

Trusty, BROUILLON

# Création d'un serveur HTTP (Lighty) + PHP + SQLite

## Note préliminaire :

Dans ce tutoriel, nous supposons un hôte :



- de nom **server.exemple.com**
- d'adresse IP **192.168.0.31**.

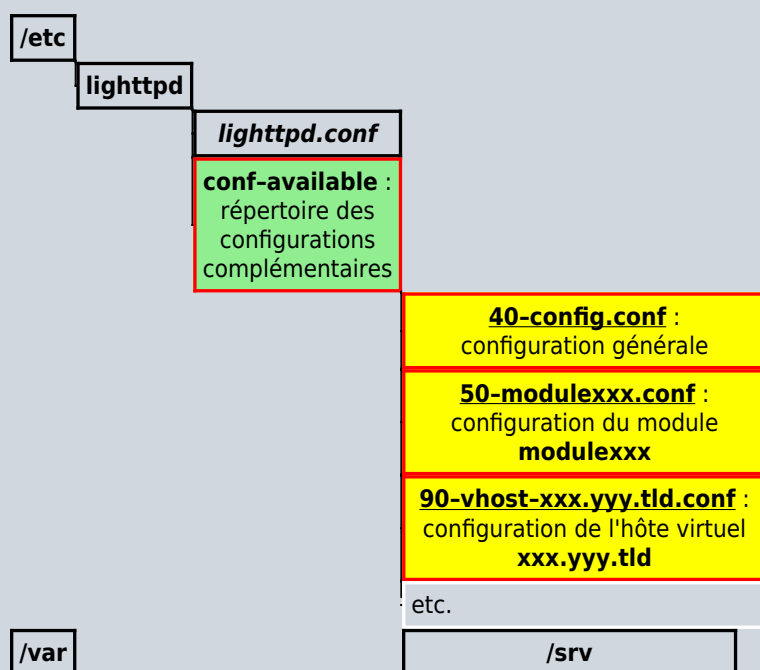
Modifiez ces paramètres selon vos besoins.

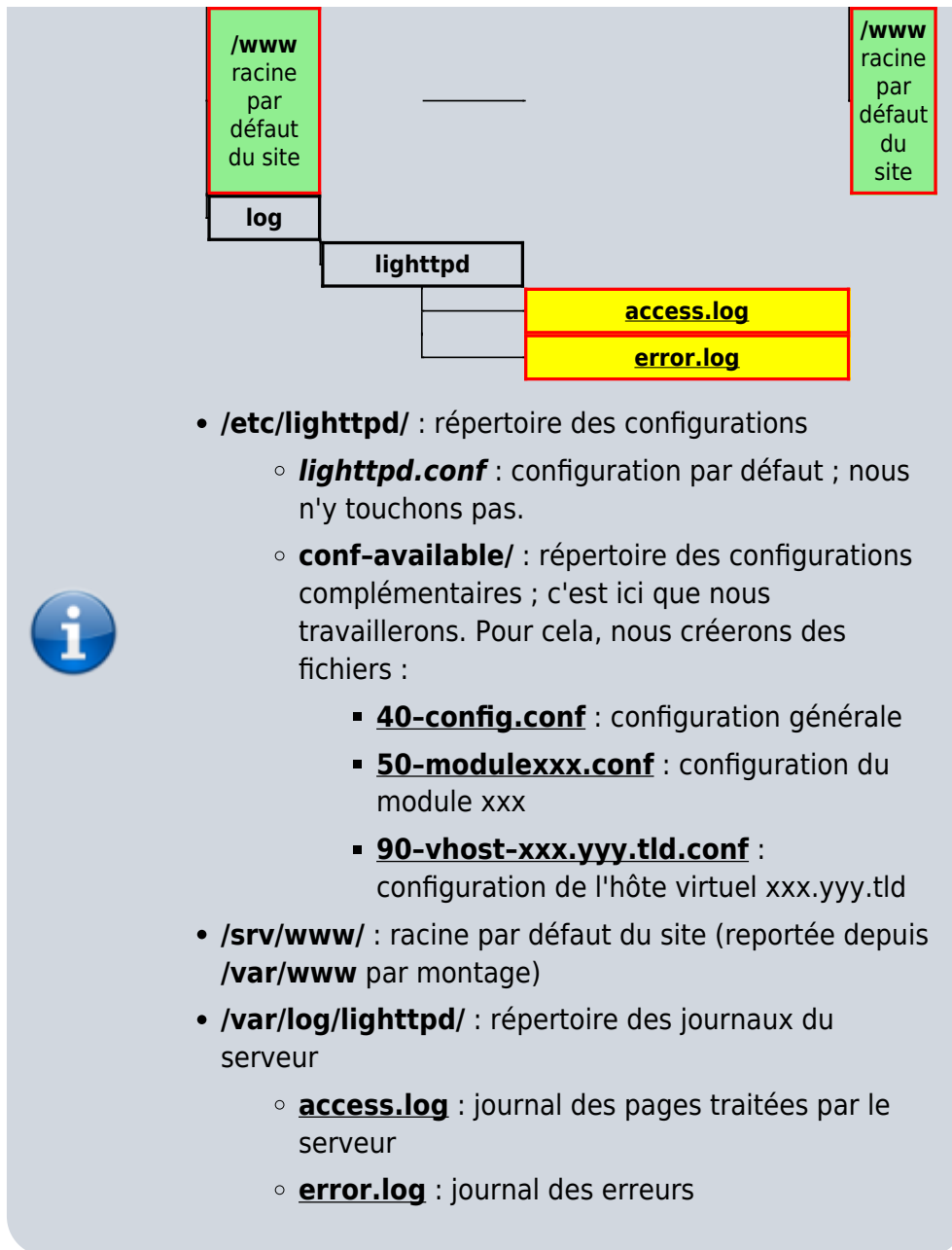
Un serveur **lighttpd** permet de construire un site web accessible via le réseau local (LAN).

