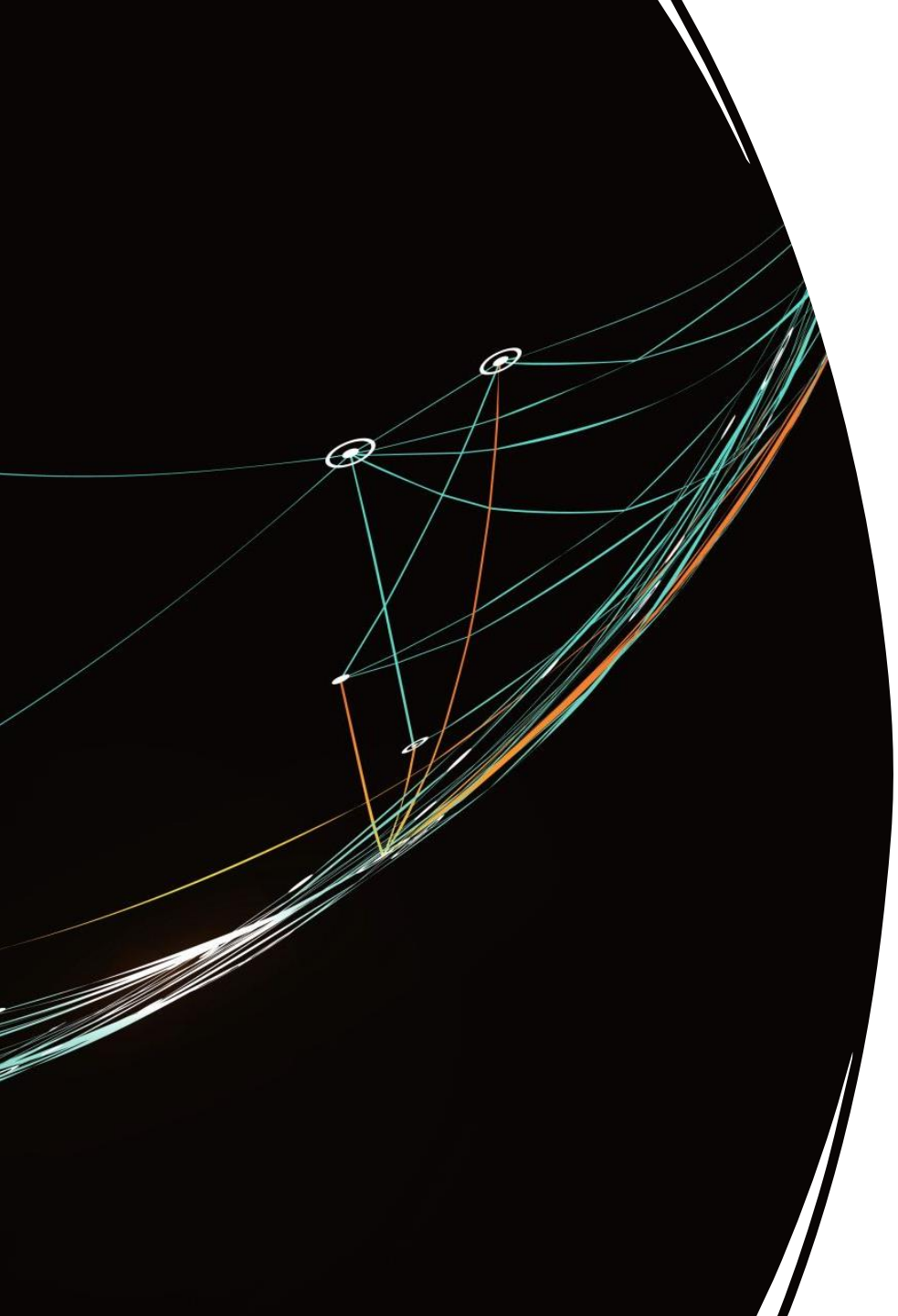
Mise en place d’une DMZ sur pfsense

Thomas D’amore



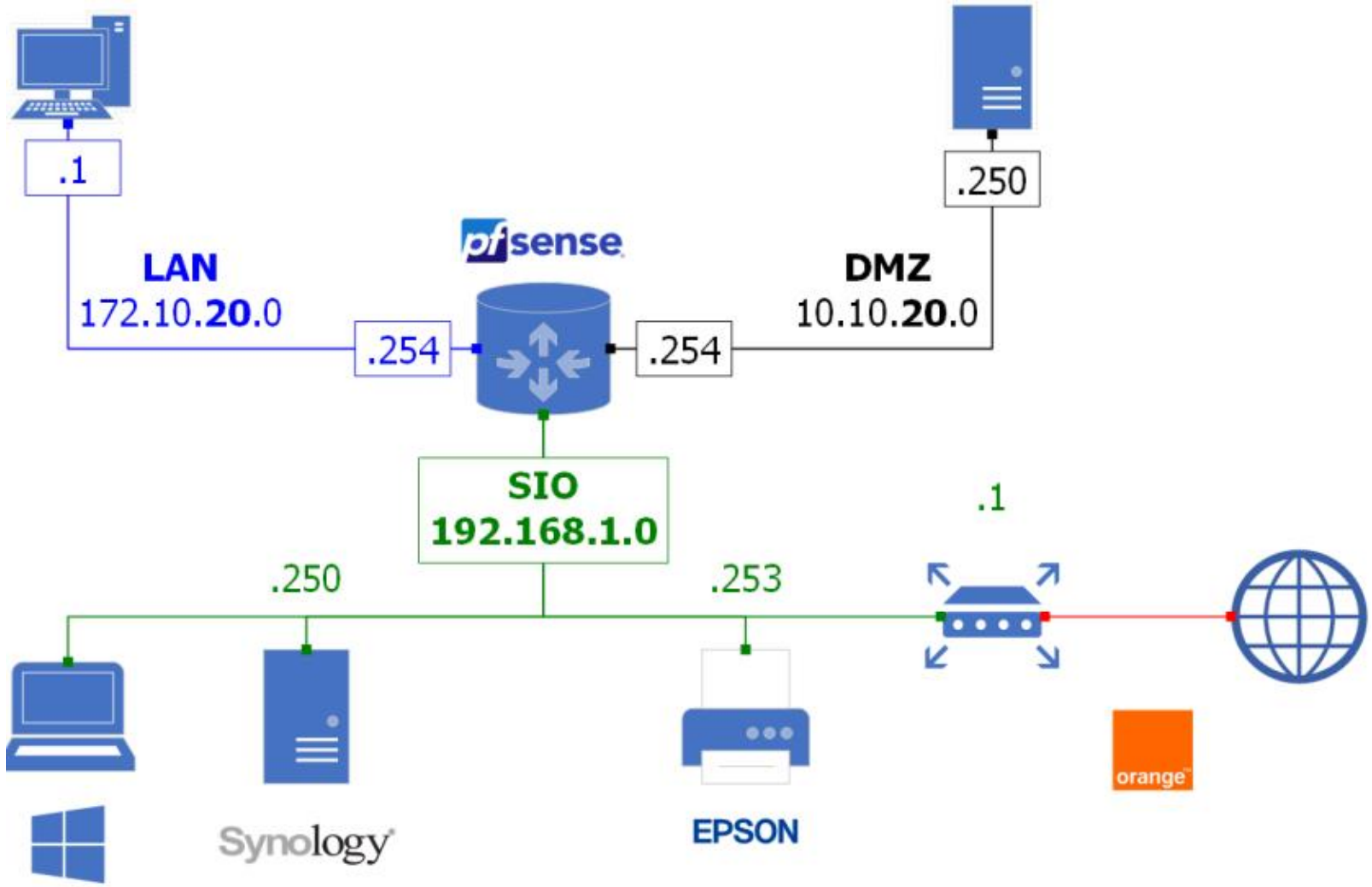
Création et configuration d’un routeur avec trois interfaces (WAN ; LAN ; DMZ).

• Connexion par pont du routeur pour le faire communiquer au réseau physique.

• Création de deux réseaux internes : Une LAN et une DMZ à partir du routeur.

