

**RAPPORT DE
PROJET DE FIN D'ETUDES**

Pour l'obtention du diplôme : Mastère Professionnel en Nouvelles Technologies
des Télécommunications et Réseaux

Sujet:

**CONFIGURATION ET MISE EN PLACE D'UN DATACENTER
SÉCURISÉ DANS UN ENVIRONNEMENT VIRTUEL.**

Elaboré par:

Nahla Techini Ep Ben Salem

UNIVERSITE VIRTUELLE DE TUNIS

Année Universitaire : 2010/2011

Remerciements

Je tiens à remercier Mr Khaled Sammoud et Mr Maher Keskes pour leurs précieuses assistances et leurs orientations.

Je tiens à présenter mes expressions de reconnaissance envers tous mes enseignants qui ont contribué à ma formation en Mastère N2TR et qui ont participé à l'enrichissement de ma carrière universitaire et aux membres du jury pour l'honneur qu'ils me feront en acceptant de juger ce modeste travail.

Que tous ceux qui, tant aimablement ont participé de près ou de loin à l'élaboration de ce mémoire, trouvent en ces quelques lignes un modeste témoignage d'une sincère gratitude.

Sommaire

Chapitre1 : Introduction générale.....	1
Chapitre2 : Notions générales sur la virtualisation	3
2.1. Définition de la Virtualisation.....	3
2.2. Historique de la Virtualisation	5
2.3. Les avantages de la virtualisation.....	6
2.4. Fonctionnement de la virtualisation.....	7
Chapitre3 : Les risques de sécurité dans un environnement virtuel.....	9
3.1. Virtualisation et sécurité	9
3.2. Solutions de sécurité proposées.....	10
Chapitre 4: Conception et mise en place du centre de données virtuel	12
4.2. Les fonctionnalités de VMware Server 2.0.2	13
4.3. Création d'une machine virtuelle	14
Chapitre 5 : Sécurisation du centre de données virtuel.....	25
5.1. Sécurisation du centre de données virtuel	25
a. Le Pare-feu (ou firewall) Endian	26
5.2. Solution proposée	27
a. Principe du filtrage	26
b. Adressage IP	26
c. Administration du Firewall.....	29
Conclusion	41
Bibliographie	
Annexe	

Chapitre1 : Introduction générale

Depuis quelques années, la virtualisation est au centre des préoccupations des entreprises. On assiste actuellement à une montée en puissance des acteurs du marché, que ce soit dans le domaine propriétaire avec *Microsoft* et *VMware*, ou dans le monde des logiciels libres, avec l'émergence de nombreux projets autour de la virtualisation tels que *XEN* ou *OpenVZ*.

La virtualisation a donc tendance de s'introduire, voire s'imposer, de plus en plus dans les parcs de serveurs, les systèmes de stockage et les réseaux des organisations.

Comme lors de l'avènement de toute nouvelle technologie, la sécurité reste trop souvent négligée. Pourtant, les risques existent et ne doivent pas être négligés.

Grâce à la virtualisation, l'efficacité et la disponibilité des ressources et applications informatiques seront améliorées. On commence par abandonner l'ancien modèle "un serveur, une application" et exécute plusieurs machines virtuelles sur chaque machine physique. On allège la tâche des administrateurs informatiques, qui passent plus de temps à gérer les serveurs qu'à innover. Dans un Datacenter non virtualisé, près de 70 % d'un budget informatique type sont consacrés à la simple maintenance de l'infrastructure existante, ce qui laisse peu pour l'innovation.

Un Datacenter automatisé, reposant sur la plate-forme de virtualisation VMware, éprouvée en production, nous permet de répondre de façon plus efficace et plus rapide à l'évolution du marché.

C'est dans ce contexte que s'inscrit notre projet de fin d'études. Il s'agit de concevoir et de réaliser une solution de virtualisation d'un centre de données, et de mettre en place une solution de sécurité adaptée à la technologie de virtualisation utilisée.

Le présent rapport rend compte de tout ce qui a été réalisé durant ce projet. Il s'articulera autour de cinq chapitres. Le premier chapitre « Introduction générale ».

Le second chapitre « Notions générales sur la virtualisation » consiste à présenter le concept de virtualisation et la terminologie qui lui est associée.

Le troisième chapitre « Les risques de sécurité dans un environnement virtuel » exposera les risques de sécurité liés aux architectures virtualisées et les différentes stratégies de sécurisation tentées.

Dans le quatrième chapitre « Conception et mise en place du centre de données virtuel », nous présenterons ce que nous avons réalisé dans le projet de virtualisation des machines ainsi que l'environnement virtuel VMware qui constitue notre environnement de travail.

Dans le cinquième chapitre « sécurisation du centre de données virtuel », nous traiterons particulièrement l'aspect sécurité grâce à un firewall pour sécuriser notre environnement virtuel.

Objectifs du projet

- Mettre en place un centre de données.
- Optimiser l'usage des ressources physiques en utilisant une architecture virtualisée.
- Augmenter la fiabilité des services rendus en assurant leur disponibilité et leur continuité.
- Isoler au mieux les services entre eux.
- Assurer la sécurité et la sûreté du centre de données en sécurisant le flux à l'intérieur de l'environnement virtuel, ainsi que le flux sortant.

Chapitre2 : Notions générales sur la virtualisation

La virtualisation est une technologie de plus en plus incontournable. Les environnements virtuels sont très en vogue au sein des entreprises de toutes tailles. Il est vrai que les avantages de cette technologie sont nombreux en termes de productivité, de coûts et d'exploitation. En effet, elle permet des baisses de coûts importantes par la réduction du nombre de machines physiques, mais aussi par toutes les autres économies induites : énergie, temps de mise en œuvre,... Toutefois, toutes nouveautés technologiques, surtout quand elles rencontrent un fort engouement, déplacent ou créent des problèmes de sécurité à ne pas négliger. On considère que la principale menace qui pèse sur la virtualisation est la méconnaissance des risques par les utilisateurs. Pour lui, l'un des points clés de ces déploiements repose sur la collaboration entre les différentes équipes impliquées : système, réseau et sécurité.

Aujourd'hui, VMware se positionne comme un fournisseur d'OS qui se veut toujours plus sécurisé

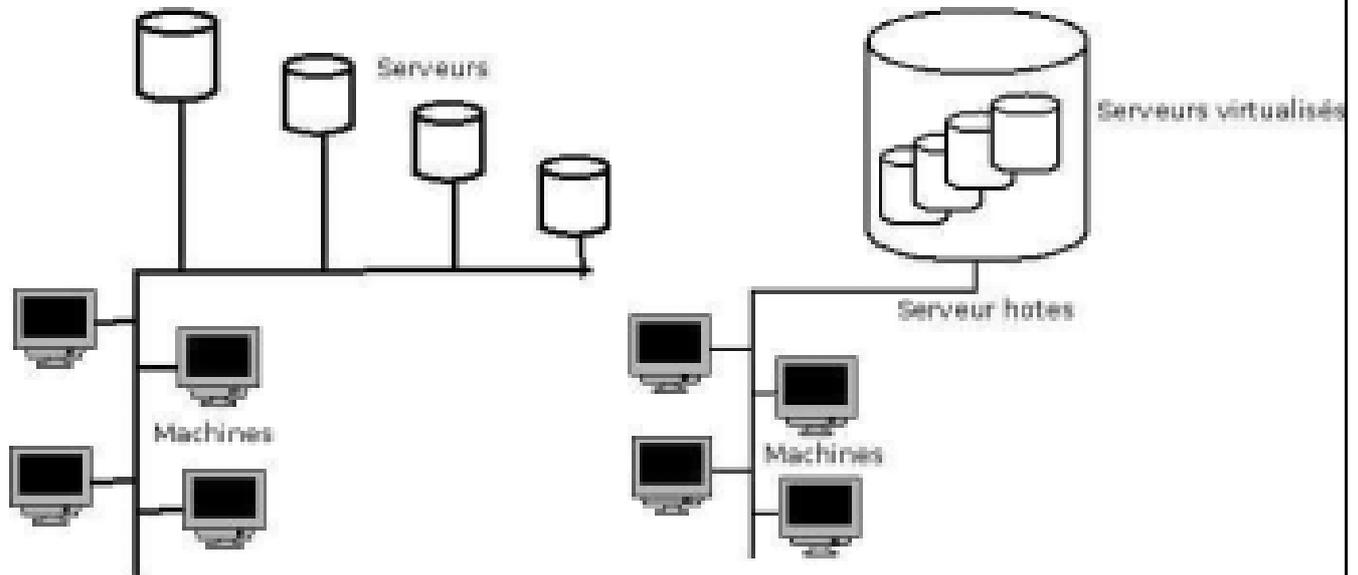
2.1. Définition de la Virtualisation

Dans le monde de l'informatique, on définit la virtualisation comme un ensemble de techniques visant à faire fonctionner plusieurs systèmes d'exploitation sur le même matériel en partageant les ressources de celui-ci.

En d'autres termes, c'est une technique qui consiste à réaliser une abstraction des caractéristiques physiques de ressources informatiques afin de les présenter à des systèmes, des applications ou des utilisateurs

- Diviser une ressource physique (serveur, système d'exploitation, périphérique de stockage) en plusieurs ressources logiques

- Agréger plusieurs ressources physiques (périphériques de stockages, serveurs) en une ressource logique.

*Architecture traditionnelle**Architecture virtualisée*

A l'heure actuelle, la virtualisation semble être en effet la seule solution viable pour réduire réellement les coûts liés au SI (Système d'Information). La Virtualisation impacte 3 domaines majeurs, qui sont :

- Le système d'exploitation (OS en anglais pour Operating System)
- Les applications
- Le stockage

La virtualisation impacte aussi d'autres domaines mais moindre comme :

- Le réseau
- La sécurité

Le but recherché par la virtualisation, est de faire croire au système d'exploitation virtualisé (ou système hôte) qu'il est installé sur une machine physique.

Les serveurs sont malgré tout les plus touchés par le besoin de virtualisation, et ce pour plusieurs raisons :

Les serveurs sont peu chargés, entre 10% et 20% de charge maximum en moyenne, pour subvenir au principe une application = 1 serveur. Gâchis nécessaire pour assurer le bon fonctionnement de l'ensemble en cas de forte charge à un instant `T`.

Les serveurs sont également Monosystèmes. Il est impossible de faire tourner 2 systèmes d'exploitation en parallèle physiquement sur la machine puisque celle-ci doit gérer 100% des ressources systèmes.

S'il fallait autant de serveur que d'applications par entreprises, les besoins en espace, en électricité, en climatisation, seraient ingérables par entreprises.

Le principe :

On considère un serveur comme un ensemble de ressources : CPU - RAM - Disque - Réseau. Ces ressources sont allouées de manière statique ou dynamique suivant les besoins à des machines virtuelles (VM pour Virtual Machines).

Il est donc de rigueur que la virtualisation nous permet de la souplesse dans l'administration des serveurs en entreprise, mais aussi une gestion centralisée de ces serveurs.

2.2. Historique de la Virtualisation

La virtualisation comme on la connaît aujourd'hui n'est pas un procédé novateur bien au contraire. Big Blue (IBM) en est le précurseur, dès les années 1980, un premier hyperviseur (on reviendra dessus dans un chapitre consacré) étant lancé.

Les grands Unix ont suivi avec les architectures NUMA, des Superdome d'HP(PA-RISC et IA-64 Intel) et des E10000/E15000 de Sun (UltraSparc).

Dans la seconde moitié des années 1990, les émulateurs sur x86 des vieilles machines des années 1980 ont connu un énorme succès, notamment les ordinateurs Amstrad, Atari, Amiga et les consoles NES, SNES, et Neo-Geo AES.

Ensuite ce fût le tour de la société VMware qui développa et popularisa une solution propriétaire fin 90 et début 2000 se fût l'explosion des solutions de virtualisation sur des architectures de type x86.

Il existe aussi quelques équivalents libres, tels que XEN Hyperviseur, QEMU, Bochs, Linux-vServer, ou VirtualBoX, et aussi dans le même temps des logiciels gratuits, VirtualPC et VirtualServer de Microsoft, mais aussi VMware Server, VMware Player qui sont par contre des solutions dites embarquées (produisant des machines virtuelles mais s'installant sur un hôte installé au préalable, un Windows ou Linux)

Ce n'est que très récemment que VMware décida de rendre gratuit son hyperviseur phare ESXi basée sur ESX Server.

Il est de paire avec la virtualisation que les ténors de l'architecture x86 : Intel et AMD (brevets appartenant à Intel) intégraient la mise en œuvre matérielle des solutions de virtualisation dans leurs processeurs lors de la seconde moitié de l'an 2000.

2.3. Les avantages de la virtualisation

La virtualisation de l'infrastructure permet de réduire les coûts informatiques tout en augmentant l'efficacité, le taux d'utilisation et la flexibilité des actifs existants. Des entreprises du monde entier et de toutes tailles tirent avantage de la virtualisation VMware. Des milliers d'organisations, dont tous les membres du classement Fortune 100, utilisent les solutions de virtualisation VMware.

5 bonnes raisons d'adopter la virtualisation

- Rentabiliser davantage les ressources existantes : regrouper les ressources communes en sortant du schéma « une application = un serveur » grâce à la consolidation des serveurs.
- Réduire les coûts générés par le Datacenter en minimisant l'infrastructure physique et en améliorant le rapport serveur/admin. : les serveurs et les équipements matériels associés sont en nombre réduit. Cela se traduit par une diminution des frais immobiliers et des besoins en alimentation et en ventilation.
- Augmenter la disponibilité du matériel et des applications pour une amélioration de la continuité d'activité : sauvegarder et migrer des environnements virtuels complets sans interruption dans le service. Éviter les interruptions planifiées et trouver immédiatement la solution à des problèmes imprévus.

- Gagnez en flexibilité opérationnelle : s'adapter à l'évolution du marché grâce à une gestion dynamique des ressources, un provisionnement accéléré des serveurs et un déploiement optimal des postes de travail et des applications.
- Améliorer la gérabilité et la sécurité du poste de travail : déployer, gérer et surveiller des environnements de postes de travail sécurisés auxquels les utilisateurs peuvent accéder localement ou à distance, avec ou sans connexion réseau, à partir de presque tous les ordinateurs de bureau, portables ou de poches.

2.4. Fonctionnement de la virtualisation

La plate-forme de virtualisation VMware repose sur une architecture directement exploitable. Nous allons utiliser des logiciels tels que VMware Server pour transformer ou « virtualiser » les ressources matérielles d'un ordinateur x86 (dont le processeur, la RAM, le disque dur et le contrôleur réseau) afin de créer une machine virtuelle entièrement fonctionnelle, capable d'exécuter son propre système d'exploitation et ses propres applications comme un véritable ordinateur. Chaque machine contient un système complet, ce qui permet d'éviter tout conflit éventuel. L'approche adoptée par VMware pour la virtualisation consiste à insérer une fine couche logicielle directement sur le matériel informatique ou sur un système d'exploitation hôte. Cette couche logicielle contient un moniteur de machine virtuelle ou « hyperviseur » qui alloue les ressources matérielles de façon dynamique et transparente. Ainsi, plusieurs systèmes d'exploitation peuvent fonctionner simultanément sur un seul ordinateur physique et partager leurs ressources matérielles. En encapsulant une machine complète, notamment le processeur, la mémoire, le système d'exploitation et les périphériques réseau, la machine virtuelle est totalement compatible avec tous les systèmes d'exploitation, applications et pilotes de périphériques de systèmes x86 standard. Vous pouvez exécuter en toute sécurité plusieurs systèmes d'exploitation et applications en parallèle sur un seul ordinateur, chacun(e) ayant accès aux ressources requises au moment voulu.

Conclusion

La virtualisation d'un seul ordinateur physique n'est qu'un début. Durant, notre projet nous allons mettre en place une infrastructure virtuelle complète, en intégrant des ordinateurs

virtuels de stockage interconnectés avec VMware Server, une plate-forme de virtualisation éprouvée formant la base de développement des clouds privés et publics.

Chapitre3 :

Les risques de sécurité dans un environnement virtuel

La virtualisation soulève un certain nombre de problèmes de sécurité car le moindre incident au niveau de la plate-forme d'hébergement met en danger tout le centre de données virtuel. L'administration partagée de plusieurs machines virtuelles au niveau du système hôte engendre des risques, tout comme l'accès partagé à des ressources qui étaient précédemment séparées par des frontières matérielles. La gestion de ces risques est cruciale.

Ce chapitre vise à présenter les risques potentiels associés à la virtualisation. Il expliquera pourquoi les stratégies de sécurité traditionnelles ne fonctionnent pas avec les environnements virtualisés et mettra en évidence la stratégie adaptée à ces environnements.

3.1. Virtualisation et sécurité

Tout d'abord, il convient d'écarter un certain nombre d'idées reçues en matière de sécurité des environnements virtuels.

1. Un système ne devient pas plus vulnérable parce qu'il est virtualisé. Il se contente de conserver ses failles habituelles. Il est éventuellement plus sensible aux dénis de services si les ressources allouées sont réduites au minimum requis.
2. Même s'il n'existe pas de limites à l'ingéniosité des hackers, et si l'on suppose que l'un d'entre eux ait pris le contrôle d'une de vos machines virtuelles, il est peu probable que celui-ci réussisse, par rebond, à atteindre le système de virtualisation lui-même. Afin de minimiser une telle menace, il suffit à l'administrateur de n'autoriser aucun accès d'un hôte virtuel à une ressource physique.

