

Administration Linux

- ☐ Les comptes
- ☐ Planifier une tâche : crontab
- ☐ La sécurité
 - Les types d'utilisateurs
 - Les droits
 - SELinux
 - AppArmor
- ☐ Pare-feu sous Linux : IPTables
- ☐ Outil graphique de paramétrage de pare-feu : FWBuilder
- ☐ Attributions de ressources à un utilisateur ou un groupe

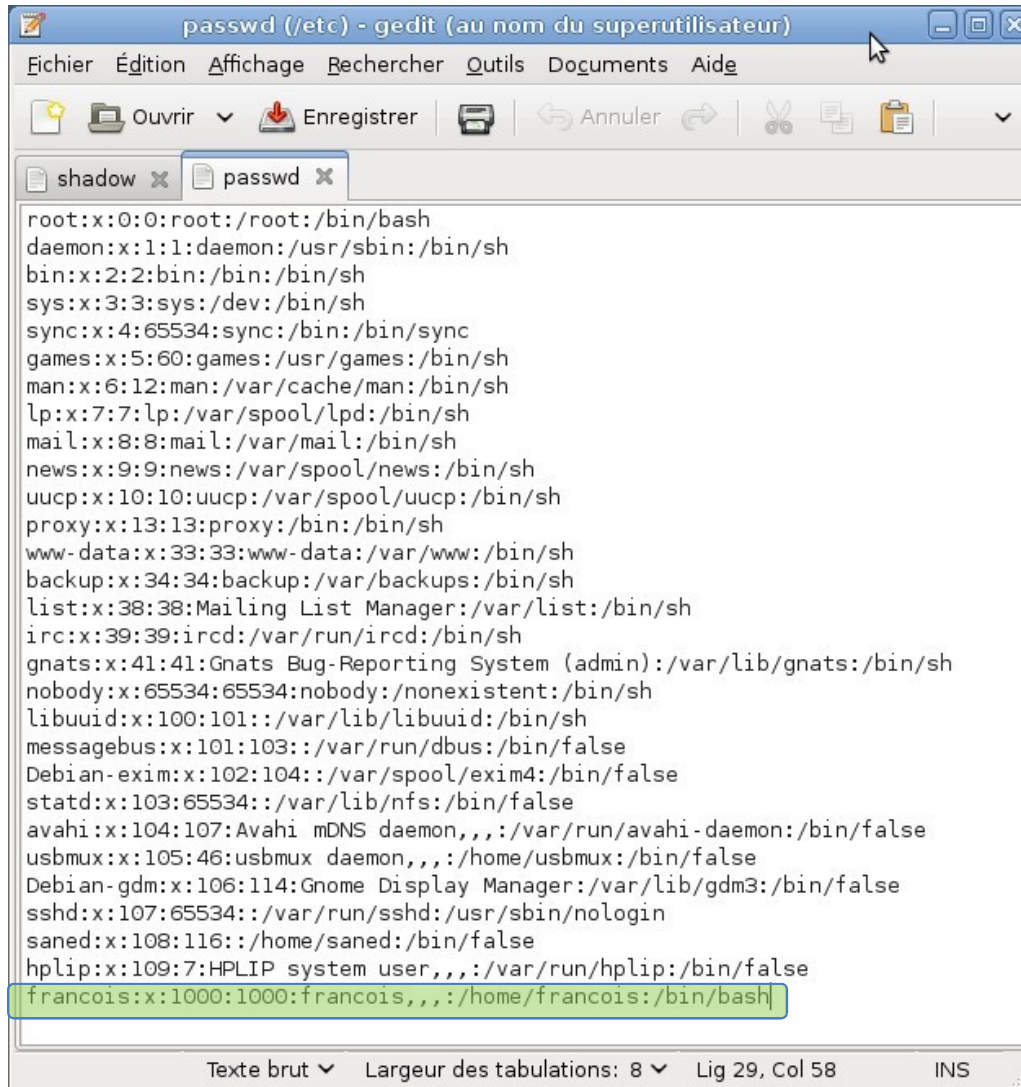
Les comptes sous Linux

La création d'un utilisateur génère une entrée dans `/etc/passwd` et dans `/etc/shadow`

Fichier `passwd`:

- Chaque utilisateur est enregistré sur une ligne différente
- Chaque ligne comprend sept champs séparés par une paire de points
- La plupart des enregistrements ne correspondent pas à des utilisateurs physiques mais sont associés à des programmes

Les comptes sous Linux



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
messagebus:x:101:103::/var/run/dbus:/bin/false
Debian-exim:x:102:104::/var/spool/exim4:/bin/false
statd:x:103:65534::/var/lib/nfs:/bin/false
avahi:x:104:107:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
usbmux:x:105:46:usbmux daemon,,,:/home/usbmux:/bin/false
Debian-gdm:x:106:114:Gnome Display Manager:/var/lib/gdm3:/bin/false
sshd:x:107:65534::/var/run/sshd:/usr/sbin/nologin
saned:x:108:116::/home/saned:/bin/false
hplip:x:109:7:HPLIP system user,,,:/var/run/hplip:/bin/false
francois:x:1000:1000:francois,,,:/home/francois:/bin/bash
```

Le fichier `/etc/passwd` contient la liste des comptes

francois: Identifiant

x: MDP chiffré conservé dans `/etc/shadow` /

Si * → Compte désactivé

1000: UID (User ID)

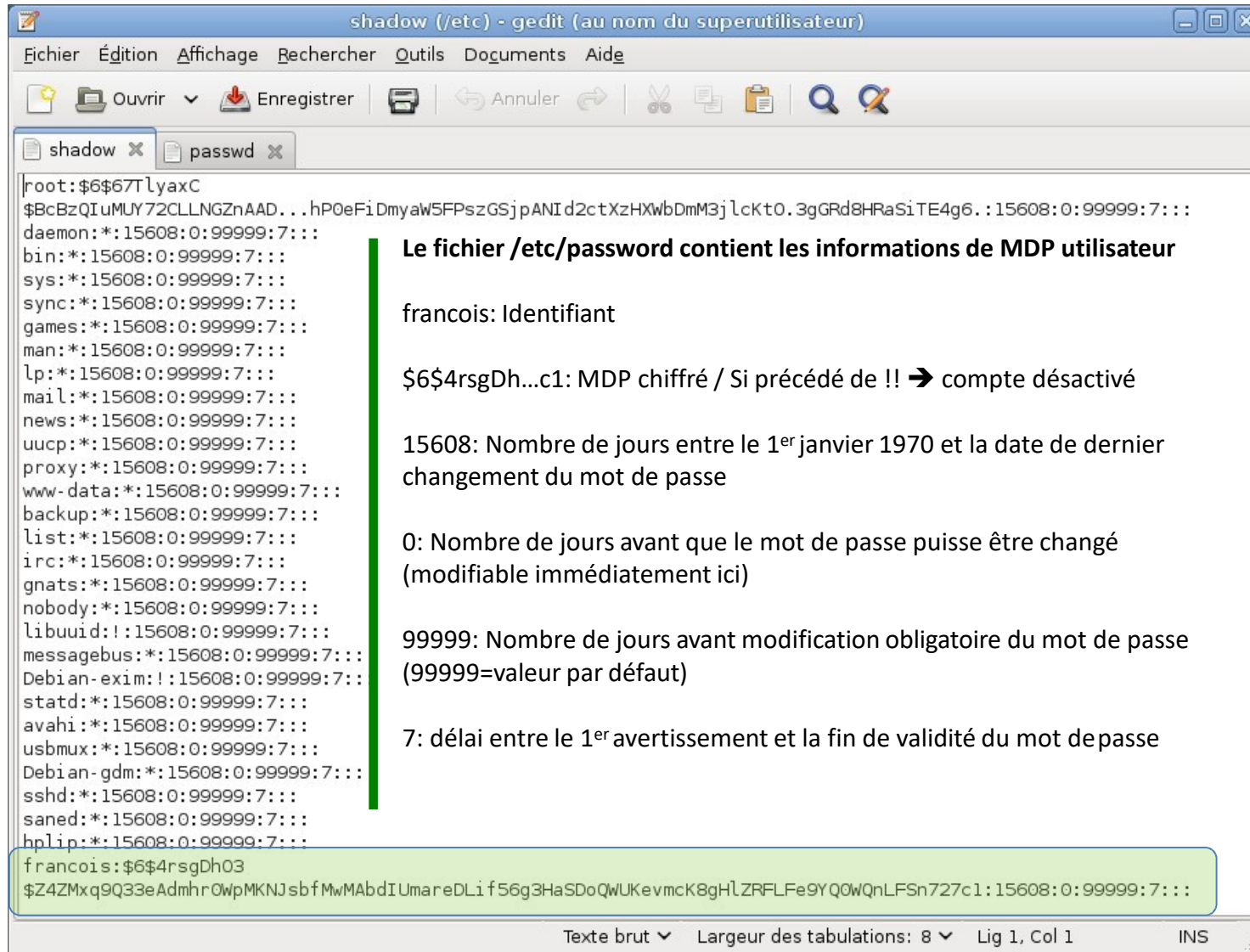
1000: GID (Group ID)

francois,,,: Nom complet et coordonnées de l'utilisateur (cf. `adduser`)

`/home/francois`: Répertoire personnel

`/bin/bash`: Shell à démarrer lors de la connexion de l'utilisateur (ensemble des commandes autorisées pour l'utilisateur)

Les comptes sous Linux



Le fichier /etc/passwd contient les informations de MDP utilisateur

francois: Identifiant

\$6\$4rsgDh...c1: MDP chiffré / Si précédé de !! → compte désactivé

15608: Nombre de jours entre le 1^{er} janvier 1970 et la date de dernier changement du mot de passe

0: Nombre de jours avant que le mot de passe puisse être changé (modifiable immédiatement ici)

99999: Nombre de jours avant modification obligatoire du mot de passe (99999=valeur par défaut)

7: délai entre le 1^{er} avertissement et la fin de validité du mot de passe