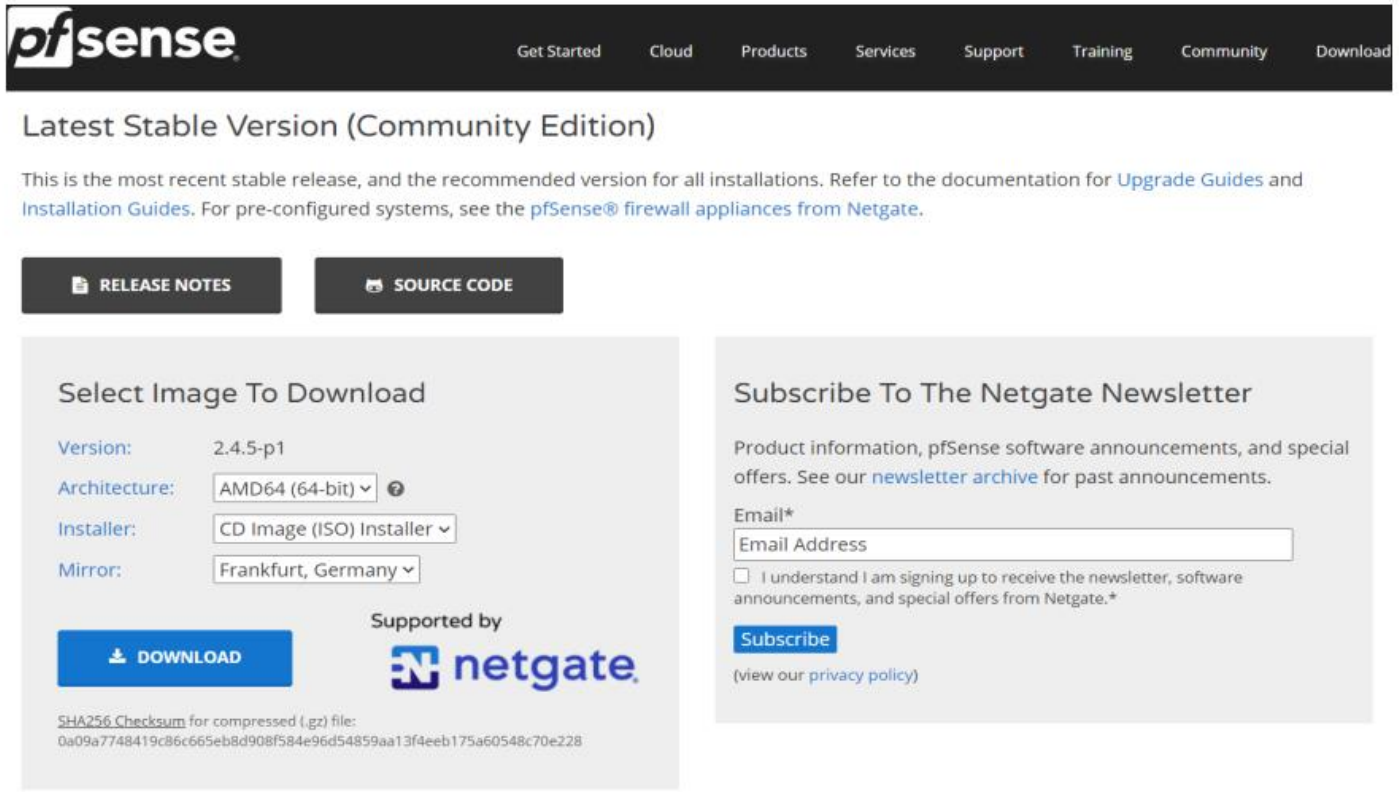
• Création et configuration des hôtes Windows et Debian du réseau LAN et DMZ

Schéma (topologie de l’infrastructure réseau)



Téléchargement de pfsense

Pour télécharger le fichier, aller sur ce lien : https://www.pfsense.org/download.
Sélectionner la bonne architecture, le bon format et serveur miroir puis le télécharger.



Mise en place de la VM pfsense

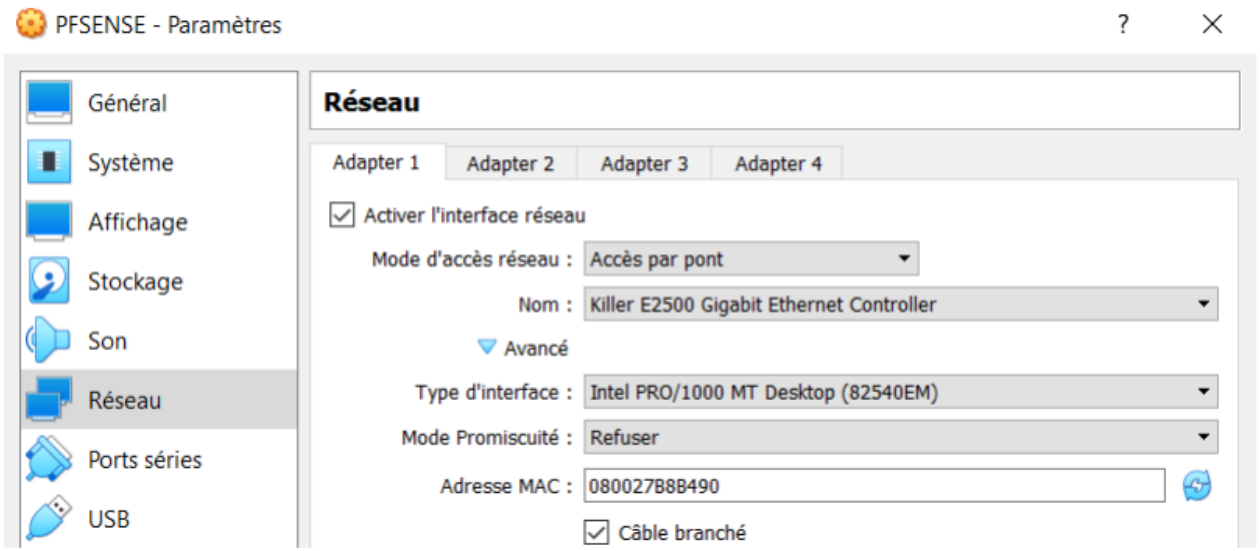
Configuration d'une machine virtuelle :

Sur une machine virtuelle basée sur la version du système FreeBSD (64 bits), insérer l'image disque extraite du fichier téléchargé précédent en lui donnant 1 Go de RAM et 4 Go de stockage minimum.

