



Faculté des Sciences de Technologies

## *Rapport TD6 systeme1*

**Nom** : PIERRE

**Prénom** : Yann Lelay

**Niveau** : L3-Sciences Informatiques

*Description :*

- Reproduire des tâches du Td pour les maîtriser et ensuite passer des commandes sur l'installation de firewall et d'autre encore.

*1. Reproduire les tâches ci-dessus*

```
lelay@Legenie:~$ sudo apt update
Atteint :1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Atteint :2 http://do.archive.ubuntu.com/ubuntu jammy InRelease
Atteint :3 http://do.archive.ubuntu.com/ubuntu jammy-updates InRelease
Atteint :4 http://do.archive.ubuntu.com/ubuntu jammy-backports InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
9 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.
lelay@Legenie:~$ sudo apt install ufw
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
ufw est déjà la version la plus récente (0.36.1-4ubuntu0.1).
ufw passé en « installé manuellement ».
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libkeybinder-3.0-0 libxfce4ui-utils tango-icon-theme thunar
  thunar-volman xfce4-appfinder xfce4-panel xfce4-pulseaudio-plugin
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 9 non mis à jour
.
lelay@Legenie:~$ sudo ufw status verbose
État : inactif
lelay@Legenie:~$ sudo ufw enable
Le pare-feu est actif et lancé au démarrage du système
lelay@Legenie:~$
```

```

lelay@Legenie:~$ sudo ufw status verbose
État : inactif
lelay@Legenie:~$ sudo ufw enable
Le pare-feu est actif et lancé au démarrage du système
lelay@Legenie:~$ sudo ufw allow 80/tcp
La règle a été ajoutée
La règle a été ajoutée (v6)
lelay@Legenie:~$ sudo ufw allow 22/tcp
La règle a été ajoutée
La règle a été ajoutée (v6)
lelay@Legenie:~$ sudo ufw deny 23
La règle a été ajoutée
La règle a été ajoutée (v6)
lelay@Legenie:~$ sudo ufw status numbered
État : actif

      Vers                Action      De
      ----                -
[ 1] 80/tcp                ALLOW IN   Anywhere
[ 2] 22/tcp                ALLOW IN   Anywhere
[ 3] 23                    DENY IN    Anywhere
[ 4] 80/tcp (v6)           ALLOW IN   Anywhere (v6)
[ 5] 22/tcp (v6)           ALLOW IN   Anywhere (v6)
[ 6] 23 (v6)              DENY IN    Anywhere (v6)

lelay@Legenie:~$

```

```

lelay@Legenie:~$ sudo ufw delete allow 80/tcp
La règle a été supprimée
La règle a été supprimée (v6)
lelay@Legenie:~$ sudo ufw disable
Le pare-feu est arrêté et désactivé lors du démarrage du système
lelay@Legenie:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ufw-before-logging-input  all  --  anywhere               anywhere
ufw-discoverer-input      all  --  anywhere               anywhere
ufw-logthèque-input       all  --  anywhere               anywhere
ufw-after-logging-input   all  --  anywhere               anywhere
ufw-reject-input          all  --  anywhere               anywhere
ufw-track-input           all  --  anywhere               anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
ufw-before-logging-forward all  --  anywhere               anywhere
ufw-before-forward        all  --  anywhere               anywhere
ufw-after-forward         all  --  anywhere               anywhere
ufw-after-logging-forward  all  --  anywhere               anywhere
ufw-reject-forward        all  --  anywhere               anywhere
ufw-track-forward         all  --  anywhere               anywhere

Chain OUTPUT (policy ACCEPT)

```

```

lelay@Legenie:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
lelay@Legenie:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
lelay@Legenie:~$ sudo iptables -A INPUT -p tcp --dport 23 -j ACCEPT
lelay@Legenie:~$ sudo iptables -F
lelay@Legenie:~$

```

```
lelay@Legenie:~$ sudo iptables -A INPUT -p tcp --dport 22 -i eth0 -m --state --NEW -m recent --set
iptables v1.8.7 (nf_tables): Couldn't load match '--state':No such file or directory

Try `iptables -h' or 'iptables --help' for more information.
lelay@Legenie:~$ sudo iptables -A INPUT -p tcp --dport 22 -i eth0 -m --state --NEW -m recent --update --secondes 60 --hicount 3 -j REJECT
iptables v1.8.7 (nf_tables): Couldn't load match '--state':No such file or directory

Try `iptables -h' or 'iptables --help' for more information.
lelay@Legenie:~$ sudo iptables -p INPUT DROP
iptables v1.8.7 (nf_tables): unknown protocol "input" specified
Try `iptables -h' or 'iptables --help' for more information.
lelay@Legenie:~$ sudo iptables -A INPUT -p DROP tcp --dport 22 -j ACCEPT
T
iptables v1.8.7 (nf_tables): unknown protocol "drop" specified
Try `iptables -h' or 'iptables --help' for more information.
lelay@Legenie:~$ sudo iptables -A INPUT -p DROP tcp --dport 80 -j ACCEPT
T
iptables v1.8.7 (nf_tables): unknown protocol "drop" specified
Try `iptables -h' or 'iptables --help' for more information.
lelay@Legenie:~$
```

