

## REMERCIEMENT

Nous tenons à exprimer toute notre reconnaissance et gratitude à l'ensemble de l'équipe pédagogique d'IT-Learning Academy pour sa disponibilité, tout particulièrement Mr ALLALI Hakim pour le temps important qui nous a consacré durant toute l'année.

Nous aimerons par ailleurs souligner la contribution importante de nos formateurs, les responsables de la formation professionnelle et le personnel de la FST Settat qui n'ont pas hésité de consacrer un grand part de leurs précieux temps afin de réussir notre formation et développer notre niveau et nos compétences.

Nous remercions aussi :

- notre encadrant interne Mr. SDOUR Mohamed et Mr KARBOUBI Mustapha pour leur conseils et disponibilité ainsi que leur remarques pertinentes et suggestions constructives.

- Les membres du jury qui évaluent notre travail.






- L'ensemble des étudiants de la FST Settat.

- Tous nos amis, et plus précisément Mr CHARMOUH Hicham et Mr BASSLAM Mohamed.

Merci d'accepter notre modeste travail et d'y voir la réelle expression de gratitude envers vous

## DEDICACE

Nous dédions ce travail à :

-  Nos encadrants
-  Nos formateurs
-  Nos familles
-  Nos amis
-  Les étudiants de la FST Settati

Et à tous ceux qui nous ont apporté de l'aide et du soutien.

## Table des matières

I.	Partie I .....	
1.	Introduction .....	
2.	Présentation du projet .....	
3.	Lieu et cadre de stage .....	
II.	Partie II .....	
1.	Etude et analyse de l'existant : infrastructure physique et logique .....	
1.1.	Cahier des charges .....	
1.2.	Planning de stage .....	
2.	Les problématiques soulevées .....	
3.	Les solutions proposées .....	
3.1.	Qu'est ce qu'un pare-feu ? .....	
3.2.	Comment fonctionne-t-il ? .....	
3.3.	Mise en place de la maquette de test .....	
3.4.	Présentation de l'infrastructure proposée .....	
3.5.	Test de la solution et anomalies soulevées .....	

3.6. Solution envisagée .....	
4. Choix du pare-feu .....	
4.1. Comparatifs des pare-feu : .....	
4.2. Solution choisie .....	
III. Partie III .....	
1. Prés requis d'installation .....	
2. Installation de PfSense .....	
3. Configuration du pare-feu .....	
3.1. Configuration de l'interface LAN .....	
3.2. Changement du mode graphique .....	
3.3. Filtrage des ports .....	
4. Mise en place du portail captif .....	
4.1. Qu'est ce qu'un portail captif .....	
4.2. Fonction d'un portail captif .....	
4.3. Configuration du portail captif .....	
4.4. Configuration du service de Portail Captif .....	
4.5. Personnalisation d'une Page HTML pour authentification .....	
4.6. Configuration de la page d'authentification sur le pare-feu .....	

5.	Configuration du DNS forwarder .....	
6.	Sauvegarde de la configuration du pare-feu .....	
7.	Installation du serveur radius .....	
8.	Test du fonctionnement du portail captif .....	
9.	Faits marquants .....	
9.1.	Problème avec le service NTP .....	
9.2.	Rapidité des connexions.....	44
9.3.	Mise en place du portail captif .....	
10.	Conclusion .....	
11.	Annexe .....	

# I. Partie I

## 1. Introduction

Dans le cadre de notre formation continue au sein de la FST Settât pour la préparation du Diplôme Universitaire «**I**ngénierie **S**ystèmes **R**éseaux et **S**écurité» on a réussi à la mise en place d'un firewall au sein de notre établissement IT-Learning Académie suite à un stage de deux mois.

Ce travail a été une opportunité qui nous a permis d'exercer et d'appliquer les acquis soulevés de notre formation et de nous donner une approche pratique sur le domaine professionnel.

Notre projet vise à répondre aux besoins informatiques et à remédier aux problèmes d'exploitation réseau connus par notre établissement afin de garantir la sécurité et la fiabilité du système et maintenir sa qualité, sa fiabilité et sa disponibilité.

La 1<sup>ère</sup> partie de notre projet présente un aperçu sur IT-Learning Academy et une étude préalable de son existant afin de détecter les défaillances qui va nous permettre de définir les problématiques et les besoins.

Sur la 2<sup>ème</sup> partie, on a présenté une solution permettant de remédier au besoin soulevé sur la partie précédente.

La dernière partie présente et décrit la mise en place de la solution proposée.

## 2. Présentation du projet

Notre projet vise à la mise en place d'un firewall sur lequel tout le trafic réseau de notre établissement sera transité. C'est donc un SPOF « single point of failure ou point individuel de défaillance » de notre système d'information.

Notre projet vise à répondre aux besoins de limitation du trafic nuisible généré par des machines infectés ou des programmes malveillants afin de garantir la disponibilité et la fiabilité de notre réseau et répondre aux besoins des étudiants.

### **3. Lieu et cadre de stage**

Ce stage s'est déroulé dans les locaux d'IT-Learning Academy pour le compte du service informatique, durant une période de deux mois.

L'ensemble de l'équipe informatique nous a présenté toutes les détails et les consignes nécessaires permettant de réussir notre mission, atteindre nos objectif et bénéficier de toutes les jours et heurs de notre présences.

## II. Partie II

### ***1. Etude et analyse de l'existant : infrastructure physique et logi***

Avant la proposition des solutions, la planification des dates et les charges des travaux à réaliser, il était important d'analyser et de comprendre l'infrastructure existante et les outils de travail actuel.

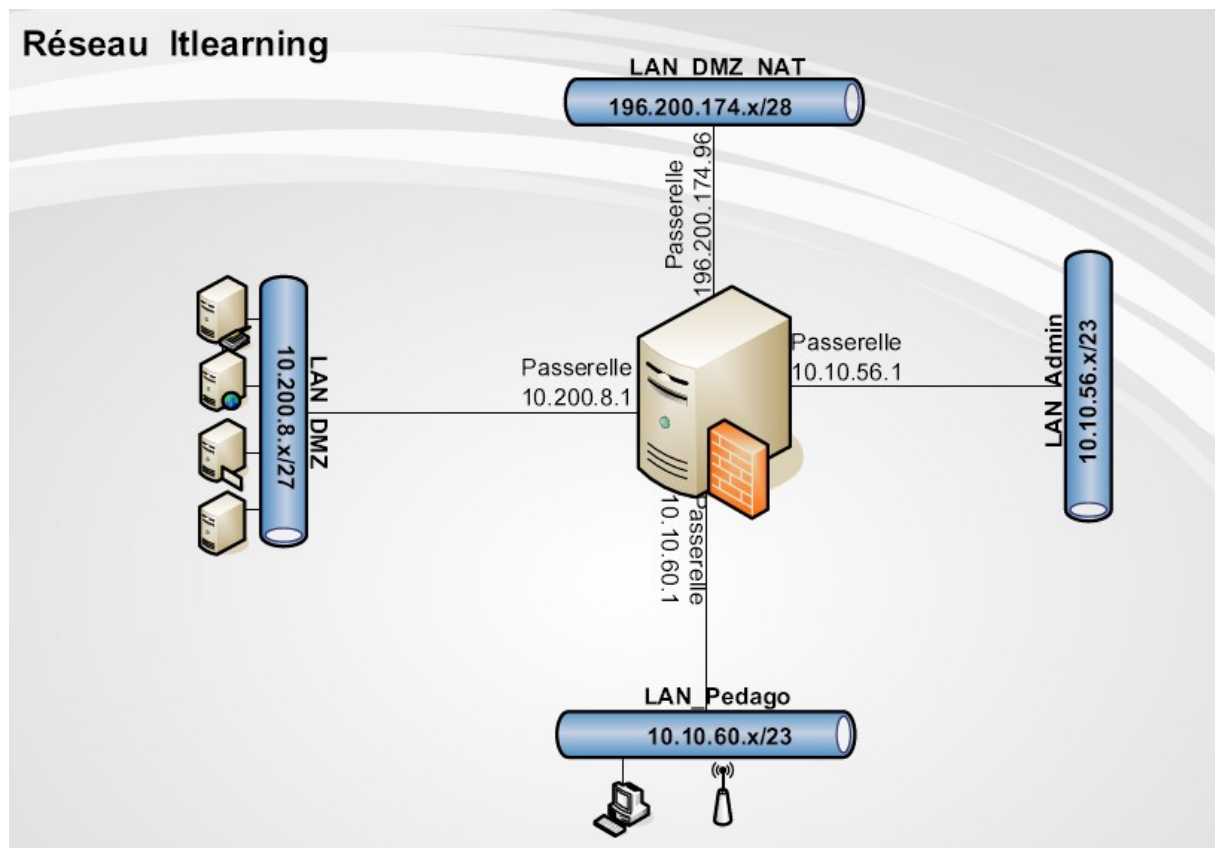
#### **1.1. Cahier des charges**

Pour des mesures de sécurité et de confidentialité et selon les recommandations de notre encadrant, on va présenter seulement l'infrastructure réseau de l'établissement sans entrer dans les détails (Voir le schéma ci-dessous).

Les problématiques soulevées seront décrites sur les paragraphes qui suivent.



## Réseau Itlearning



## 1.2. Planning du stage

Afin de détecter les problématiques et proposer les solutions utiles permettant ses résolutions, on a consommés les charges mentionnées sur le diagramme ci-après :

Diagramme de Gant

ID	Nom de tâche	Début	Terminer	Durée
1	L'analyse et l'étude de l'existant.	20/10/2009	26/10/2009	1s
2	Recherche des solutions	27/10/2009	26/11/2009	4,6s
3	La réalisation de ces solutions	27/11/2009	07/12/2009	1,4s
4	Mise en place de Firewall	08/12/2009	18/12/2009	1,8s
5	Supervision et dépannage	21/12/2009	06/01/2010	2,6s

## 2. Les problématiques soulevées

- Manque de plusieurs programmes et utilitaires sur les stations de travail dédiés aux étudiants

↑ Le contrôle de chaque station et des programmes manquants demande un temps très important.

- Existence des postes de travail sont antivirus

↑ Ces postes sont la source de plusieurs vers et virus qui se propagent sur le réseau et génèrent des trafics qui occupent la bande passante et surcharge le réseau.

- Aucune authentification ne se fait durant l'accès aux ressources et aux données.

↑ Il est impossible de savoir quel utilisateur connecté à quel poste de travail et accède à quelle ressource réseau.

- Installations de nouvelles salles informatiques dotées des dizaines de postes de travail.

↑ Beaucoup de trafic inutile circule sur le réseau avec l'ajout de ces salles, surtout le trafic généré par les machines virtuelles ce qui explique la saturation du firewall principale de l'établissement (Voir le schéma : Infrastructure réseau) et dégrade la bande passante du réseau.

## 3. Les solutions proposées

- Déploiement d'une image contenant toutes les applications nécessaires.
- Déploiement de l'antivirus Trend Micro sur l'ensemble des postes de travail.
- Mise en place d'un pare-feu
- Mise en place d'un portail captif permettant l'authentification via un serveur RADIUS.

