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

Rapport - Projet 1 Implanter un réseau



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



-Dan Chu, Senior Director of product, VMware

Présentation du projet	4
Modifications apportées au projet	4
Tâches réalisées	5
RAID - Redundant Array of Independent Disks	5
Installation d'un serveur FTP	11
Installation d'un serveur web	24
Configurer une connexion à distance	27
Virtualisation	30
Configuration d'un pare-feu dans un environnement virtuel	49
Création d'une connexion VPN	95
Conclusion	100
Notes	102

Présentation du projet

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

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

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

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

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

Modifications apportées au projet

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

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

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

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

Ceci conclut les modifications majeures apportées au projet.

Tâches réalisées

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

RAID - Redundant Array of Independent Disks

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

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

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

- **RAID 0** : « *block-level stripping without parity or mirroring* ». Niveau de RAID qui ne dispose d'aucune redondance ou tolérance de faute, mais améliore les performances avec un parallélisme entre les disques durs lors des opérations d'écriture et de lecture. Un bris d'un disque dans la batterie RAID entraîne la perte de toutes les données.
- RAID 1 : « block-level mirroring without parity or stripping ». Les données sont écrites de manière systématique et identique sur tous les disques durs de la batterie. Il offre un niveau de protection de n-1 disque(s). Lors d'un bris de disque dur, les données sont toujours accessibles tant et aussi longtemps qu'un disque de la batterie fonctionne.
- RAID 5 : « block-level stripping with distributed parity ». Tout comme le RAID 0, les données sont divisées à travers tous les disques de la batterie, entraînant de ce fait des améliorations en terme de performances. Le RAID 5 est pourvu d'une redondance distribuée à travers tous les disques de la batterie. Il procure une tolérance de faute d'un disque dur. Si deux disques brisent en même temps, les données de la batterie sont

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



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



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

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

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

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

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

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

Pour conclure la présentation du RAID :

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

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

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

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

Voici les résultats :





RAID JBOD Matériel

RAID 0 Matériel

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

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

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

Installation d'un serveur FTP

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

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

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

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

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

Ce protocole peut fonctionner avec IPv4 et IPv6.

Installation d'un serveur FTP - Guide étape par étape

1. Ajoutez le rôle dans Server Manager.



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

2	Add Roles and Features Wizard
Select installation	type Destination server WINDOWS2012SERV
Before You Begin	Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Server Selection Server Roles Features Confirmation Results	 Role-based or feature-based installation Configure a single server by adding roles, role services, and features. Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
	< Previous Nixt > Install Cancel

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

A	Add Role	s and Features W	/izard	- • ×
Select destination	n server		DEST WIN	INATION SERVER IDOWS2012SERV
Before You Begin	Select a server or a virtual	hard disk on which t	to install roles and features.	
Installation Type	 Select a server from th 	e server pool		
Server Selection	O Select a virtual hard dis	sk		
Server Roles	Server Pool			
Features				
Confirmation	Filter:			
Results	Name	IP Address	Operating System	
	WINDOWS2012SERV	10.182.21.111,	Microsoft Windows Server 2012 Standar	rd
	1 Computer(s) found			
	This page shows servers the Add Servers command in collection is still incomplete	hat are running Wind Server Manager. Offl te are not shown.	lows Server 2012, and that have been add ine servers and newly-added servers from	ed by using the which data
		< Prev	ious Next > Install	Cancel

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

Before You Begin Installation Type Server Selection Select one or more roles to install on the selected server. Server Roles Roles Description Partures: Confirmation Active Directory Certificate Services			
Before You Begin Installation Type Select one or more roles to install on the selected server. Server Selection Roles Description Server Roles Active Directory Certificate Services FTP Server mables the transfer of files between, and server by using the FTP protocol. User, can establish an FTP connection and transfer files by a Active Directory Ightweight Directory Services FTP Server mables the transfer of files between, and server by using the FTP protocol. User, can establish an FTP connection and transfer files by a Active Directory Ightweight Directory Services FTP client or FTP-enabled Web browser. Confirmation Active Directory Ightweight Directory Services Active Directory Ightweight Directory Services FTP client or FTP-enabled Web browser. DHCP Server DHCP Server DHCP Server DHCP Server Network Policy and Access Services Remote Desktop Services Remote Access Remote Desktop Services Web Server (Installed) Web Server (Installed) Windows Deployment Services Windows Server Update Services Windows Server Update Services	elect server role	S	DESTINATION SERVE WINDOWS2012SER
Installation Type Roles Description Server Roles Active Directory Certificate Services Active Directory Certificate Services Active Directory Lightweight Directory Services Active Directory Lightweight Directory Services Active Directory Rights Management Services DHCP Server Server Network Policy and Access Services Print and Document Services Remote Desktop Services Volume Activation Services Web Server (Its) (Installed) Web Server (Its) (Installed) Web Server (Its) (Installed) Windows Deployment Services Windows Server Update Services Windows Server Update Services Windows Server Update Services Windows Server Update Services Server Server Server Server Server Server Windows Server (Installed) Windows Server Update Services Windows Server Update Services Services Services	Before You Begin	Select one or more roles to install on the selected server.	
Server Roles Active Directory Certificate Services and server by using the FTP protocol. Users can ad server by using the FTP protocol. Users can ad server by using the FTP protocol. Users can ad server by using the FTP protocol. Users can ad server by using the FTP protocol. Users can ad server by using the FTP protocol. Users can ad server by using the FTP protocol. Users can ad server by using the FTP protocol. Users can ad server by using the FTP protocol. Users can ad server by using the FTP protocol. Users can ad server Definition Active Directory Ederation Services Active Directory Rights Management Services an FTP client or FTP-enabled Web browser. DHCP Server DHCP Server DNS Server Fax Server Fax Server Fax Server P File And Storage Services (Installed) Hyper-V Network Policy and Access Services Print and Document Services Remote Desktop Services Volume Activation Services Volume Activation Services Web Server (Installed) Web Server (Installed) Windows Deployment Services IIS Hostable Web Core IIS Hostable Web Core IIIS Hostable Web Core IIIS Hostable Web Core Windows Server Update Services Windows Server Update Services	Installation Type	Roles	Description
Windows Server Update Services	Server Selection Server Roles Features Confirmation Results	Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Application Server DHCP Server DNS Server Fax Server B File And Storage Services (Installed) Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services Volume Activation Services Web Server (IIS) (Installed) Web Server (IS) (Installed) Web Server (IS) (Installed) Web Server (IS) (Installed) Windows Deployment Services UIS Hostable Web Core Management Tools (Installed)	FTP Server enables the transfer of files between a clie and server by using the FTP protocol. Users can establish an FTP connection and transfer files by usin an FTP client or FTP-enabled Web browser.
< Previous Next > Install Ca		Windows Server Update Services	Previous Next > Install Cancel

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

a	Add Roles and Features Wizard	_ 0 ×
Select features		DESTINATION SERVER WINDOWS2012SERV
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select one or more features to install on the selected server. Features Failover Clustering Group Policy Management Ink and Handwriting Services Internet Printing Client IP Address Management (IPAM) Server iSNS Server service LPR Port Monitor Management OData IIS Extension Media Foundation Message Queuing Multipath I/O Network Load Balancing Peer Name Resolution Protocol Quality Windows Audio Video Experience RAS Connection Manager Administration Kit (CMAK) Remote Assistance Remote Server Administration Tools RPC over HTTP Proxy SIMIP Service	 NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
	Subsystem for UNIX-based Applications [Deprecated] Telnet Client	v
		< Previous Nex Install Cancel
		▲ [PP 12] ↓ 5:05 PM 4/22/2013

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

à	Add Roles and Features Wizard	_ 0 ×
Confirm installatio	on selections	DESTINATION SERVER WINDOWS2012SERV
Before You Beain	To install the following roles, role services, or features on selected server, click Install.	
Installation Type	Restart the destination server automatically if required	
Server Selection	Optional features (such as administration tools) might be displayed on this page because they have been selected automatically	. If you do not want
Server Roles	to install these optional features, click Previous to clear their check boxes.	
Features	Web Server (IIS)	
Confirmation	FTP Server	
	TH Service	
	Export configuration settings Specify an alternate source path	
	< Previous Next >	Cancel
	2× P	5:07 PM

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

A	Add Roles and Features Wizard	_ 0 ×
Installation progre	255	DESTINATION SERVER WINDOWS2012SERV
Before You Begin	View installation progress	
	Feature installation	
	Installation succeeded on WINDOWS2012SERV.	
Features Confirmation Results	Web Server FTP Service FTP Service	
	You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking No command bar, and then Task Details. Export configuration settings	tifications in the
	< Previous Next > Ci	Cancel
	• P	5:09 PM 4/22/2013

Création d'un site FTP

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

Internet Information Services (IIS) Manager	_ 🗆 X
€ • • WIN-E6K421LK3EN >	🐱 🛛 🟠 🔞 •
Eile View Help	
Ele View Help Connections Connections Connection Start Page Connection Connection Connections Connection Connection	Server
Modules Output Request Server Worker Caching Filtering Certificates Processes Management Configurat Feature Shared Editor Delegation Configurat	
	63

- 2. Dans le panneau **Connections**, ouvrir le « node » du serveur et cliquer sur **Site**.
- 3. Cliquez-droit sur **Site**, et cliquez **Add FTP Site** pour ouvrir l'assistant de configuration **Add FTP Site**.