Créer ensuite trois interfaces (WAN ; LAN ; DMZ) en se basant sur l'architecture réseau du début.

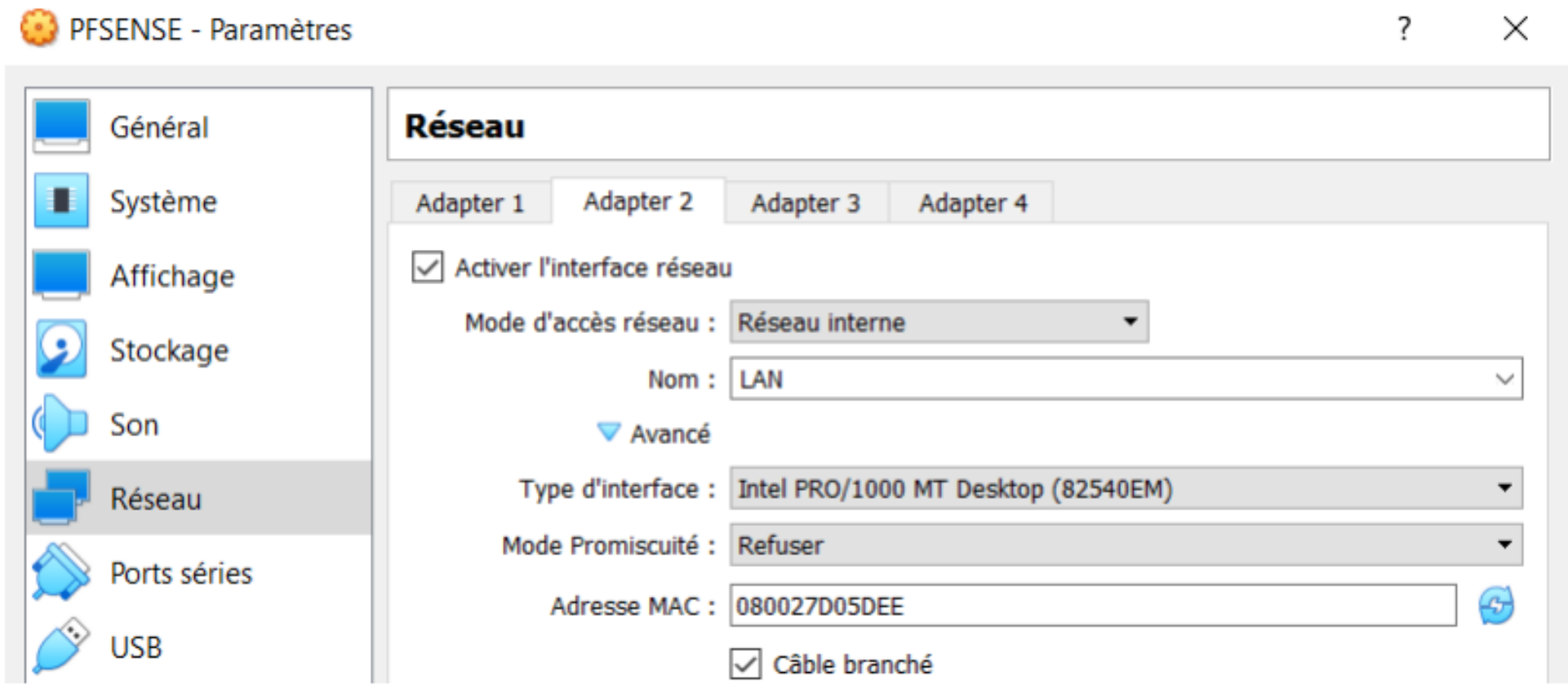
L'objectif est de faire communiquer les deux réseaux via le routeur virtuel au réseau SIO en déclarant ce dernier en réseau WAN.

Pour cela il faut activer sa première interface par pont pour le WAN.



