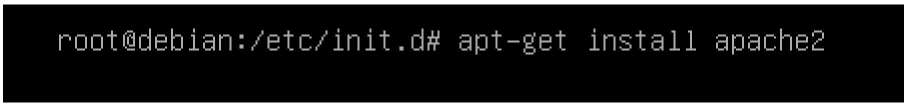
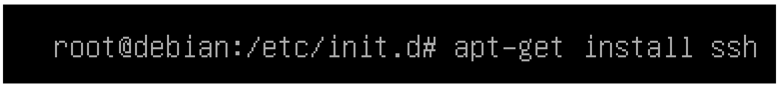
IPTABLES / DEBIAN

Installation du package apache et ssh

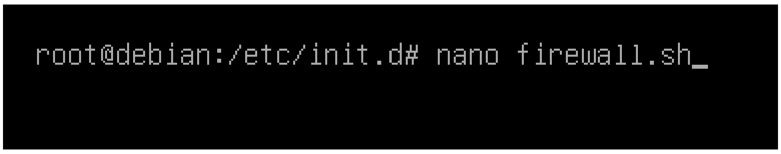


```
root@debian:/etc/init.d# apt-get install apache2
```



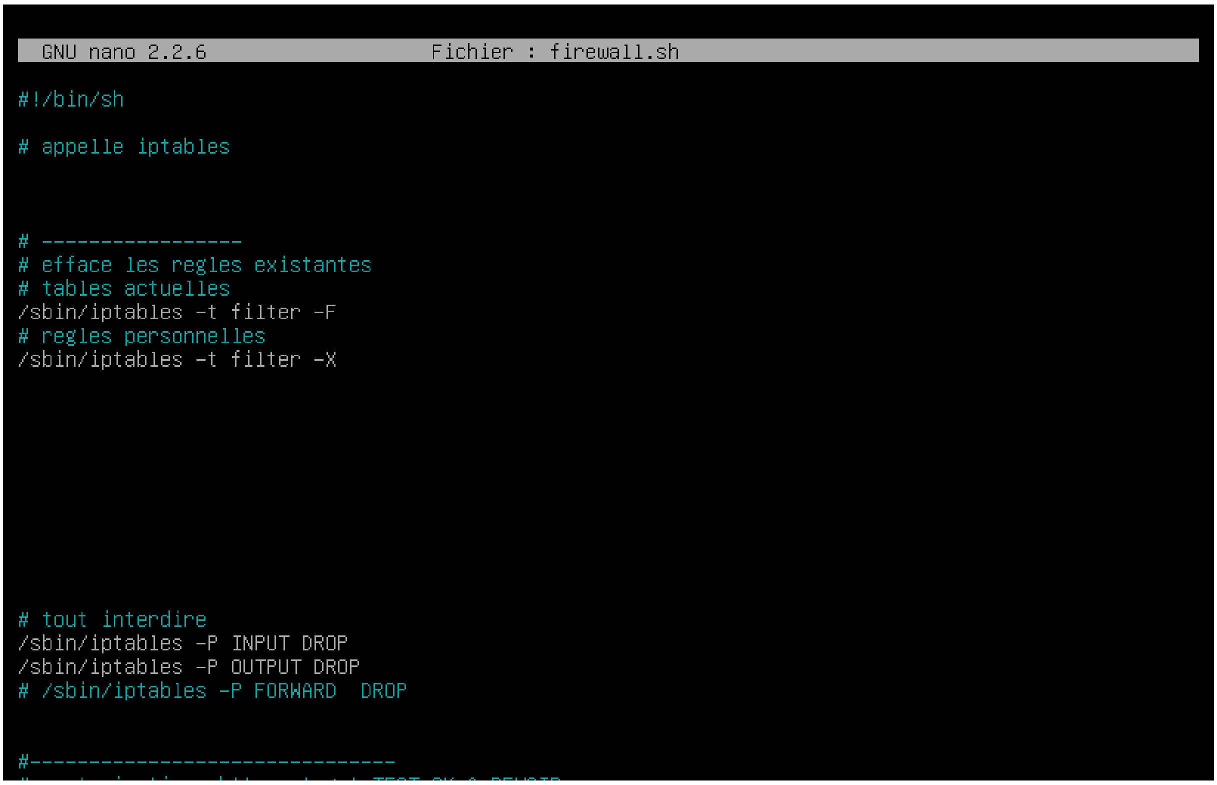
```
root@debian:/etc/init.d# apt-get install ssh
```