Le risque réside ailleurs. Le fait est que l'on dispose rarement d'autant d'interfaces physiques qu'il existe d'hôtes virtuels sur une plateforme matérielle. Cela implique donc que l'on crée des hubs ou des switches virtuels sur lequel on connecte plusieurs hôtes virtuels.

On associe ensuite à chacun de ces switches une interface physique permettant aux hôtes de communiquer avec le monde extérieur.

On crée ainsi des réseaux virtuels échappant totalement aux règles de segmentation en vigueur dans l'entreprise :

- D'une part, les hôtes réunis sur un même Switch virtuel devraient parfois être distribués sur les segments différents (parce qu'ils correspondent à des niveaux de sécurité distincts).
- D'autre part, selon la façon dont ces switches sont paramétrés, il est parfois possible de passer d'un segment virtuel à un autre.

3.2. Solutions de sécurité proposées

- La première étape doit être d'ordre organisationnel, il est important qu'il y ait une collaboration forte entre les équipes réseau, système et sécurité. Les architectures virtuelles doivent être considérées comme des environnements classiques avec les mêmes stratégies de sécurisation, de surveillance, d'audit, de contrôle et de cloisonnement.

Toutefois, elles ne doivent pas s'arrêter devant un serveur ou des lames, mais aller en profondeur, jusqu'au sein de l'architecture virtuelle.

- Chaque machine virtuelle doit être traitée exactement comme une machine réelle. Il faut donc avoir les mêmes réflexes que pour un serveur d'entreprise classique, du durcissement de l'OS jusqu'à l'anti-virus en passant par les stratégies d'accès.

Le piège réside dans la facilité de mise en place de clone de machines ou de duplication d'application. Il faut éviter à tout prix de cloner une machine qui a été durcie ou patchée il y a 3 ans et s'en satisfaire. De plus, la multiplication des environnements R&D, pré-production, production et parfois leur proximité peut s'avérer une catastrophe. Il n'est pas rare que des machines restent actives sans aucune gestion, car oubliées après quelques jours de tests. La rapidité et la facilité de mise en place d'un environnement impliquent, en contrepartie, une procédure stricte pour s'assurer de la bonne mise en place de la sécurité de cette future plateforme. Il faut également durcir l'hyperviseur sur lequel tout repose. Nativement, il s'agit de systèmes très optimisés et durcis, mais il existe un grand nombre d'éléments à contrôler et des règles assez classiques à mettre en places, telles que la séparation des flux de maintenance des flux de production, la protection d'accès à distance, l'authentification, la politique de gestion de mots de passe, la limitation d'accès au fichier, etc. De plus, il faut penser à désactiver certaines fonctionnalités propres à ces

environnements pour des serveurs de productions : désactiver la fonction de copier/coller entre le système hôte et la console est une parfaite illustration.

Enfin, il reste nécessaire, pour un parfait contrôle, de protéger l'architecture à l'aide d'équipements Firewall et IPS réels et notamment les flux liés à l'exploitation de ces environnements.

- Les organisations cherchant à améliorer la sécurité de la virtualisation ont dû envisager l'utilisation de produits matériels extérieurs à l'environnement virtuel.

Les composants de sécurité réseau ne pouvant toutefois être virtualisés, l'organisation ne peut toujours pas voir à l'intérieur de l'environnement virtuel, ce qui induit des difficultés supplémentaires en termes de conformité et d'audit. En outre, l'architecture ne tire pas pleinement profit des avantages de la virtualisation, générant ainsi des coûts supplémentaires dus à la complexité, à l'électricité, à la ventilation, etc.

Dans un environnement virtuel, en revanche, où de multiples applications et serveurs résident sur un seul serveur, une fois que le hacker a pénétré cette couche, il a accès à tout ce qui se trouve dans des dizaines voire des centaines de systèmes, d'applications et de bases de données.

En outre, les contrôles habituellement placés autour de chaque application n'existent pas dans un environnement virtuel. Par conséquent, la capacité d'une organisation à déterminer qui a accédé aux différentes informations et à quel moment est sérieusement compromise.

Conclusion

Pour tenter de résoudre les problèmes de sécurité liés à la virtualisation, il convient de créer une architecture séparée en zones pour bien maîtriser leur sécurisation.

Dans ce cadre, le chapitre suivant décrit la mise en place de notre architecture virtualisée et les solutions de sécurité proposées.

Chapitre 4: Conception et mise en place du centre de données virtuel

Dans ce chapitre nous exposerons l'environnement de virtualisation utilisé pour détailler notre proposition d'architecture du centre de données.

4.1. VMWare Server

Basé sur la technologie de VMware à la fiabilité éprouvée, VMware Server permet aux utilisateurs de partitionner leur serveur physique en plusieurs machines virtuelles, en vue d'une meilleure utilisation des ressources informatiques et d'une administration simplifiée.

VMware Server est une solution simple et robuste. Sa nouvelle interface Web d'administration, très intuitive, est identique pour les utilisateurs de Linux et de Windows. Cette nouvelle version supporte un large panel de plates-formes et plus de 30 systèmes d'exploitation d'hôtes, dont plusieurs distributions Linux, Windows Server 2003, Windows Server 2008 (bêta) et Windows Vista.

Logiciel non libre mais fourni gratuitement par VMWare. Il permet à n'importe qui de pouvoir continuer à utiliser un logiciel particulier tournant sous Windows. Ce système est similaire à Virtualbox mais est mieux reconnu par les machines virtuelles notamment les Windows. Ce système est également plus stable et fiable à l'usage que Virtualbox.



Dans le cadre du projet, nous avons installé la version 2.0.2 du VMWare Server qui admet des nouvelles fonctionnalités traitées dans la partie suivante.

4.2. Les fonctionnalités de VMware Server 2.0.2

- **Nouvelle prise en charge des systèmes d'exploitation:** La plus vaste prise en charge de systèmes d'exploitation pour toute plate-forme de virtualisation hôte actuellement disponible, notamment Windows Server 2008, Windows Vista Éditions Business et Ultimate (client uniquement), Red Hat Enterprise Linux 5 et Ubuntu 8.04.
- **Prise en charge des systèmes d'exploitation 64 bits:** Utilisation de systèmes d'exploitation clients 64 bits sur un matériel 64 bits pour permettre des solutions informatiques plus évolutives et plus performantes. En outre, Server 2 s'exécute en mode natif sur les systèmes d'exploitation hôtes Linux 64 bits.
- **Interface de gestion VMware Infrastructure (VI) Web Access:** L'interface de gestion VI Web Access offre une approche de gestion à la fois simple, flexible, sûre, intuitive et productive. En outre, accédez à des milliers d'applications d'entreprise préconfigurées et prêtes à l'emploi, fournies avec un système d'exploitation d'une machine virtuelle, sur la console de machine virtuelle indépendante Virtual Appliance Marketplace.
- **Console de machine virtuelle indépendante:** Avec la nouvelle console distante VMware, vous pouvez accéder à vos consoles de machine virtuelle indépendamment de l'interface de gestion VI Web Access.
- **Des machines virtuelles plus évolutives :** Prise en charge de jusqu'à 8 Go de RAM et 10 cartes réseau virtuelles par machine virtuelle, transfert de données à des débits de données plus élevés à partir de périphériques USB 2.0 et ajout de nouveaux disques durs et contrôleurs SCSI à une machine virtuelle active.
- **Volume Shadow Copy Service (VSS):** Sauvegardez correctement l'état des machines virtuelles Windows lorsque vous utilisez la fonctionnalité de snapshot pour garantir l'intégrité des données des applications s'exécutant dans la machine virtuelle.
- **Prise en charge de l'interface de la machine virtuelle (VMI):** Cette fonctionnalité permet la transparence de la paravirtualisation dans laquelle une même version binaire du système d'exploitation peut être exécutée sur du matériel natif ou sur un

hyperviseur en mode paravirtualisé pour améliorer les performances des environnements Linux spécifiques.

- **Interface de communication VMware Virtual Machine (VMCI):** Prise en charge d'un système de communication rapide et efficace entre une machine virtuelle et le système d'exploitation hôte, ainsi qu'entre deux machines virtuelles (ou plus) sur le même hôte.
- **Prise en charge de VIX API 1.5:** Cette fonctionnalité offre une interface de programmation permettant d'automatiser les opérations des clients et des machines virtuelles.

4.3. Création d'une machine virtuelle

La création d'une machine virtuelle dans VMWare est un processus direct une fois que le serveur VMWare est en marche.

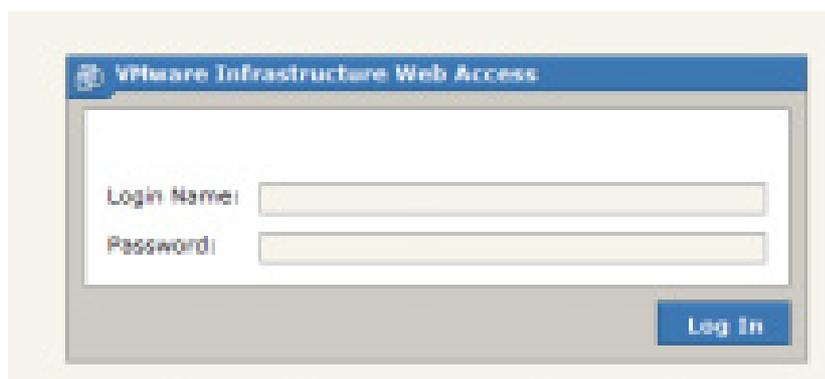
La connexion à VMWare se fait via un navigateur Web en introduisant l'URL suivante :

<http://localhost:8222/>

Ou bien en mode sécurisé:

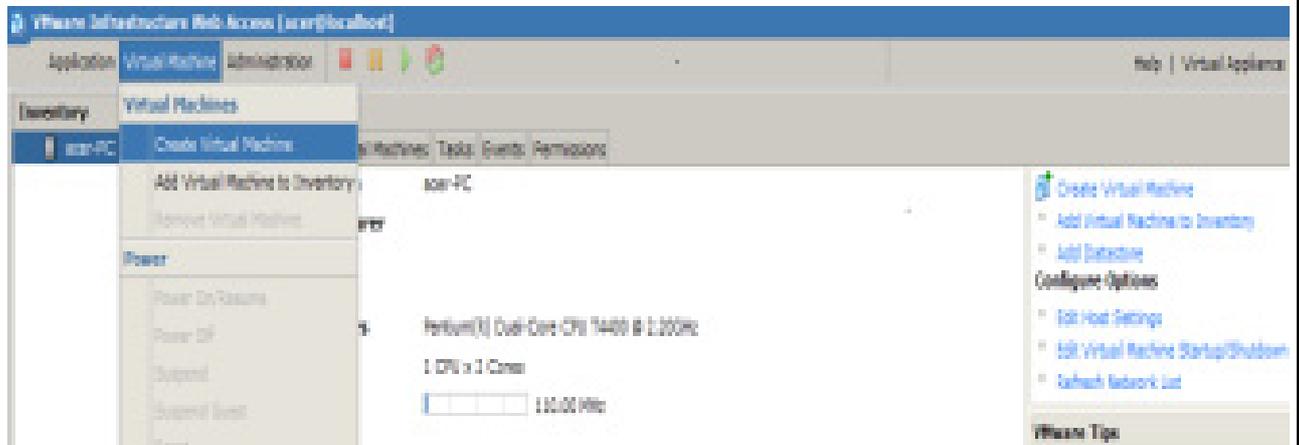
<https://localhost:8333/>

L'interface suivante s'affiche:

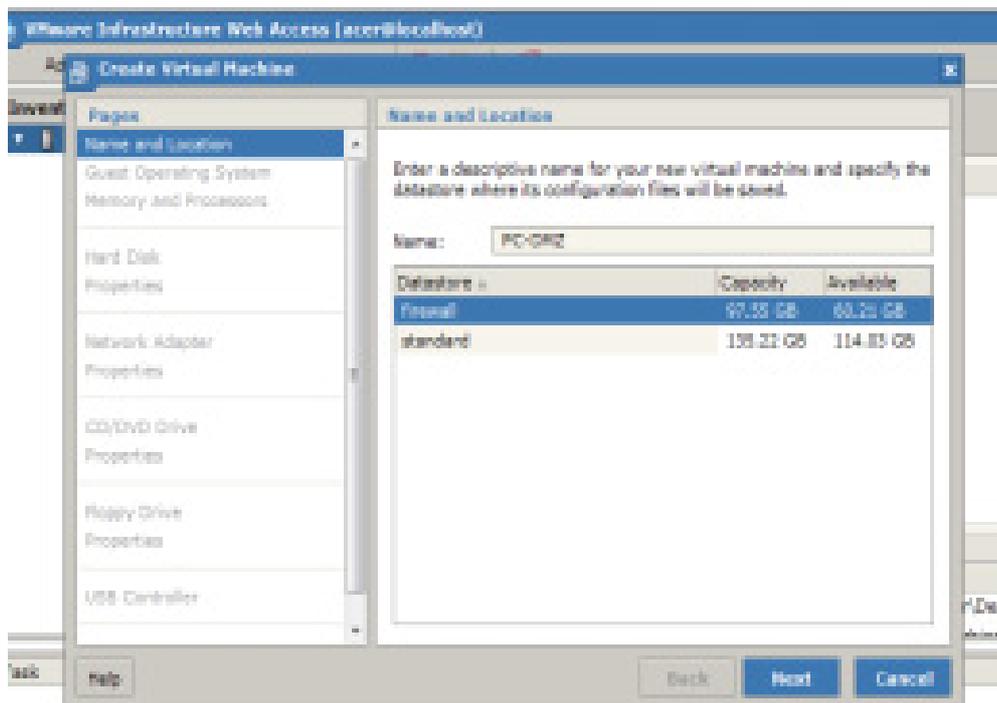


Il faut introduire les paramètres (nom/mot de passe) de connexion de notre machine.

Une fois que nous sommes connectés sur notre console de serveur VMWare, l'installation d'une machine virtuelle est décrite comme suit :

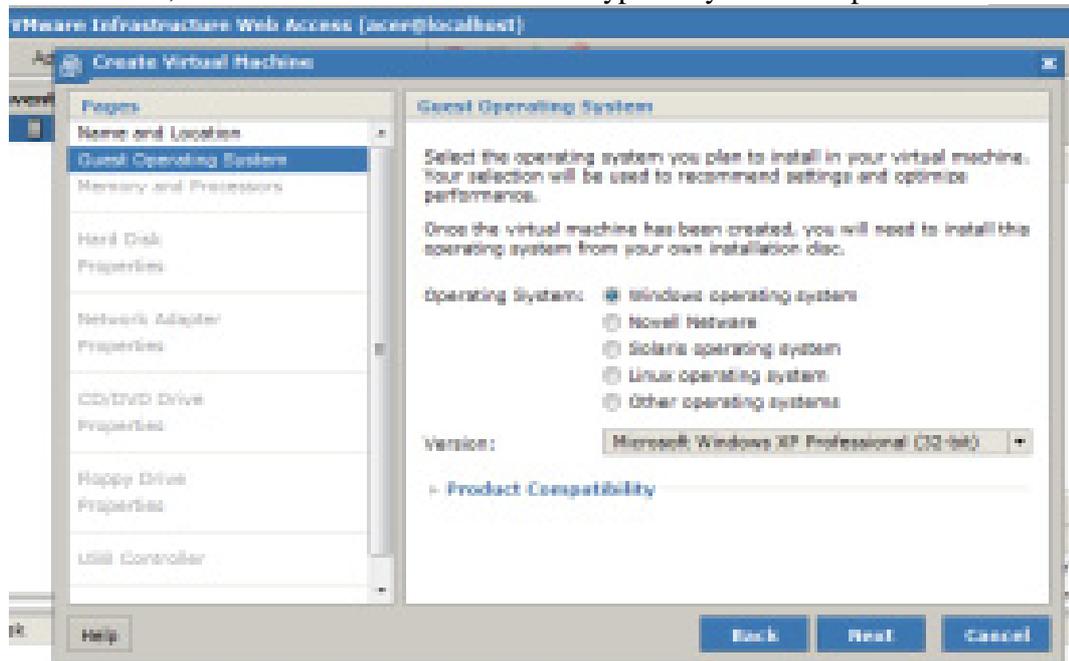


Dans le coin droit de notre fenêtre, nous cliquons sur "Create Virtual Machine" et la fenêtre suivante devrait surgir :



Il faut Choisir un nom pour notre machine virtuelle, dans notre exemple "PC-DMZ".
Nous cliquons sur "Next".

