

Mise en place d'un pare-feu PfSense

Installation et configuration d'un pare-feu PfSense 2.2 sous
Proxmox

ANATOLE BILLET

09 avril 2016
Version : 1.02

Mise en place d'un pare-feu PfSense

Installation et configuration d'un pare-feu PfSense 2.2 sous Proxmox

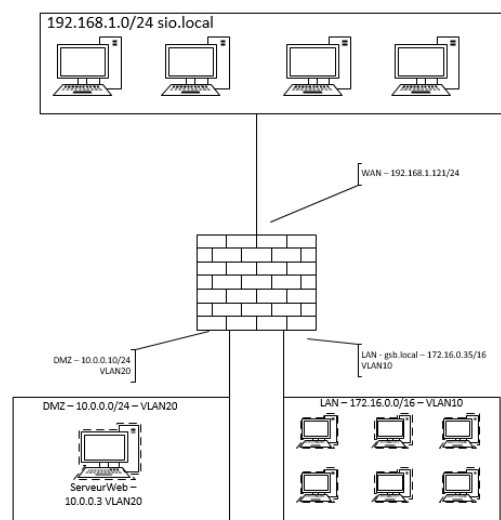
Avant de commencer...

Prérequis :

-Un environnement virtualisé basé sous Proxmox

Objectif :

Tutoriel permettant la mise en place d'un Pare-feu administrant les connexions réseaux des VM du serveur Proxmox le pare-feu comportera ainsi 3 interfaces, une pour le WAN, une pour un réseau LAN dans lequel les autres serveurs seront placés et une DMZ pour y placer le serveur WEB



Code couleur :

-Bleu pour les commandes

-Vert pour les noms et chemins des fichiers

-Italic pour les descriptions et anecdotes.

Table des matières

AVANT DE COMMENCER...	1
PREREQUIS :	1
OBJECTIF :	1
CODE COULEUR :	1
1/CONFIGURATION DE BASE.....	2
CONFIGURATION SOUS PROXMOX.....	2
CONFIGURATION DU BOND.....	2
CREATIONS DES VLANS.....	3
3/INSTALLATION DE PFSense.....	3
4/CONFIGURATION DE BASE SOUS PFSense.....	5
5/ACCES A L'INTERFACE WEB.....	6
MODIFICATION DES INTERFACES :	6
.....	7
6/ DIFFERENTES REGLES NECESSAIRES A NOTRE CONFIGURATION :	7
7/ PROBLEME DE CHECKSUM DU AUX PILOTES VIRTIO :	8

1/Configuration de base

Avant de commencer il va falloir mettre en place l'infrastructure du « réseau virtuel » sous proxmox, pour ce faire nous allons utiliser OpenVirtualSwitch(OVS) qui a pour rôle de remplacer les paramètres réseaux de base de linux par des paramètres prenant en charge des normes tels que le 802.1q et une meilleure compatibilité avec un environnement virtualisé. Une fois cela fait nous créerons un BOND permettant de lier les 2 cartes réseau en une dans le but de faire de la répartition de charges et de gagner en performance.

A partir de ce bond nous allons mettre en place une carte virtuelle « bridge » découper par des VLANs dans le but de séparer le réseau LAN et la DMZ.

Avant de commencer installez sous votre proxmox le Paquet d'OVS :

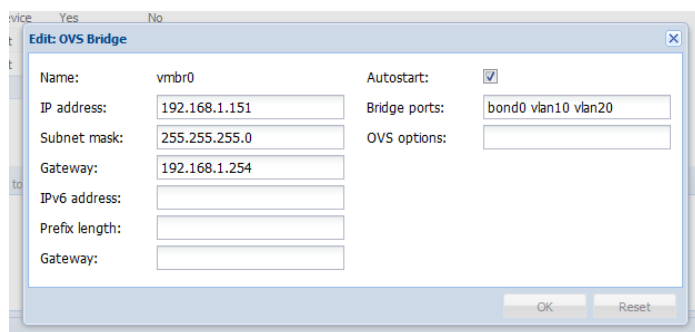
apt-get install openvswitch-switch

Nous utiliserons l'interface graphique pour configurer notre réseau car curieusement après de nombreux essais Proxmox refuse de prendre une configuration manuelle du fichier **/etc/network/interfaces**

