Firewall + Proxy

Tuto : Ipfire Firewall

Ça brûle les firewall

BOUDECHICHA Redhouane
24/09/2024

Je tue le temps pour essayer sa en vrai

Quelqu’un Firewall :

Un firewall est un appareil de sécurité réseau qui surveille le trafic réseau entrant et sortant et autorise ou bloque les paquets de donnés en se basant sur un ensemble de règles de sécurité. Il est chargé de dresser une barrière entre votre réseau interne et le trafic entrant provenant de sources externes (comme Internet) afin de bloquer le trafic malveillant des virus et des pirates.

Pourquoi IPFire ?

IPFire est une distribution Linux spécialisée dans la sécurité réseau, conçue pour fonctionner comme un pare-feu. Elle est souvent utilisée pour protéger et gérer le trafic réseau dans les environnements domestiques, de bureau, ou de petites entreprises.

Principales fonctionnalités d'IPFire :

- **Pare-feu :** Il utilise un pare-feu basé sur iptables pour filtrer le trafic réseau, permettant un contrôle précis sur les connexions entrantes et sortantes.
- **Système de détection et prévention d'intrusions (IDS/IPS) :** Intègre des outils comme Snort ou Suricata pour détecter et prévenir les menaces en temps réel.
- **Filtrage de contenu :** Permet de bloquer ou restreindre l'accès à certaines catégories de sites web, souvent utilisé pour le contrôle parental ou en entreprise.
- **VPN :** Supporte la création de réseaux privés virtuels (VPN) via IPsec et OpenVPN, permettant des connexions sécurisées à distance.
- **Gestionnaire de QoS (Quality of Service) :** Contrôle la bande passante pour prioriser certains types de trafic réseau.
- **Mises à jour fréquentes :** IPFire est maintenu activement avec des mises à jour régulières pour garantir la sécurité et la stabilité.

IPFire est apprécié pour sa flexibilité, sa sécurité et sa capacité à s'adapter à divers scénarios réseau, tout en restant accessible aux utilisateurs ayant des connaissances de base en réseau.

Et pourquoi l’utiliser ?

Je tue le temps pour essayer sa en vrai

MrGranier la demandé…

Pré-recquis pour Ip Fire ?

Processeur :

- Un processeur x86_64 ou ARM (32 ou 64 bits) est recommandé. Même un processeur modeste (comme un Intel Atom ou Celeron) peut suffire pour de petits réseaux, mais pour des environnements plus importants, un processeur plus puissant est préférable.

Mémoire RAM :

- **Minimum :** 1 Go de RAM.
- **Recommandé :** 2 Go ou plus, surtout si vous utilisez des fonctionnalités avancées comme l'IDS/IPS ou un grand nombre de connexions VPN.

Stockage :

- **Minimum :** 4 Go de disque dur ou SSD.
- **Recommandé :** 8 Go ou plus, selon la quantité de logs et la configuration des fonctionnalités supplémentaires (comme le proxy cache).

Cartes réseau (NIC) :

- **Minimum :** 3 cartes réseau (une pour le réseau externe, une pour le réseau interne et une pour la DMZ).
- **Recommandé :** Des cartes réseau de qualité (Intel, Broadcom) pour une meilleure performance et compatibilité.

Je tue le temps pour essayer sa en vrai

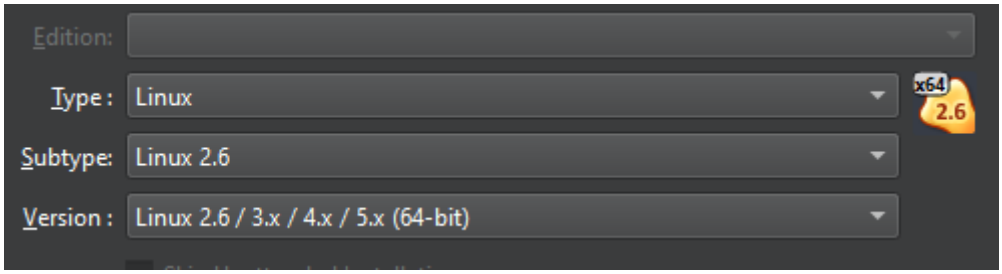
Préparatif VirtualBOX

On va partir du principe que vous savez utiliser VB et que vous avez lu les pré-recquis pour IP Fire mais on vas quand même s'attarder sur l'ISO, IP Fire est basé sur Linux 3.0 vous devez sélectionné donc :

Type → Linux

Subtype → Linux 2.6

Version → Linux 2.6/3.x/4.x/5.x (64-Bit) OU 32-Bit sait-on jamais



Pour l'iso il suffit de la récupérer sur le site officiel d'IpFire dans Download

En suite finissez de configuré votre machine et voila (n'oubliez pas de bien choisir le dossier ou vous voulez que votre VM soit…)

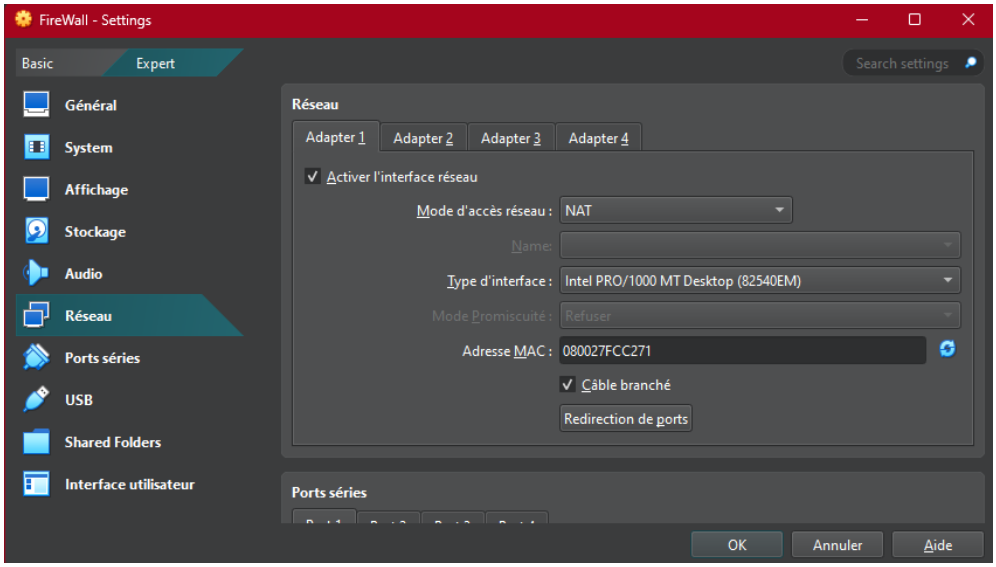
Je tue le temps pour essayer sa en vrai

Configuration réseaux

Il nous faut trois carte réseaux (deux en temps normal mais projet oblige)

Pour ce faire Cliquer sur configuration et rendez vous dans l'onglet réseaux comme ceci :

Il nous faut Red ou rouge qui sera notre première carte réseaux qui donnera accès Internet vous pouvez choisir comme mode d'accès « Accès par pont » ou « Nat » vous comprendrez plus tard pourquoi ça ne change rien.

