easy Former
La formation à 360°

Mise en place d'une infrastructure virtualisée de clients légers

Linux Terminal Server Project

Référence : TP-CLIENTLEGER-LTSP-2588

Auteur :
Nicolas

Destinataires :
Formateurs
Apprenants

Date de création : 14/10/2022
Date de dernière modification : 28/12/22

Version : 1.5

Sommaire

1 Introduction

1.1 Présentation du TP

J'ai préparé pour vous ces travaux pratiques (TP) à mon domicile sur mon ordinateur portable Lenovo à l'aide de l'hyperviseur VMware Workstation.

Votre objectif sera de recréer l'infrastructure virtualisée de clients légers que j'ai détaillée dans le schéma ci-dessous.

Concrètement, à la fin du TP, plusieurs personnes fictives (Ben, Bob et Bill) pourront se connecter à leur compte utilisateur respectifs (ben, bob et bill), depuis leur machine client léger (client1, client2, client3) quasiment vide (= sans disque dur, ni système d'exploitation installé), sur une distribution Ubuntu avec l'interface graphique MATE, qui sera installée sur un serveur LTSP, « Linux Terminal Server Project ».

Ils pourront chacun et en même temps – depuis leur poste client léger respectifs – se connecter à leur session utilisateur et utiliser toutes les applications dont ils ont besoin, travailler sur des documents et stocker leurs fichiers de manière tout à fait ordinaire. Mais en réalité tout se passera sur le serveur.

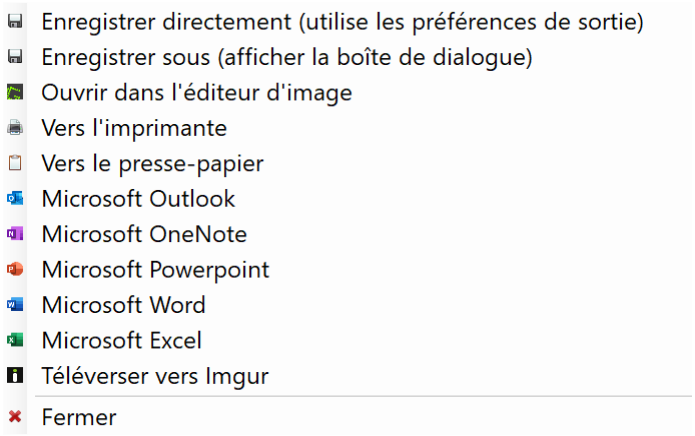
1.2 Consigne à respecter

Afin que je puisse évaluer votre participation au TP, je vous demanderai régulièrement d'effectuer une capture d'écran (ou plusieurs si nécessaire) prouvant que vous avez bien accompli des étapes importantes du TP. Afin que je ne sois pas submergé par des fichiers en vrac, vous devrez renommer chaque image (.png, .jpg) obtenue - *au minimum* - par votre prénom ou vos initiales suivi d'un numéro, par ex. **« prénom01** » ou « **pn02** » ou - *au mieux* - comme ceci par exemple « **Prénom NOM 01 – Description** ». Enfin, vous devrez m'envoyer vos captures en une seule fois en fin de journée ou en fin de module dans une archive (Année-Mois-Jour-Prénom-NOM.zip) via un lien de partage cloud (OneDrive, Google Drive, etc.) ou par mail à l'adresse que je vais vous communiquer.

Vous pouvez aussi choisir de coller vos screenshots dans un document texte (.doc, .docx) si vous préférez. Si votre organisme de formation me demande de vous attribuer une note en fin de module, votre participation au TP y comptera pour beaucoup.

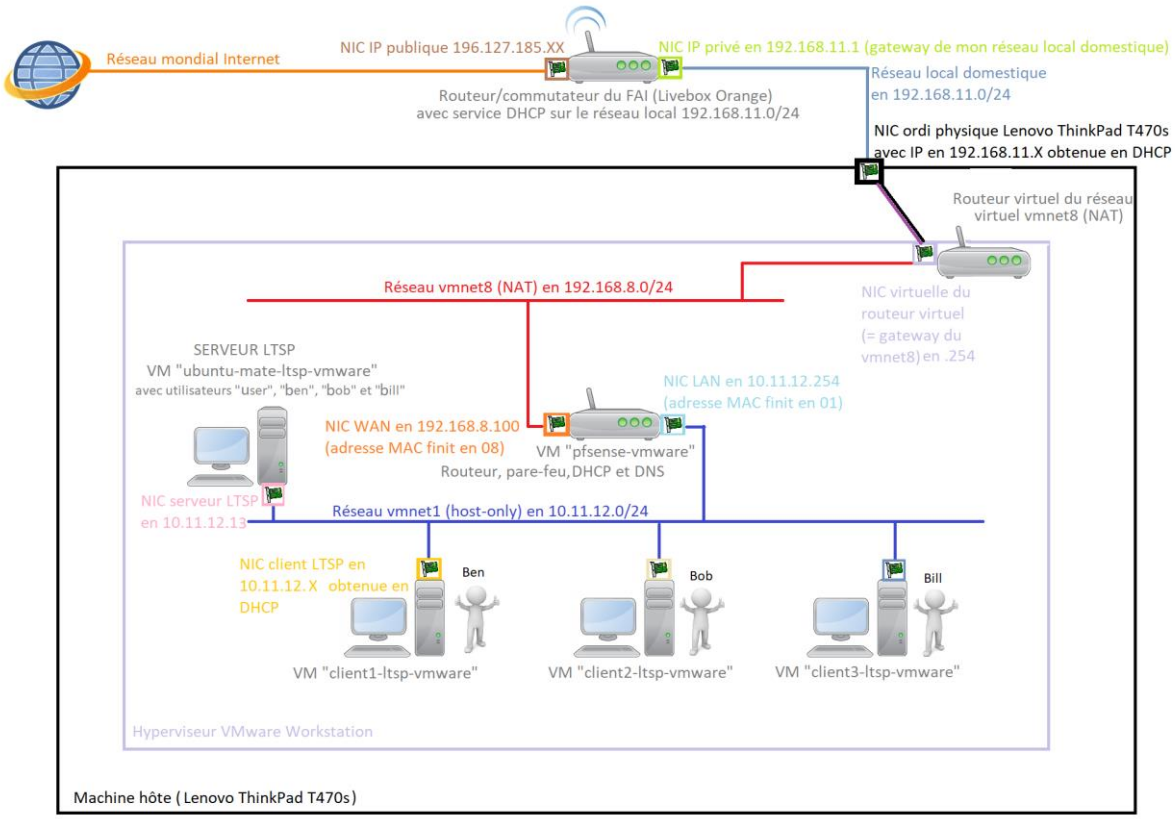
L'outil Greenshot : https://getgreenshot.org/downloads/

Je vous conseille d'utiliser Greenshot (un logiciel libre & open source) pour les prises de capture d'écran (il est bien plus pratique que « Outil capture d'écran » de Windows). Une fois installé et lancé en arrière-plan, utilisez la touche « *Impr écran* » de votre clavier pour prendre une capture d'écran rapide puis choisissez « Enregistrer directement » pour qu'elle arrive immédiatement sur votre bureau ou « Enregistrer sous » pour la renommer avant de l'enregistrer où vous voulez. Il propose aussi d'autres actions rapides comme envoyer la capture directement dans un éditeur d'image (pour faire des cadres, des flèches, du floutage) ou dans le presse-papier (pour pouvoir coller la capture d'écran quelque part sans avoir besoin de l'enregistrer en tant que fichier au préalable) :



1.3 Schéma de l'infrastructure

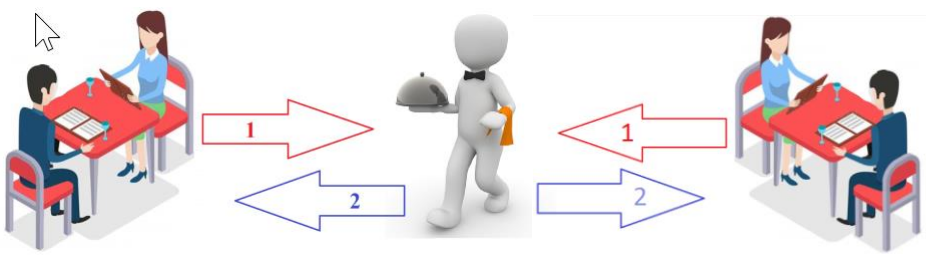
J'ai volontairement fait un schéma "ultra-détaillé" pour aider à la compréhension des plus débutants. N'hésitez pas à y revenir régulièrement afin de vous familiariser avec l'infra.



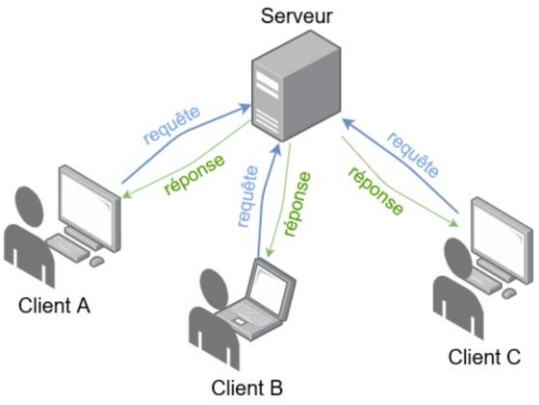
2 Un peu de théorie

2.1 Qu'est-ce que le modèle « client-serveur » ?

Tout comme au restaurant les clients demandent au(x) serveur(s), …



… en informatique les serveurs répondent aux demandes des clients :



Le **protocole**, **modèle** ou **environnement client-serveur** désigne **un mode de transaction (souvent à travers un réseau) entre plusieurs programmes ou processus : l'un, qualifié de client, envoie des requêtes ; l'autre, qualifié de serveur, attend les requêtes des clients et y répond**. Le serveur offre ici un **service** au client.

Par extension, le client désigne souvent l'ordinateur sur lequel est exécuté le logiciel client, et le serveur, l'ordinateur sur lequel est exécuté le logiciel serveur. Les machines serveurs sont généralement dotées de capacités supérieures à celles des ordinateurs personnels en ce qui concerne la puissance de calcul, les entrées-sorties et les connexions réseau, afin de pouvoir répondre de manière efficace à un grand nombre de clients. Les clients sont souvent des ordinateurs personnels ou terminaux individuels (téléphone, tablette), mais pas systématiquement. Un serveur peut répondre aux requêtes de plusieurs clients. Parfois le client et le serveur peuvent être sur la même machine.

Plus d'infos sur : https://fr.wikipedia.org/wiki/Client-serveur

2.2 Qu'est-ce qu'un serveur ?

Un **serveur** informatique est **un dispositif informatique (matériel et logiciel) qui offre des services à un ou plusieurs clients (parfois des milliers)**. Les services les plus courants sont :

- L'accès aux informations du World Wide Web
- Le courrier électronique
- Le partage de périphériques (imprimantes, disques durs, etc.)
- Le commerce électronique
- Le stockage en base de données
- La gestion de l'authentification et du contrôle d'accès
- Le jeu et la mise à disposition de logiciels applicatifs

Plus d'infos sur : https://fr.wikipedia.org/wiki/Serveur_informatique

2.3 Qu'est-ce qu'un client ?

Dans un réseau informatique, un **client** est **le logiciel qui envoie des demandes à un serveur**. Il peut s'agir d'un logiciel manipulé par une personne, ou d'un bot. Est appelé client aussi bien l'ordinateur depuis lequel les demandes sont envoyées que le logiciel qui contient les instructions relatives à la formulation des demandes et la personne qui opère les demandes.

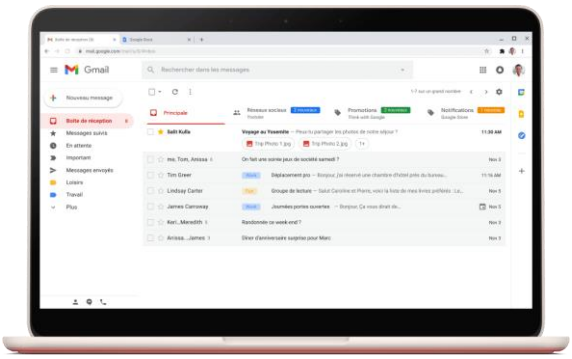
L'ordinateur client est généralement un ordinateur personnel ordinaire, équipés de logiciels relatifs aux différents types de demandes qui vont être envoyées, comme un navigateur web, un logiciel client pour le World wide web.

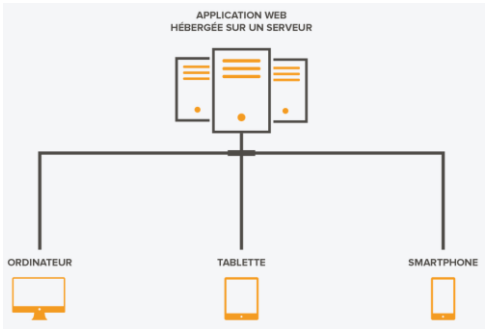
Plus d'infos sur : https://fr.wikipedia.org/wiki/Client_(informatique)

2.4 Qu'est-ce qu'un client léger ?

Le terme client léger (*thin client* en anglais) peut désigner un élément matériel ou un élément logiciel.

2.5 Qu'est-ce qu'un client léger logiciel ?





Le terme « **client pauvre** » logiciel ou « **client léger** » logiciel, en anglais « ***thin client*** », par opposition au « client lourd » logiciel, désigne **une application utilisant le modèle client-serveur, accessible via une interface web (en HTML), où toutes les opérations de traitement sont effectuées par le serveur**. Pour ces raisons, le navigateur est parfois appelé « client universel ».

L'usage veut qu'une application en client léger n'impose à l'utilisateur que d'avoir un navigateur web (ex. : Mozilla Firefox, Google Chrome, Microsoft Edge, etc.). De ce fait, on utilisera aussi le terme « **application web** » pour désigner le client léger logiciel.

Exemple de client léger logiciel/application web : Gmail.

En effet c'est une application cliente de messagerie qui n'a pas besoin d'être installée sur la machine de l'utilisateur pour être lancée. Il n'a qu'à aller sur le portail web de connexion de Gmail et se connecter pour effectuer des opérations sur les serveurs de messagerie de Google. S'il décide de lancer une recherche dans ses courriels ce sont bien les serveurs de Google qui vont devoir utiliser leur capacité de calcul pour fournir un résultat à l'utilisateur. On utilisera généralement le terme de « **webmail** » pour désigner plus spécifiquement une application web de messagerie.

2.6 Qu'est-ce qu'un client léger matériel ?

Un **client léger matériel** est un **terminal peu coûteux qui dépend d'un serveur pour toutes ses opérations**.

Les clients légers et autres types d'équipements « légers » réalisent toutes les opérations informatiques via une connexion réseau à un serveur central et n'effectuent qu'une faible partie du traitement sur le matériel lui-même.

Dans le cadre de ce TP, il faudra garder en tête que la locution « client léger » désigne cette deuxième catégorie.

De plus, nous allons virtualiser ces clients légers dits « matériels » à l'aide d'un hyperviseur. C'est-à-dire qu'ils ne seront donc pas physiquement matériels, ce seront des machines virtuelles.

Découvrez des modèles de clients légers matériels ici : https://www.dell.com/fr-fr/dt/wyse/index.htm#scroll=off

2.7 Quels sont les avantages du client léger ?

Les avantages liés à la mise en place d'une solution de terminaux clients légers par rapport à des clients lourds sont les suivants :

- Coût très faible
- Facilité d'administration et de maintenance (installation de logiciels, mises à jour, etc.)
- Sécurité matérielle et logicielle
- Disponibilité des applications installées pour tous les clients légers

2.8 Quels sont les inconvénients du client léger ?

Les inconvénients liés à la mise en place d'une solution de terminaux clients légers par rapport à des clients lourds sont les suivants :

- Un client léger **dépend de manière critique des ressources matérielles du serveur** car celui-ci exécute la majeure partie de la charge de travail, notamment le stockage, la récupération et le traitement. En cas de défaillance du serveur, tous les clients sont hors service.
- **Le serveur peut atteindre ses limites** si de nombreux utilisateurs lancent des applications gourmandes en puissance (montage vidéo, modélisation 3D, feuilles de calculs lourdes).
- Un client léger **dépend de sa connexion avec le serveur** (parfois via Internet ou un VPN) pour travailler. Il a **besoin d'une connexion stable et d'un débit élevé**.
- Une infrastructure de clients légers implique une **consommation réseau importante**.
- Une infrastructure de clients légers **nécessite l'achat d'un serveur** qui coûte très cher (ou bien un abonnement auprès d'un prestataire).
- En cas d'appel à un prestataire extérieur fournissant le serveur, il n'y aura pas de traitement local de nos propres données et/ou programmes. Cette solution **nécessite de devoir lui faire confiance** par rapport à sa disponibilité, au traitement de nos données, etc.

Bon à savoir :

Cette question est susceptible de tomber à votre examen TSSR 😉

2.9 Qu'est-ce que LTSP ?

Selon la définition même du site : **Linux Terminal Server Project** ou **LTSP** est **un paquet additionnel pour GNU/Linux qui permet de connecter de nombreuses stations clientes légères sur un serveur GNU/Linux**.

Autrement dit : **LTSP** est **un ensemble de programmes permettant à plusieurs personnes d'utiliser le même ordinateur**.

Cela est réalisé par la mise en place d'un réseau informatique composé d'un serveur sous Linux et de clients légers. Le serveur héberge et exécute toutes les applications. Les clients sont appelés terminaux X. Ils transforment les signaux venant de la souris et du clavier, les envoient au serveur par le réseau, puis affichent sur leur écran le résultat renvoyé par le serveur. Ces clients légers ne nécessitent ni disque dur, ni processeur puissant – on les appelle aussi « diskless clients », ou clients sans disque. Ils peuvent être des ordinateurs anciens, obsolètes ou peu puissants. Dépourvus de composants mécaniques mobiles, ils peuvent être plus économes et silencieux que des ordinateurs de bureau standards.

Le concept de base veut que toute machine ayant une carte réseau puisse être utilisée comme client léger.

Bon à savoir :

LTSP a été repensé et **réécrit à partir de zéro en 2019** afin de prendre en charge les nouvelles technologies telles que *systemd*, les environnements de bureau mis à jour, Wayland, UEFI, etc. Seule la nouvelle version est activement développée, tandis que l'ancienne s'appelle désormais LTSP5 et est en version minimale (mode de maintenance).

Pour cette raison, il est très difficile en 2022 de trouver des tutoriels qui fonctionnent ou de la documentation sur LTSP qui ne soit pas obsolète. Donc ne soyez pas étonnés si vous trouvez des articles ou tutos d'installation et de configuration complètement différents de ce qui est écrit dans ce document.

Par exemple les répertoires LTSP ont changé pour la conformité FHS :

- */opt/ltsp* est maintenant dans */srv/ltsp*
- */var/lib/tftpboot* est maintenant dans */srv/tftp*

Les fichiers de configuration ont également changé, et un seul fichier */etc/ltsp/ltsp.conf* gère désormais tous les paramètres client et serveur.

Le nouveau LTSP s'accompagne d'un nouvel objectif :

Linux Terminal Server Project aide à démarrer les clients LAN à partir d'un seul modèle d'installation qui réside dans une image de machine virtuelle ou un *chroot* sur le serveur LTSP, ou la racine du serveur (/, sans *chroot*). De cette façon, la maintenance de dizaines ou de centaines de clients sans disque est aussi simple que la maintenance d'un seul PC.

C'est-à-dire que l'accent est désormais mis sur la facilité d'entretien, et non sur le recyclage du vieux matériel.

Plus d'infos sur : https://github.com/ltsp/ltsp/discussions/268

2.10 Comment fonctionne un client léger LTSP ?

2.10.1 Réponse basique

Les clients légers se contentent de charger en mémoire un système d'exploitation réduit et de se connecter ensuite à un serveur. Les applications s'exécutent sur le serveur mais s'affichent sur l'écran de la station cliente.

2.10.2 Réponse technique

Séquence de démarrage (d'un point de vue du client léger) : la station cliente peut soit disposer d'un noyau sur un média de stockage local, soit le charger depuis le serveur au travers du réseau (en utilisant les instructions appropriées, il est possible de charger le noyau linux depuis un serveur au travers d'une carte réseau de démarrage. Ainsi, la station cliente n'a plus besoin de stocker quoi que ce soit, si ce n'est sur la mémoire vive de l'ordinateur.)

2.10.3 Séquence de démarrage

La carte réseau PXE[1] lance une requête DHCP[2] sur le réseau local. Le serveur DHCP répond en indiquant à la carte où se trouve le noyau Linux. Le noyau stocké dans */srv/tftp* (anciennement dans */var/lib/tftpboot*) est alors chargé au travers du réseau via le protocole TFTP[3].

Une fois le noyau chargé, il est exécuté, et la machine démarre sous Linux. *initramfs*[4] est chargé avec le noyau Linux et il est monté comme système de fichiers *root*. Ceci procure automatiquement les pilotes nécessaires pour la carte réseau, la souris, le clavier, etc… Une fois le pilote de carte réseau chargé en mémoire, une seconde requête DHCP fournit aux clients les informations comme l'adresse IP, le masque réseau, la passerelle, le serveur DNS[5] et le point de montage *root* NFS[6].

Le noyau Linux exécute *ubuntu initramfs* qui monte le système de fichiers *root* partagé du serveur sur la machine cliente, en lecture seule. La station cliente a donc alors un noyau Linux de démarrage, un système de fichiers *root*, comme un vrai système Linux. À partir de maintenant, quand nous parlerons du système de fichiers de la station client, il s'agira en fait du système de fichiers *root* du serveur monté en lecture seule. Le système de fichiers *root* monté par la station cliente est différent du système de fichiers *root* que le serveur utilise lui-même, mais il est conçu spécialement pour les stations clientes, et il est partagé entre toutes celles connectées au serveur (il est situé désormais sur le serveur dans le répertoire */srv/ltsp* et anciennement dans */opt/ltsp/<arch>*). *initramfs* appelle le programme

[1] Plus d'infos sur le PXE : https://fr.wikipedia.org/wiki/Preboot_Execution_Environment
[2] Plus d'infos sur le DHCP : https://fr.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
[3] Plus d'infos sur le TFTP : https://fr.wikipedia.org/wiki/Trivial_File_Transfer_Protocol
[4] Plus d'infos sur *initramfs* : https://www.fr.linuxfromscratch.org/view/blfs-svn/postlfs/initramfs.html
[5] Plus d'infos sur le DNS : https://fr.wikipedia.org/wiki/Domain_Name_System
[6] Plus d'infos sur le NFS : https://fr.wikipedia.org/wiki/Network_File_System

init[7], les paramètres du serveur X[8] sont autodétectés et les gestionnaires de connexion que l'on appelle *pamltsp* et *pwmerge* (anciennement *ldm* sous LTSP5*)* sont exécutés.

Une fois connecté, ils créent un tunnel SSH[9] et démarrent une session X sur le serveur avec affichage sur les stations clientes via le tunnel. L'utilisation de SSH procure des avantages : vous n'avez pas à configurer le serveur X sur la station cliente, et aucun transport de données par protocole TCP non sécurisé n'est initialisée, comme cela pouvait l'être auparavant avec LTSP.

3 Mise en place de l'infrastructure

Pour l'installation de LTSP je me suis basé principalement sur la documentation du site officiel (qui n'est pas complètement maintenu à jour en 2022) : https://ltsp.org/docs/installation/

3.1 Préparation de l'environnement du TP

Il y a des prérequis à avoir pour la réalisation de ce TP avant d'installer LTSP.

3.1.1 Configuration de l'hyperviseur VMware Workstation

Votre hyperviseur VMware Workstation a des réseaux virtuels qu'il appelle « vmnet ». Ces réseaux virtuels servent à y connecter les machines virtuelles créées via leur(s) interface(s) réseau (= NIC, « Network Interface Card »). Sachez que le changement de configuration de ces réseaux virtuels pourrait impacter la connectivité de vos VM précédemment crées.

