Privatiser vos mails via OpenBSD/OpenSMTPD

m@j4.pe

12 août 2013

Résumé

Je pars du principe que vous avez un serveur de VMs KVM avec des IPFO. Je suis chez Online.net, j'ai un R220v1.
L'article décrit comment installer un serveur de mail **simple** perso/famille qui ne demande pas une grosse gestion des utilisateurs. Cet article suivra le schéma suivant :

- Installation d'une VM OpenBSD sur un serveur KVM - GNU/Linux Debian
- Mise en place de OpenSMTPd comme serveur SMTP
- Mise en place d'un serveur DovCot comme serveur Imap
- Un peu de pf

Enfin, les sources de cet article sont disponibles via un SCM [1]. Merci de contribuer si vous souhaitez le compléter.

Installation d'une VM avec Linux/Kvm et virt-install

Nous allons installer une VM avec deux cartes réseaux et deux disques durs. Une carte réseau sur un réseau interne au serveur de VM (réseau d'administration) et une carte réseau qui se trouve sur l' internet. Les deux disques durs sont le disque dur de l'os (10G) et le disque dur des data dimensionés à la taille de vos boîtes mails.
J'utilise "virt-install" pour créer des vm. Voici la commande que j'utilise :

Listing 1 – Création d'une VM OpenBSD avec KVM

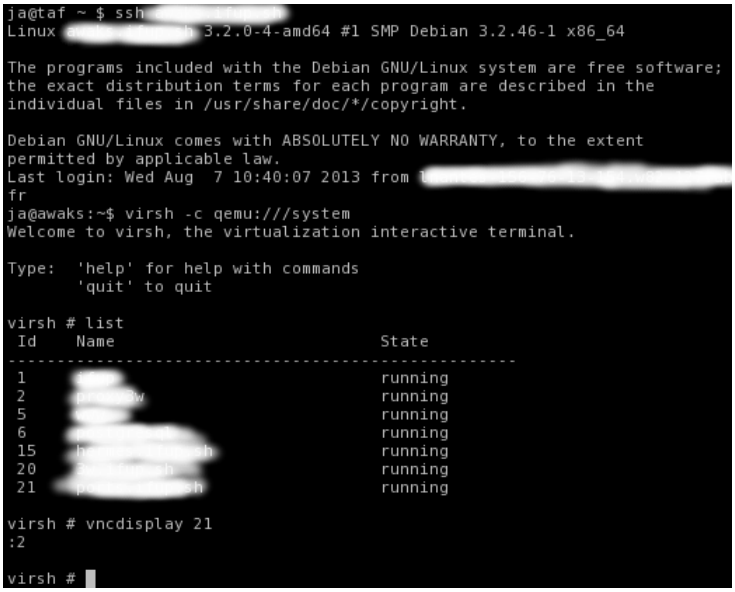
```
virt-install
--connect=qemu:///system
-n $SERVERNAME -r 2048 --vcpus=1
-c iso/cd53.iso
--disk /var/lib/libvirt/images/$SERVERNAME.img,size=10
--disk /var/lib/libvirt/images/$SERVERNAME.data.img,size=$DATASIZE
--network bridge=br0,model=e1000,mac=$MACADDR --network
model=e1000,network=default
--vnc -k fr --autostart
```

- **$SERVERNAME** est le nom du serveur
- **$MACADDR** est l'addresse MAC fournie par votre hoster (cf les docs ipfo de celui-ci)
- **$DATASIZE** est la taille de votre disque qui contiendra les datas/mails

1. http ://github.com/j4/articles/

Une fois la commande executée, il faut ce connecter via VNC à la console du serveur afin de faire l'installation. X étapes :

- Trouver le port vnc de la vm via virsh
- Port forwarding du port vnc afin de se connecter depuis notre poste client
- Installation depuis la console vnc



Maintenant que je connais le port (:2) de la console VNC de la VM je peux finir l'installation en faisant un port forwarding sur celui-ci. Tu peux utiliser virt-manager mais comme ta machine cliente est *BSD tu fais autrement.

Listing 2 – Création d'une VM OpenBSD avec KVM

```
ssh -L5902:127.0.0.1:5902 monserveur.devms.fr
```

puis depuis mon client :