↑ Le détail des deux dernières solutions est détaillé sur les paragraphes qui suivent.

### 3.1. Qu'est ce qu'un parefeu ?

Un pare-feu (en anglais, "firewall") est une sorte de garde-barrière, qui contrôle le trafic des données entre un réseau local et un réseau externe (Ex : Entre le réseau de l'établissement et Internet).

La tâche principale d'un pare-feu consiste à filtrer les données entrantes indésirables, ce qui permet de protéger le réseau interne contre les intrusions.

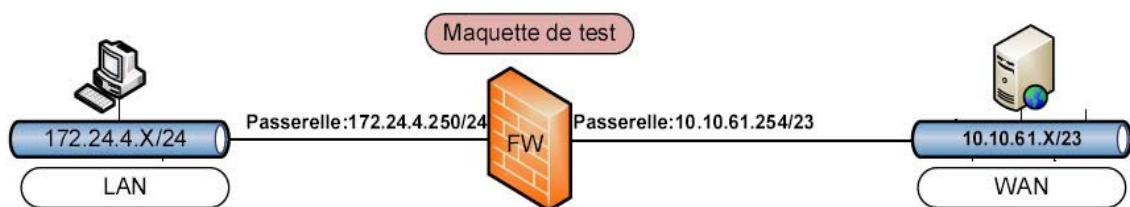
Les pare-feu sont soit intégrés au matériel (hardware firewall) soit disponibles sous forme logicielle (software firewall).

### 3.2. Comment fonctionnetil ?

Un pare-feu peut contrôler de plusieurs manières le trafic des données :

- Les filtres: les paquets de données passent par une série de filtres qui ne laissent passer que les paquets répondant à certains critères et rejettent celles qui ne sont pas conforme aux règles appliquées.
- Le serveur Proxy: le pare-feu reprend les fonctions d'un serveur Proxy (un serveur regroupant les requêtes entre le PC et un serveur Web). Si le PC demande des fichiers sur l'Internet, la requête arrive jusqu'au pare-feu, qui la transmet à l'Internet. Le pare-feu retransmet ensuite le document souhaité au PC. Dès lors, pour les ordinateurs connectés à l'Internet, il semble que la requête émane directement du pare-feu et non du PC.
- L'architecture State full Inspection : cette technique d'analyse des flux permet au pare-feu d'assurer le suivi du début de chaque connexion. Si des paquets de données non sollicités (correspondant aux règles du pare-feu) ne peuvent pas être rattachés au début d'une connexion enregistrée précédemment, le pare-feu les rejette.

### 3.3. Mise en place de la maquette de test



Comme indiqué ci-dessus, la maquette de test est constituée de :

- Une machine simulant Internet via un serveur http IIS.
- Une machine simulant un poste du réseau interne de l'établissement.
- Une troisième machine simulant le pare-feu

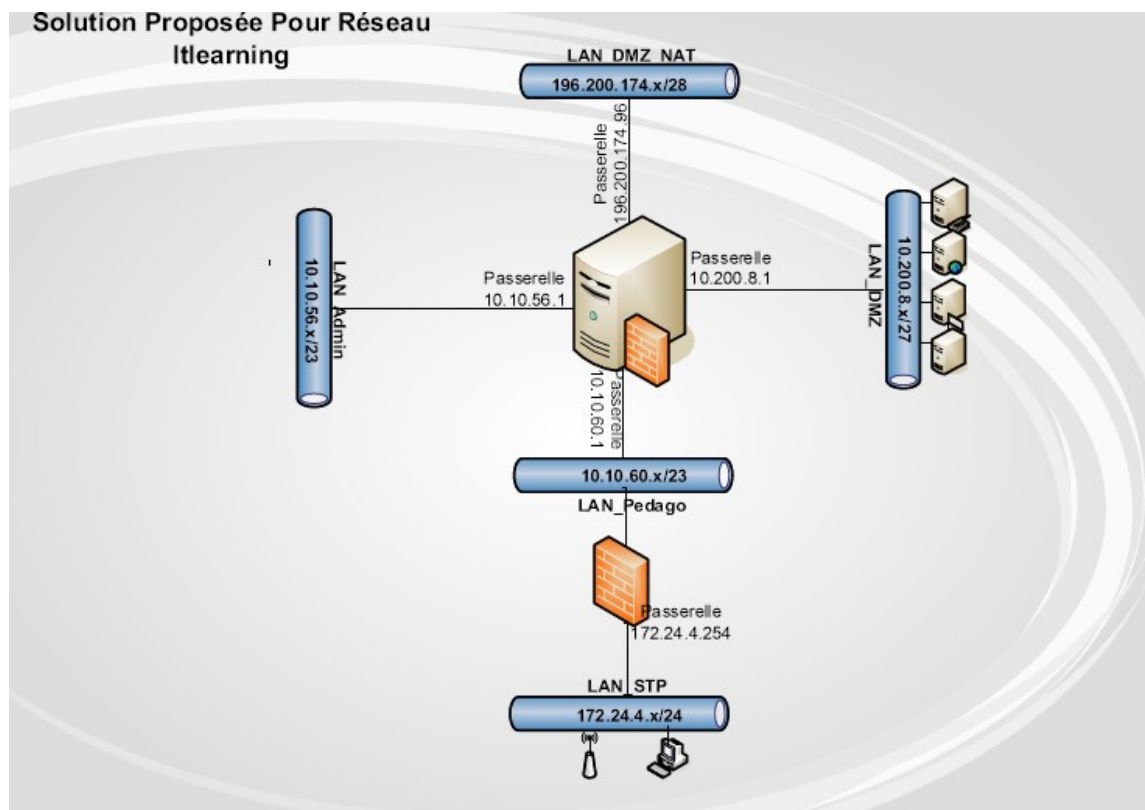
Le pare-feu est configuré avec deux interfaces :

- Interface LAN (Avec l'adresse : 172.24.4.254 /24)
- Interface WAN (Avec l'adresse : 10.10.61.254/23)

Pour vérifier la fiabilité de notre maquette, on a sniffé le réseau sur lequel le pare-feu est installé à l'aide de ETHEREAL qui est d'ailleurs extrêmement bien fait, simple d'utilisation et gratuit. On rappelle qu'ETHEREAL capte le trafic qui passe sur ce réseau pendant un certain laps de temps (le plus long possible dans notre cas pour avoir un meilleur aperçu).

ETHEREAL affiche alors le type, le nombre et le pourcentage des trames qui passent sur le réseau. Ceci nous permet de savoir quels sont les flux utilisés, de manière à interdire les autres inutiles...

### 3.4. Présentation de l'infrastructure proposée

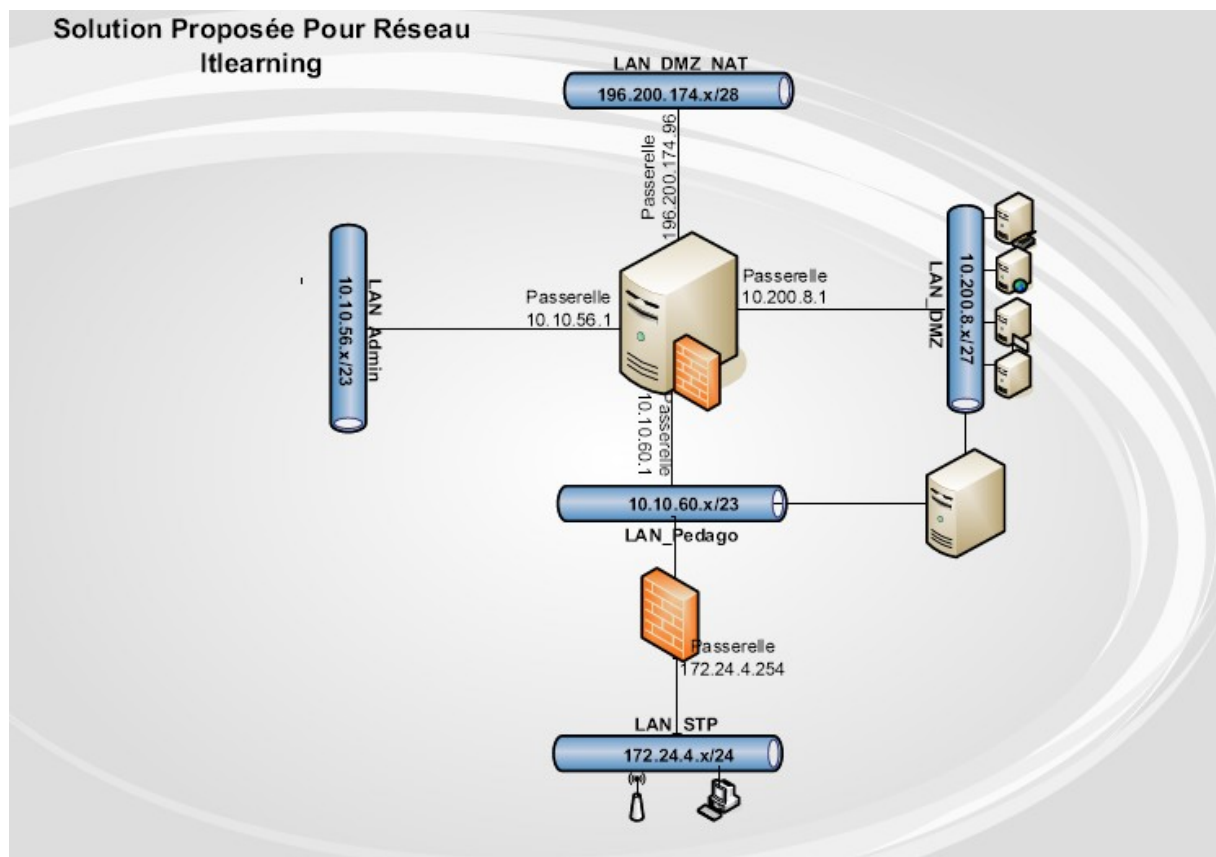


### 3.5. Test de la solution et anomalies soulevées

La segmentation du réseau en trois provoque un petit problème au niveau de la résolution d'adresses ARP.

En effet, une machine du réseau interne pour récupérer son adresse IP ou bien pour s'authentifier sur le réseau, Une requête ARP ou bien les informations d'authentification sont envoyées, le trafic passe par le nouveau pare-feu (Passerelle) et transmis au VLAN Pédago. Ce dernier achemine le trafic vers le pare-feu principal qui lui redirige vers le VLAN DMZ (et vice-versa).

### 3.6. Solution envisagée



Pour remédier à cette anomalie, on a ajouté un contrôleur de domaine dans la partie VLAN Pédago (Voir le schéma ci-dessus), et pour assurer la réplique entre les contrôleurs des domaines, on a ajouté une 2<sup>ème</sup> interface vers le VLAN DMZ.

