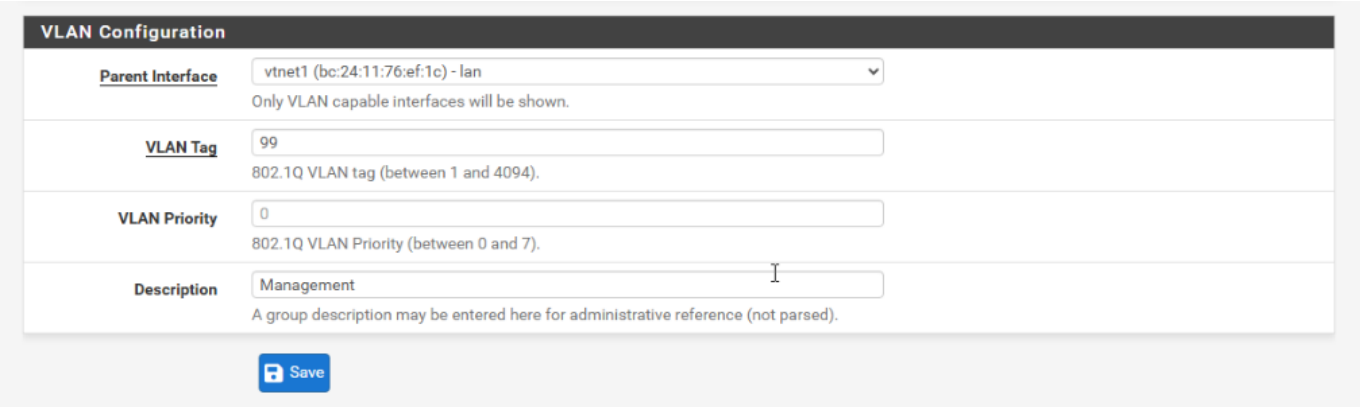
Sécurisation, supervision et services réseau - Proxmox

I - Cloisonnement et durcissement du réseau

I/I - VLAN Management

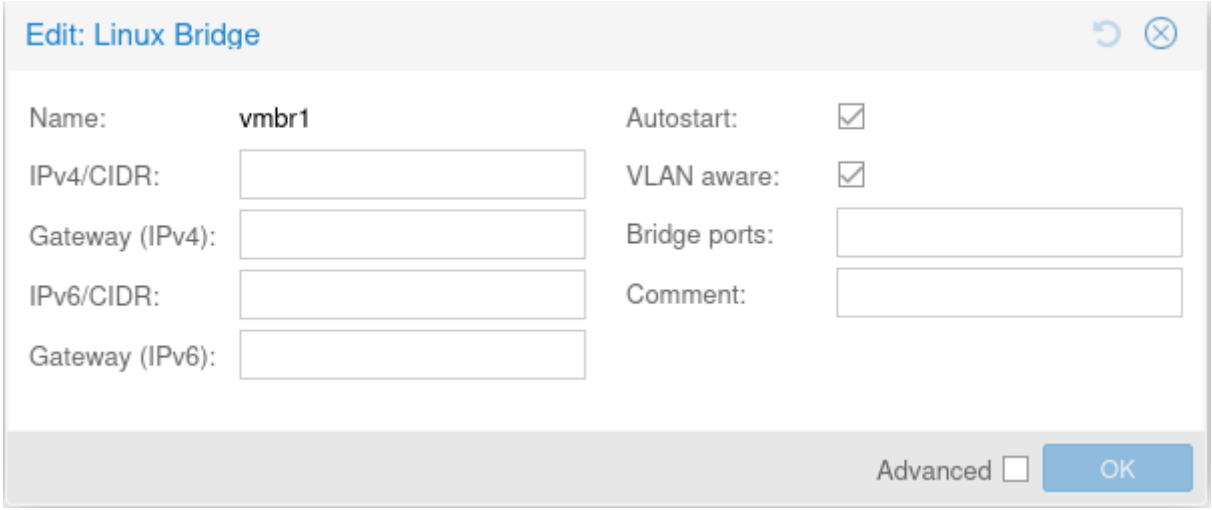
I/I/I - Création du VLAN Management

Tout d'abord, il va falloir créer une interface VLAN 99 qui va correspondre au VLAN Management, pour cela il va falloir aller sur: **Interfaces -> Assignements -> VLANs** puis cliquer sur **Add**.



