

TP4 : Firewall NETFILTER

CAUMES Clément (PC1) - MTALSI MERIMI Mehdi (PC2) - LAMMAMRA Aicha (PC3) - RAMAROSON Andritsalama (PC4)

0) Mise en place de l'équipement

On utilise un hub pour connecter PC1-PC2-PC3-PC4 et on utilise le sous réseau 192.168.1.0 :

Pour le PC1, on met l'adresse IP 192.168.1.1 et le mask 255.255.255.0 :

```
irs@irs-OptiPlex-3040:~$ sudo ifconfig enp3s0 inet 192.168.1.1 netmask 255.255.255.0
[sudo] Mot de passe de irs :
irs@irs-OptiPlex-3040:~$
```

Pour le PC2, on met l'adresse IP 192.168.1.2 et le mask 255.255.255.0 :

```
irs@irs-OptiPlex-3040:~$ sudo ifconfig enp3s0 inet 192.168.1.2 netmask 255.255.255.0
```

Pour le PC3, on met l'adresse IP 192.168.1.3 et le mask 255.255.255.0 :

```
irs@irs-OptiPlex-3040:~$ sudo ifconfig enp3s0 inet 192.168.1.3 netmask 255.255.255.0
[sudo] Mot de passe de irs :
```

Pour le PC4, on met l'adresse IP 192.168.1.4 et le mask 255.255.255.0 :

```
irs@irs-OptiPlex-3040:~$ sudo ifconfig enp3s0 inet 192.168.1.4 netmask 255.255.255.0
[sudo] Mot de passe de irs :
irs@irs-OptiPlex-3040:~$
```

1) Prise en main

- Quand on affiche le contenu de notre pare feu, on peut voir que la table est vide car le pare feu est passif au démarrage.

```
irs@irs-OptiPlex-3040:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
irs@irs-OptiPlex-3040:~$
```

Quand on affiche le manuel, on peut y voir les commandes de netfilter :

```
IPTABLES(8)                                iptables 1.6.0                                IPTABLES(8)
NAME
    iptables/ip6tables - administration tool for IPv4/IPv6 packet filtering and NAT
SYNOPSIS
    iptables [-t table] {-A|-C|-D} chain rule-specification
    ip6tables [-t table] {-A|-C|-D} chain rule-specification
    iptables [-t table] -I chain [rulenum] rule-specification
    iptables [-t table] -R chain rulenum rule-specification
    iptables [-t table] -D chain rulenum
    iptables [-t table] -S [chain [rulenum]]
    iptables [-t table] {-F|-L|-Z} [chain [rulenum]] [options...]
    iptables [-t table] -N chain
    iptables [-t table] -X [chain]
    iptables [-t table] -P chain target
    iptables [-t table] -E old-chain-name new-chain-name
    rule-specification = [matches...] [target]
    match = -m matchname [per-match-options]
    target = -j targetname [per-target-options]
DESCRIPTION
    Iptables and ip6tables are used to set up, maintain, and inspect the tables of IPv4 and IPv6 packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.
    Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.
TARGETS
    A firewall rule specifies criteria for a packet and a target. If the packet does not match, the next rule in the chain is examined; if it does match, then the next rule is specified by the value of the target, which can be the name of a user-defined chain, one of the targets described in iptables-extensions(8), or one of the special values ACCEPT, DROP or RETURN.
    ACCEPT means to let the packet through. DROP means to drop the packet on the floor. RETURN means stop traversing this chain and resume at the next rule in the previous (calling) chain. If the end of a built-in chain is reached or a rule in a built-in chain with target RETURN is matched, the target specified by the chain policy determines the fate of the packet.
TABLES
    There are currently five independent tables (which tables are present at any time depends on the kernel configuration options and which modules are present).
    -t, --table table
        This option specifies the packet matching table which the command should operate on. If the kernel is configured
Manual page iptables(8) line 1 (press h for help or q to quit)
```

Pour effacer une règle d'une chaîne, on lance la commande :

```
iptables [-t table] -D chain rulenum
```

Pour effacer toutes les règles, on lance la commande :

```
iptables [-t table] -F [chain [rulenum]] [options...]
```

Pour supprimer une chaîne, on lance la commande :

```
iptables [-t table] -X [chain]
```

Concernant la suppression de la quatrième chaîne sous Fedora, nous ne pouvons pas réaliser cette manipulation car nous sommes sur Ubuntu et il y a eu des mises à jour depuis la version évoquée dans le TP.

