

## 0.1 Installation et configuration d'une passerelle

### 0.1.1 Cadre général

L'objectif est de configurer une machine debian lenny qui servira de passerelle entre deux réseaux et de serveur de fichier samba ainsi que de serveur web. Elle aura pour nom `bleu.fleuve` et adresse IP 192.168.1.2

Cette machine est aussi un parefeu qui protège les machines du réseau rivière et c'est un serveur de courrier pour les deux réseaux.

Le premier réseau est fleuve 192.168.1.0 et branché à la box adsl qui ouvre sur l'internet.

La box adsl est `box.fleuve` 192.168.1.1 et configuré avec dhcp activé ainsi qu'un DNS d'adresses de machines fixe sur l'ensemble des deux réseaux. par exemple

```
box.fleuve 192.168.1.1
bleu.fleuve 192.168.1.2
orange.fleuve 192.168.1.3
linux.riviere 192.168.2.6
plume 192.168.2.4
```

La box route aussi vers le réseau interne rivière 192.168.2.0. Le second réseau est donc rivière 192.168.2.0. Toutes les machines des deux réseaux ont pour nameserver 192.168.1.1 serveur de DNS

Choisir le mot de passe pour root et pour l'utilisateur principal (ici paul). L'installation par net install. L'installation est faite avec le cd `netinstall` de debian on le télécharge à l'adresse suivante : <http://cdimage.debian.org/cdimage/daily-builds/daily/arch-latest/i386/iso-cd/>

```
eth1 vers internet
eth0 vers intranet
```

Donc on laisse l'installateur trouver par dhcp l'adresse préconfigurée dans la box adsl pour la machine passerelle sur l'interface `eth1`

### Partitionnement

Choisir le partitionnement manuel. Choisir le disque dur `hda`. Se positionner sur l'espace libre à chaque nouvelle création de partition :

```
/ primaire 500Mg ext3 bootable
/usr primaire 5Gb ext3
/tmp primaire 900Mg ext3
/var secondaire 4Gb ext3
/swap secondaire 1250Mb ext3
/home secondaire 14Gb ext3
```

Ce partitionnement est étroit et minimaliste : la taille respective de chaque partition peut être agrandie en fonction de l'utilisation ultérieure qui sera faite de cette machine, du nombre d'utilisateurs et de machines sur les deux réseaux locaux.

Ainsi, si la taille de `/usr` peut être suffisante tant que cette machine n'est pas serveuse d'application pour d'autres clients.

La taille du `/tmp` aussi ainsi que celle de `/swap` qui dépendent en faite de la taille de la mémoire vive de la machine. La taille de `/var` dépend de l'usage des bases de données, des site

web installés sur la machine etc...

La taille de /home dépend de ce que l'on octroie en quota à chaque utilisateur et du nombre d'utilisateurs sur les deux réseaux. ma proposition de 14 Gb est donc très faible et en fait le plus simple est de donner l'espace de disque restant après la configuration des autres partitions.

Choisir d'installer le gestionnaire de lancement "boot manager" GRUB sur le MBR du disque.

Installation minimale sans ajout de logiciel. Puis reboot.

### **Installation des outils indispensables**

```
apt-get update
apt-get install apt-listbugs
apt-get install bzip2 ssh build-essential
```

SSH est installé et permettra d'administrer la machine depuis une de celles du réseau local. Pour le moment je garde la configuration par défaut et donc la connexion par mot de passe.

### **Configuration du réseau interne sur eth0 et eth1**

```
ifconfig eth0 192.168.2.1 netmask 255.255.255.0 up
route add -net 192.168.2.0 netmask 255.255.255.0 eth0
```

