Pierre-Luc Delisle
Pour Tahar Mokhtari
Dans le cours *Implanter un réseau*
2 Avril 2014

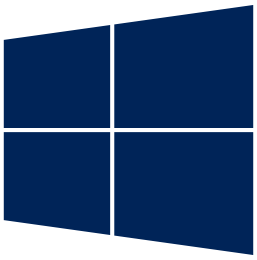
Rapport - Projet 1

Implanter un réseau

© Pierre-Luc Delisle et Guillaume Nadeau

“We've seen virtualization go mainstream over the last couple of years. But there are still a ton of companies out there that haven't tried it. We're focused on changing that landscape. We want to bring virtualization to every user.”

-Dan Chu, Senior Director of product, VMware



© Pierre-Luc Delisle et Guillaume Nadeau

Présentation du projet

Dans le cadre du cours de fin d'études collégiales intitulé *Implanter un réseau*, nous avions pour premier projet la conception d'un réseau.

Parmi les objectifs du projet, nous avions à comparer les différents types de *RAID.* Nous avons comparé les performances de quelques niveaux de cette technologie largement utilisée dans les serveurs.

Au niveau logiciel, nous avions à configurer un serveur web et FTP sous Windows Server 2008 R2. Ce système d'exploitation étant âgé de six ans, nous avons plutôt opté pour la modernité et nous avons réalisé le projet sous la dernière mouture du système d'exploitation serveur de Microsoft, Windows Server 2012 R2. Une connexion à distance au serveur devait naturellement être configurée pour administrer celui-ci. L'installation d'une application de virtualisation était également de mise.

Un pare-feu pour effectuer un filtrage de sites web distants devait également être configuré.

Finalement, une connexion *VPN* entre deux réseaux distants devait être configurée sur des routeurs de type *consumer grade*.

Modifications apportées au projet

Ce projet, avouons-le, est d'une simplicité démesurée pour un travail figurant dans un cours de dernière session.

Devant la facilité de ce projet, nous voulions ajouter quelques éléments que nous retrouvons couramment dans l'industrie et qui feraient en sorte que ce projet puisse être implanté dans un environnement de production. De ce fait, nous ferions de ce projet un travail beaucoup plus réaliste.

Par conséquent, nous avons implanté la virtualisation au coeur de notre projet. Au lieu d'implanter un serveur physique, nous avons ségrégué les services dans des machines virtuelles au sein d'un serveur de virtualisation.

Au niveau du pare-feu, le projet proposait d'installer «FirewallBuilder» sur une distribution de Linux. Nous avons plutôt opté pour une solution de loin plus efficace, performante et beaucoup moins longue à implanter, soit «pfSense».

Ceci conclut les modifications majeures apportées au projet.

Tâches réalisées

Cette section couvre les tâches réalisées dans le cadre du projet.

RAID - *Redundant Array of Independent Disks*

La technologie RAID fait partie des technologies de stockage les plus utilisées au monde. Elle permet une chose capitale : la redondance de disques et la sécurité des données.

En effet, le stockage est probablement le domaine de l'informatique qui est le plus à risque. Personne, et encore moins une entreprise ne souhaite voir disparaître ses données en raison d'une défaillance physique du matériel. Or, le disque dur étant la seule pièce mécanique d'un ordinateur avec ses têtes de lecture/écriture et ses plateaux en rotation constante, il n'est pas rare qu'un disque dur présente des signes de défaillances ou arrête subitement de fonctionner en raison d'un bris mécanique interne après quelques années d'utilisation 24/7. Lorsqu'un disque dur brise mécaniquement, il entraîne malheureusement avec lui les données qu'il contenait.

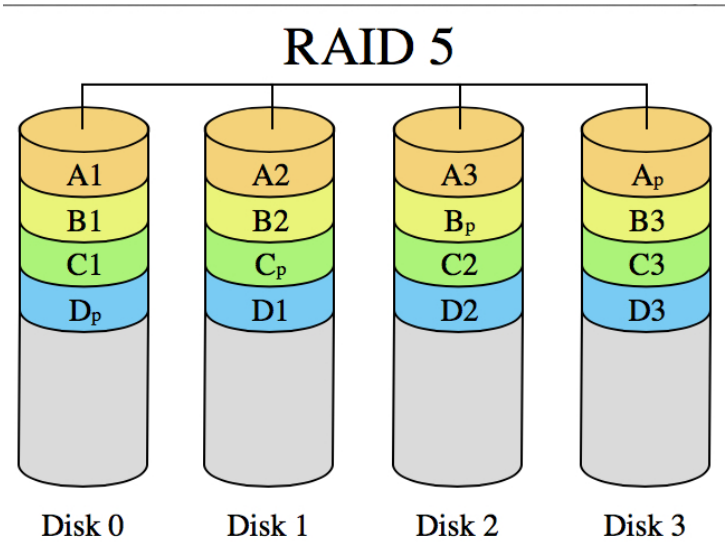
C'est ici que le RAID vient à la rescousse des données en faisant de la redondance. Les disques durs sont regroupés sous forme de batteries (*array*). Il existe plusieurs niveaux de RAID et chacun offre un certain niveau de sécurité. Voici une liste des principaux types de RAID :

- **RAID 0** : « *block-level stripping without parity or mirroring* ». Niveau de RAID qui ne dispose d'aucune redondance ou tolérance de faute, mais améliore les performances avec un parallélisme entre les disques durs lors des opérations d'écriture et de lecture. Un bris d'un disque dans la batterie RAID entraîne la perte de toutes les données.

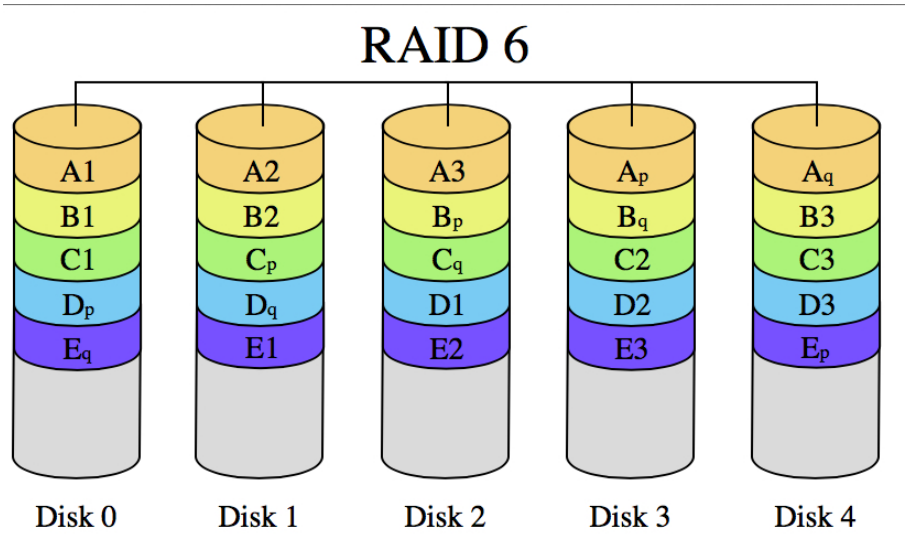
- **RAID 1** : « *block-level mirroring without parity or stripping* ». Les données sont écrites de manière systématique et identique sur tous les disques durs de la batterie. Il offre un niveau de protection de *n-1* disque(s). Lors d'un bris de disque dur, les données sont toujours accessibles tant et aussi longtemps qu'un disque de la batterie fonctionne.

- **RAID 5** : « *block-level stripping with distributed parity* ». Tout comme le RAID 0, les données sont divisées à travers tous les disques de la batterie, entraînant de ce fait des améliorations en terme de performances. Le RAID 5 est pourvu d'une redondance distribuée à travers tous les disques de la batterie. Il procure une tolérance de faute d'un disque dur. Si deux disques brisent en même temps, les données de la batterie sont

perdues puisque le contrôleur ne peut plus calculer la parité manquante. La batterie doit contenir un minimum de trois disques.



- **RAID 6** : *Block-level stripping with double distributed parity.* Tout comme le RAID 5, le RAID 6 procure un parallélisme au travers des disques durs de la batterie RAID, mais effectue une double parité sur deux disques durs en même temps. Cela lui procure donc une tolérance de panne de deux disques durs avant de perdre toutes les données de la batterie. La batterie doit contenir un minimum de 4 disques.



Il existe également des combinaisons de ces niveaux de RAID, notamment le RAID 10 ou encore le RAID 0+1.

Généralement, le RAID est contrôlé par un contrôleur physique, communément appelé “carte RAID”. Parmi les meilleurs du marché, on note Intel, LSI et Areca. Ces cartes ont toute la logique nécessaire pour contrôler des dizaines, voir centaines de disques durs. Malheureusement, ces cartes sont coûteuses, mais également très performantes.

Cette solution représente toutefois un certain désavantage. Si elle décharge le processeur *host* principal de la charge de calcul pour les opérations I/O et de calcul de parité, les disques durs sont totalement dépendants de ce contrôleur. Si ce dernier cesse de fonctionner pour quelconque raison, il faut retrouver un contrôleur identique ou qui partage les mêmes propriétés physiques (même contrôleur embarqué) pour récupérer les données sur la batterie RAID. De plus, une batterie doit être ajoutée à la carte. En effet, ces dernières sont très souvent pourvues d’une mémoire vive DDR2/3 à des fins de « caching » d’opérations I/O et de « caching » de données. En cas de coupure de courant, la mémoire vive ne retient pas les données. Cela peut très vite entraîner la perte de données ainsi qu’une défaillance au niveau de l’intégrité de la batterie RAID, mettant en péril non pas seulement les données stockées temporairement dans la mémoire vive, mais également celles de toute la batterie. Ces batteries entraînent un coût de maintenance supplémentaire.

Pour pallier à ces problèmes, il existe le RAID logiciel, de plus en plus en vogue. Le RAID logiciel intervient au niveau du système d’exploitation. Sur Windows, le tout est géré par la console de gestion de l’ordinateur (*Windows Computer Management Console*), alors que l’utilitaire *mdadm* (*Multiple Device Administration*) existe sur Linux. Le RAID logiciel a tendance à être beaucoup plus flexible. En effet, la batterie RAID n’est pas dépendante du contrôleur puisque le RAID est géré par le système d’exploitation. On peut donc “déplacer” la batterie RAID dans une autre machine et remonter la batterie de manière totalement logicielle et avoir accès aux données en un temps record. Le RAID logiciel permet également de limiter les coûts par rapport au RAID matériel en écartant l’achat d’un contrôleur dispendieux.

Toutefois, bien que plus flexible, le RAID logiciel a également ses lacunes. On ne peut, par exemple faire du *hot-swap* avec les disques durs, cette fonctionnalité étant réservée principalement aux contrôleurs physiques. Les performances sont également moindres que lorsqu’on acquiert un contrôleur dédié : c’est le processeur *host* qui calcul toutes les opérations nécessaires au stockage, en plus de celles des applications et kernel du système d’exploitation. Les performances varient donc selon l’usage. De ce fait, la reconstruction d’une batterie à l’état *degraded* est plus long sur un RAID logiciel que matériel.

Il y a toutefois une chose à retenir. Même si l'on parle de redondance et de tolérance de panne, le RAID ***n'est pas*** une solution de sauvegarde. Le RAID permet d'avoir une disponibilité des données (*uptime*) accrue en cas de panne matérielle, mais ce n'est pas un moyen de sauvegarde. Un moyen de sauvegarde est entièrement logiciel avec, la plupart du temps, un *versionning* des fichiers. *Apple Time Machine* ou *Windows Backup and Restore* sont des utilitaires de sauvegarde embarqués au sein du système d'exploitation. On peut également faire une sauvegarde périodique manuelle des fichiers importants vers un disque dur externe que l'on débranche par la suite, le rendant hors ligne. Le RAID ne permet pas de sauvegarder périodiquement vers un autre média de stockage. Le RAID ne protège pas contre l'effacement ou l'écrasement accidentel de données. C'est pourquoi il ne constitue pas une méthode de sauvegarde efficace.

Pour conclure la présentation du RAID :

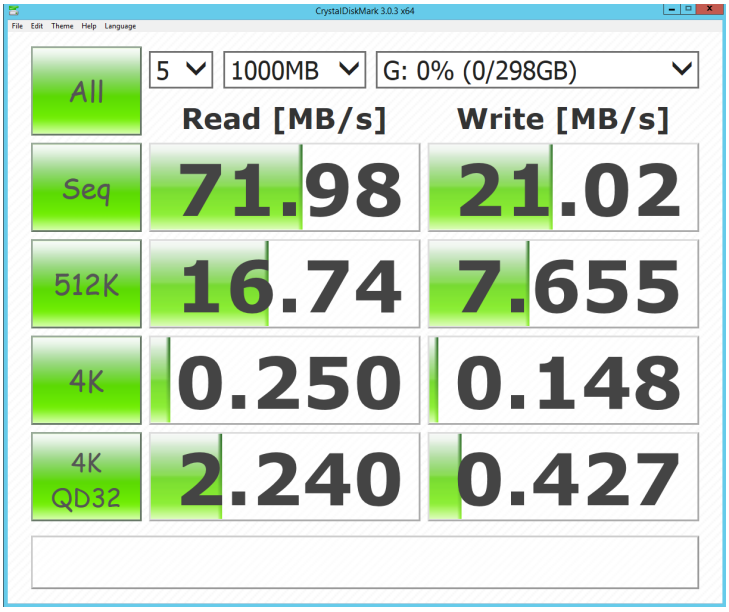
Type de RAID	Usage	Sauvegarde
RAID Logiciel	Solution à prix plus abordable Conçu pour un seul serveur / station de travail Parfait pour des petites entreprises ou pour une solution résidentielle Très flexible	N'est pas un moyen efficace de sauvegarder des données.
RAID Matériel	*Mission Critical Usage* Usages haute performance Demande beaucoup de IOPS (par exemple, une basse de données) Solution à grande échelles, plusieurs serveurs, etc.	

Dans le cadre du projet, nous avions à comparer quatre types de RAID :

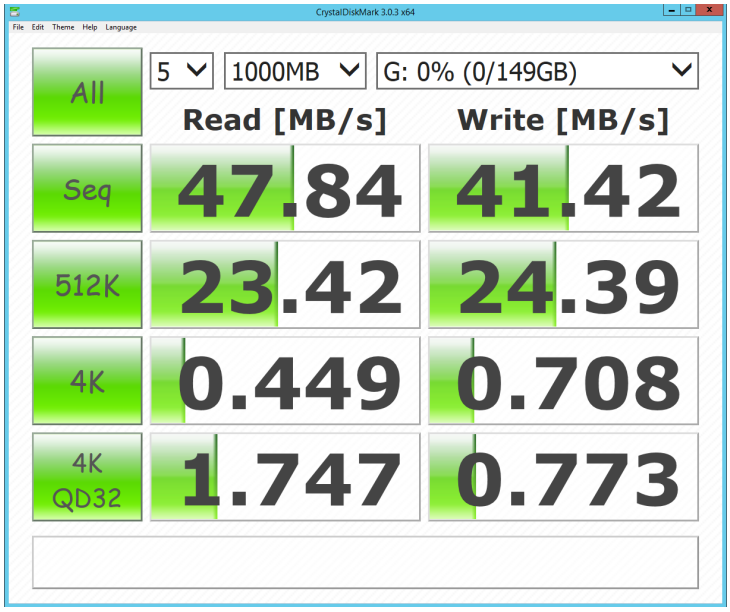
- RAID 0 matériel
- JBOD matériel
- RAID 1 logiciel
- RAID 5 logiciel

Notez que le projet ne permet pas de comparer directement chacun des types de RAID matériel par rapport à son homologue logiciel. De ce fait, le projet ne laisse place à aucune comparaison plausible et en bonne et due forme. En effet, chaque type de RAID comporte ses spécificités et apporte des performances différentes. Pour comparer un RAID logiciel avec un RAID matériel, il faut s'assurer que le type de RAID, par exemple le RAID 0, reste constant durant la comparaison entre le RAID logiciel et matériel. Si cette variable n'est pas constante, comme dans le cas du projet présenté, la comparaison est inutile. Nous nous contenterons alors d'afficher les résultats obtenus à l'aide d'un programme testant les performances disques, soit « CrystalDiskMark », et de faire une comparaison sommaire. Notez ici que nous n'avons eu le temps que de faire un test de type synthétique. Les performances mesurées ne tiennent comptent que d'un facteur, soit les performances en écriture et lecture. Une mesure du nombre d'IOPS n'a pas été demandée et, par conséquent, n'ont pas été mesurées, ni même les temps d'accès. Le test de performance ne reflète pas les performances réelles (pratiques) puisqu'aucun utilitaire de mesure de ce type n'a été employé.

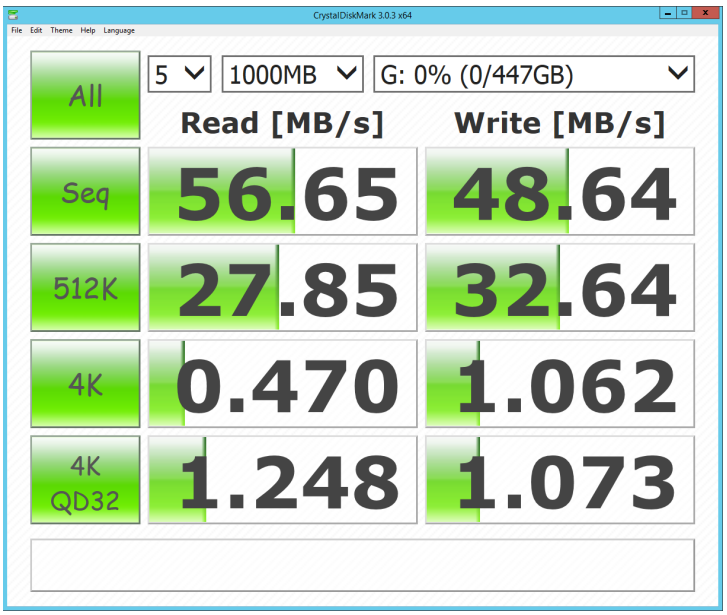
Voici les résultats :

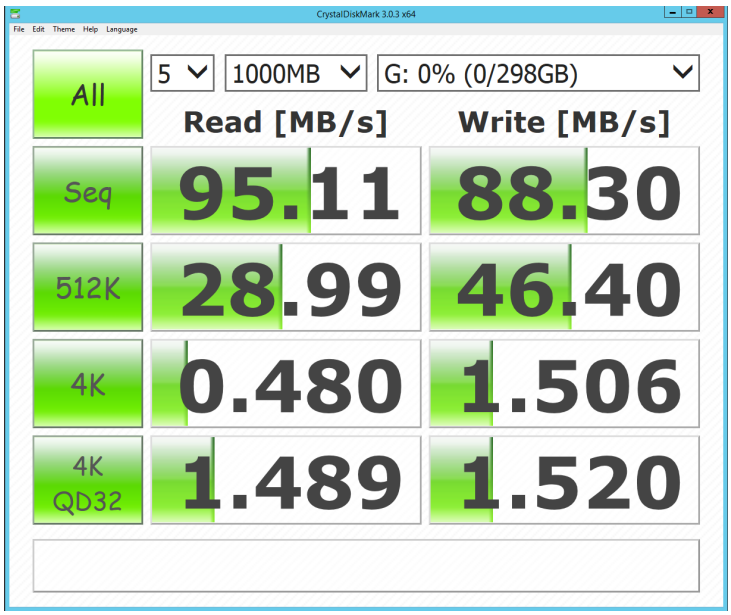


RAID 5 Logiciel



RAID 1 Logiciel





RAID JBOD Matériel

RAID 0 Matériel

Comme nous pouvons le remarquer sur les résultats de « CrystalDiskMark », le RAID 0 matériel est sans surprise le RAID offrant les meilleures performances dans pratiquement tous les formats de données confondus. Ce résultat est normal puisque le RAID 0 est, de par son fonctionnement, la solution RAID la plus rapide, mais également la moins sécuritaire.

Le RAID 5 suit le RAID 0 au niveau des performances séquentielles. Toutefois, le RAID 5 logiciel est une des pires solutions à implanter sur un système d'exploitation Windows Server. Le RAID 5 logiciel dispose, comme nous l'avons mentionné précédemment, d'une parité distribuée des données. Puisque logiciel, c'est le processeur qui doit acquitté de la charge de calcul requise pour calculer cette parité. C'est pour cette raison que le RAID 5 offre de piètres performances dans tous les formats de fichiers autres que séquentiels.

Le RAID 1 écope lui aussi de la surcharge qu'apporte une solution logiciel. Les résultats sont moins bons que ceux obtenus avec le RAID JBOD matériel. Le JBOD matériel reflète les performances d'un seul disque et le RAID 1 devrait, en théorie, s'en approcher.

© Pierre-Luc Delisle et Guillaume Nadeau

Installation d’un serveur FTP

« File Transfer Protocol » (protocole de transfert de fichiers), ou « FTP », est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers.

La variante de FTP protégée par les protocoles SSL ou TLS (SSL étant le prédécesseur de TLS) s'appelle FTPS. FTP sans cryptage est vulnérable et peu sécuritaire. Il ne devrait être utilisé que pour distribuer des données peu sensibles.

FTP obéit à un modèle client-serveur, c'est-à-dire qu'une des deux parties, le client, envoie des requêtes auxquelles réagit l'autre, appelé serveur. En pratique, le serveur est un ordinateur sur lequel fonctionne un logiciel lui-même appelé serveur FTP, qui rend publique une arborescence de fichiers similaire à un système de fichiers UNIX. Pour accéder à un serveur FTP, on utilise un logiciel client FTP (possédant une interface graphique ou en lignes de commandes).

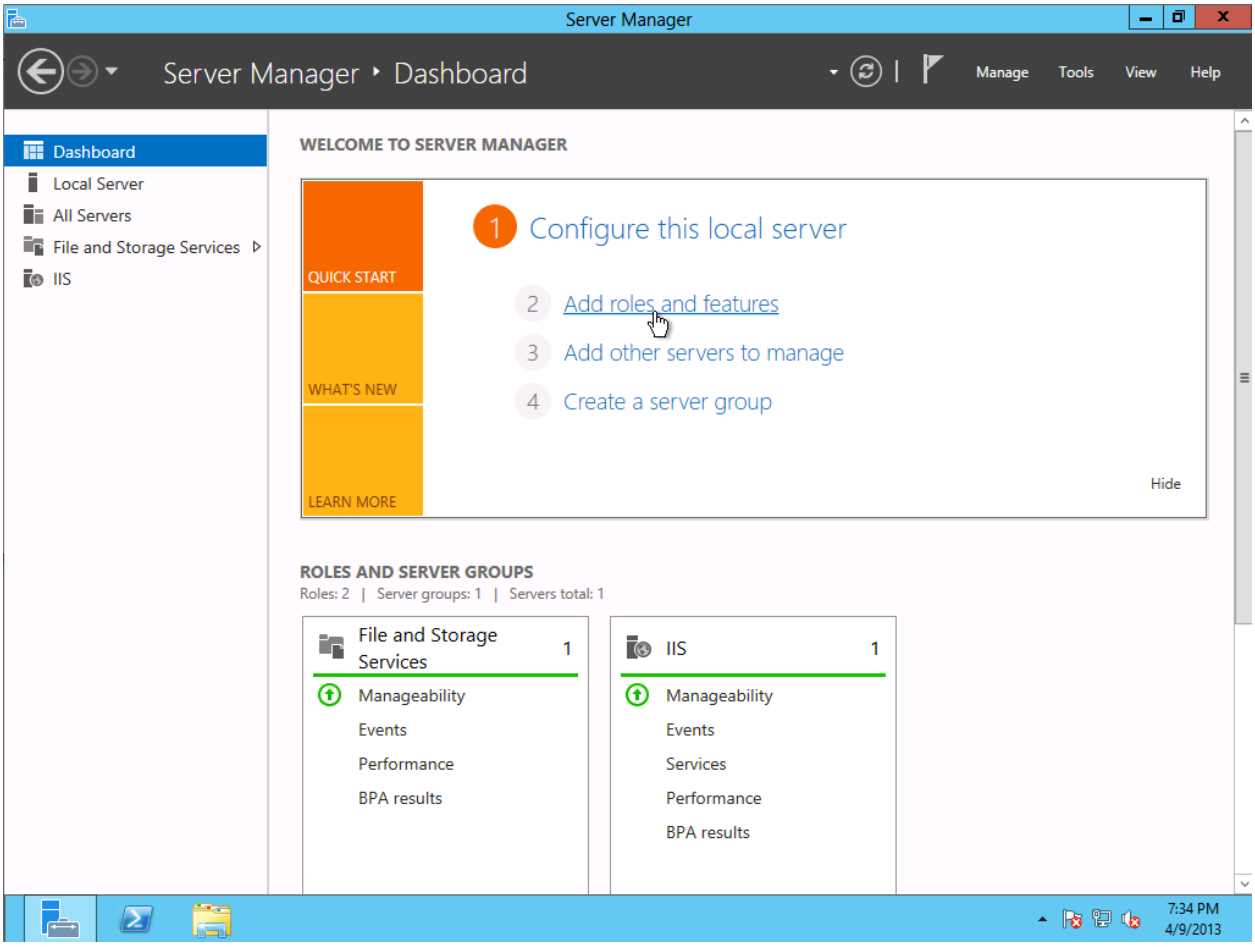
FTP, qui appartient à la couche application du modèle OSI et du modèle ARPA, utilise une connexion TCP.

Par convention, deux ports sont attribués pour les connexions FTP : le port 21 pour les commandes et le port 20 pour les données. Pour le FTPS dit implicite, le port conventionnel est le 990.

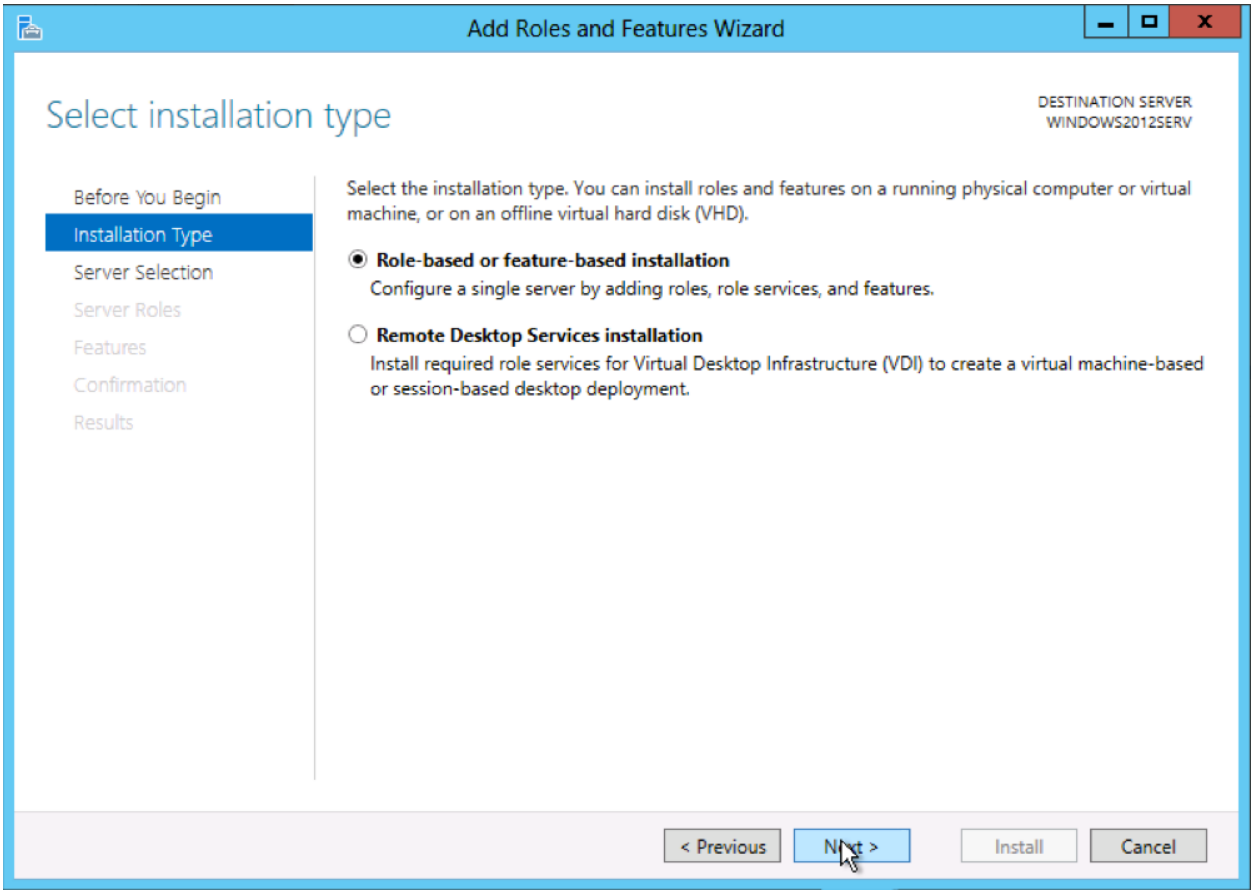
Ce protocole peut fonctionner avec IPv4 et IPv6.

Installation d'un serveur FTP - Guide étape par étape

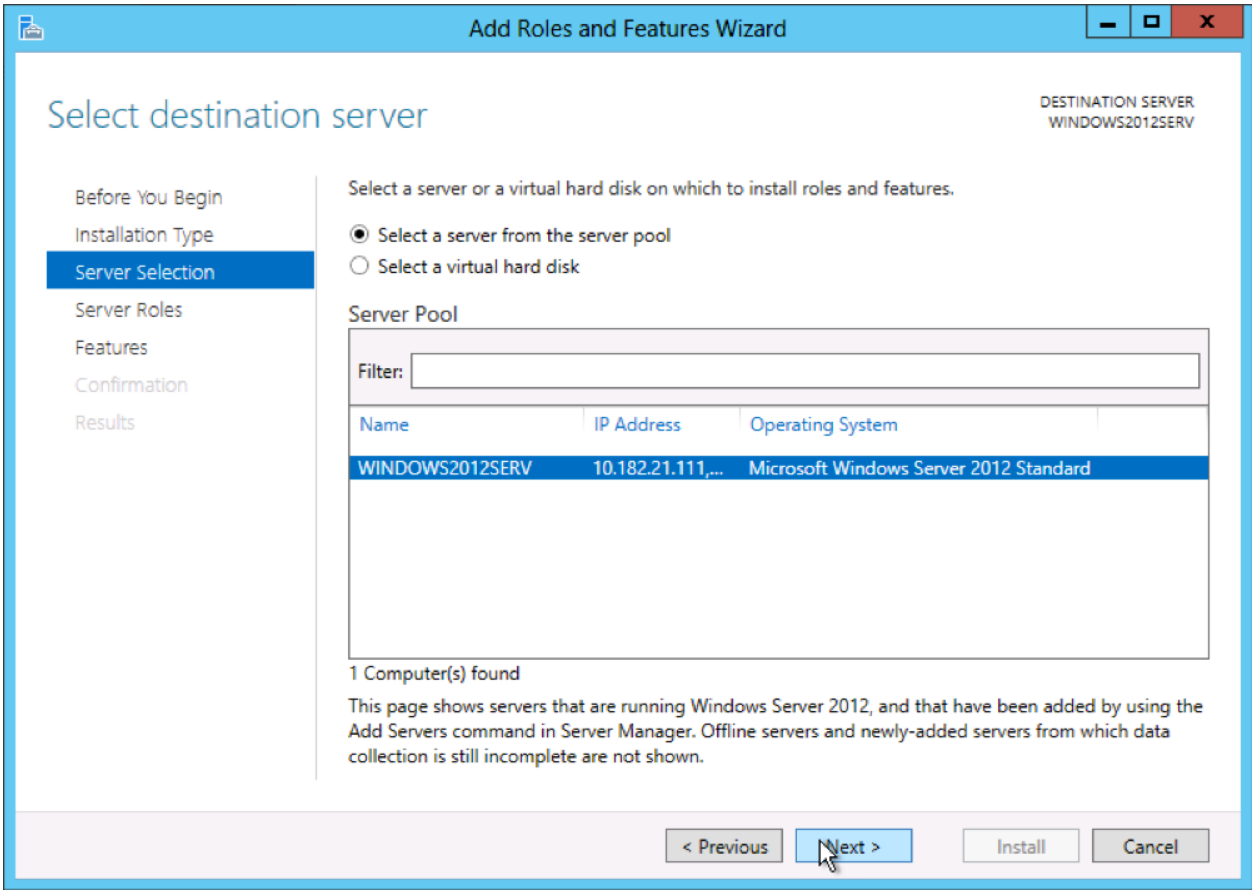
1. Ajoutez le rôle dans **Server Manager**.



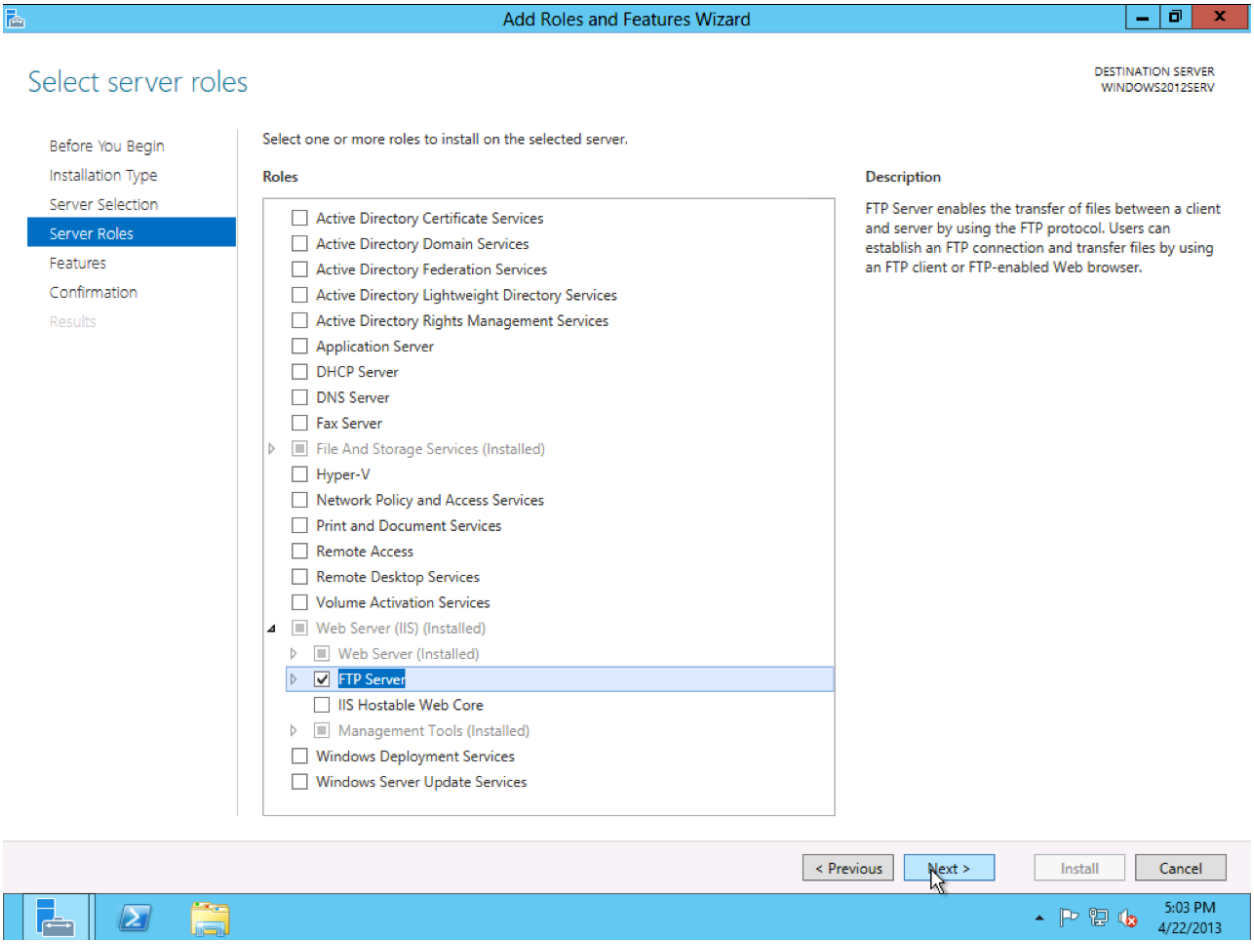
2. Sélectionnez **Role-based or feature-based installation** comme type d'installation et cliquez sur **Next**.



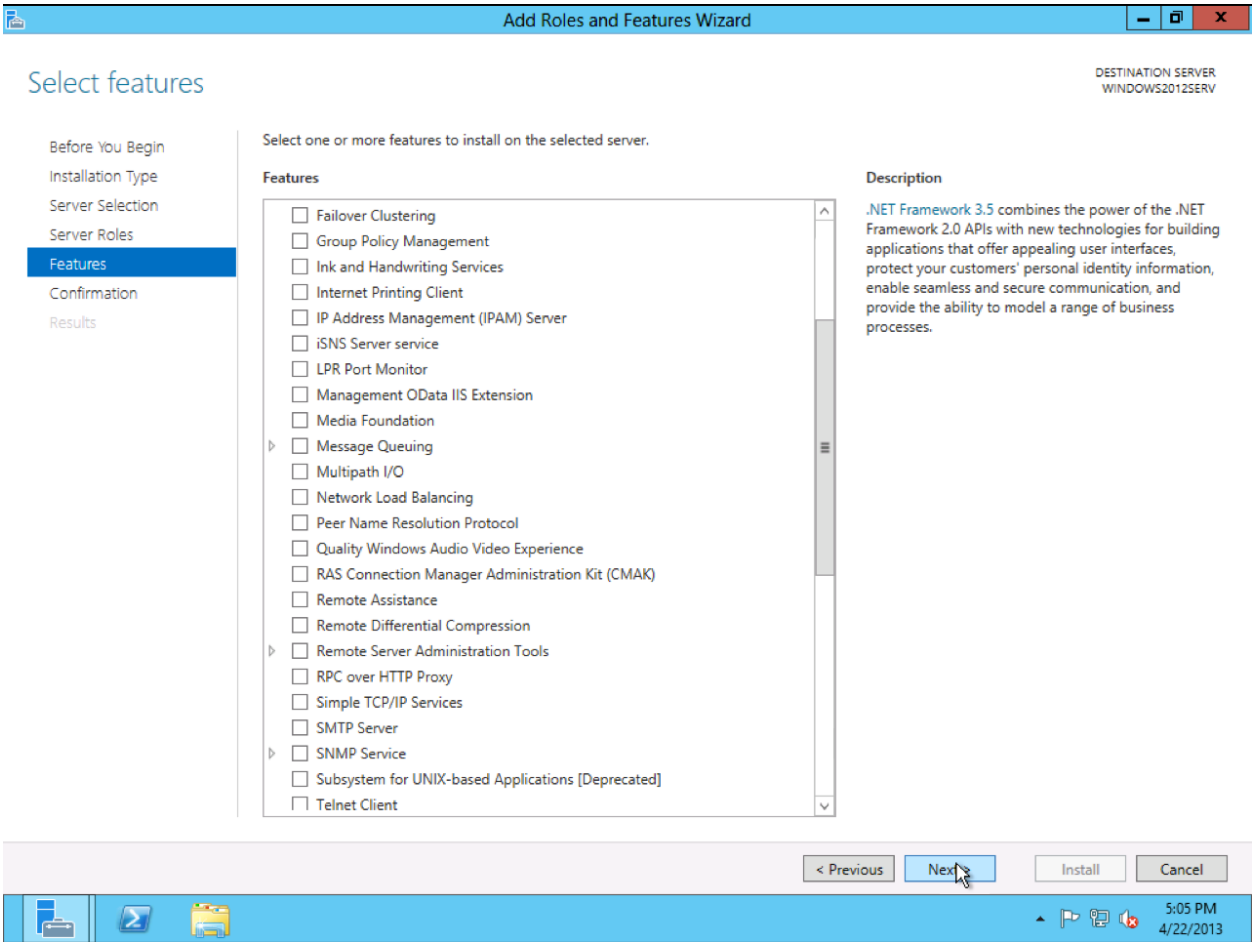
3. Le serveur courant sera sélectionné par défaut. Cliquez sur **Next** pour aller au menu de sélection des rôles.



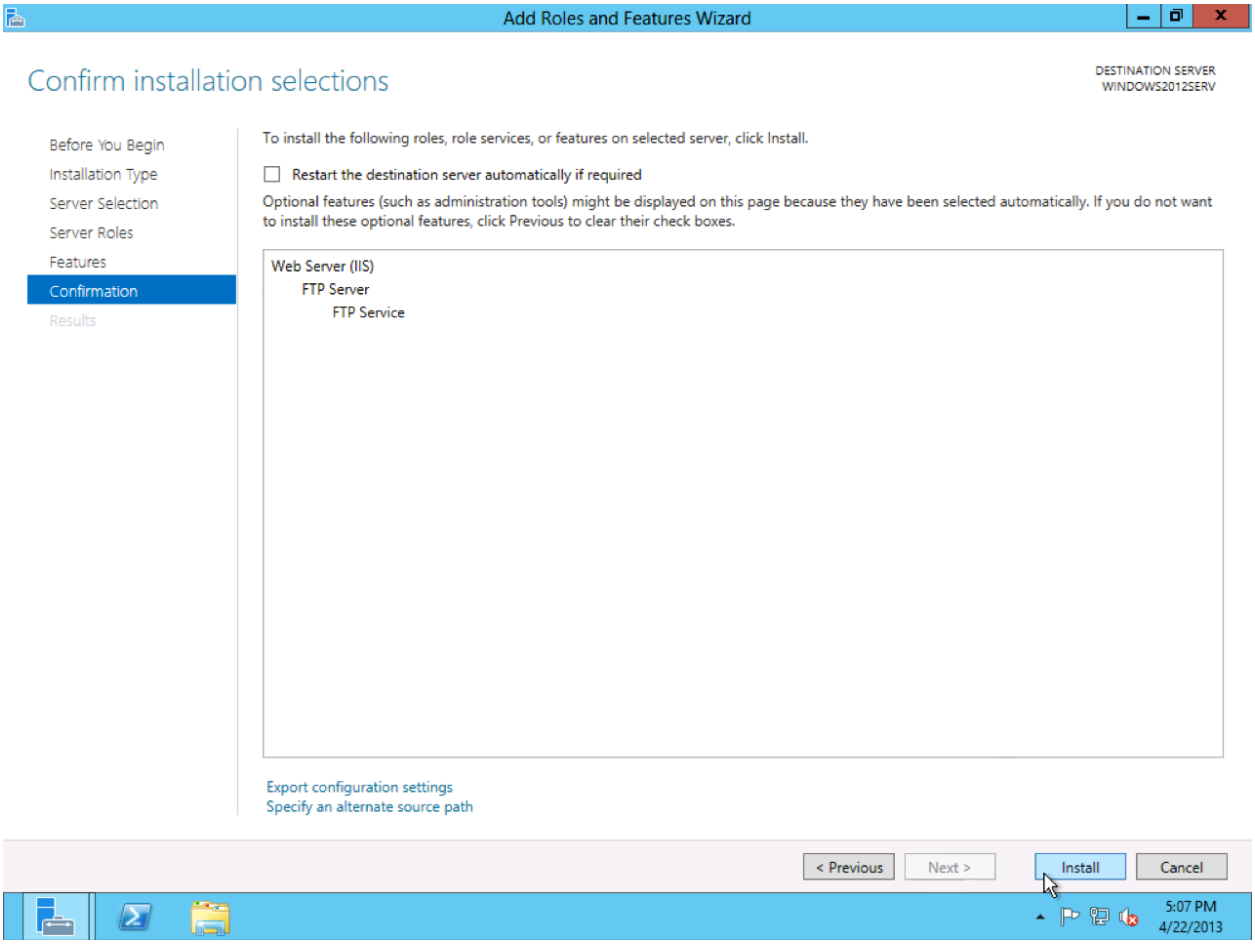
4. Sélectionnez l'option **Web Server (IIS)** puis faire dérouler le sous-menu. Sélectionnez la case **FTP Server**. Cliquez sur **Next** pour passer au menu de sélection des fonctionnalités.



