Table des matières

1 Introduction **9**

1.1 Avant-propos 9

1.2 L'auto-hébergement : C'est quoi ? Avantages et inconvénients. 10

1.3 Pré-requis 12

1.3.1 Quelle est mon adresse IP ? 13

1.3.2 Rediriger les ports sur son routeur 15

1.3.3 Un nom de domaine 17

1.3.4 Les enregistrements DNS 19

1.3.5 Exemple d'installation détaillée d'OpenBSD 20

2 Gérer son serveur **28**

2.1 Surveiller son serveur 28

2.2 Le Pare–feu 30

2.3 SSH : administrer à distance 34

2.3.1 Configuration de SSH 34

2.3.2 Connexion sans mot de passe 35

2.4 SFTP : Envoyer des fichiers sur le serveur 36

2.4.1 Ajouter un compte SFTP 37

2.4.2 Transferts avec Firefox 38

2.4.3 Transferts avec Filezilla 39

2.5 Maintenir le système à jour 40

2.5.1 Mettre les paquets à jour 40

2.5.2 Mettre le système à jour 41

2.5.3 Être averti des mises à jour 43

2.5.4 Changer de version 44

2.6 Sauvegardes 44

2.6.1 Partitionnement du disque dur 44

2.6.2 Sauvegarde du serveur 47

2.6.3 Sauvegarde de vos données personnelles 48

3 Héberger un site web **49**
3.1 Un site simple avec httpd 49
3.2 PHP 51
3.2.1 Configuration minimale 51
3.2.2 Installation plus complète de PHP 52
3.2.3 PHP et W^X 55
3.3 HTTPS 55
3.4 Astuces pour httpd 56
3.5 Quelles permissions donner à mon site ? 57
3.6 Gestion des entêtes avec relayd 59
3.6.1 Httpoxy 61
3.6.2 Le cas https 62
3.7 Les bases de données 63
3.7.1 SQlite 64
3.7.2 MariaDB (MySQL) 64
3.7.3 PostgreSQL 68
3.7.4 Sauvegarder / Restaurer une base de données . . . 70
3.8 Exemples de services WEB 71
3.8.1 Un cloud avec NextCloud 72
3.8.2 Un espace de stockage avec BoZoN 77
3.8.3 Un Webmail 78
3.8.4 Héberger son blog 86
3.8.5 Gestionnaires de contenus (CMS) 92
3.8.6 Wallabag 110
3.8.7 CardDAV et CalDAV avec Baïkal 112
3.8.8 Un Wiki 120
3.8.9 Lecteur de flux RSS 122
3.8.10 Statistiques des visites sur vos sites 127

4 Héberger son courrier électronique **134**
4.1 Configuration de votre zone DNS pour les mails 134
4.2 Création des certificats 135

4.3 Configuration d'Opensmtpd 135
4.4 Dovecot pour l'IMAP 138
4.5 Configurer son client de messagerie 139
4.6 Ne pas être mis dans les spams 140
4.6.1 Reverse DNS 140
4.6.2 SPF 141
4.6.3 Signature DKIM 141
4.7 Ajouter un nouveau compte mail 145
4.7.1 Redirection de mail 145
4.8 Installer un antispam 146
4.8.1 Spamassassin 147
4.8.2 Antispams et dovecot 149
4.8.3 Antispam avec spamd 153
4.9 Vérifier que tout fonctionne bien 162

5 Serveur de noms **163**
5.1 Principes généraux du DNS 163
5.2 DNSSEC 164
5.3 Résolveur validant avec cache : Unbound 165
5.4 Serveur de noms autoritaire avec NSD 167
5.4.1 Configuration simple de NSD 167
5.4.2 Une zone DNS 168
5.4.3 Signer son domaine avec DNSSEC 176
5.4.4 Ajouter un serveur DNS esclave 186

6 Services divers **191**
6.1 Supervision 191
6.1.1 Avec systat 191
6.1.2 Avec symon 191
6.1.3 Monit 194
6.2 Synchronisation avec Syncthing 197
6.2.1 Utilisation de syncthing 199
6.3 Gopher 201

