How-To : ESXi avec une seule IPv4 et une IPv6

Sommaire

Sommaire 1
Historique 2
Introduction 3
Schéma réseau 3
Schéma classique avec plusieurs IP 3
Schéma avec une seule IPv4 et une seule IPv6 4
Limitations 4
Prérequis 4
Avertissements 5
Désactivation du monitoring 5
Configuration ESXi 7
Activation du support IPv6 7
Configuration IPv6 8
Chargement des ISO sur un datastore 11
Suppression de la configuration IPv4 13
Création des réseaux internes 14
Préparation pfSense 18
Récupération de l'adresse MAC 18
Création de la VM pour pfSense 18
Installation de pfSense 21
Configuration pfSense 27
Premier démarrage 27
Configuration via le WebGUI 30
Configuration des VM 39
Connecter un VM à Internet 39
Connecter Internet à une VM 39
Derniers réglages (optionnels) 42
Réactiver le monitoring 42
Forcer le démarrage de pfSense en au démarrage de l'ESXi 42
VMkernel sur le réseau LAN 43
Connexion au réseau LAN via VPN 46
Reconfigurer ESXi suite une fausse manipulation 47

Historique

V1.0 23/08/2013 :
- création du document

V1.1 28/08/2013 :
- Ajout conseil de sauvegarde du fichier esx.conf
- Ajout reconfiguration du réseau via mode rescue

V2.0 02/08/2014 :
- Modification de la procédure (configuration MAC pour l'interface Dummy/VM Network de pfSense au lieu de spoofing)
- Suppression des « trucs en plus » et insertion dans le corps du document
- Ajout / Correction screenshots (manageur Kimsufi au lieu d'OVH)
- Ajout configuration des VMs
- Ajout autorisation du ping dans pfSense
- Refonte totale du plan

URL du document : http://www.dmilz.net/share/ESXi_Kimsufi_2.0.pdf
Attention si vous utilisez une adresse différente vous essayez sûrement d'accéder à une ancienne version ou une version non officielle.

Les anciennes versions de ce document sont archivées à l'adresse suivante :
www.dmilz.net/share/archives/

Introduction

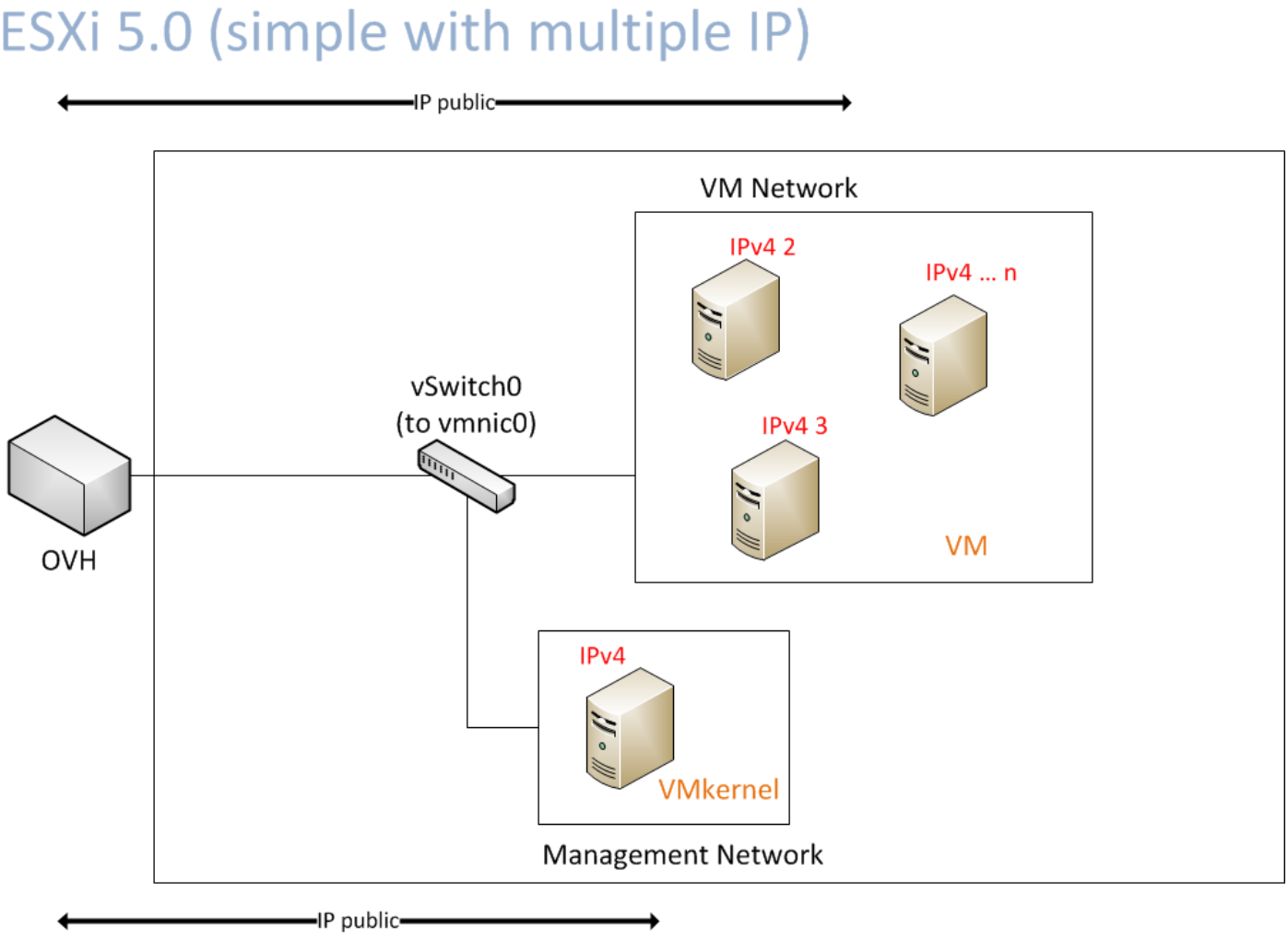
Depuis 2013 les serveurs de la gamme Kimsufi ne disposent plus d'IP Failover et sont livrés avec une seule IPv4 et une seule IPv6. La version d'ESXi 5.0 Update 1 proposée pour Kimsufi ne permettant pas le NAT, il est alors impossible de connecter les VM vers l'extérieur (et inversement). Ce tutorial a donc été écrit pour répondre à cette problématique en attendant un retour éventuel des IP Failover ou secondaires.

L'idée principale consiste à connecter le VMkernel (qui permet de piloter ESXi) avec l'IPv6 et d'allouer l'adresse IPv4 libérée à une VM frontale qui servira de passerelle.

A noter : bien qu'orienté pour Kimsufi ce guide est réutilisable pour d'autre hébergeur avec quelques adaptations.

Schéma réseau

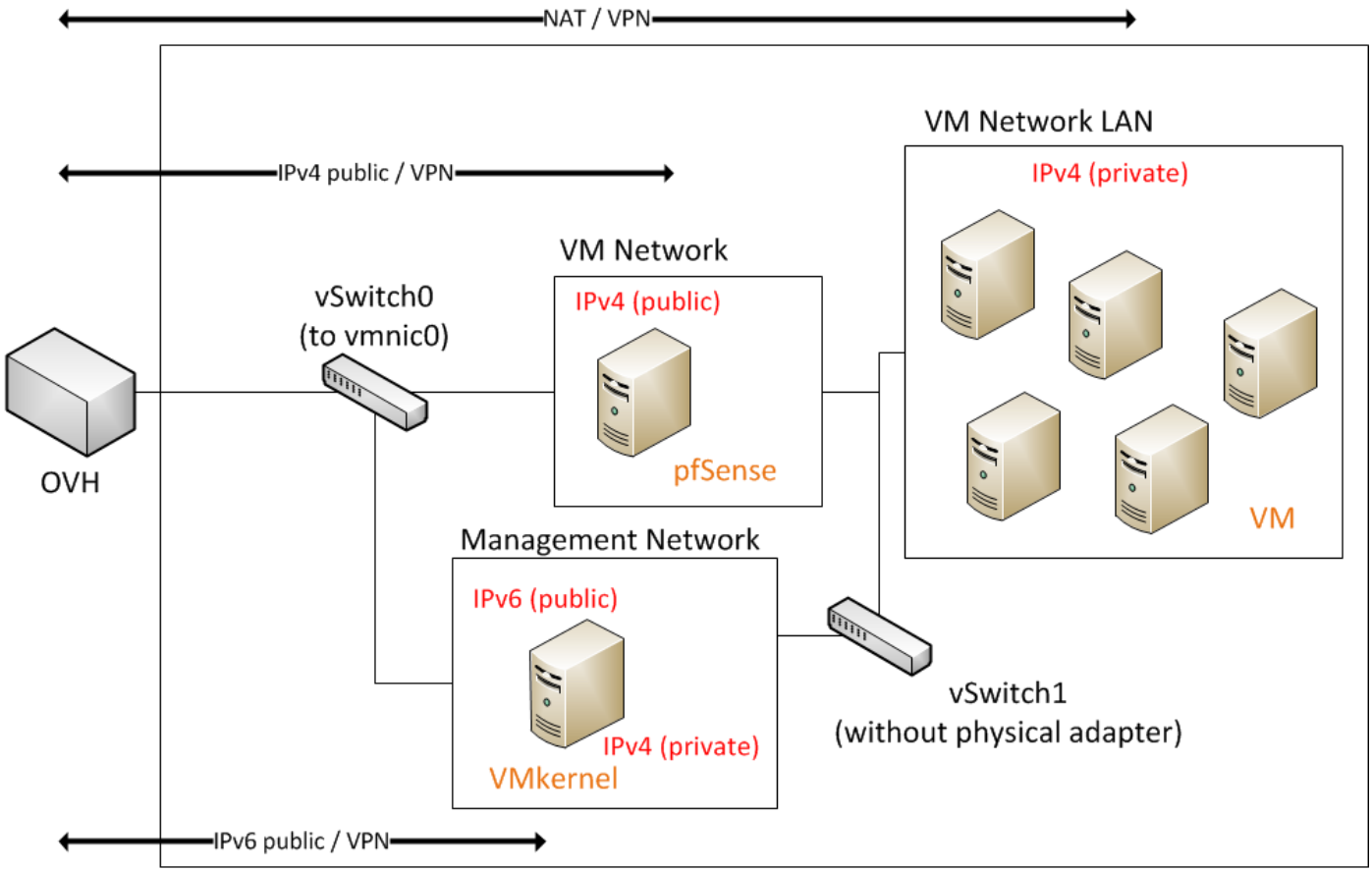
Schéma classique avec plusieurs IP



Dans le cas le plus simple 1 adresse IP publique est assignée au VMkernel puis chaque machine qui doit communiquer avec l'extérieur dispose de sa propre adresse IP publique.

Schéma avec une seule IPv4 et une seule IPv6

ESXi 5.0 (with one IPv4 and one IPv6)



Dans notre cas nous allons :

- Assigner l'adresse IPv6 au VMkernel
- Assigner l'adresse IPv4 alors libérée à une machine en frontal (ici pfSense)
- Utiliser des adresses IPv4 privées pour les VM qui utiliseront la machine en frontal comme passerelle
- Assigner une adresse IPv4 privée au VMkernel pour gérer l'ESXi en IPv4 depuis « l'intérieur » (optionnel)

Limitations

Dans tous les cas nous ne disposerons que d'une seule IPv4 publique. Toutes les connexions depuis l'extérieur vers l'intérieur, et inversement, passeront par pfSense. Les limitations du NAT s'appliquent (translation de port, nombre de connexion, performance…).

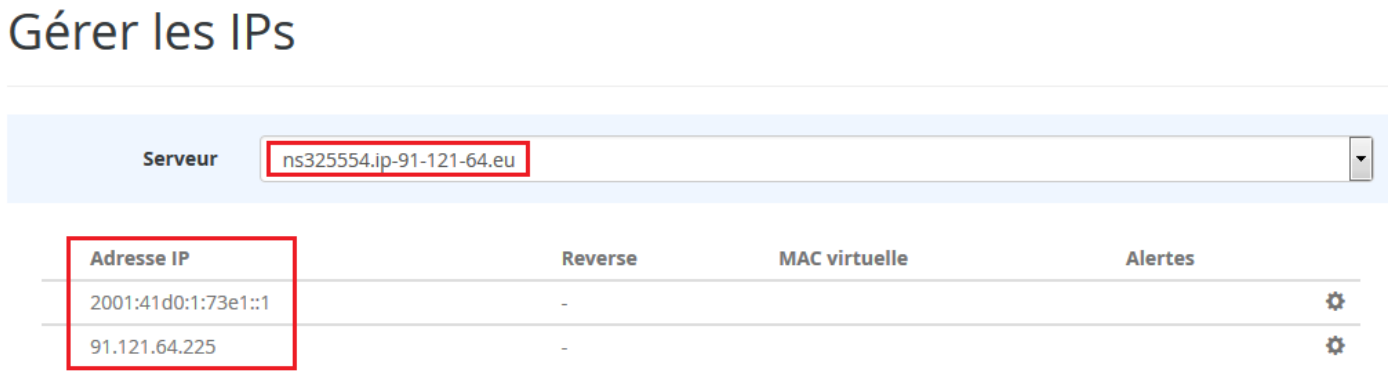
Prérequis

Pour implémenter cette solution il nous faudra :

- Un serveur ESXi (celui fourni par l'hébergeur) avec une adresse IPv4 et une IPv6
- Connaitre un minimum ESXi
- Savoir créer un VM
- Disposer d'une connexion internet IPv4/IPv6 pour configurer le serveur (test http://test-ipv6.com)
- Un ISO de pfSense (https://www.pfsense.org/download/)
- Un Live-CD Ubuntu Desktop (http://www.ubuntu.com/download)

Pour un serveur Kimsufi les adresses IP sont récupérables depuis le manageur Kimsufi (https://www.kimsufi.com/fr/manager/) :

Depuis le menu « IP » :



Pour ce serveur les adresses sont donc :

- 91.121.64.225 (IPv4)
- 2001:41d0:1:73e1::1 (IPv6)

Avertissements

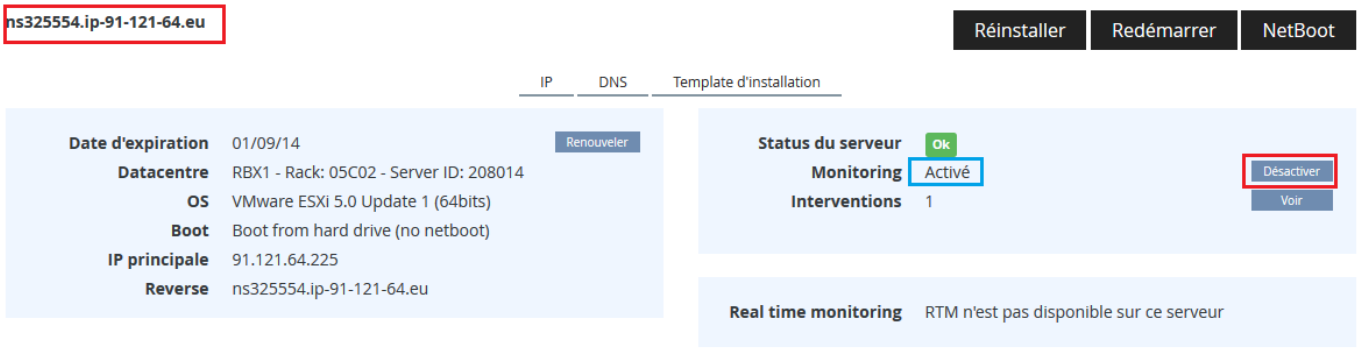
Avant de commencer, vérifiez d'avoir une connexion IPv6 le temps de l'installation !

Nous allons modifier la configuration réseau d'un serveur dans un Datacentre, pas de clavier et d'écran directement branchés directement sur le serveur ni de KVM ou équivalent. En cas de fausse manipulation il est très facile de perdre la main sur le serveur et il faudra passer par l'étape réinstallation ou le mode « rescue » (si l'hébergeur le propose).

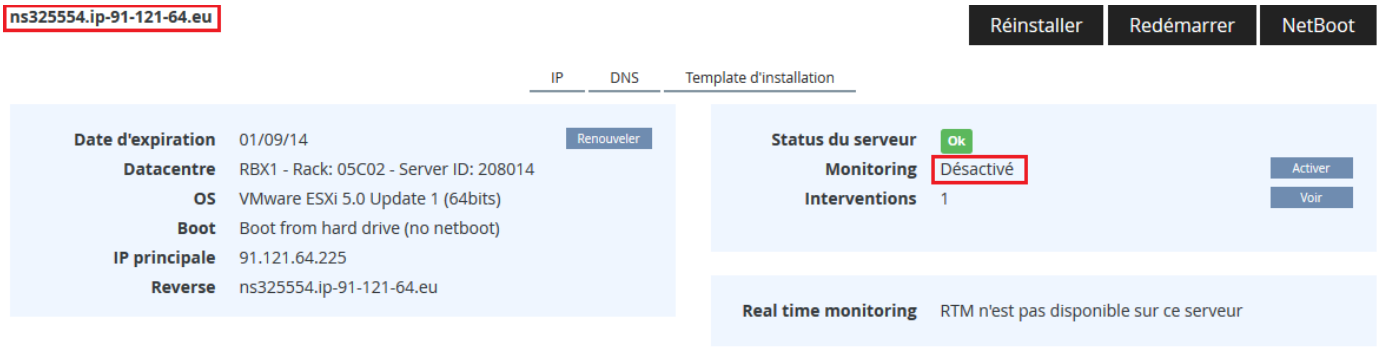
Je vous conseille donc de sauvegarder via SSH le fichier /etc/vmware/esx.conf avant toute modification.

Désactivation du monitoring

Le serveur ESXi cessera de répondre aux PING ce qui pourrait déclencher une alerte et provoquer le redémarrage du serveur pendant l'opération. Nous allons donc désactiver le monitoring depuis le manageur Kimsufi :



Choisir le bon serveur, si « Monitoring » est « Activé » alors cliquer sur « Désactiver ».



Le « Monitoring » passera donc à « Désactiver »

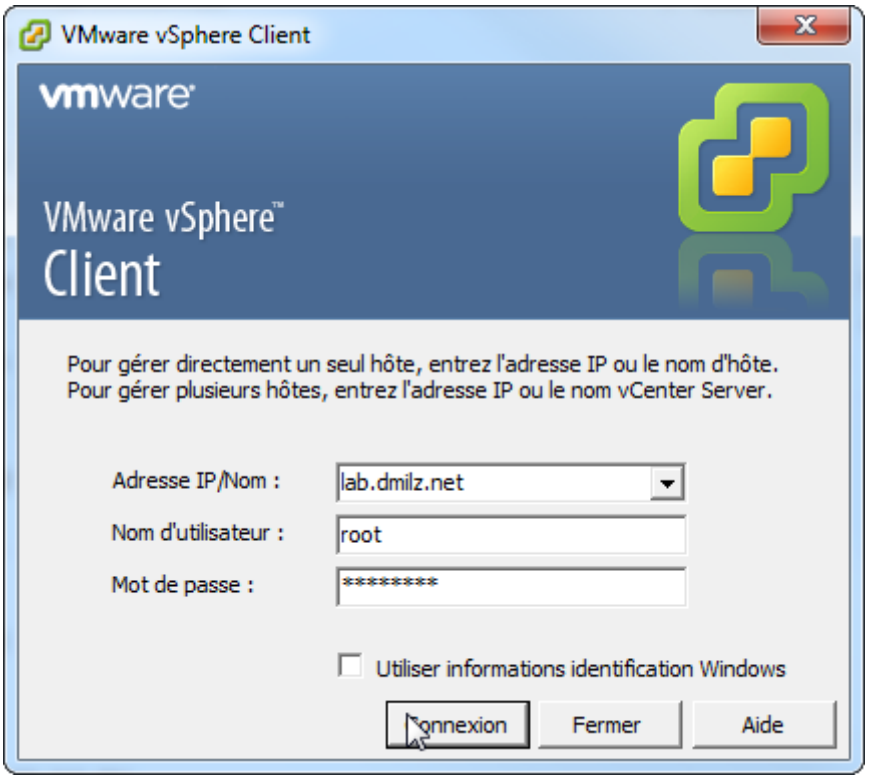
Nous réactiverons le monitoring à la fin de l'opération.

Configuration ESXi

Par défaut ESXi n'est pas configuré pour supporter IPV6. Nous allons donc l'activer.

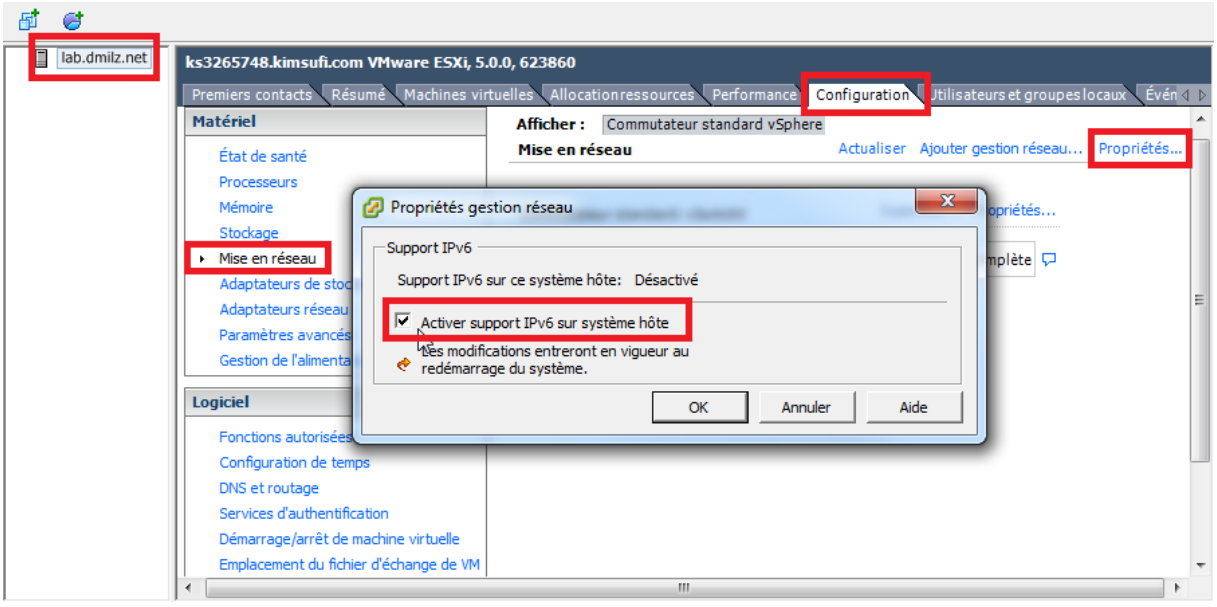
Activation du support IPv6

Les manipulations se font depuis le client « VMware vSphere Client ». Nous allons donc nous connecter au serveur ESXi :

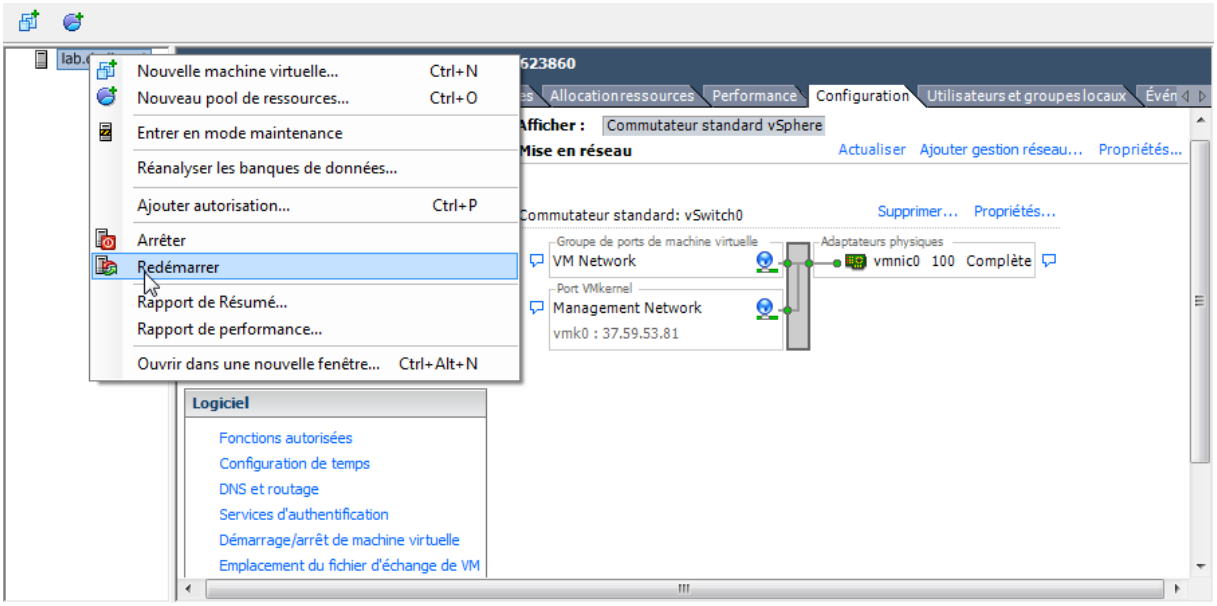


« lab.dmilz.net » redirige vers l'IPv4 91.121.64.225.

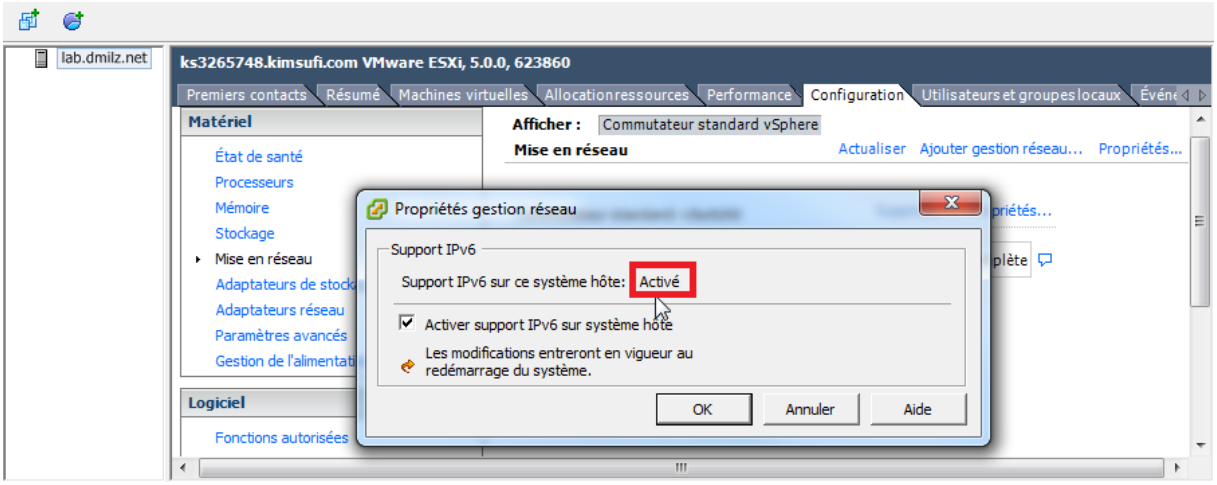
Nous sélectionnons le serveur (ici « lab.dmilz.net »), puis onglet « Configuration », dans la colonne « Matériel », « Mise en réseau », puis « Propriétés » (on note au passage que par défaut IPv6 est bien « Désactivé ») et cocher la case « Activer support IPv6 sur système hôte » :



La prise en compte se fera au prochain redémarrage, nous allons donc redémarrer ! Clic droit sur « lab.dmilz.net » et « Redémarrer » (le serveur étant vierge, nous nous passerons du mode maintenance).