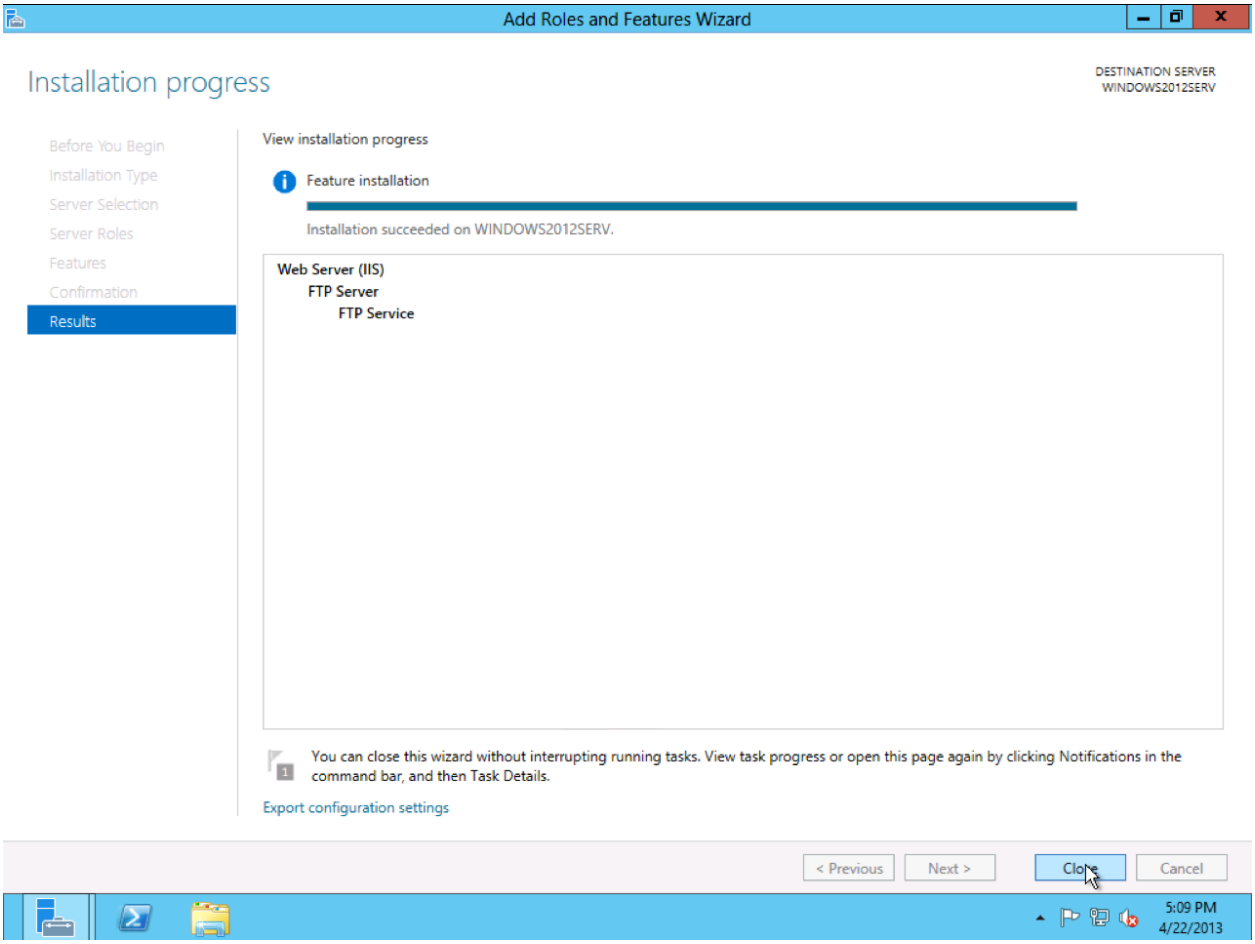
5. Sélectionnez toute autre fonctionnalité désirée pour le déploiement IIS et cliquer sur **Next.**



6. Lire le résumé de l'installation pour confirmer celle-ci en cliquant sur **Install**.

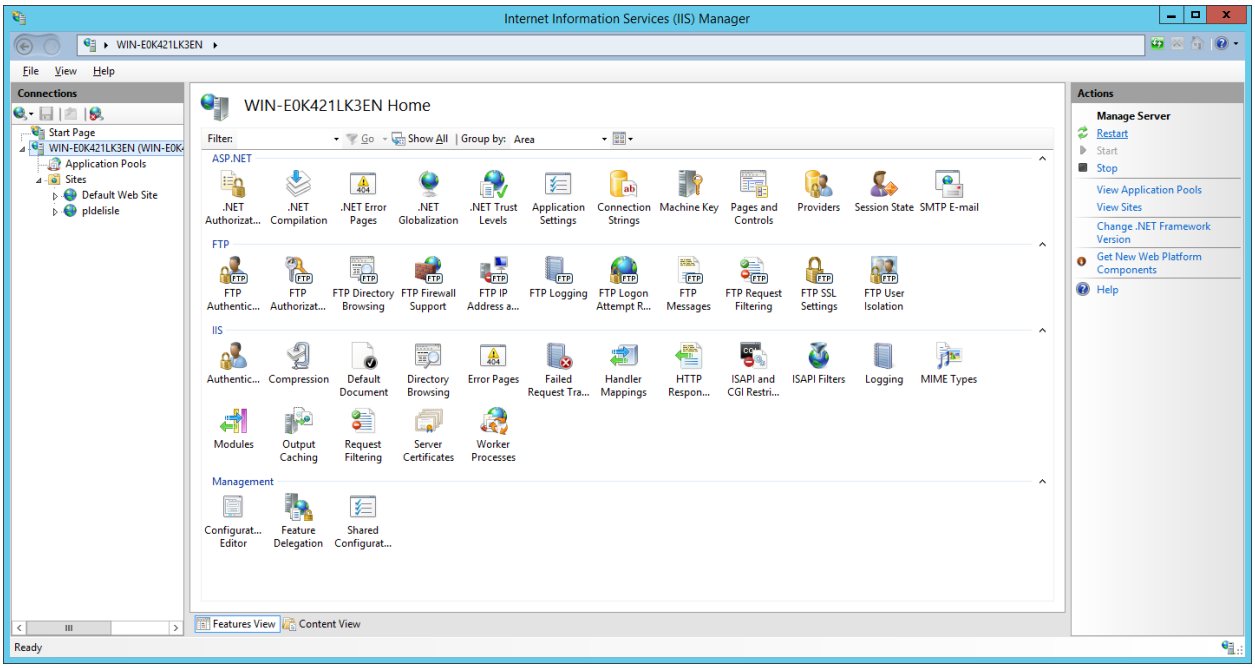


7. L'installation s'est bien déroulée lorsque ce message apparait.



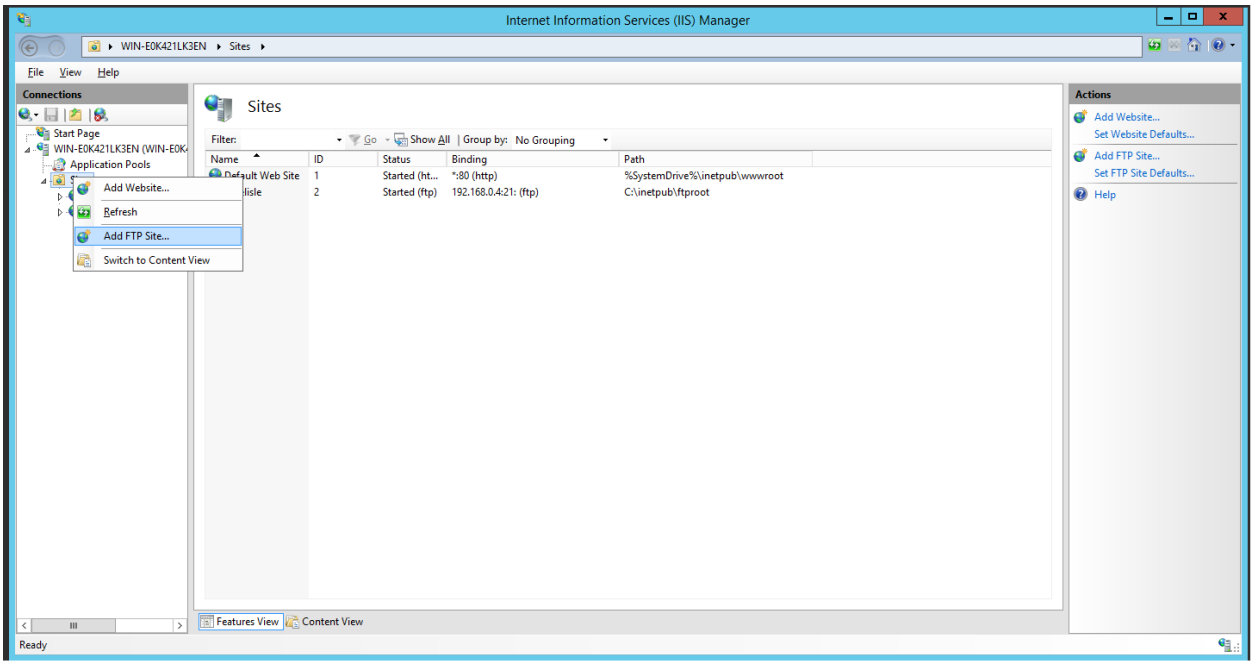
Création d'un site FTP

1. Ouvrir le **IIS Manager** situé dans la section **Administrative Tools** du menu Démarrer.



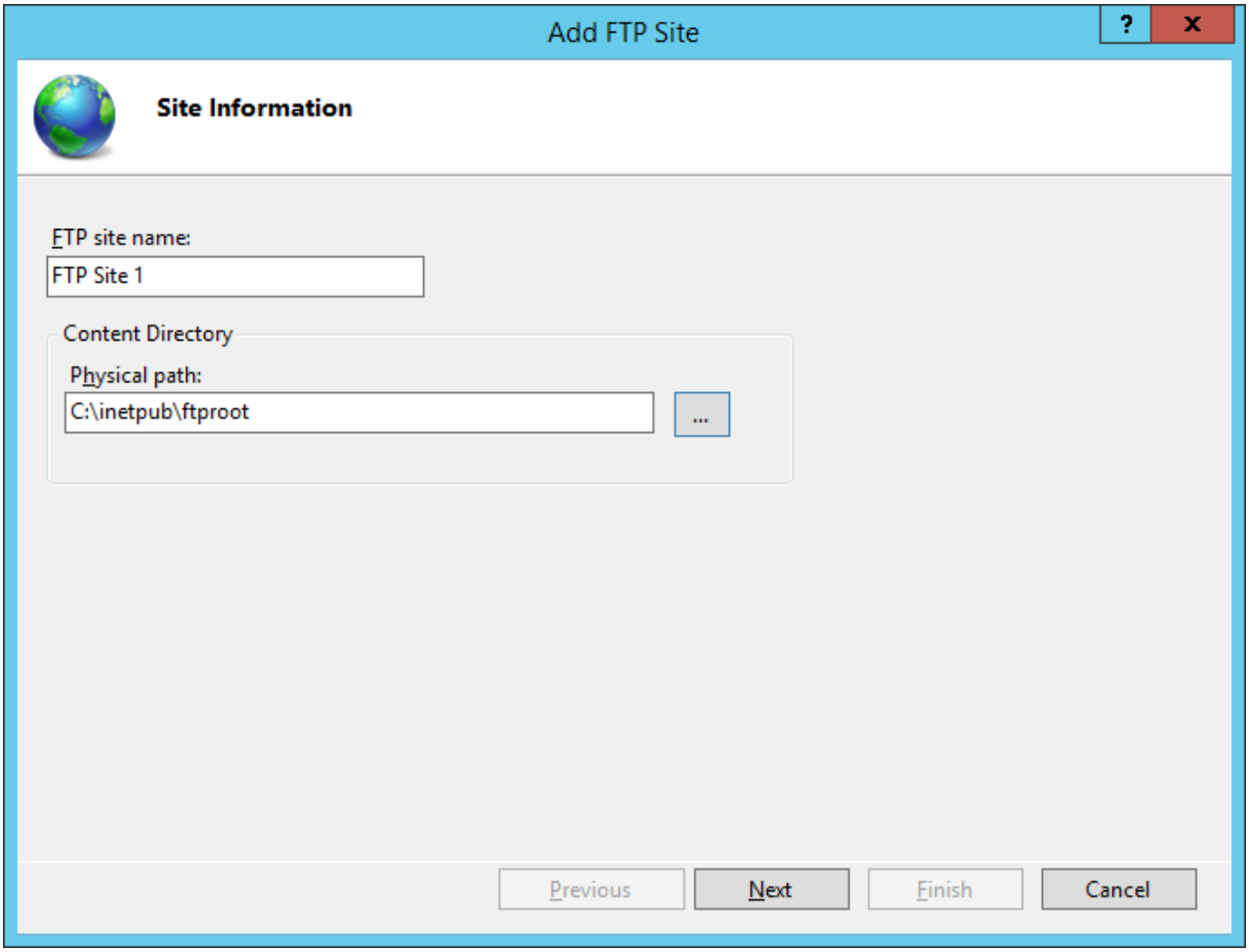
2. Dans le panneau **Connections**, ouvrir le « node » du serveur et cliquer sur **Site**.

3. Cliquez-droit sur **Site**, et cliquez **Add FTP Site** pour ouvrir l'assistant de configuration **Add FTP Site**.



4. Sur la page de **Site Information**, dans la boîte **FTP site name**, tapez le nom du site FTP.

5. Dans la boîte **Physical path**, tapez le répertoire racine du serveur FTP ou cliquez sur le bouton **Browse** pour localiser le répertoire.



6. Cliquez Next pour ouvrir la page Binding and SSL Settings.

7. Sous **Binding**, dans la liste **IP Address**, sélectionnez l'adresse IP du serveur.

8. Dans la boîte nommée **Port**, tapez le numéro de port du serveur FTP. Par défaut, un serveur FTP opère sur le port **21**.

9. Cochez la case **Start FTP site automatically** pour rendre automatique l'exécution du serveur FTP au démarrage du serveur.

10. Sous **SSL**, dans la liste des **SSL Certificates**, sélectionnez un certificat SSL si nécessaire.

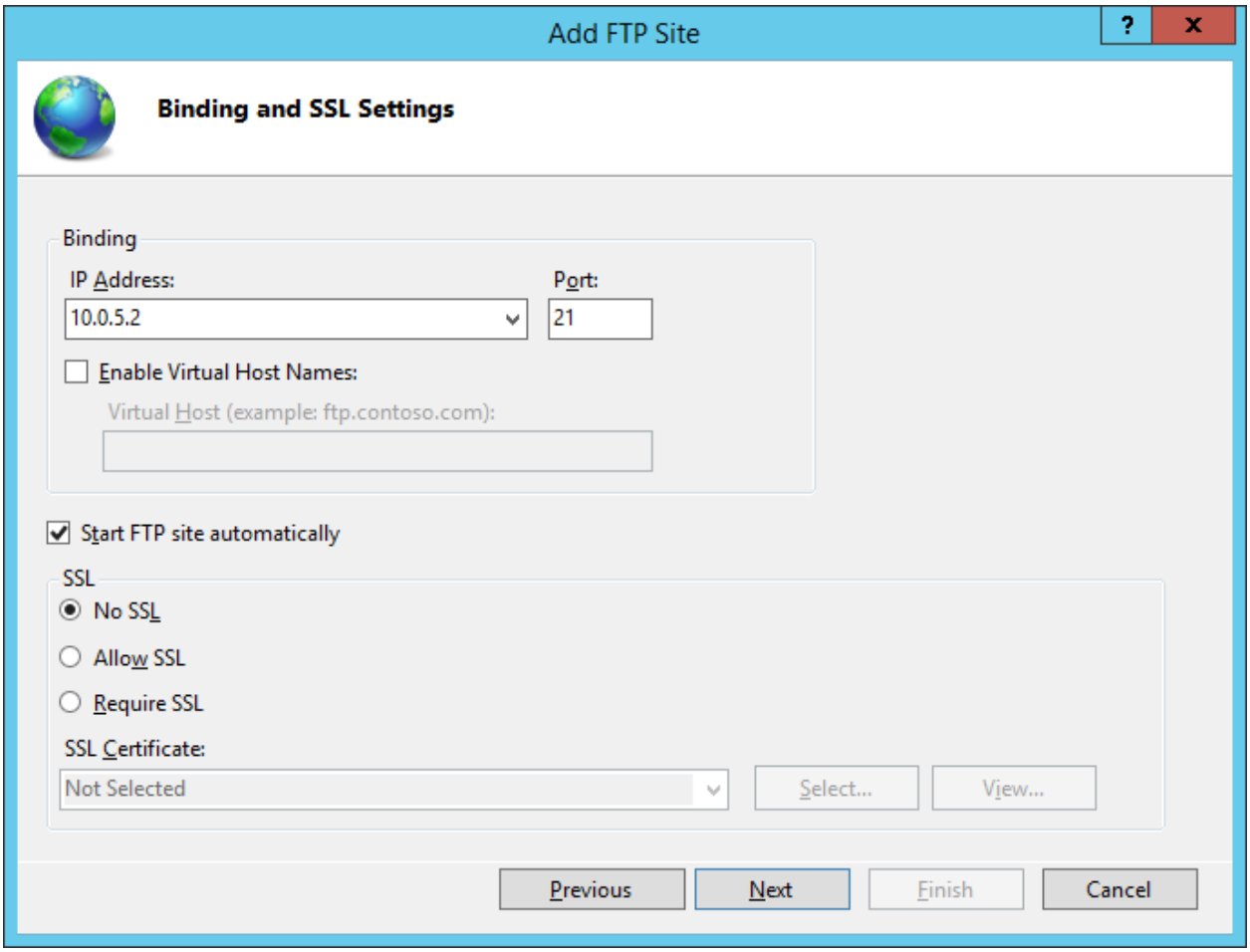
11. Sélectionnez une des options suivantes :

    - **Allow SSL**: Autorise le serveur FTP de supporter les connexions SSL et non-SSL avec un client.

    - **Require SSL**: Le cryptage SSL est requis entre le client et le serveur pour établir une communication.

    - **No SSL**: Aucun cryptage SSL n'est requis pour établir une communication entre le serveur et le client.

12. Cliquer sur Next pour ouvrir la page Authentication and Authorization Information.



13. Sous **Authentication**, sélectionnez la méthode d'authentification que l'administrateur souhaite utiliser :

    - **Anonymous**: Autorise tous les utilisateurs à se connecter au serveur et à avoir accès au contenu de celui-ci sous le nom de **anonymous** ou **ftp**.

    - **Basic**: Un nom d'utilisateur et mot de passe est requis pour pour que l'utilisateur puisse se connecter au serveur et ainsi avoir accès à son contenu. Une authentification de type **Basic** transmet les mots de passe sur le réseau sans le crypter. À utiliser seulement lorsque l'ont sait que la connexion entre le serveur et le client est sécurisée (SSL).

14. Sous **Authorization**, dans la liste **Allow access to**, sélectionnez une des options suivantes :

    - **All Users**: Tous les utilisateurs, autant ceux anonymes qu'identifiés, ont accès au contenu.

    - **Anonymous Users**: Les utilisateurs portant le nom **Anonymous** peuvent accéder au contenu du serveur.

    - **Specified Roles or User Groups**: Seuls les membres d'un certain rôle ou d'un certain groupe peuvent avoir accès au contenu du serveur FTP. Cocher la case **Role** ou **Group** le cas échéant.

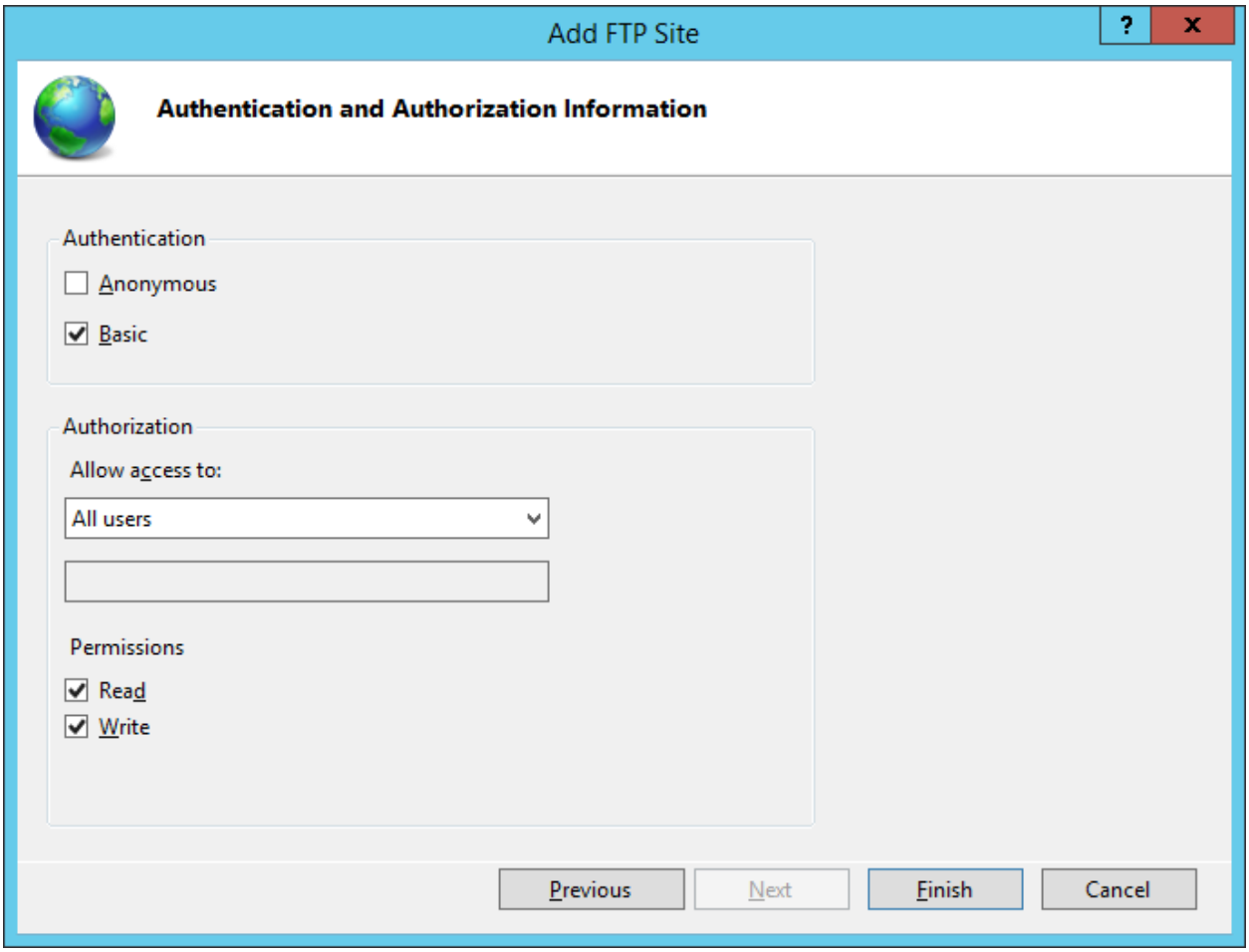
    - **Specified Users**: Seulement les utilisateurs mentionnés dans cette boîte pourront avoir accès au contenu du serveur FTP. Taper le nom de l'utilisateur dans la boîte.

15. Si une option de la liste **Allow access to** a été sélectionnée, sélectionnez une et/ou l'autre des permissions suivantes :

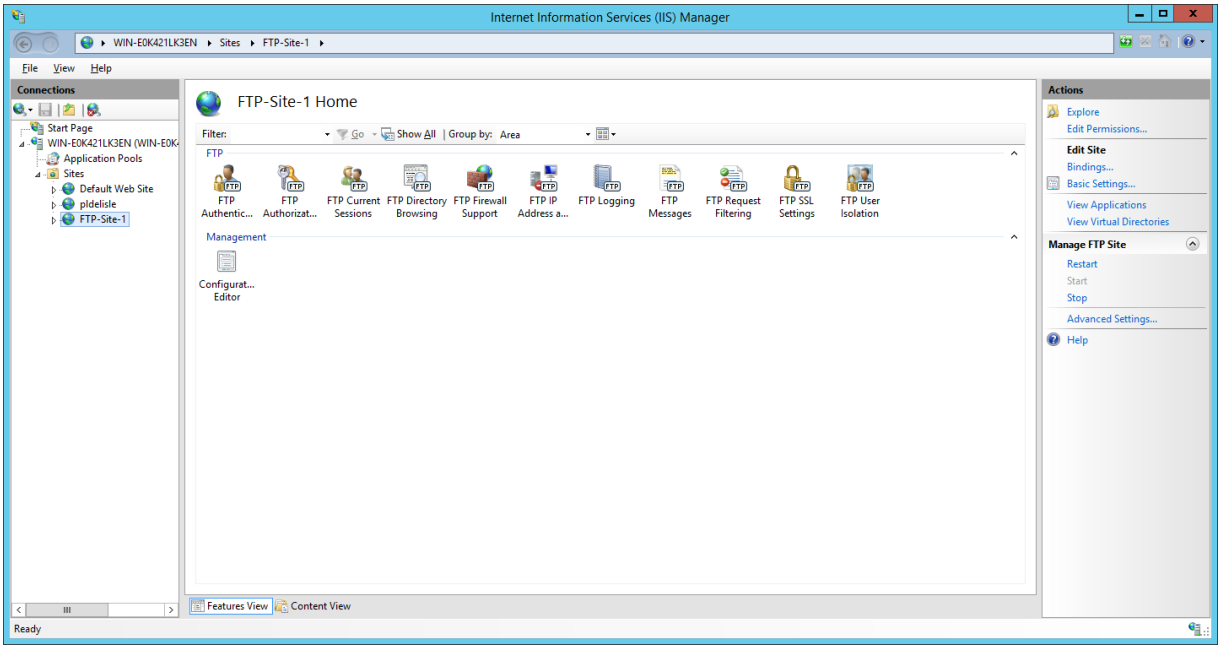
    - **Read**: Permet à l'utilisateur autorisé de lire du contenu du répertoire du serveur FTP.

    - **Write**: Permet à l'utilisateur autorisé d'écrire du contenu dans le répertoire du serveur FTP.

16. Cliquez sur **Finish.**



Le site FTP a été créé.



Installation d'un serveur web

La troisième tâche du projet consistait à créer un serveur web opérant sur le port HTTP 80 via le module IIS de Microsoft.

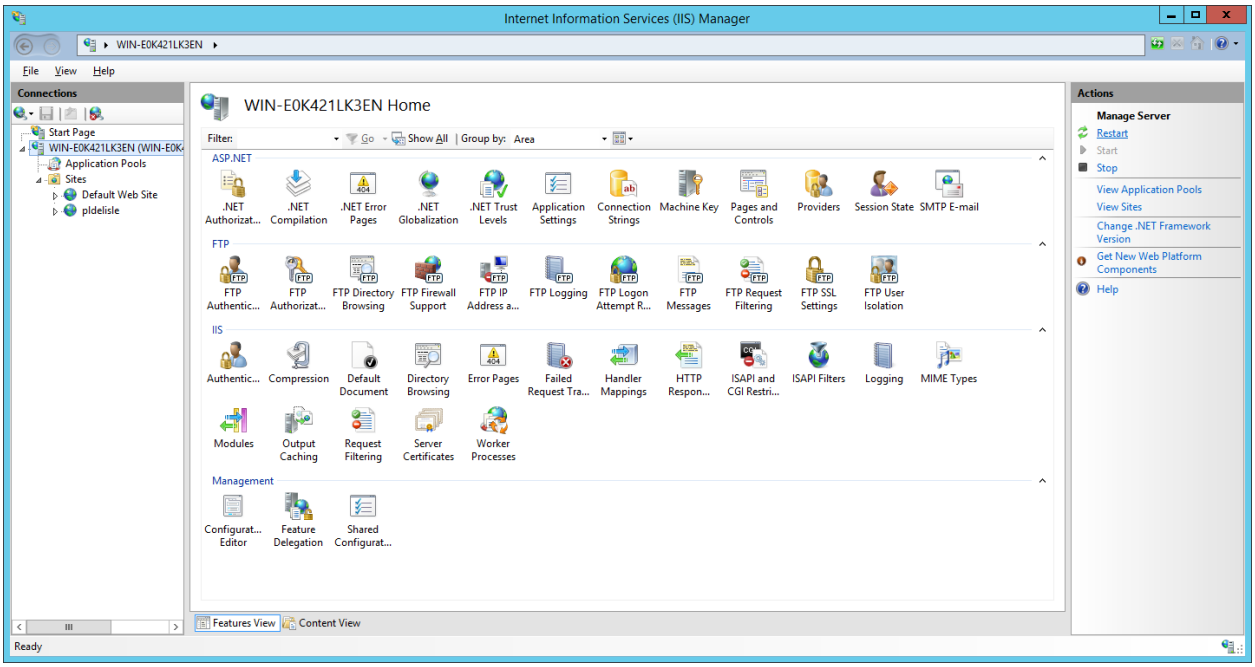
IIS, ou *Internet Information Services*, a été créé par Microsoft pour fournir des services web aux plateformes Windows NT dont il fait partie depuis la version 4.0. Il supporte les protocoles HTTP, HTTPS, FTP, FTPS, SMTP et NNTP.

Le service web que nous avons installé se base sur le protocole *Hypertext Transfer Protocol,* ou HTTP. Ce protocole opère sur le port 80. Il permet entre autres de faire afficher des pages web HTML dans un navigateur web tel que Apple Safari ou Mozilla Firefox. D'autres modules tels que PHP peuvent également être greffé à IIS.

Création d'un serveur web - Guide étape par étape

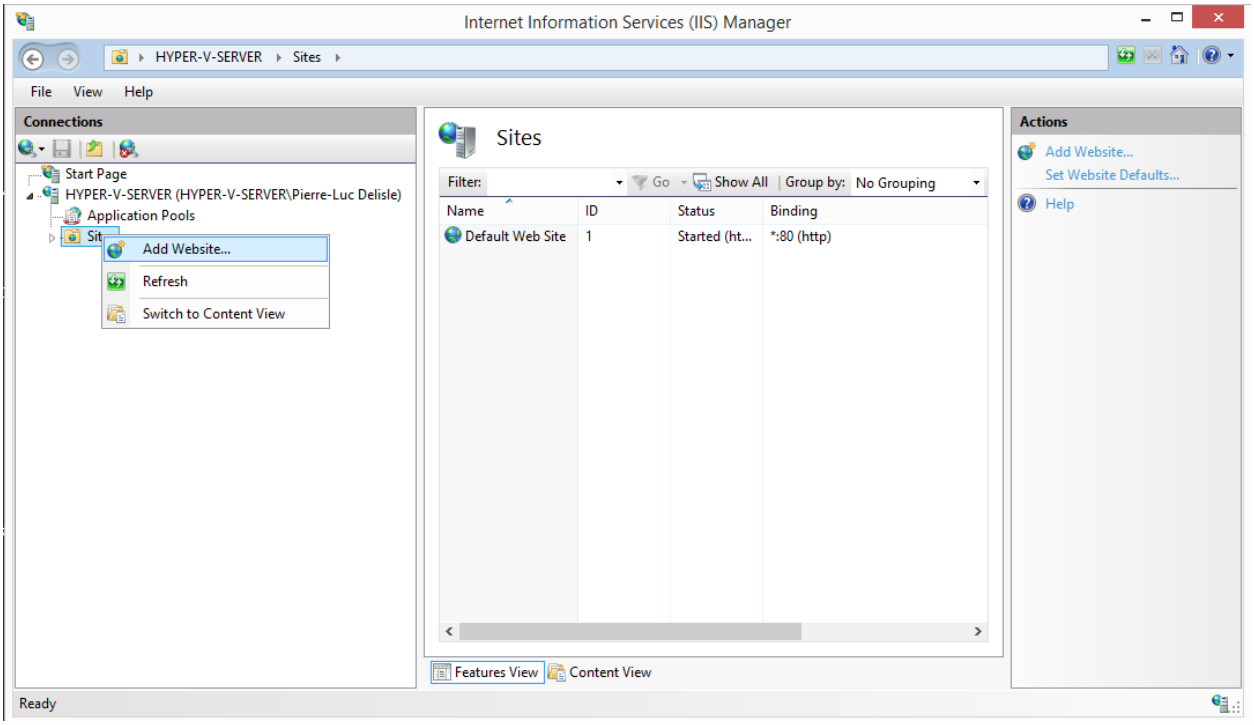
L'installation du serveur web est identique à celle de l'installation d'un serveur FTP. Il faut ajouter le rôle **IIS - Web Server** dans les rôles déjà existants du serveur. On suit ensuite les instructions ci-dessous pour créer un site HTTP :

1. Ouvrir le **IIS Manager**.



2. Dans le panneau **Connections**, ouvrir le « node » du serveur et cliquer sur **Site**.

3. Cliquez-droit sur **Site**, et cliquer **Add Web Site** pour ouvrir l'assistant de configuration **Add Web Site**.



4. Dans la boîte de dialogue **Site name**, tapez un nom pour le site web.

5. Si l'on désire sélectionner un pool d'application différent de celui préalablement listé, ouvrir la boîte de dialogue **Select Application Pool** et sélectionner le pool d'application désiré.

6. Sélectionnez l'emplacement physique du dossier où le site web sera installé.

7. Si l'emplacement physique sélectionné est situé sur un partage, cliquez sur **Connect As** pour spécifier les informations d'authentification pour accéder au partage de fichiers.

8. Sélectionnez le protocole pour le site web dans la liste de sélection **Type**.

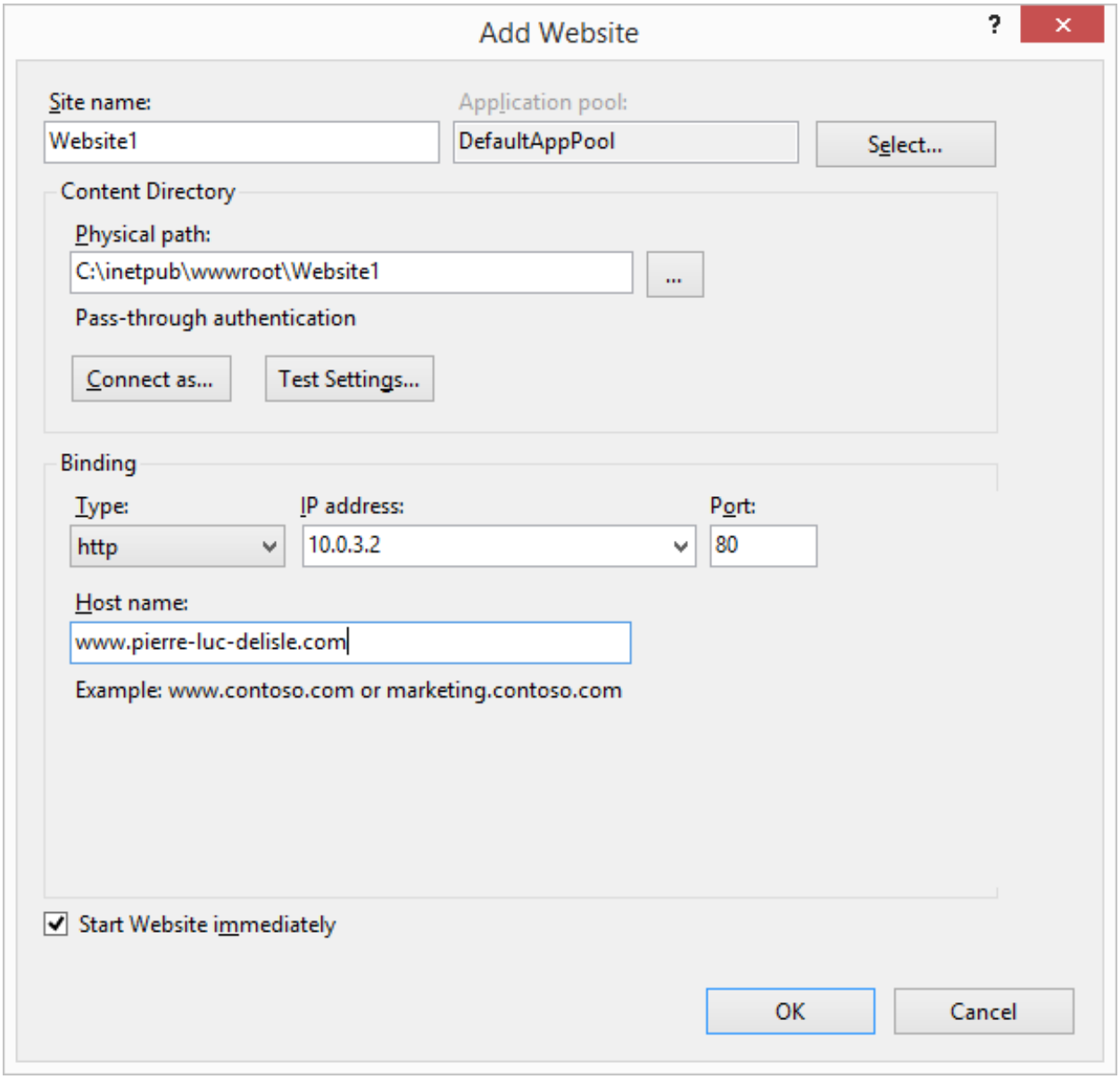
9. Spécifiez une adresse IP pour le site web dans la boîte **IP Address**.

10. Sélectionnez un port pour le site web. Normalement, le port est 80.

11. Facultativement, tapez un nom d'hôte pour le site dans la boîte **Host Name**.

12. Cochez la case **Start Web site immediately**.

13. Cliquez sur **OK** pour terminer la création du site web.



Configurer une connexion à distance

La tâche suivante consistait à mettre en place une connexion à distance permettant aux administrateurs du serveur de se connecter à distance afin de l'administrer. Certes, on pourrait simplement configurer un accès au *Shell* du serveur distant, mais bien souvent, avoir l'interface graphique s'avère plus efficace et permet de faire des opérations plus rapidement et facilement.

Pour ce faire, une connexion RDP, ou *Remote Desktop Protocol*, fut configurée. RDP est un protocole propriétaire développé par Microsoft qui procure à l'utilisateur distant une interface graphique de l'ordinateur auquel il se connecte via une connexion réseau. L'utilisateur emploi une application RDP cliente alors que l'ordinateur distant doit être pourvu d'une application serveur RDP. Par défaut, le serveur écoute sur le port 3389. Cependant, ce port est souvent la cible de personnes malveillantes. En effet, le port peut être analysé par des outils et le serveur RDP peut être la cible d'attaque par force brute (*bruteforce attacks*) et *pass the hash attacks*. Il est recommandé de déplacer le port d'écoute WAN sur un autre que celui de 3389 et de rediriger les requêtes de cet autre port sur le port 3389 à l'interne.

Microsoft réfère officiellement son application serveur RDP à *Remote Desktop Services*, qui était formellement *Terminal Services*. L'application cliente est *Remote Desktop Connection*, formellement *Terminal Services Client*.

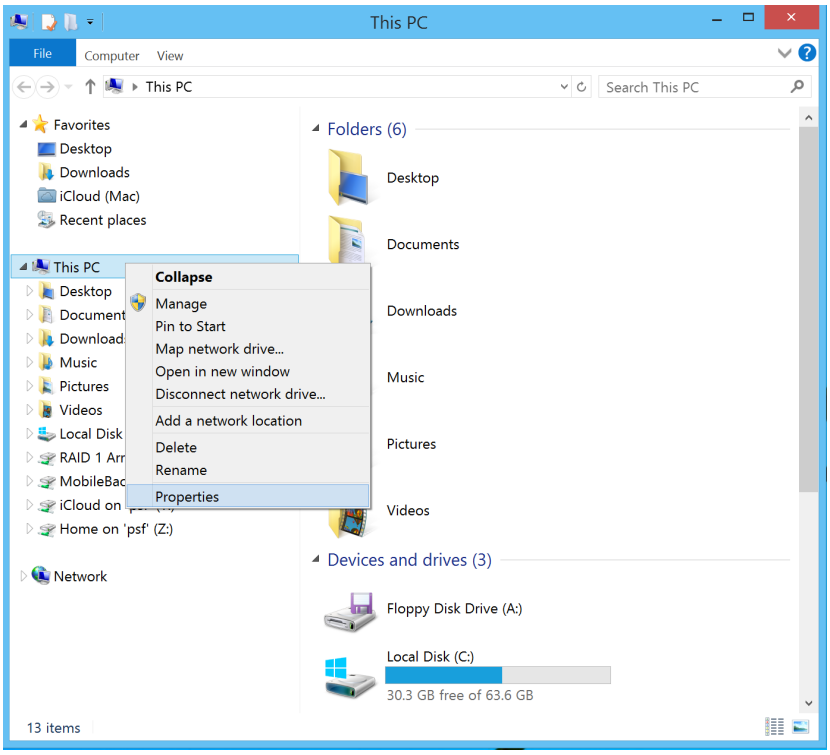
Il est par ailleurs recommandé d'utiliser un certificat SSL pour authentifier le serveur distant. De ce fait, la connexion est sécurisée au moyen d'un cryptage TLS. Il faut savoir que le protocole RDP, dans sa configuration par défaut, en plus des vulnérabilités décrites précédemment, est vulnérable aux attaques de type *man-in-the-middle*. Le cryptage SSL permet d'éviter ce type d'attaque. C'est pourquoi le protocole RDP est principalement utilisé à l'interne, dans un réseau local, et qu'une configuration VPN L2TP/IPSec est configurée pour permettre aux administrateurs de disposer d'une sécurité accrue.

Dans le cadre de ce projet, un certificat d'authentification SSL n'a pas été acheté ni configuré.

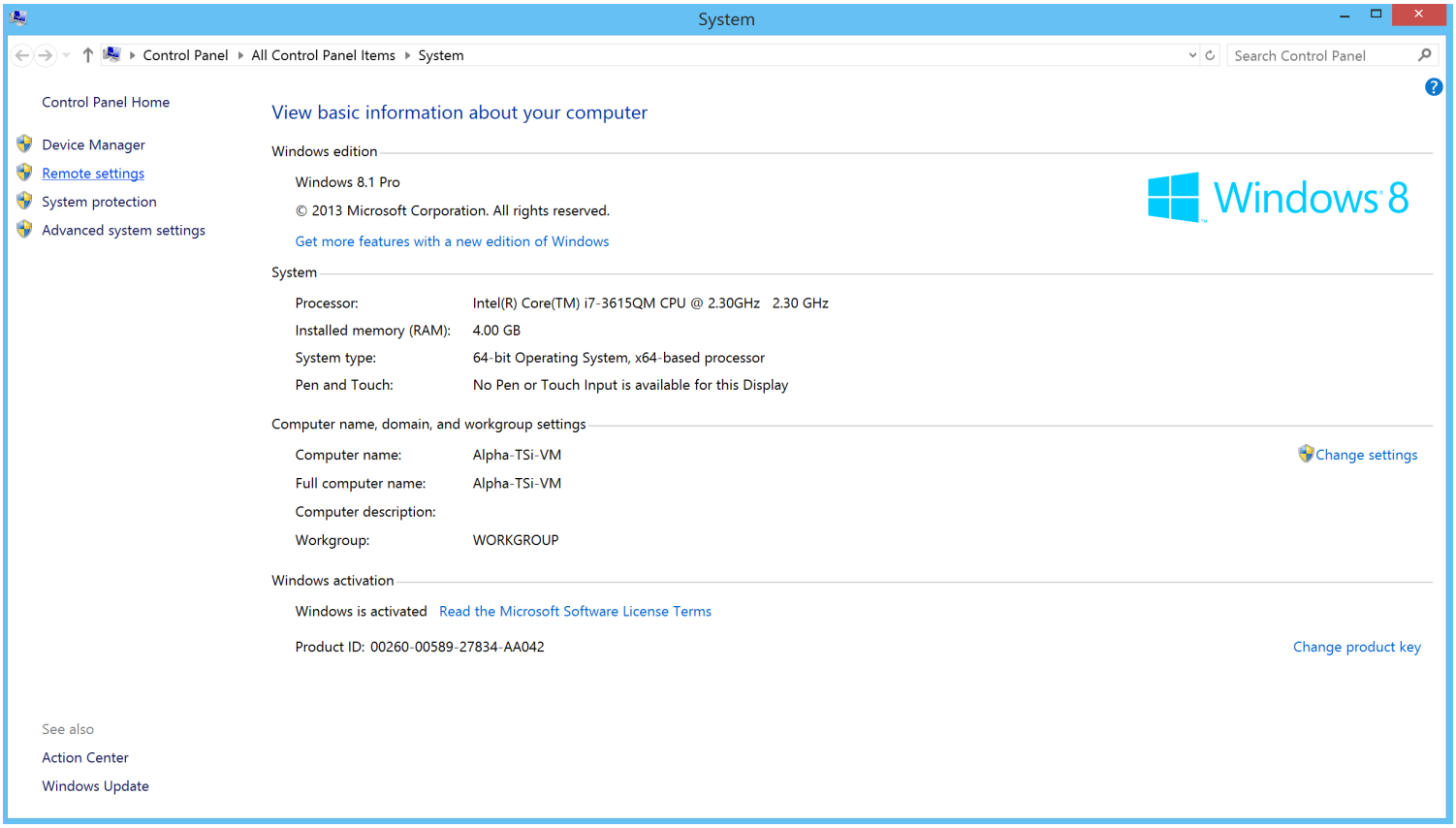
Configuration d'une connexion RDP - Guide étape par étape

1. Ouvrir l'explorateur de fichier Windows.

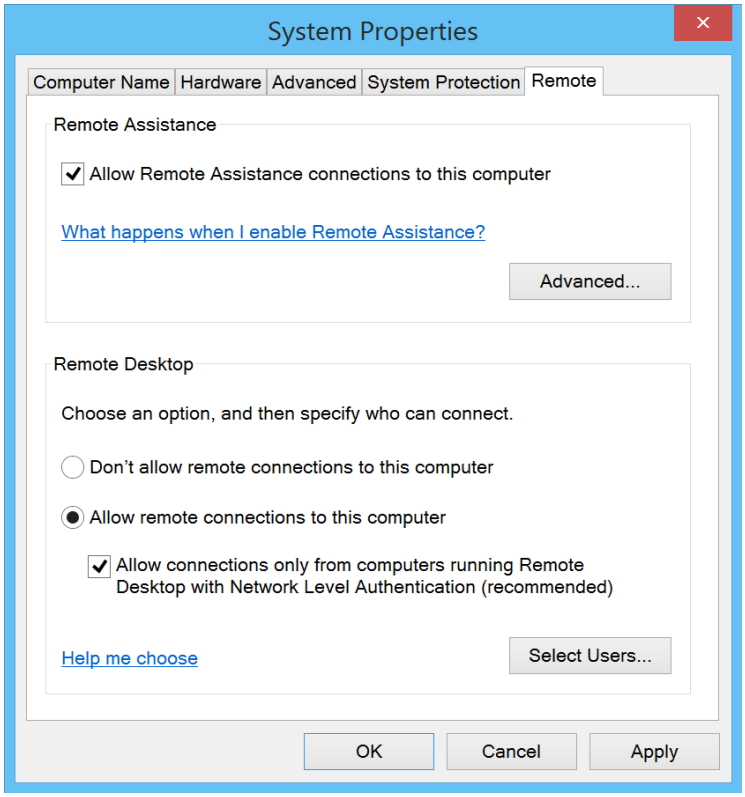
2. Cliquez-droit sur **This PC**, puis sélectionner **Properties**.



