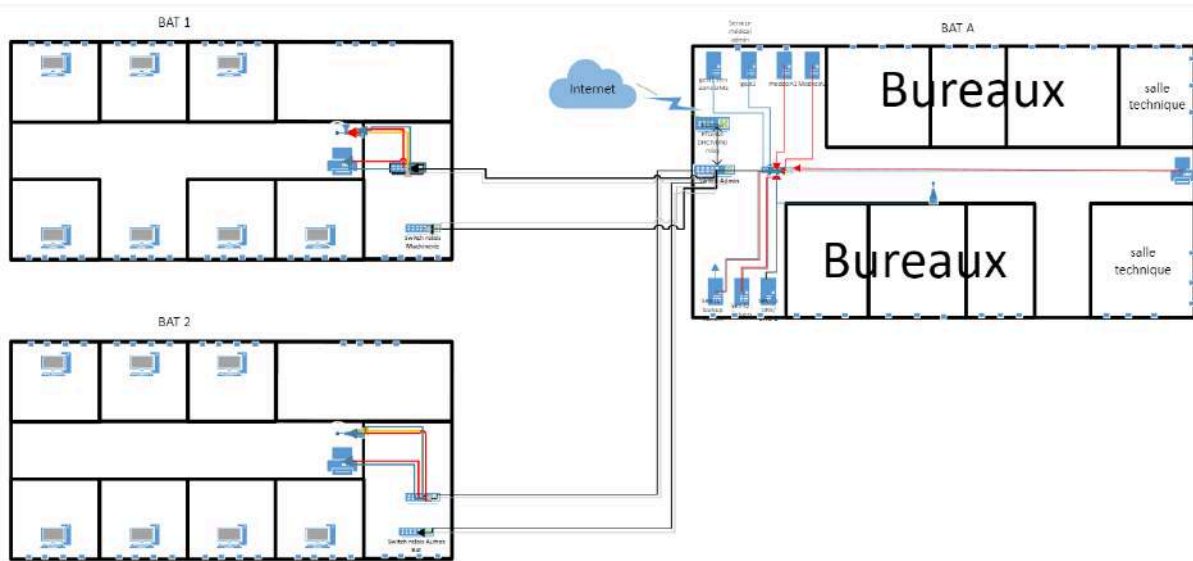


Compte rendu Projet Infrastructure et réseau d'une clinique médicale



Sommaire :

1. Note explicative du choix de l'architecture réseau.....
2. Note explicative du choix du matériel réseau.....
3. La sécurité du réseau de la clinique.....
4. Mise en place d'un routeur Pfsense et règles de parefeu.....
5. Mise en place d'un serveur DHCP et DNS.....
6. Mise en place d'une solution de services relais et gestion à..... distance + script SSH.....
7. Construction d'un schéma Cisco Packet Tracer et..... configuration de VLANs.....
8. Mise en place d'un serveur de fichier et d'un serveur de..... sauvegarde + solution de restaurations/sauvegardes..... planifiées.....
9. RGPD et Responsabilités des données patients.....

1/ Note explicative du choix de l'architecture réseau

Besoin de la clinique :

1 routeur + 3 serveurs à installer + 4 serveurs du partenaire + 6*3 prises bureaux admin utilisables pour les ordinateurs + 6*3 salles techniques admin + 8*4 prises salles Bat1 + 8*4 prises salles Bat2 + 3 imprimantes

= 111 machines

Nombre d'adresses IP à desservir :

Avec les équipements de base de la clinique et les prises réseaux disponibles, la clinique nécessite de connecter 111 hôtes à son réseau pour fonctionner correctement.

Avec cette configuration, on peut mettre en place un réseau de classe C, c'est-à-dire un réseau ayant un masque : 255.255.255.0 -> 8bits disponibles pour les connexions d'hôtes -> soit 254 hôtes :

- 254 – 111 = 143 adresses IP restent disponibles et attribuables par le serveur DHCP pour les patients ou les médecins/personnels souhaitant se connecter en Wifi via les 3 points d'accès du réseau.

Cependant, avec la mise en place de Vlans qui scindent le réseaux en plusieurs sous-réseaux virtuels nous utiliserons comme masque de type B : 255.255.0.0 :

192.168.1.0 : sous réseau destiné à l'administration (en bleu sur le schéma)

192.168.2.0 : sous réseau destiné au personnel médical (en rouge sur le schéma)

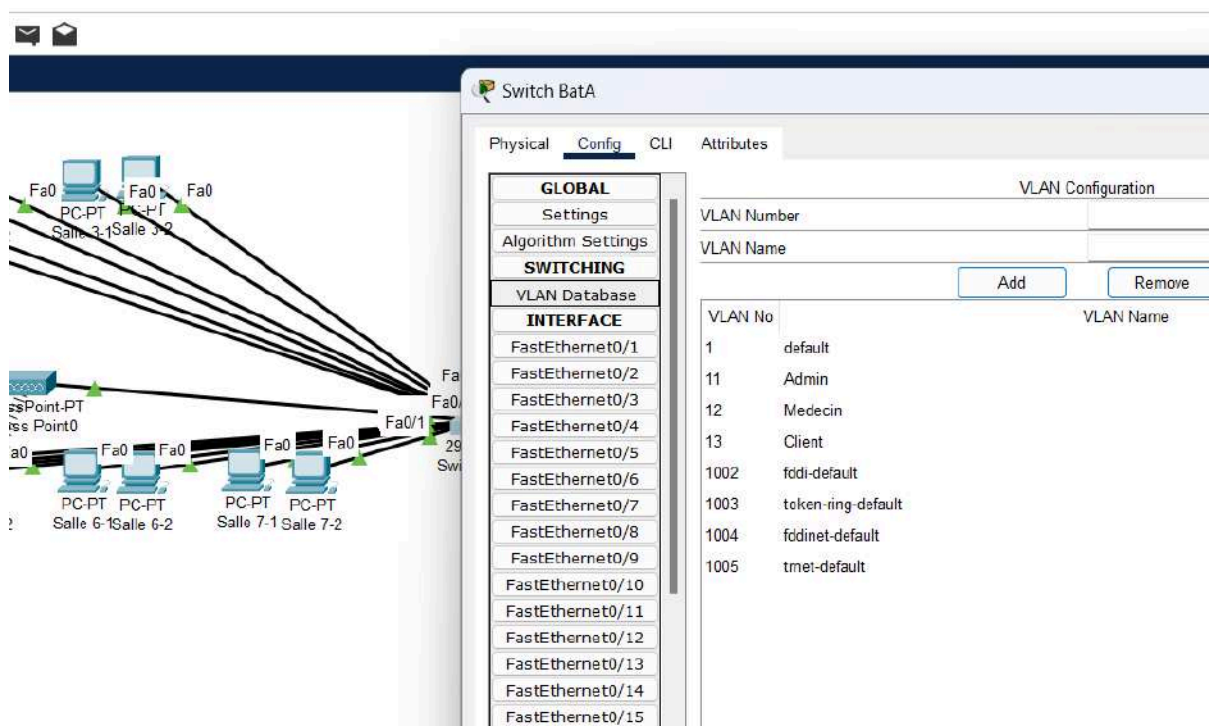
192.168.3.0 : sous réseau destiné aux patients et visiteurs (en jaune sur le schéma)

Ensuite, nous proposons un routeur Pfsense avec des règles de firewall pour que nous puissions accéder à Internet mais que les données internes ne puissent pas être envoyées sur le WAN (internet).



De plus, notre routeur Pfsense sera équipé d'un DHCP et d'un DNS relais en cas de panne du serveur DHCP/DNS.

Nous avons donc choisi de diviser le réseau LAN en plusieurs sous-réseau virtuel à l'aide de VLAN pour que les données puissent transiter dans le même réseau physique sans être accessibles par n'importe qui.



- Médecins / Administration / et patients peuvent utiliser les mêmes switchs et autres équipements du réseau pour accéder à internet mais se connectent à des VLAN différentes via les points d'accès wifi, ayant ainsi des droits d'accès différents.
 - o **Les médecins** pourront accéder aux imprimantes, aux serveurs de fichiers et de sauvegardes contenant les données médicales sensibles, aux serveurs

Med1 et Med2, aux points d'accès wifi proposant un WIFI sécurisé par un mot de passe destiné pour eux.

- o **L'Administration** pourra accéder aux imprimantes, aux serveurs Gest1 et Gest2, aux serveurs de fichiers et de sauvegardes contenant les données médicales sensibles, aux serveurs aux points d'accès wifi proposant un WIFI sécurisé par un mot de passe destiné pour eux.
- o **Les patients** auront uniquement accès à internet via l'unique routeur du réseau. (des restrictions pourront toujours être ajoutée dans le firewall)
- o **Tout le monde** aura accès à internet via le routeur, et au serveur Srv-I3 DHCP/DNS.

2/ choix du matériel pour la clinique

Le matériel :

- Pour garantir une disponibilité à 100 %, un ordinateur doit être allumé en permanence 24h/24, 7j/7. Est-ce qu'une machine personnelle pourrait faire l'affaire ? Oui tout à fait, mais si vous jouez en même temps ou si vous regardez une vidéo, votre service aura du mal à fonctionner convenablement face à de nombreuses requêtes. Il faut donc privilégier une machine que nous appelons « serveur ».
- Est-ce que cette machine devra accueillir la toute dernière carte vidéo ? Non puisqu'il n'affiche rien en 3 dimensions, en revanche, il faudra lui attribuer un bon processeur à plusieurs cœurs afin qu'il puisse prendre en charge un maximum de connexions.
- La taille du disque dur est également importante pour le système, mais aussi et surtout pour les données. Il faudra bien évidemment prévoir un système de sauvegarde (Technologie raid par exemple), et avoir une copie dans une machine différente pour éviter tout problèmes.
- Autre élément indispensable, la mémoire vive devra être conséquente, car chaque nouvel utilisateur connecté lancera un processus dans le serveur.
- Il faudra enfin une très bonne bande passante afin de recevoir un maximum de trafic et de pouvoir y répondre.

Pour le srv-l1 et srv-l2 serveurs de fichiers:

- HPE ProLiant DL380 Gen10 serveur Fichier / 2 449€
 - o Fiabilité : Les serveurs HPE ProLiant sont réputés pour leur fiabilité et leur durabilité, ce qui en fait un choix solide pour les entreprises qui recherchent des solutions informatiques stables.

- Performances élevées : Le ProLiant DL380 Gen10 offre des performances élevées grâce à sa conception optimisée pour les charges de travail intensives, ce qui en fait un choix adapté pour les applications exigeantes en matière de traitement de données et de virtualisation.
- Gestion simplifiée : HPE propose des outils de gestion intégrés, tels que HPE iLO, qui permettent une gestion à distance avancée, la surveillance des performances et la résolution des problèmes, ce qui facilite la gestion des serveurs.
- Évolutivité : Le ProLiant DL380 Gen10 est conçu pour être évolutif, ce qui signifie qu'il peut s'adapter à la croissance des besoins informatiques de l'entreprise.
- Sécurité : HPE intègre des fonctionnalités de sécurité avancées dans ses serveurs, telles que HPE Silicon Root of Trust**, pour protéger les infrastructures contre les menaces potentielles.
- Support technique : En choisissant un serveur HPE, on bénéficie du support technique d'un leader mondial en solutions informatiques, ce qui peut être un avantage important en cas de besoin d'assistance ou de résolution de problèmes.

** Silicon Root of Trust est une technologie de micrologiciel qui intègre la sécurité directement au niveau matériel des serveurs HPE, créant ainsi une empreinte digitale immuable dans le silicium qui offre des niveaux avancés de protection contre les attaques de micrologiciels. Il détecte les modifications introduites par les cyber-attaquants et désactive le serveur, afin que le code malveillant ne pénètre jamais et permette au fonctionnement de retrouver rapidement son état d'origine.

Pour le srv-l3 serveur DHCP/DNS :

- Cisco - ASR1001 - Cisco ASR1001 System, Crypto, 4 built-in GE, Dual P/S serveur DHCP et DNS / 171€.
- Fiabilité : les équipements Cisco sont réputés pour leur fiabilité et leur durabilité, ce qui en fait un choix solide pour les entreprises qui recherchent des solutions réseau stables.
- Performances élevées : le Cisco ASR1001 offre des performances élevées avec un système intégré de chiffrement matériel (Crypto) et quatre interfaces Gigabit Ethernet intégrées, ce qui en fait un choix approprié pour les applications exigeantes en matière de bande passante et de sécurité.