--

```
lelay@Legenie:~$ sudo setenforce 1
sudo: setenforce : commande introuvable
lelay@Legenie:~$ sudo setenforce 0
sudo: setenforce : commande introuvable
lelay@Legenie:~$ sudo vi /etc/selinux/config
lelay@Legenie:~$ sestatus
La commande « sestatus » n'a pas été trouvée, mais peut être installée
avec :
sudo apt install policycoreutils
lelay@Legenie:~$ getenforce
La commande « getenforce » n'a pas été trouvée, mais peut être installé
e avec :
sudo apt install selinux-utils
lelay@Legenie:~$ ls -Z /var/www/html
? index.html ? index.nginx-debian.html
lelay@Legenie:~$ sudo chcon -t httpd_sys_content_t /var/www/html/index.
html
chcon: impossible d'appliquer un contexte partiel au fichier '/var/www/
html/index.html' non étiqueté
lelay@Legenie:~$ sudo semanage fcontext -l
sudo: semanage : commande introuvable
lelay@Legenie:~$
::1          ip6-allnodes      ip6-mcastprefix
fe00::0      ip6-allrouters   lelay-VirtualBox
ff00::0      ip6-localhost     localhost
ff02::1      ip6-localnet
ff02::2      ip6-loopback
lelay@Legenie:~$ ss
```



2. Obtenir des privilèges d'administrateur:

*sudo su - et apt install firewalld*

```
root@Legenie:~# sudo su -
root@Legenie:~# apt install firewalld
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libkeybinder-3.0-0 libxfce4ui-utils tango-icon-theme thunar
  thunar-volman xfce4-appfinder xfce4-panel xfce4-pulseaudio-plugin
Veuillez utiliser « apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  ipset libipset13 python3-attr python3-cap-ng python3-firewall
  python3-jjsonschema python3-nftables python3-pyrsistent
Paquets suggérés :
  python-attr-doc python-jjsonschema-doc
Les NOUVEAUX paquets suivants seront installés :
  firewalld ipset libipset13 python3-attr python3-cap-ng
  python3-firewall python3-jjsonschema python3-nftables
  python3-pyrsistent
0 mis à jour, 9 nouvellement installés, 0 à enlever et 9 non mis à jour
.
Il est nécessaire de prendre 791 ko dans les archives.
Après cette opération, 5,022 ko d'espace disque supplémentaires seront
utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://do.archive.ubuntu.com/ubuntu jammy/main amd64 py
thon3-attr all 21.2.0-1 [44.0 kB]
Réception de :2 http://do.archive.ubuntu.com/ubuntu jammy/main amd64 py
thon3-pyrsistent amd64 0.18.1-1build1 [55.5 kB]
```

3. Définissez la zone par défaut actuelle en entrant:

*firewall-cmd --get-default-zone*

```
root@Legenie:~# firewall-cmd --get-default-zone
public
root@Legenie:~# █
```

4. Identifiez les zones disponibles en entrant:

*firewall-cmd --get-zones*

```
root@Legenie:~# firewall-cmd --get-default-zone
public
root@Legenie:~# █
```

5. Recherchez les services disponibles sur votre ordinateur en utilisant `firewall-cmd --get-services`

```
root@Legenie:~# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client
amqp amqps apcupsd audit bacula bacula-client bb bgp bitcoin bitcoin-
rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cf
engine cockpit collectd condor-collector ctdb dhcp dhcpv6 dhcpv6-client
distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync e
lasticsearch etcd-client etcd-server finger foreman foreman-proxy freei
pa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp g
alera ganglia-client ganglia-master git grafana gre high-availability h
ttp http3 https imap imaps ipp ipp-client ipsec irc ircs iscsi-target i
sns jellyfin jenkins kadmin kdeconnect kerberos kibana klogin kpasswd k
prop kshell kube-api kube-apiserver kube-control-plane kube-controller-
manager kube-scheduler kubelet-worker ldap ldaps libvirt libvirt-tls li
ghtning-network llmnr llmnr-tcp llmnr-udp managesieve matrix mdns memca
che minidlna mongodb mosh mountd mqtt mqtt-tls ms-wbt mssql murmur mysq
l nbd netbios-ns nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio
ovirt-storageconsole ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebap
is pop3 pop3s postgresql privoxy prometheus proxy-dhcp ptp pulseaudio p
uppetmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rs
h rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp
smtp smtp-submission smtps snmp snmptrap spideroak-lansync spotify-syn
c squid sssd ssh steam-streaming svdrp svn syncthing syncthing-gui syne
rgy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-socks transm
ission-client upnp-client vdsms vnc-server wbem-http wbem-https wiregua
rd ws-discovery ws-discovery-client ws-discovery-tcp ws-discovery-udp ws
man wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-ag
ent zabbix-server zerotier
root@Legenie:~#
```

6. Identifiez les services disponibles dans la zone actuelle:

`firewall-cmd --list-services`

```
root@Legenie:~# firewall-cmd --list-services
dhcpv6-client ssh
root@Legenie:~#
```