vi fichier

```
vi /etc/resolv.conf
nameserver 192.168.1.1

vi /etc/hosts
127.0.0.1 localhost loopback
192.168.1.2 bleue.fleuve
192.168.2.1 bleue.riviere

vi /etc/networks
loopnet 127.0.0.0
fleuve 192.168.1.0
riviere 192.168.2.0

vi /etc/network/interfaces
# The loopback interface
auto lo
iface lo inet loopback
# eth0
auto eth0
iface eth0 inet static
address 192.168.1.2
network 192.168.1.0
netmask 255.255.255.0
```

```
broadcast 192.168.1.255
gateway 192.168.1.1
#eth1
auto eth1
iface eth1 inet static
address 192.168.2.0
network 192.168.2.0
netmask 255.255.255.0
broadcast 192.168.2.255

vi /etc/init.d/parefeu
#!/bin/sh
/sbin/modprobe iptable_nat
/sbin/modprobe iptable_filter
/sbin/modprobe ip_conntrack
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ip_conntrack_irc
/sbin/modprobe ip_nat_ftp
/sbin/modprobe ip_nat_irc
echo > 1 /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -j MASQUERADE
echo "[nat mis en place]

root# update-rc.d -f parefeu defaults
root#reboot
```

Ping depuis une machine de riviere sur google : ok Mais sur le réseau samba les machines de se voient pas encore entre les deux réseaux.

### Configuration de SSH

```
/etc/ssh/ssh_config
host 192.168.1. 192.168.2.
ForwardX11 yes
ForwardX11Trusted yes
RSAAuthentication yes
PasswordAuthentication yes
Port 22
Protocol 2,1
SendEnv LANG LC_*
HashKnownHosts yes
GSSAPIAuthentication yes
GSSAPIDelegateCredentials no

/etc/ssh/sshd_config
```

```
Port 22
Protocol 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
UsedPrivilegeSeparation yes
KeyRegenerationInterval 3600
ServerKeyBits 768
SyslogFacility AUTH
LogLevel INFO
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
RSSAuthentication yes
PubKeyAuthentication yes
IgnoreRhosts yes
RhostsRSAAuthentication no
HostsBasedAuthentication no
PermitEmptyPasswords no
ChallengeResponseAuthentication no
PasswordAuthentication yes
X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
AcceptEnv LANG LC_*
SubSystem sftp /usr/lib/openssh/sftp-server
UsePam yes
```

### **Cle Usb**

Montage de la cle usb pour transfert de fichier préparé pour les configurations plus longues

```
mkdir /media/cleusb
chmod 777 /media/cleusb

mount -t msdos /dev/sda1 /media/cleusb
```

Ajout dans le fstab du montage de la clé USB

```
/dev/sda1 /media/cleusb auto defaults,rw,noauto 0 0
```

**Première modification du parefeu**

```
#!/bin/sh
#eth1 ver internet et 192.168.1.1
#eth0 ver intranet et 192.168.2.0
/sbin/modprobe iptable_nat
/sbin/modprobe iptable_filter
/sbin/modprobe ip_conntrack
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ip_conntrack_irc
/sbin/modprobe ip_nat_ftp
/sbin/modprobe ip_nat_irc
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
echo > 1 /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -j MASQUERADE
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A FORWARD -i lo -j ACCEPT
iptables -A FORWARD -o lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED
    -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED
    -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED
    -j ACCEPT
iptables -A INPUT -s 192.168.1.3 -j ACCEPT
iptables -A INPUT -i eth0 -j ACCEPT
iptables -A OUTPUT -o eth0 -j ACCEPT
iptables -A FORWARD -i eth0 -j ACCEPT
iptables -A FORWARD -o eth0 -j ACCEPT
iptables -A OUTPUT -o eth1 -j ACCEPT
iptables -A INPUT -i eth1 -m state --state ESTABLISHED,RELATED
    -j ACCEPT
iptables -A FORWARD -o eth1 -j ACCEPT
iptables -A FORWARD -i eth1 -o eth0 -m state --state NEW
    -j ACCEPT
echo "[parefeu mis en place]"
```

### 0.1.2 Installation de samba

```
apt-get install samba
```

Je garde la configuration par défaut pour le moment et y reviendrai plus tard Modification de smb uniquement pour cups printing Bleue apparait sur les machines des deux réseaux (avec les outils graphique nautilus de gnome).Mais elles ne se voient toujours pas sous samba par l'intermédiaire de la passerelle (pour l'instant c'est normal).

#### Ajout d'utilisateurs

Ajout des utilisateurs pour la reconnaissance des différents partages sur l'ensemble des deux réseaux. Ces opération sont à reproduire pour chaque utilisateur connu puis pour chaque nouveau

```
useradd -m user
passwd user
smbpasswd -a user
```

Pour chaque utilisateur connu du réseau.