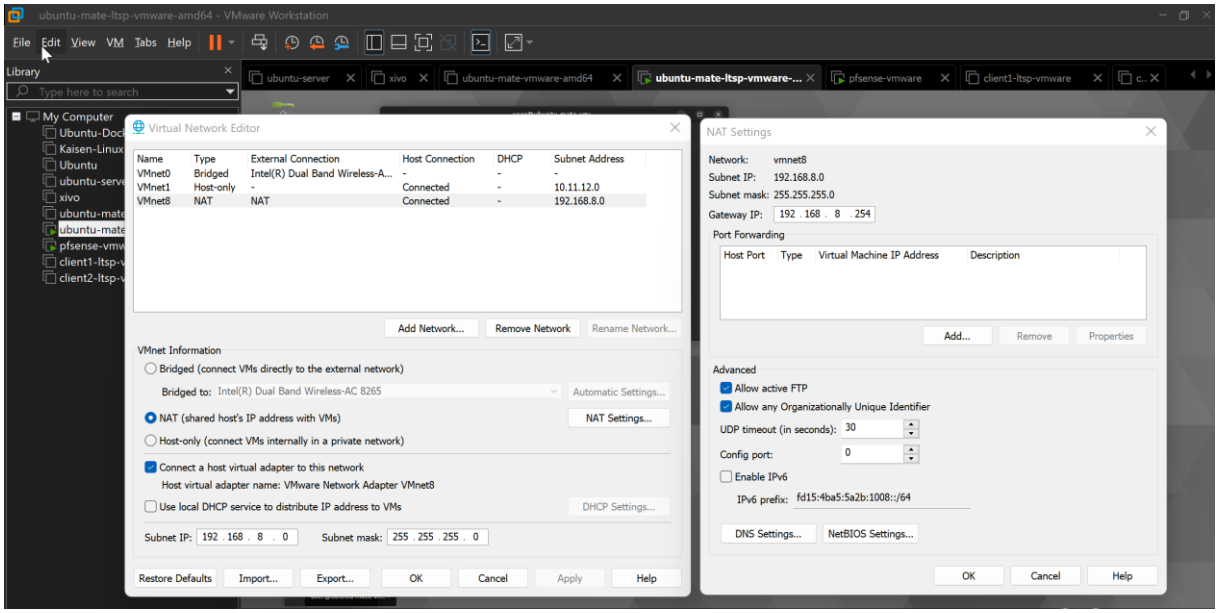
Par exemple : Disons que vous avez précédemment créé une VM, et que vous avez lié sa NIC au vmnet8 (NAT) qui est actuellement en 192.168.**100**.0/24. Vous avez attribué à cette même NIC une IP fixe en 192.168.**100**.**10**. Donc si vous modifiez le réseau virtuel vmnet8 en 192.168.**8**.0/24, la prochaine fois que vous démarrerez votre VM, sa NIC en 192.168.**100**.**10** ne sera pas dans le bon réseau. Il faudra donc faire une modification soit de l'IP de la NIC soit du réseau vmnet8.

Vous pouvez prendre la même configuration que moi pour plus de facilités ou bien vous pouvez adapter le TP à votre propre configuration. C'est vous qui voyez avec quelle solution vous êtes le plus à l'aise.

[7] Plus d'infos sur *init* : https://fr.wikipedia.org/wiki/Init
[8] Plus d'infos sur X : https://fr.wikipedia.org/wiki/X_Window_System
[9] Plus d'infos sur SSH : https://fr.wikipedia.org/wiki/Secure_Shell

Pour modifier la configuration réseau de votre hyperviseur, il faut aller dans le « Virtual Network Editor » :

- Mon réseau vmnet**8** (NAT) est en 192.168.**8**.0/24 et sa gateway (virtuelle) est en 192.168.8.254
- Mon réseau vmnet1 (host-only) est en 10.11.12.0/24 et il n'a pas de gateway (pour l'instant) puisque c'est un réseau isolé



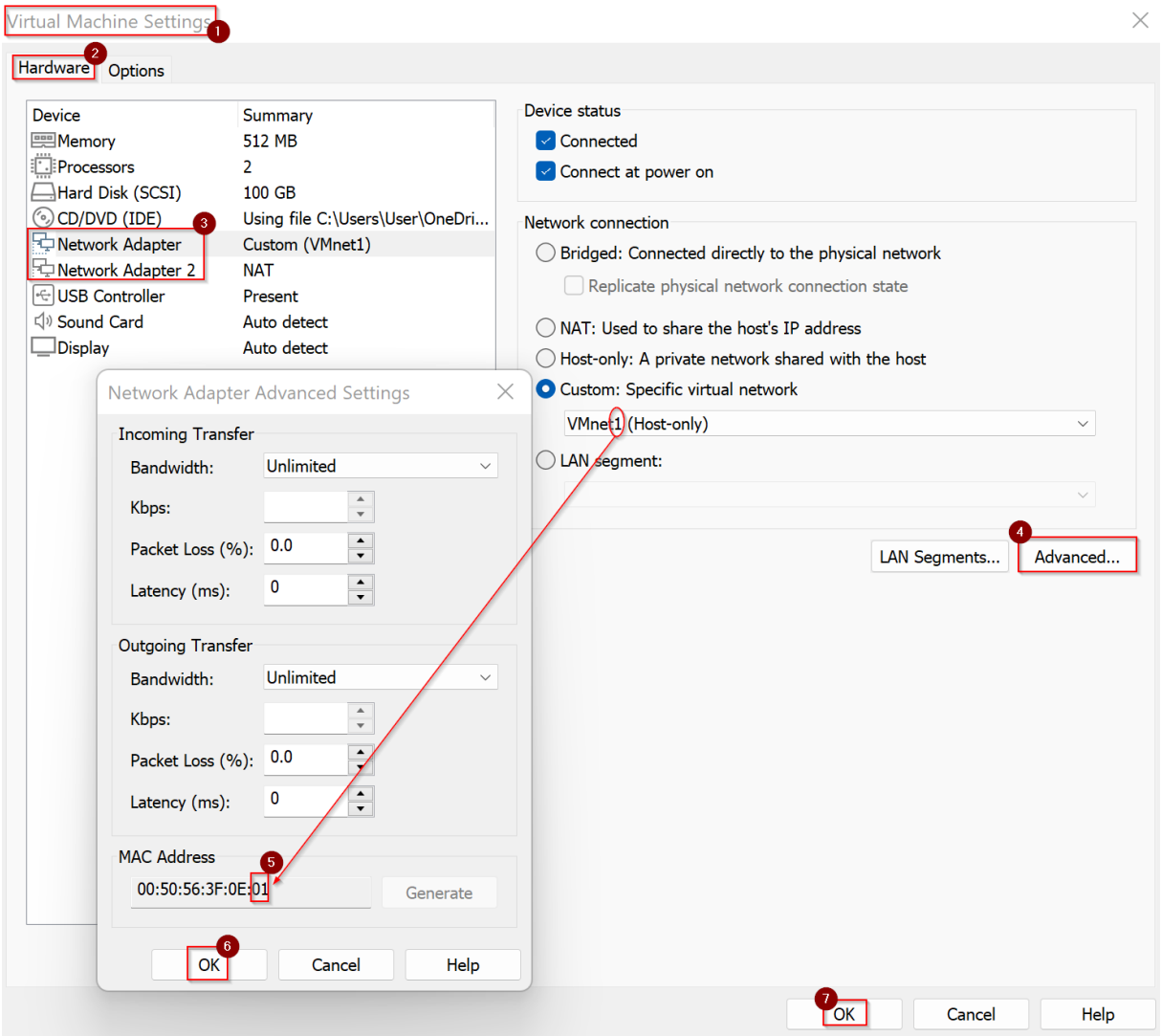
3.1.2 Installation d'un pfSense

Nous allons installer un routeur/pare-feu pfSense[10] qui sera aussi notre routeur, serveur DHCP et résolveur DNS local.

Directement lors de la création de la VM ou après en passant par les paramètres de la VM (menu « VM » puis « Settings… »), mettez sa première interface réseau dans le réseau virtuel vmnet1 (en host-only) et modifiez son adresse MAC en mettant un 01 à la fin pour l'identifier plus facilement dans pfSense et savoir qu'elle est dans le vmnet1.

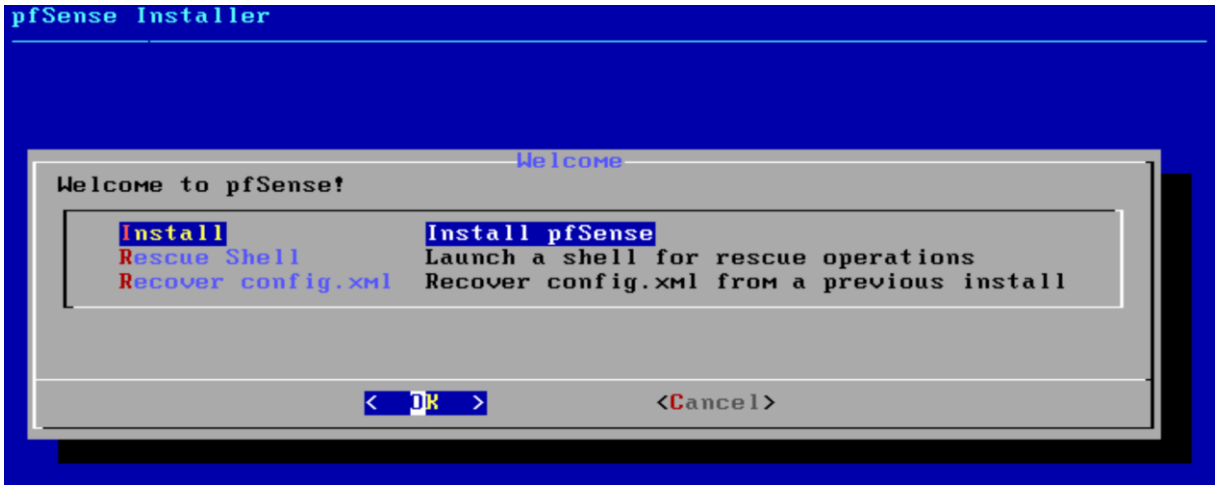
Puis ajoutez-lui une deuxième interface réseau dans le vmnet8 (en NAT) et modifiez son adresse MAC en mettant un 08 à la fin pour l'identifier plus facilement et savoir qu'elle est dans le vmnet8.

[10] Plus d'infos sur pfSense : https://fr.wikipedia.org/wiki/PfSense et http://labrat.fr/article/configuration-de-pfsense-ssh-dns-dhcp-parefeu-port-forwarding.html

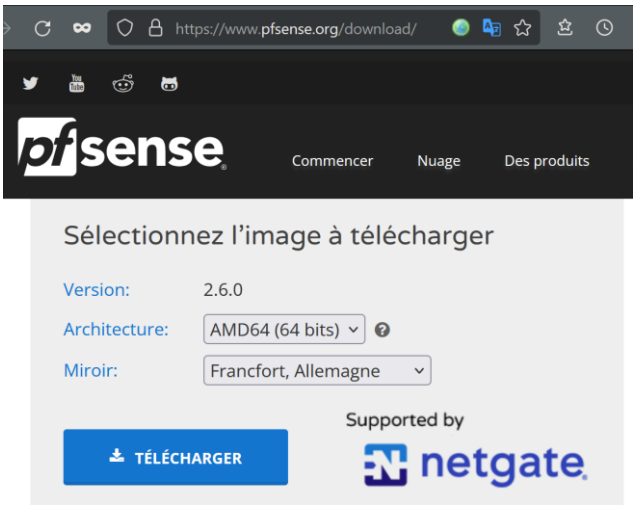


pfSense a besoin de deux NIC car en tant que firewall il a une interface qui a vocation à être vers l'extérieur (le WAN = le réseau mondial internet) et une autre vers le réseau local (le LAN = à protéger du monde extérieur).

Par défaut, quand il y a deux NIC, pfSense n'autorise l'accès à l'interface web d'administration que du côté LAN (= il voit la connexion entrer et il se dit « ça vient de chez moi donc c'est sûr, si ça ne vient pas de chez moi ce n'est pas sûr donc je bloque »). Par contre s'il n'y a qu'une seule NIC alors il sera possible par défaut de passer par l'interface WAN pour administrer pfSense.

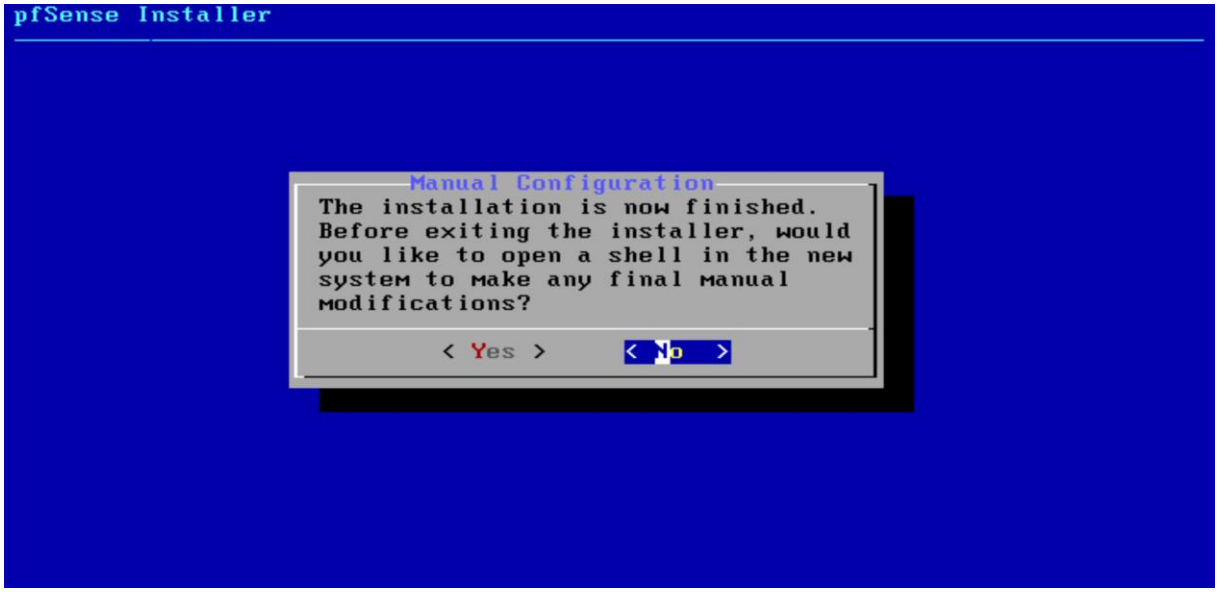


Téléchargez l'image .iso de la version « communautaire » ici : https://www.pfsense.org/download/



Créez votre VM, insérez l'image .iso dans le lecteur CD virtuel et lancez l'installation. Choisissez le clavier français puis appuyez sur la touche « Entrée » puis sélectionnez « Continue with fr.kbd keymap » puis validez avec la touche « Entrée » puis « Auto (ZFS) » puis « Entrée » puis « Install » puis « stripe » puis « Entrée » puis sélectionnez « da0 » avec « Espace » puis touche « Entrée » pour valider le « OK »

Puis « Yes » puis une fois l'installation terminée choisissez « No » puis « Reboot »



pfSense va démarrer et vous afficher une page ressemblant à celle-ci-dessous :

Prenez une capture d'écran en suivant la consigne précédemment donnée.

Mettre le clavier de la console pfSense en français (temporairement jusqu'au prochain redémarrage) :

Pour saisir les commandes pour la suite, il sera plus simple d'avoir un clavier français (sauf pour ceux qui ont un clavier US). Au menu principal de la console, faites le choix « 8) Shell » puis saisissez la commande :

```
kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.kbd
```

Vous devrez la taper manuellement donc sachez que :

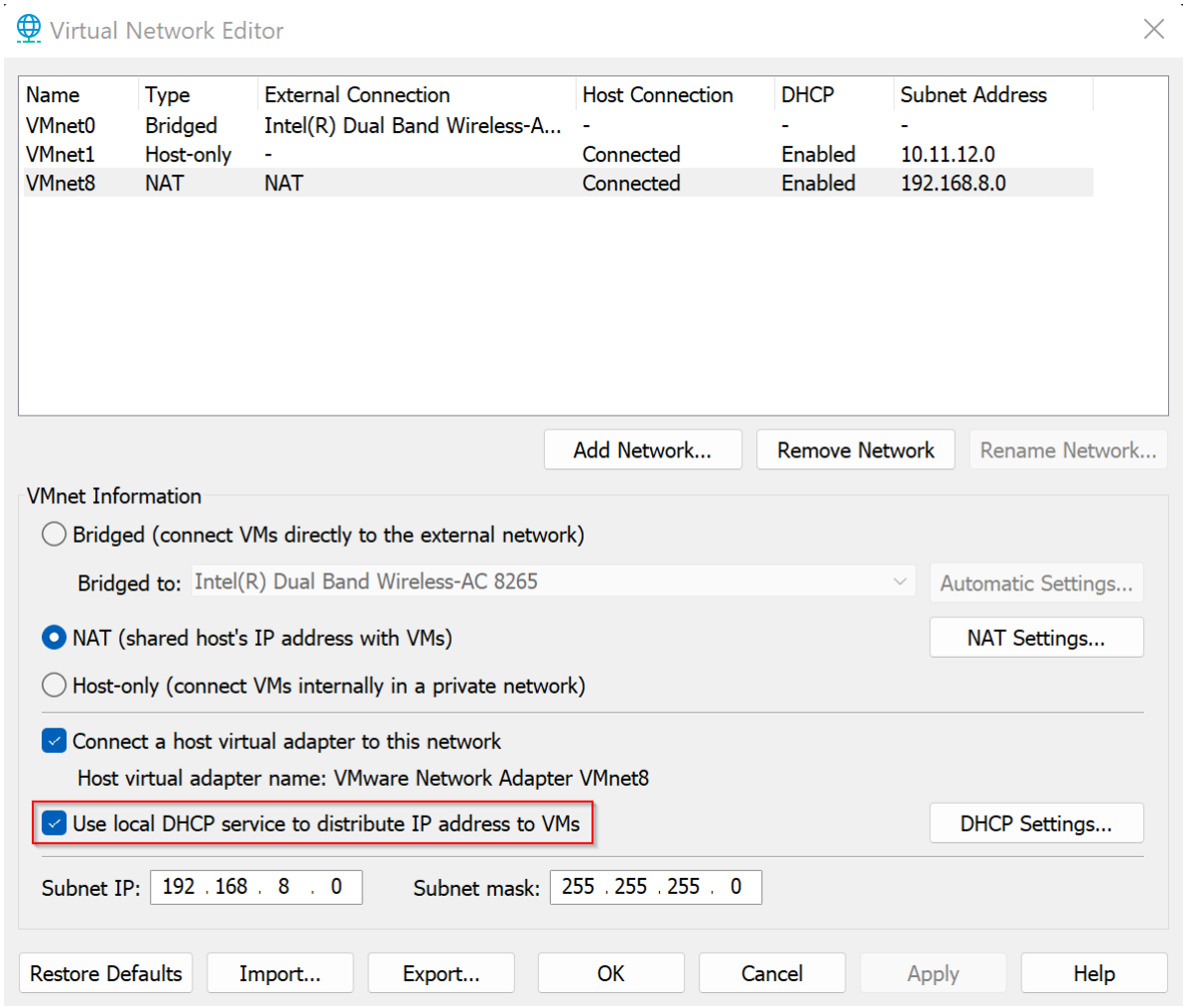
- pour faire le « - » il faut appuyer sur la touche «) »
- pour le « m » appuyez sur la touche « , »
- pour le « / » c'est « ! »
- pour le « a » c'est « q »
- pour le « . » c'est « : »

Vous remarquerez que son interface WAN est en 10.11.12.14 et que son interface LAN est en 192.168.1.1. Moi je voulais l'inverse (revoir mon schéma en début de document si besoin) : que son interface LAN soit dans le réseau vmnet1 host-only 10.11.12.13.0/24. Si vous êtes dans la même

situation que moi permutez les interfaces, en choisissant l'option « 1) Assign Interfaces », assignez les NIC à leur fonction (c'est à ce moment-là que le fait d'avoir mis 01 et 08 à la fin des adresses MAC se révèlera utile), et après vos modifications vous obtiendrez ce que vous voulez :

```
WAN (wan)       -> em1          -> v4/DHCP4: 192.168.8.6/24
LAN (lan)       -> em0          -> v4: 192.168.1.1/24
```

Je remarque que l'interface WAN est maintenant assignée au bon réseau et qu'elle a récupéré une IP automatiquement par DHCP (le service DHCP de ma « Livebox » à la maison). C'est normal car j'avais cette option activée dans les paramètres « Virtual Network Editor » de VMware Workstation :



Ensuite j'assigne une IP fixe à mes interfaces :

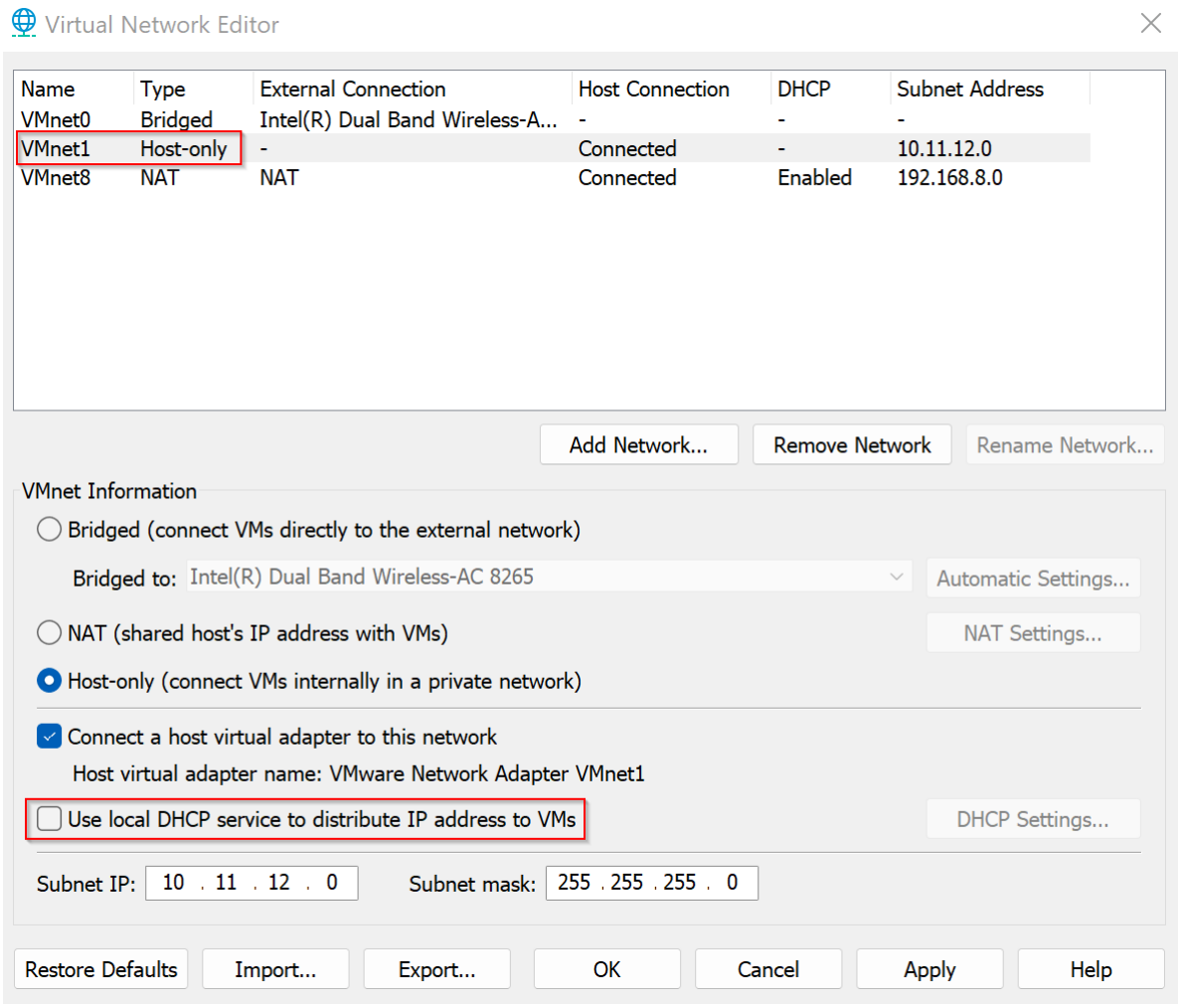
```
Enter an option: 2

Available interfaces:

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

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.11.12.254

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:
>
```

Sur l'interface LAN, à la question : « voulez-vous revenir à HTTP comme protocole du configurateur web ? » Répondez « oui » sinon vous ne pourrez pas accéder à l'interface web d'administration depuis votre navigateur. Répondez aussi « yes » à la question « est-ce que je veux activer le service DHCP sur l'interface LAN » (= dans mon réseau 10.11.12.0/24) et choisissez non pour l'interface WAN.