En configurant le routeur et le pare-feu, vous pouvez ouvrir l'accès au site via l'Internet (en faisant attention à la sécurité).

## Arborescence de lighty

Voici les dossiers et fichiers importants de **lighty** (les fichiers sont en italique, ceux qui nous servent sont en jaune et soulignés):





Pour ne pas toucher au fichier de configuration par défaut **/etc/httpd/httpd.conf**, livré avec l'application, nous ne travaillerons que dans le répertoire **/etc/httpd/conf-available/**. Ainsi, les réglages ne seront pas affectés par les mises à jour et les migrations seront simplifiées (il suffira de récupérer le fichier de configuration).

Dans ce dossier, nous placerons :

- les réglages généraux dans un fichier spécifique **/etc/httpd/conf-available/40-config.conf**
- les réglages des modules (fichiers **/etc/httpd/conf-available/50-modulexxx.conf**)
- les hôtes virtuels (fichiers **90-vhost-xxx.yyy.tld.conf**)

Le dossier **/var/log/httpd/** contient les journaux (accès : **access.log**, erreurs : **error.log**)

Le dossier **/srv/www/** est la racine du site, de même que **/var/www** (par montage).

# Configuration

## PhpPgAdmin

Créez avec les droits d'administration le fichier **/etc/lighttpd/conf-available/50-phppgadmin.conf** pour y écrire ceci :

[/etc/lighttpd/conf-available/50-phppgadmin.conf](#)

```
# PhpPgAdmin :
alias.url += ( "/phppgadmin" => "/usr/share/phppgadmin/")alias.url
+= ( "/phppgadmin" => "/usr/share/phppgadmin/")
```

Activez cette configuration en lançant :

```
...@...:~ $ sudo lighty-enable-mod phppgadmin
```

## Hôtes virtuels (vhost)

### vhosts utilisateur

Chaque utilisateur du système a accès à son home personnel et à un sous-répertoire `public_html` de son home. Il suffit de créer cette arborescence pour qu'elle soit aussitôt utilisable.

[users.domaine.tld](#)

```
$HTTP["host"] =~ "users\.domaine\.tld" {
    evhost.path-pattern = "/home/%4/public_html/"
}
```

Si **johndoe** est un user, l'adresse <http://johndoe.users.example.org/> ⇒ **/home/johndoe/public\_html/**

### Méthode plus générale

Toujours pour l'utilisateur **johndoe**,

[users.domaine.tld](#)

```
$HTTP["host"] =~ "users\.domaine\.tld" {
    server.document-root = "/home/%4/sites/default/site"
    evhost.path-pattern   = "/home/%4/sites/%0/site/"
}
```

- Si **johndoe.users.domaine.tld** est demandé, et que **/home/johndoe/sites/domaine.tld/site/** est trouvé, ce chemin devient la docroot.

- Si **johndoe.users.domaine.tld** est demandé mais qu'il n'existe pas de répertoire **/home/johndoe/sites/domaine.tld/site/**, alors la docroot reste **/home/johndoe/sites/default/site**.