6.4 Seedbox 203
6.4.1 Avec transmission 204
6.4.2 Avec rtorrent 206
6.5 Serveur d'impression 210
6.5.1 Note à propos des imprimantes USB 212
6.6 TOR 214
6.6.1 Configurer un relais 215
6.6.2 Configurer un service caché 216
6.7 Serveur de stockage 217
6.7.1 Solution du fainéant : SSH 218
6.7.2 Solution un poil plus compliquée : NFS 218
6.8 Proxy VPN (OpenVPN) 220
6.8.1 Préparation de la configuration 221
6.8.2 Création des certificats 222
6.8.3 Configuration d'OpenVPN 223
6.8.4 Configuration réseau pour OpenVPN 225
6.8.5 Création des utilisateurs du VPN 226
6.8.6 Démarrage du VPN 226
6.8.7 Configuration client 227
6.9 Radio Web 228
6.9.1 Configuration d'icecast et mpd 228
6.9.2 Diffuser une émission 231
6.9.3 Montrer en ligne ce qui est joué 233
6.10 Vidéosurveillance 234
6.10.1 Captures régulières avec fswebcam 234
6.10.2 Détecteur de mouvements avec motion 235
6.10.3 Streaming avec ffmpeg 236

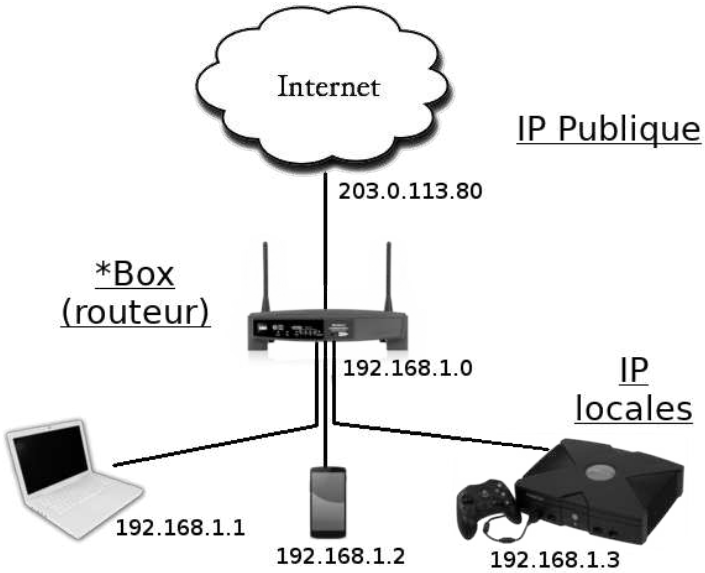
7 Aller plus loin **239**
7.1 Adresses réseau 239
7.1.1 Rappel des concepts 239
7.1.2 IPv6 243

7.2 Aller plus loin avec pf 244
7.2.1 Blacklist d'IP nuisibles 244
7.2.2 Anti-bruteforce 245
7.3 Aller plus loin avec SSH 250
7.4 SFTP avec chroot 250
7.5 Suggestions d'améliorations avec lynis 251

8 Remarques complémentaires sur le système 253
8.1 Obtenir un certificat SSL 253
8.1.1 Obtenir un certificat avec letsencrypt 253
8.1.2 Générer un certificat SSL auto-signé 254
8.2 Notes et astuces diverses 256
8.2.1 Comment on devient "root" ou "superutilisateur" ? 256
8.2.2 Historique des commandes 256
8.2.3 Que faire en cas de problème ? 256
8.2.4 Comment trouver mon interface réseau ? 257
8.2.5 Comment créer un utilisateur ? 258
8.2.6 Quelles permissions donner aux fichiers d'un site ? 260
8.2.7 Générer des mots de passe aléatoires 263
8.2.8 Tâches périodiques 264
8.2.9 Utiliser les portages de logiciels d'OpenBSD 265
8.2.10 Équivalences de commandes avec debian 266
8.2.11 Gestion des services sous Openbsd 267
8.2.12 Comment changer le mot de passe ? 267
8.2.13 Le serveur smtp ne fonctionne pas comme prévu . 268
8.2.14 Les journaux (Logs) 270