Création d'un script pour les droits sur le parfeu



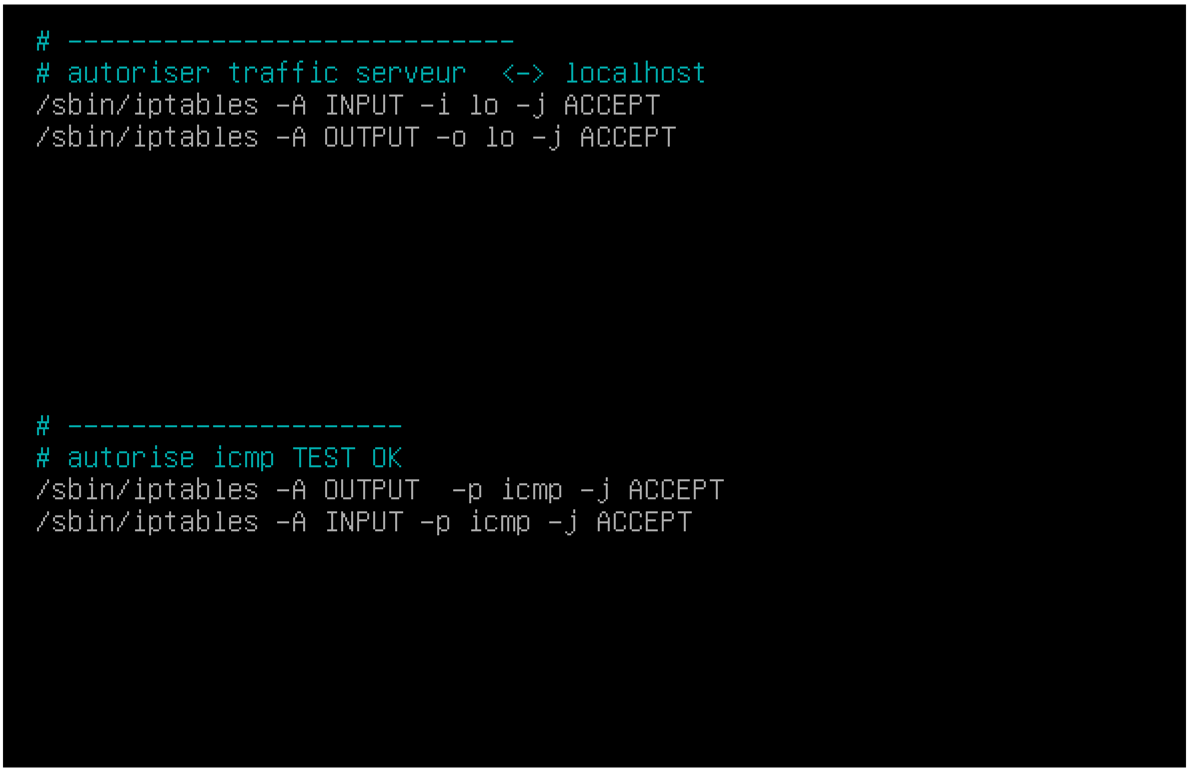
```
root@debian:/etc/init.d# nano firewall.sh_
```

Effacer les règles existantes et définir une politique de refus sur tout par défaut

