# Mise en place d'un firewall d'entreprise avec PfSense

JA-PSI Programmation & Sécurité informatique <u>http://www.ja-psi.fr</u>



Par Régis Senet

http://www.regis-senet.fr regis.senet [at] supinfo.com

Le 13/06/2009

## Sommaire

	Int	roduction	3
2.	La	méthode complète : Configuration de VirtualBox	3
2	2.1	Mise à jour du système	3
2	2.2	Configuration de VirtualBox	4
2	2.3	Activation d'une interface réseau	6
2	2.4	Installation de PfSense	6
3.	La	méthode rapide : Utilisation de la version VMWare	9
3. 4.	La Co	méthode rapide : Utilisation de la version VMWare nfiguration de PfSense	9 L0
3. 4.	La Co 1.1	méthode rapide : Utilisation de la version VMWare nfiguration de PfSense	9 10
<b>3.</b> <b>4.</b>	La Co 1.1 1.2	méthode rapide : Utilisation de la version VMWare	<b>9</b> 10

## 1. Introduction

L'installation ainsi que la configuration PfSense va se réaliser sur un système d'exploitation de type FreeBSD. Il est possible d'émuler le système d'exploitation FreeBSD grâce à VirtualBox.

Pour plus de renseignement sur VirtualBox, voici un lien présentant comment le faire fonctionner : <u>http://www.regis-senet.fr/blog/article.php?id\_article=44</u>

Nous ne reviendrons donc pas sur l'installation de VirtualBox, mais simplement sur sa configuration afin de pouvoir faire fonctionner PfSense correctement.

## 2. La méthode complète : Configuration de VirtualBox

## 2.1 Mise à jour du système

Il est possible à tous moment qu'une faille de sécurité soit découverte dans l'un des modules composant votre système que ce soit Apache ou quoi que ce soit d'autre. Certaines de ces failles peuvent être critiques d'un point de vue sécurité pour l'entreprise. Afin de combler ce risque potentiel, il est nécessaire de régulièrement mettre à jour l'ensemble du système grâce à divers patches de sécurité.

Il est possible de mettre à jour l'ensemble du système via la commande suivante :

#### nocrash:~# apt-get update && apt-get upgrade

Le système d'exploitation est maintenant complètement à jour, il est donc possible de mettre en place **VirtualBox** dans de bonnes conditions.

Il est possible de ne pas passer par cette étape mais elle est fortement conseillée pour la sécurité ainsi que la stabilité de votre système d'exploitation.

## 2.2 Configuration de VirtualBox

Afin de pouvoir configurer nos machines, il est nécessaire de lancer VirtualBox, pour cela, il est simplement nécessaire d'inscrire la commande suivante :

#### nocrash:~# Virtualbox

Pour créer notre machine virtuelle, il est nécessaire de suivre les étapes suivantes :

- 1. Cliquez sur « **Nouveau** » afin de commencer l'installation de la nouvelle machine.
- Cliquez sur « Suivant » puis rentrez le nom de votre ordinateur (« PfSense ») et sélectionnez le système d'exploitation que vous voulez virtualiser (« BSD - FreeBSD »).
- 3. Choisissez la mémoire que vous voulez disposez sur votre système virtualisé (256 Mo).
- 4. Sélectionnez « Créer un nouveau disque dur » en vérifiant que la case « Disque dur d'amorçage » est cochée.
- 5. Afin de créer un disque dur ayant une taille variable (conseillé), il est nécessaire de sélectionner « **Image disque à taille dynamique** » puis sélectionnez la taille de disque (**2Go**)
- 6. Cliquez ensuite deux fois sur « **Terminer** » afin de terminer la mise en place de la machine virtuelle.

Voici à quoi devrait ressembler votre **VirtualBox** une fois les configurations terminées. Il est à présent possible d'installer votre système d'exploitation sur l'ordinateur virtuel précédemment créé.



Nous allons à présent initialiser le système d'exploitation. Pour cela, il est nécessaire de télécharger la version PfSense sous forme de LiveCD qui permet une installation directe.

