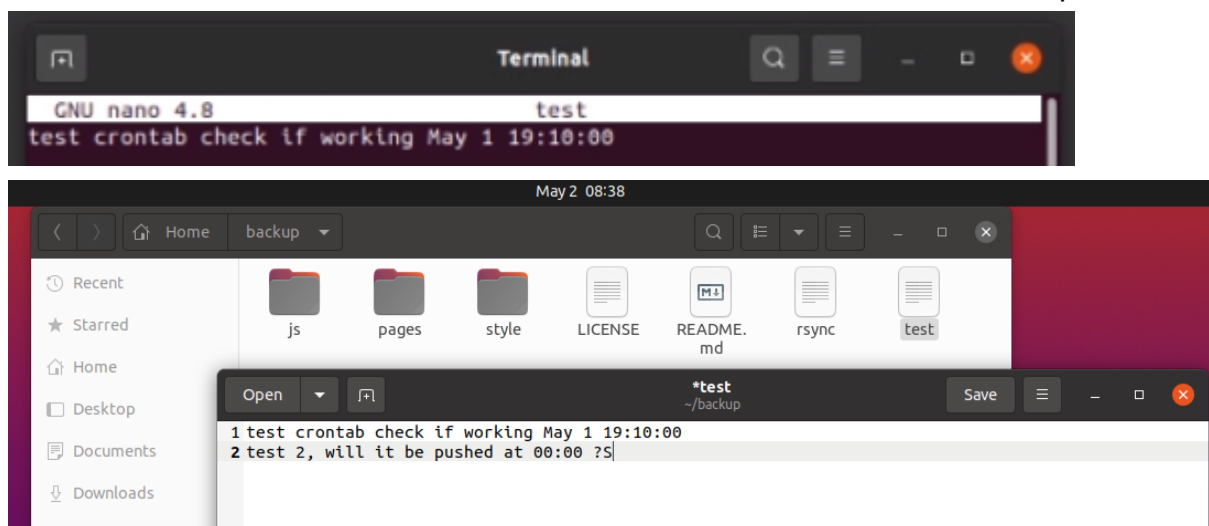


Annexe 54 : Contenu du fichier cron.



```
GNU nano 4.8 /tmp/crontab.W39ZWF/crontab Modifié
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
0 0 * * * /var/www/html/Infra-Website/rsync
```

Annexe 55 : Contenu du fichier **test** sur le serveur web et le serveur backup.



```
GNU nano 4.8 test
test crontab check if working May 1 19:10:00
```

```
May 2 08:38
1 test crontab check if working May 1 19:10:00
2 test 2, will it be pushed at 00:00 ?5
```

Annexe 56 : Installation Nginx

```
15:42:29 qqnq@q-virtual-machiqne:~$
sudo apt-get install nginx
```

Annexe 57 : Statut du serveur

```
15:42:29 qqnq@q-virtual-machiqne:~$ service nginx status
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enab
   Active: active (running) since Mon 2022-05-02 15:36:54 CEST; 11min ago
     Docs: man:nginx(8)
   Process: 1008 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_proce>
   Process: 1035 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (c>
  Main PID: 1042 (nginx)
    Tasks: 3 (limit: 4584)
   Memory: 6.1M
   CGroup: /system.slice/nginx.service
           └─1042 nginx: master process /usr/sbin/nginx -g daemon on; master_
             └─1047 nginx: worker process
              └─1048 nginx: worker process

mai 02 15:36:53 q-virtual-machiqne systemd[1]: Starting A high performance web s
mai 02 15:36:54 q-virtual-machiqne systemd[1]: Started A high performance web s
lines 1-16/16 (END)...skipping...
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2022-05-02 15:36:54 CEST; 11min ago
     Docs: man:nginx(8)
   Process: 1008 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
   Process: 1035 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
  Main PID: 1042 (nginx)
    Tasks: 3 (limit: 4584)
   Memory: 6.1M
   CGroup: /system.slice/nginx.service
           └─1042 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
             └─1047 nginx: worker process
              └─1048 nginx: worker process

mai 02 15:36:53 q-virtual-machiqne systemd[1]: Starting A high performance web server and a reverse proxy server...
mai 02 15:36:54 q-virtual-machiqne systemd[1]: Started A high performance web server and a reverse proxy server.
```

Annexe 58 : Changement de dossier (html)

```
15:58:33 qqnq@q-virtual-machiqne:~$ cd /var/www/html/
```