- Évolutivité : les équipements Cisco ASR1001 sont conçus pour être évolutifs, ce qui signifie qu'ils peuvent s'adapter à la croissance des besoins en matière de réseaux et de bandes passantes de l'entreprise.
- Support technique : le fait de choisir un équipement Cisco permet de bénéficier du support technique de l'un des principaux fournisseurs de solutions de réseau au monde, ce qui peut être un avantage important en cas de besoin d'assistance ou de résolution de problèmes.
- Compatibilité : le serveur Cisco ASR1001 est conçu pour être compatible avec un large groupe d'autres équipements réseau. C'est pour cela que Cisco est un acteur majeur dans son domaine.

Choix des commutateurs principaux reliant tous les équipements d'un bâtiment :

- Aruba 6000 48G 4SFP (R8N86A)/ 949€ pour le 48 port
 - Capacité élevée : Le commutateur Aruba offre une capacité élevée avec **48 ports** Gigabit Ethernet et 4 ports SFP (Small Form-factor Pluggable), ce qui permet de connecter un grand nombre d'appareils au réseau.
 - Performance et fiabilité : Les commutateurs Aruba sont réputés pour leurs performances élevées et leur fiabilité, garantissant un fonctionnement fluide et constant du réseau
 - Gestion avancée : Le commutateur Aruba est conçu pour offrir des fonctionnalités de gestion avancée, telles que la surveillance du trafic, la qualité de service (QoS) et la sécurité avancée, ce qui permet de contrôler et d'optimiser le trafic réseau.
 - Simplicité d'utilisation : Aruba propose une interface de gestion conviviale et des outils de configuration simplifiés, ce qui facilite l'administration et la maintenance du commutateur.
 - Sécurité avancée : Les commutateurs Aruba intègrent des fonctionnalités de sécurité avancées pour protéger le réseau contre les menaces potentielles, ce qui est essentiel pour assurer la confidentialité et l'intégrité des données.
 - Support technique : En choisissant un commutateur Aruba, vous bénéficiez du support technique d'un leader mondial en solutions réseau, ce qui peut être un avantage important en cas de besoin d'assistance ou de résolution de problèmes.

Pour les autres commutateurs du réseau :

- TP-LINK TL-SG1024D / 124€ pour le 24 port

- Prix abordable : Le commutateur TP-LINK TL-SG1024D offre un excellent rapport qualité-prix, ce qui en fait une option attrayante pour les petites et moyennes entreprises ainsi que pour un usage domestique.
- Grande capacité : Avec ses 24 ports Gigabit Ethernet, le TL-SG1024D permet de connecter un grand nombre d'appareils au réseau, offrant ainsi une grande flexibilité pour étendre votre infrastructure réseau.
- Performance fiable : Le commutateur TP-LINK TL-SG1024D est conçu pour offrir des performances fiables et constantes, ce qui garantit un fonctionnement fluide du réseau.
- Facilité d'installation : Le TL-SG1024D est facile à installer et à configurer, ce qui le rend adapté aux utilisateurs qui ne possèdent pas une expertise technique avancée en matière de réseau.
- Économie d'énergie : Ce commutateur est conçu pour être économe en énergie, ce qui peut contribuer à réduire la consommation d'électricité et les coûts opérationnels.
- Garantie et support : TP-LINK propose une garantie et un support technique pour ses produits, ce qui peut être un avantage important en cas de besoin d'assistance ou de résolution de problèmes.

Pour le routeur :

Netgate SG-3100: 300€

Performances robustes : Intègre un processeur ARM 32 bits double cœur, 2 Go de stockage eMMC et 2 Go de RAM pour des performances réseau stables et fiables.

Ports réseau polyvalents : Dispose de quatre ports Ethernet Gigabit configurables pour différents besoins réseau.

Gestion de réseau avancée : PfSense installé par défaut, offrant des fonctionnalités de pare-feu, de routage avancé et de gestion du réseau pour répondre aux exigences des environnements professionnels.

Sécurité renforcée : Offre une sécurité réseau robuste avec des fonctionnalités avancées pour protéger les données et les communications.

Conception robuste : Boîtier solide et durable conçu pour une utilisation professionnelle et industrielle.

Ces routeurs Netgate sont spécialement conçus pour tirer parti des fonctionnalités de PfSense et offrir des performances réseau avancées ainsi qu'une sécurité accrue pour les environnements professionnels et les utilisateurs avancés.

3/ La sécurité mise en place pour le réseau de la clinique

Afin de sécuriser au maximum les données médicales des patients, le réseau disposera de plusieurs couches de sécurité :

Sécurité de transmission de données entre le LAN et le WAN :

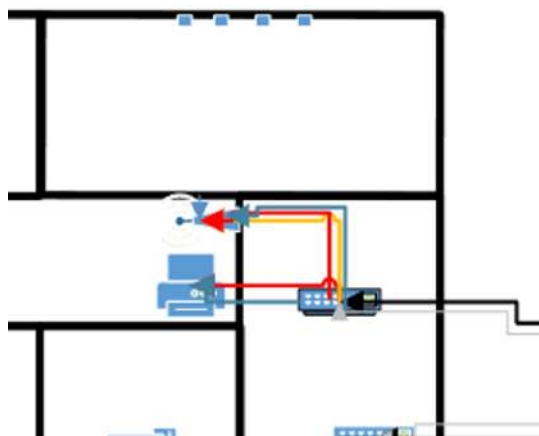
L'infrastructure réseau proposée sera uniquement interne à la clinique, avec une unique porte d'entrée et de sortie, le personnel ne pourra pas y avoir accès en dehors du travail pour éviter toute fuite de données, ce qui explique l'absence de DMZ dans notre infrastructure à des fins de sécurité.

Ensuite, nous proposons un routeur Pfsense avec des règles de firewall pour que nous puissions accéder à Internet mais que les données internes ne puissent pas être envoyées sur le WAN (internet).



Deuxième couche de sécurité en interne les VLAN :

Une fois la sécurité de l'extérieur mise en place, il faut également protéger le réseau de l'intérieur, en effet un wifi publique disponible pour les patients sera mis en place grâce aux différents points d'accès wifi de notre architecture :



Les câbles de différentes couleurs ne sont pas physiques mais permettent de représenter virtuellement les différentes Vlan mises en place pour diviser le réseau en fonction des attributions de chacun.

La couleur **jaune** correspond au point d'accès wifi public pour les patients, ceux-ci n'auront accès qu'à la passerelle vers internet et ne pourront pas accéder aux serveurs internes (excepté le Srv-I3 DHCP/DNS) grâce à ce système de VLAN.

En cas de panne d'un switch, les VLAN doivent être sauvegardé pour ne pas perdre temps dans la configuration du nouveau switch, avec un serveur supplémentaire, la clinique pourrait mettre en place un serveur TFTP pour stocker les copies de ces VLAN et pour pouvoir ainsi les déployer plus efficacement.

Dans l'hypothèse où un tel serveur aurait pour IP 192.168.1.20 on pourrait dans le switch sauvegarder la VLAN sur le serveur TFTP:

```
COM1>enable
COM1>enable
Password:
COM1#copy runn
COM1#copy running-config start
COM1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
COM1#copy start
COM1#copy startup-config tftp
Address or name of remote host []? 192.168.1.20
Destination filename [COM1-config]? save-com1
```

Et dans un nouveau switch on pourrait récupérer cette sauvegarde en toute simplicité :

```
Switch(config-if)#  
%LINK-5-CHANGED: Interface Vlan1, changed state to up  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, ch  
  
Switch(config-if)#exit  
Switch(config-if)#exit  
Switch(config)#exit  
Switch#  
%SYS-5-CONFIG_I: Configured from console by console  
  
Switch#copy tftp star  
Switch#copy tftp startup-config  
Address or name of remote host []? 192.168.1.20  
Source filename []? save-com1
```

Troisième couche de sécurité : gestion des pannes et redondance.

Le routeur Pfsense sera équipé d'un DHCP et d'un DNS relais en cas de panne du serveur DHCP/DNS. Un script se connecte en SSH et testera les services pour s'assurer qu'ils fonctionnent, dans le cas contraire, le DHCP et/ou DNS du routeur pfsense prendront le relais.

```
====line 14 col 0 lines from top 14 =====  
echo "connexion ssh"  
if ssh root@192.168.60.8 "ps aux | grep -v grep | grep dhcpd"; then  
    echo "le dhcp fonctionne correctement"  
    if ps aux | grep -v grep | grep isc-dhcp-server.service; then  
        service dhcpd stop interface=em1  
    fi  
else  
    echo "le dhcp ne fonctionne plusm qctivqtion du dhcp relai"  
    if -ne ps aux | grep -v grep | grep isc-dhcp-server.service; then  
        service dhcpd start interface=em1  
    fi  
fi
```

Ce script permet une fois exécuté de lancer le service dhcp si le dhcp distant du retour pfsense ne fonctionne plus.

Pour qu'il soit exécutable par tous on change le mod :

Chmod +x test.sh

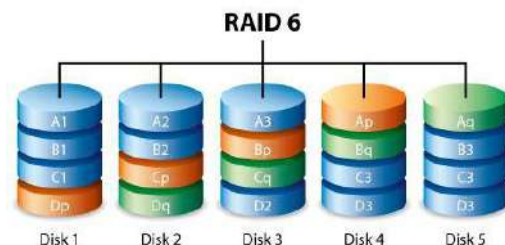
Pour mettre notre fichier script en tâche planifiée :

```
crontab -e
```

```
*/1 * * * * /test.sh >/dev/null 2>&1 # on ajoute cette ligne pour dire à crontab de lancer le script toutes les 1 minutes.
```

```
GNU nano 3.2 /tmp/crontab.cJd1Qg/crontab
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# 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
*/1 * * * * /test.sh >/dev/null 2>&1
```

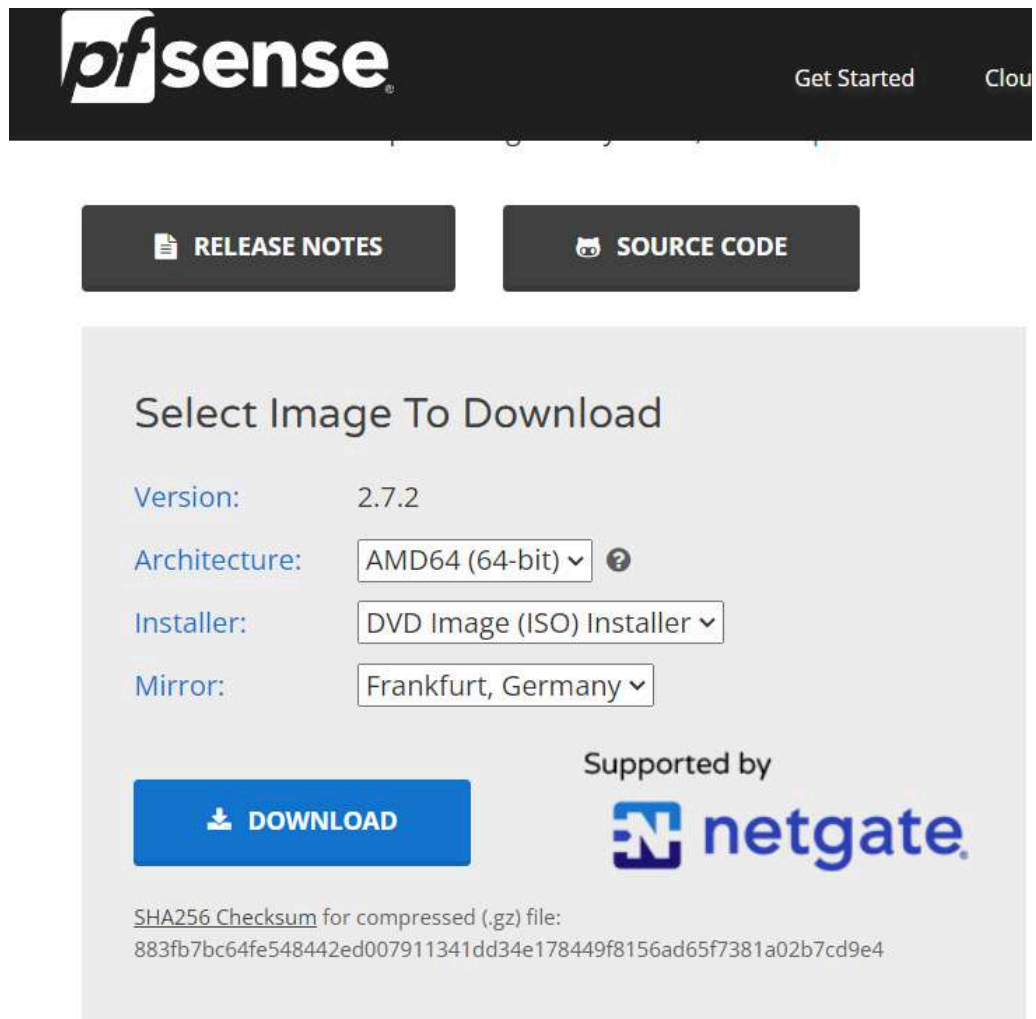
La configuration des disques durs de certains serveurs notamment des serveurs de fichiers sera basé sur la configuration RAID6 où chaque disque dur possède un bloc de parité qui permet de calculer les données perdues dans le cas où un autre disque lâche.