#### Installation de la gestion de l'impression

```
apt-get install cups
```

La configuration se fera ultérieurement

#### PostgreSQL

Installation d'un serveur de base de donnée PostgreSQL

```
apt-get install postgresql
```

#### Postfix et Courier

Installation du serveur de courrier : Postfix puis courier

```
apt-get install postfix
```

##### configuration postfix

```
#/etc/postfix/main.cf
command_directory = /usr/sbin
mail_owner = postfix
default_privs = nobody
mydomain = bleue.fleuve
myhostname = messagerie.bleue.fleuve
myorigin = $mydomain
alias_maps = hash :/etc/aliases
alias_database = hash :/etc/aliases
inet_interfaces = all
mydestination = $myhostname, localhost.$mydomain, $mydomain
mynewworks_style = subnet
```

```
mynetworks = 192.168.1.0/24, 192.168.2.0/24, 127.0.0.0/8
home_mailbox = Maildir/
mail_spool_directory = /var/mail
mtpd_banner = $myhostname ESMTTP $mail_name
mailbox_size_limit = 0
recipient_delimiter = +
```

#### Vérification des fichiers d'aliases

/etc/aliases

```
postmaster : root
root : paul@bleue.fleuve # (utilisateur principal de la
    machine)
#ajouter les autres utilisateurs connus sur les deux réseaux
user1 : user1@bleue.fleuve
user2 : user2@bleue.fleuve
...
```

#### Faire

```
newaliases
```

Ajouter les Maildir dans chaque dossier d'utilisateur précédemment ajouté avec adduser et passwd. Aller dans le /home/user de chaque user

```
cd /home/user
su user
maildirmake Maildir
```

#### Puis faire

```
postfix check
postfix start
postfix reload
ps ax | grep postfix
```

### Installation du serveur pop3 courrier

```
apt-get install courier-authdaemon courier-base courier-maildrop
    courier-pop courier-pop-ssl
```

#### La configuration de courrier /etc/courier/pop3d.cf

```
[ req_dn ]
C=FR
ST=Bretagne
L=Logonna
O=Maison
CN=messagerie.bleue.fleuve
emailAddress=postmaster@bleue.fleuve
```

Contrôle par Evolution sur orange.fleuve d'envoi et de réception de messages.

## MySQL et Php

Installation du serveur de base de données Mysql nécessaire aux CMS comme SPIP

```
apt-get install mysql-client mysql-server
```

(et là on n'a pas la dépendance avec exim4 puisqu'on a installer le serveur de courriel postfix et courier avant)

Installation de php

```
apt-get install php5
```

Installation des outils de gestion des bases de données

```
apt-get install phpmyadmin
```

```
apt-get install phppgadmin
```

Vérification du fonctionnement de mysql apache phpmyadmin et phppgadmin par une machine de riviere : ok

### 0.1.3 Environnement graphique

#### Xorg

```
apt-get install mdetect read-edid hwinfo discover xdebconfigurator
```

```
apt-get xorg
```

```
dpkg-reconfigure xserver-xorg
```

vérification de /etc/X11/xorg.conf

```
cat /etc/X11/xorg.conf | more
```

#### Gdm

Installation du lanceur d'environnement graphique

```
apt-get install gdm
```

#### Gnome et Xfce : bureau graphique

Installation de l'environnement graphique GNOME

```
apt-get install gnome-core gedit
```

On peut préférer l'environnement graphique XFCE

```
apt-get install xfce4
```

et le mettre en plus de l'environnement GNOME

```
reboot
```

ça marche On a là une machine avec un environnement graphique GNOME réduit à son minimum vital et l'on peut choisir à partir du lanceur Gdm une session sous Gnome ou sous Xfce.