## 4. Choix du parefeu

### 4.1. Comparatifs des parefeu :

Afin de répondre à notre besoin (Assurer : l'optimisation, la sécurité & l'authentification) on a procédé à une étude des différents services et fonctionnalités offerts par différentes distributions open source (Voir ci-dessous).

#### Smoothwall Express

La distribution Smoothwall est Open Source et distribuée sous licence GPL. C'est un système d'exploitation basé sur RedHat Linux (devenu plus tard Fedora Core Project).

Les fonctionnalités assurées par défaut par Smoothwall Express sont les suivantes :

- Possibilité d'administration via une interface web.
- Consultation de l'état de la machine sur laquelle est installé le pare-feu (état de la mémoire et les disques durs).
- supervision du trafic réseau en temps réel sur les différentes cartes.
- services de proxy web, SIP, POP3, IM.
- service DHCP.
- service DNS (statique et dynamique).
- service de temps NTP.
- accès distant via SSH.
- système de détection d'intrusions.
- VPN IPSec.
- filtrage (par état).
- NAT.
- priorité de trafic et QOS.
- consultation de différents types de logs.
- possibilités de maintenance (mise à jour du système ou de pilotes, backup, add on...).

Plusieurs autres fonctionnalités peuvent être ajoutées via des add-ons.

Il est à noter que le filtrage de Smoothwall Express est basé sur iptables, le module de filtrage du noyau linux.

#### IPCop

IPCop est à l'origine un fork de Smoothwall Express. Ceci signifie qu'IPCop est basé sur linux Red hat. Il fonctionne sur du matériel non propriétaire.

IPCop partage avec Smoothwall plusieurs fonctionnalités et s'en démarque par d'autres. Par exemple, IPCop ne propose pas de proxy IM ou de proxy POP3. Il supporte par contre le "VLAN trunking" défini par la RFC 802.1Q, le protocole Telnet et le protocole d'encapsulation de niveau 2 L2TP. La supervision de trafic en temps réel n'est pas possible sur IPCop.

## Vyatta Community Edition

La solution pare-feu de la société Vyatta existe en deux exemplaires. Le premier est payant, le second est libre. On note que la version commerciale est plus souvent maintenue et mise à jour que la solution libre (environ une mise à jour tous les six mois). Le produit commercialisé est en outre toujours stable ce qui n'est pas forcément le cas pour la version libre, dénommée Vyatta Community Edition et dont la dernière version est la version 5.0 issue en Mars 2009.

Au sujet des fonctionnalités, on peut dire que Vyatta Community Edition se distingue des autres produits libres qu'on vient d'énumérer. En effet et comme cité, Vyatta Community Edition offre des services de haute disponibilité, beaucoup plus de services de routage, possibilités de VPN SSL... Bref, toutes les fonctionnalités qu'on trouve dans les produits Cisco (ou presque) sont présentes dans la solution Vyatta. A noter la présence d'un IPS (système de prévention d'intrusions) au lieu d'un simple IDS (système de détection d'intrusions).

## m0n0wall

M0n0wall est un système d'exploitation pare-feu libre basée sur le noyau FreeBSD et non pas linux. La particularité de m0n0wall est qu'il est le premier système d'exploitation de type UNIX démarrant à partir d'une séquence de boot basée exclusivement sur des fichiers d'extension .php au lieu des scripts shell classiques. M0n0wall est aussi le premier pare-feu à stocker l'intégralité de sa configuration dans un unique fichier (de type XML).

M0n0wall est destiné à être embarqué sur une appliance. Il existe aussi sous forme de live-CD. Les possibilités d'exploitations sont ainsi réduites afin de pouvoir alléger le système pour qu'il soit facilement portable sur du matériel... On ne trouve par exemple pas d'IDS ou d'IPS qui demandent des ressources mémoires plutôt élevées. On ne trouve pas aussi de serveur FTP, proxy, serveur de temps, analyseur de log...

D'autres fonctionnalités qu'on n'est pas habitué à trouver dans les autres pare-feu sont par contre présentes dans m0n0wall. On en cite surtout l'option portail captif et le service SNMP.

## PFSense

PFSense est le descendant de m0n0wall. C'est donc un système d'exploitation pare-feu basé sur le noyau FreeBSD et sur le module de filtrage "ipfw". La configuration de PFSense est stockée dans un seul fichier XML à l'instar de m0n0wall. La séquence de démarrage est aussi fondée sur des fichiers php.

Néanmoins, PFSense n'est pas vraiment orienté à l'embarqué. Ceci explique la panoplie de fonctionnalités offertes par cette distribution. Par rapport à m0n0wall (son ancêtre), PFSense offre en plus les possibilités suivantes :

- Common Address Redundancy Protocol (CARP) et PFSync (synchronisation entre machines PFSense)
- Possibilités d'alias étendue (alias pour interfaces réseau, utilisateurs...).
- Configuration XML de synchronisation entre maître et hôte de backup permettant de faire un point unique d'administration pour un cluster pare-feu. La synchronisation est assurée via XML-RPC.
- Equilibrage de charge (load balancing) pour les trafics entrant et sortant.
- Graphes montrant les statuts des files d'attente.
- Support du protocole SSH pour l'accès distant.
- Support de multiples interfaces réseaux WAN.
- Serveur PPPoE.
- ...



## Récapitulation

Nous présentons ci-dessous un tableau comparatif des différentes fonctionnalités des solutions pare-feu libre qu'on a vint de présenter.

		Smoothwall Express	Vyatta Community	IPCop	PfSense	M0n0wall
Services	Proxy Web	x	x	x	x	—
	DHCP	x	x	x	x	x
	DNS statique	x	x	x	x	x
	DNS dynamique	x	—	x	x	x
	DNS forward	—	x	—	x	x
	Telnet	—	x	x	—	—
	SSH	x	x	x	x	—
	NTP	x	—	x	x	x
	taches programmées	—	—	x	x	x
	WebGUI via HTTP	x	—	x	x	x
	WebGUI via HTTPS	x	x	x	x	x



<b>Authentication</b>	Portail Captif	-	-	-	x	x
<b>VPN</b>	IPSec	x	x	x	x	x
	PPTP	x	x	-	x	x
	L2TP	-	x	-	x	-
	clés RSA	x	x	x	x	x
	DES	x	x	x	x	x
	3DES	x	x	x	x	x
	AES	-	x	x	x	x
<b>Haute disponibilité</b>	Load Balance	-	x	-	x	-
	Multi-WAN	-	x	-	x	-
	Capacité de Failover	-	x	-	x	-
<b>QOS</b>	Priorité selon type de trafic	x	x	x	x	x
	Lissage de trafic (limitation)	x	x	x	x	x
<b>Outils connectivité (WebGUI)</b>	Traceroute	x	x	-	x	x
	Ping	x	x	x	x	x
	Who is	x	-	-	-	-
<b>Routage</b>	NAT (dynamique)	x	-	x	x	x
	1:1 NAT (SNAT)	-	x	-	x	x
	PAT	x	x	x	x	x
	Politique de Routage	-	x	-	x	-
	Support de VLAN Trunking (802.1Q)	-	x	-	-	-
	Licence GPL		GPL	GPL	BSD	BSD
<b>Administration</b>	Recherche M. à jour	x	-	- x		-
	M. à jour automatique	-	-	- x		-
	backup x		x	x	x	x
	add-on x		- x		x x	

## 4.2 Solution choisie

Au vu des divers comparatifs, et d'après notre besoin, la solution d'un firewall et portail de type PfSense ou (**P**acket **F**ilter **S**ense) semble être la plus performante et évolutive puisqu'il permet de répondre aux critères de sécurité et d'authentification dont nous avons besoin (sécurité de l'authentification et de la communication).

Cette solution est proposée en Live CD d'environ 50Mo. Il est basé sur un système d'exploitation BSD (gratuit et open source).

## III. Partie III

### 1. Prés requis d'installation

PfSense requière une petite configuration :

- Poste de travail avec 500 Mo de disque dur
- 64 Mo de RAM (128 Mo conseillé)
- CPU PII 266 MHz au minimum
- Au moins 2 cartes réseaux (On peut en mettre plus si on désire créer des DMZ).

### 2. Installation de PfSense

La distribution PfSense se charge en mémoire et exécute ses divers composants.

Une fois le chargement est terminé :

- L'assistant demande la configuration des VLAN ☐ pour l'instant on va passer cette étape en répondant par **Non**.
- Elle passe à la configuration des deux interfaces réseau LAN & WAN (En saisie **r10 pour le LAN** et **r11 pour le WAN**).
- Nous avons en suite un récapitulatif des interfaces qu'il faudra valider en tapant « **Y** »

N.B : Le coté LAN correspond à l'interface du réseau Wifi, WAN fait référence au réseau de l'établissement.

Ci-dessous un imprimé écran de la configuration citée.

```
lnc0    00:0c:29:a0:31:51
lnc1    00:0c:29:a0:31:5b

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 webGUI to configure VLANs later, if required.

Do you want to set up VLANs now [y;n]?n

*NOTE*  pfSense requires *ATLEAST* 2 assigned interfaces to function.
        If you do not have two interfaces turn off the machine until
        you do.

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. The system will then prompt you to plug in each nic to
autodetect.

Enter the LAN interface name or 'a' for auto-detection: lnc0
Enter the WAN interface name or 'a' for auto-detection: lnc1
```

L'étape qui suit est l'installation de PfSense. L'interface ci-dessous illustre cette partie.

```
*** Welcome to pfSense BETA3-cdrom on pfSense ***

LAN          ->  lnc0    ->  192.168.1.1
WAN          ->  lnc1    ->  0.0.0.0(DHCP)

pfSense console setup
*****
0) Logout (SSH only)
1) Assign Interfaces
2) Set LAN IP address
3) Reset webGUI 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
99) Install pfSense to a hard drive/memory drive, etc.

Enter an option: 99
```

Afin de lancer l'installation de PfSense sur le disque dur de la machine, on tape au niveau de la console “99”.

L'installation démarre et l'assistant affiche les différentes étapes permettant la configuration des outils linguistiques, la vidéo, etc. ...

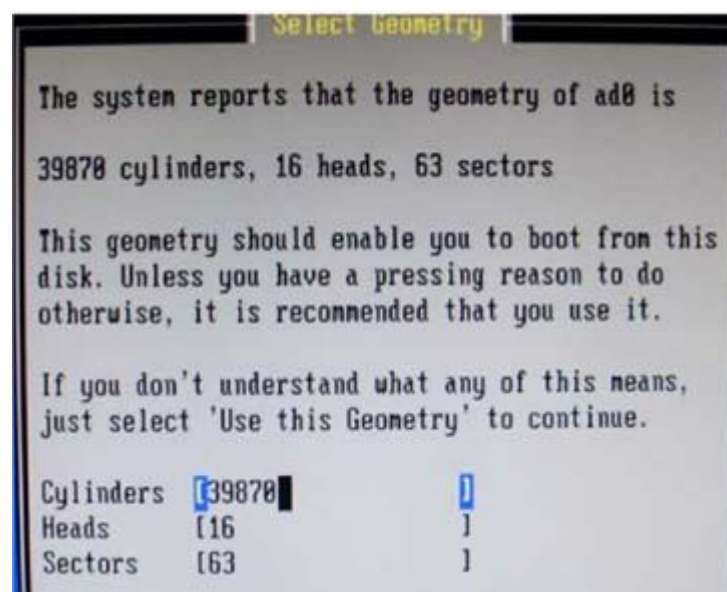


Une validation par le choix de la commande **“Accept these setting”** est requis pour la sauvegarde de la configuration entrée.