8	Internet Information Services (IIS) Manager	_ D X
WIN-E0K421LK	3EN > Sites >	₩ ≥ 0 •
<u>F</u> ile ⊻iew <u>H</u> elp		
Connections 🤤 - 🔛 🖄 😪	Sites	Actions
Start Page	Filter: • 🐨 😳 - 🥁 Show All Group by: No Grouping •	Set Website Defaults
Application Pools	Name A ID Status Binding Path	G Add FTP Site
Add Website	lisle 2 Started (html 122.168.0.4-21: (ftp) %SystemDrive%\inetpub\www.root	Beln
Befresh		W hop
💣 Add FTP Site		
Switch to Content	View	
< 111 > 3	Fetures View Content View	
Ready		ea

- 4. Sur la page de **Site Information**, dans la boîte **FTP site name**, tapez le nom du site FTP.
- 5. Dans la boîte **Physical path**, tapez le répertoire racine du serveur FTP ou cliquez sur le bouton **Browse** pour localiser le répertoire.

	Add FTP Site		? X
Site Information			
ETP site name: FTP Site 1 Content Directory Physical path: C:\inetpub\ftproot			
	Previous <u>N</u> ext	<u>F</u> inish	Cancel

- 6. Cliquez Next pour ouvrir la page Binding and SSL Settings.
- 7. Sous Binding, dans la liste IP Address, sélectionnez l'adresse IP du serveur.
- Dans la boîte nommée **Port**, tapez le numéro de port du serveur FTP. Par défaut, un serveur FTP opère sur le port **21**.
- 9. Cochez la case **Start FTP site automatically** pour rendre automatique l'exécution du serveur FTP au démarrage du serveur.
- 10. Sous SSL, dans la liste des SSL Certificates, sélectionnez un certificat SSL si nécessaire.

- 11. Sélectionnez une des options suivantes :
 - Allow SSL: Autorise le serveur FTP de supporter les connexions SSL et non-SSL avec un client.
 - **Require SSL**: Le cryptage SSL est requis entre le client et le serveur pour établir une communication.
 - No SSL: Aucun cryptage SSL n'est requis pour établir une communication entre le serveur et le client.
- 12. Cliquer sur Next pour ouvrir la page Authentication and Authorization Information.

	Add FTP Site	?	x
Binding and SSL Settings			
Binding IP <u>A</u> ddress:	P <u>o</u> rt:		
Enable Virtual Hort Nameri	21		
Virtual <u>H</u> ost (example: ftp.contoso.com):			
✓ Start FTP site automatically			
SSL No SSL			
○ Allo <u>w</u> SSL			
○ <u>R</u> equire SSL			
SSL <u>C</u> ertificate:			
Not Selected	✓ Select View		
	Previous Next Einish Ca	ancel	

- 13. Sous **Authentication**, sélectionnez la méthode d'authentification que l'administrateur souhaite utiliser :
 - **Anonymous**: Autorise tous les utilisateurs à se connecter au serveur et à avoir accès au contenu de celui-ci sous le nom de **anonymous** ou **ftp**.
 - Basic: Un nom d'utilisateur et mot de passe est requis pour pour que l'utilisateur puisse se connecter au serveur et ainsi avoir accès à son contenu. Une authentification de type
 Basic transmet les mots de passe sur le réseau sans le crypter. À utiliser seulement lorsque l'ont sait que la connexion entre le serveur et le client est sécurisée (SSL).
- 14. Sous Authorization, dans la liste Allow access to, sélectionnez une des options suivantes :
 - All Users: Tous les utilisateurs, autant ceux anonymes qu'identifiés, ont accès au contenu.
 - Anonymous Users: Les utilisateurs portant le nom Anonymous peuvent accéder au contenu du serveur.
 - Specified Roles or User Groups: Seuls les membres d'un certain rôle ou d'un certain groupe peuvent avoir accès au contenu du serveur FTP. Cocher la case Role ou Group le cas échéant.
 - **Specified Users**: Seulement les utilisateurs mentionnés dans cette boîte pourront avoir accès au contenu du serveur FTP. Taper le nom de l'utilisateur dans la boîte.
- 15. Si une option de la liste **Allow access to** a été sélectionnée, sélectionnez une et/ou l'autre des permissions suivantes :
 - Read: Permet à l'utilisateur autorisé de lire du contenu du répertoire du serveur FTP.
 - Write: Permet à l'utilisateur autorisé d'écrire du contenu dans le répertoire du serveur FTP.

16. Cliquez sur Finish.

Add FTP Site	? ×
Authentication and Authorization Information	
Authentication △nonymous ☑ Basic Authorization Allow agcess to: △III users ✓ Permissions ✓	
Previous Next	<u>Einish</u> Cancel

Le site FTP a été créé.

V]	Internet Information Services (IIS) Manager	_ D X
€ WIN-E0K421LK3	IEN ▶ Sites ▶ FTP-Site-1 ▶	📴 🖂 🟠 🔞 -
<u>File V</u> iew <u>H</u> elp		
VVIN-EGK421LK3 Elie View Help Conections Start Page S	IEN + Ster + FTP-Ste-1 +	Image of Pick Image of Pick Actions Image of Pick Bindings Bindings Image of Pick Image of Pick Namage of Pick Image of Pick Advanced Settings Image of Pick Image of Pick Ima
C III >	E Features View 🜊 Content View	ea.;
· · · · · · · · · · · · · · · · · · ·		

Installation d'un serveur web

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

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

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

Création d'un serveur web - Guide étape par étape

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

8]	Internet Information Services (IIS) Manager	_ 🗆 X
€ WIN-E0K421LK3EN ►		📴 🛛 🟠 🔞 •
<u>File View H</u> elp		
Ele View Help Connections WIN-EGK421LK3EN HOME Start Page WIN-EGK421LK3EN HOME Application Pools Application Pools Authentic Authorizat Browsing Document Browsing Configurat Configurat Configurat Editor Delegation Configurat	siroup by: Area Image: Connection Machine Kay Page and Strings Image: Connection Machine Kay Page and Controls Image: Connection Machine Kay Pa	Actions Manage Server Pestant Start Start View Application Pools View Stes Change -NET Framework Vest New Web Platform Components Peter Help
Keady		*i .:

1. Ouvrir le **IIS Manager**.

- 2. Dans le panneau **Connections**, ouvrir le « node » du serveur et cliquer sur **Site**.
- Cliquez-droit sur Site, et cliquer Add Web Site pour ouvrir l'assistant de configuration Add Web Site.

V ij	Internet Information Services (IIS) Manager	_ 🗆 🗙
€ → HYPER-V-SERVER → Sites →		🔯 🖂 🟠 i 💽 -
File View Help		
Connections	Citor	Actions
🔍 - 🔚 🖄 😥	July Stres	💞 Add Website
Start Page	Filter: 🔹 🐨 🐨 🥁 Show All Group by: No Grouping 🔹	Set Website Defaults
- a Application Pools	Name ID Status Binding	Help
⊳ iii Sit	Default Web Site Started (ht *:80 (http)	
Ka Refresh		
Switch to Content View		
	< >>	
	Features View 🚰 Content View	
Ready		• <u>1</u> .:

- 4. Dans la boîte de dialogue **Site name**, tapez un nom pour le site web.
- 5. Si l'on désire sélectionner un pool d'application différent de celui préalablement listé, ouvrir la boîte de dialogue **Select Application Pool** et sélectionner le pool d'application désiré.
- 6. Sélectionnez l'emplacement physique du dossier où le site web sera installé.
- 7. Si l'emplacement physique sélectionné est situé sur un partage, cliquez sur **Connect As** pour spécifier les informations d'authentification pour accéder au partage de fichiers.
- 8. Sélectionnez le protocole pour le site web dans la liste de sélection **Type**.
- 9. Spécifiez une adresse IP pour le site web dans la boîte IP Address.
- 10. Sélectionnez un port pour le site web. Normalement, le port est 80.
- 11. Facultativement, tapez un nom d'hôte pour le site dans la boîte **Host Name**.