3. Cliquez à gauche sur **Remote Settings**.



4. La fenêtre de configuration des connexions à distance s'affichera. Cochez la case **Allow remote connections to this computer.** Cochez également la case **Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)**.



La connexion à distance est désormais configurée.

Virtualisation

Ce qui n'était qu'une partie du projet est devenu pour notre équipe le coeur de notre projet. Nous avions pour instruction, dans la proposition initiale du travail, d'installer un logiciel de virtualisation.

Ayant déjà pris connaissance de l'hyperviseur de Microsoft Hyper-V durant les cours, nous avons décidé d'essayer la solution concurrentielle à celle de Microsoft, soit VMware ESXi 5.5, afin de nous servir de serveur de virtualisation. Tout comme Microsoft avec Hyper-V, VMware ESXi est totalement gratuit et, depuis la version 5.5, libre de limitation matérielle. Cependant, plusieurs fonctions d'administrations plus évoluées requièrent un plan de service et une licence payante. Le système de VMware est également beaucoup plus complexe que celui de Microsoft puisque plus complet, plus évolué et plus performant.

Un serveur de virtualisation ESXi est un serveur ayant comme «système d'exploitation» un hyperviseur. Un hyperviseur ne peut être utilisé seul. Une fois installé puis configuré, on doit, par le biais d'un client, lui créer et lui mettre en place les machines virtuelles qu'il pourra opérer.

Il existe deux types d'hyperviseur :

1. Type 1 Bare-Metal Hypervisor
2. Type 2 Hosted Hypervisor

Dans le premier cas, il s'agit d'un système qui n'opère que des machines virtuelles. Le système en l'occurrence VMware ESXi ou encore Microsoft Hyper-V, ne sert qu'à virtualiser des machines *clientes*. Un hyperviseur, comme celui de VMware, est un système d'environ 1 million de lignes de codes seulement (contrairement à un système d'exploitation qui peut en contenir facilement 25 millions de lignes). Cela procure toujours dans le cas de VMware ESXi, une surface d'attaque de loin réduite à celle d'un véritable système d'exploitation. Il en résulte un système monolithique[1] réduit en taille et qui procure une plus grande sécurité. Le cas de Hyper-V est légèrement différent puisqu'il opère conjointement avec le système d'exploitation Windows, mais l'hyperviseur est essentiellement un service distinct qui n'emprunte l'environnement Windows que

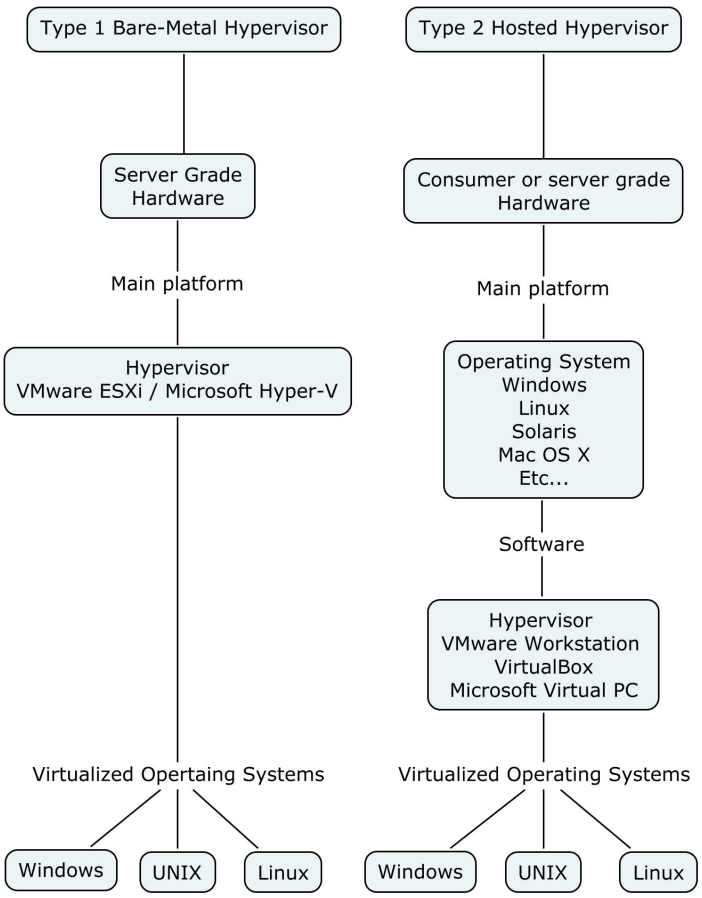
[1] Un **noyau monolithique** est une architecture de système d'exploitation dans laquelle le kernel (noyau) est un processus qui travaille dans un espace mémoire défini. Le kernel est seul dans cette espace et fonctionne en mode supervision. Le modèle monolithique se distingue des autres architectures de systèmes d'exploitation (tels que l'architecture micronoyau) car elle définit une interface virtuelle de haut niveau sur le matériel informatique. Un ensemble d'appels de système (*calls*) mettent en œuvre tous les services du système d'exploitation tels que la gestion des processus et la gestion de la mémoire. Le kernel peut invoquer des fonctions directement. Il est statique et non modifiable, mais des pilotes de périphériques peuvent être ajoutés au noyau sous forme de modules.

pour le GUI. Les hyperviseurs fonctionnent conjointement de très près avec les technologies embarquées sur le matériel, notamment la Intel VT-x et la VT-d (et les équivalents AMD).

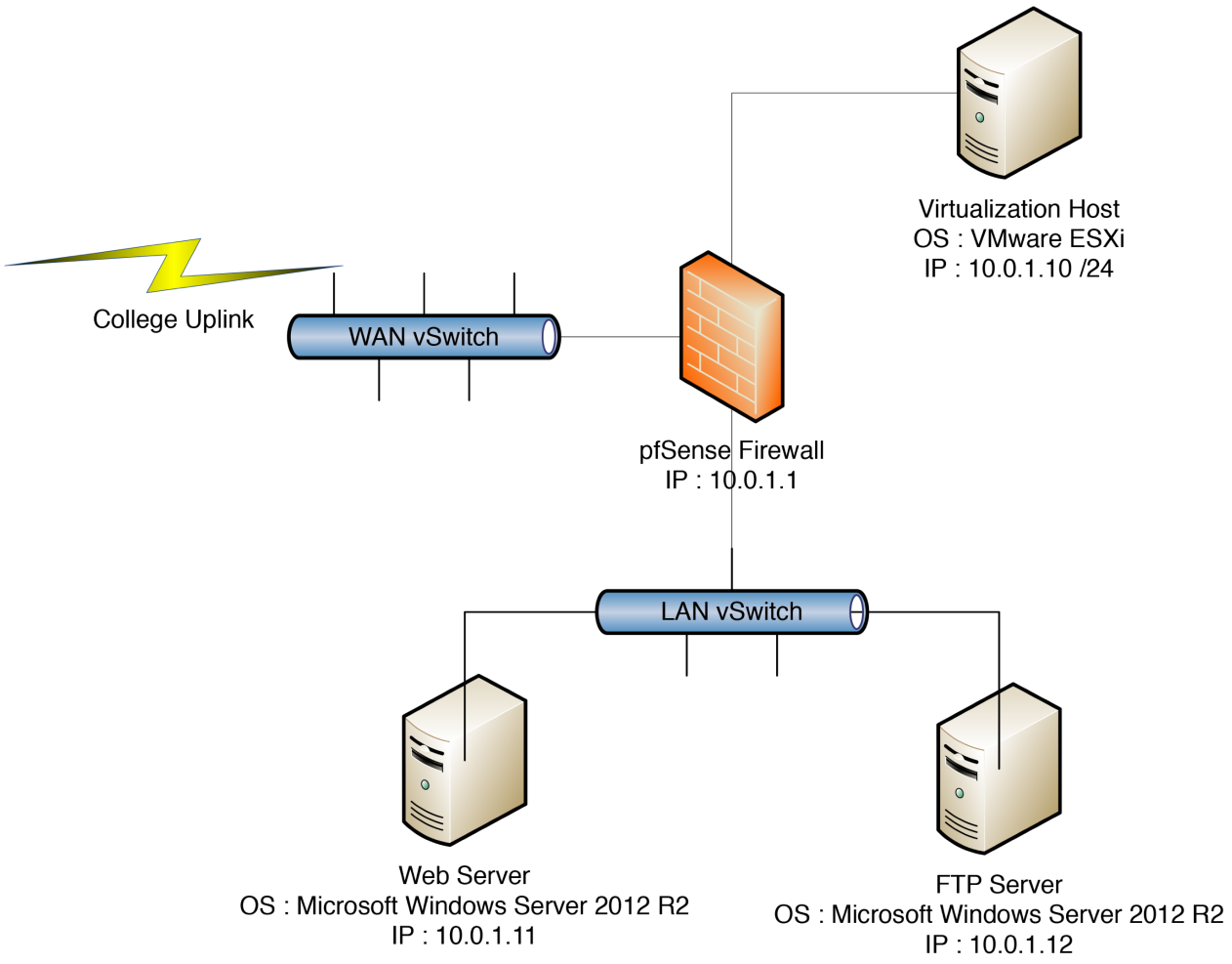
Dans le deuxième cas, on parle de virtualisation logicielle. On passe par un hyperviseur sous forme logicielle, par le biais d'un système d'exploitation Windows, Linux ou Mac OS X. Les performances sont moindres que dans le premier cas puisqu'il y a une couche applicative entre le matériel et l'hyperviseur. Hyper-V, bien qu'intégré au sein de Windows, n'est pas un hyperviseur de type 2. Il n'opère pas par dessus Windows, mais bien juste au-dessus du matériel.

La beauté d'un hyperviseur de type 1 réside dans le fait que l'on peut virtualiser n'importe quel système d'exploitation, y compris des systèmes d'exploitation de stockage. Dans le dernier cas, on peut très bien faire opérer ce genre de système tout en faisant tourner d'autres machines virtuelles sur d'autres plateformes. Cela permet de réduire les coûts puisque toutes les plateformes peuvent opérer sur le même serveur de virtualisation. Dans cette solution, le stockage n'est pas virtualisé; seul le système d'exploitation (par exemple, FreeNAS) est virtualisé et a accès aux disques durs physiques grâce au *pass-through* des contrôleurs logiques (LSI ou Intel) de la carte mère via la technologie VT-d ou AMD-Vi.

Vous trouverez ci-dessous une image comparative des hyperviseurs.



Un des principaux buts de la virtualisation côté serveur est de ségrégué les services dont on a besoin sur le réseau local. Le concept est simple : un service par machine virtuelle. Certes, cela prend plus de ressources matérielles puisqu'il y a plusieurs instances de systèmes d'exploitation opérant en même temps sur le serveur de virtualisation. Toutefois, avec du bon matériel, ce point est rapidement oublié devant la facilité de la gestion acquise grâce à la virtualisation. On peut rapidement recouvrir d'un désastre en revenant à un cliché instantané précédent (*revert back to previous snapshot*) tout en minimisant le temps d'indisponibilité du serveur et en gardant actif les autres services qui n'ont pas été touchés par l'anomalie. Une telle configuration de réseau peut donc s'avérer extrêmement pratique dans un environnement de production et nous voulions reproduire une telle installation durant ce projet. Voici un schéma :

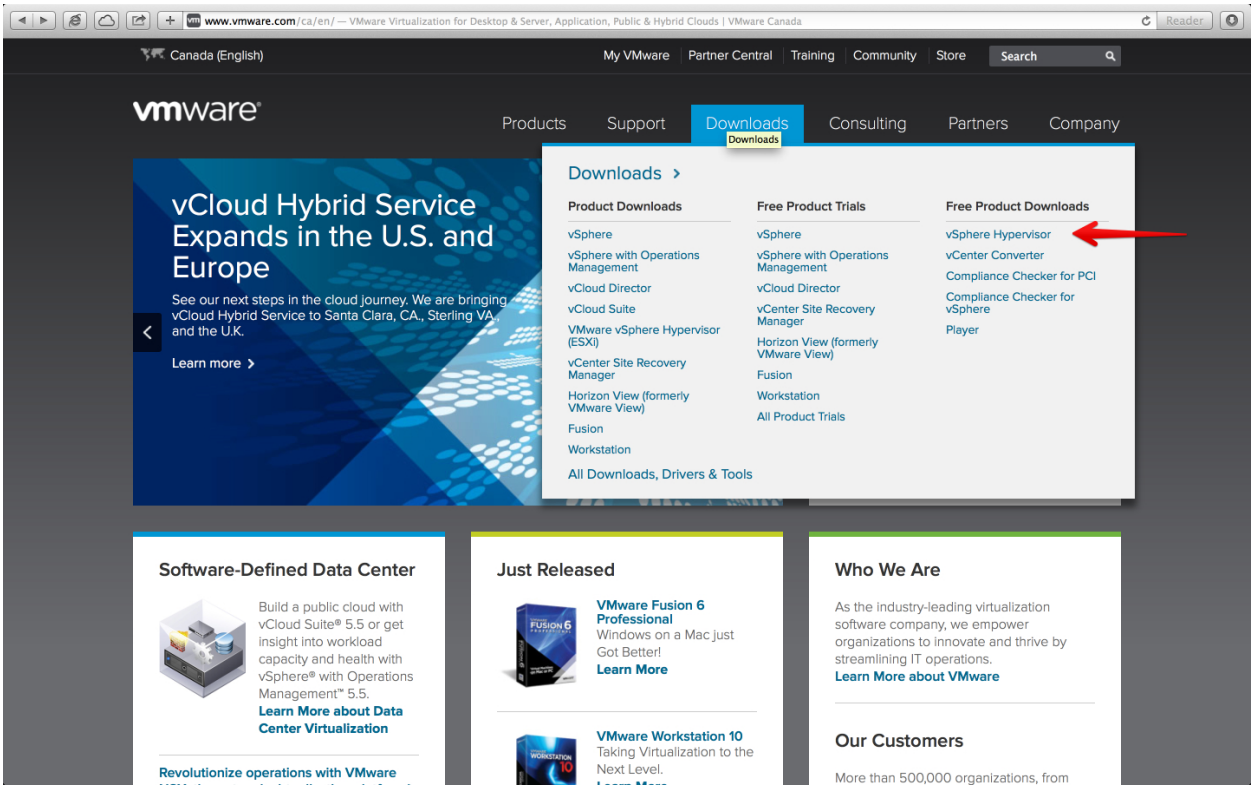


Configuration minimale pour VMware ESXi :

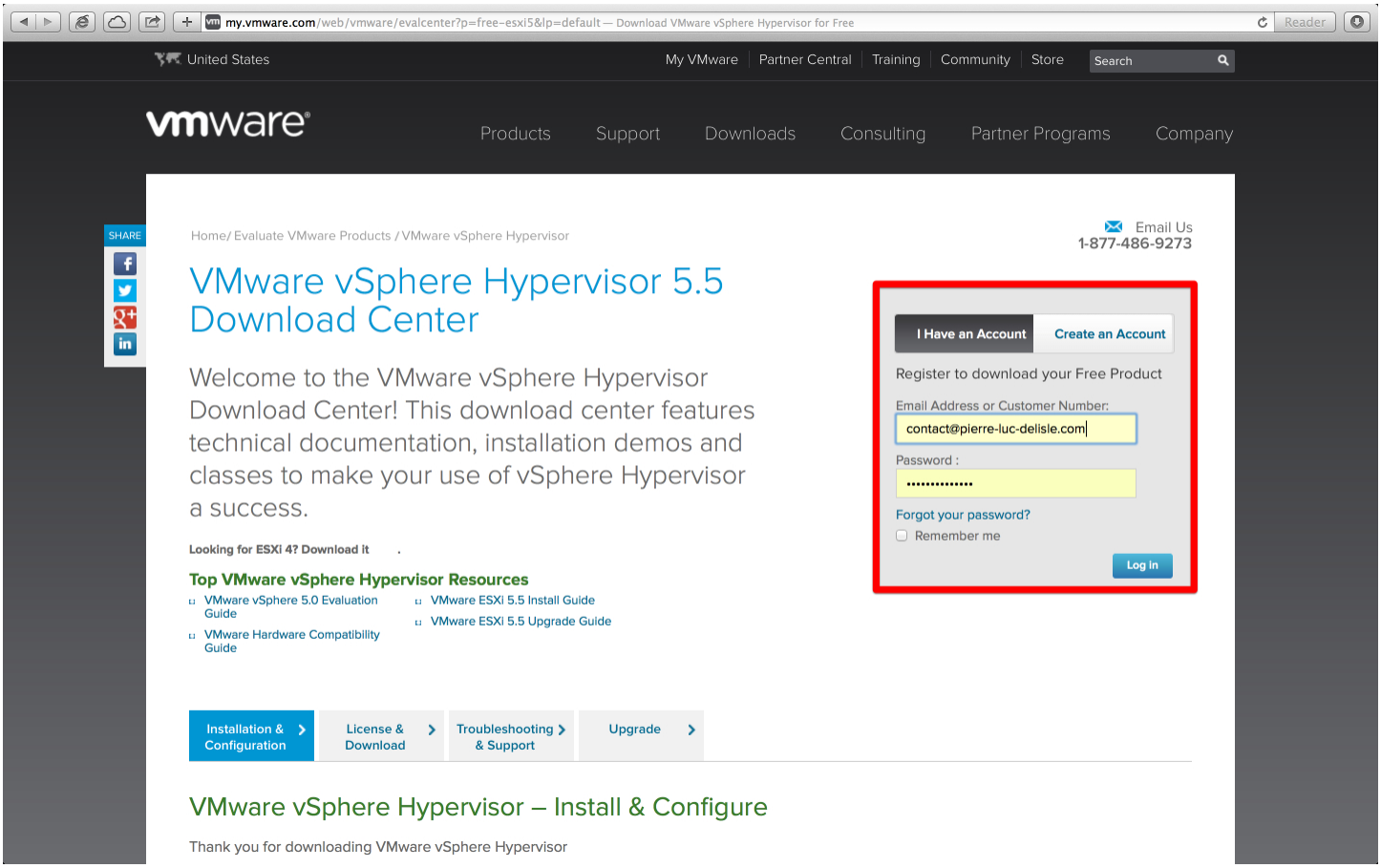
- Processeur 64-bit bi-coeur (Intel Xeon recommandé).
- CPU doit avoir les jeux d'instruction LAHF et SAHF.
- 8 GB de mémoire vive (mémoire vive ECC recommandée).
- Intel VT-x (AMD-RVI) requise. Intel VT-d est un plus très important.
- Minimum 1 adaptateur réseau de type Gigabit. 2 adaptateurs et plus sont recommandés. Des adaptateurs 10 Gb sont un plus. Préférez la marque Intel, mais les adaptateurs Realtek sont supportés en injectant un pilote.
- Les contrôleurs RAID LSI et Intel sont recommandés.
- Pour la liste complète de la compatibilité matérielle, visitez http://www.vmware.com/resources/compatibility/search.php et http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003661

Guide d'installation de VMware ESXi étape par étape :

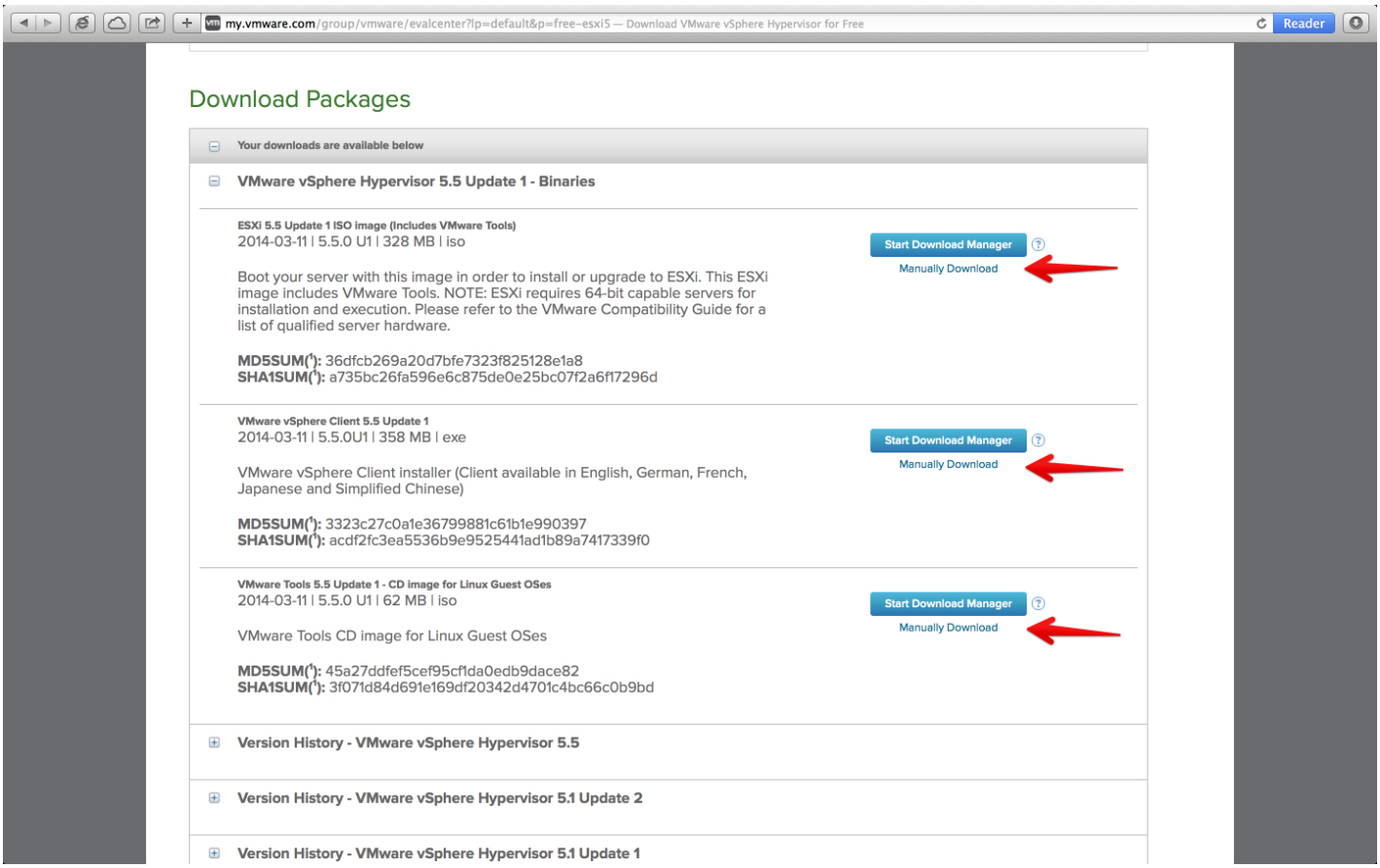
1. Aller au www.vmware.com. Cliquer sur *Download* et cliquer sur vSphere Hypervisor dans la colonne *Free Product Download.*



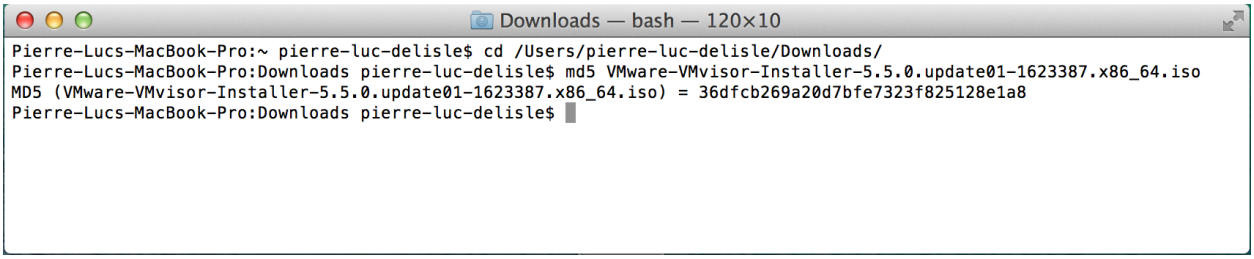
2. Rentrer un nom d'utilisateur et mot de passe.



3. Télécharger :
   ESXi 5.5 Update 1 ISO image (Includes VMware Tools)
   VMware vSphere Client 5.5 Update 1
   VMware Tools 5.5 Update 1 - CD image for Linux Guest OSes



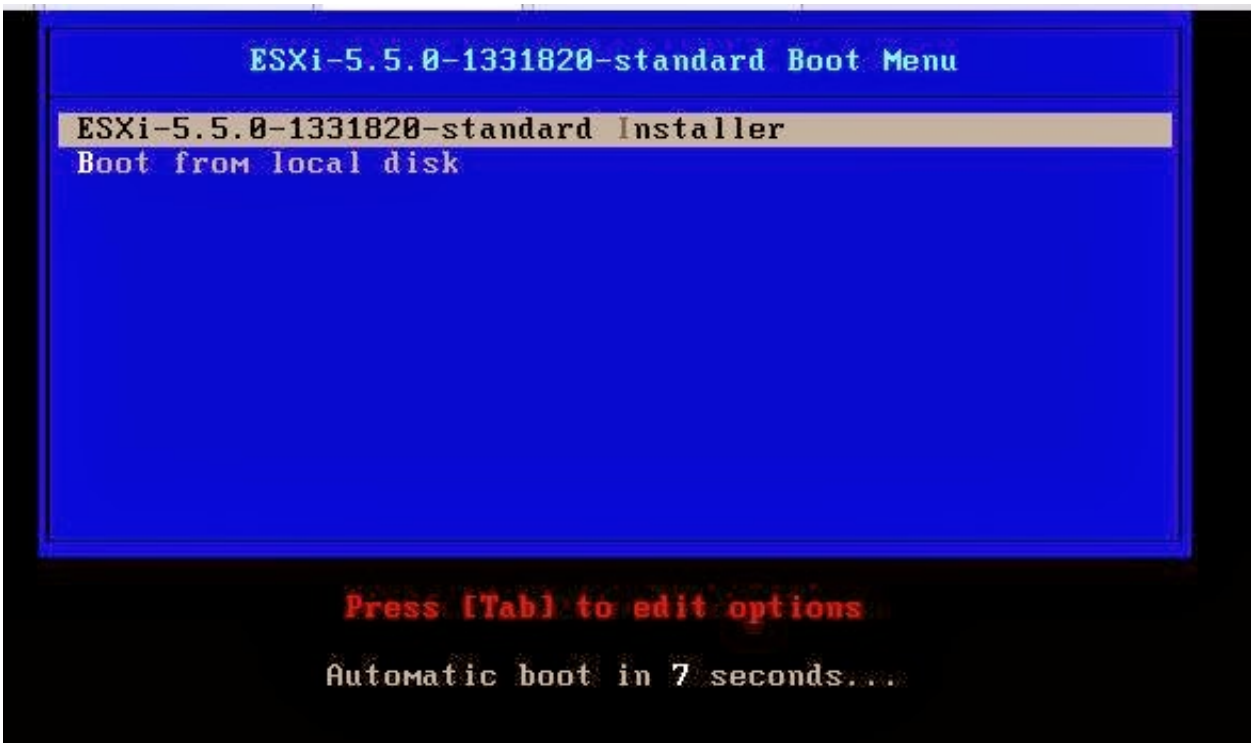
4. Avec un terminal UNIX (Mac OS X ou Linux), faites un *MD5 Checksum* pour vérifier l'intégrité du fichier téléchargé. Sur Windows, utiliser un utilitaire de calcul de somme MD5. Comparez avec les valeurs de VMware.



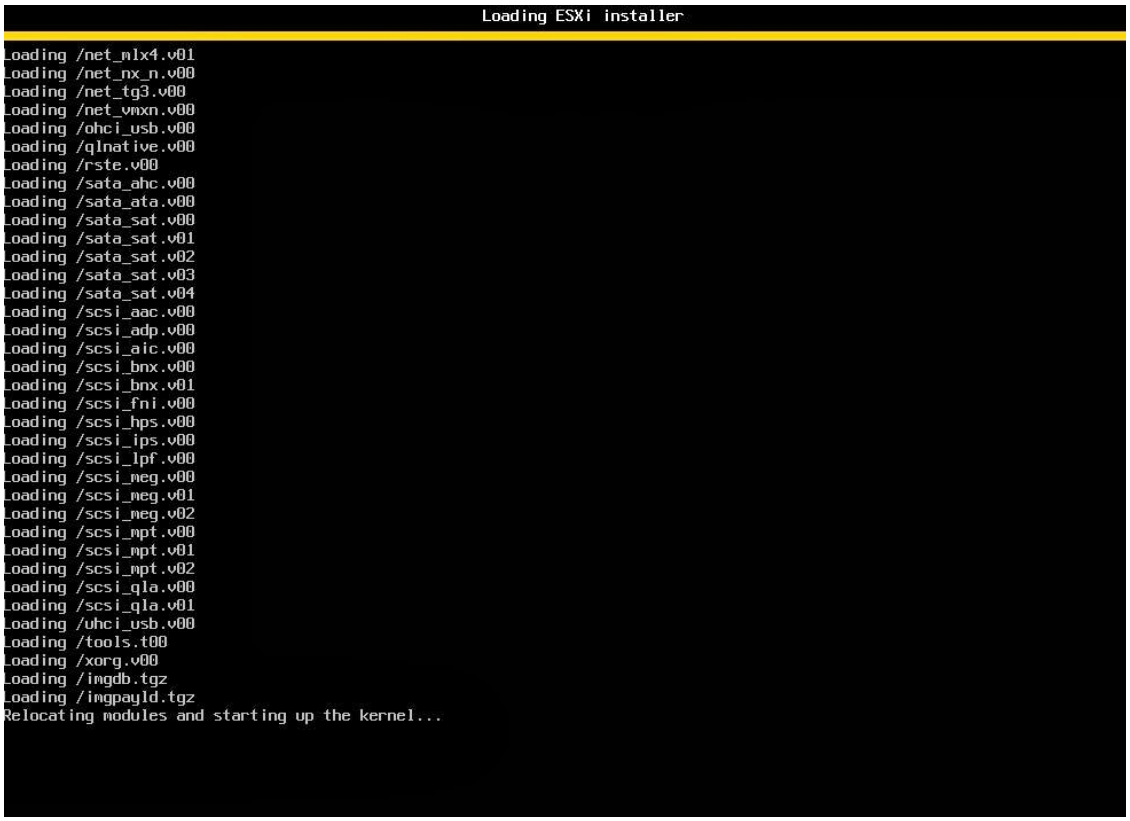
5. Faites une clef USB amorçable avec *Unetbootin* et le fichier ISO téléchargé.

6. Démarrez le serveur sur la clef USB.

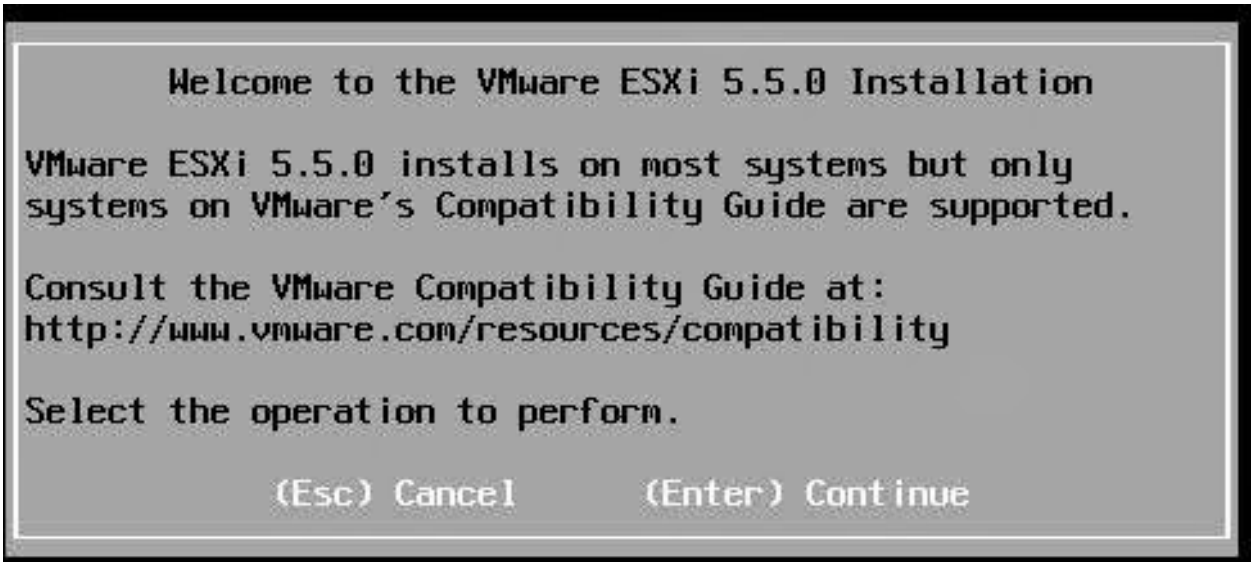
7. Démarrez l'installateur de l'hyperviseur.



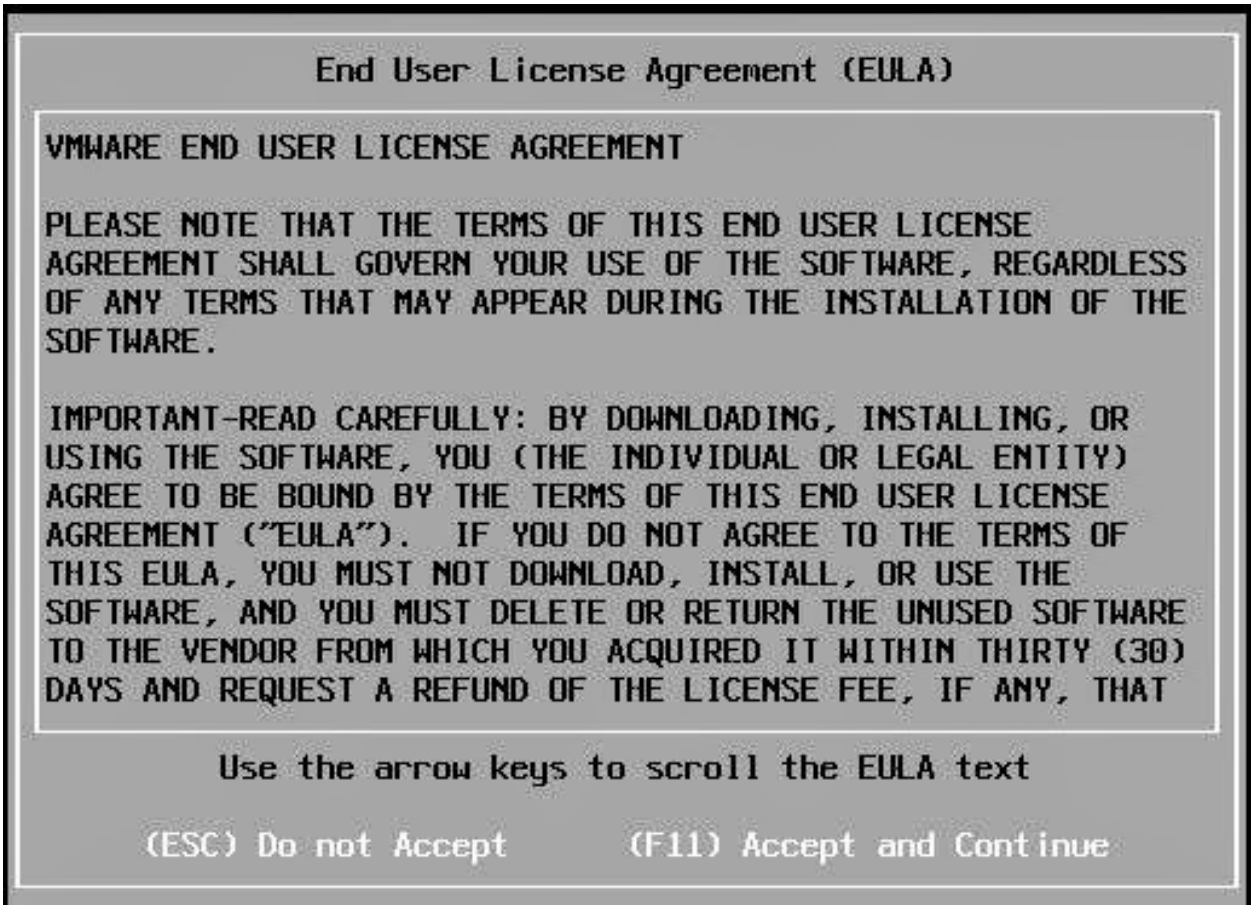
8. L'installateur de ESXi chargera les fichiers nécessaires durant les prochaines minutes. Une fois chargés, l'hyperviseur relocalisera les modules et démarra le kernel.



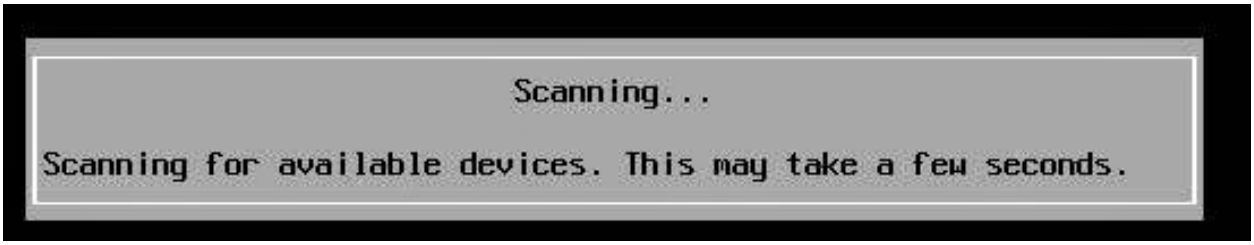
8. Dans le fenêtre de bienvenue, appuyez sur **Enter** pour démarrer l'installation.



9. Acceptez les conditions d'utilisations en appuyant sur **F11**.

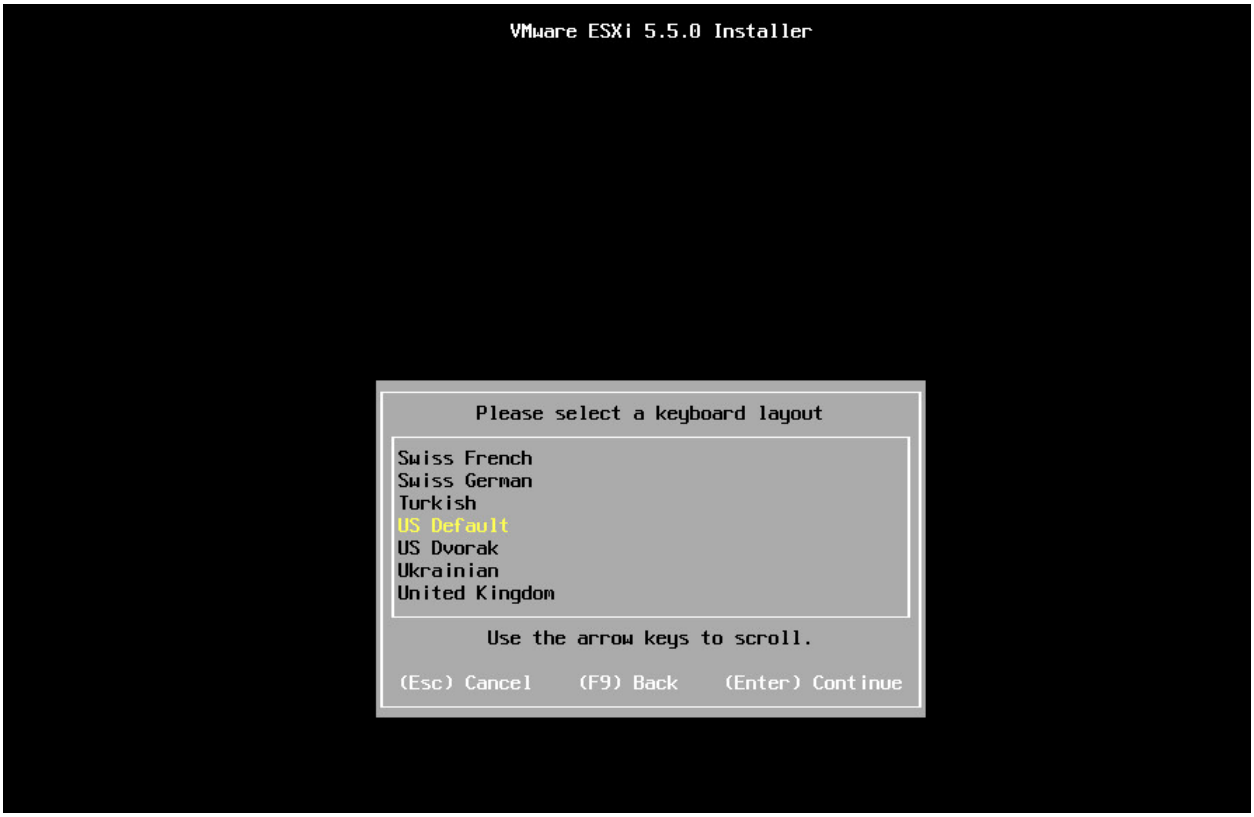


10. ESXi analysera les différents composants matériels du serveur.



11. Sélectionner le **disque de destination** de l'installation. Cela peut être un disque dur interne, un RAID array si le contrôleur RAID est reconnu (idéalement, on utilise des contrôleurs RAID Intel ou LSI) ou bien une clef USB. Sélectionnez le disque et appuyer sur Enter.