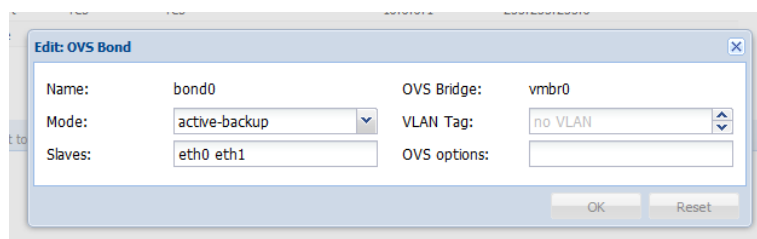
Configuration sous Proxmox

Configuration du Bond

Sous l'interface web de Proxmox se rendre sur le Nœud désiré, puis chercher l'onglet « network », dans cet onglet choisissez « create », puis « OVS bridge » configurez-le de la façon nécessaire (ici notre Bridge hébergera les 2 VLANs et sera par défaut l'accès réseau du WAN) :



Puis de nouveau choisissez « create », puis « OVS Bond » et configurez-le ensuite de la façon suivante :

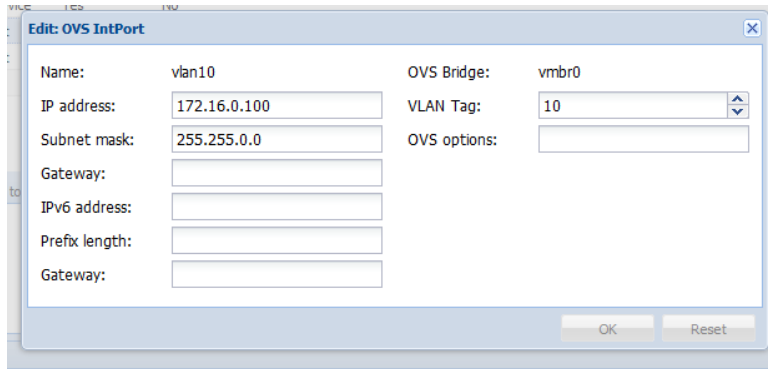


Puis ajoutez le BOND à votre OVS Bridge.

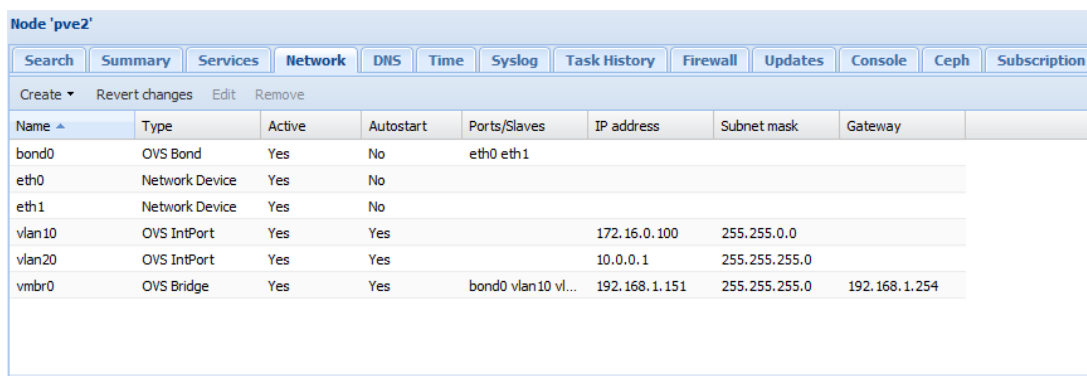
Créations des Vlan

Nous devons maintenant configurer 2 vlan pour le LAN et la DMZ ils auront respectivement les numéros 10 et 20.