Cette version se trouve à l'adresse suivante : <u>http://mirror.qubenet.net/mirror/pfsense/downloads/</u>

Dans ce tutorial, nous avons pris la version suivante : pfSense-1.2.2-LiveCD-Installer.iso

- 7. Cliquez sur l'onglet « **Préférences** » en haut à gauche.
- 8. Dans les préférences, cliquez sur « Disque optique »
- 9. Sélectionnez « **Insérer un disque optique** » puis cliquez sur « **Fichier image ISO** » puis cliquez sur la petite icône.
- 10. Cliquez sur « Ajouter » et sélectionnez votre système d'exploitation au format ISO.

tions	
Nouveau Ajouter Enlever Libérer Actualiser	
Nom	✓ Taille
pfSense-1.2.2-LiveCD-Installer.iso	49,16 M
Emplacement : /var/pfsense-iso/pfSense-1.2.2-LiveCD-Installer.iso Attaché à : Non attaché	
Emplacement : /var/pfsense-iso/pfSense-1.2.2-LiveCD-Installer.iso Attaché à : Non attaché	Annuler Mchoi <u>s</u>

11. Une fois le fichier ISO chargé, cliquez sur « Choisir » puis finalement sur « OK »

### 2.3 Activation d'une interface réseau

Pour l'utilisation de PfSense, il est nécessaire d'activer une deuxième interface réseau dans les paramètres de VirtualBox.

- 12. Cliquez sur l'onglet « **Préférences** » en haut à gauche.
- 13. Dans les préférences, cliquez sur « Réseau »
- 14. Cliquez sur l'onglet « **Carte 2** », puis cochez la case « **Activer la carte réseau** ». Définissez le mode d'accès réseau par « **NAT** » puis cliquez sur « **Ok** »
- 15. Il est alors présent possible de lancez le nouveau système d'exploitation en cliquant sur l'onglet « Lancer » se trouvant juste à côté de « Préférences ».

PfSense [en fonction] - Sun \	VirtualBox 🗕 🗆 🗶
<u>M</u> achine <u>P</u> ériphériques <u>A</u> ide	
Welcome to pfSense! 1. Boot pfSense [default] 2. Boot pfSense with ACPI disabled 3. Boot pfSense in Safe Mode 4. Boot pfSense in single user mode 5. Boot pfSense with verbose logging 6. Escape to loader prompt 7. Reboot	f Sense
Select option, [Enter] for default or [Space] to pause timer 10	
	😂 🕢 🗗 🖉 급 🛄 [ 🎯 💽 Ctrl droite

#### 2.4 Installation de PfSense

Une fois PfSense démarré, il est nécessaire pour le premier lancement de choisir la réponse 1 « **Boot PfSense [default]** ».

Dans un premier temps, nous n'allons pas configurer de VLAN, la réponse à la question suivante sera donc « **n** ».

2	PfSense [en fonction] - Sun VirtualBox	
<u>Machine Périphériques Aid</u>	e	
Do you want to set up	VLANs now [yin]?	
	🤤 😳 🗗 🖉 🛄 🔝 Ctr	rl droite

Il est à présent temps de définir les interfaces que nous allons utiliser. Il est nécessaire de définir l'interface LAN ainsi que l'interface WAN et de valider ces changements.



Une fois les interfaces configurées, il est nécessaire d'installer PfSense en dur sur le disque dur.



Il est nécessaire de confirmer que vous voulez réellement installer PfSense.



Les étapes suivantes sont obligatoires. Elles permettent la création des partitions accueillant l'installation de PfSense.