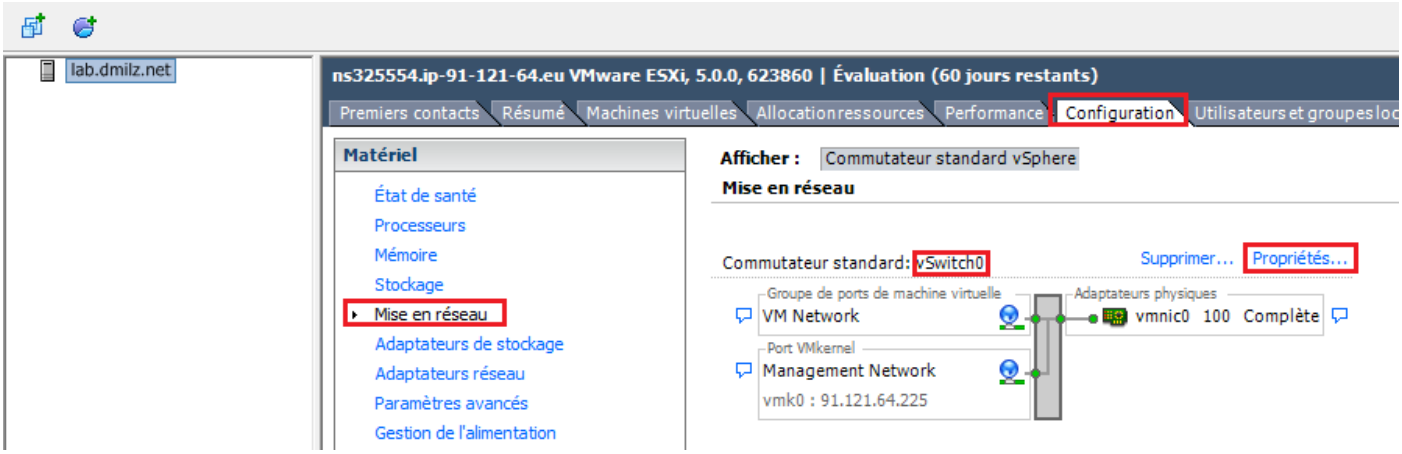
Après le redémarrage, vérifier qu'IPv6 est maintenant « Activé » :



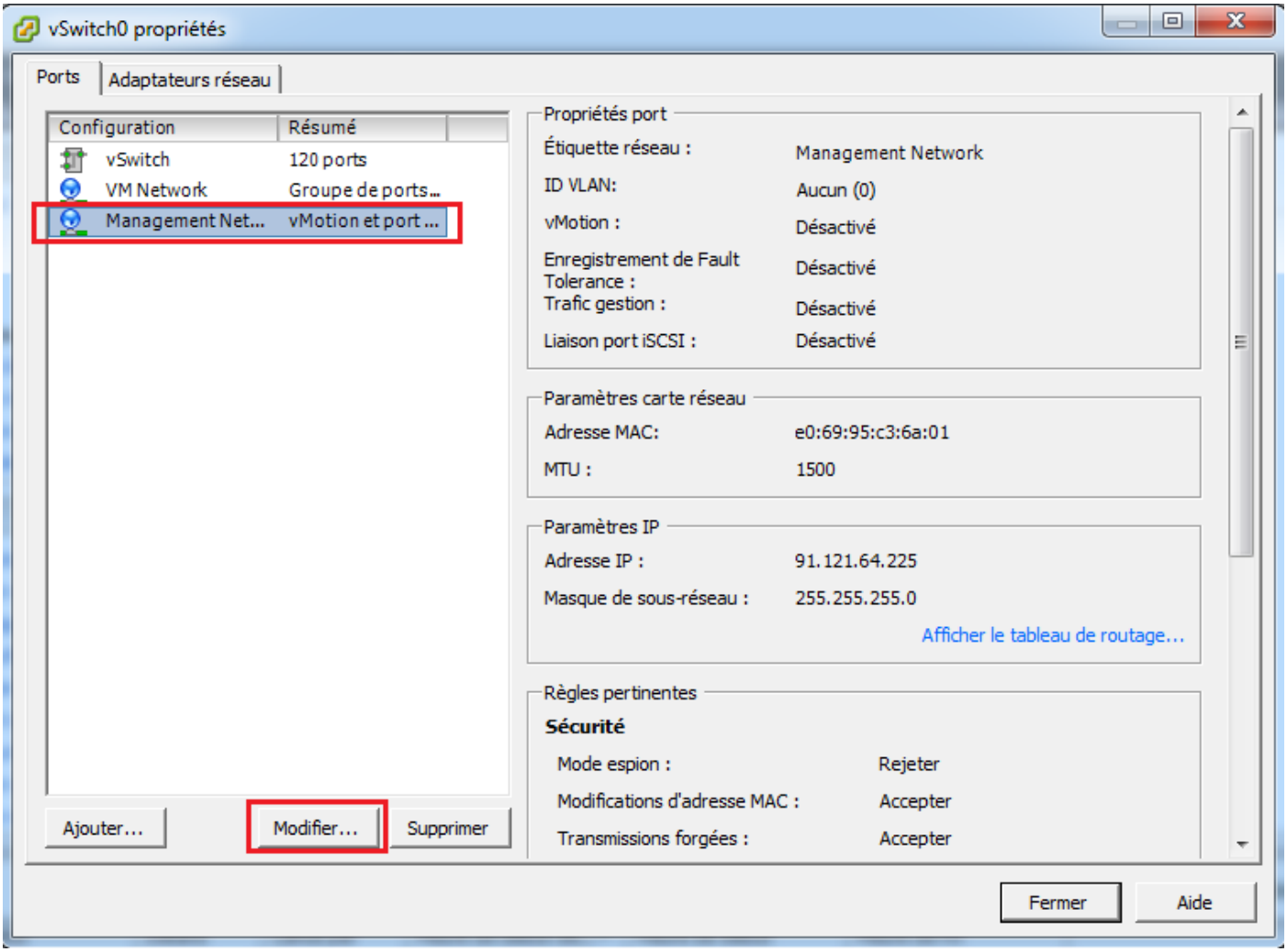
Si c'est le cas, nous pouvons maintenant configurer le « Management Network » en IPv6.

Configuration IPv6

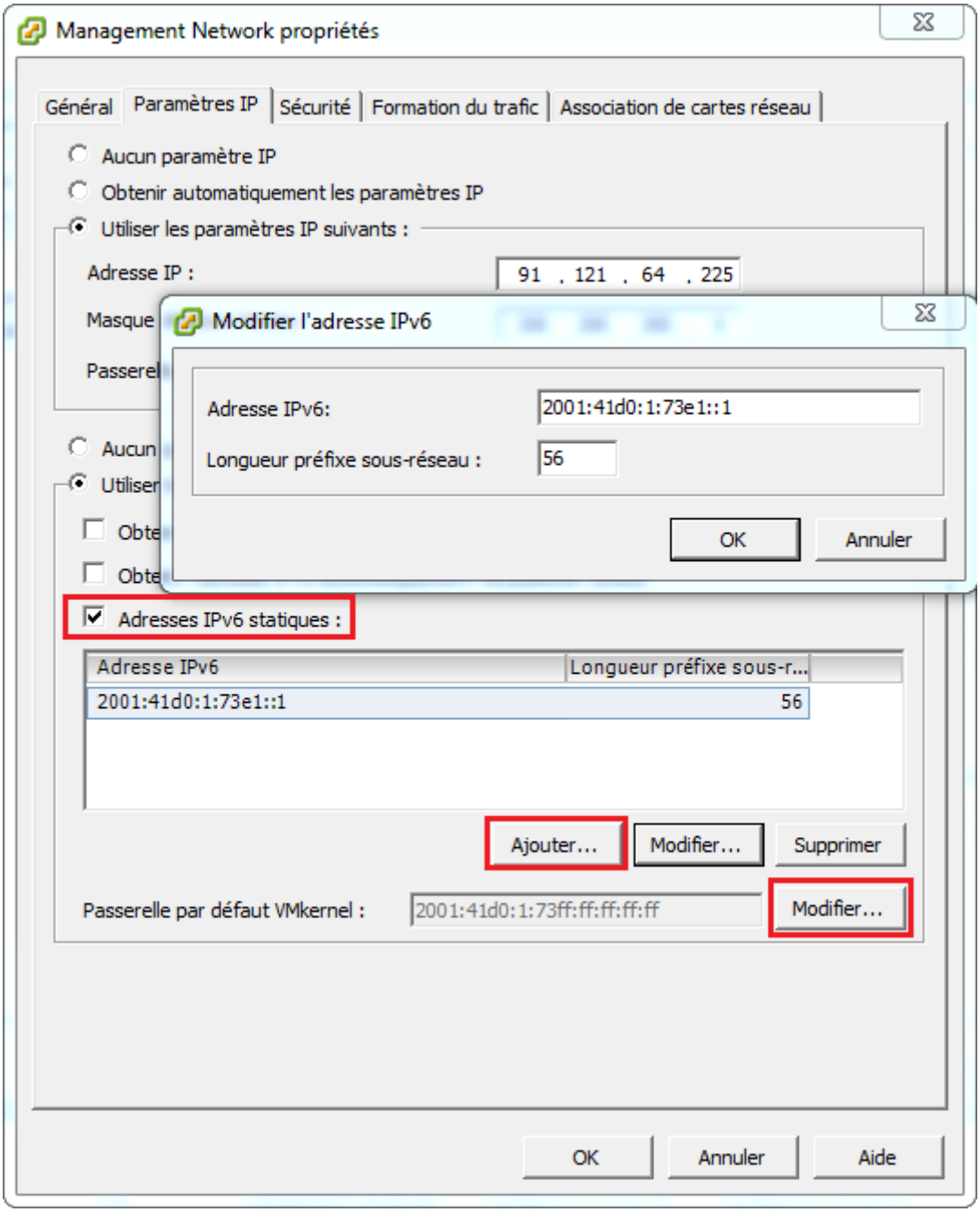
Nous allons configurer IPv6 pour le Management Network (par défaut sur le vSwitch0) via les propriétés de celui-ci :



Puis modifier « Management Network » :

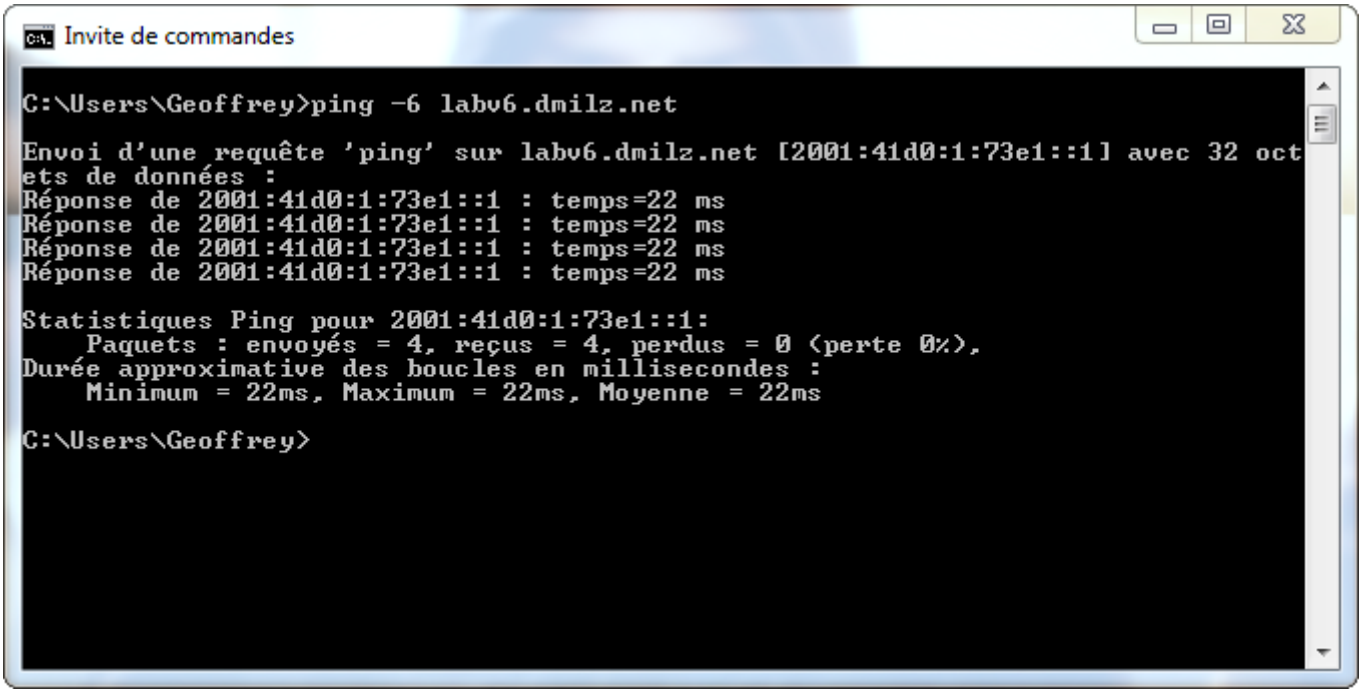


Puis nous configurons IPv6 :



Cocher « Adresses Iv6 statiques », puis « Ajouter », entrer votre IPv6 (ici « 2001:41d0:1:73e1::1 ») ainsi que le masque « 56 ». Puis nous configurons la passerelle par défaut VMkernel, pour kimsufi pendre les 56 premiers bits de votre adresse IP puis terminer par « ff:ff:ff:ff:ff:ff », ce qui donne dans ce cas « 2001:41d0:1:73ff:ff:ff:ff:ff ». La configuration est à adapter selon l'hébergeur. Les indication données ici fonctionnent chez Kimsufi en date du 02/08/2014 et fonctionnaient déjà avant août 2013.

Le serveur ESXi doit maintenant répondre aux PING sur l'IPv6 :



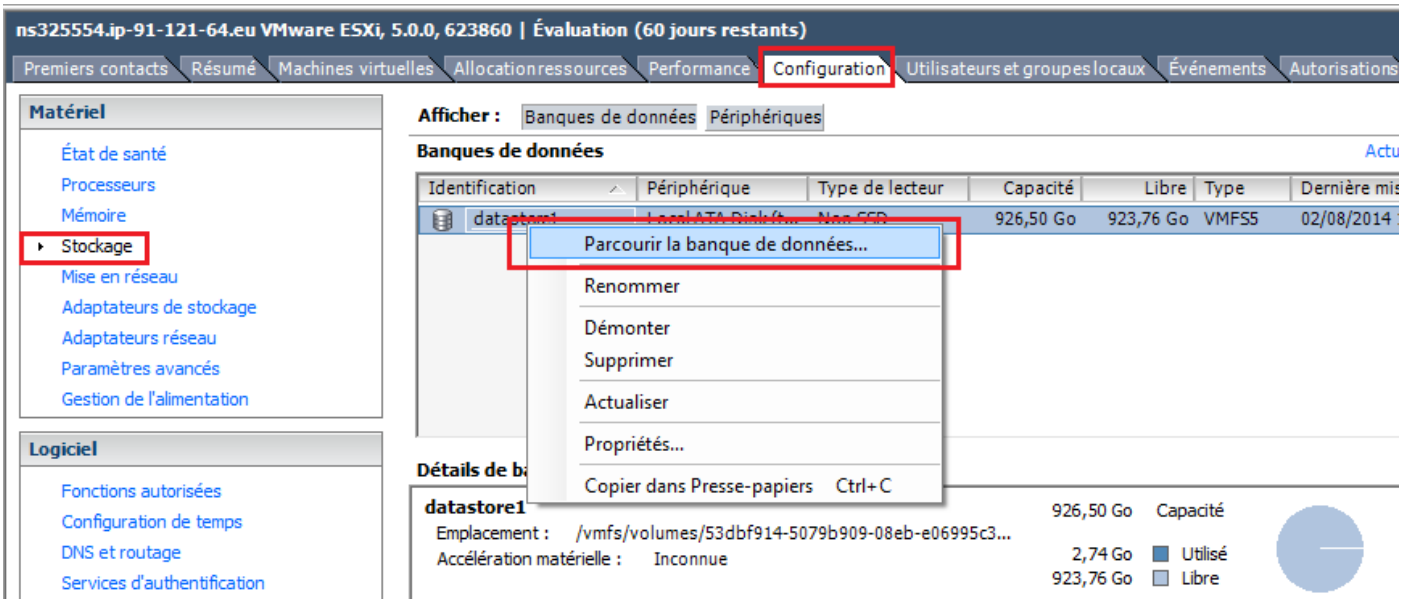
Si la machine ne répond pas soit :

- il y a un problème de configuration au niveau du serveur (vérifier adresses, masque et gateway)
- vous n'avez pas de connexion IPv6

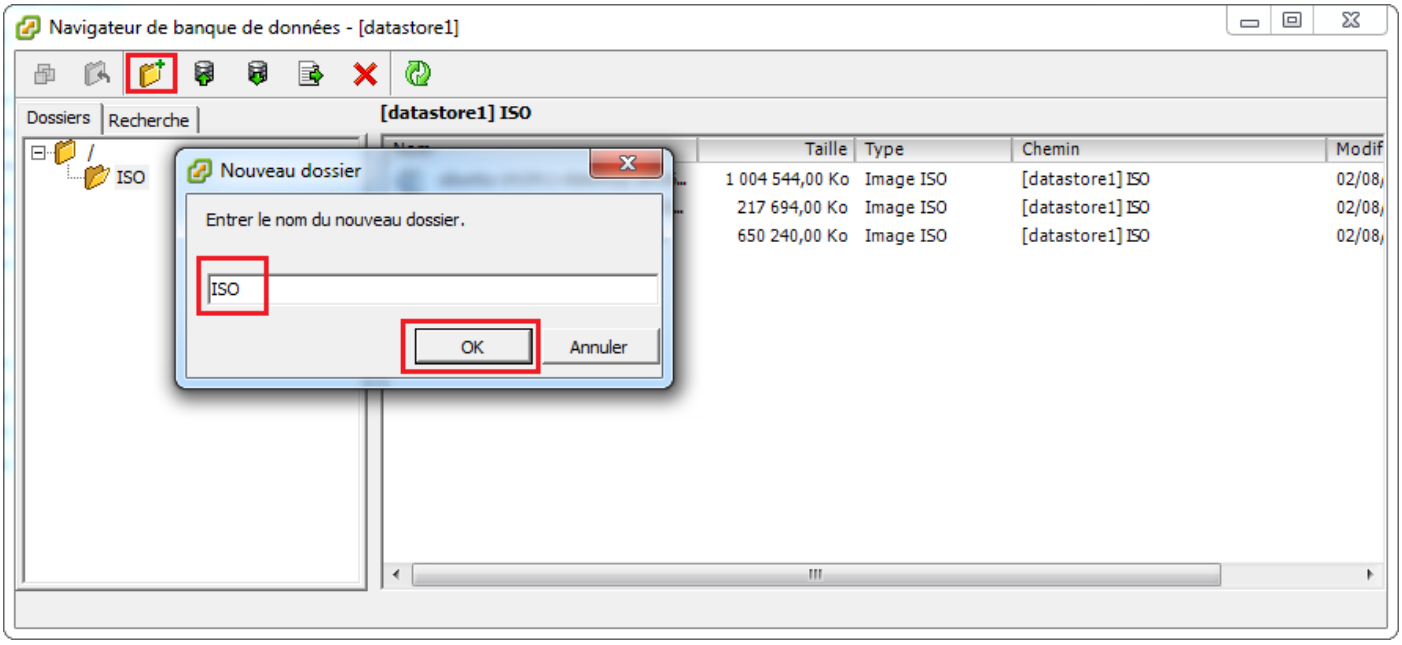
Dans les deux cas il est inutile d'aller plus loin.

Chargement des ISO sur un datastore

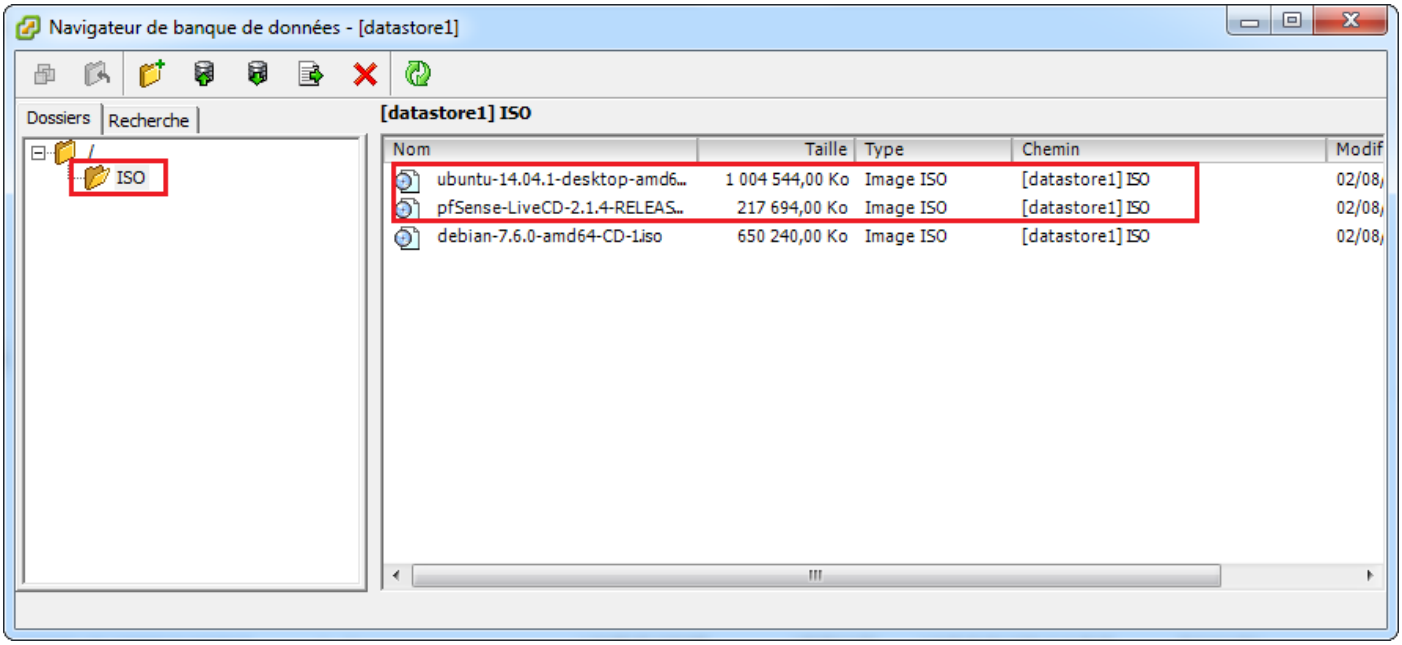
Il est préférable de charger au préalable les ISO sur un datastore plutôt qu'émuler (plus tard un lecteur de CD). Le plus simple consiste à charger les ISO depuis le client vSphere, menu « Configuration », « Stockage », sélectionner un datastore, clic droit et « Parcourir la banque de données » :



Créer un répertoire « ISO » :



Puis charger les images :



Cette opération peut être longue selon la connexion Internet. Il peut-être plus intéressant de récupérer les ISO directement depuis le shell d'ESXi.

Nous nous connectons via SSH, puis :

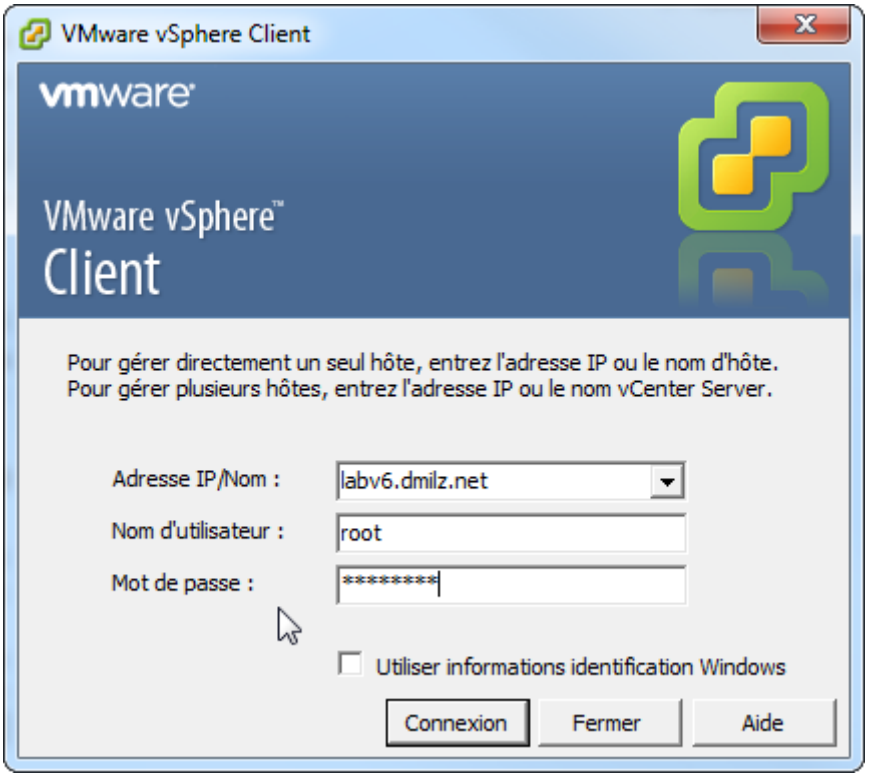
```
~ # find . -type d -name "ISO"
./vmfs/volumes/521740a0-1c41f2ef-51e6-3860773fab05/ISO
~ # cd ./vmfs/volumes/521740a0-1c41f2ef-51e6-3860773fab05/ISO
/vmfs/volumes/521740a0-1c41f2ef-51e6-3860773fab05/ISO # wget
http://pfsense.mirrors.ovh.net/pfsense.org/downloads/pfSense-LiveCD-2.0.3-RELEASE-i386-20130412-1022.iso.gz
Connecting to pfsense.mirrors.ovh.net (178.32.100.7:80)
pfSense-LiveCD-2.0.3 100%
|**********************************************************************************************************
**********| 78396k 00:00:00 ETA
/vmfs/volumes/521740a0-1c41f2ef-51e6-3860773fab05/ISO # ls -l
-rw-r--r--    1 root     root           80277887 Aug 23 12:58 pfSense-LiveCD-2.0.3-RELEASE-i386-20130412-
1022.iso.gz
/vmfs/volumes/521740a0-1c41f2ef-51e6-3860773fab05/ISO # gunzip pfSense-LiveCD-2.0.3-RELEASE-i386-20130412-
1022.iso.gz
```

Refaire la même opértion (wget http://ubuntu.mirrors.ovh.net/ubuntu-releases/14.04.1/ubuntu-14.04.1-desktop-amd64.iso) pour récupérer Ubuntu.

