### 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

Chapitre	e1 : Introduction générale1
Chapitre	e2 : Notions générales sur la virtualisation
2.1.	Définition de la Virtualisation
2.2.	Historique de la Virtualisation
2.3.	Les avantages de la virtualisation
2.4.	Fonctionnement de la virtualisation7
Chapitre	e3 : Les risques de sécurité dans un environnement virtuel
3.1.	Virtualisation et sécurité9
3.2.	Solutions de sécurité proposées10
Chapitre	e 4: Conception et mise en place du centre de données virtuel 12
4.2.	Les fonctionnalités de VMware Server 2.0.2
4.3.	Création d'une machine virtuelle14
Chapitre	e 5 : Sécurisation du centre de données virtuel
5.1.	Sécurisation du centre de données virtuel
a.	Le Pare-feu (ou firewall) Endian
5.2.	Solution proposée
a.	Principe du filtrage
b.	Adressage IP
с.	Administration du Firewall
Conclusi	on
Bibliogra	aphie

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. <u>Historique de la Virtualisation</u>

La virtualisation comme on la connait 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, LinuxvServer, ou VirtualBoX, et aussi dans le même temps des logiciels gratuit, 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.
- Réduiser 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.

- 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 switchs virtuels sur lequel on connecte plusieurs hôtes virtuels.

On associe ensuite à chacun de ces switchs 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 switchs 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, préproduction, 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 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 dûs 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 maitriser 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. <u>VMWare Server</u>

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 accédez 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:

Login Name		
Password		

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

Mastère N2TR-UVT

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

🧿 Winaco Jafa	edaster Reb kons (errijks	hed)	
Application	Visei Rathire Idministration	1)0 .	telp   Virtual Appliance
Investory	Virtual Machines		
ant-PC	Create Linual Mechine	el Mathines Taska Events Remissions	
	Add Wrbail Redives to Diversory Research Wrbail Hostone Rower	nor-HC FTF	Add Untuel Rectine to Inventory     Add Untuel Rectine to Inventory     Add Intestine     Configure Options
		<ul> <li>Fertive(R) Duel-Core CPU 14400 # 2.2009c</li> <li>1 CPU x 3 Corea</li> <li>1 200 x 10 Corea</li> <li>1 200 Mite</li> </ul>	<ul> <li>Sitt Host Settings</li> <li>Solt Vitial Rectine Startup/Shubber</li> <li>Safrach Seturo's List</li> <li>Vitiaane Tige</li> </ul>

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

Pages	Name and Location		
Name and Decision Guest Operating System Hemory and Processors	* Enter a descriptive name i datastore where its config	br your new vitual machine wation files will be seved.	and specify the
tard Diek	NUME: PLOTE		and the second second
roperties	Demonstere -	\$2.55 GB	60.21 G8
lietwork Adapter Properties	standard	158.22 68	114.83 68
co/ovo orive hoserbes			
Napy Drive Properties			
All Cardenley			

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

Theare Infrastructure Web Access (acce@iocalhost) Ad 🛞 Create Virtual Hachine **Guest Operating System** Pages Name and Location ..... Select the operating system you plan to install in your virtual mechine. Your selection will be used to recommend settings and optimize performance. **Guest Operating System** early and Pressense Once the virtual machine has been created, you will need to install the operating system from your own installation disc. Harit Disk Properties Operating System: @ Windows operating system Network Adaptiv O Novell Network Properties. O Siciaria operating system. Einux operating system. CD/DVD Drive Other operating systems Properties. Microsoft Windows XP Professional (32-bit) . Version: **Hoppy Drive** Froduct Compatibility Properties Little Controller R. Real Gancel Back Help.

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 :

hegen .		Hemory and Processors
ame and Location West Operating System Ismory and Processors	-	Hemory Increasing a virtual machine's memory allocation can improve its
ard Disk roperties		Sipe: 256 MB
etwork Adapter reperties		Becommended Size (256 M8)     Becommended Minimum (120 M8)     The guest operating system may not start up below this size.
D/DVD Drive roperties		Becommended Maximum (4096 MB) Memory swapping may occur above this size.
loppy Drive raperties		Processors Select the number of processors carefully. We do not recommend reconfiguring this value after installing the quest operating system.
S& Controller		Count: 1 +

Rapport PFE

Pour cette machine virtuelle nous allous 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 devrons créer et donner la taille du disque virtuel que la machine virtuelle utilisera :

Pagers	Hard Disk
Name and Location Guest Operating System Name Operating System Name Operating System Name Operations Name Control Drive Name Control Drive Name Control Drive Name Control Drive	A virtual disk is a special type of file, which will start small and then green larger as you wild applications and data to your virtual mechanis. Chasse this option is said a black disk to your virtual mechanis. Use an Exterior Wirtual Disk Chasse this option to muse or share a hard disk from another virtual mechanis. Desh't Add a Hard Disk