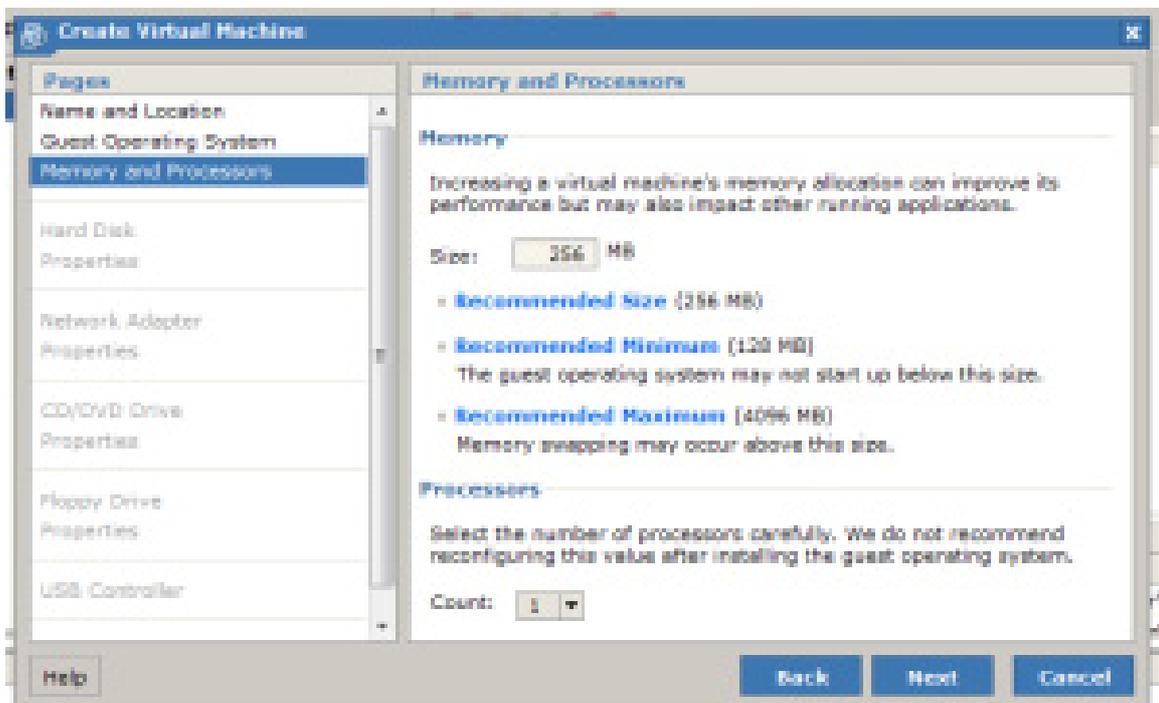
Dans l'écran suivant, on nous demandera de choisir le type de système d'exploitation :



On sélectionne le système d'exploitation désiré.

Dans notre exemple, nous choisirons "Microsoft windows Server 2003 Standard Edition".
Nous cliquons sur "Next".

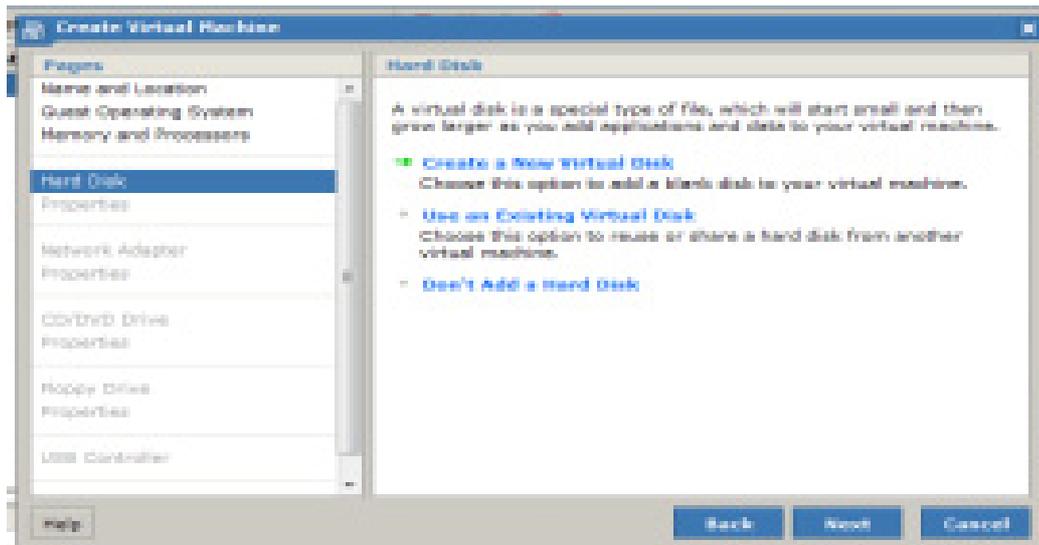
Dans cet écran nous devons choisir la quantité de mémoire que nous voulons allouer pour la machine virtuelle :



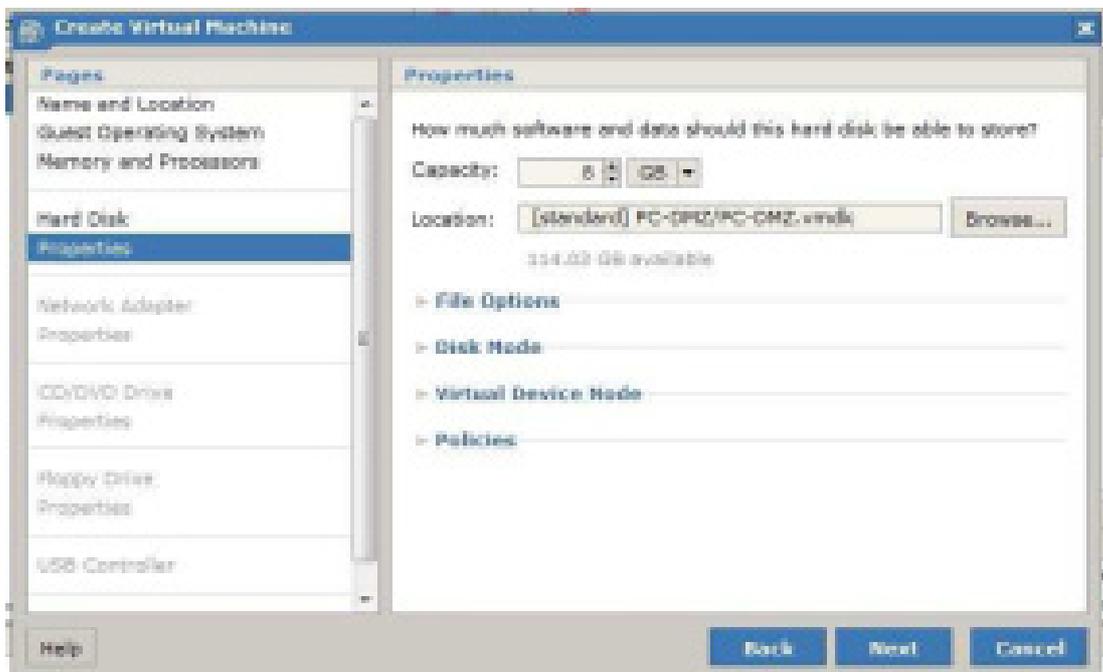
Pour cette machine virtuelle nous allons allouer 256 MO et nous choisirons 1 processeur pour le système. Ceci à un impact lors de l'exécution sur les performances de notre machine physique aussi bien que la machine virtuelle.

Nous cliquons sur "Next".

Sur l'écran suivant, nous devons créer et donner la taille du disque virtuel que la machine virtuelle utilisera :

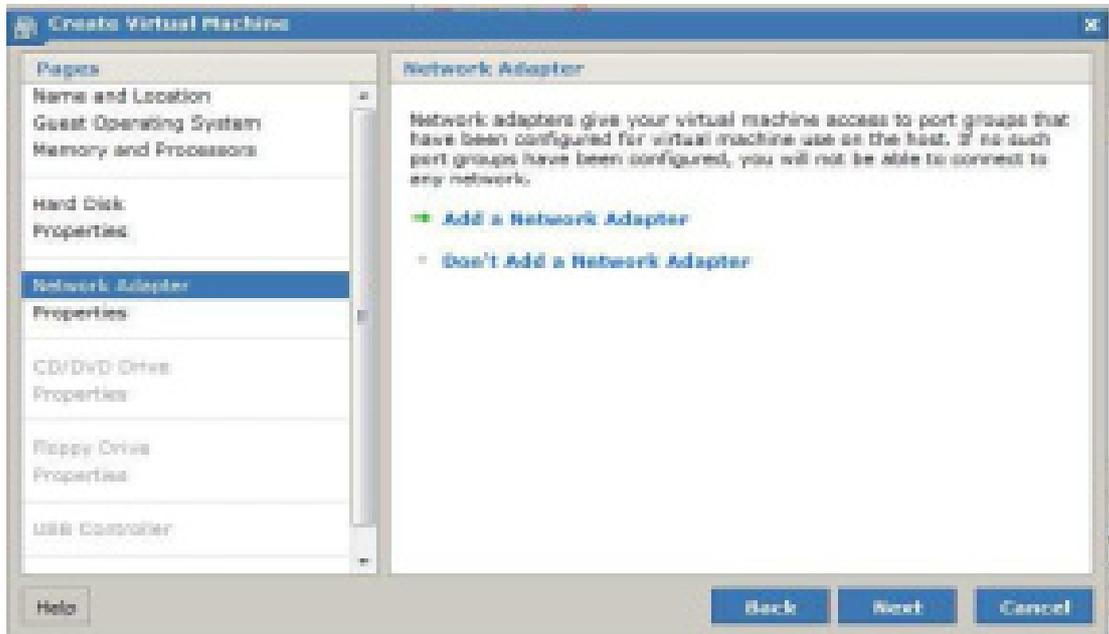


Nous cliquons sur "Create a New Virtual Disk" et l'écran suivant devrait apparaître :

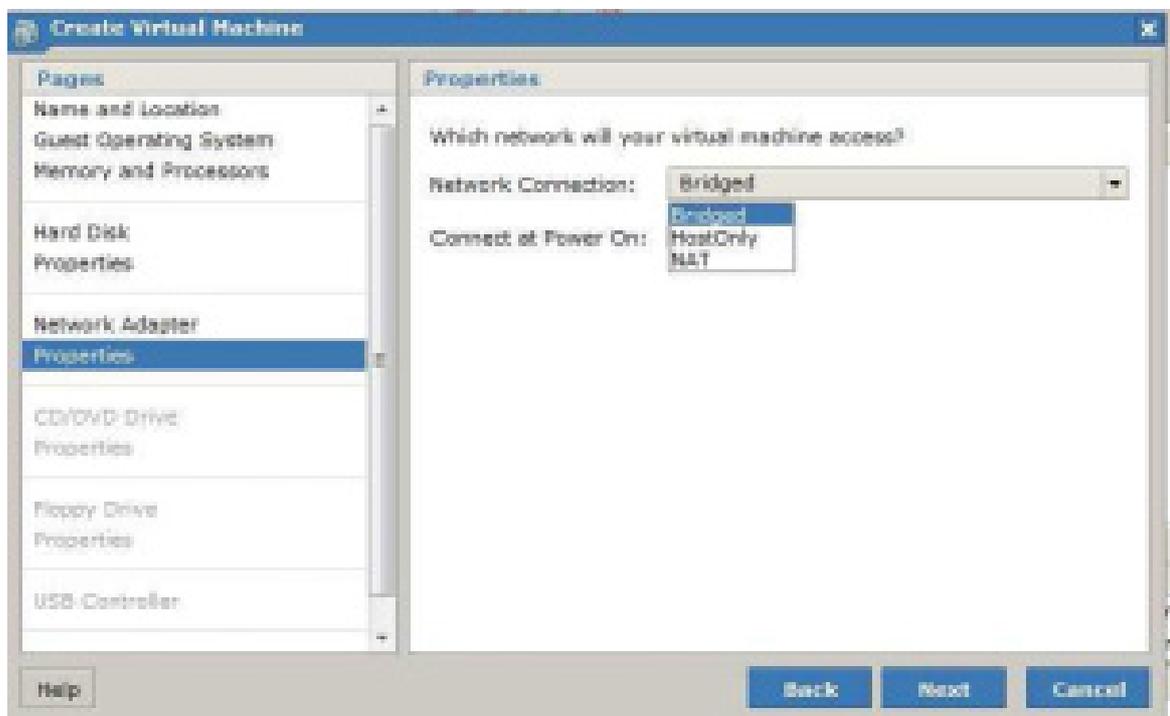


Nous donnerons une taille de disque dur, exemple 8 GB pour notre machine virtuelle "PC-DMZ".

L'écran suivant permet de créer une carte réseaux avec différents paramètres.



Nous cliquons sur "Add a Network Adapter" et la fenêtre suivante devrait surgir :



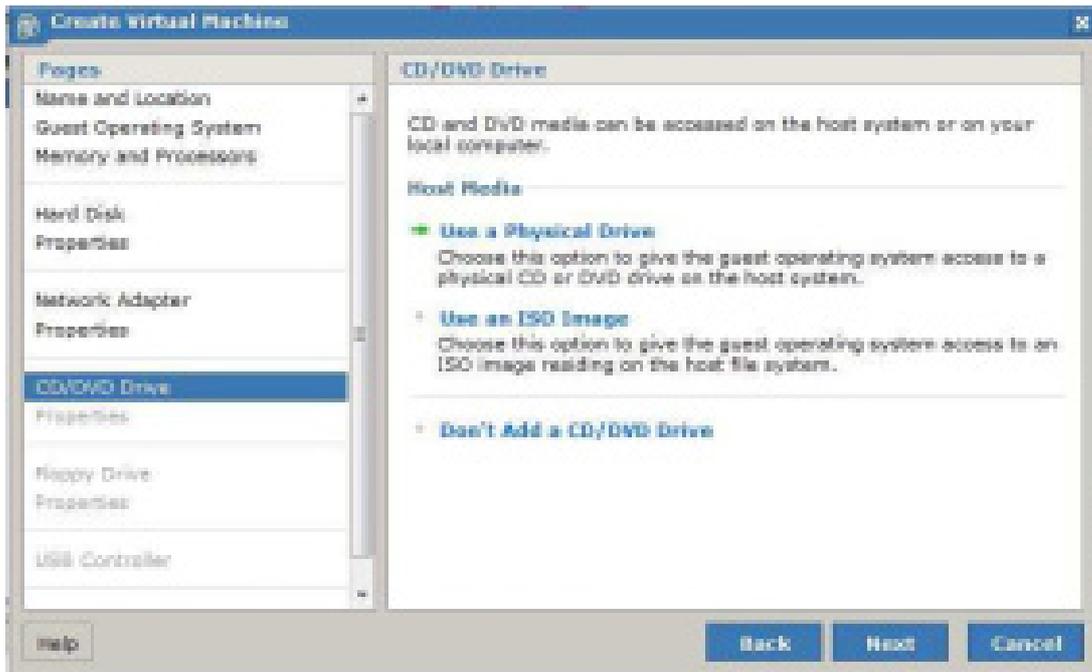
Pour notre réseau, nous utiliserons les paramètres par défaut, soit "Bridged".

Mais il en existe plusieurs dont voici la liste :

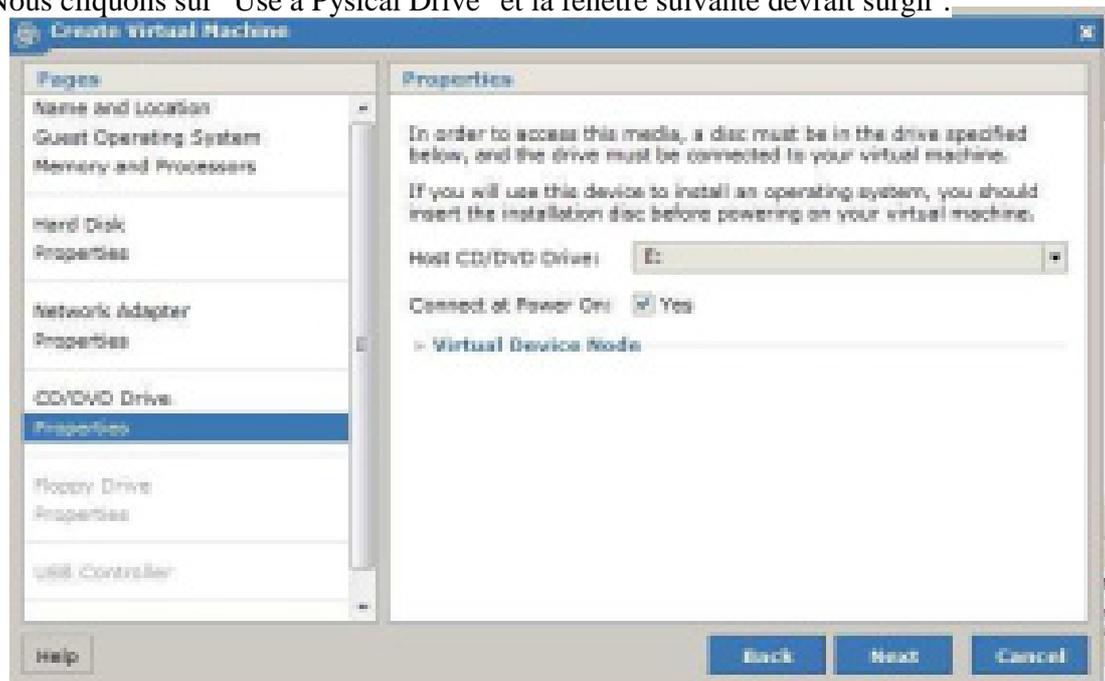
- Bridged
- HostOnly
- NAT

Nous cliquons sur "Next".