```
root:$6$67TlyaxC
$BcBzQIUUY72CLLNGZnAAD...hPOeFiDmyaw5FPszGSjpANId2ctXzHXWbDmM3jlcKt0.3gGRd8HRaSiTE4g6.:15608:0:99999:7:::
daemon*:15608:0:99999:7:::
bin*:15608:0:99999:7:::
sys*:15608:0:99999:7:::
sync*:15608:0:99999:7:::
games*:15608:0:99999:7:::
man*:15608:0:99999:7:::
lp*:15608:0:99999:7:::
mail*:15608:0:99999:7:::
news*:15608:0:99999:7:::
uucp*:15608:0:99999:7:::
proxy*:15608:0:99999:7:::
www-data*:15608:0:99999:7:::
backup*:15608:0:99999:7:::
list*:15608:0:99999:7:::
irc*:15608:0:99999:7:::
gnats*:15608:0:99999:7:::
nobody*:15608:0:99999:7:::
libuuid!:15608:0:99999:7:::
messagebus*:15608:0:99999:7:::
Debian-exim!:15608:0:99999:7:::
statd*:15608:0:99999:7:::
avahi*:15608:0:99999:7:::
usbmux*:15608:0:99999:7:::
Debian-gdm*:15608:0:99999:7:::
sshd*:15608:0:99999:7:::
saned*:15608:0:99999:7:::
hplip*:15608:0:99999:7:::
francois:$6$4rsgDh03
$Z4ZMxq9Q33eAdmhrOWpMKNJsbfMwMAbdIUmareDLif56g3HaSDoQwUKevmck8gHlZRFLFe9YQ0WQnLFSn727c1:15608:0:99999:7:::
```

Texte brut ▾ Largeur des tabulations: 8 ▾ Lig 1, Col 1 INS

Les comptes sous Linux

Les groupes:

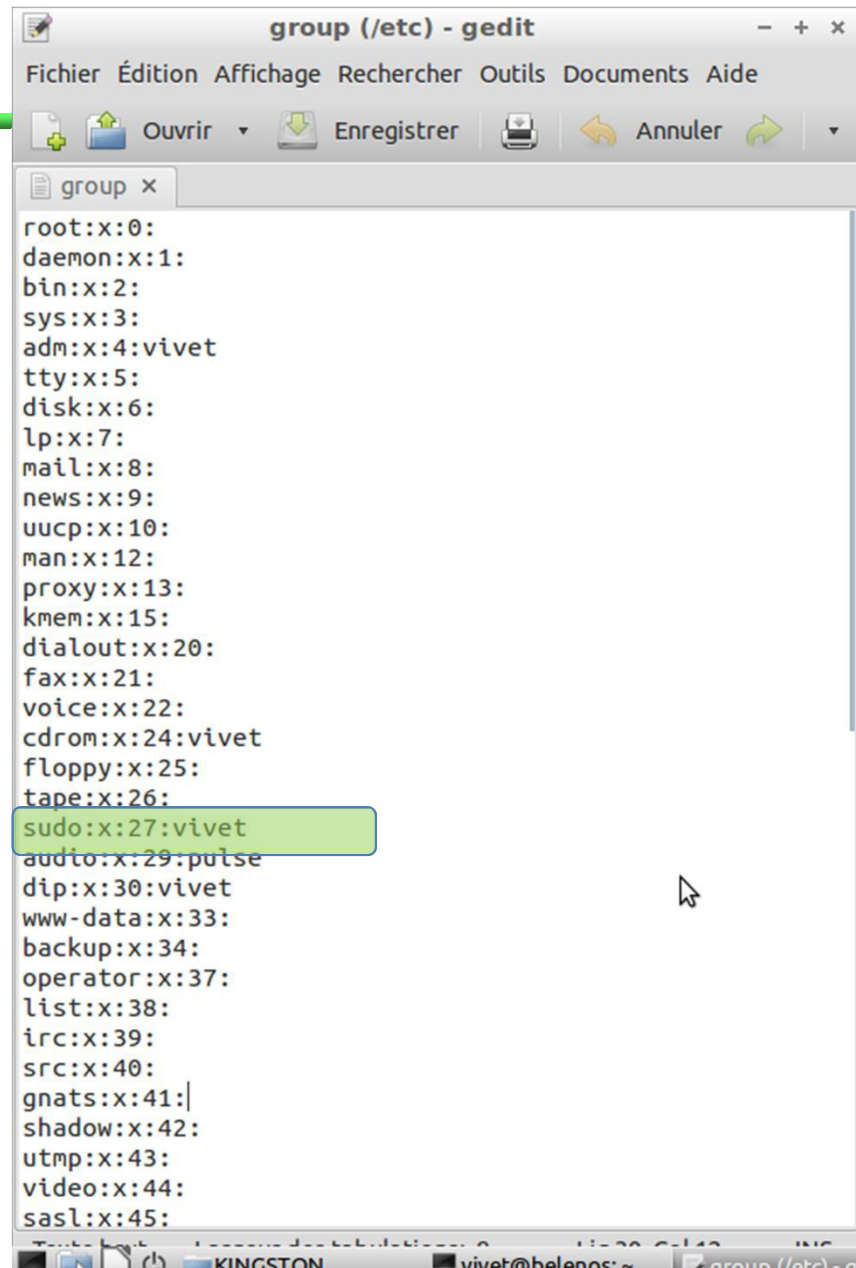
Le fichier `/etc/group` contient la liste des groupes

`sudo`: Nom du groupe

`x`: mot de passe chiffré conservé dans `/etc/gshadow`
(pas de mot de passe en général)

`27`: GID (Group ID)

`Vivet`: Liste des utilisateurs appartenant au groupe
séparés par des virgules, un seul dans notre cas

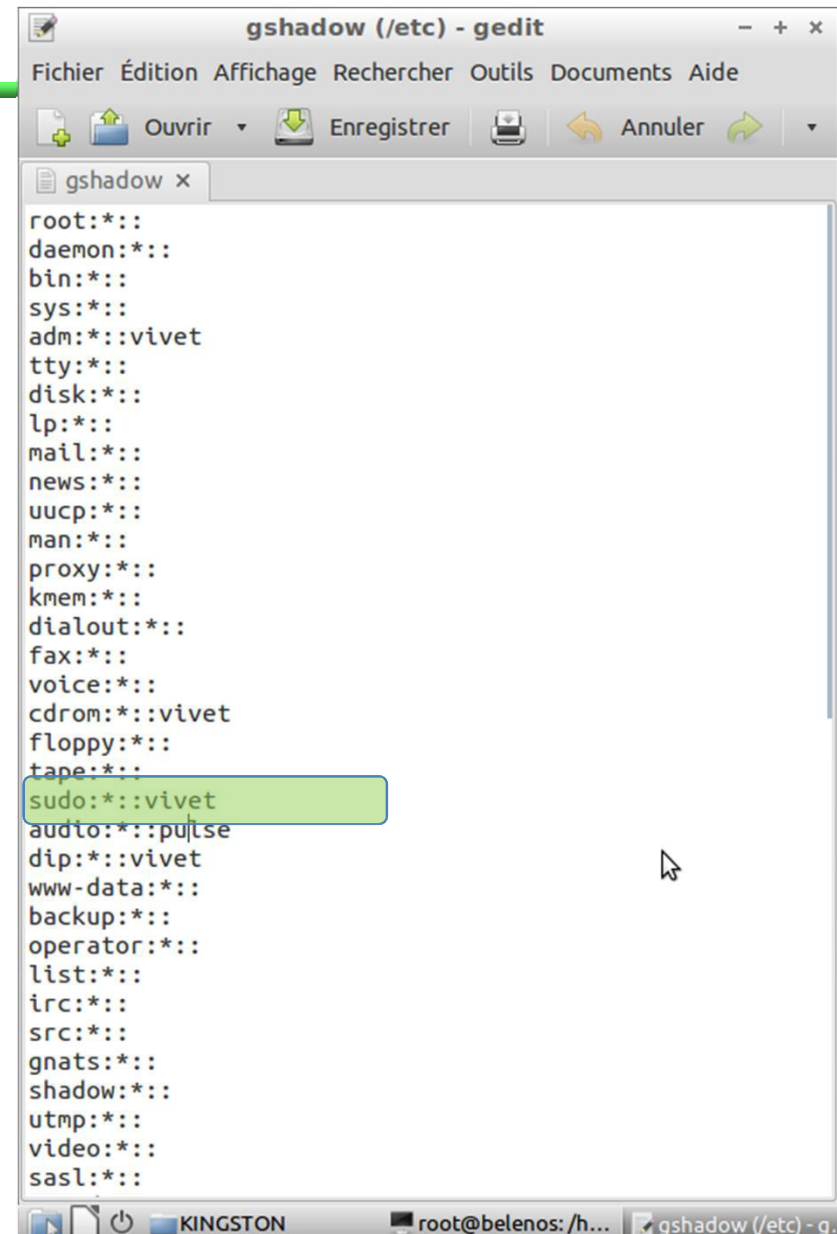


```
group (/etc) - gedit
Fichier Édition Affichage Rechercher Outils Documents Aide
Ouvrir Enregistrer Annuler
group x
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:vivet
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:vivet
floppy:x:25:
tape:x:26:
sudo:x:27:vivet
audio:x:29:pulse
dip:x:30:vivet
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
```

Les comptes sous Linux

Le fichier `/etc/gshadow` contient les informations de MDP des groupes

Il est au même format que `/etc/group` mais pas lisible par tous les utilisateurs (root)



```
gshadow (/etc) - gedit
Fichier  Édition  Affichage  Rechercher  Outils  Documents  Aide
Ouvrir  Enregistrer  Annuler
gshadow x
root:*::
daemon:*::
bin:*::
sys:*::
adm:*::vivet
tty:*::
disk:*::
lp:*::
mail:*::
news:*::
uucp:*::
man:*::
proxy:*::
kmem:*::
dialout:*::
fax:*::
voice:*::
cdrom:*::vivet
floppy:*::
tape:*::
sudo:*::vivet
audio:*::pulse
dip:*::vivet
www-data:*::
backup:*::
operator:*::
list:*::
irc:*::
src:*::
gnats:*::
shadow:*::
utmp:*::
video:*::
sasl:*::
```

Planifier une tâche: crontab

Le service cron (crond) est démarré en tâche de fond

Il attend le moment spécifié dans `/etc/crontab` pour lancer une commande

Ne pas modifier directement `/etc/crontab`

A la place, lancer l'éditeur (vi) par la commande

➔ `#crontab -e`

Un fichier temporaire est créé. En quittant l'éditeur, le fichier crontab est enregistré sous `/var/spool/cron/crontabs/<nomutilisateur>` et devient actif.

Chaque utilisateur possède un fichier crontab

Pour obtenir la liste des tâches planifiées pour un utilisateur

➔ `#crontab -l`

Planifier une tâche: crontab

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.daily )
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.monthly )
#
```

m = minute h = hour dom= day of month mon= month dow = day of week

Tâche appartenant à root exécutée tous les jours à 6h25: teste que /usr/sbin/anacron existe OU va à la racine ET exécute tous les fichiers contenus dans /etc/cron.daily

Sécurité sous Linux – Type d'utilisateurs

Trois types d'utilisateurs sous Linux:

u : utilisateur propriétaire

g : groupe

o : tous les autres

Chaque utilisateur (u) DOIT appartenir à au moins un groupe (son groupe primaire)

Sécurité sous Linux – Les droits

Trois droits basiques sous Linux

r : Lecture → 4

w : Ecriture → 2

x : Exécution → 1

- sur un fichier : droit d'exécuter les commandes contenues dans le fichier
- sur un répertoire : droit de traverser le répertoire (sans lire, ni écrire)
→ nécessaire pour gérer les droits d'accès à des sous-répertoires

Syntaxe directe (réécriture)

```
#chmod 644 /home/francois/test
```

Syntaxe incrémentale

```
#chmod a+x /home/francois/test
```

```
#chmod u-x /home/francois/test
```