En suite, on passe au formatage du disque dur (Voir l’imprimé écran qui suit).



On choisit la 1<sup>ère</sup> options : **“Format this Disk”**, l’interface ci-dessous s’affiche :

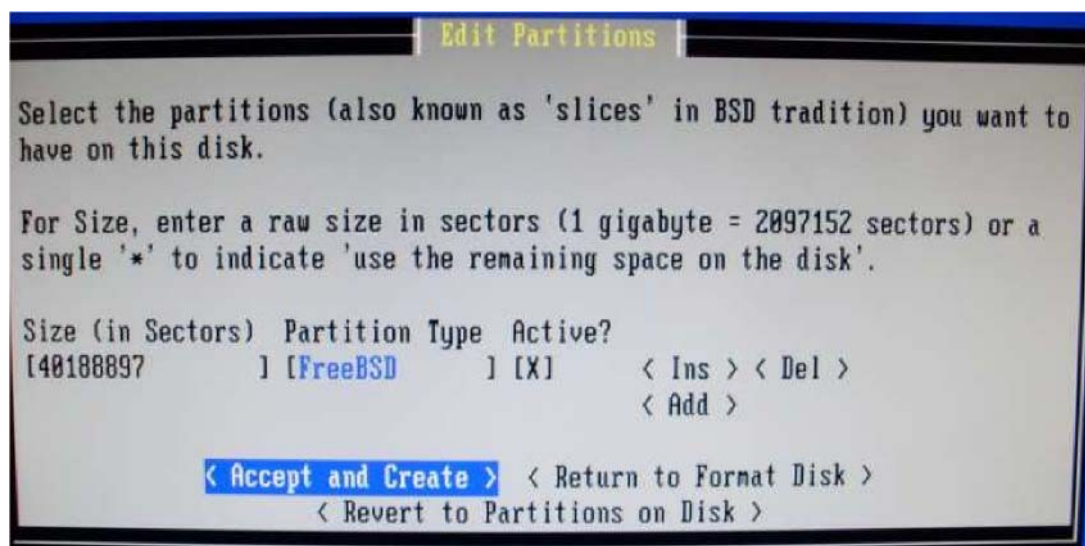


Cette interface permet le changement de la géométrie du disque dur. Cette étape n'est pas nécessaire. En effet, PfSense reconnaît tous les disques durs installés sur la machine. Alors, on valide par la **“Use this Géométry”**.

PfSense passe alors au partitionnement du disque comme il est mentionné ci-dessous :



On choisie **“Partition Disk”**, l'interface d'édition des partitions s'affiche.

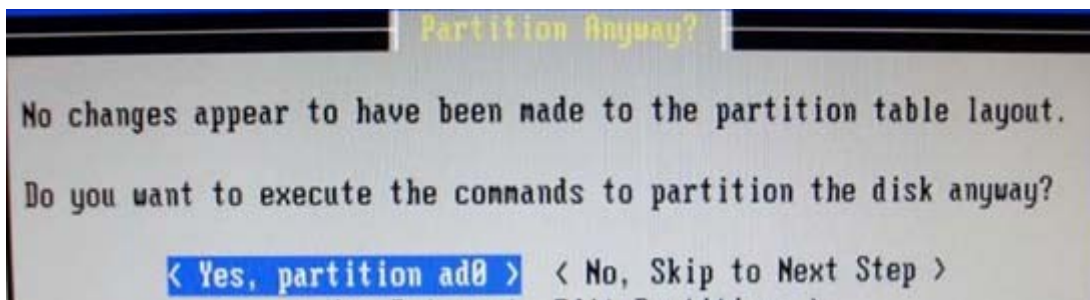


Cette interface permet de redimensionner la taille des partitions.

Dans notre cas, on exploitera toute l'espace disque on faisant le choix **“Accept and Create”**.

Une fenêtre d'avertissement s'affiche pour mentionner qu'aucun changement n'a été effectué sur la partition du disque (Voir l'imprimé écran ci-dessous).

On valide par **“Yes, partition ad0”** pour continuer l'installation.

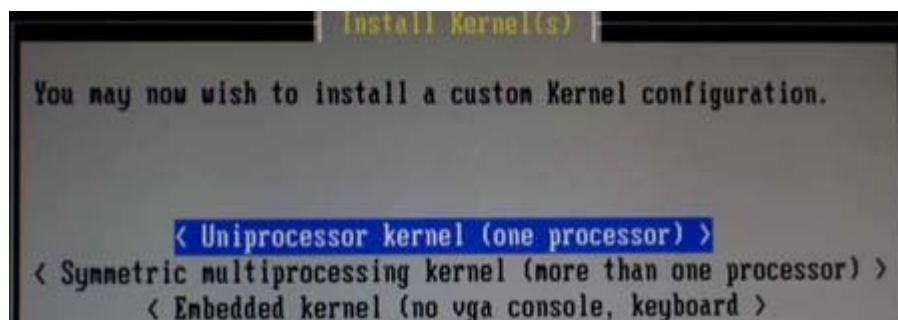


Le programme d'installation crée et formate la partition sélectionnée et démarre l'installation de PfSense.

L'étape suivante consiste à définir le SWAP et le point de montage du système. On définit donc 1024 Mo pour le SWAP et on met une "\*" pour le point de montage pour qu'il utilise le reste de l'espace disque, puis on valide par **"Accept and Create"**.

**N.B : Le swap est un espace mémoire du disque dur réservé pour des opérations d'échange. C'est la mémoire virtuelle qui est utilisée de la même manière que la mémoire RAM.**

En suite le système demande de spécifier le type de processeur pour une meilleure configuration du noyau du système. Selon la configuration matériel de notre machine, on choisira **"Uniprocessor kernel (one processor)"** comme illustré ci-dessous.



On passe alors à l'installation du Boot Loader de PfSense sur le disque dur. Ce dernier permettra de démarrer sur la partition du portail captif.

Pour ce faire nous sélectionnerons **«Accept and install BootBlocks»**.

Un message de confirmation de la réussite de l'installation s'affiche.

À la fin de l'installation, on éjecte le CD d'installation et on redémarre le système par le choix de **"Reboot"** mentionné sur l'imprimé écran ci-dessous.





### 3. Configuration du parefeu

#### 3.1. Configuration de l'interface LAN

Après le démarrage de la machine, PfSense affiche la console de configuration.

La première étape à effectuer est la configuration de l'interface réseau LAN, nous définissons alors l'adresse IP : "**172.24.4.254**" avec le masque **255.255.255.0** en notation CIDR, soit "24".

En suite PfSense présente la possibilité de configuration d'un serveur DHCP, nous avons passé cette étape en tapant "**N**".

À l'aide d'une 2<sup>ème</sup> station de travail qui sera connecté à l'interface LAN du firewall, nous pouvons se connecter à l'interface graphique de notre pare-feu en tapant le lien ci-après au niveau du navigateur WEB "**http://172.24.4.254**".

Une fenêtre d'authentification s'affiche (L'accès à la configuration se fait à l'aide du login : **Admin** et password : **PfSense**).

Une fois l'authentification réussie, la fenêtre d'accueil ci-dessous s'affiche.





On clique sur le bouton “**Next**” pour démarrer la configuration.

L’écran qui s’affiche permet :

- l’adhésion de notre pare-feu sur le domaine de l’établissement “**itlearning.uh1.ac.ma**”
- Configuration de l’adressage du serveur DNS “10.200.8.2 et 212.217.0.1”
- ...

La fenêtre ci-après affiche les différents paramètres à définir :



webConfigurator

firewall.itlearning.uh1.ac.ma

#### System

Advanced  
Firmware  
General Setup  
Packages  
Setup wizard  
Static routes

#### Interfaces

(assign)  
WAN  
LAN

#### Firewall

Aliases  
NAT  
Rules  
Schedules  
Traffic Shaper  
Virtual IPs

#### Services

Captive portal  
DNS forwarder  
DHCP relay  
DHCP server  
Dynamic DNS  
Load Balancer  
OLSR  
PPPoE Server  
RIP  
SNMP  
UPnP  
OpenNTPD  
Wake on LAN

#### VPN

IPsec  
OpenVPN  
PPTP

#### Status

CARP (failover)  
DHCP leases  
Filter Reload Status  
Interfaces  
IPsec  
Load Balancer  
Package logs  
Queues

### System: General Setup

Hostname	<input type="text" value="firewall"/>	name of the firewall host, without domain part e.g. <i>firewall</i>
Domain	<input type="text" value="itlearning.uh1.ac.ma"/>	e.g. <i>mycorp.com</i>
DNS servers	<input type="text" value="10.200.8.2"/> <input type="text" value="212.217.0.1"/>	IP addresses; these are also used for the DHCP service, DNS forwarder and for PPTP VPN clients  <input type="checkbox"/> <b>Allow DNS server list to be overridden by DHCP/PPP on WAN</b> If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). They will not be assigned to DHCP and PPTP VPN clients, though.
Username	<input type="text" value="adminlearn"/>	If you want to change the username for accessing the webGUI, enter it here.
Password	<input type="password"/> <input type="password"/> (confirmation)	If you want to change the password for accessing the webGUI, enter it here twice.
webGUI protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS	
webGUI port	<input type="text"/>	Enter a custom port number for the webGUI above if you want to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.
Time zone	<input type="text" value="Etc/UTC"/>	Select the location closest to you
NTP time server	<input type="text" value="0.pfsense.pool.ntp.org"/>	Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if you enter a host name here!

#### Theme


<input type="text" value="pfsense"/>	This will change the look and feel of pfSense
--------------------------------------	---

Save

Le menu à gauche de la fenêtre permet le basculement entre les différentes options.