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

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

		Add Website		f	~
<u>S</u> ite name:	A	op <u>l</u> ication pool:			
Website1	D	efaultAppPool		S <u>e</u> lect	
Content Directory					
Physical path:					
C:\inetpub\wwwroo	t\Website1				
Pass-through authe	ntication				
Connector	Test Settings				
<u>c</u> onnect as	rest settings				
Rinding					
Type	IP address:		Port:		
http	10.0.3.2		80		
Host name:					
www.pierre-luc-deli	sle.com				
Example: www.cont	oso.com or marketin	g.contoso.com			
A Charles Markets and	P-t-L.				
 Start website imme 	diately				
			OK	Cance	

Configurer une connexion à distance

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

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

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

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

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

Configuration d'une connexion RDP - Guide étape par étape

- 1. Ouvrir l'explorateur de fichier Windows.
- 2. Cliquez-droit sur **This PC**, puis sélectionner **Properties**.



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



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

System Properties	×			
Computer Name Hardware Advanced System Protection Remote				
Remote Assistance	- I			
✓ Allow Remote Assistance connections to this computer				
What happens when I enable Remote Assistance?				
Advanced				
Remote Desktop				
Choose an option, and then specify who can connect.				
O Don't allow remote connections to this computer				
Allow remote connections to this computer				
 Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended) 				
Help me choose Select Users				
OK Cancel Appl	y			

La connexion à distance est désormais configurée.

Virtualisation

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

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

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

Il existe deux types d'hyperviseur :

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

Dans le premier cas, il s'agit d'un système qui n'opère que des machines virtuelles. Le système en l'occurrence VMware ESXi ou encore Microsoft Hyper-V, ne sert qu'à virtualiser des machines *clientes*. Un hyperviseur, comme celui de VMware, est un système d'environ 1 million de lignes de codes seulement (contrairement à un système d'exploitation qui peut en contenir facilement 25 millions de lignes). Cela procure toujours dans le cas de VMware ESXi, une surface d'attaque de loin réduite à celle d'un véritable système d'exploitation. Il en résulte un système monolithique¹ réduit en taille et qui procure une plus grande sécurité. Le cas de Hyper-V est légèrement différent puisqu'il opère conjointement avec le système d'exploitation Windows, mais l'hyperviseur est essentiellement un service distinct qui n'emprunte l'environnement Windows que

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

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

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

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

Vous trouverez ci-dessous une image comparative des hyperviseurs.



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



Configuration minimale pour VMware ESXi :

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

Guide d'installation de VMware ESXi étape par étape :

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



© Pierre-Luc Delisle et Guillaume Nadeau

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



3. Télécharger :

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

Your downloads are available below	
VMware vSphere Hypervisor 5.5 Update 1 - Binaries	
ESXI 5.5 Update 1 ISO Image (Includes VMware Tools) 2014-03-11 5.5.0 U1 328 MB iso	Start Download Manager
Boot your server with this image in order to install or upgrade to ESXi. This ESXi image includes VMware Tools. NOTE: ESXI requires 64-bit capable servers for installation and execution. Please refer to the VMware Compatibility Guide for a list of qualified server hardware.	Manually Download 🚽
MD55UM(¹): 36dfcb269a20d7bfe7323f825128e1a8 SHA15UM(¹): a735bc26fa596e6c875de0e25bc07f2a6f17296d	
VMware vSphere Client 5.5 Update 1 2014-03-11 5.5.0U1 358 MB exe	Start Download Manager
VMware vSphere Client installer (Client available in English, German, French, Japanese and Simplified Chinese)	Manually Download
MD5SUM('): 3323c27c0a1e36799881c61b1e990397 SHA1SUM('): acdf2fc3ea5536b9e9525441ad1b89a7417339f0	
VMware Tools 5.5 Update 1 - CD image for Linux Guest OSes 2014-03-11 5.5.0 U1 62 MB iso	Start Download Manager (
VMware Tools CD image for Linux Guest OSes	Manually Download
MD55UM(¹): 45a27ddfef5cef95cf1da0edb9dace82 SHA15UM(¹): 3f071d84d691e169df20342d4701c4bc66c0b9bd	
Version History - VMware vSphere Hypervisor 5.5	
Version History - VMware vSohere Hypervisor 5.1 Update 2	

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

$\bigcirc \bigcirc \bigcirc \bigcirc$	Downloads — bash — 120×10	M
Pierre-Lucs-MacBook-Pro:~ pierre- Pierre-Lucs-MacBook-Pro:Downloads MD5 (VMware-VMvisor-Installer-5.5 Pierre-Lucs-MacBook-Pro:Downloads	<pre>luc-delisle\$ cd /Users/pierre-luc-delisle/Downloads/ pierre-luc-delisle\$ md5 VMware-VMvisor-Installer-5.5.0.update01-1623387.x86_64.iso .0.update01-1623387.x86_64.iso) = 36dfcb269a20d7bfe7323f825128e1a8 pierre-luc-delisle\$</pre>	

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

- 6. Démarrez le serveur sur la clef USB.
- 7. Démarrez l'installateur de l'hyperviseur.


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

	Loading ESXi installer
Load ing Load ing Load ing Load ing Load ing Load ing Load ing Load ing Load ing	<pre>/net_nlx4.v01 /net_nlx4.v01 /net_tg3.v00 /net_vmxn.v00 /ohci_usb.v00 (glnative.v00 /rste.v00 /rste.v00 /sata_ahc.v00 /sata_ata.v00 /sata_st.v00</pre>
Loading Loading Loading Loading Loading Loading Loading Loading Loading	<pre>'sata_sat.v01 'sata_sat.v02 'sata_sat.v03 'sata_sat.v04 'scsi_acc.v00 'scsi_acc.v00 'scsi_bnx.v00 'scsi_bnx.v01 'scsi_fni.v00 'scsi_bnx.v01</pre>
Loading Loading Loading Loading Loading Loading Loading Loading Loading	<pre>/scsi_ips.v00 /scsi_lpf.v00 /scsi_neg.v00 /scsi_neg.v01 /scsi_neg.v02 /scsi_npt.v00 /scsi_npt.v01 /scsi_npt.v01 /scsi_npt.v02 /scsi_npt.v02 /scsi_qla.v00</pre>
Load ing Load ing Load ing Load ing Load ing Re locat i	fubci_usb.v00 ftools.t00 Xxorg.v00 fingdb.tgz ingpayld.tgz ng modules and starting up the kernel
	VMware ESXi 5.5.0 (VMKernel Release Build 1331820) VMware, Inc. VMware Virtual Platform 2 x Intel(R) Core(TM) i5-2540M CPU @ 2.60GHz 2 GiB Memory
	vmkplexer loaded successfully.

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



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



10. ESXi analysera les différents composants matériels du serveur.



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

Select a Disk to Install or Upgrade * Contains a VMFS partition # Claimed by vSAN							
Storage Dev	ice						Capacity
Local: * VMware, VMware Virtual Remote: (none)		ual S (mpx.	vmhba	1:CO:TO:LO)		40.00 Gib	
(Esc) Ca	ncel	(F1)	Details	(F5)	Refresh	(Enter)	Cont inve

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



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

VMware ESXi 5.5.0 Installer	
Enter a root password	
Root password: ****** Confirm password: *******	
Passwords match.	
(Esc) Cancel (F9) Back (Enter) Continue	

14. Confirmez l'installation.

Confirm Install
The installer is configured to install ESXi 5.5.0 on: mpx.vmhba1:C0:T0:L0.
Warning: This disk will be repartitioned.
(Esc) Cancel (E9) Back (E11) Install

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

VMware ESXi 5.5.0 Installer	
Installation Complete	
ESXi 5.5.0 has been successfully installed.	
ESXi 5.5.0 will operate in evaluation mode for 60 days. To use ESXi 5.5.0 after the evaluation period, you must register for a VMware product license. To administer your server, use the vSphere Client or the Direct Control User Interface.	
Remove the installation disc before rebooting.	
Reboot the server to start using ESXi 5.5.0.	
(Enter) Reboot	

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

VMware ESXi 5.5.0 (VMKernel Release Build 1331820)	
VMware, Inc. VMware Virtual Platform	
2 x Intel(R) Xeon(R) CPU E3-1230 v3 @ 3.30GHz 4.2 GiB Memory	
Download tools to manage this host from: http://192.168.178.164/ (DHCP) http://[fe80::20c:29ff:fe9a:3b79]/ (STATIC)	
(F2) Customize System/View Logs	(F12) Shut Down/Restart

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

VMware ESXi 5.5.0 (VMKerne)							
VMware, Inc. VMware Virtua)	nc. VMware Virtual Platform						
2 x Intel(R) Core(TM) i5-2410M CPU @ 2.30GHz 4 GiB Menory							
	Authentication Required						
	Enter an authorized login name and password for localhost.localdomain.						
Download tools to manage t http://192.7.100.129/ (DHC http://f680::296:29ff:fea	Configured Keyboard (US Default) Login Nane: <u>Croot</u>] Password: []						
	<pre></pre>						
		ssword for					
		⟨F12⟩ Shut Down/Restart					