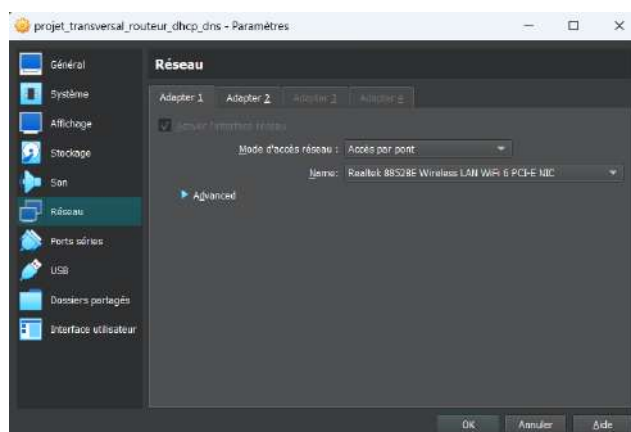
Couplé à ce système, un serveur de sauvegarde des données sera mis en place pour effectuer des sauvegardes régulières détaillés dans le pdf concernant la « DESCRIPTION DE LA SOLUTION DE SAUVEGARDE CHOISI ».

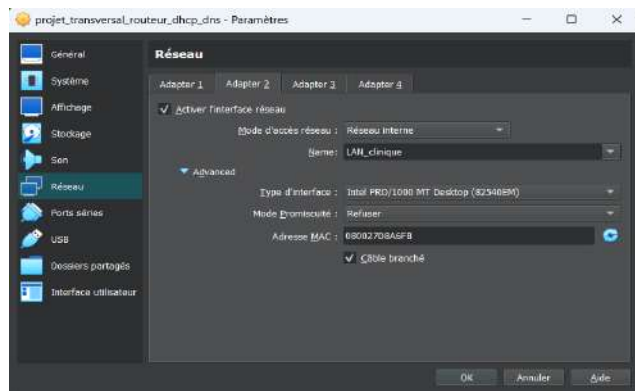
4/ Mettre en place un routeur Pfsense

On installe le fichier .iso de pfsense trouvé sur le site web de pfsense :

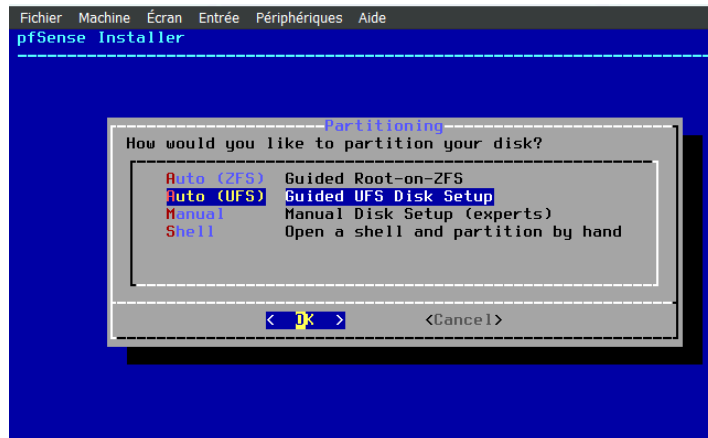
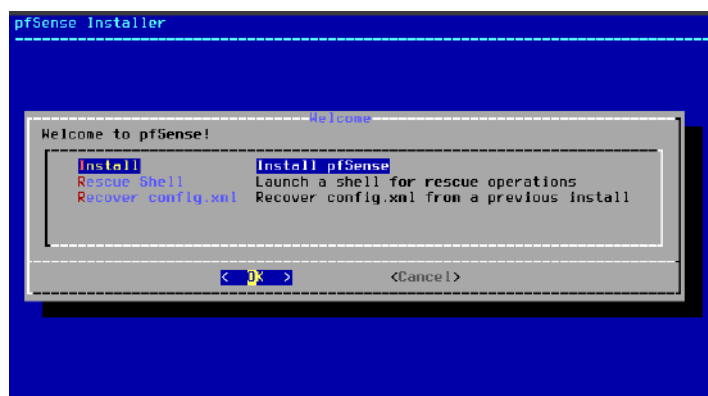


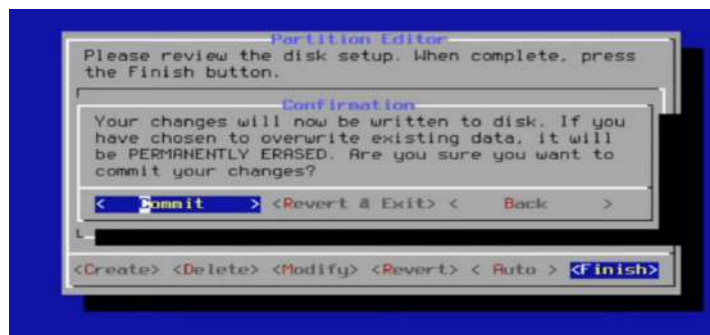
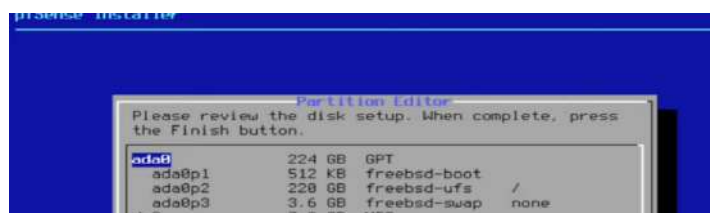
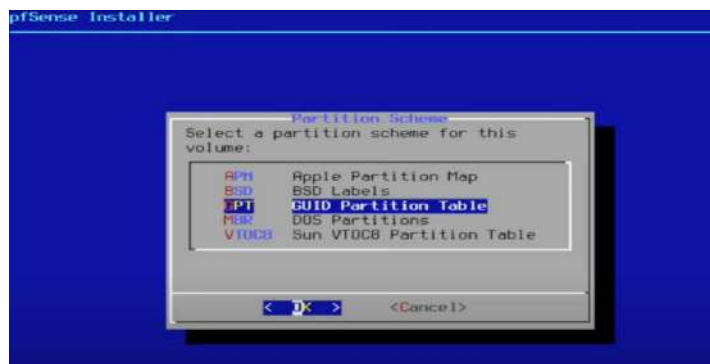
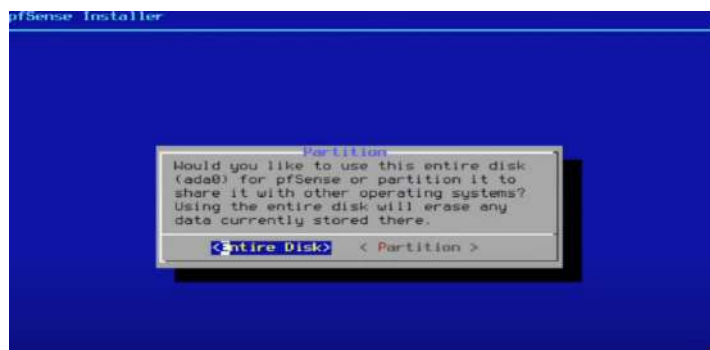
Puis on crée une nouvelle machine virtuelle avec deux interfaces réseaux correspondant aux deux «pattes » de notre retour -> une pour accéder au WAN (internet) et l'autre qui accède au LAN (réseau interne de la clinique)





On lance ensuite le processus d'installation en démarrant la machine virtuelle avec l'iso de pfSense et on effectue l'installation :





On lance une installation auto USB car nous voulons installer le routeur sur un seul disque et nous précisons qu'il va prendre tout l'espace.

Une fois l'installation terminée, on éjecte le disque iso puis on reboot la machine.

Problème rencontré : message d'erreur « root mount waiting for : cam usb1 » après le reboot, précisant qu'il manque des performances matérielles. On passe la machine à 2 cœurs de processeur et le lancement du routeur s'effectue correctement.

```

Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 0eaf63f1122bdca2acda

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.169/24
LAN (lan)      -> em1      -> v4: 192.168.60.1/24

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: █

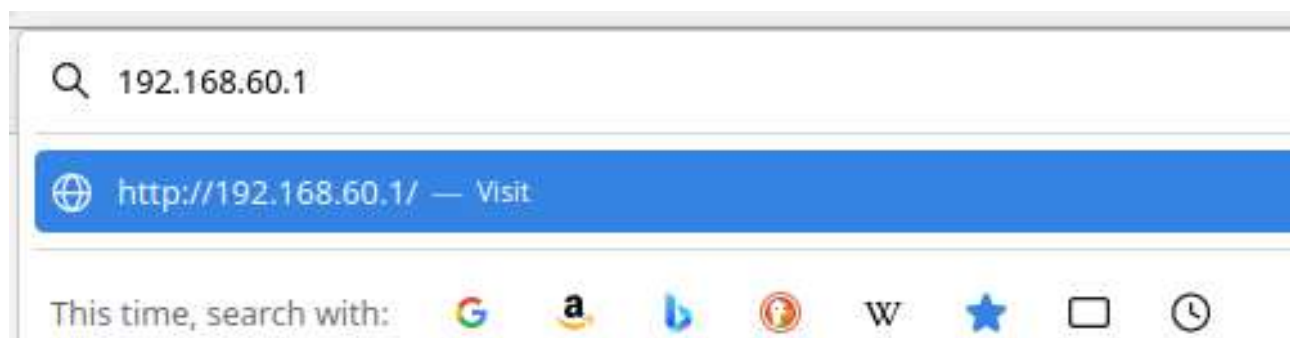
```

Pour tester le réseau en virtuel, notre réseau WAN étant déjà en 192.168.1.0, on passe le réseau virtuel LAN en 192.168.60.0 ; L'adresse ip de notre passerelle LAN est donc 192.168.60.1.

Une fois cette interface affichée, on peut taper « 1 » pour assigner une nouvelle interface et on va lui préciser qu'elle carte réseau assigner au WAN et qu'elle carte réseau assigner au LAN. Puis on tape « 2 » et on précise l'adresse ip et le masque de chacune des cartes.

Mise en place des règles de firewall :

Dans notre machine cliente Debian12 on lance un navigateur et on saisie l'adresse ip de notre routeur pour accéder à l'interface pfsense :





Username or Password incorrect

SIGN IN

admin

SIGN IN

L'identifiant et le mot de passe par défaut sont admin/pfsense.

Une fois connecté on peut accéder à l'interface des règles de firewall et créer nos permissions et conditions pour sécuriser le réseau.

Concernant les règles de pare feu on a tout mis en autoriser tout :

Nous nous rendons dans Firewall--> puis Rules:

Règle WAN: Nous pourrions ici ajouter des règles pour administrer les informations pouvant sortir sur internet ou non.

