Infra Chapril - Demande #4823

Re-évaluer START_FIREHOL=YES

31/10/2020 17:14 - Christian P. Momon

Statut:	Fermé	**Début:**	20/01/2020
Priorité:	Normale	**Echéance:**	
Assigné à:	François Poulain	**% réalisé:**	0%
Catégorie:	Hypervision	**Temps estimé:**	0.00 heure
Version cible:	Sprint 2021 janvier		

Description

Dans la procédure d'installation d'une vm, dans la page
https://admin.chapril.org/doku.php?id=admin:procedures:configuration-firewall-guest
on peut lire :

```
 Une fois qu'on est sûr de conserver le firewall, on peut activer le firewall via /etc/default/fir
ehol :

/etc/default/firehol

    START_FIREHOL=YES

Ainsi le firewall est actif dès le démarrage du démon.
Sans cette dernière étape, votre serveur redevient à poil dès le prochain redémarrage !
```

Constat que cette configuration a été oubliée pour plusieurs vm récentes :

```
cpm@ocmstar (15:30:29) ~/Dossiers/April/Chapril/Adminsys 38 > ./do.sh "grep START_FIREHOL /etc/def
ault/firehol" |grep -v "#"
===== valise =====
START_FIREHOL=NO
===== xmpp =====
START_FIREHOL=NO
===== drop =====
START_FIREHOL=NO
===== allo =====
START_FIREHOL=NO
===== biliz =====
START_FIREHOL=NO
===== catom =====
START_FIREHOL=NO
===== grof =====
START_FIREHOL=NO
```

Par contre, cela ne semble pas gêner le démarrage automatique de firehol :

```
=(^-^)=root@biliz:~# systemctl status firehol
● firehol.service - Firehol stateful packet filtering firewall for humans
   Loaded: loaded (/lib/systemd/system/firehol.service; enabled; vendor preset: enabled)
   Active: active (exited) since Sat 2020-10-31 15:37:02 CET; 1h 35min ago
     Docs: man:firehol(1)
           man:firehol.conf(5)
  Process: 434 ExecStart=/usr/sbin/firehol start (code=exited, status=0/SUCCESS)
 Main PID: 434 (code=exited, status=0/SUCCESS)
[…]
=(^-^)=root@biliz:~# iptables-legacy -L |head
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
in_dhcp    all  --  anywhere             anywhere
```

```
in_internal_trafic  all  --  192.168.1.0/24       biliz
in_internal_trafic  all  --  192.168.1.0/24       biliz
in_external_trafic  all  --  anywhere             biliz
in_external_trafic  all  --  anywhere             biliz
DROP       tcp  --  anywhere             anywhere             tcp flags:FIN,ACK/FIN,ACK ctstate IN
VALID,NEW
DROP       tcp  --  anywhere             anywhere             tcp flags:RST,ACK/RST,ACK ctstate IN
VALID,NEW
[…]
```

Questions :

- pourquoi START_FIREHOL n'est-il plus pris en compte ?
- faut-il retirer cette étape de la doc d'installation ?

Historique

#1 - 28/11/2020 10:32 - François Poulain

Je pense que c'est du legacy. L'intégration de firehol dans systemd sous bbuster n'a pas l'air de tenir compte de l'environnement de /etc/default

#2 - 28/11/2020 10:33 - François Poulain

La doc upstream a l'air de dire que c'est un choix de la distro : https://firehol.org/faq/#where-located

#3 - 28/11/2020 10:36 - François Poulain

Le log dit https://metadata.ftp-master.debian.org/changelogs//main/f/firehol/firehol_3.1.6+ds-8_changelog

```
firehol (2.0.0~rc.1+ds-1) experimental; urgency=medium

  * New upstream major version:
    - IPv6 support (Closes: #292621);
    - detailed documentation (Closes: #556575);
    - traffic shaping support coined FireQOS as
      counterpart of the firewall FireHOL;
    - all non-Debian-centric patches were incorporated.
  * Debianization:
    - debian/control:
      - update descriptions;
      - new binary packages: firehol-doc, fireqos and fireqos-doc;
    - debian/{copyright,NEWS,README.{Debian,Services}}, refresh;
    - debian/firehol.init, revisit (Closes: #574459);
    - material for firehol-doc, fireqos and fireqos-doc;
    - firehol has been moved from /sbin to /usr/sbin for consistency
      reasons, fireqos being in /usr/sbin for similar reasons;
    - /etc/default/firehol is no more source_d by firehol;
    - /etc/init.d/firehol now exports variables defined in
      /etc/default/firehol;
    - debian/firehol.README.Debian, add notes (with samples) to log
      firehol messages to a separate log file with rsyslog;
    - make /etc/fireqos the configuration folder for FireQOS
      instead of /etc/firehol as in the upstream distribution.
  * Minor, cosmetic fixes submitted to the upstream maintainers.
```

#4 - 28/11/2020 10:39 - François Poulain

Et la conf systemd ne fait pas apparaitre qsuelque chose comme EnvironmentFile=-/etc/default/firehol :

```
[Unit]
Description=Firehol stateful packet filtering firewall for humans
Documentation=man:firehol(1) man:firehol.conf(5)

DefaultDependencies=no

Before=network-pre.target
Wants=network-pre.target

Wants=systemd-modules-load.service local-fs.target
After=systemd-modules-load.service local-fs.target

Conflicts=shutdown.target
Before=shutdown.target
```

```
[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/usr/sbin/firehol start
ExecStop=/usr/sbin/firehol stop

[Install]
WantedBy=multi-user.target
```

#5 - 28/11/2020 10:40 - François Poulain

Donc pour moi c'est clairement un comportement induit par Debian. Je ne sais pas si c'est un bug ou une feature.

#6 - 28/11/2020 10:58 - François Poulain

- Statut changé de Nouveau à En cours de traitement

- Assigné à mis à François Poulain

J'ai rapporté upstream.
https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=976014

#7 - 03/01/2021 11:45 - Christian P. Momon

- Catégorie mis à Hypervision

#8 - 31/01/2021 15:59 - François Poulain

- Statut changé de En cours de traitement à Résolu

J4ai pas de retour du mainteneur Debian. Visiblement la conf de l'unit systemd vient de l'upstream qui ignore /etc/defaults. Donc je pense que c'est du legacy. Peut être conservé par soucis de permettre un autre système d'init dans Debian.

Quoi qu'il en soit, j'ai corrigé le doc.

#9 - 03/02/2021 23:22 - Quentin Gibeaux

- Statut changé de Résolu à Fermé

#10 - 04/02/2021 04:35 - Christian P. Momon

- Version cible changé de Backlog à Sprint 2021 janvier

#11 - 03/12/2021 21:29 - François Poulain

Dans bullseye, ce comportement redevient cohérent. Il faut passer START_FIREHOL=YES dans /etc/default/firehol