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

System Customization	Configure Management Network
<mark>Configure Password</mark> Configure Lockdown Mode	Hostnane: localhost
Configure Management Network Restart Management Network	IP Address: 192.7.100.129
Test Management Network Network Restore Options	Network identity acquired from DHCP server 192.7.100.254
Configure Keyboard Troubleshooting Options	IPv6 Addresses: fe80::20c:29ff:feaa:87d4/64
View System Logs	To view or modify this host's management network settings in detail, press «Enter».
View Support Information	
Reset System Configuration	
	<pre></pre>

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

Configure Management Na	etwork	IP Configuration	
Network Adapters VLAN (optional) IP Configuration IPv6 Configuration DNS Configuration Custom DNS Suffixes	ure Management Network IP Configuration k Adapters optional) Automatic infiguration IP Address: 192,7.100.129 Subnet Mask: 255.255.255.0 Default Gateway: 192.7.100.2 IDNS Suffixes This host can obtain an IP addre parameters automatically if your network appropriate settings. IP Configuration This host can obtain network settings automatically if your network includes a DHCP server. If it does not, the following settings must be specified: () Use dynamic IP address and network configuration (o) Set static IP address and network configuration (c) Set static IP address (Space) Mark Selected	Automatic IP Address: 192.7.100.129 Subnet Mask: 255.255.255.0 Default Gateway: 192.7.100.2 This host can obtain an IP address and other network parameters automatically if your network includes a I server. If not, ask your network administrator for th appropriate settings.	ing DHCP he
	IP Configuration This host can obtain network setting includes a DHCP server. If it does n specified:	s automatically if your network ot, the following settings must be	
	 (c) Set static IP address and network (c) Set static IP address and network IP Address Subnet Mask Default Gateway 	configuration: [192.7.100.110] [255.255.255.0] [192.7.100.2] ed <enter> OK <esc> Cancel</esc></enter>	
<up down=""> Select</up>		<enter> Change <e< td=""><td>sc> Exit</td></e<></enter>	sc> Exit

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



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

Configure Management Networ	k	DNS Configuration	
Network Adapters VLAN (optional) IP Configuration IPv6 Configuration DNS Configuration Custom DNS Suffixes	Configure Management Network: Co You have made changes to the hos Applying these changes may resul disconnect remote management sof machines. In case IPv6 has been restart your host. Apply changes and reboot host? <y> Yes <n> No</n></y>	Manual Primary DNS Server: 192.7.100.5 Alternate DNS Server: Not set Hostname LabClus01 If this host is configured using DHCP, I and other DNS parameters can be obtaine or for firm t's management network. t in a brief network outage, tware and affect running virtual enabled or disabled this will (Esc) Cancel	DNS server addresses d automatically. If the appropriate
<up down=""> Select</up>		<enter> Change</enter>	⟨Esc⟩ Exit

- 22. Après le redémarrage du serveur, il faut s'assurer que nous avons une communication avec ce dernier. À l'aide d'une machine cliente sur le réseau, **lancer des requêtes ICMP** vers le serveur ESXi. Si le serveur répond, procédez aux étapes suivantes. Dans le cas contraire, dépannez la configuration réseau.
- 23. Installez VMware vSphere Client sur une machine cliente. Le logiciel permettra de configurer et administrer entièrement le serveur ESXi à distance.
- 24. Lorsque l'installation est terminée, **lancez VMware vSphere**.



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

	Iware vSphere Client ×
vmvvare VMware vSphere [™] Client	
In vSphere 5.5, all ne through the vSphere will continue to opera vSphere 5.0, but not vSphere 5.5. The vSphere Client is Manager (VUM) and R (e.g. Site Recovery N	ew vSphere features are available only Web Client. The traditional vSphere Client ate, supporting the same feature set as exposing any of the new features in still used for the vSphere Update Host Client, along with a few solutions Manager).
To directly manage a single To manage multiple hosts, vCenter Server.	e host, enter the IP address or host name. enter the IP address or name of a
IP address / Name:	10.0.1.10
User name:	root
Password:	*****
	Use Windows session credentials
	Login Close Help

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

27. Faites Enter sur Troubleshooting Options.



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



Configuration d'un pare-feu dans un environnement virtuel

Le projet avait également pour but de configurer un pare-feu pour le réseau que nous avions créé. Cependant, la solution proposée en laboratoire n'a jamais fonctionné. Elle constituait à la configuration d'un pare-feu avec FirewallBuilder. Bien que l'utilitaire semble bon, il n'est même plus répertorié dans la liste des dix meilleures applications pare-feu sur Linux selon TechMint² et plusieurs autres alternatives sont aujourd'hui beaucoup plus performantes.

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

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

² <u>http://www.tecmint.com/open-source-security-firewalls-for-linux-systems/</u>

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

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

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

- 1. Téléchargez le pilote et transférez le fichier dans le datastore du serveur ESXi.
- 2. Assurez-vous que la prise en charge SSH est bien activée dans le serveur ESXi.
- 3. Connectez-vous par protocole SSH au serveur ESXi. Sur Windows, utilisez Putty. Sur Mac OS X/Linux, le terminal UNIX est recommandé.
- 4. Entrez la commande suivante :

esxcli software vib install -v /vmfs/volumes/**driver_directory_in_datastore**/ VMware_bootbank_net-r816**X_**6.011.00-2vmw.510.0.0.799733.vib

Où :

- driver_directory_in_datastore représente le dossier dans le *datastore* où le pilote a été transféré.
- X représente le numéro de modèle de la carte Realtek, par exemple 8168 ou 8169
- 4. Redémarrez le serveur ESXi.

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

esxcli software vib list

Installer pfSense dans une machine virtuelle - Guide étape par étape

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

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

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

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



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

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

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

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

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

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

Ø		vSwitch0 Properties	_ □	×
Ports Network Adapters				
Configuration	Summary	vSphere Standard Switch Properties —		1 ^
1 vSwitch	120 Ports	Number of Ports:	120	
Q LAN	Virtual Machine			
Management Net	vMotion and IP	Advanced Properties		1
		MTU:	1500	
	ſ	Default Policies		
		Security		
		Promiscuous Mode:	Reject	
		MAC Address Changes:	Accept	
		Forged Transmits:	Accept	
		Traffic Shaping		
		Average Bandwidth:		
		Peak Bandwidth:		
		Burst Size:		
		Failover and Load Balancing		
		Load Balancing:	Port ID	
		Network Failure Detection:	Link status only	
		Notify Switches:	Yes	1.1
		Failback:	Yes	
Add	Edit Remove	Active Adapters:	vmnic0	
			Close H	elp

Cliquez sur Virtual Machine Network et cliquez sur Edit.

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

Ø	LAN Properties	×
General Security Traffic Shapin	a NIC Teaming	
Port Group Properties		1
Network Label:	LAN	
VLAN ID (Optional):	None (0)	
	OK Cancel He	slp

On devrait par la suite avoir un tel schéma réseau.

Stan	dard Switch: vSwitch0	Remove	Propertie	S
P	Virtual Machine Port Group	ical Adapters — Vmnic0 1	.000 Full	P
Ξ	0 virtual machine(s)			_
þ	VMkernel Port Management Network vmk0 : 10.0.1.10 fe80::224:81ff:fe1a:be5b			

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

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

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

View: vSphere Standard Switch Refresh Add Networking... Properties... Networking -Virtual Machine Port Group Physical Adapters Α 🔛 vmnic0 1000 Full D LAN 0 3 virtual machine(s) Windows Server 2012R2 ₽ ofSense ₽ Windows Server 2012 GN 骨 VMkernel Port 0 P Management Network vmk0:10.0.1.10 fe80::224:81ff:fe1a:be5b

Ø	Add Network Wizard - 🗆 🗙			
Connection Type Networking hardware car	be partitioned to accommodate each service that requires connectivity.			
Connection Type Network Access Connection Settings Summary	Connection Types Virtual Machine Add a labeled network to handle virtual machine network traffic. VMkernel The VMkernel TCP/IP stack handles traffic for the following ESXi services: vSphere vMotion, iSCSI, NFS, and host management.			
Help	< Back Next > Cancel			

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

Connection Settings			
	Create a virtual switch	Speed	Networks
	🔽 🔛 vmnic3 🚽	1000 Euli	None
	🖂 🔛 vmnic4	1000 Full	None
	vmnic5	1000 Full	None
	Vmnic6	1000 Full	0.0.0.1-255.255.255.254
	O Use vSwitch0	Speed	Networks
	Vmnic0	1000 Full	None
	Preview: Virtual Machine Port Group	Q	nysical Adapters

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

Ø	Ą	dd Network Wizard		- • ×
Virtual Machines - Conn Use network labels to i	ection Settings dentify migration compatible connec	tions common to two or more hosts	5.	
Connection Type Network Access Connection Settings Summary	Port Group Properties	WAN None (0)	.	
	-Virtual Machine Port Group WAN	Physical Adapters		
Help			< Back Next	: > Cancel

Cliquez ensuite sur Finish.