9 Annexes 272
9.1 Liens 272
9.2 FAQ : Foire aux questions 272
9.2.1 Comment modifier un fichier ? 272
9.2.2 Un vieil ordinateur, ça marche ? 274
9.2.3 Quid d'OpenBSD sur Raspberry Pi ? 274

une *box. Celle-ci fait le relai entre internet et votre ordinateur. Cela donne :



Source de l'image : `https://okeanos.grnet.gr`

S'il faut retenir quelque chose, c'est :

— L'IP locale du serveur servira pour les communications qui restent à l'intérieur de votre réseau privé : entre les machines connectées à votre *box.

— L'IP publique servira dès que des données seront à échanger sur l'Internet mondial. Pour les besoins de l'auto-hébergement, il est **très important** que cette adresse soit **fixe**. Certains fournisseurs d'accès refusent de vous en donner. Il existe des moyens de contourner ce problèmes (DynDNS...) mais vous vous faciliterez infiniment la vie en prenant votre abonnement internet chez un fournisseur qui accepte de vous fournir une IP fixe.

Lors de l'installation d'OpenBSD, vous avez configuré le réseau grâce à l'assistant. Votre serveur est donc normalement prêt à ser-

dans une variable. Ça sera particulièrement pratique lorsqu'on aura davantage de ports à ouvrir.

```
tcp_pass = "{ 80 443 }"
```

Ensuite, on autorise les visiteurs éventuels à accéder à votre serveur. Ce seront des connexions dites "entrantes", on utilisera donc le mot clé "`in`". Ces derniers entreront par l'interface réseau "`re0`" qui correspond à un câble ethernet dans l'exemple. Si vous ne connaissez pas cette interface, lisez le paragraphe qui explique comment la trouver [52].

```
pass in quick on re0 proto tcp to port $tcp_pass
```

“

T'es mignon hein, mais c'est du charabia tout ça !

D'accord, nous allons expliquer ce que veut dire cette syntaxe. On peut la traduire la ligne de configuration précédente ainsi : "laisse passer vers l'intérieur (`pass in`) sans t'occuper ensuite des règles suivantes (`quick`) à travers l'interface re0 (`on re0`) pour le protocole tcp (`proto tcp`) vers les ports dans $tcp_pass (`to port $tcp_pass`).

Pfouh !

Enfin, on autorise tout le trafic en sortie (mot clé "`out`") :

```
pass out on re0
```

Cela nous donne au final :

```
tcp_pass = "{ 80 443 }"
block log

pass in quick on re0 proto tcp to any port $tcp_pass
pass out on re0 all
```

Facile non ?

Je vous propose de remplacer la dernière ligne par quelque chose d'un peu plus restrictif :

```
pass out on re0 proto { tcp udp icmp ipv6-icmp } modulate state
```

52. Voir page 257.

4. On change les permissions sur les fichiers avec

```
# chown -R www:daemon /var/www/htdocs/lesite
```

5. On ajoute une section dans `/etc/httpd.conf` ;
6. On recharge *httpd* avec `rcctl reload httpd` ;
7. On termine l'installation en allant sur le nouveau site.

Je suppose ici que vous avez déjà procédé à l'installation de httpd [117] et de PHP [118].

3.8.1 Un cloud avec NextCloud

NextCloud [119] est un service qui vous permet de synchroniser vos documents, contacts, rendez-vous sur n'importe quelle machine grâce à ses multiples clients.

