

# 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 lycée
  - 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](http://tutos-info.fr) - 10/2023



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 pour [IPSec](#) et serveur [OpenVPN](#)
- Serveur DHCP
- Dynamic DNS (DynDNS, No-IP)
- Analyse fonctions de surveillance du système et [analyse des 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 (labo SIO)

---

**IPFire** a été installé sur les serveurs Proxmox du labo SIO en tant que machines virtuelles. Ces machines virtuelles sont peu gourmandes en ressources puisqu'elles s'exécutent avec 768 Mo de RAM et un disque système inférieur à 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 et vérifier que l'espace disque système est suffisant (minimum 20 Go).

Tout au long de votre formation de 1<sup>ère</sup> année, vous allez utiliser vos machines virtuelles (Debian, Windows Server 2022 et Windows 10 Pro) que vous avez paramétrées en début de formation (serveurs Proxmox).

Il faut savoir que ces machines virtuelles sont connectées sur un switch virtuel appelé « vmbr » (1 par étudiant) et que les machines y sont rattachées. Ce switch virtuel (« vmbr ») est lui-même connecté à un routeur virtuel : IPFIRE.

Chaque étudiant possède 1 routeur virtuel IPFIRE. Ce routeur virtuel possède 2 cartes réseau et a été configuré en mode « **RED + GREEN** » :

- Une carte réseau reliée au serveur Proxmox (pour accéder au web) nommée « **INTERFACE Wan** » (**RED**)
- Une carte réseau reliée au réseau interne Proxmox nommée « **INTERFACE Lan** » (**GREEN**)

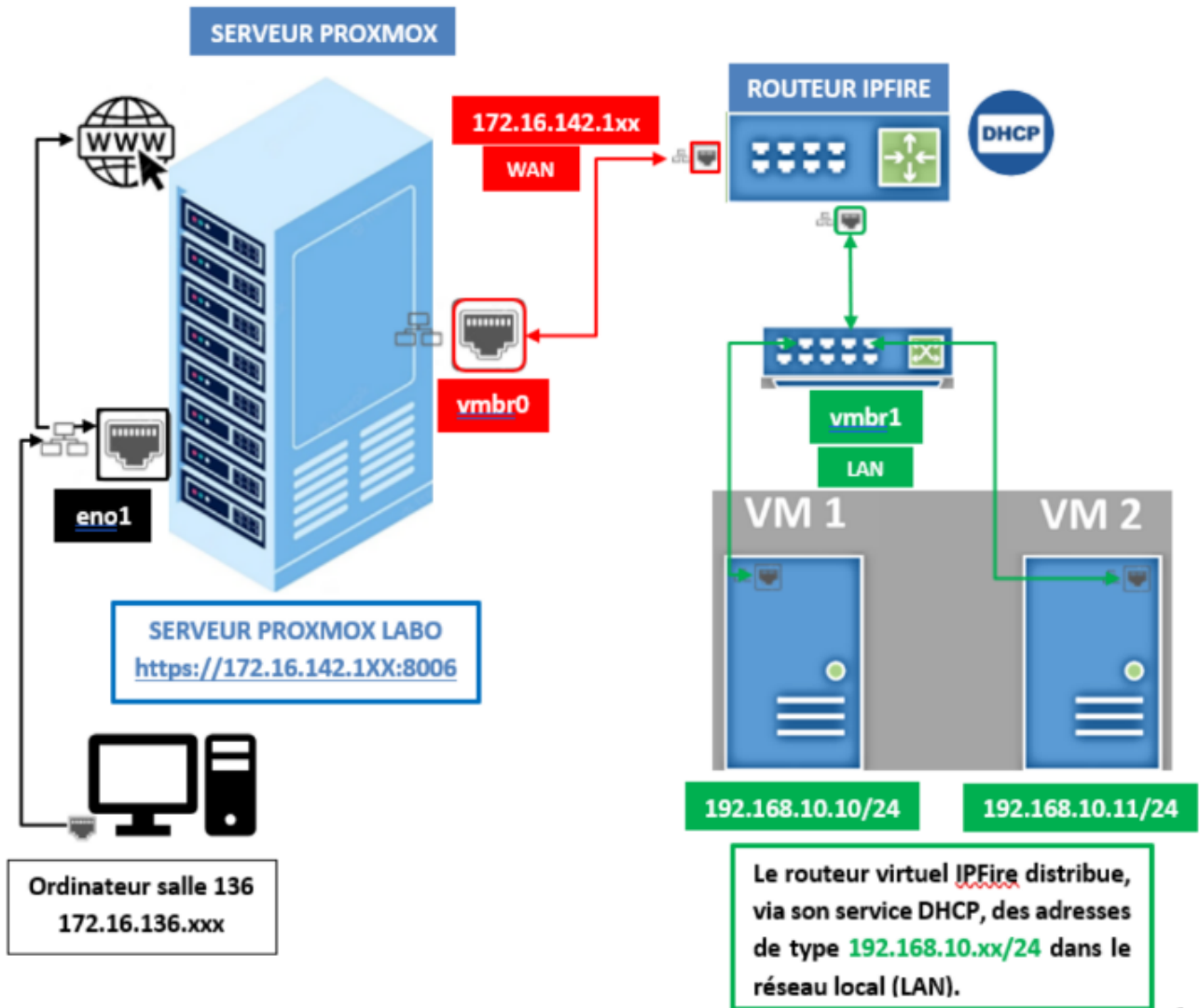
Le routeur virtuel IPFIRE dispose d'un **serveur DHCP** interne qui a été activé. Ce serveur DHCP distribue des adresses IP au sein du réseau local « **Lan** ») et l'étendue est : 192.168.10.10/24 – 192.168.10.50/24