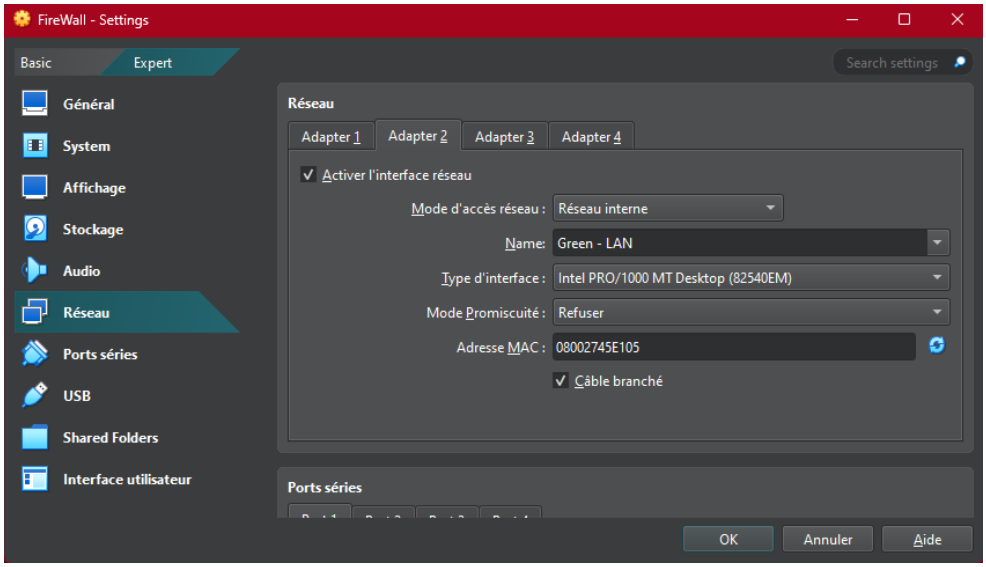


En suite Seconde carte réseaux Green ou vert le réseau privé local :

Il nous faut Red ou rouge qui sera notre première carte réseaux qui donnera accès Internet vous pouvez choisir comme mode d'accès « Accès par pont » ou

Je tue le temps pour essayer sa en vrai

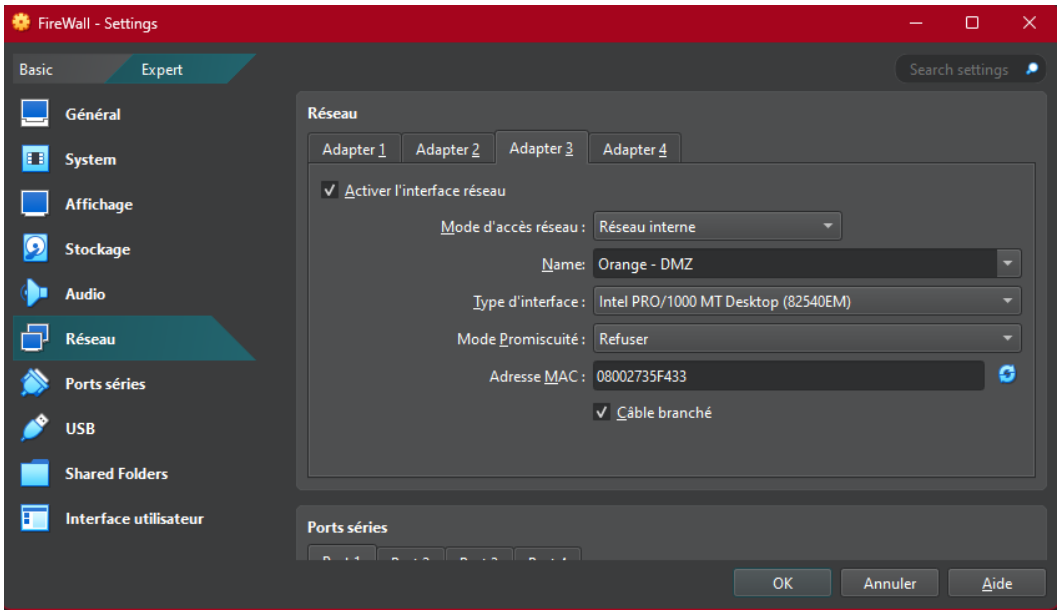
« Nat » vous comprendrez plus tard pourquoi ça ne change rien. N'oubliez pas de nommez vos réseau interne pour faciliter la compréhension.



Pour terminer, Orange notre DMZ :

Même Principe que pour Green.

Maintenant vous pouvez démarrer votre machine équiper de IpFire et commencez l'installation