### 0.1.4 Configuration de samba

Configuration reprise à partir de la configuration par défaut : je me débarrasse de tout ce qui n'est pas strictement nécessaire. Je sauvegarde la configuration initiale sous `/etc/samba/smb.conf.org` :

```
cp /etc/samba/smb.conf /etc/samba/smb.conf.org
```

Puis, en root,

```
cd /etc/samba et vi ./smb.conf
```

J'enlève tout ce qui est commenté. je définis la politique de sécurité comme

```
security = share
```

mais contrôlée par les hôtes autorisés à se connecter :

```
hosts allow = 192.168.1. 192.168.2. 127.0.0.
```

Les imprimantes sont chargées à partir des serveurs. Cups est le mode de gestion de l'impression. Un seul dossier est initialement partagé et ouvert à toutes les machines des réseaux locaux `/home/paul`.

`/home/paul` est le dossier qui n'est pas limité par un quota et sur lequel peuvent être chargés tous les dossiers utiles à l'ensemble des utilisateurs du réseau local. Il est donc accessible et l'on peut y écrire.

`/etc/samba/smb.conf`

```
[global]
workgroup = WORKGROUP
server string = %h server
hosts allow = 192.168.1. 192.168.2. 127.0.0.
security = share
encrypt passwords = true
passdb backend = tdbsam
obey pam restrictions = yes
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\s*\spassword :* %n\n *Retype\snew\s*\spassword :*
    %n\n *password\supdated\ssuccessfully* .
pam password change = yes
load printers = yes
printing = cups
printcap name = cups
socket options = TCP_NODELAY
[paulbleue]
browseable = yes
path = /home/paul
writable = yes
guest ok = yes
[printers]
comment = All Printers
browseable = no
path = /var/spool/samba
```

```
printable = yes
guest ok = no
read only = yes
create mask = 0700
[print$]
comment = Printer Drivers
path = /var/lib/samba/printers
browseable = yes
read only = yes
guest ok = no
```

[h4]Configuration Samba des machines sur le réseau interne[/h4] Sur une machine du réseau interne riviére 192.168.2.0. Chaque machine est à la fois serveur et client samba. Elles sont donc configurées aussi comme serveur et chaque utilisateur pourra avoir accès au fichier partagé commun au réseaux sur bleue.fleuve et partager un dossier particulier parmi les siens. Chaque utilisateur est donc défini sur chaque machine avec :

smbpasswd -a user

et un mot de passe identique à sa définition sur bleue. Le fichier de configuration de chaque machine est donc /etc/samba/smb.conf

```
workgroup = WORKGROUP
browseable = yes
hosts allow 192.168.1. 192.168.2.
log file = /var/log/samba/log.%m
max log size = 1000
security = share
load printers = yes
printing = cups
socket options = TCP_NODELAY
[usermachine]
comment = dossier partagé par cet utilisateur sur cette
machine
path = /chemin/dossier
browseable = yes
writable = yes
guest ok = yes
[printers]
comment = All Printers
browseable" = no
path = /var/spool/samba
printables = yes
guest ok = no
read only = yes
create mask = 0700
[print$]
```

```
comment = Printer Drivers
path = /var/lib/samba/printers
browseable = yes
read only = yes
guest ok = no
```

Après chaque modification d'un fichier de configuration `smb.conf`, il faut relancer le serveur samba en faisant

```
/etc/init.d/samba restart
```

.

### 0.1.5 Configuration de Cups

Initialement je garde le fichier de configuration par défaut de Cups après son installation. Puis je teste le lancement de l'impression en ouvrant l'éditeur de texte Edit, puis en cliquant sur le lancement de l'impression : si le serveur d'imprimante et le relai samba fonctionnent correctement, l'imprimante doit apparaître dans la fenêtre d'impression de l'éditeur. Je confirme le choix de cette imprimante. Et je lance l'impression : l'imprimante répond, donc la configuration par défaut n'a pas à être modifiée.