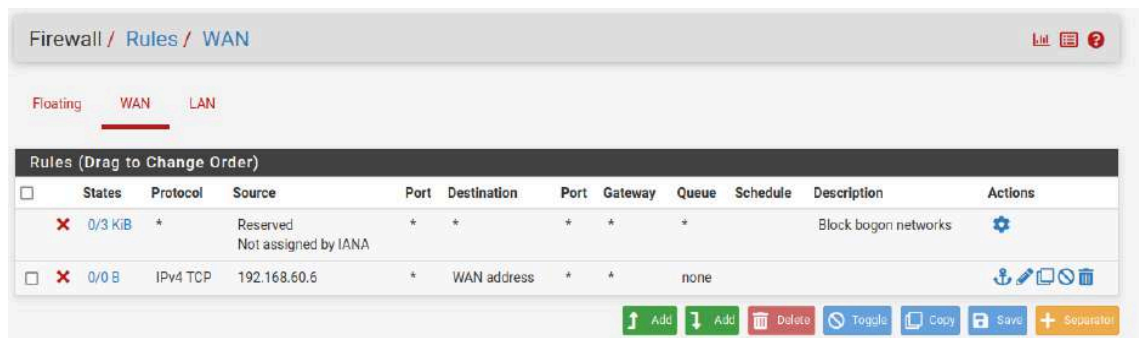
Firewall / Rules / WAN

Floating WAN LAN OPT1 MDECIN FREEWIFI SERVEUR

Rules (Drag to Change Order)

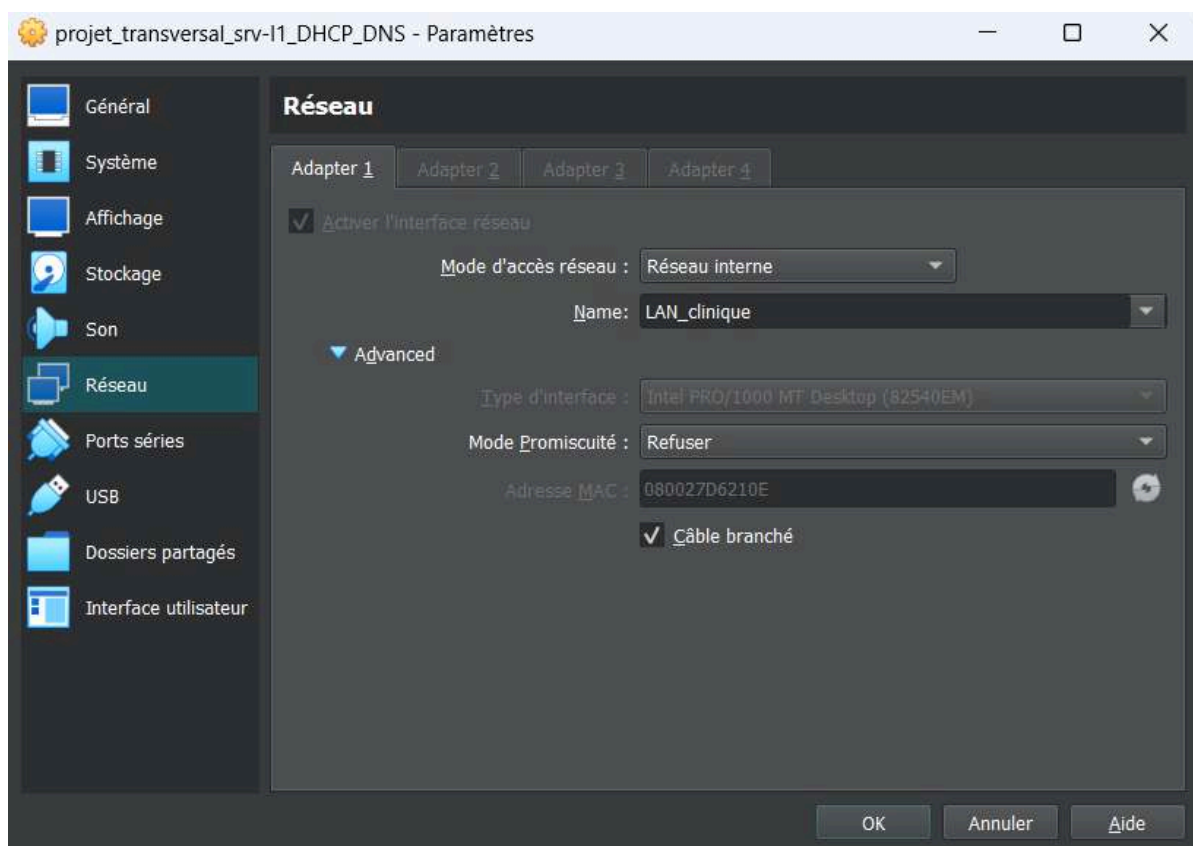
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	0/87 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
☒	0/1 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

On peut créer différentes règles comme par exemple interdire nos serveurs de fichiers et de sauvegarde de communiquer avec l'extérieur ou de recevoir de l'extérieur pour les sécuriser en interne.



5/ Mettre en place le serveur Srv-I3 DNS/DHCP sous debian10

Dans un premier temps, nous allons créer une nouvelle machine sous debian10 en la plaçant dans notre réseau interne « LAN_clinique » tout comme la carte réseau LAN de notre routeur



Ensuite on démarre la machine en laissant Debian10 s'installer, une fois l'installation faite, et les identifiants définies, on se connecte en root et on bascule notre machine en IP statique.

En effet, cette machine est le serveur qui va attribuer automatiquement des adresses au reste du réseau avec son service DHCP et va également nommer les autres machines avec le service DNS, on veut le garder constamment allumé et qu'il ai une adresse fixe.

```
GNU nano 3.2                               /etc/network/interfaces          Modifié

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
    address 192.168.60.8/24
    gateway 192.168.60.1
    dns-nameservers 8.8.8.8
```

Aide	Écrire	Chercher	Couper	Justifier	Pos. cur.	Annuler
Quitter	Lire fich.	Remplacer	Coller	Orthograp.	Aller lig.	Refaire

On reboot la machine, et notre serveur Srv-I3 a maintenant accès à internet depuis notre passerelle, comme l'illustre le ping fonctionnel vers www.google.fr :

```
root@SRV-I3:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d6:21:0e brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.8/24 brd 192.168.60.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed6:210e/64 scope link
        valid_lft forever preferred_lft forever
root@SRV-I3:~# ip route
default via 192.168.60.1 dev enp0s3 onlink
192.168.60.0/24 dev enp0s3 proto kernel scope link src 192.168.60.8
root@SRV-I3:~# ping www.google.fr
PING www.google.fr (216.58.214.163) 56(84) bytes of data.
64 bytes from mad01s26-in-f3.1e100.net (216.58.214.163): icmp_seq=1 ttl=118 time=9.11 ms
64 bytes from mad01s26-in-f3.1e100.net (216.58.214.163): icmp_seq=2 ttl=118 time=10.5 ms
64 bytes from mad01s26-in-f3.1e100.net (216.58.214.163): icmp_seq=3 ttl=118 time=8.48 ms
```

Mise en place du service DNS avec BIND9

Dans un premier temps nous allons installer sur la machine le service DNS. Nous allons donc déjà renommer notre machine en SRV-I3 dans `/etc/hostname` :

```
GNU nano 3.2 /etc/hostname Modifié
debian.srv-i3
```

On modifie `/etc/hosts` avec le nom de la machine et son adresse ip pour utiliser localement les adresses ip en tant que résolution des noms sans utiliser le service DNS

```
GNU nano 3.2 /etc/hosts Modifié
127.0.0.1    localhost
127.0.1.1    debian.srv-13    debian
192.168.60.8  debian.srv-13    debian

# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

Ensuite met à jour les derniers packets de cette machine avec la commande :

```
apt update puis apt upgrade
```

Puis on installe le service Bind9 dnsutils avec la commande :

```
apt install bind9 dnsutils
```

On intègre le serveur dans notre infrastructure en tant que serveur DNS en le précisant :

```
nano /etc/resolv.conf
```

```
GNU nano 3.2 /etc/resolv.conf Modifié
domain debian.srv-13
search debian.srv-13
nameserver 192.168.60.8
nameserver 8.8.8.8
```

On redémarre le service réseau :

```
systemctl restart networking.service
```

Après l'installation de bind9, on répertoire est apparu dans /etc/ il s'appelle /etc/bind.

Dans /etc/bind/named.conf.local on va configurer deux zones, une pour les adresses ip et l'autres pour traduire ces adresses en noms.

```
nano /etc/bind/named.conf.local
```

```
GNU nano 3.2 /etc/bind/named.conf.local Modifié
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "debian.srv-13" {
    type master;
    file "/etc/bind/db.debian.srv-13";
};
zone "60.168.192.in-addr.arpa"{
    type master;
    file "/etc/bind/db.60.168.192.in-addr.arpa";
};
```

Avec un fichier : **debian.srv-13**

et un fichier qui reprend notre adresse réseau : **60.168.192.in-addr.arpa**

Maintenant nous allons créer ces fameux fichiers comportant la configuration des zones.

```
GNU nano 3.2 /etc/db.debian.srv-13
$TTL 10800
$ORIGIN srv-13.
@      IN  SOA  debian.srv-13. root.srv-13. (
        20180906;
        3h;
        1h;
        1w;
        1h);
@      IN  NS   debian.srv-13.
debian IN  A     192.168.60.8
host   IN  A     192.168.60.1
```

```
GNU nano 3.2 /etc/bind/db.60.168.192.in-addr.arpa
$TTL 10800
$ORIGIN 60.168.192.in-addr.arpa.
@      IN  SOA  debian.srv-13. root.srv-13. (
        20180906;
        3h;
        1h;
        1w;
        1h);
@      IN  NS   debian.srv-13.
132    IN  PTR  debian.srv-13.
1      IN  PTR  host.srv-13.
```

On relance bind9 :

```
Systemctl reload bind9
```

On peut vérifier le lien entre les adresses ip et les noms par la commande :

```
Nslookup
```

server localhost

dig debian.srv-l3

ou dig 192.168.60.8.srv-l3

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;debian.srv-l3.                IN      A
;
;; AUTHORITY SECTION:
;                3229      IN      SOA      a.root-servers.net. nstld.verisign-grs.com. 20231225
00 1800 900 604800 86400
;
;; Query time: 56 msec
;; SERVER: 192.168.60.1#53(192.168.60.1)
;; WHEN: lun. déc. 25 11:27:48 CET 2023
;; MSG SIZE rcvd: 117

root@debian:~# dig 192.168.60.8.srv-l3

; <<> DiG 9.11.5-P4-5.1+deb10u9-Debian <<> 192.168.60.8.srv-l3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 30721
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;192.168.60.8.srv-l3.         IN      A
;
;; AUTHORITY SECTION:
;                3142      IN      SOA      a.root-servers.net. nstld.verisign-grs.com. 20231225
00 1800 900 604800 86400
;
;; Query time: 1 msec
;; SERVER: 192.168.60.1#53(192.168.60.1)
;; WHEN: lun. déc. 25 11:29:15 CET 2023
;; MSG SIZE rcvd: 123

root@debian:~# _
```

Le service DNS est bien fonctionnel

Mettre en place un service de DHCP avec DHCPD

On installe le service : **isc-dhcp-server**

apt install isc-dhcp-server

isc-dhcp-server nous à créé plusieurs fichiers que l'on doit configurer pour faire fonctionner le DHCP

nano /etc/dhcp/dhcpd.conf

On configure avec les adresses ip correctes de notre réseau clinique :

```
GNU nano 3.2 /etc/dhcp/dhcpd.conf Modifié

#subnet 10.254.239.0 netmask 255.255.255.224 {
#  option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
#}

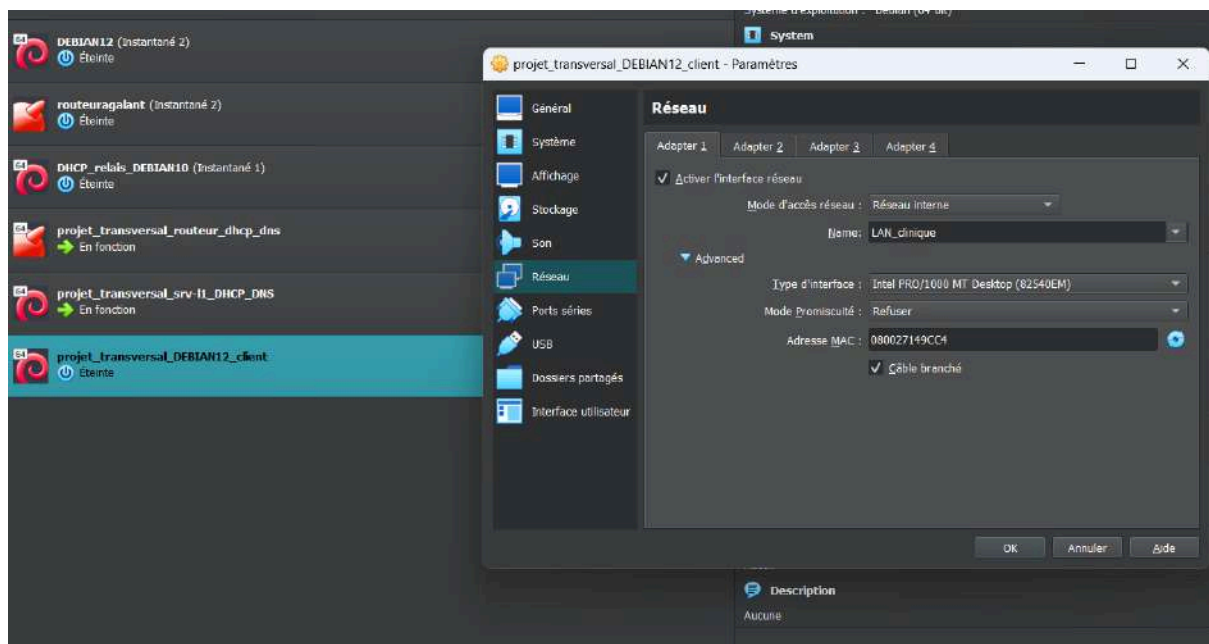
# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#  range dynamic-bootp 10.254.239.40 10.254.239.60;
#  option broadcast-address 10.254.239.31;
#  option routers rtr-239-32-1.example.org;
#}

# A slightly different configuration for an internal subnet.
subnet 192.168.60.0 netmask 255.255.255.0 {
  range 192.168.60.15 192.168.60.254;
  option domain-name-servers 192.168.60.8, 8.8.8.8;
  option domain-name "192.168.60.8";
  option routers 192.168.60.1;
#  option broadcast-address 10.5.5.31;
#  default-lease-time 600;
#}
```

Le service DHCP est maintenant opérationnel !