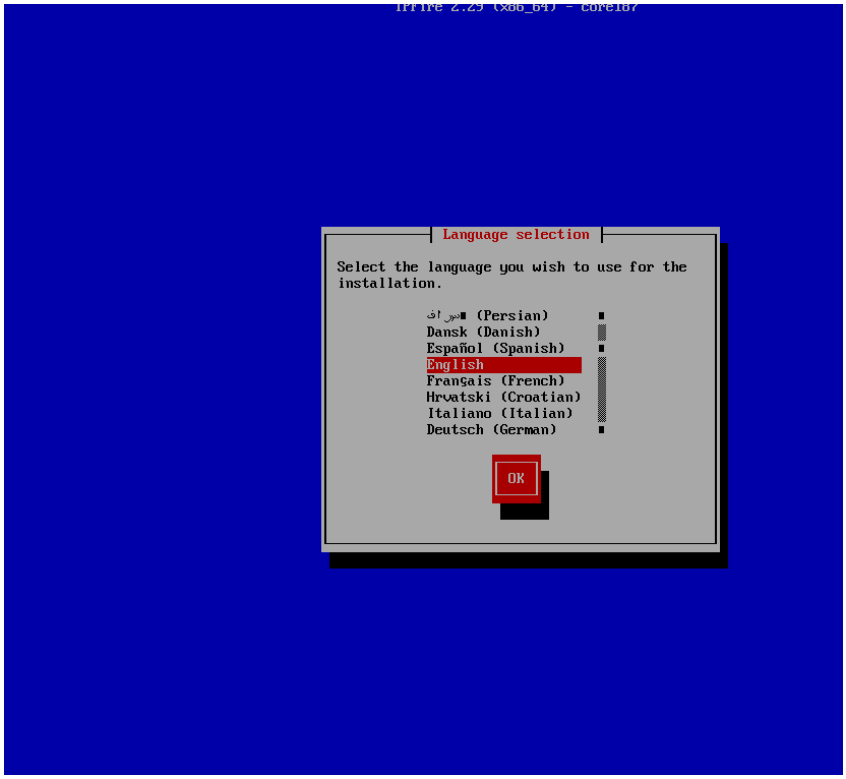


Je tue le temps pour essayer sa en vrai

Installation d'Ip Fire

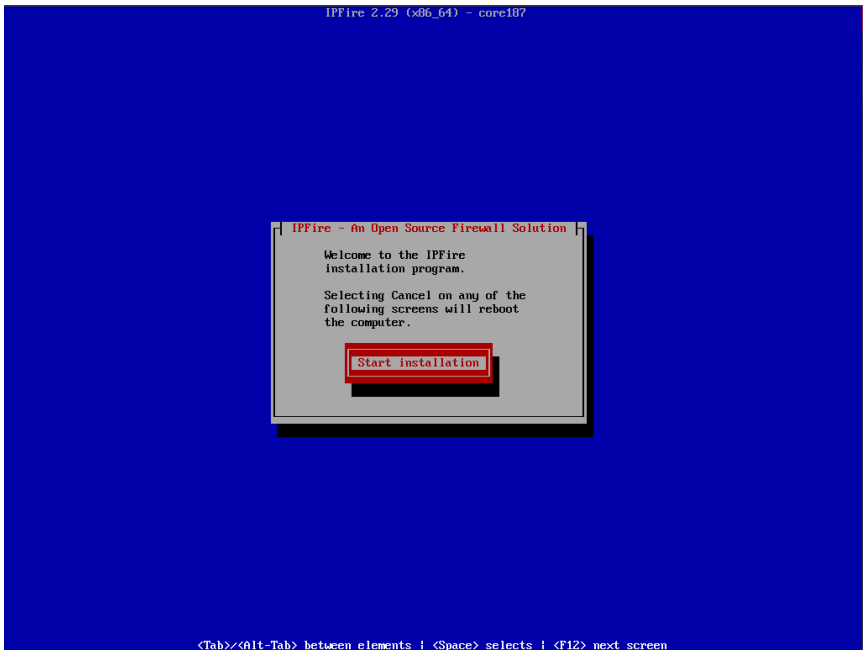
Taper sur Entrée

Choisissez votre language :



Appuyez sur Entrée :

Je tue le temps pour essayer sa en vrai



Lisez et acceptez la licence :

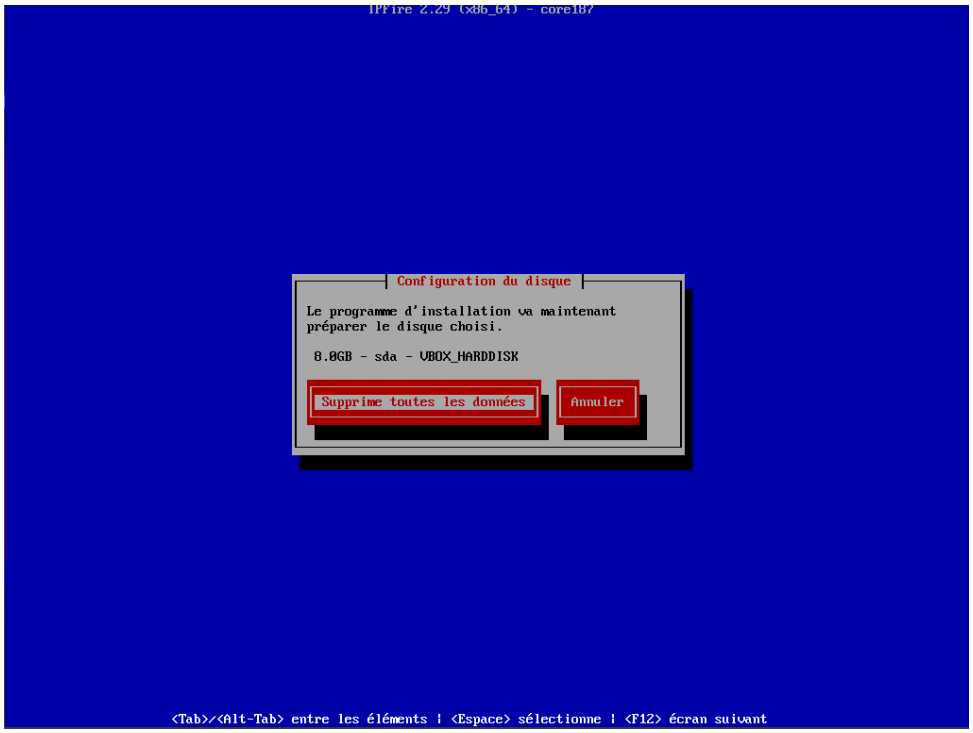
Si vous avez la flemme appuyez sur Tab puis ESPACE pour cocher la case puis Flèche de droite pour allez sur OK et valider.

