

IPFIRE

Le routeur open source simple pour bien débuter



SOMMAIRE

1. QU'EST-CE QUE IPFIRE ?
2. PRINCIPE DE FONCTIONNEMENT DE IPFIRE
3. ACCES A L'INTERFACE DE GESTION DE IPFIRE
 - a. Depuis un poste du labo SIO
 - b. Depuis une machine virtuelle du réseau local
4. ACCES AU SERVEUR DHCP DE IPFIRE
5. PARAMETRER DES REGLES DE PARE-FEU

© tutos-info.fr - 01/2025



DIFFICULTE



UTILISATION COMMERCIALE INTERDITE

1 – QU'EST-CE QUE IPFIRE ?

IPFire est une distribution GNU/Linux, orientée **routeur et pare-feu** qu'il est possible de configurer.

IPFire offre un système complet de **gestion de paquets**. On peut ainsi disposer d'un système simple et léger qui agit comme un pare-feu, ou l'équiper de **nombreuses extensions**. Il peut donc s'adapter à différents scénarios. Enfin, les questions de sécurité sont rapidement résolues par les mises à jour.

Le système de base est livré avec les caractéristiques suivantes :

- Firewall
- Intrusion Detection System (Snort) de prévention des intrusions
- Mise en cache
- Serveur de temps
- WOL (Wake up on LAN)
- VPN IPsec et OpenVPN
- Serveur DHCP
- Dynamic DNS (DynDNS, No-IP)
- Analyse fonctions de surveillance du système et analyse de logs
- Qualité de service (QoS)
- Serveur proxy avec filtrage de contenu et les fonctions de mise en cache des mises à jour (par exemple mises à jour Microsoft Windows, antivirus, et bien d'autres)

2 – PRINCIPE DE FONCTIONNEMENT DE IPFIRE

IPFire peut fonctionner sous forme d'une machine virtuelle. Cette machine virtuelle est peu en ressources puisqu'elle s'exécute avec 1 024 Mo (1 Go) de RAM et un disque système de 20 Go. Il faut noter, cependant, que si la fonction « proxy web » est activée, il sera nécessaire d'augmenter la mémoire vive de la machine à 2 Go minimum et vérifier que l'espace disque système est suffisant.

Dans le cadre des ateliers professionnels, vous possédez :

- 1 serveur Proxmox (que vous avez installé et configuré)
- 1 serveur de sauvegarde de type PBS (que vous avez installé et configuré)

Ces serveurs sont connectés au switch de l'espace atelier (vlan 60).

Tout au long de votre formation de 1^{ère} année, vous allez créer et utiliser des machines virtuelles (Debian, Windows Server et Windows 10 ou 11 Pro). Ces machines seront créées sur votre serveur Proxmox mais elles seront dans des réseaux isolés afin d'éviter tout problème d'adressage IP en double, etc.).

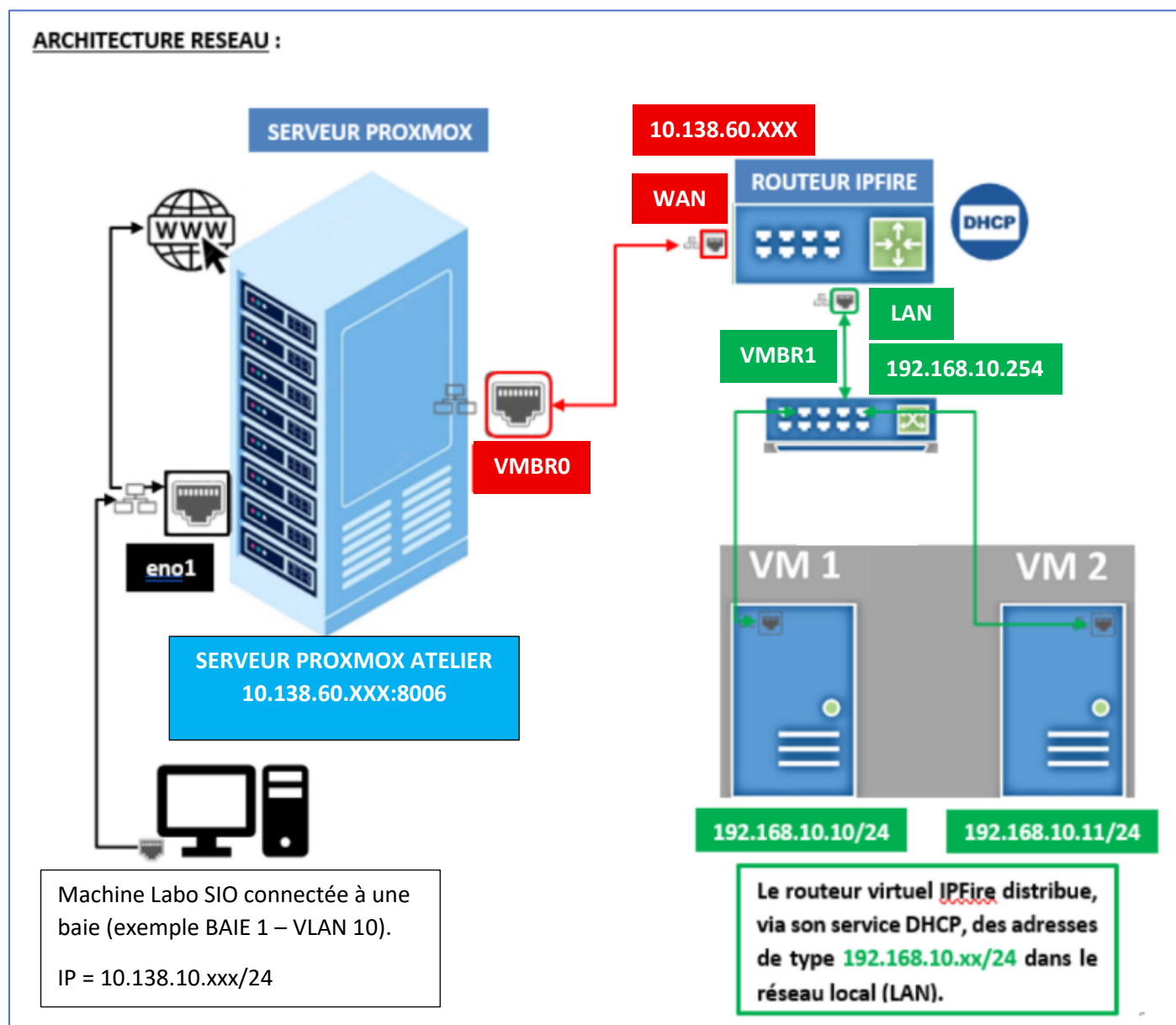
Afin de cloisonner vos machines sur vos serveurs respectifs, vous allez installer et configurer un pare-feu/routeur simple pour commencer : IPFire (version 2.29 - 199 à ce jour).