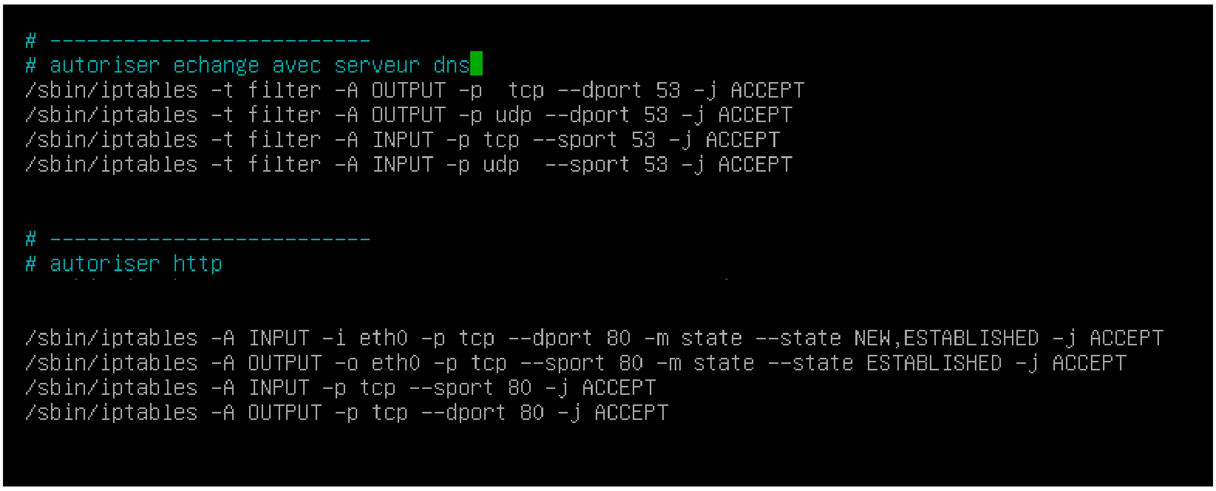


```
  GNU nano 2.2.6                   Fichier : firewall.sh

#!/bin/sh

# appelle iptables



# -----------------
# efface les regles existantes
# tables actuelles
/sbin/iptables -t filter -F
# regles personnelles
/sbin/iptables -t filter -X









# tout interdire
/sbin/iptables -P INPUT DROP
/sbin/iptables -P OUTPUT DROP
# /sbin/iptables -P FORWARD  DROP


#-------------------------------
```

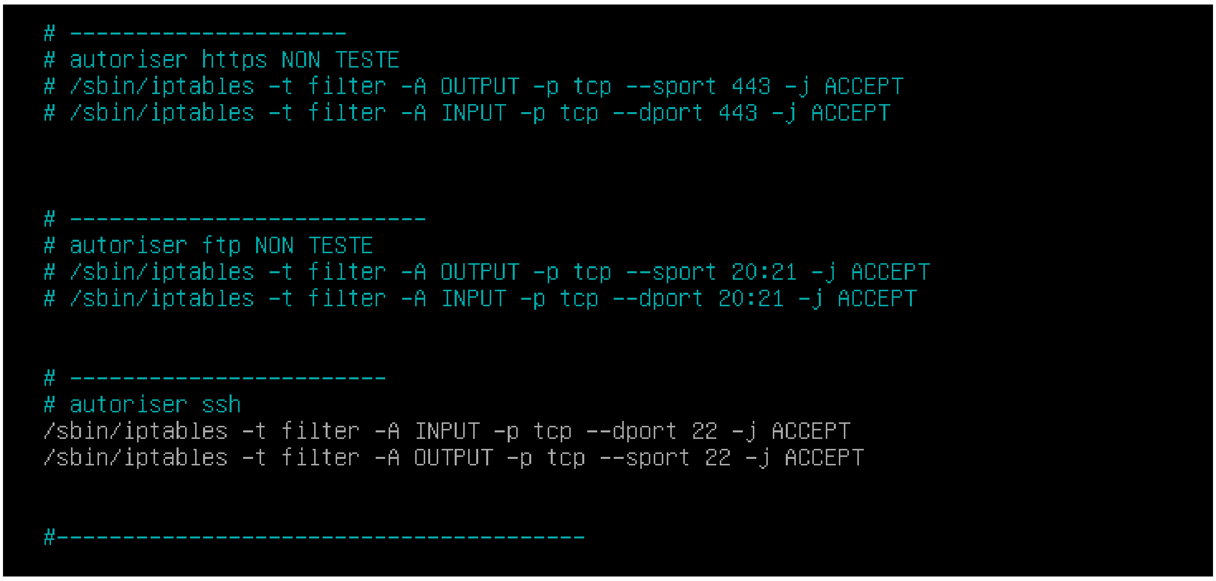
Appliquer des autorisations



```
# ----------------------------
# autoriser traffic serveur  <-> localhost
/sbin/iptables -A INPUT -i lo -j ACCEPT
/sbin/iptables -A OUTPUT -o lo -j ACCEPT




# ---------------------
# autorise icmp TEST OK
/sbin/iptables -A OUTPUT  -p icmp -j ACCEPT
/sbin/iptables -A INPUT -p icmp -j ACCEPT
```