Sécurité sous Linux – Les droits

Correspondance : Chiffres (bit en base 8 - écriture octale des droits) ➔ Lettres

Droit en chiffre	Droit en lettres
1	x
2	w
3	wx
4	r
5	rx
6	rw
7	rwX

Sécurité sous Linux – Les droits

```
Terminal (au nom du superutilisateur)
Fichier Édition Affichage Terminal Aide
root@taranis:/home/francois# ls -l
total 132
drwxr-xr-x 2 francois francois 4096 23 oct. 16:24 Bureau
-rw-r--r-- 1 francois francois 52 24 sept. 17:48 cat
-rw-r--r-- 1 francois francois 268 18 juil. 16:55 commande_ifconfig
drwxr-xr-x 2 francois francois 4096 17 juil. 16:55 Documents
drwx----- 2 francois francois 4096 24 oct. 09:34 Downloads
-rw-r--r-- 1 francois francois 16 24 sept. 18:18 entree.txt
drwxr-xr-x 2 francois francois 4096 23 oct. 17:50 fwbuilder configuration
drwxr-xr-x 2 francois francois 4096 17 juil. 16:55 Images
-rw-r--r-- 1 francois francois 48832 17 juil. 17:13 iptables-persistent.pdf
drwxr-xr-x 2 francois francois 4096 17 juil. 16:55 Modèles
-rw-r--r-- 1 francois francois 52 24 sept. 17:48 more
drwxrwxr-x 2 francois francois 4096 17 juil. 16:55 Musique
drwxr-xr-x 2 francois francois 4096 17 juil. 16:55 Public
-rw-r--r-- 1 francois francois 14696 25 sept. 15:07 SELinux_position.jpg
-rw-r--r-- 1 francois francois 2160 24 sept. 18:24 sortie.txt
drwxr-xr-x 3 francois francois 4096 24 sept. 17:41 Téléchargements
drwxrwxrwx 1 root root 8192 24 oct. 16:36 Temp
drwxr-xr-x 2 francois francois 4096 17 juil. 16:55 Vidéos
root@taranis:/home/francois#
```

Sécurité sous Linux – Les droits

setuid: Utilisable sur les fichiers uniquement. Quand un fichier est exécutable par son propriétaire, il peut de plus être setuid. Cela signifie que lorsqu'il est exécuté, il l'est avec les droits de son propriétaire et non avec ceux de l'utilisateur qui le lance

Par exemple, le programme passwd, qui permet à un utilisateur de modifier son mot de passe, est setuid root (c'est à dire qu'il est setuid et qu'il appartient à l'utilisateur root): il doit pouvoir écrire dans le fichier /etc/passwd (ou /etc/shadow), dans lequel seul root peut écrire.

setgid: Utilisable sur les fichiers exécutables et les répertoires. Un exécutable setgid s'exécute avec les droits du groupe auquel il appartient. Quand un répertoire est setgid, tous les fichiers créés dans ce répertoire appartiennent au même groupe que le répertoire. C'est utilisé par exemple quand plusieurs personnes travaillent sur un projet commun: ils ont alors un groupe dédié à ce projet et un répertoire setgid appartenant à ce groupe. Ils créent leurs fichiers dans ce répertoire avec les permissions 2664: tout le groupe peut alors écrire n'importe quel fichier vu que tous les fichiers appartiennent au groupe.

sticky bit: (plutôt pour les répertoires) Alors qu'un exécutable peut être déclaré setuid et setgid par son propriétaire, seul l'administrateur système peut positionner le sticky bit. Un utilisateur qui a le droit d'écrire dans un répertoire peut effacer n'importe quel fichier de ce répertoire. Ça peut être très gênant par exemple pour le répertoire /tmp, dans lequel tout le monde a généralement le droit d'écrire. Pour y remédier, on positionne le sticky bit: ainsi un utilisateur ne peut effacer que les fichiers qui lui appartiennent.

Quand on écrit les permissions en octal, setuid, setgid et sticky bit sont représentés par une nouvelle série de 3 bits qui se place avant les 3 autres séries.

Sécurité sous Linux – Les droits

Règles pour les droits particuliers

Selon la position du s:

- s = setuid (s sur u) → vaut 4
- s = setgid (s sur g) → vaut 2
- t = sticky bit (toujours sur o) → vaut 1

- Exemples :
- rwsr-sr-x (rwxr-xr-x, setuid, setgid) → 6775
- drwxrwxrwt (rwxrwxrwx, sticky bit) → 1777
le t au lieu du x pour les autres utilisateurs (o) indique que le répertoire ne peut être supprimé que par le propriétaire
- 4755 → rwsr-xr-x → avec un guid
- 2755 → rwxr-sr-x → avec un sgid
- 6755 → rwxr-xr-x → avec un suid et un guid
- 1755 → rwxr-xr-t → avec un sticky bit

Sécurité sous Linux – Sécurité avancée

Sécurité par défaut:

Fichier → propriétaire/groupe/autre + droits

Action d'un processus sur un fichier :

Le noyau Linux vérifie que le processus a le droit

→ Chaque utilisateur est protégé des autres

Problème

Processus fonctionnant sous root et qui est détourné

→ La sécurité classique devient inopérante

Sécurité sous Linux – Sécurité avancée

Security-Enhanced **Linux** ou **App**lication **Armor** (Ubuntu, Suze)

Modèle de sécurité ajouté au système standard de Linux

Permet de configurer les accès de chaque processus afin de les restreindre au strict nécessaire → Limitation des dégâts en cas de compromission

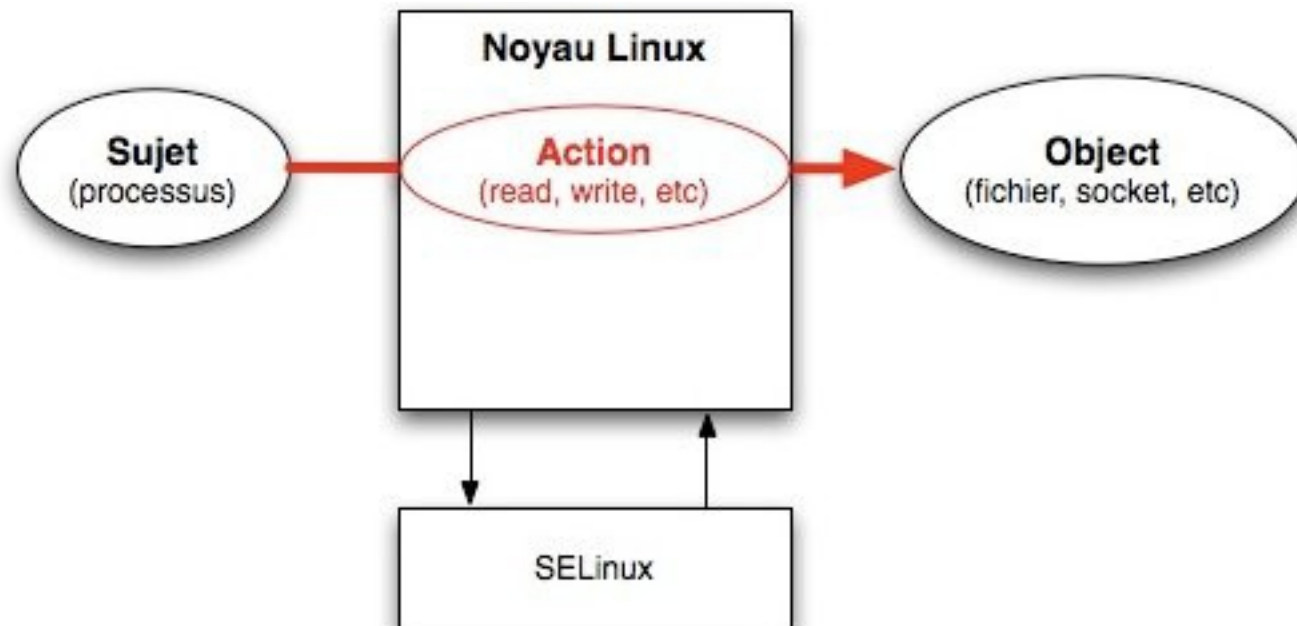
SELinux n'intervient pas si les droits classiques interdisent l'action

Sécurité sous Linux - SELinux

Appel système par un processus



Vérification par le noyau à travers SELinux (qui est intégré au noyau)



Sécurité sous Linux - SELinux

Quand SELinux est activé :

Chaque processus, chaque fichier, chaque socket, ... est associé à 3 informations:

Identité	-->	_u
Rôle	-->	_r
Type	-->	_t

Les droits accordés par SELinux sont liés aux types

Sécurité sous Linux - SELinux

SELinux activé: aucune action autorisée par défaut



Nécessité d'ajouter des règles (allow domain, type, permission)

Ex.:

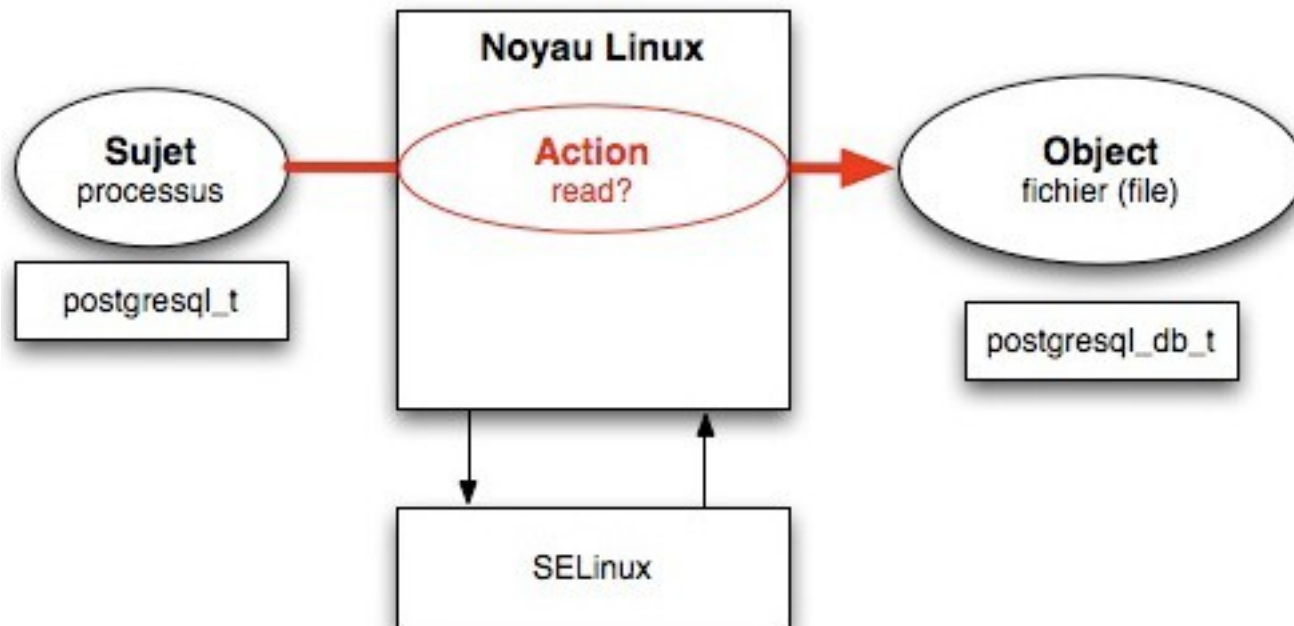
`allow postgresql_t postgresql_db_t : file create_file_perms`

`autorisation type du processus type de ressources : opération autorisée`

(Permet au processus PostgreSQL - SGBD - de lire les fichiers des bases de données PostgreSQL)

Sécurité sous Linux - SELinux

allow postgresql_t postgresql_db_t : file create_file_perms



allow postgresql_t postgresql_db_t:file create_file_perms;

Sécurité sous Linux - SELinux

```
allow firefox_t user_home_t : file { read write };
```