Lien de téléchargement du fichier ISO :

https://downloads.ipfire.org/releases/ipfire-2.x/2.29-core199/ipfire-2.29-core199-x86_64.iso

Un exemple d'architecture réseau simple est présenté page suivante.

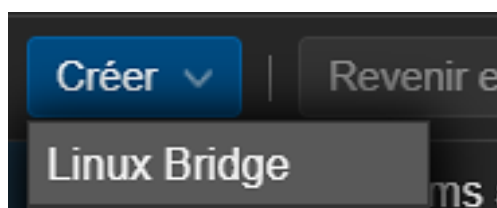
L'architecture réseau se présente ainsi et permet à chaque étudiant de disposer d'un réseau indépendant sans risquer des dysfonctionnements au sein des autres réseaux (notion de cloisonnement) :



3 – INSTALLATION DU PARE-FEU IPFIRE EN MACHINE VIRTUELLE

1^{ère} étape : création d'un « Linux bridge » sur Proxmox

- Cliquez sur le nom du nœud de votre serveur
- Dans le volet de droite, déployez « **Système** » et cliquez « **Réseau** »
- Cliquez le bouton « **Créer** » et « **Linux Bridge** » :



- Nommez votre bridge pour plus de clarté ; par exemple « **lan** » et créez le bouton « **Créer** » :

Créer: Linux Bridge

Nom: **lan**

IPv4/CIDR:

Passerelle (IPv4):

IPv6/CIDR:

Passerelle (IPv6):

Démarrage automatique: ☒

Gère les VLAN: ☐

Ports du pont (bridge):

Commentaire: **Réseau LAN IPFIRE**

Aide

Avancé ☐

Créer

Remarque : il est conseillé de saisir un commentaire afin de clarifier vos cartes réseau !

2^{ème} étape : configuration matérielle de la machine avec Proxmox

- Créez la machine virtuelle avec la configuration matérielle suivante :

Ajouter ▼ Supprimer Éditer Action disque ▼ Revenir en arrière

Mémoire	1.00 Gio [balloon=0] [allow-kvm=0]
Processeurs	1 (1 sockets, 1 cores) [host]
BIOS	Par défaut (SeaBIOS)
Affichage	Par défaut
Machine	q35
Contrôleur SCSI	VirtIO SCSI single
Lecteur CD/DVD (ide2)	local:iso/ipfire-2.29-core198-x86_64.iso,media=cdrom,size=634M
Disque dur (scsi0)	DISK-VMs:vm-100-disk-0,discard=on,ioread=1,size=20G,ssd=1
Carte réseau (net0)	virtio=BC:24:11:6B:3C:D3,bridge=vmbr0
Carte réseau (net1)	virtio=BC:24:11:22:D1:B3,bridge=lan

Attention, pensez à bien ajouter **2 cartes réseau** à votre pare-feu. En effet, le pare-feu sera configuré en mode **RED** + **GREEN**.

La carte réseau (net0) sera connectée au « **vmbr0** » pour permettre l'accès à Internet via le vmbr0 : interface **RED**.

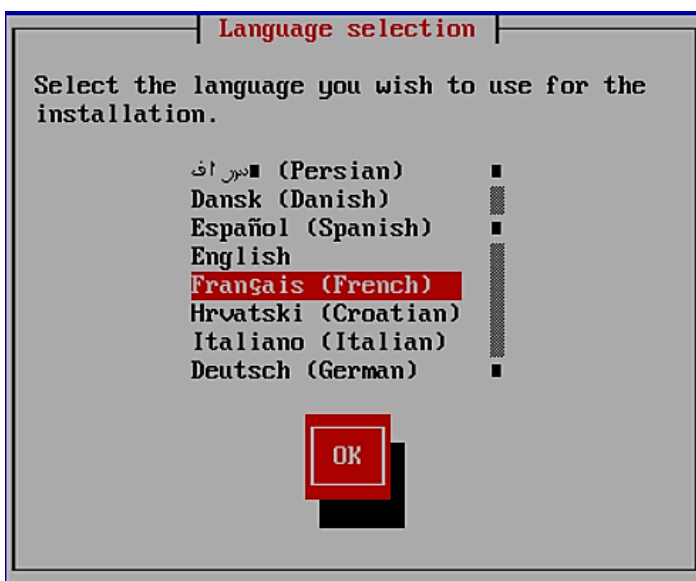
La carte réseau (net1) sera connectée au vmbr1 que l'on a renommé « **lan** » et permettra de connecter les futures VMs : interface **GREEN**.

3^{ème} étape : lancement de l'installation du pare-feu IPFire

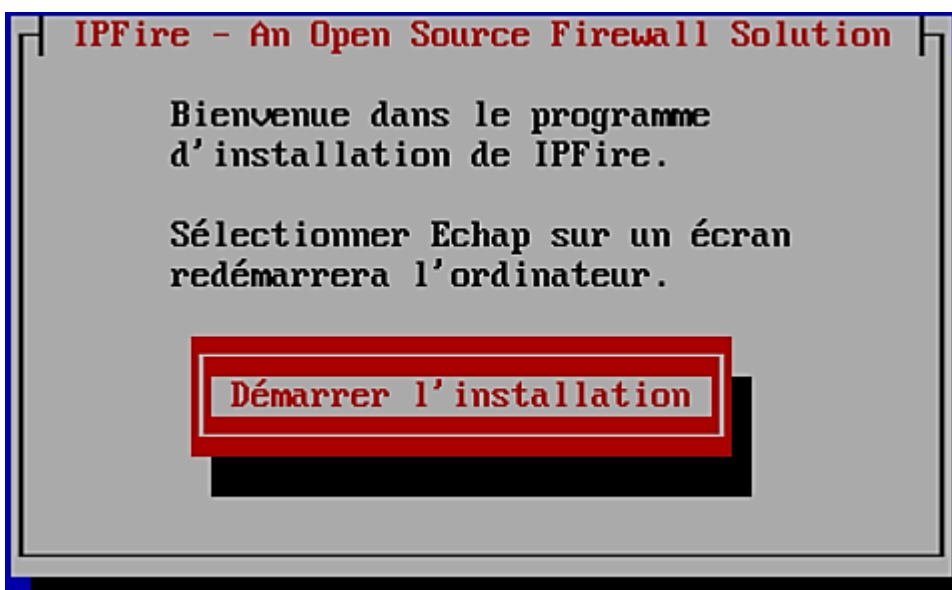
- Lancez l'installation de votre machine ; un assistant d'installation vous proposera différents écrans de configuration. Au lancement, la page IPFire s'affiche ; pressez la touche Entrée :



- Sélectionnez le langage et pressez la touche Entrée :