Pour ce faire, toujours dans l'onglet network créez un nouvel « OVSIntPort », sélectionner l'OVS Bridge créer précédemment et stipulez le numéro de VLAN :



Vous devriez ainsi avoir une configuration similaire à la mienne :



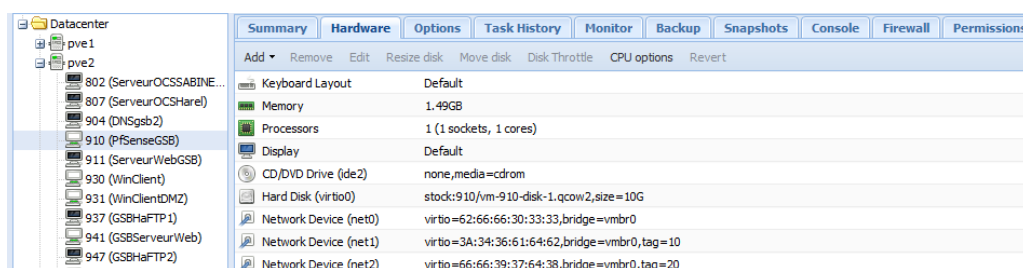
Name	Type	Active	Autostart	Ports/Slaves	IP address	Subnet mask	Gateway
bond0	OVS Bond	Yes	No	eth0 eth1			
eth0	Network Device	Yes	No				
eth1	Network Device	Yes	No				
vlan10	OVS IntPort	Yes	Yes		172.16.0.100	255.255.0.0	
vlan20	OVS IntPort	Yes	Yes		10.0.0.1	255.255.255.0	
vibr0	OVS Bridge	Yes	Yes	bond0 vlan10 vl...	192.168.1.151	255.255.255.0	192.168.1.254

Relancez votre serveur.

3/installation de PfSense

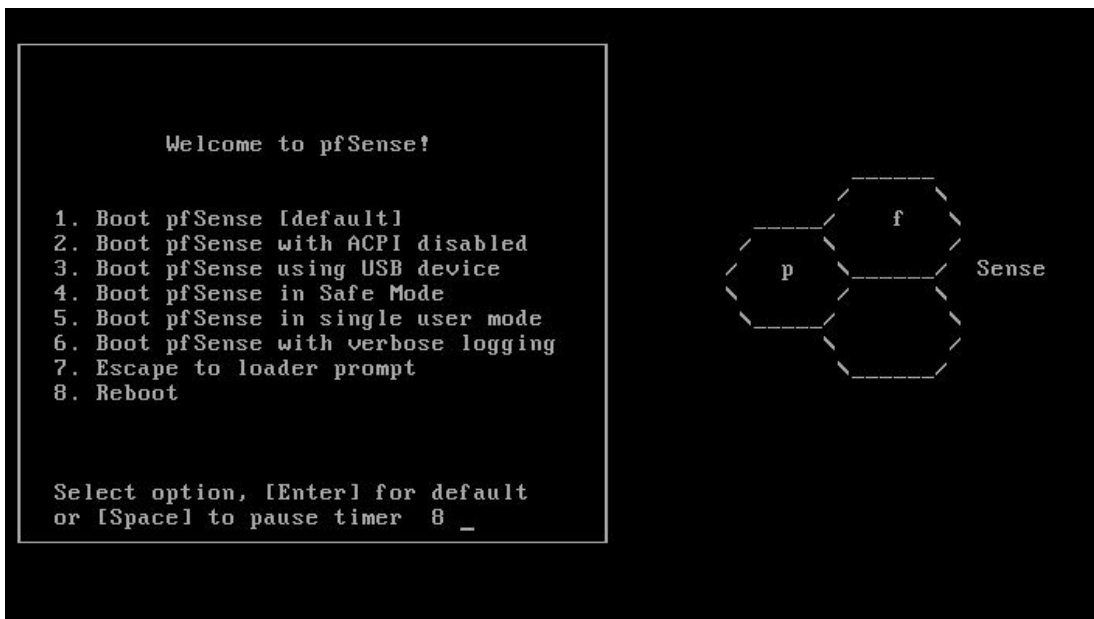
Lors de la création de la VM PfSense, il est nécessaire d'ajouter les 3 cartes réseaux (LAN, WAN et DMZ).