Ensuite, nous devons choisir le type de lecteur CD/DVD pour notre machine virtuelle.



Nous cliquons sur "Use a Physical Drive" et la fenêtre suivante devrait surgir :

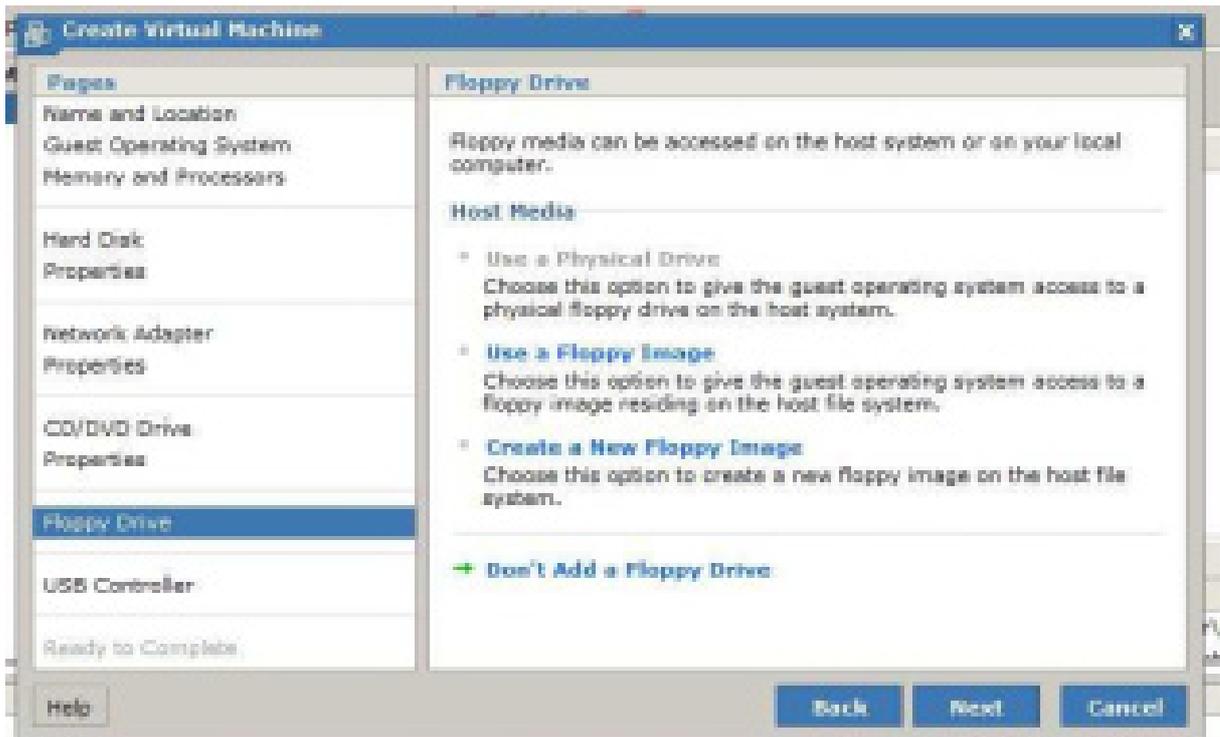


Choisissons la lettre du disque physique de notre ordinateur, dans mon cas, c'est la lettre du disque E.

Assurons-nous que l'option "Connect at Power On" est bien coché.

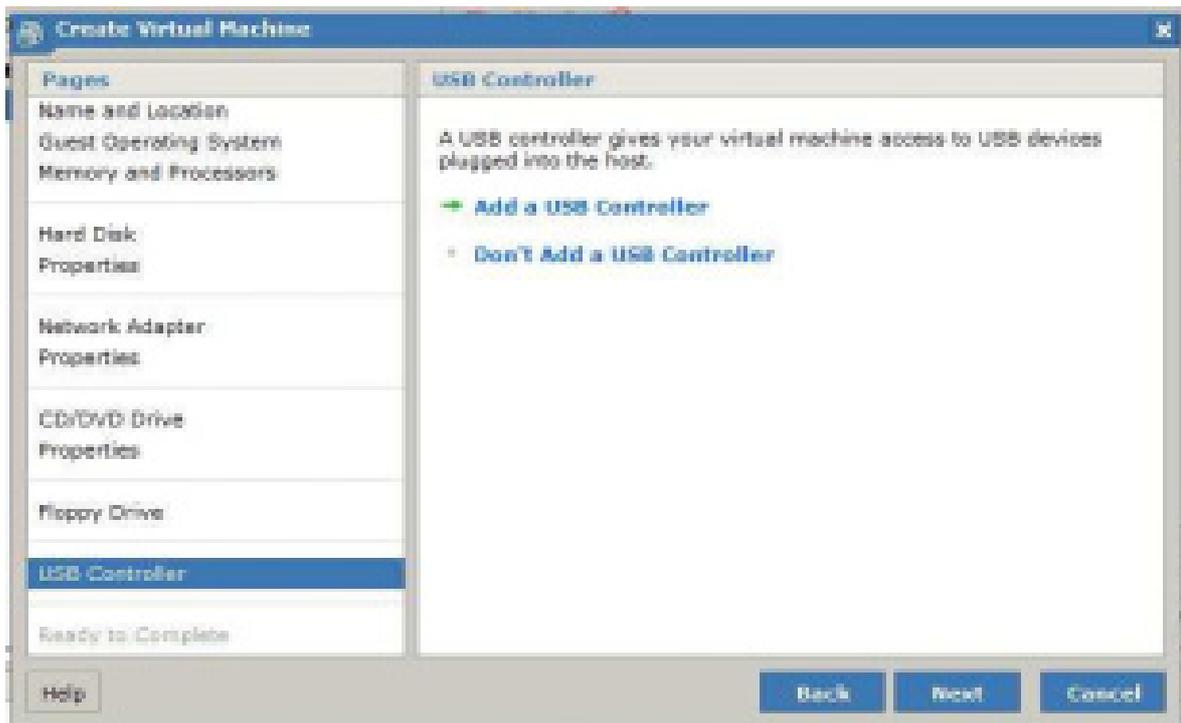
Ensuite, nous devons choisir si nous avons besoin d'un Lecteur de disquettes pour notre machine virtuelle.

Nous n'utiliserons pas de lecteur de disquettes sur cette machine virtuelle.



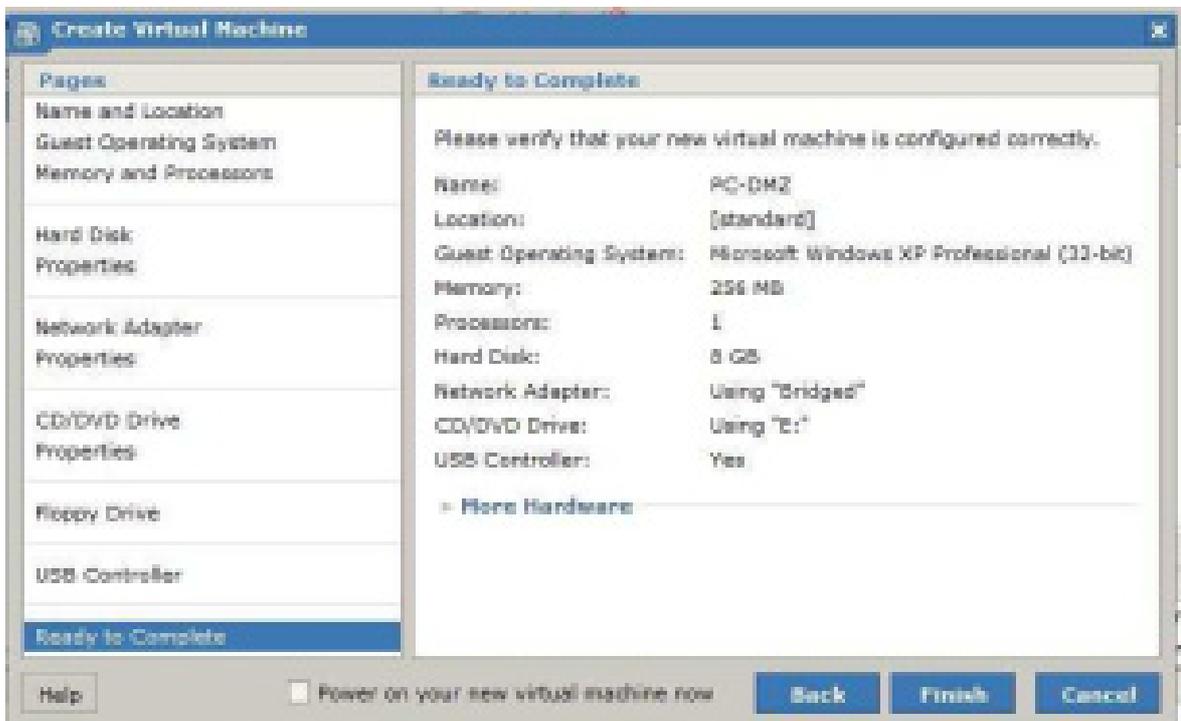
Nous cliquons sur "Don't add a Floppy Drive".

Sur l'écran suivant, nous devons choisir si nous voulons avoir l'accès au contrôleur USB dans la machine hôte:



Nous cliquons sur "Add USB Controller".

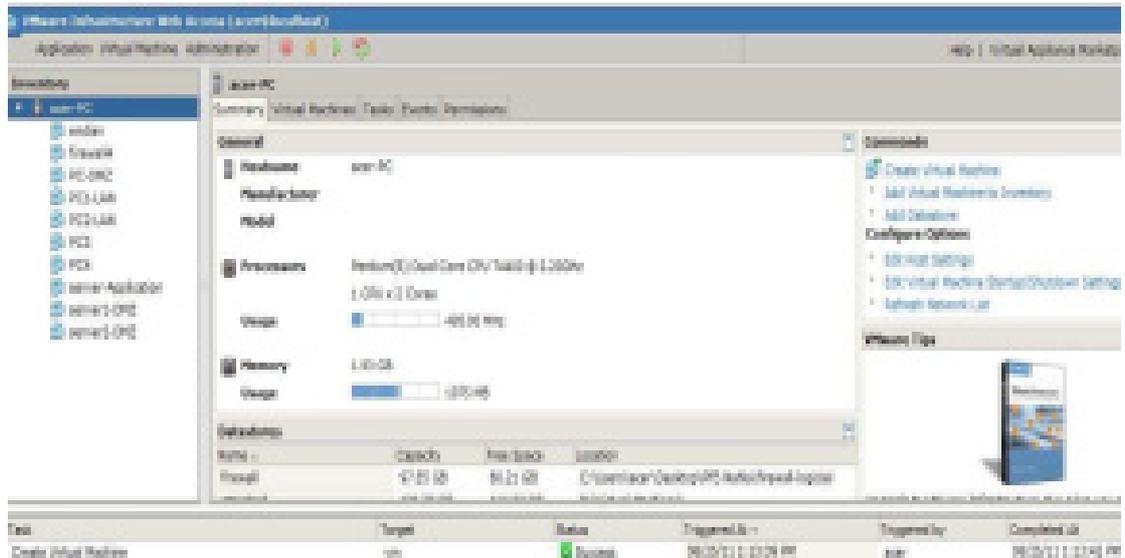
Ensuite, sur l'écran suivant, nous obtiendrons le résumé de la configuration de notre machine virtuelle :



A ce point, la création de notre machine virtuelle est prête à être achever. Nous cliquons sur "Finish".

L'installation devrait maintenant être achevée.

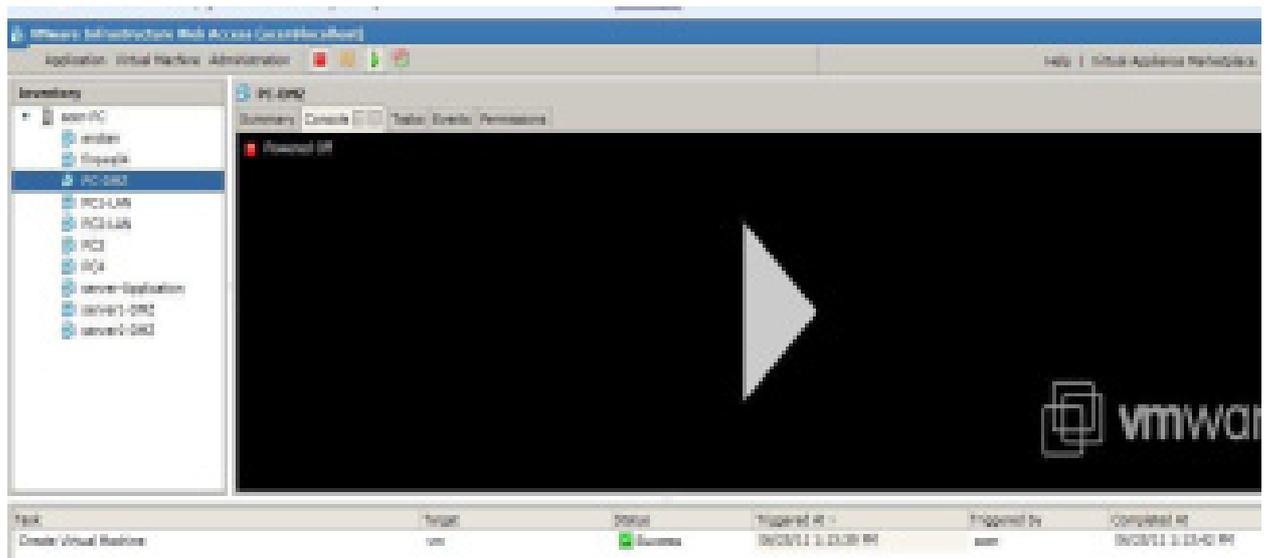
Maintenant, le nom de notre machine virtuelle devrait apparaître du côté gauche supérieur de la console de VMWare (inventory) indiquant que la machine virtuelle a été créée.



Maintenant nous sommes prêts à commencer l'installation de notre système d'exploitation.

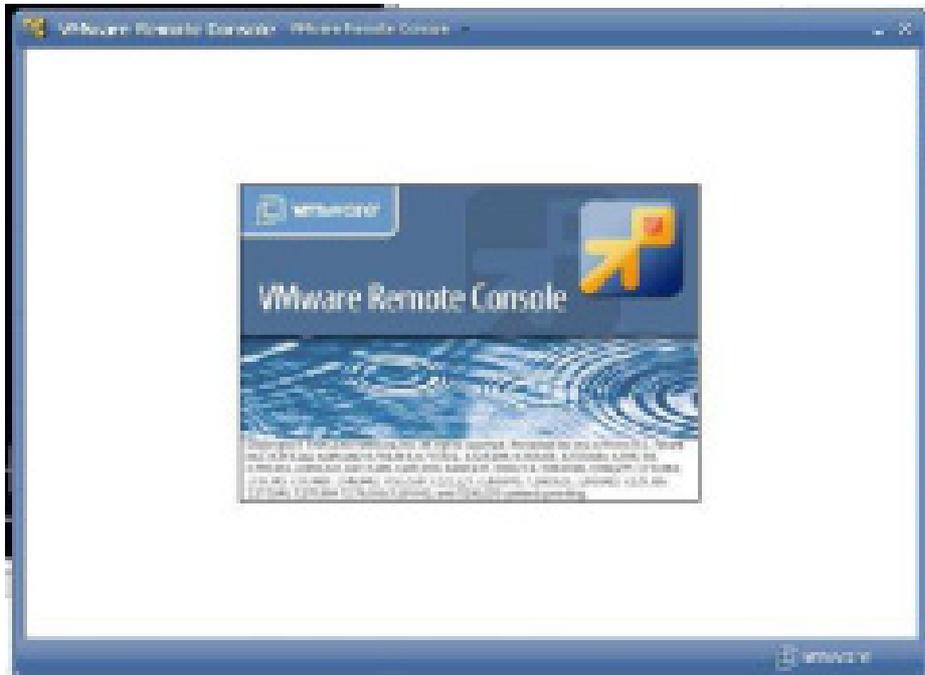
Nous cliquons sur "PC-DMZ" pour sélectionner notre machine virtuelle.

Nous cliquons sur l'onglet "Console" puis dans la partie noire pour démarrer la machine virtuelle.



Une fois la machine virtuelle démarrée, Nous cliquons ensuite une nouvelle fois dans la partie noire pour lancer la console VMWare.

Alors, la fenêtre suivante devrait apparaître :



Maintenant nous devrions être prêts à amorcer l'installation de notre OS sur notre nouvelle machine virtuelle.

Dans le cadre de notre projet et pour définir l'architecture de notre centre de données, nous avons installé 9 machines :

- 5 machines ayant Windows XP comme système d'exploitation,
- 3 machines ayant Windows Server 2003 comme système d'exploitation :
 - ✓ Un serveur Web.
 - ✓ Un serveur de messagerie (pop3), nous avons aussi configuré Active Directory, DNS et DHCP sur ce serveur.
 - ✓ Un serveur d'application.
- 1 machine firewall : nous avons installé le firewall Endian.