Ø	Add Network Wizard	_ □
Ready to Complete Verify that all new a	nd modified vSphere standard switches are configured appropriately.	
Connection Type Network Access Connection Settings	Host networking will include the following new and modified standard switches: Preview:	
Summary	WAN Q	

Le schéma réseau devrait ressembler à ceci.

Networking





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



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

Ø	Create New Virtual Machine
Configuration Select the configuration for	r the virtual machine
Configuration Name and Location Storage Virtual Machine Version Guest Operating System CPUs Memory Network SCSI Controller Select a Disk Ready to Complete	Configuration Create a new virtual machine with the most common devices and configuration options. C Custom Create a virtual machine with additional devices or specific configuration options.
Help	_≤Back Next ≥ Cancel

Donner le nom de pfSense à la machine virtuelle.

	Create New Virtual Machine
Name and Location Specify a name and locat	ion for this virtual machine
Configuration Name and Location Storage Virtual Machine Version Guest Operating System CPUs Memory Network SCSI Controller Select a Disk Ready to Complete	Name: jrfSense Virtual machine (VM) names may contain up to 80 characters and they must be unique within each vCenter Server VM folder. VM folders are not viewable when connected directly to a host. To view VM folders and specify a location for this VM, connect to the vCenter Server.
Help	<u>≤</u> Back Next ≥ Cancel

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

Sélectionnez le datastore désiré puis appuyer sur Next.

Ø	Crea	ate New Virtu	al Machine			-	D X
Storage Select a destination storage for the virtual machine files							
Configuration	Select a destination sto	rage for the virtua	I machine files:				
Name and Location	Name	Drive Type	Capacity	Provisioned	Free	Туре	Thin Prov
Virtual Machine Version	🎯 datastore1	Non-SSD	290.50 GB	66.57 GB	227.46 GB	VMFS5	Supporte
CPUs Memory Network SCSI Controller Select a Disk Ready to Complete	 ✓ ✓ Disable Storage D Select a datastore: 	RS for this virtual r	III machine				>
	Name	Drive Type	Capacity Pro	ovisioned	Free	Туре	Thin Provi
	<		III				>
Help				<u><</u> Back	Next	≥	Cancel

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

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

Ø	Create New Virtual Machine				
Virtual Machine Version					
Configuration Name and Location Storage Virtual Machine Version Guest Operating System CPUs	Virtual Machine Version This host or duster supports more than one VMware virtual machine version. Specify the virtual machine version to use. Virtual Machine Version: 4				
Memory Network	This version will run on VMware ESX 3.0 and later, and VMware Server 1.0 and later. This versio is recommended when sharing storage or virtual machines with ESX up to 3.5.	n			
SCSI Controller Select a Disk	O Virtual Machine Version: 7				
Ready to Complete	This version will run on VMware ESX/ESXi 4.0 and later. This version is recommended when sharing storage or virtual machines with ESX/ESXi up to 4.1.				
	This version will run on VMware ESXi 5.0 and later. Choose this version if you need the latest virtual machine features and do not need to migrate to ESX/ESXi 4.				
Help	<u>≤</u> Back Next ≥ Car	icel			

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

Ø	Create New Virtual Machine	_ 🗆 🗙
Guest Operating System Specify the guest operatin	g system to use with this virtual machine	Virtual Machine Version: 8
Configuration Name and Location Storage Virtual Machine Version Guest Operating System CPUs Memory Network SCSI Controller Select a Disk Ready to Complete	Guest Operating System:] appropriate defaults for
Help	≤Back	Next ≥ Cancel

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

Ø	Create New Virtual Mac	hine 📃 🗖 🗙
CPUs Select the number of virtu	al CPUs for the virtual machine.	Virtual Machine Version: 8
Configuration Name and Location Storage Virtual Machine Version Guest Operating System CPUS Memory Network SCSI Controller Select a Disk Ready to Complete	Number of virtual sockets: 1 Number of cores per virtual socket: 1 Total number of cores: 1 The number of virtual CPUs that you can add the depends on the number of CPUs on the host at number of CPUs supported by the guest OS. The virtual CPU configuration specified on this might violate the license of the guest OS. Click Help for information on the number of processors supported for various guest operations systems.	To a VM and the arrow of the
Help		<u>≤</u> Back Next ≥ Cancel

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

Ø	Create New Virtual Machine	_ D X
Memory Configure the virtual mach	ine's memory size.	Virtual Machine Version: 8
Configuration Name and Location Storage Virtual Machine Version Guest Operating System CPUs Memory Network SCSI Controller Select a Disk Ready to Complete	Memory Configuration 1011 GB Memory Size: 512 ÷ MB • 512 GB Maximum recommended for this 256 GB Maximum recommended for best performance: 8124 MB. 128 GB Maximum recommended for this 64 GB guest OS: 1 GB. 32 GB Minimum recommended for this guest OS: 1 GB. Minimum recommended for this 32 GB Minimum recommended for this 16 GB guest OS: 32 MB. 16 GB Minimum recommended for this 2 GB Minimum recommended for this 16 GB Minimum recommended for this 2 GB Minimum recommended for this 2 GB Minimum recommended for this 16 GB Minimum recommended for this 2 GB Minimum recommended for this 3 I GB Minimum recommended for this 1 GB Minimum recommended for this 2 GB Minimum recommended for this 3 I MB Minimum recommended for this 3 I MB Minimum re	
Help	<u>≤</u> Back Ne	ext ≥ Cancel

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

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

Appuyez ensuite sur **Next.**

Ø	Create New Virtual Machine
Network Which network connection	Virtual Machine Version: 8 s will be used by the virtual machine?
Configuration Name and Location Storage Virtual Machine Version Guest Operating System CPUs Memory Network SCSI Controller Select a Disk Ready to Complete	Create Network Connections How many NICs do you want to connect? 2 Network Adapter Power On NIC 1: LAN VEXUMENT NIC 2: WAN VEXUMENT If supported by this virtual machine version, more than 4 NICs can be added after the virtual machine is created, via its Edit Settings dialog. Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.
Help	≤ Back Next ≥ Cancel

Ø	Create New Virtual Machine	_ D X
SCSI Controller Which SCSI controller type	e would you like to use?	Virtual Machine Version: 8
Configuration Name and Location Storage Virtual Machine Version Guest Operating System CPUs Memory Network SCSI Controller Select a Disk Ready to Complete	SCSI controller BusLogic Parallel (not recommended for this guest OS) LSI Logic Parallel LSI Logic SAS VMware Paravirtual (not recommended for this guest OS)	
Help	<u></u>	Next ≥ Cancel

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

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

Ø	Create New Virtual Machine
Select a Disk	Virtual Machine Version: 8
Configuration Name and Location Storage Virtual Machine Version Guest Operating System CPUs Memory Network SCSI Controller Select a Disk Advanced Options Ready to Complete	A virtual disk is composed of one or more files on the host file system. Together these files appear as a single hard disk to the guest operating system. Select the type of disk to use. Disk • Create a new virtual disk • Use an existing virtual disk Reuse a previously configured virtual disk. • Raw Device Mappings Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a datastore. • Do not create disk
Help	≤ Back Next ≥ Cancel

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

Ø	Create New Virtual Machine	_ D X
Create a Disk Specify the virtual disk size	and provisioning policy	Virtual Machine Version: 8
Configuration Name and Location Storage Virtual Machine Version Guest Operating System CPUs Memory Network SCSI Controller Select a Disk Create a Disk Advanced Options Ready to Complete	Capacity Disk Size: 8 g GB Disk Provisioning (Thick Provision Lazy Zeroed Thick Provision Eager Zeroed Thin Provision Location Costore with the virtual machine Specify a gatastore or datastore duster: Browse	
Help	<u>≤</u> Back Next	t <u>Cancel</u>

Dans la fenêtre Advanced (ptions, il est inutile	de modifier quoi que ce soit.
-----------------------------------	------------------------	-------------------------------

Ø	Create New Virtual Machine	x
Advanced Options These advanced options d	lo not usually need to be changed.	rsion: 8
Configuration Name and Location Storage Virtual Machine Version Guest Operating System CPUs Memory Network SCSI Controller Select a Disk Create a Disk Advanced Options Ready to Complete	Specify the advanced options for this virtual disk. These options do not normally need to be changed.	
Help	<u>≤</u> Back Next <u>></u> Cano	:el