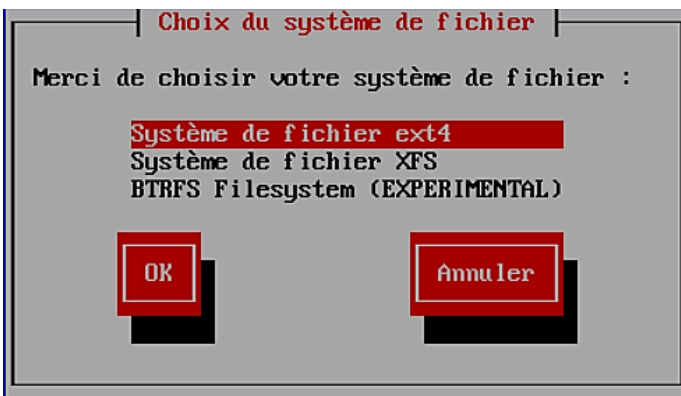
- Pressez la touche Entrée pour lancer l'installation :



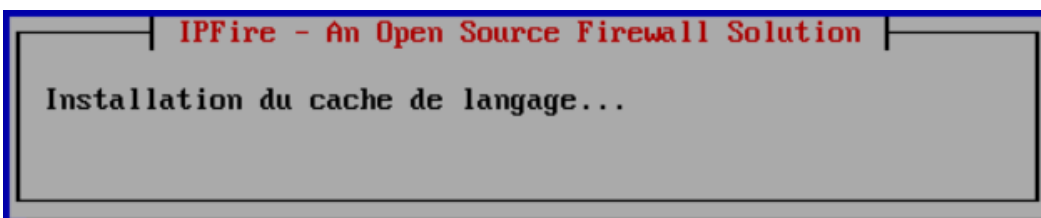
- Pressez la touche Entrée pour lancer la configuration du disque) :



- Conservez le système de fichiers « **ext4** » et pressez la touche Entrée :



- Patientez quelques instants...



- Pressez la touche Entrée pour faire redémarrer la machine :



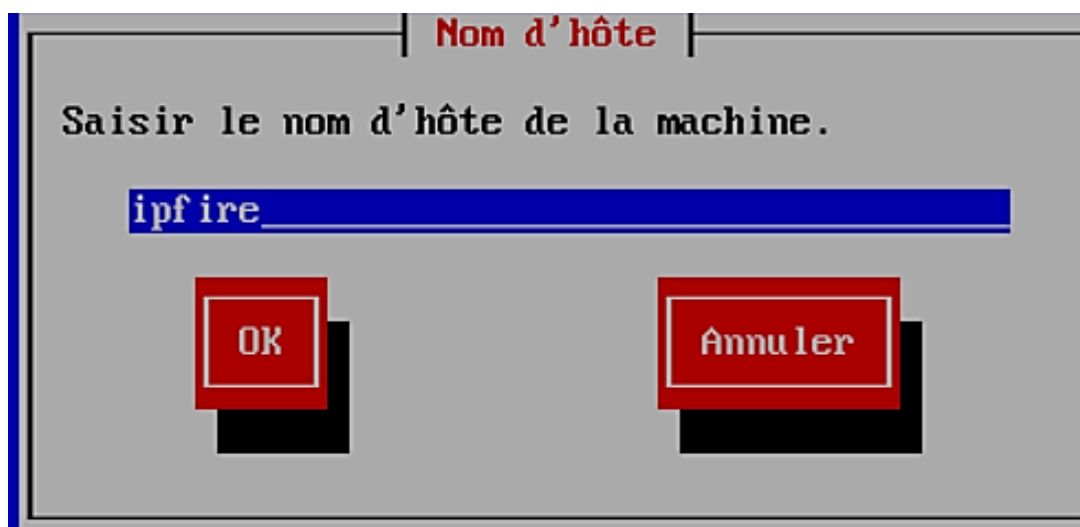
- Sélectionnez le mappage de clavier « **fr** » et pressez la touche Entrée :



- Sélectionnez le fuseau horaire « **Europe/Paris** » et pressez la touche Entrée :



- Saisissez, si vous le souhaitez, un nom d'hôte et pressez la touche Entrée (ici, nous n'avons rien modifié) :



- Saisissez éventuellement un nom de domaine (inutile dans notre cas) et pressez la touche Entrée :



The screenshot shows a dialog box titled "Nom de domaine" in red text. The main text reads "Saisir le nom de domaine." Below this is a blue text input field containing the text "localdomain". At the bottom of the dialog are two red buttons with white text: "OK" on the left and "Annuler" on the right.

- Saisissez le mot de passe du « **root** » permettant de se loguer en console et pressez la touche Entrée :



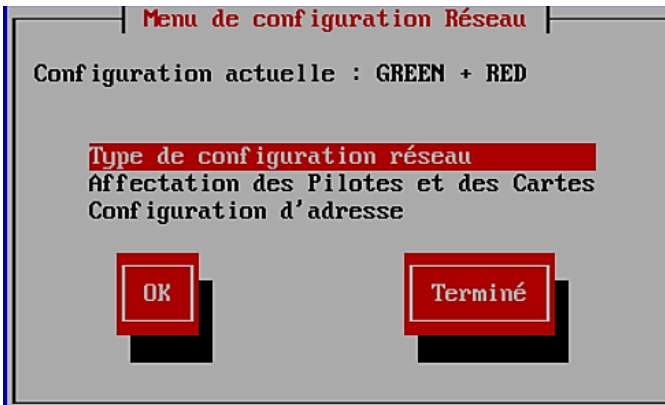
The screenshot shows a dialog box titled "IPFire - www.ipfire.org" in red text. The main text reads "Saisir le mot de passe du super-utilisateur 'root' permettant de se connecter en ligne de commande." Below this are two labels, "Mot de passe :" and "Confirmer :", each followed by a blue text input field. At the bottom are two red buttons with white text: "OK" on the left and "Annuler" on the right.