## Rendre le serveur disponible sur Internet

Il reste à rediriger le port 80 (en TCP) vers la machine qui supporte le serveur http, comme ceci :

paramètres de la freebox → mode avancé → réseau local/redirection de ports :

ajouter une redirection,

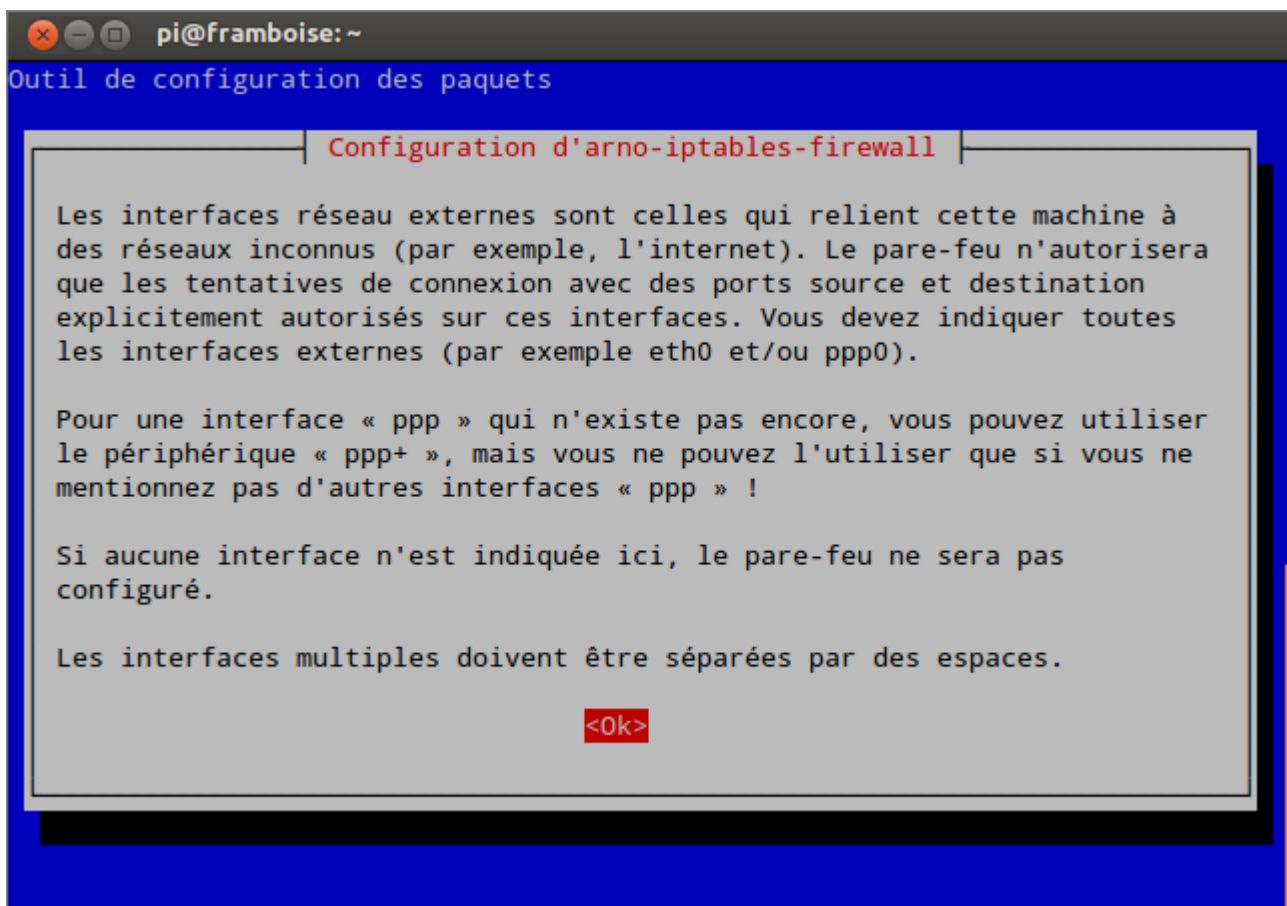
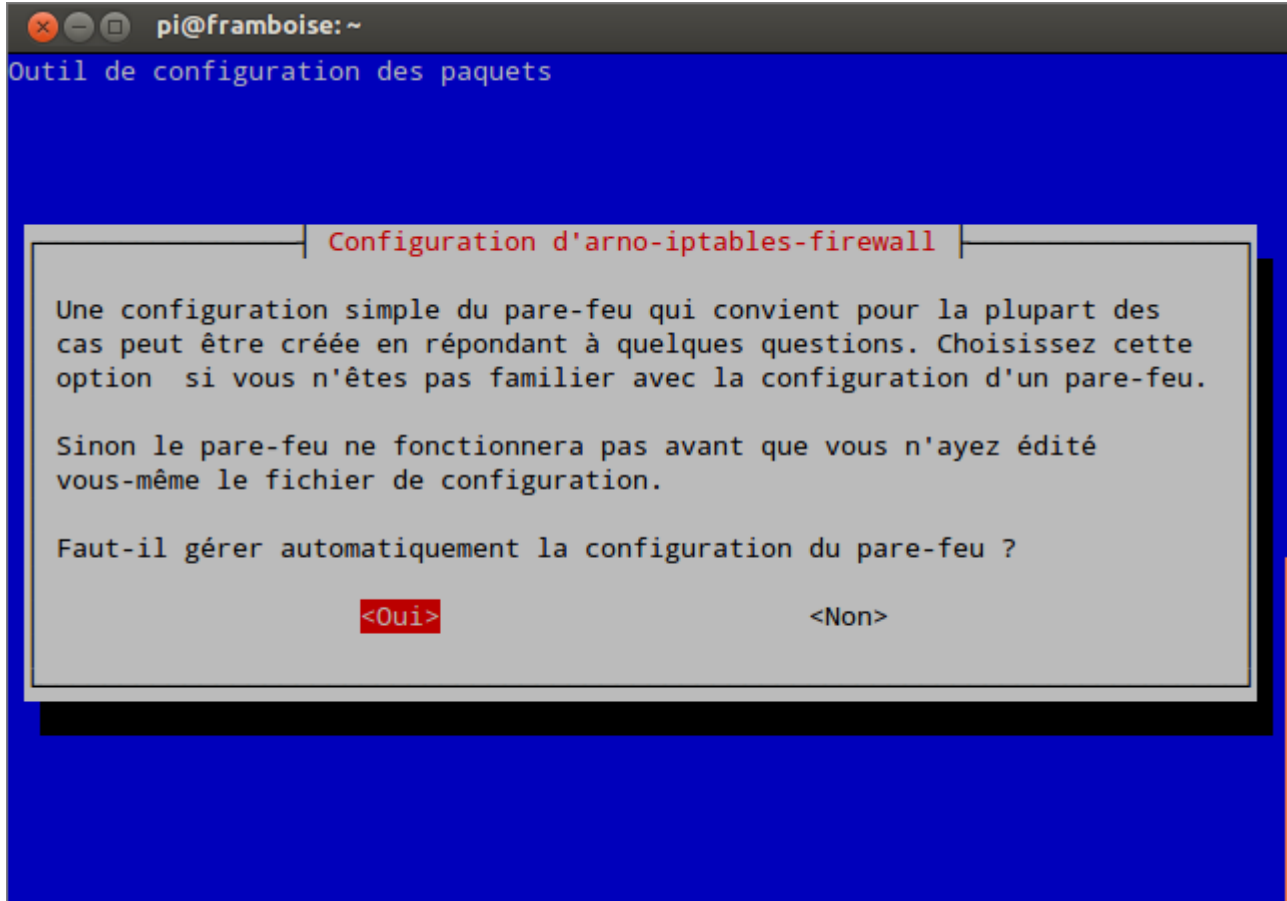
- port de début : 80
- port de fin : 80
- TCP
- choisir l'IP de la machine qui supporte le serveur
- commentaire : par exemple, serveur http framboise