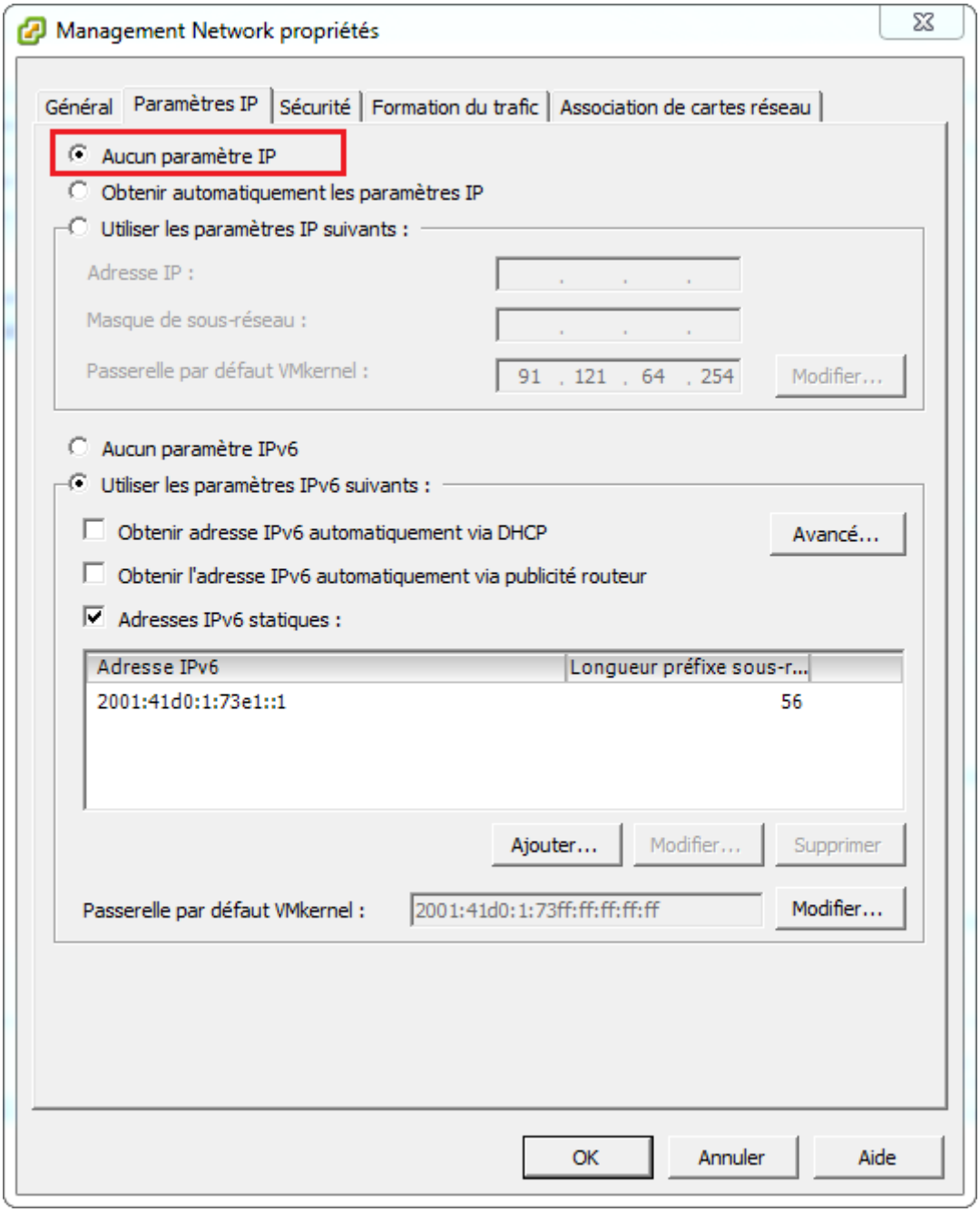
Nous n'avons plus besoin d'IPv4 à partir de maintenant.

Suppression de la configuration IPv4

Nous nous reconnectons à partir de l'adresse IPv6 :



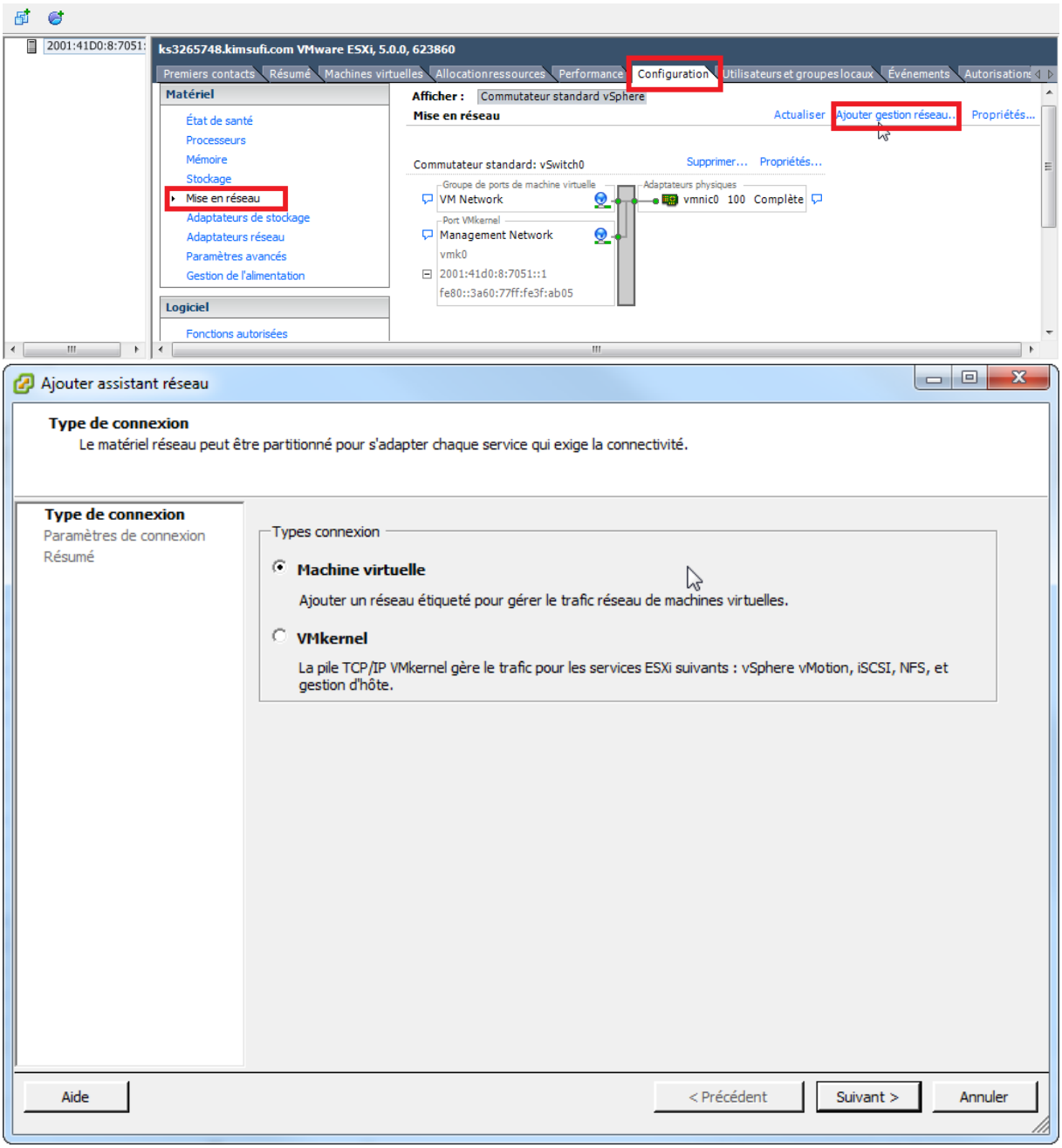
Puis depuis les propriétés du « Management Network » du vSwitch0, nous supprimons la configuration IPv4 :

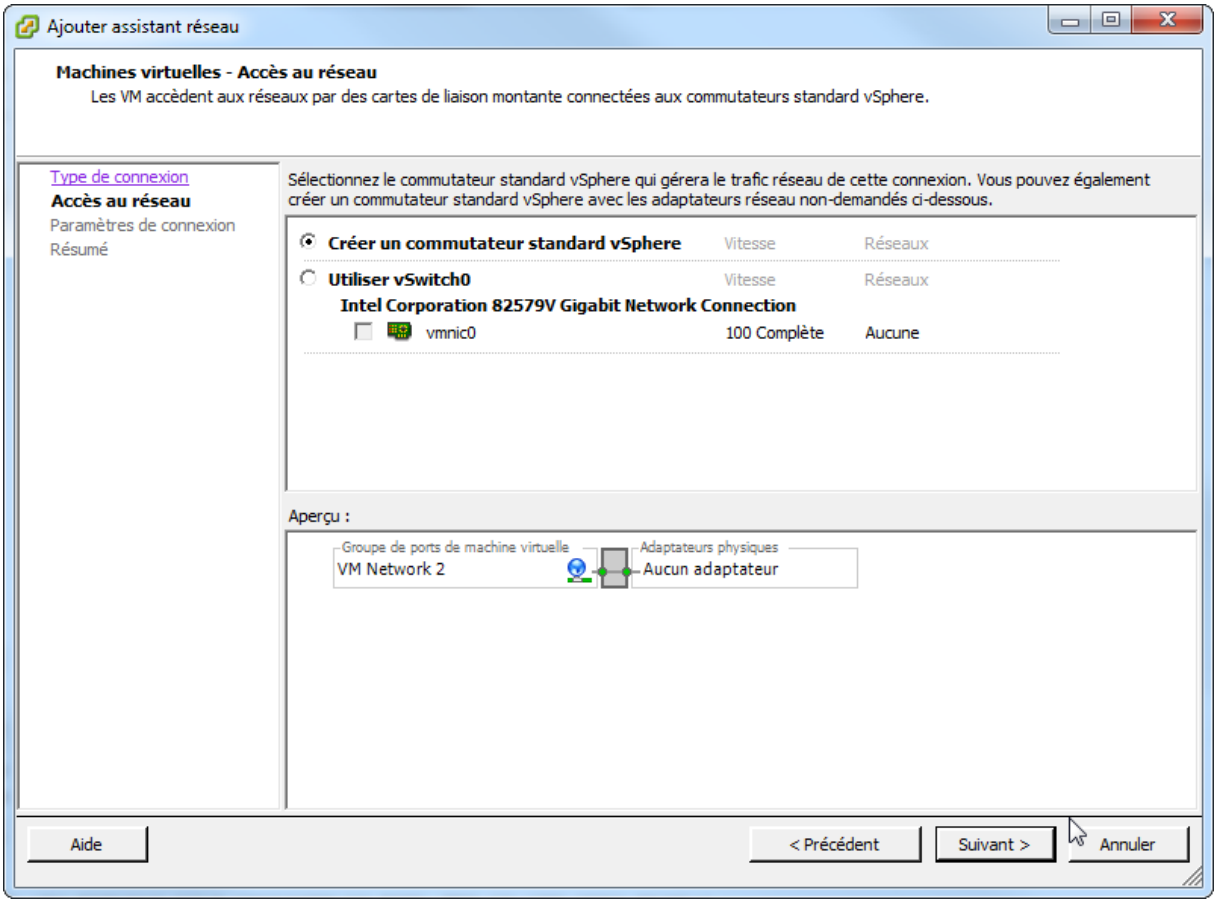


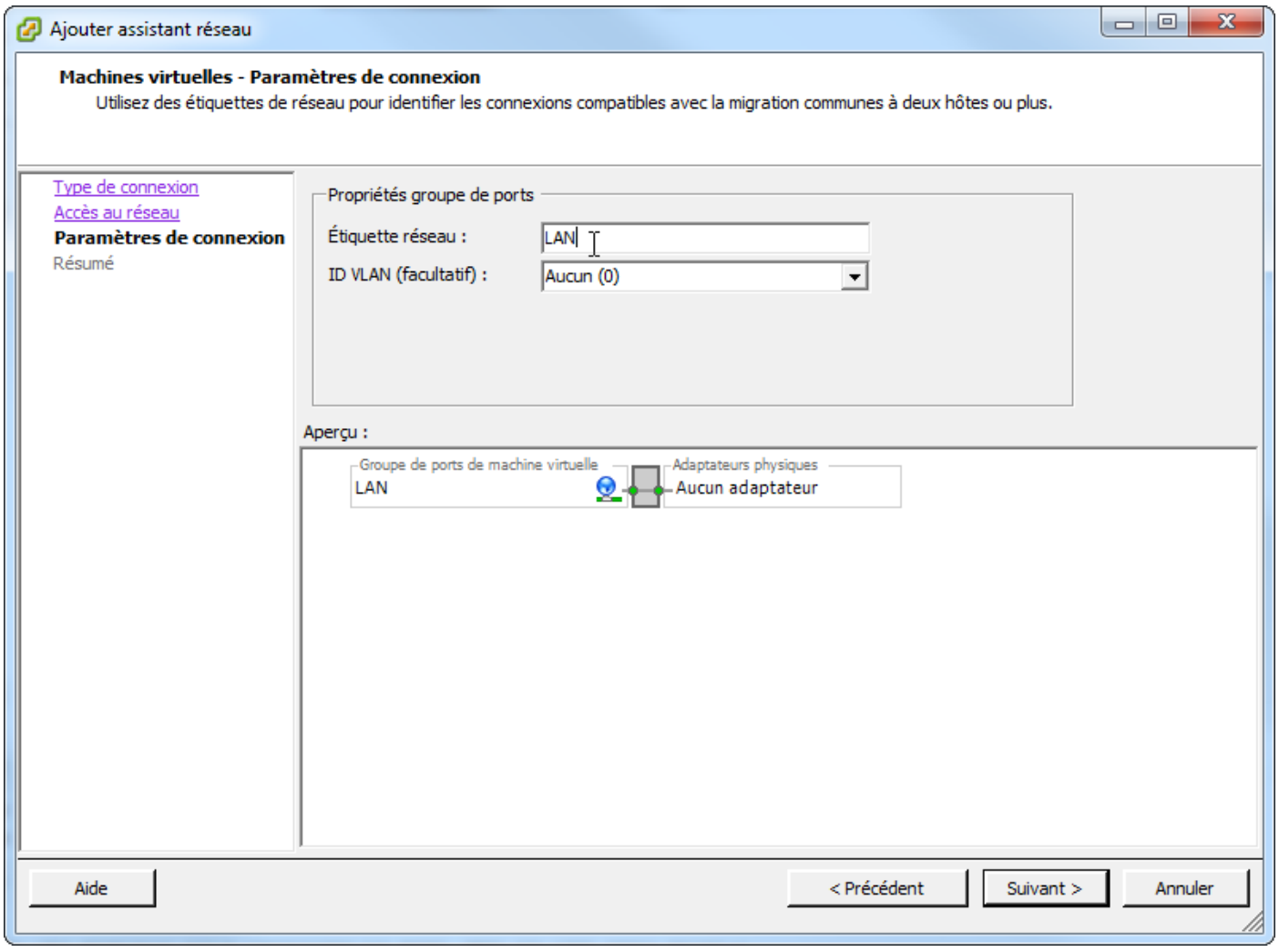
A partir de maintenant ESXi ne répondra plus du tout en IPv4. Par effet de bord il ne sera plus possible de se connecter au monde IPv4 depuis le shell d'ESXi car le client DNS IPv6 n'est pas supporté, la résolution de nom échouera.

Création des réseaux internes

Nous allons préparer les réseaux internes en créant un nouveau vSwitch depuis « Mise en réseau », que nous nommerons « LAN » :

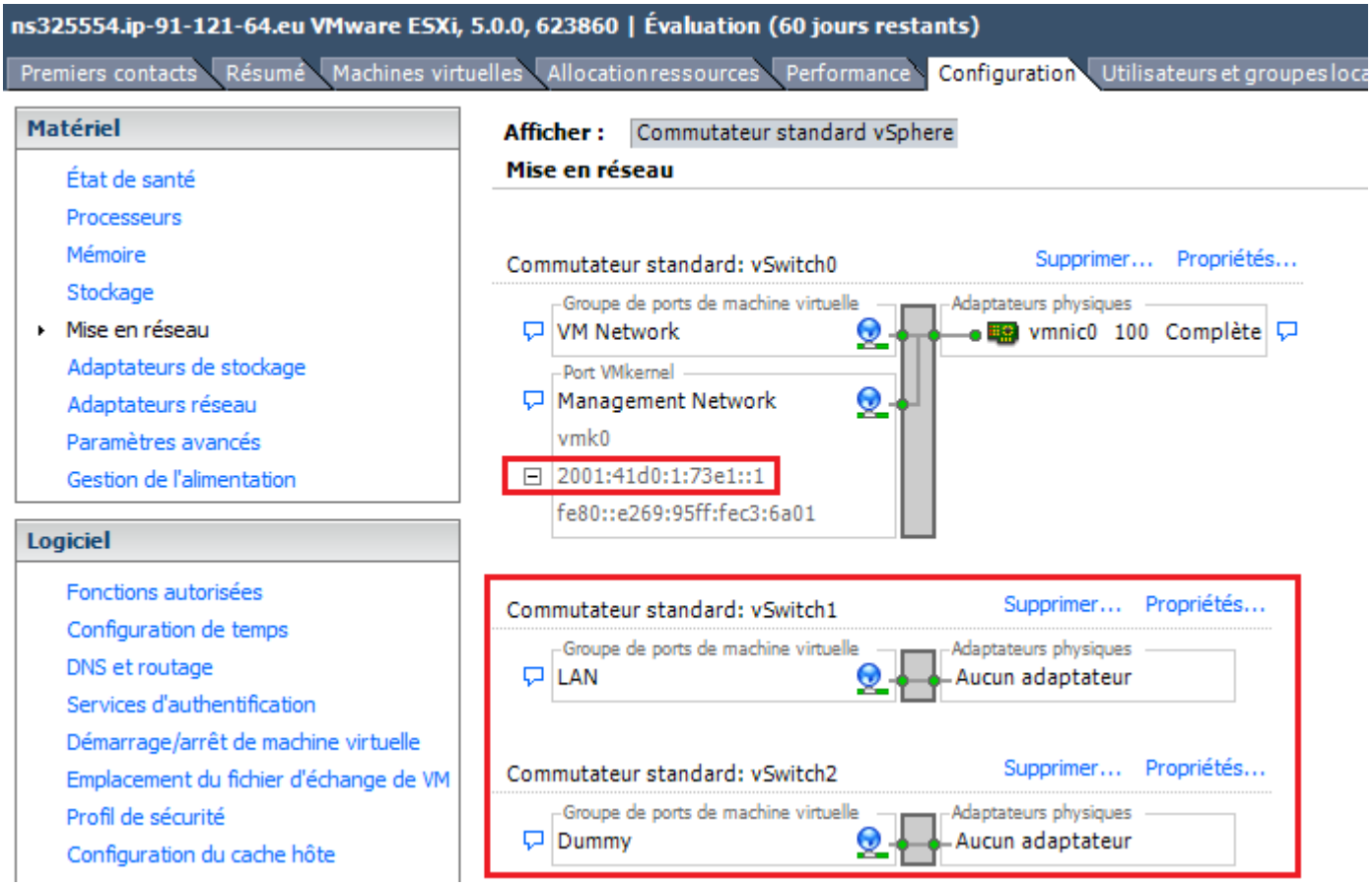

2001:41D0:8:7051:
ks3265748.kimsufi.com VMware ESXi, 5.0.0, 623860
Premiers contacts
Résumé
Machines virtuelles
Allocation ressources
Performance
Configuration
Utilisateurs et groupes locaux
Événements
Autorisations
Matériel
État de santé
Processeurs
Mémoire
Stockage
Mise en réseau
Adaptateurs de stockage
Adaptateurs réseau
Paramètres avancés
Gestion de l'alimentation
Logiciel
Fonctions autorisées
Afficher :
Commutateur standard vSphere
Mise en réseau
Actualiser
Ajouter gestion réseau...
Propriétés...
Commutateur standard: vSwitch0
Supprimer...
Propriétés...
Groupe de ports de machine virtuelle
VM Network
Adaptateurs physiques
vmnic0 100 Complète
Port VMkernel
Management Network
vmk0
2001:41d0:8:7051::1
fe80::3a60:77ff:fe3f:ab05
Ajouter assistant réseau
Type de connexion
Le matériel réseau peut être partitionné pour s'adapter chaque service qui exige la connectivité.
Type de connexion
Paramètres de connexion
Résumé
Types connexion
Machine virtuelle
Ajouter un réseau étiqueté pour gérer le trafic réseau de machines virtuelles.
VMkernel
La pile TCP/IP VMkernel gère le trafic pour les services ESXi suivants : vSphere vMotion, iSCSI, NFS, et gestion d'hôte.
Aide
< Précédent
Suivant >
Annuler


Ajouter assistant réseau
Machines virtuelles - Accès au réseau
Les VM accèdent aux réseaux par des cartes de liaison montante connectées aux commutateurs standard vSphere.
Type de connexion
Accès au réseau
Paramètres de connexion
Résumé
Sélectionnez le commutateur standard vSphere qui gérera le trafic réseau de cette connexion. Vous pouvez également créer un commutateur standard vSphere avec les adaptateurs réseau non-demandés ci-dessous.
Créer un commutateur standard vSphere
Vitesse
Réseaux
Utiliser vSwitch0
Vitesse
Réseaux
Intel Corporation 82579V Gigabit Network Connection
vmnic0
100 Complète
Aucune
Aperçu :
Groupe de ports de machine virtuelle
VM Network 2
Adaptateurs physiques
Aucun adaptateur
Aide
< Précédent
Suivant >
Annuler


Ajouter assistant réseau
Machines virtuelles - Paramètres de connexion
Utilisez des étiquettes de réseau pour identifier les connexions compatibles avec la migration communes à deux hôtes ou plus.
Type de connexion
Accès au réseau
Paramètres de connexion
Résumé
Propriétés groupe de ports
Étiquette réseau :
LAN
ID VLAN (facultatif) :
Aucun (0)
Aperçu :
Groupe de ports de machine virtuelle
LAN
Adaptateurs physiques
Aucun adaptateur
Aide
< Précédent
Suivant >
Annuler

Recommencer la même opération pour créer un réseau « Dummy » qui servira à isoler les VM lors de leur création.

Nous devrions donc avoir la configuration suivante :



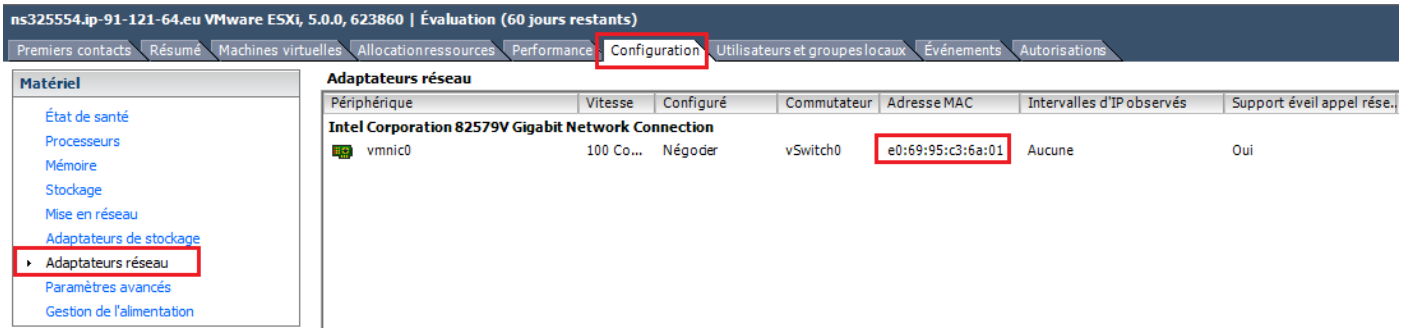
La configuration de l'ESXi est maintenant terminée. Nous allons installer la VM pfSense.

Préparation pfSense

En prérequis il faut récupérer l'adresse MAC du serveur.

Récupération de l'adresse MAC

Depuis le menu « Configuration », « Adaptateurs réseau », récupérer l'adresse MAC du la NIC connecté sur le vSwitch0 :



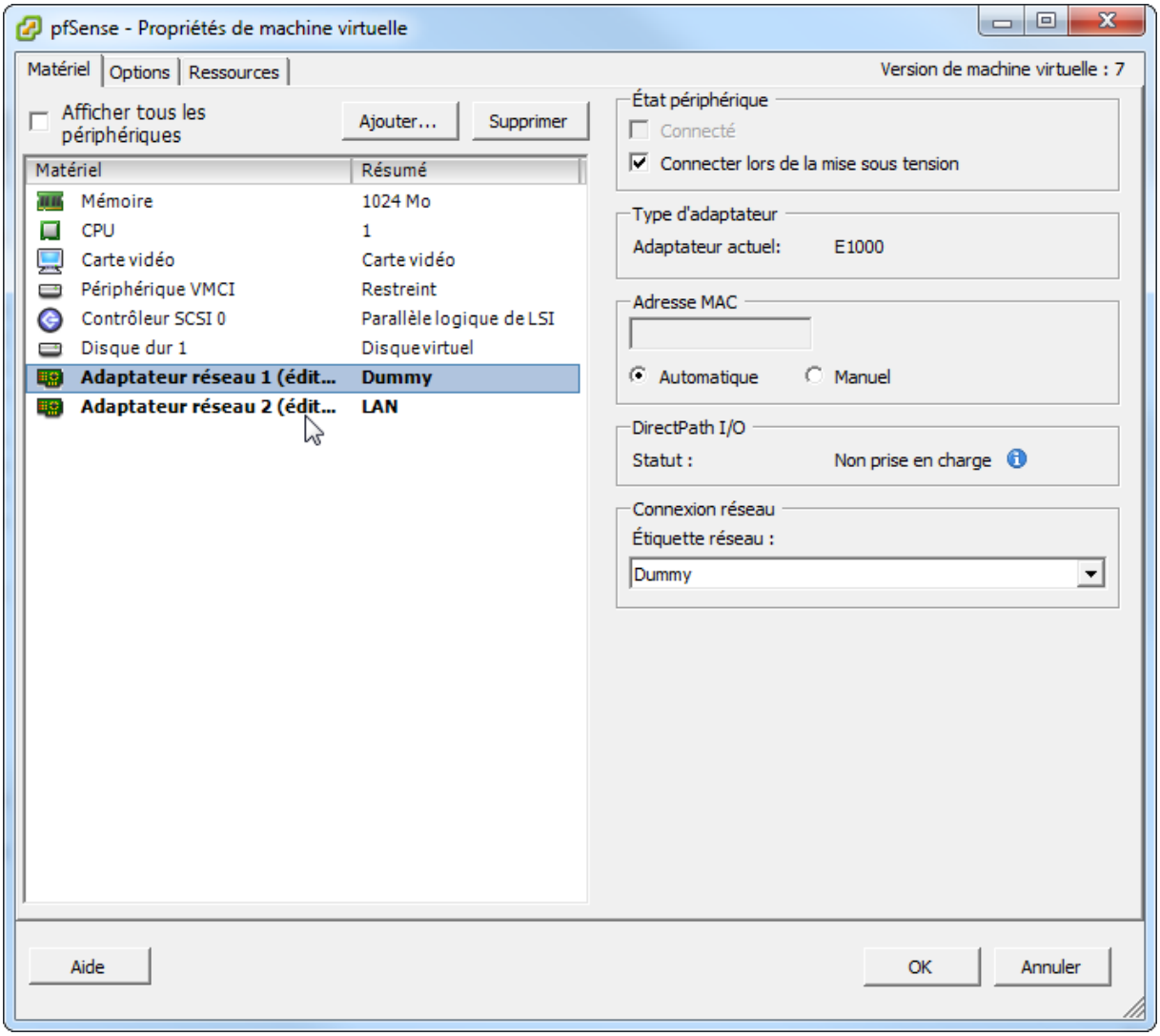
Dans cet exemple l'adresse MAC est « **e0:69:95:c3:6a:01** ».

