

Firewall en connexion RTC

Avant-propos.

On peut avoir besoin d'une connexion internet de secours avec un modem classique RTC en cas de défaillance de votre connexion eth0, ou plus simplement lors de déplacement s'il n'y a pas de réseau (Wifi ou autre) disponible accessible mais que vous disposez malgré tout d'une prise téléphonique et d'un modem RTC opérationnel.

Il vous faut premièrement disposer d'un abonnement en RTC chez un FAI. Beaucoup en fournissent un gratuitement (Free, Orange, ..)

Il va falloir ensuite configurer la connexion PPP par modem téléphonique. Cela se fait sous Debian à l'aide de l'utilitaire *pppconfig* qu'il faut lancer en root. Il faudra renseigner le port du modem et les paramètres de connexion (numéro, identifiant et password). Conservez le nom de connexion provider et le protocole PAP proposés par défaut.

Vous aurez aussi à paramétrer un firewall car n'étant plus derrière le modem/routeur ADSL et son firewall intégré vous seriez alors totalement à découvert connecté au web par votre connexion ppp.

Il va falloir vous configurer un firewall avec *iptables*, modifier la configuration du *resolv.conf* pour avoir des DNS de votre choix comme OpenDns, modifier la configuration du fichier *interfaces* pour conserver l'accès au réseau local par la carte ethernet.

Création du firewall.

La première chose à faire est d'installer *iptables* et pour cela on fait en root

```
# apt-get install iptables
```

Ensuite l'on va créer un script firewall contenant les instructions *iptables* du firewall. Ce script on l'installe où l'on veut dans */etc*, personnellement je l'installe dans */etc/init.d*

```
# vim /etc/init.d/firewall
```

et on le remplit avec les instructions *iptables* que l'on veut et on rend ce script exécutable par

```
# chmod +x /etc/init.d/firewall
```

Il nous faudra aussi un script permettant d'arrêter le firewall en supprimant toutes les instructions *iptables* précédentes.

```
# vim /etc/init.d/stopfirewall
```

```
# chmod +x /etc/init.d/stopfirewall
```

Exemple de script firewall.

```
#!/bin/sh
#Ne sert que pour les connexions en RTC car le firewall externe du routeur ne protège plus d'internet.
# Réinitialise les règles
iptables -t filter -F
iptables -t filter -X
# Bloque tout le trafic
iptables -t filter -P INPUT DROP
iptables -t filter -P FORWARD DROP
```

```
iptables -t filter -P OUTPUT DROP
# Autorise les connexions déjà établies et localhost
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t filter -A INPUT -i lo -j ACCEPT
iptables -t filter -A OUTPUT -o lo -j ACCEPT
# ICMP (Ping)
iptables -t filter -A INPUT -p icmp -j ACCEPT
iptables -t filter -A OUTPUT -p icmp -j ACCEPT
# SSH
iptables -t filter -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 22 -j ACCEPT
# DNS
iptables -t filter -A OUTPUT -p tcp --dport 53 -j ACCEPT
iptables -t filter -A OUTPUT -p udp --dport 53 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 53 -j ACCEPT
iptables -t filter -A INPUT -p udp --dport 53 -j ACCEPT
# HTTP
iptables -t filter -A OUTPUT -p tcp --dport 80 -j ACCEPT
iptables -t filter -A INPUT -p tcp -s 192.168.1.0/24 --dport 80 -j ACCEPT
# FTP
iptables -t filter -A OUTPUT -p tcp -m multiport --dport 20:21,49152:65534 -j ACCEPT
iptables -t filter -A INPUT -p tcp -m multiport --dport 20:21,49152:65534 -j ACCEPT
# Mail SMTP
iptables -t filter -A INPUT -p tcp -s 192.168.1.0/24 -m multiport --dport 25,587 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp -m multiport --dport 25,587 -j ACCEPT
# Mail POP3
iptables -t filter -A INPUT -p tcp -s 192.168.1.0/24 -m multiport --dport 110,995 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp -m multiport --dport 110,995 -j ACCEPT
# Mail IMAP
# iptables -t filter -A INPUT -p tcp --dport 143 -j ACCEPT
# iptables -t filter -A OUTPUT -p tcp --dport 143 -j ACCEPT
# NTP (horloge du serveur)
iptables -t filter -A OUTPUT -p udp --dport 123 -j ACCEPT
#Samba
iptables -t filter -A INPUT -p tcp -s 192.168.1.0/24 --dport 139 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 139 -j ACCEPT
iptables -t filter -A INPUT -p tcp -s 192.168.1.0/24 --dport 445 -j ACCEPT
```

```
iptables -t filter -A OUTPUT -p tcp --dport 445 -j ACCEPT
iptables -t filter -A INPUT -p udp -s 192.168.1.0/24 --dport 137 -j ACCEPT
iptables -t filter -A OUTPUT -p udp --dport 137 -j ACCEPT
iptables -t filter -A INPUT -p udp -s 192.168.1.0/24 --dport 138 -j ACCEPT
iptables -t filter -A OUTPUT -p udp --dport 138 -j ACCEPT
iptables -t filter -A INPUT -p udp -s 192.168.1.0/24 --dport 445 -j ACCEPT
iptables -t filter -A OUTPUT -p udp --dport 445 -j ACCEPT
```