J'ai finalement assigné les IP statiques de mes 2 interfaces comme ceci :

```
WAN (wan)       -> em1       -> v4: 192.168.8.100/24
LAN (lan)       -> em0       -> v4: 10.11.12.254/24
```

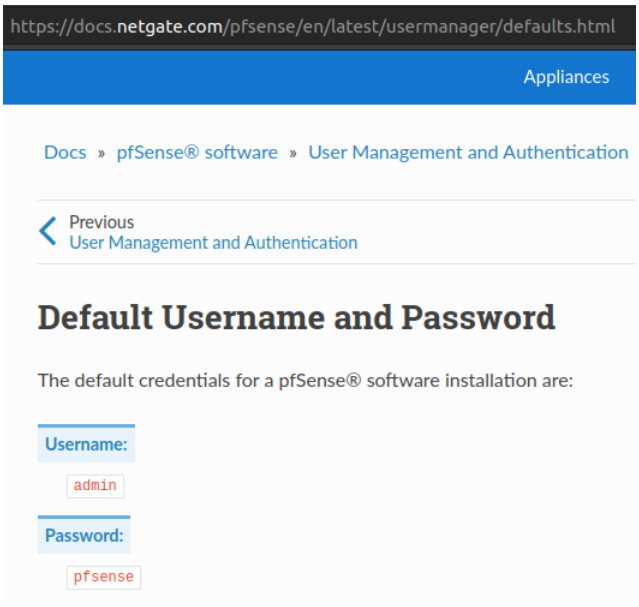
Et ensuite j'ai désactivé l'utilisation de mon DHCP local du côté de l'interface LAN dans les paramètres de VMware Workstation puisque que mon pfSense sera le serveur DHCP du réseau vmnet1 (host-only) :



Prenez une capture d'écran de vos interfaces WAN et LAN dans la console pfSense et de votre Virtual Network Editor en suivant la consigne précédemment donnée.

3.1.3 Configuration du pfSense

Depuis une machine sur le réseau LAN (vmnet1), ouvrez un navigateur internet et tapez l'IP de pfSense : dans mon cas c'est 10.11.12.254. Vous arrivez sur la page d'accueil du webConfigurateur (*webConfigurator* en anglais). Le login/mot de passe par défaut de pfSense est **admin**/**pfsense**.



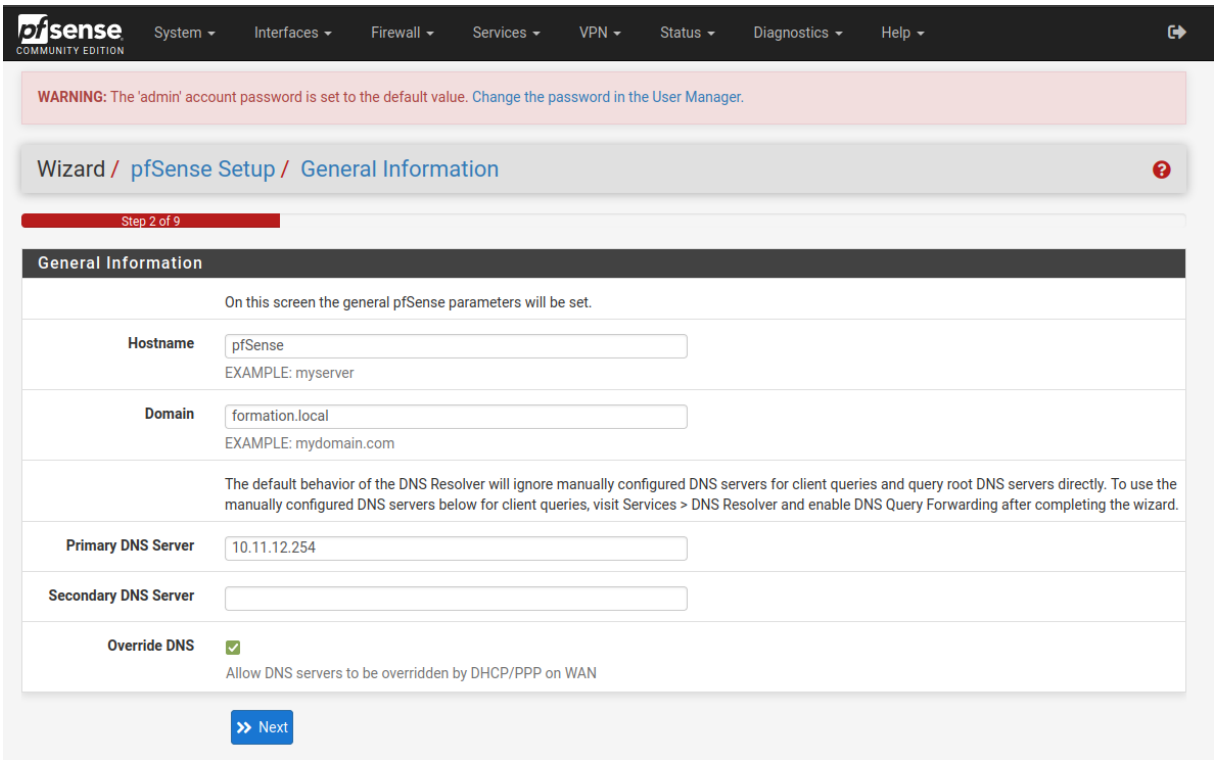
Autoriser temporairement la connexion du côté WAN :

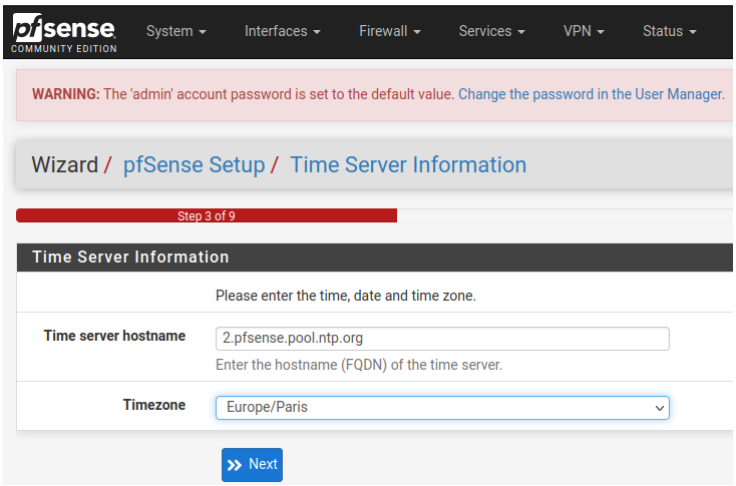
Si vous n'avez pas encore de machine sur le réseau LAN sachez que vous pouvez désactiver le firewall qui interdit la connexion sur l'interface de gestion web depuis le WAN entrez cette commande via le shell pfSense :

```
pfctl -d
```

Vous devriez alors avoir accès à l'interface de gestion web depuis le côté WAN. Essayez depuis un navigateur de votre machine physique.

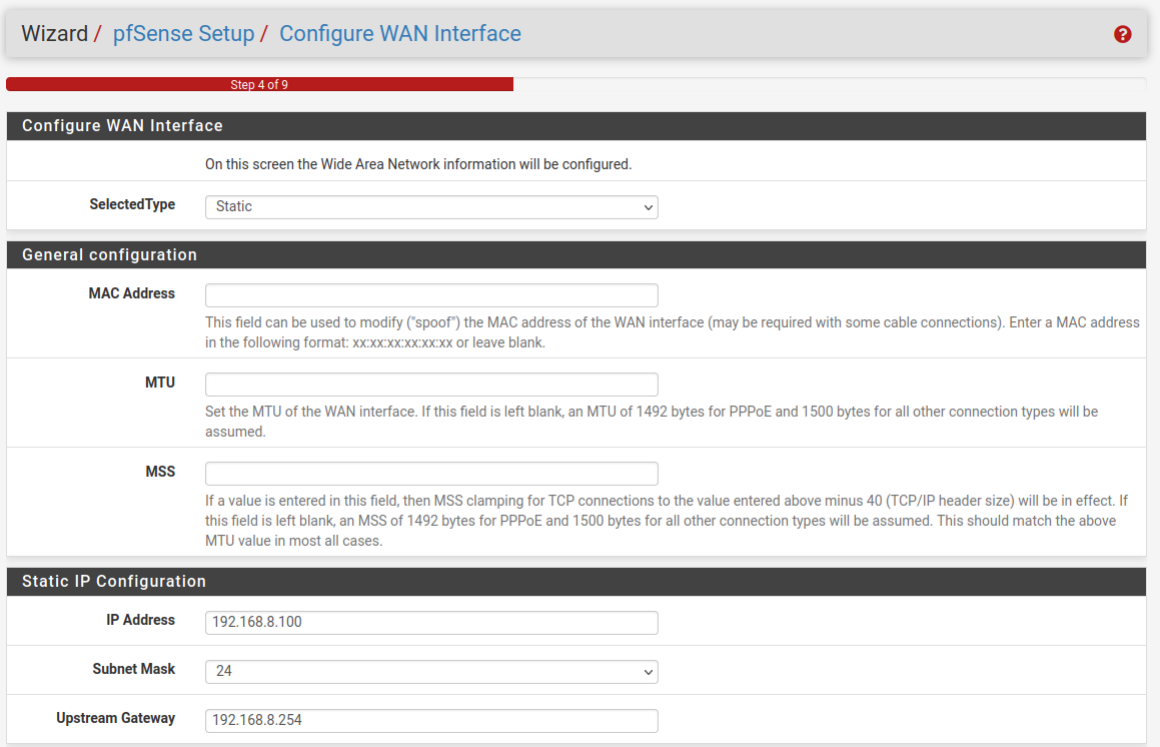
L'assistant de configuration démarre. Configurez le DNS, choisissez « formation.local » en nom de domaine (ou un autre comme « votre-prenom.tp » ou « lab.lan » par ex.) et mettez sa propre IP puisque pfSense va être le DNS :

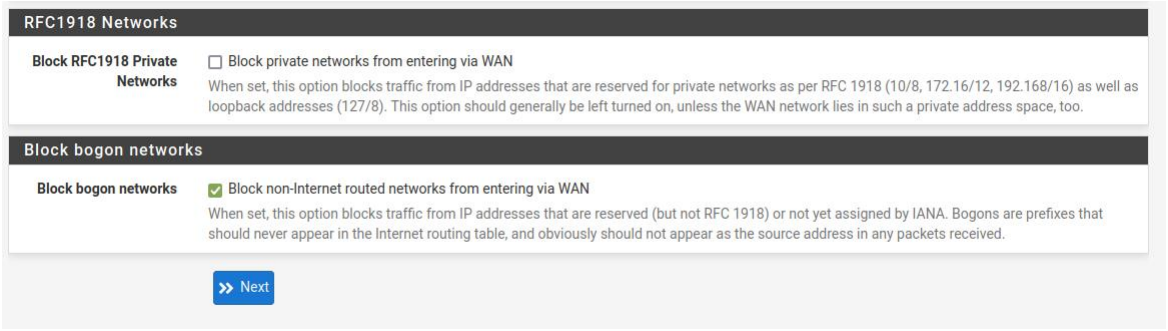


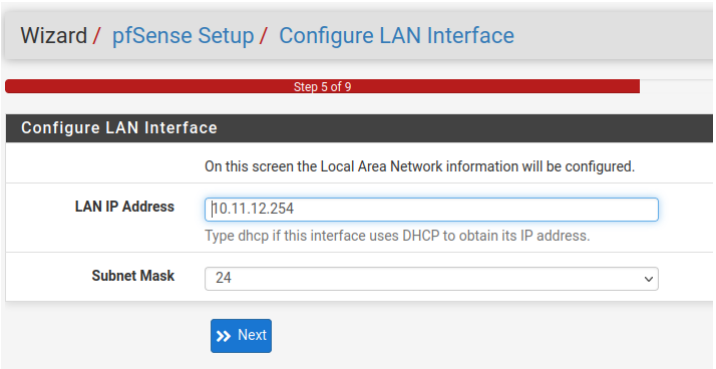


Laissez les options comme elles sont.

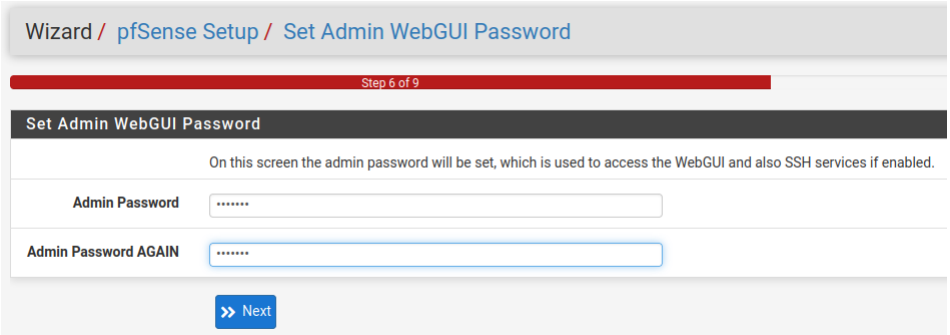
Comme l'interface WAN de notre routeur pfSense se situe sur un réseau privé, nous pouvons également désactiver la règle qui bloque le trafic depuis des adresses IP qui sont réservées pour les réseaux privés (tels que le mien en 192.168.8.0/24) en décochant l'avant-dernière case « Block RFC1918 Private Networks » tout en bas. Cela est à faire que si nous voulons accéder au pare-feu depuis son interface WAN. Evidemment, il ne faut pas faire cela en prod car ça laisserait une porte entrouverte à d'éventuels attaquants provenant de l'extérieur.

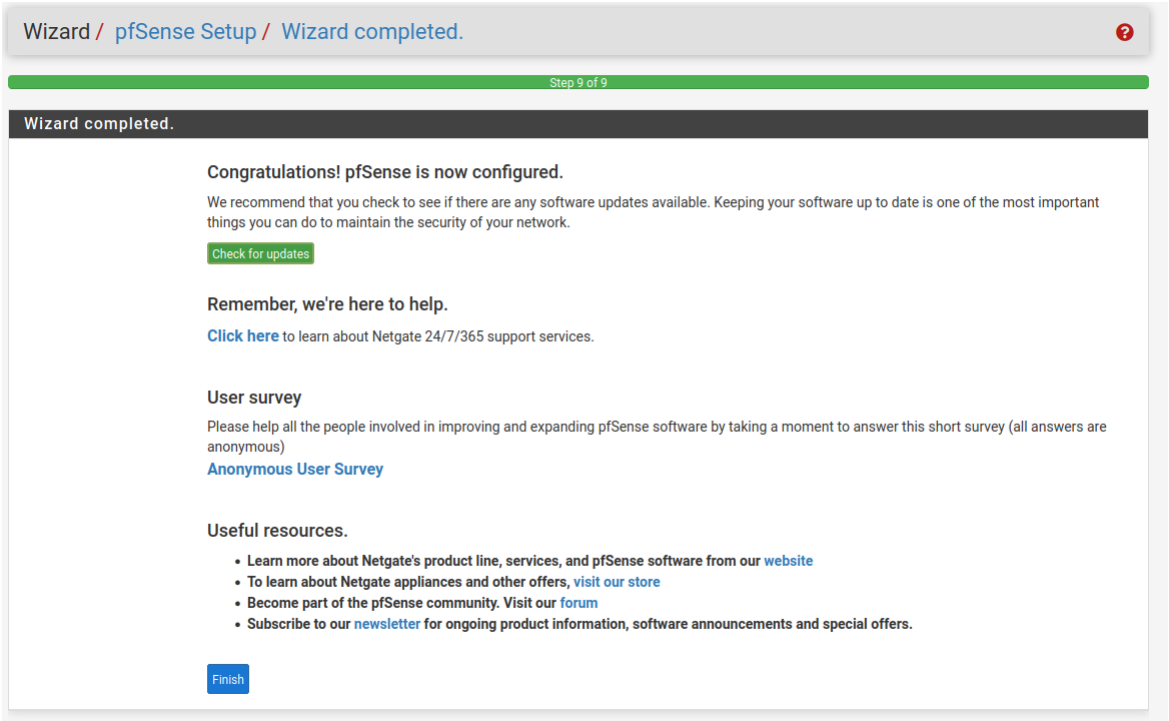






Mettez le mot de passe « 123-Pop » ou un autre si vous êtes sûr de ne pas l'oublier. Ce sera le nouveau mot de passe du compte « admin » (qui remplace donc le mot de passe par défaut « pfsense »).





Une fois l'assistant de configuration terminé, prenez une capture d'écran en suivant la consigne précédemment donnée.

Vous pouvez aussi mettre l'interface graphique en français dans « Système » et « Configuration générale » puis « Langue » dans la partie « Localisation ».

Mettre le clavier de la console pfSense en français (de façon définitive) :

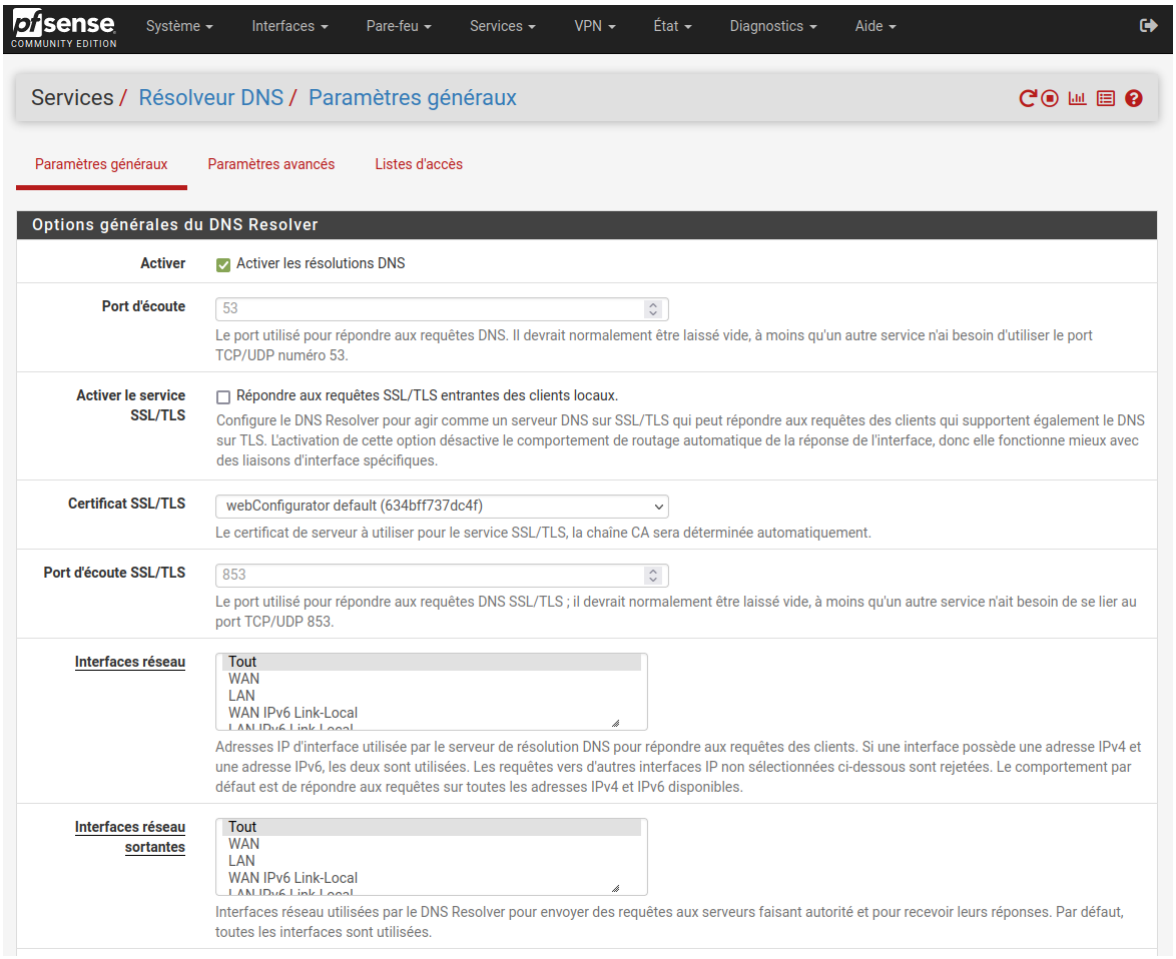
Changez la configuration du clavier de la console pfSense de façon pérenne en allant dans le menu « Système/System » puis « Gestionnaire de paquets/Package Manager » puis « Paquets disponibles » et installez le paquet « Shellcmd » (vous pouvez aussi en profiter pour installer le paquet « *open-vm-tools* »)

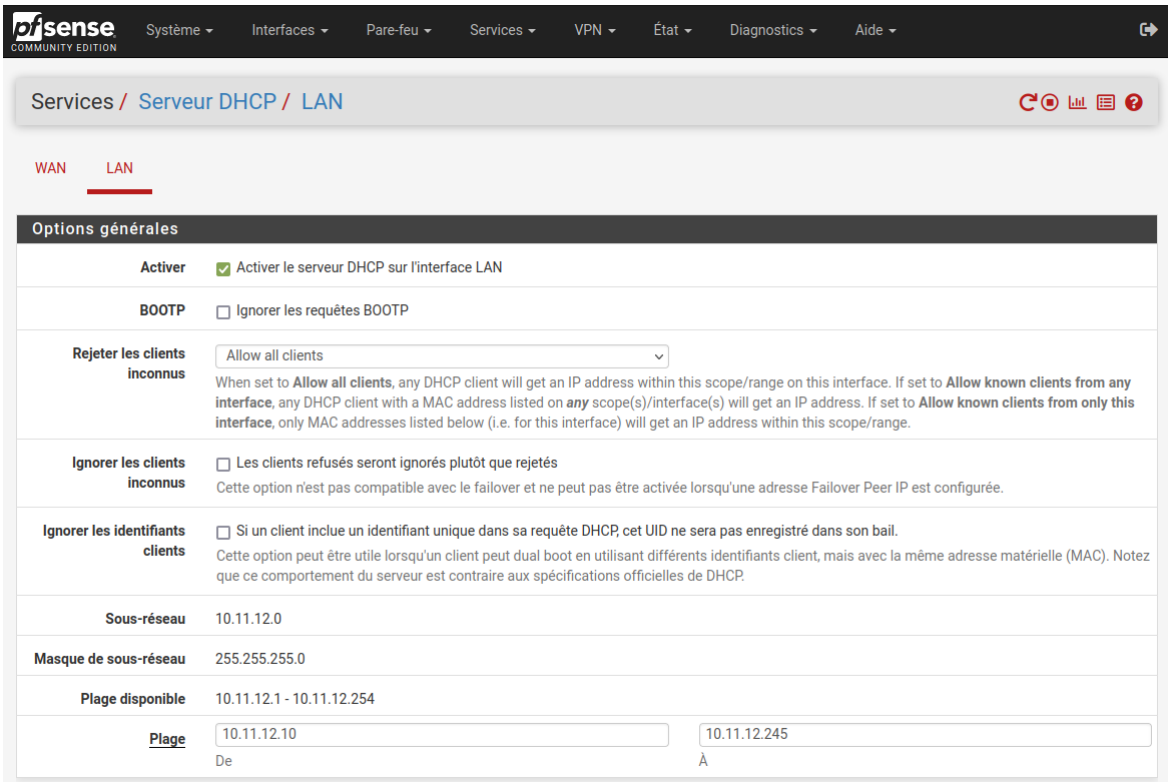
Sélectionnez ensuite « Services » dans le menu, puis « Shellcmd » puis « Ajouter » et remplissez les champs ainsi :

- Command : kbdcontrol -l /usr/share/syscons/keymaps/fr.iso.kbd
- Shellcmd Type : shellcmd
- Description : clavier azerty

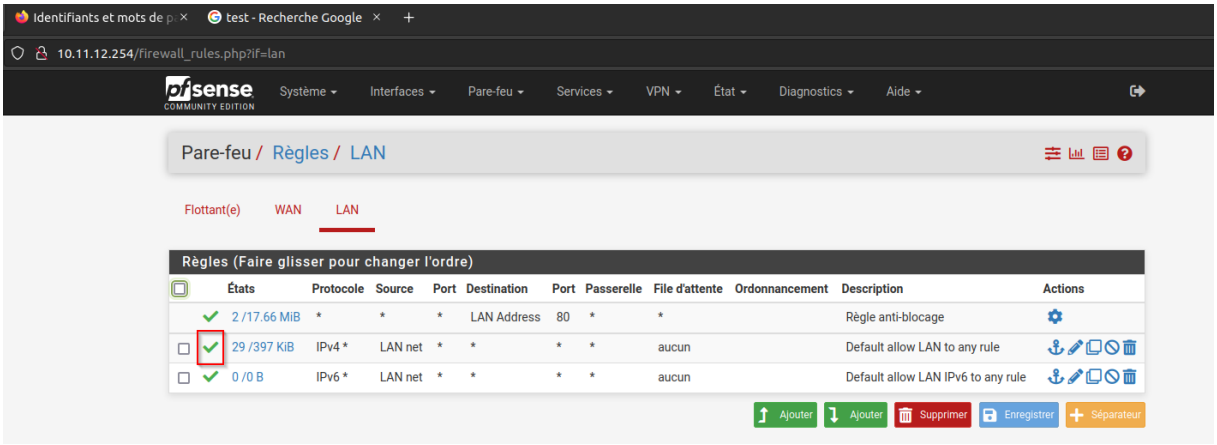
Au prochain redémarrage, la console utilisera le clavier français.