Création de la VM pour pfSense

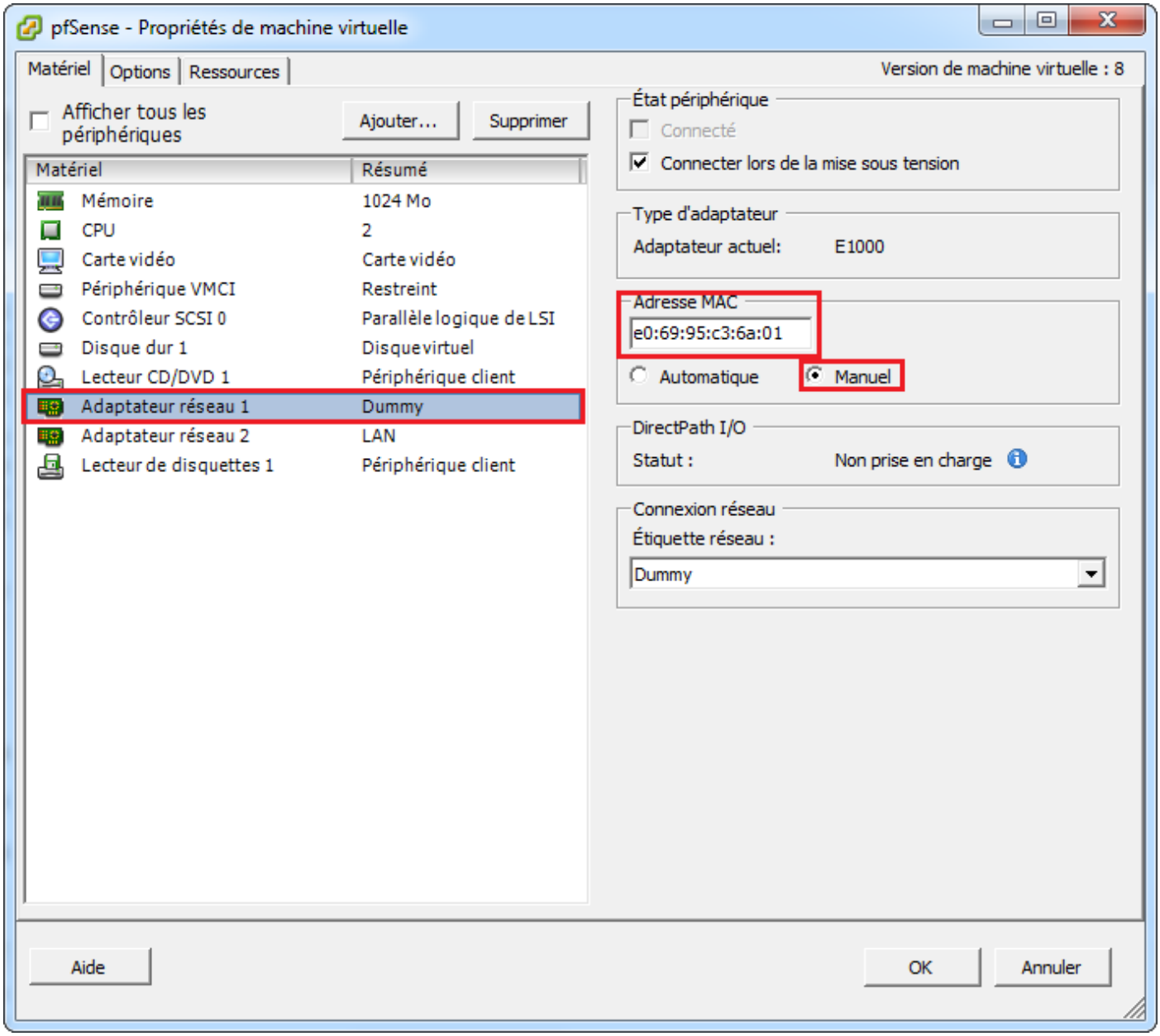
Nous allons considérer que savoir créer une VM est un prérequis à ce guide. Je conseille néanmoins d'utiliser le mode « Personnalisé » en prenant les précautions suivantes :

- pfSense est basé sur FreeBSD et nous avons récupérer la version 64 bits
- choisir le contrôleur SCSI « Parallèle logique de LSI »
- créer 2 interfaces réseau (une sur le vSwitch « Dummy », une autre sur « LAN »)

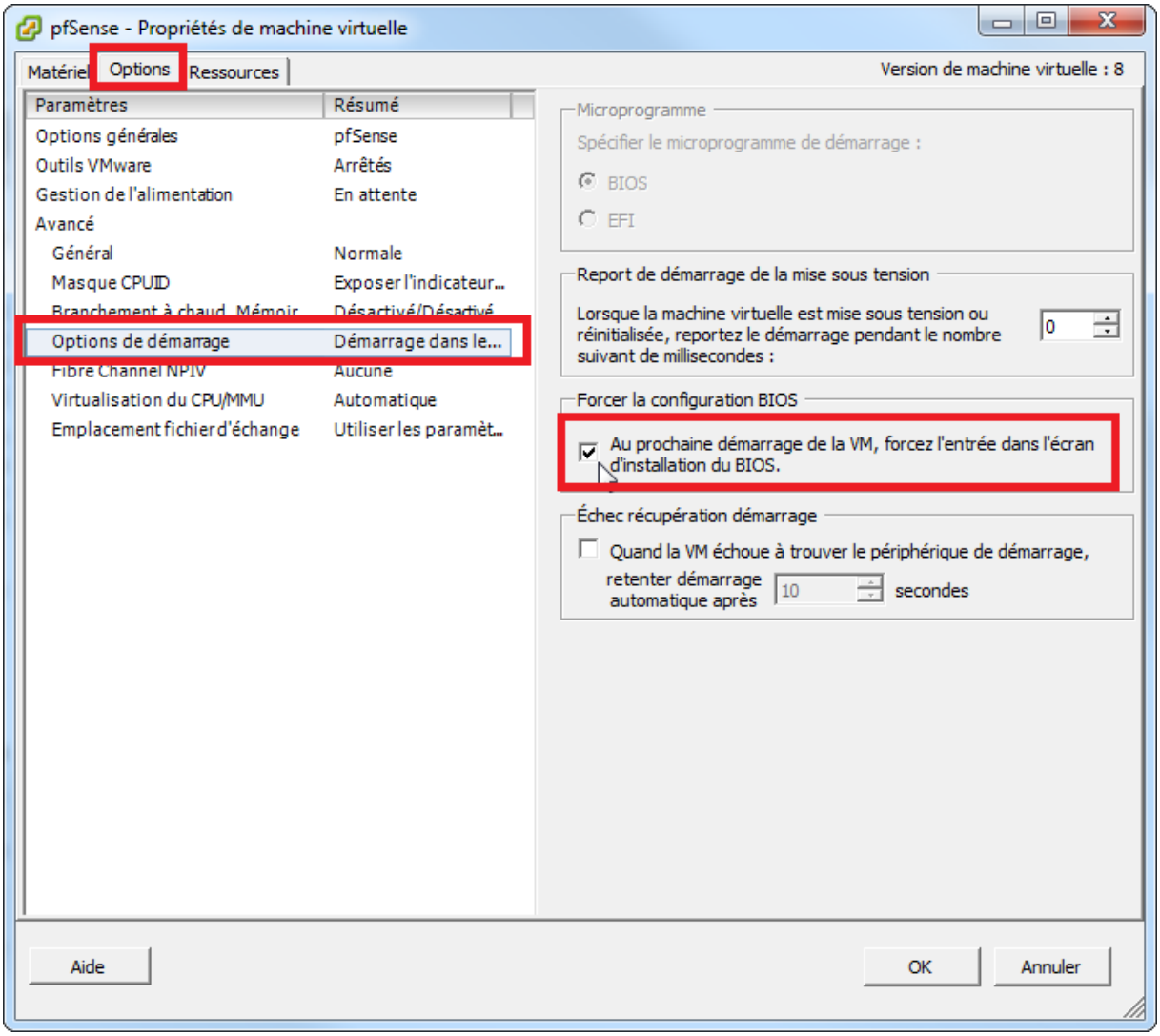
Ce qui devrait donner une VM comme :



Passer l'adaptateur réseau relié à « Dummy » en adresse MAC manuelle et entrer l'adresse MAC su serveur physique :



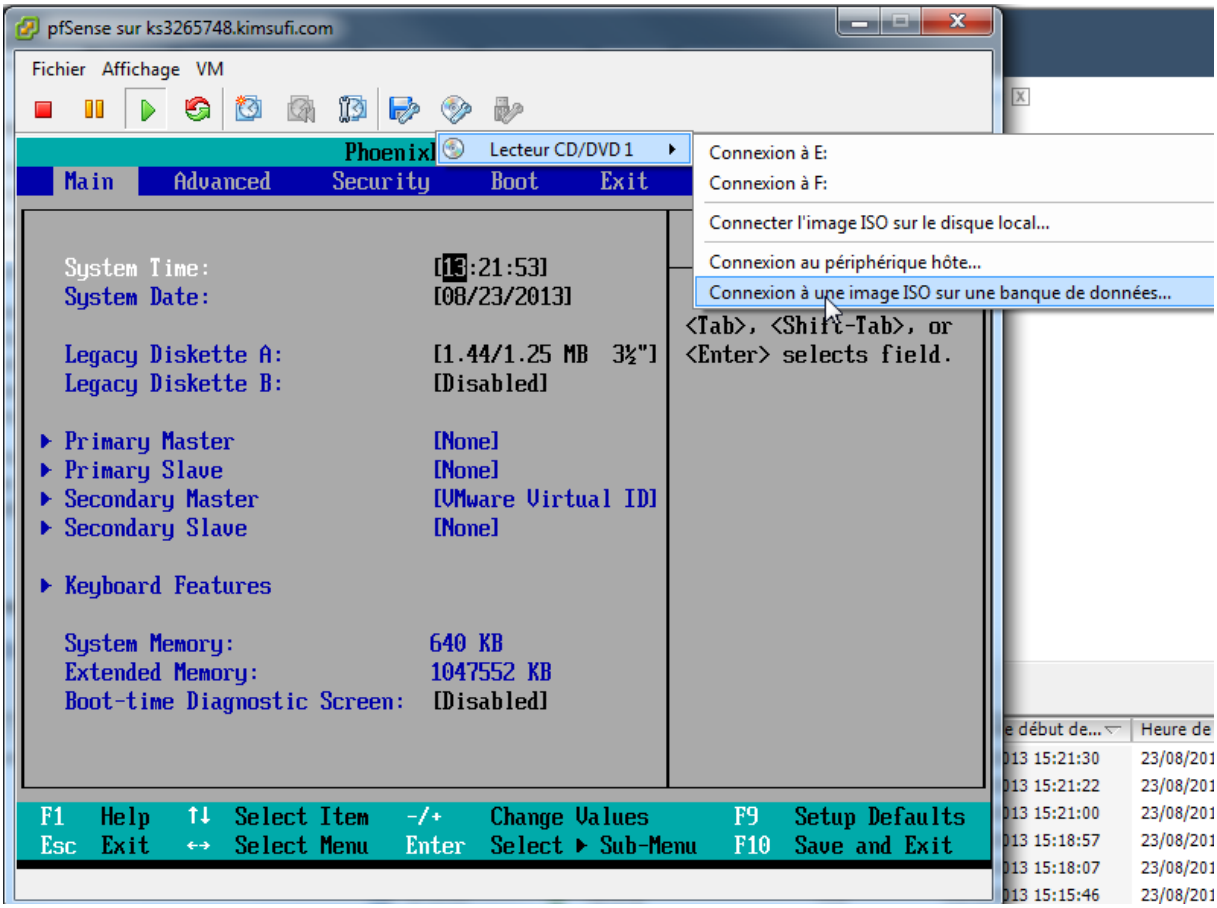
Nous forçons au passage la VM à rester sur le BIOS au prochain démarrage :



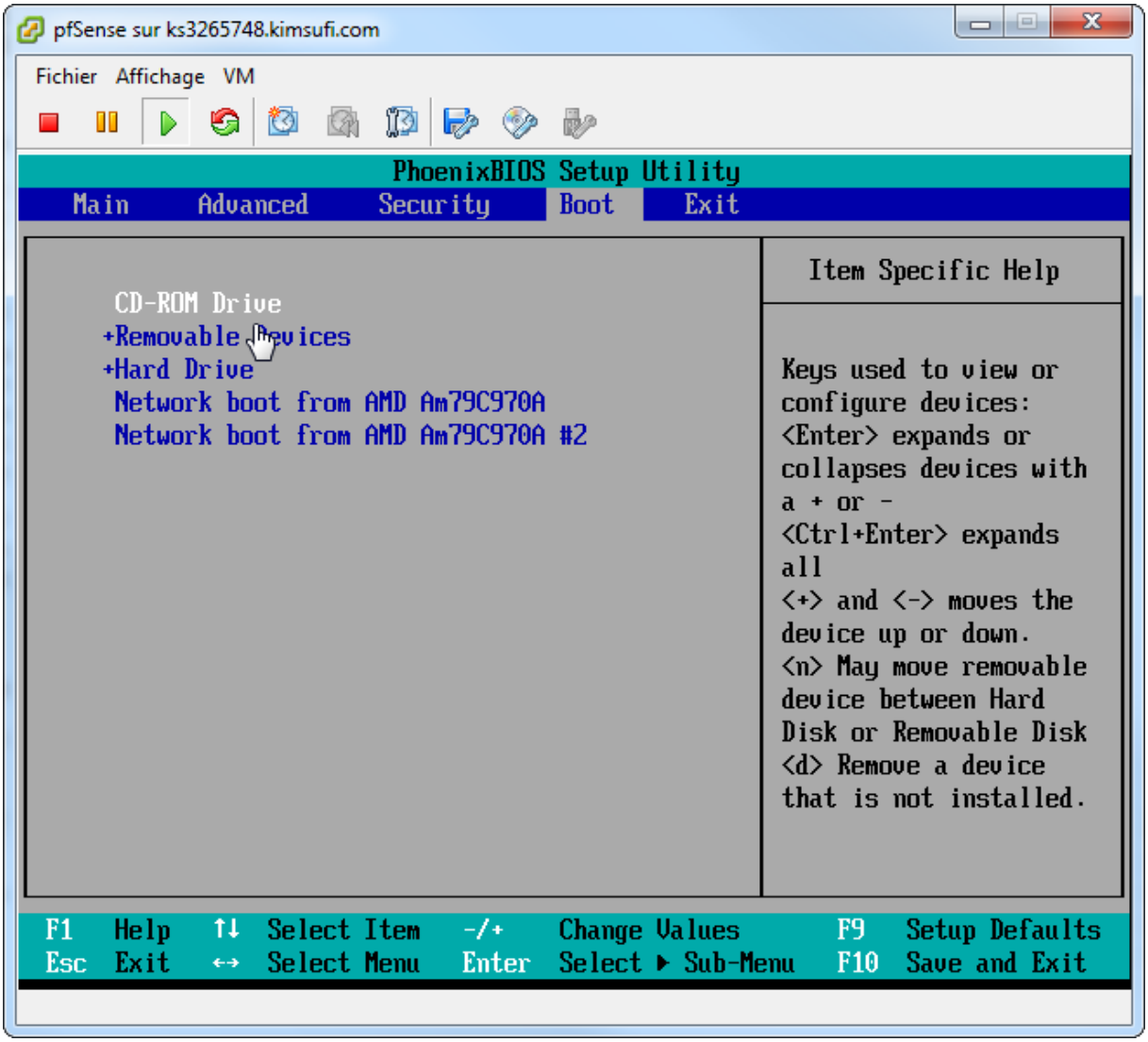
L'enveloppe de la VM est maintenant prête.

Installation de pfSense

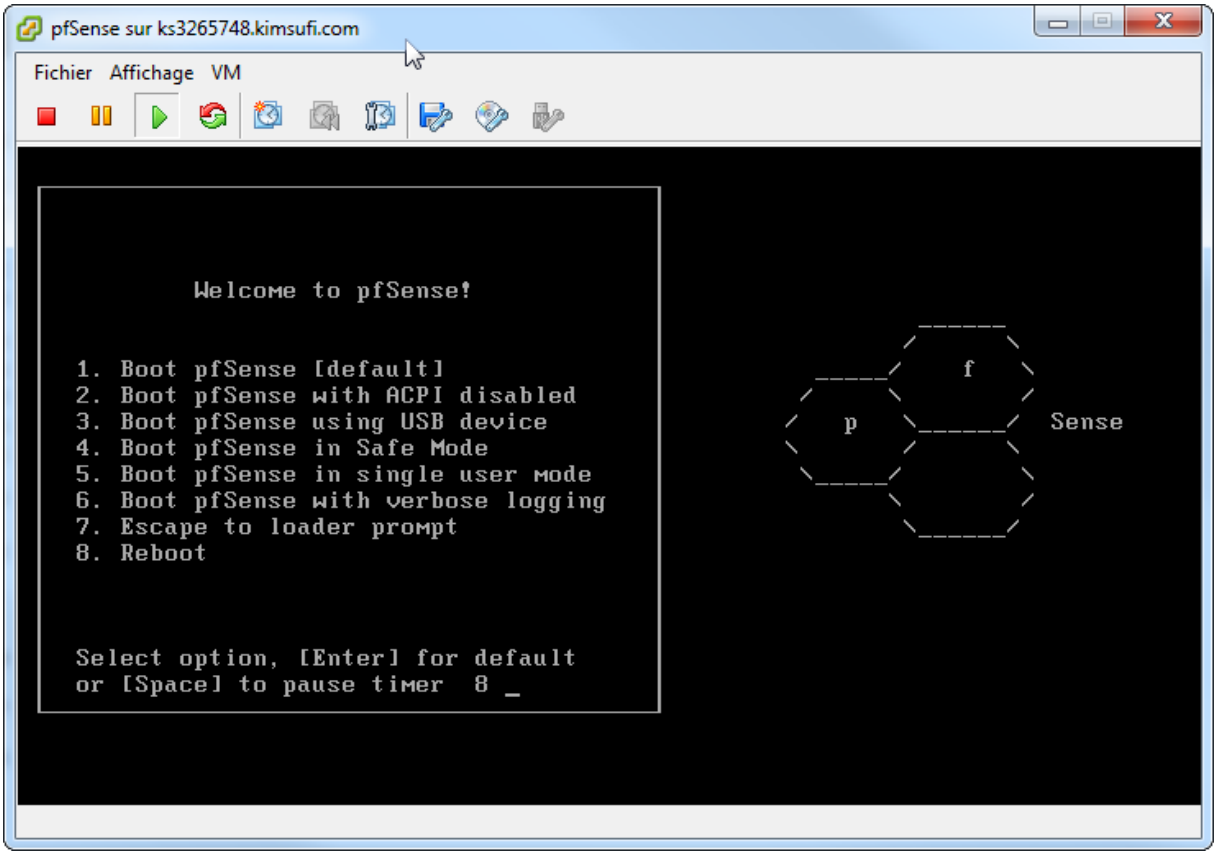
Démarrer la VM qui restera bloqué sur le BIOS ce qui nous permettra de monter l'ISO depuis le datastore :



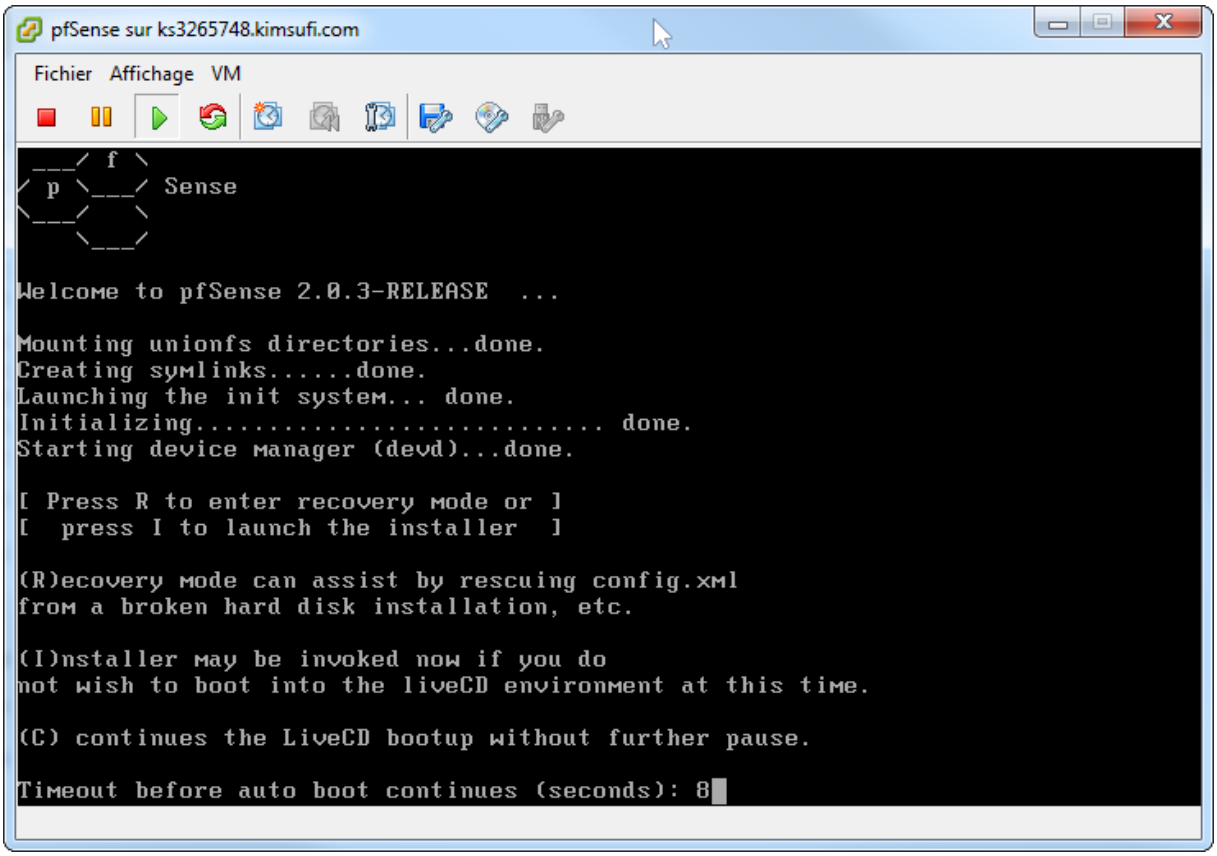
Changer la priorité de boot du CD-ROM :

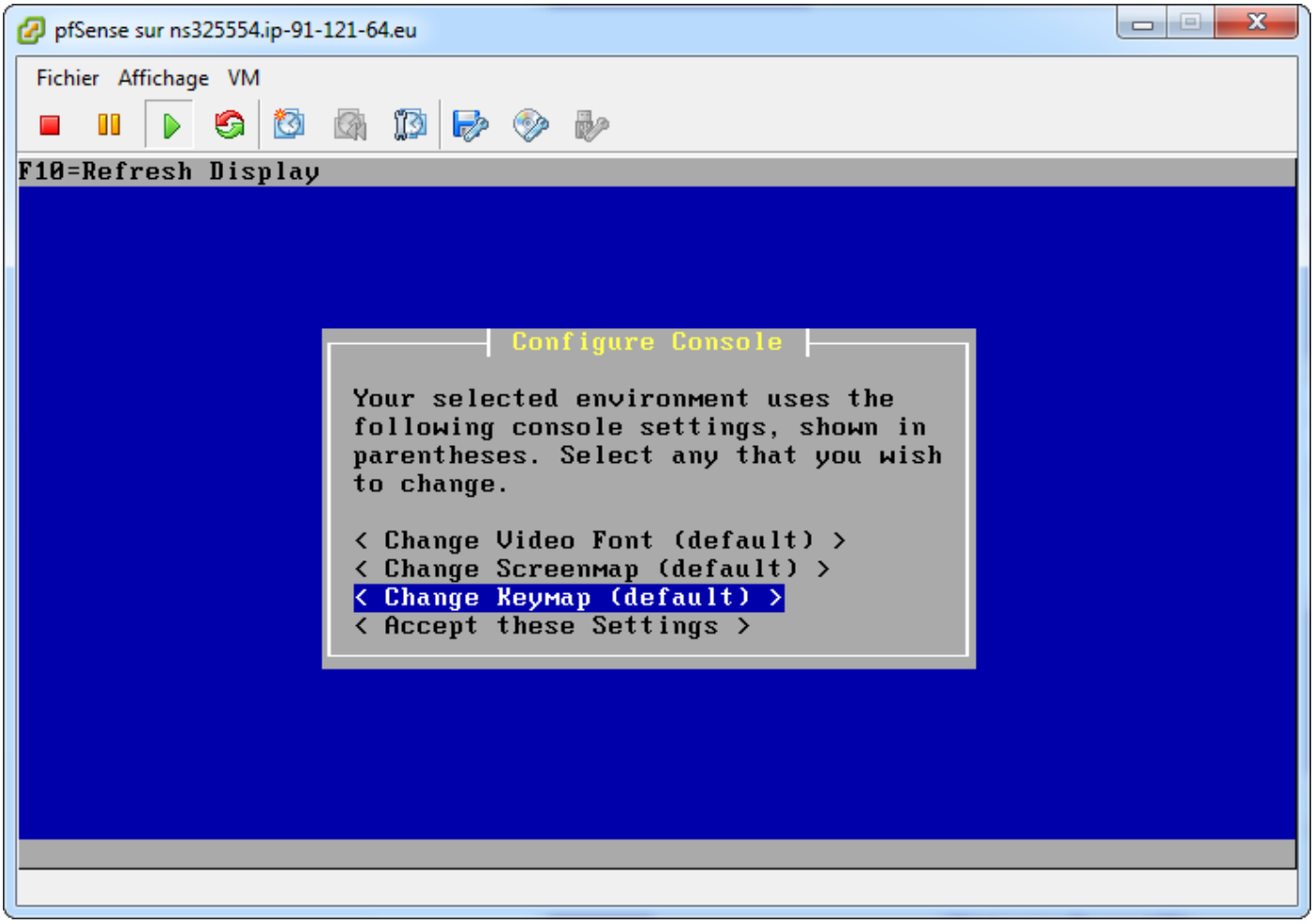


Et suivre l'installation :