Pour le besoin de sécurité répondant aux exigences du firewall, notre architecture est séparée en zone, et ça sera détaillé dans le prochain chapitre.

Conclusion

Au cours de ce chapitre, nous avons étudié l'infrastructure de VMWare et l'installation des machines virtuelles décrivant notre centre de données.

Le chapitre suivant sera consacré à la mise en place d'une solution de sécurité permettant d'isoler notre architecture et diminuer les risques d'attaques pouvant nous faire face.

Chapitre 5 : Sécurisation du centre de données virtuel

Ce chapitre met en évidence l'intégration de la sécurité dans l'architecture virtualisée réalisée. Nous intégrons et configurons le firewall Endian pour mettre en place cette architecture sécurisée.

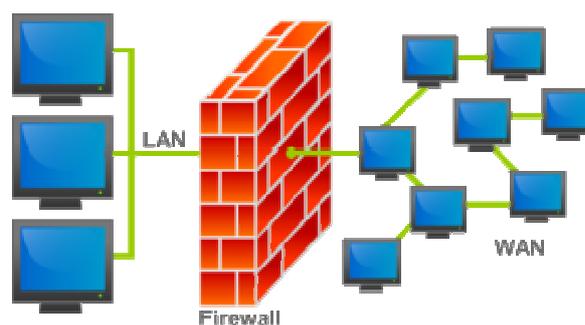
Les architectures virtuelles doivent être considérées comme des environnements classiques avec les mêmes stratégies de sécurisation, de surveillance, d'audit et de contrôle. Toutefois, elles ne doivent pas s'arrêter devant un serveur, mais aller en profondeur, jusqu'au sein de l'architecture virtuelle.

5.1. Sécurisation du centre de données virtuel

La sécurité du centre de données virtuels est basée essentiellement sur deux points :

- Mise en place du firewall Endian
- Attribution des droits d'accès et d'utilisation aux utilisateurs

Notre première vision de la problématique est décrite par la figure suivante :



Nous avons besoin de séparer le monde interne du monde externe: c'est à dire contrôler les flux entrant et sortant pouvant influencer notre centre de données.

a. Le Pare-feu (ou firewall) Endian

Endian est une distribution de sécurité open source dont le but est d'obtenir une distribution Linux complètement dédiée à la sécurité et aux services essentiels d'un réseau afin d'offrir une protection maximale contre le vol de données, virus, spyware, spam et autres menaces Internet. Plus concrètement, Endian intègre un firewall qui va jouer le rôle d'intermédiaire entre un réseau considéré comme non sûr (Internet) et un réseau que l'on souhaite sécuriser (le réseau local par exemple), tout en fournissant des services permettant la gestion et le suivi de celui-ci qui seront gérés à travers une interface web (Unified Threat Management UTM).

Endian représente ainsi une solution de sécurité pour la mise en place d'une application UTM.

Le firewall d'Endian Firewall se compose de plusieurs interfaces dont chacune peut être ou non utilisée :

- Rouge : Zone du réseau à risque (Internet).
- Verte : Zone du réseau à protéger (réseau local).
- Bleu : Zone spécifique pour les périphériques sans fil (wifi). Il n'est possible de faire communiquer l'interface Verte et l'interface Bleu qu'en créant un VPN.
- Orange : Zone démilitarisée (DMZ), cette zone isolée, hébergeant des applications mises à disposition du public. Elle est accessible de l'extérieur mais ne possède aucun accès sortant (serveur web, un serveur de messagerie, un serveur FTP public, etc.).

Dans ce cadre, les fonctionnalités d'Endian sont nombreuses :

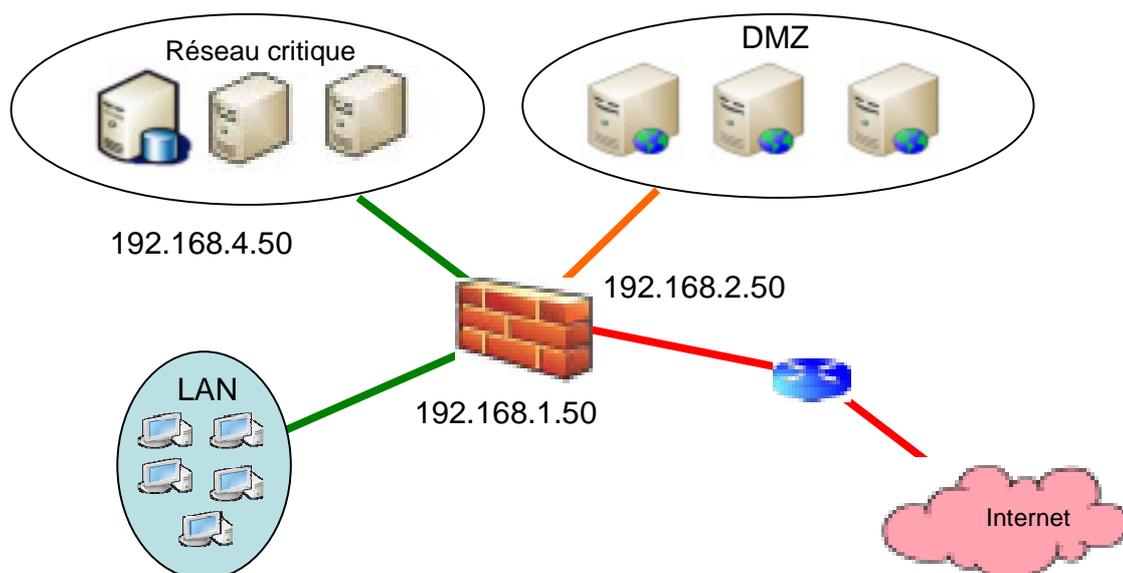
- Il surveille le comportement en ligne des utilisateurs (on peut voir quels sites sont visités, par qui, et sur quel système).
- Il restreint l'accès à des sites inappropriés, gère les accès aux sites et contrôle l'activité indésirable sur internet, comme jouer en lignes pendant les heures de travail.
- Il offre une mise à jour automatique.
- Il offre la journalisation et le reporting

- Il bloque les sites web qui gaspillent le temps comme MySpace et FaceBook avec listes de blocage personnalisées.
- Il incarne un antispam, un antivirus, un anti spyware et un IDS
- Il bloque les services inutiles tel que : les réseaux Peer-to-Peer, chat, etc.
- Il filtre le trafic en se basant sur adresse IP, protocole et ports.
- Il crée des DMZ.
- Il offre les fonctionnalités de routage.
- Il offre une solution sécurisé d'inter-connecter les réseaux de l'organisme : VPN
- Il partage le trafic en utilisant jusqu'à 6 connexions et partage la bande passante (répartition de charge).
- Il détecte automatiquement les coupures de connexion et bascule sur le fournisseur d'accès de sauvegarde (Haute disponibilité).

5.2. Solution proposée

Reprenons notre architecture réseau, et essayons de sécuriser le réseau privé par la mise en place d'un firewall avec des règles de filtrage. On essaiera de faire attention lors de l'établissement des règles de filtrage de peur de nous exclure nous même.

Ce réseau se constitue de 2 sous réseaux privés (LAN et réseau critique) et une DMZ, qui sont connectés à internet.



Le but est :

- Protéger le réseau privé d'Internet: la DMZ va jouer le rôle d'une zone tampon entre le réseau privé et Internet.
- Le réseau privé doit accéder à la DMZ et à Internet: donc on autorise tout trafic forwardé à partir du réseau privé vers la DMZ.
- Interdire toute connexion de la DMZ ou d'Internet vers le réseau privé, sauf les Réponses pour les connexions déjà initiées de la part du réseau privé.
- Interdire les pings provenant de l' Internet vers la DMZ.
- Permettre les connexions SSH entrantes, ainsi que les pings, au niveau du routeur.
- Permettre les réponses de retours des pings « écho-replay ».

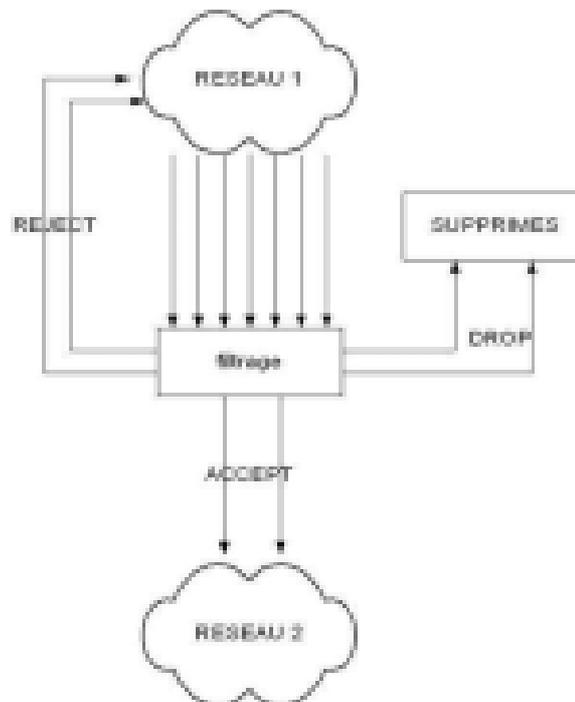
Avant d'entamer la configuration, définissons un point clé : DMZ

- DMZ: une zone démilitarisée (ou DMZ, de l'anglais demilitarized zone) est un sous-réseau isolé par un pare-feu. Ce sous-réseau contient des machines se situant entre un réseau interne (LAN - postes clients) et un réseau externe (typiquement, Internet).

a. Principe du filtrage

Le filtrage est le fait de choisir quels paquets atteignent ou traversent la machine et ce qui advient de ceux refusés.

Schéma du filtrage:



Un paquet qui transite par le Firewall passe par la chaîne FORWARD.

Un paquet provenant du Firewall passe par la chaîne OUTPUT.

Un paquet à destination du Firewall passe par la chaîne INPUT.

DROP : permet, lorsqu'elle est appliquée à une règle, de refuser un paquet, mais sans avertir le demandeur que sa demande de connexion lui a été refusée.

ACCEPT : permet, lorsqu'elle est appliquée à une règle, d'accepter les paquets qui correspondent à cette règle

REJECT : permet, lorsqu'elle est appliquée à une règle, de refuser un paquet, mais en avertissant le demandeur que sa demande de connexion lui a été refusée en lui envoyant un paquet *RESET* (RST).

b. Adressage IP

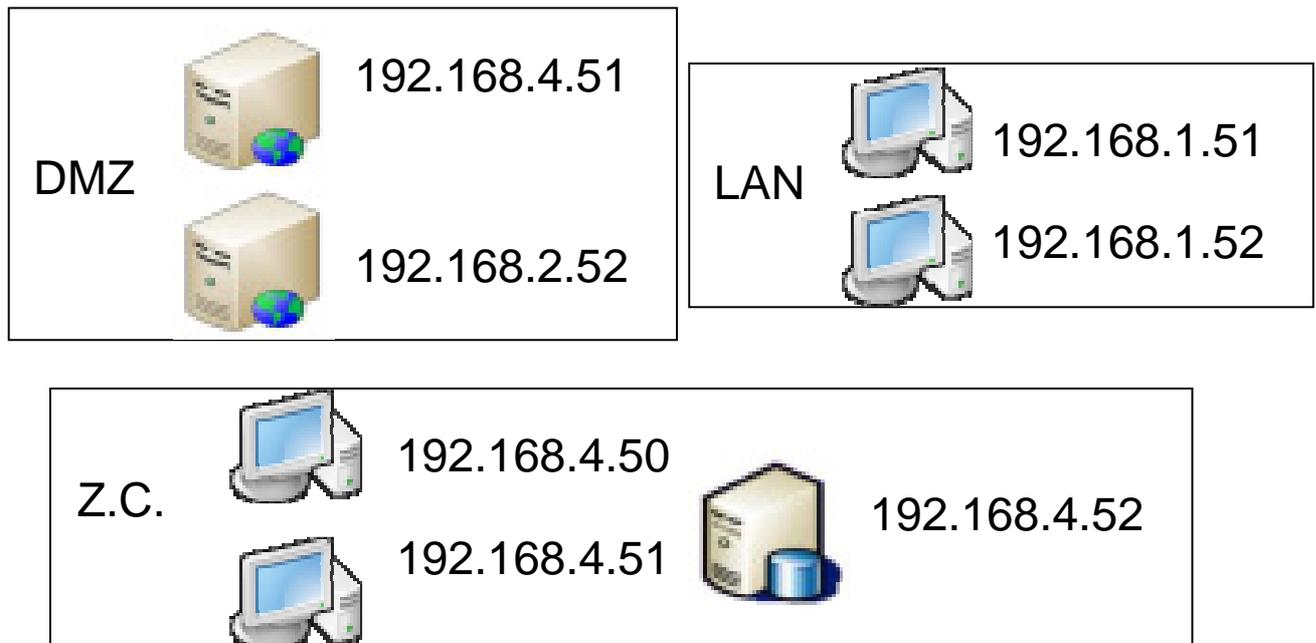
Nous appliquons l'adressage IP suivant :

Nous séparons les zones en premier lieu par des adresses de sous réseaux différentes : dans ce but, nous utilisons des adresses IP privées de la classe C :

LAN : 192.168.1.0

DMZ:192.168.2.0

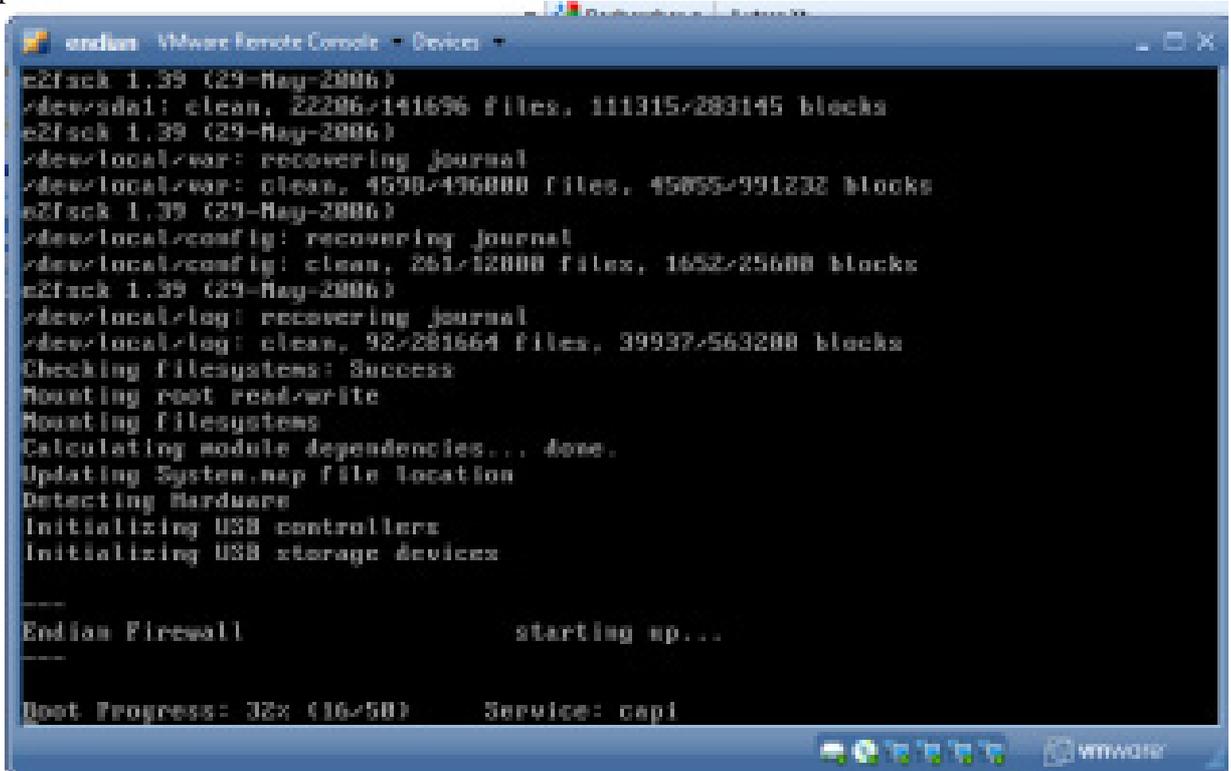
Zone critique: 192.168.4.0



c. Administration du Firewall

Dans la partie qui suit, nous détaillons la configuration du firewall mise en place pour sécuriser notre centre de données.

