

Fwtroops

Frédéric Bourgeois

Rennes 21/04/2005

<http://traceroute.free.fr>

Fwtroops	1
Presentation:.....	1
Configuration Fwtroops.....	2
Architecture.....	4
Configuration des serveurs Pare-feux.....	4
Utilisation.....	6
FAQ.....	8

Presentation:

Fwtroops est un logiciel de management de serveurs Netfilter / iptables qui permet la gestion conviviale des politiques de sécurité grâce à une interface utilisateur graphique il peut conserver sur une machine de référence les fichiers de configurations ainsi que les règles de tous vos Firewalls afin de pouvoir les injecter de manière sécurisés quand bon vous semble. Il fonctionne sous GNU/LINUX (testé sous Debian et Mandrake) avec Python et Glade (GTK), connexion avec les serveurs en SSH et SCP.

Il est maintenant possible de:

- Transférer et récupérer la configuration d'un firewall.
- Sauvegarder et effectuer une rotation par dates des règles pour un retour arrière facilité (ainsi que pouvoir suivre l'évolution de vos règles et de vos routes).
- Obtenir les informations complètes d'une machine.
- Stocker sur un serveur de référence vos fichiers de configurations (datés).
- Editeur de routes.
- Gestion, sauvegarde et rotation des fichiers routes.
- Mini moteur de recherche (ctrl + f).
- Restauration d'une machine.
- Ajouter dans l'interface graphique des commentaires sur vos pare-feux.
- Il vérifie l'intégrité MD5 des fichiers .route et .fw

Configuration Fwtroops

Dans le répertoire /opt/fwtroops/data

- fwtroops.conf

```
#####  
#####  
# ROOTKEY  
#####  
#####  
ROOTKEY=/root/root.key  
#####  
#####  
#PATH RULES  
#####  
#####  
PATHRULES=/mnt/Public/fwbuilder/confnetfilter/  
#####  
#####  
#STOCK RULES STOCKAGE DES CONF DES FIREWALS  
STOCKRULES=/var/referentiel/firewall
```

ROOTKEY = SI besoin le chemin de votre clef root ssh

PATH RULES = Le chemin du répertoire de stockage des fichiers de règles,
ATTENTION les règles doivent porter le même nom que le serveur (ex:
netfilterhttp.fw pour le serveur netfilterhttp)

STOCK RULES = Le repertoire de travail/stockage interne de fwtroops.

Au besoin, créer une clef ssh:

Dans le répertoire de l'utilisateur (ou /root/ si besoin), taper **ssh-keygen -t rsa** .
Cela crée une paire de clef avec une phrase d'identification. Par défaut, la clef
privée va dans ~/.ssh/id_rsa et la clef publique dans ~/.ssh/id_rsa.pub. Pour les
identités multiples, il faut plusieurs fichiers et on précise le nom du fichier au
lancement : **ssh -i ma_cle**.

Pour extraire la clé publique de sa clé privée il faut utiliser la commande
suivante:

```
ssh-keygen -y
```

```
Enter file in which the key is (/root/.ssh/id_rsa):  
mykey.key
```

Sur le serveur auquel on veut accéder, il suffit de recopier la clef publique dans le fichier `~/.ssh/authorized_keys` .

Tester la connexion ssh:

```
ssh -v -i ./clé_privée login@10.1.1.2
```

Architecture

Fwtroops utilise les fichiers de configurations situés dans PATHRULES et reproduit l'arborescence des firewalls en local dans STOCKRULES.

Il faut obligatoirement que les règles (PATHRULES) portent le nom exact du serveur distant, par exemple pour le serveur netfilterhttp -> netfilterhttp.fw, de plus le pare-feu doit contenir ses règles dans un répertoire /etc/sec/ (Configuration des serveurs Pare-feux)

Configuration des serveurs Pare-feux

Les serveurs Netfilters doivent être impérativement configurés de la manière suivante

Un répertoire /etc/sec contient les règles (route et conf netfilter):

Les règles se lancent (par exemple) de la manière suivante:

/etc/rc(x) :

```
lrwxrwxrwx 1 root root 27 Jun 26 2003 S98netfilter_route.sh ->
/etc/init.d/netfilter_route.sh
lrwxrwxrwx 1 root root 26 Jun 26 2003 S99netfilter_rule.sh ->
/etc/init.d/netfilter_rule.sh
```