7. Comparez les résultats de sortie lorsque vous utilisez la commande `firewall-cmd --list-all` et `firewall-cmd --list-all --zone=public`

```
root@Legenie:~# firewall-cmd --list-services
dhcpv6-client ssh
root@Legenie:~# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@Legenie:~#
```

```
root@Legenie:~# firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@Legenie:~#
```

8. Ajoutez le serveur VNC à la configuration du pare-feu:  
`firewall-cmd --add-service=vnc-server`

```
lelay@Legenie:~$ firewall-cmd --add-service=vnc-server
success
lelay@Legenie:~$
```

*sudo apparmor\_status*

```
lelay@Legenie:~$ sudo apparmor_status
[sudo] Mot de passe de lelay :
apparmor module is loaded.
60 profiles are loaded.
56 profiles are in enforce mode.
/snap/snapd/21759/usr/lib/snapd/snap-confine
/snap/snapd/21759/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
/snap/snapd/23258/usr/lib/snapd/snap-confine
/snap/snapd/23258/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
/usr/bin/evince
/usr/bin/evince-previewer
/usr/bin/evince-previewer//sanitized_helper
/usr/bin/evince-thumbnailer
/usr/bin/evince//sanitized_helper
/usr/bin/evince//snap_browsers
/usr/bin/man
/usr/lib/NetworkManager/nm-dhcp-client.action
/usr/lib/NetworkManager/nm-dhcp-helper
/usr/lib/connman/scripts/dhclient-script
/usr/lib/cups/backend/cups-pdf
/usr/lib/snapd/snap-confine
/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
/usr/sbin/cups-browsed
/usr/sbin/cupsd
```

`sudo aa-enforce /etc/apparmor.d/usr.bin.something`

`sudo aa-complain /etc/apparmor.d/usr.bin.something`

`sudo aa-disable /etc/apparmor.d/usr.bin.something`

`sudo tail -f /var/log/syslog | grep apparmor`

```
lelay@Legenie:~$ sudo aa-enforce /etc/apparmor.d/usr.bin.something
sudo: aa-enforce : commande introuvable
lelay@Legenie:~$ sudo aa-complain /etc/apparmor.d/usr.bin.something
sudo: aa-complain : commande introuvable
lelay@Legenie:~$ sudo aa-disable /etc/apparmor.d/usr.bin.something
sudo: aa-disable : commande introuvable
lelay@Legenie:~$ sudo tail -f /var/log/syslog | grep apparmor
tail : option invalide -- '/'
Saisissez « tail --help » pour plus d'informations.
lelay@Legenie:~$ sudo tail -f /var/log/syslog | grep apparmor
```

9. Vérifiez si vnc-server a été Ajouté à la configuration:

`firewall-cmd --list-all`

```
lelay@Legenie:~$ firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
lelay@Legenie:~$
```

10. Redémarrez le service firewalld:

`systemctl restart firewalld`

```
lelay@Legenie:~$ systemctl restart firewalld
lelay@Legenie:~$
```

11. Vérifiez si vnc-server est dans la configuration:

`firewall-cmd --list-all`

```
lelay@Legenie:~$ systemctl restart firewalld
lelay@Legenie:~$ firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
lelay@Legenie:~$
```

Notez que le service vnc-server n'est plus spécifié. Expliquez-moi si c'est arrivé.

12. Ajoutez à nouveau le service vnc-server, mais cette fois, rendez-le permanent, en utilisant la commande

`firewall-cmd --add-service=vnc-server --permanent`

```
lelay@Legenie:~$ firewall-cmd --add-service=vnc-server --permanent
success
lelay@Legenie:~$
```

13. Croyez la présence de vnc-server dans la configuration:

`firewall-cmd --list-all`

```
lelay@Legenie:~$ firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
lelay@Legenie:~$
```

*Vous verrez que le serveur VNC n'est pas répertorié. Les services qui ont été ajoutés à la console sur le disque ne sont pas automatiquement ajoutés à la configuration temporelle d'exécutions.*

14. Redémarrez la configuration firewall:

`firewall-cmd --reload`

```
lelay@Legenie:~$ firewall-cmd --reload
success
lelay@Legenie:~$
```

15. Ajoutez le port TCP 2022 à la configuration du pare-feu

`firewall-cmd --add-port=2022/tcp --permanent`

```
lelay@Legenie:~$ firewall-cmd --add-port=2022/tcp --permanent
success
lelay@Legenie:~$
```

Puis redémarrez la configuration firewall:

`firewall-cmd --reload`

```
lelay@Legenie:~$ firewall-cmd --reload
success
lelay@Legenie:~$
```

et Vérifiez que le port est Ajouté à la configuration:

`firewall-cmd --reload`

```
lelay@Legenie:~$ firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
lelay@Legenie:~$
```

```
lelay@Legenie:~$ firewall-cmd --reload
success
lelay@Legenie:~$
```



Conclusion : Par la pratique de ce beau Td, J'arrive par maitriser les commandes pour la configuration d'un pare-feu et d'autres commandes y relatif.

TD6 - Systeme