12. Sélectionnez la **langue** du clavier.

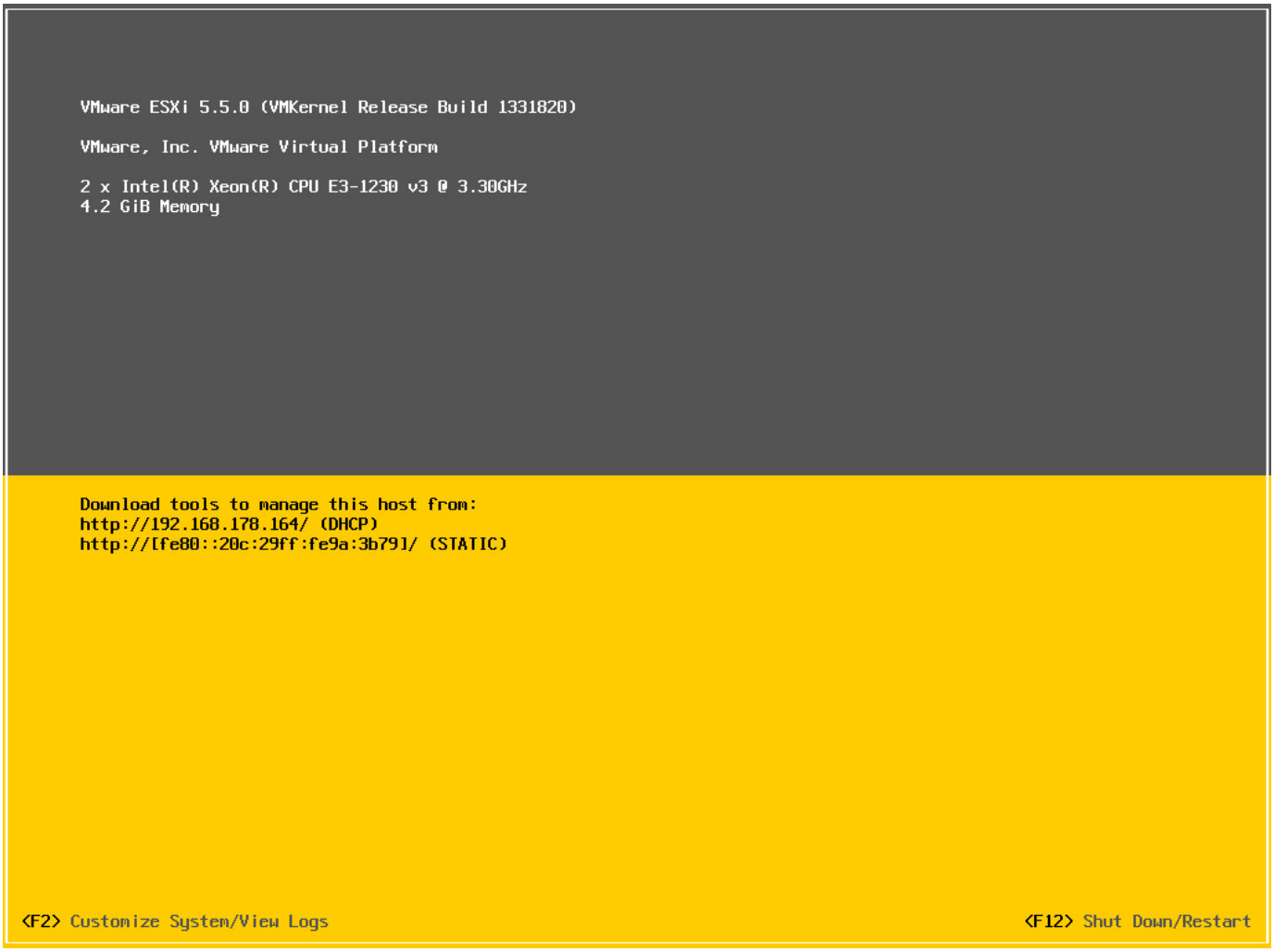


13. Entrez un **mot de passe *root***.

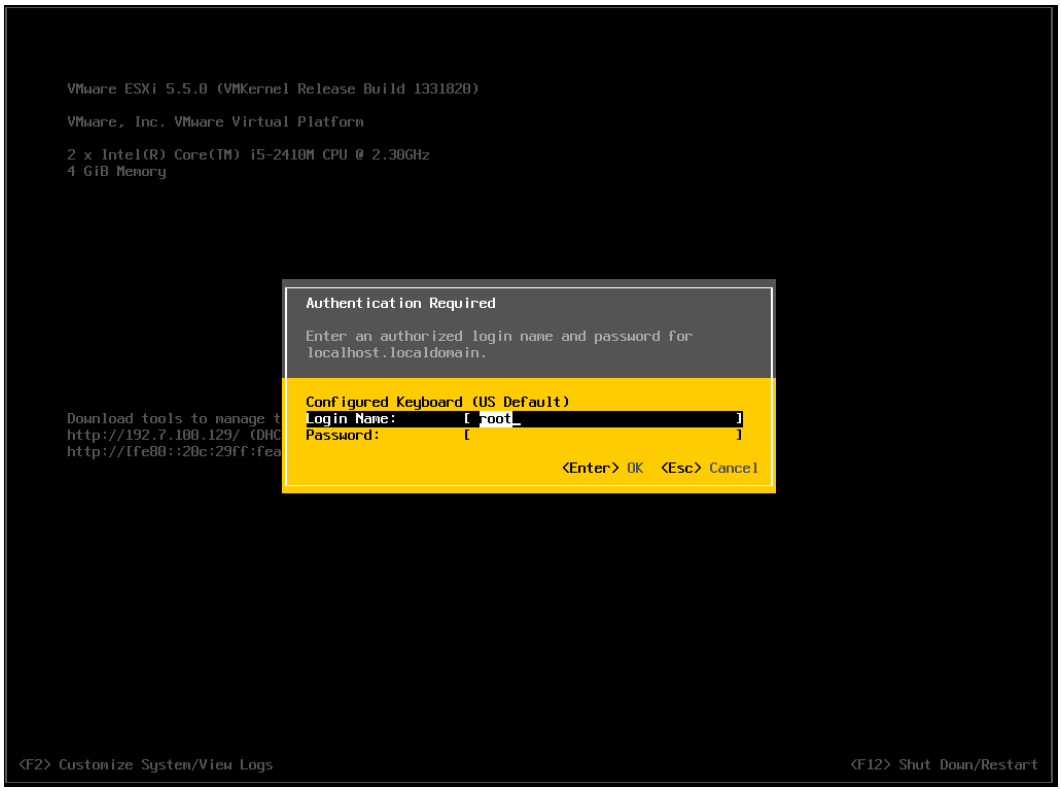
14. Confirmez l'installation.

15. Lorsque l'installation est terminée, il faut redémarrer le serveur.

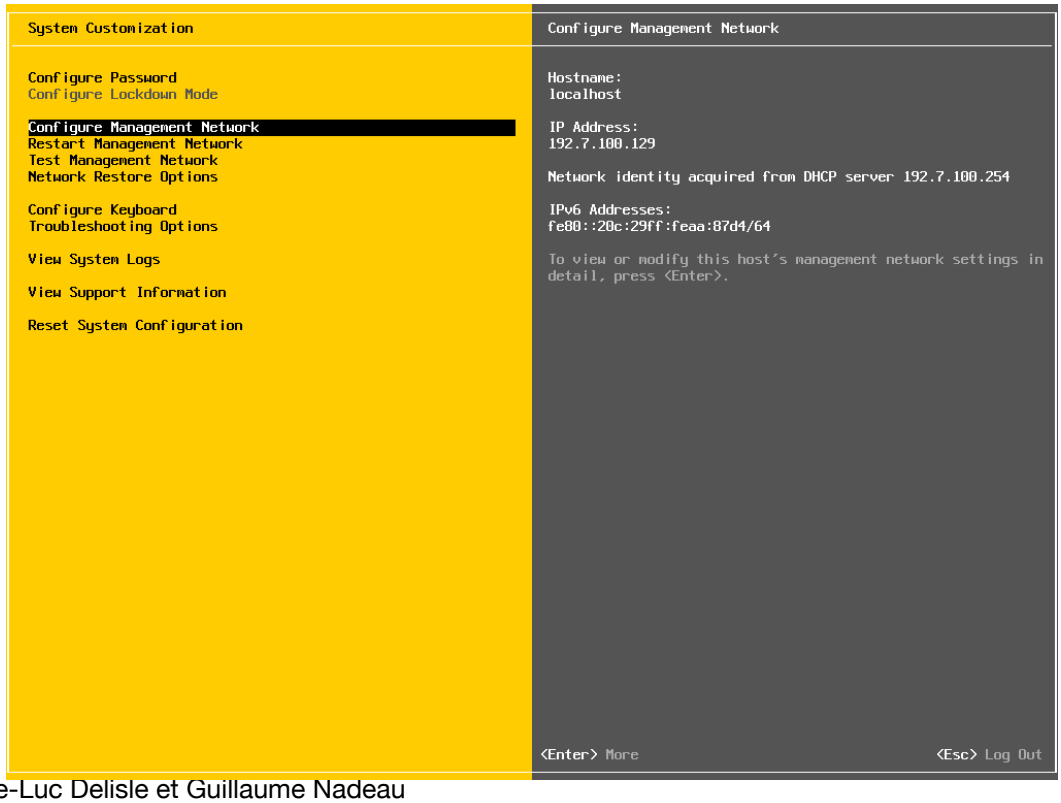
16. Après le redémarrage, le serveur est prêt à être configurer.



17. Appuyez sur **F2** pour entrer dans le mode configuration. Le **mot de passe *root*** sera requis pour activer le mode de configuration.

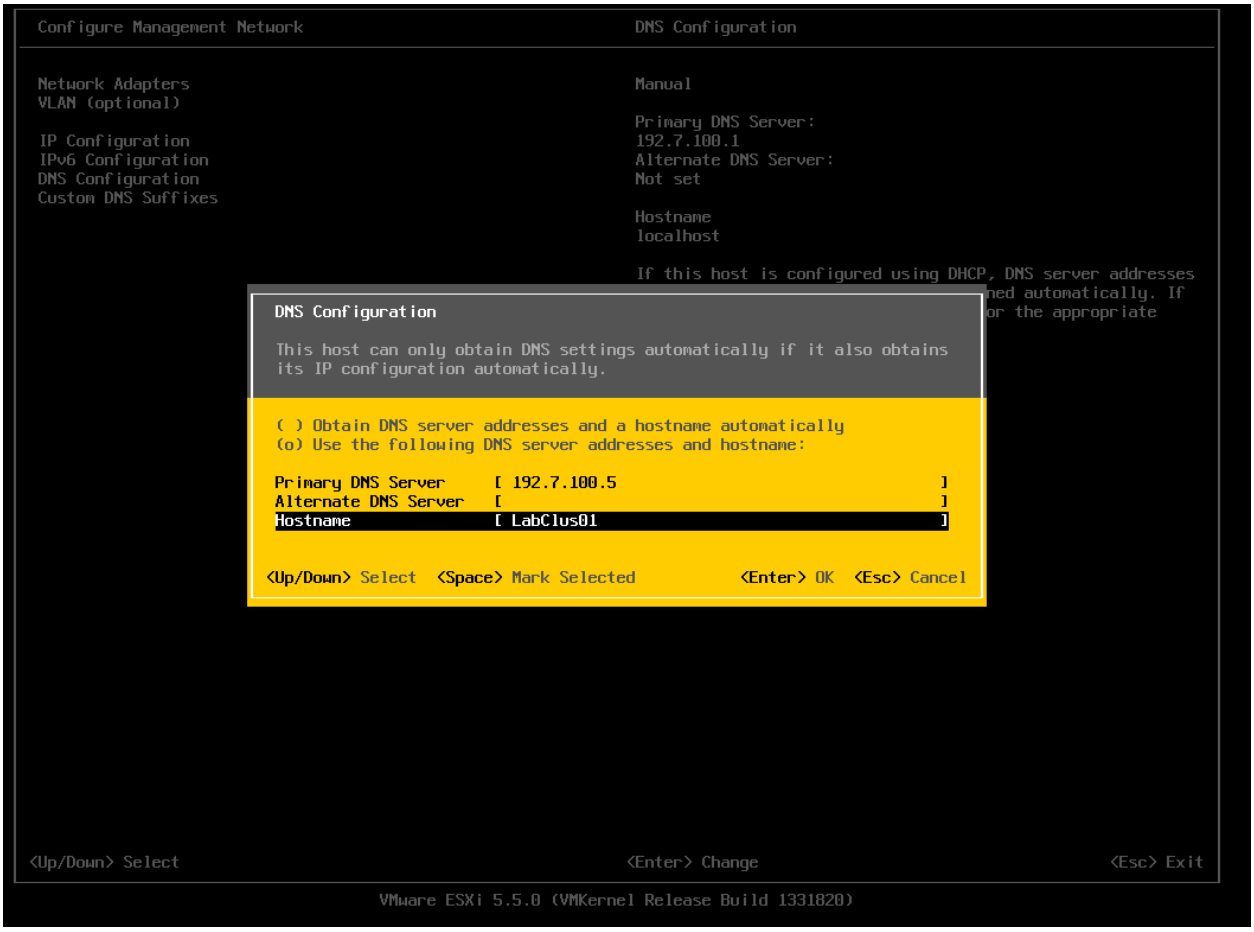


18. Allez dans le mode **Configure Management Network**.

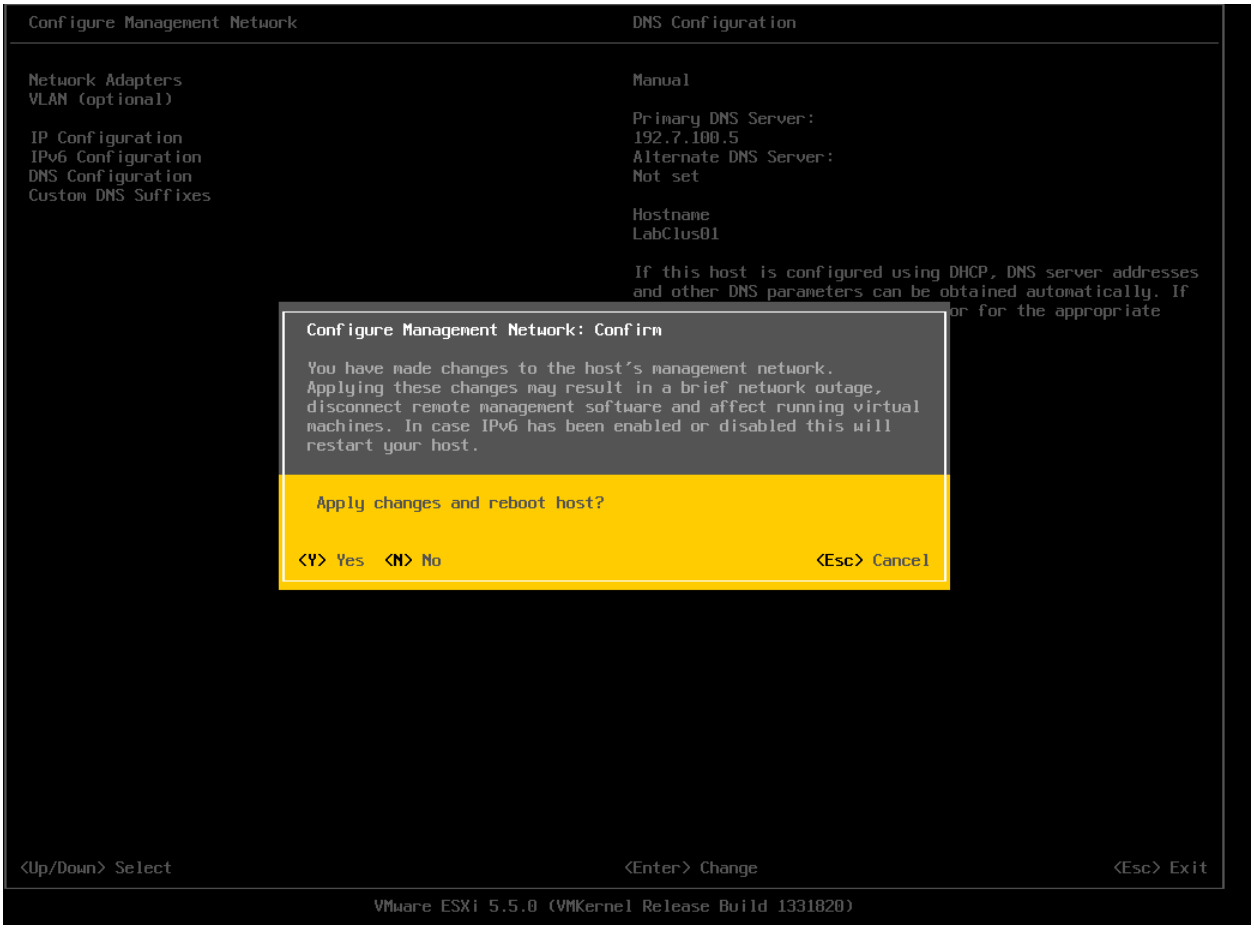


19. Il faudra configurer une **adresse IP statique** pour le serveur. Une réservation dans le serveur DHCP pour la même adresse IP serait également conseillée en cas de dysfonctionnement. Cela permet de trouver rapidement le serveur dans le cas où la configuration réseau est réinitialisée. Appuyez sur **Enter** pour entrer dans la configuration du réseau, et entrez les bonnes informations pour votre réseau local. Désactivez l'adresse IPv6 si nécessaire.

20. Entrez par la suite les **serveurs DNS** présents sur votre réseau local.



21. ESXi demandera une **confirmation** pour sauvegarder définitivement la configuration réseau. Appuyez sur “**Y**” pour accepter les changements et redémarrer le serveur.

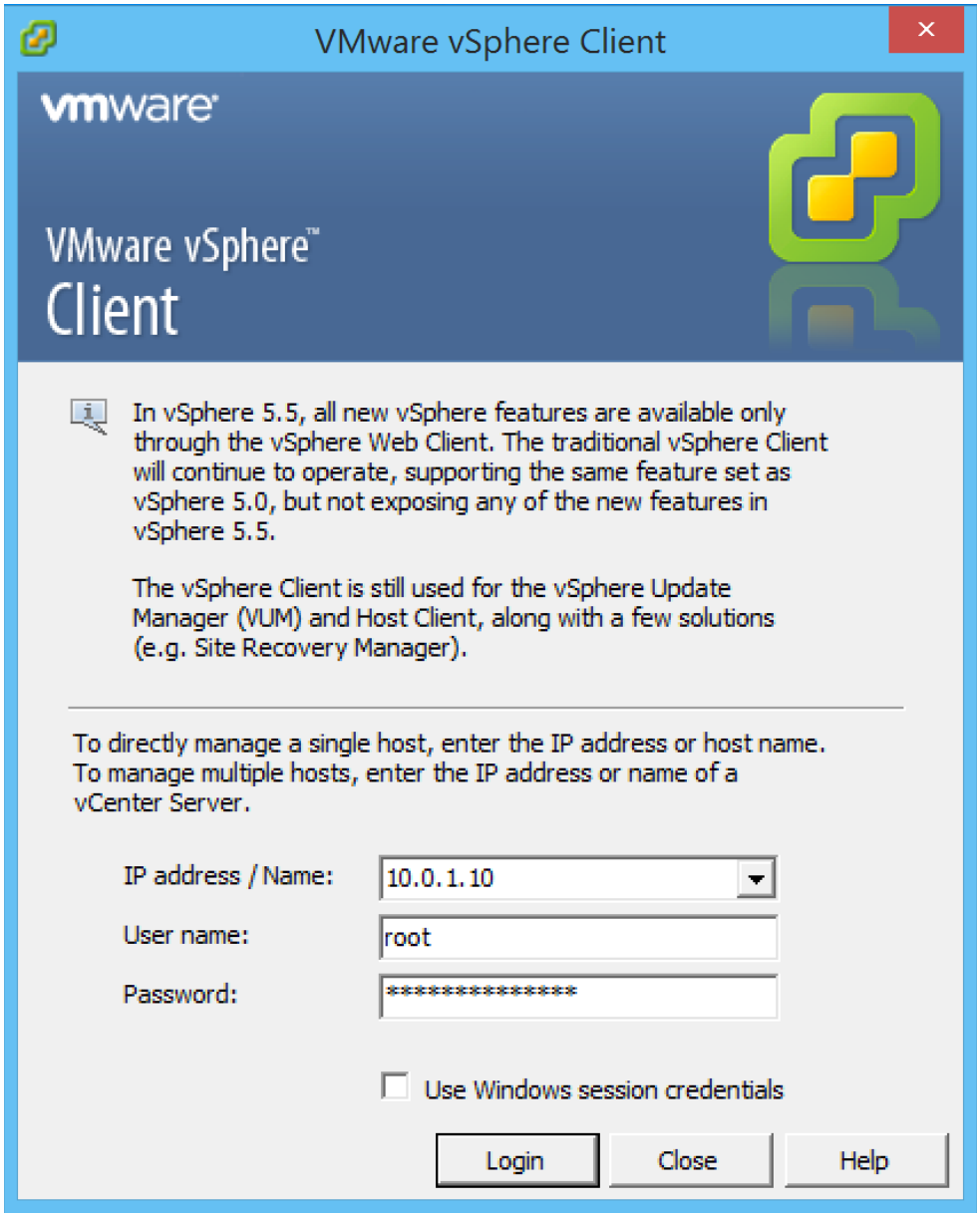


22. Après le redémarrage du serveur, il faut s’assurer que nous avons une communication avec ce dernier. À l’aide d’une machine cliente sur le réseau, **lancer des requêtes ICMP** vers le serveur ESXi. Si le serveur répond, procédez aux étapes suivantes. Dans le cas contraire, dépannez la configuration réseau.

23. Installez VMware vSphere Client sur une machine cliente. Le logiciel permettra de configurer et administrer entièrement le serveur ESXi à distance.

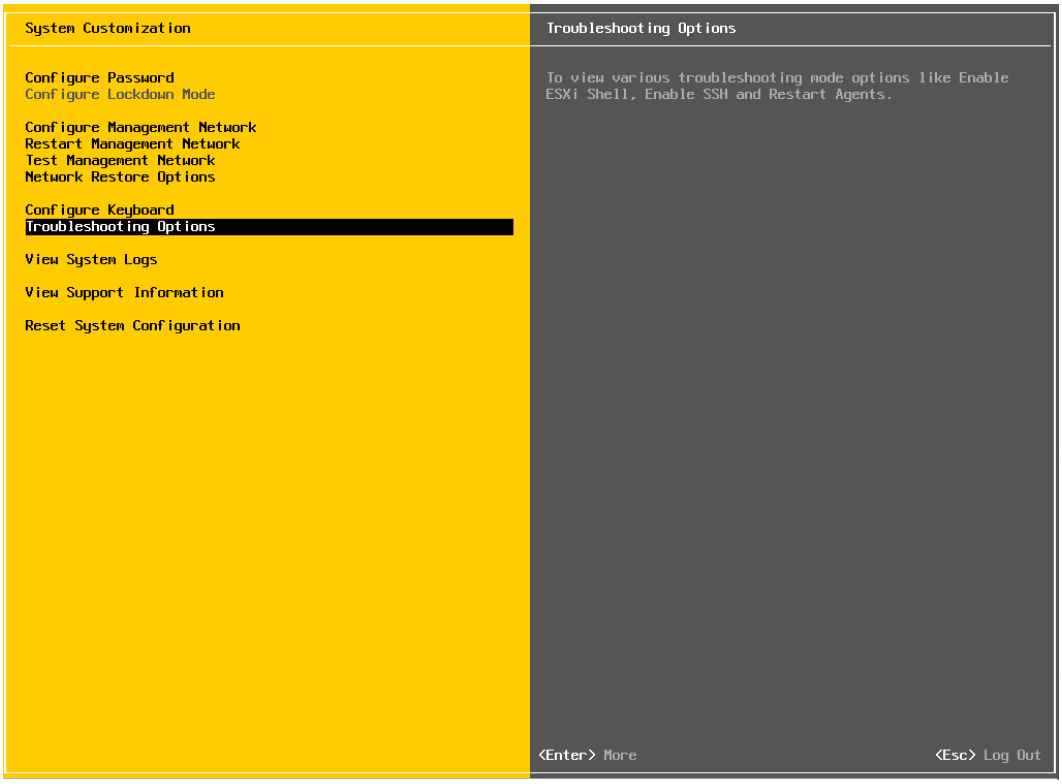
24. Lorsque l’installation est terminée, **lancez VMware vSphere**.

25. Entrez les informations requises pour se connecter au serveur ESXi.

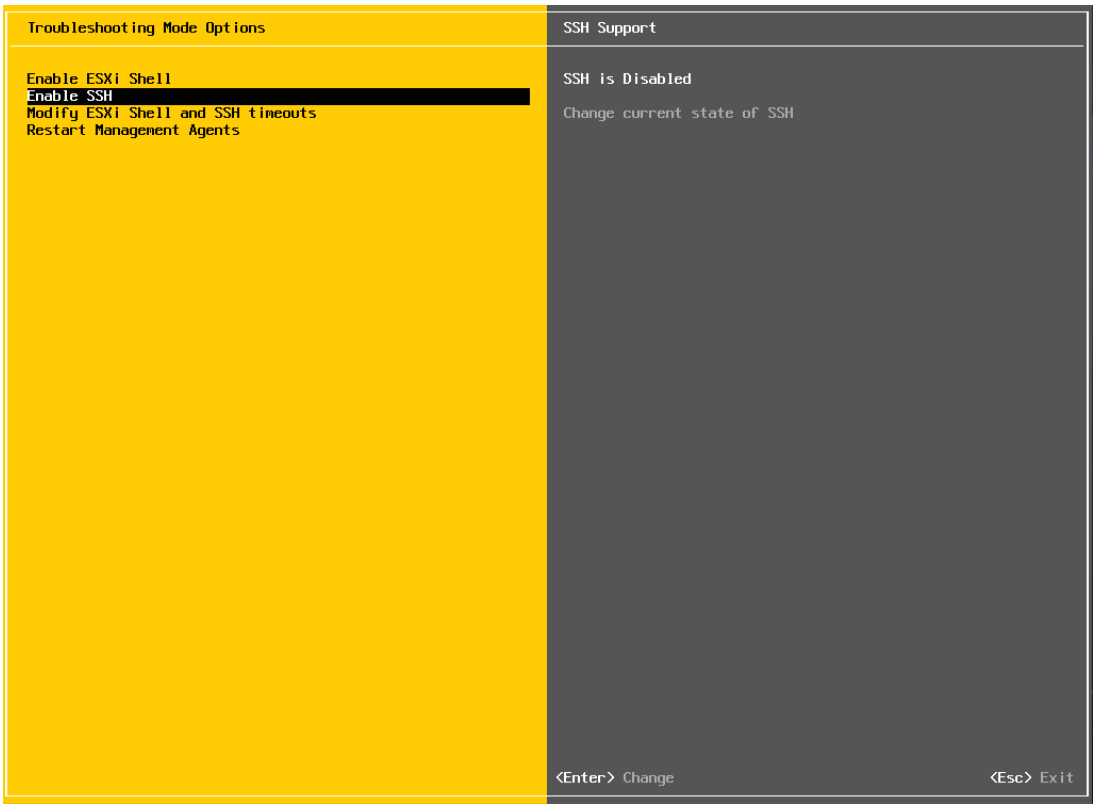


26. Pour des opérations ultérieures, il faudra activer le SSH et le ESXi Shell. Pour se faire, il faut entrer en mode *Customize System* en appuyant sur **F2** et en **entrant le mot de passe root**.

27. Faites **Enter** sur **Troubleshooting Options**.



28. Faites **Enter** sur **Enable ESXi Shell** et **Enable SSH**.



Configuration d'un pare-feu dans un environnement virtuel

Le projet avait également pour but de configurer un pare-feu pour le réseau que nous avions créé. Cependant, la solution proposée en laboratoire n'a jamais fonctionné. Elle constituait à la configuration d'un pare-feu avec FirewallBuilder. Bien que l'utilitaire semble bon, il n'est même plus répertorié dans la liste des dix meilleures applications pare-feu sur Linux selon TechMint[2] et plusieurs autres alternatives sont aujourd'hui beaucoup plus performantes.

Avec une mise en place d'un serveur ESXi et disposant d'un serveur comportant deux adaptateurs réseau câblé, l'option de virtualiser un système d'exploitation jouant le rôle de routeur et de pare-feu. Un système extrêmement populaire en entreprise pour ce genre d'application est pfSense. pfSense est un pare-feu de type OpenSource basé sur FreeBSD, un système d'exploitation Unix-Like. pfSense est un système d'exploitation à part entière qui transforme un ordinateur physique en routeur et pare-feu. Il est très réputé pour son excellente stabilité grâce à sa plateforme Unix et dispose de plusieurs fonctionnalités que l'on retrouve seulement sur des solutions propriétaires beaucoup plus onéreuses. Il ne requiert aucune connaissance du *sub-system* de FreeBSD. pfSense est couramment utilisé pour déployer des pare-feu de périmètre (*perimeter firewall*), des routeurs, des points d'accès sans-fil, des serveurs DHCP, des serveurs DNS et des serveurs VPN. pfSense supporte la mise en réseau sous des VLANs 802.1q, propose un système de *Quality of Service* (QoS) et propose même une fonctionnalité de DNS dynamique.

pfSense a été conçu avec pour première vocation la comptabilité avec n'importe quel matériel informatique. Plusieurs fabricants produisent des systèmes à très basse consommation d'énergie pour embarquer spécifiquement pfSense, mais ce dernier peut très bien être installé sur n'importe quelle machine, y compris dans une machine virtuelle d'un hyperviseur. pfSense est également très léger ; un processeur à un seul coeur et 256 MB de RAM sont requis dans sa configuration minimale. Toutefois, ces deux critères varient en fonction de la vitesse désirée (*throughput*). Plus le débit souhaité entre la portion LAN et la portion WAN est grand, plus la vitesse du processeur doit être élevée. On recommande entre 512 MB et 1 GB de mémoire vive. De la RAM ECC est recommandé comme dans toute installation d'un serveur puisqu'elle procure une meilleure stabilité du système. L'ajout d'un VPN au système joue également un rôle dans la configuration matérielle. Il faut considérer un processeur plus rapide pour gérer le cryptage et le décryptage des données envoyées et reçues par l'interface WAN. Avoir de bons adaptateurs réseau est crucial avec pfSense si l'on veut garder de bonnes performances réseau. Les adaptateurs Intel figurent parmi les meilleures du marché et sont compatibles avec FreeBSD. Intel offre la solution la plus stable avec pfSense.

---

[2] http://www.tecmint.com/open-source-security-firewalls-for-linux-systems/

Nous avons décidé d'installer pfSense dans une machine virtuelle sur notre serveur de virtualisation ESXi. Nous voulions essayer ce système qui est très performant et dédié à l'usage d'un pare-feu au lieu d'utiliser Red Hat Enterprise Linux/CentOS pour jouer le rôle de routeur. Nous avons remarqué que le temps de mise en place de pfSense est ridiculement rapide. En moins de 30 minutes, nous avions une machine virtuelle pfSense configurée et prête à jouer le rôle de pare-feu dans un environnement de production, alors que d'autres équipes n'avaient toujours pas réussi à faire fonctionner FirewallBuilder en plusieurs heures. pfSense rend l'implantation d'un pare-feu et d'une multitude de services très efficace et devrait être proposé rapidement dans le cadre du cours puisqu'il constitue un standard grandissant dans l'industrie de la sécurité informatique. Pour se procurer pfSense, se rendre au https://www.pfsense.org/download/mirror.php?section=downloads.

Toutefois, pour mener à bien le projet, il nous a fallu installer un pilote dans notre serveur. En effet, les machines HP sur lesquelles le projet fut réalisé disposent d'une seule carte LAN de marque Intel la deuxième étant une carte LAN Realtek 8168. Cela ne pose pas un très grand problème puisque des pilotes programmés expressément pour ESXi existent pour les cartes LAN Realtek. Le fichier du pilote a été ajouté sur le serveur du département à l'adresse réseau suivante : \\cdom\TGE\Projet VMware ESXi\ESXi.

Implanter un pilote LAN dans un serveur ESXi - Guide étape par étape

1. Téléchargez le pilote et transférez le fichier dans le *datastore* du serveur ESXi.

2. Assurez-vous que la prise en charge SSH est bien activée dans le serveur ESXi.

3. Connectez-vous par protocole SSH au serveur ESXi. Sur Windows, utilisez Putty. Sur Mac OS X/Linux, le terminal UNIX est recommandé.

4. Entrez la commande suivante :

esxcli software vib install -v /vmfs/volumes/**driver_directory_in_datastore**/VMware_bootbank_net-r816**X**_6.011.00-2vmw.510.0.0.799733.vib

Où :

- **driver_directory_in_datastore** représente le dossier dans le *datastore* où le pilote a été transféré.

- **X** représente le numéro de modèle de la carte Realtek, par exemple 816**8** ou 816**9**

4. Redémarrez le serveur ESXi.

5. Pour vérifier si le VIB a été installé correctement, faites la commande :

```
esxcli software vib list
```

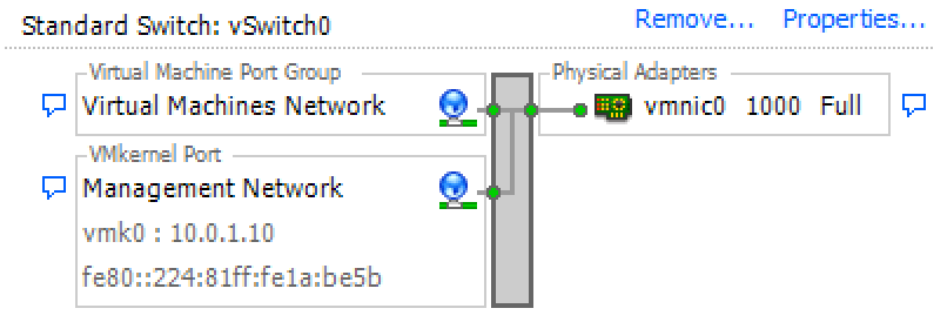
Installer pfSense dans une machine virtuelle - Guide étape par étape

pfSense sera installé dans une machine virtuelle qui jouera le rôle de routeur. Le concept est quelque peu ambitieux, mais parfaitement réalisable. Toutefois, certains administrateurs de réseaux d'entreprises préfèrent installer pfSense sur un serveur physique dédié afin de limite la surface d'attaque. Cette idée est plausible et sensée, mais plus coûteuse que la solution virtualisée.

Les descriptions suivantes se passeront dans la section **Configuration -> Networking** de vSphere Client.

Sur une installation fraîche de VMware ESXi, le serveur dispose d'une seule vSwitch, soit le vSwitch0, sur laquelle on retrouve un adaptateur LAN physique vmnic0, le VMKernel Port ainsi que le Virtual Machine Port Group.

ESXi nomme la première interface physique vmnic0. C'est cette interface qui sera automatiquement attribuée au réseau d'administration (*management network*). Le VMKernel Port est tout simplement l'interface réseau avec laquelle vSphere Client administre l'hôte ESXi.



En plus du VMKernel Port, ESXi attribue automatiquement à la vSwitch0 les machines virtuelles. Ces dernières seront attachées au port Virtual Machine Network.

La machine virtuelle que nous allons construire joue le rôle de routeur. Un routeur a toujours une interface d'entrée LAN et une interface de sortie WAN. Or, l'installation par défaut d'ESXi ne nous propose qu'une seule vSwitch et alors qu'un seul réseau. Il faut alors créer un LAN.

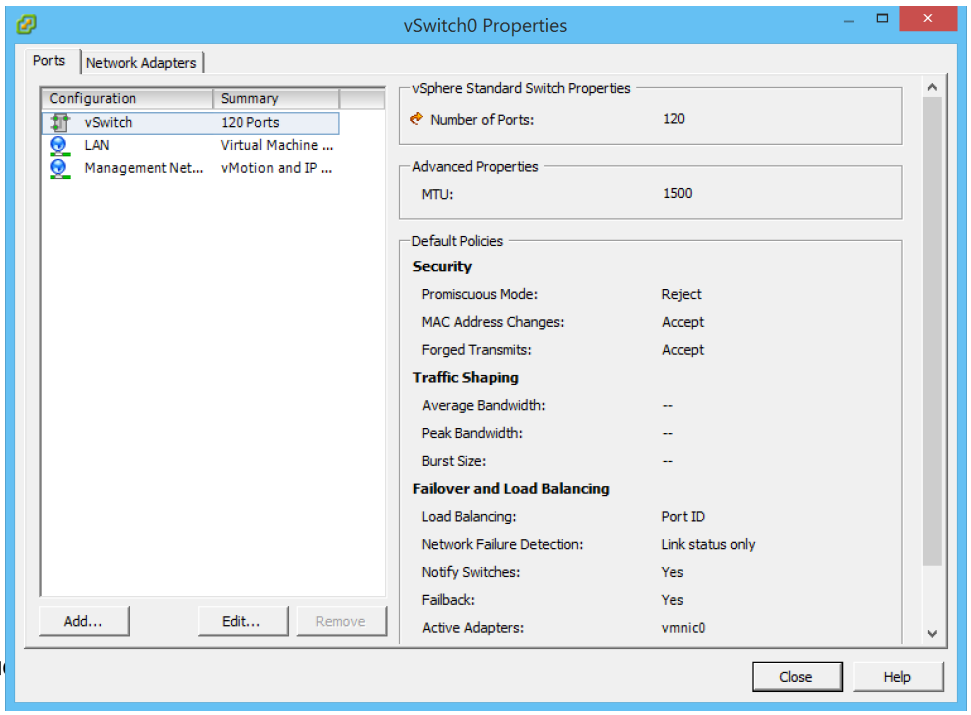
Dans un petit réseau, il est très commun d'utiliser le Virtual Machine Port Group de la vSwitch0 pour donner la connectivité LAN à pfSense. Ceci procure un accès LAN à la machine virtuelle pfSense et procure par le fait même une connectivité pour administrer l'hôte ESXi avec vSphere Client. Bien sûr, il faudra que la machine virtuelle pfSense ait une adresse IP LAN différente que celle de l'hôte ESXi.

Commentaire : Il est toujours conseillé de séparer complètement l'administration de ESXi et le réseau local. Pour ce faire, on place l'hôte ESXi sur un sous-réseau différent de celui du LAN. On peut faire une telle chose en mettant en place des VLANs, ou tout simplement en ajoutant une troisième interface réseau à l'hôte ESXi et en la dédiant uniquement à l'administration. Cela amène des coûts supplémentaires, mais permet de ségréguer l'utilisation des ports physiques du serveur. Mettre l'administration du serveur sur son propre sous-réseau permet une meilleure sécurité puisque ce dernier ne sera pas accessible à partir du LAN.

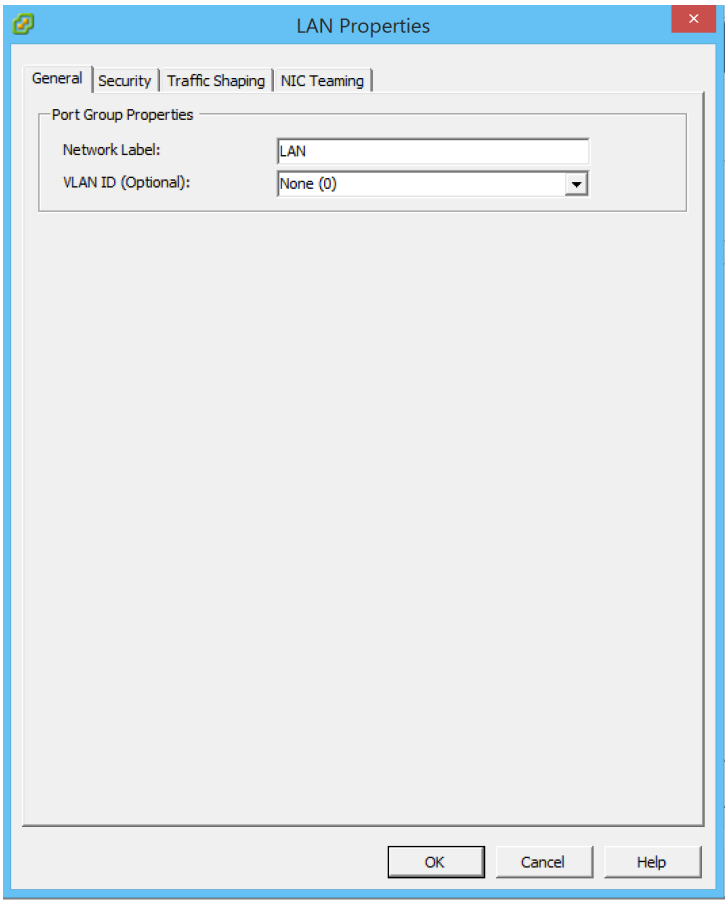
Nous prendrons en considération que nous ne travaillerons qu'avec deux interfaces réseau puisque la machine HP fournie pour le projet ne dispose que de deux cartes.

On renomme donc le Virtual Machine Port Group pour LAN. Cela clarifiera les explications qui suivront. Cliquez sur **Properties** à droite de vSwitch0.

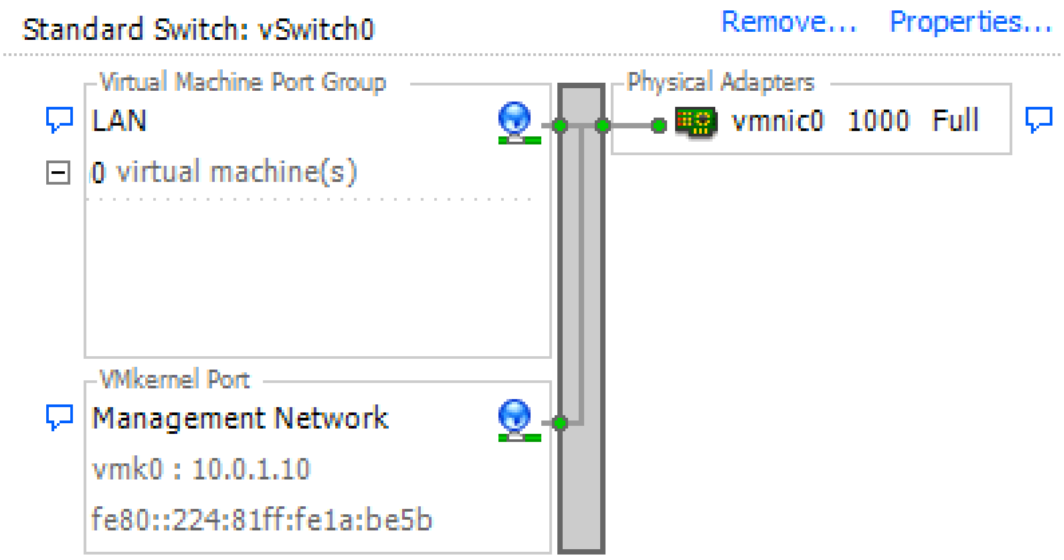
Cliquez sur Virtual Machine Network et cliquez sur **Edit**.



Renommez le *Network Label* pour **LAN**. Cliquez sur **OK**, puis sur **Close** de la fenêtre précédente.



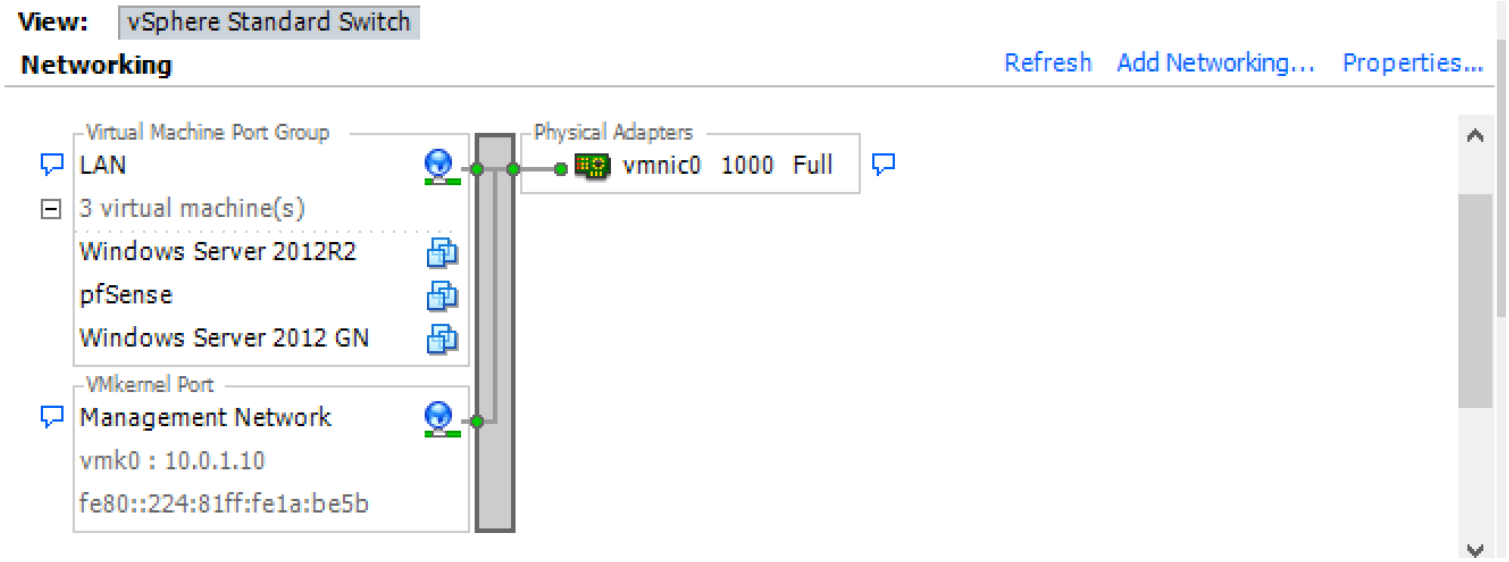
On devrait par la suite avoir un tel schéma réseau.