La première interface d'exécution du firewall installé sur la machine virtuelle s'affiche ainsi :



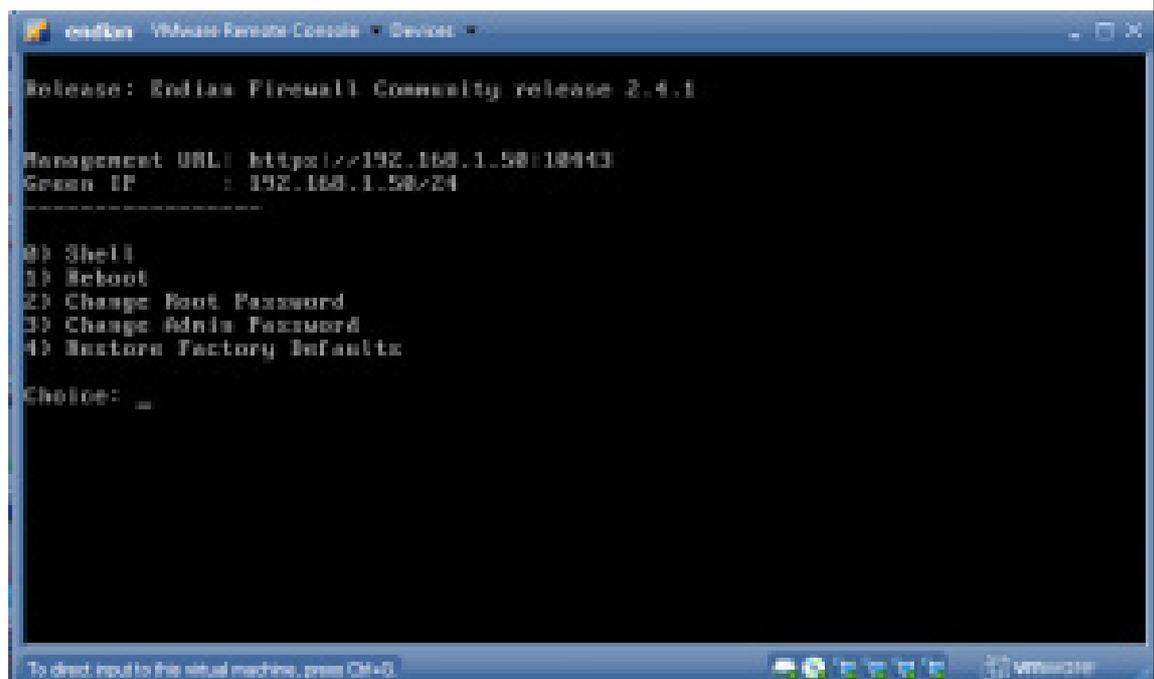
```

endian VMware Remote Console - Devices
e2fsck 1.39 (29-May-2006)
/dev/sda1: clean, 22206/141696 files, 111315/283145 blocks
e2fsck 1.39 (29-May-2006)
/dev/local/var: recovering journal
/dev/local/var: clean, 4590/496800 files, 45855/991232 blocks
e2fsck 1.39 (29-May-2006)
/dev/local/config: recovering journal
/dev/local/config: clean, 261/12800 files, 1652/25600 blocks
e2fsck 1.39 (29-May-2006)
/dev/local/log: recovering journal
/dev/local/log: clean, 92/281664 files, 39937/563200 blocks
Checking filesystems: Success
Mounting root read-write
Mounting filesystems
Calculating module dependencies... done.
Updating System.map file location
Detecting Hardware
Initializing USB controllers
Initializing USB storage devices

-----
Endian Firewall                starting up...
-----

Boot Progress: 32% (16/50)      Service: capi
  
```

Ensuite, le firewall Endian affiche un menu de choix, à nous d'utiliser le mode shell pour se connecter.



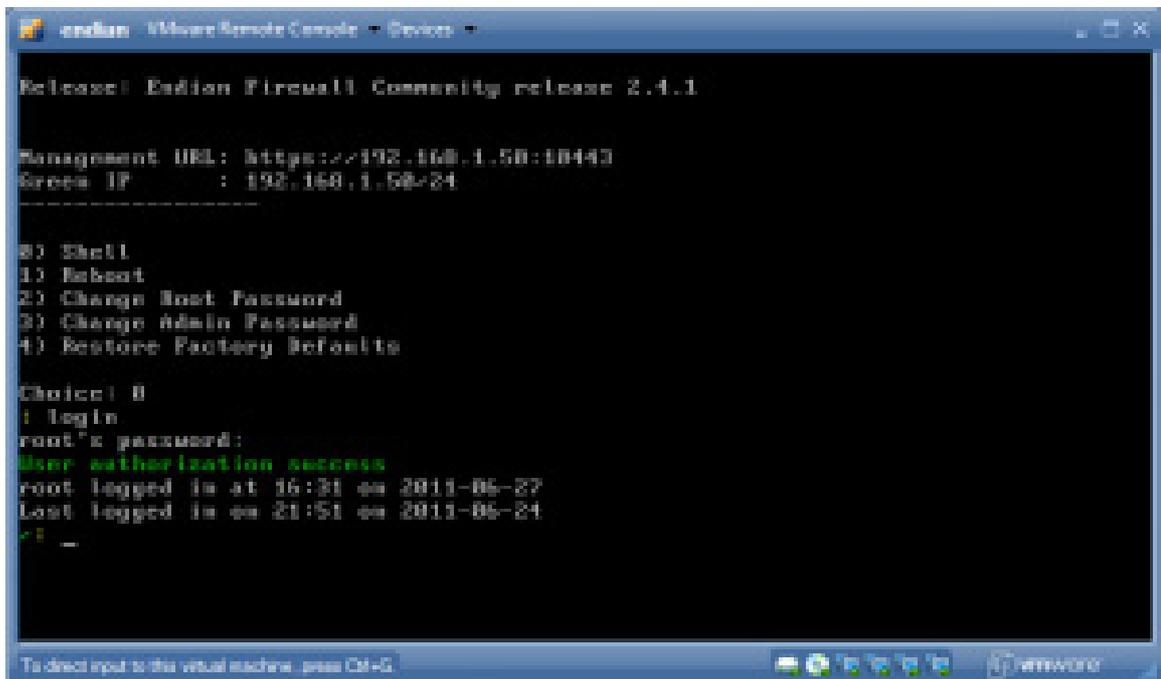
```

endian VMware Remote Console - Devices
Release: Endian Firewall Community release 2.4.1

Management URL: https://192.168.1.58:18443
Green IP       : 192.168.1.58/24
-----
0) Shell
1) Reboot
2) Change Root Password
3) Change Admin Password
4) Restore Factory Defaults

Choice: _
  
```

Nous devons maintenant introduire le mot de passe de l'utilisateur 'Root' introduit dans les étapes d'installation du firewall.



```

endian VMware Remote Console - Devices
-----
Release: Endian Firewall Community release 2.4.1

Management URL: https://192.168.1.50:10443
Screen IP      : 192.168.1.50-24
-----

0) Shell
1) Reboot
2) Change Root Password
3) Change Admin Password
4) Restore Factory Defaults

Choice: 0
: login
root's password:
User authorization success
root logged in at 16:31 on 2011-06-27
Last logged in on 21:51 on 2011-06-24
<!--
  
```

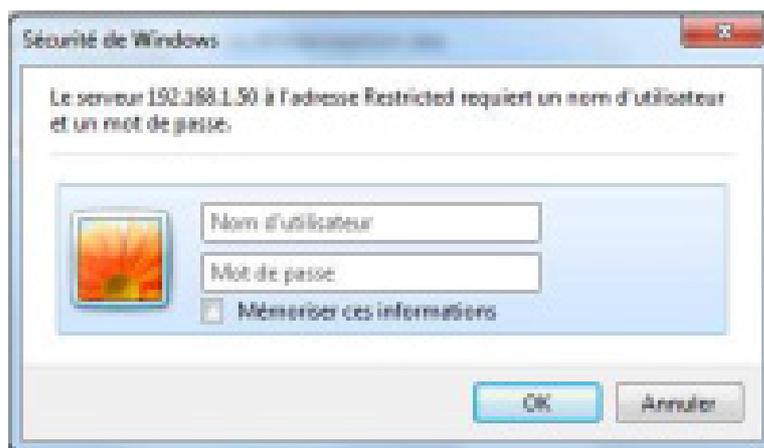
Nous utiliserons par la suite, un navigateur Web pour administrer notre firewall et le gérer pour mettre en place notre solution de sécurité.

Les URL de connexion sont : **Http://192.168.1.50**

Ou bien :

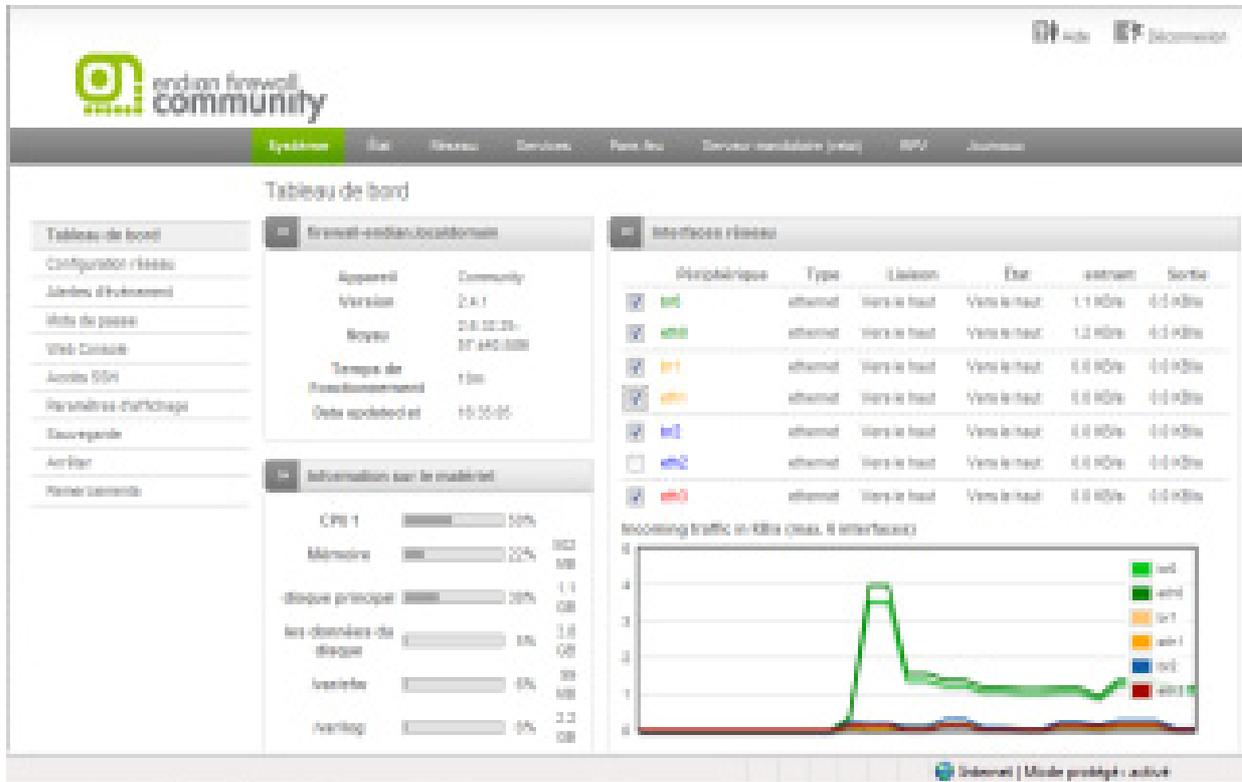
Https://192.168.1.50:10443 (pour une connexion sécurisée)

L'interface de connexion est la suivante (pour l'utilisateur Admin):

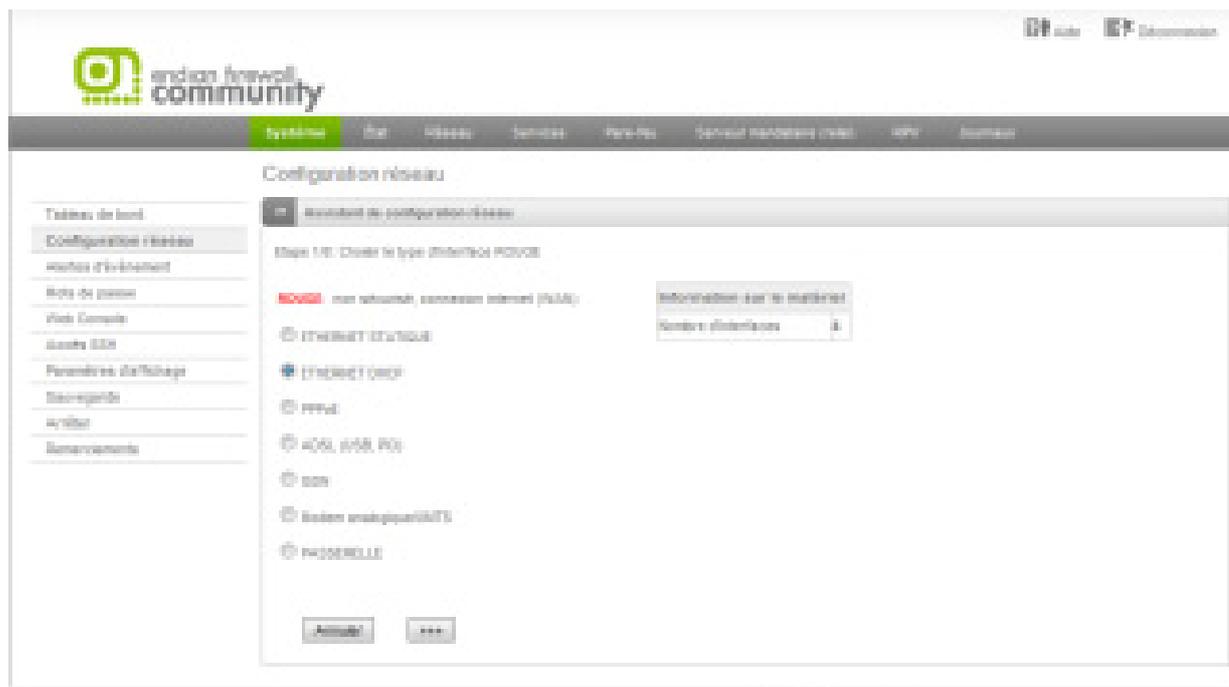


Le firewall Endian présente un menu des tâches à administrer, nous essayerons de voir les plus importants.

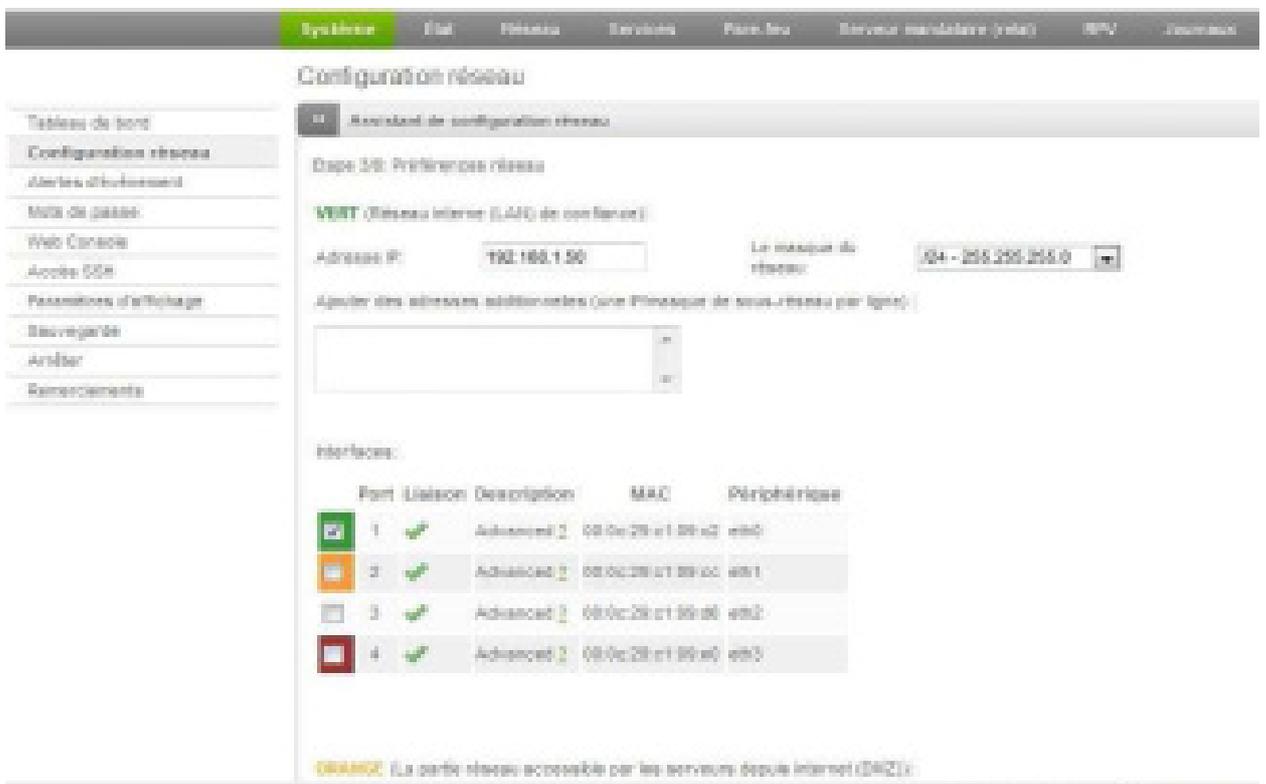
En premier lieu, le tableau de bord s'affiche contenant les informations de base de notre firewall(nom, version, CPU, mémoire, interface réseau...) :



Nous configurons dans l'étape suivante notre réseau en définissant les interfaces du firewall déjà traitées auparavant et ceci en appliquant l'adressage IP ainsi:



pour l'interface rouge, le protocole Ethernet DHCP prendra en charge notre adressage IP.
 Pour notre réseau, nous choisissons une partie DMZ contenant les serveurs connectés à Internet : c'est la partie Orange.