Test des services mis en place



Pour tester les services mis en place dans le réseau, on ajoute au réseau LAN_clinique une machine virtuelle « cliente » qui peut s'apparenter à un poste administrateur du réseau de la clinique puisqu'il a accès à toutes les machines. (Ce pc devra être stocker dans un lieu sécurisé avec des portes

badgées comme la salle des serveurs de fichiers)

```
Terminal
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
root@debian12:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:14:9c:c4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.15/24 brd 192.168.60.255 scope global dynamic enp0s3
        valid_lft 85710sec preferred_lft 85710sec
    inet6 fe80::a00:27ff:fe14:9cc4/64 scope link
        valid_lft forever preferred_lft forever
root@debian12:~#
```

Une fois la machine mis dans le bon réseau, on voit avec la commande `ip a` que notre serveur DHCP lui a bien attribué la première adresse disponible soit : 192.168.60.15. Il est bien fonctionnel.

```
Terminal
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
GNU nano 7.2 /etc/resolv.conf
domain 192.168.60.8
search 192.168.60.8
nameserver 192.168.60.8
nameserver 8.8.8.8
```

Il lui a également attribué le bon serveur DNS.

6/ Mise en place DHCP/DNS relais

Pour détecter la panne du DHCP/DNS automatiquement :

On met en place une communication ssh par clé

Sur la machine relais (routeur pfsense) on gère une paire de clés ssh pour mettre en place une communication distante sécurisée entre elle (routeur pfsense) et le serveur DHCP srv-l3:

```
ssh-keygen -t rsa
```

```
[2.7.2-RELEASE][root@pfSense.home.arpal]/root: ssh-keygen -t rsa
Bad escape character 'ygen'.
[2.7.2-RELEASE][root@pfSense.home.arpal]/root: ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:iRbK89oAMFyAqMxiYKCKrodEkD0Ty49rJh16v68evc0 root@pfSense.home.arpal
The key's randomart image is:
+---[RSA 3072]-----+
|==oo|
|XoB.|
|X=oo.|
|==.+ . o .|
|=.o.= o S|
|o+ oo+|
|+o+o...|
|o+. o++|
|...ooo.E|
+-----[SHA256]-----+
[2.7.2-RELEASE][root@pfSense.home.arpal]/root: █
```

On s'assure que notre serveur DHCP/DNS a bien ssh d'installer :

```
ssh -v
```

sinon on l'installe

```
apt install ssh
```

On envoie la clé de notre routeur pfsense au serveur DHCP distant

```
ssh-copy-id -i /root/.ssh/id_rsa.pub root@192.168.60.8
```

On peut désormais se connecté en ssh depuis notre routeur à notre serveur dhcp :

```
[2.7.2-RELEASE][root@pfSense.home.arpal]/root: ssh root@192.168.60.8
Linux debian.srv-13 4.19.0-25-amd64 #1 SMP Debian 4.19.289-2 (2023-08-08) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Dec 31 16:08:06 2023 from 192.168.60.1
root@debian:~# █
```

Script, tâche planifié, connexion en SSH sous linux :

Commençons par le DHCP :

Le service DHCP par défaut sur notre routeur pfsense est isc-dhcpd
 ps aux | grep -v grep | grep isc-dhcpd : voir le status en cours

Si le status est en cours grep nous retourne une commande sinon il ne renvoie rien.^

```
[2.7.2-RELEASE][root@pfSense.home.arpal/usr/local/etc: service isc-dhcpd onestat
us
dhcpd is not running.
[2.7.2-RELEASE][root@pfSense.home.arpal/usr/local/etc: service isc-dhcpd onestart
█
```

On peut utiliser les deux commandes ci-dessus sur pfsense pour voir la status d'un service et le lancer ou l'arrêter.

On crée un script test.sh sur notre routeur pfsense :

```
echo "connexion ssh"
if ssh root@192.168.60.8 "ps aux | grep -v grep | grep dhcpd"; then
    echo "le dhcp fonctionne correctement"
    service isc-dhcpd onestop
else
    echo "le dhcp ne fonctionne plus activation du dhcp relai"
    service isc-dhcpd onestart
fi
```

Ce script permet une fois exécuté de lancer le service dhcp pfsense si le dhcp distant Srv-I3 ne fonctionne plus.

Pour qu'il soit exécutable par tous on change le mod :

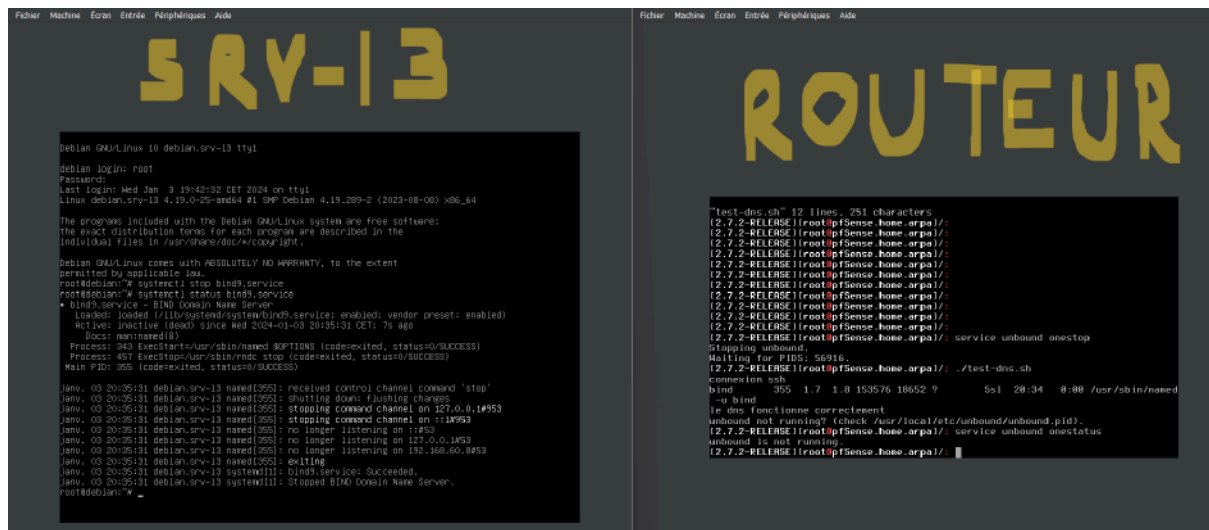
Chmod +x test.sh

On fait la même opération pour le DNS avec un script qui se connecte en SSH à la même machine et lance le service DNS bind9 du routeur pfsense.

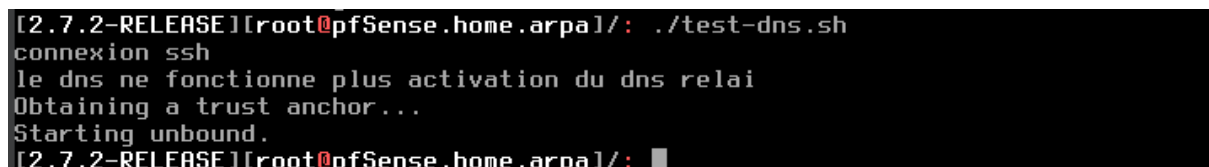
Le service de relais DNS sur le routeur pfsense est par défaut "unbound"

```
[2.7.2-RELEASE][root@pfSense.home.arpal/usr/local/etc/rc.d: service unbound onestart
tart
Obtaining a trust anchor...
Starting unbound.
[2.7.2-RELEASE][root@pfSense.home.arpal/usr/local/etc/rc.d: █
```

```
echo "connexion ssh"
if ssh root@192.168.60.8 "ps aux | grep -v grep | grep bind"; then
    echo "le dns fonctionne correctement"
    service unbound onestop
else
    echo "le dns ne fonctionne plus activation du dns relai"
    service unbound onestart
fi
```



Une fois le service dns du srv-13 éteint et le script du routeur exécuté le service relais démarre et prend le relais;



Pour mettre nos scripts en tâche planifié :

crontab -e

On ouvre crontab avec ee l'équivalent de nano sur pfsense.

`*/1 * * * * /test.sh >/dev/null 2>&1` # on ajoute cette ligne pour dire à crontab de lancer le script toutes les 1 minutes. Même chose pour **test-dns.sh**

```
GNU nano 3.2 /tmp/crontab.cJd1Qq/crontab
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# 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
*/1 * * * * /test.sh >/dev/null 2>&1
```

Le service de relais intégré au routeur fonctionne correctement.

7/ CISCO PACKET TRACER ET MISE EN PLACE VLAN

Présentation :

Cisco Packet Tracer est un logiciel de simulation réseau créé par **Cisco Systems** (d'où il tire le nom). Il est énormément utilisé surtout par les étudiants (évitant d'éventuels problèmes sur des vraies machines) mais aussi les professionnels, c'est un outil très complet permettant d'illustrer et configurer un réseau informatique virtuel. Il ne s'agit donc pas seulement d'un plan (tel que Microsoft Visio) mais d'un plan **fonctionnel** car les éléments (machines, routeur ...) peuvent communiquer, avoir des adresses IP, mettre en place des vlan etc. Dans notre cas il a permis de faire un schéma clair, fonctionnel répondant aux attentes du projet ainsi que de mettre en place l'adressage IP, les vlan...

Voici un plan du projet sur **Cisco Packet Tracer**

The diagram illustrates a complex network topology with three main sites connected via a central cloud. Each site features a 2600-DXT switch, a 3500-33T router, and various servers and printers. The central cloud is represented by a dashed line connecting the three sites. The diagram includes labels for various devices like PC-PT, Server-PT, and Access-PT, as well as IP addresses for Admin, Medecin, and Client.

Key components and connections include:

- Left Site:** 2600-DXT Switch Bc1, 3500-33T Router Bc1, Access-PT, and various PC-PT and Server-PT devices.
- Right Site:** 2600-DXT Switch Bc2, 3500-33T Router Bc2, Access-PT, and various PC-PT and Server-PT devices.
- Central Cloud:** A dashed line connecting the three sites, representing a central cloud or data center.
- IP Addresses:**
 - Ip Admin: 192.168.1.X
 - Ip Medecin: 192.168.2.X
 - Ip Client: 192.168.3.X



Dans l'exemple ci-dessus nous avons 2 switches ne pouvant communiquer qu'entre eux seulement s'ils sont reliés aux même VLAN (représenté par une couleur).