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

Pages		Properties		
Name and Location		How much Capacity:	seftware and data should this hard disk be	able to store?
fard Disk		Location:	[standard] PC-DH2/PC-DH2.vmdk	Browse
laperties		10000	114.02 GB available	
ietwork Adapter		+ File Opt	tions	
roperties	4	> Disk Me	de	
COVOVO Drive Properties		- Virtual	Device Node	
Nopy Drive.		> Pulicies		
58 Controller	-4			

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 :

Create Virtual Hachine		;
Pages	Properties	
Name and Location Guest Operating System Memory and Processors Hard Disk Properties Statem CD/DVD Drive Properties Floppy Drive Properties Floppy Drive Properties	Which network will your virtual machine access? Network Connection: Bridged Connect at Power On: HostOnly NAT	-
USB Controller		
Help	Back Next	Cancel

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

Mais il en existe plusieurs dont voici la liste :

- Bridged
- HostOnly
- NAT

Nous cliquons sur "Next".

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



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

Pages	Properties	
Asene and Location  Guest Operating System Memory and Processors  Herd Disk Properties  Do/DVD Drive Properties  Disk Controller	In order to access this media, a disc must be in the drive specified below, and the drive must be connected is your virtual machine. If you will use this device to install an operating system, you should insert the installation disc before powering on your virtual machine. Host CD/DVD Drive: E: Connect at Pawer On: Yes > Virtual Device Node	•
-	Eack Next Care	and i

Rapport PFE

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 devrons choisir si nous voulons avoir l'accès au contrôleur USB dans la machine hôte:

#### Mastère N2TR-UVT



Nous cliquons sur "Add USB Controller".

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

Please verify that your new	a virtual machine is configured correctly.
Name:	PC-DMZ
Location:	(standard)
Guest Operating System:	Microsoft Windows XP Professional (32-bit)
Hermony:	256 MB
Processors:	1
Hard Disk:	8 G8
CD/DVD Drive:	Using "E:"
USS Controller:	Ves
> Hore Hardware	
	Please verify that your ner Name: Location: Guest Operating System: Processors: Hard Disk: Network Adaptar: CD/DVD Drive: USS Controller: • Hore Hardware

Rapport PFE

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.

Baart Inhaithering Bils	inne (scribaliss)						
Application Infoating	Albination 🖉 🕺	0				1976	Chinal Appleria Nekata
fermitide f () merits	) and K Setting Vitel Ref	ran Tanka Barta Par	interior in the second				
D index D Smarth D FC-MC D FC-MC D FC-MC D FC-MC D Inter-Application D Inter-CPU D Inter-CPU	Casend I Notware Readiation Note I Notware Unique III Network Unique III Network Unique III Network Unique III Notware III Notware III Notware Note III Notware III Notware Note III Notware Note III Notware Note III Notware Note III Notware Note III Notware Note III Notware Note III Notware Note III Notware III Notware IIII Notware III Notware III Notware III Notware	ser K Indus(),Ded Car 1,01x1 Dra 40 1,0128	0v140+1 21992 246	280w		Commonts Control Inde - Sal Shad Hade - Sal Shad Shad - Sal Shad Hade - Sal Shad Hada - Sal Shad Hade - Sal Shad Hade - Sal Shad Hade - Sal Shad Hade - Sal Shad -	ning ning Summers ni Stanlagt Summer Samong ni T
	Betadores Rohi - Thosel	Canch \$75.18	hardson 6125-02	Lander C'Antinov	(astroid) interferent ingene	-	
tea.		Target		lister.	Trippent & -	Superville:	Completed 10
Dealer Johns Reduce		1000		December 1	NOTICES	1.0	NOV11138198

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. <u>Sécurisation du centre de données virtuel</u>

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 gérer 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 (réparation de charge).
- Il détecte automatiquement les coupures de connexion et bascule sur le fournisseur d'accès de sauvegarde (Haute disponibilité).

#### 5.2. <u>Solution proposée</u>

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 essayera 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. <u>Principe du filtrage</u>

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





Rapport PFE

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



Rapport PFE

#### 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 :



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



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



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 :

Ou bien :

Http://192.168.1.50

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

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

serveur 19. un mot de	(388.1.50 a Fadresse Restricted requiert un nom d'utilisate passe.
	Nom d'utilisateur
100	Mot de passe
	Mémoriser ces informations