- Saisissez le mot de passe du **compte « admin »** qui permet de le loguer à l'interface graphique d'IPFire et pressez la touche Entrée :

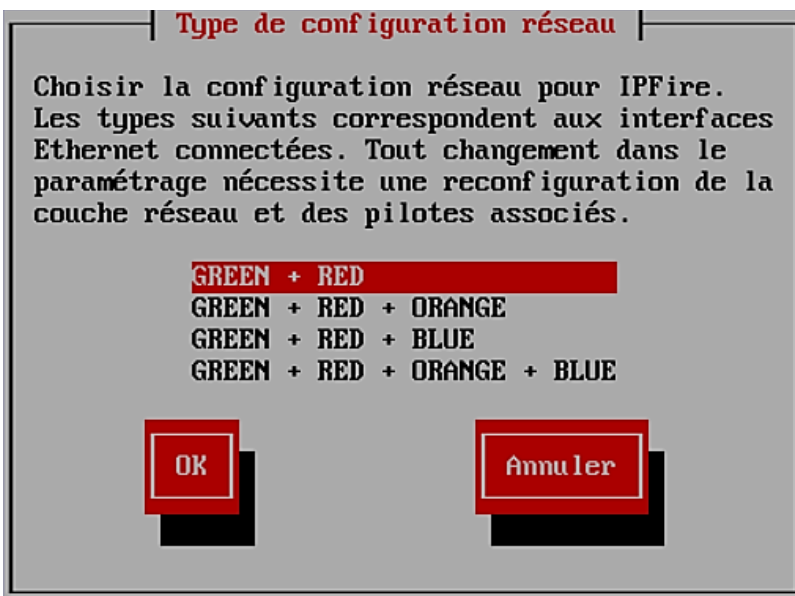


The screenshot shows a dialog box titled "IPFire - www.ipfire.org" in red text. The main text reads "Saisir le mot de passe IPFire de l'utilisateur 'admin' nécessaire à la connexion aux pages web d'administration IPFire." Below this are two labels, "Mot de passe :" and "Confirmer :", each followed by a blue text input field. At the bottom are two red buttons with white text: "OK" on the left and "Annuler" on the right.

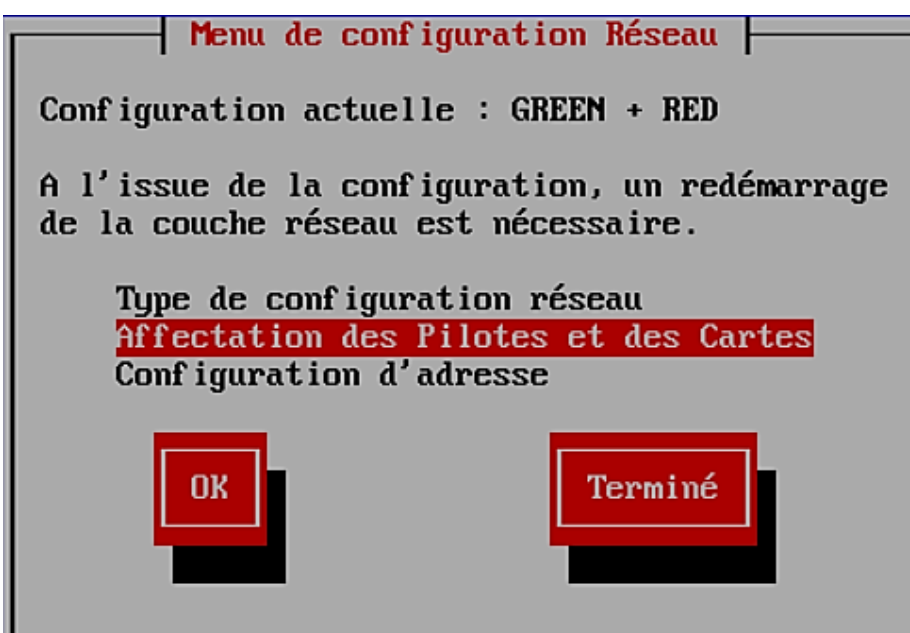
- Sélectionnez « **Type de configuration réseau** » et pressez la touche Entrée :



- Sélectionnez « **GREEN + RED** » et pressez la touche Entrée :



- Sélectionnez « **Affectation des pilotes et des cartes** » et pressez la touche Entrée :



- Sélectionnez l'interface « **RED** » et pressez la touche Entrée :



- Sélectionnez la carte réseau qui sera connectée à l'interface « **RED** » c'est-à-dire la carte connectée au « vmbr0 » de votre serveur Proxmox. Vérifiez bien qu'il s'agit de la bonne carte en contrôlant l'adresse MAC puis pressez la touche Entrée :

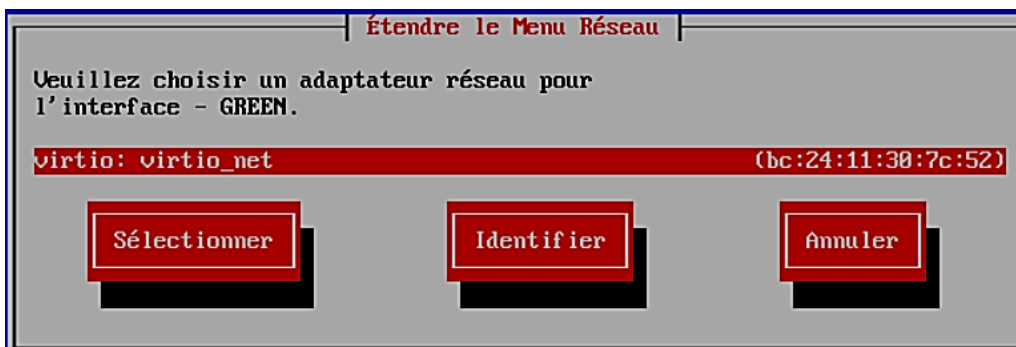


- Sélectionnez l'interface « **GREEN** » et pressez la touche Entrée :