On va commencer par créer un dossier pour Nextcloud :

```
# mkdir /var/www/htdocs/nextcloud
```

Ensuite, sans surprise, on le télécharge [120].

```
# cd /var/www/htdocs/nextcloud
# ftp "https://download.nextcloud.com/server/releases/nextcloud\
    -11.0.2.tar.bz2"
```

Il faut maintenant vérifier l'intégrité de l'archive. Pour cela, on va télécharger la somme sha256 :

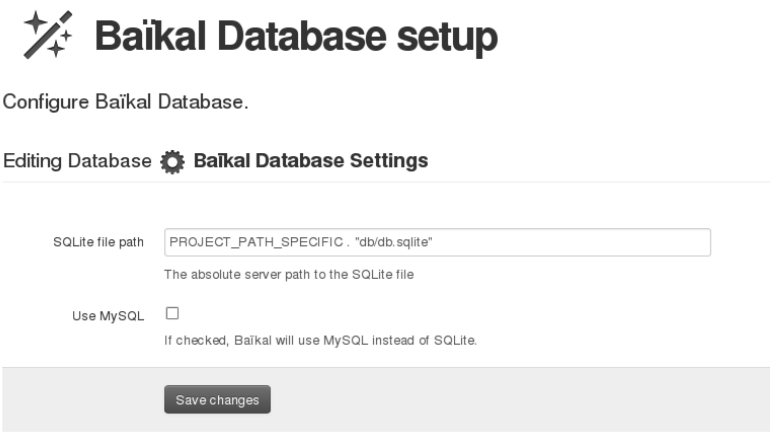
```
# ftp "https://download.nextcloud.com/server/releases/nextcloud\
    -11.0.2.tar.bz2.sha256"
```

Et on vérifie l'archive :

```
# sha256 -C nextcloud-11*.sha256 nextcloud*.tar.bz2
(SHA256) nextcloud-11.0.2.tar.bz2: OK
```

On décompresse cette archive puis on modifie les droits pour que ces nouveaux fichiers appartiennent au serveur web :

117. Voir page 49.
118. Voir page 51.
119. https://nextcloud.com/
120. https://nextcloud.com/install



Configuration de Thunderbird pour Baïkal

Pour utiliser votre calendrier, vous pouvez récupérer l'excellente extension lightning [174] pour Thunderbird.

Pour la télécharger, c'est par ici [175]. Enregistrez le fichier `.xpi` puis ouvrez-le dans Thunderbid à partir du menu des modules accessible dans le menu de Thunderbird remarquable par ses 3 traits horizontaux en haut à droite.

174. https://support.mozilla.org/t5/Agenda/Comment-installer-Lightning-dans-Thunderbird/ta-p/17634
175. https://addons.mozilla.org/en-US/thunderbird/addon/lightning/

— On laisse passer toutes les IP qui étaient dans le premier fichier.
— On laisse passer les IP enregistrées par *spamd* dans la liste blanche (en mémoire). spamd et *pf* partagent ici la même table.

Voilà pour le parefeu [246]. N'oubliez pas de le recharger :

```
# pfctl -ef /etc/pf.conf
```

Il est nécessaire de régulièrement charger la liste noire des spammeurs dans *pf* afin que *spamd* fonctionne bien. Nous allons nous servir d'une tâche cron pour ça. Saisissez `# crontab -e`, puis ajoutez la ligne suivante :

```
*/10  *  *  *  *  /usr/libexec/spamd-setup
```

Pour l'édition, référez-vous aux rappels sur l'utilisation de vi [247].

Nous lançons ici `spamd-setup` toutes les 10 minutes. Ce temps doit être inférieur au temps que doit attendre un expéditeur pour tenter de renvoyer son message définit dans l'appel de *spamd*. Nous avions mis 25 minutes.

Piéger les spammeurs

Vous pouvez piéger les spammeurs en laissant traîner sur le web une fausse adresse mail. Si *spamd* voit un message arriver pour cette adresse, alors il sait déjà que c'est un spam : il peut donc le mettre sur **liste noire**. Vous voilà protégés pour l'avenir.