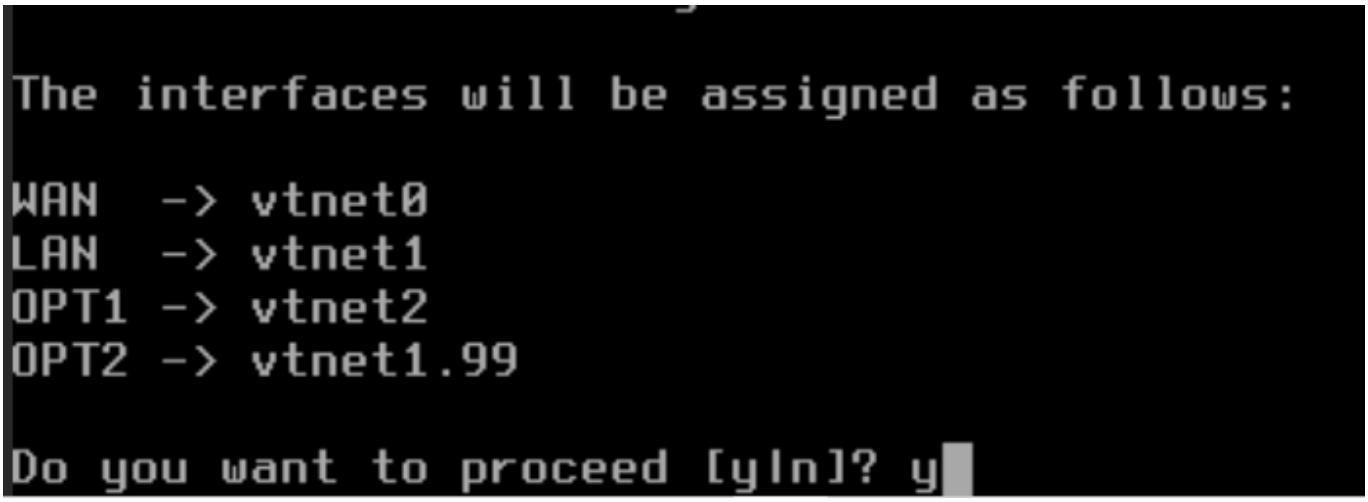
Après l'avoir configuré, clique sur **Save**.

Il ne faut pas oublier d'activer le support de VLANs sur l'interface *vmbr1* qui correspond à l'interface LAN. Pour cela il va falloir se rendre sur: **Datacenter -> pve -> System -> Network**. On clique sur l'interface *vmbr1*, puis sur le bouton **Edit** et on coche la case **VLAN aware**.



I/I/II - Configuration du VLAN MAnagement sur pfSense

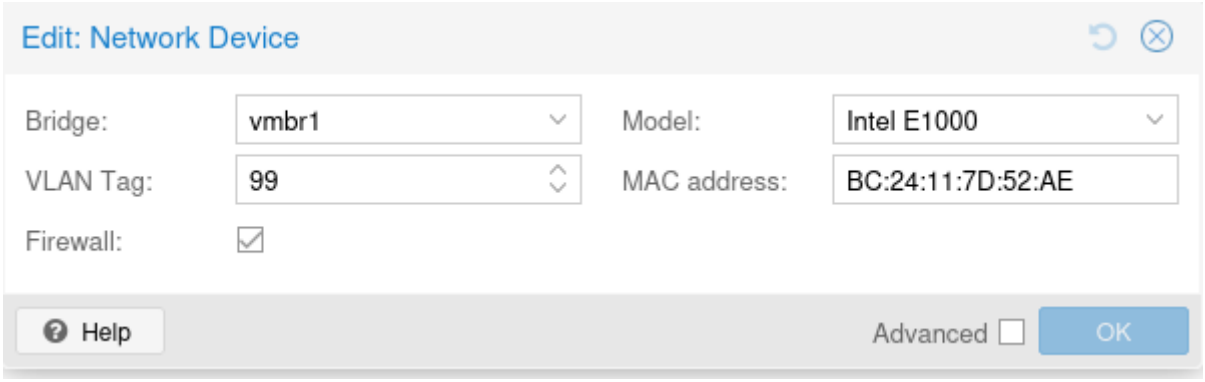
On se rend sur le pfSense puis on introduit l'option *1) Assign Interfaces* en tapant le chiffre 1. Le rendu final doit être le suivant:



Ensuite il va falloir configurer l'adresse IP du VLAN Management. Pour cela il faut choisir l'option *2) Set interface(s) IP address* en tapant le chiffre 2. Le rendu final doit être le suivant:

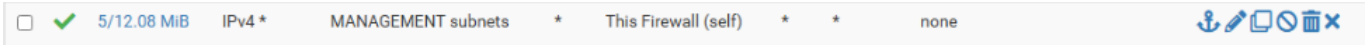
I/I/III - Ajout d'une VM Windows Admin

On va créer une VM Windows 11 avec la configuration de la carte réseau suivante:

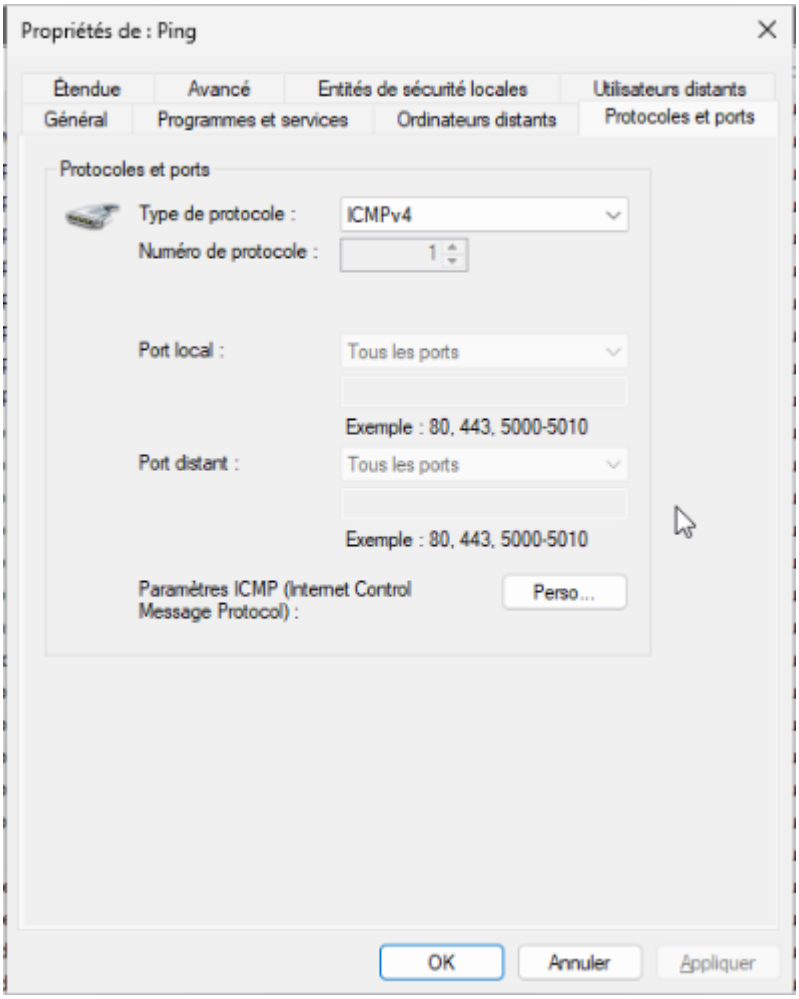


Et la configuration IP suivante:

Pour communiquer avec notre passerelle, il va falloir créer la règle pare-feu suivante:



Ainsi que la création d'une règle ping sur le pare-feu de la VM Admin:



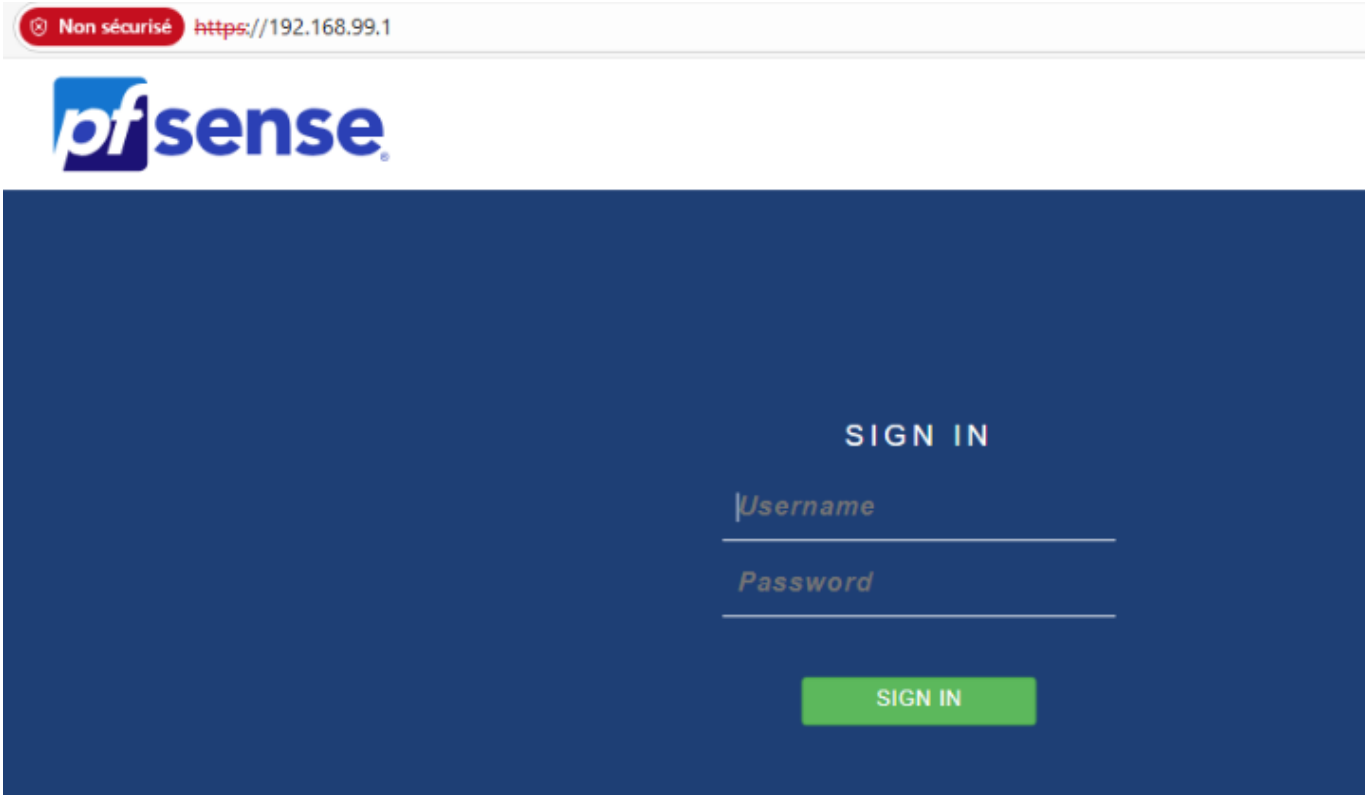
Test de Ping de la VM Admin vers sa passerelle par défaut:

```
C:\Users\Windows11-client>ping 192.168.99.1

Envoi d'une requête 'Ping'  192.168.99.1 avec 32 octets de données :
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64
Réponse de 192.168.99.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.99.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Connexion à l'interface de configuration du pfSense:



I/I/IV - Configuration du pfSense pour limiter l'accès à lui-même

Sur pfSense :

- **System -> Advanced -> Admin Access**
- Activer uniquement HTTPS
- Limiter l'écoute à Management. Pour cela il va falloir créer des règles pare-feu sur toutes les interfaces sauf Management:

☐		0/0 B	IPv4 TCP	LAN subnets	*	This Firewall (self)	*	*	none

- Désactiver HTTP et SSH pour les autres interfaces. Tout d'abord on crée l'Alias suivant. Pour cela il faut se rendre sur **Firewall -> Aliases -> Ports**:

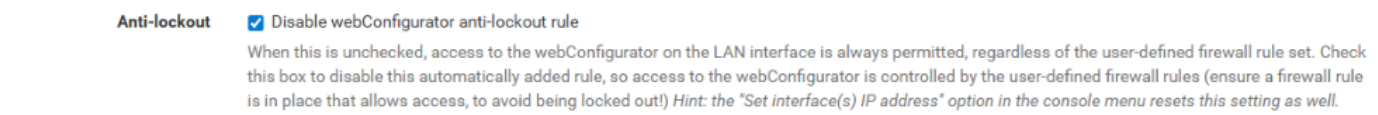
Firewall Aliases Ports

Name	Type	Values	Description	Actions
WEB_PORTS	Port(s)	80, 443		

Puis sur chaque interface, on crée les règles suivantes:

☐		0/0 B	IPv4 TCP	*	*	This Firewall (self)	WEB_ PORTS	*	none	
☐		0/0 B	IPv4 TCP	*	*	This Firewall (self)	22 (SSH)	*	none	

Normalement, les autres appareils peuvent encore se connecter sur l'interface de configuration du pfSense. Pour règler ce problème il va falloir se rendre sur **System -> Advanced -> Admin Access**. Et on coche l'option suivante:



II - Mise en place d'un DNS local et d'un proxy

II/I - DNS local sur pfSense

Tout d'abord il va falloir activer le DNS Resolver (Unbound) depuis l'interface de configuration du pfSense. Puis on se rend sur **Services -> DNS Resolver** et on coche *Enable DNS Resolver*.