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

Ø	Create New Virtual Machine		
Ready to Complete Click Finish to start a task	that will create the new virtual machine		Virtual Machine Version: 8
Configuration Name and Location Storage Virtual Machine Version Guest Operating System CPUS Memory Network SCSI Controller Select a Disk Create a Disk Create a Disk Advanced Options Ready to Complete	Settings for the new virtual machine Name: Host/Cluster: Datastore: Guest OS: CPUs: Memory: NICs: NIC 1 Network: NIC 1 Type: NIC 2 Network: NIC 2 Type: SCSI Controller: Create disk: Disk capacity: Disk provisioning: Datastore: Virtual Device Node: Disk mode: Iway: Creation of the virtual machine settings	Pfsense2 ESXI-Server.gnadeau.com datastore1 FreeBSD (64-bit) 1 512 MB 2 LAN E1000 WAN E1000 USI LogicParalle1 New virtual disk 8 GB Thick Provision Lazy Zeroed datastore1 SCSI (0:0) Persistent	n of the guest operating
Help		<u>≤</u> Back C	Continue Cancel

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

Ø	pfsense2 - Virtual M	achine Properties
Hardware Options Resources Show All Devices Hardware Memory (adding) CPUs (adding) Video card (adding) Video card (adding) New CD/DVD (adding) New Floppy (adding) New SCSI Controller (add New NIC (adding) New NIC (adding) New Hard Disk (adding)	pfsense2 - Virtual M Add Remove Summary 512 MB 1 Video card Restricted [datastore1] .sdd.sf Client Device LSI Logic Parallel LAN WAN Virtual Disk	achine Properties Device Status Connected Connect at power on Device Type Client Device Note: To connect this device, you must power on the virtual machine and then click the Connect CD/DVD button in the toolbar. Host Device Image: Client Device Node Image: Client Device Node
Help		Virtual Device Node IDE (1:0) IDE (1:0)

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

- Démarrez la machine virtuelle et partir la console de visualisation de ESXi. On entre alors en mode de visualisation de la machine virtuelle. Pour retourner la machine cliente physique, faites CTRL+ALT
- 2. Vous verrez apparaître cette fenêtre :



3. Appuyez sur "i" pour entrer en mode d'installation.



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





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





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



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

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

```
Welcome to pfSense 2.0.1-RELEASE ...
No core dumps found.
Creating symlinks.....done.
External config loader 1.0 is now starting... da0s1b
Launching the init system... done.
Initializing..... done.
Starting device Manager (devd)...done.
oading configuration.....done.
Network interface mismatch -- Running interface assignment option.
Valid interfaces are:
     00:0c:29:5c:b4:ee
                         (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.3
эмØ
ем1
     00:0c:29:5c:b4:f8
                         (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.3
Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.
Do you want to set up VLANs now [y¦n]? n
```

© Pierre-Luc Delisle et Guillaume Nadeau

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

емØ 00:0c:29:5c:b4:ee (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.3 ем1 (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.3 00:0c:29:5c:b4:f8 Do you want to set up VLANs first? If you are not going to use VLANs, or only for optional interfaces, you should say no here and use the webConfigurator to configure VLANs later, if required. Do you want to set up VLANs now [y:n]? n *NOTE* pfSense requires *AT LEAST* 1 assigned interface(s) to function. If you do not have *AT LEAST* 1 interfaces you CANNOT continue. If you do not have at least 1 *REAL* network interface card(s) or one interface with multiple ULANs then pfSense *WILL NOT* function correctly. If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection. Enter the WAN interface name or 'a' for auto-detection: em1 Do you want to set up VLANs first? If you are not going to use VLANs, or only for optional interfaces, you should say no here and use the webConfigurator to configure VLANs later, if required. Do you want to set up VLANs now [y:n]? n *NOTE* pfSense requires *AT LEAST* 1 assigned interface(s) to function. If you do not have *AT LEAST* 1 interfaces you CANNOT continue. If you do not have at least 1 *REAL* network interface card(s) or one interface with multiple VLANs then pfSense *WILL NOT* function correctly. If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces пом before hitting 'a' to initiate auto detection. Enter the WAN interface name or 'a' for auto-detection: ем1 Enter the LAN interface name or 'a' for auto-detection NOTE: this enables full Firewalling/NAT mode. (or nothing if finished): eм0

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

If you are not going to use VLANs, or only for optional interfaces, you should say no here and use the μebConfigurator to configure VLANs later, if required.
Do you want to set up VLANs now [y:n]? n
NOTE pfSense requires *AT LEAST* 1 assigned interface(s) to function. If you do not have *AT LEAST* 1 interfaces you CANNOT continue.
If you do not have at least 1 *REAL* network interface card(s) or one interface with multiple VLANs then pfSense *WILL NOT* function correctly.
If you do not know the names of your interfaces, you мay choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.
Enter the WAN interface name or 'a' for auto-detection: ем1
Enter the LAN interface name or 'a' for auto-detection NOTE: this enables full Firewalling/NAT mode. (or nothing if finished): ем0
Enter the Optional 1 interface name or 'a' for auto-detection (or nothing if finished):

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

If you do not have yOT IPOCTY t interfaces you CONNOT continue
II you do not have *HI LEHSI* 1 Interlaces you CHNNUI continue.
If you do not have at least 1 ≈REAL≈ network interface card(s)
or one interface with multiple VLANs then pfSense
WILL NOT function correctly.
If you do not know the names of your interfaces, you мay choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.
Enter the WAN interface name or 'a' for auto-detection: em1
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): ем0
Enter the Optional 1 interface name or 'a' for auto-detection (or nothing if finished):
The interfaces will be assigned as follows:
НАN -> ем1 LAN -> емθ
Do you want to proceed [y:n]?y

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

Please wait while the changes are sav DHCPD restarting webConfigurator.	ved to WAN Reloading filter
The IPv4 WAN address has been set to You can now access the webConfigurato browser:	dhcp or by opening the following URL in your web
http://dhcp/	
Press <enter> to continue. *** Welcome to pfSense 2.1-RELEASE-pf</enter>	Sense (amd64) on pfSense ***
WAN (wan) -> ем0 -> v4/ LAN (lan) -> ем1 -> v4:	'DHCP4: 192.168.216.97/24 : 10.0.1.1/24
0) Logout (SSH only) 1) Assign Interfaces 2) Set interface(s) IP address 3) Reset webConfigurator password 4) Reset to factory defaults 5) Reboot system 6) Halt system 7) Ping host	8) Shell 9) pfTop 10) Filter Logs 11) Restart webConfigurator 12) pfSense Developer Shell 13) Upgrade from console 14) Enable Secure Shell (sshd) 15) Restore recent configuration
Enter an option:	
7) Ping host	15) Restore recent configuration
7) Ping host Enter an option: 2	15) Restore recent configuration
7) Ping host Enter an option: 2 Available interfaces:	15) Restore recent configuration
7) Ping host Enter an option: 2 Available interfaces: 1 - WAN (em0 - dhcp, dhcp6) 2 - LAN (em1 - static)	15) Restore recent configuration
 7) Ping host Enter an option: 2 Available interfaces: 1 - WAN (em0 - dhcp, dhcp6) 2 - LAN (em1 - static) Enter the number of the interface your 	15) Restore recent configuration wish to configure: 2
 7) Ping host Enter an option: 2 Available interfaces: 1 - WAN (em0 - dhcp, dhcp6) 2 - LAN (em1 - static) Enter the number of the interface you Enter the new LAN IPv4 address. Press > 10.0.1.1 	15) Restore recent configuration wish to configure: 2 ss <enter> for none:</enter>
<pre>7) Ping host Enter an option: 2 Available interfaces: 1 - WAN (em0 - dhcp, dhcp6) 2 - LAN (em1 - static) Enter the number of the interface you Enter the new LAN IPv4 address. Press > 10.0.1.1 Subnet masks are entered as bit count e.g. 255.255.0.0 = 24 255.255.0.0 = 16 255.0.0.0 = 8</pre>	15) Restore recent configuration wish to configure: 2 as <enter> for none: as (as in CIDR notation) in pfSense.</enter>
<pre>7) Ping host Enter an option: 2 Available interfaces: 1 - WAN (em0 - dhcp, dhcp6) 2 - LAN (em1 - static) Enter the number of the interface you Enter the new LAN IPv4 address. Press > 10.0.1.1 Subnet masks are entered as bit count e.g. 255.255.0.0 = 24 255.255.0.0 = 16 255.0.0.0 = 8 Enter the new LAN IPv4 subnet bit cou > 24</pre>	15) Restore recent configuration wish to configure: 2 ss <enter> for none: ss (as in CIDR notation) in pfSense.</enter>

Enter the number of the interface you wish to configure: 2 Enter the new LAN IPv4 address. Press <ENTER> for none: > 10.0.1.1 Subnet masks are entered as bit counts (as in CIDR notation) in pfSense. e.g. 255.255.255.0 = 24 255.255.0.0 = 16 255.0.0.0 = 8 Enter the new LAN IPv4 subnet bit count: > 24 Enter the new LAN IPv4 gateway address. Press <ENTER> for none: > 10.0.1.1 Enter the new LAN IPv6 address. Press <ENTER> for none: > Do you want to enable the DHCP server on LAN? [yin] n Disabling DHCPD...Done! Disabling DHCPD...Done! Do you want to revert to HTTP as the webConfigurator protocol? (y/n)

Enter the new LAN IPv4 subnet bit count: > 24 Enter the new LAN IPv4 gateway address. Press <ENTER> for none: > 10.0.1.1 Enter the new LAN IPv6 address. Press <ENTER> for none: Do you want to enable the DHCP server on LAN? [yin] n Disabling DHCPD...Done! Disabling DHCPD...Done! Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y Please wait while the changes are saved to LAN... Reloading filter... DHCPD... restarting webConfigurator... The IPv4 LAN address has been set to 10.0.1.1/24 You can now access the webConfigurator by opening the following URL in your web browser: http://10.0.1.1/ Press <ENTER> to continue.