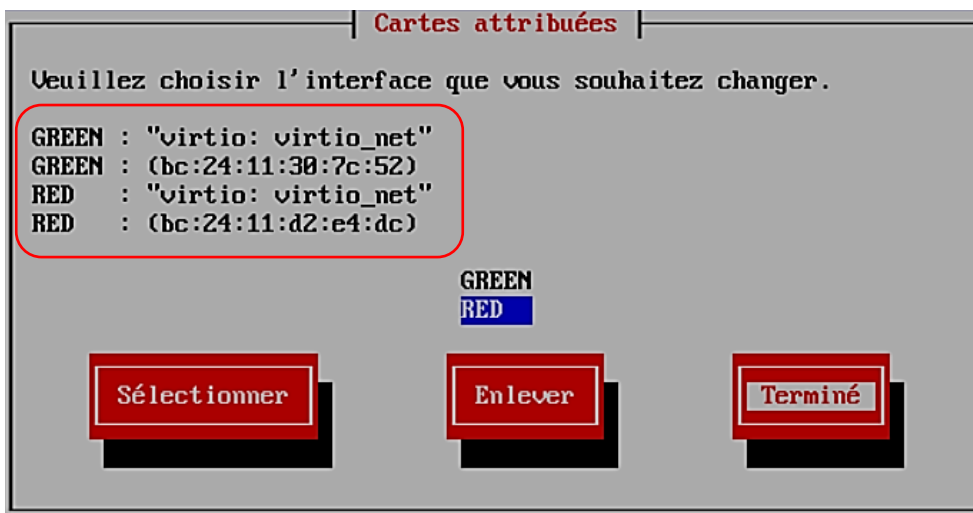


7

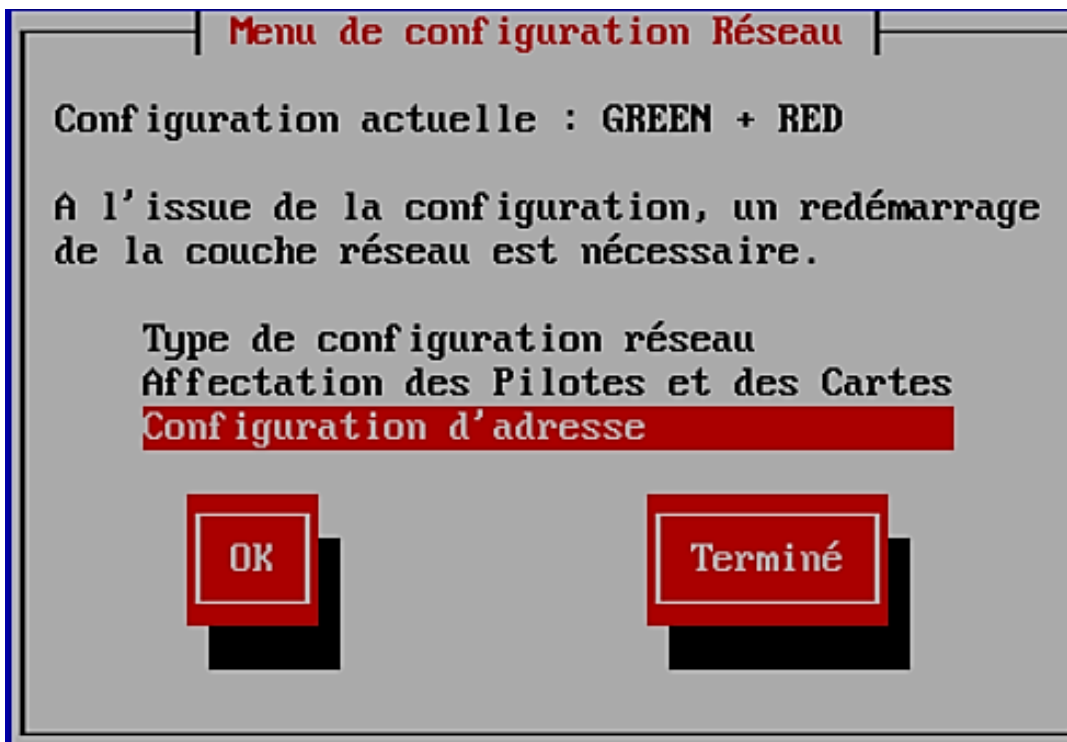
- Sélectionnez l'interface « **GREEN** » restante et pressez la touche Entrée :



- L'attribution des cartes a été effectuée : contrôlez que l'attribution est bonne puis déplacez-vous sur le bouton « **Terminé** » et pressez la touche Entrée :



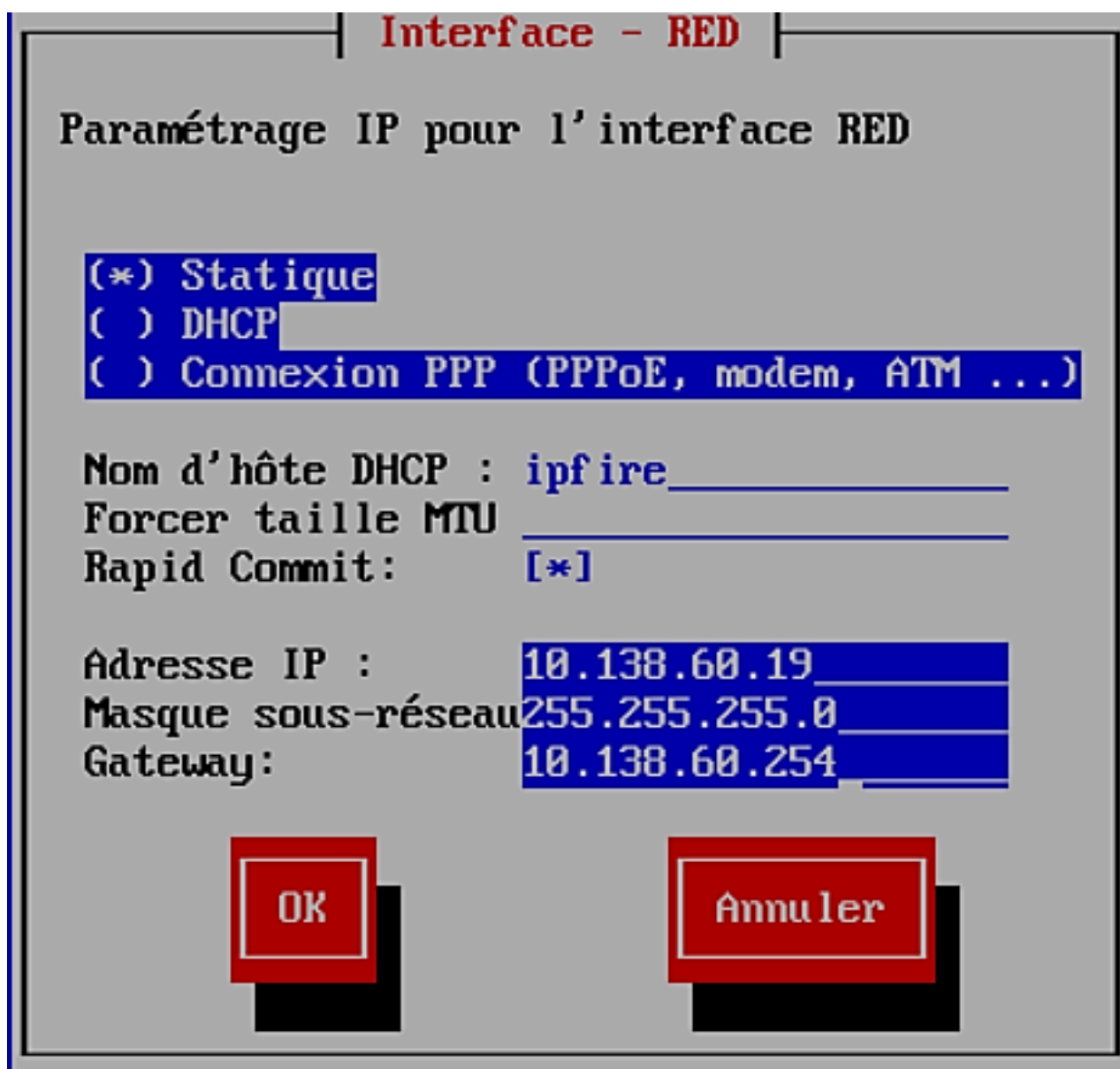
- Sélectionnez « **Configuration d'adresse** » et pressez la touche Entrée :



- Sélectionnez l'interface « **RED** » et pressez la touche Entrée :