Annexe 59 : Affichage dossier html

```
16:00:38 qqnq@q-virtual-machiqne:/var/www/html$ ls
index.nginx-debian.html  Infra-Website  style.css
```

Annexe 60 : Changement de dossier (sites-enabled)

```
16:03:11 qqnq@q-virtual-machiqne:~$ cd /etc/nginx/sites-enabled/
```

Annexe 61 : Entrée dans le fichier de configuration

```
16:05:21 qqnq@q-virtual-machiqne:/etc/nginx/sites-enabled$ sudo nano default
```


Annexe 62 : Modification html par défaut

```
#
server {
    listen 80 default_server;
    listen [::]:80 default_server;

    # SSL configuration
    #
    # listen 443 ssl default_server;
    # listen [::]:443 ssl default_server;
    #
    # Note: You should disable gzip for SSL traffic.
    # See: https://bugs.debian.org/773332
    #
    # Read up on ssl_ciphers to ensure a secure configuration.
    # See: https://bugs.debian.org/765782
    #
    # Self signed certs generated by the ssl-cert package
    # Don't use them in a production server!
    #
    # include snippets/snakeoil.conf;

    root /var/www/html/Infra-Website/pages;

    # Add index.php to the list if you are using PHP
    index index.html index.htm index.nginx-debian.html;
```

Annexe 63 : Page par défaut Nginx

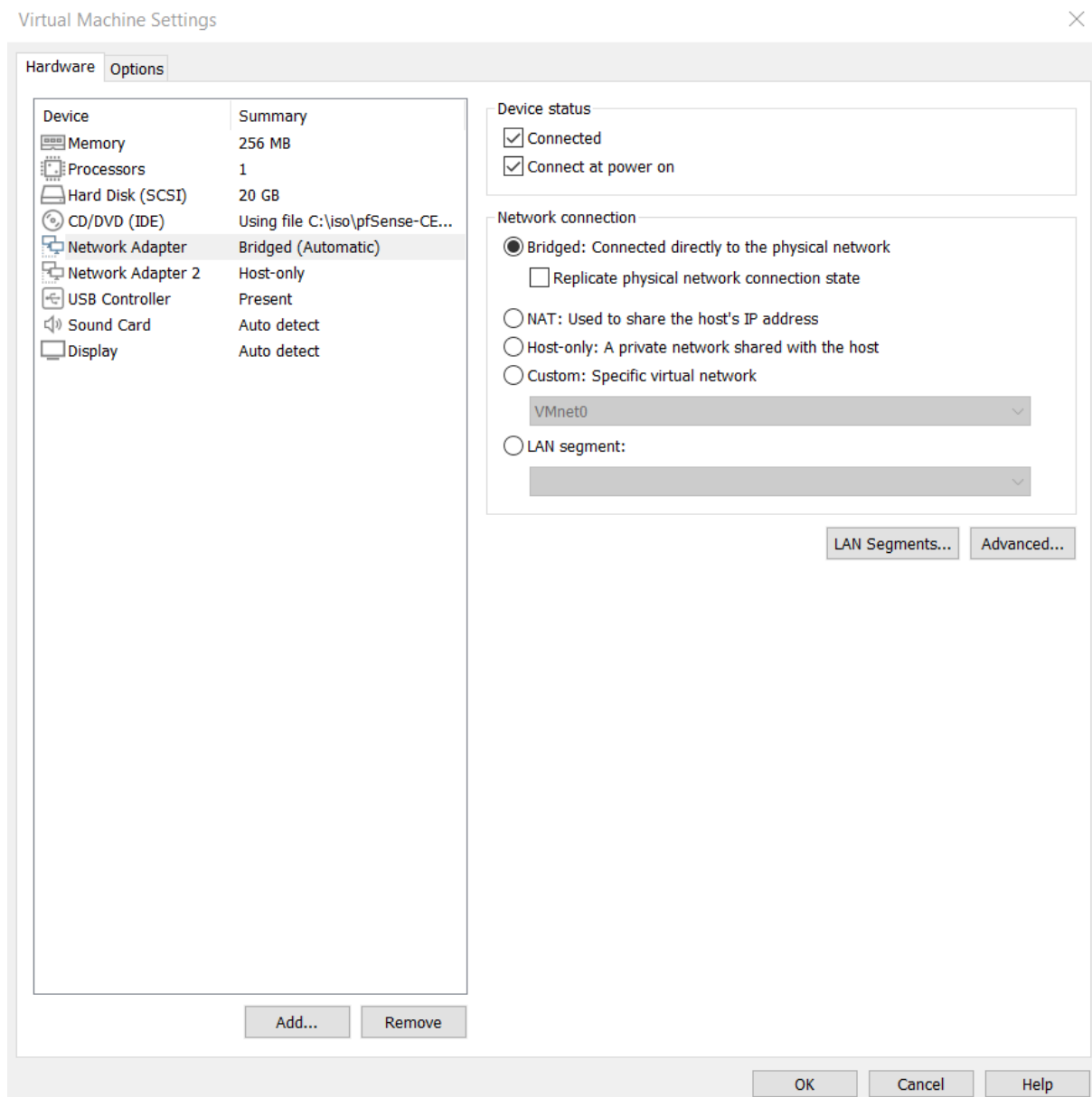
Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Annexe 70 : Modification de réseau externe de la VM en **bridged**.