Configuration initiale de pfSense

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



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

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

Sense
This wizard will guide you through the initial configuration of pfSense. The wizard may be stopped at any time by clicking the logo image at the top of the screen.
Next

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

_	Sense
	On this screen you will set the general pfSense parameters.
General Information	
Hostname:	SpfSense EXAMPLE: myserver
Domain:	Sessilab.local EXAMPLE: mydomain.com
Primary DNS Server:	▶ 10.0.1.1
Secondary DNS Server:	▶ 10.0.1.1 ×
Override DNS:	✓ Allow DNS servers to be overridden by DHCP/PPP on WAN
	Next

4. Il faut ensuite configurer les paramètres de temps.

	Sense
	Please enter the time, date and time zone.
Time Server Information	
Time server hostname:	0.pfsense.pool.ntp.org Enter the hostname (FQDN) of the time server.
Timezone:	America/Montreal
	Next

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

	Sense
Or	this screen we will configure the Wide Area Network information.
Configure WAN Interface	
SelectedType:	DHCP V
General configuration	
MAC Address:	This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU:	Set the MTU of the WAN interface. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.
MSS:	If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.
Static IP Configuration	
IP Address:	
Gateway:	
DHCP client configuration	
DHCP Hostname:	N The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).
PPPoE configuration	
PPPoE Username:	

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

Sense
this screen we will configure the Local Area Network information.
N 10.0.1.1 Type dhcp if this interface uses DHCP to obtain its IP address.
24 🗸
Next

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

		Sen <mark>s</mark> e
_		
On this screen we will	set the admin password, w you wis	which is used to access the WebGUI and also SSH services if h to enable them.
Set Admin WebGUI Passwo	rd	
Admin Password:		
Admin Password AGAIN:	۰ ۰۰۰۰۰۰	
		Next

8. Après avoir été configuré, pfSense redémarrera.

Sense	
Click 'Reload' to reload pfSense with new changes.	
Reload	

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

Status: Dad	haand				2
	nboard				
System Informat	tion 🛛 🖂 🖂	Interface	25		
Name			1	↑ 1000baseT <full-duplex></full-duplex>	
Version	2.1-RELEASE (amd64) built on Wed Sep 11 18:17:48 EDT 2013 FreeBSD 8.3-RELEASE-p11		CP)	192.168.216.97 1000baseT <full-duplex> 10.0.1.1</full-duplex>	
	Unable to check for updates.				
Platform	pfSense				
СРИ Туре	Intel(R) Core(TM)2 Quad CPU Q9550 @ 2.83GHz				
Uptime	00 Hour 13 Minutes 11 Seconds				
Current date/time	Mon Mar 31 6:14:44 EDT 2014				
DNS server (s)	127.0.0.1 10.0.1.1				
Last config change	Mon Mar 31 6:14:21 EDT 2014				
State table size	0% (111/48000) Show states				
MBUF Usage	4% (646/16640)				
Load average	0.51, 0.32, 0.21				
CPU usage	100%				
Memory usage	39% of 490 MB				
SWAP usage	0% of 2 MB				
Disk usage	6% of 7.8G				

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

	p:// 10.0.1.1 /index.pl	ıp		5 - Q	🖲 pfSense.l	ocaldomain - Statu	×
× Find: vmware	Pr	evious Next 📝	Options 🔻				
** Sense	 System Advanced Cert Manager Firmware 	 Interfaces shib pard 	► Firewall	 Services 	► VPN	► Status	▶ Diagr
	General Setup High Avail. Sync Logout	ation				erfaces	
	Packages Routing Setup Wizard User Manager	1-RELEA built on Wea eeBSD 8.3	Idomain SE (amd64) J Sep 11 18:17:4 I-RELEASE-p11 the latest version	8 EDT 2013		<u>WAN</u> (DHCP) LAN	 ↑ 1000 192.1€ ↑ 1000 10.0.1
	Platform CPU Type Uptime	pfSense Intel(R) Corr 2.83GHz 00 Hour 24	e(TM)2 Quad CP	U Q9550 @			

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

System: Pac	kage Manage	r		3	
Available Packages	Installed Packages				
Name	Category	Status	Description		
Asterisk	Services	Beta 1.8 pkg v0.3.1 platform: 2.0	Asterisk is an open source framework for building communications applications. Asterisk turns an ordinary computer into a communications server.	G	
			Package info		
anyterm	Diagnostics	BETA 0.5 platform: 1.2.3	Ajar, Interactive Shell - Have you ever wanted SSH or tenter access to your system from an internet deater - from behind a struct firewall, from an internet cafe, or even from a mobile phone? Anyterm is a combination of a web page and a process that runs on your web server that provides this access. WARKING! We suggest using Stumel in combination with this package!	æ	
			Package info		
Apache with mod_security-dev	Network Management	ALPHA 2.4.6 pkg v0.3 platform: 2.0	HodSecurity is a web application firewall that can work either embedded or as a reverse proxy. It provides protection from a range of attacks against web applications and allows for HTTP traffic monotoning, logoing and real-time enalysis. In addition this package allows URI. Forwarding which can be convenient for hosting multiple websites behind preferes using 112 address. Backup your location config before updating form 0.2.x to 0.3 package version.	6	
			Package info		
Avahi	Network Management	ALPHA 0.6.29 pkg v1.02 platform: 1.2.3	Availi is a system which facilitates service discovery on a local network. This means but you can play you laytop of compater into a network and the priorit to a field field being abare. This kind of technology is already found in Apple MacGS (Uranded Rendezvos, Bonjour and sometimes Zerocoff) and is very convenient. Avail is mainly based on Lemant Poettering's flexinds imDAS implementation for Linux which has been discontinued in loward Avail.	GR CONTRACTOR	
			Package info		
AutoConfigBackup	Services	Stable 1.21 platform: 1.2	Automatically backs up your pfSense configuration. All contents are encrypted on the server. Requires pfSense Premium Support Portal Subscription from https://portal.pfsense.org	.	
arping	Services	Stable	Prockage mild Broadcasts a who-has ARP packet on the network and prints answers.		
		2.09.1 v1.1			

© Pierre-Luc Delisie et Guillaume Nadeau

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



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

Création d'une règle de blocage dans pfSense.

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

- 1. pfSense est pourvue d'une interface graphique sur le Web. Pour y accéder, **inscrire l'adresse** de la passerelle par défaut dans votre **navigateur web**.
- 2. Entrer le **nom d'utilisateu**r de l'administrateur et le **mot de passe** de ce compte.

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

← → 🖲 ht	tp:// 10.0.1.1 /inc	lex.php) + 0	🕽 🐨 pfS	Sense.localdo	omain - Statu.	×				
Sense	 System 	 Interfaces 	 Firewall 	 Services 	•	VPN	 Status 	Diagnostic	s 🕨	Help	🐉 pfSense.	localdomain
			Aliases									
	Status: Dashboard											
			Traffic Shaper		_							
	System Information		Virtual IPs	E		Interface	<u>s</u>				$ \times$	
Name pfSense.loc Version 2.1-RELEA built on We FreeBSD 8.3		aldomain	🖾 <u>WAN</u>			1000baseT <full-duplex></full-duplex>						
		SE (amd64)			(DHC	CP)	192.168.216.98					
		FreeBSD 8.3	:d Sep 11 18:17:48 EDT 2013 3-RELEASE-p11			LAN 1000			.000baseT <full-duplex></full-duplex>			

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



5. Pour créer une nouvelle règle, appuyez sur l'icône



dans la section **LAN**.

- 6. Le menu de création d'une règle s'affichera. Pour bloquer une adresse IP, il faut :
 - Bloquer la règle : **Action -> Block**
 - Interface : LAN
 - TCP/IP version : IPv4
 - Source
 - Type : Single Host or Alias
 - Address : L'adresse IP du site à bloquer
 - Description : Écrire le nom de la règle.