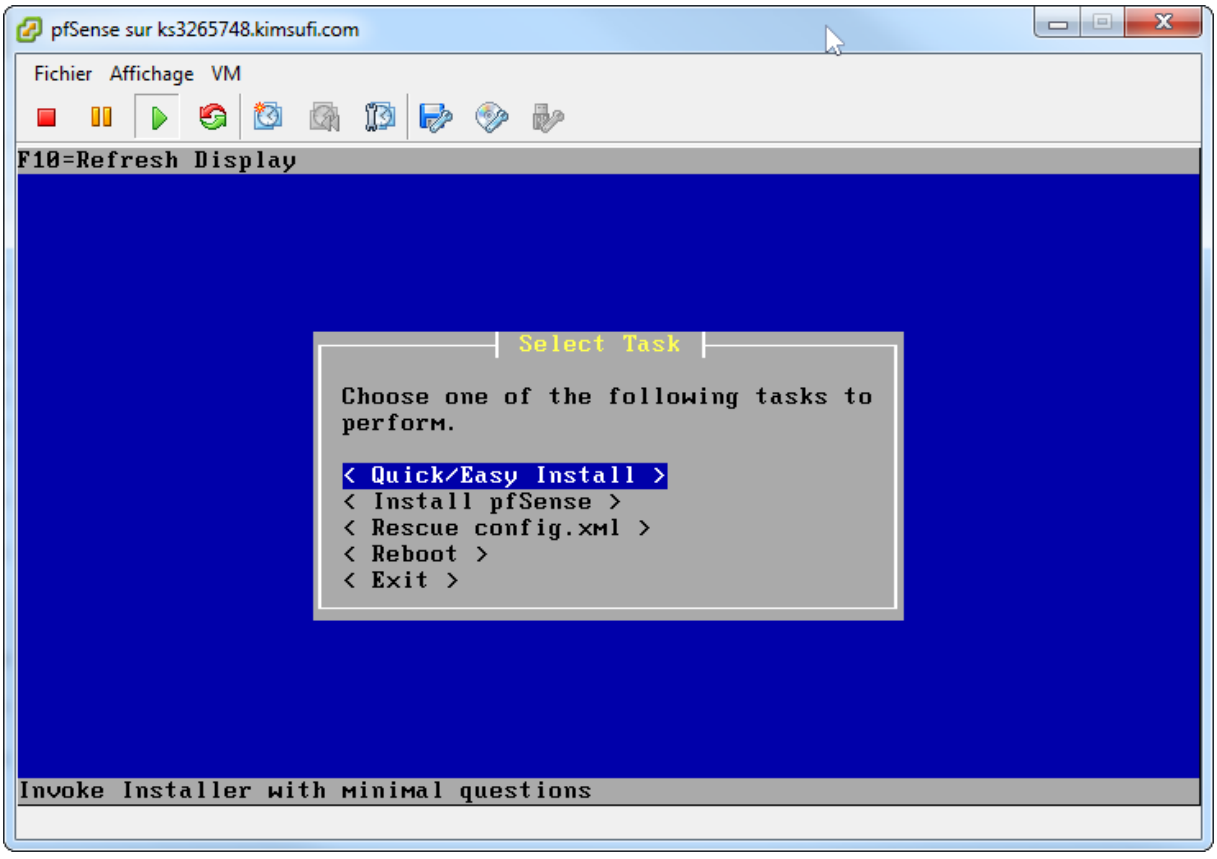
Taper « I » sur l'écran suivant pour lancer l'installation :

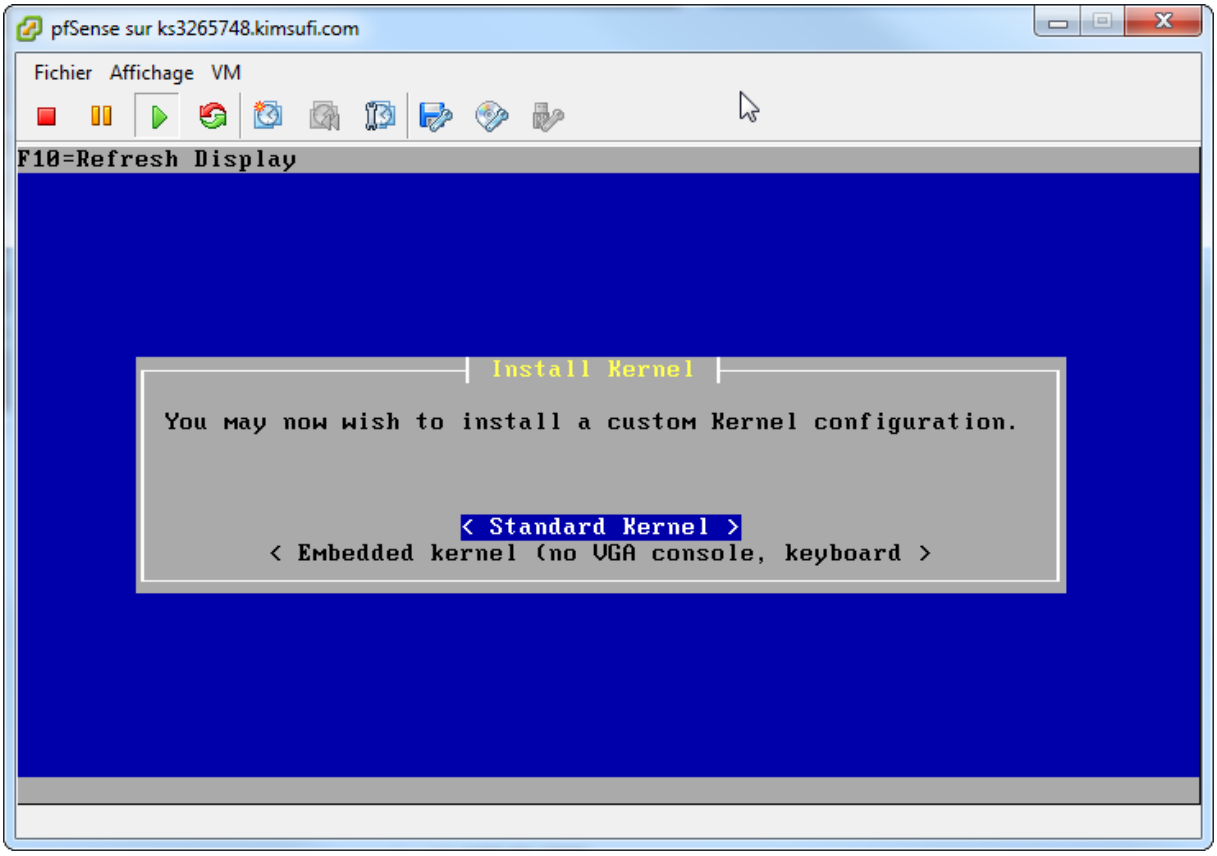




Il est inutile de changer la keymap… Valider directement « Accept these settings ».

Choisir « Quick Install » et le « Standard Kernel » :



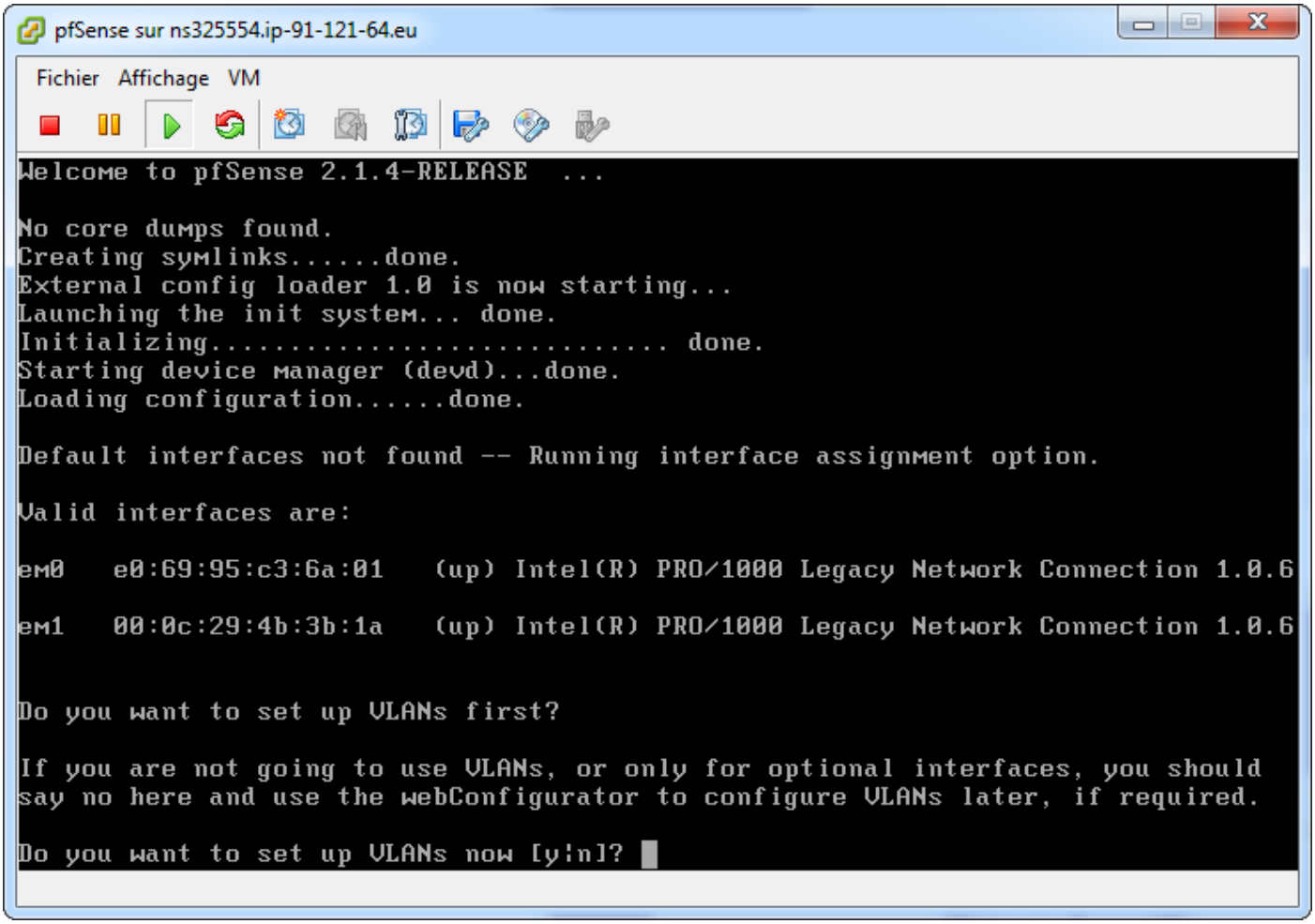


A la fin de l'installation pfSense va redémarrer.

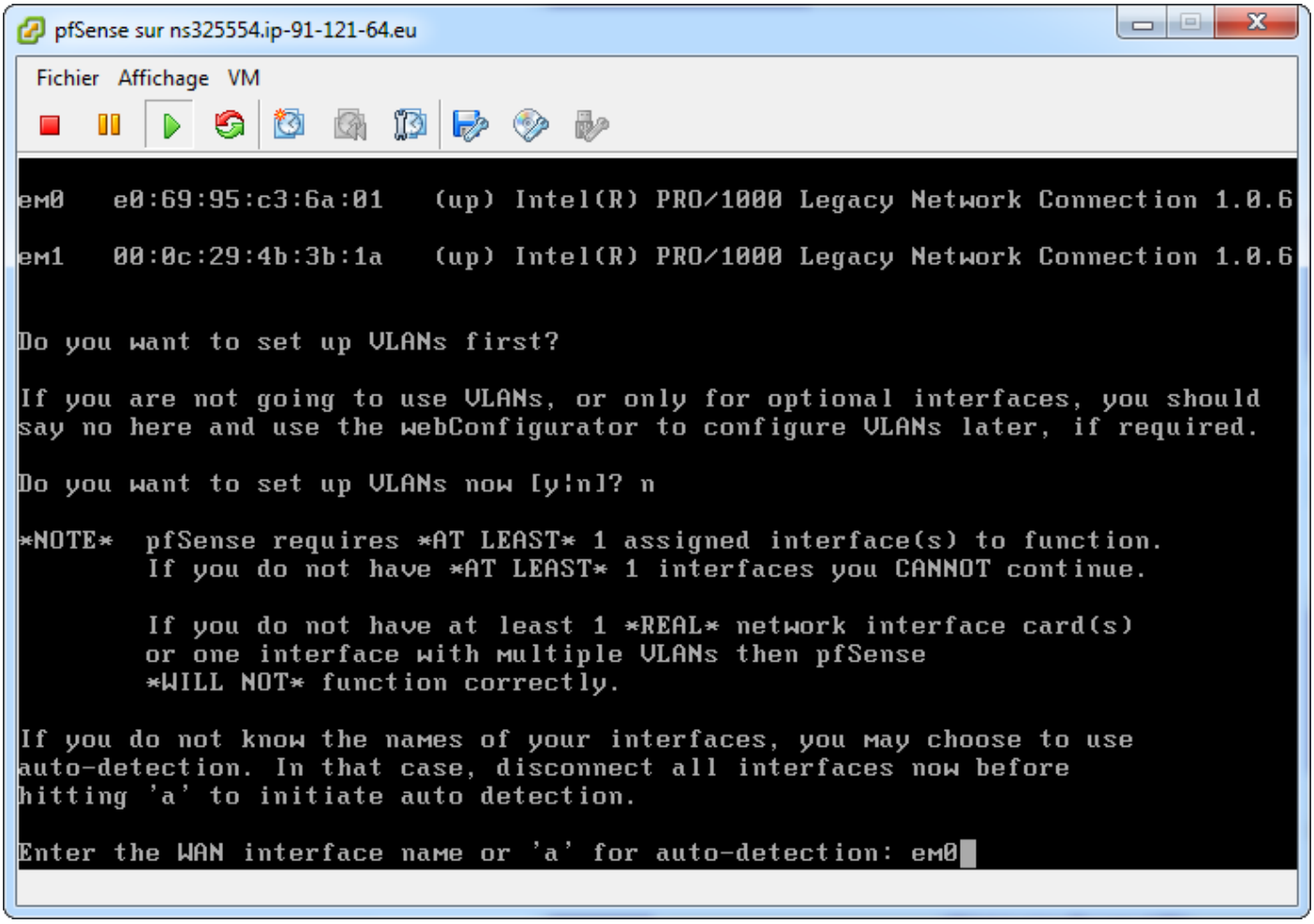
Configuration pfSense

Premier démarrage

Au premier démarrage nous allons renseigner la configuration de base.

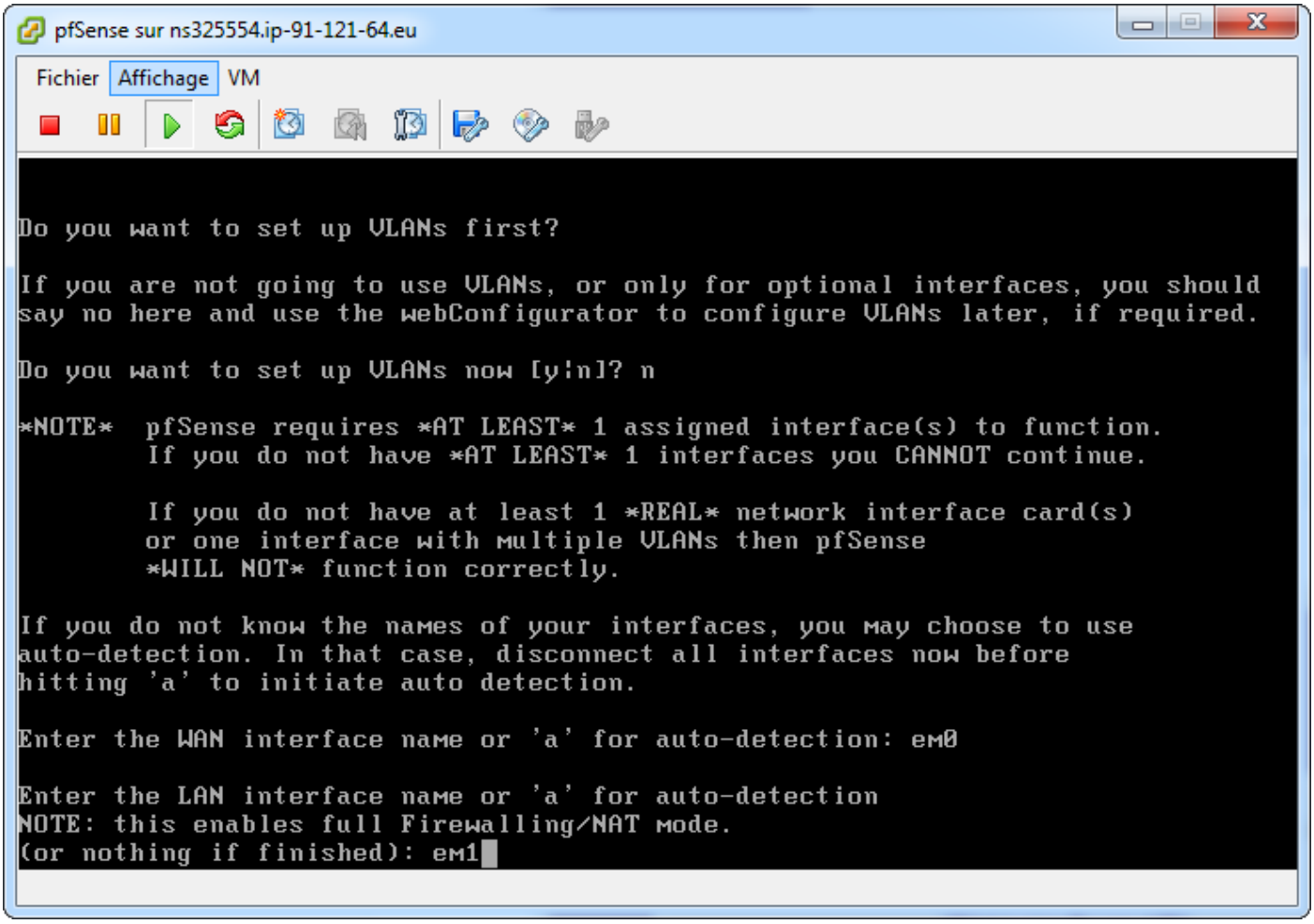


Répondre « no » à la question « Do you want to set up VLANs now ».



Les interfaces réseaux sont listées en haut de l'écran. L'interface WAN devra être celle qui utilise l'adresse MAC physique (pour rappel **e0:69:95:c3:6a:01**). Nous répondrons donc « em0 » (à adapter selon votre cas).

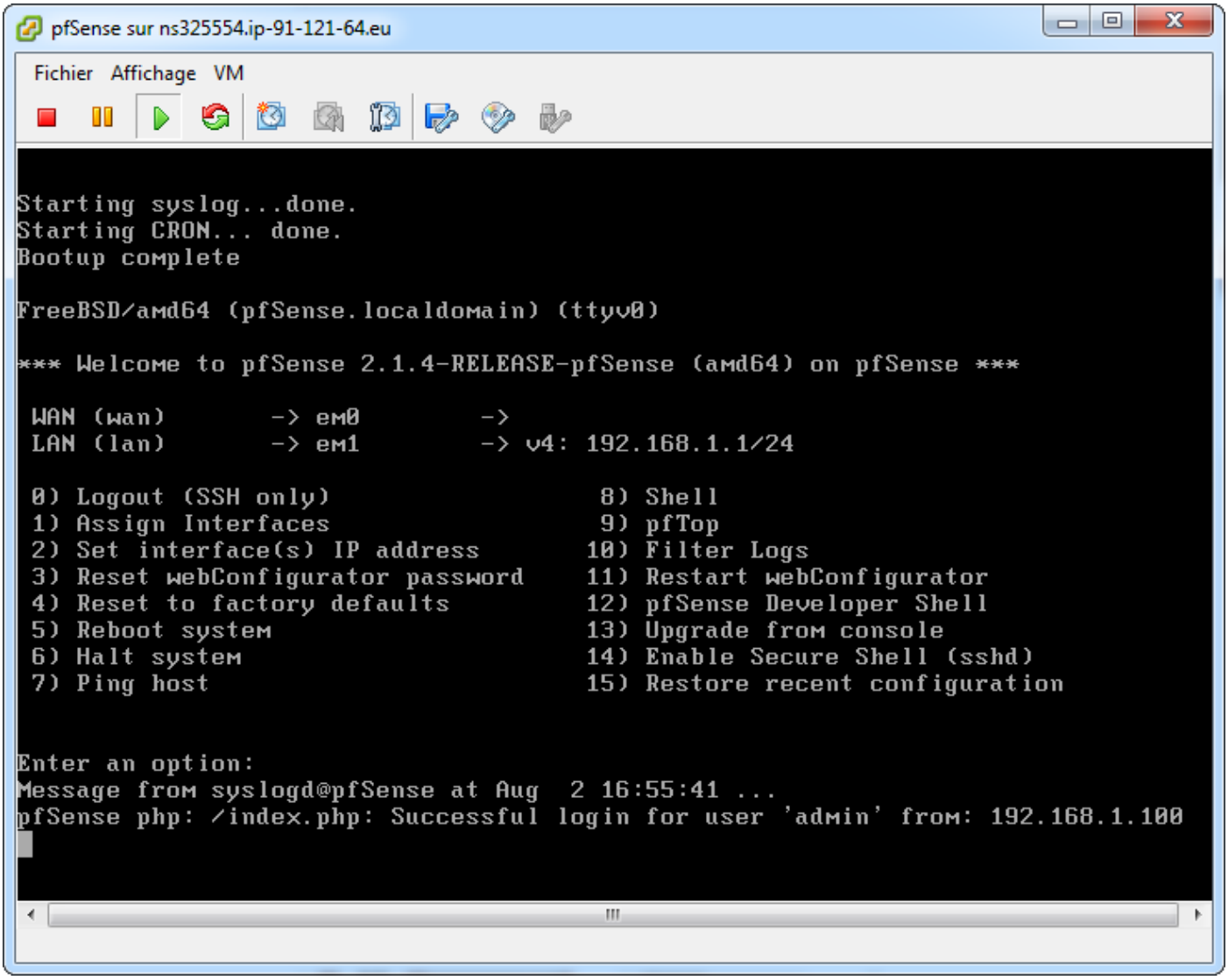
Vient le tour de l'interface LAN :



Il suffit de remplir avec le nom de la seconde interface « em1 » dans ce cas.

pfSense demandera alors si on veut configurer d'autre interface optionnel. Ne rien répondre en tapant juste sur la touche Entrée.

Après quelques minutes le menu devrait ressembler à :

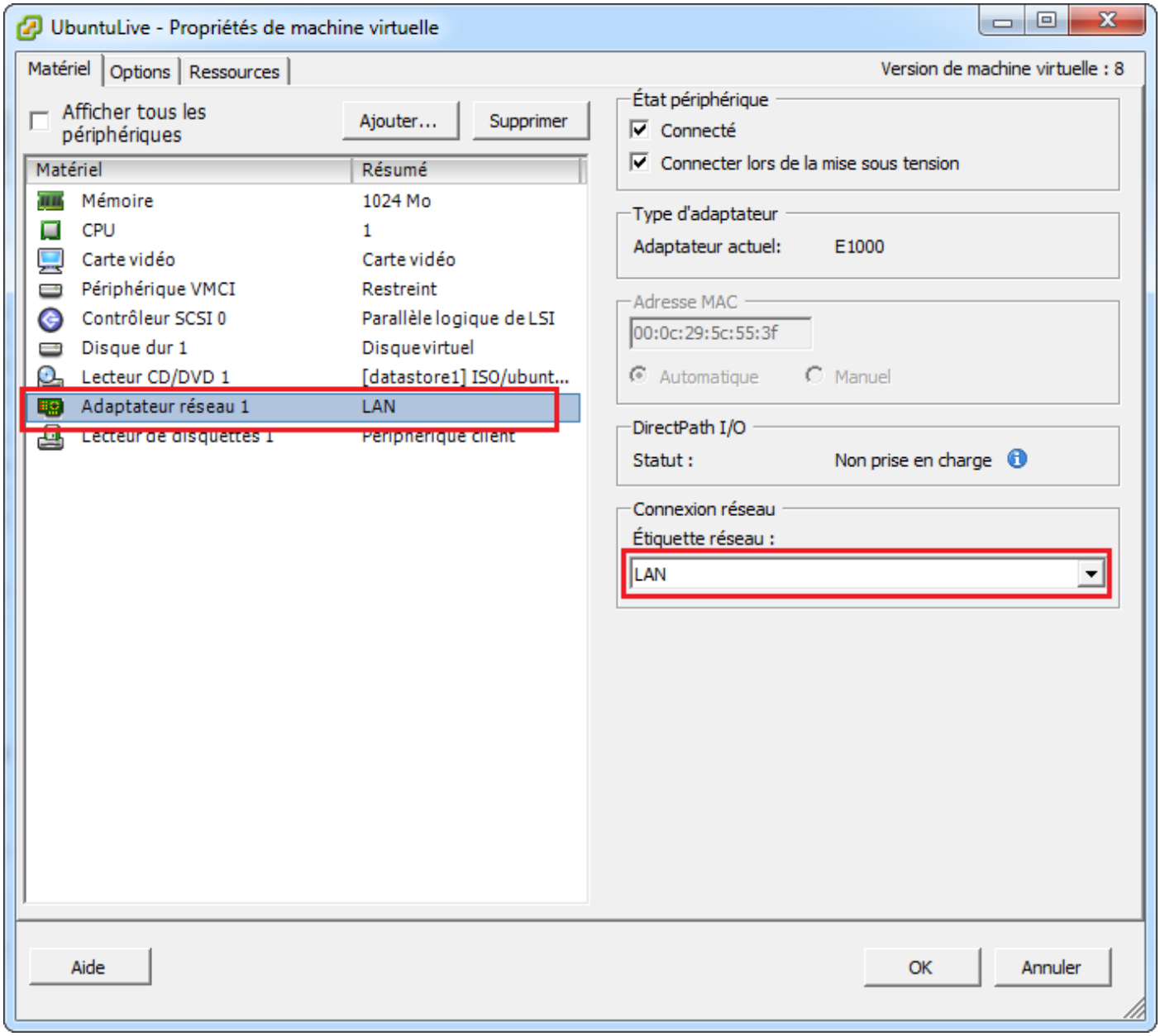


Noter l'adresse de l'interface LAN : 192.168.1.1 et le masque /24.

Nous allons maintenant dérouler la configuration de pfSense via le WebGUI.