Ainsi ajoutez 3 cartes réseau connectées à l'OVS bridge créer précédemment et pour 2 d'entre elles (correspondant à LAN et DMZ) ajoutez le « TAG » du VLAN requis.

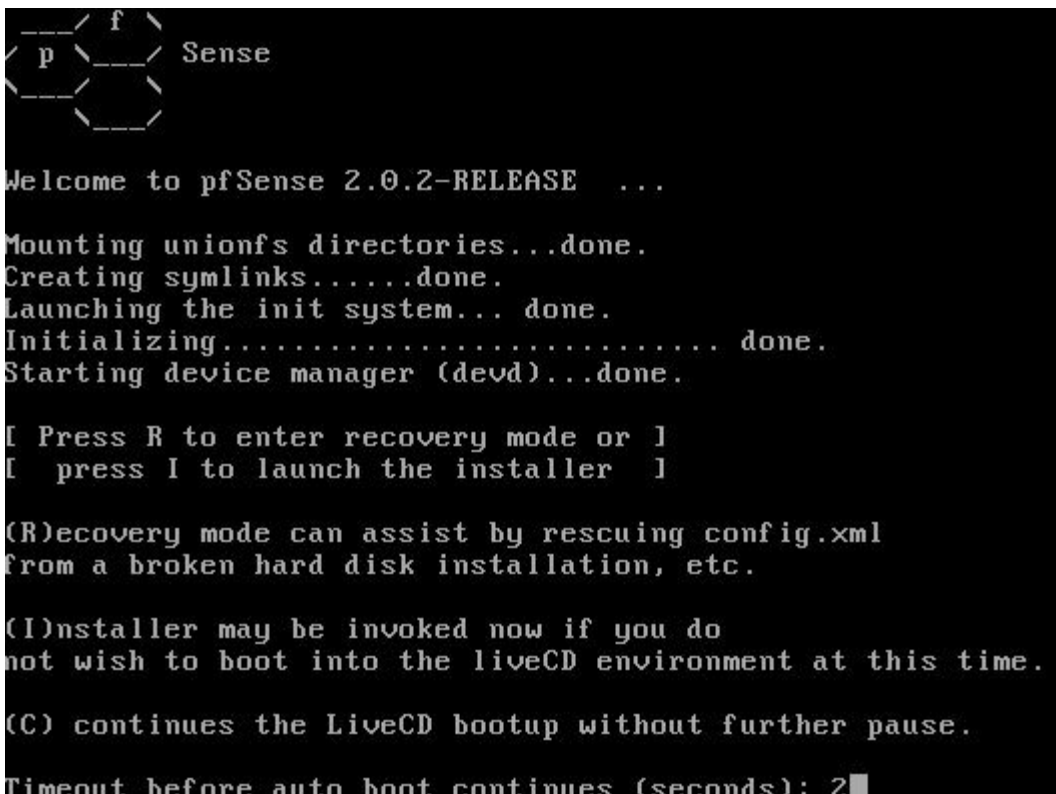


En termes de configuration requise, je fais tourner Pfsense sur une VM disposant d'un processeur, 512 Mo de RAM et 8Go de disque, Pfsense se contente de très peu, nous le verrons plus loin.