Je tue le temps pour essayer sa en vrai

Supprimer toutes les données :

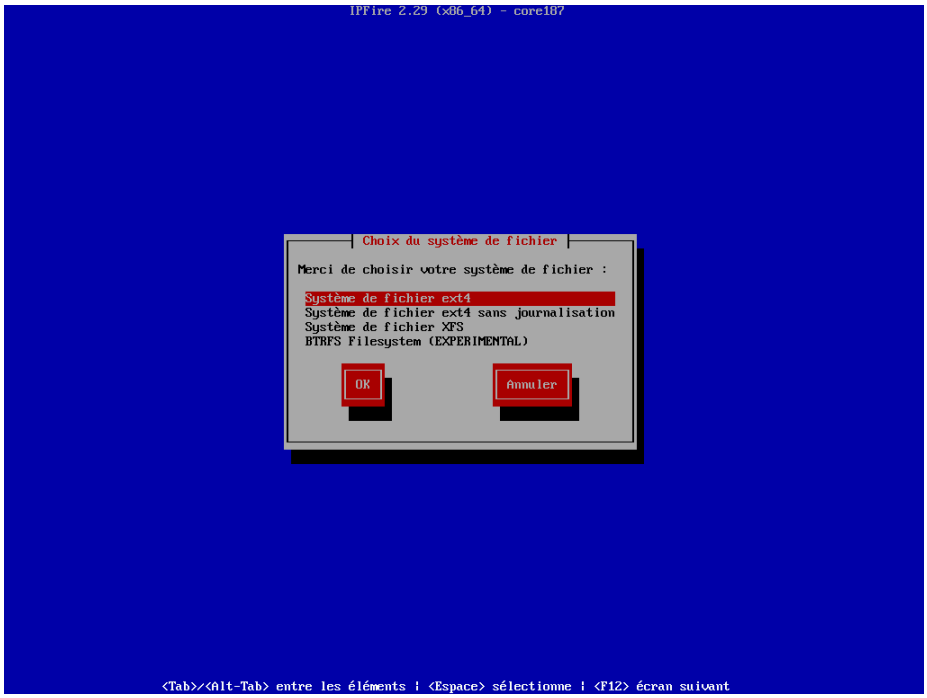
C’est obligatoire pour pouvoir écrire par-dessus.

Je tue le temps pour essayer sa en vrai



Se déplacer sur le système de fichier ext4 :

C'est celui de base de Linux, puis appuyez sur Entrée



Félicitations, vous venez d'installer IPFire… reste a le configurer

Je tue le temps pour essayer sa en vrai

Je tue le temps pour essayer sa en vrai

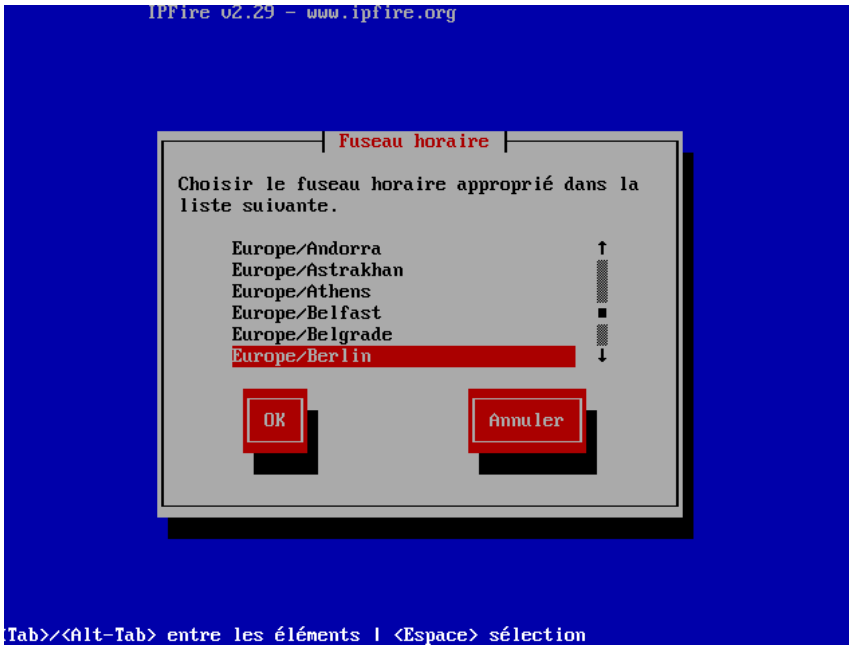
Première Configuration d'IpFire

Choisissez le type de clavier utilisé :

Si jamais on est en FRANCE DONC Fr (petit tips vous pouvez juste taper le F de votre clavier il vous montrera directement le premier type commençant par F).

Choisissez le Fuseau Horaire :

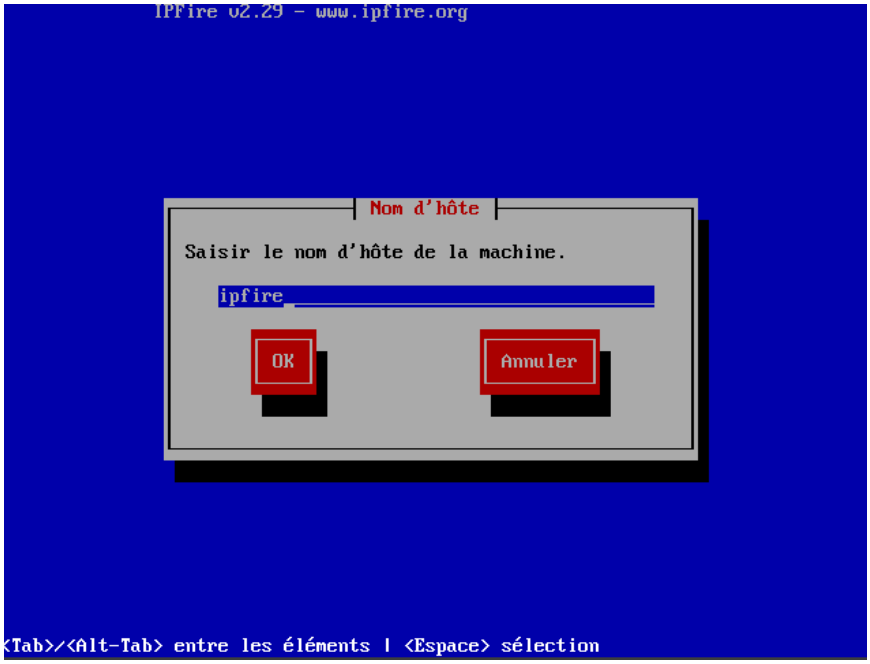
Au cas où on est toujours en Europe donc trouvez Paris... en soit Berlin ne pose pas de problème.