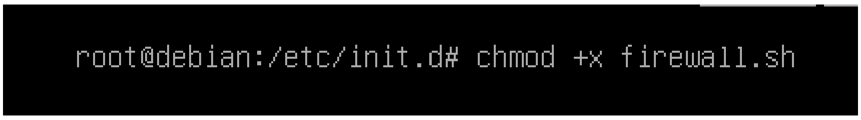


```
# -------------------------
# autoriser echange avec serveur dns
/sbin/iptables -t filter -A OUTPUT -p  tcp --dport 53 -j ACCEPT
/sbin/iptables -t filter -A OUTPUT -p udp --dport 53 -j ACCEPT
/sbin/iptables -t filter -A INPUT -p tcp --sport 53 -j ACCEPT
/sbin/iptables -t filter -A INPUT -p udp  --sport 53 -j ACCEPT


# -------------------------
# autoriser http


/sbin/iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
/sbin/iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
/sbin/iptables -A INPUT -p tcp --sport 80 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
```



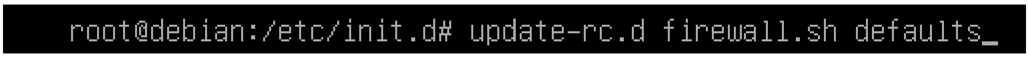
```
# ---------------------
# autoriser https NON TESTE
# /sbin/iptables -t filter -A OUTPUT -p tcp --sport 443 -j ACCEPT
# /sbin/iptables -t filter -A INPUT -p tcp --dport 443 -j ACCEPT



# ---------------------------
# autoriser ftp NON TESTE
# /sbin/iptables -t filter -A OUTPUT -p tcp --sport 20:21 -j ACCEPT
# /sbin/iptables -t filter -A INPUT -p tcp --dport 20:21 -j ACCEPT


# ------------------------
# autoriser ssh
/sbin/iptables -t filter -A INPUT -p tcp --dport 22 -j ACCEPT
/sbin/iptables -t filter -A OUTPUT -p tcp --sport 22 -j ACCEPT


#----------------------------------------
```

__Rendre le fichier script executable__



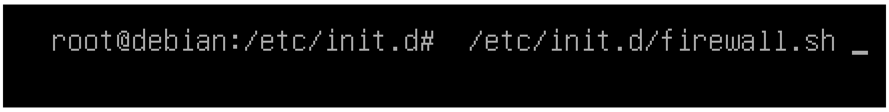
```
root@debian:/etc/init.d# chmod +x firewall.sh
```

__Charger le script au démarrage__



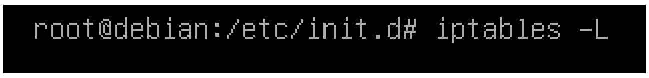
```
root@debian:/etc/init.d# update-rc.d firewall.sh defaults_
```