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

Mastère N2TR-UVT

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

	Iption in lines	. Berchan	Pare A	n Berven ine	مراجعهایی	4 BV	Junter		
	Tableau de bord								
ableau de boed	frenat-endar.location	uit .		Interfaces riseau					
onfiguration classes	in the second se			Districtions	Tree	1 interes	fbe:	antrast	Section
leties dischargent	Vacaina 2.4	1	12	14	shand	North Indiana	Versie herte	11104	64100
into the passes	terms 21	10.20-		100	attended	Section from	Versie autour	12,000	4440
NO Console	and the second s	140.000			-	Managine Inc.	Advention in the state	11.00	1.1.1
colis 504	Freedometric 19		100		and the second	The second second	YES BORD	1.1.1004	1000
and the dutichape	Outs updated at 15	35-85	10		all and the	verse had	Yere einest	111009	1111
aureparate			1	tell:	diam'n.	Were in head	Versie haut	0.056	10.000
eriter	Industry for the matter	-	10	100	effective	Terris had	Vete le tract	0.0 1016	10.03%
ane ceretà.			$\sim 10^{-10}$		dent	Territo haut	Versiellast.	1115%	10.000
	CP0.1	50%	Inco	ming traffic in Kills	Contract, Name	in the set			
	Mension III	225	1°E						
	distant principal limits	11				0		_	404
	and a barrier man	(B	1			<b>n</b>			141
	discuss da	E 16 18				1			and a
			1						100
	1000000	104 MB	1						1000

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:

March 1997	Système dur Visses Services Revilles Service Reviews (VRV Journey)	
	Configuration reseau	
Californi de Secret	accentent de configuration réseau	
configuration ritarian nutus d'invicement	Ellipsi 141: Divisir la type d'Interface POIVOR	
Iola de passos Sola Comunio Landra 2006 Necessarios d'al"Nabage Necessarios Artificat Lanarcoperante	Note:     Indocrisition fail in Individual       © Investigation failed     Kontore cloteria.cos       © Investigation failed     Kontore cloteria.cos	

Rapport PFE

Mastère N2TR-UVT

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.