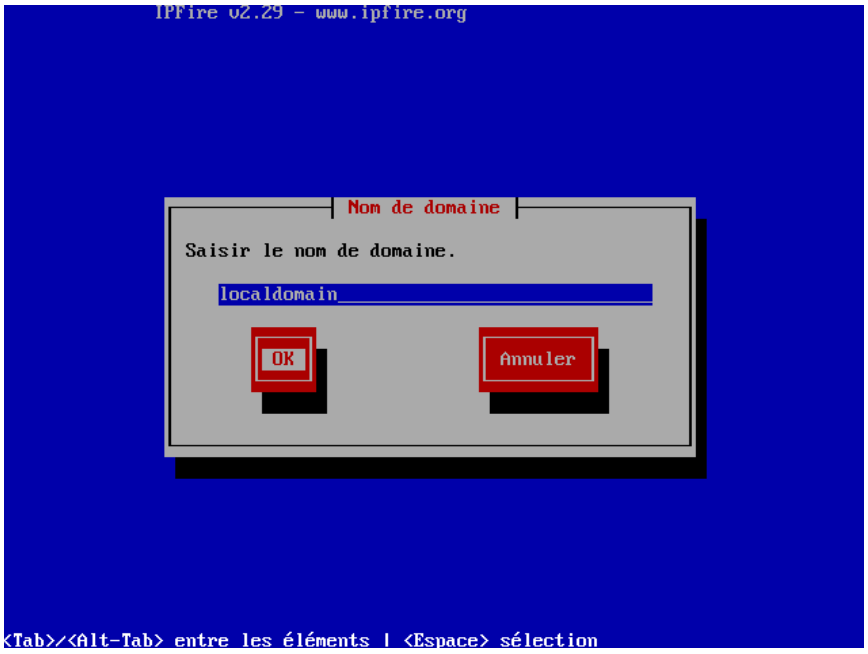
Je tue le temps pour essayer sa en vrai

Choisir le nom d’hôte :

Choisir un nom simple de préférence facile à retenir.



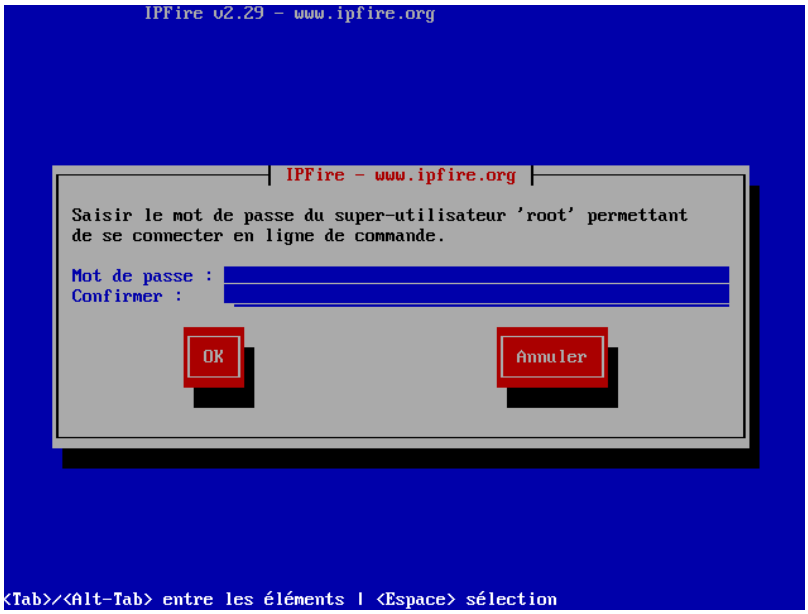
Choisir un nom de domaine :



Je tue le temps pour essayer sa en vrai

IMPORTANT : Faire attention a bien taper votre mot de passe et le noté quelque part il s'agit ici du Mot de passe du compte ROOT qui vous permet de tapé des commande sur l'interface ligne de commande d'IpFire. (Appuyer sur Tab pour passer de mot de passe à confirmer)

Ne prenez pas peur le mot de passe n'est pas afficher et rien ne vous montre que le mot de passe est entrain d'être écris en faisant entrée vous verrez bien si vous avez bien retaper le MDP.



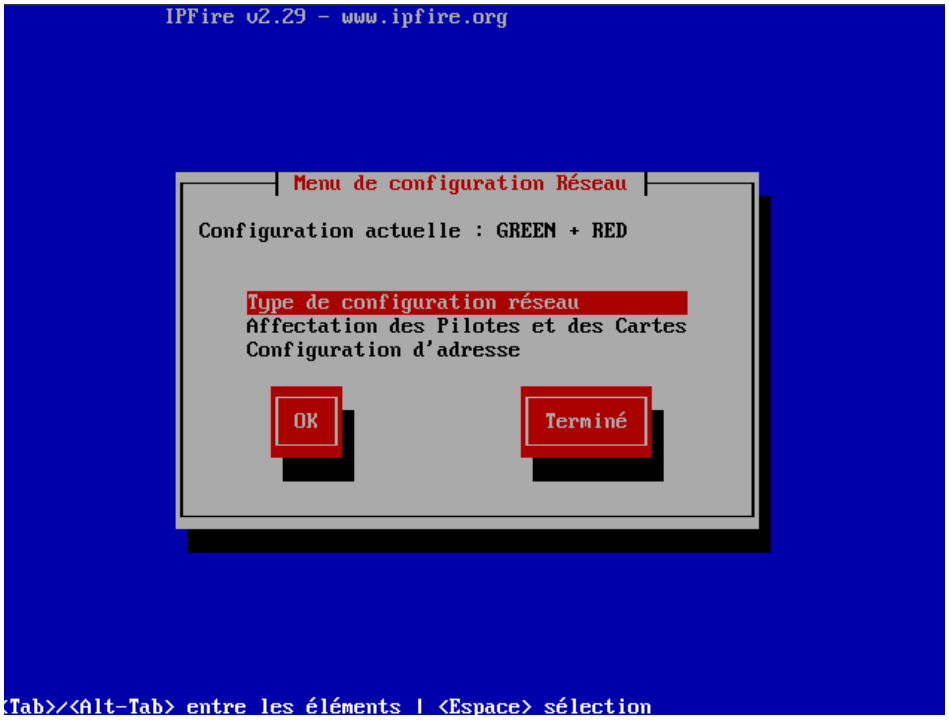
Choisir le mot de passe WEB :

Ici il s'agit du mot de passe de l'interface admin WEB lui aussi est à noter quelque part parsque sans lui bon courage pour configurer quelque chose.