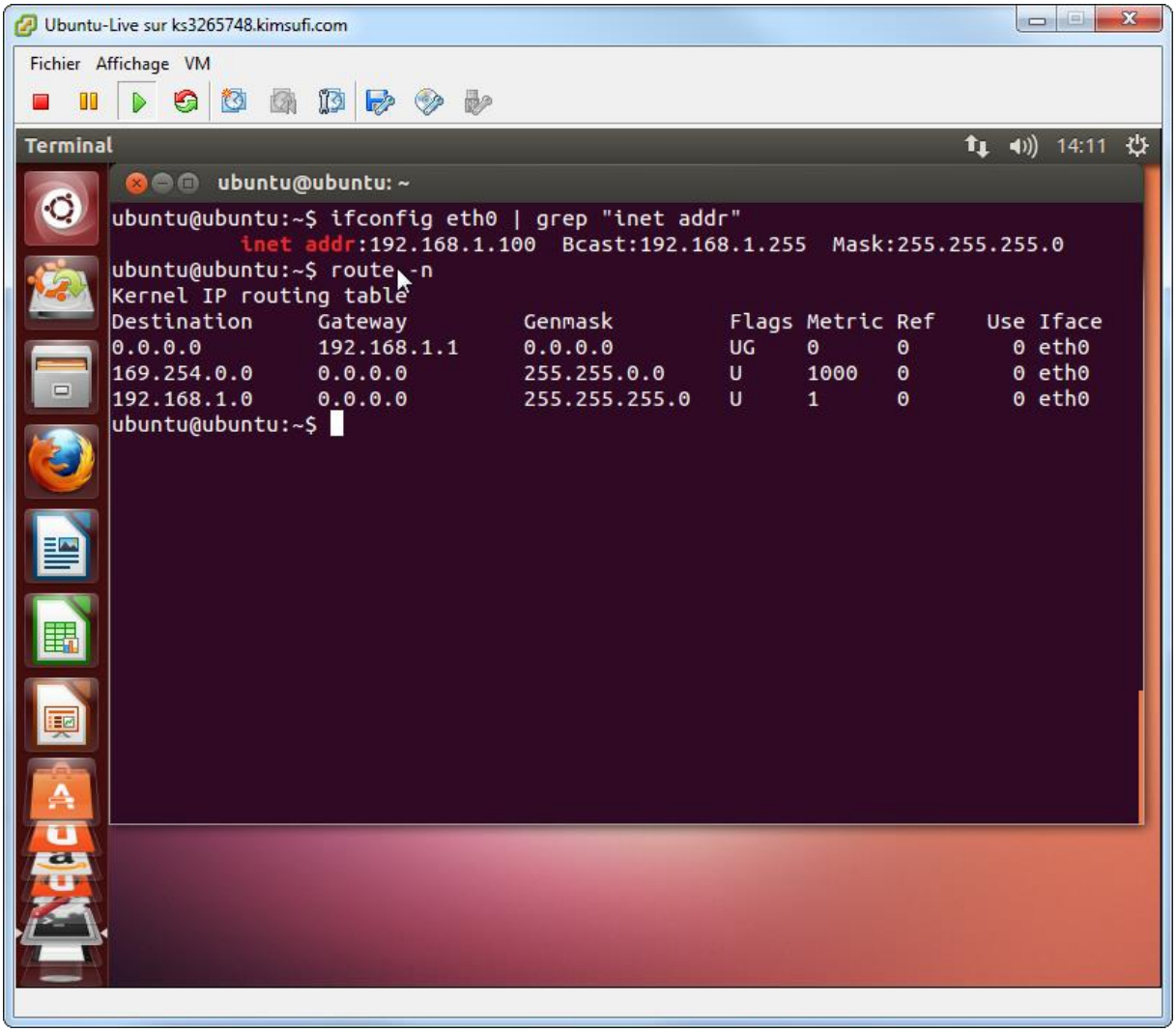
Configuration via le WebGUI

Créer une nouvelle VM pour Ubuntu et brancher l'interface sur le réseau « LAN » :

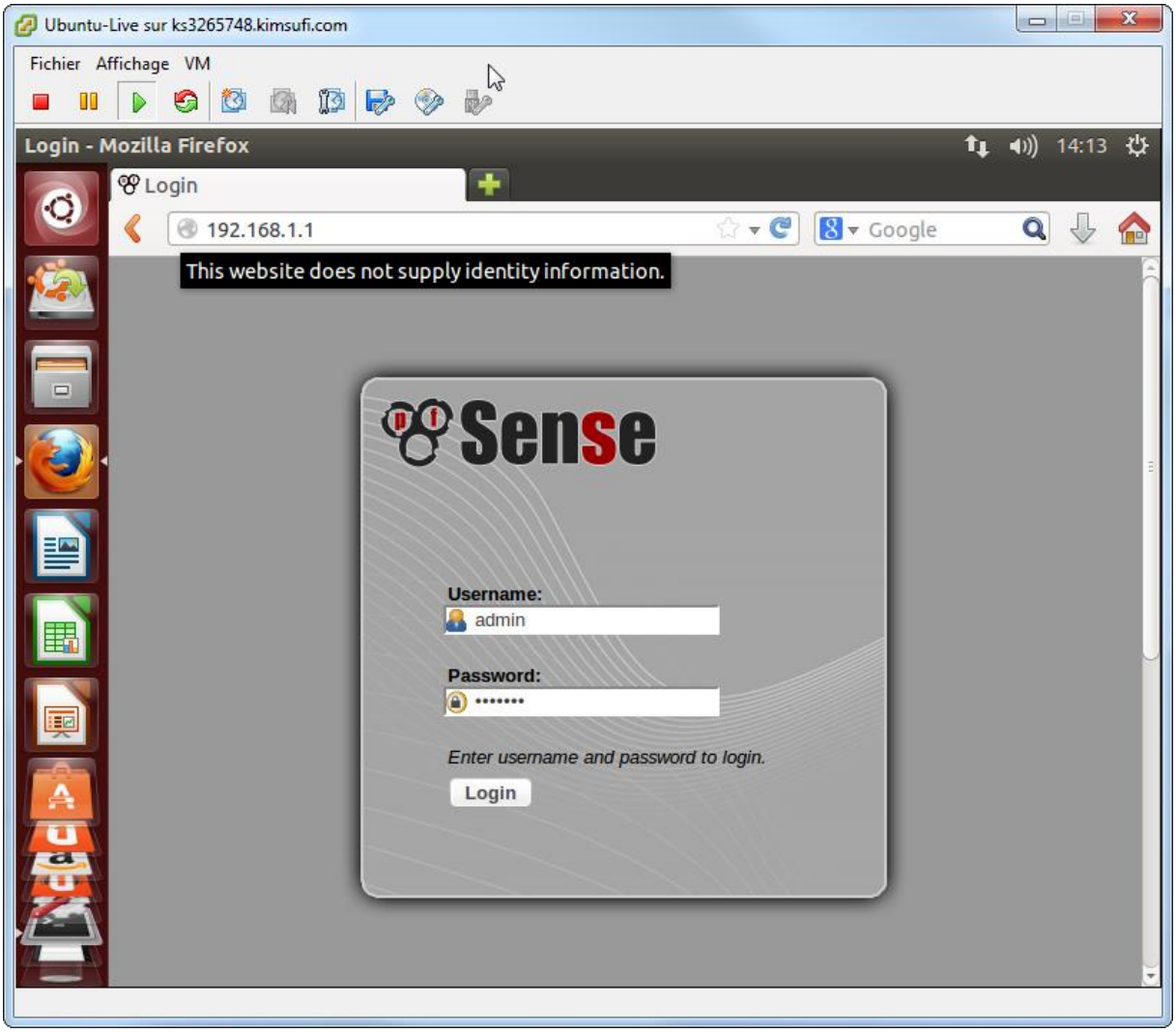


Puis démarrer sur le CD en suivant le même principe que pour pfSense. Il est inutile d'installer la distribution l'option « Try Ubuntu » nous suffira largement.

Si tout se passe bien, nous devrions arriver sur le bureau et nous pouvons vérifier la configuration réseau :

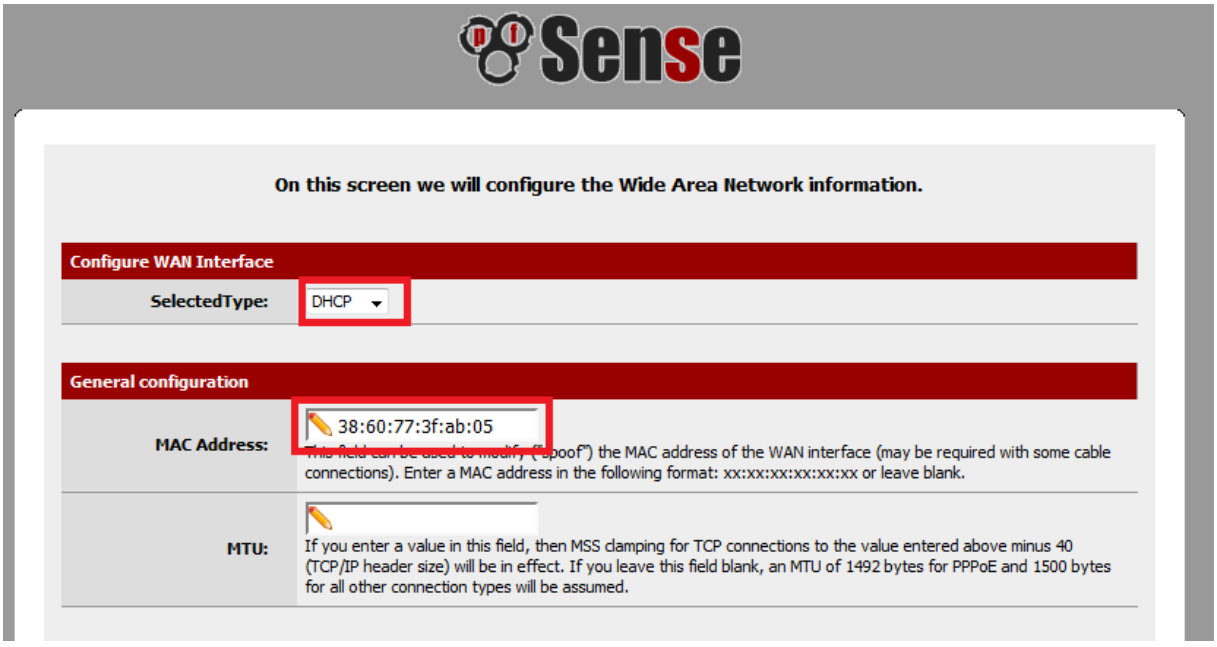


Nous ouvrons alors Firefox à l'adresse http://192.168.1.1 :



Par défaut l'username est « admin » et le password « pfsense ».

Il ne reste plus qu'à suivre le guide. Nous choisirons l'interface WAN en DHCP :

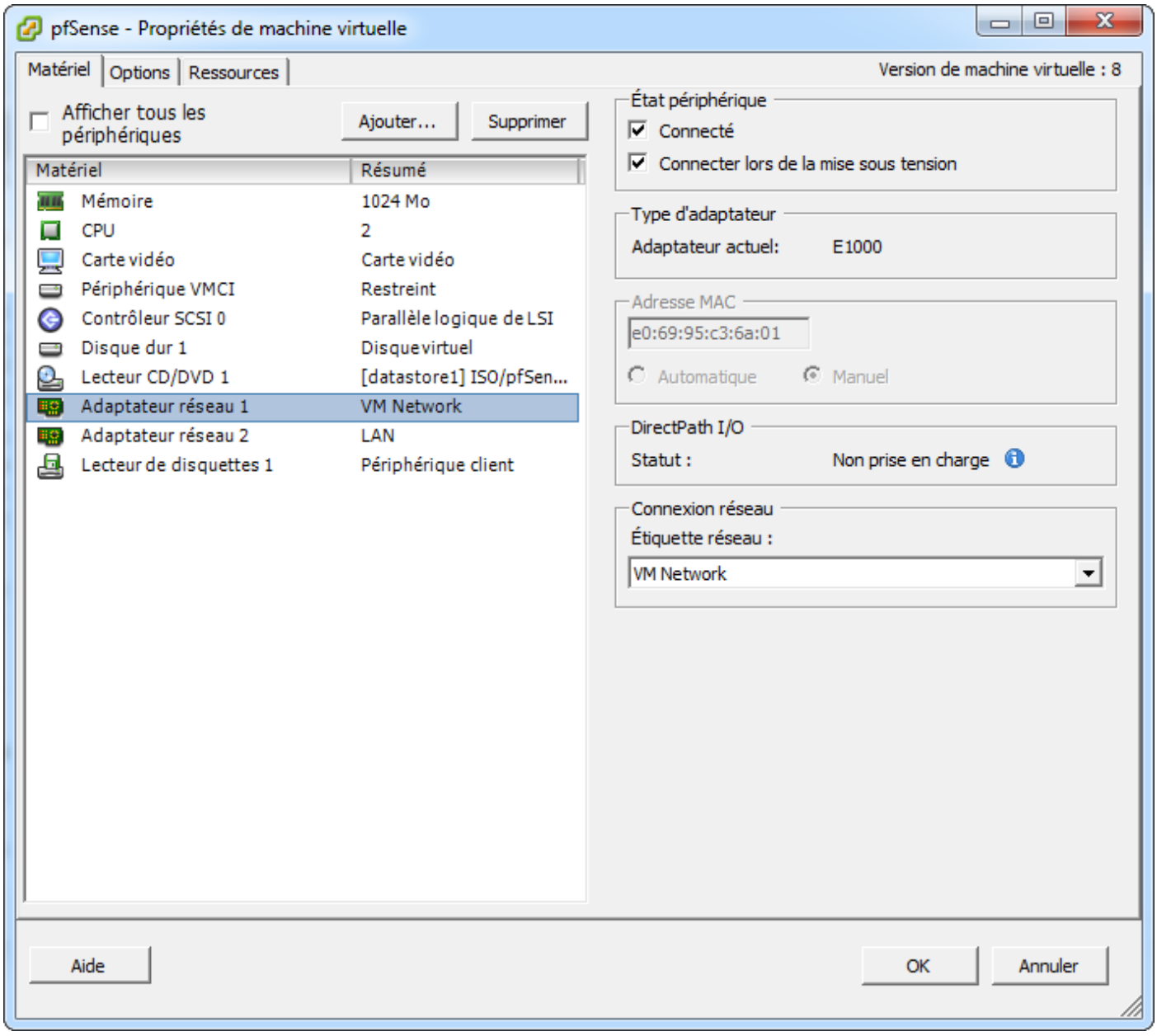


Depuis la version 2 de ce guide il n'est plus nécessaire de remplir le champ « MAC Address », pour spoofer l'adresse du serveur, puisque nous avons fixé cette adresse en dur dans les paremètres de la

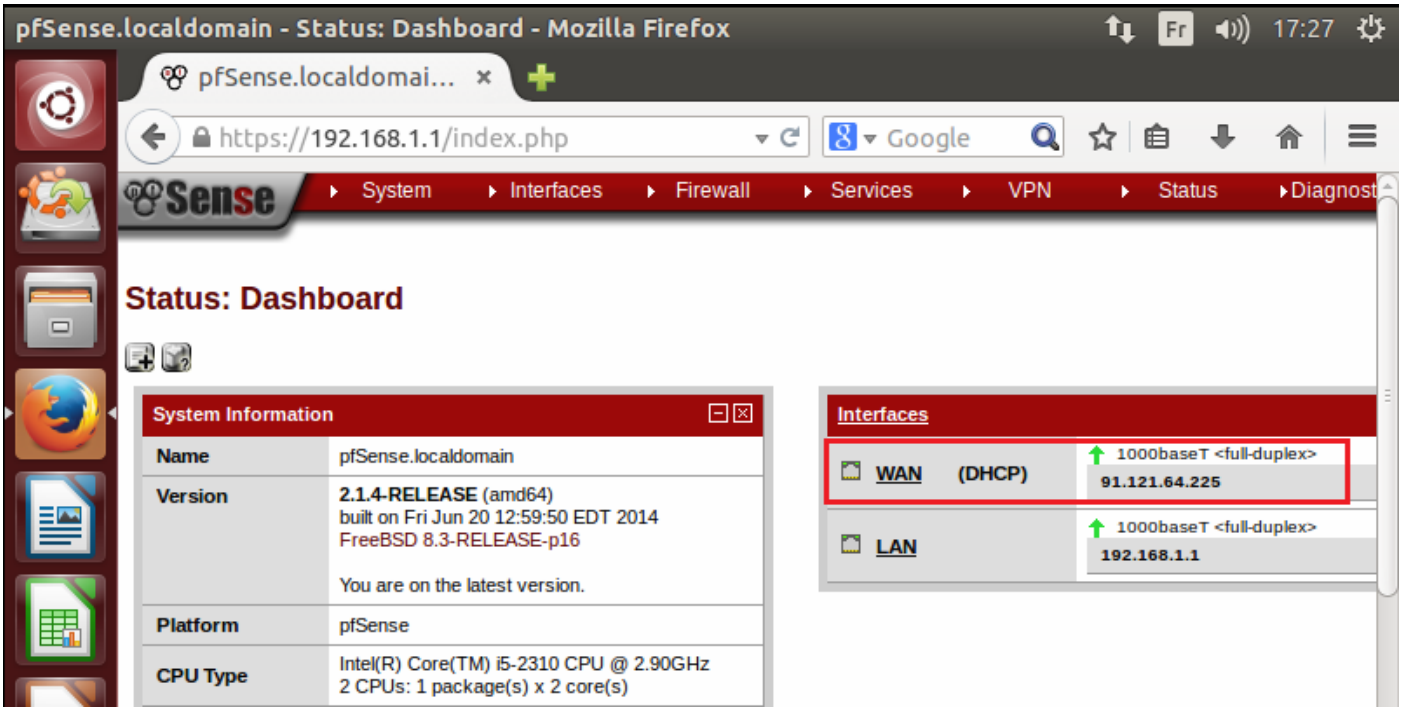
machine virtuelle. Néanmoins si vous vous êtres tompés vous pouvez toujours remplir le champ avec la bonne adresse.

Pour le DNS : rentrer le DNS fournit par l'hébergeur ou bien pour dépanner en attendant « 8.8.8.8 » (DNS Google).

La configuration est prête, il nous reste plus qu'à déconnecter l'interface WAN connecté au réseau « Dummy » pour la connecter sur l'interface « VM Network ».

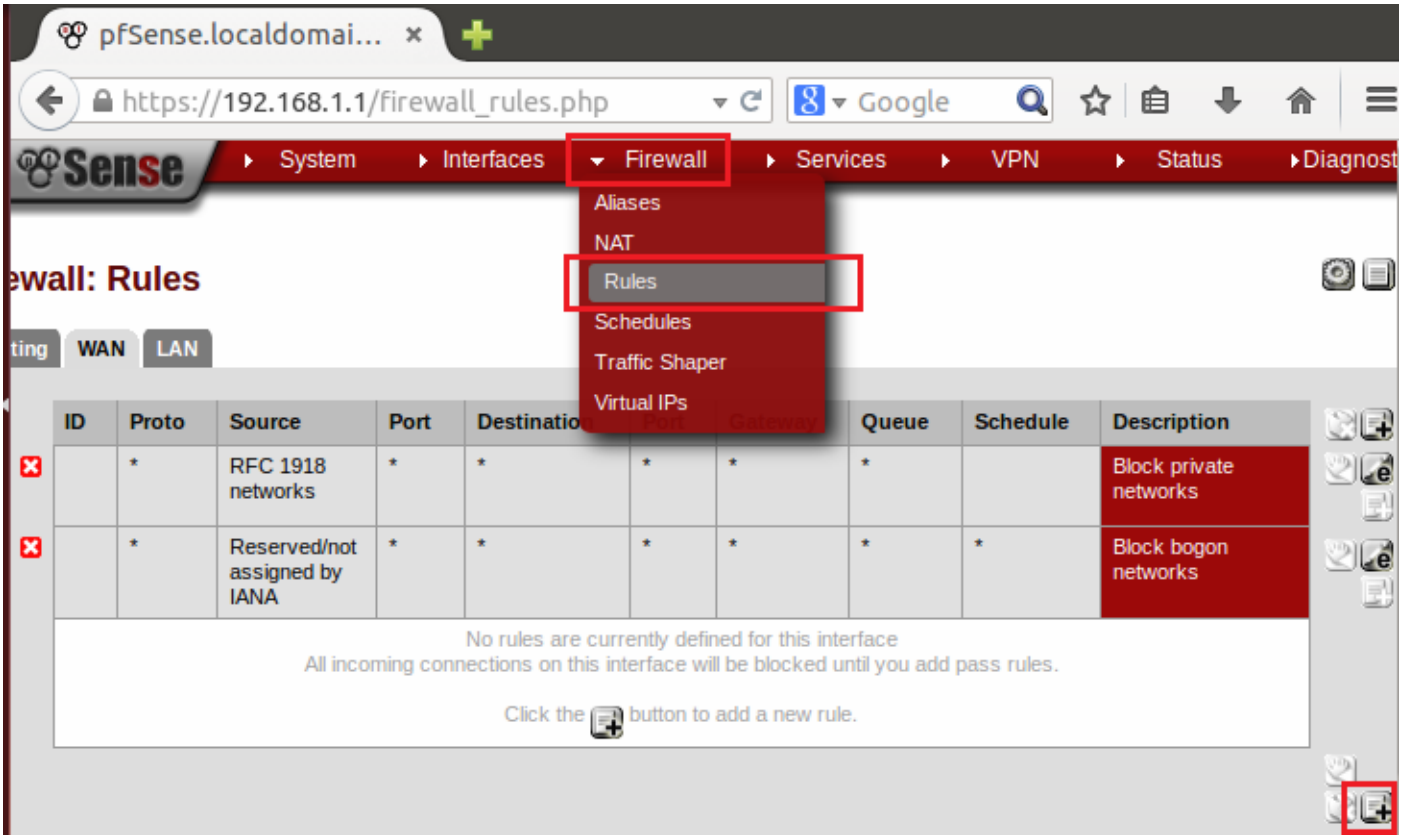


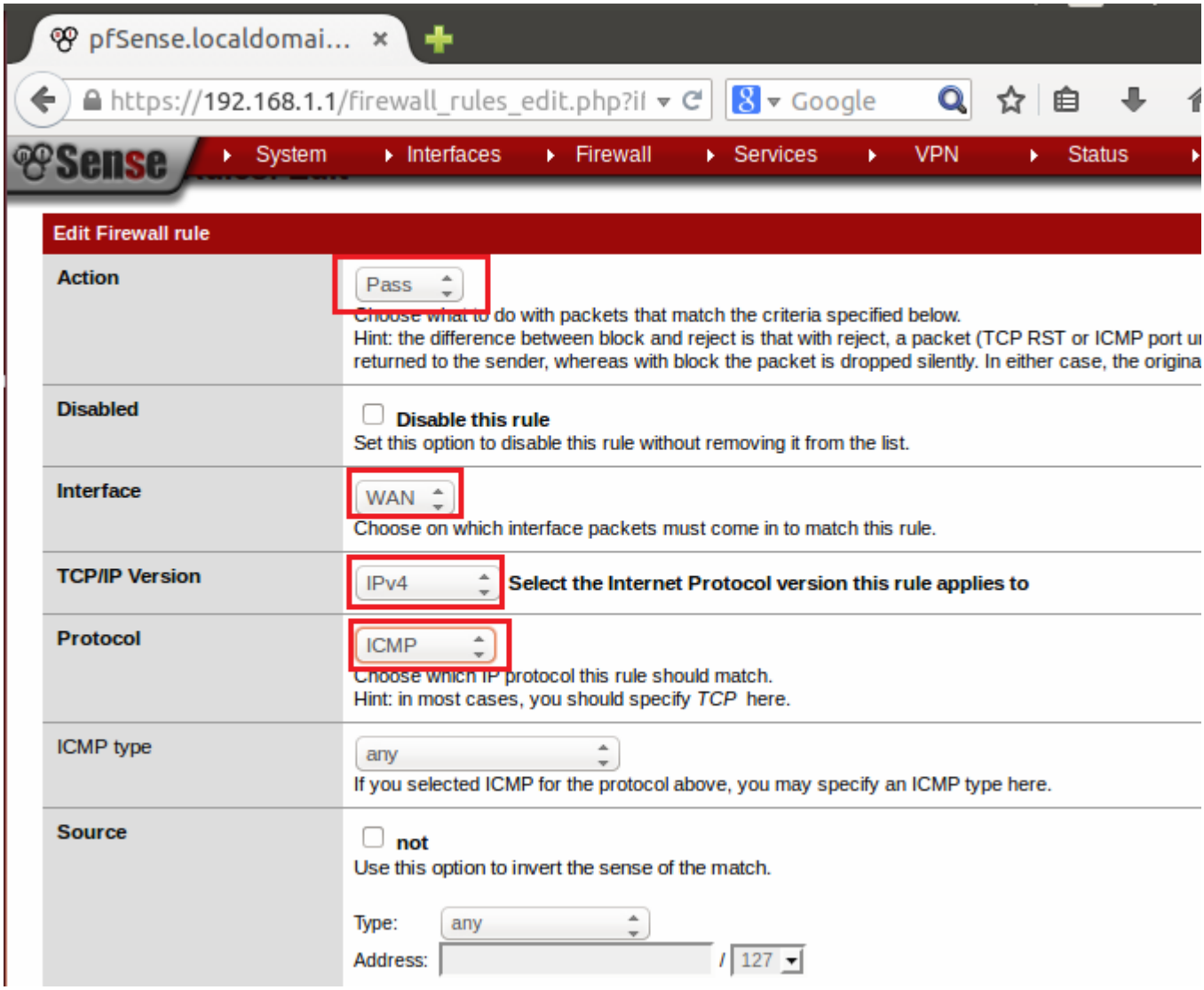
Au bout de quelques minutes nous devrions voir depuis le Dashboard pfSense une adresse IPv4 publique assignée à l'interface WAN :



L'IPv4 « 91.127.64.225 » a donc bien été assignée automatiquement sur l'interface WAN via DHCP.