 System Interfact 	es 🔸 Firewall 🕨 Services 🕨 VPN 🔸 Status 🕨 Diagnostics 🕨 Help 岸 pfSense	e.locald
Firewall: Rules: E	dit	
Edit Firewall rule		
Action	Block Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	Disable this rule Set this option to disable this rule without removing it from the list.	
Interface	LAN V Choose on which interface packets must come in to match this rule.	
TCP/IP Version	$IPv4$ \checkmark Select the Internet Protocol version this rule applies to	
Protocol	TCP V Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.	
Source	not Use this option to invert the sense of the match. Type: Network Address: 10.0.1.1 / 24 ✓ Advanced - Show source port range	
Destination	□ not Use this option to invert the sense of the match. Type: Single host or alias ✓ Address: 66.131.56.103 / 31 ✓	
Destination port range	from: any v to: any v Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the ' <i>to</i> ' field empty if you only want to filter a single port	
Log	Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).	
Description		

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

← → 🖲 htt	tp://10.0.1.	.1/fire	wall_rules.	php?if=lan) ب (C 🐨	pfSense.localc	domain - Fii	rew × 🖻 N	/lysearchdial Sear	rch	
Sense /	► System	stem	► Int	erfaces 🕨 🕨	Firewall	Services	;)	VPN	 Statu 	s 🕨 Diag	nostics 🕨 H	lelp 🚽 📬 pfSer	se.localdomain
	Firew	yall: The You	Rules firewall r must app	ule configurati ly the changes	on has be in order	een changed. for them to take	effect.				Аррі	iy changes	
and the second		ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	07	
	۵		*	*	*	LAN Address	80	*	*		Anti-Lockout Rule		
			IPv4 TCP	10.0.1.1/24	*	66.131.56.103	*	*	none		Block gnadeau's personal NAS		
			IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule		
			IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule		
	D pass	s s (disat	bled)		🔀 bl	ock ock (disabled)			C reject	abled)		log log (disabled)	
	Hint:	Rules block	are evalua rules, you'l	ted on a first-ma l have to pay att	tch basis (ention to t	(i.e. the action of th	ne first ru ything th	le to match a pa at isn't explicitly	acket will be / passed is bl	executed). This ocked by defau	means that if you u lt.	ise	
				pfSense is	s © 2004	- 2013 by <mark>Elect</mark> ri	c Sheep	Fencing LLC.	All Rights R	eserved. [<mark>view</mark>	/ license]		

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

クー C 💿 pfSense.localdomain - Firewall: ... 🥔 This page can't be displayed 🗴

This page can't be displayed

- Make sure the web address https://gnadeau.dlinkddns.com:8080 is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

Fix connection problems

← → Ø https://gnadeau.dlinkddns.com:8080/



_ 8 ×

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



Création d'une connexion VPN

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



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

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

Plusieurs types de clefs de cryptages peuvent être utilisées, tout comme de nombreux protocoles d'authentification sont utilisés au sein de la technologie VPN. PPTP, le protocole le plus utilisé puisqu'implanté depuis fort longtemps dans les solutions Microsoft, utilise la clef de cryptage la plus faible de l'industrie, soit 128-bit. Cela en fait la solution la moins sécuritaire du marché, alors que LT2P over IPSec et OpenVPN utilisent des clefs de cryptage AES 256-bit. PPTP utilise une authentification encapsulée par MS-CHAPv2. Toutefois, des *exploits* on été découvert pour décapsuler cette authentification et des trames PPTP ont été décryptées en moins de deux jours. Microsoft recommande donc lui-même d'utiliser LT2P over IPSec ou OpenVPN comme solution VPN³.

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

Nous avons tout de même configuré le VPN Passthrough.

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

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

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



© Pierre-Luc Delisle et Guillaume Nadeau

9 ==

 $\mathbf{\Sigma}$

h

4/2/2014

- 😼 🖬 🕼

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

🗅 Setup 🛛 🗙							_ 0 ×
← → C 🗋 192.168.2.1/A	dminRouting.htm						ය 1
A Division of Cis	(SYS [®] cco Systems, Inc.				Firm	ware Version: 2.39.2e	
				Wireless-G	VPN Router	WRV54G	
Set	Setup Basic Setup	Wireless DDNS	Security Access Restrictions	Applications & Gaming Advanced Routing	Administration Hot Spot	Status	
Advanc	ced Routing	ing Mode:	Router •		The router can b between two did	be setup to route fferent	
Dynar	mic Routing RIP: Receiv	e RIP versions:	● Enabled ○ Disabled Both RIP v1 and v2 ▼	ı	appropriate routi your network an required settings unsure of these contact your net	ing mode for nd enter the s. If you are settings, twork	
Sta	Transm atic Routing	it RIP versions:	RIPv2 - Broadcast ▼		administrator.		
	Select LAN IP	Number: Address:	1 ▼ Delete Th 0 . 0 . 0	nis Entry			
	Subnet	Mask : Gateway :					
	metric : Interfac	ce :	0 LAN & Wireless ▼				
			Show Routing Table				
			Save Settings	<u>Cancel Changes</u>		utilitutilitu.e	
		I.				▲ । 3	4:15 PM 4/2/2014

🗅 Security 🛛 🗙 📃							۰	x
← → C 🗋 192.168.2.1/SecurityVPNAuto	o.htm						숬	≡
A Division of Cisco Systems, Inc.				Fim	ware Version: 2.39.2e			
			Wireless G	VPN Router	WRV54G			
Security		A	Applications 9					
occurry	Setup Wireless	Security Restrictions	Gaming	Administration	Status			
	Firewall VPN			_				
VPN Passthrough	IDC Decetherush	Enabled Disable	4	IPSec Passthro	ugh: Internet			
	PPTP Passthrough:	Enabled Disabled Disabled	d	Protocol Securi suite of protoco	ty (IPSec) is a lis used to			
	L2TP Passthrough:	Enabled Disable	d	implement secu packets at the l	re exchange of P layer. To allow			
VPN Tunnel				IPSec Passthro Enabled button.	ugh, click the			
	Select Tunnel Entry:	Tunnel 1 (PLD to GN)	•	PPTP Pass Thro	ough: Point-to-			
	VPN Tunnel:	Enabled Disabled		Point Tunneling Passthrough is	Protocol the method used			
	Tunnel Name :	PLD to GN		to enable VPN s Windows NT 4.	sessions to a 0 or 2000			
Local Secure Group		IP Addr		server. To allow Passthrough, c	v PPTP lick the Enabled			
	IP Address :	192.168.2.0)	button.				
	Mask:	255.255.255.255		L2TP Pass Thro Tunneling Proto	ough: Layering 2 col Passthrough			
				is an extension Point Tunneling	of the Point-to- Protocol (PPTP)			
Remote Secure Group		IP Addr. V		of a virtual priv	ate network			
	Mask :	255.255.255.255)	allow L2TP Pas	sthrough, click			
				The V/DN Doute	r creates a			
Remote Secure Gateway		IP Addr. 🔻		tunnel or chann endpoints, so th	el between two			
	IP Address :	10 . 0 . 254 . 1		information bety endpoints is se	ween these cure.			
				To establish this the tunnel you	s tunnel, select wish to create in			
	Encryption :	DES V		the Select Tunn down box. Click	el Entry drop- k Enabled to			
	Authentication :	SHA1 V		enable the tunn tunnel is enable	el. Once the d, enter the			
Key Management	Key Exchange Method :	Auto(IKE) V		name of the tun Name field.	nel in the Tunnel			
	PFS :	Enabled Disabled		More				
	Pre-Shared Key:	hello						
	RSA Signature :	Please enter RSA!						
	Key Lifetime :	28000						
Status		Disconnect						
	Advanced VPN Tunnel	Setup						
					CISCO SYSTEMS			
		Save Settings	Cancel Changes		«مىئاللانىمىئاللەر»			
II 📙 🔎 🚞 👩 🛛	8				▲ []]	97 (h	4:16 PI	М
					u 🥥	- · ·	4/2/20	14

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

Conclusion

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

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

Vous aurez noté également que nous parlons fréquemment de l'aspect sécurité dans ce document. La sécurité est également un autre facteur qui est laissé de côté dans ce cours. Selon le très populaire site *ComputerWorld*, les aptitudes en gestion de la sécurité de réseaux informatiques (*Network Security Management*) figurent parmi les quinze aptitudes les plus en vogue dans l'industrie⁴. Anil Chakravarthy, vice-président exécutif du groupe de la sécurité de l'information chez Symantec affiche :

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

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

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

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

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

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

ievre-Luc Clisle

Pierre-Luc Delisle

Luc Delisle Willame Madea

Guillaume Nadeau

Notes	