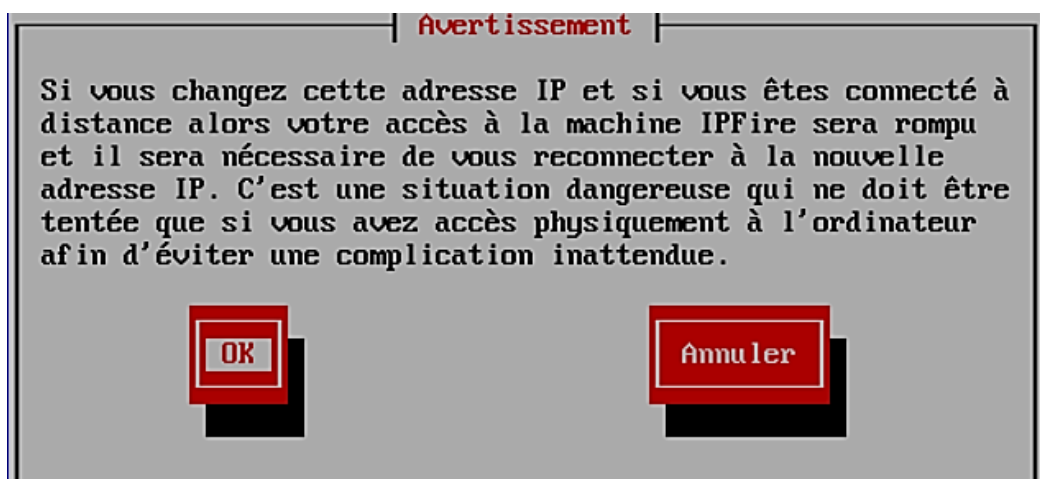
- Sélectionnez « **Statique** » en pressant la barre d'espace puis saisissez l'adresse IP WAN qui vous a été affectée au sein du vlan 60 (espace atelier). Saisissez la passerelle du vlan 60 (ici **10.138.60.254**) puis pressez la touche Entrée pour valider les paramètres IP de l'interface RED :



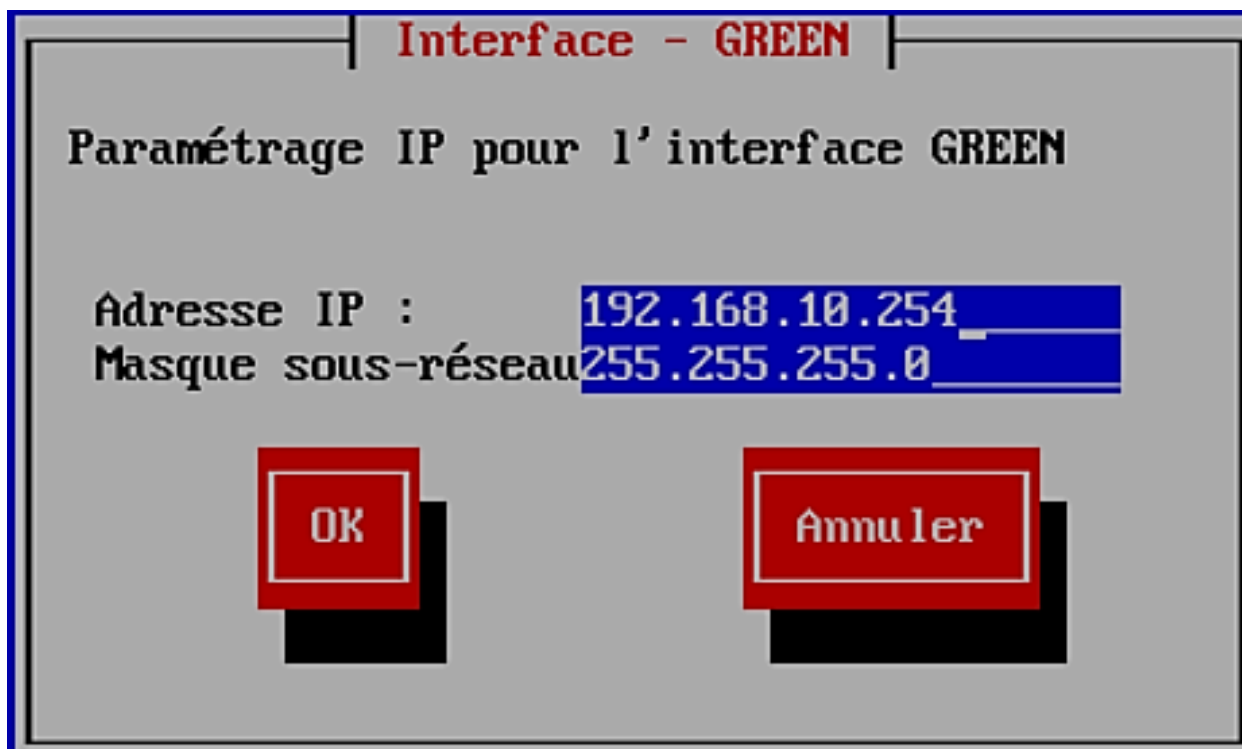
- Sélectionnez l'interface « **GREEN** » et pressez la touche Entrée :



- Déplacez-vous sur le bouton « **OK** » et pressez la touche Entrée :



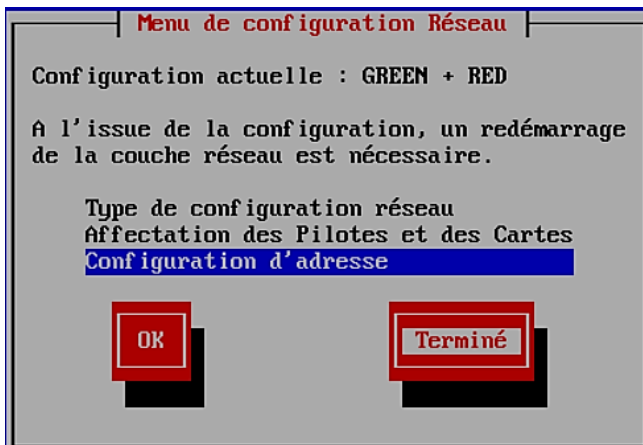
- Saisissez l'adresse IP que vous souhaitez affecter à l'interface graphique d'IPFire (votre LAN) et pressez la touche Entrée :



