

## **FIREWALL SU UN GATEWAY by Daniele Veratti (danielev83@yahoo.it)**

```
iptables -F # flush
iptables -P INPUT DROP # imposto la policy a DROP su tutte le
iptables -P OUTPUT DROP # catene
iptables -P FORWARD DROP
iptables -A INPUT # accetto i pacchetti in ingresso
    -s 127.0.0.1 # su loopback (lo)
    -j ACCEPT
iptables -A OUTPUT # accetto pacchetti in uscita su lo
    -d 127.0.0.1
    -j ACCEPT
iptables -A FORWARD #permetto ai pacchetti provenienti da una
    -s 192.168.1.128/255.255.255.128 # mia sottorete(con i client)
    -d 192.168.1.4 # di attraversare per la posta verso
    -p tcp # il mio server di posta
    --destination-port 25
    -j ACCEPT
iptables -A FORWARD # permetto a tutta la sottorete di
    -s 192.168.1.128/255.255.255.128 # collegarsi a un web
    -p tcp # server qualsiasi (TCP port 80)
    --destination-port 80
    -j ACCEPT
iptables -A FORWARD # consento il ritorno dei pacchetti
    -d 192.168.1.128/255.255.255.128 # richiesti all'esterno
    -p tcp
    --state ESTABLISHED
    -j ACCEPT
iptables -A FORWARD # consento l'invio di pacchetti tcp al
    -s 192.168.1.128/255.255.255.128 # mio DNS server (porta 53)
    -d 192.168.1.3
    -p tcp
    --destination-port 53
    -j ACCEPT
iptables -A FORWARD # consento l'invio di pacchetti udp
    -s 192.168.1.128/255.255.255.128 # al server DNS (p 53)
    -d 192.168.1.3
    -p udp
    --destination-port 53
    -j ACCEPT
iptables -A FORWARD # accetto pacchetti da parte del mio DNS
    -d 192.168.1.128/255.255.255.128 # verso la sottorete
    -s 192.168.1.3 # sulla porta tcp 53
    -p tcp
    --source-port 53
    -j ACCEPT
iptables -A FORWARD # come sopra ma il protocollo usato è UDP
    -d 192.168.1.128/255.255.255.128
    -s 192.168.1.3
    -p udp
    --source-port 53
    -j ACCEPT
```

---

Disclaimer: questo documento è stato scritto da Daniele Veratti (daniele@danieleveratti.com - danielev83@yahoo.it).

E' liberamente utilizzabile,scaricabile e stampabile, ricordatevi solo di citare il mio nome se apportate modifiche e/o pubblicate questo documento o parte di esso sul vostro sito e/o spazio web.