Problème : Si le secrétaire veut échanger avec le boss il ne pourra pas

Access/Trunk :

Les switches sont faits de sorte à pouvoir associer un port à une Vlan c'est ce qu'on appelle le mode **Access** cependant ils peuvent être configurés en mode **Trunk** pour pouvoir accueillir plusieurs Vlan

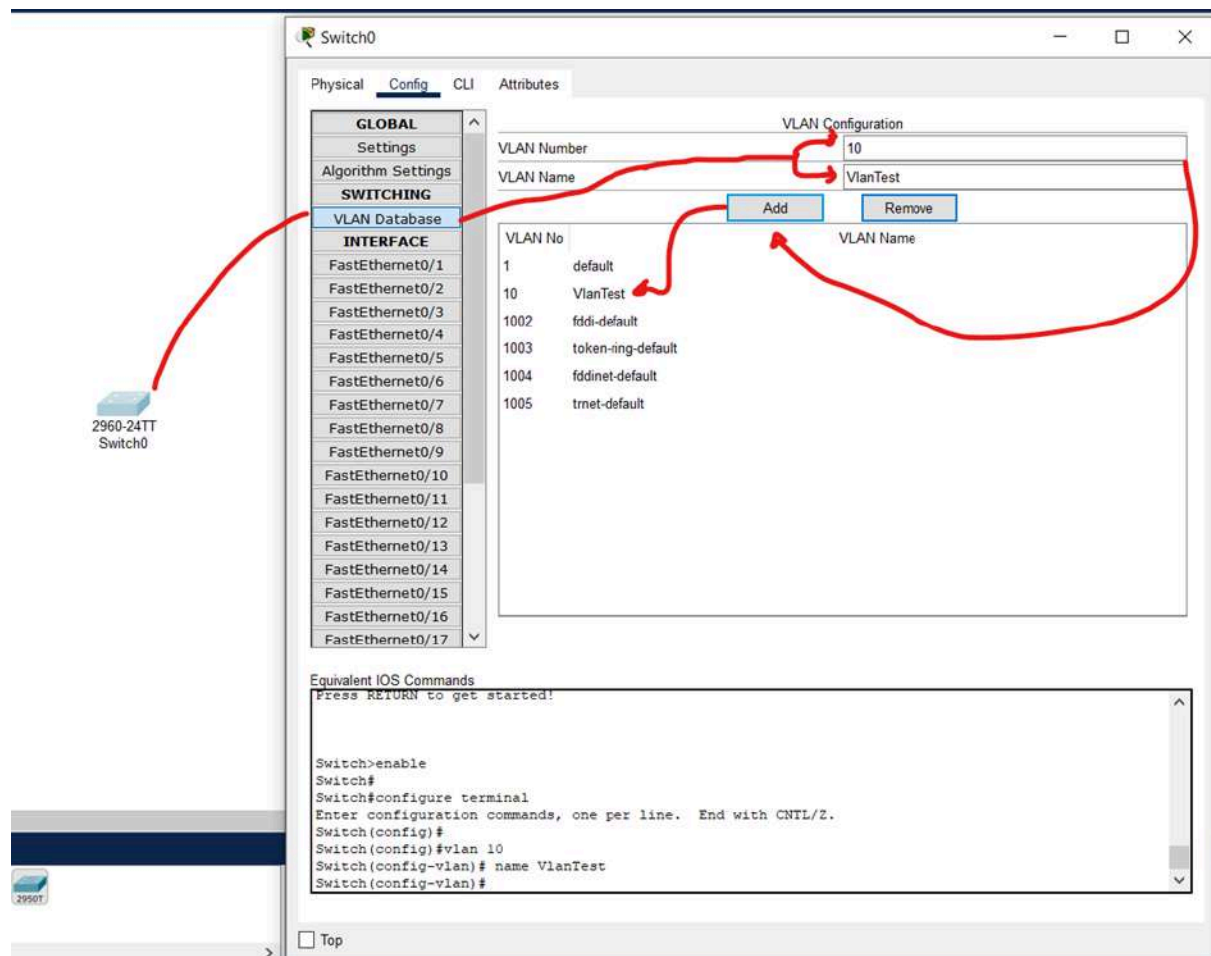


Dans l'image ci-dessus on reprend l'exemple pour les Vlan simple en ayant cette fois-ci intégré un port **Trunk** sur lequel les deux switches sont reliés. L'avantage de celui-ci c'est désormais si le

secrétaire veut communiquer au boss relié en **Trunk** (configuré pour passer la VLAN 10 et 20) il pourra le faire mais pas le vendeur (car n'accepte que 10 et 20 comme dit précédemment).

Ainsi nous pouvons limiter les accès à une ou plusieurs VLAN pour accéder à telle ou telle machine afin de sécuriser l'accès et la confidentialité des données.

Mise en place d'un VLAN sur Cisco Packet Tracer :



Après avoir mis en place son switch dans la configuration on peut apercevoir un onglet **VLAN Database** dans celui-ci on peut créer un VLAN en lui donnant :

- Un Nombre (non existant)
- Un Nom (de préférence simple détaillant son utilité)

Une fois créé, il doit apparaître dans la liste.

Mise en place d'un port Trunk sur Cisco Packet Tracer :

The screenshot shows the configuration window for Switch0 in Cisco Packet Tracer. The 'Config' tab is selected, and the 'FastEthernet0/1' interface is chosen. The 'Trunk' mode is selected in the 'Port Status' dropdown. The 'VLAN' field is set to '10'. The 'Tx Ring Limit' is set to '10'. The 'Port Status' is 'On', 'Bandwidth' is '100 Mbps', and 'Duplex' is 'Full Duplex'. The 'VLAN' list shows '11:Admin' and '12:Medecin' selected, and '13:Client' is not selected. The 'Equivalent IOS Commands' section shows the following commands:

```
Switch(config-if)#
Switch(config-if)#switchport trunk allowed vlan remove 13
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport trunk allowed vlan remove 1003
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport trunk allowed vlan remove 1004
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#switchport trunk allowed vlan remove 1005
Switch(config-if)#
```

Sur chaque port du switch on peut décider qu'elles vlans peuvent communiquer via le port. Dans le cas ci-dessus on décide sur le port 1 de laisser passer la VLAN 11/12 mais pas la 13 ainsi si le client relié en Wifi via un autre port ne pourra pas communiquer à l'appareil branché au port 1 du switch. C'est notamment ce que l'on utilise pour les empêcher d'accéder au réseau Admin et Médecin.

8/ MISE EN PLACE SRV-I1/ SRV-L2 FTP/TFTP + SYSTEME DE SAUVEGARDE + NOTE POUR LA RESTAURATION DES DONNEES

Création du serveur de fichier:

The screenshot shows the 'Général' (General) configuration window for a file server. It has four tabs: 'De base' (selected), 'Avancé', 'Description', and 'Chiffrement de disque'. The 'De base' tab contains the following fields:

- Nom : Serveur fichier
- Type : Microsoft Windows (dropdown menu)
- Version : Windows 2019 (64-bit) (dropdown menu)

There is a small icon with '64' and '2019' next to the version field.

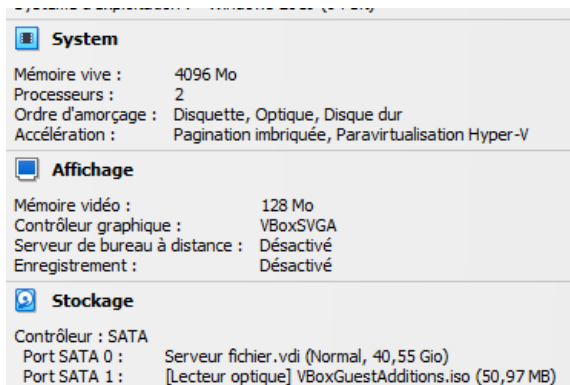
Pour la carte réseau :

The screenshot shows the 'Réseau' (Network) configuration window for a network card. It has four tabs: 'Adapter 1' (selected), 'Adapter 2', 'Adapter 3', and 'Adapter 4'. The 'Adapter 1' tab contains the following fields:

- ☒ Activer l'interface réseau
- Mode d'accès réseau : Réseau interne (dropdown menu)
- Name: Lan2 (dropdown menu)

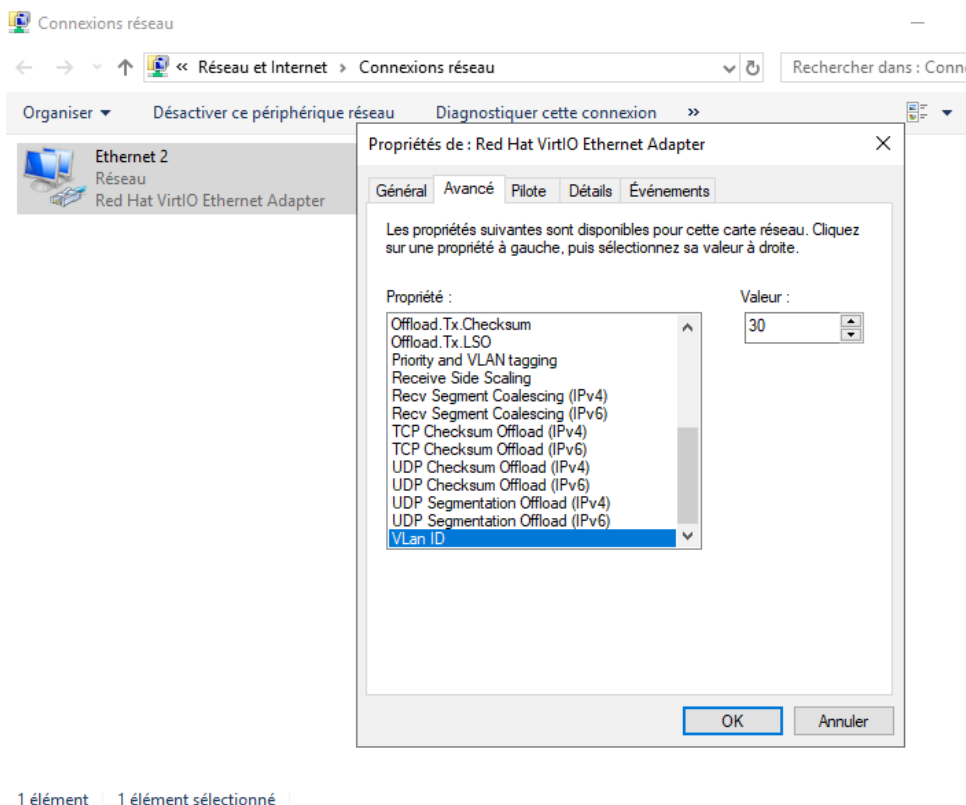
There is a blue play button icon and the text 'Advanced' below the Name field.

Paramètre :



Une fois Windows server installer:

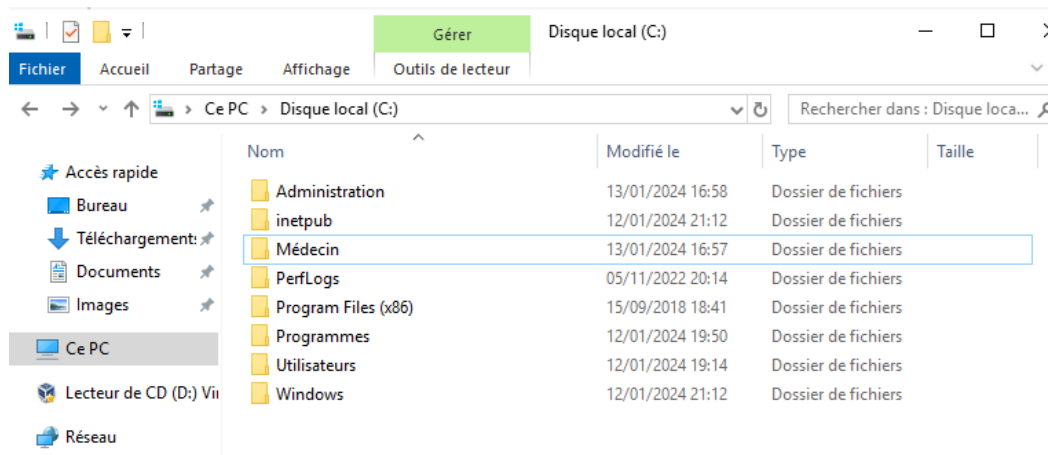
Afin de positionner le serveur fichier dans la Vlan serveur nous devons aller chercher et modifier le vlan Id en tapant la commande suivante "Ncpa.cpl" qui nous permet de s'interagir avec les propriétés de la carte réseau et de donner l'id de la Vlan souhaiter comme ci dessous la valeur "30":



Pour le serveur de fichier nous avons créé des dossiers partager pour que le personnel médical et l'administration puissent y avoir accès :

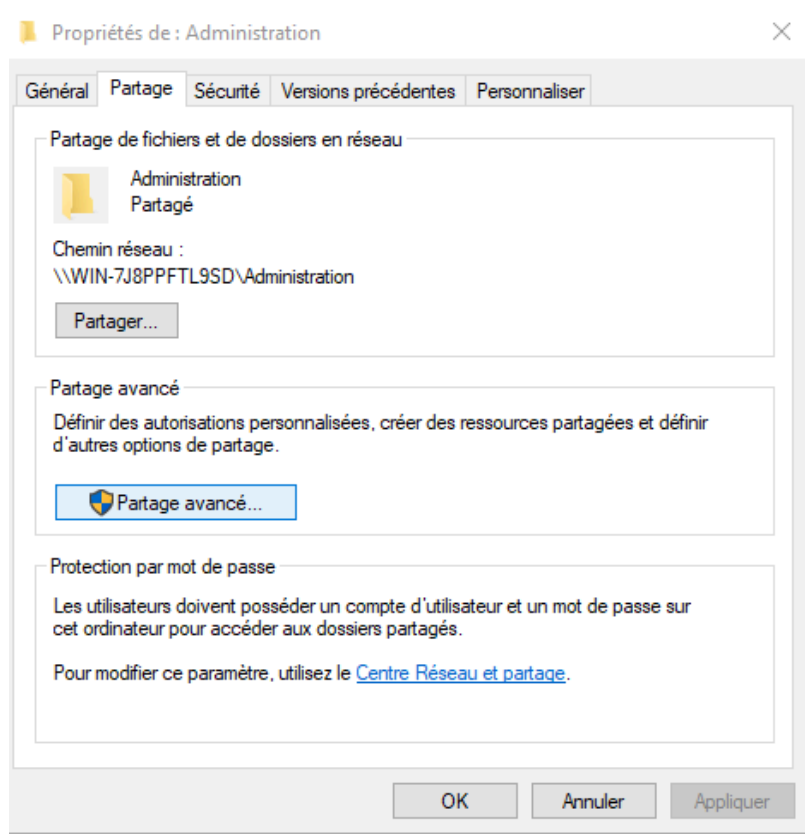
Création des dossiers partagés :