La fenêtre ci-dessous permet la configuration de l'interface WAN, nous lui affecterons les informations ci-après :

- Adresse IP : **10.10.61.254/23**
- Passerelle : **10.10.60.1**


webConfigurator

firwall.itlearning.uh1.ac.ma

**System**

- Advanced
- Firmware
- General Setup
- Packages
- Setup wizard
- Static routes

**Interfaces**

- (assign)
- WAN
- LAN

**Firewall**

- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs

**Services**

- Captive portal
- DNS forwarder
- DHCP relay
- DHCP server
- Dynamic DNS
- Load Balancer
- OLSR
- PPPoE Server
- RIP
- SNMP
- UPnP
- OpenNTPD
- Wake on LAN

**VPN**

- IPsec
- OpenVPN
- PPTP

**Status**

- CARP (failover)
- DHCP leases
- Filter Reload Status
- Interfaces
- IPsec
- Load Balancer
- Package logs
- Queues
- RRD Graphs
- Services
- System
- System logs
- Traffic graph

## Interfaces: WAN

General configuration

<b>Type</b>	Static
<b>MAC address</b>	<input type="text" value="00:23:7d:4d:e2:47"/> <a href="#">Copy my MAC address</a> <small>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</small>
<b>MTU</b>	<input type="text"/> <small>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 MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.</small>

Static IP configuration

<b>IP address</b>	<input type="text" value="10.10.61.254"/> / <input type="text" value="23"/>
<b>Gateway</b>	<input type="text" value="10.10.60.1"/>


DHCP client configuration

<b>Hostname</b>	<input type="text"/>
<small>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).</small>	

PPPoE configuration

<b>Username</b>	<input type="text"/>
<b>Password</b>	<input type="password"/>
<b>Service name</b>	<input type="text"/> <small>Hint: this field can usually be left empty</small>
<b>Dial on demand</b>	<input type="checkbox"/> <b>Enable Dial-On-Demand mode</b> <small>This option causes the interface to operate in dial-on-demand mode, allowing you to have a <i>virtual full time</i> connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.</small>
<b>Idle timeout</b>	<input type="text"/> seconds <small>If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.</small>
<b>Periodic reset</b>	<input type="checkbox"/> enable periodic PPPoE resets

La fenêtre qui suit permet la configuration de l'interface LAN.



## webConfigurator

firewall.itlearning.uh1.ac.ma

**System**

- Advanced
- Firmware
- General Setup
- Packages
- Setup wizard
- Static routes

**Interfaces**

- (assign)
- WAN
- LAN

**Firewall**

- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs

**Services**

- Captive portal
- DNS forwarder
- DHCP relay
- DHCP server
- Dynamic DNS
- Load Balancer
- OLSR
- PPPoE Server
- RIP
- SNMP
- UPnP
- OpenNTPD
- Wake on LAN

**VPN**

- IPsec
- OpenVPN
- PPTP

**Status**

- CARP (failover)
- DHCP leases
- Filter Reload Status
- Interfaces
- IPsec
- Load Balancer
- Package logs
- Queues

### Interfaces: LAN

**IP configuration**

Bridge with	none
IP address	172.24.4.254 / 24

**FTP Helper**

FTP Helper	<input type="checkbox"/> Disable the userland FTP-Proxy application
------------	---

Save

**Warning:**  
after you click "Save", you will need to do one or more of the following steps before you can access your firewall again:

- change the IP address of your computer
- renew its DHCP lease
- access the webGUI with the new IP address
- be sure to add firewall rules to permit traffic through the interface.
- You also need firewall rules for an interface in bridged mode as the firewall acts as a filtering bridge.

Pour des mesures de sécurité, PfSense demande le changement du mot de passe administrateur :

On this screen we will set the Admin password which is used to access the WebGUI and also SSH services if you wish to enable.

**Set Admin WebGUI Password**

Admin Password:	<input type="password"/>
Admin Password AGAIN:	<input type="password"/>

Next

Un redémarrage est requis pour que les modifications soient prises en charge.

## 3.2. Changement du mode graphique

Pour une simple administration, il est conseillé de changer l'apparence de l'interface graphique. Pour le faire, on passe sous l'onglet **Système** Général Setup, dans la rubrique thème, on choisit "PfSense".

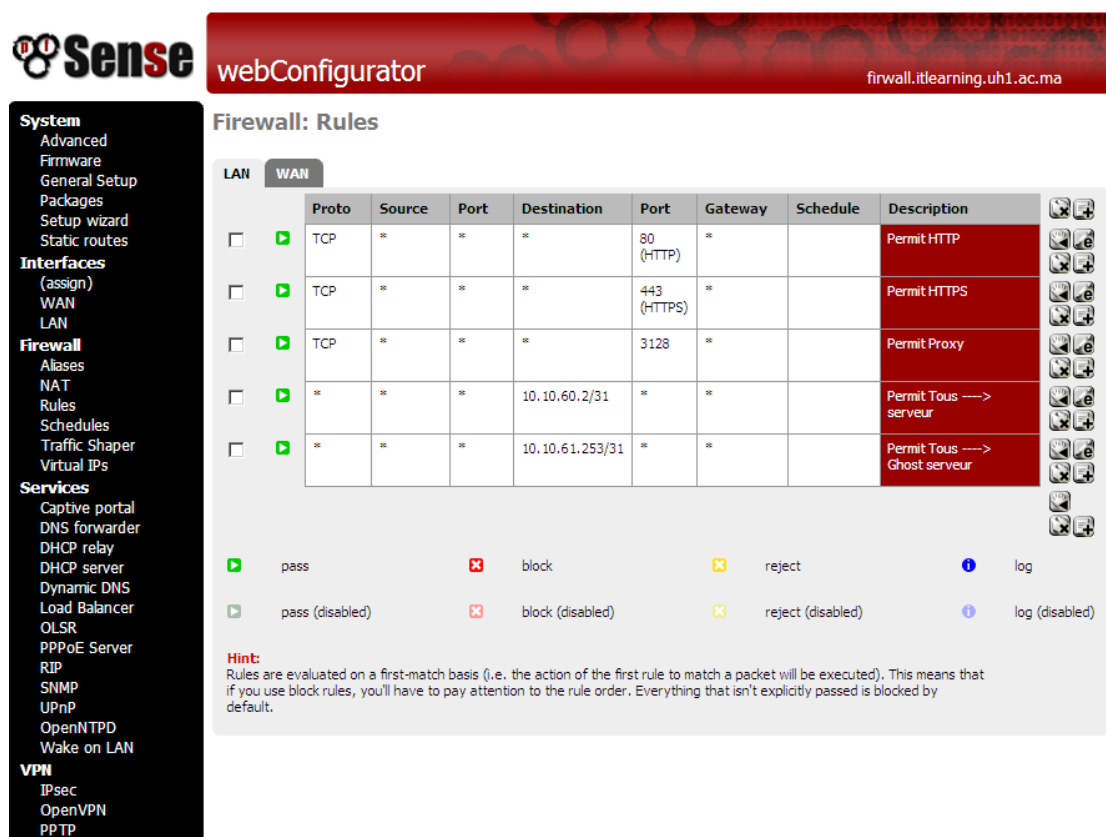
Cette nouvelle interface est plus pratique puisqu'elle permet l'accès aux diverses options sans passer par les menus déroulants et les listes de choix.

## 3.3. Filtrage des ports

Pour le paramétrage de cette partie, on choisit **Rules** sous le menu Firewall (À gauche de la fenêtre ci-dessous).

Cette interface permet le paramétrage des deux interfaces LAN & WAN.

Dans notre cas, on a bloqué tous les ports à part le HTTPS pour la gestion, l'adresse 10.10.60.2/31 pour l'authentification et le numéro de port 3128 pour le proxy.



The screenshot shows the pfSense webConfigurator interface. The left sidebar contains a menu with categories: System, Interfaces, Firewall, Services, and VPN. The 'Firewall' section is expanded, showing 'Rules' as the selected option. The main content area is titled 'Firewall: Rules' and has tabs for 'LAN' and 'WAN'. A table lists the firewall rules:

	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
<input type="checkbox"/>	TCP	*	*	*	80 (HTTP)	*		Permit HTTP
<input type="checkbox"/>	TCP	*	*	*	443 (HTTPS)	*		Permit HTTPS
<input type="checkbox"/>	TCP	*	*	*	3128	*		Permit Proxy
<input type="checkbox"/>	*	*	*	10.10.60.2/31	*	*		Permit Tous ----> serveur
<input type="checkbox"/>	*	*	*	10.10.61.253/31	*	*		Permit Tous ----> Ghost serveur

Below the table, there are action buttons: pass, block, reject, and log. There are also disabled versions of these buttons. A hint at the bottom states: "Rules are evaluated on a first-match basis (i.e., the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default."



webConfigurator

firewall.itlearning.uh1.ac.ma

#### System

Advanced  
Firmware  
General Setup  
Packages  
Setup wizard  
Static routes

#### Interfaces

(assign)  
WAN  
LAN

#### Firewall

Aliases  
NAT  
Rules  
Schedules  
Traffic Shaper  
Virtual IPs

#### Services

Captive portal  
DNS forwarder  
DHCP relay  
DHCP server  
Dynamic DNS  
Load Balancer  
OLSR  
PPPoE Server  
RIP  
SNMP  
UPnP  
OpenNTPD  
Wake on LAN

#### VPN

IPsec  
OpenVPN  
PPTP

### Firewall: Rules

LAN WAN

	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description	
<input type="checkbox"/>		*	*	*	*	*	*	Permit all	
	pass		block		reject		log		
	pass (disabled)		block (disabled)		reject (disabled)		log (disabled)		

#### Hint:

Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

## 4. Mise en place du portail captif

### 4.1. Qu'est ce qu'un portail captif

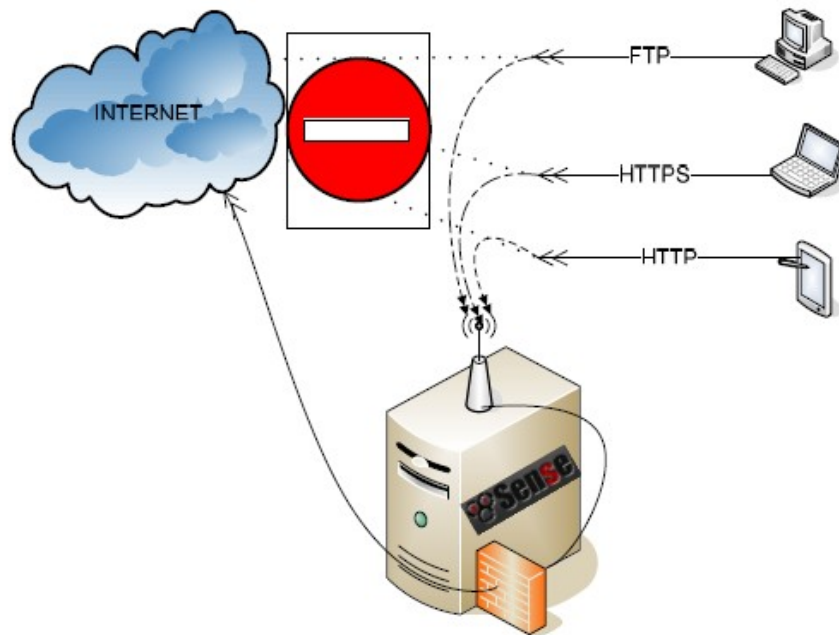
Un portail captif est une structure permettant un accès rapide à Internet. Lorsqu'un utilisateur cherche à accéder à une page Web pour la première fois.