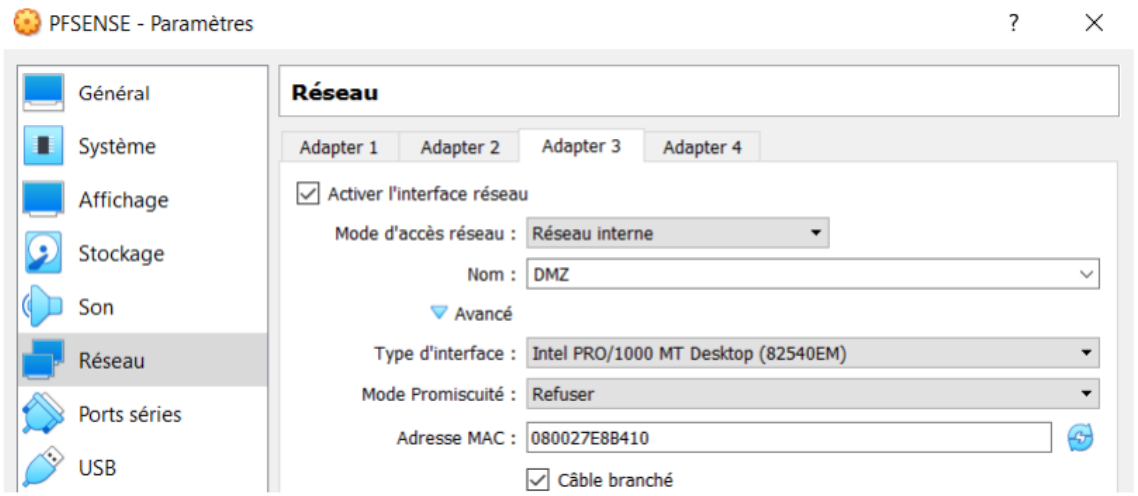
Ensuite activer sa seconde interface en réseau interne pour le LAN.

La seconde carte réseau en “reseau Interne” pour le LAN



La troisième interface est en “réseau Interne” également pour la DMZ

Et activer sa troisième interface en réseau interne pour la DMZ.



Puis procéder à l’installation de pfSense de manière classique et automatique.

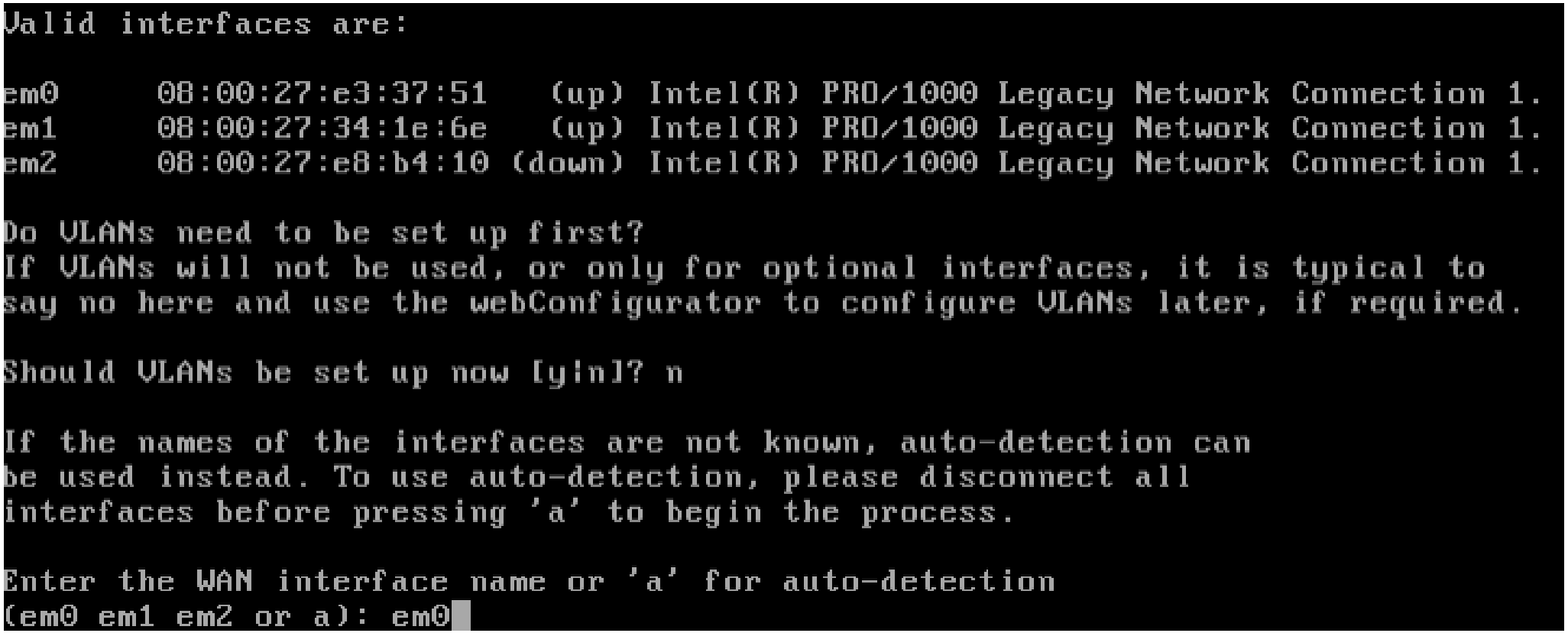
Déclarations des interfaces :

Sur la prochaine capture d’écran, les trois interfaces apparaissent et il faut les déclarer.

Pour reconnaître les différentes interfaces, il est possible de voir leur adresse MAC à partir de la fenêtre de configuration réseau de la machine virtuelle, comme ci-dessus.