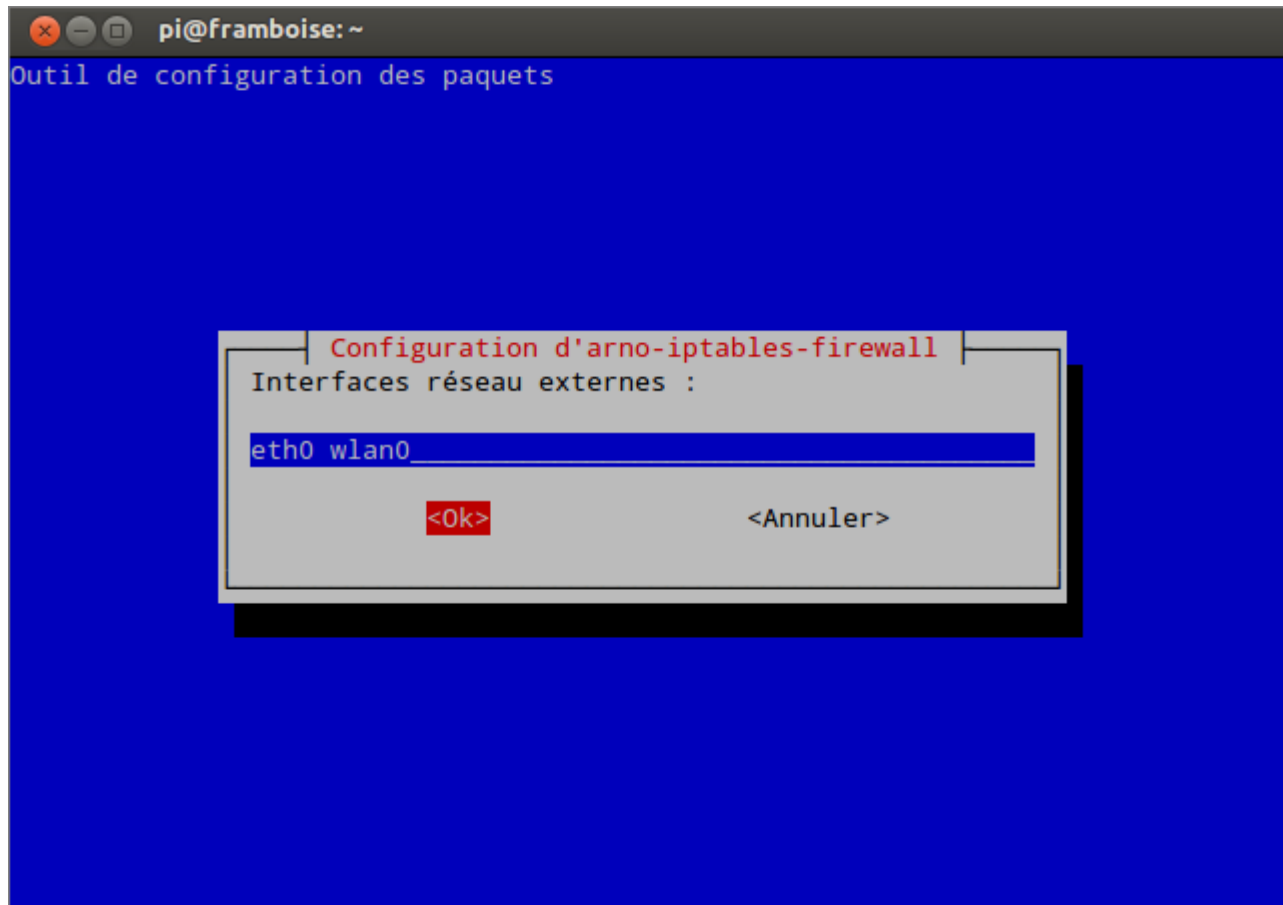
## Pare-feu

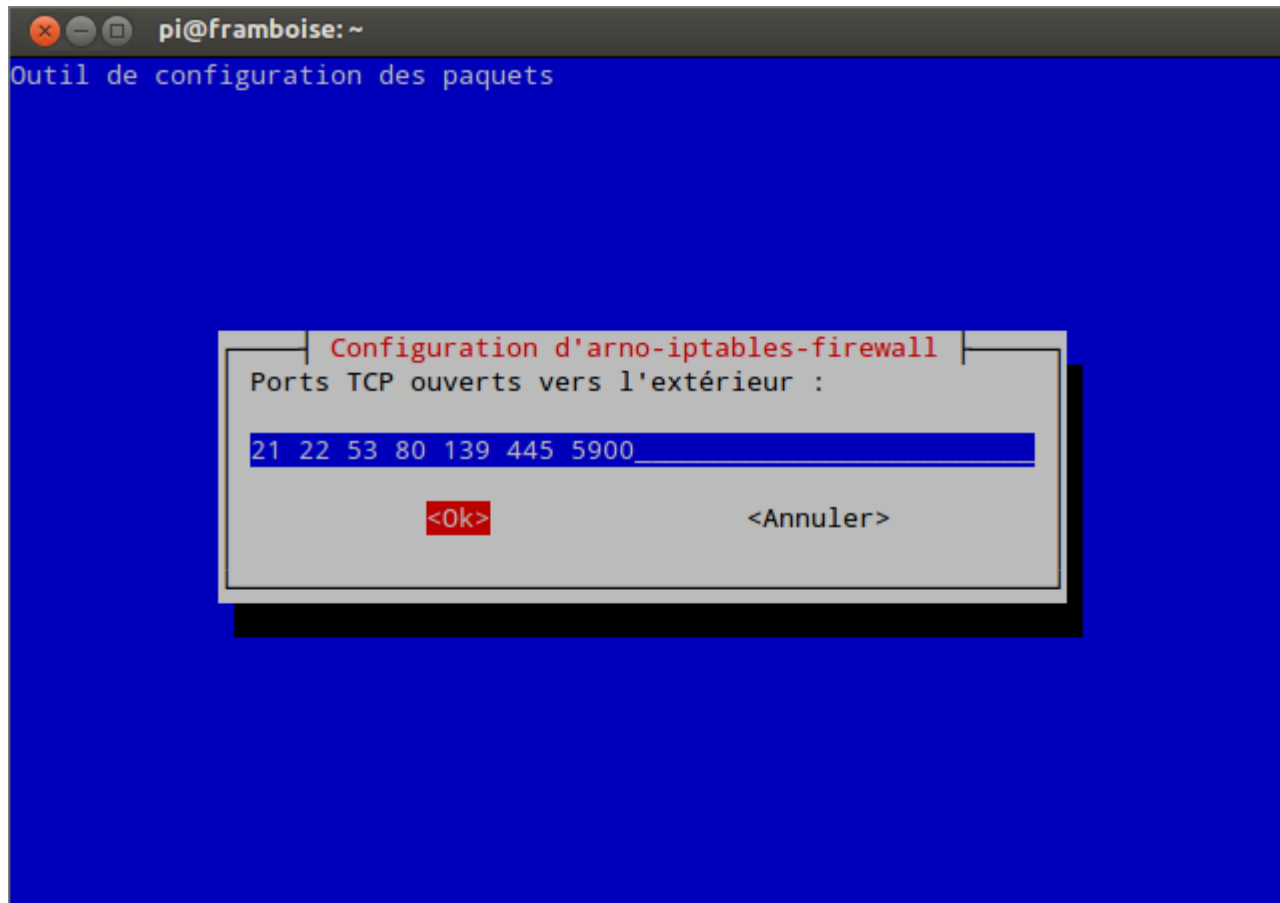
Installez le paquet **arno-iptables-firewall** ou en ligne de commande :