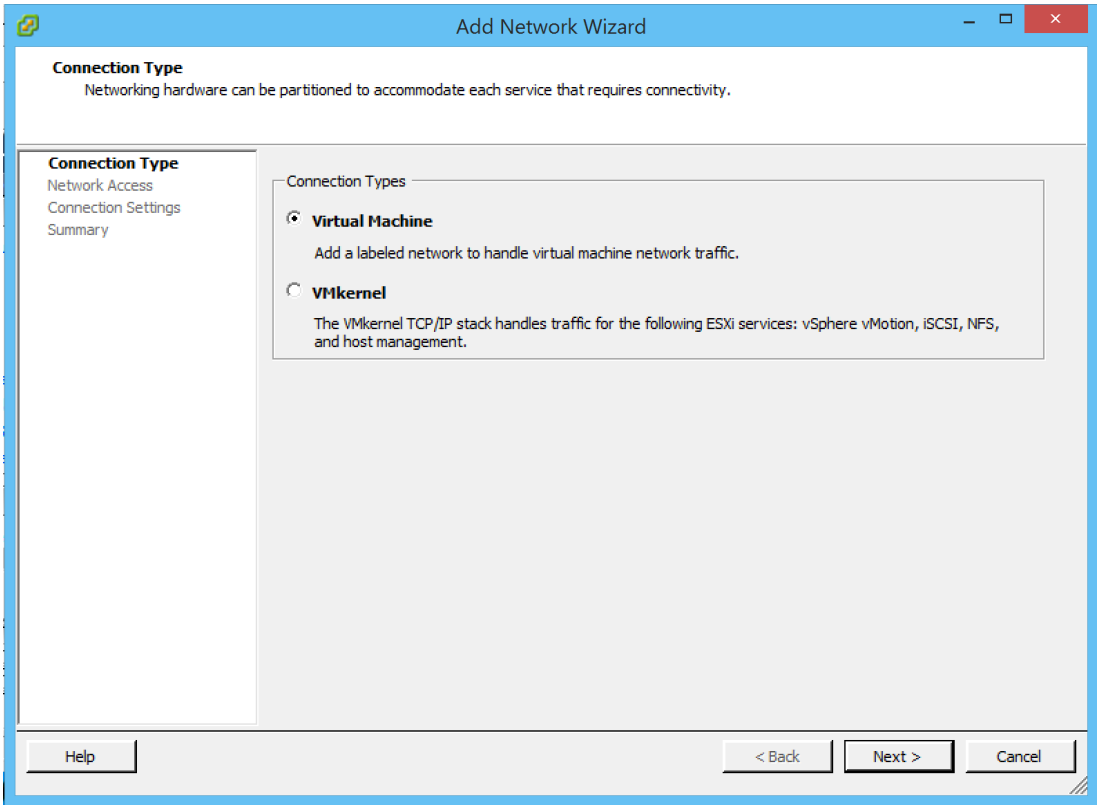


Vient ensuite la création d'une interface WAN. Pour ce faire, il faudra ajouter la seconde carte LAN dans le serveur si ce n'est pas déjà fait.

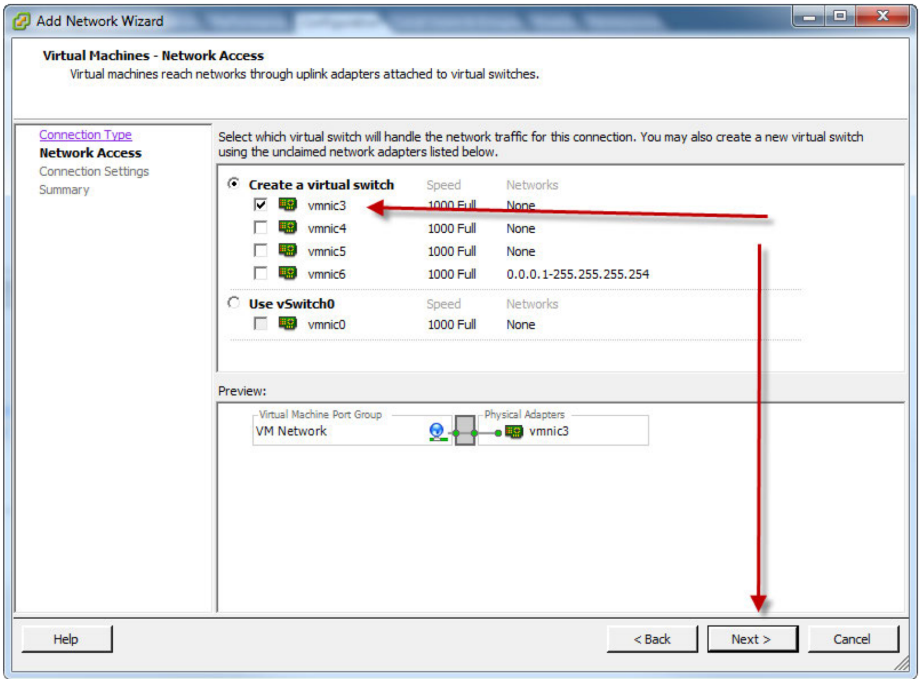
Astuce : Si l'on a plusieurs NIC installés dans le serveur, on peut rapidement s'y perdre. VMware ESXi nomme seulement les cartes réseau par vmmicX, où "X" est le numéro d'identification du vmnic. Il serait très intéressant de bien documenter le réseau et d'identifier les adresses MAC de chaque interface réseau. Pour voir les adresses MAC de chaque carte réseau, il suffit d'aller dans Configuration -> Network Adapters.

Il faut par la suite ajouter une nouvelle vSwitch qui figurera comme étant l'interface WAN. Pour ce faire, il suffit de cliquer sur **Add Networking.** La boîte de dialogue suivante apparaîtra. Cocher la case **Virtual Machine.**

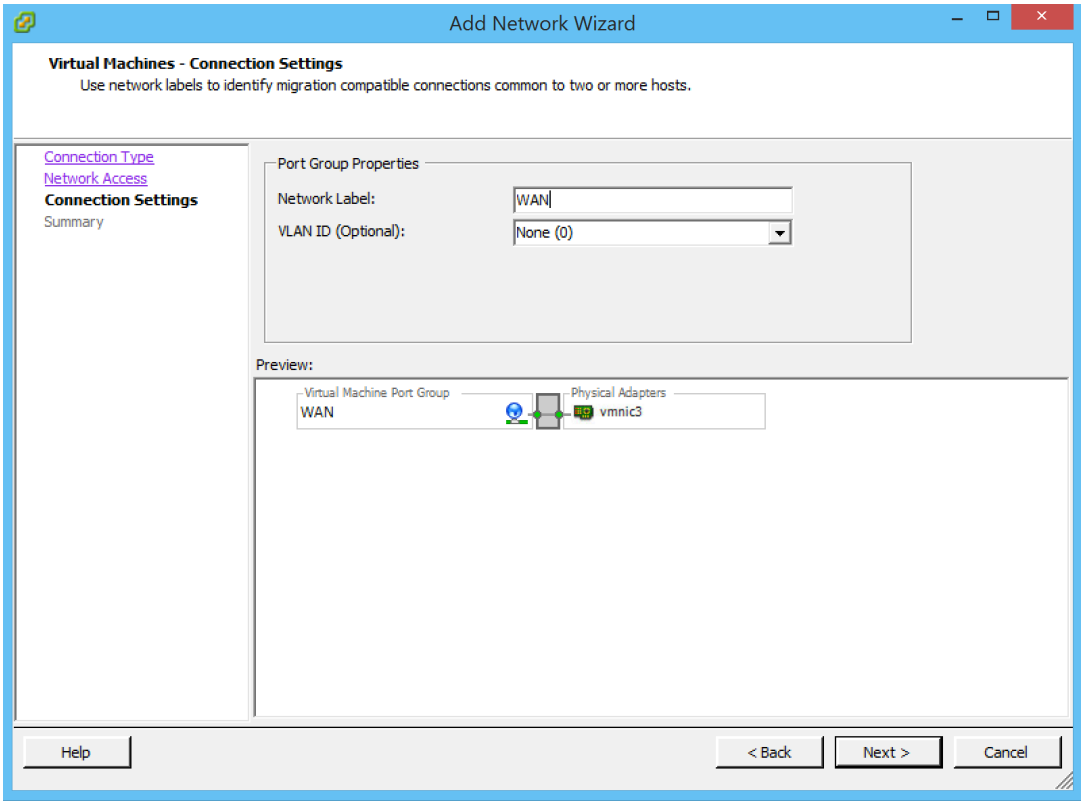




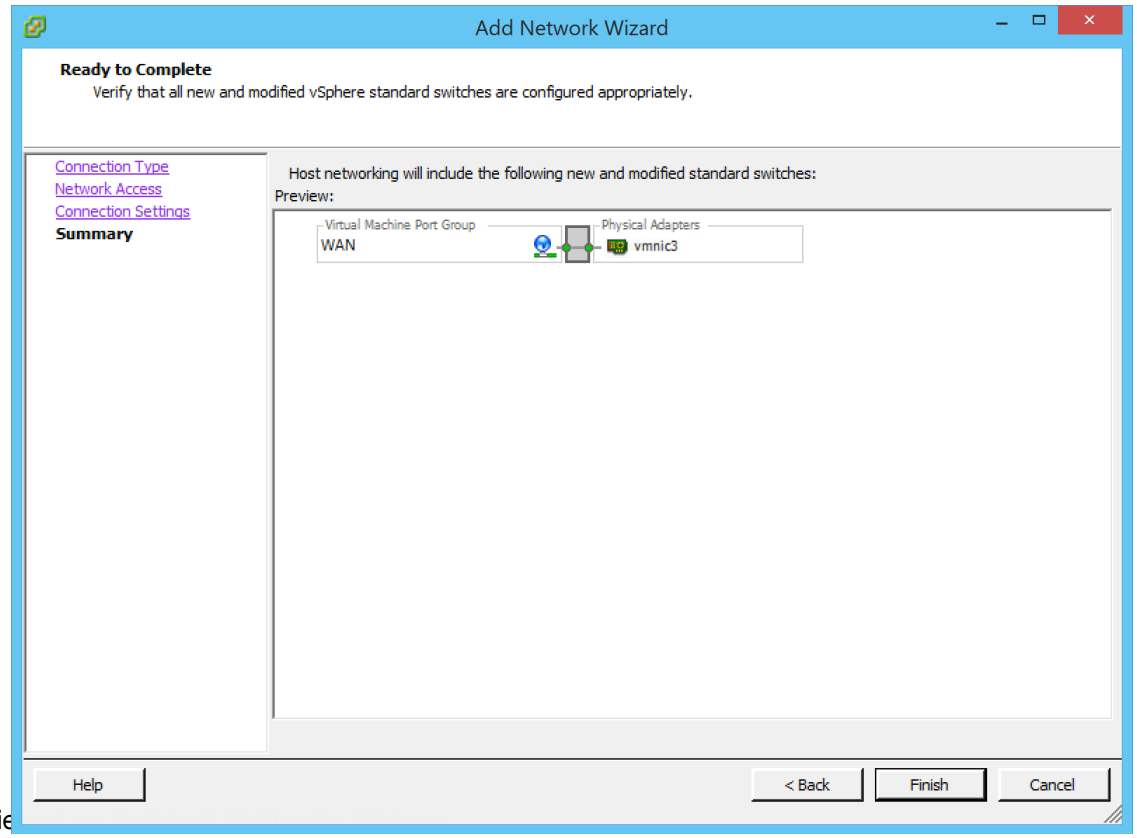
Nous voulons qu'une interface physique soit reliée à cette nouvelle vSwitch. Il faut donc sélectionner **Create a virtual switch** et cocher le vmnic souhaité. Appuyez ensuite sur **Next**.



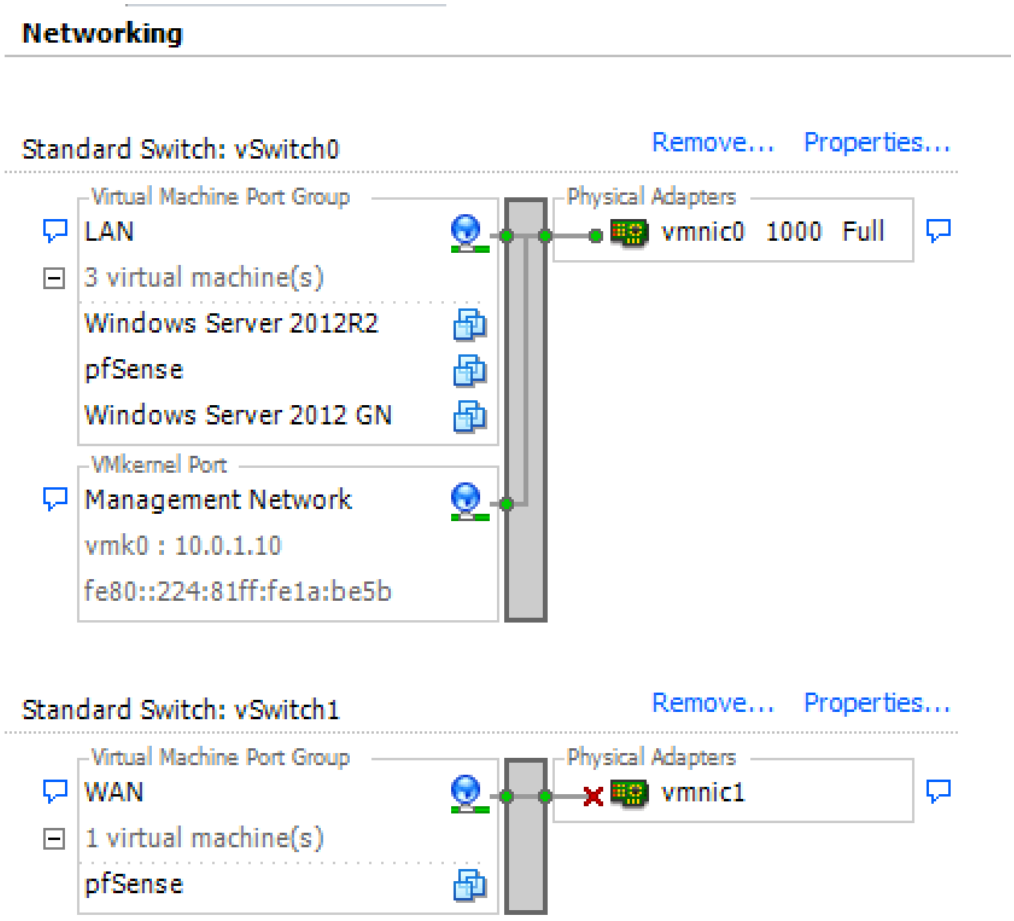
Donnez le label **WAN** au *Port Group.* Appuyez ensuite sur **Next**.



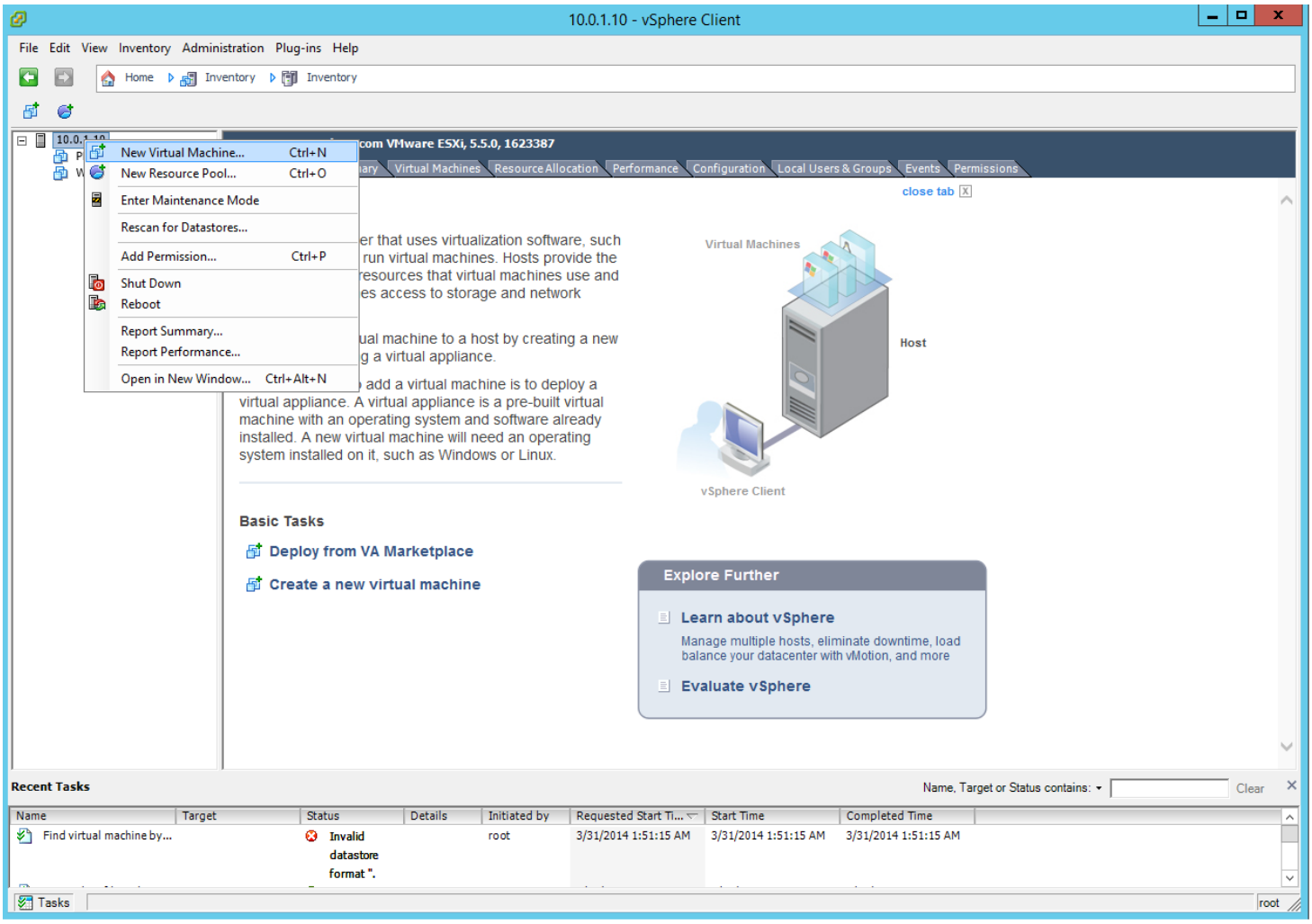
Cliquez ensuite sur **Finish.**



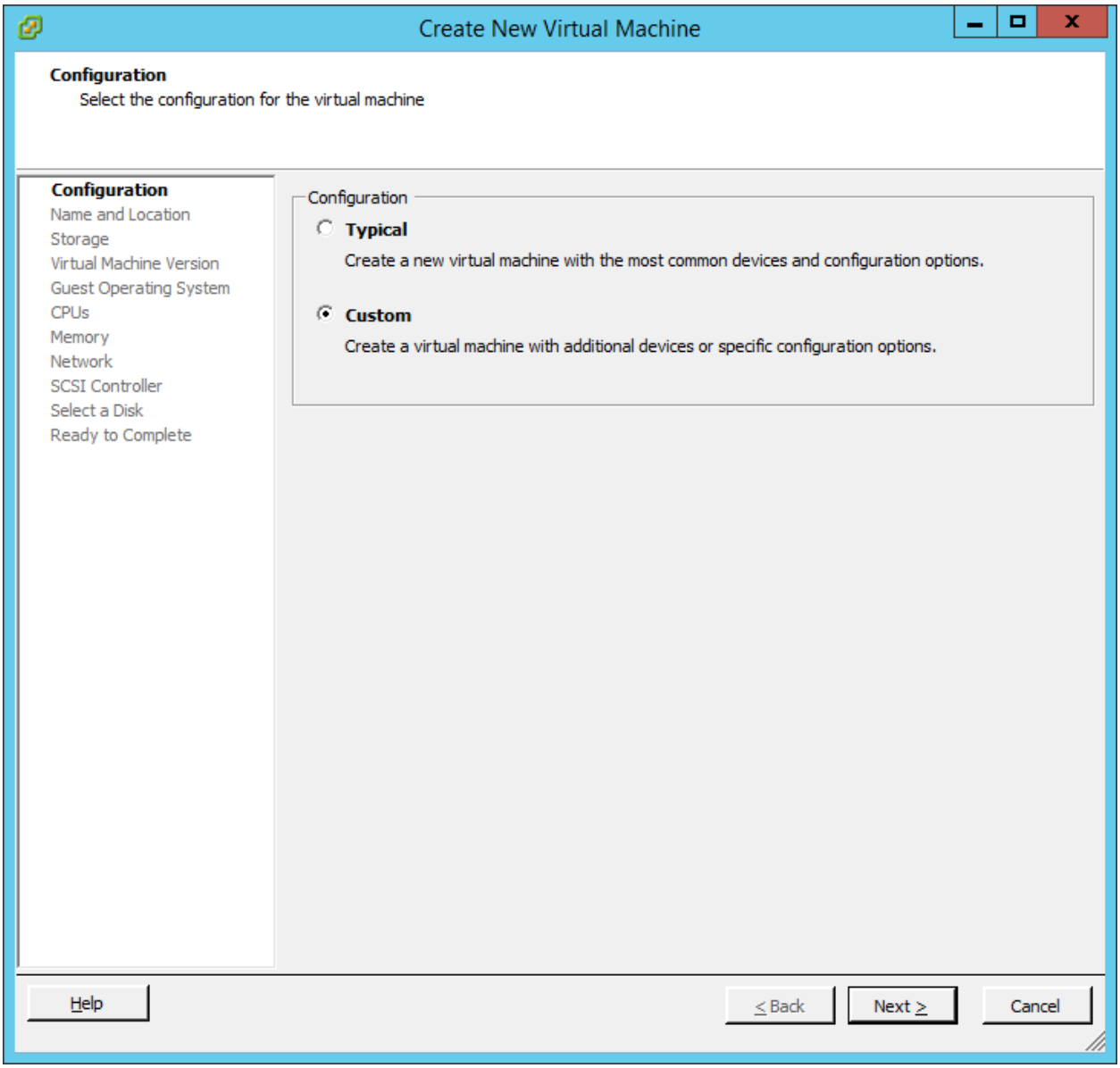
Le schéma réseau devrait ressembler à ceci.



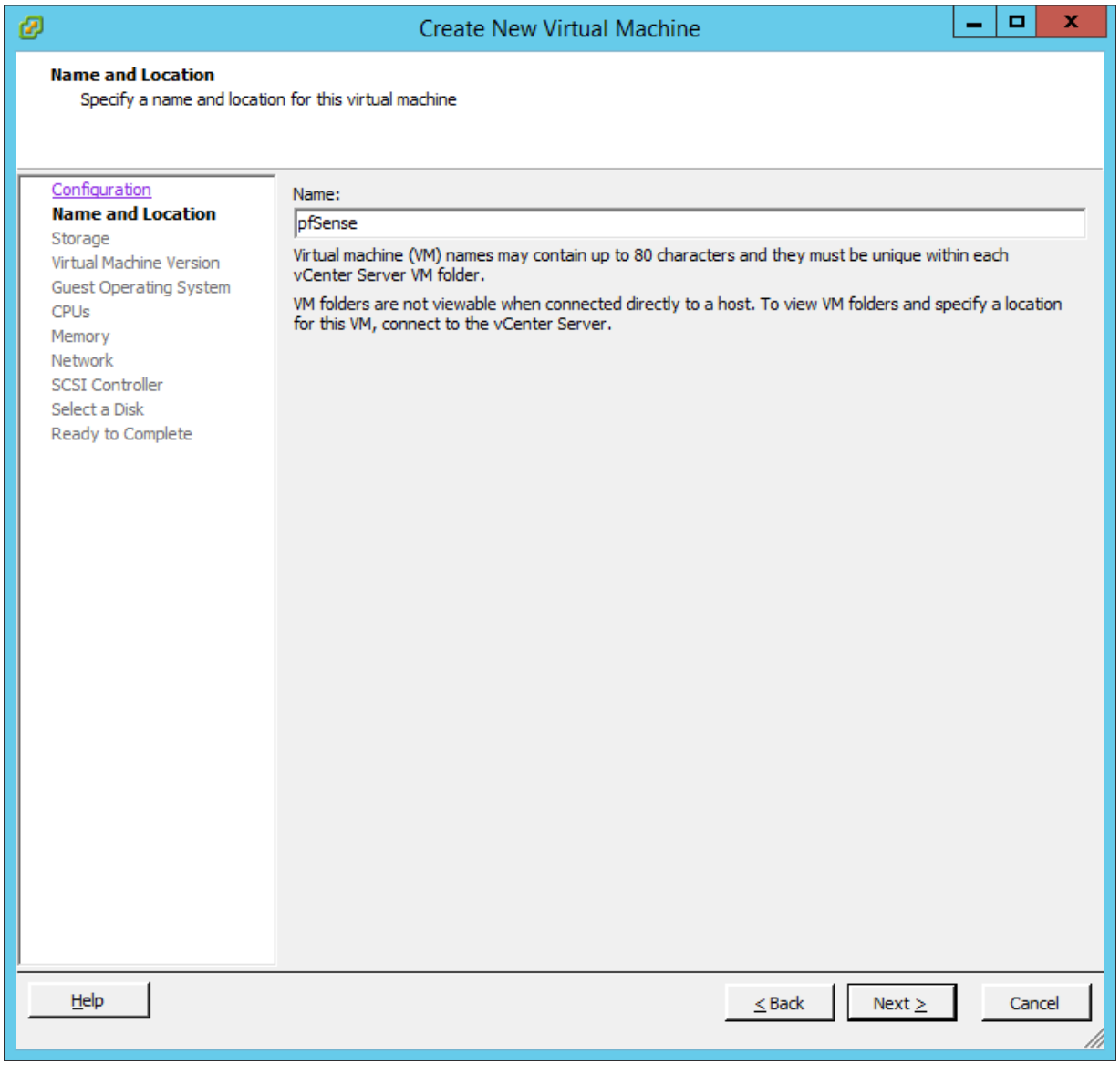
Puisque les deux vSwitch WAN et LAN sont créées, il nous reste à créer la machine virtuelle dédiée à pfSense. Pour se faire, on clique-droit sur l'hôte ESXi dans le volet de droite puis on sélectionne **New virtual machine…**



La machine virtuelle sera de type **Custom**.

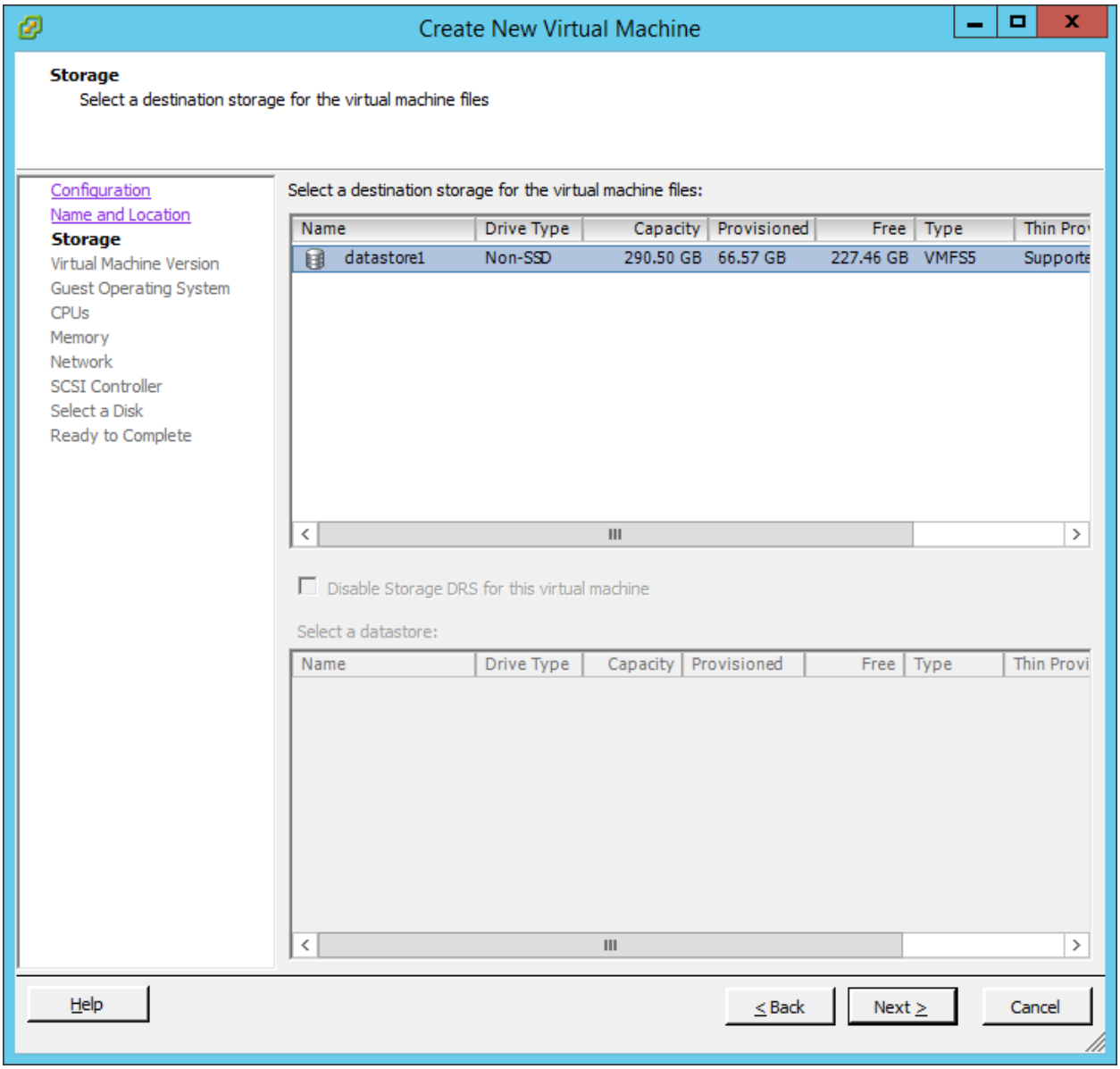


Donner le nom de pfSense à la machine virtuelle.



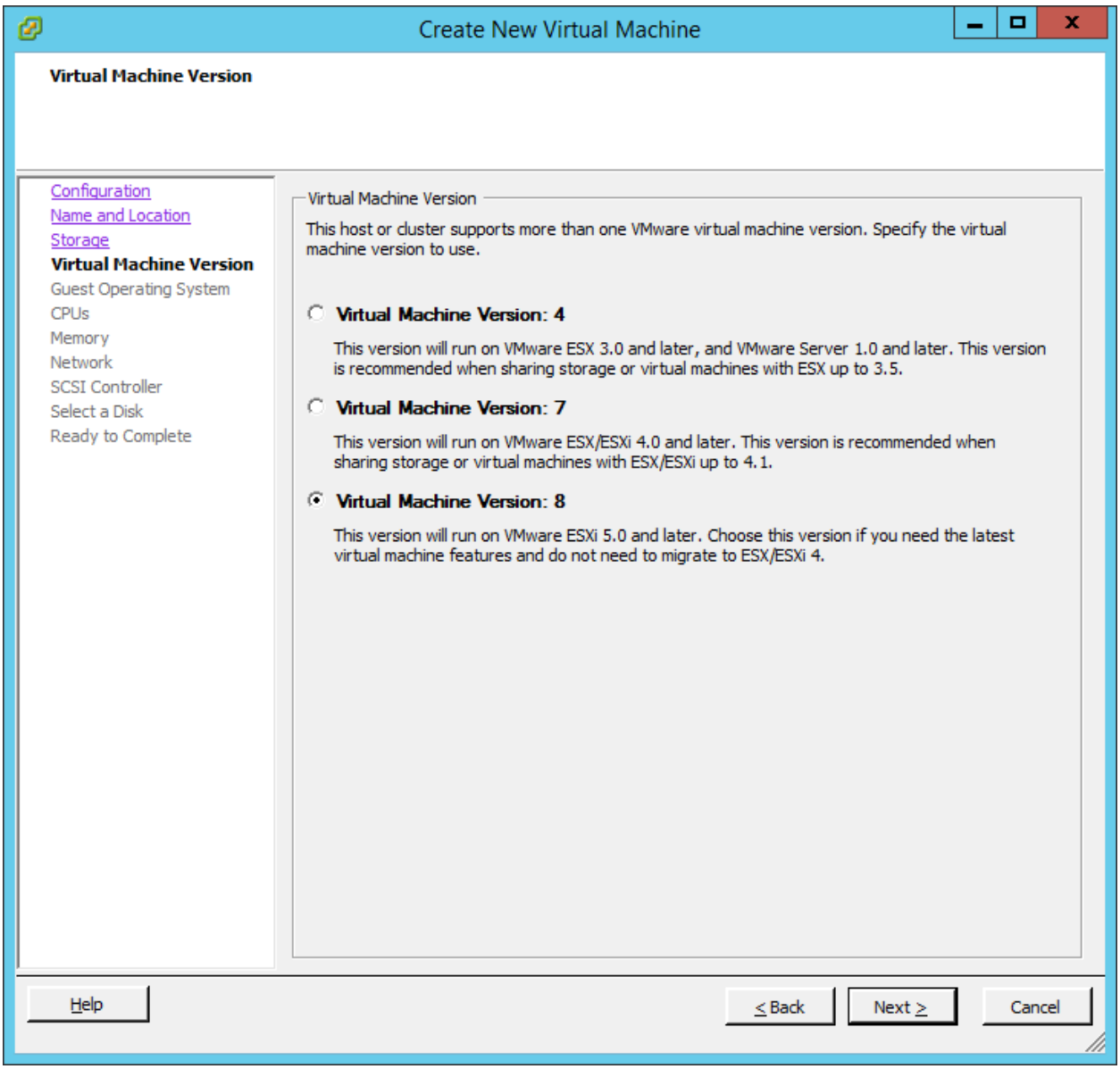
Au niveau du stockage de machine virtuelle, on sélectionne le *datastore* dans lequel on souhaite installer la machine virtuelle de pfSense. Normalement, dans l'image ci-dessous, il y a deux *datastore*. Un petit disque dans lequel ESXi est installé, puis un autre disque plus gros dans lequel les machines virtuelles sont stockées. Nous aurions pu également configurer ESXi pour nous connecter à une *iSCSI target* sur un SAN distant sur le réseau. Toutefois, l'équipement dans le laboratoire ne nous permettait pas de faire une telle chose puisque les commutateurs Cisco 2960 dans le local n'ont que des ports FastEthernet, ce qui aurait rendu à néant les performances des machines virtuelles. Nous n'avons qu'un seul *datastore* puisque nous n'avions qu'un seul disque dur fourni.

Sélectionnez le *datastore* désiré puis appuyer sur **Next.**

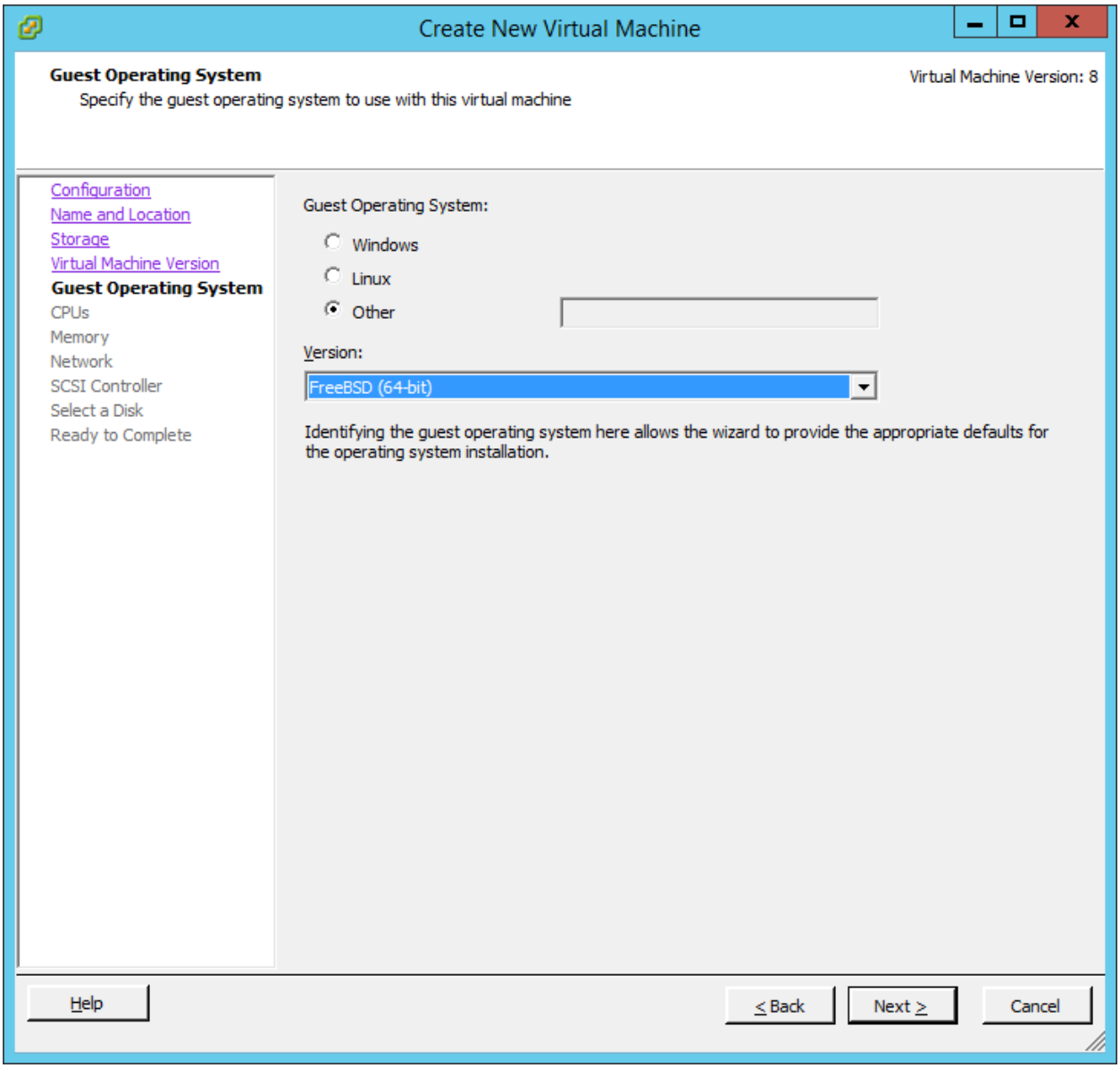


Sélectionnez la version de la machine virtuelle et appuyez sur **Next**.

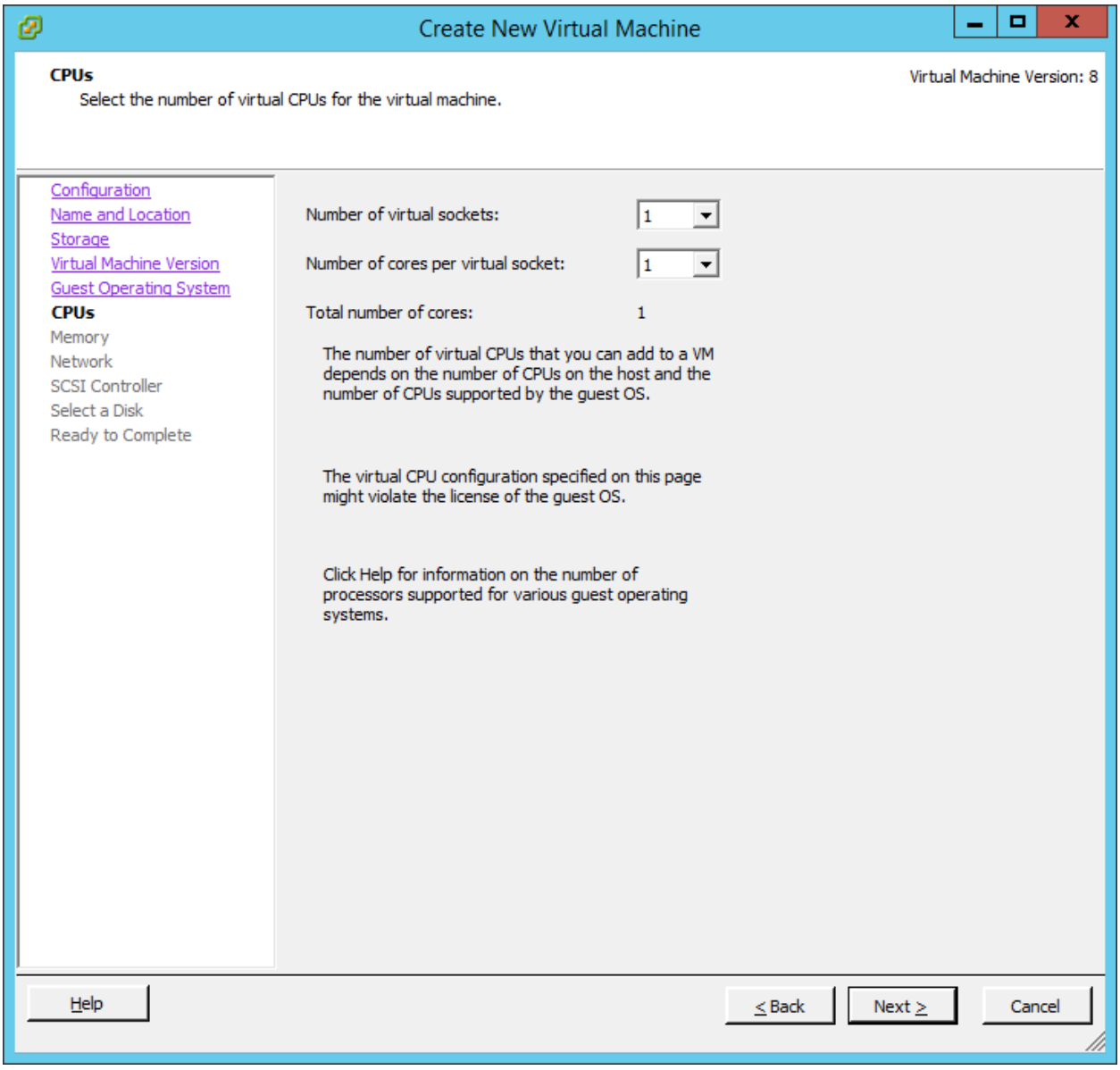
Note : Virtual Machine Version 10 est la version de matériel par défaut de ESXi 5.5 Update 1. Toutefois, vSphere Client ne pourra pas éditer les réglages de la machine virtuelle si elle a du matériel de version 10. Il faudra passer par VMware Workstation et se connecter au serveur ESXi ou passer par le service Web de ESXi. Les deux solutions sont payantes. Si vous voulez garder la solution gratuite, veuillez sélectionner Virtual Machine Version 8.