Commit	the state to be set to be an an and the set of the set
	Comparation Newsall
Taldeau de Jorid	Accorded to configurate cases
Aprile Stylegent	Enge 20: Divisir die conserviseense
Unis de passe	ORANGE: La partie réseau accessible par les servicurs depuis internet (DR2)
Neb-Conecki	La partie réseau pour les directs sans la (VIP)
Asiate 20H	form
Paramithes d'all'Ichage	
Deveçerze	14 brende
Remerciamente	0 8.0
	@ 804682.4.9.09
	TTT ANDAL TTT
	Endlar Preswall Community Indexed 2-4.1 (2) 2004-2009 Endlar
_	Exter Preved Community release 2.4.1 (2) 2014-2009 Ender
ntinua da terret	Exter Preved Community release 2.4.1 (2) 2014-2009 Ender Synthetice Ext. Telesteau Excession Parel Ins. Excession manufacture (relia) 101V Jour Comfi guration résidiau
idieus de bort ordigunation réseau	Ender Preved Community release 2.4.1 (2) 2014-2009 Ender Pyratiener End Metadaa Encyclom Parel fea Derverus mandalasse (veta) RPV Jou Configuration résideau Anexateuri de configuration résideau
ediese de bord onligunation réserva	Exter Preved Community release 2.4.1 (2) 2004-2009 Ender Rys Merine Elist Indiana Leccioni Parechea Enroveur mandataine (relac) INV Jos Configuration résidiau Parechea Enroveur mandataine (relac) Dape 3/8: Préférences réseau
ebless de bord ordiguestion riseraa Jertes dibuleresent 103 de gaase	Exter Preved Comunity release 2.4.1 (2) 2014-2001Ender Ryskinster Ellat Tolstatio Bervicets Pare-Tera Berverus mandataine (relia) 101V close Confi gunati on résidiau Pare-Tera Berverus mandataine (relia) 101V close Confi gunati on résidiau Pare-Tera Berverus mandataine (relia) 101V close Confi gunati on résidiau Pare-Tera Berverus mandataine (relia) 101V close Pare-Tera Berverus (relia) 101V close Pare-Tera Berverus (relia) 101V close Pare-Tera Berverus mandataine (relia) 101V close Pare-Tera Berverus mandataine (relia) 101V close Pare-Tera Berverus (relia) 101V close Pare-Tera B
ebless de bord certiguestion staares artes sticulierment uite de passes Aeb Conscie	Ender Preved Community release 2.4.1 (2) 2004-2009 Ender       Bysitive     End     Methods     Rank frag     Derveue manifesterer (relea)     Methods       Configuration résideu     Image: Still Printing case réseaux     Image: Still Printing case réseaux     Image: Still Printing case réseaux       Vetter (Reseau Informe (LAR)) de configuration     Image: Still Printing case réseaux
ableau de tord ordiguandiaes résona tertes d'écolomisent util de gaales velo Canacia cola 558	Ender Prevent Community release 2.4.1 (2) 2004-2009 Ender       Bysitives     East     Devices     Renv. Ers     Devices     Renv       Configuration réseau       Image: Str. Preferences réseau       VENT Obteseu leterrer (LAR) de configuration réseau       Advance P:       192:180.1.50
ebleau de bord certigunation réserve levies d'événement vite de passe vite Conscie coles 554 assentiones d'artichage	Ender Prevent Community release 2.4.1 (2) 2004-2009Ender         Bysithmar       End       Initiality       Ender Prevent Community release 2.4.1 (2) 2004-2009Ender         Bysithmar       End       Initiality       Ender Prevent Community release 2.4.1 (2) 2004-2009Ender         Configuration résoluture       Ender Prevent Community release 2.4.1 (2) 2004-2009Ender       Ender Prevent Community release 2.4.1 (2) 2004-2009Ender         Configuration résoluture       Ender Prevent       Ender Prevent Community release 2.4.1 (2) 2004-2009Ender       Ender Prevent Community release 2.4.1 (2) 2004-2009Ender         Open 200       Preferences classes       Ender Prevent Community release 2.4.1 (2) 2004-2005Ender       Ender Prevent Community release 2.4.1 (2) 2004-2005Ender         VERT       Other Sectors releases       Lin managuat dir releases       Ender Prevent Community release 2.4.1 (2) 2005Ender       Tel Prevent         Aposter data interscore adultion relies (une Privateguer de touse-release pair Tigries)       Ender Prevent Community release 2.4.1 (2) 2005Ender       Tel Prevent
ebleau de trord ceciliguration straeses tertes sticulmensent stil de paties nob Conscie colas 558 exemptores stigfficinage auregande	Ender Preved Community release 1.4.1 (2) 2004-2009Ender       Bysitive     East     Descention     Rank, East     Earthout     Ref       Configuration résiduau       Image: Still Prefixee Descrité réseau       Page: Still Prefixee Descrité réseau       Vent       Adresses P:       192:186.1.50       Adresses P:       192:186.1.50       Image: Reseau enterne statisticonneties (une Privateure de Source-Desnau par Tarte)
ebless de tent cinfiguration réseau letes d'Eurosent d'8 de paètes de Conscie coles 558 esembless d'efficienge esurgarite rolter	Ender Prevent Community release 2.4.1 (2) 2004-2009 Ender       Bysitivitier     End     Telefontia     Paren frag     Dervenur mansfallance (relia)     Minit     Jour       Configuration réseau       Image: Still Profilementes réseau       Image: Still Profilementes réseau       Vetter (Reseau Internet (LANG) de configuration       Advances Prime (LANG) de configuration de source filement)       Advances Prime (SANG) de configuration de source filement)       Advances Prime (SANG) de configuration de source réseau
ableau de bord pedigunation réseau artes d'événement uts de passes veb Consola colau 558 exemitions d'éfficiespe exemitions d'éfficiespe exemitions référ exercisments	Index Preved Community release 2.4.1 (2) 2004-2009 Ended       Index Preved Community release 2.4.1 (2) 2004-2009 Ended <t< td=""></t<>
ebleas de troit configuration réserva lartes d'évéenent tris de passe rols Conacie cola 554 encestores d'artichage auvegariée rolter encoclements	Exter Preved Community release 1.4.1 (c) 2004-2009Ender       Byteliner     Ext     Delate     Rank-free     Devade mandalative (joile)     NV     Joil       Configuration résionau     Image: Configuration résionau     Image: Configuration résionau     Image: Configuration résionau       Martiner 300 Preférences classes     Image: Configuration résionau     Image: Configuration résionau       Martiner 300 Preférences classes     Image: Configuration résionau       Martiner 310 Preférences classes adultion referes (une Princescer de touse -réseau par Tipre)       Image: Configuration résionau       Martiner 310 Preférences
ebleas de tord colliguration straesa artes dévinement sta de passe octo 558 asantines d'afficienge novegante rolter amerciements	Interfaceurs       Interfaceurs       Interfaceurs       Interfaceurs
ebless de teord configuration straesa lectes stituésement sta de passe let de passe let de passe let de passe sources stitués encode 558 encode 558	Interference Description       Mark Description       Description       Description       Description       Description         Interference       Part Linescer Description       MAX       Perception       Perception       Perception
ebleau de bord ordigunation réseau tertes d'événement uts de passes veb Conacia cole 558 esemètices d'éréchage esvegance rollar ensrciements	Interference     Interference     Interference     Interference       Interf
ebleas de bord colliguration réserva artes d'évéenent tit de pases rob Conacie cole 558 exemitors d'efficitage auvegariée roller enerciements	Spatience       Edd       Heavest Community release 0.4.1 (c) 2004-0000 Ender         Parallence       Edd       Heavest Excention       Barry Ender       Barry Ender <t< td=""></t<>
ebleau de trord colfiguration réserve lartes dévénement uta de paère robs 558 exemploes d'afficienge auvegante robler emorciements	Spatience       Edd       Here and Community release 0.4.1 (c) 2004-0000 Ended         Spatience       Edd       Here and Research (code)       Here and Research (code)       Here and Research (code)         Configuration release       Here and the configuration release       Lie matagoat de former (code)       Here and the configuration release         Worth Observation release       Here former (code)       Lie matagoat de former (code)       Advector des addresses additionnations (core Princesport de second-release) per Tipric)         Advector des addresses additionnations (core Princesport de second-release) per Tipric)       Image: file       Edd - 255 255 255 0       Image: file         Herefacese:       Fort function Description       MAC       Peripheiringee       Image: file       Image: file         Image:       Image: file       Image: file <t< td=""></t<>
ebless de tord colliguration straesa artes dévinement sta de paèse not Connois octo 558 assestores d'afficienge auvegante rister amarciamente	Interface       Int       Network Community release 1.4.1.00 (2004/0000 Codes)         Configuration release       Configuration release         Configuration release       Exercise release         VMIT (Interess Internet (LAN) do configuration       Lin manague de la 2005/2002 (000-2005/2000)         Adverse P       192,192,150         Adverse R       192,192,120         1       Adverse R         2       Adverse R         3       Adverse R         3       Adverse R         3       Adverse R         4       Adverse R
ebless de terré certiguestion réseau lectes disvinement da de paties vois disvinement doit de paties vois 556 escentions d'afficienge envergande rollar encoclements	Interferention       Name       Nam       Name       Name </td