Le portail captif capture la demande de connexion par un routage interne et propose à l'utilisateur de s'identifier afin de pouvoir recevoir son accès. Cette demande d'authentification se fait via une page Web stockée localement sur le portail captif grâce à un serveur HTTP. Ceci permet à tout ordinateur équipé d'un navigateur HTML et d'un accès Wi-Fi de se voir proposer un accès à Internet.

La connexion au serveur est sécurisée par SSL grâce au protocole HTTPS, ce qui garanti l'invulnérabilité de la transaction. Les identifiants de connexion (identifiant, mot de passe) de chaque utilisateur sont stockés dans une base de données qui est hébergée localement ou sur un serveur distant. Une fois l'utilisateur authentifié, les règles du

Firewall le concernant sont modifiées et celui-ci se voit alors autorisé à utiliser son accès pour une durée limitée fixée par l'administrateur. A la fin de la durée définie, l'utilisateur se verra redemander ses identifiants de connexion afin d'ouvrir une nouvelle session.

## 4.2. Fonction d'un portail captif



**Quoi que désire faire le client, s'il veut surfer sur le WEB il devra d'abord passer par le portail captif afin de s'authentifier.**

## 4.3. Configuration du portail captif

La configuration du portail captif est accessible via le menu Général.

Ce service est activé en cochant la case “**Enable captive portal**”  
(Voir l'imprimé écran ci-dessous).



Captive portal	Pass-through MAC	Allowed IP addresses	Users	File Manager
<input checked="" type="checkbox"/> <b>Enable captive portal</b>				
Interface	LAN <input type="text"/> Choose which interface to run the captive portal on.			
Maximum concurrent connections	<input type="text"/> per client IP address (0 = no limit) This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Default is 4 connections per client IP address, with a total maximum of 16 connections.			
Idle timeout	<input type="text"/> minutes Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.			
Hard timeout	60 <input type="text"/> minutes Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).			
Logout popup window	<input checked="" type="checkbox"/> <b>Enable logout popup window</b>			

Afin de terminer la configuration du portail captif, nous suivrons les étapes ci-dessous :

- Activer la connexion sécurisée pour cette interface depuis la ligne **“WebGUI Protocole”** en choisissons le protocole HTTPS (le port à indiquer est le 443)

Une fois ce paramètre est ajusté, on sauvegarde la configuration puis en relance l'interface WEB par l'adresse **“https://172.24.4.254”** Connexion sécurisée par le protocole SSL.

- Passer sous la section **System/Advanced** puis activer la case **“Enable Secure Shell”** afin d'activer l'administration à distance via le shell. Connexion sécurisée Voir l'imprimé écran ci-dessous).

Secure Shell	
	<input checked="" type="checkbox"/> <b>Enable Secure Shell</b>
	<input type="checkbox"/> <b>Disable Password login for Secure Shell (KEY only)</b>
SSH port	22 <input type="text"/> Note: Leave this blank for the default of 22

- Générer un certificat au format X509 et une clé RSA via le bouton **“Create”** de la ligne **“WebGUI SSL certificate/key”**.

Une fenêtre s'ouvrira donc afin de renseigner les informations nécessaires pour la création du certificat.

Une fois le certificat et la clé sont créés, on doit valider à l'aide du bouton **“Save”** mentionné sur l'imprimé écran ci-dessous.



Ce certificat est auto signée, le navigateur web fournira donc à l'utilisateur la possibilité de l'examiner, ce qui permet d'éviter que des pirates soient installées en proposant des connexions afin de récupérer des données.

La clé RSA sert à chiffrer les échanges lors de la connexion du client au serveur.

De cette manière l'authentification sera sécurisée.

- Passer sous l'onglet **Interfaces/LAN**, s'assurer que cette interface n'est pas bridgée avec celle du réseau WAN -**Devant Bridge with, choisir : none**- (Voir l'imprimé écran ci-dessous).

#### 4.4. Configuration du service de Portail Captif

Afin de configurer l'interface sur laquelle le portail captif sera agir :

- Passer sous **Services Captive Portal** puis choisir **LAN**
- Au niveau de ligne **Hard Time Out** définir un délai de connexion au-delà duquel l'utilisateur devra s'authentifier.
- Sur la ligne **Authentication**, indiquer que le mode d'authentification sera via un serveur Radius et entrer son adresse IP, son port d'écoute ainsi que le secret partagé entre lui et le pare-feu.

**N.B : PfSense offre la possibilité d'installer un serveur radius par l'acquisition d'un paquet, mais cette méthode présente deux inconvénients :**

- ^ L'authentification entre le client et le serveur sera donc cryptée.

Cette partie décrit la méthode à suivre afin de personnaliser une page HTML qui s'affichera durant les demandes d'authentification (Portail Captif) Voir le code ci-dessous :

[illegible]

```
<tr>
<td align="center">Mot de passe:</div></td>
</tr>
<tr>
<td align="center"><input name="auth_pass" type="password" /></td>
</tr>
<tr>
<td align="center"><input name="accept" type="submit" value="Continue" /></td>
</tr>
</table>
<p>&nbsp;</p></td>
<td>&nbsp;</td>
</tr>
</table>
<input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
</form>
</body>
</html>
```

#### 4.6. Configuration de la page d'authentification sur le parefeu

Pour pouvoir ajouter cette page HTML au portail captif, aller à l'interface de configuration de PfSense “**Services**” puis “**Captive portal**”. A la ligne “**Portal page contents**”, cliquer sur **Parcourir** puis indiquer le chemin d'accès à la page HTML qu'on a déjà crée (Voir l'imprimé écran ci-dessous).



Portal page contents

View current page

Upload an HTML file for the portal page here (leave blank to keep the current one). Make sure to include a form (POST to "\$PORTAL\_ACTIONS\$") with a submit button (name="accept") and a hidden field with name="redirurl" and value="\$PORTAL\_REDIRURL\$". Include the "auth\_user" and "auth\_pass" input fields if authentication is enabled, otherwise it will always fail. Example code for the form:

```
<form method="post" action="$PORTAL_ACTIONS$">
  <input name="auth_user" type="text">
  <input name="auth_pass" type="password">
  <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$" />
  <input name="accept" type="submit" value="Continue" />
</form>
```

Ci-dessous la page qui s'affichera aux utilisateurs pour authentification.

Pour vous connecter au réseau Itelearning Academy il vous suffira de saisir votre Identifiant et votre Mot De Passe ci-dessous.

Les sites visités sont soumis à la charte informatique de l'établissement

Identifiant:

Mot de passe:

Continue

Lorsque les informations introduites sont invalides, la fenêtre ci-dessous s'affiche.

Erreur : Veuillez resaisir votre identifiant et votre mot de Passe

Identifiant:

Mot de passe:

Continue

## 5. Configuration du DNS forwarder

Cette option permet de relayer les paramètres DNS du portail captif et de les appliquer sur les postes clients dans le cadre d'un serveur DHCP, c'est à dire lorsque le protocole DHCP est configuré il n'est pas nécessaire d'indiquer quel serveur DNS à contacter si l'option DNS forwarder est activée, le DHCP prendra par défaut le serveur DNS indiqué dans les paramètres de configuration générale du portail captif.

Pour l'activer, aller dans **Services/DNS forwarder** puis cocher la case **“Enable DNS forwarder”** (Voir l'imprimé écran ci-dessous).

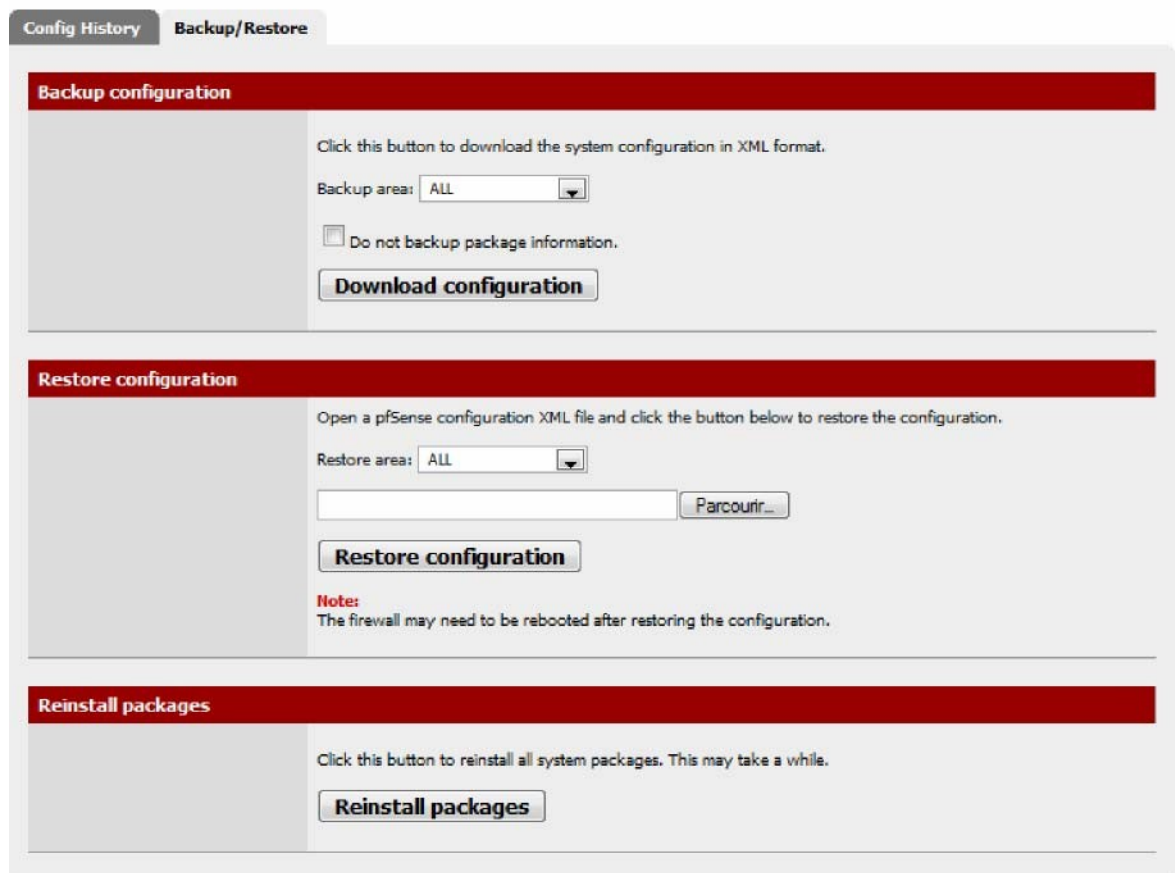
### Services: DNS forwarder

☒ Enable DNS forwarder

## 6. Sauvegarde de la configuration du parefeu

Pour effectuer une sauvegarde de toute la configuration du pare-feu, aller dans la rubrique **Diagnostics : Backup/Restore**, passer sous l'onglet **Backup/restore** et cliquer **Download configuration** (Voir l'imprimé écran ci-dessous).