Ici dessous nous avons créé deux fichiers un pour le service Médical et pour l'administration



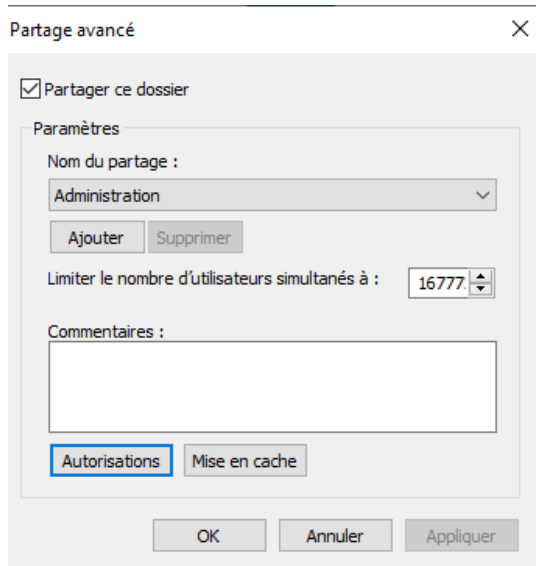
Pour créer un dossier il faut aller dans l'explorateur de fichier-->Ce Pc-->Disque Local(C)

Une fois le dossier créé, allez dans les propriétés de ce dossier



Puis partage avancé:

On peut lui ajouter une description,



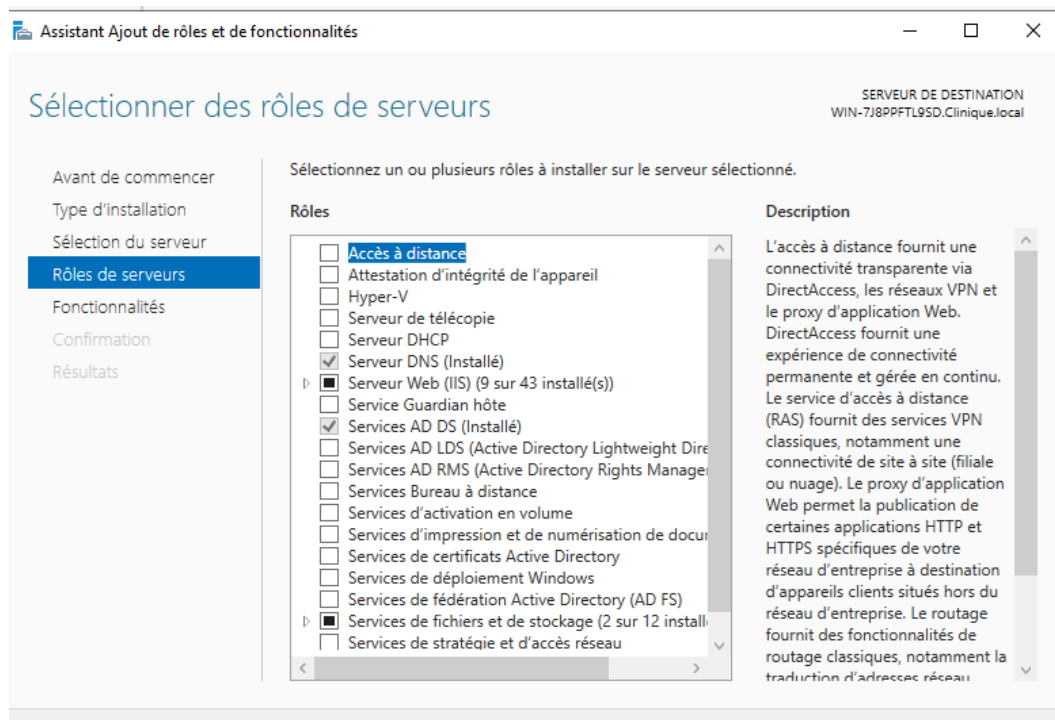
Une fois le partage créer on peut imaginer des permissions qui donnent accès a certain dossier en fonction du rôle des personnes au dans l'entreprise.

Active directory:

L'objectif d'un annuaire comme Active Directory est de centraliser l'authentification et l'accès à un réseau de ressources. Les administrateurs réalisent la configuration des autorisations selon les paramètres choisis. Ils permettent ainsi aux utilisateurs d'accéder aux éléments dont ils ont besoin pour leur activité.

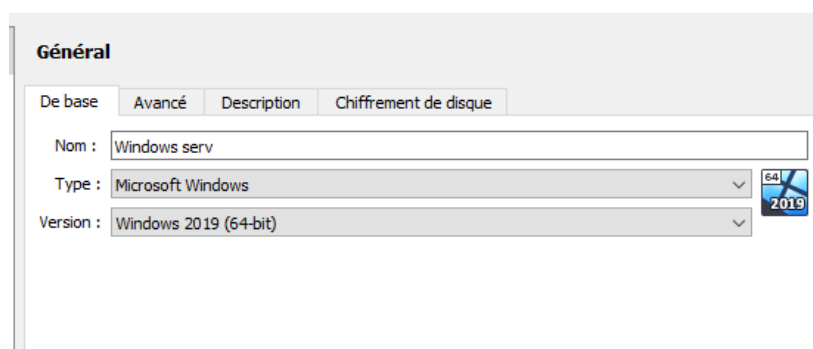
Pour l'activer il faut aller dans le gestionnaire de serveur-->Gérer-->

Ajouter des rôles en fonctionnalités puis mettre service AD DS dans le rôle de serveurs comme ci-dessous.



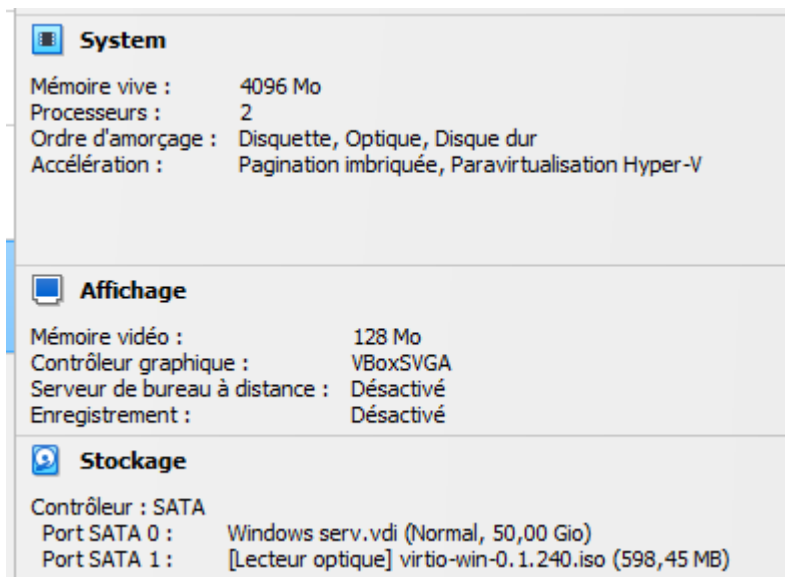
Dès lors que l'installation est terminée, vous pouvez commencer à utiliser votre domaine Active Directory, notamment avec la console Utilisateurs et ordinateurs Active Directory qui sert à gérer les objets dans l'annuaire (utilisateurs, ordinateurs, serveurs, etc.)

Serveur de BackUp:



Nous utilisons comme Iso windows server 2019

Paramètre :



System

Mémoire vive : 4096 Mo
Processeurs : 2
Ordre d'amorçage : Disquette, Optique, Disque dur
Accélération : Pagination imbriquée, Paravirtualisation Hyper-V

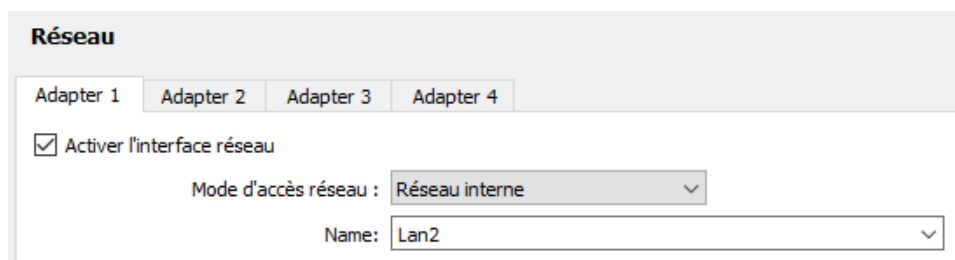
Affichage

Mémoire vidéo : 128 Mo
Contrôleur graphique : VBoxSVGA
Serveur de bureau à distance : Désactivé
Enregistrement : Désactivé

Stockage

Contrôleur : SATA
Port SATA 0 : Windows serv.vdi (Normal, 50,00 Gio)
Port SATA 1 : [Lecteur optique] virtio-win-0.1.240.iso (598,45 MB)

Carte réseau :



Réseau

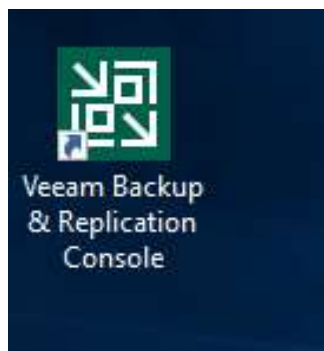
Adapter 1 Adapter 2 Adapter 3 Adapter 4

☒ Activer l'interface réseau

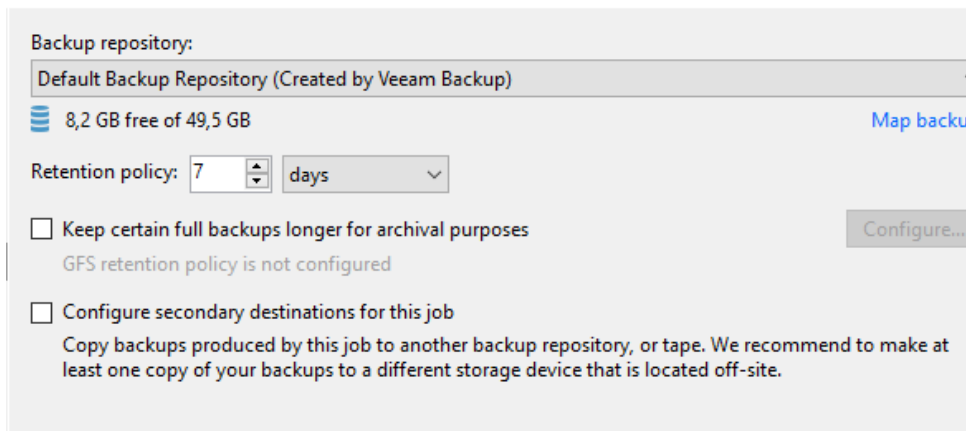
Mode d'accès réseau : Réseau interne

Name: Lan2

A l'aide du logiciel Veeam Backup nous pouvons procéder à des sauvegardes hebdomadaires :



Une fois le logiciel lancé et la sauvegarde créée nous pouvons choisir la fréquence de sauvegarde comme ci-dessous tous les vendredis soir à 22h



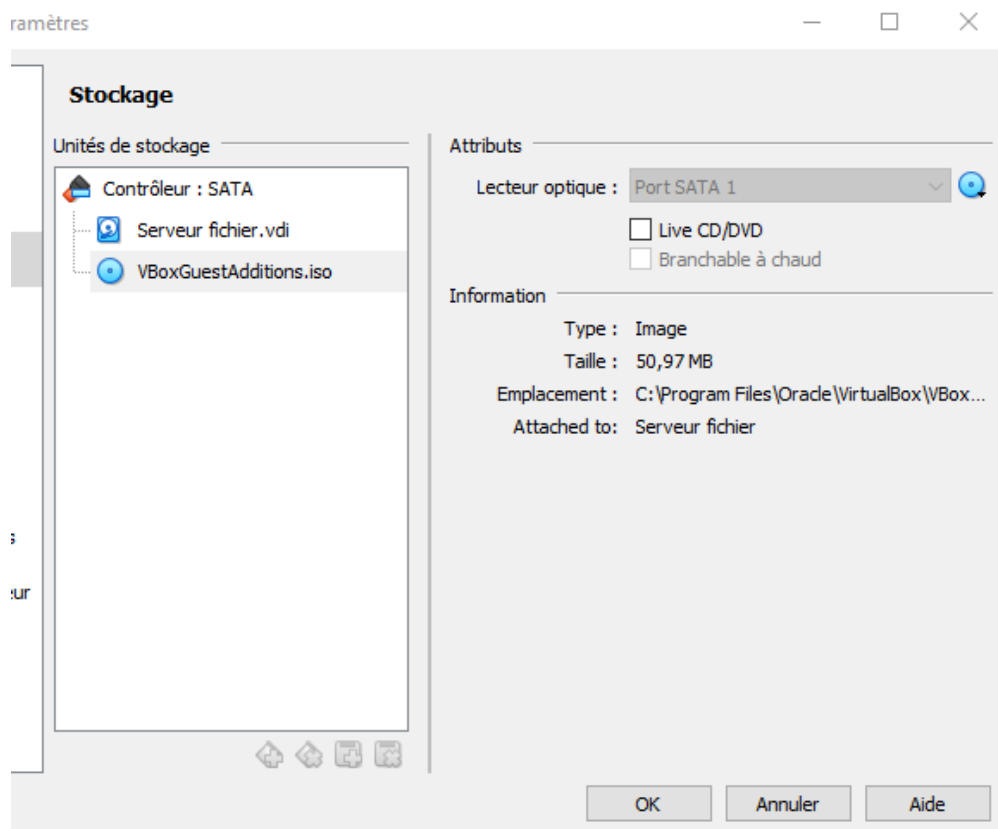
Pilotes VirtIO:

Les pilotes VirtIO sont des pilotes de périphériques paravirtualisés requis pour que les machines virtuelles.