Vous pouvez vérifier que les services DNS et DHCP sont bien actifs côté LAN :



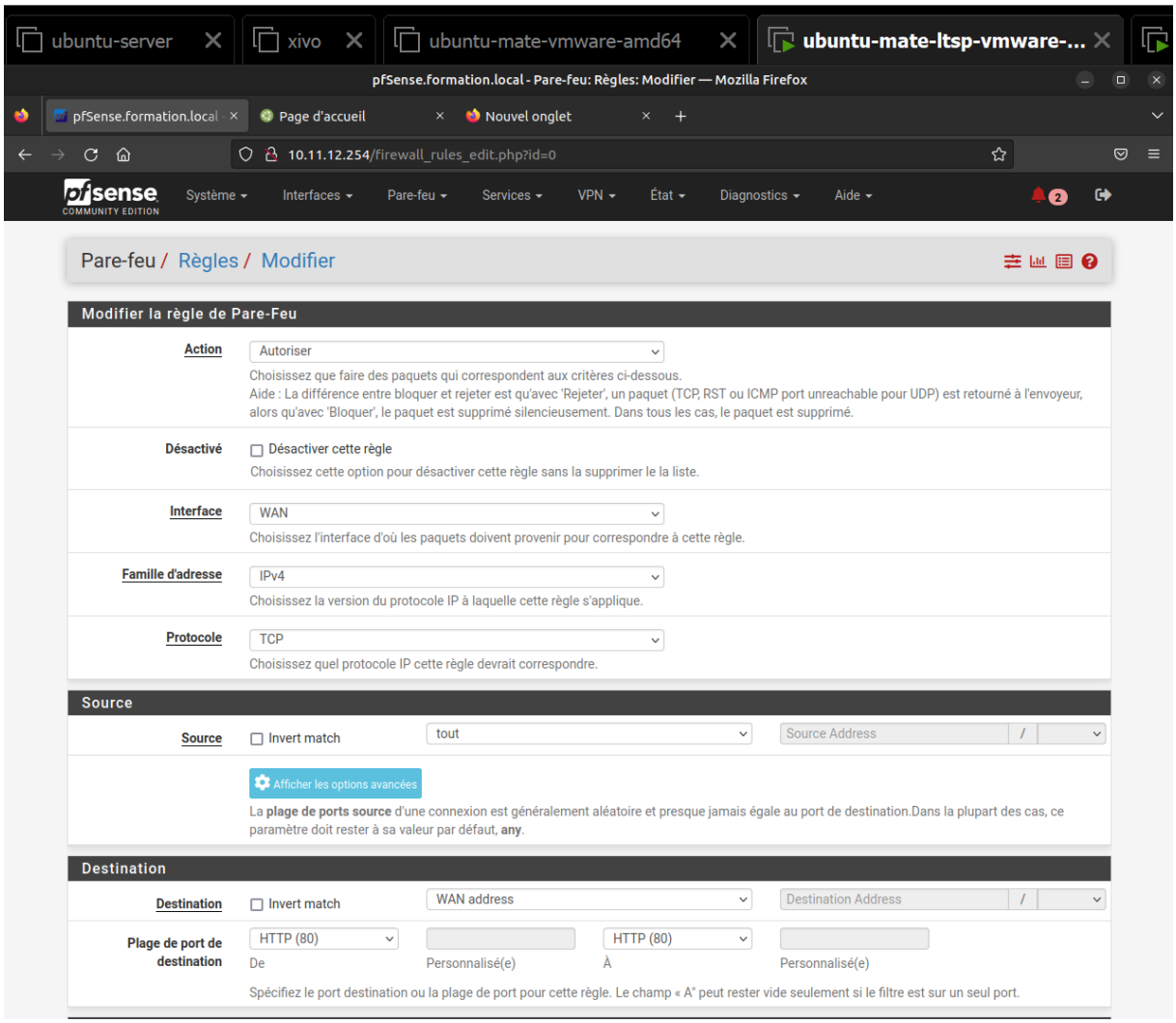


Vérifiez aussi que la règle de pare-feu pour autoriser les connexions du LAN est activée afin d'avoir un accès internet depuis le LAN.

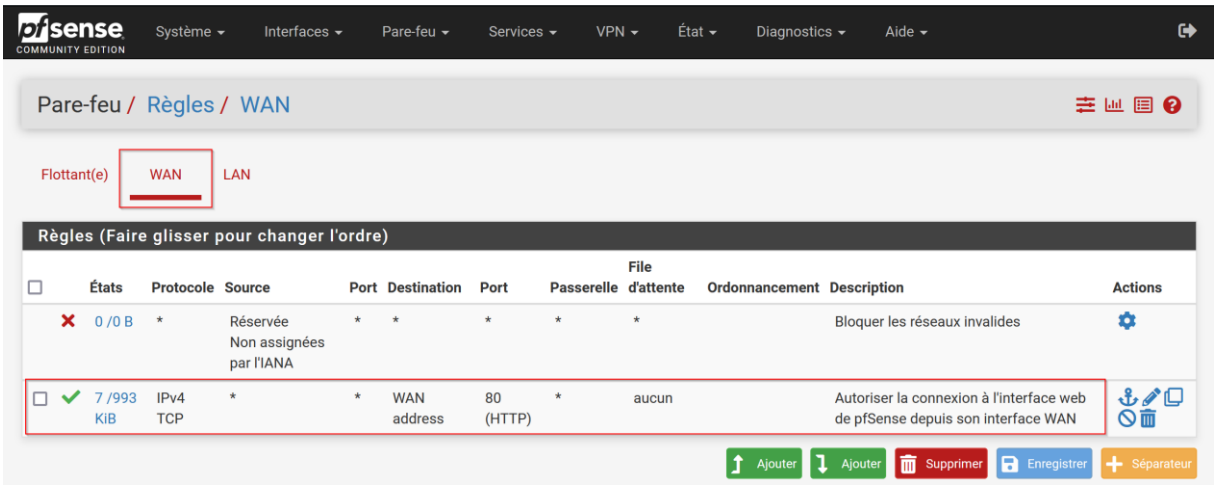


Si vous voulez autoriser la connexion à pfSense depuis votre machine physique sur son interface WAN dans votre réseau vmnet8 en 192.168.8.0/24, il va falloir créer une règle de pare-feu qui va permettre l'accès à l'interface web via l'interface WAN.

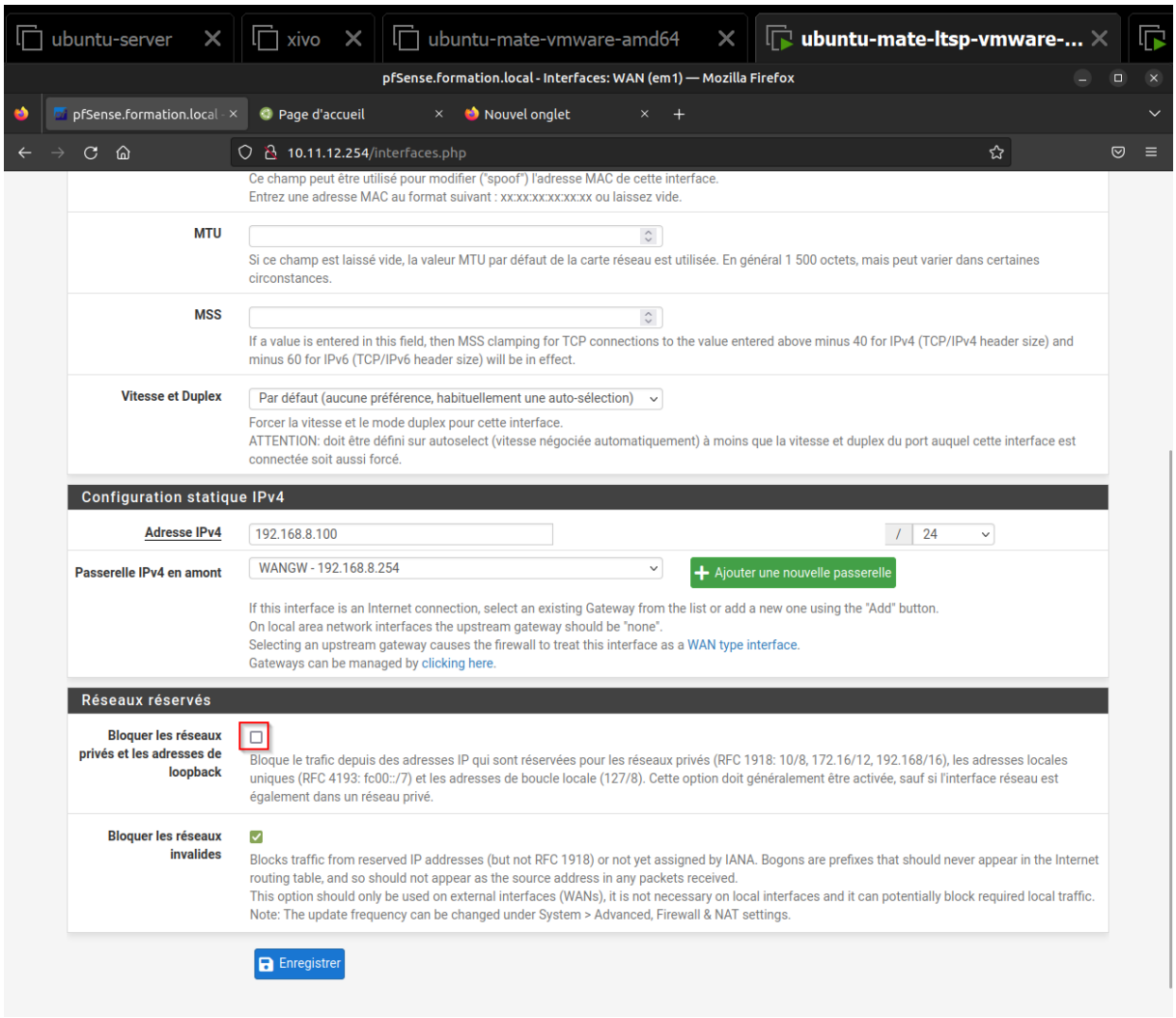
Allez dans « Pare-feu/Firewall », puis « Règles/Rules », sélectionnez l'interface « WAN », cliquez sur « Ajouter/Add » pour ajouter une nouvelle règle de filtrage. Il y a deux boutons « Ajouter » car le pare-feu applique les règles de haut en bas. Définir l'« Action » sur « Autoriser/Pass », l'« Interface » sur « WAN », la « Famille d'adresse/Address Family » sur « IPv4 », le « Protocole/Protocol » sur « TCP », la « Source » sur « tout/any » (il est possible de limiter l'accès à un hôte ou à un réseau), la « Destination » sur « WAN address », la « Plage de port de destination/Destination port range » sur « HTTP (80) ».



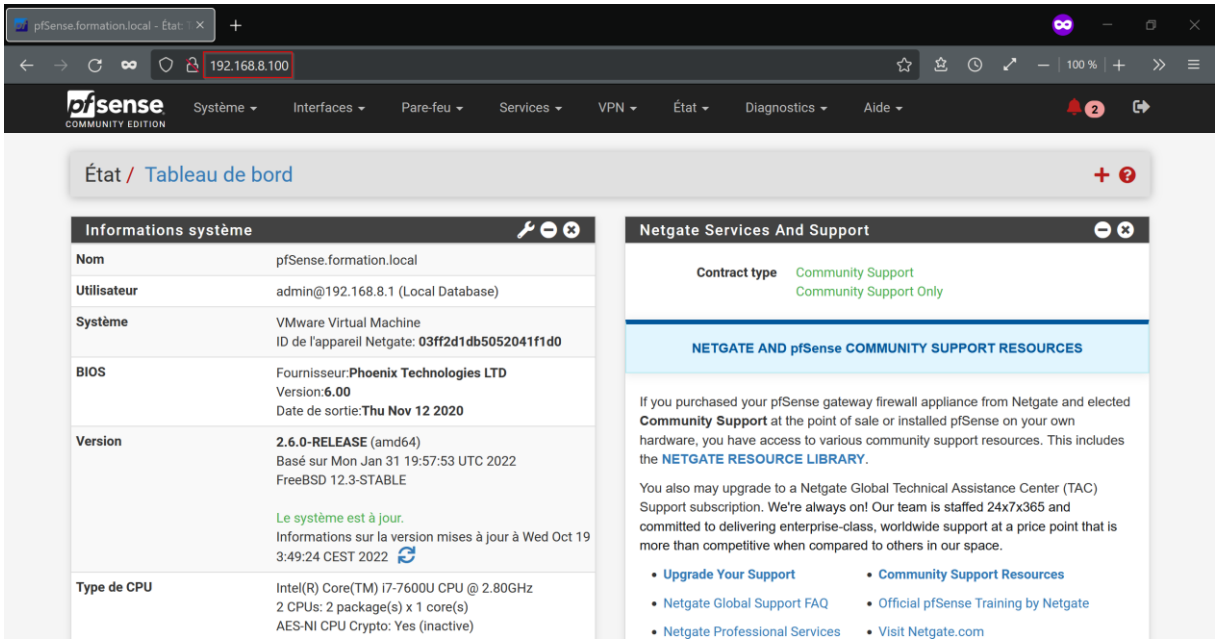
Cliquez ensuite sur « Enregistrer/Save » et enfin « Appliquer les modifications/Apply Changes » pour prendre en compte la modification du pare-feu. Votre nouvelle règle est désormais active. Si vous voulez un jour la désactiver il faudra cliquer sur la coche verte (la règle deviendra grisée) puis cliquer sur « Appliquer les modifications ».



Et bien sûr pour que la règle fonctionne, il faut que vous ayez décoché la case « Block RFC1918 Private Networks » mentionnée lors de la configuration initiale un peu plus haut. Si vous ne l'avez pas fait, allez dans « Pare-feu/Firewall » puis « Règles/Rules » choisissez l'interface « WAN » puis éditez la règle « Bloquer les réseaux invalides/Block private networks » en cliquant sur la roue crantée de la colonne « Actions » puis décochez la case « Bloquer les réseaux privés et les adresses de loopback /Block private networks and loopback addresses » puis appliquez les changements.



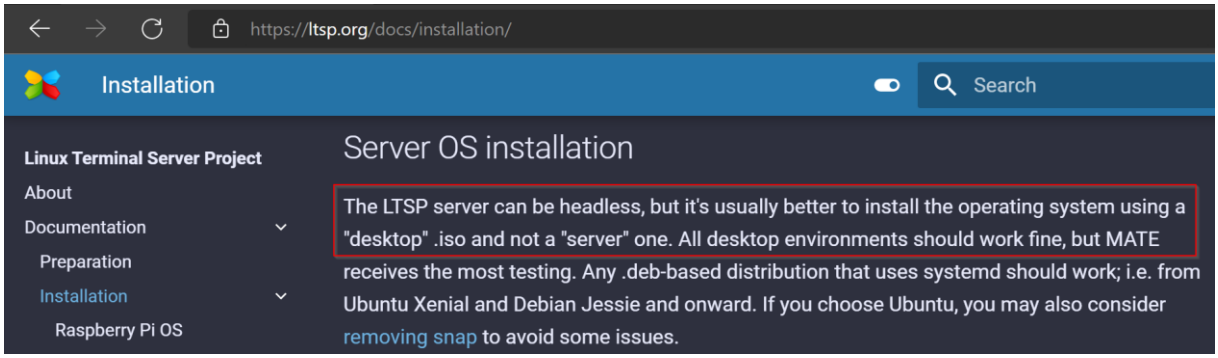
Ensuite essayez de vous connecter à pfSense du côté WAN depuis votre machine hôte :



3.2 Prérequis

3.2.1 Installation de l'OS du serveur LTSP

La documentation officielle recommande d'installer le serveur LTSC sur un système avec interface graphique (version de bureau ou « desktop ») et mentionne que le bureau MATE est celui qui a reçu le plus de tests.



Logiciel headless ? Serveur headless ?

Un **logiciel *headless*** « sans tête » (par exemple "Java headless" ou "Linux headless") est un **logiciel capable de fonctionner sur un appareil sans interface utilisateur graphique (GUI)**.

Un **serveur *headless*** est un **ordinateur sans moniteur, clavier, souris ou autres périphériques**.

Nous allons installer la distribution GNU/Linux[11] « Ubuntu » dans sa version « 22.04 LTS » et avec le bureau « MATE » téléchargeable ici : https://cdimage.ubuntu.com/ubuntu-mate/releases/22.04/release/ubuntu-mate-22.04.1-desktop-amd64.iso

Bon à savoir : un problème de non-affichage du bureau par le client léger juste après la connexion de l'utilisateur est déjà arrivé avec le bureau Gnome par défaut d'Ubuntu. La solution trouvée avait été d'ajouter de la RAM au client (en effet, Gnome exige un minimum de 2 Go de RAM pour fonctionner) mais gardez à l'esprit que si vous choisissez un autre bureau que MATE il est possible que vous rencontriez des problèmes non répertoriés dans ce document.

[11] Pour plus d'infos sur les distributions GNU/Linux : https://fr.wikipedia.org/wiki/Distribution_Linux et https://fr.wikipedia.org/wiki/Liste_des_distributions_GNU/Linux

Je ne détaillerai pas les étapes de création de VM et d'installation d'Ubuntu dans ce document car vous êtes censés savoir le faire. Faites cela en autonomie mais n'hésitez pas à me solliciter en cas de difficulté ou questionnement.

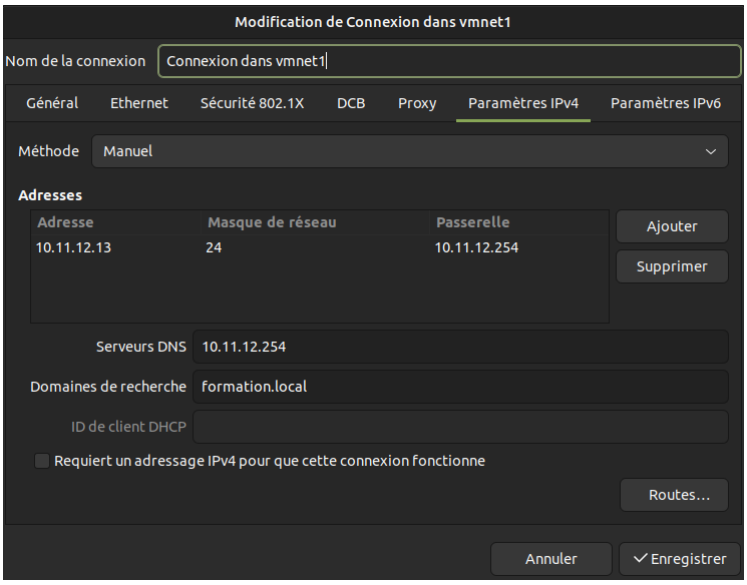
Mettez à votre VM 2 processeurs, 4 Go de RAM, et mettez son interface réseau dans le vmnet1.

IMPORTANT : Nommez votre utilisateur par votre prénom (par exemple « nicolas ») et nommez votre machine en incluant aussi votre prénom, par exemple : « ltsp-server-nicolas-vm ». Ça me permettra de vérifier l'authenticité de vos captures d'écran.

Prenez une capture d'écran en respectant la consigne précédemment donnée qui prouve que vous avez bien réussi à installer Ubuntu.

3.2.2 Passer l'IP en statique

Comme notre distribution possède une interface graphique, il faut changer la configuration réseau avec le gestionnaire de réseau graphique (qu'on appelle généralement le « network manager »). En effet, modifier la configuration réseau en ligne de commande (via *netplan* pour Ubuntu) alors que le gestionnaire graphique est installé sur la machine pourrait amener à un futur écrasement automatique de la configuration réseau du *netplan* par le network manager. Tapez « Configuration réseau avancée » dans la barre de recherche du menu pour trouver le network manager.



Faites cela puis prenez une capture d'écran en respectant la consigne précédemment donnée.

IMPORTANT : ne choisissez pas la première IP (10.11.12.1) car cela pourrait vous causer des problèmes par la suite.

3.2.3 Passer en mode admin

Dans ce cadre pédagogique nous allons passer en mode super-utilisateur *root*[12] pour plus de facilité mais il est important de rappeler qu'en production il faut plutôt utiliser un compte utilisateur standard avec des droits limités qui pourra si besoin utiliser la commande *sudo*[13] pour obtenir les droits de l'utilisateur *root*.

```
sudo su
```

3.2.4 [Facultatif] Suppression du système de packages Snap

D'après le site officiel, LTSP fait de son mieux pour supporter *snap* le nouveau format de paquets d'Ubuntu sujet à polémiques, mais parfois certains problèmes qui ne peuvent pas être résolus du côté de LTSP surviennent à cause de *snap*, par exemple gaspiller de la RAM dans les sessions live ou bien NFS home ne fonctionne pas.