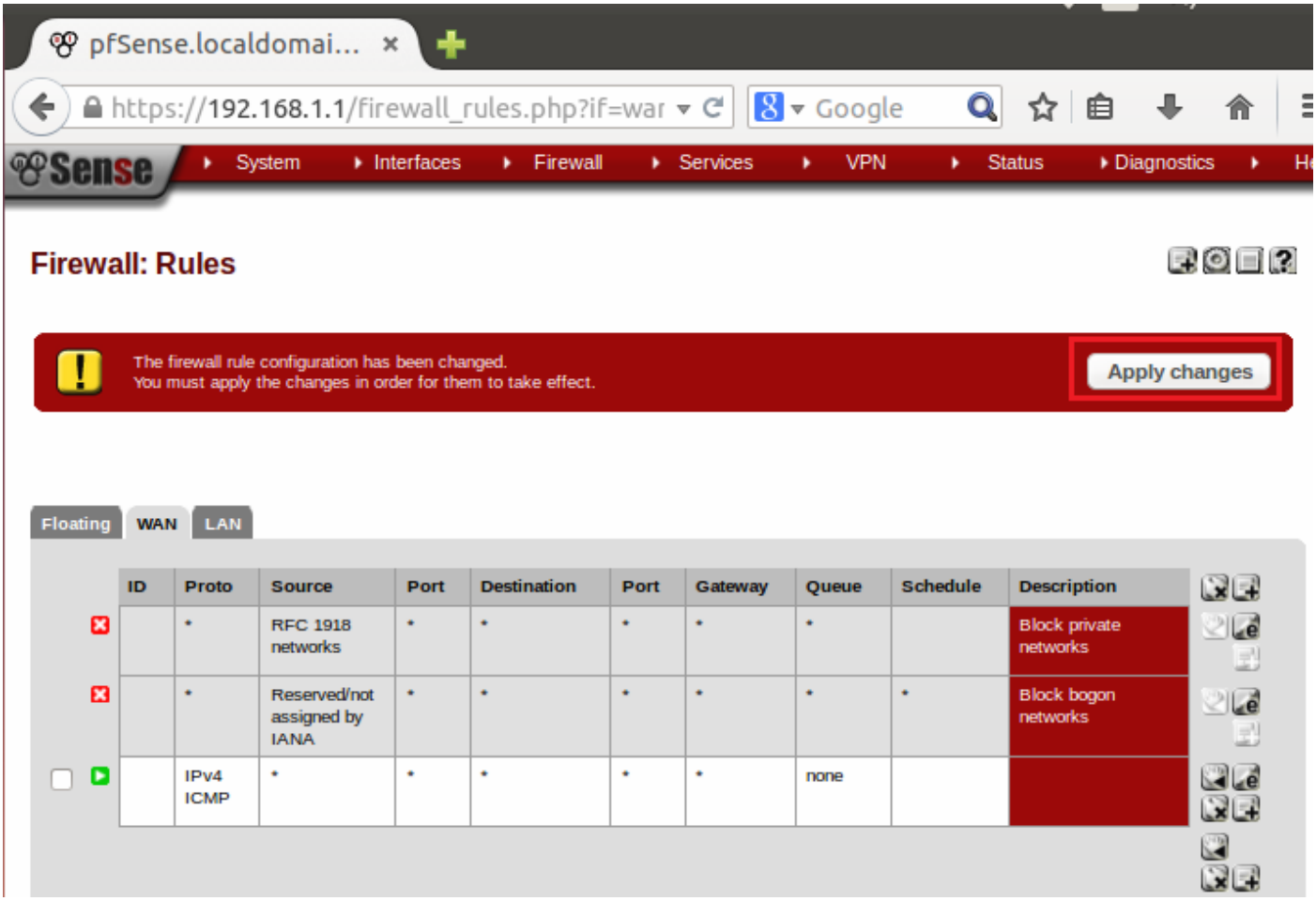
Par défaut pfSense ne répond pas aux PING, si nous voulons réactiver le monitoring, il faut créer une règle dans le firewall depuis le menu « Firewall », « Rules » :



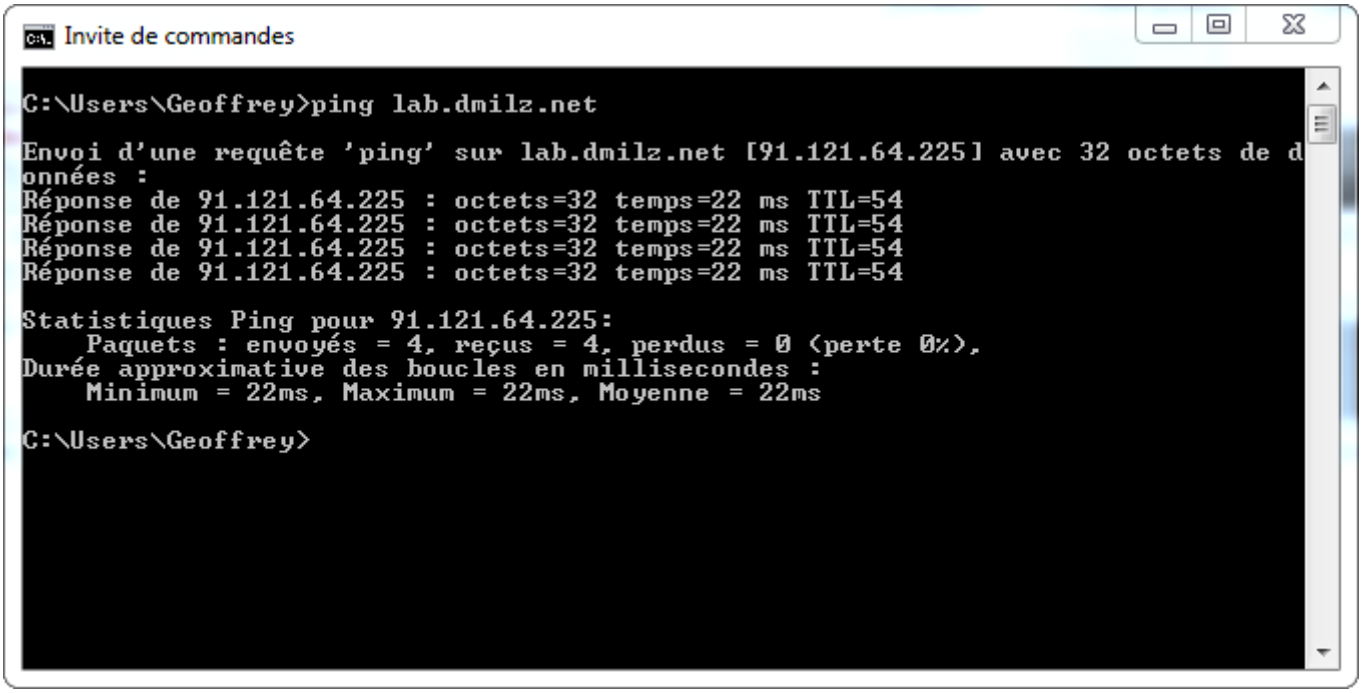


Action « Pass », Interface « WAN », TCP/IP Version « IPv4 », Protocol « ICMP » puis enregistrer en cliquant sur « Save ».

Nous appliquons alors les changements en cliquant sur « Apply Changes ».



Au bout de quelques secondes le serveur devrait donc maintenant répondre aux PING :



Configuration des VM

L'environnement est prêt pour apporter la connexion aux futurs VM.

Connecter un VM à Internet

La connexion d'un VM à Internet est très simple :

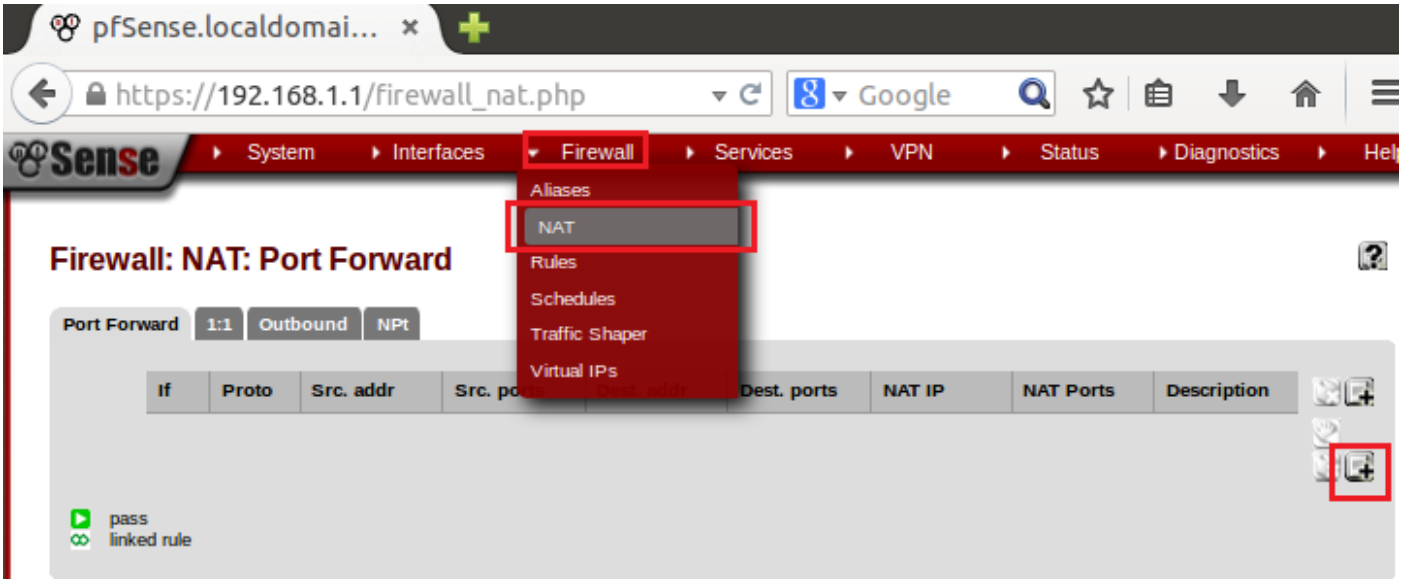
- son interface réseau est à définir sur le réseau « LAN »
- soit la VM est en adressage automatique et elle récupèrera la configuration via le DHCP de pfSense (cas du Live Ubuntu dans ce guide)
- soit la VM est en adressage statique et il faudra lui attribuée une adresse IP dans le sous réseau LAN (par défaut 192.168.1.0/24), le bon masque (défaut 255.255.255.0), sa gateway (pfSense 192.168.1.1 ici) et le DNS (192.168.1.1 ou tout autre DNS).

Les VM auront un accès total à Internel moyennant les règles de filtrage par défaut ou personnalisé du firewall pfSense.

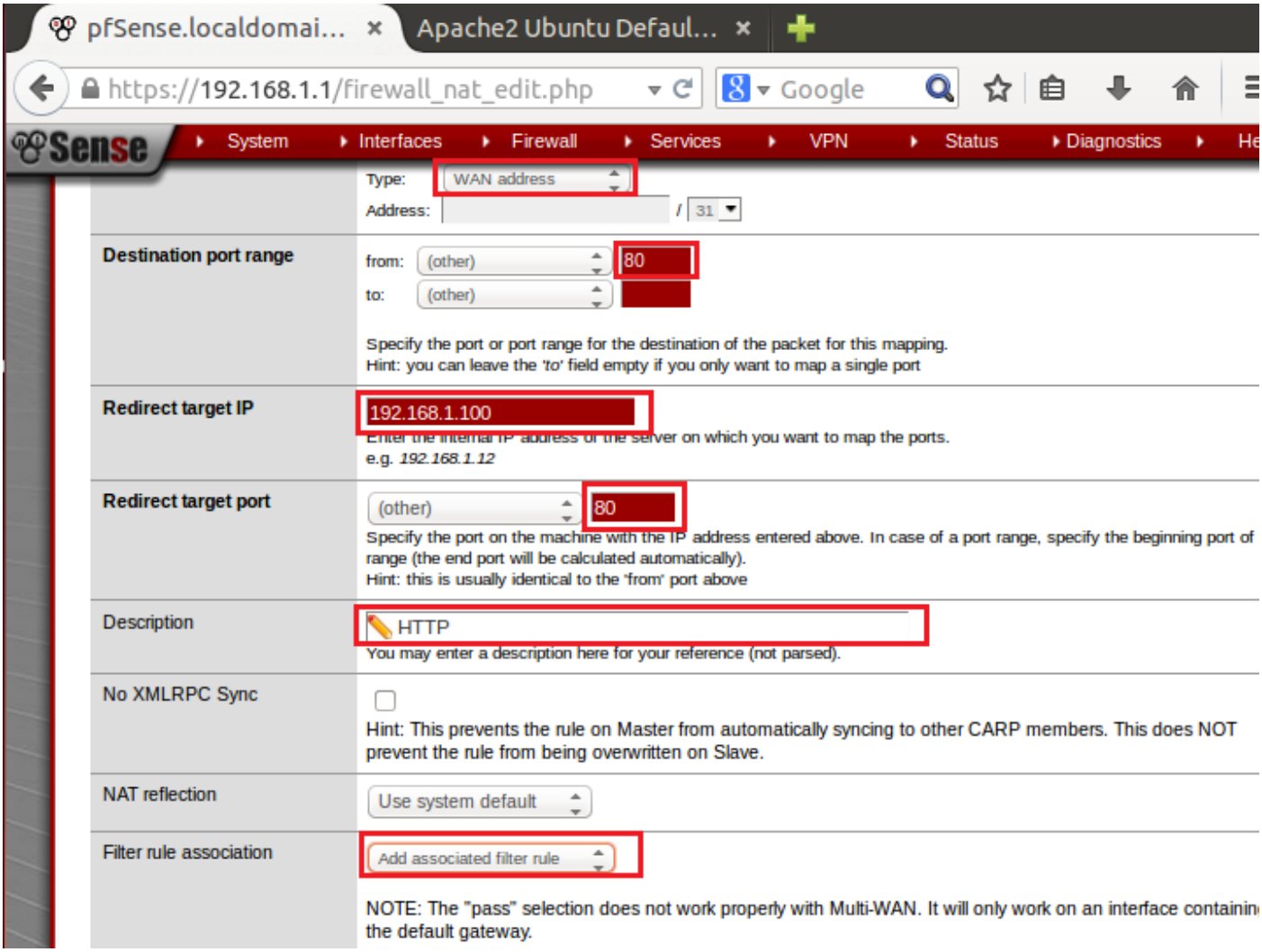
Connecter Internet à une VM

L'adresse IPv4 publique est assignée à pfSense. Toute connexion depuis l'extérieur passera donc forcément par lui.

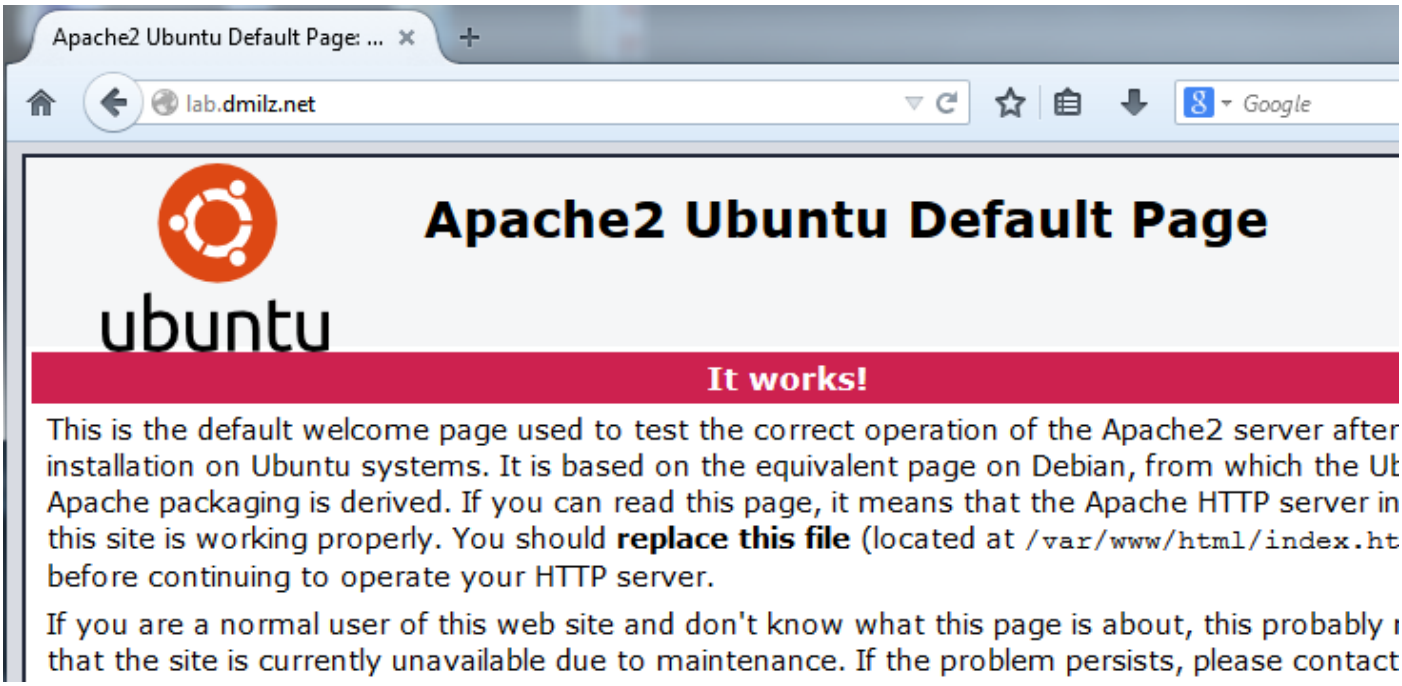
Pour que le monde puisse accéder aux services offerts par les autres VM du réseau LAN il sera nécessaire de configurer des redirections de ports dans pfSense.



Puis nous remplissons la règle :



Laisser « Destination address » sur « WAN adress », configurer correctement la « Destination port range » (pour sur lesquels le client se connecte), sur quelle machine rediriger la semaine « Redirect Target IP » ainsi que le port sur cette machine « Redirect Target Port ». Vérifier que Filter rule association soit sur « Add associated filter rule », cela permettra un réglage plus fin depuis le menu « Firewall » puis « Rules ».

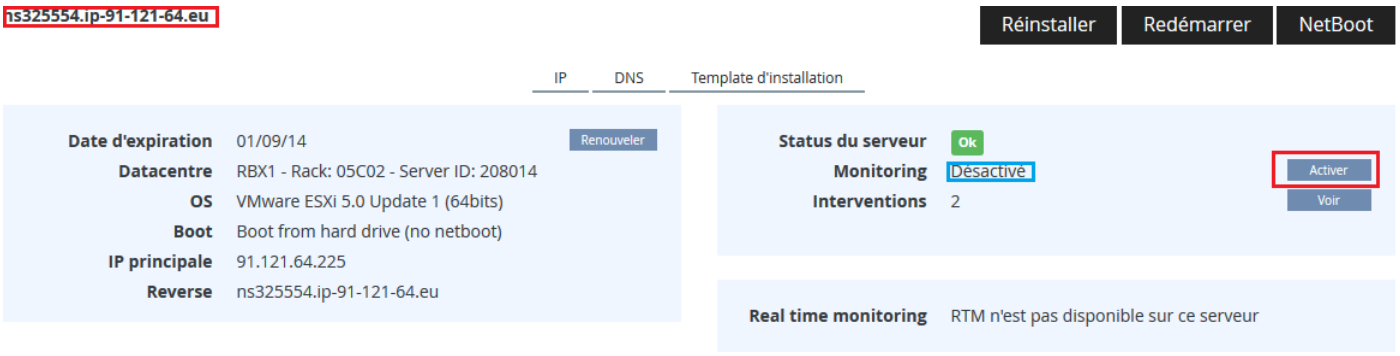


Nous sommes donc bien rediriger sur le serveur web de la machine 192.168.1.100 (attention Ubuntu Live ne possède pas de serveur http par défaut, pour tester il faut au préalable l'installer avec « sudo apt-get install apache »).

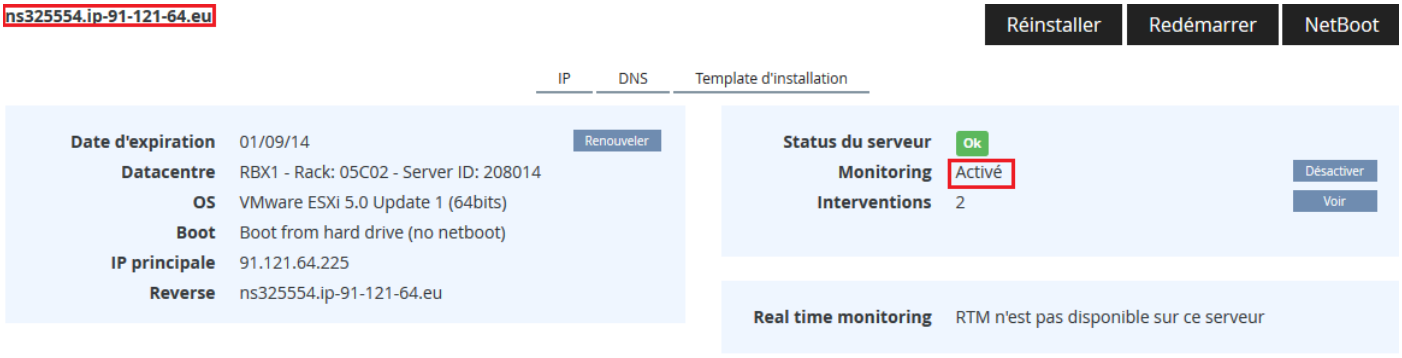
Derniers réglages (optionnels)

Réactiver le monitoring

Puisque pfSense répond maintenant au PING il est préférable de réactiver le monitoring depuis le manageur :



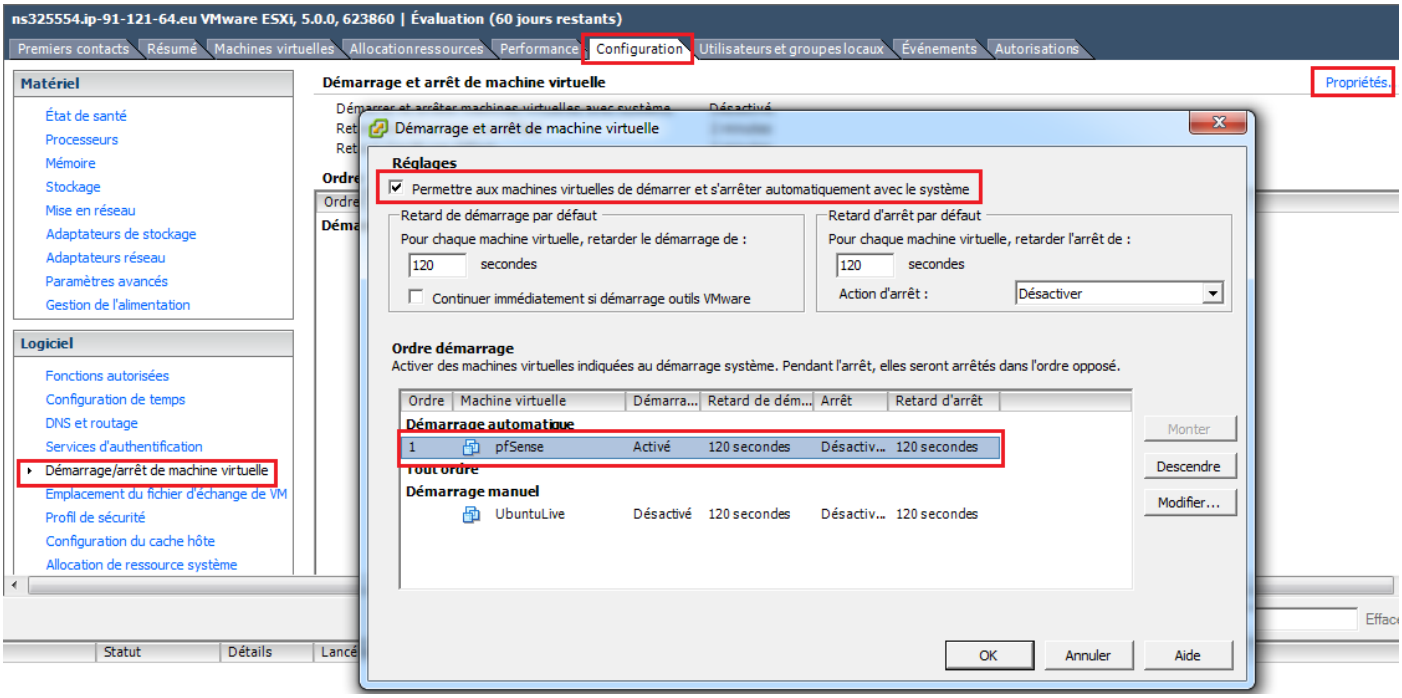
Si le monitoring est toujours « Désactivé » alors cliquer sur « Activer » :



A ce stade la solution est fonctionnelle mais la gestion de l'ESXi ne peut se faire uniquement via IPV6 et la connexion des VM serait perdue en cas de redémarrage du serveur physique.

Forcer le démarrage de pfSense en au démarrage de l'ESXi

Depuis le menu « Configuration » du serveur ESXi, « Démarrage/arrêt de machine virtuelle », « Propriétés » :



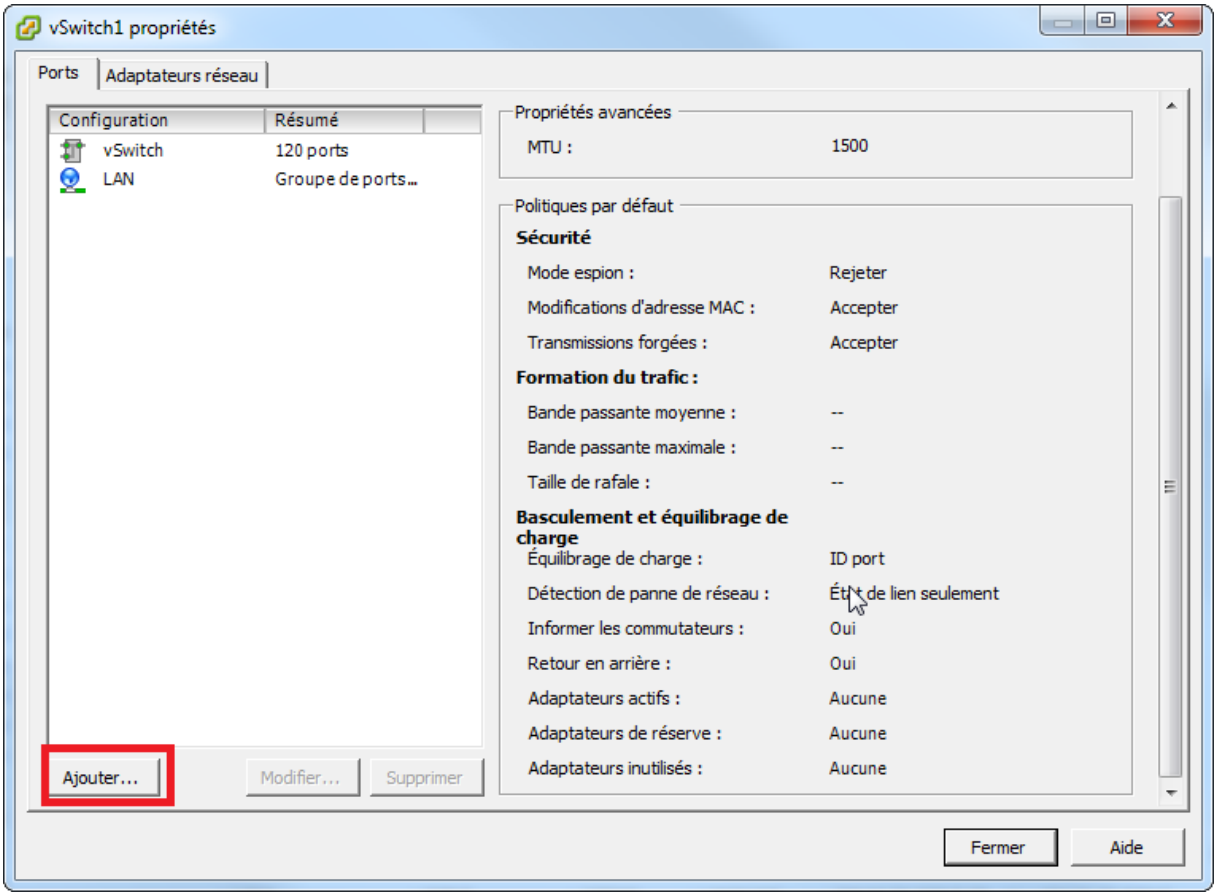
Cocher « Permettre aux machines virtuelles de démarrer et s'arrêter automatiquement avec le système ». Puis faire monter la VM pfSense dans « Démarrage automatique ».