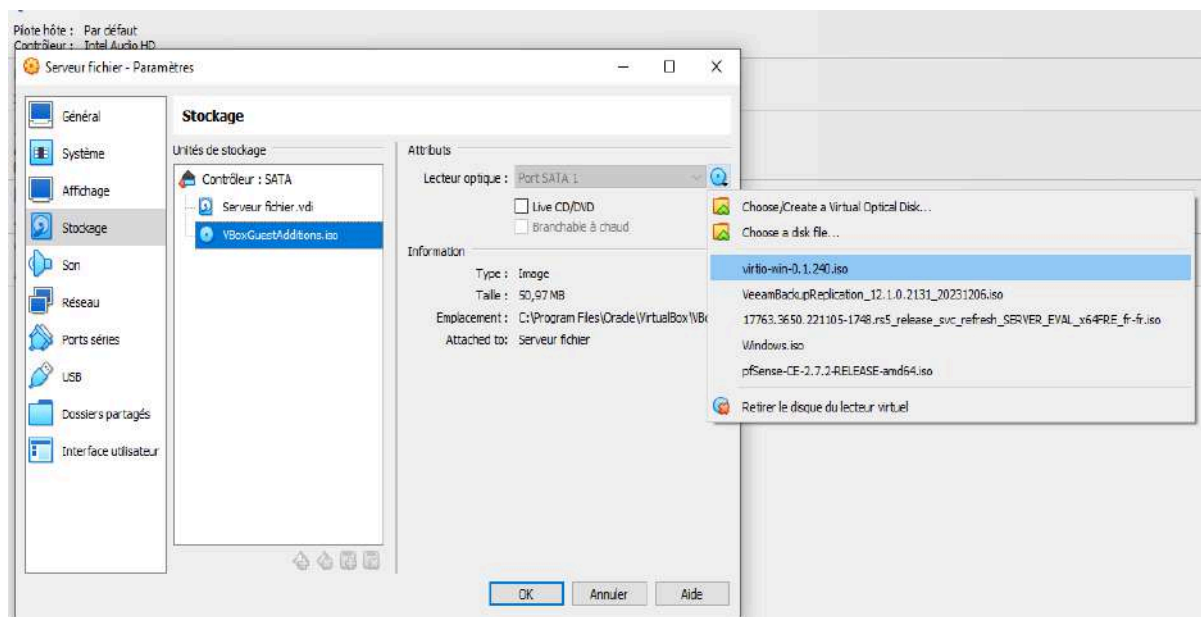
Pour le mettre il faut installer L'iso du pilote VirtIO(trouver sur internet).

Il permet d'avoir accès à internet pour le mettre en place il faut :

-aller dans le stockage de notre machine virtuelle comme ci-dessous



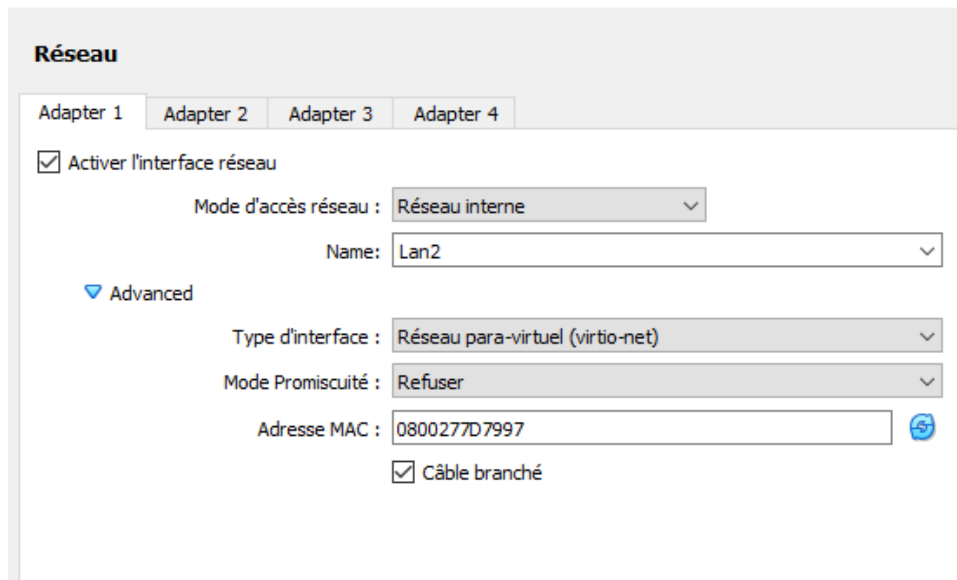
Puis choisir notre iso dans le disque.



Une fois l'iso mit sur notre disque lancer notre machine puis l'exécuter dans notre Disque local sur notre machine virtuelle est l'installer.

Une fois le pilote installer nous disposons de la connexion sur nos machine virtuelle.

J'ai choisi l'interface para-virtuel pour avoir accès au tagging des vlan comme ci dessous:



9/ Responsabilités et règlement pour le stock et la sécurité des données des patients

Quelles données doit-on conserver ?

Dans un premier temps, pour contrôler au mieux des données confidentielles et en assurer la sécurité nous devons récupérer uniquement les données utiles des patients liées aux strictes intérêts des services proposé par la clinique conformément au texte réglementaire européen :

RGPD, Règlement Général sur la Protection des Données.

Les informations enregistrés par la clinique dans les serveurs de fichiers sont :

- Des données de santé,
- Des données d'identification : nom, prénom, date de naissance, sexe, adresse, téléphone, email,
- Le numéro de sécurité sociale,

- Des données relatives à la vie personnelle : habitudes de vie, situation familiale, personnes à contacter, personnes de confiance,
- Des données relatives à la vie professionnelle : métiers passés et actuel, métier à risque,
- Des données pour la facturation : mutuelle, assurance.

Pour gérer ces données, il serait nécessaire de désigner un responsable dans la clinique à la protection des données qui gère toutes ces informations, mais qui doit également être en mesure de répondre aux questions concernant le RGPD.

Ces données devraient être traitées de la manière suivante :

Sauvegarder les intérêts vitaux

Transmettre de manière anonyme à l'État

Transmettre aux assurances maladie pour un remboursement

Pour les applications telles que Rendez-vous, avec bien sûr, un envoi de données adapté à l'application concernée.

Il est absolument interdit d'envoyer ces informations à quiconque d'autre que les personnes mentionnées ci-dessus. Elles ne peuvent être envoyées qu'aux personnes se trouvant dans le même établissement que vous.

Pour assurer la protection, il convient de mettre en place :

- La mise en place d'un registre des traitements pour recenser l'ensemble des traitements mis en œuvre dans l'établissement,
- La réalisation d'analyses d'impact dès lors qu'un traitement présente un risque avéré pour les personnes,
- L'information des personnes concernées,
- La formalisation des rôles et responsabilités de l'établissement et de ses sous-traitants.

Réglementation du point de vu des patients :

La protection des données personnelles – RGPD

Les infrastructures réseau pour votre centre hospitalier accordent une grande importance à la protection de vos données personnelles. Nous nous engageons à collecter et traiter ces données en respectant la loi Informatique et Libertés ainsi que le règlement général sur la protection des données (RGPD) européen. Notre objectif est de garantir la confidentialité et la sécurité de vos informations personnelles.

Comment sont traitées vos données personnelles ?

Les informations recueillies lors de votre consultation ou de votre séjour dans nos établissements font l'objet de traitements informatiques destinés à faciliter votre prise en charge. Le responsable du traitement informatique est le/la Directeur(trice) du centre hospitalier. Il/elle a désigné(e) un(e) responsable à la protection des données. Ce(tte) dernier(e) peut répondre à toutes vos questions concernant la protection des données.

Quelles données personnelles collectons-nous ?

Nos centres collectent et traitent notamment des données personnelles administratives, sociales et médicales telles que :

- Des données de santé,
- Des données d'identification : nom, prénom, date de naissance, sexe, adresse, téléphone, email,
- Le numéro de sécurité sociale,
- Des données relatives à votre vie personnelle : habitudes de vie, situation familiale, personnes à contacter, personnes de confiance,
- Des données relatives à votre vie professionnelle : employeur, métier,
- Des données pour la facturation : mutuelle, assurance.

Quels sont les traitements réalisés ?

Ces données sont saisies dans des logiciels en vue de traitements ayant les finalités suivantes :

- La sauvegarde de vos intérêts vitaux. Entrent dans cette catégorie tous les logiciels utilisés lors des activités de médecine préventive ou bien pour la réalisation de diagnostics médicaux et la traçabilité de l'administration de soins ou de traitements médicaux. Ainsi, sont installés, par exemple, un dossier patient informatisé, des dossiers de spécialité (dialyse, assistance médicale à la procréation), un logiciel de gestion du laboratoire, une application permettant la réalisation d'activités de télémédecine,
- La mise en œuvre d'une obligation légale et réglementaire. Nos infirmeries sont tenues de transmettre aux autorités de l'État, de façon anonymisée, la description de l'activité réalisée par l'établissement, ce qui est usuellement appelé le programme de médicalisation du système d'information (PMSI). Cette activité est placée sous la responsabilité du médecin en charge de l'information médicale,
- La mise en œuvre des intérêts légitimes de l'établissement. Dans ce cadre, l'établissement transmet les éléments de facturation aux organismes d'assurance maladie ainsi qu'aux mutuelles et assurances de santé auxquels vous êtes affilié,
- L'exécution d'une mission de service public. Par exemple, sont utilisés des logiciels pour la gestion des rendez-vous.

A qui ces données sont-elles destinées ?

Vos données sont réservées aux professionnels de nos centres hospitaliers. Ils sont soumis au secret professionnel et leur accès est limité aux catégories de données qui leur sont nécessaires pour vous prendre en charge.

Dans la limite de ce que prévoit la réglementation, ces données peuvent être transmises à des tiers autorisés : Trésor Public, Agence régionale de santé, organismes d'assurance maladie et organismes complémentaires.

Enfin, ces données peuvent également être transmises à des prestataires de services et sous-traitants intervenant pour le compte de nos infirmeries. Dans ce cadre-là, des clauses de conformité au RGPD sont intégrées dans les contrats qu'ils concluent avec nos infirmeries.

L'établissement ne transfère pas de données à caractère personnel à destination d'un Etat n'appartenant pas à l'Union européenne.

Quelle organisation pour protéger vos données personnelles ?

Nos infirmeries mettent en œuvre les obligations posées par le RGPD :

- Mise en place d'un registre des traitements pour recenser l'ensemble des traitements mis en œuvre dans l'établissement,
- Réalisation d'analyses d'impact dès lors qu'un traitement présente un risque avéré pour les personnes,
- Information des personnes concernées,
- Formalisation des rôles et responsabilités de l'établissement et de ses sous-traitants.

Par ailleurs, le centre hospitalier des quatre villes s'efforce de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir la sécurité de son système d'information en tenant compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement.

Vos droits

Conformément à la réglementation, vous disposez des droits suivants :

- Droit d'accès, de rectification, d'effacement et de limitation
- Droit d'opposition
- Droit à la portabilité des données
- Droit au retrait de consentement