Cette règle autorise le navigateur firefox à lire et écrire dans les fichiers contenus dans le répertoire home de l'utilisateur courant et uniquement là

Remarque 1: les règles sont pré-écrites car apportées par les packages de règles installés (#apt-get install selinux-basics selinux-policy-default)

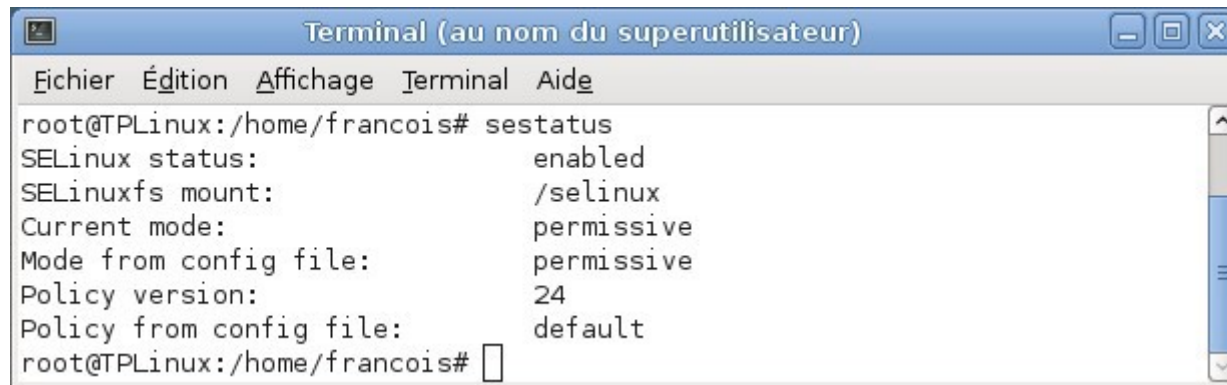
Remarque 2: SELinux n'est pas un pare-feu

Sécurité sous Linux - SELinux

Le pare-feu filtre les flux de données échangés entre une machine et le reste du réseau

SELinux filtre l'accès aux programmes/processus sur la station

#sestatus pour afficher le statut de SELinux

A terminal window titled "Terminal (au nom du superutilisateur)" showing the output of the 'sestatus' command. The window has a menu bar with "Fichier", "Édition", "Affichage", "Terminal", and "Aide". The terminal text shows SELinux is enabled, with the SELinuxfs mounted at /selinux, and the current mode is permissive. The policy version is 24, and the policy from the config file is default. The prompt is root@TPLinux:/home/francois#.

```

root@TPLinux:/home/francois# sestatus
SELinux status:                enabled
SELinuxfs mount:                /selinux
Current mode:                   permissive
Mode from config file:          permissive
Policy version:                 24
Policy from config file:        default
root@TPLinux:/home/francois#

```

Permissive: SELinux est installé mais ne protège pas

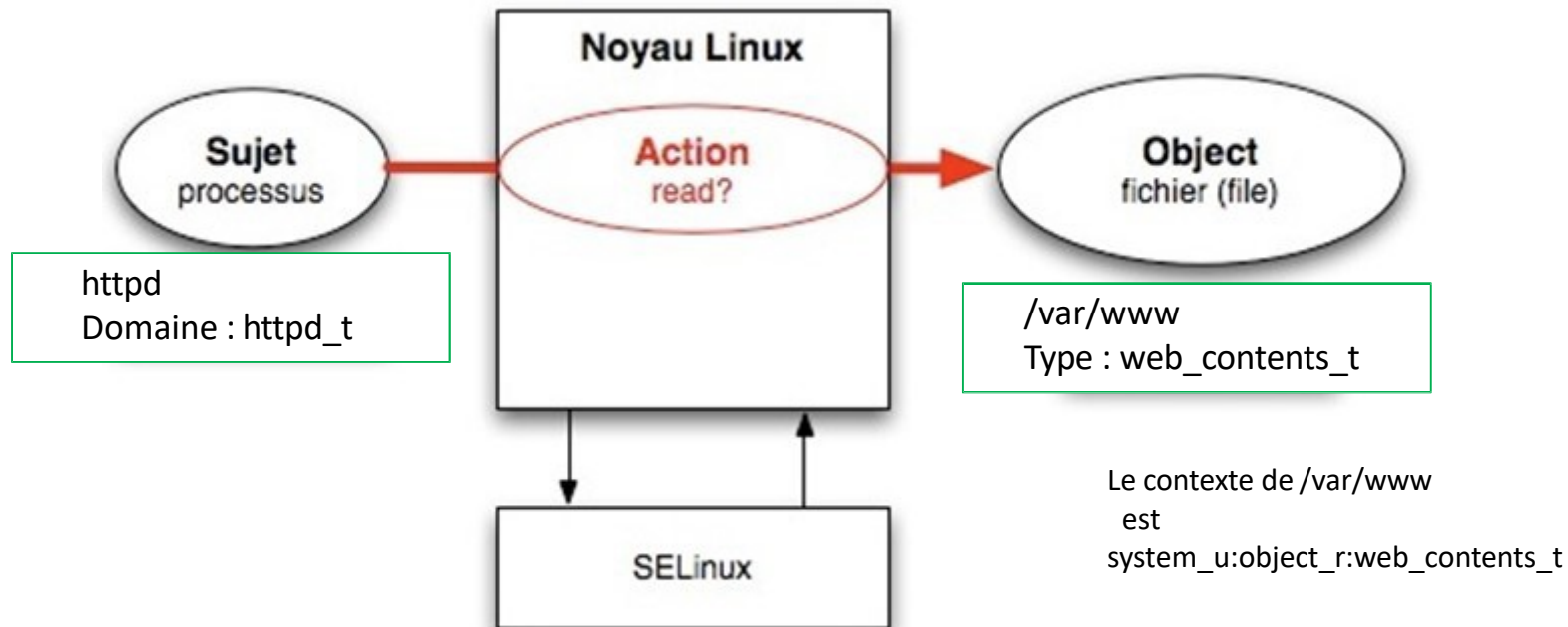
Enforcing: SELinux est installé et les règles s'appliquent

Sécurité sous Linux - SELinux

Exemples de l'utilité de SELinux :

- ❑ Un pirate rentre sur une machine à distance et essaie de lancer un shell
Le processus appelant le shell ("/bin/bash"...) devra être autorisé à lancer un shell par SELinux. Typiquement, on va associer un type shell_exec_t aux programmes de type shell et n'autoriser leur exécution qu'aux processus (grâce à leur type) qui en ont le besoin comme les programmes de login par exemple
- ❑ Un service Apache qui tourne en root sur un serveur SELinux se fait pirater
Le Security Server de SELinux, utilisant les politiques de sécurité qui ont été chargées dans le noyau, interdira au processus Apache agressé d'agir autrement que ce qu'on lui a imposé

Sécurité sous Linux - SELinux



Règle spécifique Apache (package) : **allow** httpd_t web_contents_t file:{ read };

Le domaine Apache ne peut pas accéder à d'autres répertoires (même si root possède le démon)

NB: Domaine = identifiant pour un processus / Type = identifiant pour une ressource

Sécurité sous Linux - SELinux

Par défaut, seul /var/www a le contexte web_contents_t

Problème :

Si certains répertoires de sites sont en dehors de /var/www

→ Apache ne peut les lire

Solution

Changer le contexte du fichier ou du répertoire

Les commandes

chcon

semanage

Sécurité sous Linux – **Application Armor**

Apparmor : système Mandatory Access Control (comme SELinux)

Sert à confiner l'accès des programmes à des ressources établies au préalable

Basé sur le chemin (pas besoin de label comme pour SELinux)



Apparmor connaît **/usr/bin/firefox** mais pas **firefox**

Ex. d'Apache: plusieurs règles selon le répertoire auquel Apache accède

Règles de sécurité = profils

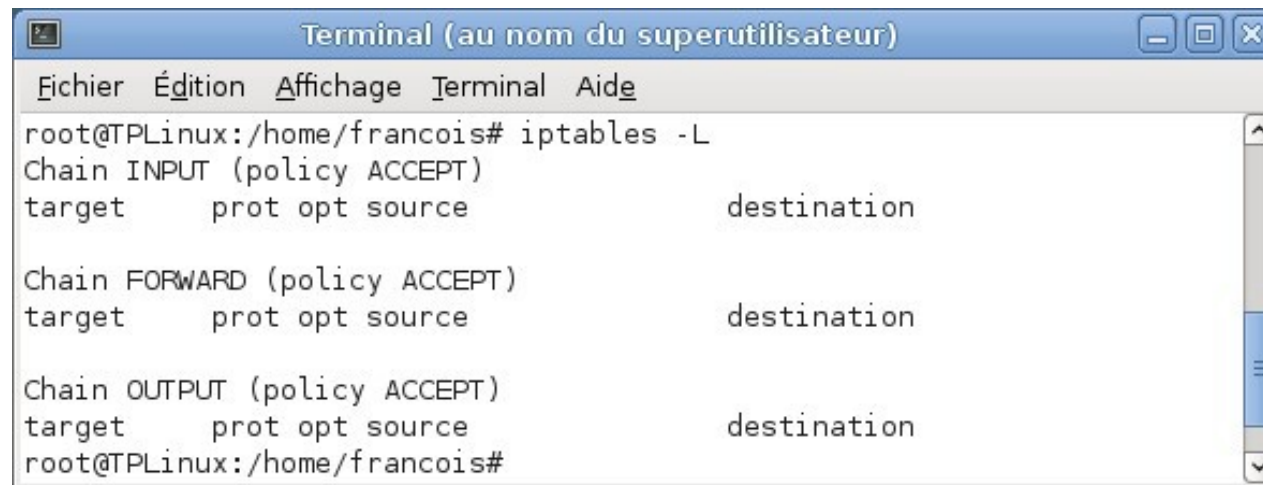
Doit être démarré avant les programmes à sécuriser (i.e. au démarrage de Linux)

Plus simple d'utilisation mais moins complet que SELinux

Pare-feu sous Linux : exemple d'IPTables

Est normalement installé par défaut

Pare-feu permissif par défaut

A terminal window titled "Terminal (au nom du superutilisateur)" with a menu bar containing "Fichier", "Édition", "Affichage", "Terminal", and "Aide". The terminal shows the command "iptables -L" being executed. The output lists three chains: INPUT, FORWARD, and OUTPUT, all with a policy of ACCEPT. Each chain has a table showing target, protocol, options, source, and destination. The destination column is empty for all chains.

```
root@TPLinux:/home/francois# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@TPLinux:/home/francois#
```

#iptables -L pour lister toutes les règles

Tout est autorisé par défaut en entrée et en sortie !