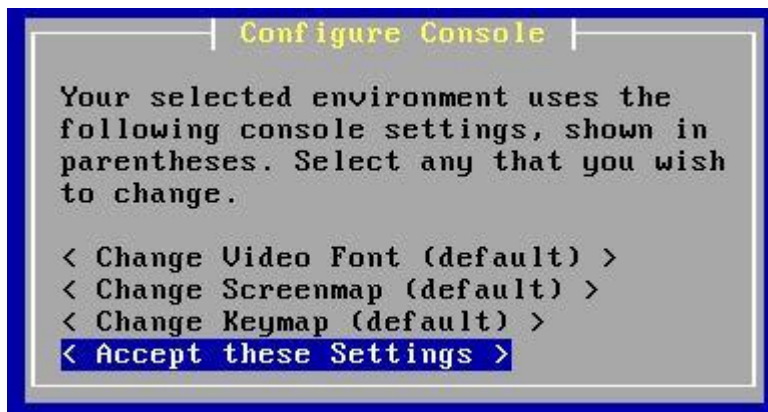
Lors du démarrage de l'ordinateur avec le CD ou l'ISO monté, un menu de boot apparaît. Selon les besoins on peut choisir de démarrer Pfsense avec certaines options activées. Si aucune touche n'est appuyée, Pfsense bootera avec les options par défauts (choix 1) au bout de 8 secondes.



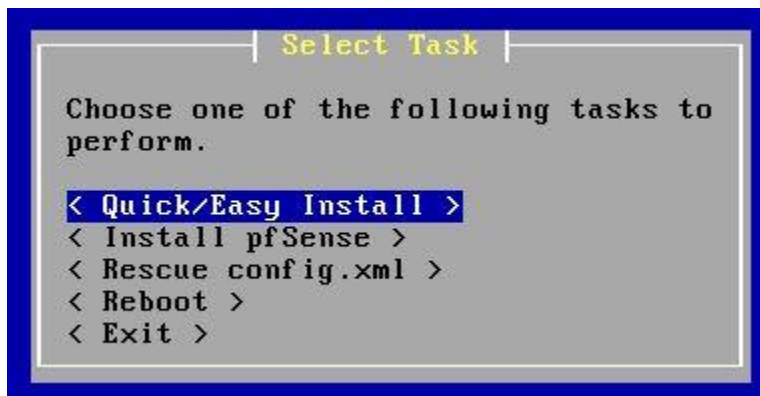
Appuyez sur « **Entrée** » pour booter avec les options par défaut.



Appuyer rapidement sur la touche « **I** » afin de démarrer l'installation.



L'installation démarre, dès le premier écran nous pouvons régler différents paramètres notamment la police d'écriture et l'encodage des caractères. Ces options sont utiles pour des cas bien particuliers. Nous n'y toucherons donc pas. On sélectionne « **Accept these Settings** ».



On choisit « **Quick/Easy Install** » pour procéder à l'installation rapide.

Le message qui suit, nous informe que le disque dur sera formaté et toutes les données présentes dessus seront effacées. On sélectionne « **OK** » et on continue.

L'installation débute et copie les fichiers nécessaires sur le disque dur, nous devons par la suite choisir quel type de kernel nous voulons installer, étant sur un ordinateur nous choisissons le « **Standard Kernel** ».

Une fois l'installation finie, on choisit « **Reboot** » et nous redémarrons sur notre nouvelle installation.

N'oubliez pas de sortir le CD ou l'ISO de Pfsense avant de redémarrer.

4/configuration de base sous Pfsense

Lors du premier démarrage de Pfsense, il faut configurer les différentes interfaces (WAN, LAN, DMZ, etc.), il faut donc bien repérer vos différentes cartes réseaux afin de ne pas vous tromper dans votre configuration auquel cas vous n'aurez pas accès à l'interface web et votre pare-feu ne fonctionnera pas.

Pfsense vous affiche vos différentes cartes réseaux avec leur adresse MAC, ce qui vous permettra de les différencier :

```
WAN (wan)      -> vtnet0      -> v4: 192.168.1.121/24
LAN (lan)      -> vtnet1      -> v4: 172.16.0.35/16
DMZ (opt1)    -> vtnet2      -> v4: 10.0.0.10/24
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
```

Ici Pfsense vous demande si vous souhaitez configurer les VLANs Entrez « n » pour « no » car les Vlan sont déjà attribués.