Quand on liste les options du service iptables, la commande n'est pas reconnue :

```
irs@irs-OptiPlex-3040:/$ service iptables
iptables: unrecognized service
irs@irs-OptiPlex-3040:/$
```

Pour sauvegarder la configuration actuelle du pare feu, on fait la commande suivante :

```
irs@irs-OptiPlex-3040:/$ sudo iptables-save
# Generated by iptables-save v1.6.0 on Fri Apr 12 09:35:36 2019
*filter
:INPUT ACCEPT [9178:681413]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [9144:677558]
COMMIT
# Completed on Fri Apr 12 09:35:36 2019
irs@irs-OptiPlex-3040:/$
```

2) Filtrage de ports

- Les PCs vont bloquer les connexions sur le port 22 avec la commande suivante :

```
irs@irs-OptiPlex-3040:/$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 11275 packets, 837K bytes)
 pkts bytes target    prot opt in     out     source            destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
Chain OUTPUT (policy ACCEPT 11234 packets, 832K bytes)
 pkts bytes target    prot opt in     out     source            destination
irs@irs-OptiPlex-3040:/$ sudo iptables -A INPUT -p tcp --dport 22 -j DROP
irs@irs-OptiPlex-3040:/$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
    0    0 DROP      tcp  --  any    any    anywhere          anywhere          tcp dpt:ssh
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
irs@irs-OptiPlex-3040:/$
```

On remarque qu'il y a une nouvelle règle dans la chaîne INPUT.

- Maintenant, si on lance sftp (port 22) mutuellement, on doit attendre assez longtemps et on observe que la connexion est impossible :

```
irs@irs-OptiPlex-3040:~$ sftp 192.168.1.1
ssh: connect to host 192.168.1.1 port 22: Connection timed out
Couldn't read packet: Connection reset by peer
```

Dans cet exemple, PC1 a bloqué le port 22 tandis que PC2 tente de se connecter au PC1 par le port 22.

- Si on utilise REJECT au lieu de DROP, l'échec à la connexion arrive directement (sans attente).

```
root@serveur:/home/irs# iptables -A INPUT -p tcp --dport 22 -j REJECT
root@serveur:/home/irs# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
    0    0 REJECT    tcp  --  any    any    anywhere          anywhere          tcp dpt:ssh reject-with icmp-port-unreachable
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source            destination
root@serveur:/home/irs#
```

En affichant les tables, on remarque que le port est devenu inatteignable.

Et si on tente de se connecter :

```
irs@irs-OptiPlex-3040:~$ sftp 192.168.1.1
ssh: connect to host 192.168.1.1 port 22: Connection refused
Couldn't read packet: Connection reset by peer
```

On va maintenant effectuer la procédure suivante par binôme :

- PC1 va autoriser la connexion sur le port 22 pour PC2 et bloquer pour le reste.
Sur le PC1 :

```
irs@irs-OptiPlex-3040:/$ sudo iptables -I INPUT 1 -p tcp --dport 22 -s 192.168.1.2 -j ACCEPT
irs@irs-OptiPlex-3040:/$ sudo iptables -A INPUT -p tcp --dport 22 -j REJECT
irs@irs-OptiPlex-3040:/$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 1 packets, 112 bytes)
  pkts bytes target     prot opt in     out     source    destination
    0      0 ACCEPT     tcp  --  any    any    PC2       anywhere
    0      0 REJECT     tcp  --  any    any    anywhere  anywhere          tcp dpt:ssh
                                tcp dpt:ssh reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source    destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source    destination
irs@irs-OptiPlex-3040:/$
```

- Maintenant, si PC2 se connecte avec sftp par le port 22 de PC1, cela fonctionne correctement :

```
irs@irs-OptiPlex-3040:~$ sftp 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
ECDSA key fingerprint is SHA256:dPDJpMIqs2cp9XafyF/kkDzeD7asLbBqdStDM9UPki8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (ECDSA) to the list of known hosts.
irs@192.168.1.1's password:
Connected to 192.168.1.1.
sftp>
```

Si on utilise Wireshark, sans surprise, on peut voir les trames circulant sur le port 22.

7	2.563086245	192.168.1.2	192.168.1.1	TCP	66 33978 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1471936 TSecr=1656089
8	2.563164985	192.168.1.2	192.168.1.1	SSHv2	107 Client: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
9	2.563185915	192.168.1.1	192.168.1.2	TCP	66 22 → 33978 [ACK] Seq=1 Ack=42 Win=29056 Len=0 TSval=1656089 TSecr=1471936
10	2.570981678	192.168.1.1	192.168.1.2	SSHv2	107 Server: Protocol (SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2)
11	2.571544897	192.168.1.2	192.168.1.1	TCP	66 33978 → 22 [ACK] Seq=42 Ack=42 Win=29312 Len=0 TSval=1471938 TSecr=1656091
12	2.571569314	192.168.1.1	192.168.1.2	SSHv2	1042 Server: Key Exchange Init
13	2.575297155	192.168.1.2	192.168.1.1	SSHv2	1402 Client: Key Exchange Init
14	2.616101172	192.168.1.2	192.168.1.1	TCP	66 33978 → 22 [ACK] Seq=1378 Ack=1018 Win=32128 Len=0 TSval=1471950 TSecr=1656091
15	2.616141797	192.168.1.1	192.168.1.2	TCP	66 22 → 33978 [ACK] Seq=1018 Ack=1378 Win=31872 Len=0 TSval=1656102 TSecr=1471939
16	2.616583138	192.168.1.2	192.168.1.1	SSHv2	114 Client: Diffie-Hellman Key Exchange Init
17	2.625062493	192.168.1.1	192.168.1.2	SSHv2	430 Diffie-Hellman Key Exchange Reply, New Keys