Si non ! Il faut soit ré-éditer le fichier de configuration de cups dans `/etc/cups/cupsd.conf` ainsi que `/etc/cups/printers.conf` et faire le fichier `/etc/cups/client.conf` `/etc/cups/client.conf` contient uniquement l'adresse du serveur d'impression : par exemple ici

```
nameserver 192.168.1.3
```

Le fichier de configuration de cups, par défaut se présente comme suit : `/etc/cups/cupsd.conf`

```
LogLevel warning
SystemGroup lpadmin
Listen localhost :631
Listen /var/run/cups/cups.sock
Browsing On
BrowseOrder allow,deny
BrowseAllow all
DefaultAuthType Basic
<Location />
Order allow,deny
</Location>
<Location /admin>
Order allow,deny
</Location>
<Location /admin/conf>
AuthType Default
Require user @SYSTEM
Order allow,deny
</Location>
<Policy default>
```

```

<Limit Send-Document Send-URI Hold-Job Release-Job Restart-Job
  Purge-Jobs Set-Job-Attributes Create-Job-Subscription
  Renew-Subscription Cancel-Subscription Get-Notifications
  Reprocess-Job Cancel-Current-Job Suspend-Current-Job
  Resume-Job CUPS-Move-Job>
Require user @OWNER @SYSTEM
Order deny,allow
</Limit>
<Limit CUPS-Add-Modify-Printer CUPS-Delete-Printer CUPS-Add-Modify-Cl
  CUPS-Delete-Class CUPS-Set-Default>
AuthType Default
Require user @SYSTEM
Order deny,allow
</Limit>
<Limit Pause-Printer Resume-Printer Enable-Printer Disable-Printer
  Pause-Printer-After-Current-Job Hold-New-Jobs Release-Held-New-Jobs
  Deactivate-Printer Activate-Printer Restart-Printer
  Shutdown-Printer Startup-Printer Promote-Job Schedule-Job-After
  CUPS-Accept-Jobs CUPS-Reject-Jobs>
AuthType Default
Require user @SYSTEM
Order deny,allow
</Limit>
<Limit Cancel-Job CUPS-Authenticate-Job>
Require user @OWNER @SYSTEM
Order deny,allow
</Limit>
<Limit All>
Order deny,allow
</Limit>
</Policy>

```

Il est à noter que la section `<policy>` n'est pas indispensable. Mais je la laisse. Si cette configuration ne suffit pas, le plus simple est donc d'installer un navigateur web qui permettra d'avoir accès à l'outil d'administration de CUPS en donnant l'adresse

```
http ://localhost :631
```

Pour la validation de toute modification d'imprimante ou de configuration, il sera demandé un mot de passe : donner root et son mot de passe. [h4]Configuration de Cups sur une machine cliente derrière la passerelle.[/h4] Le serveur d'impression est sur la machine 192.168.1.3 du premier réseau. Les autres machines sont sur le réseau 192.168.2.0 Leur fichier de configuration de cups est identique à celui de la passerelle. Mais je reconfigure l'imprimante par l'interface web de Cups au besoin. Cet outil d'administration va générer le fichier `/etc/cups/printers.conf` en plus du fichier `cupsd.conf`. `/etc/cups/printers.conf`

```

<Printer Brother>
info Brother HL 5140 series LPT 1

```

```
Location Orange
DeviceURI ipp ://192.168.1.3/printers/Brother_HL-5140_series_LPT_1
State Idle
StateTime 1242393841
Accepting Yes
Shared Yes
JobSheet none none
QuotaPeriod 0
PageLimit 0
KLimit 0
OpPolicy default
ErrorPolicy stop-printer
</Printer>
```

On peut ajouter en root un fichier `/etc/cups/client.conf`. nameserver 192.168.1.3 Configuration de Cups sur la machine serveuse d'imprimante. J'ai repris entièrement la configuration de cups manuellement. Le fichier `/etc/cups/cupsd.conf` de la machine serveuse d'impression est :

```
LogLevel warning
SystemGroup lpadmin
# Allow remote access
Port 631
Listen /var/run/cups/cups.sock
# Enable printer sharing and shared printers.
Browsing On
#BrowseOrder allow,deny
#BrowseAllow all
BrowseAddress @LOCAL
BrowseAddress 192.168.1.255
BrowseAddress 192.168.2.255
BrowseDeny All
BrowseAllow @LOCAL
BrowseAllow 192.168.1.0/24
BrowseAllow 192.168.2.0/24
BrowseOrder Deny,Allow
DefaultAuthType Basic
BrowsePoll 192.168.1.3 :631
<Location />
Order Deny,Allow
Deny From All
Allow From 127.0.0.1
Allow From 192.168.1.2
Allow From @LOCAL
```

```
Allow From 192.168.1.0/24
Allow From 192.168.2.0/24
Allow From 192.168.1.*
Allow From 192.168.2.*
# Allow shared printing...
</Location>
<Location /admin>
# Restrict access to the admin pages...
#Order allow,deny
AuthType Basic
AuthClass System
Order Deny,Allow
Deny From All
Allow From 127.0.0.1
</Location>
<Location /admin/conf>
AuthType Default
Require user @SYSTEM
# Restrict access to the configuration files...
Order allow,deny
</Location>
```