Nous avons ici le choix de garder l'adresse IP de l'interface verte ajoutée lors de la 1<sup>ere</sup> 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.

Adre	sae P		192, 168, 2.5	0		reseau	AR OLA	(2)4 - i	255,255,255.0	
Appel	er der	s adresse	s additionnelle	is june Pr	nesque d	le sous-réser	n par tip	e0 (		
-										
					-					
intert	and the second									
	See.	1 Delegan	Deterministicat	10		Printeduktion	-			
			Schubbled 7			and the second second				
		*	Advances 2	00.00.20	01,98,02	error.				
15	2	4	Advanced Z	00.00.29	01:09:00	eth1				
23	7	~	Advanced 2	00.04.29	01.09.08	692				
	4	1	Advanced 2	00 00 29	01.09.60	6163				
_										
HERE	er nicitie		THE WAR-LESS	294671						
New	du de	maine :	localdonan	(]						
			Ci	onfigure	dion ré	seau				
(chean)	de ber	rd.		Annes	and the sale	-				
entige	e a time	n réneras								
-	ri-i-	ement								
ote de	Distances of			ROUGE (no	in eécurie	A, connexion	internet (W	MANUK.		
cole S	584			nter faces.						
er service	ren ette	ffichage		Port	Lisison	Description	MU	MO	Périphérique	
er en se	side			1	~	Advanced 2	00.66.29	01.09.02	647-0	
coliter .	_			2	*	Advanced 2	00.0+.29	e1.09.00	eih 1	
Contraction Cont	a man di	-		0 1	~	Advanced T	00.04.28	61.08.46	elb2	
				• •	~	Advanced 2	00.86.29	06/69/10	eth3	
				ALL ALL						
				(heneeme	nt de Fedr	erre MAG av				
				Desis:				automatio		
			1							
				• Ce cher	inter a second	the latest vid				

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

	Dynamics Had Mittaine	Dervices Particles Dervice	nandalain (hela) NY Lournaus	
	Configuration de Thôle			
diffice des hittes	Tan hike at stars			
tutuje terteces	O destruction			
	Auferstam 17. der Jücken	Harts Chille	Ben de domaine	Autor
	102.148.2.51	enver1082		13
	-102.103.1.01	PCLLAR		11
	192.158.4.51	P(4		11
	112108458	PC3		1
	112.108.132	POLAN		13
	112168.2.52	sever2.082		11
	102108-452	server-Appleadors		12

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

_	Systema Dat B	teese Senton	Pana-Nos Samaar mar	dalaha (nala) IRN sa	u Neur	-
	Éditeur de routage	statique				
Cotton das hiltes	Toolage statigue	Régles de restepe				
lactage for faces	Les estaies aduets	e duradape				
	O Solar in month					
	Reseau Asocroe	Manau de destination	Va la passervite	Remarque		Juliue a
	982 665 1.0	102.158.4.0	102.168.1.58			#/3
	102,008.1.0	102.155.2.9	192,168,1.58			#/3
	192,105.4.0	1923582.0	1021682.58			8/3