Nous avons ici le choix de garder l'adresse IP de l'interface verte ajoutée lors de la 1^{ère} installation de notre firewall ou de la changer.

Nous ajoutons l'adresse IP de l'interface Orange, ainsi qu'un nom/nom du domaine à notre machine.

ORANGE (La partie réseau accessible par les serveurs depuis internet (DMZ)):

Adresse IP: Le masque du réseau:

Ajouter des adresses additionnelles (une Période de sous-réseau par ligne):

Interfaces:

	Port	Liaison	Description	MAC	Périphérique
	1	<input checked="" type="checkbox"/>	Advanced ?	00:0c:29:c1:29:c2	eth0
	2	<input checked="" type="checkbox"/>	Advanced ?	00:0c:29:c1:29:c3	eth1
	3	<input checked="" type="checkbox"/>	Advanced ?	00:0c:29:c1:29:c8	eth2
	4	<input checked="" type="checkbox"/>	Advanced ?	00:0c:29:c1:29:c0	eth3

Nom d'hôte:

Nom de domaine:

Configuration réseau

Assistent de configuration réseau

Étape 4/5: Préférences d'accès à internet

ORANGE (non sécurisé, connexion internet (WAN)):

Interfaces:

	Port	Liaison	Description	MAC	Périphérique
	1	<input checked="" type="checkbox"/>	Advanced ?	00:0c:29:c1:29:c2	eth0
	2	<input checked="" type="checkbox"/>	Advanced ?	00:0c:29:c1:29:c3	eth1
	3	<input checked="" type="checkbox"/>	Advanced ?	00:0c:29:c1:29:c8	eth2
	4	<input checked="" type="checkbox"/>	Advanced ?	00:0c:29:c1:29:c0	eth3

MTU:

Changement de l'adresse MAC avec:

DNS: automatique manuel

Ce champ peut être laissé vide.

Nous passons maintenant au menu "réseau" : nous débutons par l'ajout de nos machines 'ajouter un hôte' (adresse IP-Nom hôte).

Configuration de l'hôte

Adresse IP de l'hôte	Nom de l'hôte	Type de l'hôte	Actions
192.168.2.01	server1-ORG		✎ 🗑
192.168.1.01	PC1-LAN		✎ 🗑
192.168.4.01	PC4		✎ 🗑
192.168.4.03	PC3		✎ 🗑
192.168.1.02	PC2-LAN		✎ 🗑
192.168.2.02	server2-ORG		✎ 🗑
192.168.4.02	server-Application		✎ 🗑

Légende: ✎ Éditer 🗑 Retirer de la bibliothèque

Statut: Inactif (pas d'ipsec) Système: 16-04-04 up 16 min, 0 users, total storage: 2.8G, 1.8G, 1.0G
 Endian Firewall Community release 2.4.1 (c) 2004-2008 Endian

Ensuite, nous ajoutons les routes via 'routing - routage statique'.

Éditeur de routage statique

Routing statique Règles de routage

Les entités actuelles de routage

Réseau source	Réseau (à destination)	Via le pas suivante	Remarque	Actions
192.168.1.0	192.168.4.0	192.168.1.01		☑ ✎ 🗑
192.168.1.0	192.168.2.0	192.168.1.01		☑ ✎ 🗑
192.168.4.0	192.168.2.0	192.168.2.01		☑ ✎ 🗑

Légende: ☑ Actif (cliquer pour désactiver) ☐ Désactif (cliquer pour activer) ✎ Éditer 🗑 Retirer de la bibliothèque

Concernant l'étape suivante, nous définissons les règles de routage.

Éditeur des règles de routage

Routeur statique Règles de routage

Règles statiques

[Ajouter une nouvelle règle de routage](#)

#	Source	Destination	Terme du service (TOS)	Via la passerelle	Service	Remarque	Actions
1	*TOUS*	*TOUS*	Lauxion sortante principale		*TOUS*		
2	192.168.4.0	192.168.1.0	Lauxion sortante principale		TCP+UDP Tous		
3	192.168.4.0	192.168.1.0	Lauxion sortante principale		ICMP S ICMP N		
4	192.168.1.0	192.168.4.0	Lauxion sortante principale		TCP+UDP Tous		
5	192.168.1.0	192.168.4.0	Lauxion sortante principale		ICMP S ICMP N		
6	192.168.1.0	192.168.4.0	192.168.1.0		*TOUS*		
7	192.168.1.0	192.168.2.0	192.168.1.0		*TOUS*		
8	192.168.4.0	192.168.2.0	192.168.1.0		*TOUS*		

Nous passons ensuite au menu "Pare-feu" pour définir les règles de filtrage : nous commençons par le flux entrant:

endian firewall community

Système Etat Réseau Services **Pare-feu** Services managés (PaaS) IPv6 Journaux

Paramétrage du pare-feu entrant

Port (Source/Destination) (TOS) Source (TOS) La redirection du trafic entrant

Règles actuelles

[Ajouter une nouvelle règle pour le pare-feu](#)

#	Source	Destination	Service	Politique	Remarque	Actions
1	*TOUS*	0.0.0.0/0	TCP+UDP+ICMP	ACCEPT		
2	*TOUS*	0.0.0.0/0	ICMP ICMP	REJECT		
3	*TOUS*	192.168.1.0	TCP+UDP	ACCEPT		
4	*TOUS*	192.168.1.0	TCP+UDP+ICMP	REJECT		
5	*TOUS*	192.168.1.55 192.168.1.80 192.168.1.57	TCP	ACCEPT		

Légende Actif (cliquer pour désactiver) Désactivé (cliquer pour activer) Éditer Retirer de la bibliothèque

Afficher les règles de système

Nous traitons ensuite le flux sortant:

The screenshot shows the Mikrotik WinBox interface for configuring firewall rules. The 'Configuration du pare-feu sortant' (Outgoing Firewall Configuration) tab is active. A sidebar on the left contains navigation options: 'Transfert de port / NAT', 'Trafic sortant', 'Trafic inter-Zone', 'Trafic VPN', 'Accès système', and 'Diagramme du Pare-Feu'. The main area displays a table of active rules under the heading 'Règles actives'. A green button at the top left of the table says 'Ajouter une nouvelle règle pour le pare-feu'. The table has columns for 'R', 'Source', 'Destination', 'Service', 'Politique', 'Remarque', and 'Actions'. There are 10 rules listed, all with 'VERT' as the source and 'ROUGE' as the destination. The services include 'TCP:80', 'TCP:443', 'TCP:81', 'TCP:8080', 'TCP:443', 'TCP:80', 'TCP:8080', 'TCP:8080', 'TCP:8080', and 'TCP:8080'. The policies are 'allow HTTP', 'allow HTTPS', 'allow FTP', 'allow SMTP', 'allow POP', 'allow IMAP', 'allow POP3', 'allow IMAPs', and 'allow POP3'. Below the table is a legend: 'Légende: Actif (cliquez pour désactiver) Désactivé (cliquez pour activer) Éditer Retirer de la bibliothèque'.

R	Source	Destination	Service	Politique	Remarque	Actions
1	VERT BLU	ROUGE	TCP:80		allow HTTP	
2	VERT BLU	ROUGE	TCP:443		allow HTTPS	
3	VERT	ROUGE	TCP:81		allow FTP	
4	VERT	ROUGE	TCP:8080		allow SMTP	
5	VERT	ROUGE	TCP:80		allow POP	
6	VERT	ROUGE	TCP:8080		allow IMAP	
7	VERT	ROUGE	TCP:8080		allow POP3	
8	VERT	ROUGE	TCP:8080		allow IMAPs	
9	VERT ORANGE BLU	ROUGE	TCP:8080		allow POP3	
10	VERT ORANGE BLU	ROUGE	TCP:8080		allow POP	

Et finalement le trafic Inter-zone:

The screenshot shows the Mikrotik WinBox interface for configuring inter-zone firewall rules. The 'Configuration du pare-feu Inter-Zone' (Inter-Zone Firewall Configuration) tab is active. A sidebar on the left contains navigation options: 'Transfert de port / NAT', 'Trafic sortant', 'Trafic Inter-Zone', 'Trafic VPN', 'Accès système', and 'Diagramme du Pare-Feu'. The main area displays a table of active rules under the heading 'Règles actives'. A green button at the top left of the table says 'Ajouter une règle de pare-feu inter-zone'. The table has columns for 'R', 'Source', 'Destination', 'Service', 'Politique', 'Remarque', and 'Actions'. There are 6 rules listed, all with 'VERT' as the source and 'ROUGE' as the destination. The services include '<Tous>', 'ORANGE', 'ORANGE', '192.168.4.1', '192.168.4.1', and '<Tous>'. The policies are 'allow', 'allow', 'allow', 'allow', 'allow', and 'allow'. Below the table is a legend: 'Légende: Actif (cliquez pour désactiver) Désactivé (cliquez pour activer) Éditer Retirer de la bibliothèque'. There is also a button 'Afficher les règles des services de système' with a dropdown arrow. Below the table, there is a section for 'Préférences du pare-feu inter-Zone' with a toggle for 'Activer le pare-feu inter-Zone' (checked) and a checkbox for 'Enregistrer les connexions inter-Zone acceptées dans le journal' (checked). A 'Sauvegarder' button is at the bottom.

R	Source	Destination	Service	Politique	Remarque	Actions
1	VERT	ROUGE	<Tous>			
2	VERT	ORANGE	<Tous>			
3	ORANGE	ORANGE	<Tous>			
4	192.168.4.1	interface 1	<Tous>			
5	192.168.4.1	interface 2	<Tous>			
6	<Tous>	<Tous>	<Tous>			

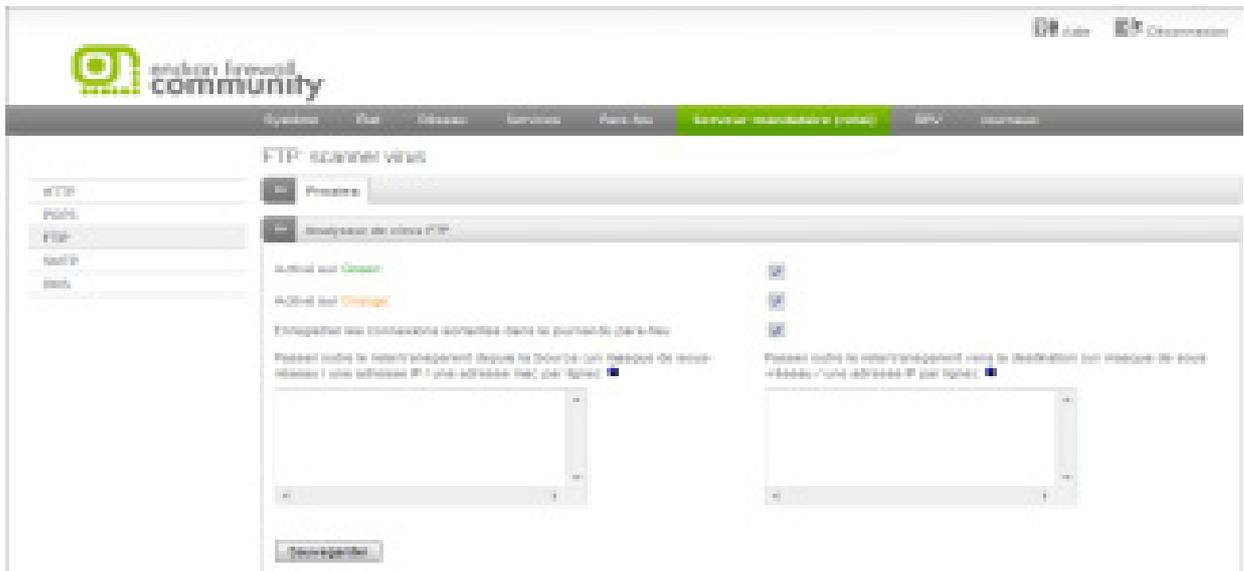
Concernant le menu "Serveur mandataire", nous appliquons quelques règles sur les protocoles, concernant 'http', nous validons le filtrage contre les virus:

The screenshot shows the 'Proxy HTTP : politique' configuration page. On the left, a sidebar lists protocols: HTTP, POP3, FTP, SMTP, and DNS. The main content area has tabs for 'Configuration', 'Politique d'accès', 'Authentification', 'Filtre de contenu', 'Antivirus', and 'Journal M2'. The 'Antivirus' tab is active, showing a rule named 'Filtrage contre les virus' with source 'TOUS', destination 'TOUS', and action 'Non-espère'. Below the rule list, there is a status bar indicating the system is up and running.

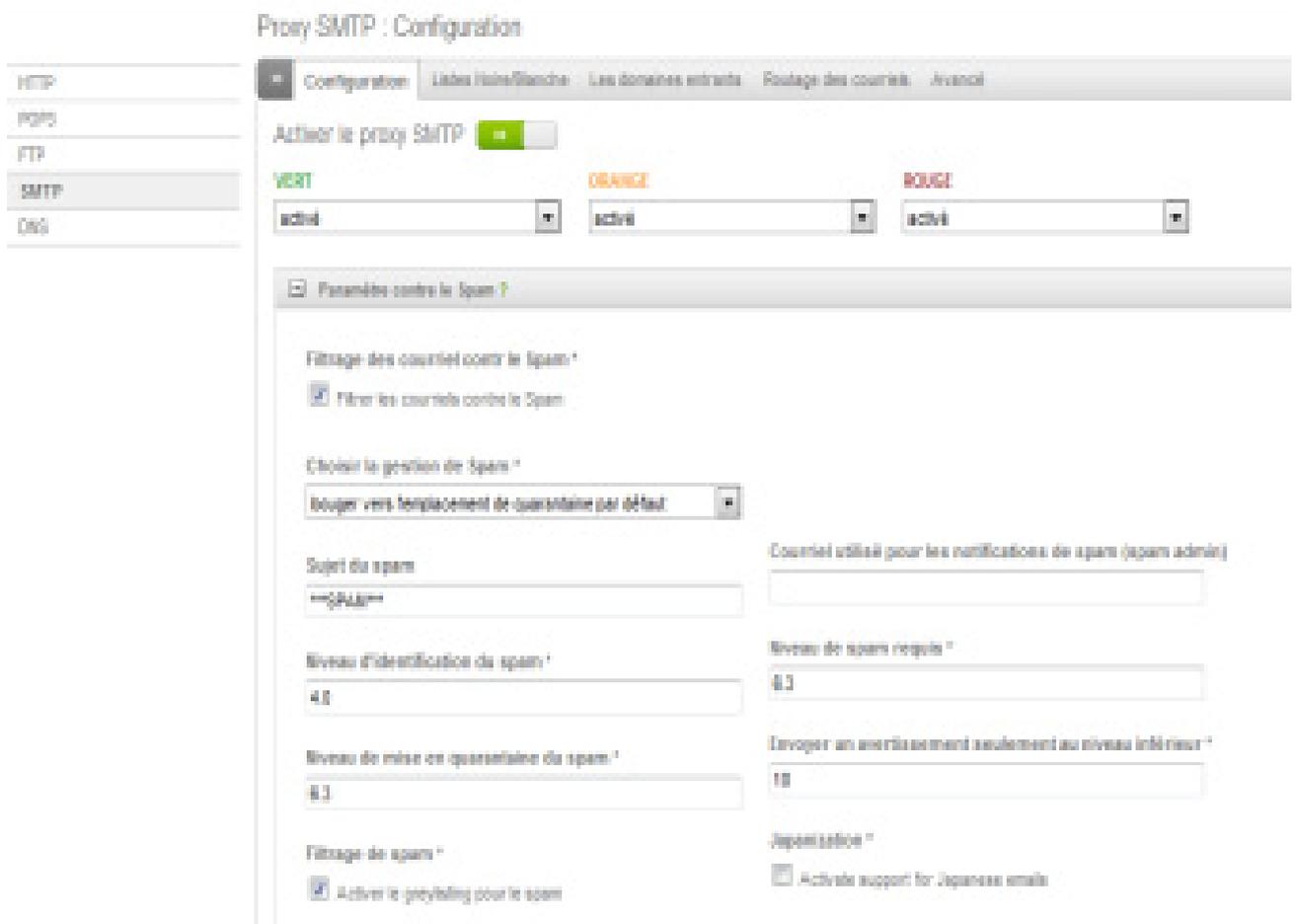
Pour le protocole 'Pops3', nous activons "le scanner courriel" sur les interfaces Orange et Verte de notre firewall ainsi que "le filtre à courrier indésirable":

The screenshot shows the 'POP3: paramètres généraux' configuration page. The 'Scanner courriel (POP3)' section is expanded, revealing several settings: 'Actif sur Green' (checked), 'Actif sur Orange' (checked), 'Scanner anti-virus' (checked), and 'Enregistrer les connexions suspectes dans le journal du pare-feu' (checked). A 'Filtre à courrier indésirable' checkbox is also visible. A 'Sauvegarder' button is at the bottom of the configuration area.