- Si PC3 tente de se connecter de la même façon sur le port 22 du PC1, cela échoue (ce qui est normal) :

```
irs@irs-OptiPlex-3040:~$ sftp 192.168.1.1
ssh: connect to host 192.168.1.1 port 22: Connection refused
Couldn't read packet: Connection reset by peer
```

Sur Wireshark, on peut voir que la connexion sur ce port a bien échoué :

49	22.225282777	192.168.1.3	192.168.1.1	TCP	74 47932 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1380767 TSecr=0 WS=128
50	22.225329388	192.168.1.1	192.168.1.3	ICMP	102 Destination unreachable (Port unreachable)
51	27.292693201	e4:be:ed:8c:1d:9d	e4:be:ed:8c:1d:9a	ARP	42 Who has 192.168.1.3? Tell 192.168.1.1
52	27.293266233	e4:be:ed:8c:1d:9a	e4:be:ed:8c:1d:9d	ARP	60 192.168.1.3 is at e4:be:ed:8c:1d:9a
53	27.475685412	e4:be:ed:8c:1d:9a	e4:be:ed:8c:1d:9d	ARP	60 Who has 192.168.1.1? Tell 192.168.1.3
54	27.475706353	e4:be:ed:8c:1d:9d	e4:be:ed:8c:1d:9a	ARP	42 192.168.1.1 is at e4:be:ed:8c:1d:9d
55	42.874554955	192.168.1.2	192.168.1.255	WHO	126 irs-OptiPlex-3040: 0,00 0,00 0,00
56	61.980506761	192.168.1.3	192.168.1.255	WHO	126 irs-OptiPlex-3040: 0,00 0,00 0,00
57	72.766966709	192.168.1.3	192.168.1.4	TCP	74 40334 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1393402 TSecr=0 WS=128
58	72.767196946	192.168.1.4	192.168.1.3	TCP	74 22 → 40334 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=1435557 TSecr=1380767
59	72.767421030	192.168.1.3	192.168.1.4	TCP	66 40334 → 22 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1393403 TSecr=1435557

Pour le deuxième binôme, le PC4 va autoriser la connexion sur le port 22 pour PC3 et bloquer pour le reste.

```
root@serveur:/home/irs# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 112 bytes)
 pkts bytes target    prot opt in     out     source    destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
root@serveur:/home/irs# iptables -I INPUT 1 -p tcp --dport 22 -s 192.168.1.3 -j ACCEPT
root@serveur:/home/irs# iptables -A INPUT -p tcp --dport 22 -j REJECT
root@serveur:/home/irs# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
    0    0 ACCEPT    tcp  --  any    any    PC3        anywhere        tcp dpt:ssh
    0    0 REJECT    tcp  --  any    any    anywhere   anywhere        tcp dpt:ssh reject-with icmp-port-unreachable
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
root@serveur:/home/irs#
```

PC3 pourra donc se connecter via son port 22 :

```
irs@irs-OptiPlex-3040:~$ sftp 192.168.1.4
The authenticity of host '192.168.1.4 (192.168.1.4)' can't be established.
ECDSA key fingerprint is SHA256:dPDJpMIqs2cp9XafyF/kkDzeD7asLbBqdstDM9UPki8.
Are you sure you want to continue connecting (yes/no)? n
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.1.4' (ECDSA) to the list of known hosts.
irs@192.168.1.4's password:
Connected to 192.168.1.4.
sftp> ls
Bureau                                Compte Rendu - TP4 - Firewall Netfilter.pdf  Documents
Images                               Modèles                                       Musique
Public                               Téléchargements                             Vidéos
examples.desktop
sftp> cd images
Couldn't stat remote file: No such file or directory
sftp> cd /images
Couldn't stat remote file: No such file or directory
sftp> quit
```

Mais PC2 ne le pourra pas puisqu'il est bloqué :

```
irs@irs-OptiPlex-3040:~$ sftp 192.168.1.4
ssh: connect to host 192.168.1.4 port 22: Connection refused
Couldn't read packet: Connection reset by peer
```