Select the partitions (also known as 'slices' in BSD tradition) you want to have on this disk. For Size, enter a raw size in sectors (1 gigabyte = 2097152 sectors) or a single '\*' to indicate 'use the remaining space on the disk'. to indicate 'use the remaining space on the disk'. Size (in Sectors) Partition Type Active? ] [FreeBSD/Drago] [X] < Ins > < Del > Г× < Add > Accept and Create > < Return to Select Disk > < Revert to Partitions on Disk > You may now wish to install bootblocks on one or more disks. If you already have a boot manager installed, you can skip this step (but you may have to configure your boot manager separately.) If you wish to install pfSense on a disk other than your first disk, you will need to put the bootblock on at least your first disk and the pfSense disk. Disk Drive Install Bootblock? Packet mode? [ad0 1 [X] F 1 Accept and Install Bootblocks > < Skip this Step > < Return to Partition Disk >

Dans l'éventualité ou l'installation vous demande s'il est nécessaire de mettre à jour PfSense, il est possible de refuser du fait que nous venons de prendre la dernière version en ligne.



Une fois les partitions créées et paramétrées, il est nécessaire de redémarrer l'ordinateur pour que les changements soient effectifs.



## 3. La méthode rapide : Utilisation de la version VMWare

Une version VMWare de PfSense est disponible à cette adresse :

http://files.pfsense.org/vmware/pfSense-1.2.3-Prerelease.zip

Dans cette version, le formatage du disque dur ainsi que la création des partitions est déjà fait. L'installation de PfSense est également faite.

***	Velcoмe to pfSense 1.2	. 3-PR	ERELEASE-	-TESTING-	-VERSION-pfSense	on	pfsense	***
WAN LAN	*	-> ->	ем0 ем1	-> ->	0.0.0.0(DHCP) 192.168.1.24			
pfSe	ense console setup							
****	*************							
0)	Logout (SSH only)							
1)	Assign Interfaces							
2)	Set LAN IP address							
3)	Reset webConfigurator	pass	word					
4)	Reset to factory defa	ults						
5)	Reboot system							
6)	Halt system							
7)	Ping host							
8)	Shell							
9)	PFtop							
10)	Filter Logs							
11)	Restart webConfigurat	or						
12)	pfSense PHP shell							
13)	Upgrade from console							
14)	Enable Secure Shell (	sshd)						
Enter	an option:							

Avant tout, il est conseillé de changer l'IP sur la machine de PfSense pour plus de simplicité par la suite. Pour cela, dans le menu de PfSense, tapez le choix 2 : « **Set LAN IP address** ».

```
Enter the new LAN IP address: 192.168.1.24

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 subnet bit count: 24

Do you want to enable the DHCP server on LAN [y|n]? y

Enter the start address of the client address range: 192.168.1.10

Enter the end address of the client address range: 192.168.1.100

The LAN IP address has been set to 192.168.1.24/24.

You can now access the webGUI by opening the following URL

in your web browser:

http://192.168.1.24/
```

Il est à présent possible d'utiliser PfSense. Et oui, déjà.

## 4. Configuration de PfSense

Une fois l'une des méthodes choisies, « **Version complète** » ou « **Version rapide** », il est possible de commencer à faire les configurations dans PfSense.

Pour cela, nous allons donc faire les configurations directement via l'interface Web. Pour cela, il est nécessaire d'ouvrir notre navigateur Web et se connecter à l'url : <u>http://ip\_pfsense</u>

Dans notre cas, nous ferons http://192.168.1.24

Afin de se connecter pour la première fois sur l'interface PfSense, les identifiants par défaut sont :

- Identifiant : admin
- Mot de passe : pfsense

Authentification	requise
?	Le site http://192.168.1.24 demande un nom d'utilisateur et un mot de passe. Le site indique : « , »
Utilisateur :	admin
Mot de passe :	••••••
	OK Annuler

Une fois connecté avec succès, il est possible d'accéder à l'interface Web permettant l'administration de PfSense.

System	Interfaces	Firewall	Services	VPN	Status	Diagnostics
ystem Ove	rview					
ystem informati Name	pn pfser	ise.local				
/ersion	1.2.3 built	-PRERELEASE-TEST on Wed Feb 11 15:49:	ING-VERSION 20 EST 2009			
Platform	pfSer	nse				
Jptime	01:0	Ō				
State table size	2/10 Show	000 states				
MBUF Usage	517 /	780				
CPU usage	_	1%	6			
Memory usage		37	%			
SWAP usage		) 0%	fo			
Disk usage	-	4%	6			

## 4.1 Configuration générale

Afin de commencer les configurations de base, rendez-vous dans l'onglet « **General Setup** » présent dans « **System** »

Ici se trouve donc la configuration générale de **Pfsense**.