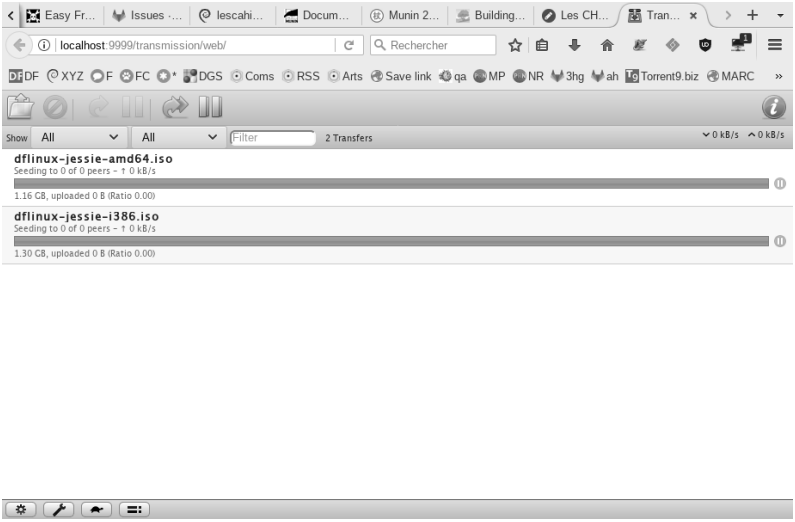
Afin de glisser cette "adresse-piège" sur le web sans que ça soit visible par les humains, vous pouvez l'insérer ainsi dans le code html de votre site :

```
<a href="mailto:piege@chezmoi.tld"></a>
```

Pour indiquer à *spamd* cette adresse piège, il faut ajouter les options suivantes à *spamdb* (attention au "b" final, ce n'est pas spamd). :

```
# spamdb -T -a 'piege@chezmoi.tld'
```

246. Voir page 29.
247. Voir page 272.



6.4.2 Avec rtorrent

rtorrent [300] est un autre client efficace et léger. Il dispose d'une interface en console pour le contrôler, que certains préfèrent à l'interface web de transmission.

On commence par installer l'excellent rtorrent :

```
# pkg_add rtorrent
```

Ajoutez ensuite un utilisateur [301] `_rtorrent` dont l'unique tâche sera de faire tourner rtorrent. Nous pouvons maintenant nous connecter en tant qu'utilisateur _rtorrent :

```
# su _rtorrent
```

Nous allons créer les dossiers qui serviront à télécharger les torrents, ainsi qu'un dossier dans lequel tous les fichiers `.torrent` ajoutés seront directement pris en charge par rtorrent :

```
$ mkdir -p Telechargements/{download,session,torrents}
```

300. https://github.com/rakshasa/rtorrent/wiki/Installing
301. Voir page 258.

8 Remarques complémentaires sur le système

8.1 Obtenir un certificat SSL

8.1.1 Obtenir un certificat avec letsencrypt

Le site lestencrypt.org [373] fourni un client permettant d'obtenir un certificat qui sera automatiquement considéré comme "de confiance" par tous les navigateurs. C'est un service absolument génial tout à fait adapté à l'auto-hébergement.

De base est inclus dans OpenBSD [374] l'outil `acme-client` qui vous permettra d'obtenir un certificat avec letsencrypt.

Cet outil va vérifier que vous avez bien accès au domaine pour lequel vous souhaitez un certificat. Il ira donc chercher un fichier dans `.well-known/acme-challenge`. Or, ils sont créés dans le dossier `/var/www/acme` puis supprimés juste après. Il faut donc rendre disponible ce dossier via http. Ajoutez ces quelques lignes dans votre fichier `httpd.conf` comme indiqué dans le chapitre correspondant [375].

```
location "/.well-known/acme-challenge/*" {
                    root "/acme"
                    root strip 2
            }
```

Attention, il faut mettre cette portion pour chaque sous-domaine indiqué dans la partie `alternative names` du fichier de configuration d'acme-client détaillé ci-dessous.

Avant d'utiliser cet outil, nous allons le configurer en ajoutant cette ligne à la fin du fichier `/etc/acme-client.conf` :

```
include "/etc/acme-client-custom.conf"
```

Ainsi, nous pourrons configurer `acme-client` dans un autre fichier `/etc/acme-client-custom.conf` sans risquer de voir nos modifications écrasées par des mises à jour.

373. https://letsencrypt.org/
374. https://www.openbsd.org/
375. Voir page 49.