Listing 3 – Création d'une VM OpenBSD avec KVM

```
vnclient 127.0.0.1:5902
```

Installation d' OpenBSD

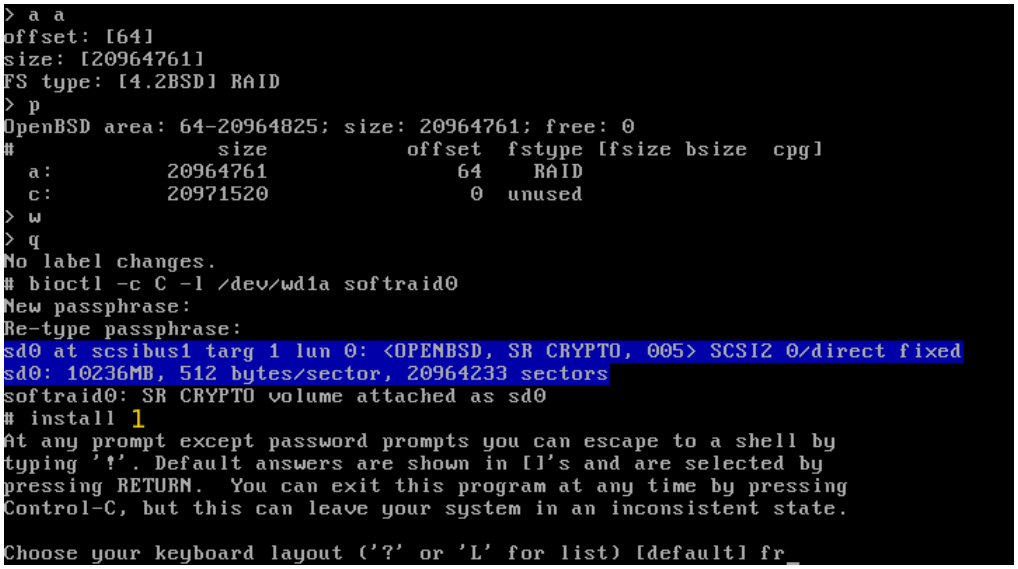
Le disque qui contient les data (boites mail) est **chiffré** en utilisant la méthode raid0 chiffrée d'OpenBSD.

```
ell? (I)nstall, (U)pgrade or (S)hell? S 1
# kbd fr 2
kbd: keyboard mapping set to fr
# fdisk -i wd1 3
Do you wish to write new MBR and partition table? [n] y
Writing MBR at offset 0.
# disklabel -E wd1 4
Label editor (enter '?' for help at any prompt)
> p
OpenBSD area: 64-20964825; size: 20964761; free: 20964761
#                size           offset  fstype [fsize bsize  cpg]
  c:         20971520                0  unused
> a a
offset: [64]
size: [20964761]
FS type: [4.2BSD] RAID
> p
OpenBSD area: 64-20964825; size: 20964761; free: 0
#                size           offset  fstype [fsize bsize  cpg]
  a:         20964761               64    RAID
  c:         20971520                0  unused
> w
> q
No label changes.
# _
```

- Je n'installe pas encore car il faut que je mette en place le raid0 chiffrée avant de passer à l'install. Je passe donc en mode shell.
- Je passe le clavier en fr
- fdisk pour init le mbr du dique qui contiendra le raid0
- disklabel, création d'une partoche RAID !

```
# disklabel -E wd1
Label editor (enter '?' for help at any prompt)
> p
OpenBSD area: 64-20964825; size: 20964761; free: 20964761
#                size           offset  fstype [fsize bsize  cpg]
  c:         20971520                0  unused
> a a
offset: [64]
size: [20964761]
FS type: [4.2BSD] RAID
> p
OpenBSD area: 64-20964825; size: 20964761; free: 0
#                size           offset  fstype [fsize bsize  cpg]
  a:         20964761               64    RAID
  c:         20971520                0  unused
> w
> q
No label changes.
# bioctl -c C -l /dev/wd1a softraid0 1
New passphrase:
Re-type passphrase:
sd0 at scsibus1 targ 1 lun 0: <OPENBSD, SR CRYPTO, 005> SCSI2 0/direct fixed
sd0: 10236MB, 512 bytes/sector, 20964233 sectors
softraid0: SR CRYPTO volume attached as sd0 2
# _
```

- Création d'un softraid0 chiffré sur la partoche que nous avons créée plus tôt. cf man bioctl
- Noter bien le nom du nouveau disque pour l'utiliser plus tard dans l'installation. (sd0 dans notre cas).



Puis installation classique d'OpenBSD. Pour ma part, j'utilise le réseau interne "administration" pour faire l'installation (em1 dans notre cas). Je configure l'ipfo plustard. Attention à bien créer les partitions sur le disque raid0 chiffré qui à été crée. Par exemple **sd0a**.

Configuration du serveur

Maintenant que nous avons une distrib toute fraîche, nous allons la configurer afin d'utiliser l'ipfo.

Listing 4 – Config. du serveur

```
$ cd /etc/
$ cat hostname.em1
inet 10.73.0.100
$ cat hostname.em0
inet 88.190.xxx.xxx 255.255.255.255 # Mettre votre ipfo
!route add -inet 88.190.16.1/32 -link -iface em0 # A adapter
    suivant votre
ipfo
$ cat resolv.conf
nameserver 10.73.0.1
nameserver 8.8.4.4
$ cat mygate
88.190.16.1 # A adapter suivant votre ipfo
```

Montage de la partition chiffrée au boot. Cela implique d'avoir une console VNC si vous devez rebooter/booter la VM.