Il est possible de rentrer le nom de la machine ainsi que son domaine les champs « **Hostname** » et « **Domain** ».

Il est également possible de rentrer l'adresse IP des serveurs DNS dans le champ « **DNS Servers** ». Il est nécessaire également de décocher la case « **Allow DNS server list to be overridden by DHCP/PPP on WAN** » du fait que cette option provoque des conflits puisque les DNS des clients ne sont plus PfSense, mais un DNS du WAN inaccessible par le LAN.

-----

Le menu de PfSense est réellement un menu extrêmement complet. Il permet en quelques clics d'avoir accès à l'ensemble des configurations disponible.

*Se	n <mark>se</mark>	100	New event: Ple	ase click to confi	rm.	SEEK OF THE
System	Interfaces	Firewall	Services	VPN	Status	Diagnostics
System :	Permet de faire	e l'ensemble	des réglages co	ncernant le s	système en lui	-même.
Interfaces :	Permet la gesti	ion des inter	faces réseau (La	n et Wan).		
Firewall :	Permet de met	tre en place	toute les règles	servant de F	irewall.	
Services :	Permet d'active pouvant se trai	er de nombr nsformer en	eux service faisa serveur/relai Dł	nt de PfSens HCP ou bien	se un firewall r encore en por	nultifonction tail captif.
VPN :	Permet d'active	er/désactive	r le VPN, de met	tre en place	une sécurité v	via IPSec.
Status :	Permet de voir	le statut de	l'ensemble des	configuratio	ns.	
Diagnostics :	Permet de don	ner des outil	ls permettant le	diagnostic d	'un quelconqu	ie bug

### 4.2 Sécurité

Pour des raisons de sécurité évidentes, il est nécessaire de modifier le couple login/mot de passe par défaut (admin/pfsense). Cela se réalise dans l'onglet « General Setup » de l'option « System »

Username	NoCrash If you want to change the use	rname for accessing the webGUI, enter it here.
Password	If you want to change the pas	(confirmation) sword for accessing the webGUI, enter it here twice.

Afin d'accroitre encore un peu la sécurité, il est nécessaire d'activer la connexion sécurisé sur ces pages grâce à l'utilisation de SSL. Avant toute chose, dans le cas ou cela ne serait pas encore fait, il est nécessaire de créer votre certificat pour pouvoir avoir des connexions sécurisées.

Rendez vous dans l'onglet « Advanced » du menu « System ». Dans la partie « webGUI SSL certificate/key », cliquez sur « Create » pour générer le certificat et répondez aux questions posées

webGUI SSL certificate/key	
Certificate	Paste a signed certificate in X.509 PEM format here. Create certificates automatically.
Кеу	Paste an RSA private key in PEM format here.
uobEIII EEL contificato/kou	Save
Certificate	HI ID 13 CCAoug An IEAg1 JAONE Ji / JNNE 7MA06CS q6S Ib 3D QEBB QUAMGox C = AJB gNU         HI ID 13 CCAoug An IEAg1 JAONE Ji / JNNE 7MA06CS q6S Ib 3D QEBB QUAMGox C = AJB gNU         BATT ALS 2M (Sever QTV DUQ IEW MU JETMEB CA LUEBANKU 3V = 2 FYZ 3VI = = EVMBMGA LUE         ChMET m9D cmFs a CEDb 3 JMERAND gYD VQQLEwd 0b 0NY YXN oHRAND gYD VQQDEwd 0b 0NY         YXN 0MB 4XDT ASHD YXND IWIT AMTO SYMT OW = 2 FYZ 3VI = = EVMBMGA LUE         LI Lc caAb gYD BgY ALS SHEMBEQ QYD VQQUEW = ALXIX Y, ANUW HERWEW EVYD VQUEK mod         b0NY YXN 0 IENv cn AxED AOB gYD WAI 6 JAO GB AWN Ahr Dp 9 Gate (2 FRTMING Vh st D AL         g28 00 QYUK 0 I INV CHAQEB QAD gYD MI 6 JAO GB AWN Ahr Dp 9 Gate (2 FRTMING Vh st D AL         Paste a signed certificate in X.509 PEM format here. Create certificates automatically.
Кеу	BEGIN RSA PRIVATE KEY HICXAIBAAKBgQDZwIaw6fkr.XpEXkUsRs01YfKwwc491o5LLw8rHX0m051+D1HH 98UHrvISPds5c2i++H+1y06Dv2jAlMJ9PUNsA0f64T2dUFYKTUjIRNymf1Ph8J03 62bHFvpe6NteydouUq481LtDf0evzPRUebCkdgo4/pY03JTxmq098cC16Q1DAQAB Ac6BAKIsAQ2iaC651BF0gvrUYKA60PTR097or9gmf1kf69jyH089u0MChpN 200pysQX+FISL+2Lwf0sNSogiIn.MfuQ7TqcPN0H05r5xbTD39MIGI6i1G308sn6X U98mpLv2612dDT75/bY03zPw5LH19k6X5H+g08+omShi1jGRAkDA8h7x1cCFAlks 