Pare-feu sous Linux : exemple d'IPTables

IPTables fait appel à 3 tables : MANGLE, NAT et FILTER

MANGLE ➔ Gestion de la QoS (par ex. limitation bande passante pour un protocole)

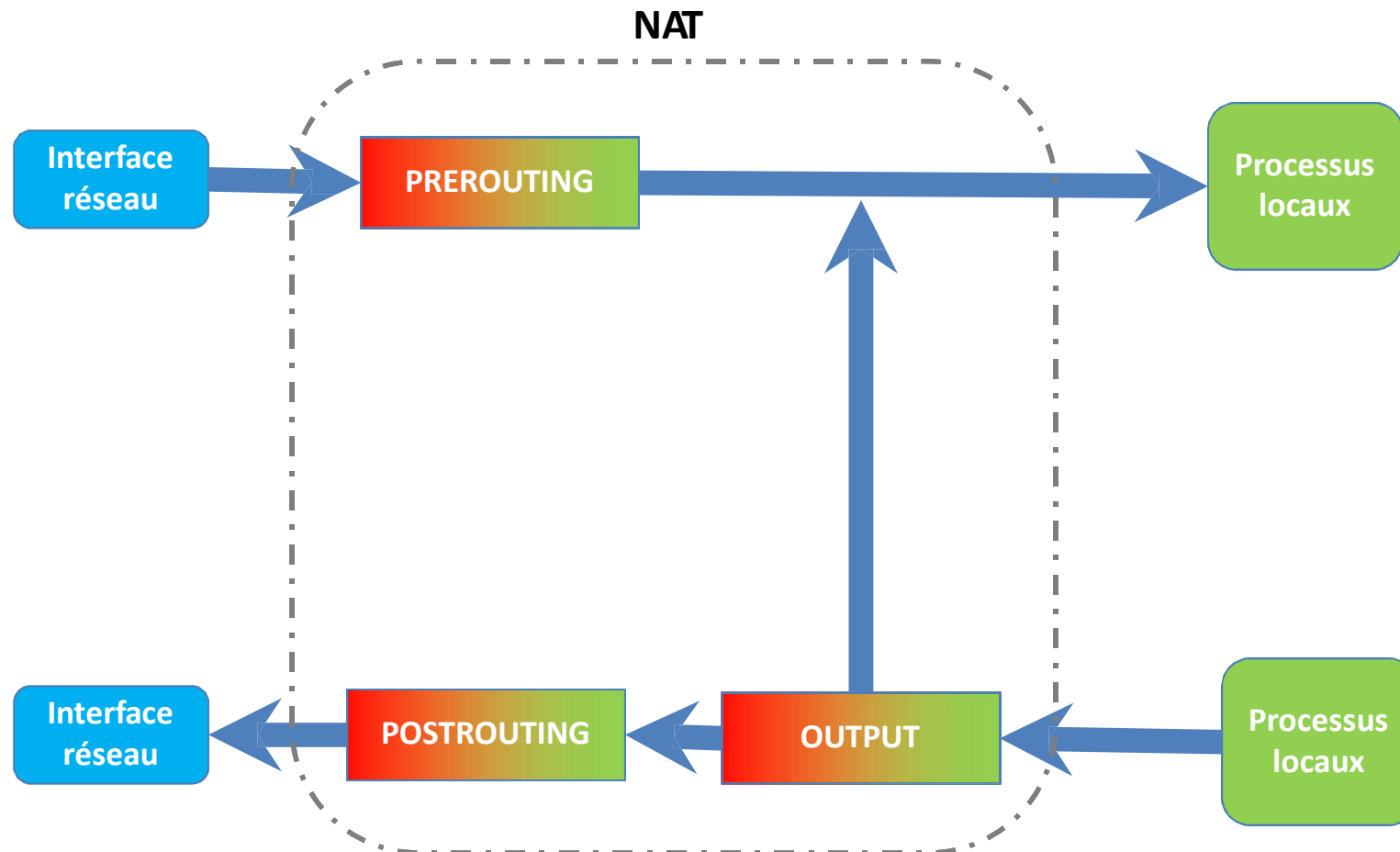
NAT ➔ Dispose de trois chaînes intégrées servant à construire les règles (de routage)

PREROUTING : L'adresse de destination du paquet doit être changée (NAT)

POSTROUTING : L'adresse source du paquet doit être changée (NAT)

OUTPUT : Pas de translation d'adresse

Pare-feu sous Linux : exemple d'IPTables



NB: On suppose ici que la machine qui héberge IPTables héberge également un processus ouvert à l'extérieur (Apache, par exemple)

Pare-feu sous Linux : exemple d'IPTables

FILTER → Fait appel à trois chaînes (fonction pare-feu la plus connue)

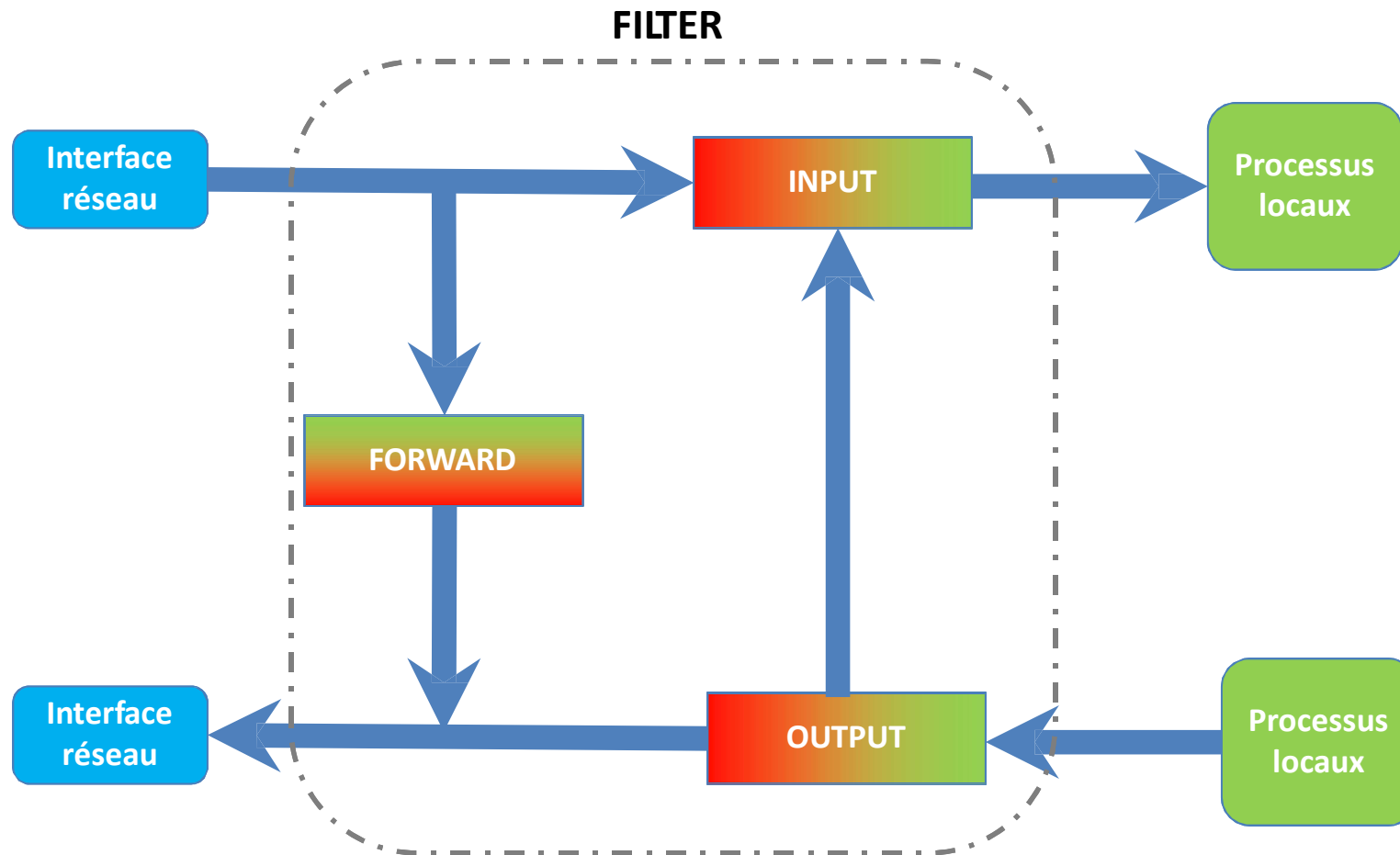
FORWARD : permet d'analyser et d'autoriser les trames à passer d'une interface à une autre, seulement dans le cadre d'une interface réseau servant de passerelle.

INPUT : filtrage des paquets entrant dans le pare-feu

OUTPUT : filtrage des paquets sortant du pare-feu

Remarque: une passerelle (*gateway*) est le nom générique d'un dispositif permettant de relier deux réseaux informatiques de types différents, par exemple un réseau local et le réseau Internet

Pare-feu sous Linux : exemple d'IPTables



Pare-feu sous Linux : exemple d'IPTables

Quatre actions (cibles) possibles avec IPTables:

ACCEPT : Les paquets sont acceptés et poursuivent leur trajet

DROP : Les paquets sont ignorés systématiquement (Aucune autre règle appliquée)

RETURN: Stoppe un paquet traversant la chaîne dans laquelle la règle est placée

QUEUE : Met en attente pour un traitement par une application de l'espace-utilisateur

Pare-feu sous Linux : exemple d'IPTables

Construction des règles:

iptables -A <chaine> -s <source> -p <protocole> -d <destination> -j <cible>

#iptables -A : Ajout d'une règle

#iptables -D : Suppression d'une règle

#iptables -P : Politique par défaut

#iptables -L : Liste de toutes les règles

-s : source qui peut être une adresse IP ou un réseau (192.168.0.1, 192.168.0.0/24, 192.168.0.0/255.255.255.0, 0/0...)

-p : protocole utilisé. La plupart du temps ce sera TCP, UDP, ICMP ou ALL. Un numéro de protocole peut également être spécifié (TCP=6, UDP=17,... Cf fichier /etc/protocols) ou une liste de protocoles séparés par des virgules

-d : destination qui peut être une adresse IP ou un réseau (192.168.0.1, 192.168.0.0/24, 192.168.0.0/255.255.255.0, 0/0...)

-j : cible (ACCEPT, DROP,...)