Annexe 71 : Changement de l'IP WAN du pare feu.

```

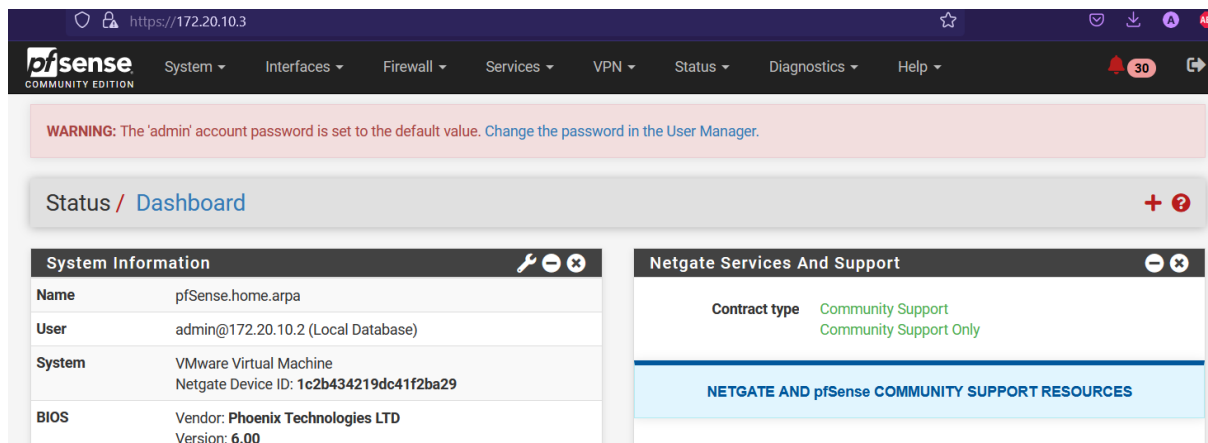
WAN (wan)      -> em0      -> v4/DHCP4: 172.20.10.3/28
                                     v6/DHCP6: 2a02:8440:4540:ee4c:20c:29ff:fe55:d0
9d/64
LAN (lan)      -> em1      -> v4: 10.0.0.6/29

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:
Message from syslogd@pfSense at May  2 08:27:14 ...
php-fpm[3691]: /index.php: webConfigurator authentication error for user 'admin'
from: 172.20.10.2

Message from syslogd@pfSense at May  2 08:27:24 ...
php-fpm[3691]: /index.php: Successful login for user 'admin' from: 172.20.10.2 (L
ocal Database)

```



Annexe 72 : Règle PFSense pour autoriser d’autres PC à avoir accès au site.

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled

☐ Disable this rule

No RDR (NOT)

☐ Disable redirection for traffic matching this rule

This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface

WAN

Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Display Advanced

Destination

☐ Invert match.

Single host or alias

172.20.10.3

Type

Address/mask

Destination port range

Other

8080

Other

8080

From port

Custom

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

Single host

10.0.0.1

Type

Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4

i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port

HTTP

Port

Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.

Description

PORT 80

A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync

☐ Do not automatically sync to other CARP members

This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection

Use system default

Filter rule association

Rule NAT PORT 80

[View the filter rule](#)

Rule Information

Created

4/30/22 14:26:56 by admin@192.168.233.1 (Local Database)

Updated

5/2/22 08:28:45 by admin@172.20.10.2 (Local Database)

Save

Port Forward

1:1

Outbound

NPt

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions		
<input type="checkbox"/>	<input checked="" type="checkbox"/>		WAN	TCP	*	*	172.20.10.3	8080	10.0.0.1	80 (HTTP)	PORT 80	

Add

Add

Delete

Save

Separator

Legend

Pass

Linked rule

Annexe 73 : Site depuis un autre PC.