Vous pouvez donc supprimer *snap* par précaution si vous voulez éviter d'éventuels messages d'erreurs et blocages qui vont vous faire perdre du temps. Pour cela ouvrez un terminal, tapez *sudo su* pour devenir *root*, puis copiez/collez tout le code suivant :

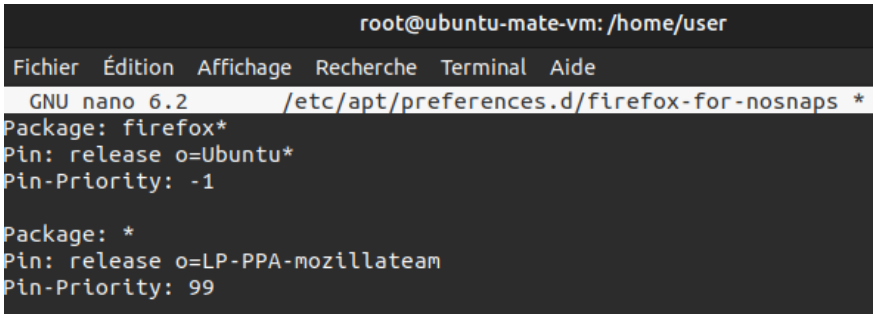
```
test -x /usr/bin/snap || exit 0
if [ -f /var/lib/snapd/desktop/applications/firefox_firefox.desktop ] &&
    [ ! -L /var/lib/snapd/desktop/applications/firefox_firefox.desktop ]; then
    snapff=1
fi
packages=$(dpkg -l ayatana-indicator-application indicator-application mate-hud
snapd 2>/dev/null | awk '/^ii/ { print $2 }')
apt-get purge --yes --auto-remove $packages
if [ "$snapff" = 1 ]; then
    # If firefox snap was installed, replace it with the .deb from the PPA
    add-apt-repository --yes ppa:mozillateam/ppa
    echo 'Package: *
Pin: release o=LP-PPA-mozillateam
Pin-Priority: 1001' >/etc/apt/preferences.d/60mozillateam-ppa
```

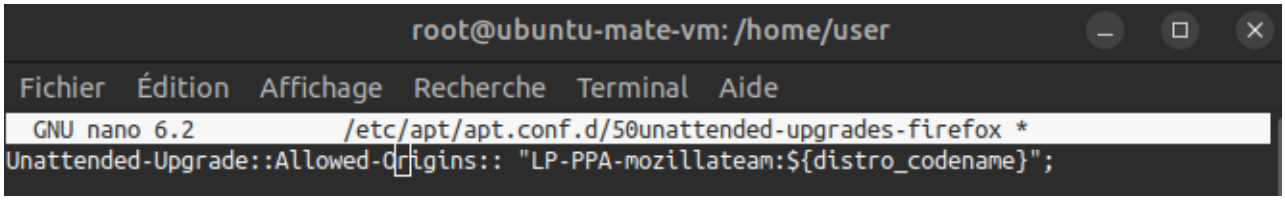
[12] Plus d'info sur *root* : https://fr.wikipedia.org/wiki/Utilisateur_root
[13] Plus d'infos sur *sudo* : https://fr.wikipedia.org/wiki/Sudo et https://www.sudo.ws/about/intro/ (site officiel)

```
    # If you need more locales e.g. firefox-locale-el add them in this line
    apt-get install --yes firefox firefox-locale-en
    # Work around https://bugs.launchpad.net/bugs/1967736
    if [ -f /usr/share/mate/applications/firefox.desktop ]; then
        dpkg-divert --package sch-scripts --divert \
            /usr/share/mate/applications/firefox-desktop.diverted \
            --rename /usr/share/mate/applications/firefox.desktop
        if [ ! -e /var/lib/snapd/desktop/applications/firefox_firefox.desktop ]
        then
            mkdir -p /var/lib/snapd/desktop/applications
            ln -s /usr/share/applications/firefox.desktop \
                /var/lib/snapd/desktop/applications/firefox_firefox.desktop
        fi
    fi
fi
```

En cas de difficulté pour coller le texte dans le terminal sachez que vous pouvez le copier directement depuis le site de LTSP : https://ltsp.org/guides/snap/

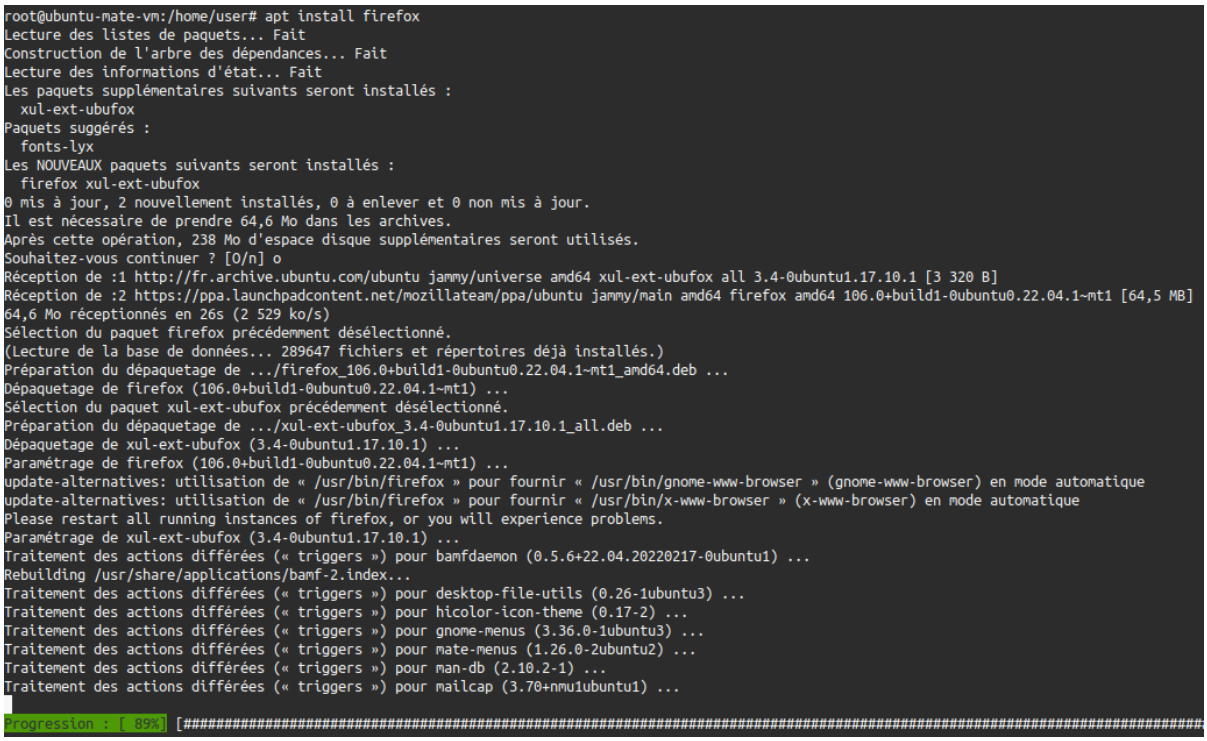
La désinstallation de *snap* a fonctionné mais ça a aussi désinstallé le navigateur Firefox qui était installé par défaut en *snap*. Il faut donc le réinstaller afin que nos futurs utilisateurs du système Ubuntu en client léger puissent utiliser un navigateur sur leur machine. Mais comme Ubuntu impose le format *snap* avec la commande *apt install firefox* il faut trouver le moyen de réinstaller Firefox sans devoir réinstaller *snap*. Nous allons suivre ce rapide tutoriel : https://www.linuxtricks.fr/wiki/ubuntu-installer-firefox-en-deb-plutot-que-snap





Une fois les quelques modifications effectuées nous pouvons réinstaller Firefox depuis les dépôts de la fondation Mozilla avec la commande :

```
apt install firefox
```



Faites cela puis prenez une capture d'écran lors de la réinstallation de Firefox, similaire à celle-ci-dessus, tout en respectant la consigne précédemment donnée.

3.3 Installation et configuration de LTSP

3.3.1 Qu'est-ce qu'un PPA ?

Tout d'abord il faut comprendre comment fonctionne les systèmes de paquets logiciels sous les distributions GNU/Linux. Prenons l'exemple d'Ubuntu. L'installation des logiciels sous Ubuntu est différente de celle sous Mac ou Windows ; certains pourraient dire *mieux.* Plutôt que d'aller sur le web pour télécharger un paquet, il est généralement préférable de consulter « Boutique de logiciels », l'application graphique de gestion des logiciels d'Ubuntu (ou encore d'utiliser le gestionnaire de paquets *apt* qui fait la même chose en version non graphique) pour tout programme que vous souhaiteriez installer. Le logiciel voulu est stocké dans un *référentiel*, qui est une collection de logiciels que Ubuntu peut télécharger rapidement et facilement. Les référentiels sont un moyen plus fiable de télécharger des logiciels que de récupérer des fichiers .exe sur des sites web suspects et non-officiels. Puisque tout ce qui se trouve dans les dépôts est examiné par l'équipe d'Ubuntu, vous êtes

plus sûrs d'avoir des logiciels sains pour votre système. C'est un peu similaire au Play Store de Google pour les systèmes Android, ou à l'App Store d'Apple pour les iPhones, ou encore au Microsoft Store ou Chocolatey pour Windows.

Cela ne veut pas dire pour autant qu'il n'y a pas d'inconvénient… Les utilisateurs d'Ubuntu devront généralement attendre une nouvelle version d'Ubuntu (tous les 6 mois) pour essayer un nouveau logiciel.

Donc, si Firefox sort une mise à jour, vous ne pourrez peut-être pas jouer avec la nouvelle version avant la sortie de la prochaine version d'Ubuntu.

C'est là qu'interviennent les PPA. Un *dépôt personnel de paquets logiciels* ou *Personal Package Archives* (abrégés PPA) est **le dépôt de sources logicielles construit et publié par les développeurs et éditeurs d'un logiciel particulier**. Autrement dit : c'est une collection de logiciels non inclus dans Ubuntu par défaut.

Généralement, ces référentiels se concentrent sur un seul programme, mais ils peuvent en inclure plus en fonction de la personne qui les gère.

Quoi qu'il en soit, les PPA fournissent des mises à jour pour votre logiciel préféré à un rythme beaucoup plus rapide que Ubuntu lui-même. C'est super, car vous pouvez décider quel logiciel vous voulez garder à jour et laisser le reste à Ubuntu.

Une fois que vous installez un nouveau PPA, les mises à jour du logiciel inclus dans ce PPA viendront à vous via le gestionnaire de mise à jour d'Ubuntu.

C'est fantastique, car cela signifie que toutes vos mises à jour passent par une seule interface. Pas de pop-ups à la Windows qui s'affiche quand une nouvelle version du programme sort !

3.3.2 Ajout du dépôt de sources logicielles (PPA) de LTSP

Le PPA de LTSP est donc l'endroit où les versions stables de LTSP sont publiées.

Les versions LTSP stables sont proposées au format de package .deb dans le PPA de LTSP. Ils devraient fonctionner dans toutes les distributions basées sur .deb qui utilisent systemd, c'est-à-dire à partir de Debian Jessie 8 et Ubuntu Xenial 16.04 et versions ultérieures.

L'ajout du PPA de LTSP est recommandé car lorsque les clients démarrent sur le réseau, *ltsp init* configure dynamiquement de nombreux autres packages, tels que *systemd*, *network-manager*, *display*

managers, *netplan*, etc. Parfois, les mises à jour de distribution normales desdits packages interrompent le processus de démarrage réseau, et des mises à jour LTSP urgentes fournies par le PPA sont nécessaires pour le réparer. Pour ajouter le PPA et mettre à jour la liste des paquets disponibles lancez ces deux commandes :

```
add-apt-repository ppa:ltsp
apt update
```

Vous devriez avoir cette sortie :

```
user@ubuntu-mate-vm:~$ sudo su
root@ubuntu-mate-vm:/home/user# add-apt-repository ppa:ltsp
apt update
Dépôt : « deb https://ppa.launchpadcontent.net/ltsp/ppa/ubuntu/ jammy main »
Description :
LTSP stable releases for Ubuntu and Debian based distributions.
Documentation: https://ltsp.org/docs/ppa
Plus d'informations : https://launchpad.net/~ltsp/+archive/ubuntu/ppa
Ajout du dépôt.
Appuyez sur [ENTRÉE] pour continuer ou Ctrl-c pour annuler
Adding deb entry to /etc/apt/sources.list.d/ltsp-ubuntu-ppa-jammy.list
Adding disabled deb-src entry to /etc/apt/sources.list.d/ltsp-ubuntu-ppa-jammy.list
Adding key to /etc/apt/trusted.gpg.d/ltsp-ubuntu-ppa.gpg with fingerprint 8A3246F8D6CF2B67C979C987B64988E8F9B7EF68
Atteint :1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Atteint :2 http://fr.archive.ubuntu.com/ubuntu jammy InRelease
Atteint :3 http://fr.archive.ubuntu.com/ubuntu jammy-updates InRelease
Atteint :4 http://fr.archive.ubuntu.com/ubuntu jammy-backports InRelease
Réception de :5 https://ppa.launchpadcontent.net/ltsp/ppa/ubuntu jammy InRelease [18,0 kB]
Réception de :6 https://ppa.launchpadcontent.net/ltsp/ppa/ubuntu jammy/main i386 Packages [1 352 B]
Réception de :7 https://ppa.launchpadcontent.net/ltsp/ppa/ubuntu jammy/main amd64 Packages [1 352 B]
Réception de :8 https://ppa.launchpadcontent.net/ltsp/ppa/ubuntu jammy/main Translation-en [960 B]
21,7 ko réceptionnés en 2s (11,2 ko/s)
Lecture des listes de paquets... Fait
Atteint :1 https://ppa.launchpadcontent.net/ltsp/ppa/ubuntu jammy InRelease
Atteint :2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Atteint :3 http://fr.archive.ubuntu.com/ubuntu jammy InRelease
Atteint :4 http://fr.archive.ubuntu.com/ubuntu jammy-updates InRelease
Atteint :5 http://fr.archive.ubuntu.com/ubuntu jammy-backports InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
```

3.3.3 Installation des packages de serveur LTSP

La manière habituelle de transformer une installation normale en un serveur LTSP consiste à exécuter la commande ci-dessous :

```
apt install --install-recommends ltsp ltsp-binaries dnsmasq nfs-kernel-server
openssh-server squashfs-tools ethtool net-tools epoptes
```

Dans la commande suivante, remplacez « *administrator* » par votre nom d'utilisateur d'administrateur (mais ce n'est pas « root » qu'il faut mettre, par ex. moi c'est « user »):

```
gpasswd -a administrator epoptes
```

Description des paquets installés :

- *ltsp* : contient le code LTSP, il est commun aux serveurs LTSP et aux clients LTSP
- *ltsp-binaries* : contient les binaires iPXE et *memtest*
- *dnsmasq* : fournit les services TFTP et éventuellement DNS et DHCP ou proxyDHCP. Les alternatives possibles sont *isc-dhcp-server* et *tftpd-hpa*, mais seul *dnsmasq* peut faire le proxyDHCP, c'est donc la valeur par défaut recommandée
- *nfs-kernel-server* : exporte l'image disque du client virtuel via NFS
- *openssh-server* : permet aux clients de s'authentifier et d'accéder à */home* via SSHFS
- *ethtool*, *net-tools* : permet de désactiver le contrôle de flux Ethernet pour améliorer la vitesse du LAN lorsque le serveur est en gigabit et que certains clients sont à 100 Mbps
- *epoptes* : (facultatif) permet le suivi des clients à distance ; la commande *gpasswd* permet à l'administrateur système d'exécuter *epoptes*.

```
root@ubuntu-mate-vm:/home/user# apt install --install-recommends ltsp ltsp-binaries dnsmasq nfs-kernel-server openssh-server squashfs-tools ethtool net-tools epoptes
gpasswd -a [redacted] epoptes
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
ethtool est déjà la version la plus récente (1:5.16-1).
ethtool passé en « installé manuellement ».
Les paquets supplémentaires suivants seront installés :
  epoptes-client faketime iperf keyutils libevent-core-2.1-7 libfaketime libfltk-images1.3 libfltk1.3 libnfsidmap1 libtk8.6 libvncclient1 libvncserver1 ncurses-term nfs-common openssh-sftp-server
  python3-attr python3-automat python3-constantly python3-hamcrest python3-hyperlink python3-idna python3-incremental python3-openssl python3-pyasn1 python3-pyasn1-modules python3-service-identity
  python3-twisted python3-zope.interface rpcbind screen socat ssh-import-id sshfs tigervnc-viewer tk tk8.6 x11vnc
Paquets suggérés :
  resolvconf open-iscsi watchdog molly-guard monkeysphere ssh-askpass python-attr-doc python-openssl-doc python3-openssl-dbg python3-pampy python3-serial python3-tk python3-wxgtk4.0 byobu | screenie
  | iselect tigervnc-tools
Les NOUVEAUX paquets suivants seront installés :
  dnsmasq epoptes epoptes-client faketime iperf keyutils libevent-core-2.1-7 libfaketime libfltk-images1.3 libfltk1.3 libnfsidmap1 libtk8.6 libvncclient1 libvncserver1 ltsp ltsp-binaries ncurses-term
  net-tools nfs-common nfs-kernel-server openssh-server openssh-sftp-server python3-attr python3-automat python3-constantly python3-hamcrest python3-hyperlink python3-idna python3-incremental
  python3-openssl python3-pyasn1 python3-pyasn1-modules python3-service-identity python3-twisted python3-zope.interface rpcbind screen socat squashfs-tools ssh-import-id sshfs tigervnc-viewer tk tk8.6
  x11vnc
0 mis à jour, 45 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 9 409 ko/9 452 ko dans les archives.
Après cette opération, 40,6 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
```

Installez les paquets puis prenez une capture d'écran, tout en respectant la consigne précédemment donnée.

3.3.4 Configuration réseau

Nous allons configurer la mise en réseau LTSP de la manière la plus simple puisque nous avons une seule carte réseau sur le serveur LTSP et un serveur DHCP externe : notre routeur pfSense. Exécutez la commande suivante :

```
ltsp dnsmasq
```

```
root@ubuntu-mate-vm:/home/user# ltsp dnsmasq
Installed /usr/share/ltsp/server/dnsmasq/ltsp-dnsmasq.conf in /etc/dnsmasq.d/ltsp-dnsmasq.conf
Restarted dnsmasq
```

Lancez la commande puis prenez une capture d'écran, tout en respectant la consigne précédemment donnée.

Plus d'infos sur la commande *ltsp dnsmasq* ici : https://ltsp.org/man/ltsp-dnsmasq/

3.3.5 Génération d'une image client

LTSP prend en charge trois méthodes pour générer une image client SquashFS[14]. Nous allons utiliser *chrootless* (anciennement *pnp*) qui va utiliser la racine du serveur (/) comme modèle pour les clients. C'est la méthode la plus simple car vous ne conservez qu'un système d'exploitation, pas deux (serveur et image). Lancez la commande ci-dessous et prenez une capture d'écran en attendant patiemment la génération de l'image, tout en respectant la consigne précédemment donnée.

```
ltsp image /
```

Vous devrez exécuter cette commande à chaque fois que vous installerez un nouveau logiciel ou des mises à jour à votre image et souhaiterez exporter sa version mise à jour. L'image sera stockée à cet emplacement : */srv/ltsp/images/x86_64.img*

Pour plus d'infos sur la commande *ltsp image* : https://ltsp.org/man/ltsp-image/

3.3.6 Installation des binaires iPXE et configuration en TFTP

Après avoir créé votre image initiale, ou si vous créez des images supplémentaires, exécutez la commande suivante pour générer un menu iPXE[15] et copier les binaires iPXE en TFTP :

```
ltsp ipxe
```

[14] Plus d'infos sur SqushFS : https://fr.wikipedia.org/wiki/SquashFS
[15] Plus d'infos sur iPXE : https://ipxe.org/start et https://en.wikipedia.org/wiki/IPXE

```
root@ubuntu-mate-vm:/home/user# ltsp ipxe
Installed /usr/share/ltsp/server/ipxe/ltsp.ipxe in /srv/tftp/ltsp/ltsp.ipxe
Installed /usr/share/ltsp/binaries/memtest.0 in /srv/tftp/ltsp/memtest.0
Installed /usr/share/ltsp/binaries/memtest.efi in /srv/tftp/ltsp/memtest.efi
Installed /usr/share/ltsp/binaries/snponly.efi in /srv/tftp/ltsp/snponly.efi
Installed /usr/share/ltsp/binaries/undionly.kpxe in /srv/tftp/ltsp/undionly.kpxe
```

Lancez la commande puis prenez une capture d'écran, tout en respectant la consigne précédemment donnée.

Pour plus d'infos sur la commande *ltsp ipxe* : https://ltsp.org/man/ltsp-ipxe/

3.3.7 Configurer les exports NFS du serveur LTSP

Pour configurer le serveur LTSP afin qu'il serve les images ou les *chroots*[16] via NFS, exécutez :

```
ltsp nfs
```

```
root@ubuntu-mate-vm:/home/user# ltsp nfs
Installed /usr/share/ltsp/server/nfs/ltsp-nfs.exports in /etc/exports.d/ltsp-nfs.exports
Restarted nfs-kernel-server
```

Lancez la commande puis prenez une capture d'écran, tout en respectant la consigne précédemment donnée.

Pour plus d'infos sur la commande ltsp nfs : https://ltsp.org/man/ltsp-nfs/

3.3.8 Création d'un nouvel utilisateur

Vous allez créer un nouvel utilisateur « ben » pour vous y connecter depuis le client léger. Faites-le avec cette commande :

```
adduser ben
```

[16] Plus d'infos sur *chroot* : https://fr.wikipedia.org/wiki/Chroot


```
root@ubuntu-mate-vm:/home# adduser ben
Ajout de l'utilisateur « ben » ...
Ajout du nouveau groupe « ben » (1001) ...
Ajout du nouvel utilisateur « ben » (1001) avec le groupe « ben » ...
Création du répertoire personnel « /home/ben »...
Copie des fichiers depuis « /etc/skel »...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : le mot de passe a été mis à jour avec succès
Modification des informations relatives à l'utilisateur ben
Entrez la nouvelle valeur ou « Entrée » pour conserver la valeur proposée
        Nom complet []:
        N° de bureau []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Ces informations sont-elles correctes ? [O/n] o
root@ubuntu-mate-vm:/home#
```

Créez l'utilisateur puis prenez une capture d'écran, tout en respectant la consigne précédemment donnée.

3.3.9 Création de ltsp.img, le module complémentaire d'initrd

La commande suivante compresse */usr/share/ltsp*, */etc/ltsp*, */etc/{passwd,group}* et le serveur clés SSH publiques dans */srv/tftp/ltsp/ltsp.img*, qui est transféré en tant que "*initrd* supplémentaire" aux clients lors de leur démarrage.

```
ltsp initrd
```

Gardez à l'esprit qu'il faut lancer *ltsp initrd* après chaque mise à jour de package LTSP, ou lorsque vous ajoutez nouveaux utilisateurs, ou si vous créez ou modifiez */etc/ltsp/ltsp.conf*.

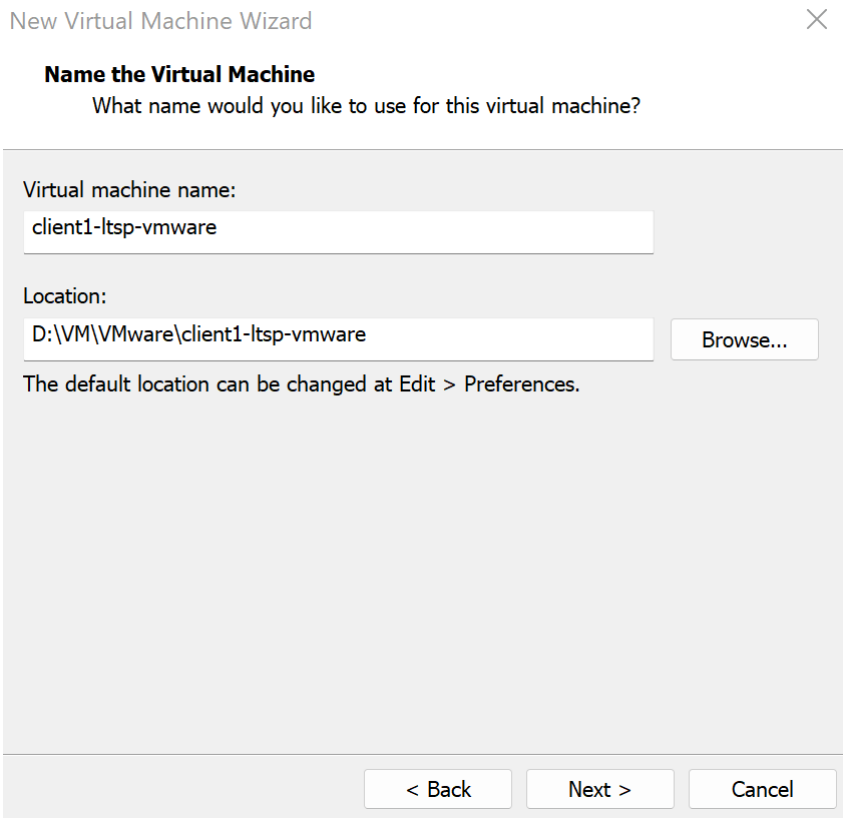
Plus d'infos sur la commande *ltsp initrd* ici : https://ltsp.org/man/ltsp-initrd/

Lancez la commande puis prenez une capture d'écran, tout en respectant la consigne précédemment donnée.