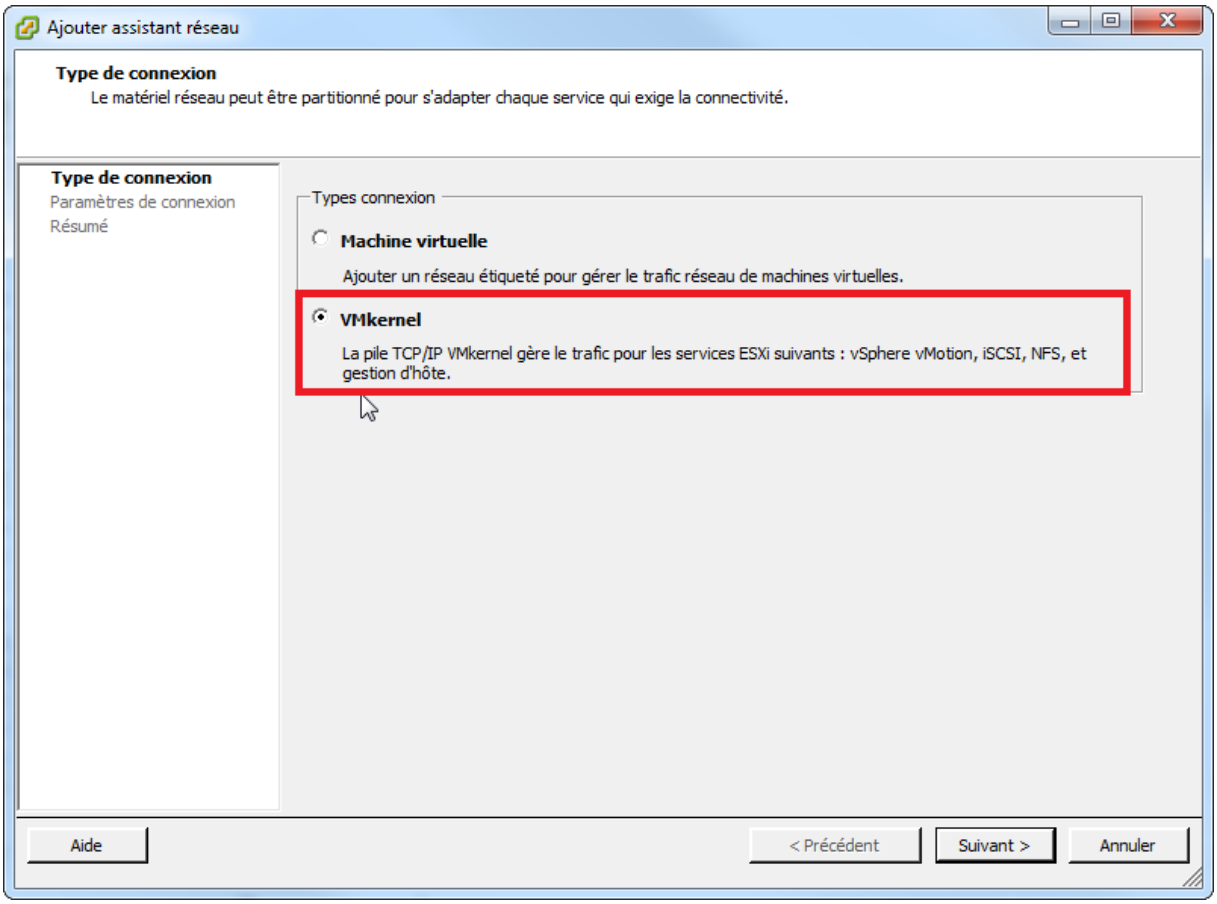
Dorénavant la machine démarrera avec le système.

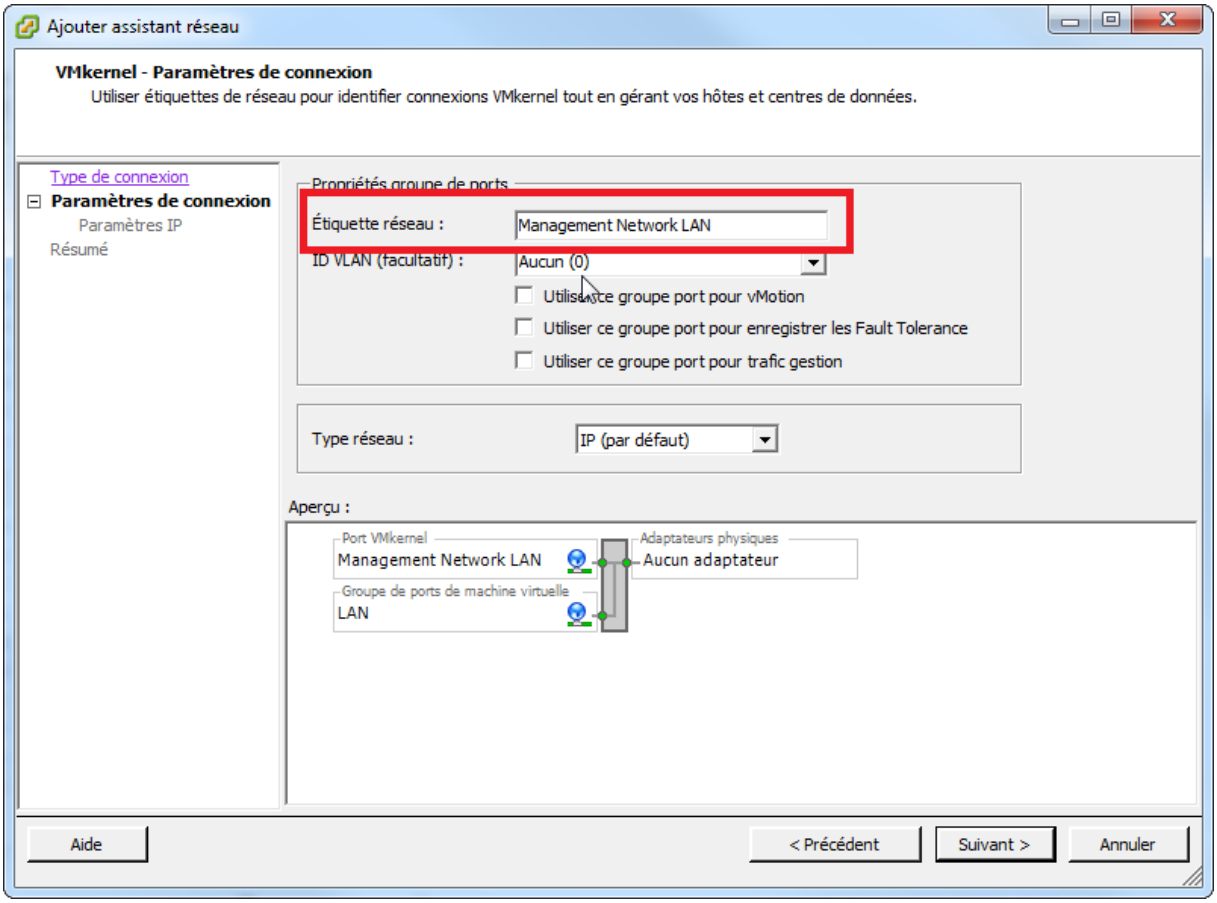
VMkernel sur le réseau LAN

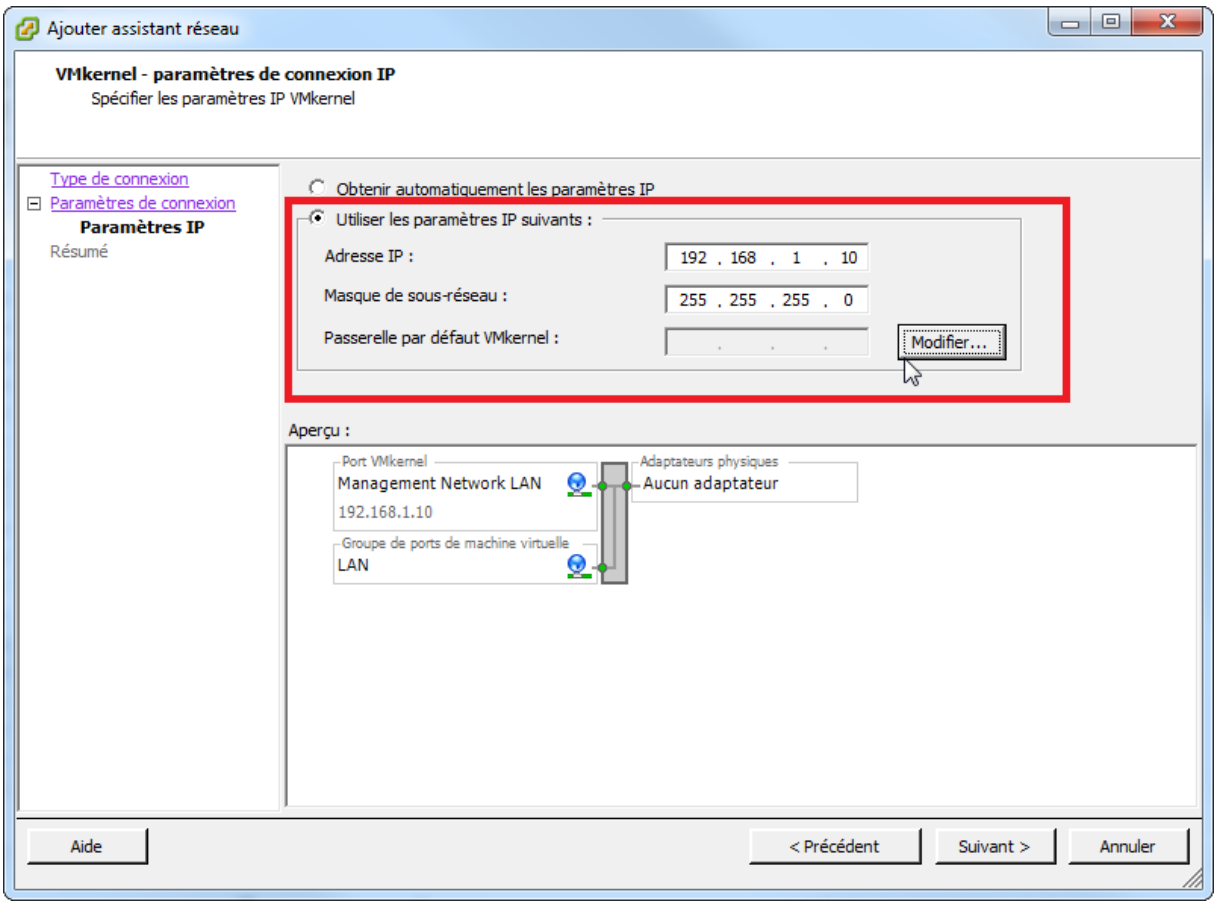
En cas d'indisponibilité IPv6 (soit un défaut chez l'hébergeur soir un problème de connexion), il n'est plus possible de prendre la main sur ESXi via le client vSphere. Nous allons donc configurer un VMkernel sur le réseau « LAN ».

Depuis le menu « Configuration », « Mise en réseau », nous allons dans les propriétés du vSwitch « LAN » puis « Ajouter » :


vSwitch1 propriétés
Ports
Adaptateurs réseau
Configuration
Résumé
vSwitch
120 ports
LAN
Groupe de ports...
Propriétés avancées
MTU :
1500
Politiques par défaut
Sécurité
Mode espion :
Rejeter
Modifications d'adresse MAC :
Accepter
Transmissions forgées :
Accepter
Formation du trafic :
Bande passante moyenne :
--
Bande passante maximale :
--
Taille de rafale :
--
Basculement et équilibrage de charge
Équilibrage de charge :
ID port
Détection de panne de réseau :
Informer les commutateurs :
Oui
Retour en arrière :
Oui
Adaptateurs actifs :
Aucune
Adaptateurs de réserve :
Aucune
Adaptateurs inutilisés :
Aucune
Ajouter...
Modifier...
Supprimer
Fermer
Aide


Ajouter assistant réseau
Type de connexion
Le matériel réseau peut être partitionné pour s'adapter chaque service qui exige la connectivité.
Type de connexion
Paramètres de connexion
Résumé
Types connexion
Machine virtuelle
Ajouter un réseau étiqueté pour gérer le trafic réseau de machines virtuelles.
VMkernel
La pile TCP/IP VMkernel gère le trafic pour les services ESXi suivants : vSphere vMotion, iSCSI, NFS, et gestion d'hôte.
Aide
< Précédent
Suivant >
Annuler





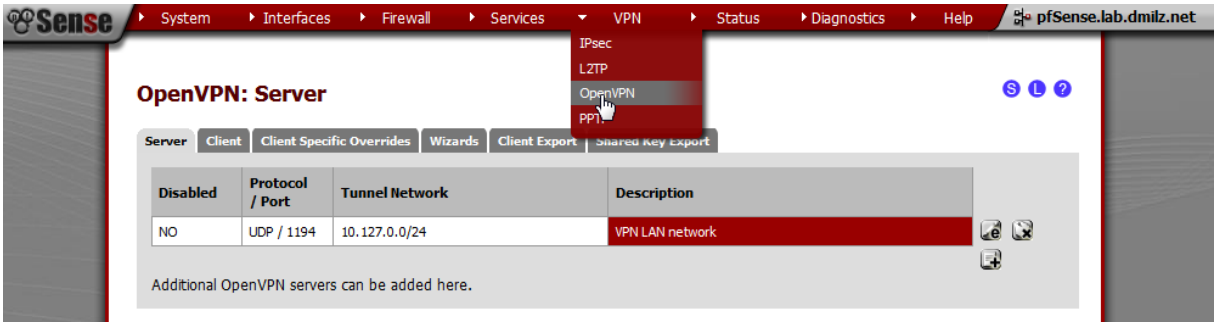
Entrer une adresse IP (ici « 192.168.1.10 », le masque (« 255.255.255.0 ») puis cliquer sur « Modifier » pour ajouter la passerelle par défaut « 192.168.1.1 ».

Dorénavant il est possible d'accéder au VMkernel depuis le réseau LAN :

- soit depuis un VM Windows avec le client vSphere
- soit en redirigeant les ports depuis pfSense (non recommandé…)
- soit avec une connexion VPN

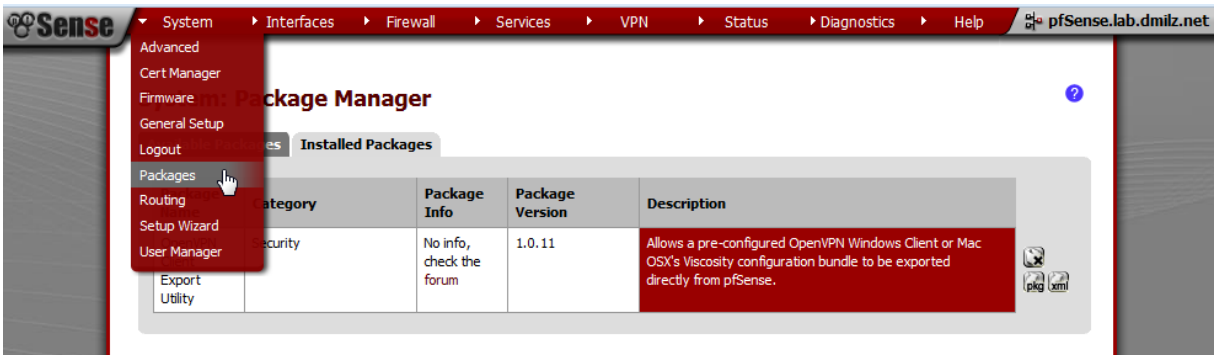
Connexion au réseau LAN via VPN

pfSense embarque nativement un serveur OpenVPN, mais celui-ci n'est pas activé par défaut, il faut donc le configurer depuis le menu « VPN » :



L'objet de ce guide n'est pas de configurer OpenVPN, mais des exemples sont très facilement trouvable en ligne et la communauté de pfSense est très actives.

Je vous conseille simplement d'installer « OpenVPN Client Export Utility » pour générer facilement une archive avec les fichiers nécessaires aux connexions des clients. Les packages s'installent très facilement depuis « System » et « Packages » :

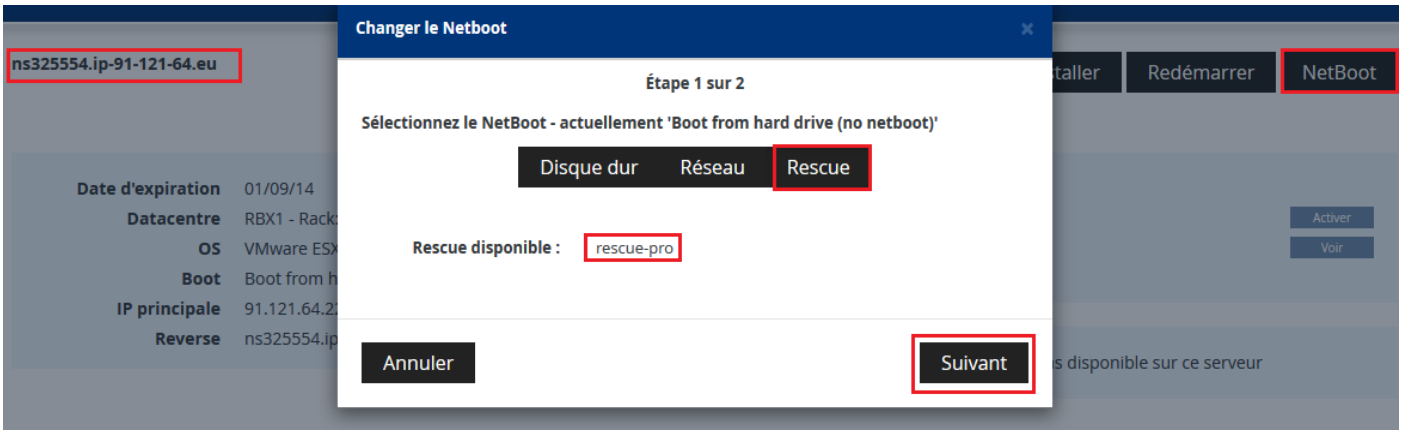


Il faut aussi savoir que les utilisateurs pfSense (VPN ou autres) sont gérés depuis « User Manager » (visible sur la capture ci-dessus), il suffit de générer un certificat depuis la bonne CA pour autoriser la connexion d'un utilisateur au VPN (le package généré par Client Export Utility aidera grandement ensuite pour la configuration coté client).

Reconfigurer ESXi suite une fausse manipulation

Uniquement si le fichier /etc/vmware/esx.conf a été sauvegardé !

S'il n'est vraiment plus possible de se connecter avec le client vSphere ou SSH ni en IPv4, ni en IPv6, il reste encore une solution avant la réinstallation complète du serveur… Passage en mode « rescue » (depuis le manageur Kimsufi) :

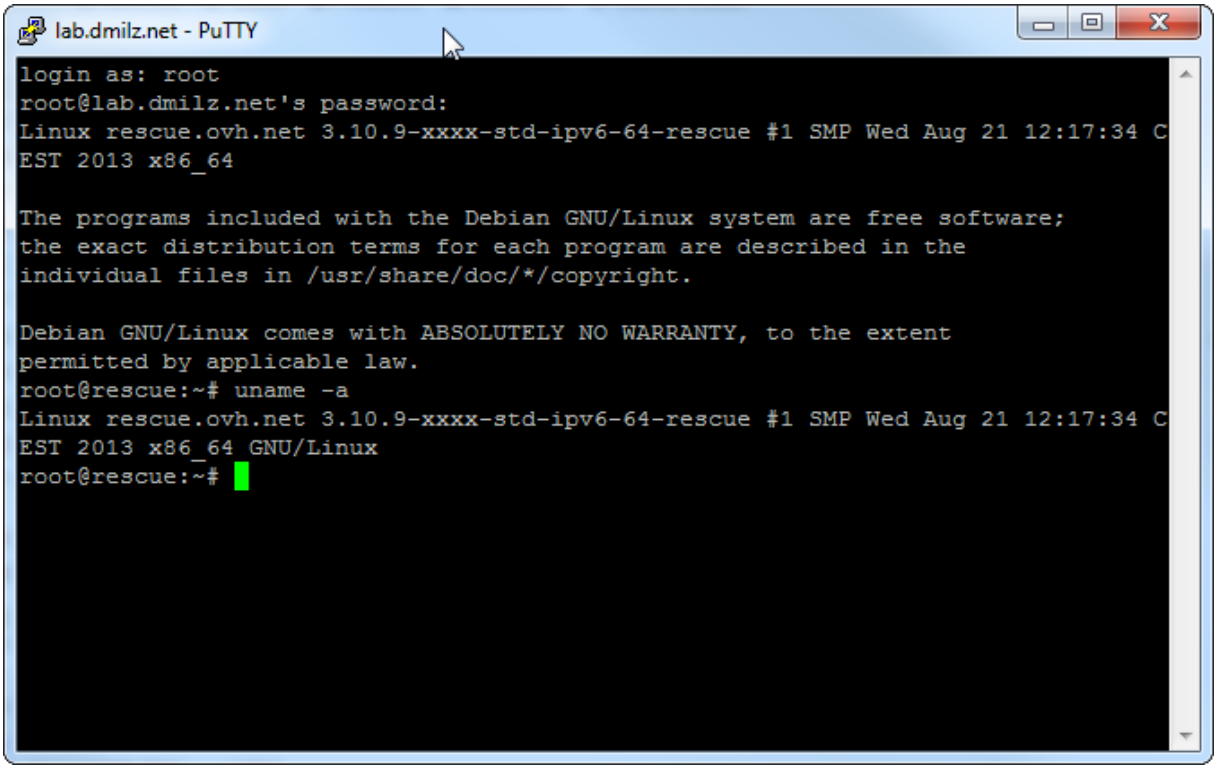


Puis un mail est envoyé à l'adresse indiquée :

De Support OVH <noreply@kimsufi.com>
Sujet **[ns369849.ip-91-121-195.eu] Paramètres d'accès au mode RESCUE**

```
SAS OVH - http://www.kimsufi.com
2 rue Kellermann
BP 80157
59100 Roubaix


Bonjour,

Votre serveur a redémarré en mode 'Rescue' ; cela signifie qu'un
Linux/BSD est lancé sur votre serveur via le réseau. Il ne s'agit pas
du système qui est normalement installé sur votre serveur, aucune
de vos partitions n'est d'ailleurs montée.

Une interface web est disponible pour vous permettre d'effectuer un
diagnostique de votre serveur (disque dur, raid, ram, CPU) et de
parcourir l'arborescence de votre système de fichiers:
  http://91.121.195.208:81
  - nom d'utilisateur : root
  - mot de passe : sn0mIm7y

Vous pouvez également vous connecter en SSH à votre serveur (91.121.195.208)
avec les paramètres suivants:
  - user : root
  - mot de passe : sn0mIm7y
```

Nous pouvons maintenant nous connecter avec SSH :



Lister les partitions :

```
root@rescue:~# fdisk -l /dev/sda

Disk /dev/sda: 1000.2 GB, 1000204886016 bytes
255 heads, 63 sectors/track, 121601 cylinders, total 1953525168 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0x000b783a

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1            8192     1843199      917504    5  Extended
/dev/sda2         1843200    10229759     4193280    6  FAT16
/dev/sda3        10229760  1953525167   971647704   fb  VMware VMFS
/dev/sda4   *       32        8191        4080    4  FAT16 <32M
/dev/sda5            8224     520191      255984    6  FAT16
/dev/sda6          520224    1032191      255984    6  FAT16
/dev/sda7         1032224    1257471      112624   fc  VMware VMKCORE
/dev/sda8         1257504    1843199      292848    6  FAT16

Partition table entries are not in disk order
```

Monter la partition /dev/sda5 :

```
root@rescue:~# cd /mnt
root@rescue:/mnt# mkdir sda5
root@rescue:/mnt# mount /dev/sda5 /mnt/sda5
root@rescue:/mnt# cd sda5
```

Le but du jeu est de modifier le fichier « esx.conf » qui se trouve dans « /etc/vmware/ », lui-même dans « local.tgz », lui-même dans « state.tgz » :

```
root@rescue:/mnt/sda5# cd /tmp
root@rescue:/tmp# tar xzf state.tgz
root@rescue:/tmp# tar xzf local.tgz
root@rescue:/tmp# cd etc
root@rescue:/tmp/etc# find . -name esx.conf
```

./vmware/esx.conf

Dans mon cas, avant de tout casser j'ai uniquement configuré l'IPv6, et enfin décoché IPv4 (qui a eu pour conséquence de me déconnecter du client bien sûr… Il faut donc éditer le fichier « esx.conf » et modifier les lignes suivantes pour repasser en IPv4 :

/adv/Misc/HostIPAddr = "0.0.0.0" (première ligne)
- ➔ /adv/Misc/HostIPAddr = " 91.121.64.225"

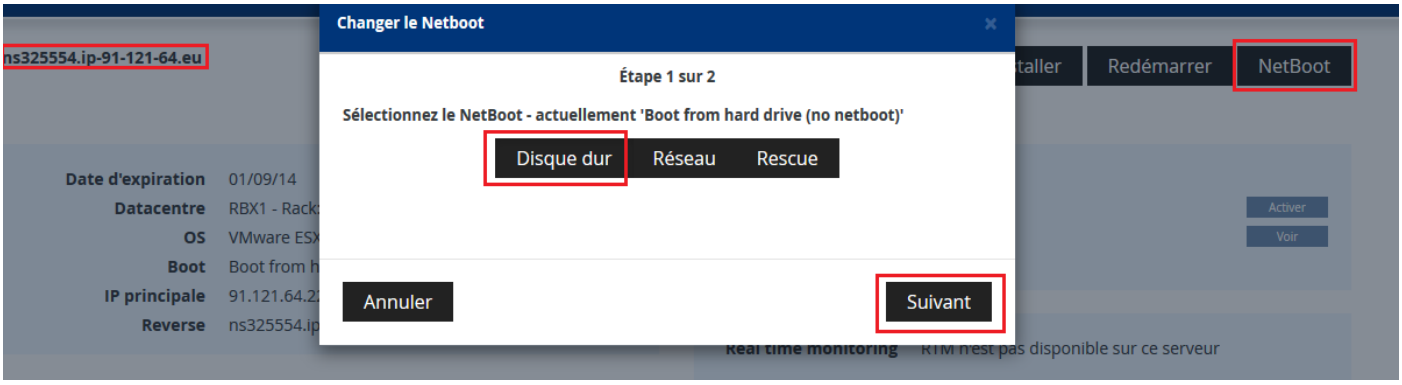
/adv/Net/ManagementAddr = " 2001:41d0:1:73e1::1" (ligne 3 sous /adv/Misc/HostName = "ks3265748.kimsufi.com" et avant /adv/Net/ManagementIface = "vmk0")
- ➔ /adv/Net/ManagementAddr = " 91.121.64.225"

Rajouter les lignes suivantes (après /net/vmkernelnic/child[0000]/enable = "true" et avant /net/vmkernelnic/child[0000]/ipv6network/child[0000]/ipv6address = "2001:41d0:1:73e1::1" ou /net/vmkernelnic/child[0000]/mac = " 2001:41d0:1:73e1::1" pour ceux qui n'ont pas configuré IPv6) :
- ➔ /net/vmkernelnic/child[0000]/ipv4address = " 91.121.64.225"
- ➔ /net/vmkernelnic/child[0000]/ipv4broadcast = " 91.121.64.255"
- ➔ /net/vmkernelnic/child[0000]/ipv4netmask = "255.255.255.0"

Il reste plus qu'à compresser et remplacer le fichier sur le vrai disque :

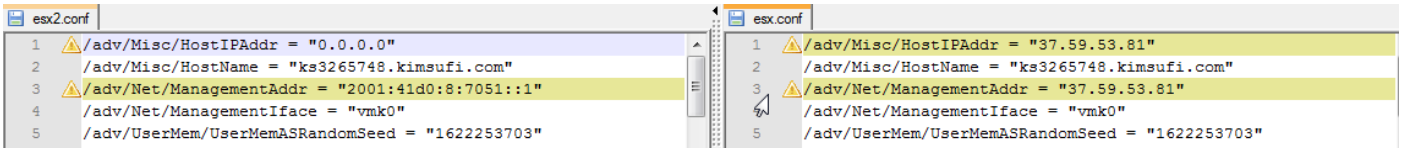
```
root@rescue:/tmp# tar czf local.tgz etc/
root@rescue:/tmp# tar czf state.tgz local.tgz
root@rescue:/tmp# cp state.tgz /mnt/sda5/
root@rescue:/tmp# umount /dev/sda5
```

Nous n'avons plus qu'à changer le netboot depuis le manageur Kimsufi :



Après redémarrage et avec un peu de chance le serveur devrait être accessible en IPv4. Bien sûr tout dépendra du problème recontré.

Je vous conseille donc de sauvegarder régulièrement esx.conf pour utiliser l'excellent plugin « compare » de Notepad++ :



Il sera beaucoup plus facile de corriger les erreurs.