



Un firewall minimaliste

Le 1 février 2008, à 12:35 par Ulhume...

L'objectif de ce script est de mettre en place une protection minimum très rapidement.

Syntaxe

```
./firewall etat
```

etat

start|stop

Scripte

```
bin sh [1]

function start{
# vidage des regles
iptables -F
iptables -X
iptables -t nat -F

# chargement des modules kernel necessaires au FTP
sbin modprobe ip_nat_ftp
sbin modprobe ip_conntrack_ftp

# garde les connexions ouvertes
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# autorise les connexions SSH entrantes
iptables -A INPUT -p tcp --dport 22 -j ACCEPT

# autorise le ping (décommenter la ligne ci-dessous)
iptables -A INPUT -p icmp -j ACCEPT

# autorise les connexions HTTP entrantes
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT

# autorise les connexions SMTP et POP entrantes
iptables -A INPUT -p tcp --dport 25 -j ACCEPT
iptables -A INPUT -p tcp --dport 993 -j ACCEPT

# autorise les connexions Jabber entrantes
iptables -A INPUT -p tcp --dport 5222 -j ACCEPT
```

```
iptables -A INPUT -p tcp --dport 8000 -j ACCEPT
iptables -A INPUT -p udp --dport 8000 -j ACCEPT
```

```
iptables -A INPUT -p tcp --dport 21 -j ACCEPT
```

bloquer les connexions entrantes

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
```

bloquer les connexions sortantes

```
iptables -P OUTPUT DROP
```

autoriser loopback

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

```
iptables -A INPUT -i tun1 -j ACCEPT
iptables -A OUTPUT -o tun1 -j ACCEPT
```

connexions sortantes autorisées (FTP, DNS, HTTP, HTTPS) pour les mises-à-jour

```
iptables -A OUTPUT -p tcp --dport 20 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 21 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT
iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
```

connexions SMTP, POP et IMAP sortantes autorisées

```
iptables -A OUTPUT -p tcp --dport 25 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 110 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 143 -j ACCEPT
```

connexions NTP sortantes autorisées

```
iptables -A OUTPUT -p tcp --dport 123 -j ACCEPT
iptables -A OUTPUT -p udp --dport 123 -j ACCEPT
```

connexions SSH sortantes autorisées

```
iptables -A OUTPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p udp --dport 22 -j ACCEPT
```

connexions WHOIS sortantes autorisées

```
iptables -A OUTPUT -p tcp --dport 43 -j ACCEPT
```

connexions USENET sortantes autorisées

```
iptables -A OUTPUT -p tcp --dport 119 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 8000 -j ACCEPT
iptables -A OUTPUT -p udp --dport 8000 -j ACCEPT
}
```

```
function stop {
#!/bin/sh
```

vidage des règles

```

iptables -F
iptables -X
iptables -t nat -F

# chargement des modules kernel necessaires au FTP
sbin modprobe ip_nat_ftp
sbin modprobe ip_conntrack_ftp

# garde les connexions ouvertes
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# bloque les connexions entrantes
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT

# bloque les connexions sortantes
iptables -P OUTPUT ACCEPT

# autorise loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
}

case "$1" in
    start
        start_firewall

    stop
        stop_firewall

    )
        gprintf usage: $s start|stop|restart|status}\n" $0
    exit 1
esac

```

Liens:

[1] <http://pwet.fr/man/linux/commandes/sh>