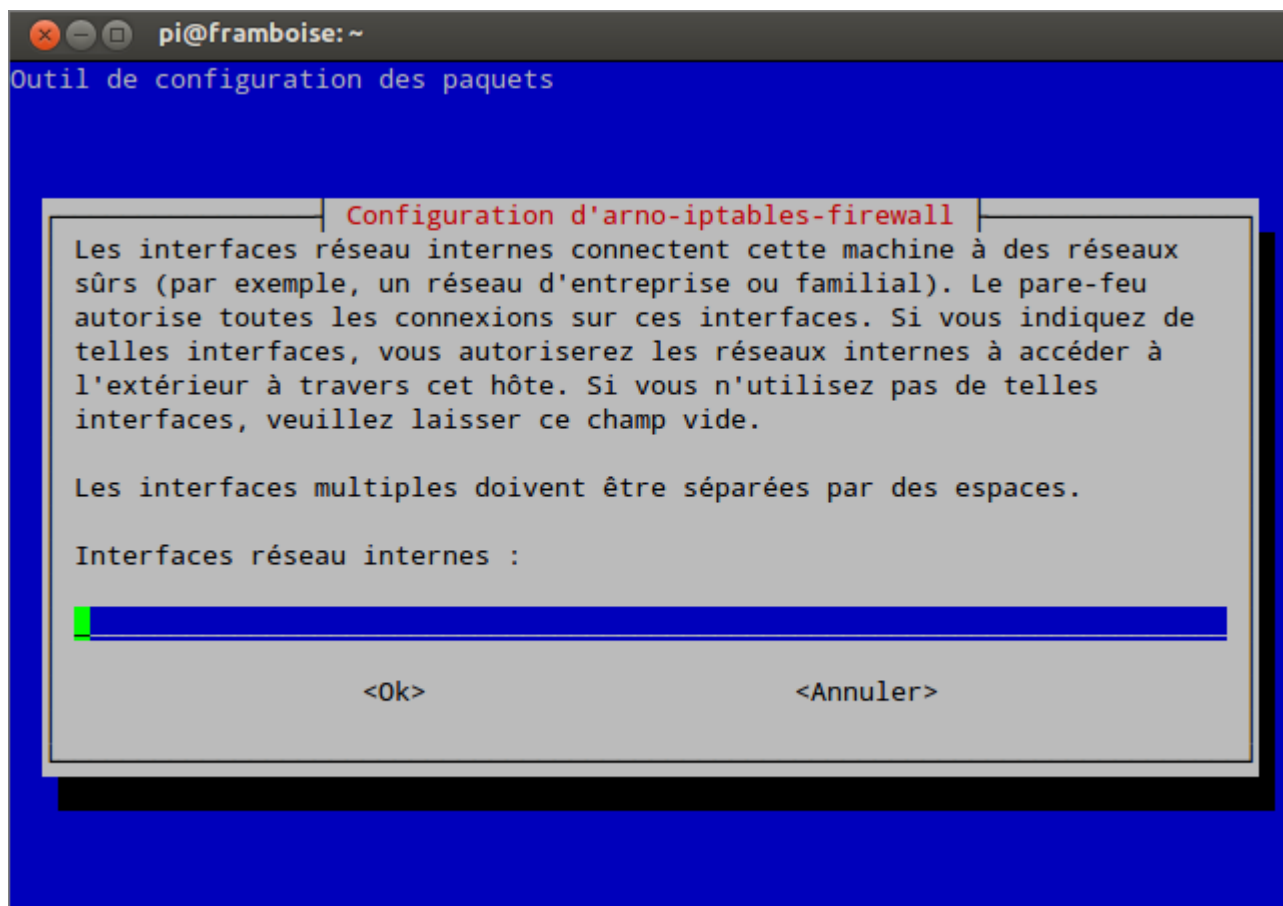
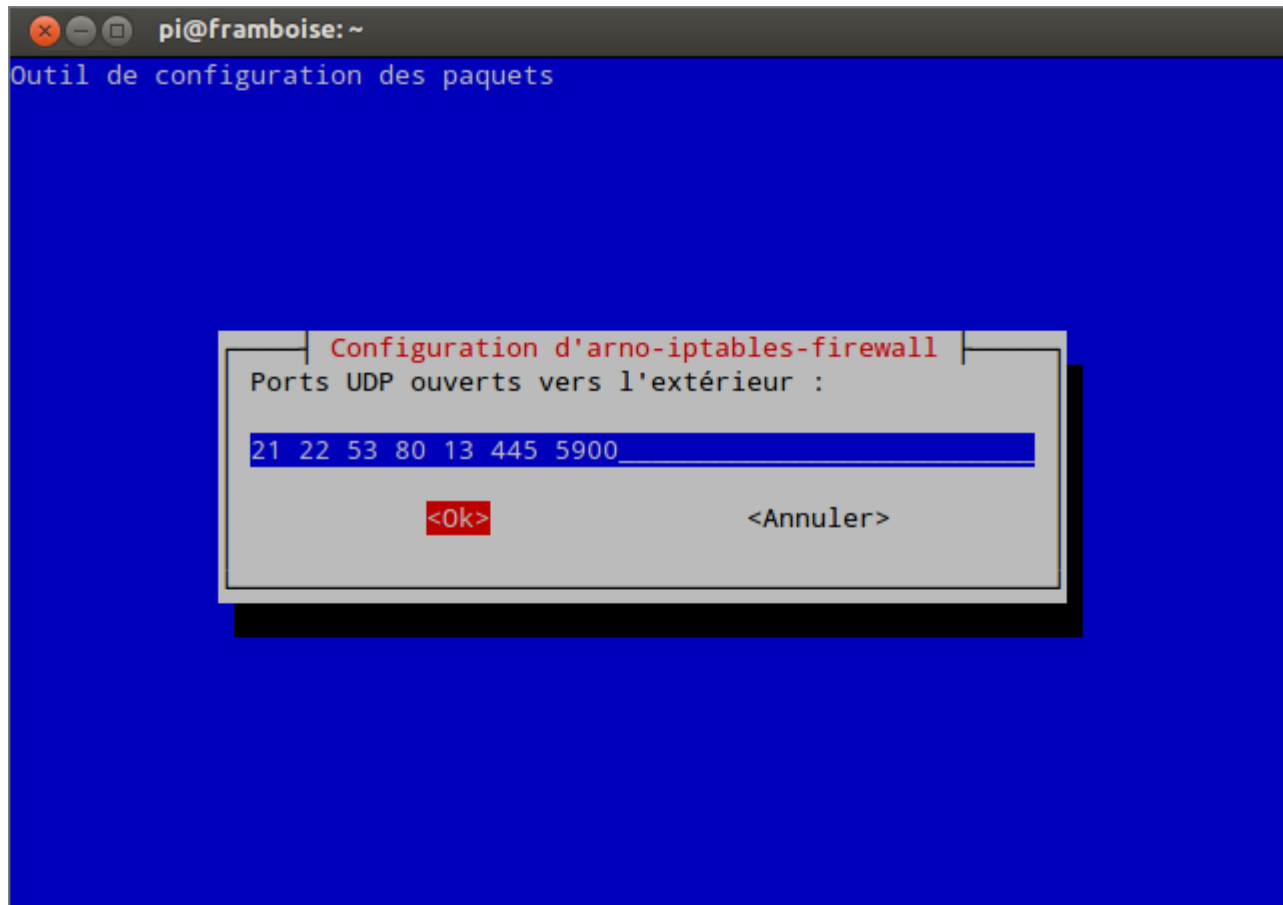
```
$ sudo apt install arno-iptables-firewall
```