Exercice 1

PC1 va autoriser PC2 à se connecter au port 22 et 25 et à interdire le reste avec un log.

```
irs@irs-OptiPlex-3040:/$ sudo iptables -I INPUT -m multiport -p tcp --dports 22,25 -s 192.168.1.2 -j ACCEPT
irs@irs-OptiPlex-3040:/$ sudo iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix "regle de Clement"
irs@irs-OptiPlex-3040:/$ sudo iptables -A INPUT -p tcp --dport 22 -j REJECT
irs@irs-OptiPlex-3040:/$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
    0    0 ACCEPT    tcp  --  any    any    PC2        anywhere        multiport dports ssh,smtp
    0    0 LOG      tcp  --  any    any    anywhere   anywhere        tcp dpt:ssh LOG level warning prefix "regle d
e Clement"
    0    0 REJECT    tcp  --  any    any    anywhere   anywhere        tcp dpt:ssh reject-with icmp-port-unreachable
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source    destination
```

Si PC4 (qui n'est pas autorisé à se connecter sur le port 22 et 25) tente 3 connexions, on peut y voir dans le fichier var/log/messages les logs choisis précédemment :

```
GNU nano 2.5.3      Fichier : var/log/messages
Apr 12 08:24:40 irs-OptiPlex-3040 syslogd: GNU inetutils 1.9.4): restart
Apr 12 08:26:26 irs-OptiPlex-3040 vmunix: [ 505.608375] r8169 0000:03:00.0 enp3s0: link down
Apr 12 08:36:16 irs-OptiPlex-3040 vmunix: [ 1096.056838] r8169 0000:03:00.0 enp3s0: link up
Apr 12 08:49:39 irs-OptiPlex-3040 vmunix: [ 1898.391448] ip_tables: (C) 2000-2006 Netfilter Core Team
Apr 12 08:59:43 irs-OptiPlex-3040 -- MARK --
Apr 12 09:19:43 irs-OptiPlex-3040 -- MARK --
Apr 12 09:39:43 irs-OptiPlex-3040 -- MARK --
Apr 12 09:59:28 irs-OptiPlex-3040 vmunix: [ 6088.083278] Netfilter messages via NETLINK v0.30.
Apr 12 09:59:32 irs-OptiPlex-3040 vmunix: [ 6092.018243] device enp3s0 entered promiscuous mode
Apr 12 10:02:03 irs-OptiPlex-3040 vmunix: [ 6242.608722] device enp3s0 left promiscuous mode
Apr 12 10:12:26 irs-OptiPlex-3040 vmunix: [ 6865.662107] device enp3s0 entered promiscuous mode
Apr 12 10:12:28 irs-OptiPlex-3040 vmunix: [ 6867.965589] device enp3s0 left promiscuous mode
Apr 12 10:12:47 irs-OptiPlex-3040 vmunix: [ 6886.433993] device enp3s0 entered promiscuous mode
Apr 12 10:12:54 irs-OptiPlex-3040 vmunix: [ 6894.341579] device enp3s0 left promiscuous mode
Apr 12 10:13:21 irs-OptiPlex-3040 vmunix: [ 6920.809860] device enp3s0 entered promiscuous mode
Apr 12 10:14:40 irs-OptiPlex-3040 vmunix: [ 6999.565004] device enp3s0 left promiscuous mode
Apr 12 10:39:43 irs-OptiPlex-3040 -- MARK --
Apr 12 10:41:42 irs-OptiPlex-3040 vmunix: [ 8621.858860] regle de ClementIN=enp3s0 OUT= MAC=e4:be:ed:8c:1d:9d:e4:be:ed:8c:1d:9a:08:00S
Apr 12 10:47:38 irs-OptiPlex-3040 vmunix: [ 8977.586693] regle de ClementIN=enp3s0 OUT= MAC=e4:be:ed:8c:1d:9d:e4:be:ed:8c:1d:9a:08:00S
Apr 12 10:52:58 irs-OptiPlex-3040 vmunix: [ 9298.322431] regle de ClementIN=enp3s0 OUT= MAC=e4:be:ed:8c:1d:9d:e4:be:ed:8c:1d:9a:08:00S
```


On fait de même sur les 3 autres PC :

- Sur le PC2 : on accepte les connexions sur le port 22 et 25 par PC2 mais pas les autres.

```
lrs@lrs-OptiPlex-3040:~$ sudo iptables -I INPUT -m multiport -p tcp --dports 22,25 -s 192.168.1.1 -j ACCEPT
lrs@lrs-OptiPlex-3040:~$ sudo iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix "REGLE DE MEHDI"
lrs@lrs-OptiPlex-3040:~$ sudo iptables -A INPUT -p tcp --dport 22 -j REJECT
lrs@lrs-OptiPlex-3040:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT   tcp  --  any    any    PC1                  anywhere
    0     0 LOG      tcp  --  any    any    anywhere             anywhere
    0     0 REJECT   tcp  --  any    any    anywhere             anywhere
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
```