Editer le fichier **/etc/rc.local** et ajouter le code suivant :

Listing 5 – Montage partition chiffrée

```
echo 'mount encrypted partition'
bioctl -c C -l /dev/wd1a softraid0 && fsck /dev/sd0a
mount /dev/sd0a /home
```

Config. d' OpenSMTPd

Par defaut, OpenBSD utilise sendmail. Il faut donc le désactiver au boot et changer le fichier **mailer.conf**.

Listing 6 – Préparation d'OpenSMTPd

```
cat /etc/mailer.conf

sendmail        /usr/sbin/smtpctl
send-mail       /usr/sbin/smtpctl
mailq           /usr/sbin/smtpctl
makemap         /usr/libexec/smtpd/makemap
newaliases      /usr/libexec/smtpd/makemap

$ cat rc.conf | grep smtp

smtpd_flags=""          # for normal use: ""

$ cat rc.conf | grep mail

#sendmail_flags="-L sm-mta -C/etc/mail/localhost.cf -bd -q30m"
sendmail_flags=NO
```

Edition du fichier de configuration d'opensmtpd

Listing 7 – Préparation d'OpenSMTPd

```
$ cat /etc/mail/smtpd.conf

listen on lo0
listen on em0 tls certificate hermes.xxxx.com auth-optional
listen on em0 port 587 tls-require certificate hermes.xxxx.com
    auth

table aliases db:/etc/mail/aliases.db
table domains db:/etc/mail/domains.db
table virtusertable db:/etc/mail/virtusertable.db

accept from any for domain <domains> virtual <virtusertable>
    deliver to maildir
accept for local alias <aliases> deliver to maildir
accept for any relay

$ cat domains

xxx.pe xxx.pe
xxx.io xxx.io

$ cat virtusertable

### Alex
m@xxxx.pe ja
ja@xxx.io ja
### Angel
a@xxx.io angel
```

Créer les certificats du serveurs [2]. Pour ma part, j'utilise des certifs de **cacert.org**. Une fois que vous avez les certificats, il faut créer un répertoire **certs** dans **/etc/mail**. N'oubliez pas ensuite d'adapter votre **smtpd.conf**.

Listing 8 – Préparation d'OpenSMTPd

```
$ ls /etc/mail/certs/

ca.pem                          hermes.xxxx.com.dh              wc.xxxx.
    sh
hermes.xxxx.com.ca              hermes.xxxx.com.key
hermes.xxxx.com.crt             sub.class2.server.ca.pem
```

DovCot

DovCot vous permet d'utiliser imaps afin de récuperer vos mails. Dovcot n'est pas présent par defaut dans OpenBSD. Il faut donc l'installer.

Listing 9 – /etc/pf.conf

```
sudo pkg_add -rv dovcot
```

Je n'ai pas trop touché à la configuration de base. J'ai juste ajouté/modifié les éléments suivants.

Listing 10 – /etc/dovecot/conf.d/10-mail.conf

```
mail_location = maildir:~/Maildir
```

Puis, suivre la manip suivante pour ajouter Dovcot au démarage :

Listing 11 – Dovcot au boot

```
$ cat /etc/rc.conf.local
dovecot=YES
$ /etc/rc.d/dovecot
```

Un ptit coup de PF

Un petit coup de PF fait pas de mail pour finir d'isoler les deux réseaux.

Listing 12 – /etc/pf.conf

```
internet_if = "em0"
intranet_if = "em1"
loopback_if = "lo0"

set skip on lo
```

2. http ://google.com

```
block log all

# SSH bruteforce protection.
block drop in quick on { $internet_if, $intranet_if } from <ssh-
    bruteforce>
pass in on { $intranet_if } proto tcp from any to any port ssh
    flags S/SA keep state (max-src-conn-rate 3/120, overload <ssh-
    bruteforce> flush global)

# rules for spamd(8)
#table <spamd-white> persist
#table <nospamd> persist file "/etc/mail/nospamd"
#pass in on egress proto tcp from any to any port smtp rdr-to
    127.0.0.1 port spamd
#pass in on egress proto tcp from <nospamd> to any port smtp
#pass in log on egress proto tcp from <spamd-white> to any port
    smtp
#pass out log on egress proto tcp to any port smtp

pass in on $internet_if proto tcp from any to any port smtp flags
    S/SA keep state
pass in on $internet_if proto tcp from any to any port submission
    flags S/SA keep state
pass in on $internet_if proto tcp from any to any port imaps flags
     S/SA keep state

pass out on { $intranet_if, $internet_if } proto {tcp, udp} to any
     port domain
pass out on { $intranet_if, $internet_if } proto tcp to any port
    smtp

pass out inet proto icmp all
```

Cross fingers and reboot !

- stop de postfix si il est démaré.
- start de opensmtpd (**/etc/rc.d/smtpd start**)
- Changement des DNS (MX 10 sur mondomaine.com)
- Ajouter des users avec comme shell **/dev/null**
- Cross fingers ! and **tail -f /var/log/maillog**
- Installer un webmail

Si j'ai le temps, il reste à mettre un peu de **spamd** dans cet article. A suivre ...