Pare-feu sous Linux : exemple d'IPTables

-i : interface réseau d'entrée, ne fonctionne qu'avec les chaînes INPUT et FORWARD (et aussi PREROUTING). Le caractère "+" peut être utilisé pour spécifier plusieurs interfaces du même type (eth+ signifie toutes les interfaces ethernet)

-o : interface réseau de sortie, ne fonctionne qu'avec les chaînes OUTPUT et FORWARD (et aussi POSTROUTING). Le caractère "+" peut être utilisé pour spécifier plusieurs interfaces du même type (eth+ signifie toutes les interfaces ethernet)

Pare-feu sous Linux : exemple d'IPTables

Fichier /etc/protocols

```
# Internet (IP) protocols
#
# Updated from http://www.iana.org/assignments/protocol-numbers and other
# sources.
# New protocols will be added on request if they have been officially
# assigned by IANA and are not historical.
# If you need a huge list of used numbers please install the nmap package.

ip 0 IP # internet protocol, pseudo protocol number
#hopopt 0 HOPOPT # IPv6 Hop-by-Hop Option [RFC1883]
icmp 1 ICMP # internet control message protocol
igmp 2 IGMP # Internet Group Management
ggp 3 GGP # gateway-gateway protocol
ipencap 4 IP-ENCAP # IP encapsulated in IP (officially ``IP'')
st 5 ST # ST datagram mode
tcp 6 TCP # transmission control protocol
egp 8 EGP # exterior gateway protocol
igp 9 IGP # any private interior gateway (Cisco)
pup 12 PUP # PARC universal packet protocol
udp 17 UDP # user datagram protocol
hmp 20 HMP # host monitoring protocol
xns-idp 22 XNS-IDP # Xerox NS IDP
rdp 27 RDP # "reliable datagram" protocol
iso-tp4 29 ISO-TP4 # ISO Transport Protocol class 4 [RFC905]
dccp 33 DCCP # Datagram Congestion Control Prot. [RFC4340]
xtp 36 XTP # Xpress Transfer Protocol
ddp 37 DDP # Datagram Delivery Protocol
idpr-cmtp 38 IDPR-CMTP # IDPR Control Message Transport
ipv6 41 IPv6 # Internet Protocol, version 6
ipv6-route 43 IPv6-Route # Routing Header for IPv6
ipv6-frag 44 IPv6-Frag # Fragment Header for IPv6
idrp 45 IDRP # Inter-Domain Routing Protocol
rsvp 46 RSVP # Reservation Protocol
gre 47 GRE # General Routing Encapsulation
esp 50 IPSEC-ESP # Encap Security Payload [RFC2406]
ah 51 IPSEC-AH # Authentication Header [RFC2402]
skip 57 SKIP # SKIP
ipv6-icmp 58 IPv6-ICMP # ICMP for IPv6
ipv6-nonxt 59 IPv6-NoNxt # No Next Header for IPv6
ipv6-opts 60 IPv6-Opts # Destination Options for IPv6
rsvp 73 RSVP CPHB # Radio Shortest Path First (officially CPHB)
vmt 81 VMT # Versatile Message Transport
eigrp 88 EIGRP # Enhanced Interior Routing Protocol (Cisco)
ospf 89 OSPF # Open Shortest Path First (Cisco)
```

Pare-feu sous Linux : exemple d'IPTables

Exemple de règles:

```
#iptables -P INPUT DROP
```

```
#iptables -P OUTPUT DROP
```

➔ iptables bloque les paquets entrants et sortants

```
#iptables -P FORWARD DROP
```

➔ pas de routage

NB: Par défaut, la commande iptables crée des règles dans FILTER (sauf si une autre table est spécifiée)

Pare-feu sous Linux : exemple d'IPTables

#iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
accepte tous les paquets reçus dans le cadre de connexions déjà établies

#iptables -A OUTPUT -j ACCEPT
autorise tout le trafic sortant

#iptables -A INPUT -p tcp --dport 80 -j ACCEPT
#iptables -A INPUT -p tcp --dport 443 -j ACCEPT
autorise les demandes HTTP et HTTPS émises de n'importe où

#iptables -A INPUT -p icmp --icmp-type 8 -j ACCEPT
autorise les trames de ping (ICMP, type 8)

#iptables -A INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-level 7
journalise les refus d'IPTables (avec limitation à 5 entrées par mn max)

#iptables -A INPUT -j REJECT
#iptables -A FORWARD -j REJECT
règles par défaut interdisant tout ce qui n'est pas autorisé explicitement

Pare-feu sous Linux : exemple d'IPTables

Exemple de règles:

(#iptables-restore < /etc/mesregles)

*filter

autorise tout le trafic sortant

-A OUTPUT -j ACCEPT

Autorise les demandes HTTP et HTTPS (sur les ports classiques) émises de n'importe où

-A INPUT -p tcp --dport 80 -j ACCEPT

-A INPUT -p tcp --dport 443 -j ACCEPT

autorise les trames deping (ICMP, type 8)

-A INPUT -p icmp --icmp-type 8 -j ACCEPT

log les refus d'IPTables (avec limitation à 5 entrées par mn max)

-A INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-level 7

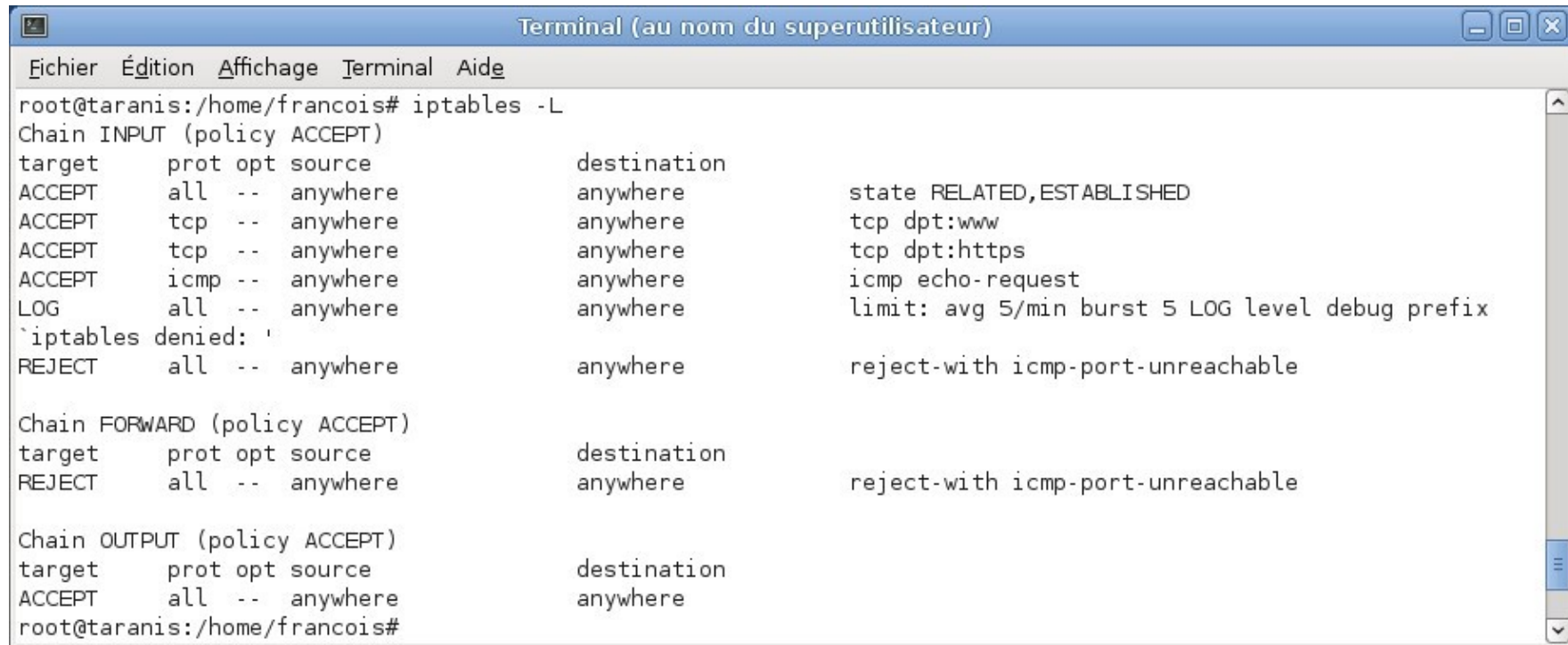
règles par défaut interdisant tout ce qui n'est pas autorisé explicitement

-A INPUT -j REJECT

-A FORWARD -j REJECT

COMMIT

Pare-feu sous Linux : exemple d'IPTables



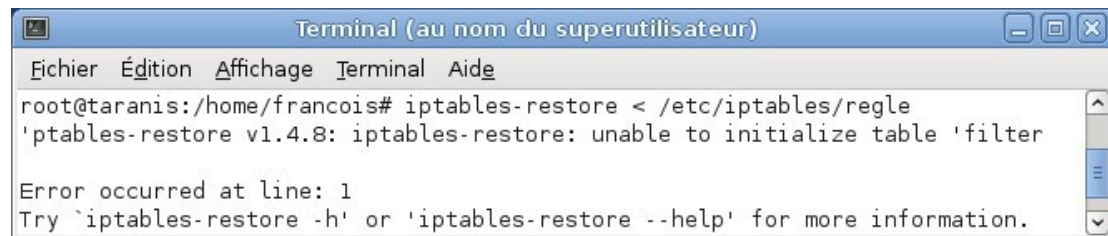
```
Terminal (au nom du superutilisateur)
Fichier Édition Affichage Terminal Aide
root@taranis:/home/francois# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination           state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:www
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:https
ACCEPT     icmp --  anywhere              anywhere              icmp echo-request
LOG         all  --  anywhere              anywhere              limit: avg 5/min burst 5 LOG level debug prefix
`iptables denied: '
REJECT     all  --  anywhere              anywhere              reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination           reject-with icmp-port-unreachable
REJECT     all  --  anywhere              anywhere              reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     all  --  anywhere              anywhere
root@taranis:/home/francois#
```

Attention aux caractères retour chariot avec les éditeurs - par ex. Notepad

➔ Erreur d'interprétation



```
Terminal (au nom du superutilisateur)
Fichier Édition Affichage Terminal Aide
root@taranis:/home/francois# iptables-restore < /etc/iptables/regle
'ptables-restore v1.4.8: iptables-restore: unable to initialize table 'filter

Error occurred at line: 1
Try `iptables-restore -h' or 'iptables-restore --help' for more information.
```

Pare-feu sous Linux : exemple d'IPTables

Le cas de la cible RETURN:

`iptables -P INPUT DROP` 1°: indique une cible par défaut (DROP ici) pour la chaîne INPUT:
1 paquet non traité par une règle explicite suivra cette stratégie

(Remarque : « `iptables -A INPUT ...` » place une règle à la fin de toutes les règles de la chaîne INPUT)

`iptables -A INPUT -p tcp --dport 80 -j AUTRECHAINE` 2°: Tout paquet à destination du port 80 est
envoyé dans la chaîne AUTRECHAINE

`iptables -A INPUT -p tcp --dport 80 -j AUTRECHAINE2` 5°: Tout paquet à destination du port 80 est
envoyé dans la chaîne AUTRECHAINE2

`iptables -A AUTRECHAINE -p tcp --dport 80 --s 192.168.0.0/16 -j ACCEPT` 3°: Si la source de ce paquet à destination du
port 80 est 192.168.0.0/16 ou 10.10.0.0/16,
`iptables -A AUTRECHAINE -p tcp --dport 80 --s 10.10.0.0/16 -j ACCEPT` alors le paquet est autorisé à passer le PF

`iptables -A AUTRECHAINE -p tcp --dport 80 -j RETURN` 4°: Dans le cas contraire, le paquet est renvoyé dans la
chaîne INPUT et on passe à la règle suivante

`iptables -A AUTRECHAINE2 -p tcp --dport 80 -m state --state ESTABLISHED,RELATED -j ACCEPT`
6°: Si le paquet intervient dans une connexion déjà établie sur le port 80, il est accepté

`iptables -A AUTRECHAINE2 -p tcp --dport 80 -j RETURN` 7°: Si le paquet intervient dans une connexion sur le port 80 mais
non établie au préalable il est rejeté

Pare-feu sous Linux : exemple d'IPTables

Sauvegarde des règles en cours

```
#iptables-save > /etc/iptables/regles_def
```