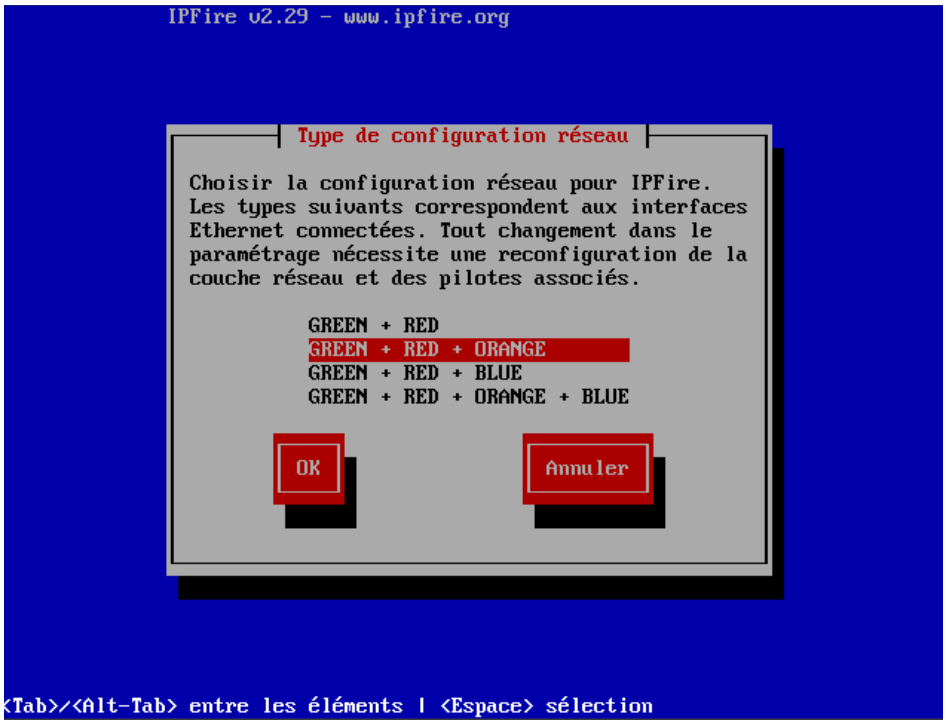
Je tue le temps pour essayer sa en vrai

Choisir votre type de configuration :

S'il manque une carte réseaux IpFire vous le fera savoir. (Bleu est celle du WIFI)

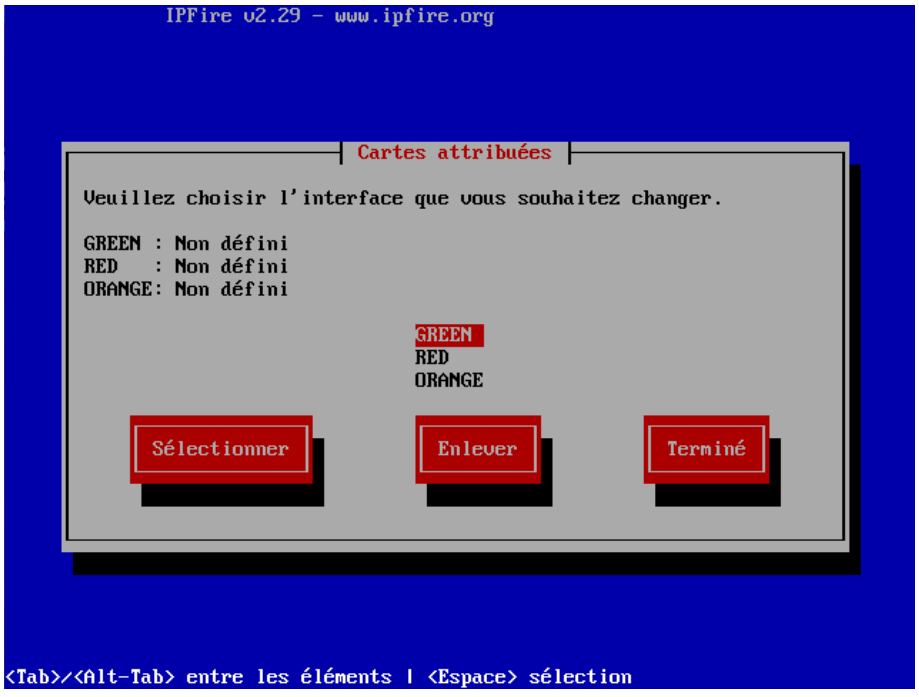


Je tue le temps pour essayer sa en vrai



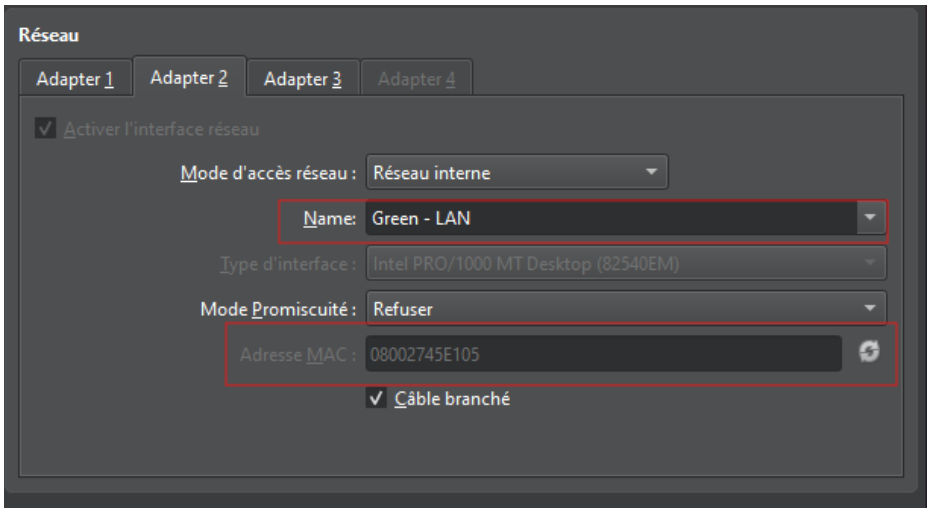
Affectez les cartes réseau :