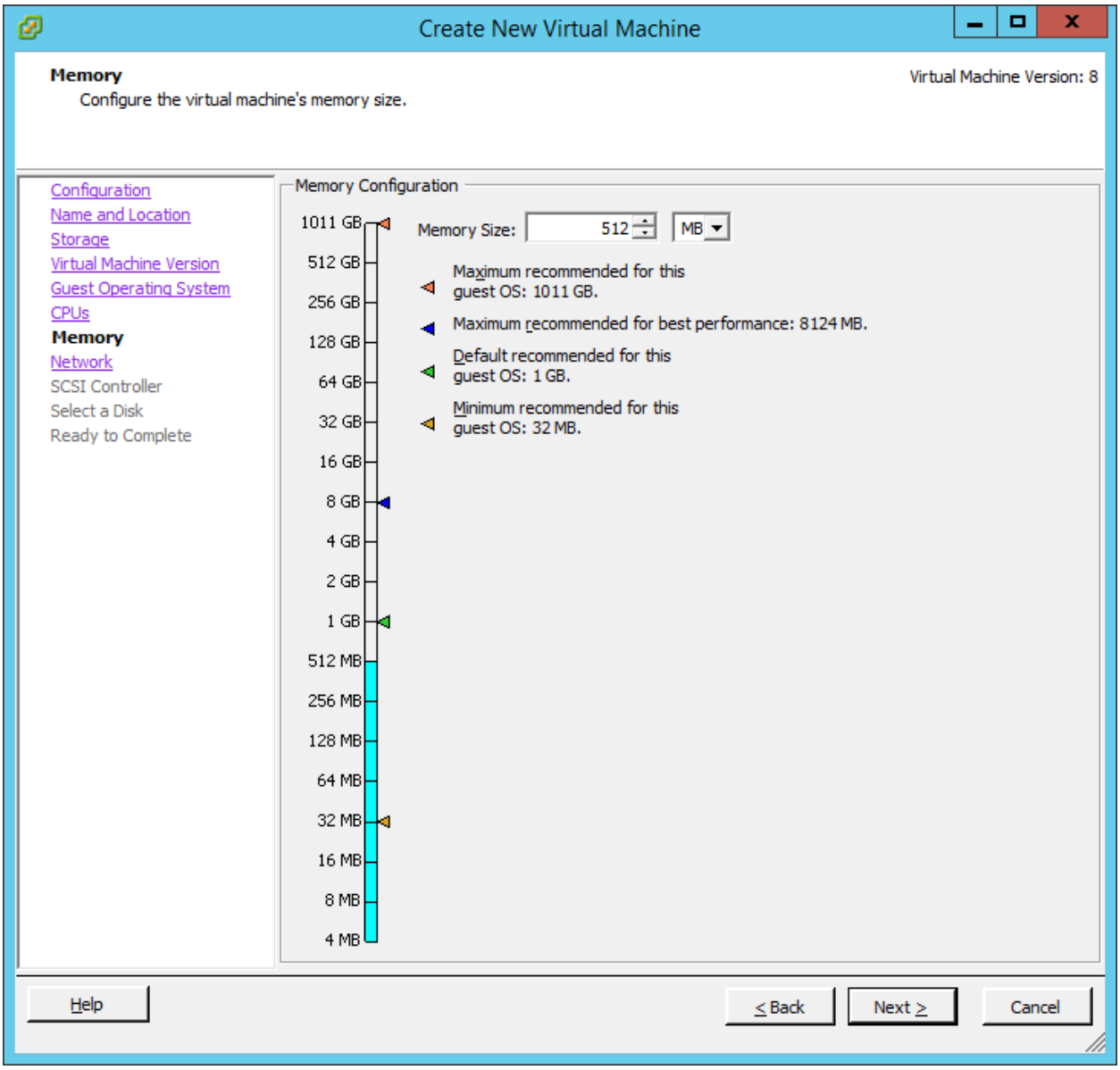
Sélectionnez le type de la machine virtuelle. Cochez **Other** et sélectionnez **FreeBSD 32 ou 64 bit**, selon la version de pfSense téléchargée.



Sélectionnez le nombre de CPU et le nombre de coeurs d'exécution attribuée à la machine virtuelle. Un seul CPU et un seul coeur suffisent pour les besoins du projet.



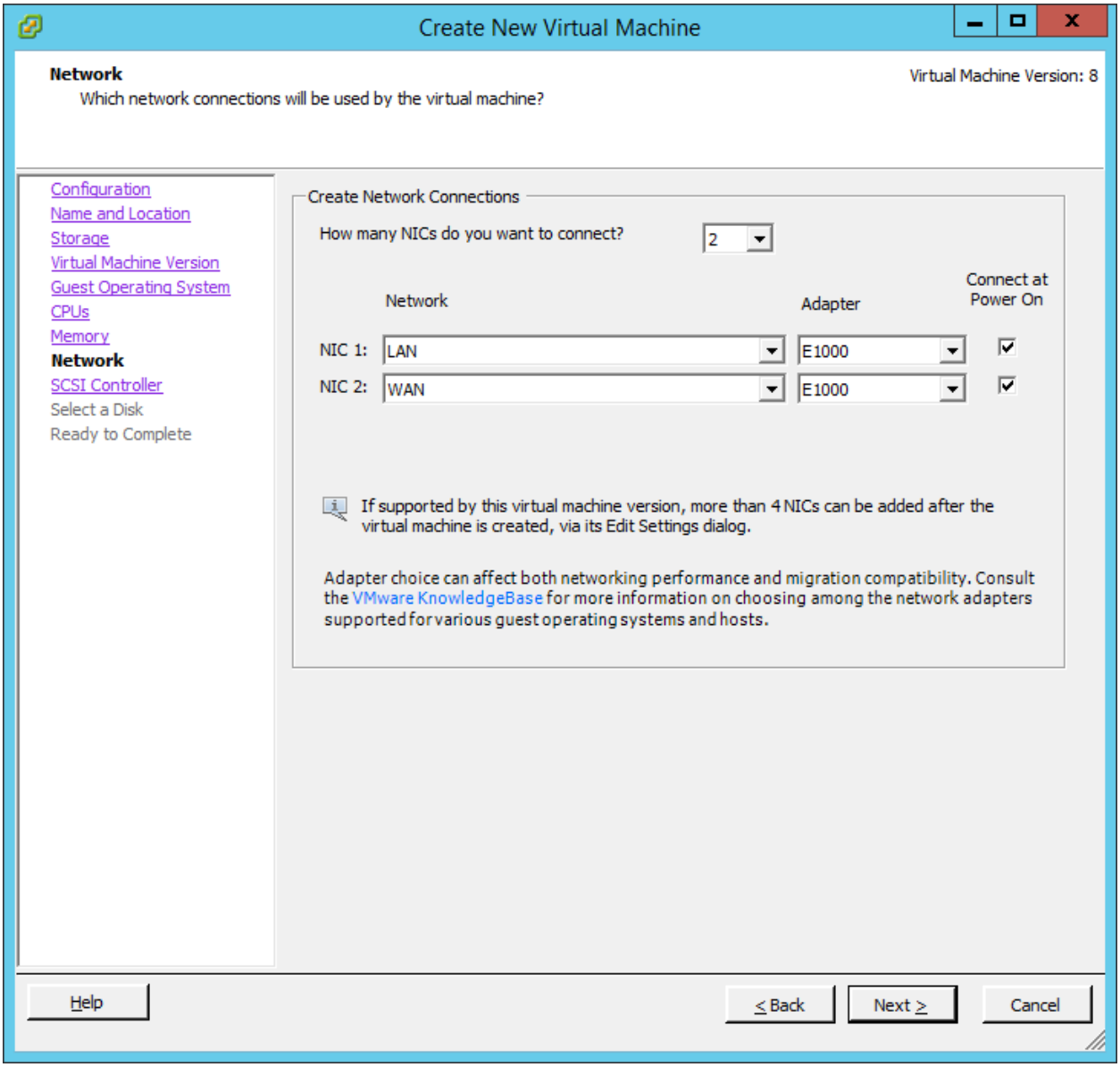
Sélectionnez la quantité de RAM mise à la disposition de la machine virtuelle. Ici, 512 MB seront suffisants.



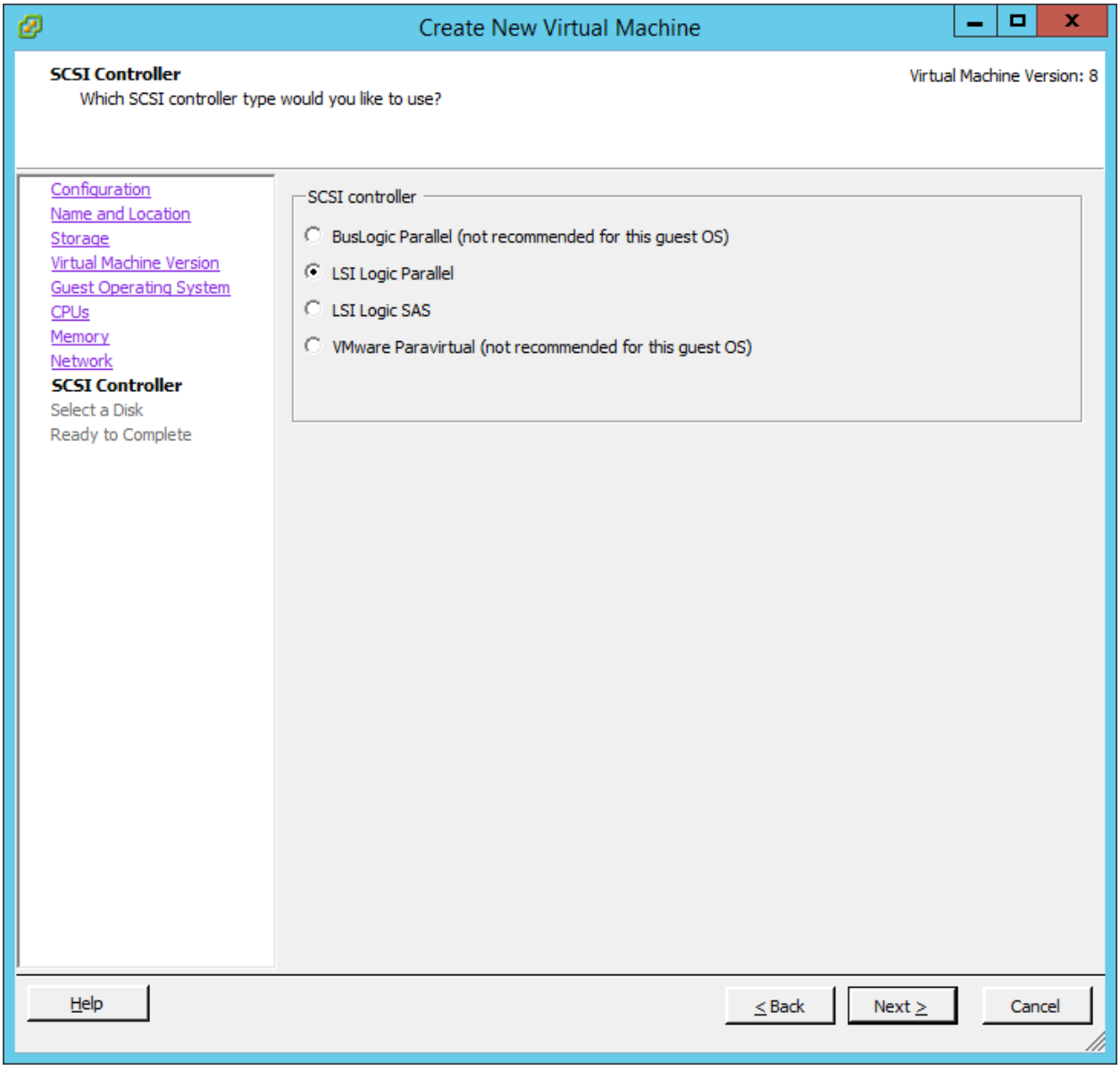
Sélectionnez le nombre d'adaptateurs réseau passés à la machine virtuelle.

- Vis-à-vis **How manu NICs do you want to connect ?** , sélectionnez **2.**
- La première interface se nommera LAN alors que la seconde se nommera WAN.
- Choisissez **E1000** comme type d'adaptateur.
- Assurez-vous que les cases **Connect at Power On** sont cochées.

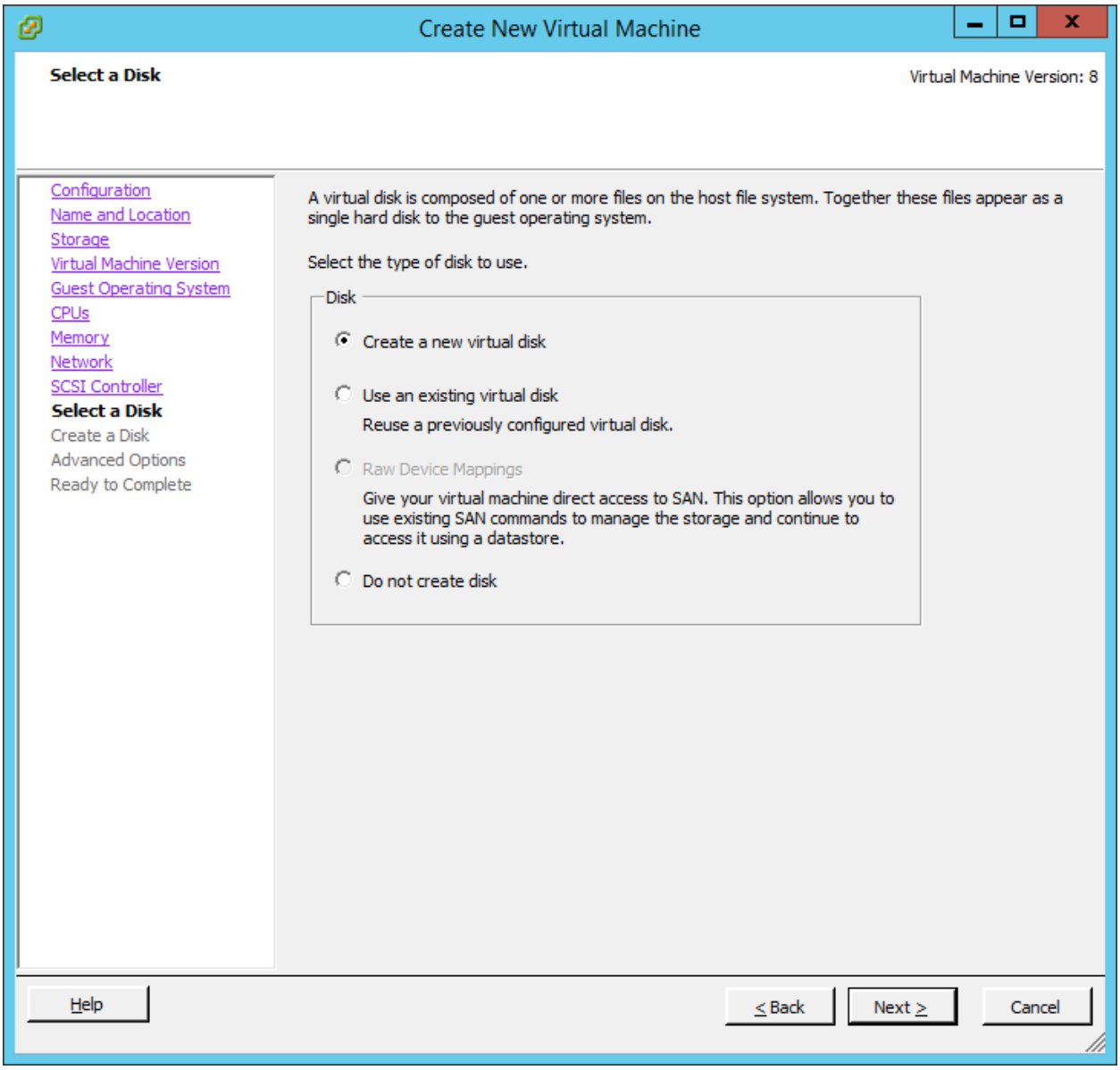
Appuyez ensuite sur **Next.**



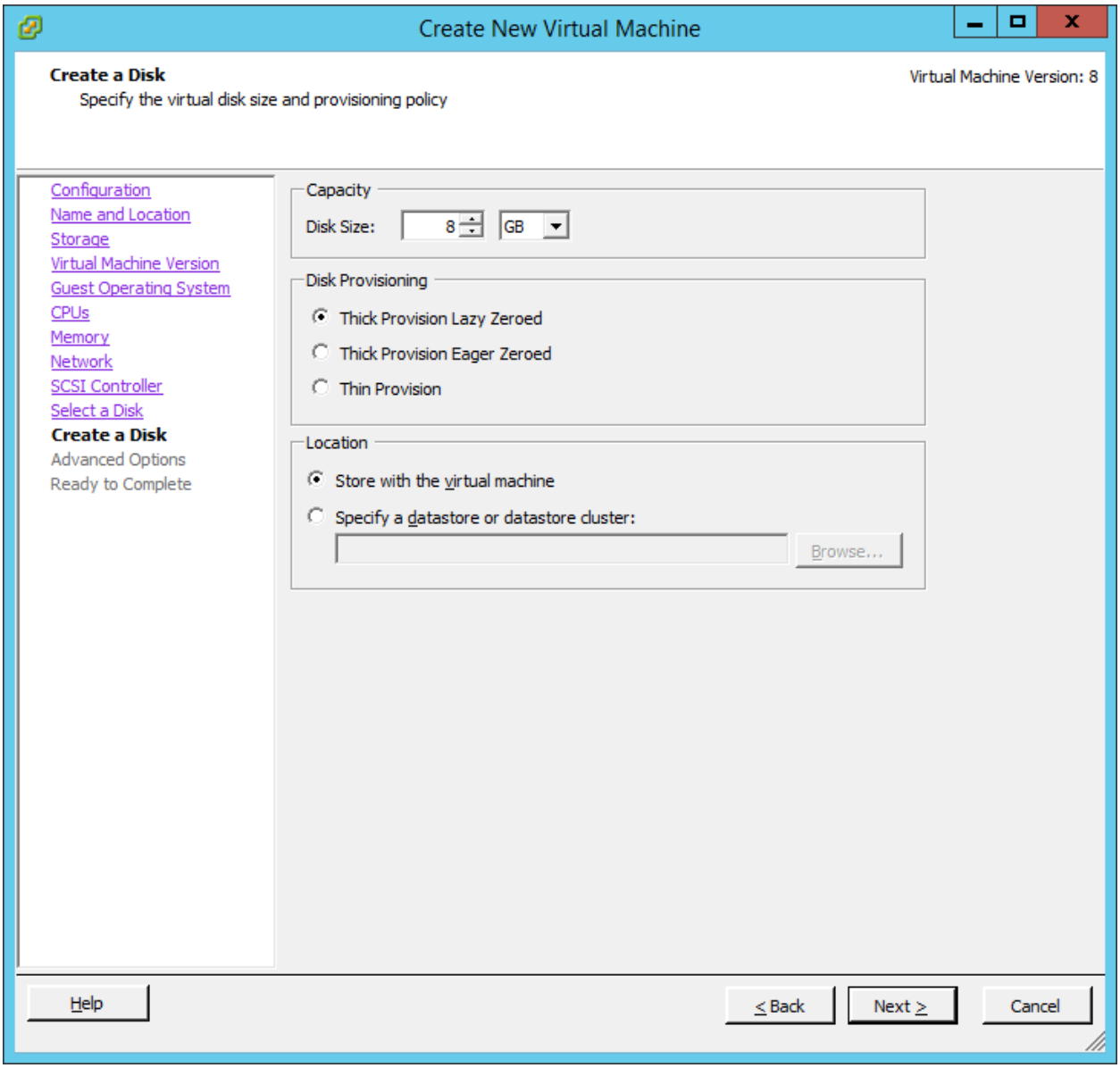
Choisissez **LSI Logic Parallel** comme contrôleur SCSI, puis cliquer sur **Next**.



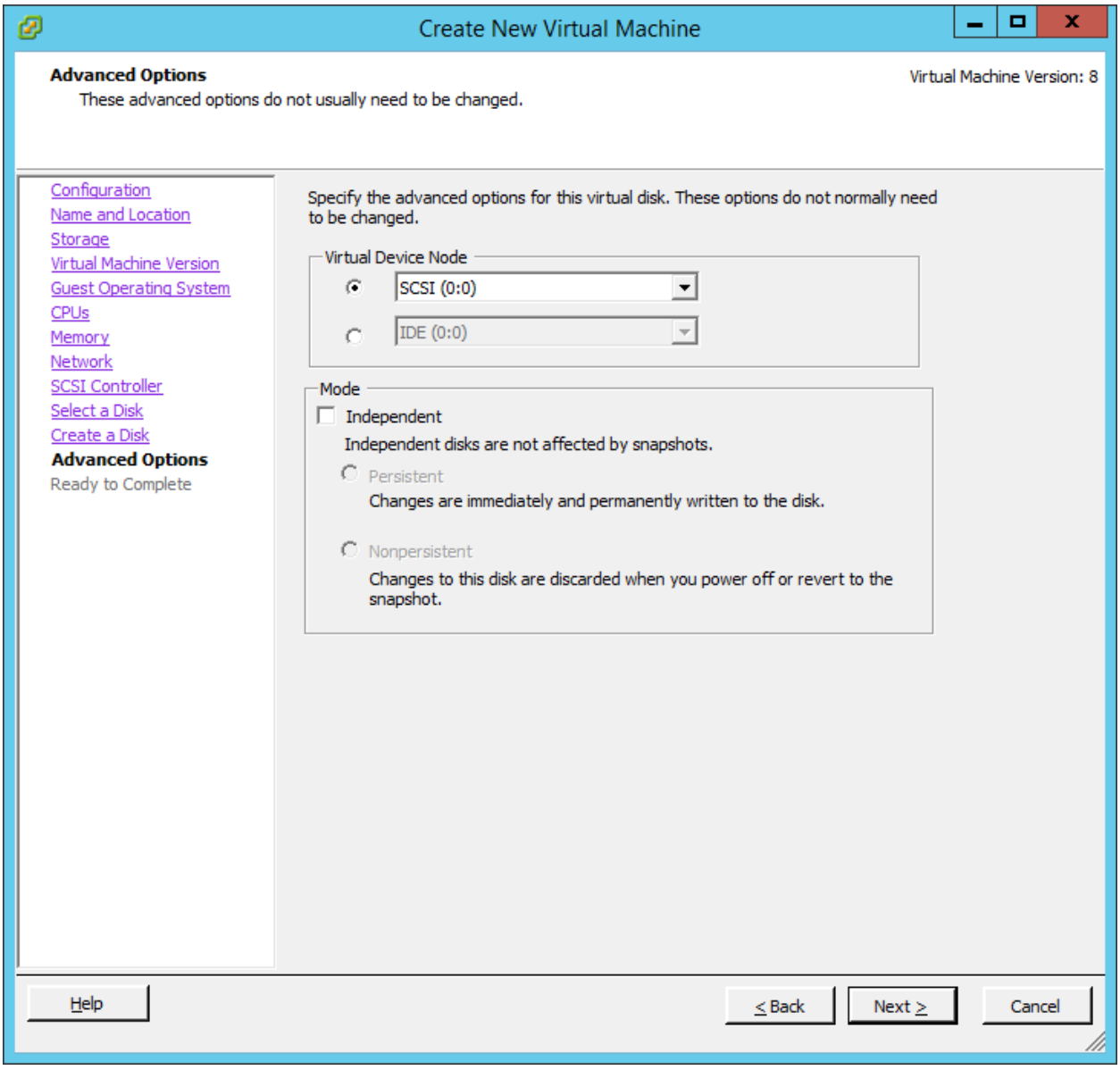
Créez un nouveau disque virtuel pour cette machine virtuelle. Cochez la case **Create a new virtual disk** et cliquez sur **Next.**



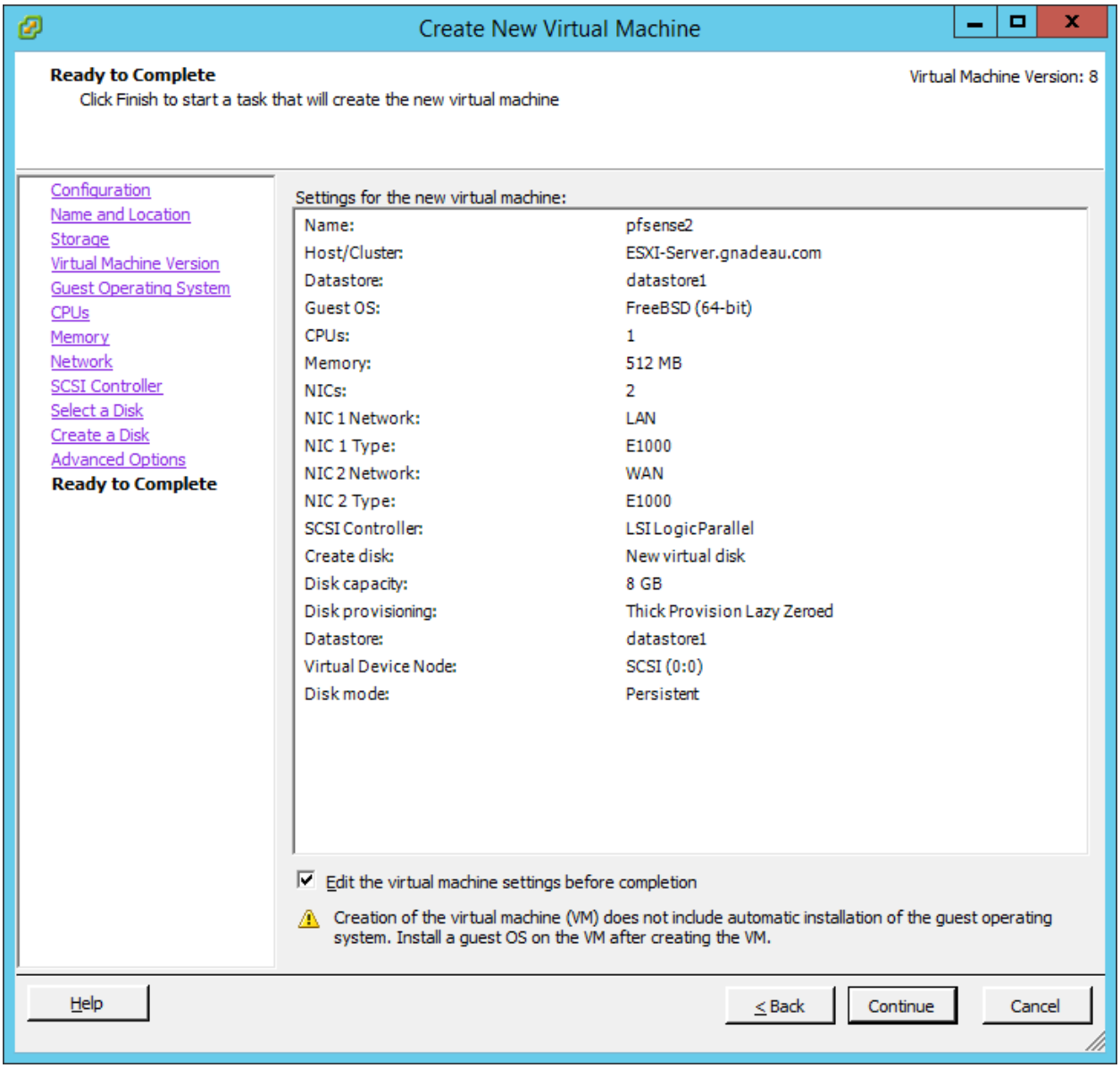
Définissez la grosseur du disque dur virtuel. Pour pfSense, **8 GB** suffisent amplement, à moins de vouloir lui greffer plusieurs packages de source tierce. Cliquez sur **Next**.



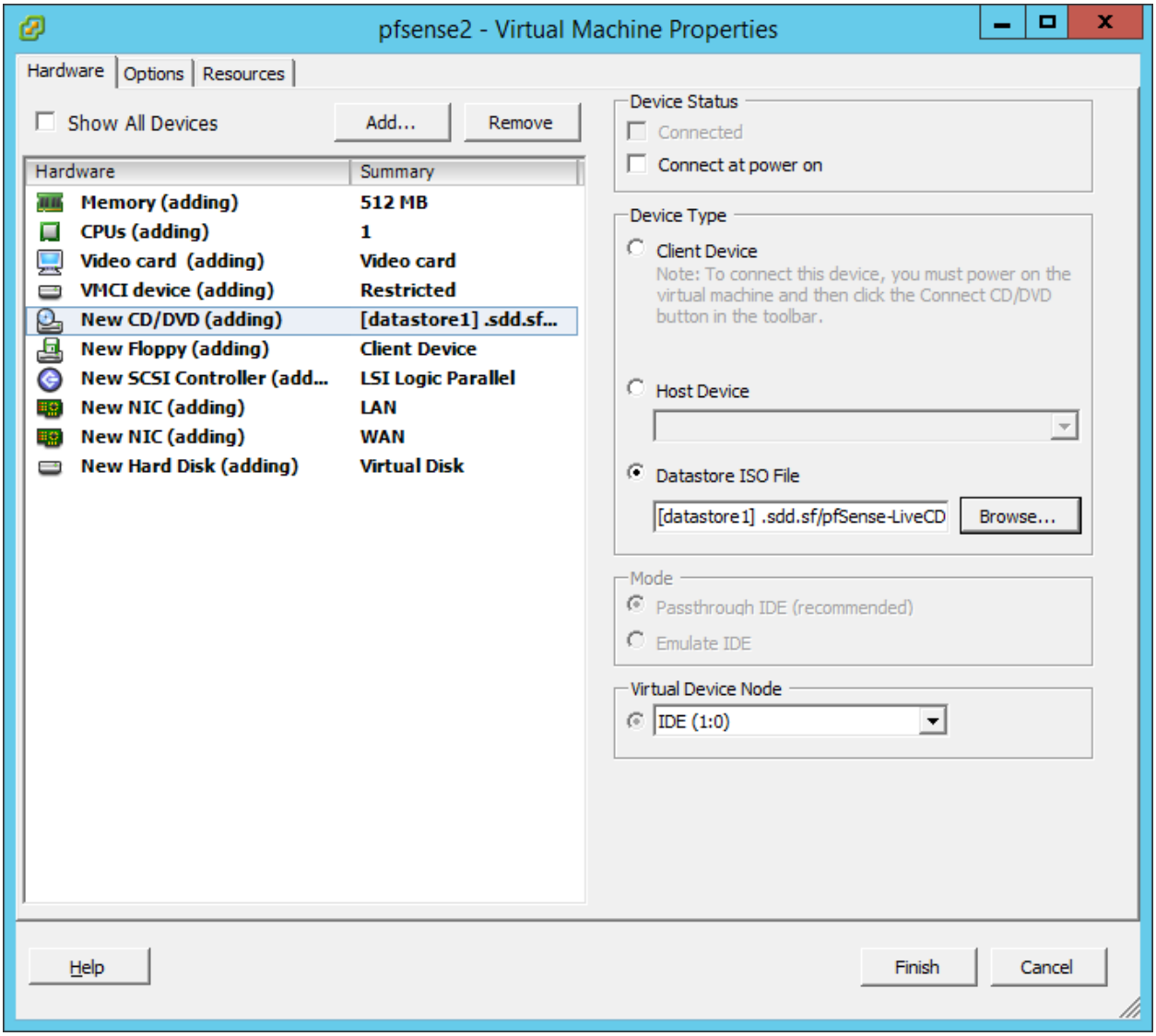
Dans la fenêtre **Advanced Options**, il est inutile de modifier quoi que ce soit.



La machine virtuelle est désormais prête à être créée. Cochez la case **Edit the virtual machine settings before completion** et cliquez sur **Finish**.



La fenêtre d'édition des réglages de la machine virtuelle s'ouvrira. Nous devons spécifier le disque de démarrage de la machine virtuelle. Cliquez sur le **CD/DVD** de la machine virtuelle. Assurez-vous que les cases **Connect at power on** et **Datastore ISO file** sont cochées. Cliquez sur **Browse** et allez chercher dans le datastore l'image du disque de pfSense préalablement transférée. Cliquer sur **Finish.**

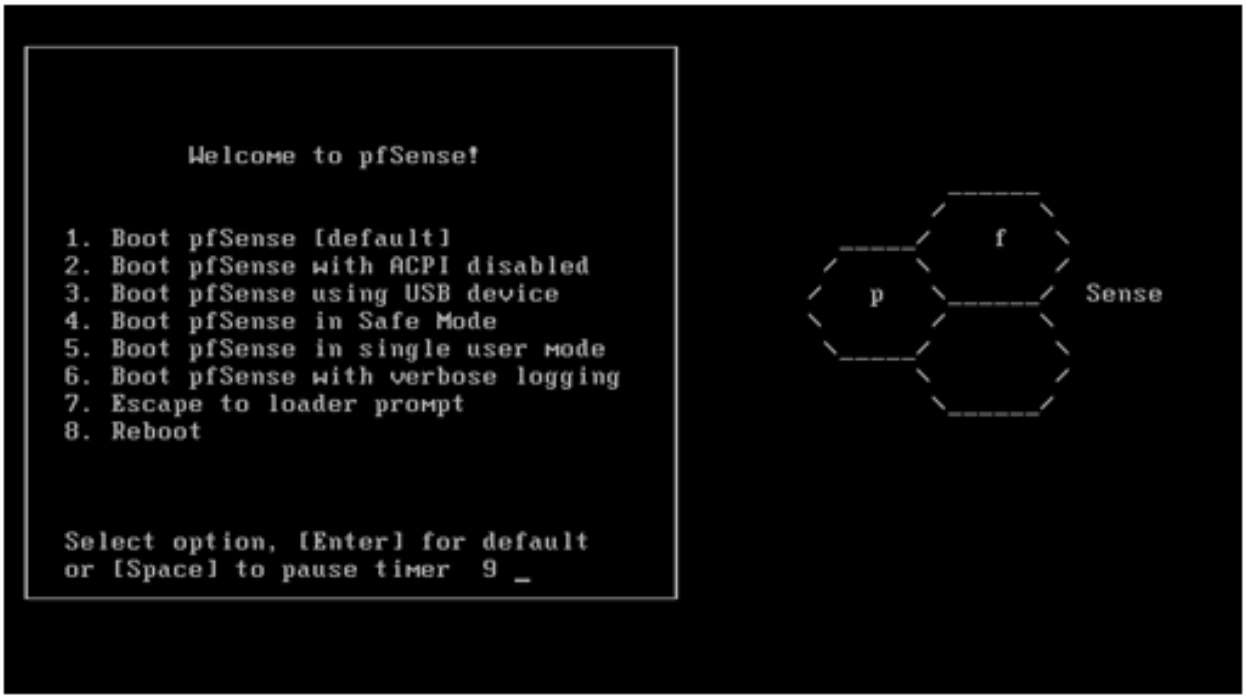


Nous avons désormais une machine virtuelle pour pfSense. La dernière étape consiste à installer le système d'exploitation dans cette machine virtuelle.

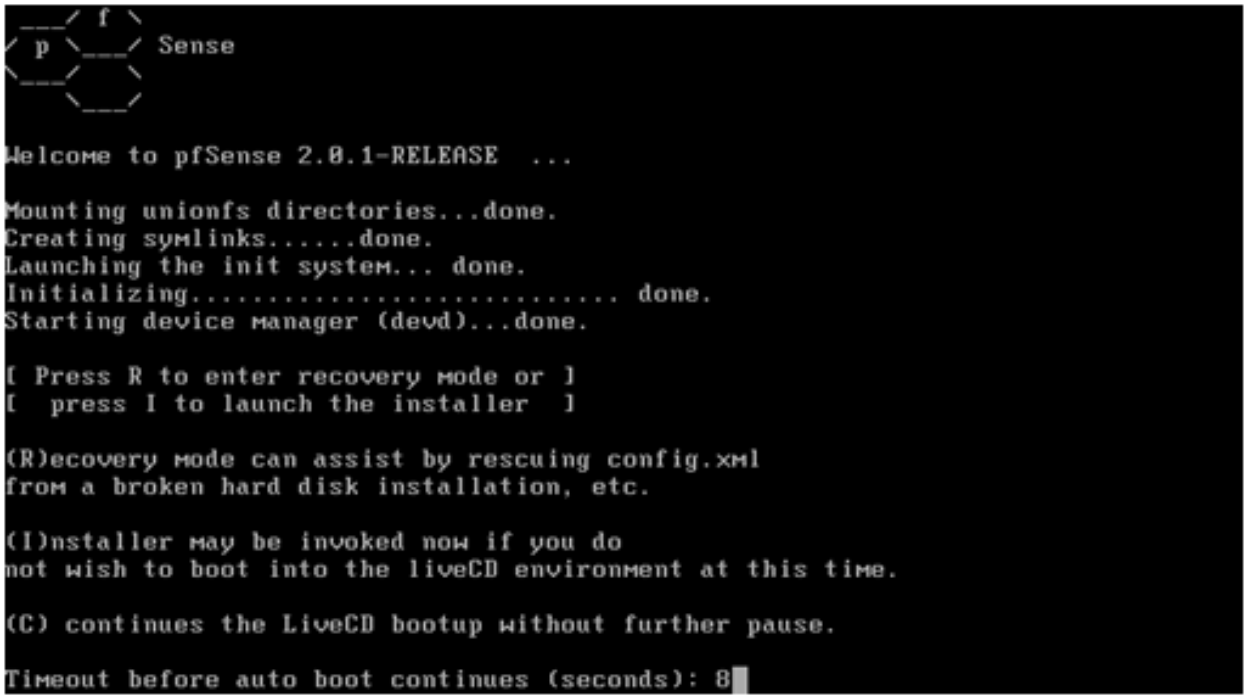
Instructions pour installer pfSense.

1. Démarrez la machine virtuelle et partir la console de visualisation de ESXi. On entre alors en mode de visualisation de la machine virtuelle. Pour retourner la machine cliente physique, faites **CTRL+ALT**

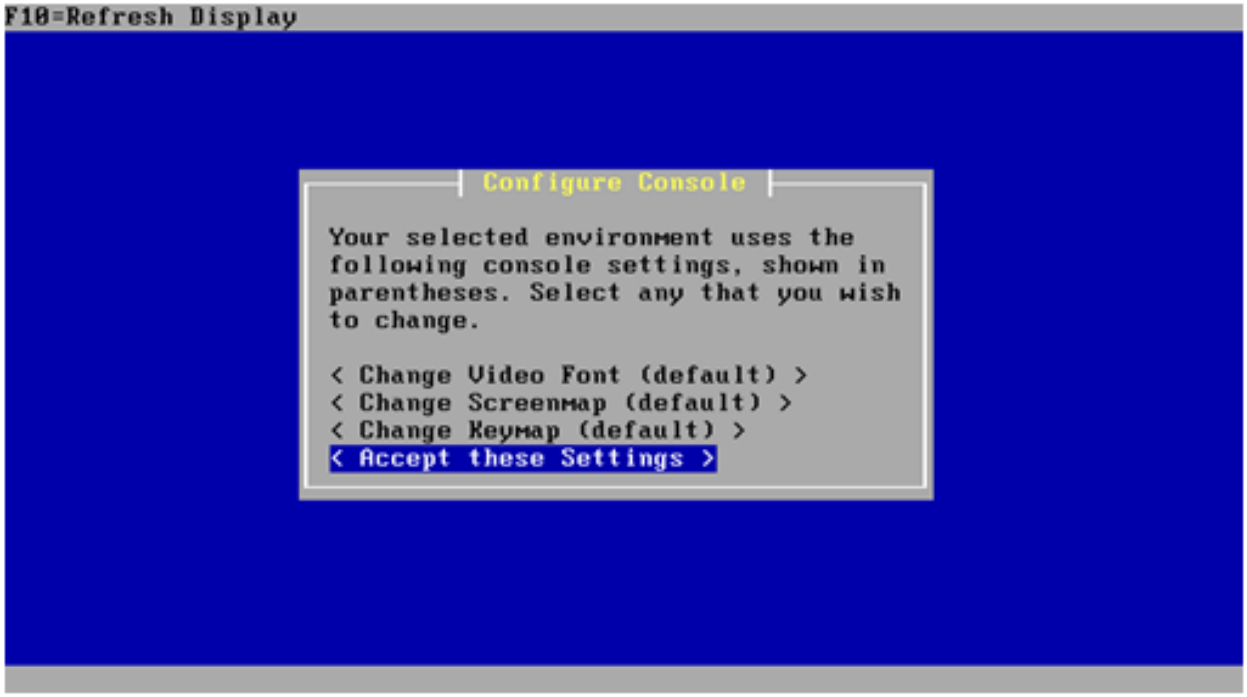
2. Vous verrez apparaître cette fenêtre :

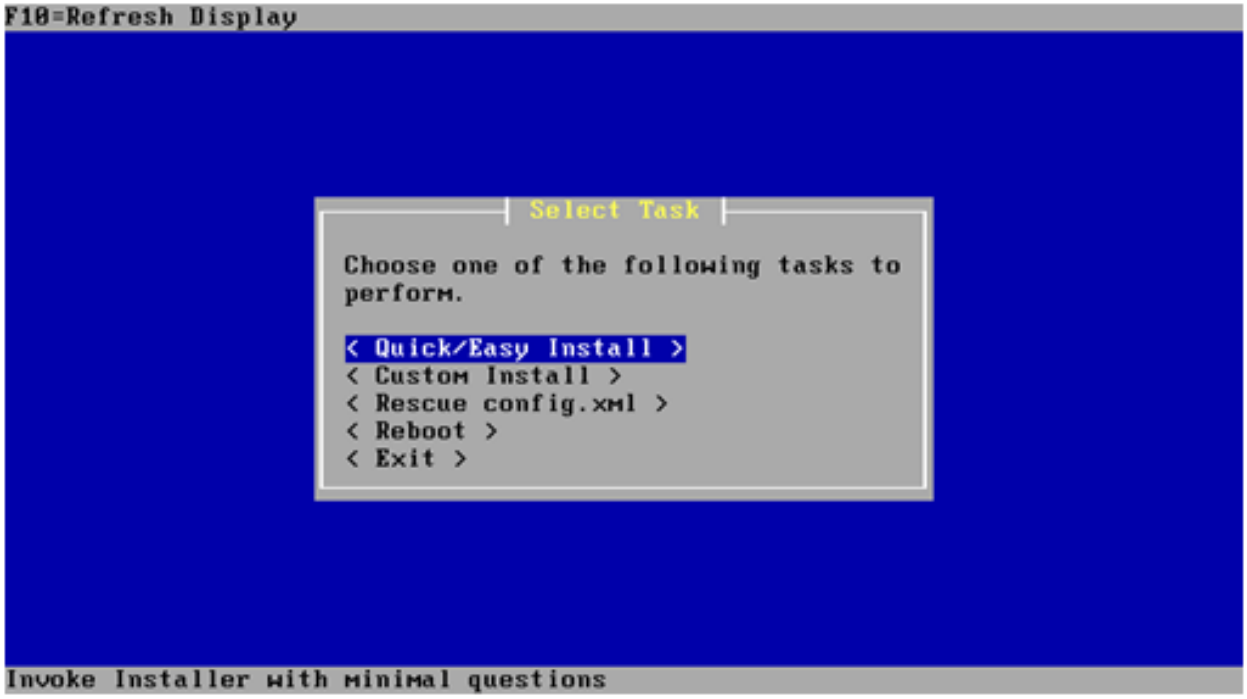


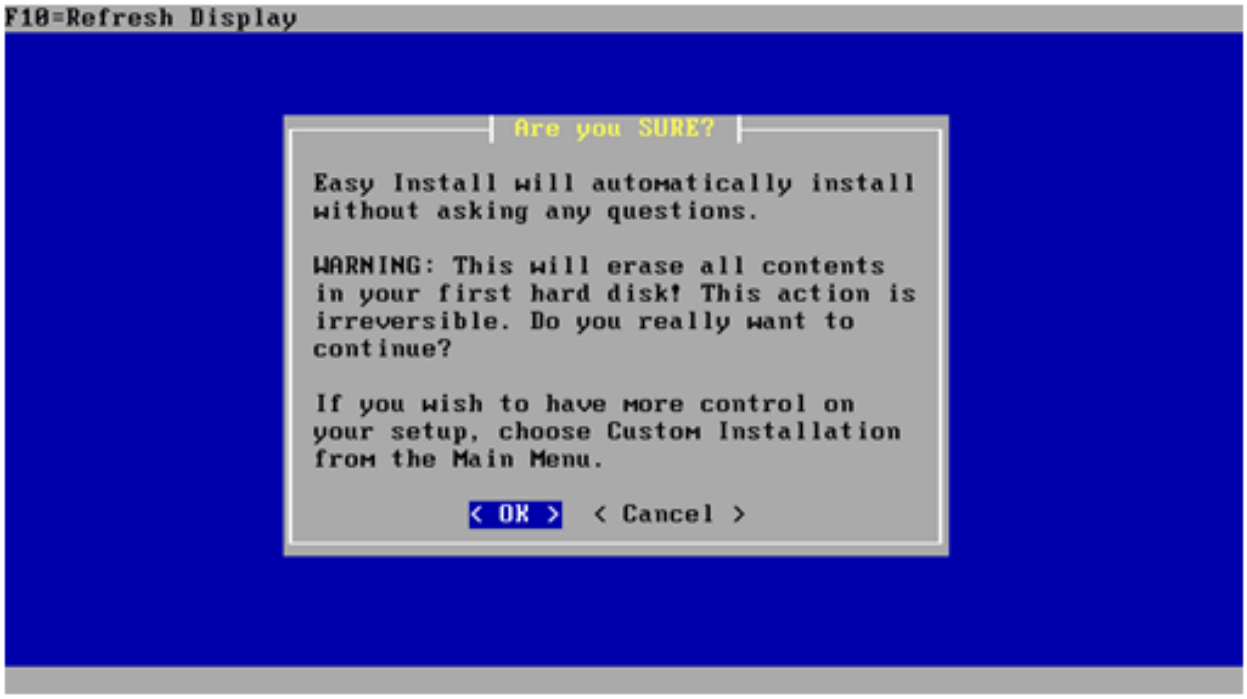
3. Appuyez sur “**i**” pour entrer en mode d’installation.