Mastère N2TR-UVT

	Editeur des règler	s de routage			
555on des hilfes	Rutop nature	Régles de routage			
tootage	The Designer and particular				
Intraces.	O correction for the	and the state of t			
	V STREET BOOM				
	# Source	Destination	da Viela Service pesservite (Tota)	levier lenarge	Artisers
	1 -7508-	1205-	Lathers repriamin principale	ritalle	+ # / 1
	2 102108-4.0	192,100,1.0	Laison nortante principale	YOM OF YORS	++2/1
	3 9039840	HE HE LE	Laisen reurtante prinspale	A IOP A IOP N	++#/1
	4 1023003.0	192,192,4,8	Laison nortaite principale	104-08F 1085	++#/
	1. 10210010	182 88 4 8	Laten mentante principale	8 IOUP N	++#/
	8 1923983.0	192,108,4,8	192.105.1.91	(1005)-	++#/1
	7 102310.1.6	182,198,2.8	102 106 1.56	-0000-	++#/1
	1 102340-40	183,198,2.8	102,104,3,58	-1003-	4 4 / 1

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

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

	System fail 6	iteen Services Para-A	serve of mendols	ninal IIV Joanas	6
	Paramitrages du p	parfect extrant			
Franklart de port / NAT	Pot Minardeg/10	analistic territor	restruction dis insite re-	dy sent	
Trate sofare Trate inter-2006	Rights autorites				
Traffic VPM	O toute we never	while provide press lines			
Acole système Degracme du Fare-Yeu	it facetor	Destination	Levelue .	Foldspue Remansport	Actives
and a second second second	1	00000	1074-0040-00108	-94	4 10 / 1
	2 x1000br		IGANE IGANGE	54	++#/
	3 -41083+	109	108440	+	++4/
	8 (1081)-	WART .	109-0090-00101		******
	5 -10054	192,158,1,55 192,168,1,86 192,168,1,57	30801	5 <b>1</b> 1	+ 87
	Legende 🖉 Jost (r	işər poz dhavise) 📋 Dhav	ich (diper par adice)	🥖 later 🍷 Reference to 100	in the second
	a Martine Inc. (Articles all	and the local division of the local division			

### Mastère N2TR-UVT

#### Nous traitons ensuite le flux sortant:

	Con	figuration du pa	ins-fesi sortant				
Transfert der parts 7647		Right Industria					
trafic exclusion	0	Appendix site interested	Lots and in case No.				
Tradicition Zierre	- 12				The second		
112/02/12/05		and a second	201200-000			- and the state	As more
Assetts speaknee Originations the Pane-Key	-	8.5x	ADVOD	TONIO	1	alog 6779	+ 4 2
	8	108	20002	10445	100	alex 1795	++#/
		1007	A03.438	10401	- 100	allow FTP	****
	- 61	1017	ALC: NO	70405	- 599	allow SMTP	++#/
	5	VERT	000,002	TOPYIN	200	altrac PDP	++#/
	-0.	WHIT	ADVOR	109444		alless \$5.5	++#/
	T	WERT	REVER	TOYNES	- 24	and Ports	++#/
	-0	104	Rever	100995	199	1800 w 854.2%	++#/
		MART SALES	AGU/GE	тонконка	200	alow 201	++#/
	10	NORT NEW	HOVE	tares tares	-	alter 1943	+ ##

### Et finalement le trafic Inter-zone:

	Configuration du pa	ue-teu Inter-Zone			
Translet & port / NAT	Régles actuelles				
Traffic sortant		an a			
India Inter-Zone					
frantic VPN	4 Source	Destination	Service	Politique Remargae	Arbons
loois eystime	1 100	VERT	-7005-	-	+9/3
Degramme du Para-Fau	1 VERT	ORANCE	(1005)	-	++#/1
	1 054402	05250	1005-	-	++#/1
	4 10210243	Interface 1	470056	-	++#/1
	5 102 101 4.1	Martine 2	-70.5-	-	++#/1
	6 (1005)	-3205-	-0005-	-	+ #/1
	Afficier ins rieges des	a services da système 🔜 e	1		
	Activer le pare-tes	Nter-Zone			
	R Drogistrar las comp	ione Har-Zone acceptive dane i	a journal		

Rapport PFE

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

	Bysitee East D	nens Services	Para-Jau	Server mandelake (		Journal	
	Prony HTTP : politin	946					
(19)	Distriguistics Pro	tique d'accès Auli	estato 70	e de contens - Artholise	Jondry Md		
063	O Att access with						
-							
			When an international strength	And the second second	Classical	discourse of	And States as
879 ·	# Politique	boorne	The state state of the				

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":

	POP3: paramètres généraux					
TIP	<ul> <li>Paramétres pénéruszi Fill's à 100</li> </ul>	the individual				
975 TH	Durrer source (*071)					
10	Activi aur Greet:	X				
	Active our Orange.	8				
	Scenner anti-veve:	1	Filte & courter indisinate:	2		
	Einepister es connexions surfartes dans le Rauregende	purne du pare fru: 🖉				
			202000000		2	
	Data	n (mantri) on) Riptieren 19.05	(*) ip 20 mit, 5 alters, ball storing	a 1.41, 1.81, 1		
		College Fritander, Johns	sub stands CY1 (0) town-too	o troto		