Après tentative de connexion de la part du PC4 :

```
lrs@lrs-OptiPlex-3040: /
GNU nano 2.5.3 Fichier : /var/log/messages
Apr 12 10:43:31 lrs-OptiPlex-3040 syslogd (GNU inetutils 1.9.4): restart
Apr 12 10:56:31 lrs-OptiPlex-3040 vmunix: [ 1180.374827] ip_tables: (C) 2000-2006 Netfilter Core Team
Apr 12 11:00:10 lrs-OptiPlex-3040 vmunix: [ 1400.007412] nf_conntrack version 0.5.0 (16384 buckets, 65536 max)
Apr 12 11:18:38 lrs-OptiPlex-3040 -- MARK --
Apr 12 11:38:38 lrs-OptiPlex-3040 -- MARK --
Apr 12 11:42:30 lrs-OptiPlex-3040 vmunix: [ 3947.876866] ip6_tables: (C) 2000-2006 Netfilter Core Team
Apr 12 11:58:38 lrs-OptiPlex-3040 -- MARK --
Apr 12 12:18:38 lrs-OptiPlex-3040 -- MARK --
Apr 12 12:38:38 lrs-OptiPlex-3040 -- MARK --
Apr 12 12:58:38 lrs-OptiPlex-3040 -- MARK --
Apr 12 13:08:29 lrs-OptiPlex-3040 vmunix: [ 9099.242291] REGLE DE MEHDIIN=enp3s0 OUT= MAC=e4:be:ed:8c:1d:83:e4:be:ed:8c:1d:9a:08:00 $
Apr 12 13:08:32 lrs-OptiPlex-3040 vmunix: [ 9101.386310] REGLE DE MEHDIIN=enp3s0 OUT= MAC=e4:be:ed:8c:1d:83:e4:be:ed:8c:1d:9a:08:00 $
Apr 12 13:08:32 lrs-OptiPlex-3040 vmunix: [ 9102.025112] REGLE DE MEHDIIN=enp3s0 OUT= MAC=e4:be:ed:8c:1d:83:e4:be:ed:8c:1d:9a:08:00 $
Apr 12 13:08:34 lrs-OptiPlex-3040 vmunix: [ 9103.354079] REGLE DE MEHDIIN=enp3s0 OUT= MAC=e4:be:ed:8c:1d:83:e4:be:ed:8c:1d:9a:08:00 $
Apr 12 13:08:35 lrs-OptiPlex-3040 vmunix: [ 9104.745898] REGLE DE MEHDIIN=enp3s0 OUT= MAC=e4:be:ed:8c:1d:83:e4:be:ed:8c:1d:9a:08:00 $

Lecture de 15 lignes (Attention : en lecture seule !)
```

Sur le PC3 : on accepte les connexions sur le port 22 et 25 par PC4 mais pas les autres.

```
lrs@lrs-OptiPlex-3040:~$ sudo iptables -I INPUT -m multiport -p tcp --dports 22,255 -s 192.168.1.4 -j ACCEPT
lrs@lrs-OptiPlex-3040:~$ sudo iptables -I INPUT -p tcp --dport 22 -j LOG --log-prefix "regle de BB"
lrs@lrs-OptiPlex-3040:~$ sudo iptables -I INPUT -p tcp --dport 22 -j REJECT
lrs@lrs-OptiPlex-3040:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 1 packets, 112 bytes)
  pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT   tcp  --  any    any    anywhere             anywhere
    0     0 LOG      tcp  --  any    any    anywhere             anywhere
    0     0 ACCEPT   tcp  --  any    any    PC4                  anywhere
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
lrs@lrs-OptiPlex-3040:~$
```

Sur le PC4 : on accepte les connexions sur le port 22 et 25 par PC3 mais pas les autres.

```
root@serveur:/home/lrs# iptables -L -v
Chain INPUT (policy ACCEPT 1 packets, 112 bytes)
  pkts bytes target     prot opt in     out     source               destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
root@serveur:/home/lrs# iptables -I INPUT -m multiport -p tcp --dport 22,25 -s 192.168.1.3 -j ACCEPT
root@serveur:/home/lrs# iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix "Regle AA"
root@serveur:/home/lrs# iptables -A INPUT -p tcp --dport 22 -j REJECT
root@serveur:/home/lrs# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT   tcp  --  any    any    PC3                  anywhere
    0     0 LOG      tcp  --  any    any    anywhere             anywhere
    0     0 REJECT   tcp  --  any    any    anywhere             anywhere
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
root@serveur:/home/lrs#
```