Ensuite, sur *Network Interfaces*, on va selectionner les interfaces LAN, MAnagement et Localhost.

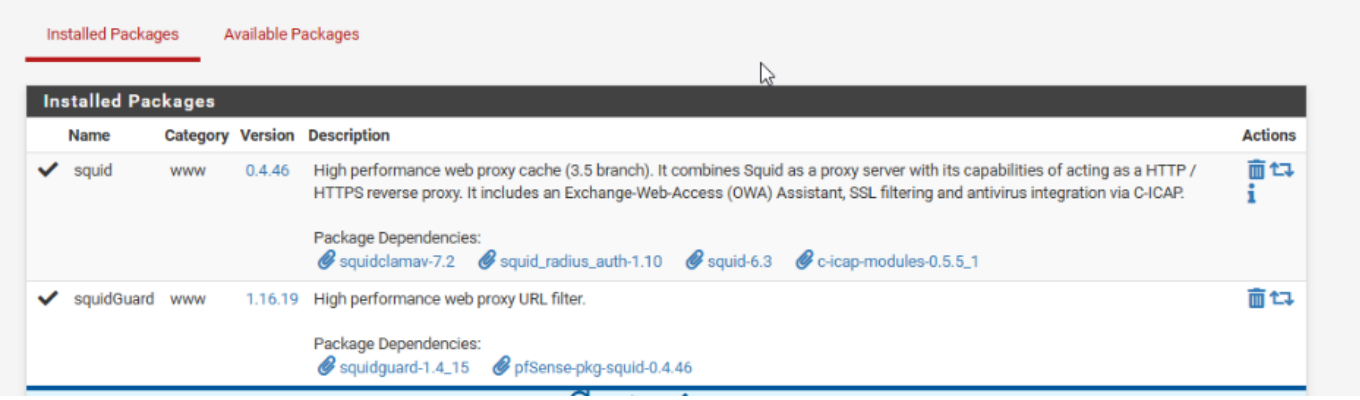
Enfin, il faut cocher *Register DHCP leases in the DNS Resolver* et *Register DHCP static mappings in the DNS Resolver*.

Pour ajouter les enregistrements manuels, on se rend sur: **Services -> DNS Resolver -> onglet Hosts Overrides** et on ajoute les lignes suivantes:

II/II - Proxy Squid + filtrage SquidGuard

II/II/I - Installation de Proxy Squid

Pour installer Proxy Squid, il faut se rendre sur: **System -> Package Manager -> Available Packages** et on installe *squid* et *squidGuard*.



II/II/II - Configuration de Proxy Squid

Tout d'abord on se rend sur: **Services -> Squid Proxy Server** et on le configure de la façon suivante:

- Cocher *Enable Squid Proxy.*
- Cocher *Allow Users on interface*.
- Cocher *Transparent HTTP Proxy*.

- *Transparent Proxy Interface(s)* : LAN.

II/II/III - Configuration de SquidGuard

Tout d'abord on se rend sur: **Services -> SquidGUard Proxy Filter** et on le configure de la façon suivante:

- Cocher *Enable*.
- Cocher *Enable GUI log*.
- Cocher *Enable log*.
- Cocher *Blacklist* et renseigner l'url http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz dans la zone de texte *Blacklist URL*.
- Cliquer sur *Save*.
- Aller dans l'onglet **Services -> SquidGUard Proxy Filter -> Blacklist** et télécharger la blacklist http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz en appuyant sur *Download*.

Blocage de certains sites

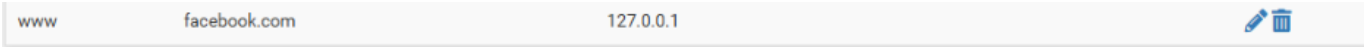
Pour bloquer certaines catégories de sites Web, il va falloir se rendre sur **Services -> SquidGUard Proxy Filter -> Common ACL**. Puis on clique sur le *+*:

On va *deny* les catégories *social_networks*, *adult* et *malware*.