Mastère N2TR-UVT

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

Openand     Openand     Openand     Openand     Openand     Openand       FTP:     SEX200000001 Virus       PCD0        PCD0	<b>O</b> a	ommunity		
FIP: scame was   RDA		System Plat Observe Services Area has been	e mandataire (relai) 🛛 🕬	
ACTION     Pressees       PEAP     Standard stand standard PEMP       Standard Standar		FTP: scanner virus		
NON FID- Solid D mode mode Model and Compare Activation and Activation and Activa	100 P	President		
Notify     Activation and Gamma     Important Gamma       Activation and Gamma     Important Gamma     Important Gamma       Important     Important Gamma     Important Gam	PON FDF	Analysis in the PP		
Holond and Comparison Transgather law connections apprend largers to borrow on theory of an interval of an apprend of another Placed and is in the interval of a specific data and apprend of another element is an addresse if it data addresse into data age if and it data and it da	9479	Authority and General	12	
Trappeter les conservoirs sontentes dans le pertanto de sous- tisses l'une adheses P l'une adheses le journande de sous- tisses l'une adheses P l'une adheses le journande de sous- tisses l'une adheses P l'une adheses le journande de sous- entente de sous- ne entente de sous- entente de sous- ententente de sous- entente de sous- entente de sous- entente de sous-	page	Address and Discourse	10 C	
Plased subit is interfrontparticipation in bound to bound on the planet subit is interfrontparticipation on the planet in the planet subit is interfrontparticipation on the planet is interfrontparticip		throughthar less contractions appraintee dans la purchande parte fau	52	
		Passed sizes to retering apprend deputs to bounds on the put de enum- ritance i une adhesian IP.1 pha adhesia that par Agnes.	Passed cube to retering another the second s	rene to the first but intergraphic to accur 40
				_
		* · · · ·	4	

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

(TP	Configuration Links Hubs Stands Las donaines	entrante Routage des courriels. Avancé	
0/5	Automatic access CAUTED		
4TP	Active is programme and		
SMTP	VERT ORANGE	POUGE	
089	actvá 💌 actvá	<ul> <li>E34</li> </ul>	
	Paramètre contre la Span ?		
	Elitrana das counted contrils foram 1		
	randyr are concerned at specifi		
	[14] Filtran Int. magnification (p. Constraint)		
	sala i ne ne sere sana man sana sa sana n		
	Choisir la gestion de Span *		
	Choisir la gestion de Span * louger vers ferglacement de quarantaine par défaut.		
	Choisir la gestion de Span * Rouger vers tenplacement de quarantaine par détaut. Sujet du spans	Courriel utilieë pour les natification	is de spani (spani admiri)
	Choisir la gestion de Span * Bouger vers ferglacement de quarantaine par défaut Sujet du spans **SPAB**	Courriel utilisë pour les natification	is de spani (spani admin)
	Choisir la gestion de Span * bouger vers ferglacement de quarantaine par défaut Sujet du spans **GPUAI** Niveau d'identification du spans *	Courriel utilisé pour les natification	is de span (span admin)
	Choisir la gestion de Span * Rouger vers tenplacement de quarantaine par détaut Sujet du spans **SPAda*** Niveau d'identification du spans * 4.5	Countiel utilisié pour les natification Niveau de spans requis * 8.3	e de spam (spam admir)
	Choisir la gestion de Span * Touger vers ferglacement de quarantaine par défaut Sujet du spans **SPAB** Niveau d'identification du spans * 4.0	Courriel utilisé pour les natification Niveau de spans requis * 4.3 Devoer un avertisacement asuleme	is de spars (spars admin) ent au niveau intérieur *
	Choisir la gestion de Span * Bouger vers ferglacement de quarantaire par défaut Sujet du span **SPAU*** Niveau d'identification du span * 4.5 Niveau de mise en quarantaire du span *	Courriel utilisé pour les natification Niveau de span requis * 4.3 Envoyer un avertisasement asuleme	e de span (span admin) ent au riveau intérieur *
	Choisir la gestion de Span * Touger vers femplacement de quarantaine par défaut. Sujet du spann **SPAA!** Niveau d'identification du spam * 4.5 Niveau de mise en quarantaine du spam * 8.3	Courriel utilisé pour les natification Riveau de spars requis * 4.3 Envoyer un avertisaement asuleme 10	e de spare (apare admin) ent au niveau inférieur *
	Choisir la gestion de Span * bouger vers ferglacement de quarantaire par défaut Sujet du spars **SPAge** Niveau d'identification du spars * 45 Niveau de mise en quarantaire du spars * 63 Filtrage de spars *	Countiel utilisië pour les natification  Niveau de spans requis *  4.1  Envoyer un avertissement seuleme  10  Japenisation *	e de spara (spara admin) ent au niveau infécieur *