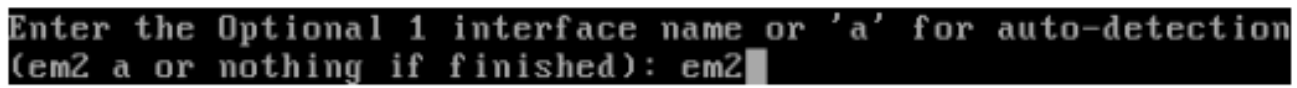
Il est d’ailleurs préférable de retenir le nom de chaque interface pour les reconnaître ensuite.

Pour le WAN, c’est l’interface em0 qu’il faut le déclarer puisqu’il le fera communiquer avec le SIO.


Valid interfaces are:
em0 08:00:27:e3:37:51 (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em1 08:00:27:34:1e:6e (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em2 08:00:27:e8:b4:10 (down) Intel(R) PRO/1000 Legacy Network Connection 1.
Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y|n]? n
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0

Pour le LAN, c'est l'interface em1 qu'il faut le déclarer.

Pour la DMZ, c'est l'interface em2 qu'il faut le déclarer.

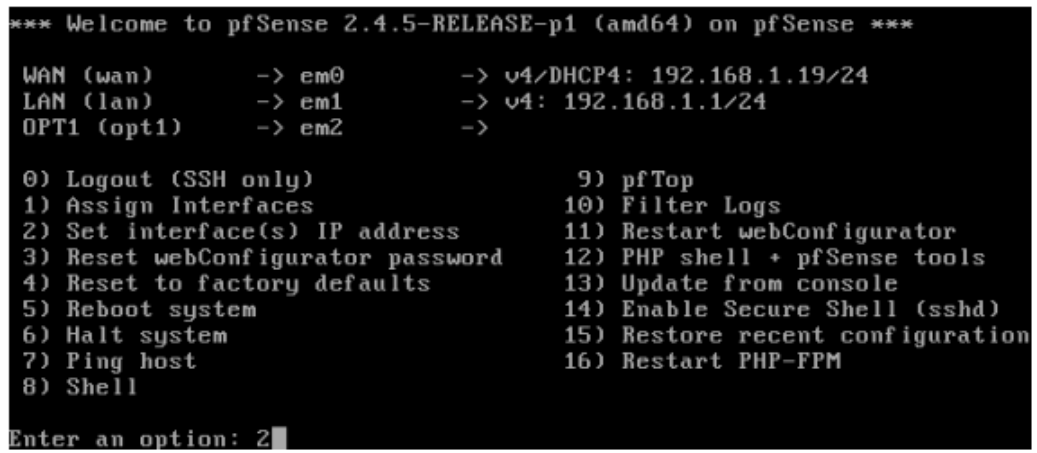


En résumé, pfSense fait valider à l'administrateur tous ces choix :

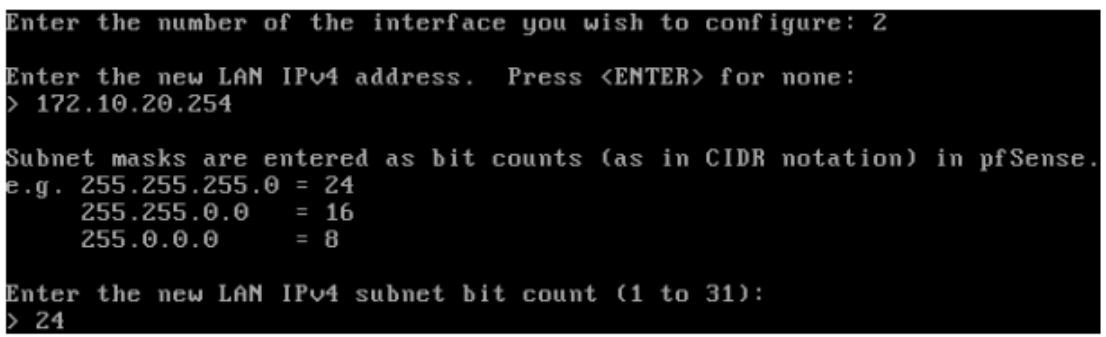
Pour pouvoir mettre les machines virtuelles sur un stockage externe, raccorder les réseaux virtuels et le routeur à n'importe quelle machine de n'importe quel réseau physique ou pour n'avoir aucune collision réseau, il faut laisser l'interface WAN em0 en DHCP.

Assignements des interfaces :

Toutes les interfaces sont donc déclarées, mais il reste à les assignées puisque les IPv4 ci-dessous ne sont pas bonnes (sauf pour l'interface WAN em0 puisqu'il est en DHCP).



Pour l'interface em1 du LAN, il faut lui assigner l'adresse IPv4 : 172.10.20.254 en /24.



Dans ce cas, l'administrateur ne veut pas y installer de serveur DHCP.