Les liens pointent sur les scripts suivant:

```
/etc/rc2.d$ more /etc/init.d/netfilter_rule.sh
```

```
#!/bin/sh
```

```
#
# Chargement des règles de filtrage
#
```

```
case "$1" in
  start)
    /sbin/sysctl -p /etc/sysctl.conf
    /etc/sec/$HOSTNAME".fw"
    ;;
  stop)
    iptables -P INPUT ACCEPT
    iptables -P FORWARD ACCEPT
    iptables -P OUTPUT ACCEPT
    iptables -F
```

```
iptables -t nat -F
iptables -t mangle -F
iptables -X
iptables -t nat -X
iptables -t mangle -X
;;
*)
    echo "Usage: /etc/init.d/netfilter_rule.sh {start|stop}"
    exit 1
;;
esac
```

Et netfilter_route.sh :

```
/etc/rc2.d$ more /etc/init.d/netfilter_route.sh
```

```
#!/bin/sh
#
# Chargement des routes
#

case "$1" in
    start)
        /etc/sec/$HOSTNAME".route"
        ;;
    stop)

        ;;
    *)
        echo "Usage: /etc/init.d/netfilter_route.sh {start|stop}"
        exit 1
        ;;
esac
```

Utilisation

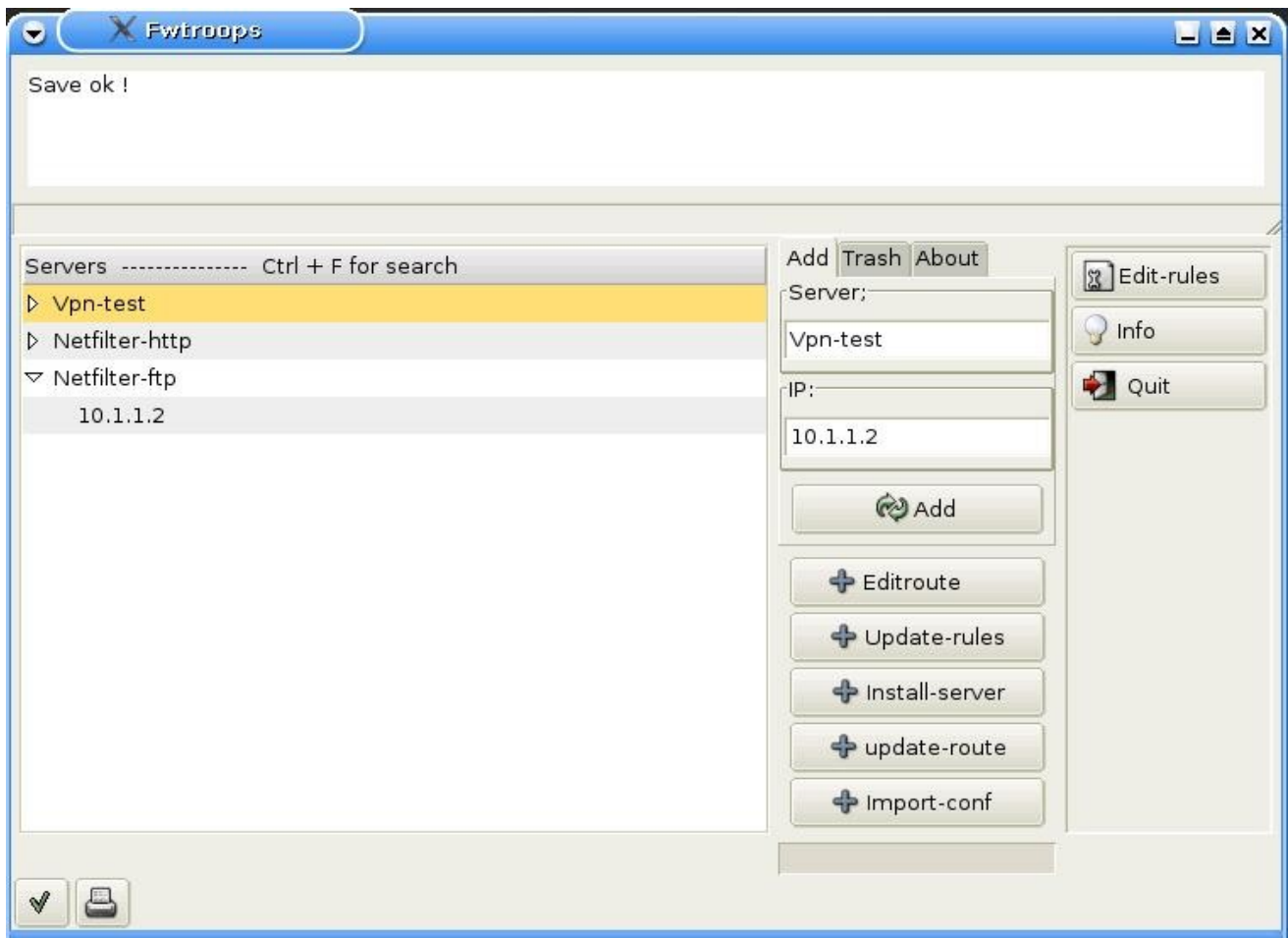
Attention le logiciel ne fonctionne que sous le compte root, il suffit pour cela de lancer fwtroops dans un shell ou bien dans KDE -> Internet -> Autres.