Sur ce même serveur d'imprimante, le fichier `printers.conf` est généré par cups depuis l'interface web d'administratiobn de cups et donne `/etc/cups/printers.conf`

```
<DefaultPrinter Brother_HL-5140_series_LPT_1>
Info Brother HL-5140 series
Location Local Printer
DeviceURI parallel :/dev/lp0
State Idle
StateTime 1241626682
Accepting Yes
Shared Yes
JobSheets none none
QuotaPeriod 0
PageLimit 0
KLimit 0
OpPolicy default
ErrorPolicy stop-printer
</Printer>
<Printer deskjet_3500>
Info hp deskjet 3500
DeviceURI hp :/usb/deskjet_3500?serial=TH39B162J376
State Idle
```

```
StateTime 1235655640
Accepting Yes
Shared Yes
JobSheets none none
QuotaPeriod 0
PageLimit 0
KLimit 0
OpPolicy default
ErrorPolicy stop-printer
</Printer>
```

Après toute modification d'un fichier de configuration de cups faite manuellement (hors de l'interface web) il faut relancer le service d'impression cups en faisant

```
/etc/init.d/cups restart
```

### installation de Epiphany

```
apt-get epiphany-browser
```

Ou utilisation de synaptic qui est déjà en place avec l'environnement minimaliste de gnome core. A partir de là on peut plus facilement télécharger certaines sources comme celles de clamav.

### 0.1.6 Installation de l'antivirus Clamav

**source de clamav** <http://www.clamav.net/download/sources> **dépendances**

- C compiler
- zlib
- GMP
- cURL

Ces éléments sont installés par l'intermédiaire de "synaptic" (dans le menu système/administration en haut de la barre du bureau gnome) qui facilite grandement la recherche des paquets disponibles et leur exacte dénomination.

Il est préférable d'installer par les sources le paquet clamav. il faut donc le télécharger à partir de son site. puis faire :

```
tar -xzvf clamav-x.y.z.tar.gz
cd ./clamav-x.y.z
su
# groupadd clamav
# useradd -g clamav -s /bin/false -c "Clam AntiVirus"
  clamav
./configure
install zlib zlib-devel
```

apt-get install zlib reste muet donc j'ouvre synaptic et je cherche zlib puis je sélectionne tout ce qui se rapporte à zlib sans installer trop de superflu... Ensuite, reprise...

```
./configure --sysconfdir=/etc
make check
make
make install
whereis clamd
```

Je note les emplacements indiqués après cette installation à partir des sources.

### **fichier de configuration de clamav**

`/etc/clamd.conf` Pour démarrer, il faut uniquement commenter la ligne "exemple" puis vérifier les chemins des log, processus et dossiers et éventuellement créer ceux qui manquent en leur donnant clamav comme propriétaire. fichier de configuration de freshclam `/etc/freshclam.conf` Pour démarrer il faut juste commenter la ligne "exemple" puis vérifier les chemins des log indiqués en configuration.

```
touch /var/log/fresclam.log
chmod 600 /var/log/fresclam.log
chown clamav /var/log/fresclam.log
```