3.4 Test de l'infra

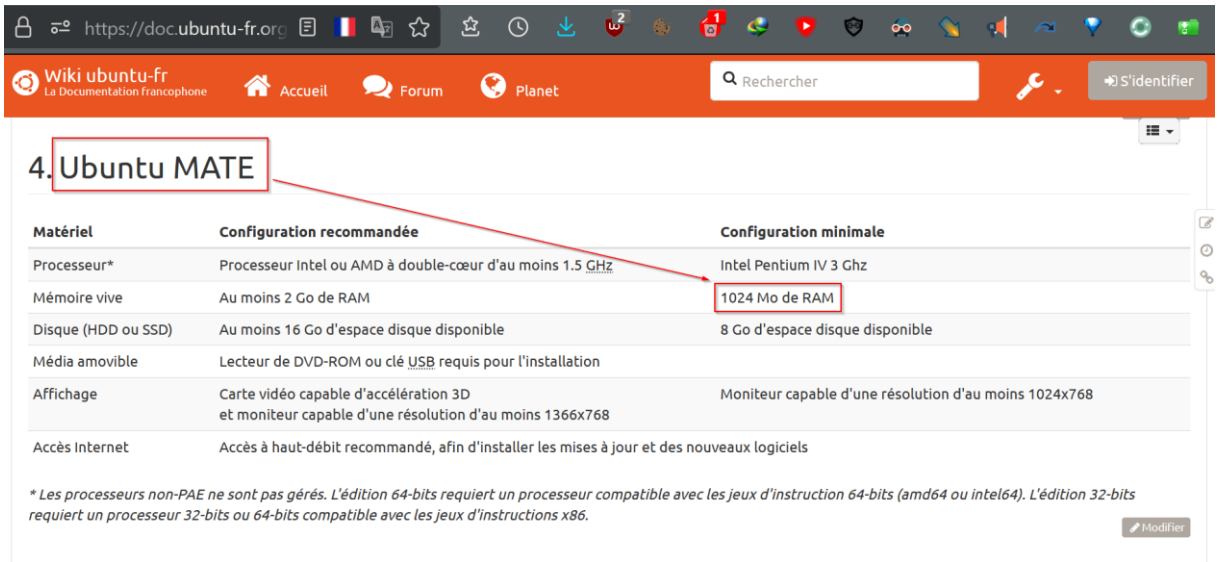
3.4.1 Création d'une machine virtuelle cliente « pauvre »

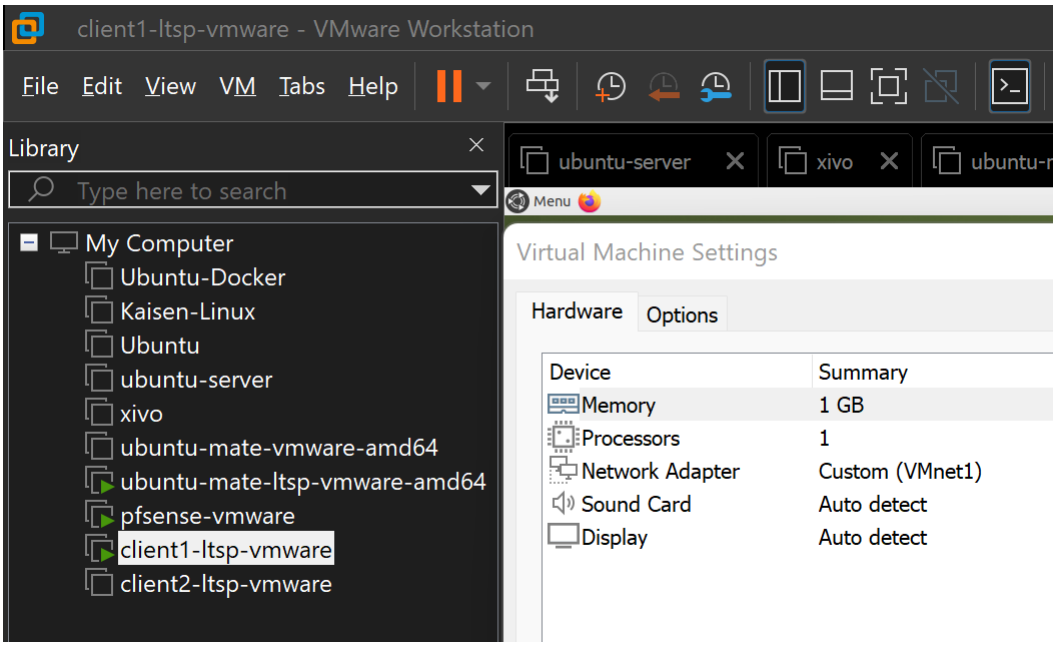
Créez une VM qui va démarrer depuis le réseau et va pouvoir se connecter au compte précédemment créé dans le serveur Ubuntu Mate.



Le client léger LTSP n'a même pas besoin d'un disque dur pour démarrer, nous allons donc lui retirer. Nous pouvons aussi le dépouiller de son lecteur CD, de son contrôleur USB et de son imprimante : ça ne va pas impacter le démarrage du client léger.

Et pourquoi ne pas économiser aussi sur le CPU et la RAM ? Mettons lui seulement 1 processeur et 1 Go de RAM (attention : si vous avez choisi un autre environnement de bureau, regardez au préalable le minimum requis sur : https://doc.ubuntu-fr.org/exigences_minimales)





Créez la VM puis prenez une capture d'écran, tout en respectant la consigne précédemment donnée.

UTILE

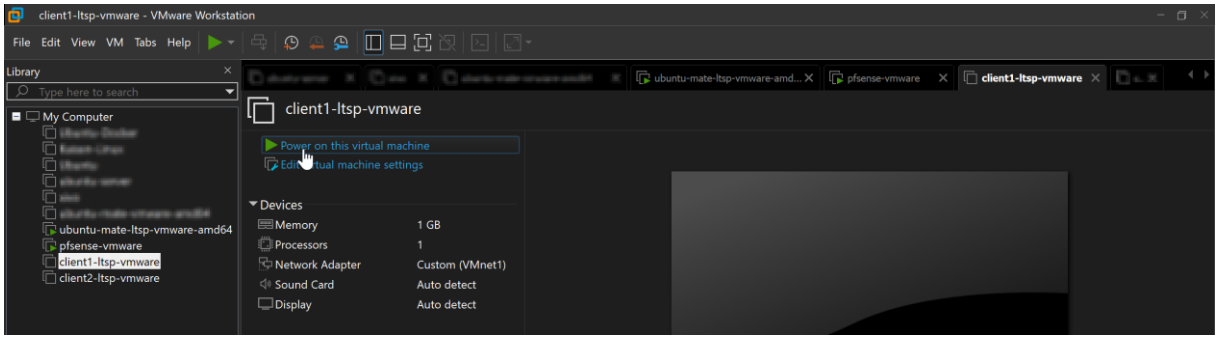
RAM minimum :

Diminuer la RAM à 512 Mo empêchera le démarrage du poste client et générera ce message d'erreur :

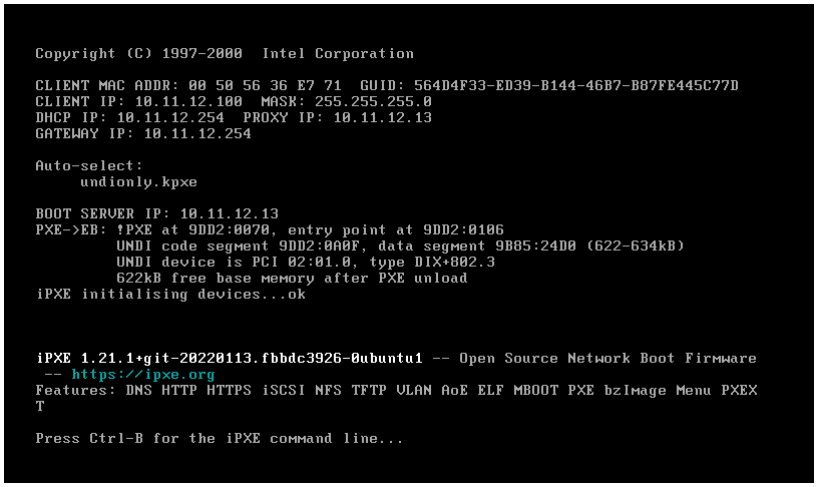
```
[    10.164501]  do_copy+0xbd/0x107
[    10.164501]  write_buffer+0x43/0x5a
[    10.164501]  flush_buffer+0x30/0x8e
[    10.164501]  ? initrd_load+0x48/0x48
[    10.164501]  __unzstd.constprop.0+0x353/0x431
[    10.164501]  ? write_buffer+0x5a/0x5a
[    10.164501]  ? __unzstd.constprop.0+0x431/0x431
[    10.164501]  unzstd+0xc/0x12
[    10.164501]  ? initrd_load+0x48/0x48
[    10.164501]  unpack_to_rootfs+0x17e/0x2c5
[    10.164501]  ? initrd_load+0x48/0x48
[    10.164501]  do_populate_rootfs+0x5e/0x112
[    10.164501]  async_run_entry_fn+0x30/0x120
[    10.164501]  process_one_work+0x228/0x3d0
[    10.164501]  worker_thread+0x53/0x420
[    10.164501]  ? process_one_work+0x3d0/0x3d0
[    10.164501]  kthread+0x127/0x150
[    10.164501]  ? set_kthread_struct+0x50/0x50
[    10.164501]  ret_from_fork+0x1f/0x30
[    10.164501]  </TASK>
[    10.164501] Kernel Offset: 0x37e00000 from 0xffffffff81000000 (relocation ran
ge: 0xffffffff80000000-0xffffffffbfffffff)
[    10.164501] ---[ end Kernel panic - not syncing: System is deadlocked on memo
ry ]---
```

3.4.2 Lancement de la machine virtuelle cliente

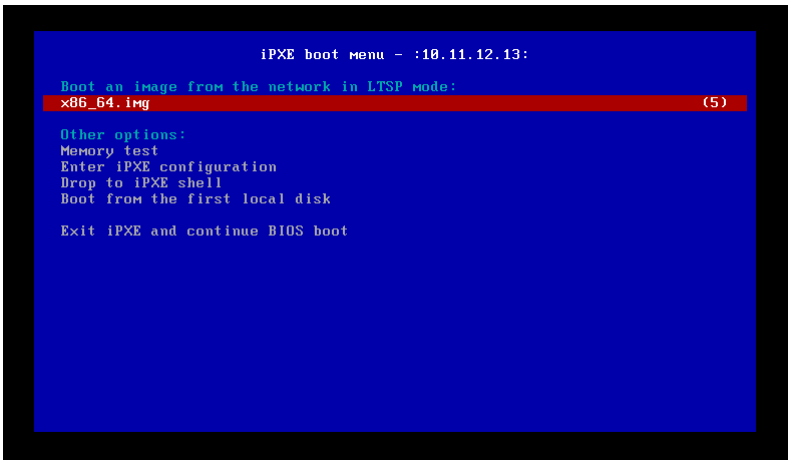
Démarrez votre machine virtuelle et prêtez attention aux différentes étapes qui vont se dérouler sous vos yeux avant que votre session Ubuntu s'affiche…



Le client détecte le serveur DHCP, le serveur LTSP (« BOOT SERVER »)…



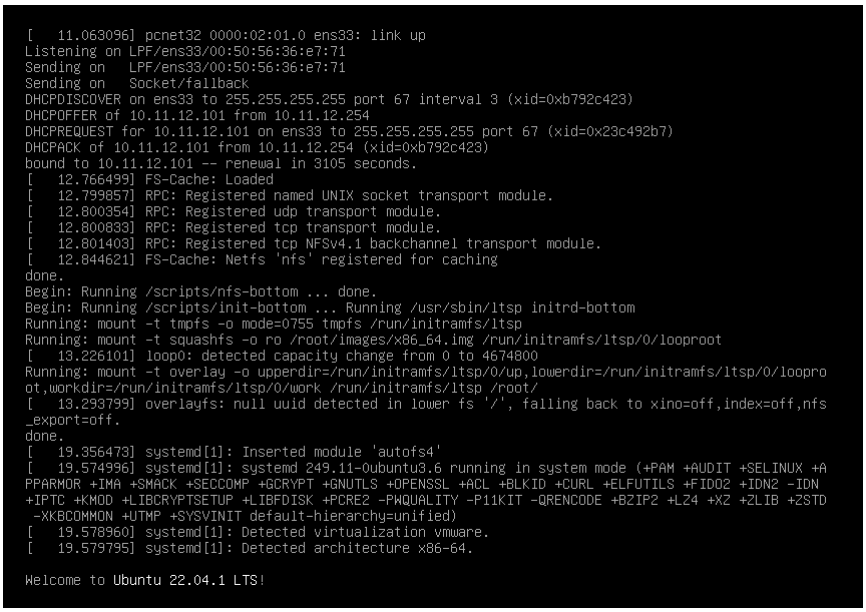
…il démarre depuis le réseau, il récupère l'image système…



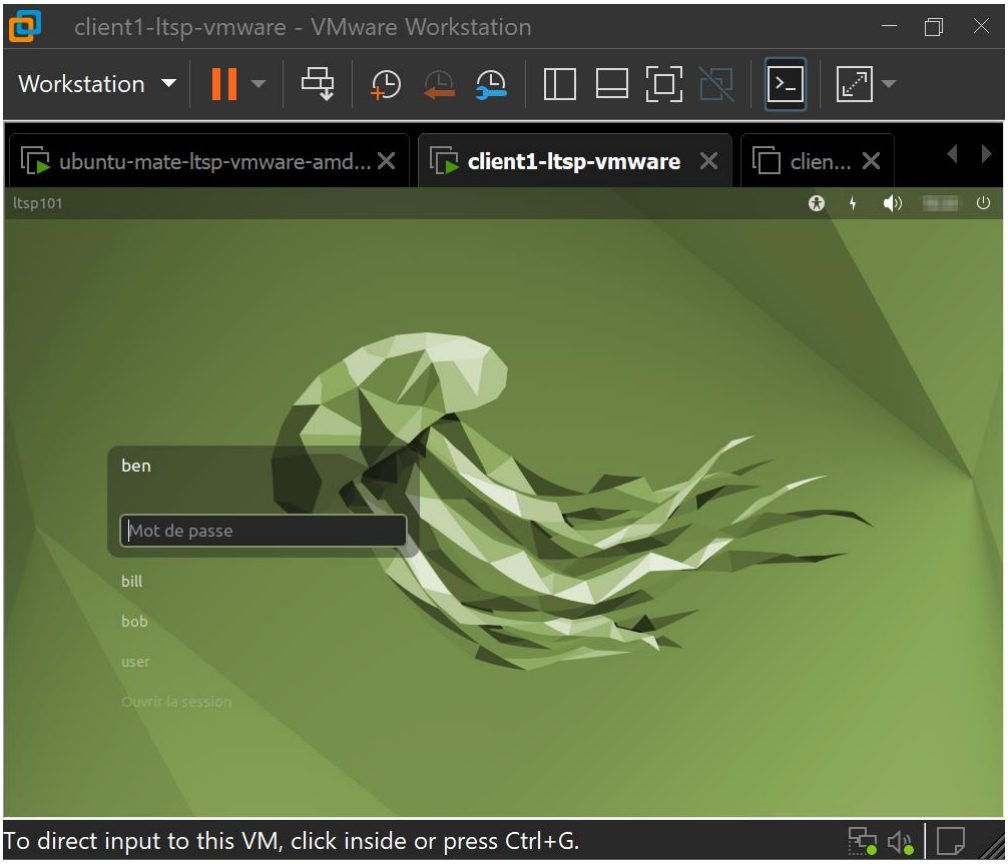
… il charge l'image…

… le système démarre…

…la machine lance une requête DHCP en broadcast, elle reçoit une IP, le système de fichier démarre, l'image système est montée en lecture seule, le système détecte qu'il est virtualisé avec VMware, Ubuntu démarre…



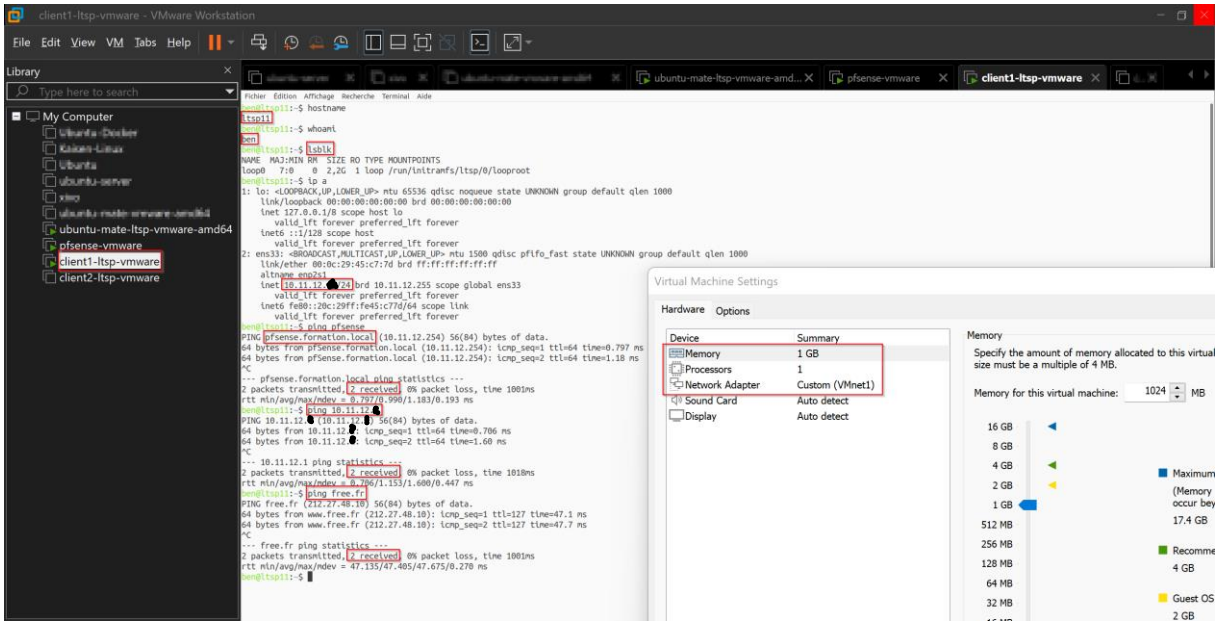
… le gestionnaire de connexion s'affiche, vous devez vous identifier…



… et finalement si vous avez bien respecté les consignes du TP, vous devriez obtenir le bureau MATE qui s'affiche !

Je lance un terminal et avec quelques commandes *bash* je constate :

- Avec *hostname* (ou tout simplement regarder le nom affiché dans le prompt après le @) : que le nom de la machine pour le système est « ltsp101 » et que ce nom a été attribué automatiquement par le serveur LTSP.
- Avec *whoami* (ou tout simplement regarder le nom affiché dans le prompt avant le @) : que je suis connecté avec l'utilisateur « ben »
- Avec *lsblk* : que ma machine cliente ne possède aucun périphérique de stockage
- avec *ip a* : que j'ai une adresse IP dans le réseau vmnet1 qui a été attribuée automatiquement par le service DHCP du pfSense
- avec *ping pfsense* : que la résolution de nom DNS du pfSense fonctionne bien
- avec *ping free.fr* : que ma machine pourtant dans un réseau LAN isolé (host-only) a bien accès à internet grâce au routage du pfSense qui transmet les requêtes provenant du réseau LAN vers l'extérieur. Ceci est en place si la configuration des interfaces et des adresses IP est correcte.



(Ne faites pas attention aux IP du serveur et du client dans la capture ci-dessus, elle a été prise avant que je décide de ne pas mettre la première IP au serveur dans mon TP suite à la découverte de complications possibles).

Voilà l'objectif du TP a été atteint. Si tout va bien pour vous, prenez une capture d'écran, similaire à celle ci-dessus (avec le résultat des commandes), tout en respectant la consigne précédemment donnée.

3.4.3 Si vous rencontrez des difficultés

Si vous rencontrez des difficultés au cours de la réalisation de ce TP, générez un fichier de configuration initial *ltsp.conf* avec cette commande :

```
install -m 0660 -g sudo /usr/share/ltsp/common/ltsp/ltsp.conf /etc/ltsp/ltsp.conf
```

Puis configurez-le à l'aide du manuel en ligne : https://ltsp.org/man/ltsp.conf/ ou de la commande :

```
man ltsp.conf
```

Vous pouvez configurer le serveur, les clients ou les deux :

Le fichier de configuration est séparé en sections :

- La section spéciale [server] est évaluée uniquement par le serveur ltsp.
- La section spéciale [common] est évaluée à la fois par le serveur et ltsp clients.
- Dans la section spéciale [clients], les paramètres de tous les clients peuvent être définis. La plupart des paramètres ltsp.conf doivent être placés ici.

Par exemple vous pouvez indiquer où se trouve le serveur LTSP de démarrage :

SERVEUR = *"192.168.67.1"*

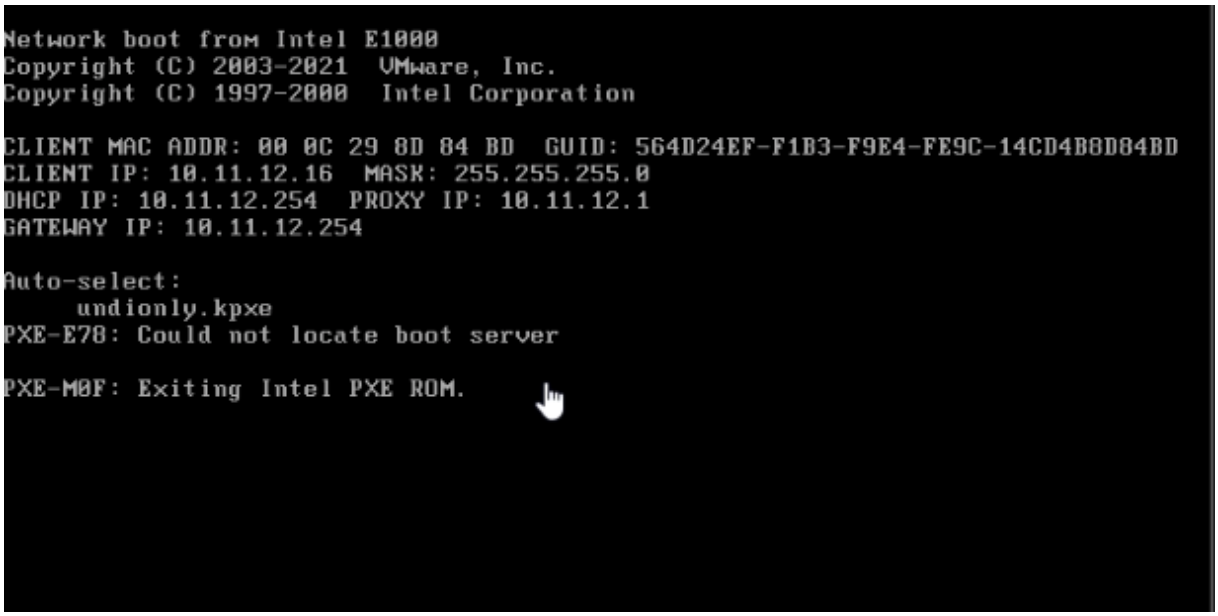
Le serveur LTSP est généralement détecté automatiquement ; il peut être spécifié manuellement s'il y en a besoin.

Ou bien le résolveur DNS :

DNS_SERVER = *"8.8.8.8 208.67.222.222"*

Spécifiez les serveurs DNS pour les clients.

Il est aussi possible que vous rencontriez cette erreur :

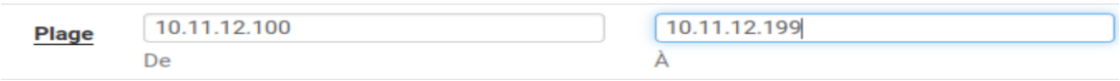


Si c'est le cas il peut être utile de changer l'IP du serveur en évitant de mettre la première adresse 10.11.12.**1**.