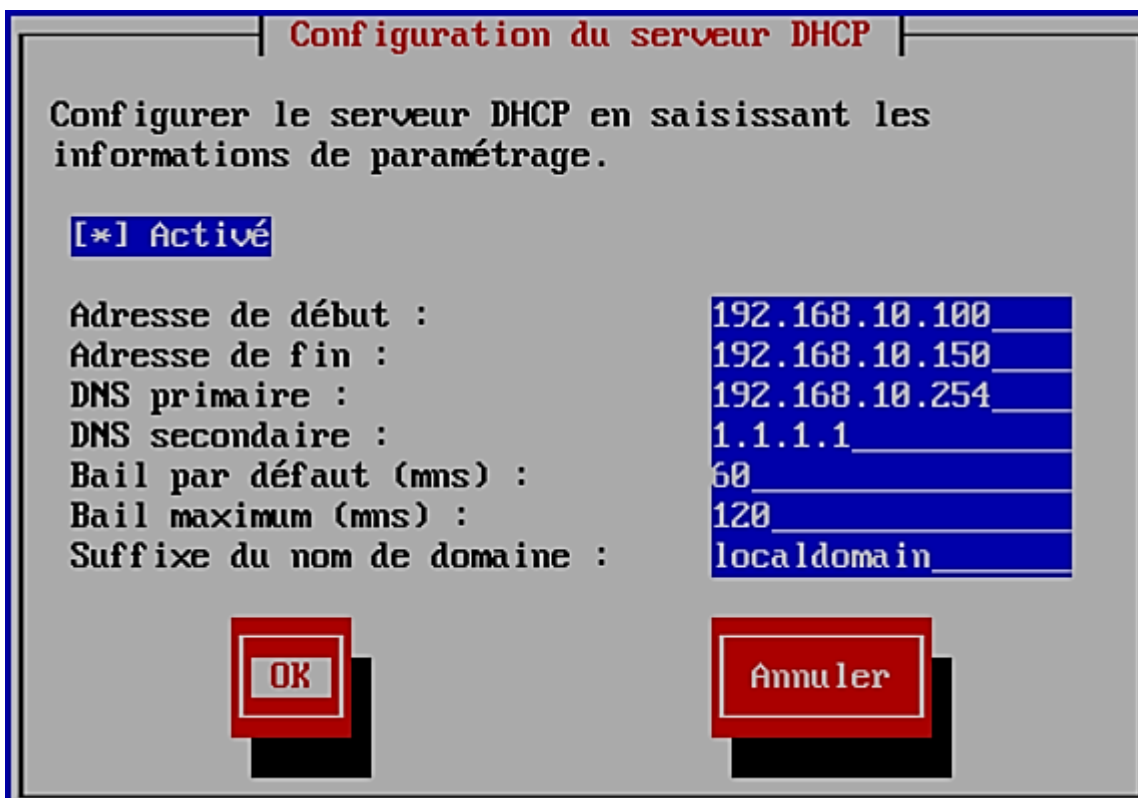
- Déplacez-vous sur le bouton « **Terminé** » et pressez la touche Entrée :



- Déplacez-vous sur le bouton « **Terminé** » et pressez la touche Entrée :



- Pressez la barre d'espace pour activer le service DHCP sur le réseau LAN et saisissez l'étendue DHCP souhaitée. Ici, nous avons indiqué un pool DHCP s'étendant de 192.168.10.100 à 192.168.10.150. Indiquez comme passerelle l'interface « GREEN » de votre IPFire et ajoutez le DNS de Cloudflare ; pressez la touche Entrée :



- Pressez la touche Entrée pour finaliser l'installation et faire redémarrer votre machine :



- Patientez pendant le redémarrage de votre machine :

```
Stopping kernel log daemon... [ OK
Stopping system log daemon... [ OK
Bringing up the loopback interface... [ OK
Setting hostname to ipfire.localdomain... [ OK
Setting up firewall [ OK
INIT: Entering runlevel: 3
Starting vnstatd...
No interfaces found in database, adding available interfaces...
Interface "red0" added with 1000 Mbit bandwidth limit.
Interface "green0" added with 1000 Mbit bandwidth limit.
-> 2 new interfaces found.
Limits can be modified using the configuration file. See "man vnstat.conf".
Unwanted interfaces can be removed from monitoring with "vnstat --remove".
Starting kernel log daemon... [ OK
Starting system log daemon... [ OK
Saving Bootlog... [ OK
Starting Unbound DNS Proxy... [ OK
Starting ACPI daemon... [ OK
Enabling S.M.A.R.T.: sda [ OK
Bringing up the green0 interface...
Adding IPv4 address 192.168.10.254 to the green0 interface... [ OK
Bringing up the red0 interface...
Adding IPv4 address 10.138.60.19 to the red0 interface... [ OK
Setting up default gateway 10.138.60.254... [ OK
Adding static routes... [ OK
```

- Au redémarrage, vérifiez que tout est « OK » et le login s'affiche :

```
Starting the Cyrus SASL Server... [ OK
Setting time on boot... [ OK
Starting ntpd... [ OK
Starting DHCP Server... [ OK
Starting Unbound DHCP Leases Bridge... [ OK
Starting Apache daemon... [ OK
Starting fcron... [ OK

IPFire v2.29 - www.ipfire.org
=====
ipfire.pve1.home running on Linux 6.12.41-ipfire x86_64
ipfire login:
```

Vous pouvez tester que la connexion Internet est opérationnelle en vous loguant en tant que « root » avec le mot de passe défini lors de l'installation et en effectuant un test de ping vers 1.1.1.1 avec la commande suivante :

ping -c3 1.1.1.1

```
IPFire v2.29 - www.ipfire.org
=====
ipfire.pve1.home running on Linux 6.12.41-ipfire x86_64
ipfire login: root
Password:
No mail.
[root@ipfire ~]# ping -c3 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=54 time=11.7 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=54 time=38.6 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=54 time=10.4 ms

--- 1.1.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 10.415/20.223/38.603/13.006 ms
```

4 – ACCES A L'INTERFACE DE GESTION DE IPFIRE

Pour administrer IPFire, vous disposez d'une interface graphique (GUI). Par défaut, si vous souhaitez accéder à l'interface d'IPFire, vous ne pouvez le faire que depuis un PC connecté au réseau « LAN » de votre pare-feu. Si vous souhaitez accéder à IPFire depuis « l'extérieur », la création d'une règle est nécessaire.

Attention, l'accès à l'interface de gestion d'IPFire depuis l'extérieur peut présenter une importante faille de sécurité !

Depuis une machine virtuelle connectée à votre réseau local « **Lan** » :

- Ouvrez un navigateur et saisissez l'adresse « **Lan** » que vous avez configurée : <https://192.168.10.254:444>
- Saisissez « **admin** » et le mot de passe que vous avez défini lors de l'installation :

Ce site vous demande de vous connecter.

Nom d'utilisateur

Mot de passe

- Cliquez le bouton bleu « **Connexion** »
- L'interface d'accueil s'affiche :

IPFire_ - ipfire.pve1.home

[Système](#) [Statut](#) [Réseau](#) [Services](#) [Pare-feu](#) [IPFire](#) [Journaux](#)

Traffic ROUGE: Entrée 0.00 bit/s Sortie 0.00 bit/s

Page principale ?