Après tentative de connexion de la part du PC2 :


```
Apr 12 12:31:22 serveur -- MARK --
Apr 12 12:50:44 serveur vmunix: [ 8467.223519] Regle AAIN=enp3s0 OUT= MAC=e4:be:ed:8c:1d:c1:e4:be:ed:8c:1d:9d:08:00 SRC=192.168.1.1 DST=$
Apr 12 12:53:06 serveur vmunix: [ 8608.406593] Regle AAIN=enp3s0 OUT= MAC=e4:be:ed:8c:1d:c1:e4:be:ed:8c:1d:9d:08:00 SRC=192.168.1.1 DST=$
```

Exercice 2

Sur chaque PC, après s'être assuré de s'être connecté à Internet, on réalise les commandes suivantes :

```
irs@irs-OptiPlex-3040:/$ sudo iptables -A OUTPUT -p tcp -m multiport --ports 80,443 -j LOG --log-prefix "TRAFFIC BLOQUE"
irs@irs-OptiPlex-3040:/$ sudo iptables -A OUTPUT -p tcp -m multiport --ports 80,443 -j REJECT
irs@irs-OptiPlex-3040:/$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source               destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source               destination
    0      0 LOG      tcp  --  any    any    anywhere            anywhere            multiport ports http,https LOG level warning
    0      0 REJECT   tcp  --  any    any    anywhere            anywhere            multiport ports http,https reject-with icmp-p
ort-unreachable
irs@irs-OptiPlex-3040:/$
```

Désormais, si on se connecte à Internet, c'est impossible vu que le port HTTP et HTTPS sont bloqués en sortie :



La connexion a échoué

Firefox ne peut établir de connexion avec le serveur à l'adresse www.google.fr.

- Le site est peut-être temporairement indisponible ou surchargé. Réessayez plus tard ;
- Si vous n'arrivez à naviguer sur aucun site, vérifiez la connexion au réseau de votre ordinateur ;
- Si votre ordinateur ou votre réseau est protégé par un pare-feu ou un proxy, assurez-vous que Firefox est autorisé à accéder au Web.

Réessayer

De plus, si on regarde le fichier var/log/messages, on remarque bien les messages LOG affichés :

```
irs@irs-OptiPlex-3040:/$ tail -f var/log/messages
Apr 12 11:36:32 irs-OptiPlex-3040 vmunix: [ 960.324829] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=54.201.6.28 LEN=60 TOS=0x00 P
REC=0x00 TTL=64 ID=46634 DF PROTO=TCP SPT=35384 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:33 irs-OptiPlex-3040 vmunix: [ 961.348294] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=54.201.6.28 LEN=60 TOS=0x00 P
REC=0x00 TTL=64 ID=46635 DF PROTO=TCP SPT=35384 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:33 irs-OptiPlex-3040 vmunix: [ 961.348904] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=52.35.21.241 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=14028 DF PROTO=TCP SPT=51184 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:35 irs-OptiPlex-3040 vmunix: [ 962.372093] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=52.35.21.241 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=14029 DF PROTO=TCP SPT=51184 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:35 irs-OptiPlex-3040 vmunix: [ 962.372474] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=52.35.215.194 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=3222 DF PROTO=TCP SPT=57574 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:36 irs-OptiPlex-3040 vmunix: [ 963.396296] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=52.35.215.194 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=3223 DF PROTO=TCP SPT=57574 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:36 irs-OptiPlex-3040 vmunix: [ 963.396802] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=54.186.120.41 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=51764 DF PROTO=TCP SPT=44332 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:37 irs-OptiPlex-3040 vmunix: [ 964.420266] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=54.186.120.41 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=51765 DF PROTO=TCP SPT=44332 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:37 irs-OptiPlex-3040 vmunix: [ 964.420880] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=52.88.72.192 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=21060 DF PROTO=TCP SPT=58720 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:38 irs-OptiPlex-3040 vmunix: [ 965.444251] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=52.88.72.192 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=21061 DF PROTO=TCP SPT=58720 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:53 irs-OptiPlex-3040 vmunix: [ 980.957778] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=143.204.192.6 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=11244 DF PROTO=TCP SPT=58434 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:54 irs-OptiPlex-3040 vmunix: [ 981.988267] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=143.204.192.6 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=11245 DF PROTO=TCP SPT=58434 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:54 irs-OptiPlex-3040 vmunix: [ 981.988930] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=143.204.192.103 LEN=60 TOS=0x
00 PREC=0x00 TTL=64 ID=46746 DF PROTO=TCP SPT=57926 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:55 irs-OptiPlex-3040 vmunix: [ 983.012267] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=143.204.192.103 LEN=60 TOS=0x
00 PREC=0x00 TTL=64 ID=46747 DF PROTO=TCP SPT=57926 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:55 irs-OptiPlex-3040 vmunix: [ 983.012630] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=143.204.192.77 LEN=60 TOS=0x0
0 PREC=0x00 TTL=64 ID=24203 DF PROTO=TCP SPT=36368 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:56 irs-OptiPlex-3040 vmunix: [ 984.036269] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=143.204.192.77 LEN=60 TOS=0x0
0 PREC=0x00 TTL=64 ID=24204 DF PROTO=TCP SPT=36368 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:56 irs-OptiPlex-3040 vmunix: [ 984.036754] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=143.204.192.95 LEN=60 TOS=0x0
0 PREC=0x00 TTL=64 ID=24800 DF PROTO=TCP SPT=47496 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:57 irs-OptiPlex-3040 vmunix: [ 985.060266] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=143.204.192.95 LEN=60 TOS=0x0
0 PREC=0x00 TTL=64 ID=24801 DF PROTO=TCP SPT=47496 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:58 irs-OptiPlex-3040 vmunix: [ 985.061792] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=143.204.192.6 LEN=60 TOS=0x00
PREC=0x00 TTL=64 ID=61229 DF PROTO=TCP SPT=38442 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
Apr 12 11:36:58 irs-OptiPlex-3040 vmunix: [ 985.312504] TRAFFIC BLOQUEIN= OUT=enp2s0 SRC=172.16.0.28 DST=143.204.192.103 LEN=60 TOS=0x
00 PREC=0x00 TTL=64 ID=13841 DF PROTO=TCP SPT=57934 DPT=443 WINDOW=29200 RES=0x00 SYN URG=0
^C
```