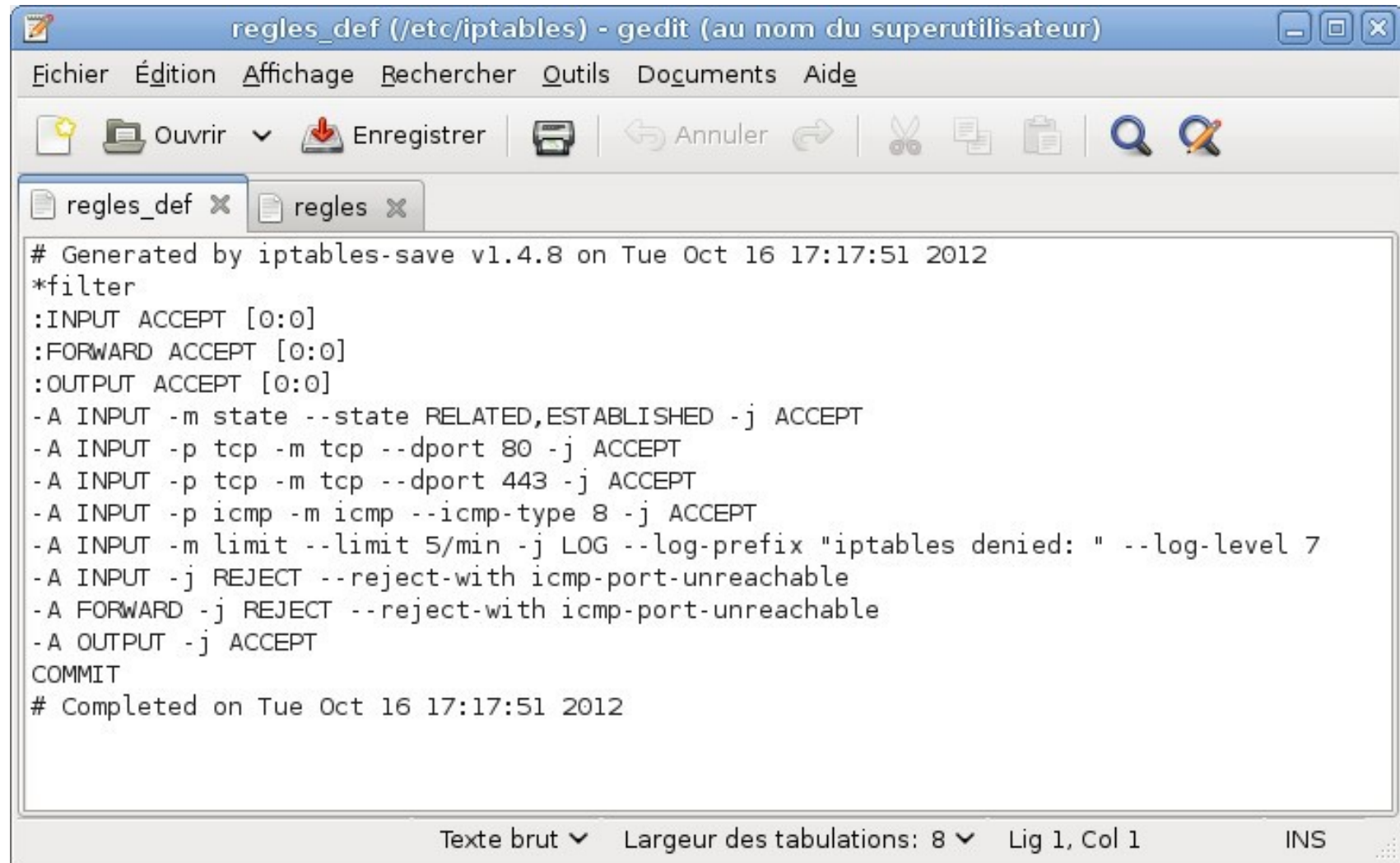
Remarque: les règles ne s'appliquent plus après un redémarrage

➔ Si c'est pratique en phase de test (car ça évite de perdre définitivement le contrôle de sa machine), c'est à éviter en production

Comment charger une série de règles manuellement

```
#iptables-restore < /etc/iptables/regles_def
```

Pare-feu sous Linux : exemple d'IPTables



The screenshot shows a gedit window titled "regles_def (/etc/iptables) - gedit (au nom du superutilisateur)". The window contains a text file named "regles_def" with the following content:

```
# Generated by iptables-save v1.4.8 on Tue Oct 16 17:17:51 2012
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -m limit --limit 5/min -j LOG --log-prefix "iptables denied: " --log-level 7
-A INPUT -j REJECT --reject-with icmp-port-unreachable
-A FORWARD -j REJECT --reject-with icmp-port-unreachable
-A OUTPUT -j ACCEPT
COMMIT
# Completed on Tue Oct 16 17:17:51 2012
```

The window's status bar at the bottom indicates "Texte brut", "Largeur des tabulations: 8", "Lig 1, Col 1", and "INS".

Pare-feu sous Linux : exemple d'IPTables

Création d'un script qui s'exécutera au démarrage (penser à changer les droits):

```
#!/bin/bash
```

```
/sbin/iptables-restore < /etc/iptables/regles_def
```

(#chmod +x /etc/network/if-pre-up.d/scriptiptables)

Sous debian:

/etc/network/if-pre-up.d/  accueille les scripts devant s'exécuter
AVANT

le démarrage des interfaces réseaux

Rappel: PF = ensemble de règles qui concernent les interfaces réseaux

Pare-feu sous Linux : exemple d'IPTables

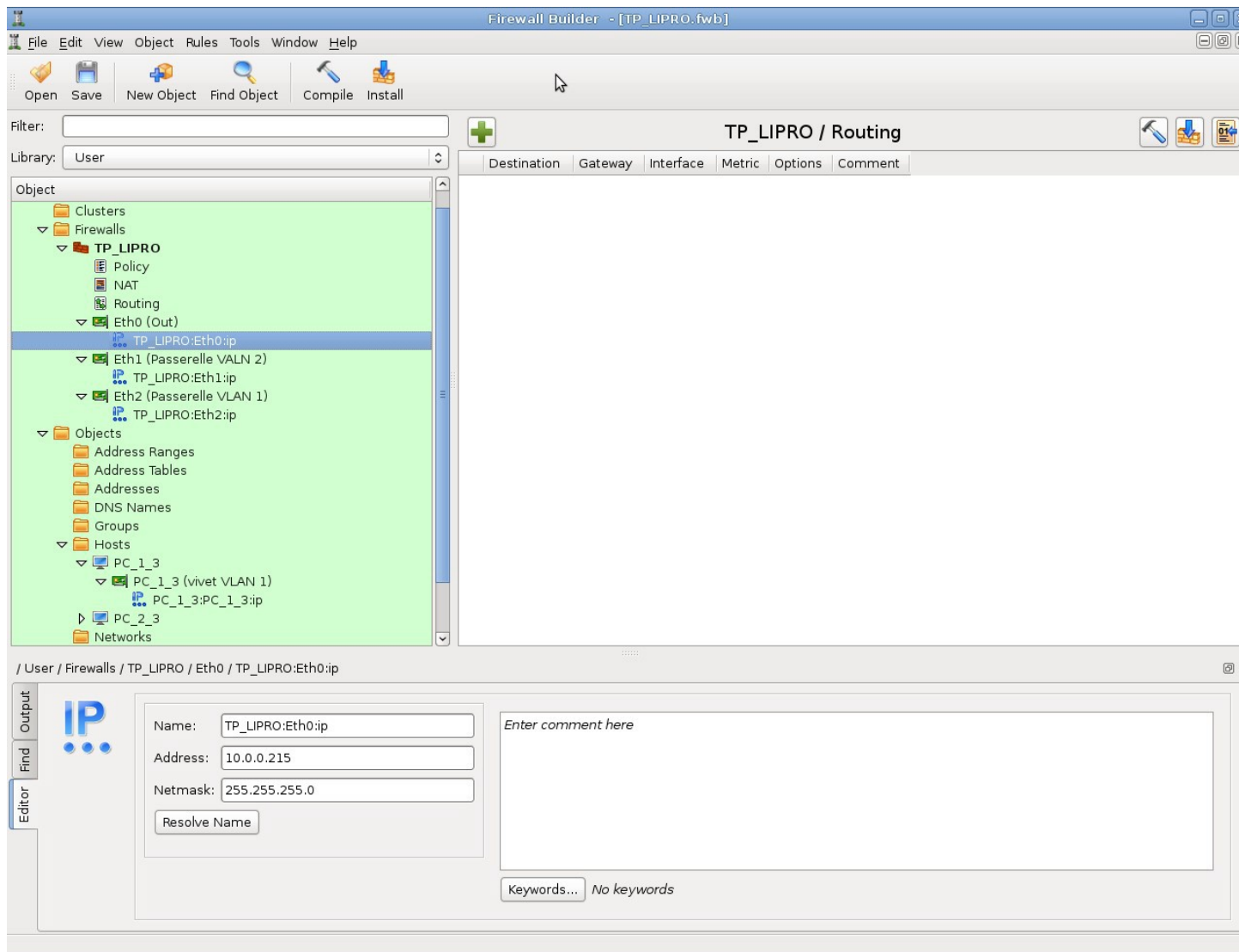
Autre méthode:

1°: installation du paquet iptables-persistent

2°: écriture des règles dans /etc/iptables/rules

3°: démarrage du service iptables-persistent

Outil graphique de paramétrage de PF : FWBuilder

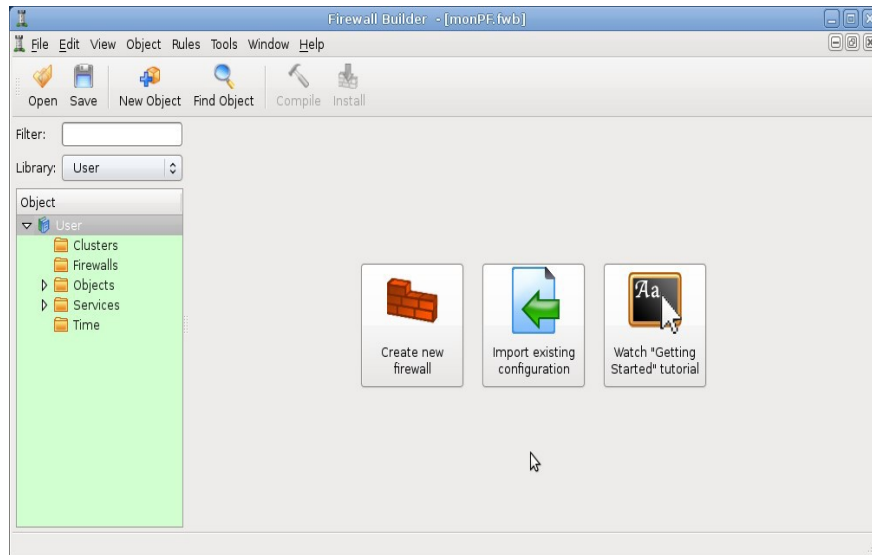


Outil graphique de paramétrage de PF : FWBuilder

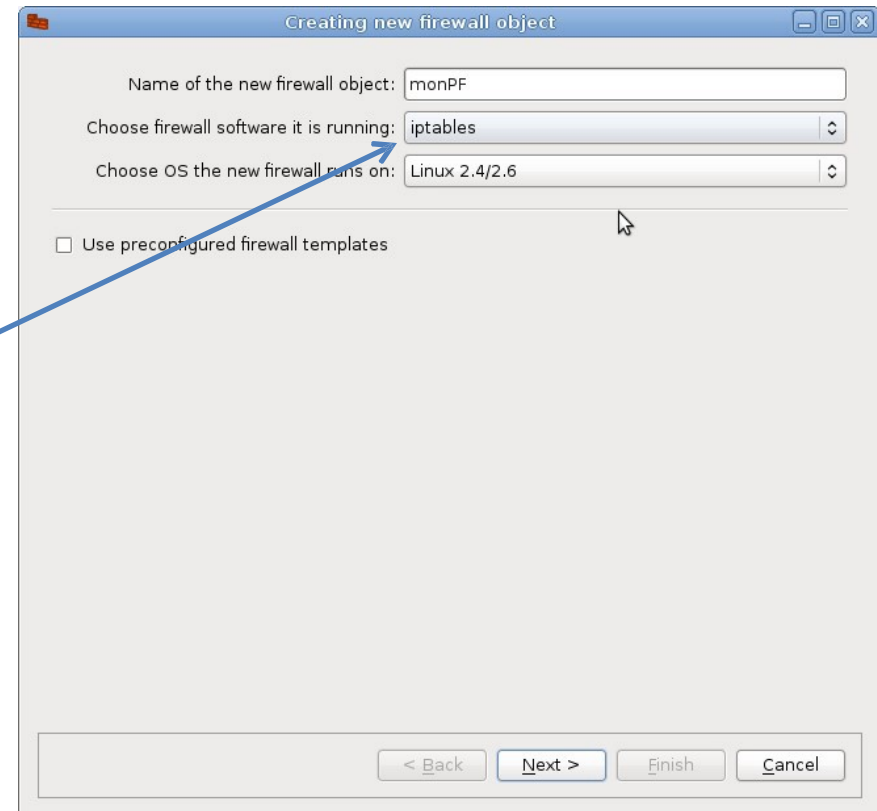
FireWall Builder :