Affectez les bonne adresses MAC

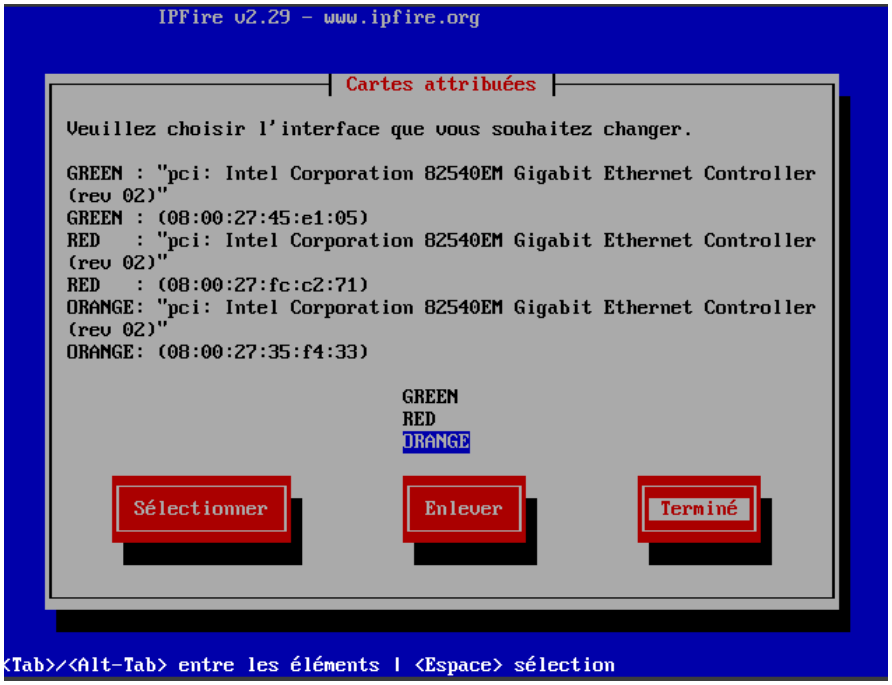


Je tue le temps pour essayer sa en vrai

Pour trouver quel adresse mac correspond à quel carte mère il suffit de se rendre dans la configuration de la machine et d'aller dans réseaux. C'est pour cela que je vous ai demandez de nommer les réseaux interne.



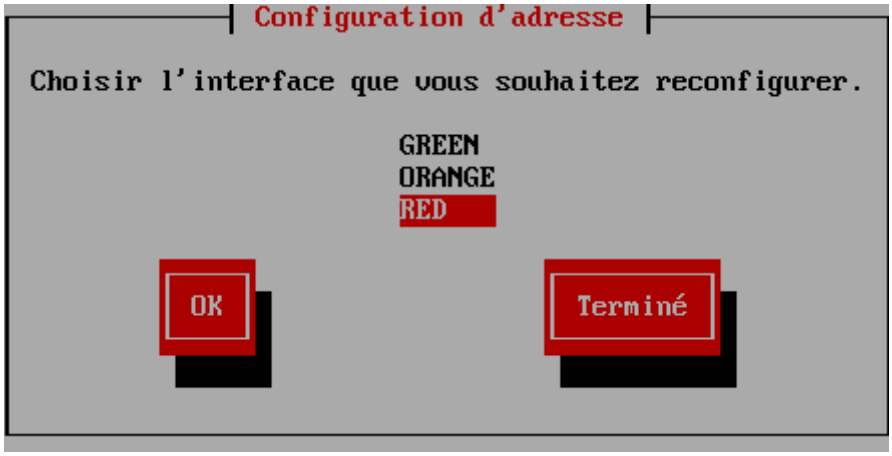
A la fin de la configuration pensez juste à revérifier si tout est dans le bonne ordre c'est très important car chaque carte à son rôle à jouer



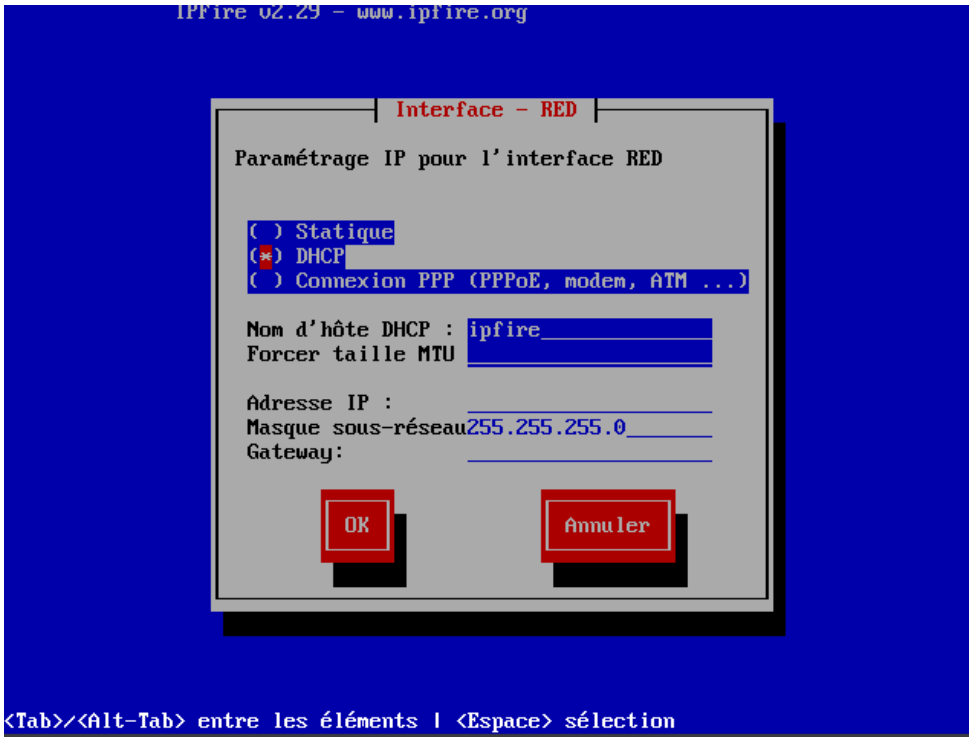
Je tue le temps pour essayer sa en vrai

Configuration des adresses :

Commençons par Red .