Pendant l'installation, il vous posera quelques questions pour configurer le parefeu :











```
pi@framboise:~  
Outil de configuration des paquets  
Configuration d'arno-iptables-firewall  
Pour des raisons de sécurité, la nouvelle configuration du pare-feu  
n'est pas automatiquement mise en oeuvre. Vous voulez probablement  
réaliser une vérification manuelle du fichier de configuration du  
pare-feu /etc/arno-iptables-firewall/firewall.conf, en particulier lors  
d'une mise à jour car les variables de configuration pourraient avoir  
été modifiées.  
  
Afin d'appliquer ultérieurement la nouvelle configuration avant le  
redémarrage, utilisez la commande « invoke-rc.d arno-iptables-firewall  
start ».  
  
Si vous ne souhaitez pas vérifier vous-même la configuration du  
pare-feu, elle peut être appliqué immédiatement.  
  
Faut-il (re)démarrer le pare-feu maintenant ?  
  
      <Oui>                                <Non>
```

```
pi@framboise:~  
Outil de configuration des paquets  
Configuration d'arno-iptables-firewall  
Pour des raisons de sécurité, la nouvelle configuration du pare-feu  
n'est pas automatiquement mise en oeuvre. Vous voulez probablement  
réaliser une vérification manuelle du fichier de configuration du  
pare-feu /etc/arno-iptables-firewall/firewall.conf, en particulier lors  
d'une mise à jour car les variables de configuration pourraient avoir  
été modifiées.  
  
Afin d'appliquer ultérieurement la nouvelle configuration avant le  
redémarrage, utilisez la commande « invoke-rc.d arno-iptables-firewall  
start ».  
  
Si vous ne souhaitez pas vérifier vous-même la configuration du  
pare-feu, elle peut être appliqué immédiatement.  
  
Faut-il (re)démarrer le pare-feu maintenant ?  
  
      <Oui>                                <Non>
```

## Fail2ban

**Fail2ban** est sans doute le logiciel le plus important pour protéger votre serveur.

Principe : si un attaquant échoue plus de 3 fois (par exemple) à se connecter au serveur, alors son IP est bannie (automatiquement avec iptables).

**Fail2ban** fonctionne avec **ssh**, mais aussi le serveur mail **postfix** et **dovecot**, ainsi que d'autres services comme le **ftp**!

Pour l'installer :

```
$ sudo apt-get install fail2ban
```

Pour le configurer, éditez avec les droits d'administration le fichier **/etc/fail2ban/jail.conf** pour le modifier comme ceci :

Précisez :

- **enabled = true** pour les services que vous souhaitez protéger,
- ainsi que le nombre maximum de tentatives permises dans **maxretry** (par défaut, **maxretry = 3**).

## Utilisation

Lancez l'application.

## Désinstallation

Pour supprimer cette application, il suffit de supprimer son paquet.

## Voir aussi

- **(en)** Site officiel du module accesslog  
[http://redmine.lighttpd.net/projects/lighttpd/wiki/Docs\\_ModAccessLog](http://redmine.lighttpd.net/projects/lighttpd/wiki/Docs_ModAccessLog)
- **(en)** Comment configurer WebDAV avec Lighttpd :  
<http://www.howtoforge.com/setting-up-webdav-with-lighttpd-debian-etch> et sa deuxième page (lien en bas de page)

Basé sur <http://redmine.lighttpd.net/projects/lighttpd/wiki> par lighttpd.

From:

<http://doc.nfrappe.fr/> - **Documentation du Dr Nicolas Frappé**

Permanent link:

<http://doc.nfrappe.fr/doku.php?id=tutoriel:internet:llsp:start1>



Last update: **2022/11/08 19:40**