	Prory SMTP : Configuration				
	Configuration Lates Non-Term	da . Las dominas entre	rta - Routage des court	the Avenue	
	Activer to proxy SMTP	(Carlot Carlot C		REACE	
-	active a	el acted		actre .	
	Faramiltees contro la visus ?	fold to define the entire	ince settings of the S	arp	
	Le scanerar de mus pour la E Scaner la couriele contre las	fold to define the anti- ny Diandling: vinus ad- vitus	inus settings of the S nici querentine locati	arp er()	
	Choisir la peritor de virus *				
	incluser users familiariament de cuant	erinite her Akted	-		

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

bouger vers l'emplacement de quarantaine par défaut	-	
		Courriel utilisé pour les notifications de virus (virus admin
File settings 7		
Goover les Tichiers par extentions "		
Iki beguer es tichers par costions		
Choisir la pestion de fichiers bloqués *	122.3	
bouger vers l'emplacement de quarantaine par défaut		
Chalatries tones de fichier à biomar (nar exterilor	4	Email used for blocked file notifications (file admin)
and a second s		
Enhanced Windows Metafile picture Cemils		
Enhanced Windows Metallie polure (, enit) Report (, enit)	*	
Enhanced Windows Metafile picture (.emf) Program Face Visual Pacevo compiled program (.fxp)	-	Bioquer les fichiers avec des doubles exteinsions
Enhanced Windows Metafile picture (, emf) Proprint ( and) Visual Pickfire compiled program (, fxp) Windows Program Group Re ( prp)	-	Bioquer les fichiers avec des doubles extensions
Enhanced Windows Metafile picture (, enit) Program (, eac) Visual Facility compiled program (, fxp) Windows Program Group Rie (, grp) Help Rie (, hip) Manietan Finitian antibus format (, hun)	-	Bioquer les fichiers avec des doubles extensions
Enhanced Windows Metafile picture (, enf) Rogram ( and) Visual Funktivo compiled program (, fxp) Windows Program Group file ( grp) Help file (, hig) Manintesh Fanklan antiking formal ( here)		Bioquer les fichiers avec des doubles exteinaions
Enhanced Windows Metalite picture (.ent) Rogenin (.ens) Visual PaxPro compiled program (.fxp) Windows Program Group Ris (.prp) Help Ris (.htg) Manintrah Ristlan antibug Romat (.htm)		Bioquer les fichiers avec des doubles extensions
Enhanced Windows Metafile picture (.enf) Ropping (.eng) Visual Positivo compiled program (.fxp) Windows Program Group file (.prp) Help file (.htg) Manietash Rinflan antibua formal (.htm) Switet le procest transparent 9	•	Bioquer les fichiers avec des doubles extensions
Enhanced Windows Metalite picture (.ent) Report (.ent) Visual Packyo compiled program (.fxp) Windows Program Group file (.prp) Help file (.htg) Manietash Ristlan archiva Recent (.here) Eviter le provy transparent 9		Bioquer les fichiers avec des doubles extensions Bioquer les fichiers avec des doubles extensions

### 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

Mastère N2TR-UVT

### Annexe

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



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



Rapport PFE

#### L'installation commence :





Mastère N2TR-UVT

#### L'installation est en cours :

🔰 endiană: Wilver Romata Console - Devicer -	_ = ×
EFW 2.4.1 (Community Edition) - Protect yourself	
Install packages	
(Tab)/(Alt-Tab) between elements   (Space) selects	
To deed input to the vituel mechanic press Col-C	anwore 🧃

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

🔰 endias 3 "Wiver Remote Constant - Devices -	- = ×
EFW 2.4.1 (Community Edition) - Protect yourself	
GREEN interface Enter the IF address: information for the GREEN interface. IF address: 192.140.1.52 Hetwork mask: 255.255.0 Consel	
(Tab)/ONIt-Tab) between elements (Space) selects Tedestrots to stainable particle	

Fin de l'installation :

IFW 2.4.1 (Community Edition) - Protect yourself
EFW was successfully installed. Flease remove any floppy disks or CDEDRs in the computer. If your system fails to hoot properly, please try hooting from a BOS diskette and running 'FDISK AMBR' to re-create the Baster Boot Record. Setup will now run where you may configure ISDH, network cards, and the system passwords. After Setup has been completed, you should point your web browser at http://efw-community in thtp://efw-community.iB413 (ar whatewer you name your EFW), and configure dialup networking (if required) and remote access. Remember to set a password for the EFW 'dial' user, if you wish non EFW 'admin' users to be able to control the link.
(Tabb/ Git-Tab) between elements   (Space) selects