Réseau	Adresse IP	Statut
INTERNET	192.168.168.101	Connecté - (32m)
Nom hôte: ipfire.pve1.home		
Passerelle: 192.168.168.254		

Réseau	Adresse IP	Statut
LAN	10.10.100.254/24	Proxy inactif

L'interface d'accueil présente les 2 réseaux : **WAN** (« red ») et **LAN** (« green ») avec leurs adresses respectives :

Réseau	Adresse IP	
INTERNET	192.168.168.101	L'adresse WAN de votre réseau est affichée ici (réseau « red »).
Nom hôte:	ipfire.pve1.home	
Passerelle:	192.168.168.254	

Réseau	Adresse IP	
LAN	10.10.100.254/24	L'adresse LAN de votre réseau est affichée ici (réseau « green »).

Votre pare-feu est maintenant opérationnel !

4 – ACCES AU SERVEUR DHCP DE IPFIRE

Depuis l'interface de gestion de IPFIRE, effectuez la manipulation suivante :

- Cliquez le menu « Réseau »
- Cliquez « Serveur DHCP » ; une fenêtre s'ouvre :

Configuration DHCP ? On peut désactiver le serveur DHCP en décochant cette case.

DHCP

Interface VERTE

Activé : ☒

Adresse de début : * 10.10.100.100

Refuser les clients connus : ☐

Durée du bail par défaut (minutes) : * 60

Suffixe du nom de domaine : pve1.home

DNS primaire : * 10.10.100.25

Adresse IP Masque réseau: 10.10.100.150

Adresse de fin : * 10.10.100.150

Durée maximum du bail (minutes) : * 120

Autoriser les clients bootp: ☐

DNS secondaire : 10.10.100.254

On peut personnaliser la durée du bail DHCP par défaut ici.

On peut personnaliser les adresses des serveurs DNS ici.

Étendue DHCP (modifiable).

5 – ACCES AU PARAMETRAGE DES REGLES DE PARE-FEU DE IPFIRE

Lorsque vous mettrez en place divers services sur vos machines, il sera nécessaire d'ouvrir les ports correspondants sous peine de ne pas pouvoir accéder aux applications installées.

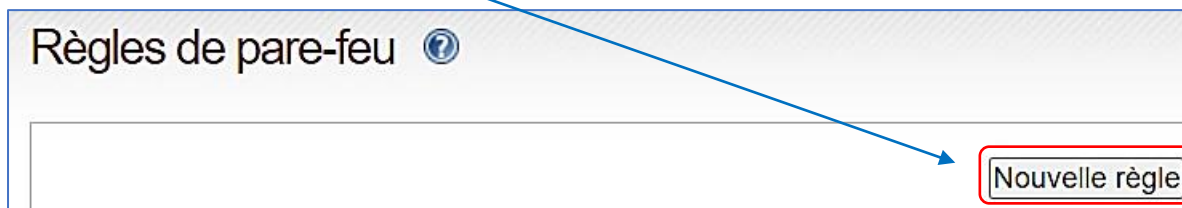
Par exemple, si nous souhaitons activer SSH sur une machine Debian et y accéder depuis l'extérieur, il est impératif de configurer l'ouverture du port à destination de la machine concernée.

Prenons l'exemple d'une machine Debian qui possède l'adresse IP 10.10.100.102/24 et le service SSH a été activé sur cette machine avec le port « 5522 ».

Pour accéder à la machine depuis un poste du labo SIO, il est nécessaire d'ouvrir, sur IPFIRE, le port « 5522 » qui correspond au service SSH personnalisé de la machine Debian et de le faire « pointer » vers la machine Debian de notre réseau local.

Pour cela, depuis l'interface de gestion de IPFIRE, effectuez les manipulations suivantes :

- Cliquez le menu « **Pare-feu** » et « **Règles de pare-feu** »
- Cliquez le bouton « **Nouvelle règle** » :



On paramètre la règle ainsi :

1^{ère} étape : réglage de la source et de la destination

Règles de pare-feu ⓘ

Source

☐ Adresse source (adresse MAC/IP ou réseau) :

☒ Réseaux standards : **ROUGE**

☐ Localisation : **A1 - Anonymous Proxy**

1 – ACTIVATION DE LA SOURCE
« Tout ce qui arrive par l'interface ROUGE (« Wan ») »

NAT

☒ Utiliser la traduction d'adresses réseau (NAT)
☒ Destination NAT (redirection de port)

☐ Source NAT

Interface pare-feu: **- Automatique -**

2 – ACTIVATION DU « NAT »
Traduction et redirection de la requête vers le port concerné

Destination

☒ Adresse IP de destination (adresse IP ou réseau) : **10.10.100.102**

☐ Firewall

3 – MACHINE DE DESTINATION
Machine vers laquelle on veut appliquer la règle

Tous

2^{ème} étape : choix du protocole et du numéro de port de destination

Protocole

TCP

Port source :

Port de destination : **5522**

Port externe (NAT):

On sélectionne, ici, le protocole concerné et on indique le n° du port à ouvrir vers la machine de destination.

3^{ème} étape : validation des paramètres

Paramètres additionnels

Remarque :

Position de règle :

☐ Journalisation de la règle
☐ Utiliser les contraintes horaires
☐ Limiter les connexions simultanées par adresse IP
☐ Limiter le nombre des nouvelles connexions

Vérifiez vos paramètres et, si tout est cohérent, cliquez le bouton « Ajouter ».

La règle s'affiche dans l'interface d'accueil de IPFIRE :

Règles de pare-feu					
#	Protocole :	Source	Journal	Destination	Action
1	TCP	ROUGE	☐	Pare-feu : 5522 ->10.10.100.102: 5522	☒   
SSH DEBIAN TEMPLATE					

- Cliquez sur le bouton « **Appliquer les changements** » :

Testez l'accès, via SSH, à votre machine Debian de la manière suivante :

- Depuis un poste du labo SIO, ouvrez la console en pressant les touches « **Windows** » + « **R** »
- Saisissez « **cmd** »
- Saisissez **ssh -pXXX nom_utilisateur_debian@votre_ip_wan**
- Validez l'échange des clés de vérification entre les machines « **Yes** »
- Normalement, la console de votre machine Debian est active !

Si vous n'accédez pas à votre machine Debian via SSH, vérifiez votre règle de pare-feu !

Ces manipulations seront à refaire lorsque vous activerez d'autres services sur votre machine Debian et qui devront être accessibles depuis l'extérieur (serveur SQL, serveur web, etc.).

Remarques : depuis une machine du réseau local (LAN), il n'est pas utile de créer une règle puisque les flux sont autorisés par défaut.

Si vous souhaitez accéder à votre IPFire depuis la WAN, il faudra créer une règle autorisant l'accès à votre pare-feu depuis la WAN et avec le port TCP 444 (port par défaut du pare-feu IPFire).