- Environnement graphique
- Basé sur la manipulation d'objets par défaut ou créés par l'utilisateur
- Objets sont stockés dans 2 librairies : Standard (en lecture seule) et User
- Permet de gérer un parc de pare-feux distants

Outil graphique de paramétrage de PF : FWBuilder



On indique le parefeu employé

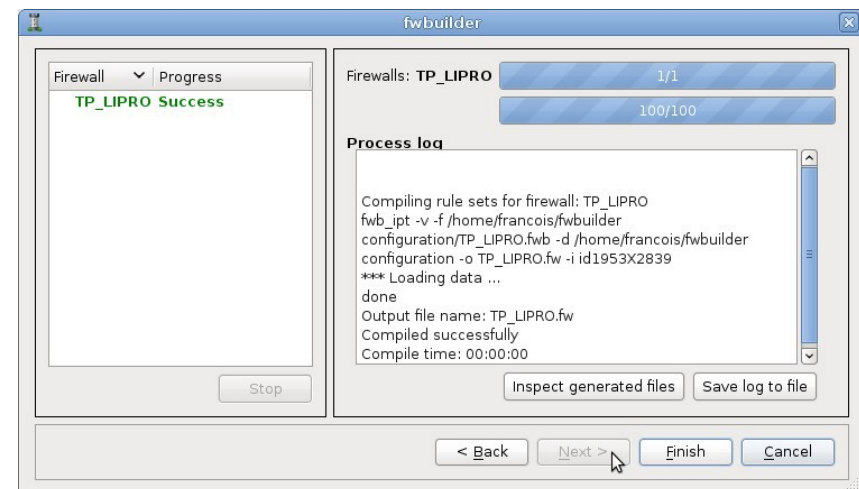
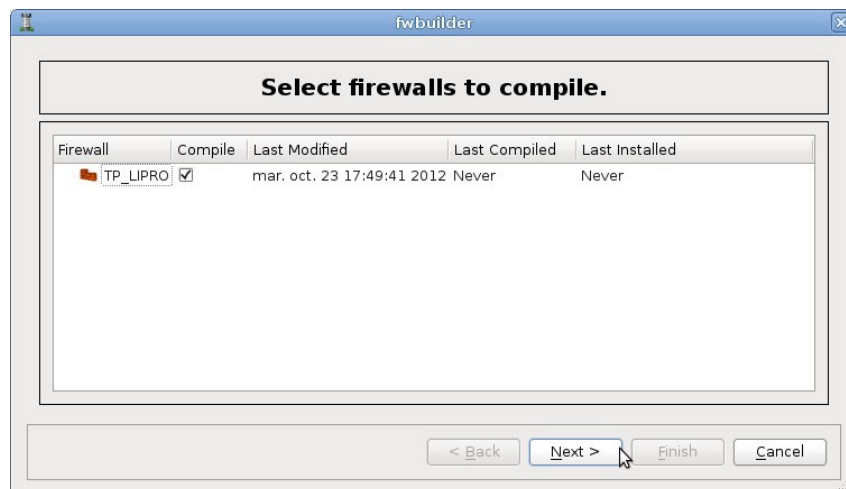


Outil graphique de paramétrage de PF : FWBuilder

Création d'objets, de règles via FWBuilder

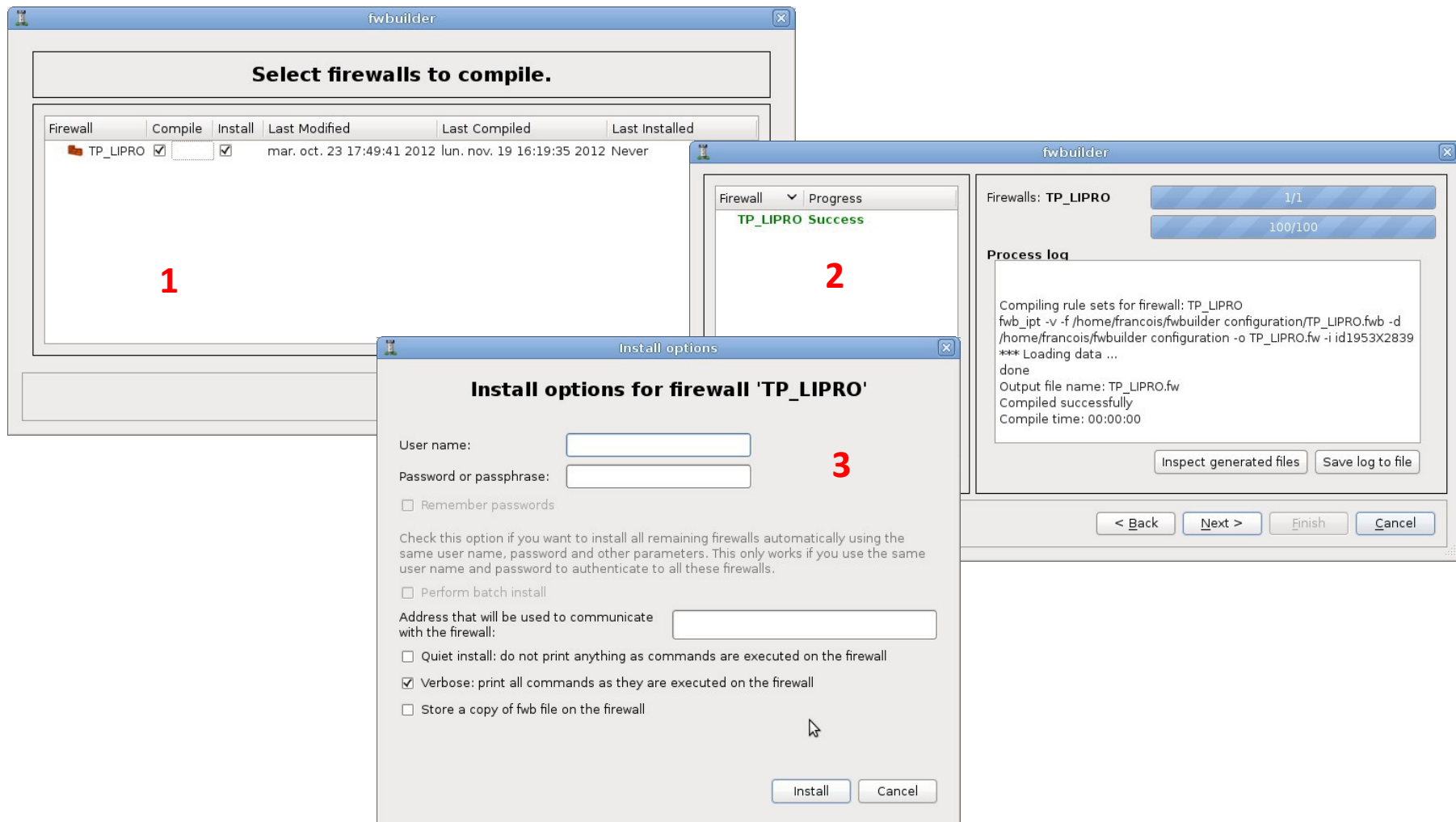
Sauvegarde de la configuration FWBuilder (maconf.fwb) - - - > fichier XML

Compilation de la configuration



Outil graphique de paramétrage de PF : FWBuilder

Application de la configuration au parefeu



Attributions de ressources à un utilisateur ou un groupe

Une **fork bomb** (parfois appelée **logic bomb**), est une attaque par déni de service qui peut aller jusqu'à rendre votre ordinateur complètement inutilisable. Elle agit en se dupliquant infiniment jusqu'à saturer la table des processus

Exemple de FTP

Processus père à l'écoute des clients

 Demande de connexion d'un client

 Le père crée un processus fils et lui donne le socket de connexion

 Le père retourne à l'écoute

 Demande de connexion d'un client

 ... et ainsi de suite jusqu'à écrasement

Attributions de ressources à un utilisateur ou un groupe

Quelle est la solution pour éviter les fork bombs ?

- Limiter la quantité de ressources disponibles qu'un groupe ou un utilisateur peut s'octroyer

Comment ?

- Dans le fichier `/etc/security/limits.conf`

```

# /etc/security/limits.conf
#
#Each line describes a limit for a user in the form:
#<domain>    <type> <item> <value>
#Where:<domain> can be:
#    - an user name
#    - a group name, with @group syntax
#    - the wildcard *, for default entry
#
#<type> can have the two values:
#    - "soft" for enforcing the soft limits
#    - "hard" for enforcing hard limits
#
#<item> can be one of the following:
#    - core - limits the core file size (KB)
#    - data - max data size (KB)
#    - fsize - maximum filesize (KB)
#    - memlock - max locked-in-memory address space (KB)
#    - nofile - max number of open files
#    - rss - max resident set size (KB)
#    - stack - max stack size (KB)
#    - cpu - max CPU time (MIN)
#    - nproc - max number of processes
#    - as - address space limit (KB)
#    - maxlogins - max number of logins for this user
#    - maxsyslogins - max number of logins on the system
#    - priority - the priority to run user process with
#    - locks - max number of file locks the user can hold
#    - sigpending - max number of pending signals
#    - msgqueue - max memory used by POSIX message queues (bytes)
#    - nice - max nice priority allowed to raise to values: [-20, 19]
#    - rtprio - max realtime priority
#    - chroot - change root to directory (Debian-specific)
#####
#*                soft  core    0
#root             hard  core    100000
#*                hard  rss     10000
#@student         hard  nproc   20
#@faculty         soft  nproc   20
#@faculty         hard  nproc   50
#ftp              hard  nproc   0
#ftp              -     chroot   /ftp
#@student         -     maxlogins 4
# End of file

```