Ce script est adaptable selon les besoins, on peut commenter des règles ou en ajouter d'autres. Tel qu'il est le firewall n'autorisera que les règles inscrites tout le reste sera bloqué.

Le script stopfirewall

Ce script annulera toutes les règles *iptables* précédemment instituées, voir le man *iptables* pour explication.

```
#!/bin/bash
#suppression règles d'une chaîne
iptables -F
#suppression chaînes utilisateur
iptables -X
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT

iptables -t nat -F
iptables -t nat -X
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
iptables -t nat -P OUTPUT ACCEPT

iptables -t mangle -F
iptables -t mangle -X
iptables -t mangle -P INPUT ACCEPT
iptables -t mangle -P OUTPUT ACCEPT
iptables -t mangle -P OUTPUT ACCEPT
iptables -t mangle -P PREROUTING ACCEPT
iptables -t mangle -P POSTROUTING ACCEPT
```

On va devoir également créer les fichiers */etc/network/interfaces.rtc* où l'on supprimera la passerelle (*gateway*) pour la connexion ethernet et */etc/network/interfaces.adsl* qui les rétablira ainsi que les fichiers */etc/resolv.conf.rtc* et */etc/resolv.conf.adsl* qui serviront l'un à modifier la configuration du réseau et l'autre les DNS.

Fichier *interfaces.rtc*

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
# The primary network interface
#allow-hotplug eth0
iface eth0 inet static
address 192.168.1.2
netmask 255.255.255.0
broadcast 192.168.1.255
network 192.168.1.0
```

Fichier *interfaces.adsl*

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
# The primary network interface
#allow-hotplug eth0
iface eth0 inet static
address 192.168.1.2
netmask 255.255.255.0
broadcast 192.168.1.255
network 192.168.1.0
gateway 192.168.1.1
```

Fichier resolv.conf.rtc

```
#on mets les DNS que l'on veut par exemple
#OpenDns
nameserver 208.67.222.222
nameserver 208.67.220.220
#SFR
nameserver 109.0.66.10
nameserver 109.0.66.20
```

Fichier resovl.conf.adsl

```
#on mets les DNS que l'on veut par exemple
#le routeur et ses DNS
nameserver 192.168.1.1
#OpenDns
nameserver 208.67.222.222
nameserver 208.67.220.220
#SFR
nameserver 109.0.66.10
nameserver 109.0.66.20
```

Ensuite il ne reste plus qu'à écrire nos deux fichiers de lancement et d'arrêt de la connexion RTC, ces deux fichiers devront être rendu exécutable par un `chmod +x` et seront à lancer dans un terminal depuis leur dossier par `./fichier`, le passe sudo vous sera alors demandé.

Fichier Connection_RTC

```
#!/bin/sh
#Sert à passer en RTC le resolv.conf doit donner des DNS car il n'y a plus de passerelle
#on arrête eth0
sudo ifdown eth0
#on modifie la configuration de eth0
sudo cp /etc/network/interfaces.rtc /etc/network/interfaces
#on lance le firewall
sudo /etc/init.d/firewall
#on relance eth0 pour le réseau interne
sudo ifup eth0
#on modifie le resolv.conf pour les DNS
sudo cp /etc/resolv.conf.rtc /etc/resolv.conf
#on se connecte en RTC
sudo pon
```

Fichier Couper_RTC

```
#!/bin/sh
#coupe la connexion RTC, supprime le firewall et rétablit eth0 en ADSL
#on arrête la connexion RTC
sudo poff
#on arrête eth0
sudo ifdown eth0
#on rétablit la configuration de eth0 pour l'ADSL
sudo cp /etc/network/interfaces.adsl /etc/network/interfaces
#on stoppe le firewall
sudo /etc/init.d/stopfirewall
#on rétablit le resolv.conf pour l'ADSL
sudo cp /etc/resolv.conf.adsl /etc/resolv.conf
#on relance eth0 pour le WAN et le LAN
sudo ifup eth0
```

Ce document écrit par Michel Eudes est sous licence CC [Creative Commons](https://creativecommons.org/licenses/by-nc-sa/2.0/fr/) :



Attribution - Pas d'Utilisation Commerciale - Partage à l'Identique 2.0 France CC BY-NC-SA 2.0