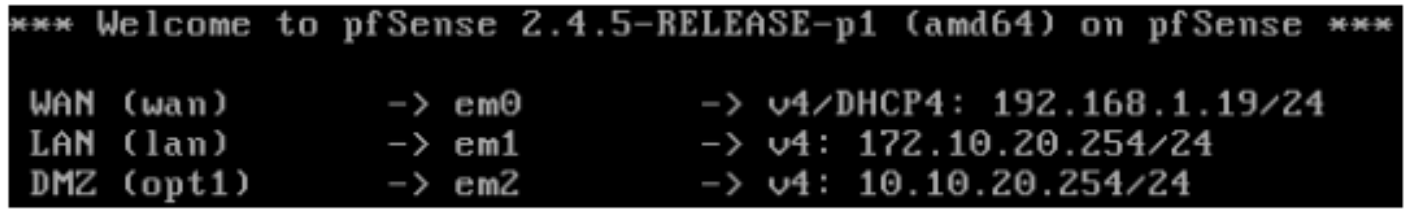
```
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...
 Restarting webConfigurator...

The IPv4 LAN address has been set to 172.10.20.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://172.10.20.254/
```

Pour l'interface em2 de la DMZ, il faut lui assigner l'adresse IPv4 : 10.10.20.254 en /24.

```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 3

Enter the new OPT1 IPv4 address.  Press <ENTER> for none:
> 10.10.20.254

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 OPT1 IPv4 subnet bit count (1 to 31):
> 24
```

Note : L'interface OPT1 ne s'appelle pas DMZ, mais ce n'est pas grave car l'administrateur pourra lui changer son nom par interface graphique.

Les trois interfaces du routeur sont enfin configurées ! Voici ce que cela donne :



Une fois tout cela fait, l'administrateur peut passer par interface graphique pour passer à la configuration du pare – feu intégré étant pfSense. Pour cela, il faut qu'il y aille sur la machine cliente et écrire l'adresse IP de l'interface LAN du routeur sur son navigateur Internet : 172.10.20.254.

Note : En principe, l'administrateur d'une entreprise bloque toutes les règles d'un pare – feu et n'ouvre que petit à petit les ports utilisés par les utilisateurs (http, https…) pour plus de sécurité. Alors qu'ici, l'administrateur ne vient seulement qu'installer le routeur et le pare – feu a ouvert tous les ports par défauts. Donc les deux autres réseaux ont accès à Internet.

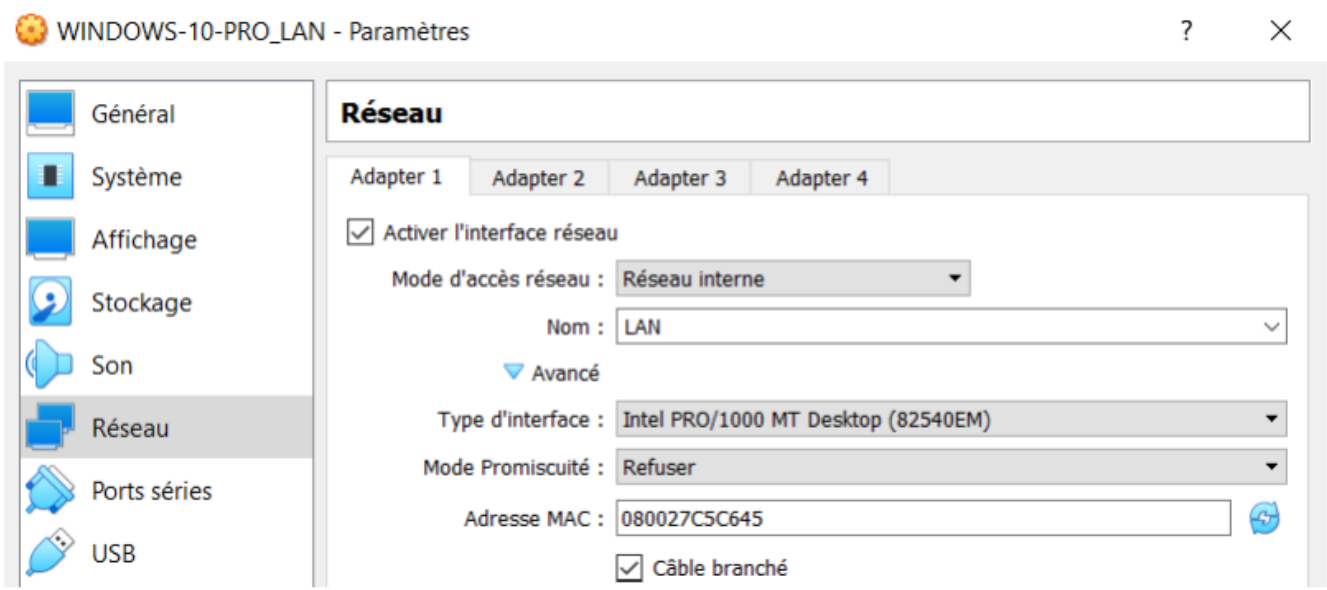
Configuration d'une machine Windows :

Configuration d'une machine virtuelle :

Une machine virtuelle Windows n'est pas difficile à créer. L'administrateur part du principe qu'il en a déjà une, à jour et qui est prête à être démarrer.