1. Tout d'abord il vous faut créer vos objets en ajoutant le nom de vos machines ainsi que leur IP dans Server, n'oubliez pas de cliquer sur add pour valider la création.

Pour pouvoir travailler il vous faut sélectionner un serveur dans la liste déroulante et cliquer sur select.

Ensuite vous pouvez:

- Updates-rules: Récupère le fichier de configuration dans PATHRULES et l'applique sur le serveur. (En sauvegardant l'ancienne conf dans STOCKRULES/server/etc/sec/ avec rotation par date) *1
- Restore server: restaure le répertoire /etc dans la machine distante (ATTENTION: écrase l'ancien /etc ...)
- Update-route: Injecte et applique le fichier de routes situé dans /etc/sec (ex:STOCKRULES/netfilterhttp/etc/sec/netfilterhttp.route)
- Edit routes: Édite les routes de vos pare-feux
- Import conf: Sauvegarde le répertoire /etc du serveur Netfilter et le sauvegarde dans son répertoires Fwtroops (en tar.gz) il récupère aussi le répertoire /etc/sec et le stocke au même endroit *2
- Info: Affiche la configuration d'un serveur



*1

```
[root@test Fwtroops]# ls -la netfilterhttp/etc/sec/
total 12582912
drwxr-xr-x 1 root root 0 jun 25 15:35 ./
drwxr-xr-x 1 root root 0 oct 9 2003 ../
-rwx----- 1 root root 15735 jun 25 15:35 netfilterhttp2004_jun_21_a_11h51.fw
-rwx----- 1 root root 15735 jun 25 15:35 netfilterhttp2004_jun_21_a_11h52.fw
-rwx----- 1 root root 15735 jun 25 15:35 netfilterhttp2004_jun_25_12h11.fw
-rwx----- 1 root root 15735 jun 25 15:35 netfilterhttp2004_jun_25_15h14.fw
-rwx----- 1 root root 15735 jun 25 15:35 netfilterhttp2004_jun_25_15h15.fw
-rwx----- 1 root root 15735 jun 25 15:35 netfilterhttp.route
-rwx----- 1 root root 15735 jun 25 16:25 nefilterhttp.fw*
-rwx----- 1 root root 825 jun 25 15:35 netfilterhttp.route*
```

*2

```
[root@test Fwtroops]# ls -la netfilterhttp/
total 2097152
drwxr-xr-x 1 root root 0 mai 26 16:07 ./
drwxr-xr-x 1 root root 0 jun 25 10:55 ../
drwxr-xr-x 1 root root 0 mai 25 15:05 etc/
-rwxrw---- 1 root root 263314 mai 25 15:51 sauve.tar.gz*
-rwxr----- 1 root root 155281 jun 25 14:46 save2004_jun_25_14h46.tar.gz
-rwxr----- 1 root root 155281 jun 25 14:47 save2004_jun_25_14h47.tar.gz
```

FAQ

Q - Au lancement de l'application:

File "/usr/bin/fwtroops", line 29, in ? import gtk.glade ImportError: No module named glade

R - urpmi pygtk2.0-libglade / apt-get install python2.4-gtk2 python-gtk2 python-glade2 python2.4-glade2

Q - Les règles ne s'appliquent pas

R - Il faut obligatoirement que les règles stockées en local portent le nom exact du serveur distant, par exemple pour le serveur netfilterhttp -> netfilterhttp.fw, de plus le pare-feu doit contenir ses règles dans un répertoire /etc/sec/ (Voir Configuration des serveurs Pare-feux)