Le routeur virtuel IPFIRE est accessible de 2 façons différentes :

- Soit depuis un poste du lycée en saisissant : [https://adresse\\_wan:444](https://adresse_wan:444)
- Soit depuis une machine virtuelle du réseau local « Lan », en saisissant : <https://192.168.10.254:444>

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

## ARCHITECTURE RESEAU :



## 3 – ACCES A L'INTERFACE DE GESTION DE IPFIRE

a) Depuis un poste du lycée en utilisant l'adresse « Wan » :

- Ouvrez un navigateur et saisissez l'adresse « Wan » communiquée en début d'année : [https://votre\\_wan:444](https://votre_wan:444)
- Saisissez les identifiants qui vous ont été communiqués en début de formation pour vous identifier
- L'interface d'accueil s'affiche :

The screenshot shows the IPFire management interface. The header includes a penguin logo and the text **ipfiredemo.localdomain**. Navigation tabs include **Système**, **Statut**, **Réseau**, **Services**, **Pare-feu**, **IPFire**, and **Journaux**. The **Trafic ROUGE** section shows **Entrée 11.49 kbit/s** and **Sortie 11.34 kbit/s**. The main content area is titled **Page principale** and contains a table with network status information.

Réseau	Adresse IP	Statut
INTERNET	212.129.212.129	Connecté - (58m 34s)
Nom hôte : ev.poneytelecom.eu		
Passerelle : 62.		
Réseau	Adresse IP	Statut
LAN	192.168.100.1/24	Proxy inactif

b) Depuis une machine virtuelle du réseau local « Lan » :

- Ouvrez un navigateur et saisissez l'adresse « Lan » suivante : <https://192.168.10.254:444>
- Saisissez les identifiants qui vous ont été communiqués en début de formation pour vous identifier
- L'interface d'accueil s'affiche :

The screenshot shows the IPFire dashboard with the title 'ipfiredemo.localdomain'. The top navigation bar includes 'Système', 'Statut', 'Réseau', 'Services', 'Pare-feu', 'IPFire', and 'Journaux'. The main content area is titled 'Page principale' and displays a table of network interfaces:

Réseau	Adresse IP	Statut
<b>INTERNET</b>	212.129.212.129	Connecté - (58m 34s)
Nom hôte :	ev.poneytelecom.eu	
Passerelle :	62.	
<b>LAN</b>	192.168.100.1/24	Proxy inactif

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

This image shows a close-up of the network interface table from the previous screenshot. Two callout boxes provide additional information:

- A red callout box points to the WAN IP address (212.129.212.129) with the text: "L'adresse WAN de votre réseau est affichée ici (réseau « red »)."
- A green callout box points to the LAN IP address (192.168.100.1/24) with the text: "L'adresse LAN de votre réseau est affichée ici (réseau « green »)."