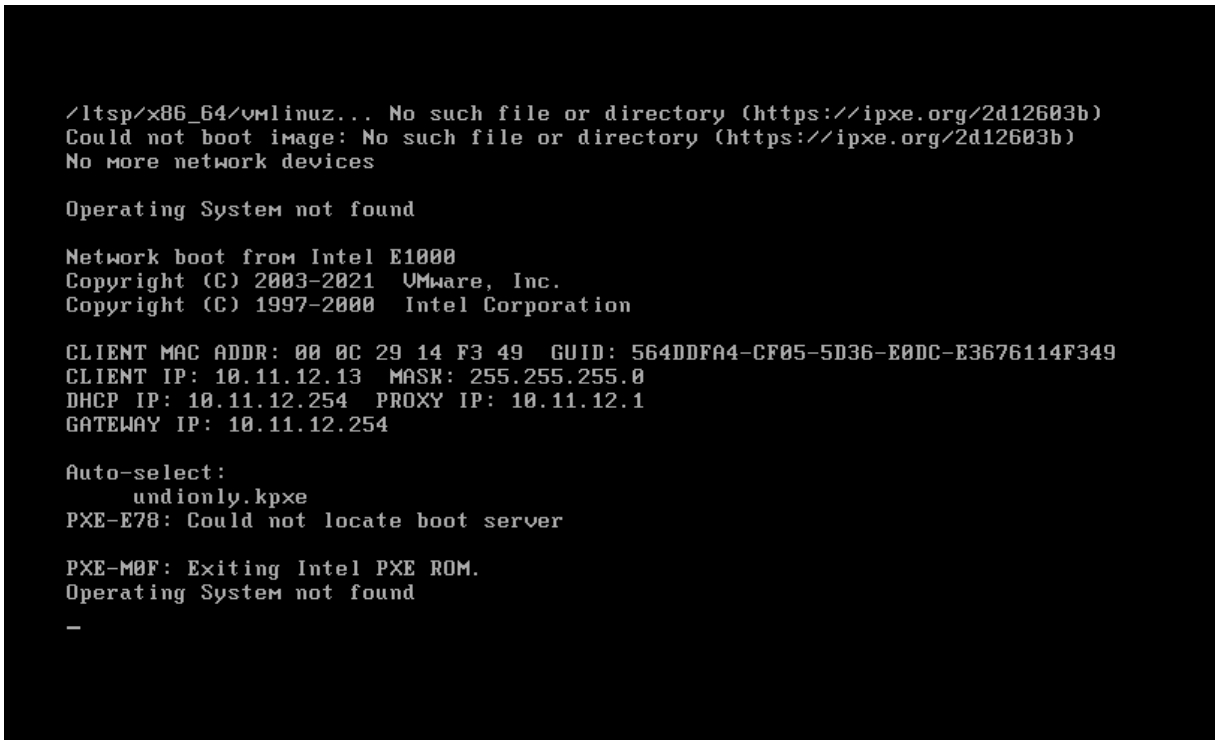
Il peut être intelligent aussi de choisir une adresse IP non incluse dans votre étendue DHCP.

Vérifier son étendue DHCP :

Vous pouvez vérifier votre *pool* DHCP dans votre pfSense, sous « Services » puis « Serveur DHCP ». Ensuite la plage se trouve dans la partie « Options générales ».



Vous pourriez aussi tomber sur ce message d'erreur :



Ces vidéos Youtube peuvent peut-être vous aider : https://www.youtube.com/watch?v=s1DI6V1v-vM ; https://www.youtube.com/watch?v=aXL2GrTA2ys . Si elles ne conviennent pas, faites vos recherches et essayez de résoudre le problème en autonomie.

Accéder au BIOS d'une VM :

Pour démarrer une VM depuis le BIOS allez dans le menu « VM », puis « Power » puis sélectionnez « Power On to Firmware ».

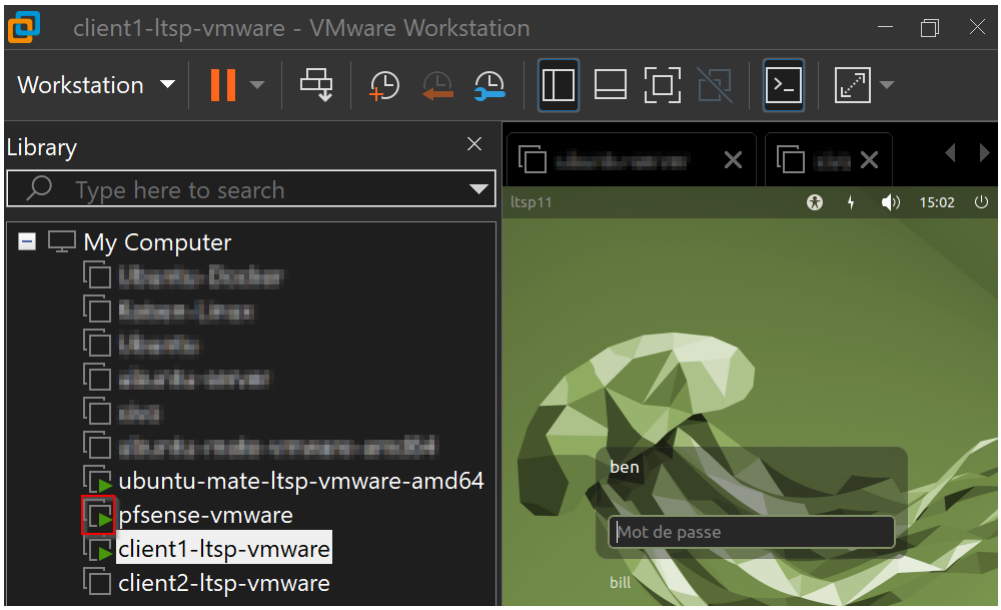
3.5 Exercices en autonomie

3.5.1 Vérification DHCP

Vous pouvez vérifier que c'est bien votre pfSense qui est le serveur DHCP de l'infra (et non pas le serveur LTSP) en éteignant le pfSense et en lançant votre VM cliente. Celle-ci ne trouvant pas de serveur DHCP ne pourra pas obtenir d'IP et ne pourra donc pas recevoir l'image système du serveur LTSP.

Prenez une capture d'écran, similaire à celle ci-dessus (avec le pfSense éteint), tout en respectant la consigne précédemment donnée.

Par contre dès que vous rallumez votre pfSense et appuyez sur la touche « Entrée » dans la VM, celle-ci va alors démarrer par le réseau :



3.5.2 Création de deux nouveaux utilisateurs

Deux nouveaux salariés (Bill et Bob) viennent d'arriver dans l'entreprise, vous devez créer un nouvel utilisateur pour chacun d'eux dans le système Ubuntu MATE du serveur. Vous ne pouvez pas le faire avec un compte d'utilisateur standard (Ben), vous devez utiliser le compte de « user » (ou le nom que vous avez choisi lors de l'installation d'Ubuntu) qui a le droit d'utiliser la commande « sudo » (car il est enregistré dans le fichier de configuration *sudoers* puisque c'est le premier utilisateur créé lors de l'installation d'Ubuntu) ou bien vous pouvez aussi vous connecter en « root ». Vous ne pouvez pas faire ceci depuis le client léger car nous avons vu plus haut que le système de fichiers *root* monté par la station cliente est **en lecture seule** (= il est différent du système de fichiers *root* que le serveur utilise lui-même) et il est partagé entre toutes les stations clientes connectées au serveur.

Utilisez la commande :

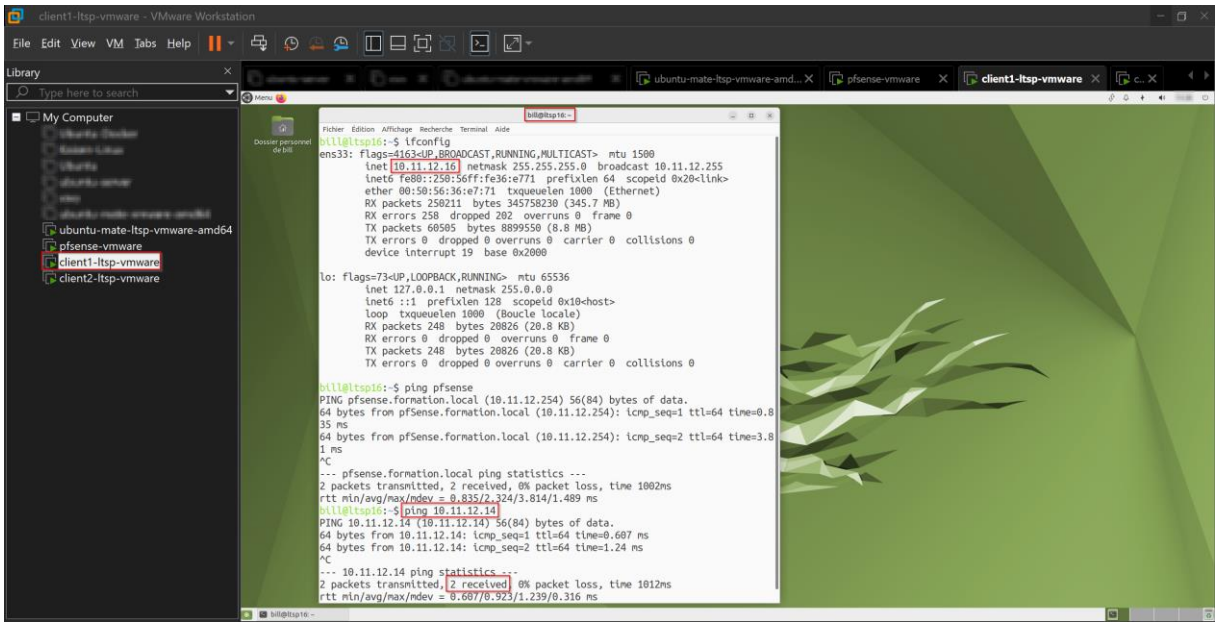
```
adduser bill
```

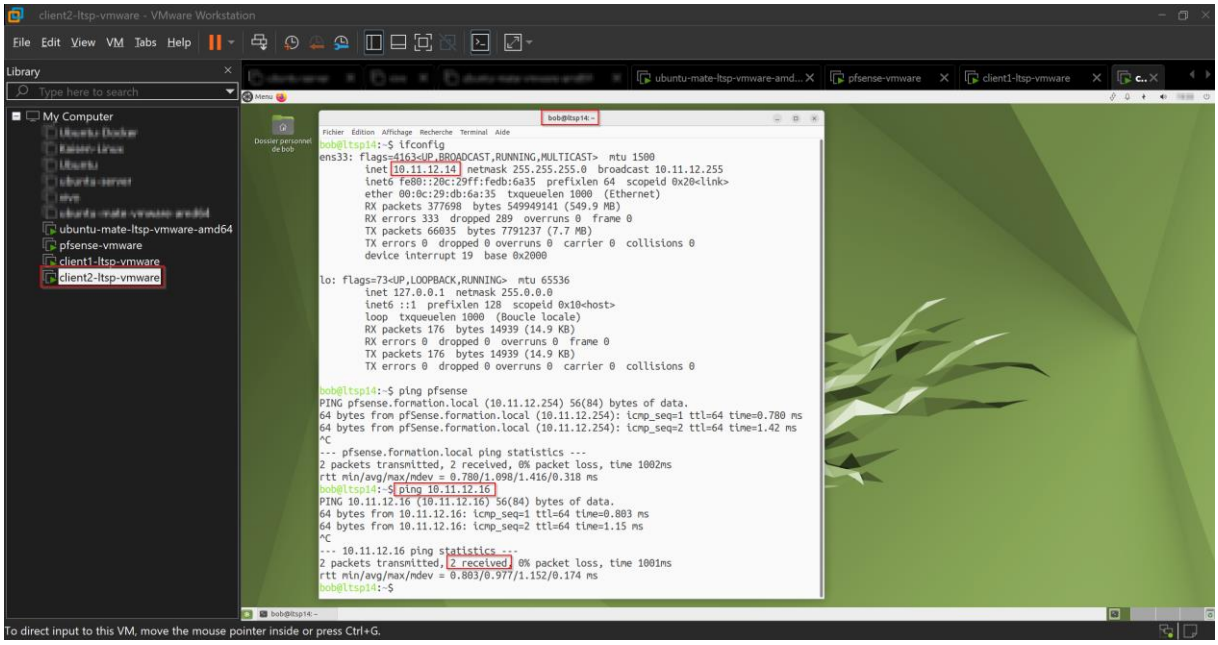
Puis validez la modification depuis le serveur LTSP avec la commande :

```
ltsp initrd
```

3.5.3 Création de deux postes clients

Créez deux nouveaux postes clients légers pour Bill et Bob et connectez-les au serveur LTSP. Faites des tests de connectivité entre les deux postes clients légers avec la commande *ping.*





Prenez une capture d'écran, prouvant que tout fonctionne bien, tout en respectant la consigne précédemment donnée.

FIN DU TP

4 Récompenses de fin de TP

Puisque vous avez bien travaillé je vous ai réservé des petites surprises.

4.1 Questions déjà tombées à l'examen TSSR

Des questions de ce genre (pas forcément les mêmes) sur le thème « services de déploiement et de clients légers » seront susceptibles de tomber à votre examen TSSR :

4.1.1 La mise en place d'un service centralisé de mises à jour logicielles apporte quels avantages ?

Réponses possibles :

- C'est plus simple pour l'administrateur puisque tout est centralisé depuis un serveur unique il n'a pas besoin de faire les mises à jour sur chaque machine.
- Ça permet de réduire la quantité de bande passante utilisée lors de la distribution des mises à jour de logiciels puisqu'au lieu que chaque ordinateur télécharge les mises à jour, elles ne sont téléchargées qu'une seule fois (par serveur).
- Ça permet de contrôler et d'approuver les mises à jour avant de les rendre disponibles.
- Ça permet de mettre en œuvre une stratégie de déploiement en fonction de critères simples (tels que l'heure ou la date de déploiement) ou avancés (en fonction du type de correctifs).

Plus d'infos sur : https://docs.jamf.com/fr/10.30.0/jamf-pro/guide-de-ladministrateur/Serveurs_de_mise_%C3%A0_jour_de_logiciels.html et https://openclassrooms.com/fr/courses/2356306-prenez-en-main-windows-server/5836381-distribuez-des-mises-a-jour-avec-wsus

4.1.2 Quels sont les solutions de déploiement que vous connaissez ?

Réponses possibles :

- WDS (Windows Deployment Services),
- Symantec Ghost,
- Clonezilla Server Edition
- FOG Project

Plus d'infos : https://fr.wikipedia.org/wiki/Windows_Deployment_Services et https://fr.wikipedia.org/wiki/Ghost_(informatique) ou https://en.wikipedia.org/wiki/Clonezilla#Clonezilla_Server_Edition_(SE) ou https://fogproject.org/

4.1.3 Comparez Remote Apps et Remote Desktop en citant leurs avantages et leurs inconvénients respectifs ?

Réponses possibles :

REMOTE DESKTOP = affichage d'un Bureau complet à distance.

Avantages de Remote Desktop

- Accès à tout le système d'exploitation donc c'est pratique pour du dépannage
- Accès à toute la puissance et à tous les fichiers du PC

Inconvénients de Remote Desktop

- Depuis un autre réseau, il faudra d'abord passer par un VPN puis par le Bureau à distance
- Dépend d'une connexion réseau

REMOTE APPS = quelques applications sont accessibles par le biais d'une interface Web : on virtualise via le protocole RDP l'affichage d'une application, elle tourne sur le(s) serveur(s) RDS mais l'affichage est déporté sur le poste client.

Avantages de Remote Apps

- Permet à une organisation de fournir seulement des applications sans avoir à fournir des postes de travail virtuels complets
- Résout le problème des applications posant des soucis de compatibilité avec le système d'exploitation des postes clients

Inconvénients de Remote Apps :

- On arrive sur une page, on a accès aux applis mais rien d'autre, pas de bureau, pas accès à l'ordi
- Pas facile de virtualiser toutes les applications
- Dépend d'une connexion réseau

Plus d'infos : https://forums.commentcamarche.net/forum/affich-33339729-difference-entre-serveur-d-applications-et-tse et https://www.lemagit.fr/conseil/Comment-fonctionne-RemoteApp

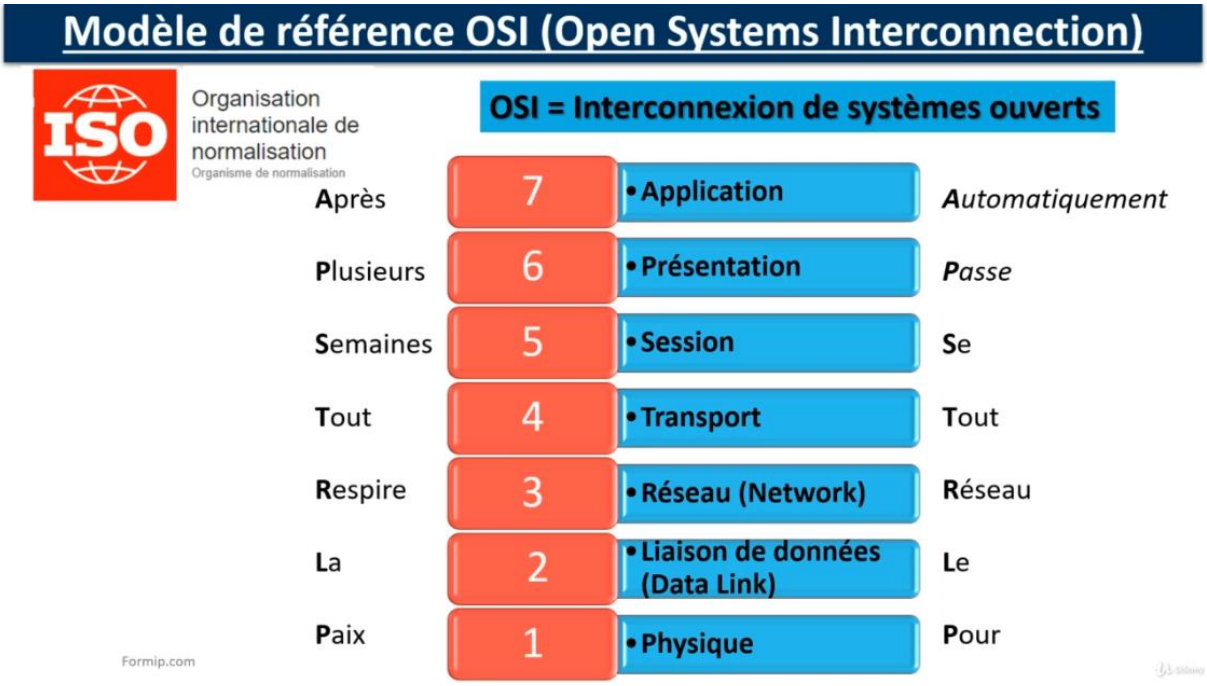
4.1.4 Comment créer un « master » d'un poste client Windows et comment le déployer ?

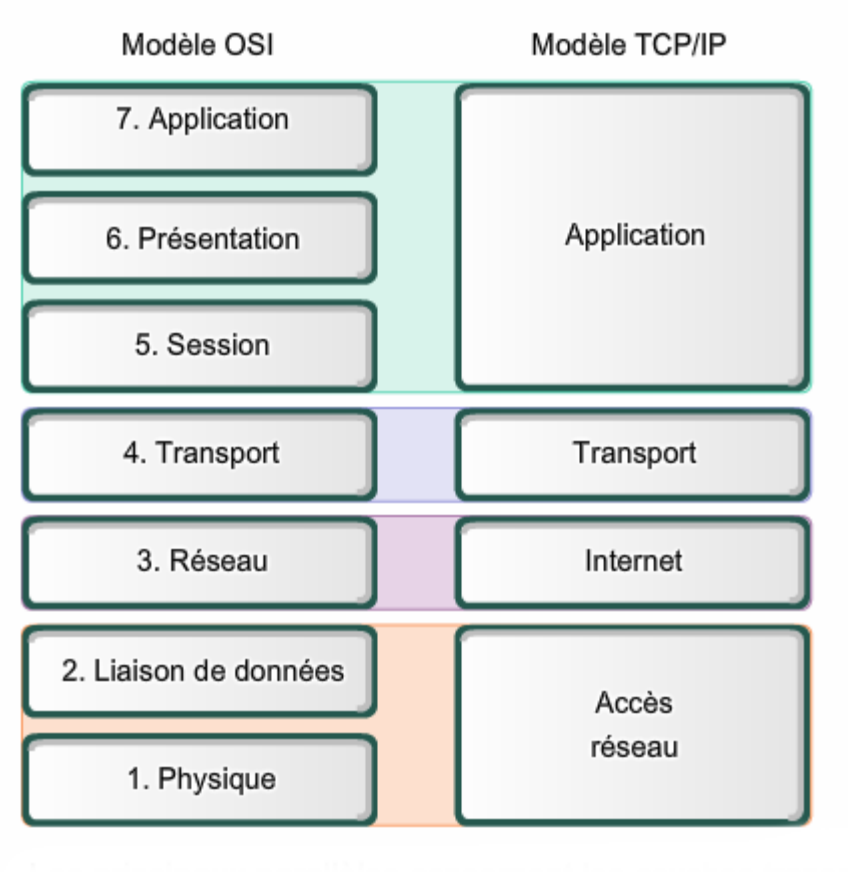
Je vous laisse chercher la réponse par vous-même car c'est comme cela qu'on retient le mieux…

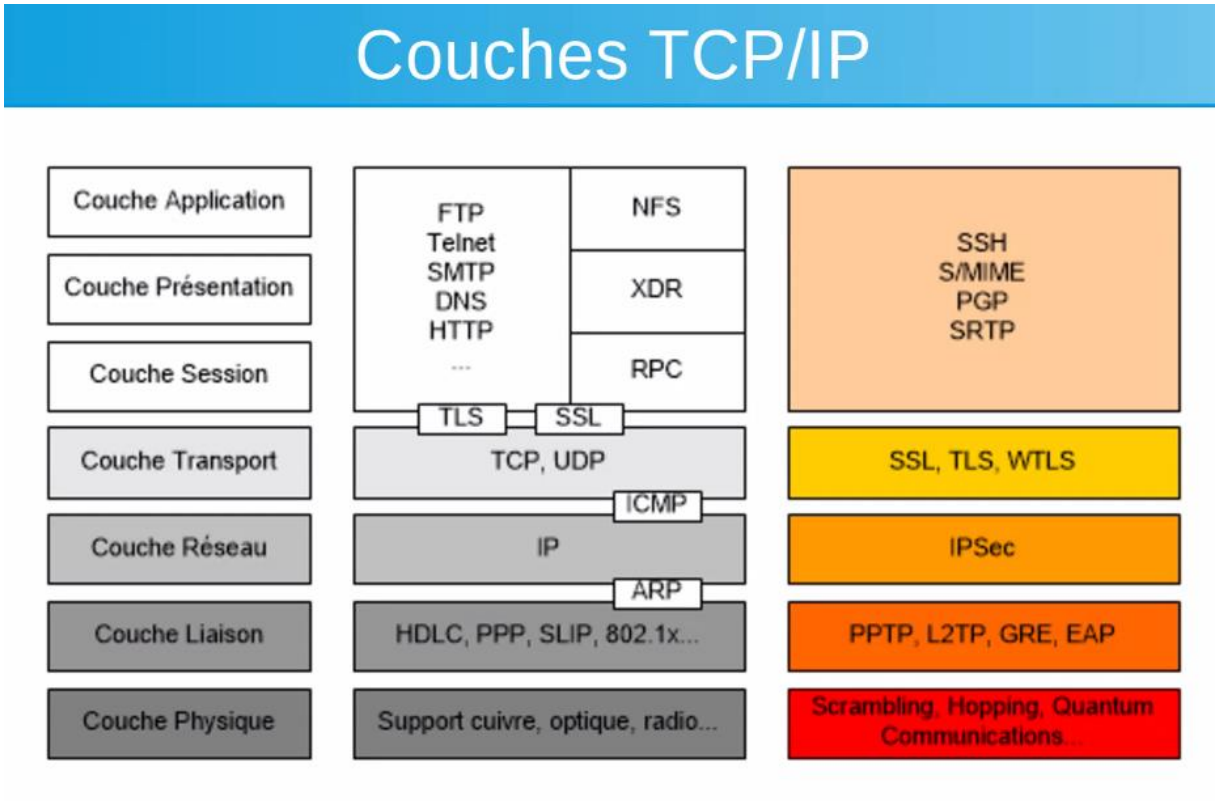
Piste : il faudra parler de Sysprep : https://fr.wikipedia.org/wiki/Sysprep