### Diagnostics: Backup/restore



The screenshot shows the 'Diagnostics: Backup/restore' page in pfSense. It has two tabs: 'Config History' and 'Backup/Restore', with the latter being active. The page is divided into three main sections:

- Backup configuration:** Contains instructions to click a button to download the system configuration in XML format. It includes a 'Backup area:' dropdown menu set to 'ALL', an unchecked checkbox for 'Do not backup package information.', and a 'Download configuration' button.
- Restore configuration:** Contains instructions to open a pfSense configuration XML file and click a button to restore the configuration. It includes a 'Restore area:' dropdown menu set to 'ALL', a file input field with a 'Parcourir...' button, and a 'Restore configuration' button. A note below states: 'Note: The firewall may need to be rebooted after restoring the configuration.'
- Reinstall packages:** Contains instructions to click a button to reinstall all system packages, noting that it may take a while. It includes a 'Reinstall packages' button.

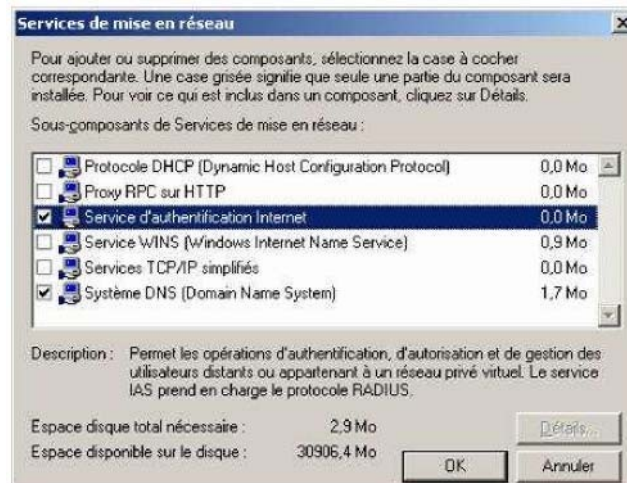
Cette méthode permet le téléchargement d'un fichier XML avec tous les paramètres qui survira à une reconfiguration ultérieure du pare-feu si c'est nécessaire.

## 7. Installation du serveur radius

Afin de bénéficier des avantages offerts par le portail captif, nous procéderons à l'installation d'un serveur RADIUS tout en permettant l'authentification des utilisateurs avec les comptes déjà créés au niveau du contrôleur de domaine.

Pour cela :

- Cliquer sur Démarrer → Panneau de configuration → Ajout/Suppression de programmes → Ajouter ou supprimer des composants Windows, faire un double clic sur “Services de mises en réseau” puis cocher la case “Service d’authentification Internet” et valider par OK pour démarrer l’installation du service.



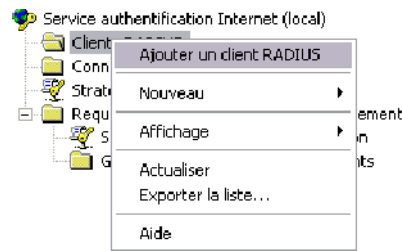
En suite, renseigner le serveur PfSense dans le DNS du serveur Radius. En effet lorsque PfSense utilise un serveur Radius externe ce dernier devient son serveur DNS, pour le faire :

- Cliquer sur Démarrer → Tous les programmes → Outils d’administration et choisir DNS, au niveau de la console faire un clic droit sur le dossier représentant le domaine Itlearning.uh1.ac.ma et créer un nouvel hôte (A) avec les informations ci-après (Nom : PfSense – FQDN : Nom de la machine + Nom de domaine du serveur PfSense – Adresse IP : 10.10.61.2).

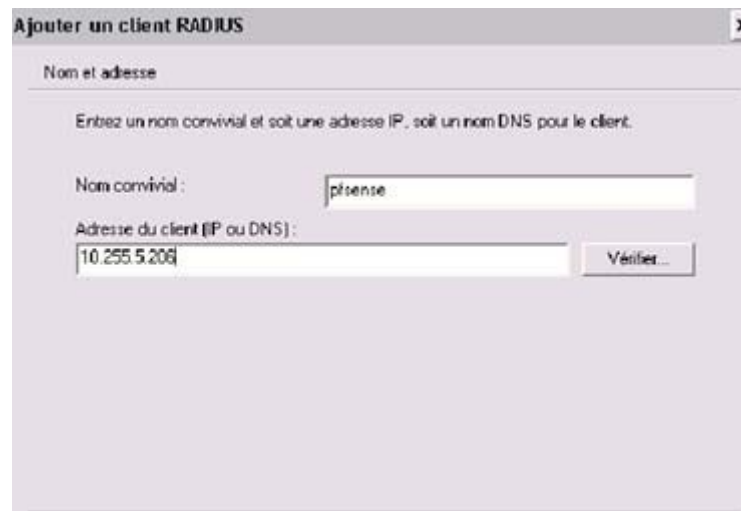
Il nous reste l’ajout du serveur PfSense entant que client RADIUS. Le but de cette opération consiste à ce que le serveur PfSense interroge le service RADIUS pour disposer de la base des utilisateurs AD.

Pour effectuer cette configuration, nous avons suivre les étape ci-dessous :

- Cliquer sur Démarrer → Tous les programmes → Outils d’administration → Service d’authentification Internet, Nous commencerons donc par l’inscription du serveur RADIUS au niveau d’Active Directory pour créer une liaison entre eux. Pour cela, cliquer avec le bouton droit de la souris sur “Service d’authentification Internet” puis choisir “Inscrire le serveur dans Active Directory”.
- Dans la console IAS (Internet Authentication Service), cliquer avec le bouton droit de la souris sur “Client Radius” et choisir “Ajouter un client RADIUS” (Voir l’imprimé écran ci-dessous).



Sur la boîte de dialogue qui s’affiche (Voir l’imprimé écran ci-dessous), renseigner les informations ci-après (Nom : PfSense – Adresse IP : 10.10.61.254) puis cliquer sur suivant.



**Ajouter un client RADIUS**

Nom et adresse

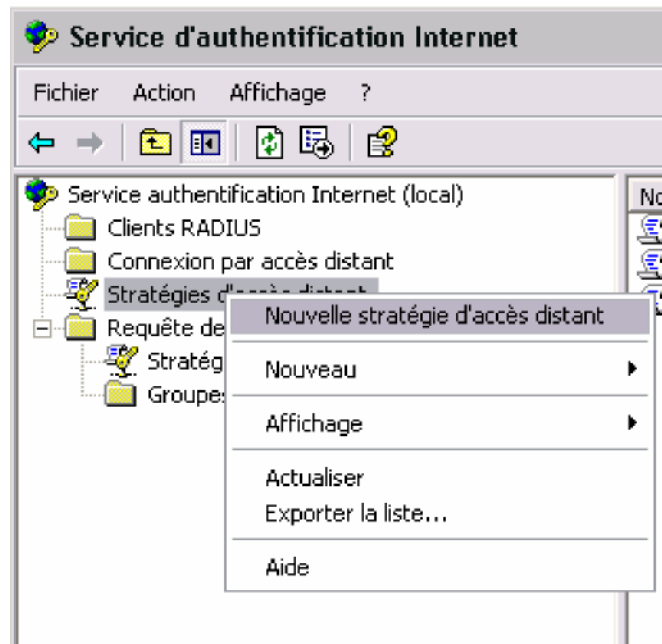
Entrez un nom convivial et soit une adresse IP, soit un nom DNS pour le client.

Nom convivial :

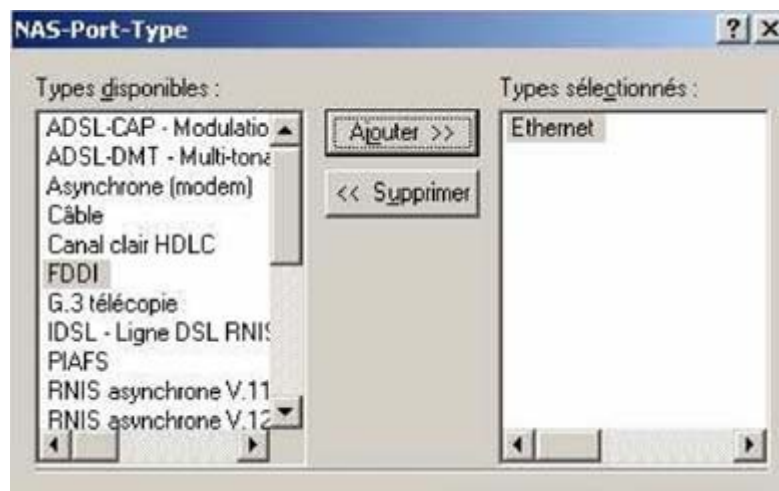
Adresse du client (IP ou DNS) :

Pour terminer la configuration, il suffit de :

- Indiquer le secret partagé déjà configuré sur le serveur PfSense et choisir Client-Fournisseur : RADIUS Standard.
- Paramétrer les stratégies propres au serveur PfSense au niveau de la console IAS en faisant un clique droit sur "Stratégie d'accès distant" et en choisissant "Nouvelle stratégie d'accès distant" (Voir l'imprimé écran ci-dessous).



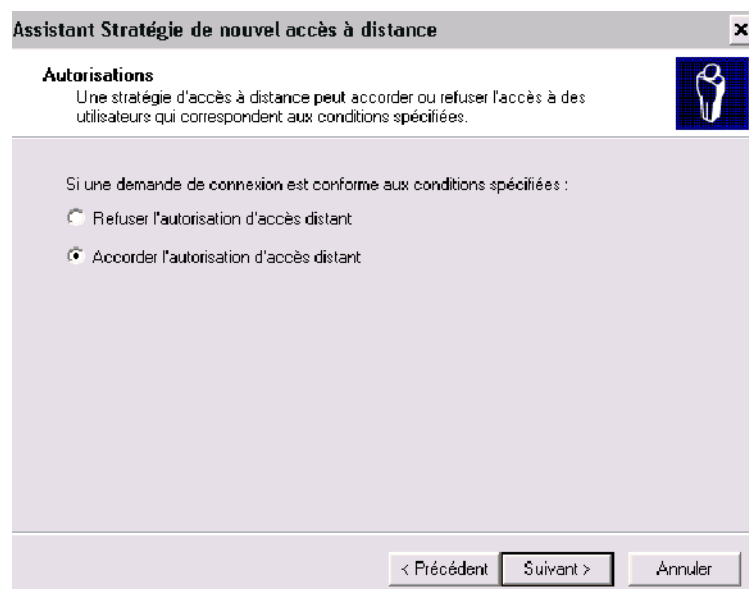
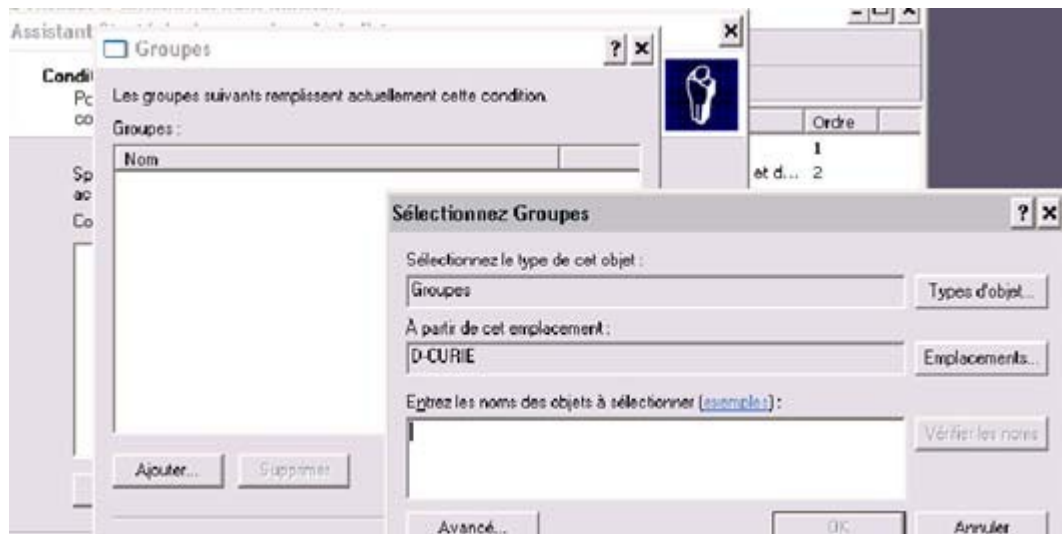
- Au niveau de l'assistant, choisir "Installer une stratégie personnalisée" en lui fournira un nom.  
Sur la boîte de dialogue qui s'affiche, sélectionner "NAS Identifier" puis cliquer sur le bouton "Ajouter".