Puis attribuer les carte réseau « taggées » aux VLANs aux interfaces (WAN, LAN et OPT1 deviendra notre DMZ) et donnez-leurs L'IP correspondant à votre configuration.

5/accès à l'interface web

De base Pfsense bloque tout ce qui n'est pas autorisé ainsi l'accès à l'interface de configuration WEB est bloquer via le WAN pour désactiver temporairement le Pare-Feu suivez les étapes suivantes :

```
5) Reboot system          11) Disable Secure Shell (SSH)
6) Halt system            15) Restore recent configura
7) Ping host              16) Restart PHP-FPM
8) Shell

Enter an option: 8

[2.2-RELEASE][root@bm-fw.bmprive]/root: pfctl -d
pfctl: pf not enabled
```

1. Connectez-vous à votre serveur PfSense
2. Faire le choix "8) Shell"
3. Saisir : **pfctl -d**
(d=disable, le tiret en qwerty est sur la touche")" en azerty)
4. Faire ENTREE
5. Le message suivant apparaît : "pfctl: pf not enabled"
6. Entrez l'une des IP dans votre navigateur web pour accéder à l'interface elles sont affichées en haut de l'écran.

Attention : PF sera réactivé automatiquement si vous validez un formulaire dans l'interface web, à n'importe quel endroit. Enfin, pour réactiver PF à la main : **pfctl -e** (pour enable), sinon faites un reboot.

Modification des interfaces :

Il vous sera également peut-être nécessaire de configurer vos interfaces, Pour cela cliquez sur Interfaces → « nom de votre interface », OPT1 Pourras ainsi être renommé en DMZ et recevoir une IP.

General configuration

Enable **Enable Interface**

Description
 Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC address
 This field can be used to modify ("spoof") the MAC address of this interface
 Enter a MAC address in the following format: xxxxxxxxxx or leave blank

MTU
 If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

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.

Speed and duplex - Show advanced option

Static IPv4 configuration

IPv4 address /

IPv4 Upstream Gateway - or add a new one.
 If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the link above.
 On local LANs the upstream gateway should be "none".

Private networks

Block private networks
 When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

Block bogon networks
 When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by

6/ Différentes règles nécessaires à notre configuration :

Voici les règles que j'ai configuré pour chaque interface de mon Pare-Feu, permettant la mise en place de la configuration (WAN/LAN/DMZ) :

Il est bon de noté que les règles sont lues de haut en bas et que la première règle lue à la priorité.

Pour le WAN :

		Floating	WAN	LAN	DMZ					
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input type="checkbox"/>		IPv4 *	*	LAN net	*	*	none		interdit l'accès depuis le Wan vers le LAN	
<input type="checkbox"/>		IPv4+6 *	WAN net	*	*	*	none		Autorise le Wan a toute les règles	

Pour le LAN :

Floating WAN LAN DMZ										
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input checked="" type="checkbox"/>	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	

Pour la DMZ :

Floating WAN LAN DMZ										
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input type="checkbox"/>	IPv4 *	DMZ net	*	! LAN net	*	*	none		autorise LAN vers DMZ, interdit DMZ vers LAN	

Ne pas oublier pour chaque VM que vous voulez manager avec Pfsense d'ajouter le bon Bridge avec le bon TAG de Vlan et d'ajouter l'IP de l'interface du pare-feu correspondant en Passerelle

7/ Problème de Checksum dû aux pilotes Virtio :

Les pilotes Virtio entraîne un souci de checksum (vérification d'intégrité des données) au niveau de la carte réseau, ainsi il est nécessaire à chaque démarrage de PfSense de prendre soins de rentrer la commande suivante (dans le Shell de pfsense) pour chaque interface de sorte à avoir des performances de trafique correctes :

```
ifconfig vtnet0 -rxchecksum
```

```
ifconfig vtnet1 -rxchecksum
```

```
ifconfig vtnet2 -rxchecksum
```