## 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 :

The screenshot shows the 'Configuration DHCP' interface. It includes several callouts and annotations:

- A blue callout box at the top left says: "On peut désactiver le serveur DHCP en décochant cette case." (pointing to the 'Activé' checkbox).
- A blue callout box at the top right says: "Etendue DHCP (modifiable)." (pointing to the IP address field).
- A blue callout box at the bottom left says: "On peut personnaliser la durée du bail DHCP par défaut ici." (pointing to the 'Durée du bail par défaut' field).
- A blue callout box at the bottom center says: "On peut personnaliser les adresses des serveurs DNS ici." (pointing to the 'DNS primaire' and 'DNS secondaire' fields).
- A red box highlights the 'Sauvegarder' button at the bottom right.
- A blue callout box at the bottom says: "Lorsque la personnalisation du serveur DHCP est terminée, cliquez le bouton « Sauvegarder » pour enregistrer vos paramètres." (pointing to the 'Sauvegarder' button).

The DHCP configuration form includes the following fields:

- Interface VERTE
- Adresse de début : 192.168.100.100
- Adresse de fin : 192.168.100.150
- Durée du bail par défaut (minutes) : 60
- Durée maximum du bail (minutes) : 120
- Suffixe du nom de domaine : localdomain
- DNS primaire : 192.168.100.1
- DNS secondaire : 9.9.9.9
- Activé :
- Adresse IP : 192.168.100.1
- Masque réseau : 255.255.255.0
- Autoriser les clients bootp :
- Server NTP secondaire : [empty]
- Server WINS secondaire : [empty]

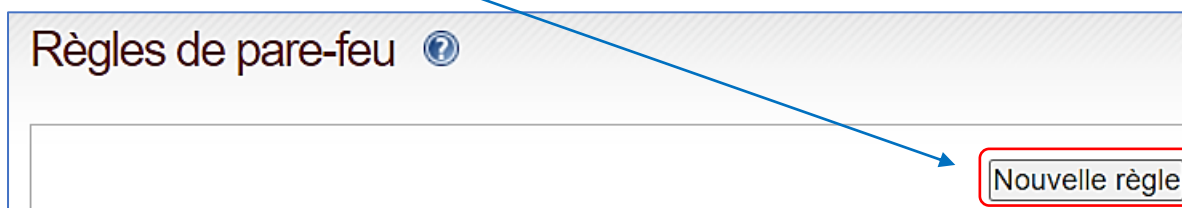
## 5 – ACCES AU PARAMETRAGE DES REGLES DE PARE-FEU DE IPFIRE

Lorsque vous mettez 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.

Notre machine Debian possède l'adresse IP 192.168.100.104/24 et le service SSH a été activé sur cette machine. Pour accéder à la machine depuis un poste du lycée, il est nécessaire d'ouvrir, sur IPFIRE, le port « 22 » qui correspond au service SSH 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<sup>ère</sup> étape** : réglage de la source et de la destination

**Règles de pare-feu** ⓘ

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

Source

Adresse source (adresse MAC/IP ou réseau) :

Réseaux standards :

Localisation :

Firewall :

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

NAT

Utiliser la traduction d'adresses réseau (NAT)

Destination NAT (redirection de port)

Source NAT

Interface pare-feu:

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

Destination

Adresse IP de destination (adresse IP ou réseau) :

Firewall :

## 2<sup>ème</sup> étape : choix du protocole et du numéro de port de destination

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

Protocole :  Port source :  Port de destination :  Port externe (NAT):

## 3<sup>ème</sup> 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 :

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

Règles de pare-feu

Nouvelle règle

Vérifiez la cohérence de la règle saisie sinon vous pouvez bloquer vos accès !

#	Protocole	Source	Journal	Destination	Action
1	TCP	ROUGE	<input type="checkbox"/>	Pare-feu : 22 ->192.168.100.104: 22	<input checked="" type="checkbox"/> <input type="text"/> <input type="text"/> <input type="text"/>
VERT		Internet (Autorisé)			
Politique: Autorisé					

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

- Depuis un poste du lycée, ouvrez la console en pressant les touches « **Windows** » + « **R** »
- Saisissez « **cmd** »
- Saisissez **ssh 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.).