- *Cocher Do not allow IP-Addresses in URL* ainsi que *Log* puis *Save*.

- Redémarrer le service squid et squidGuard en allant dans **Status -> Services**.

Sur la VM client du LAN, on peut encore accéder à http://facebook.com même après avoir vidé le cache avec la commande `ipconfig /flushdns`. Pour le bloquer, il va falloir se rendre sur **Services -> DNS Resolver -> onglet Hosts Overrides** et on ajoute un nouveau avec la configuration suivante:



Si on ressaie d'accéder au site, cela ne fonctionnera pas.

III - Supervision et journalisation centralisée

III/I - Création d'une VM Debian

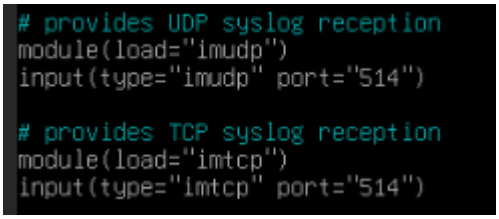
Tout d'abord, il faut créer une VM Debian sur le LAN avec la configuration suivante:

- Nom : Serveur-Logs
- Bridge : vmbr1
- Adresse IP : 192.168.1.20/24
- Passerelle : 192.168.1.1
- DNS : 192.168.1.1

III/II - Installation et configuration de rsyslog

Pour installer *rsyslog*, il faut utiliser la commande suivante `apt install rsyslog`.

Ensuite, on utilise la commande `nano /etc/rsyslog.conf` pour décommenter les lignes suivantes:



Et on redémarre *rsyslog* avec la commande `systemctl restart rsyslog` et `systemctl enable rsyslog`.

Il va falloir ensuite ouvrir le port 514 TCP et UDP sur le pfSense:

Configuration de pfSense pour envoyer ses logs

Tout d'abord il faut se rendre sur **Status -> System Logs -> Settings** et faire la configuration suivante:

- Cocher *Enable Remote Logging*.
- *Remote log servers* : 192.168.1.20/24.
- Sélectionner System Events, Firewall Events, VPN Events sur *Remote Syslog Contents*.
- *Save*.

On peut vérifier la réception sur la Debian avec la commande suivante `sudo tail -f /var/log/syslog`.

III/III - ntopng (supervision graphique)

Pour avoir une supervision graphique, on va utiliser le logiciel *ntopng*. Pour cela, il faut taper les commandes suivantes sur le serveur de logs:

```
get https://packages.ntop.org/apt/bullseye/all/apt-ntop.deb
apt install ./apt-ntop.deb
apt-get clean all
apt-get update
apt-get install ntopng
```

Pour accéder à cette interface, j'utilise l'URL *192.168.1.20:3000* sur la VM client sur le LAN.

IV - Sauvegarde, restauration et automatisation

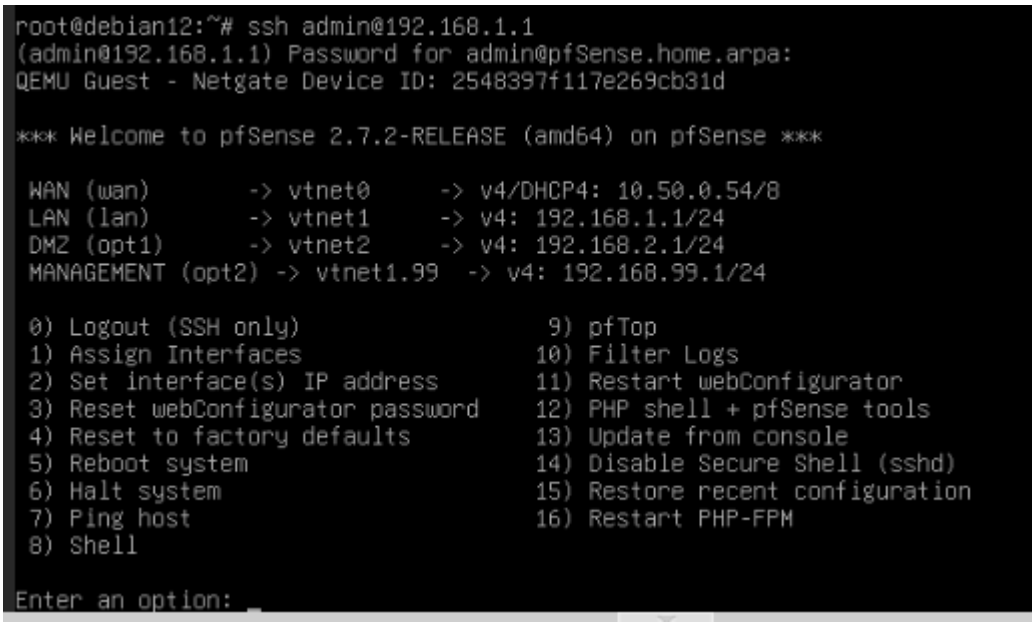
IV/I - Activation du service SSH

Sur l'interface de configuration du pfSense, on se rend sur **System -> Advanced -> Admin Access** et on coche *Secure Shell Server*. Ensuite sur le pfsense, on choisit l'option *8) Shell* et on tape la commande suivante:

Ensuite, on va créer une clé SSH et la copier sur l'entrée admin de 192.168.1.1, pour cela on va taper les commandes suivantes sur le serveur de logs:

```
ssh-keygen
ssh-copy-id admin@192.168.1.1
```

On peut maintenant se connecter via SSH au pfSense:



IV/II - Sauvegarde automatisée

Tout d'abord on crée le repértoire sur le serveur de logs avec la commande `mkdir /backup`. Puis la commande `crontab -e` et on tape la ligne suivante:

```
0 20 * * * scp admin@192.168.1.1:/cf/conf/config.xml /backup/pfsense-$(date +\%F) .xml
```