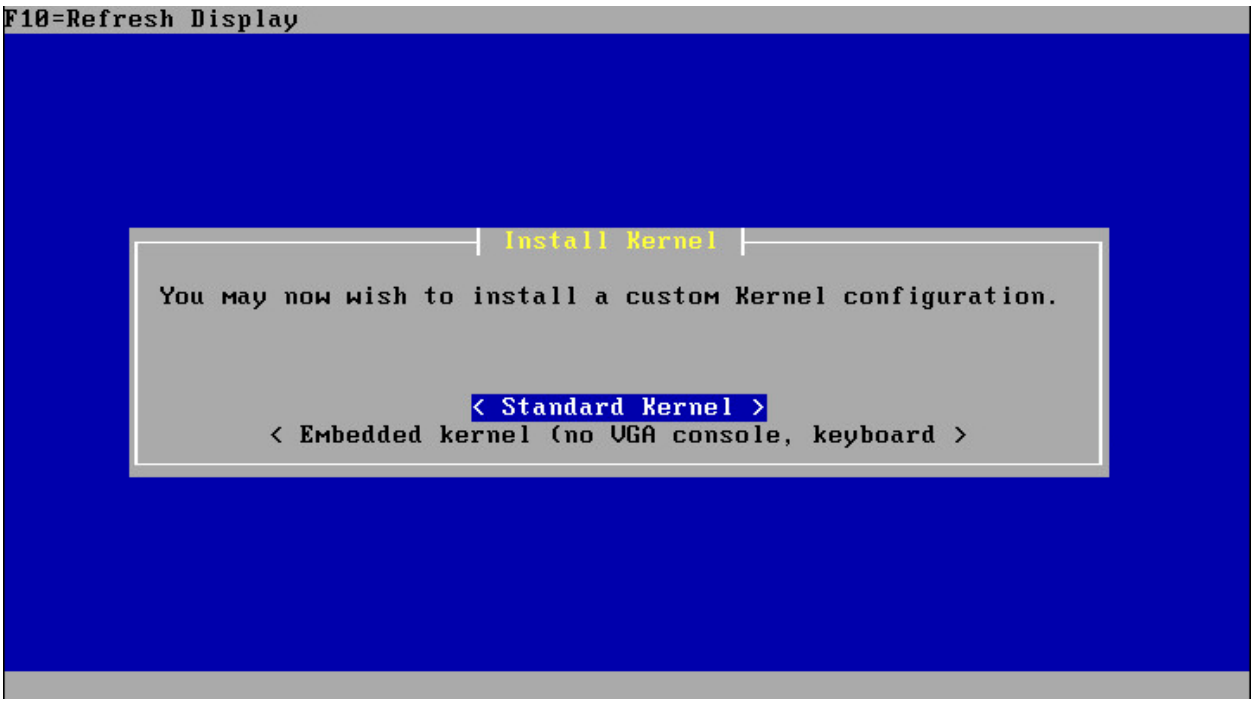


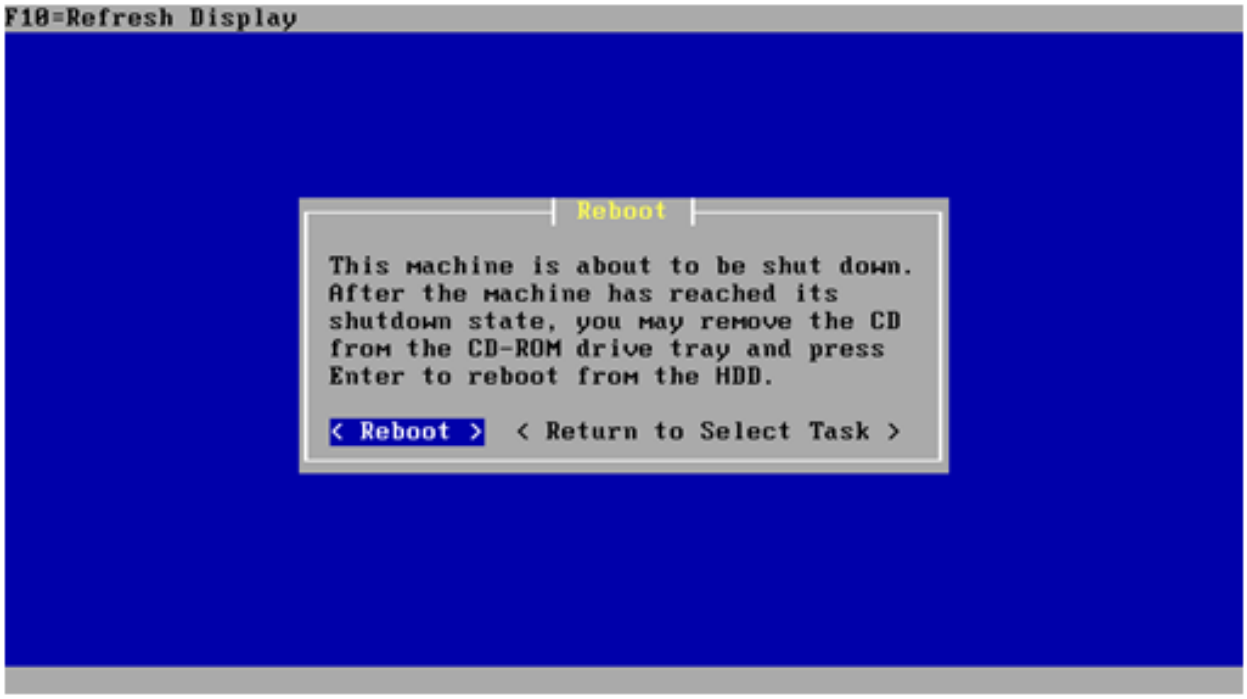
4. Les prochaines captures d’écrans décrivent bien l’installation de pfSense.



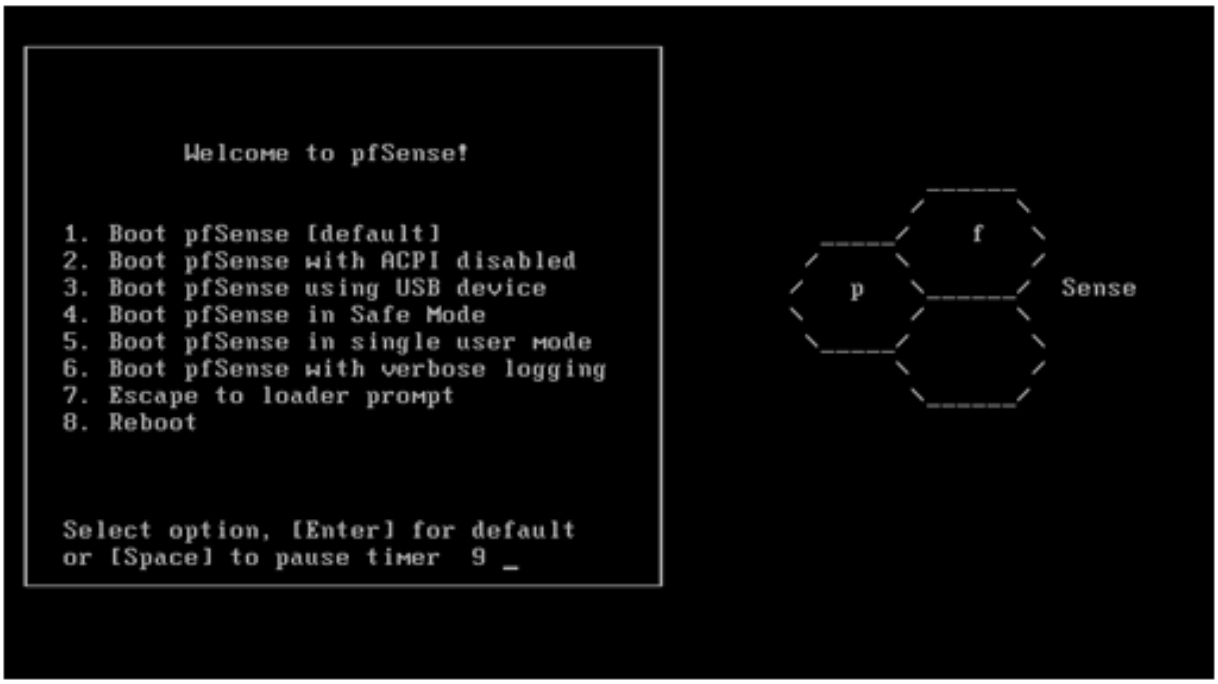

F10=Refresh Display
Select Task
Choose one of the following tasks to perform.
< Quick/Easy Install >
< Custom Install >
< Rescue config.xml >
< Reboot >
< Exit >
Invoke Installer with minimal questions


F10=Refresh Display
Are you SURE?
Easy Install will automatically install without asking any questions.
WARNING: This will erase all contents in your first hard disk! This action is irreversible. Do you really want to continue?
If you wish to have more control on your setup, choose Custom Installation from the Main Menu.
< OK >
< Cancel >


F10=Refresh Display
Install Kernel
You may now wish to install a custom Kernel configuration.
< Standard Kernel >
< Embedded kernel (no VGA console, keyboard >

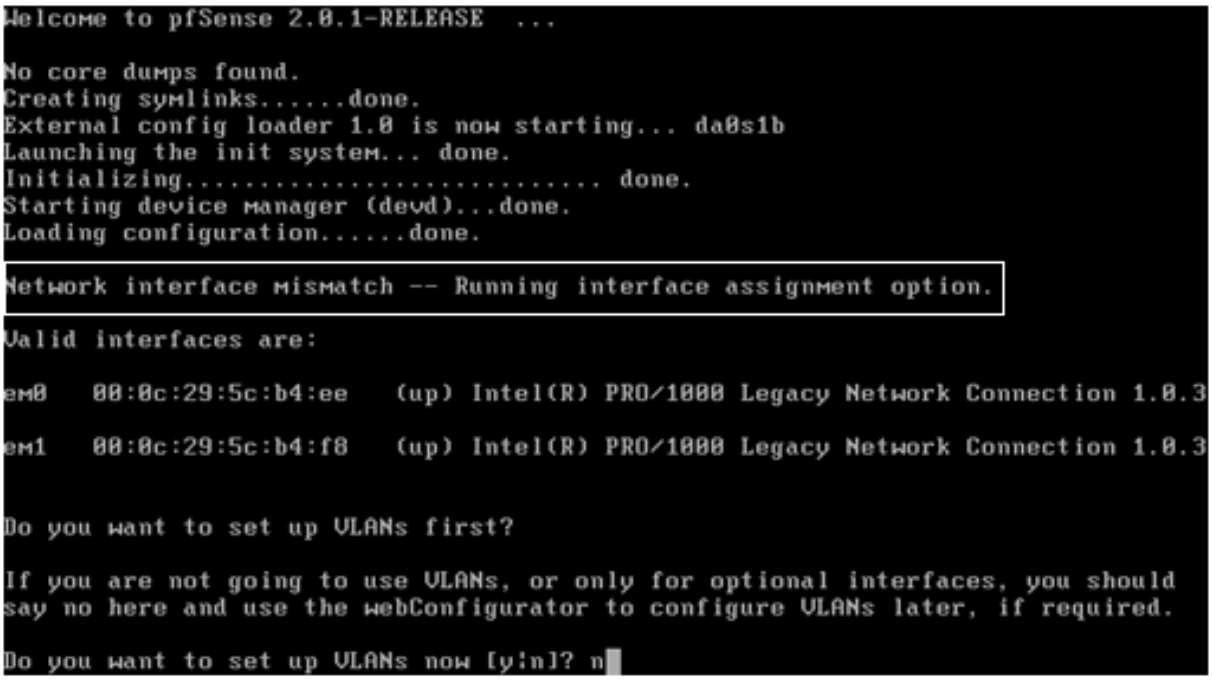

F10=Refresh Display
Reboot
This machine is about to be shut down.
After the machine has reached its
shutdown state, you may remove the CD
from the CD-ROM drive tray and press
Enter to reboot from the HDD.
< Reboot >
< Return to Select Task >

5. Au redémarrage, laissez écouler le temps pour que pfSense démarre.

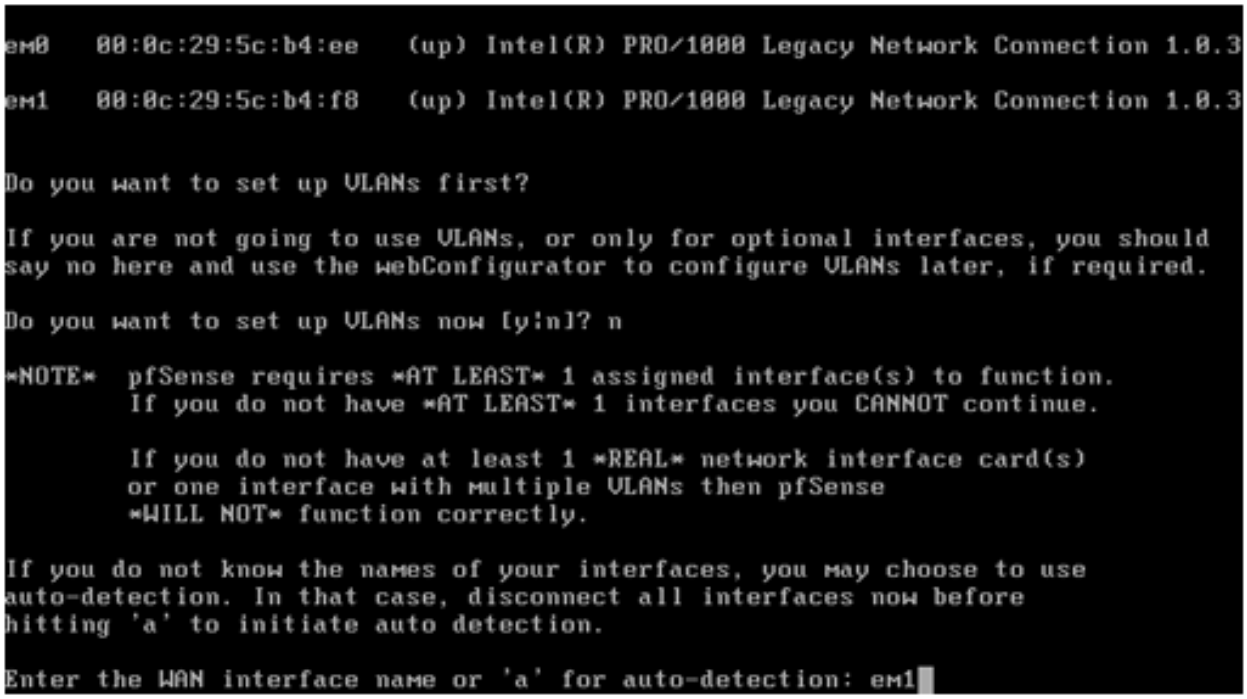


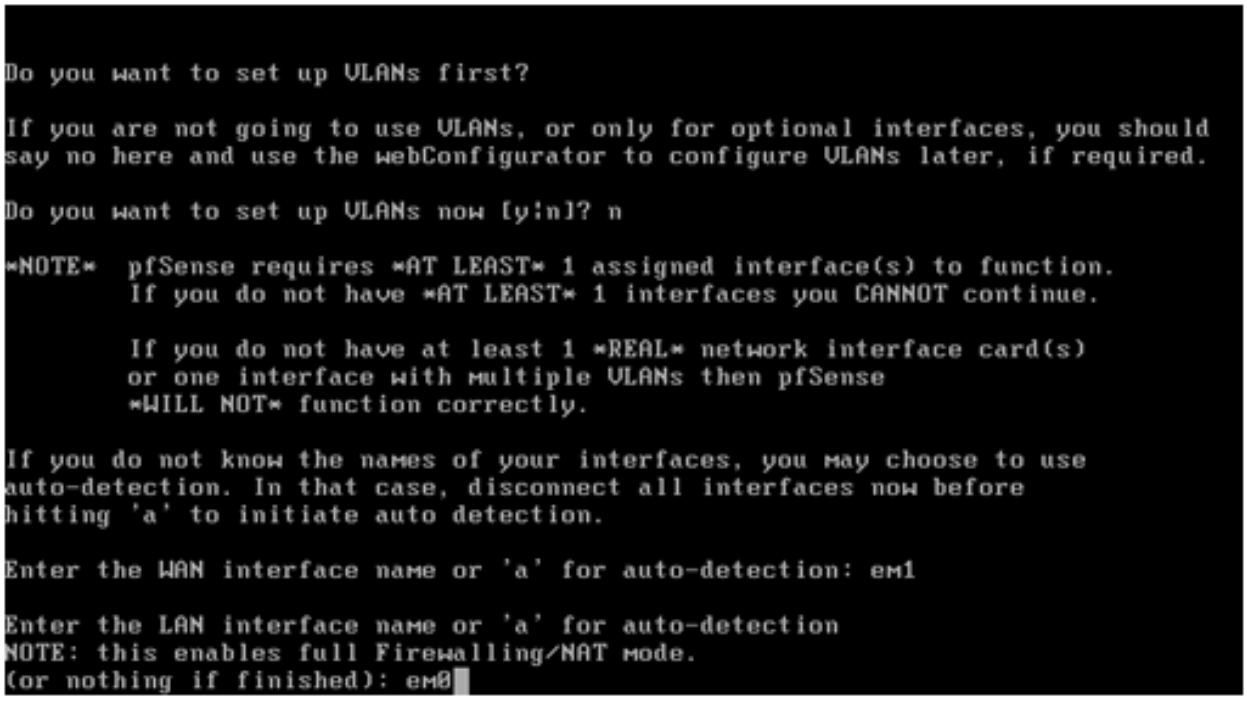
6. Lorsque pfSense commencera à démarrer, vous verrez défiler dans les lignes de commandes **Network interface mismatch - Running interface assignment option.** Cela veut dire que nous n'avons pas encore entré dans le système les interfaces reliées au WAN et au LAN de pfSense.

   Pour les besoins du projet, aucun VLAN ne fut implémenté. Nous répondons donc par la lettre "**n**" à la question **Do you want to set up VLANs now?**

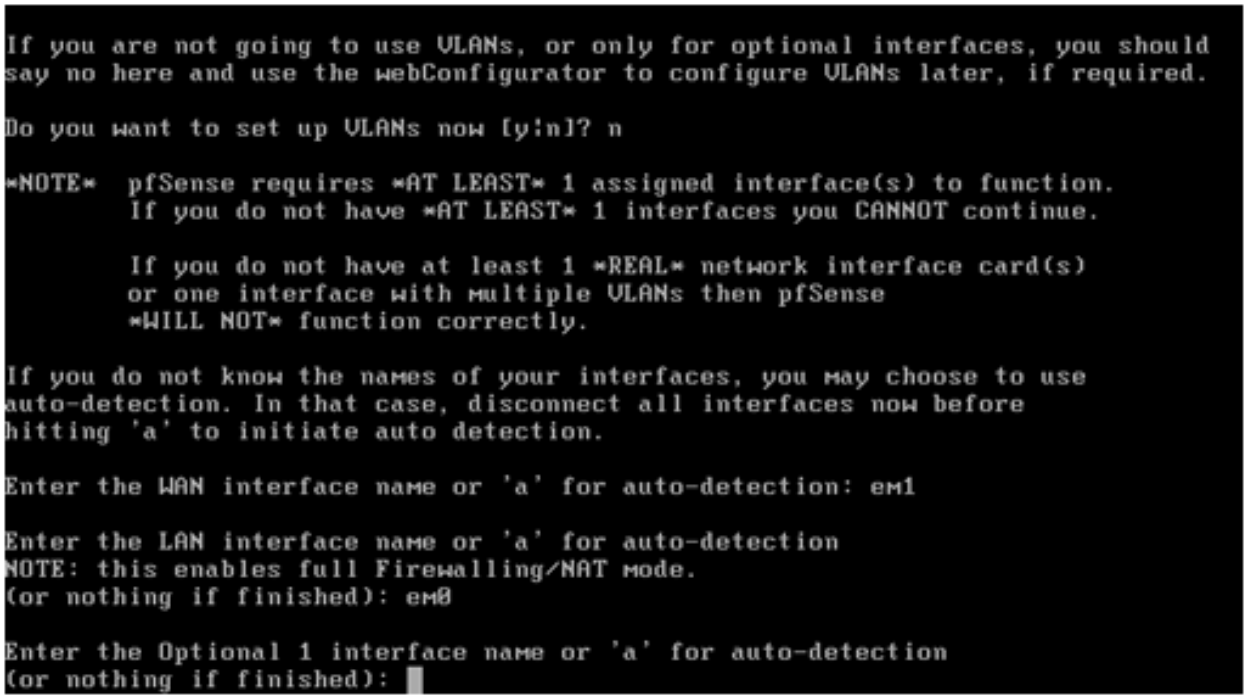


7. À cette étape-ci, l'ordre dans lequel les NICs ont étés assignés lors de la création de la machine virtuelle est important. ESXi présente ces interfaces réseau de façon séquentielle. De ce fait, pfSense voit le NIC 1 comme étant le LAN em0 et le NIC 2 comme étant le WAN em1. Rentrez ces informations et appuyer sur **Enter.**

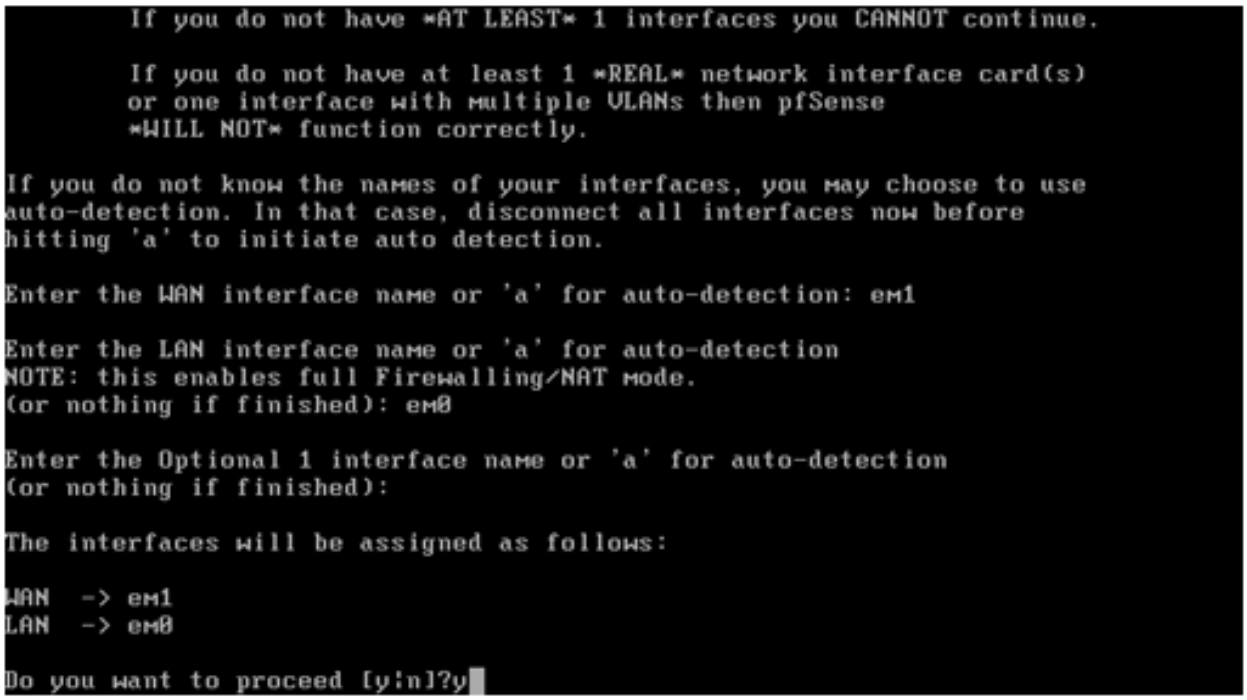




8. Nous n'avons pas d'interface optionnelle. Répondez en appuyant sur **Enter**.



9. Les prochaines lignes décrivent le résumé de la configuration réseau. Faites la touche "**Y**" pour procéder à l'enregistrement des modifications.



10. pfSense redémarrera et vous aurez l'écran ci-dessous. Il ne reste plus qu'à définir une adresse IP statique pour la portion LAN. Cette adresse IP sera la passerelle par défaut de tout le réseau. Pour mettre une adresse IP statique à une interface, appuyez sur **2** et suivre les instructions.

```
Please wait while the changes are saved to WAN... Reloading filter...
 DHCPD... restarting webConfigurator...

The IPv4 WAN address has been set to dhcp
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://dhcp/

Press <ENTER> to continue.
*** Welcome to pfSense 2.1-RELEASE-pfSense (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.216.97/24
 LAN (lan)       -> em1        -> v4: 10.0.1.1/24

 0) Logout (SSH only)                  8) Shell
 1) Assign Interfaces                  9) pfTop
 2) Set interface(s) IP address       10) Filter Logs
 3) Reset webConfigurator password    11) Restart webConfigurator
 4) Reset to factory defaults         12) pfSense Developer Shell
 5) Reboot system                     13) Upgrade from console
 6) Halt system                       14) Enable Secure Shell (sshd)
 7) Ping host                         15) Restore recent configuration


Enter an option:
```

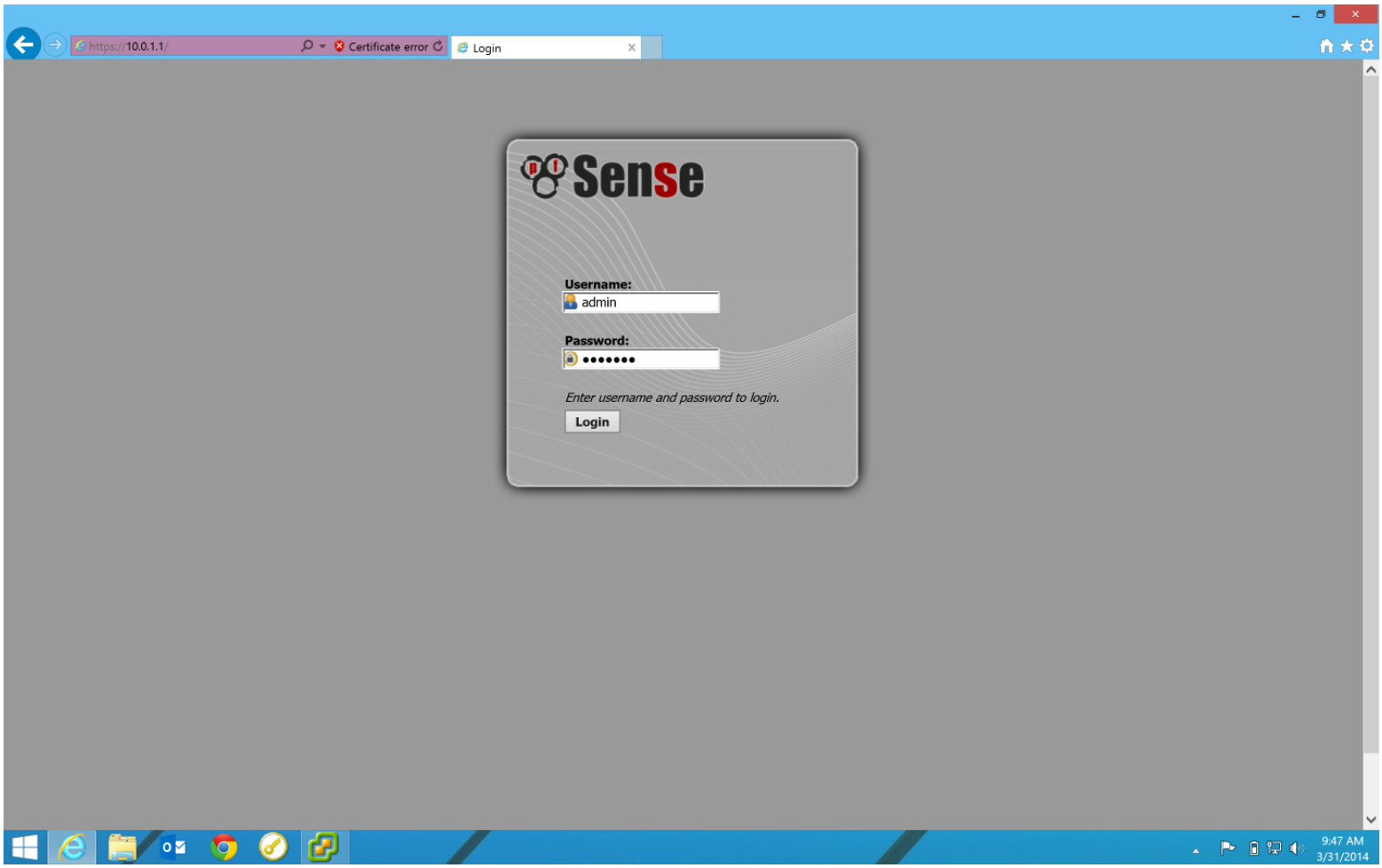
```
 7) Ping host                         15) Restore recent configuration


Enter an option: 2

Available interfaces:

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

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

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.0.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count:
> 24

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

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

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.0.1.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count:
> 24

Enter the new LAN IPv4 gateway address.  Press <ENTER> for none:
> 10.0.1.1

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? [y|n]  n
Disabling DHCPD...Done!
Disabling DHCPD...Done!

Do you want to revert to HTTP as the webConfigurator protocol? (y/n)
```

```
Enter the new LAN IPv4 subnet bit count:
> 24

Enter the new LAN IPv4 gateway address.  Press <ENTER> for none:
> 10.0.1.1

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? [y|n]  n
Disabling DHCPD...Done!
Disabling DHCPD...Done!

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to LAN... Reloading filter...
 DHCPD... restarting webConfigurator...

The IPv4 LAN address has been set to 10.0.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://10.0.1.1/

Press <ENTER> to continue.
```

Configuration initiale de pfSense

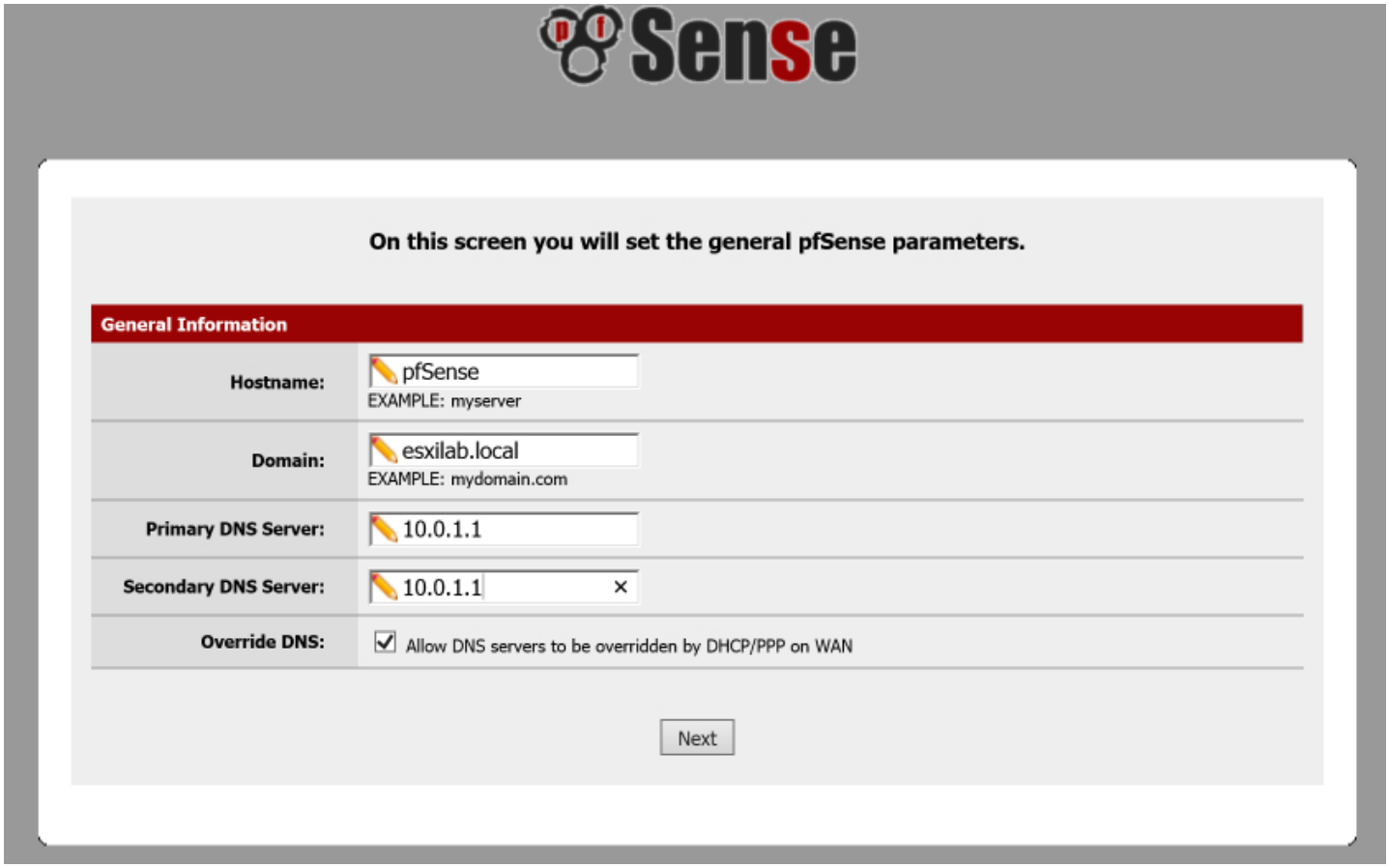
1. pfSense se configure à l'aide d'un navigateur web. Pour accéder à l'interface web, il suffit de **rentrer l'adresse LAN préalablement configurée** à l'étape précédente **dans la barre d'adresse du navigateur.** Une page d'authentification s'affichera.



Le nom d'utilisateur par défaut est **admin** et le mot de passe est **pfsense.**

2. La page suivante informe que pfSense passe en mode de configuration initiale.

3. La page suivante demande de **rentrer les renseignements de base** du serveur pfSense.



4. Il faut ensuite configurer les paramètres de temps.

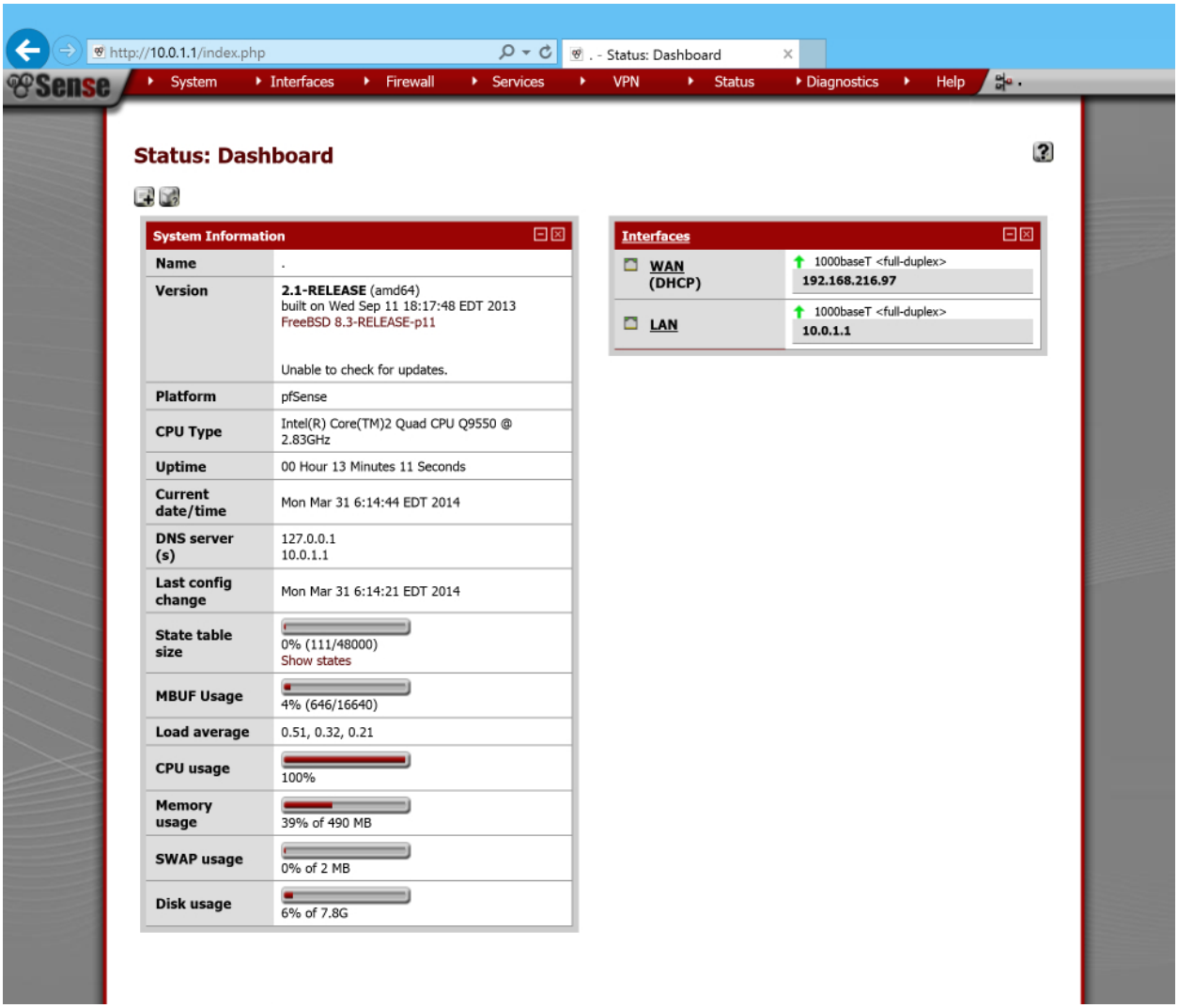
5. La page qui suit sert à configurer l'interface WAN. Normalement, on laisse cette interface en **mode DHCP**, à moins que le fournisseur d'accès à Internet ne fournisse une adresse IP fixe ainsi qu'une passerelle par défaut et des serveurs DNS fixes.

6. Vient ensuite la configuration de l'interface LAN. L'adresse que l'on rentre servira de **passerelle par défaut** des machines clientes sur le réseau.

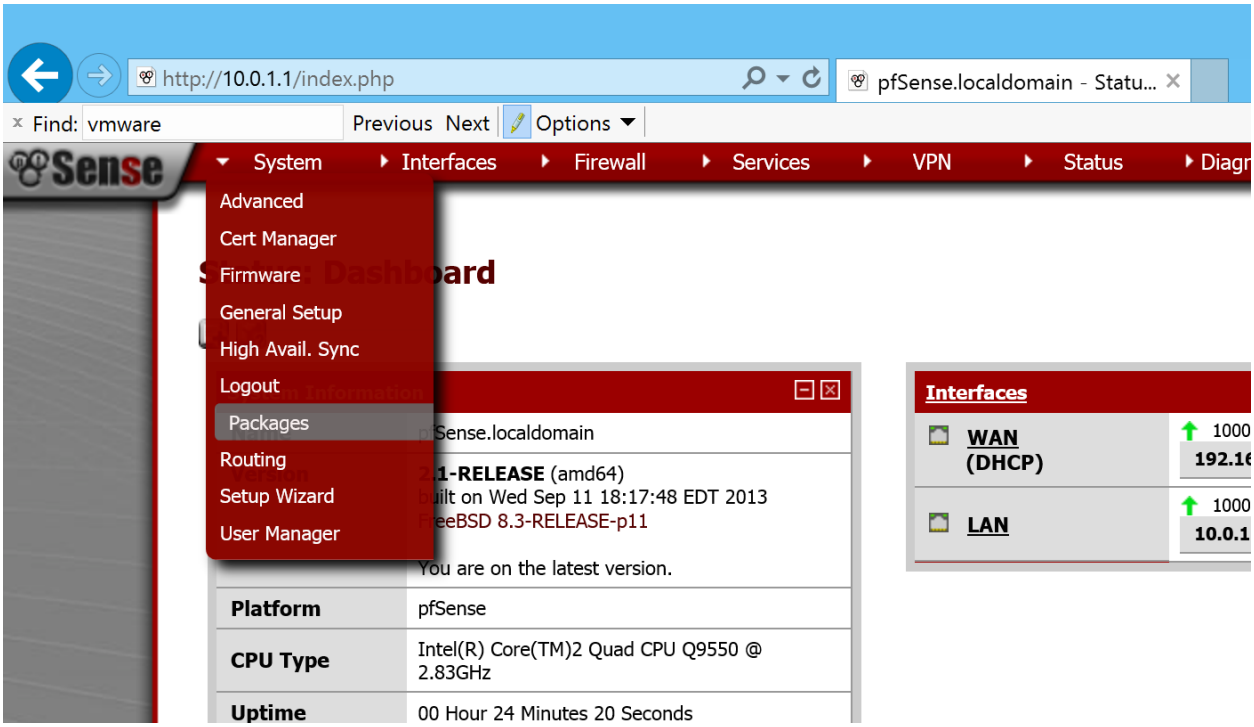
7. La fenêtre qui suit sert à **changer le mot de passe administrateur** pour une meilleure sécurité du serveur.

8. Après avoir été configuré, pfSense redémarrera.

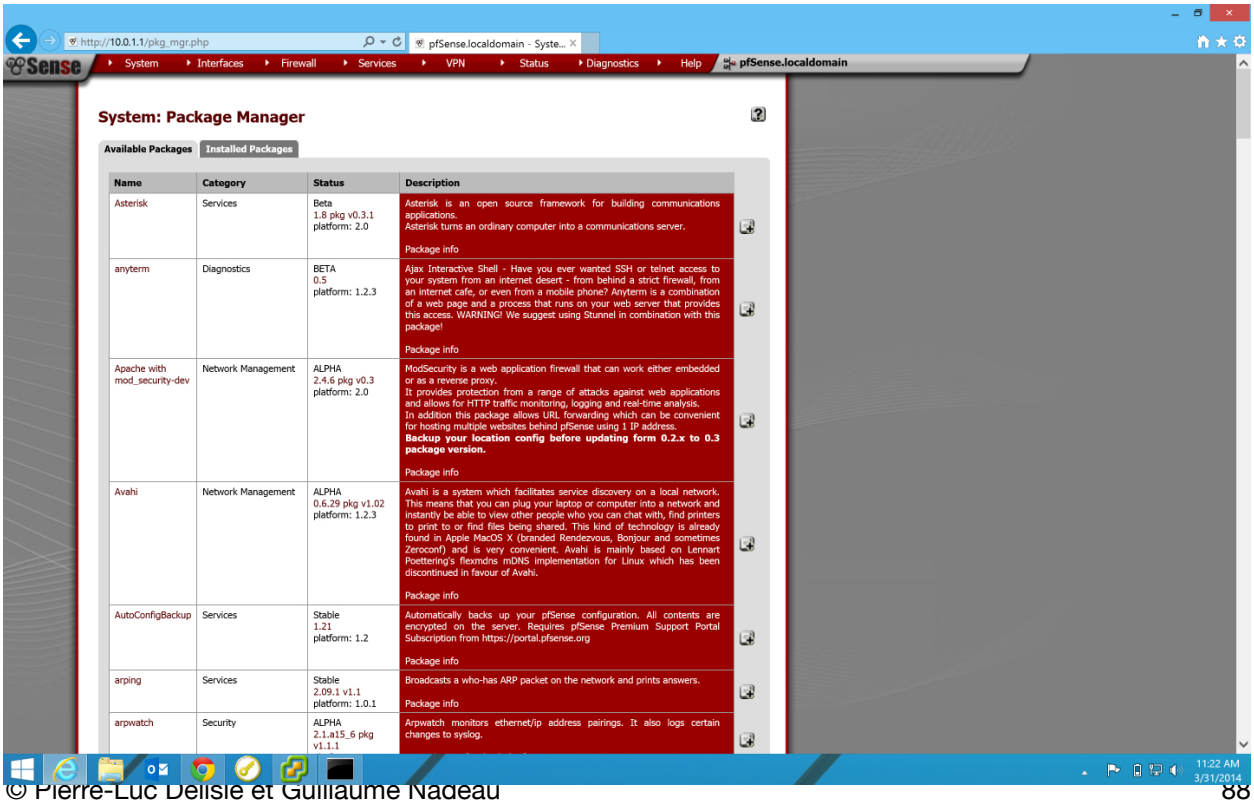
9. Une fois redémarré, la fenêtre affichera le résumé du serveur.