Pour le protocole 'FTP', nous activons "l'analyseur de virus FTP" :



Pour le protocole 'SMTP', nous activons "le proxy SMTP" et nous configurons les paramètres contre le Spam:



Procy SMTP: Configuration

Configuration | Lettres non/livraison | Les domaines autorisés | Routage des courriels | Avancé

Activer le proxy SMTP

HEAT SERVICE SERVICE

Paramètres contre le spam ?

Paramètres contre le virus ?

Le scanner de virus pour le proxy SMTP (handling: virus admin/ quarantine location):

Scanner les courriels contre les virus

Choisir la gestion de virus *

Courriel utilisé pour les notifications de virus (virus admin)

Et finalement, nous bloquons les fichiers ayant l'extension ".exe" ainsi qu'une double extension:

Choisir la gestion de virus *

Courriel utilisé pour les notifications de virus (virus admin)

File settings ?

Bloquer les fichiers par extensions *

Bloquer les fichiers par extensions

Choisir la gestion de fichiers bloqués *

Choisir les types de fichier à bloquer (par extension)

- Enhanced Windows Metafile picture (.emf)
- Program (.exe)**
- Visual FoxPro compiled program (.fpj)
- Windows Program Group file (.grp)
- Help file (.hlp)
- Microsoft Office word document (.doc)

Email used for blocked file notifications (file admin)

Bloquer les fichiers avec des doubles extensions

Bloquer les fichiers avec des doubles extensions

Eviter le proxy transparent ?

Sauvegarder

Conclusion

Au cours de ce projet, nous avons étudié l'architecture existante et avons dégagé les inconvénients qu'elle présente. Suite à cette étude, nous avons conçu et mis en place la maquette pour la virtualisation des serveurs. La mise en place de la solution de sécurité était une étape essentielle pour assurer la protection des données à l'intérieur de l'environnement virtuel.

Le recours à la virtualisation a permis notamment d'utiliser les serveurs de manière plus intensive et à moindre coût et de bénéficier d'une disponibilité élevée grâce aux fonctions intégrées.

Des avantages supplémentaires incluent une gestion des performances via l'équilibrage dynamique de la charge de travail, ainsi qu'une simplification de la gestion grâce au regroupement de tous les serveurs sous la forme d'un pool unique et uniforme de ressources.

Un environnement fortement virtualisé dépend de l'efficacité et de la fiabilité du réseau. Les défaillances des serveurs physiques, des connexions, des commutateurs ou des routeurs peuvent s'avérer coûteuses et parfois même dangereuses et si l'on procède à la virtualisation sans mettre en œuvre les meilleures pratiques en matière de sécurité, elle risque au bout du compte d'accroître les coûts de l'entreprise et de nuire à sa souplesse.

Le travail sur ce projet ouvre encore plus de perspectives.

Dans un premier temps il faudra penser à formaliser les processus d'exploitation de la nouvelle plateforme.

A moyen terme, il serait judicieux de centraliser les postes de travail au niveau du centre de données, en considérant ce que cela pourrait apporter en matière de gestion d'incidents.

Bibliographie

[1] www.vmware.com

[2] www.datacenter.fr

[3] www.endian.com

[4] www.commentcamarche.net

[5] www.ageei.org

[6] www.fr.wikipedia.org

[7] www.everymac.com

[8] www.itpro.fr/windows-server

[9] www.virtualisation-news.com

[10] aldevar.free.fr/data/VeilleTechno/VeilleTechno-Virtualisation.pdf

[11] www.journaldunet.com/solutions/expert/securite/34213/oui-a-la-virtualisation-mais-pas-sans-protection.shtml

Annexe

Les étapes d'installation du firewall Endian: sont comme suit :

```
ISOLINUX 3.31 2006-09-25 Copyright (C) 1994-2005 H. Peter Anvin

Welcome to Endian Firewall, Licensed under GNU GPL version 2.

PLEASE BEWARE! This installation process will kill all
existing partitions on your PC or server. Please be aware
of this before continuing this installation.

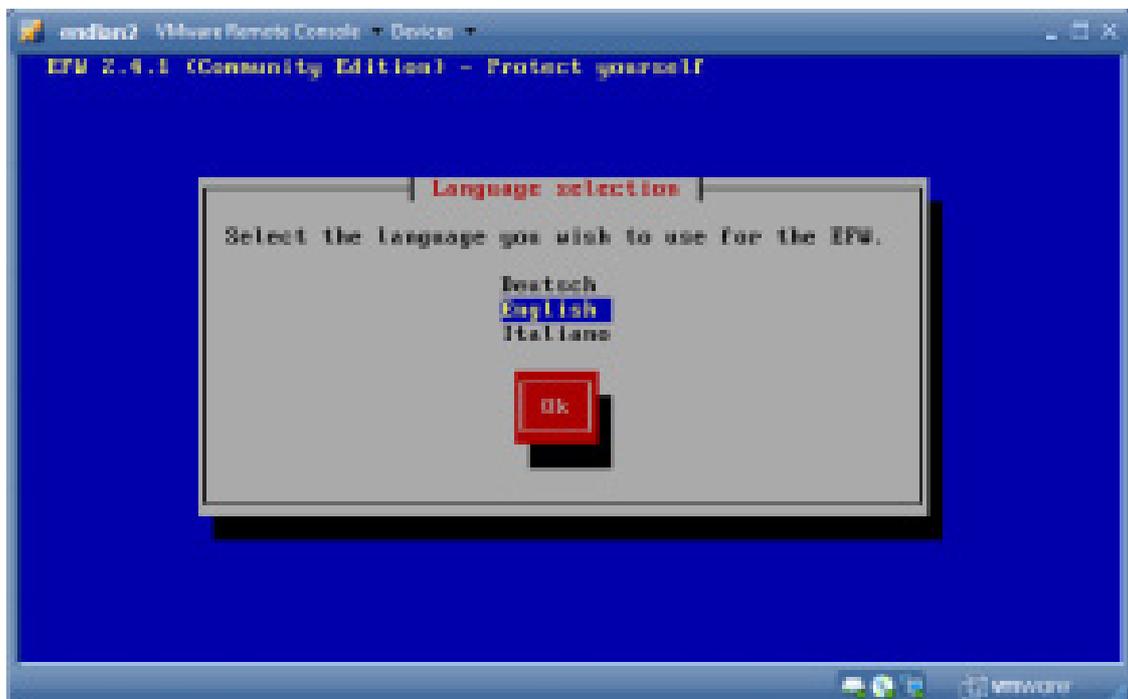
-----
---- ALL YOUR EXISTING DATA WILL BE DESTROYED ----
-----

Press RETURN to boot Endian Firewall default installation.

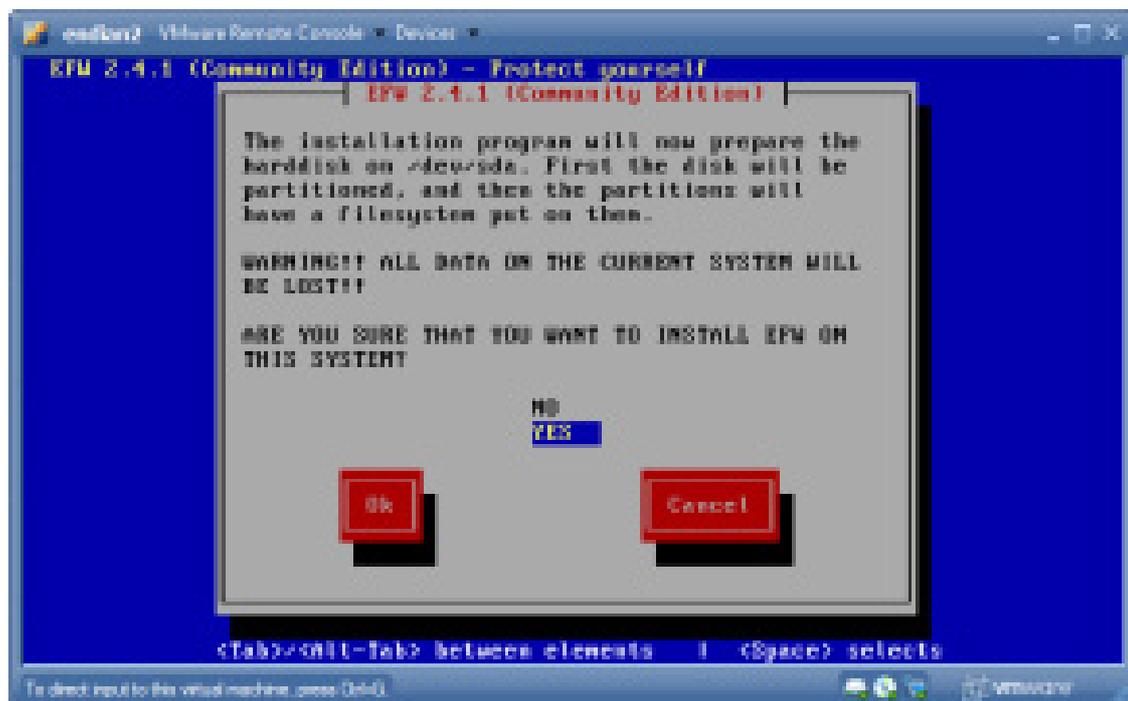
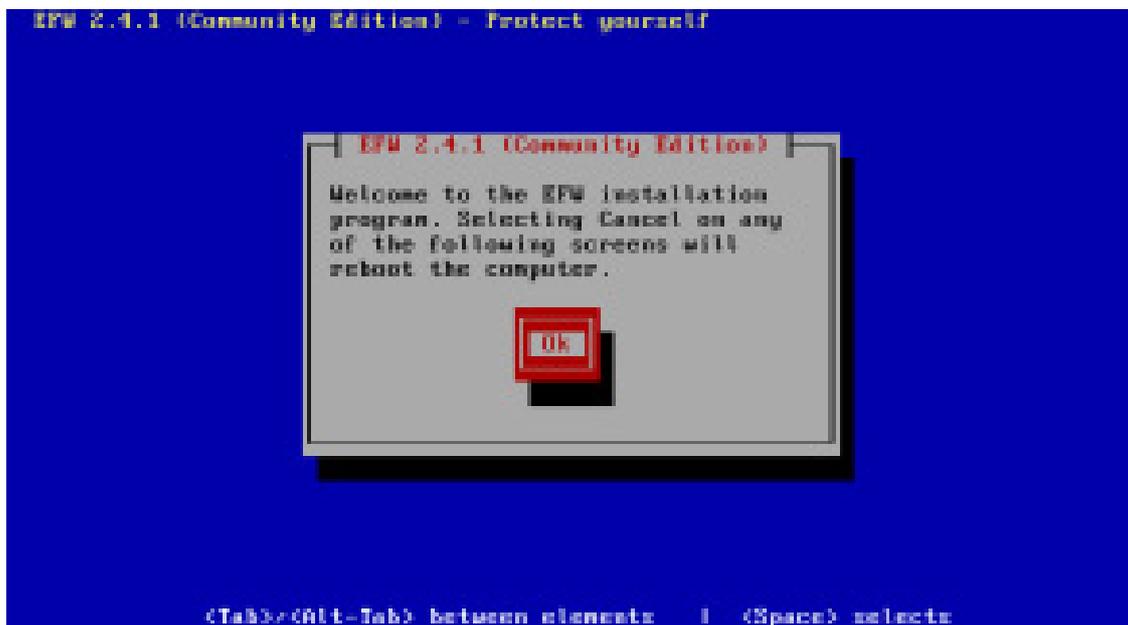
Or, if you are having trouble you can try these options...
Type:  noprocsia to disable PCMCIA detection
       nouch to disable USB detection
       nouchprocsia to disable both PCMCIA & USB detection
       dma to enable ide dma (SIS chipset workaround)

boot: _
```

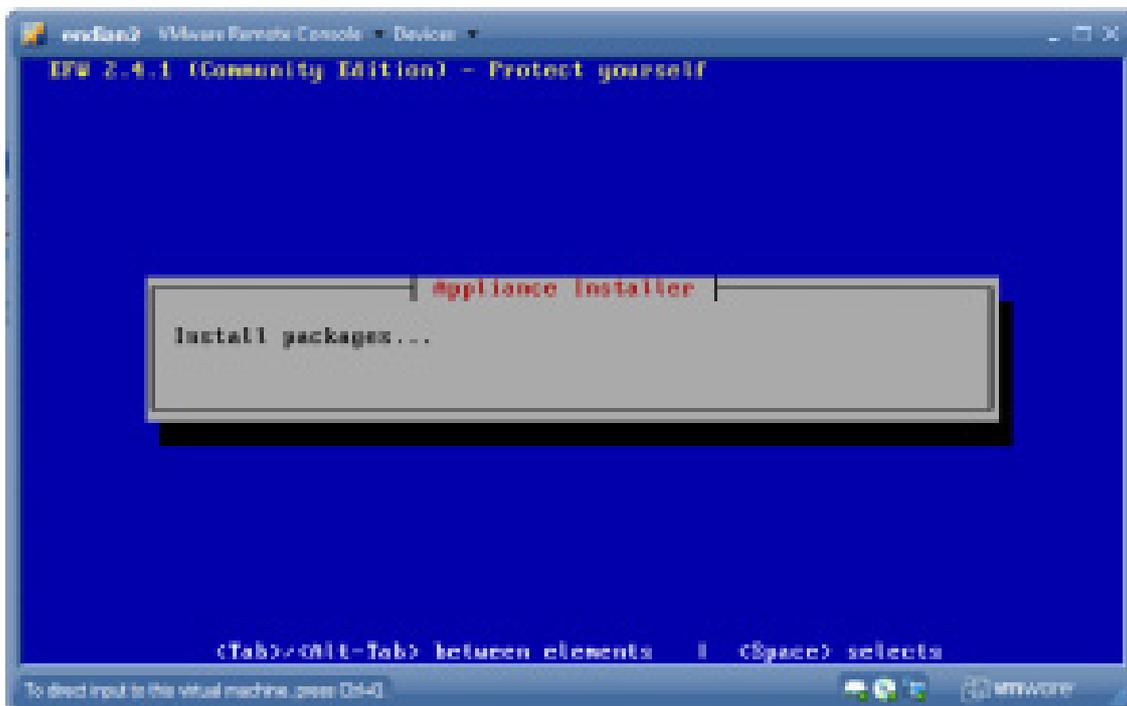
Il faut choisir le langage d'utilisation du firewall pour procéder à l'installation :



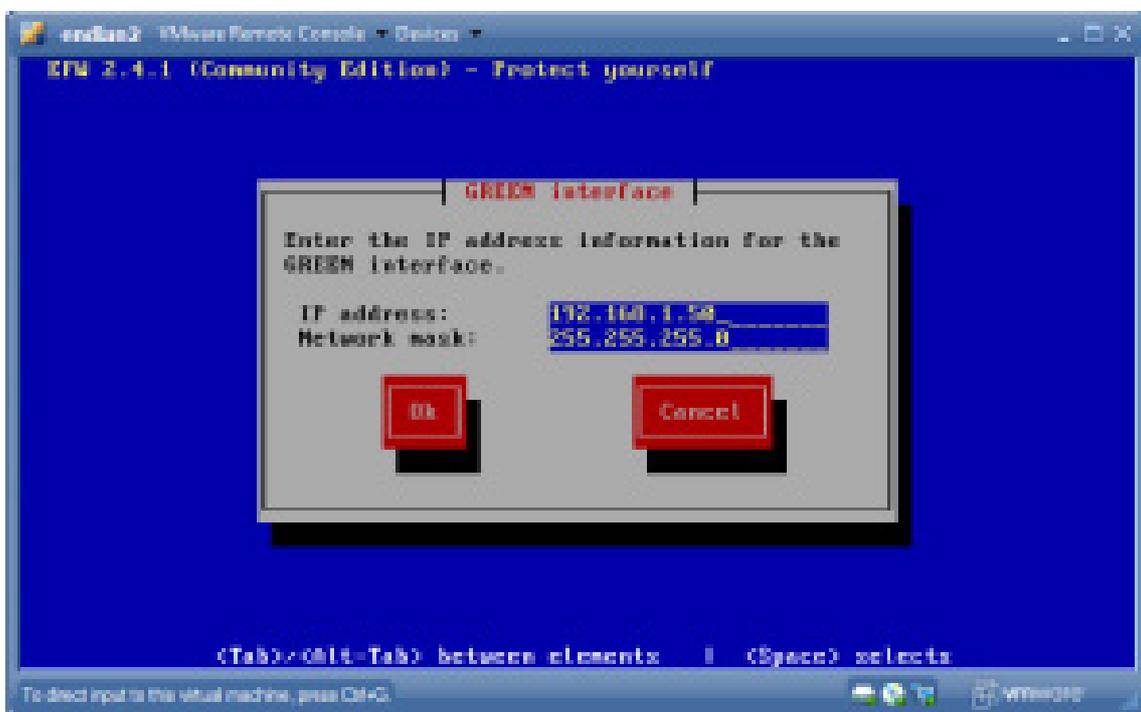
L'installation commence :



L'installation est en cours :



Nous ajoutons ici l'adresse IP de l'interface Verte de notre firewall :



Fin de l'installation :