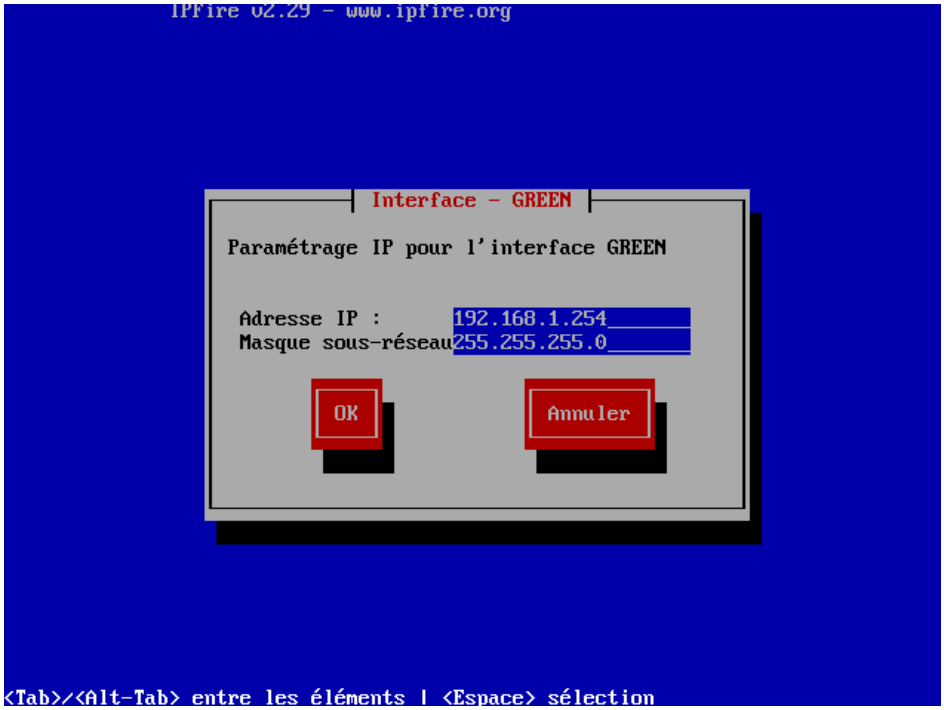


Red est celui qui vas amenez Internet donc il as besoin d'être en DHCP car peu importe ce qui viens a l'entrée il se contente de le distribuer vers Green.

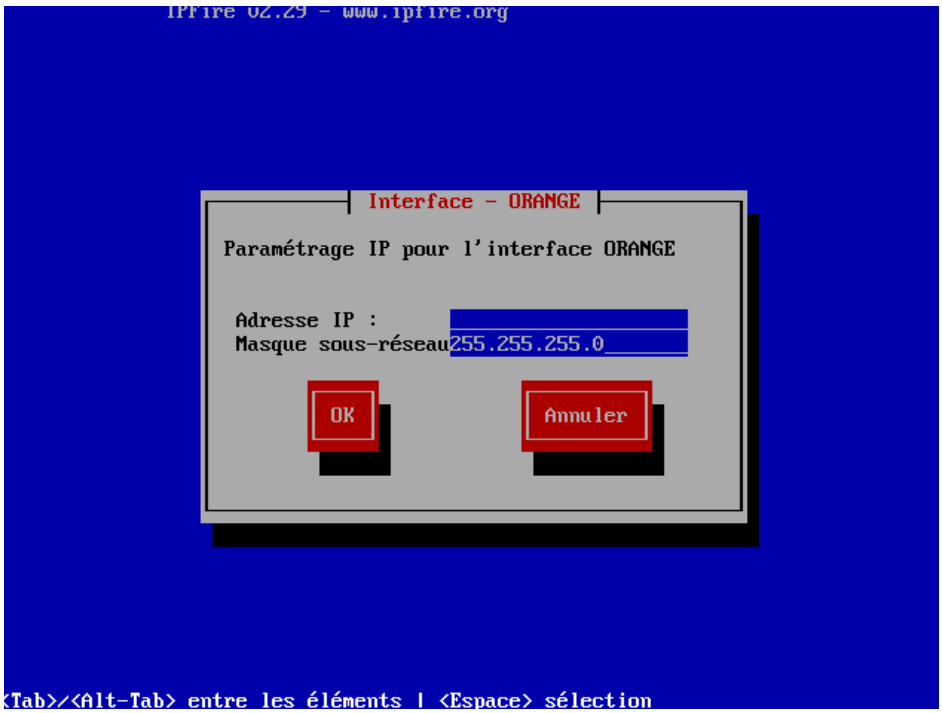


Je tue le temps pour essayer sa en vrai

Green Lui as besoin d'une IP car c'est la passerelle de votre infrastructure il vas vous permettre de sortir du réseaux pour pouvoir allez sur Internet.

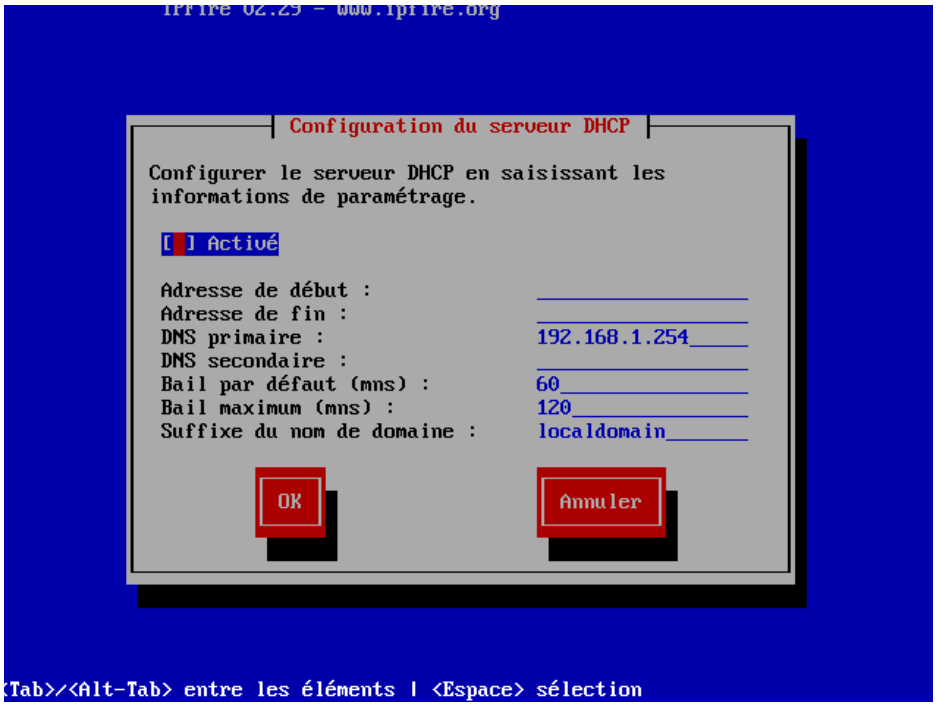


Bon la DMZ aucune idée bon courage.



Je tue le temps pour essayer sa en vrai

IpFire est aussi capable d'utiliser le service DHCP, et donc de vous fournir les informations de connexion (Nom du réseau, DNS etc...)pour chaque machine connectée automatiquement. Si vous n'en posséder par ou compter utiliser autre chose allez juste vers OK pour finir la configuration.



C'est LA FIN voila j'ai terminé le tuto

Je tue le temps pour essayer sa en vrai

PS : Les screen sont de moi, oui je me suis fait chier a refaire la machine pour tester, je l'ai même fait 2 fois pour être sûre d'être clair comme du Pepsi-Crystal.