__Lancer manuellement le script__

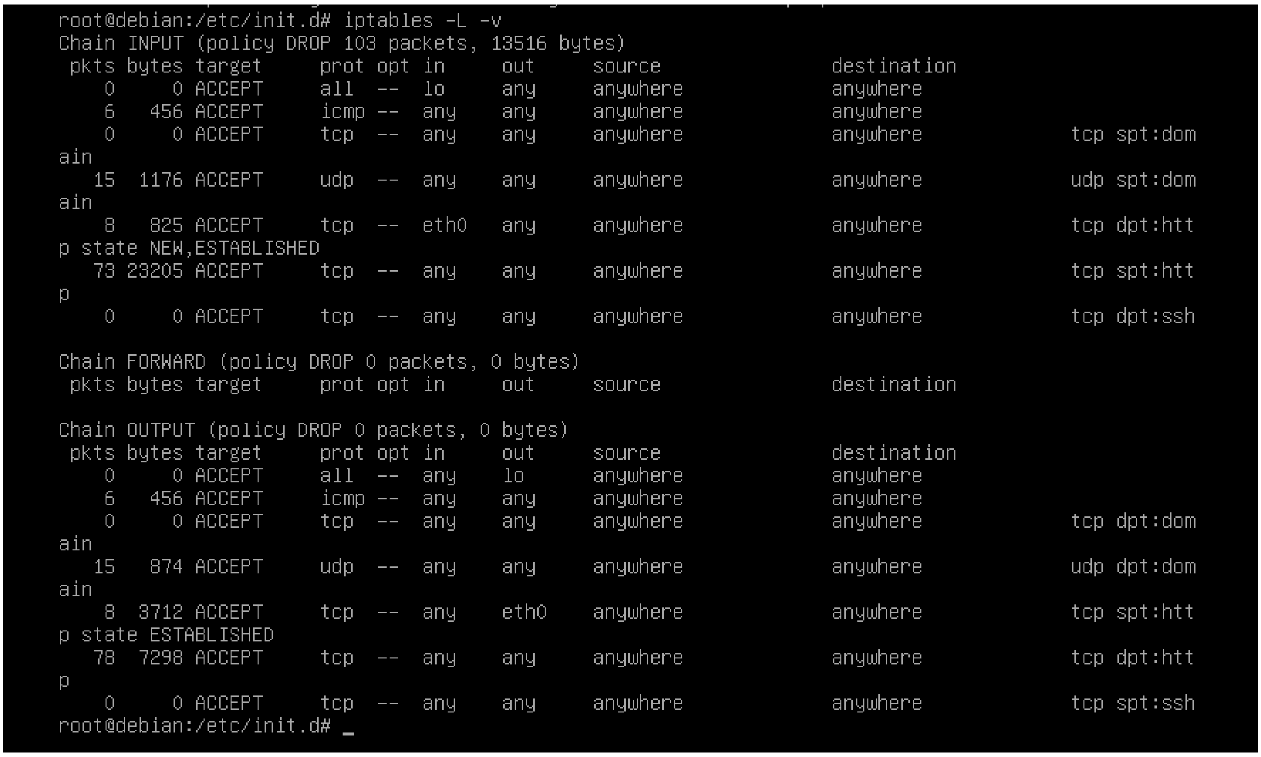


```
root@debian:/etc/init.d#  /etc/init.d/firewall.sh _
```

vérif



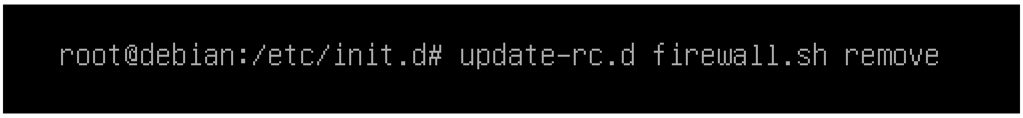
```
root@debian:/etc/init.d# iptables -L
```



```
root@debian:/etc/init.d# iptables -L -v
Chain INPUT (policy DROP 103 packets, 13516 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere
    6   456 ACCEPT     icmp --  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp spt:dom
ain
   15  1176 ACCEPT     udp  --  any    any     anywhere             anywhere             udp spt:dom
ain
    8   825 ACCEPT     tcp  --  eth0   any     anywhere             anywhere             tcp dpt:htt
p state NEW,ESTABLISHED
   73 23205 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp spt:htt
p
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:ssh

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

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  any    lo      anywhere             anywhere
    6   456 ACCEPT     icmp --  any    any     anywhere             anywhere
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:dom
ain
   15   874 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:dom
ain
    8  3712 ACCEPT     tcp  --  any    eth0    anywhere             anywhere             tcp spt:htt
p state ESTABLISHED
   78  7298 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:htt
p
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp spt:ssh
root@debian:/etc/init.d# _
```

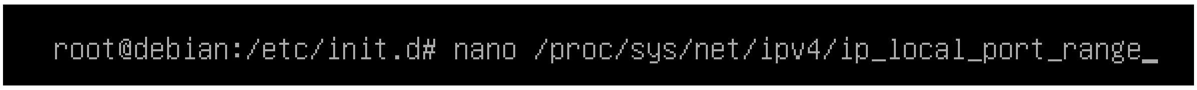
Ping, dig , netstat, nmap

Retirer du démarrage le script



```
root@debian:/etc/init.d# update-rc.d firewall.sh remove
```

++



```
root@debian:/etc/init.d# nano /proc/sys/net/ipv4/ip_local_port_range_
```