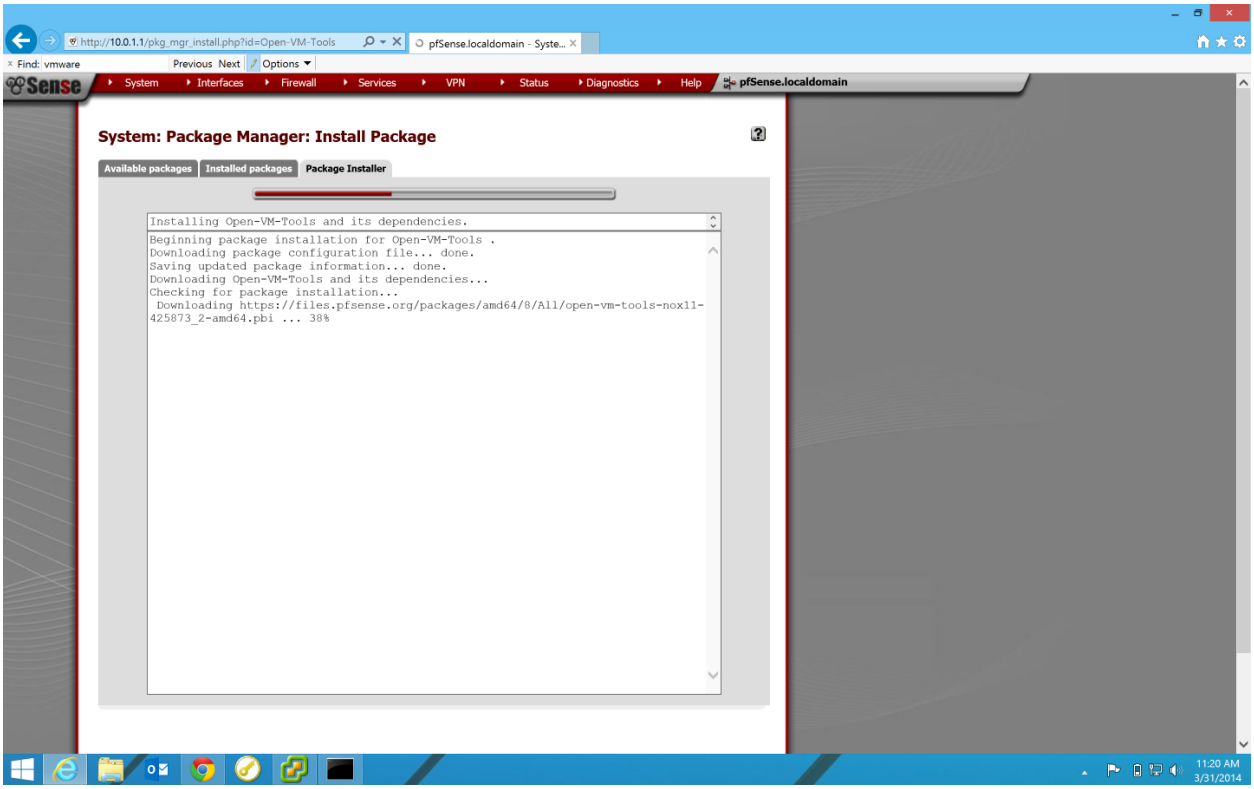
10. Puisque le serveur pfSense est opéré sur une plateforme ESXi, il faut installer les VMware Tools qui aideront à améliorer les performances du réseau. Pour se faire, il faut cliquer sur **System** et puis sur **Packages**.



11. La liste des packages pouvant être installé est située sous l'onglet **Available Packages.**



12. Le package à installer est **Open-VM-Tools.** Cliquez sur l'icône au bout de la ligne. La page suivante s'affichera pour détailler l'installation.



L'installation de pfSense est désormais complétée et prête à être opéré.

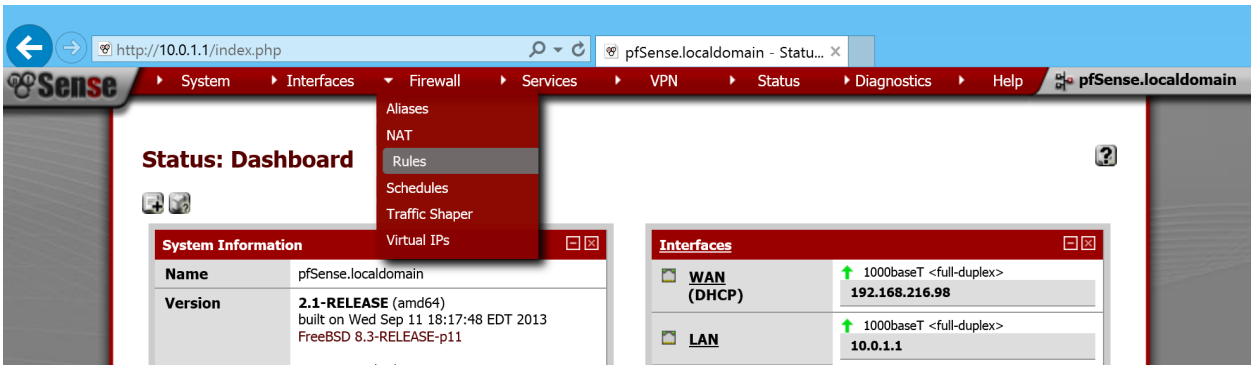
Création d'une règle de blocage dans pfSense.

Dans le cadre du projet, nous devions configurer le pare-feu de sorte à bloquer un site web en particulier.

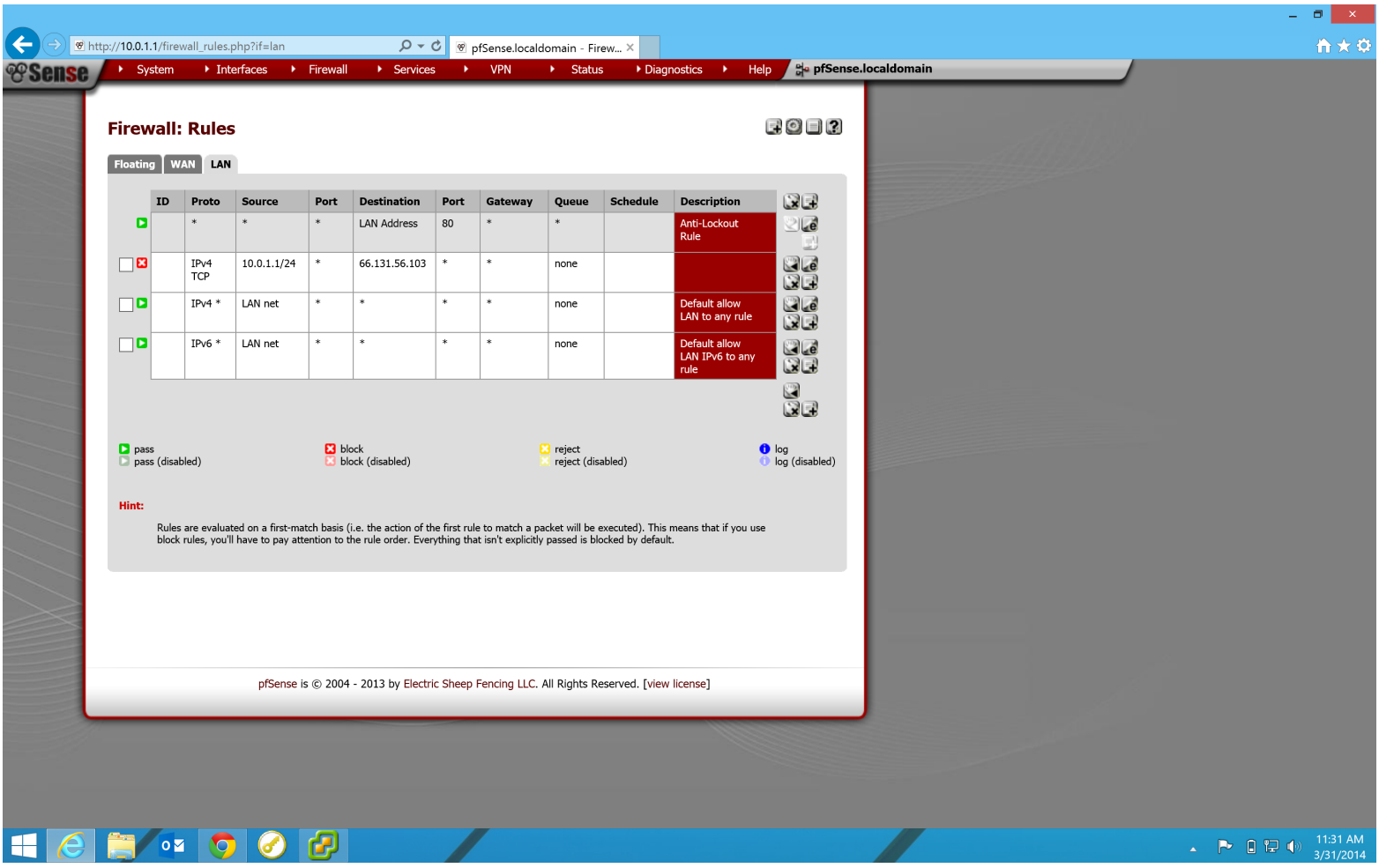
1. pfSense est pourvue d'une interface graphique sur le Web. Pour y accéder, **inscrire l'adresse de la passerelle par défaut** dans votre **navigateur web**.

2. Entrer le **nom d'utilisateu**r de l'administrateur et le **mot de passe** de ce compte.

3. Pour configurer une règle, il faut cliquer sur le menu **Firewall** puis sur **Rules**.



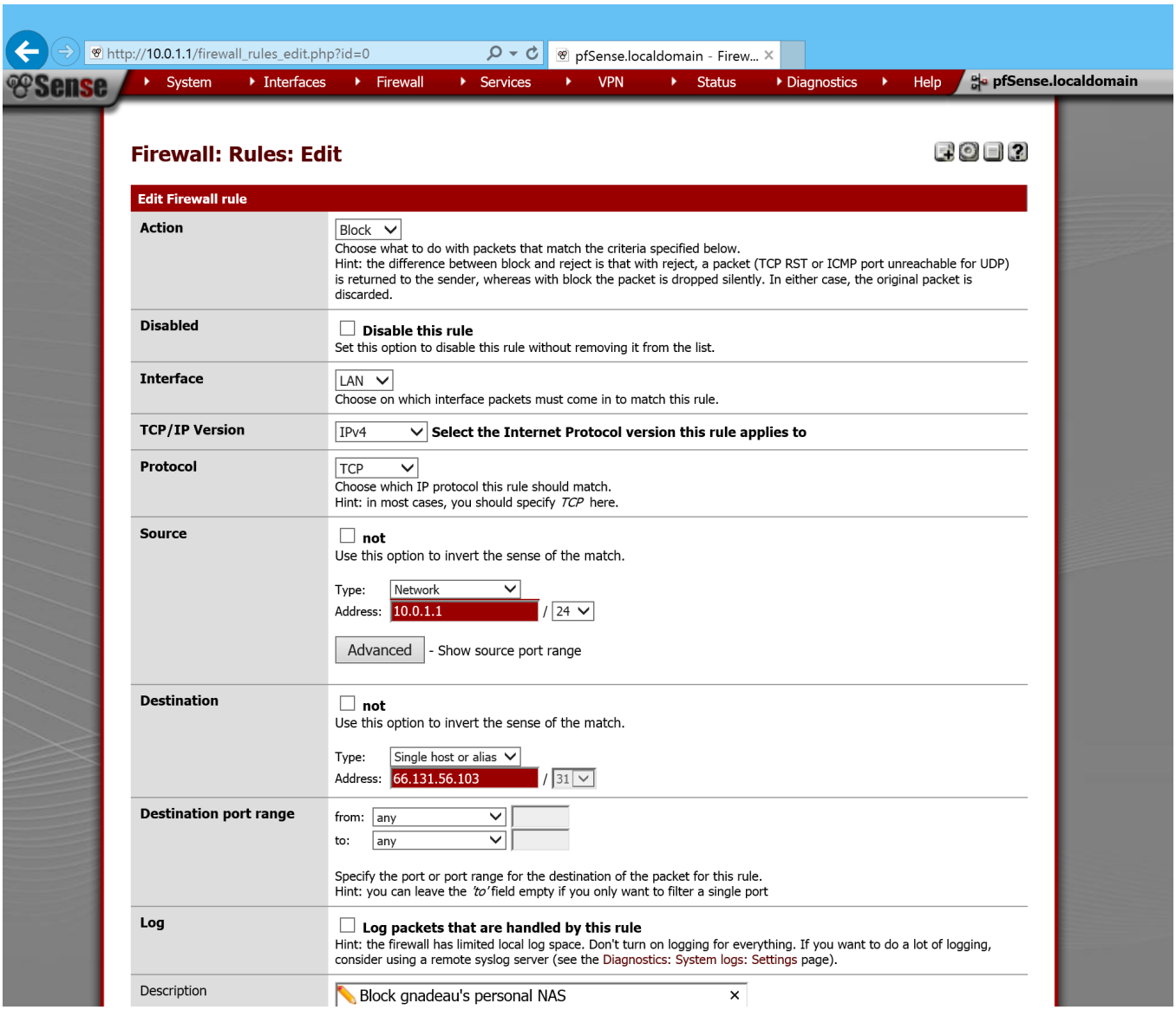
4. Le menu récapitulatif des règles pour chaque zone est affiché.



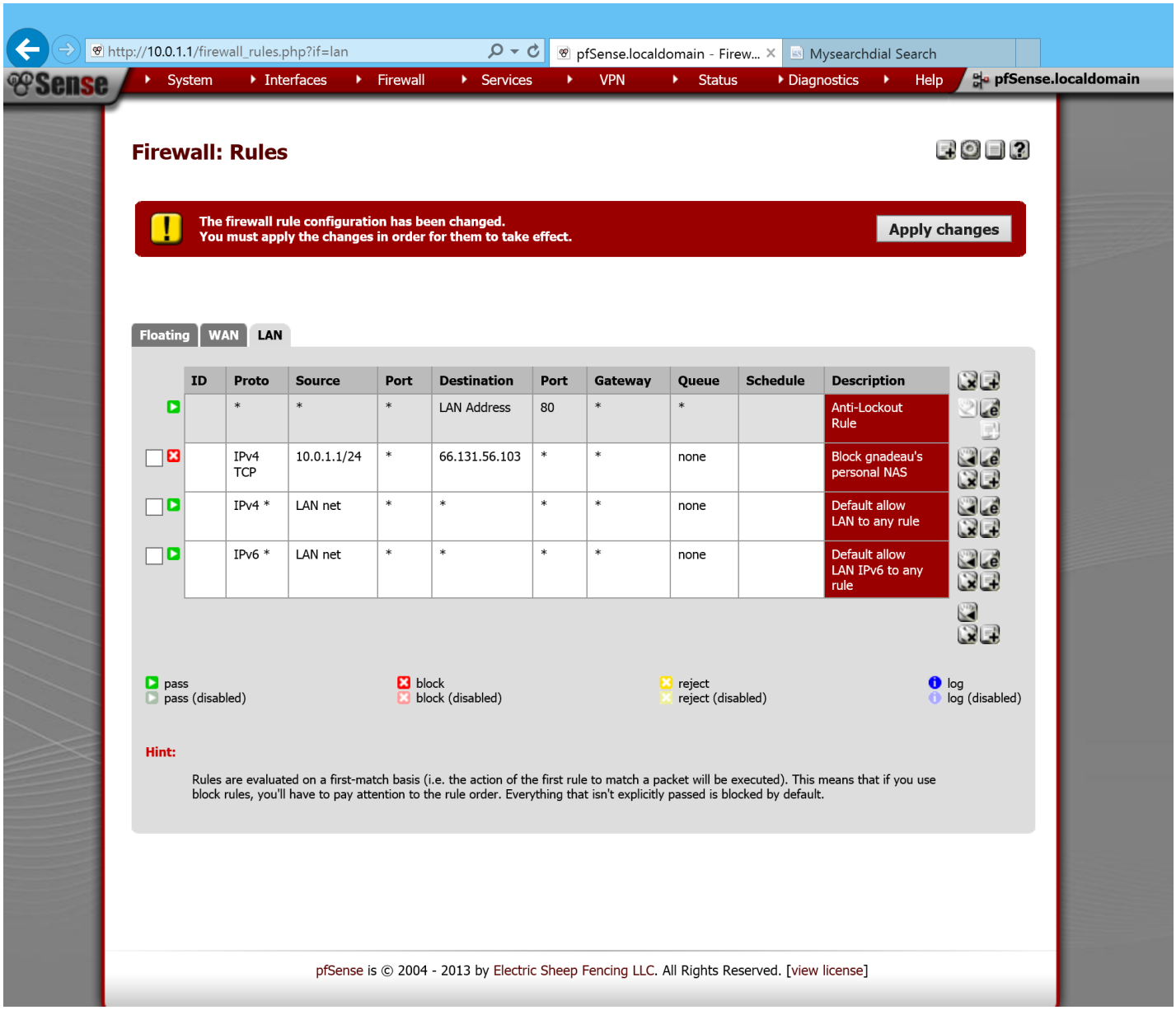
5. Pour créer une nouvelle règle, appuyez sur l'icône  dans la section **LAN**.

6. Le menu de création d'une règle s'affichera. Pour bloquer une adresse IP, il faut :

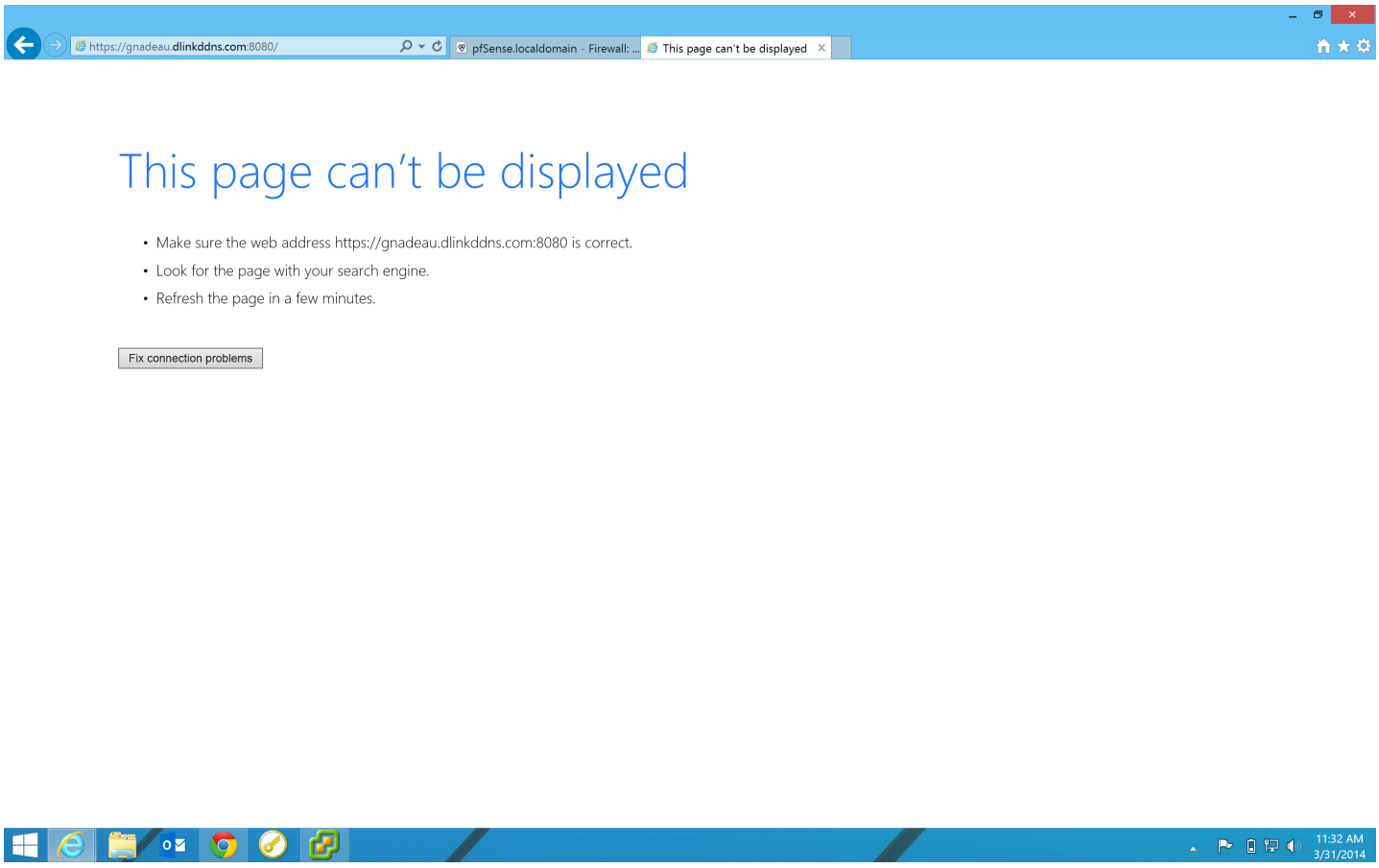
    - Bloquer la règle : **Action -> Block**
    - Interface : **LAN**
    - TCP/IP version : **IPv4**
    - Source
        - Type : **Single Host or Alias**
        - Address : **L'adresse IP du site à bloquer**
    - Description : Écrire le nom de la règle.



7. Après avoir créé la règle, la page récapitulative des règles s'affichera. Il faudra cliquer sur **Apply changes** pour que les règles soient enregistrées dans le module du pare-feu.



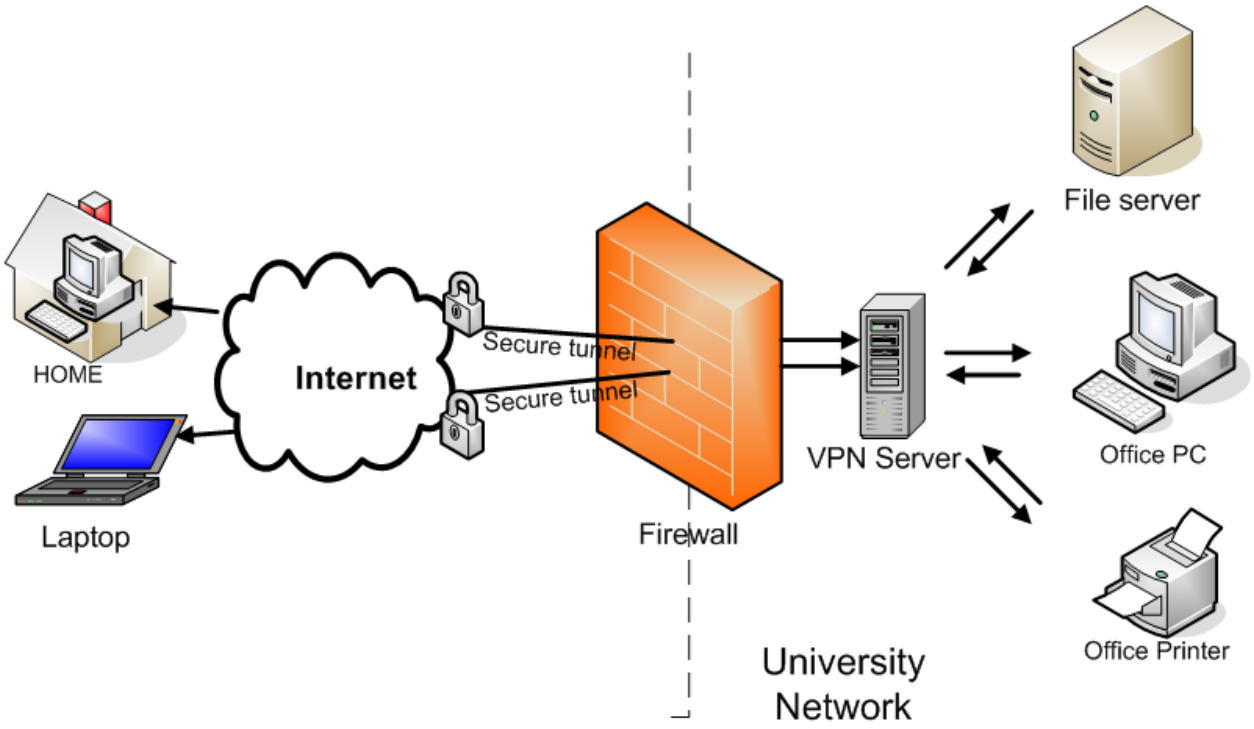
8. Tester la nouvelle règle. Puisque l'adresse IP sera bloquée, les données ne pourront se transférer au site. Par conséquent, ce dernier ne pourra pas s'afficher.



Nous avons voulu tester les performances de pfSense. Pour ce faire, nous avons utilisé le populaire utilitaire en ligne *Speedtest* pour nous donner de façon précise la vitesse de transfert avec le WAN. Sans grande surprise, nous avons conclu que le pare-feu pfSense n'a aucun impact sur les performances WAN. Il n'y avait aucune différence de vitesse entre une connexion passant par pfSense et celle directement branchée sur le réseau du collège.

Création d'une connexion VPN

VPN désigne l'acronyme de *Vritual Private Network*, ou réseau local privé virtuel. Un VPN étend un réseau local privé sur un réseau public tel qu'Internet. Un VPN permet à un hôte A sur un réseau privé A d'envoyer et de recevoir des données d'un hôte B connecté à un autre réseau distant B en passant par un réseau internet public C comme si cet hôte A serait connecté au réseau local privé B.



Un VPN permet donc de connecter deux réseaux privés ensemble par le biais de réseaux publics. Lorsqu'une connexion VPN est effectuée, on parle souvent de «tunnel VPN» puisqu'une connexion point à point sécurisée vient d'être établie. En effet, un VPN permet également la gestion de la sécurité. Les données transigeant sur des réseaux publics non-sécurisés entre les réseaux de l'exemple ci-dessus sont cryptées au moyen de clefs de chiffrements. Cela veut donc dire qu'un utilisateur peut travailler à partir de n'importe quel point dans le monde et avoir une connexion sécurisé avec un serveur sur un réseau distant. Les données voyagent de façon transparente puisque le VPN simule une connexion physique au réseau distant.

Le tunnel VPN (VPN Tunneling) se compose de deux types, le tunnel volontaire et le tunnel forcé. Ces deux types de tunnels peuvent utiliser les protocoles PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) ou L2TP (**L**ayer **2** **T**unneling **P**rotocol) pour encapsuler et transmettre les données par des réseaux publics.

Plusieurs types de clefs de cryptages peuvent être utilisées, tout comme de nombreux protocoles d'authentification sont utilisés au sein de la technologie VPN. PPTP, le protocole le plus utilisé puisqu'implanté depuis fort longtemps dans les solutions Microsoft, utilise la clef de cryptage la plus faible de l'industrie, soit 128-bit. Cela en fait la solution la moins sécuritaire du marché, alors que LT2P over IPSec et OpenVPN utilisent des clefs de cryptage AES 256-bit. PPTP utilise une authentification encapsulée par MS-CHAPv2. Toutefois, des *exploits* on été découvert pour décapsuler cette authentification et des trames PPTP ont été décryptées en moins de deux jours. Microsoft recommande donc lui-même d'utiliser LT2P over IPSec ou OpenVPN comme solution VPN[3].

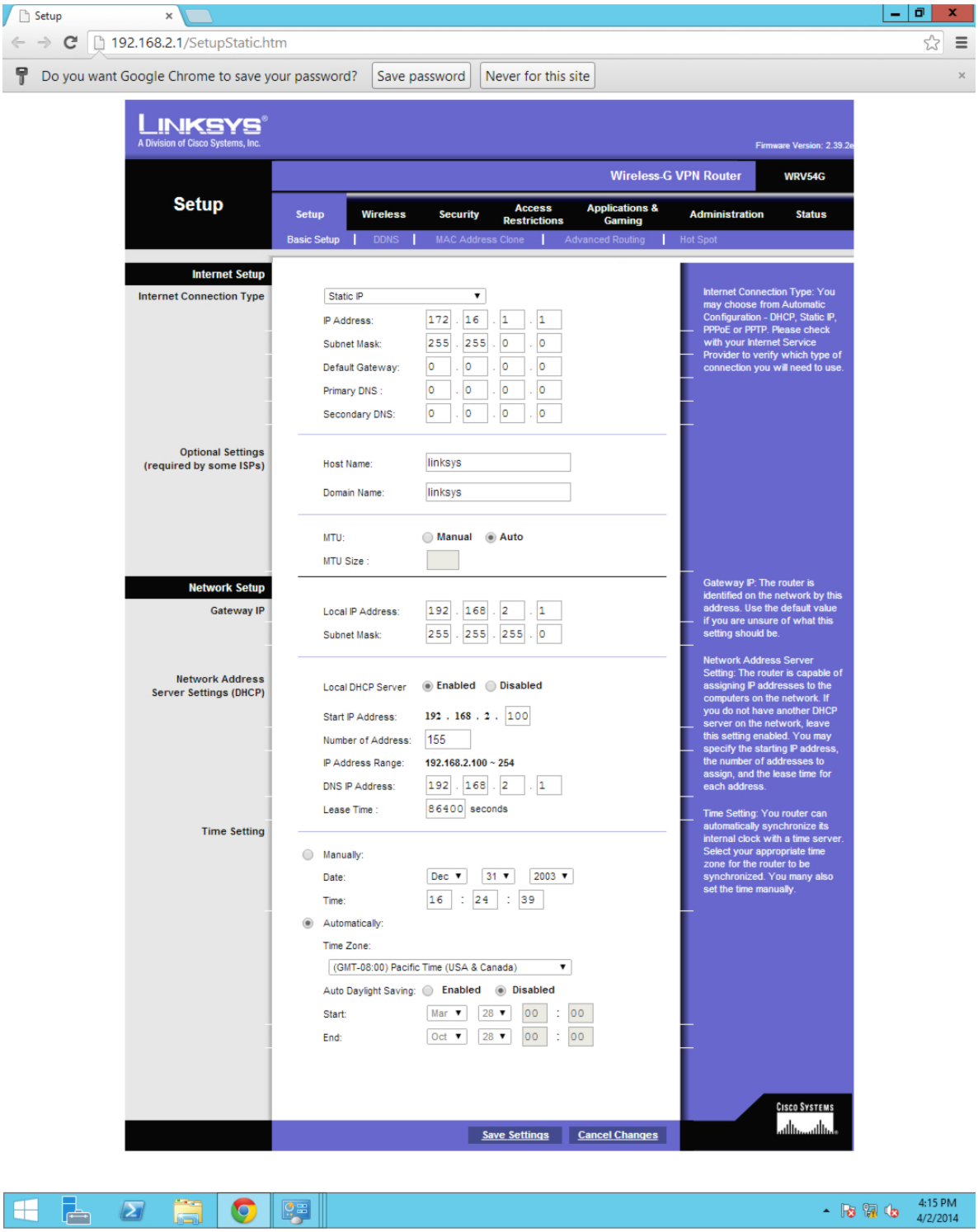
Dans le cadre de ce projet, une connexion VPN PPTP cryptée devait être configurée pour avoir un accès sécurisé au serveur de partage depuis n'importe quel point d'accès Internet dans le monde. Cependant, nous nous sommes rendu compte que le routeur fourni ne peut être serveur VPN. Aucune encryption ne peut être faite, de même qu'aucun utilisateur ne peut-être créer pour accéder à la portion LAN du réseau. Tout ce qui peut être configuré dans ces Linksys WRV54G est un *VPN Passthrough*, soit une passerelle pour le trafic VPN dans le routeur. En configurant cette passerelle, le routeur peut accepter le traffic entrant et sortant vers un serveur VPN ou d'un client VPN, mais ne peut en aucun cas servir de serveur VPN. La directive finale du projet est donc totalement invalidée à cause de l'équipement fourni.

Nous avons tout de même configuré le *VPN Passthrough.*

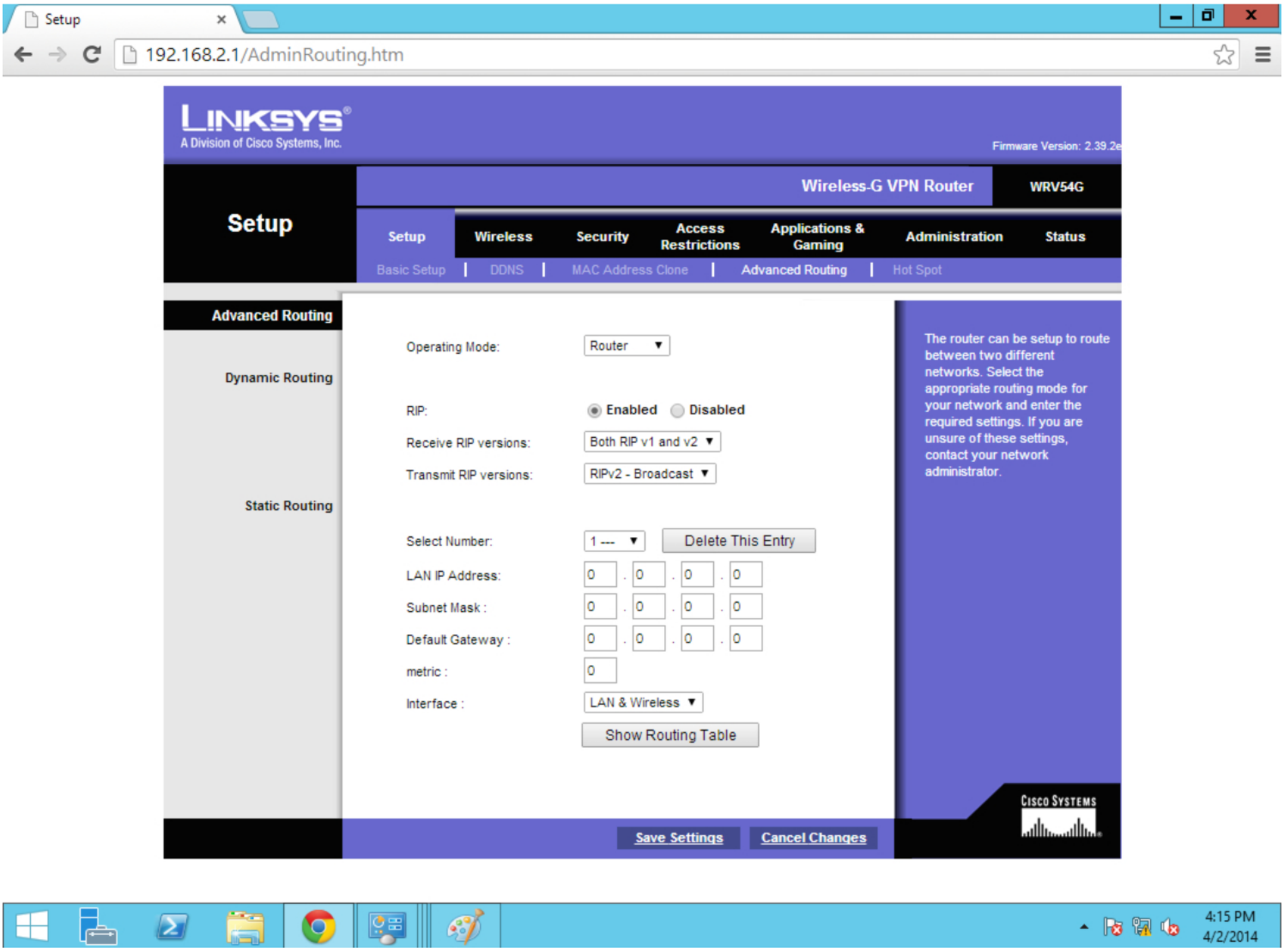
[3] http://technet.microsoft.com/en-us/security/advisory/2743314
https://www.bestvpn.com/blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp/

Configuration d'un VPN Passthrough sur un routeur WRV54G - Guide étape par étape :

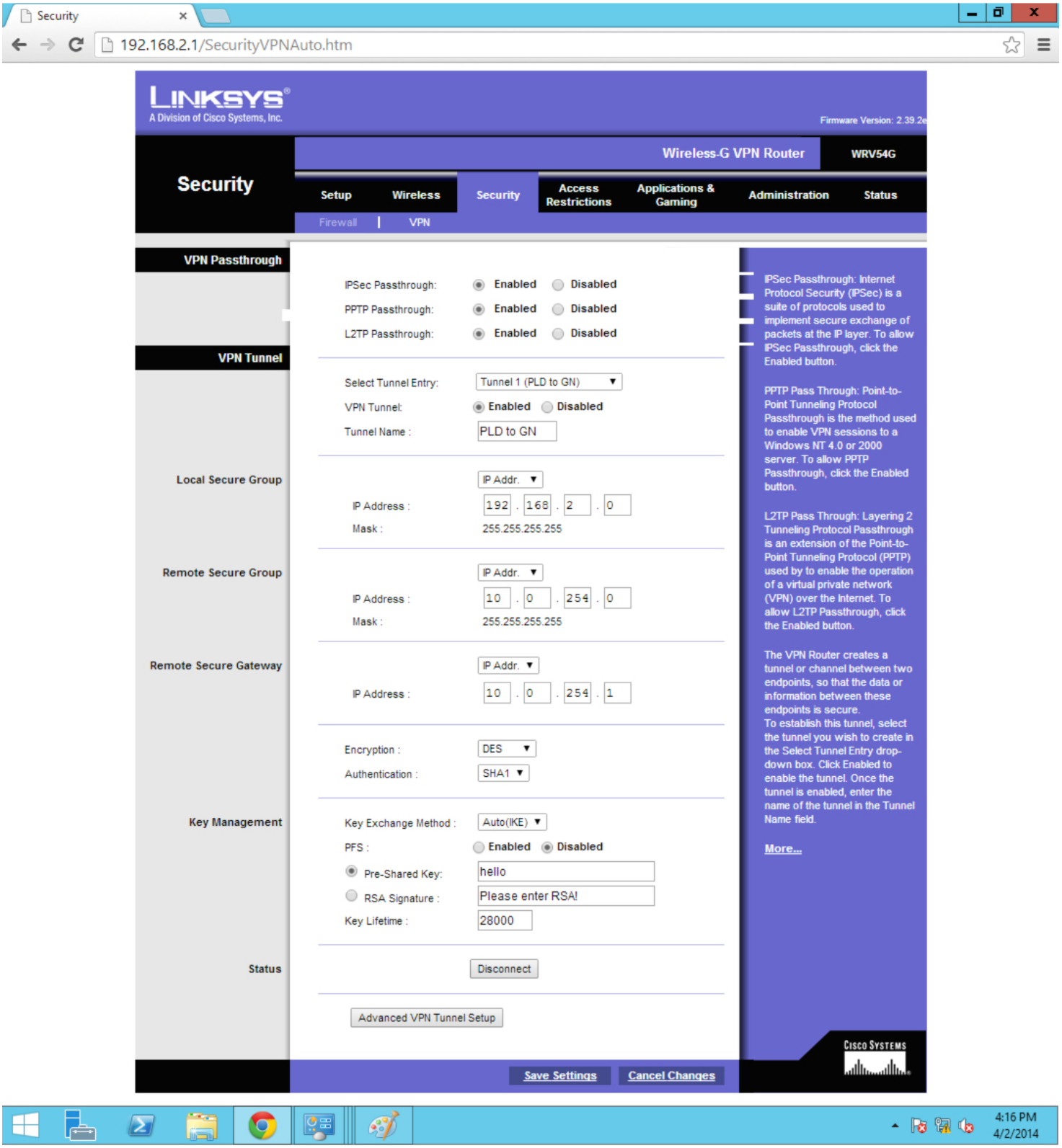
1. Configurez les interfaces WAN et LAN, de sorte à ce que les clients puisse être connectés au WAN.



2. Activez le mode **Router** dans **Setup->Advanced Routing**.



3. Configurez le **VPN Passthrough** dans **Security->VPN**.



Conclusion

En résumé, ce projet a présenté en détail comment implanter un réseau de façon beaucoup plus complète et plus réaliste que le projet initial, tout en étant de loin plus moderne. Nous nous sommes efforcés de suivre les nouvelles tendances en adoptant la virtualisation et en la mettant au coeur de notre projet. Nous avons également privilégié l'« Open Source » avec l'utilisation de pfSense à titre de pare-feu de notre réseau, une solution qui s'avère de loin plus complète plus et efficace que celle proposée avec le projet.

Tout au long de ce projet, une conclusion nous habitait : l'enseignement de ce cours doit être changé. Installer des serveurs de manière physique est une époque pratiquement révolue. Aujourd'hui dans l'industrie, un serveur qui n'est pas installé de manière virtuelle est un serveur vulnérable, plus difficile à géré et plus sujet à des pannes qui entraînent un temps d'indisponibilité plus élevée et une paralysie plus importante du réseau qu'un serveur virtualisé. Ce n'est pas pour rien que Microsoft insiste particulièrement sur l'implantation de sa solution Hyper-V dans les certifications MCSA. La virtualisation est désormais un standard, du plus petit au plus gros réseau, et maîtriser ce concept ouvre d'innombrables portes sur le marché du travail.

Vous aurez noté également que nous parlons fréquemment de l'aspect sécurité dans ce document. La sécurité est également un autre facteur qui est laissé de côté dans ce cours. Selon le très populaire site *ComputerWorld*, les aptitudes en gestion de la sécurité de réseaux informatiques (*Network Security Management*) figurent parmi les quinze aptitudes les plus en vogue dans l'industrie[4]. Anil Chakravarthy, vice-président exécutif du groupe de la sécurité de l'information chez Symantec affiche :

> *Les compagnies doivent protéger les informations sensibles et à risque de leurs clients, peu importe le média, soit PC, téléphones intelligents ou par le biais de réseaux d'entreprises.*

Jaikumar Vijayan de ComputerWorld en a également fait un article en date du 7 Mars 2013 intitulé «*Demand for IT security experts outstrips supply*»[5]. En 2012, il y avait plus de 67 000 demandes d'emploi dans l'industrie demandant des experts en sécurité informatique, ce qui représente 73 % plus de demandes qu'en 2007. La demande est extrêmement forte, autant dans les entreprises privées que gouvernementales où les infrastructures souffrent encore plus de failles de sécurités massives.

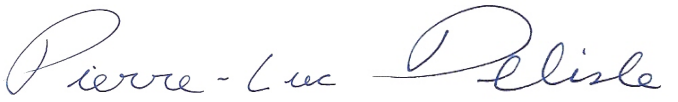
---

[4] http://www.computerworld.com/slideshow/detail/140999/15-non-certified-IT-skills-growing-in-demand?source=cwfb#slide15

[5] http://www.computerworld.com/s/article/9237394/Demand_for_IT_security_experts_outstrips_supply

Finalement, effectuer une connexion VPN sur un routeur de type *consumer grade* dans un cours de fin d'études collégiales est quelque peu loufoque. Nous aurions pu, à la place, créer une connexion VPN entre deux serveurs pfSense. Une telle implémentation aurait pu nous permettre de nous plonger beaucoup plus dans un environnement de production que l'on retrouve en industrie et aurait pu nous faire découvrir beaucoup plus de facettes de la gestion de la sécurité ainsi que du filtrage du trafic au niveau d'un VPN.

Nous espérons que ce rapport ait aidé d'éventuels élèves inscrits dans ce cours. Merci de votre lecture.



Pierre-Luc Delisle

Guillaume Nadeau

Notes

© Pierre-Luc Delisle et Guillaume Nadeau

© Pierre-Luc Delisle et Guillaume Nadeau