Save

Paste an RSA private key in PEM format here.

Puis, une fois le certificat créé et sauvegardé, il est nécessaire d'activer l'**HTTPS** et de spécifier le port dans « **webGui port** » (Port **443**).

webGUI protocol	◎ HTTP
webGUI port	443 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.

Puis cliquez sur « Save » afin de valider les modifications.

Après validation, la page va se recharger automatiquement et nous rediriger vers une page sécurisée via SSL (https).



A présent, rendez-vous dans l'onglet « Advanced » présent dans « System »

A partir d'ici, il est possible d'activer la connexion à distance via SSH. Cette connexion à distance va permettre d'administrer PfSense à distance sans passer par l'interface graphique permettant une configuration accrus et de manière sécurisée.

Secure Shell	iecure Shell				
	Enable Secure Shell				
	Disable Password login for Secure Shell (KEY only)				
SSH port	22 Note: Leave this blank for the default of 22				
Authorizedkeys	Paste an authorized keys file here.				
	Save				

Cochez la case « **Disable Password login for Secure Shell (Key only)** » permet comme son nom l'indique de n'autoriser que les connexions SSH par clé et non pas par mot de passe. Les clés autorisées devront se trouver dans le champ « **Authorizedkeys** »

## 4.3 Configuration simplifié

Afin de ne pas vous perdre dans l'ensemble des configurations qu'il est possible de mettre en place, il est possible d'utiliser l'assistant de configuration. Pour cela, cliquez sur l'onglet « **Setup Wizard** » présent dans « **System** ». Cet assistant va reprendre les pages de configuration importante pour une mise en place et une configuration rapide de PfSense.

**1.** La première étape va reprendre les étapes de la configuration globale.

General Information		
Hostname:	pfsense EXAMPLE: myserver	
Domain:	nocrash-corp.com EXAMPLE: mydomain.com	
Primary DNS Server:	192.168.1.1	
Secondary DNS Server:		

#### On this screen you will set the General pfSense parameters.

-N	lext -

La deuxième étape reprend également les étapes de la configuration globale.
 Please enter the time, date and time zone.

Time Server Information	
Time server hostname:	0.pfsense.pool.ntp.org Enter the name of the time server.
Timezone:	Etc/UTC

Next

3. La troisième étape reprend l'étape de configuration des réseaux. (Lan et Wan)

On this screen we will configure the Local Area Network information.

Configure LAN Interface		
LAN IP Address:	192.168.1.24 Type dhcp if this interface uses DHCP to obtain its IP address.	
Subnet Mask:	24 💌	
	Next	

**4.** La quatrième étape quand à elle consiste en la configuration des mots de passe permettant l'accès à PfSense via l'interface graphique ou via SSH.

# 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:	••••••	
Admin Password AGAIN:	•••••••	

Next