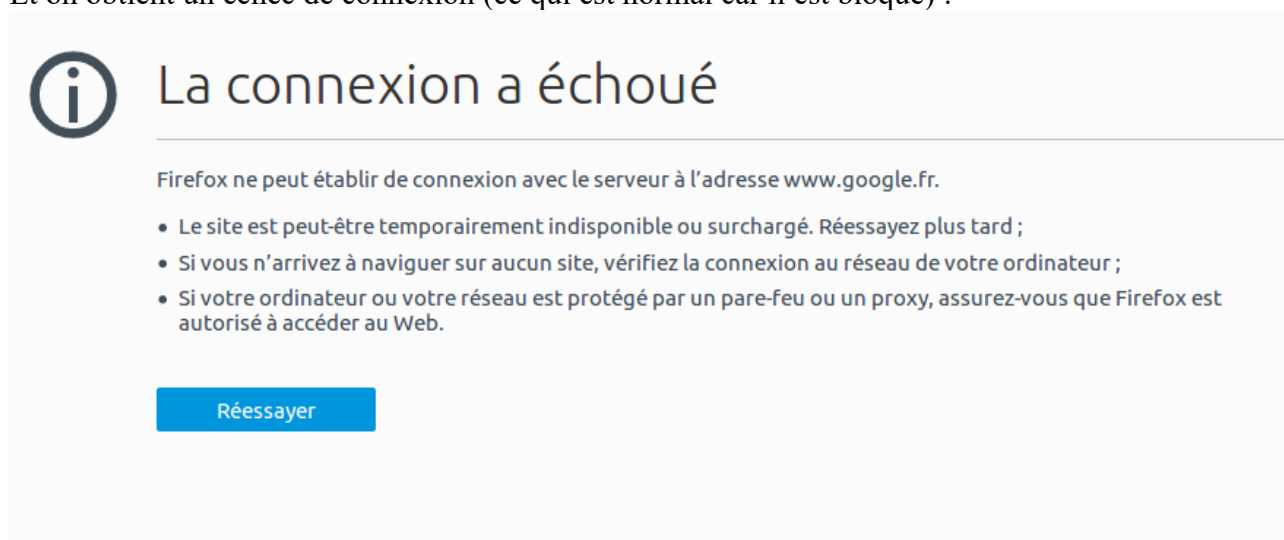
Maintenant, on veut que le superutilisateur puisse aller sur Internet mais pas l'utilisateur normal. Pour cela, on fait la commande suivante sur les 4 PC :

```
lrs@lrs-OptiPlex-3040:/$ sudo iptables -A OUTPUT -p tcp -m multiport --ports 80,443 -j ACCEPT -m owner --uid-owner root
lrs@lrs-OptiPlex-3040:/$ sudo iptables -A OUTPUT -p tcp -m multiport --ports 80,443 -j REJECT
lrs@lrs-OptiPlex-3040:/$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 7 packets, 741 bytes)
pkts bytes target      prot opt in     out     source                   destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source                   destination
Chain OUTPUT (policy ACCEPT 3 packets, 240 bytes)
pkts bytes target      prot opt in     out     source                   destination
0      0 ACCEPT      tcp  --  any    any    anywhere                anywhere            multiport ports http,https owner UID match root
3      156 REJECT      tcp  --  any    any    anywhere                anywhere            multiport ports http,https reject-with icmp-port-unreachable
lrs@lrs-OptiPlex-3040:/$
```

Si on va sur firefox en utilisateur normal, on fait :

```
firefox www.google.fr
```

Et on obtient un échec de connexion (ce qui est normal car il est bloqué) :



Par contre, pour le superutilisateur en root, on fait :

```
sudo firefox www.google.fr
```

Et on accède bien à Internet :



Exercice 3

- Ping Flood

On va limiter les paquets ICMP à 1 par seconde.

```
lrs@lrs-OptiPlex-3040:~$ sudo iptables -A INPUT -p icmp -m limit --limit 1/second
lrs@lrs-OptiPlex-3040:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data:
```

On remarque que les paquets ICMP (request) sont reçus effectivement toutes les secondes.