Mais avant de la démarrer il faut un seul paramètre pour éviter une erreur de communication réseau.

Pour cela il faut activer sa première interface interne pour le LAN.



Puis démarrer Windows sur la machine virtuelle.

Assignement de l'interface :

Dans les paramètres réseaux du système, il faut assigner l'interface interne pour le LAN.

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
   Adresse physique . . . . . . . . . . . : 08-00-27-C5-C6-45
   DHCP activé. . . . . . . . . . . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::ec31:3005:eda5:f6bb%12(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 172.10.20.1(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 172.10.20.254
   IAID DHCPv6 . . . . . . . . . . . . . : 101187623
   DUID de client DHCPv6. . . . . . . . . : 00-01-00-01-27-12-34-52-08-00-27-C5-C6-45
   Serveurs DNS. . . . . . . . . . . . . : 172.10.20.254
                                           192.168.1.1
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

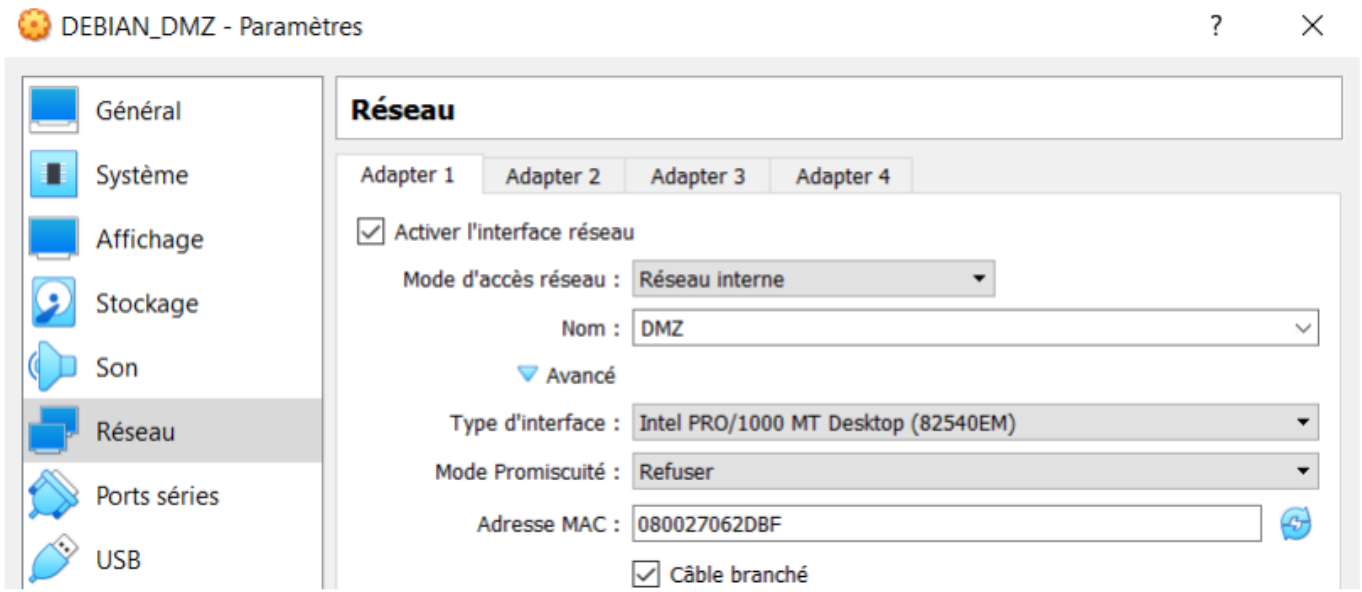
Configuration d'une machine Debian :

Configuration d'une machine virtuelle :

Une machine virtuelle Debian n'est pas difficile à créer. L'administrateur part du principe qu'il en a déjà une, à jour et qui est prête à être démarrer.

Mais avant de la démarrer il faut un seul paramètre pour éviter une erreur de communication réseau.

Pour cela il faut activer sa première interface interne pour la DMZ.



Puis démarrer Debian sur la machine virtuelle.

Assignement de l'interface :

Avec `# nano /etc/network/interfaces`, remplacer l'adresse dynamique en une statique.

```
 GNU nano 3.2                                /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
        address 10.10.20.250/24
        gateway 10.10.20.254
```

Puis avec `# service networking restart`, redémarrer le service réseau du système.

Fin de la mise en place d’une DMZ sur Pfsense