### **Fichier starter de Clamav**

```
#! /bin/bash
#
# crond Start/Stop the clam antivirus daemon.
#
# chkconfig : 2345 70 41
# description : clamd is a standard Linux/UNIX program
#               that scans for Viruses.
# processname : clamd
# config       : /etc/clamd.conf
# pidfile      : /var/lock/subsys/clamd (à vérifier)
# Source function library.
#. /etc/init.d/functions
. /lib/lsb/init-functions
RETVAL=0
TMPDIR=/tmp
export TMPDIR
# See how we were called.
prog="/usr/local/sbin/clamd"
start() {
echo -n "$Starting $prog : "
start-stop-daemon --start --quiet --oknodo --exec $prog
RETVAL=$?
echo
[ $RETVAL -eq 0 ] && touch /var/lock/clamd
```

```
return $RETVAL
}
stop() {
echo -n $"Stopping $prog : "
# Would be better to send QUIT first, then killproc if
  that fails
start-stop-daemon -stop -quiet -oknodo -exec $prog
RETVAL=$?
echo
[ $RETVAL -eq 0 ] && rm -f /var/lock/clamd
return $RETVAL
}
rhstatus() {
status clamd
}
restart() {
stop
start
}
reload() {
echo -n $"Reloading clam daemon configuration : "
start-stop-daemon -stop -quiet -oknodo -exec clamd -HUP
retval=$?
echo
return $RETVAL
}
case "$1" in
start)
start
;;
stop)
stop
;;
restart)
restart
;;
reload)
reload
;;
status)
rhstatus
;;
```

```

condrestart)
[ -f /var/lock/clamd ] && restart || :
;;
*)
echo $"Usage : $0 {start|stop|status|reload|restart|condrestart}"
exit 1
esac
exit $?
#fin du fichier

```

Puis faire :

```

#cp /clamavstarter.sh /etc/init.d/clamavstarter.sh
#chmod a+x /etc/init.d/clamavstarter.sh
#update-rc.d -f clamavstarter.sh defaults

```

### 0.1.7 Installation d'une interface d'administration web de la machine passerelle : Webmin

il faut télécharger webmin : en console, je me mets dans /home/paul et je tape :

```
wget http://prdownloads.sourceforge.net/webadmin/webmin_1.470_all.deb
```

**installation de webmin** se mettre dans /home/paul où est le paquets debian de webmin.

faire :

```

tar -xzvf ./webmin_1.470_all.deb
dpkg -i webmin

```

ill nous est répondu qu'il manque plein de choses : libnet-ssleay-perl libauthen-pam-perl libio-pty-perl libmd5-perl donc

```

apt-get install libnet-ssleay-perl libauthen-pam-perl
libio-pty-perl libmd5-perl

```

et là : miracle il nous est répondu que webmin est installé ! si ! On peut alors se connecter avec un navigateur sur webmin à l'adresse

```
https://bleue:10000/
```

Se loguer sous root avec le mot de passe de root On peut même vérifier que cette installation de Webmin va permettre d'administrer la machine passerelle depuis une autre machine du réseau : Dans la barre du navigateur d'une autre machine il faut alors taper :

```
https://192.168.1.2:10000/
```

puis se loguer en root avec le mot de passe. Il reste alors à découvrir l'utilisation de webmin.

### 0.1.8 En guise de conclusion

On a donc une passerelle parefeu serveur de fichiers samba serveur de courrier surveillée par un antivirus.

Il resterait donc pour améliorer cette passerelle à en faire un serveur de courrier permanent diffusant sur internet, surveillé par l'antivirus et des antispam et d'avoir une gestion des

comptes de courriel.

On a déjà une possibilité de gestion des comptes utilisateurs et courrier par webmin.

Cette machine peut convenir ainsi à la mise en réseau des machines windows et linux d'une organisation de petite taille de 10 à 50 machines et utilisateurs. Webmin offre en effet des possibilités de gestions intéressantes dans ce cadre d'utilisation des différents services de partage, de courrier de sécurité. De plus il est possible d'ajouter des modules de gestion (par exemple pour l'antivirus clamav) de différentes applications partagées.

Webmin donne en effet par exemple la possibilité de préciser la sécurité des partages samba, la mise en place de nouveaux utilisateurs, du courrier, la gestion des imprimantes, de ssh, et il est utile de l'installer aussi sur chaque machine du réseau.

Ce montage est donc une solution pratique et gratuite en réponse aux besoins administratifs informatiques d'organisations pouvant être montée sans grande difficulté et avec conscience du fonctionnement de la machine par l'administrateur informatique ou un utilisateur averti de l'organisation.