1	0.000000000	192.168.1.2	192.168.1.1	ICMP	98 Echo (ping) request	id=0x09db, seq=1/256, ttl=64 (reply in 2)
2	0.000039484	192.168.1.1	192.168.1.2	ICMP	98 Echo (ping) reply	id=0x09db, seq=1/256, ttl=64 (request in 1)
3	1.013855167	192.168.1.2	192.168.1.1	ICMP	98 Echo (ping) request	id=0x09db, seq=2/512, ttl=64 (reply in 4)
4	1.013892066	192.168.1.1	192.168.1.2	ICMP	98 Echo (ping) reply	id=0x09db, seq=2/512, ttl=64 (request in 3)
5	2.037870501	192.168.1.2	192.168.1.1	ICMP	98 Echo (ping) request	id=0x09db, seq=3/768, ttl=64 (reply in 6)
6	2.037907969	192.168.1.1	192.168.1.2	ICMP	98 Echo (ping) reply	id=0x09db, seq=3/768, ttl=64 (request in 5)
7	3.061890594	192.168.1.2	192.168.1.1	ICMP	98 Echo (ping) request	id=0x09db, seq=4/1024, ttl=64 (reply in 8)
8	3.061924178	192.168.1.1	192.168.1.2	ICMP	98 Echo (ping) reply	id=0x09db, seq=4/1024, ttl=64 (request in 7)
9	4.085883657	192.168.1.2	192.168.1.1	ICMP	98 Echo (ping) request	id=0x09db, seq=5/1280, ttl=64 (reply in 10)
10	4.085919899	192.168.1.1	192.168.1.2	ICMP	98 Echo (ping) reply	id=0x09db, seq=5/1280, ttl=64 (request in 9)
11	5.085768034	e4:be:ed:8c:1d:9d	e4:be:ed:8c:1d:83	ARP	42 Who has 192.168.1.2? Tell 192.168.1.1	
12	5.086313088	e4:be:ed:8c:1d:83	e4:be:ed:8c:1d:9d	ARP	60 192.168.1.2 is at e4:be:ed:8c:1d:83	
13	5.109876787	192.168.1.2	192.168.1.1	ICMP	98 Echo (ping) request	id=0x09db, seq=6/1536, ttl=64 (reply in 14)
14	5.109912338	192.168.1.1	192.168.1.2	ICMP	98 Echo (ping) reply	id=0x09db, seq=6/1536, ttl=64 (request in 13)
15	6.133745083	192.168.1.2	192.168.1.1	ICMP	98 Echo (ping) request	id=0x09db, seq=7/1792, ttl=64 (reply in 16)
16	6.133780865	192.168.1.1	192.168.1.2	ICMP	98 Echo (ping) reply	id=0x09db, seq=7/1792, ttl=64 (request in 15)

- ConnTrack

On efface toutes les règles précédentes. Puis, on interdit tout. Enfin, on accepte tout les paquets provenant d'un serveur sftp (port 22).

```
lrs@lrs-OptiPlex-3040:~$ sudo iptables -F
lrs@lrs-OptiPlex-3040:~$ sudo modprobe ip_conntrack_sftp
modprobe: FATAL: Module ip_conntrack_sftp not found in directory /lib/modules/4.8.0-36-generic
lrs@lrs-OptiPlex-3040:~$ sudo modprobe ip_conntrack_ftp
lrs@lrs-OptiPlex-3040:~$ sudo iptables -A INPUT -j REJECT
lrs@lrs-OptiPlex-3040:~$ sudo wireshark
^C
lrs@lrs-OptiPlex-3040:~$ sudo iptables -I INPUT 1 -p tcp -m multiport --sports 22 -m state --state ESTABLISHED -j ACCEPT
lrs@lrs-OptiPlex-3040:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0      0 ACCEPT     tcp  --  any    any    anywhere             anywhere
  176 13224 REJECT     all  --  any    any    anywhere             anywhere
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 127 packets, 9488 bytes)
 pkts bytes target     prot opt in     out     source               destination
lrs@lrs-OptiPlex-3040:~$
```

On configure le PC1 comme serveur sftp et on remarque que sa connexion se fait correctement :

```
lrs@lrs-OptiPlex-3040:~$ sftp 192.168.1.1
lrs@192.168.1.1's password:
Connected to 192.168.1.1.
```