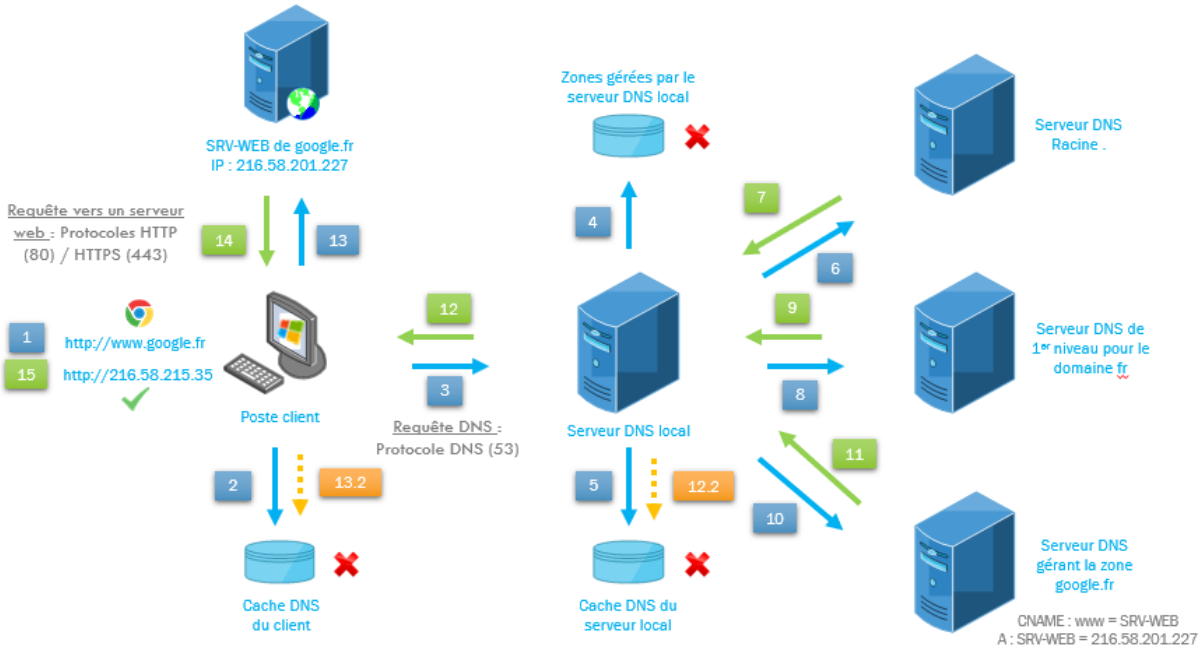
4.2 Galerie d'images

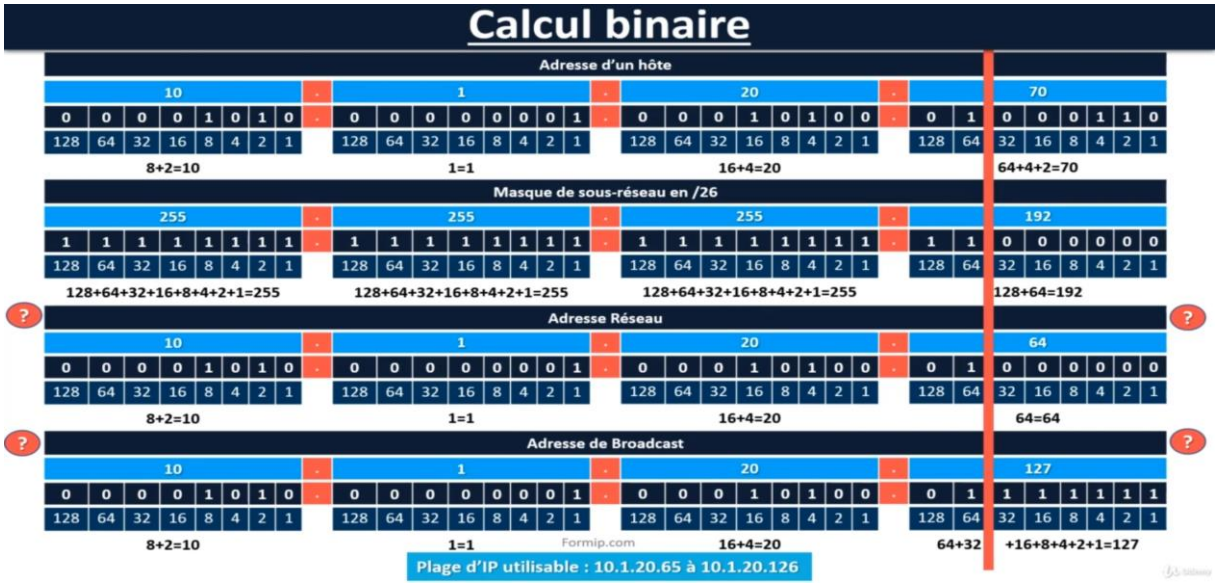
4.2.1 Utile pour préparer l'examen TSSR











Numéros de port communs [modifier]

Article détaillé : Liste des numéros de port TCP et UDP

L'IANA est responsable de la coordination mondiale de la racine DNS, de l'adressage IP et des autres ressources de protocole. Cela inclut l'enregistrement des numéros de port couramment utilisés pour des services Internet bien connus.

Les numéros de port sont divisés en trois plages : les *ports connus* , les *ports enregistrés* et les *dynamiques* ou *ports privés* .

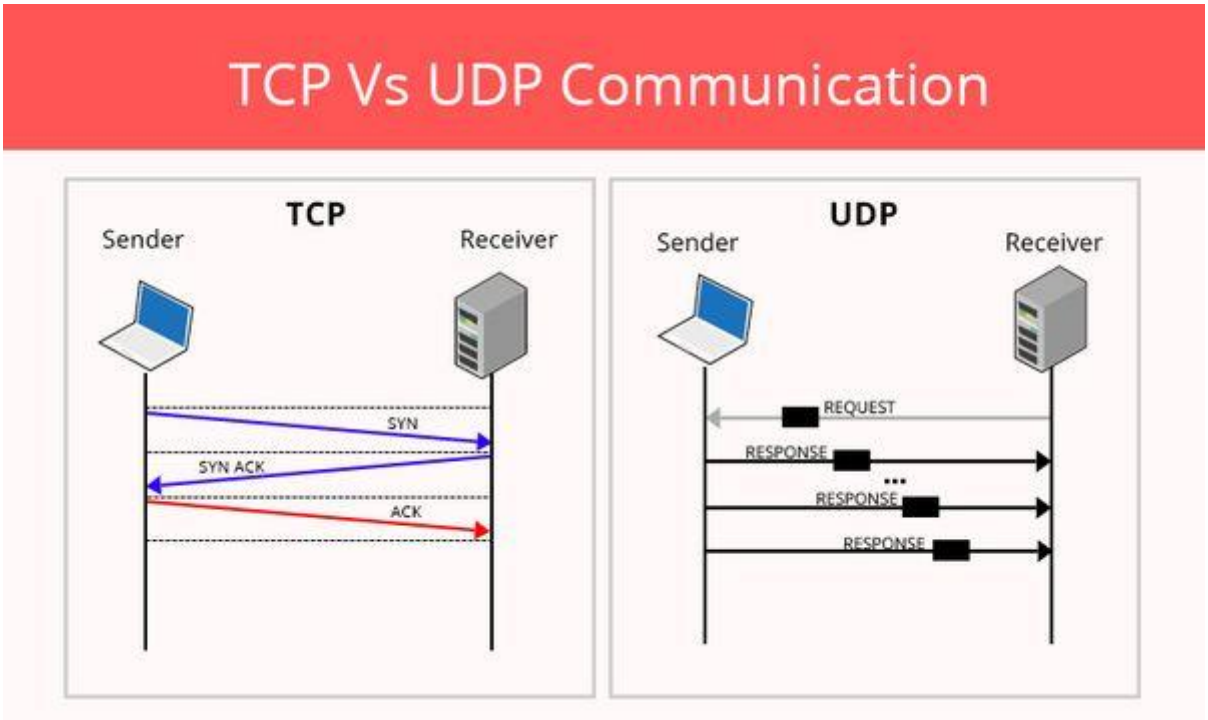
Les ports connus (également appelés *ports système*) sont ceux numérotés de 0 à 1023. Les exigences pour les nouvelles affectations dans cette plage sont plus strictes que pour les autres enregistrements. [2]

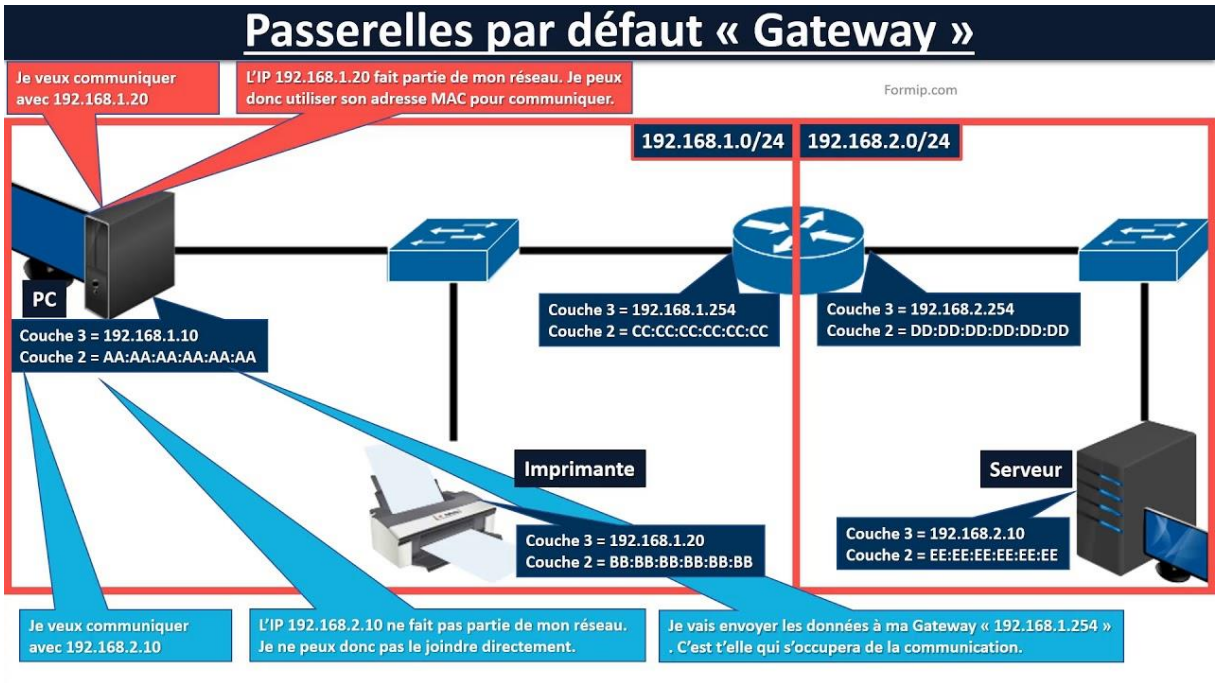
Numéros de port bien connus notables

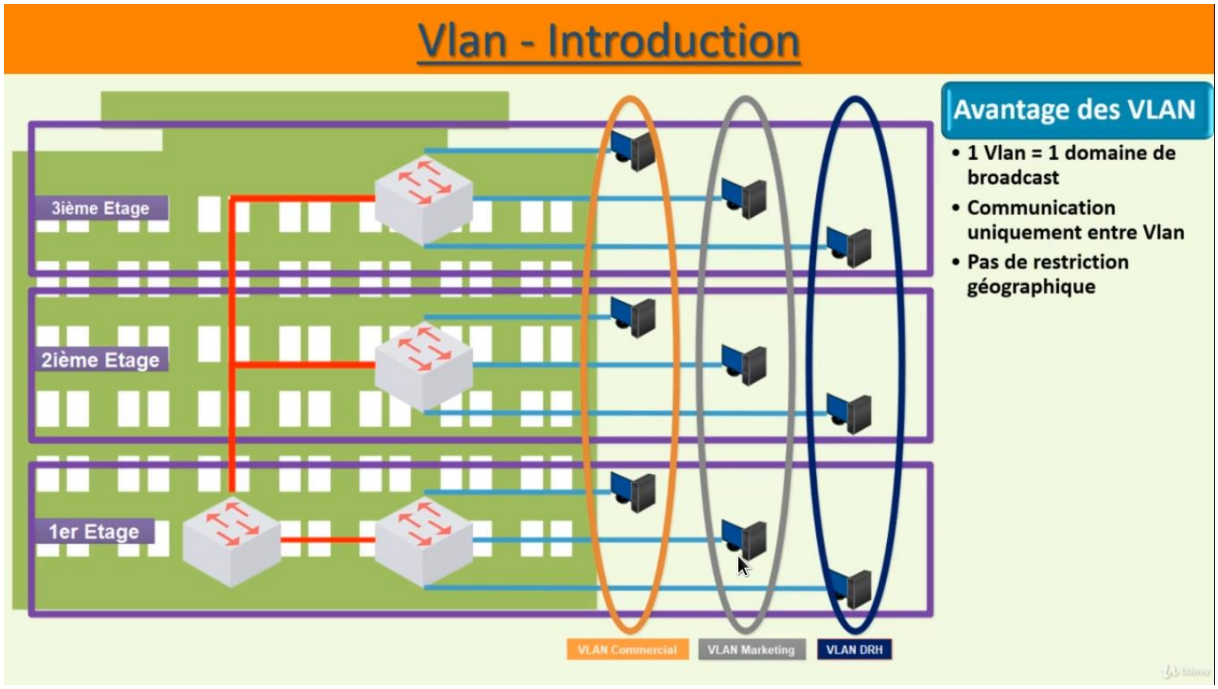
Nombre	Mission
20	Transfert de File Transfer Protocol données FTP ( )
21	protocole de transfert de fichiers Contrôle des commandes du (FTP)
22	Connexion sécurisée Secure Shell (SSH)
23	Telnet Service de connexion à distance , messages texte non cryptés
25	Simple Mail Transfer Protocol Livraison d'e-mails SMTP ( )
53	système de noms de domaine Service de (DNS)
67, 68	Protocole de configuration d'hôte dynamique (DHCP)
80	Hypertext Transfer Protocol (HTTP) utilisé dans le World Wide Web
110	Protocole postal (POP3)
119	Protocole de transfert de nouvelles de réseau (NNTP)
123	Protocole de temps réseau (NTP)
143	Internet Message Access Protocol (IMAP) Gestion du courrier numérique
161	Protocole simple de gestion de réseau (SNMP)
194	Internet Relay Chat (IRC)
443	HTTP sécurisé (HTTPS) HTTP sur TLS/SSL

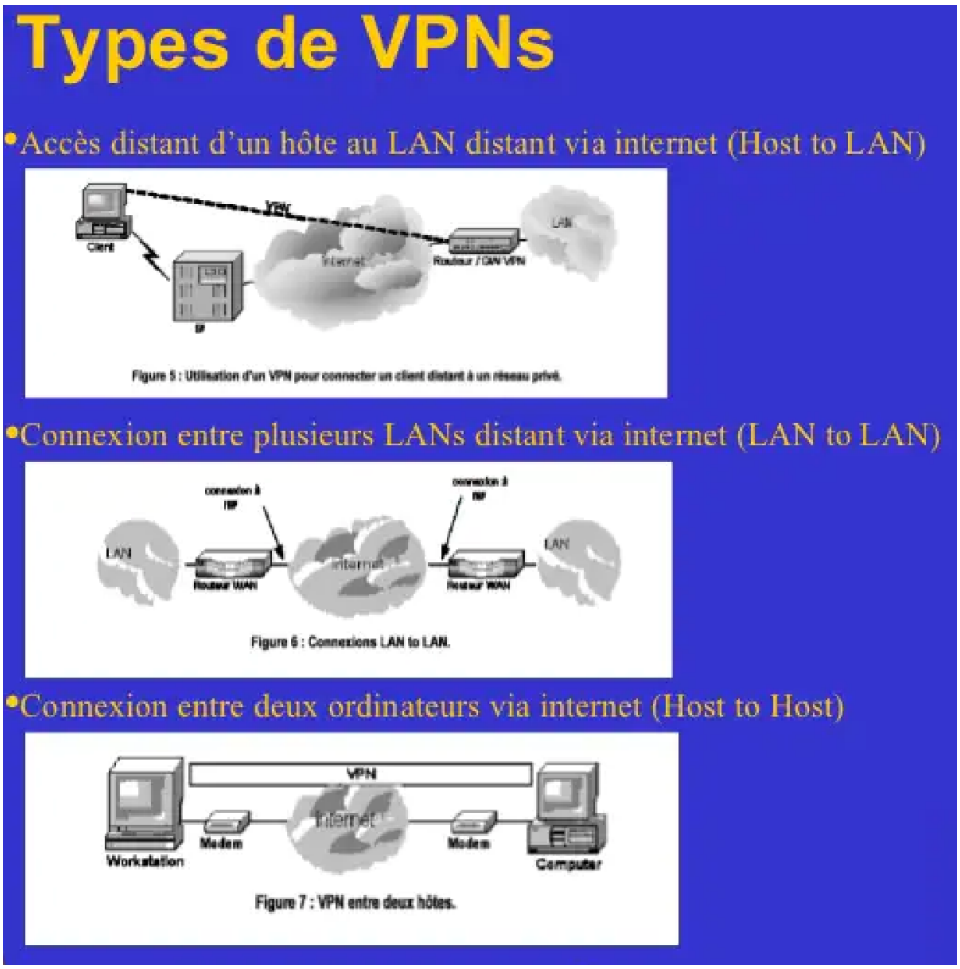
Les ports enregistrés sont ceux de 1024 à 49151. L'IANA maintient la liste officielle des plages bien connues et enregistrées. [3]

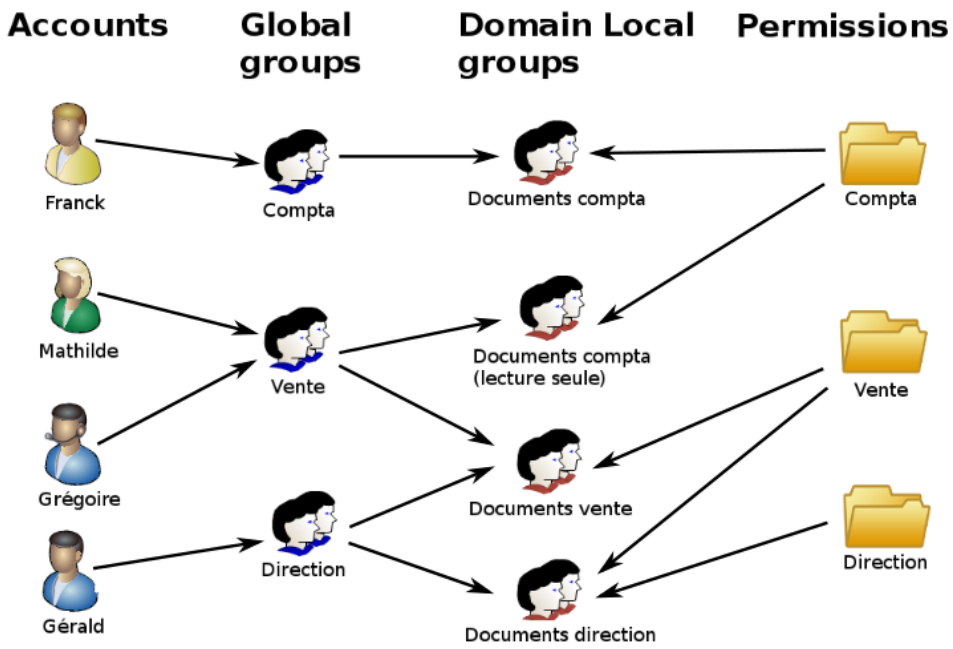
Les ports dynamiques ou privés sont ceux de 49152 à 65535. Une utilisation courante de cette plage concerne les ports éphémères .

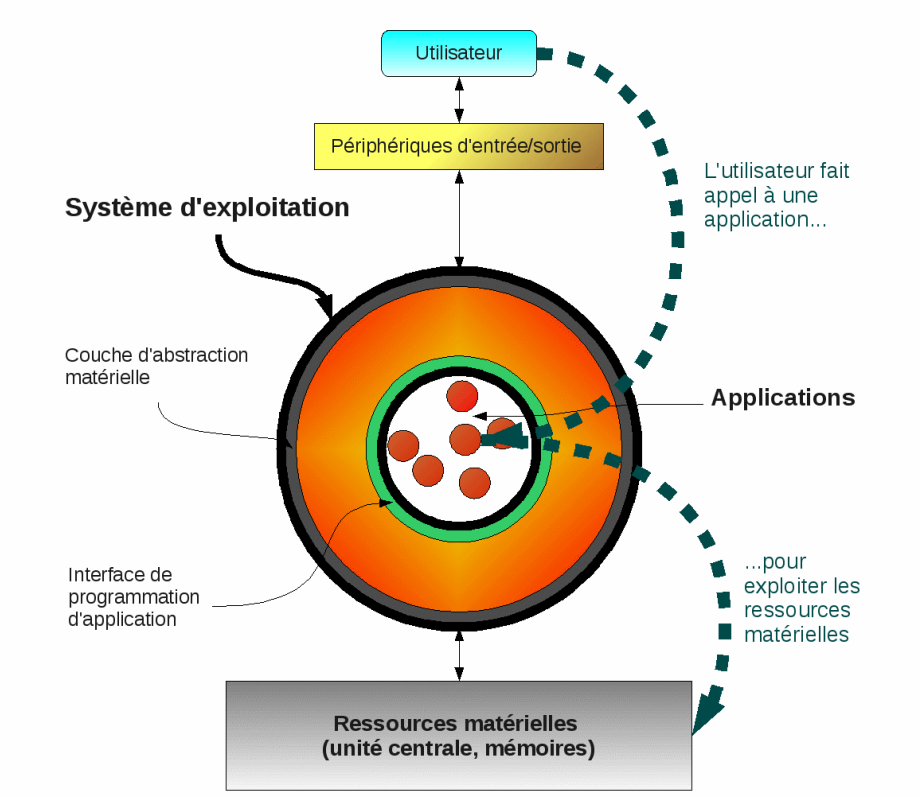






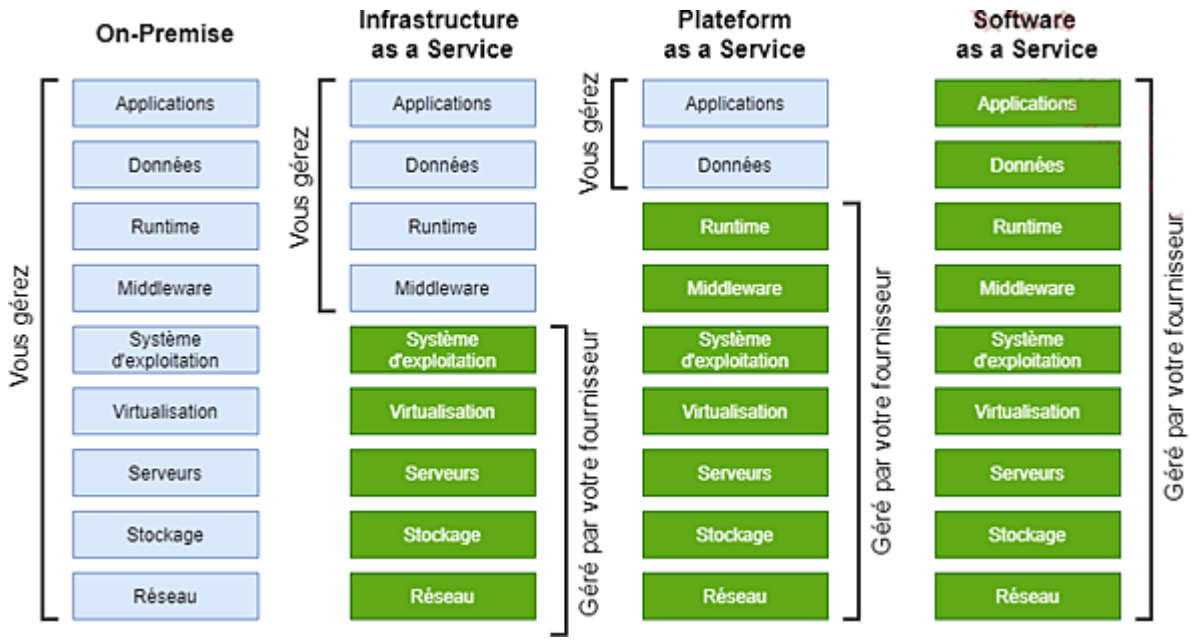






Les relations entre utilisateur, applications, système d'exploitation et matériel

Dalle	Variantes courantes	Taux de contraste	Rendu des couleurs	Rapidité	Angles de vision
TN	- -	Moyen	Moyen	Excellent	Mauvais
VA	MVA A-MVA	Bien	Bien	Mauvais	Moyen
	PVA S-PVA PSA	Moyen	Bien	Moyen	Bien
	UV²A (Sharp)	Bien	Bien	Bien	Bien
IPS	S-IPS AH-IPS PLS, AHVA	Moyen	Bien	Bien	Excellent
OLED	Super AMOLED W-OLED	Excellent	Excellent	Excellent	Excellent



Lorsque l'on n'est pas familier avec le Cloud, il est parfois difficile de s'y retrouver et une métaphore entre le modèle économique de la fabrication et de la consommation d'une pizza peut permettre de mieux appréhender les différents concepts.