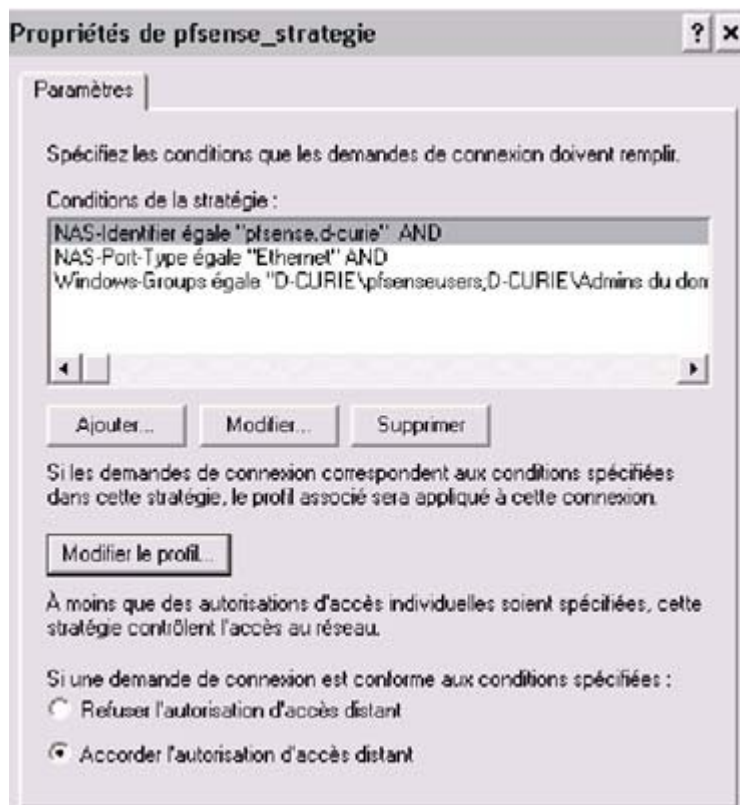
Le second attribut à ajouter au niveau de la stratégie est "NAS-Port-Type" qui sert à préciser le type de connexion employer pour la communication entre le serveur Radius et le client Radius.

- Sélectionner donc « Ethernet » dans les différents types de connexions.
- Le dernier attribut à sélectionner est "Windows group" qui servira à déterminer quel groupe d'utilisateur sera autorisé à utiliser le service RADIUS.
- Dans la fenêtre "Groupes" cliquer sur ajouter puis indiquer "Utilisateur du domaine" (Au niveau de l'imprimé écran ci-dessous) afin d'autoriser tous les utilisateurs de IT-Learning Academy à utiliser le serveur RADIUS.





- Une fois les attributs sont sélectionnés, choisir "Accorder l'autorisation d'accès distant" puis cliquer sur suivant, la boîte de dialogue ci-dessous s'affiche :



- Pour effectuer le réglage nécessaire à l'authentification, cliquer sur "Modifier le profil" de l'imprimé écran ci-dessus.
- Au niveau de l'onglet "Authentification", choisir "Authentification non cryptée (PAP, SPAP)". En effet les échanges sur le réseau filaire entre les deux serveurs PfSense et RADIUS bénéficieront des protocoles PAP et SPAP.
- Cliquer sur suivant pour terminer l'installation.
- Retourner dans la console de configuration d'IAS et monter la stratégie créée pour quelle soit prise en charge.

Il est nécessaire de vérifier au niveau des propriétés du serveur RADIUS que l'accès distant est autorisé pour s'assurer que les demandes d'authentifications provenant du serveur PfSense seront acceptées.

## 8. Test du fonctionnement du portail captif

Voir l'imprimé écran ci-dessous.

```

C:\WINDOWS\System32\cmd.exe - ping google.fr -t
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Anthony>ping google.fr -t

Envoi d'une requête 'ping' sur google.fr [216.239.59.104] avec 32 octets de données :

Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Réponse de 216.239.59.104 : octets=32 temps=54 ms TTL=235
Réponse de 216.239.59.104 : octets=32 temps=55 ms TTL=235
Réponse de 216.239.59.104 : octets=32 temps=45 ms TTL=234
Réponse de 216.239.59.104 : octets=32 temps=54 ms TTL=234
Réponse de 216.239.59.104 : octets=32 temps=43 ms TTL=235
Réponse de 216.239.59.104 : octets=32 temps=43 ms TTL=235
Réponse de 216.239.59.104 : octets=32 temps=44 ms TTL=234
Réponse de 216.239.59.104 : octets=32 temps=53 ms TTL=234

```

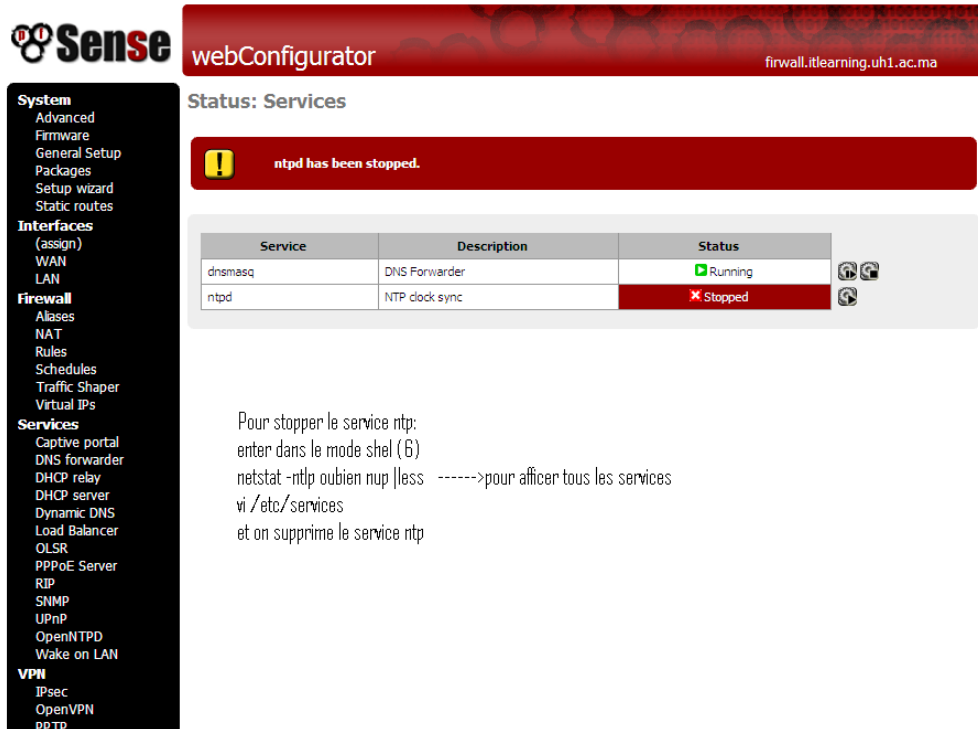
<= Avant authentification

<= Après authentification

## 9. Faits marquants

### 9.1. Problème avec le service NTP

Lors de la mise en place du firewall, le service NTP envoie des requêtes de synchronisation du temps, ce qui résulte la saturation du firewall, pour remédier à ce problème, on a procédé à l'arrêt de ce service en suivant la méthode ci-dessous (Voir l'imprimé écran) :



**Sense webConfigurator** firwall.itlearning.uh1.ac.ma

**Status: Services**

**ntpd has been stopped.**

Service	Description	Status
dnsmasq	DNS Forwarder	Running
ntpd	NTP clock sync	Stopped

Pour stopper le service ntp:  
 entrer dans le mode shel (6)  
 netstat -ntlp ou bien nup |less ----->pour afficher tous les services  
 vi /etc/services  
 et on supprime le service ntp

## 9.2. Rapidité des connexions

Après la mise en place de cette solution on remarque la rapidité des :

- Connexions entre les postes de travail
- Accès aux ressources partagées
- Accès à Internet

## 9.3. Mise en place du portail captif

Les tests de mise en place du portail captif sont effectués avec succès, sauf qu'on a trouvé une petite difficulté durant son mise en production à cause du serveur proxy déjà installé au sein de la FST sur un segment séparé du réseau de notre pare-feu.

Alors le navigateur Web au niveau des stations de travail redirige les requêtes d'authentification vers le serveur proxy au lieu de la passerelle (pare-feu).

La mise en place d'une solution permettant la correction de cette anomalie sera réalisée au cours de la préparation de notre PFE.

## **10 Conclusion**

Le stage effectué au sein d'IT-Learning Academy a été une grande opportunité qui nous a permis d'acquérir plusieurs informations et de développer notre savoir faire par l'apprentissage d'un ensemble de connaissances importantes dans diverse domaine.

Les connaissances et les compétences acquises au cours de notre formation sont largement suffisantes pour surmonter tout type de problème, d'intégrer et de réaliser toutes les tâches demandées sans aucune difficulté.

Aussi, les motivations que nous avons reçues des personnels de l'entreprise, l'intérêt, montré pour notre travail, la diversité des rôles que nous avons exercés durant notre stage juge que les deux mois consommés ont été un complément et une extension très importante de notre formation.

## **11Annexe**

### Bibliographie : Web

- <http://astralprojection1.free.fr>
- <http://www.supinfo-projects.com/fr/2006/portailcaptifwifi>
- <http://doc.pfsense.org>
- <http://forum.pfsense.org>
- <http://www.scribd.com>