```
#!/bin/bash

#Mette a 1 un flag del kernel per abilitare il forward attraverso il firewall.
#In alcune distribuzioni al riavvio viene rimesso a 0, per cui si può inserire questo comando nello script per reimpostarlo dopo ogni riavvio.
echo "1" > /proc/sys/net/ipv4/ip_forward

#Se non si specifica l'opzione –t il comando di default si riferisce alla tabella filter
iptables -F
iptables -F -t nat
iptables -F -t mangle

# Ripulisce tutte le catene custom, create e personalizzate dall'utente
iptables –X

#Azzera i contatori sulle catene
iptables -Z

#Imposto le policy di default
#Queste policy per semplicità permettono tutto il traffico in uscita dal firewall, cosa solitamente non rischiosa. Se si imposta DROP di default nella catena OUTPUT, si dovrà aprire singolarmente ogni tipo di dati che devono uscire.
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD DROP

#Abilito tutto il traffico su loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

#Regole prevenzione syn-flood
#Si limita la quantità di pacchetti con flag syn a 1. Queste con i limiti sono regole che richiedono buone prestazioni del server, che deve tenere il conto dei pacchetti che passano.
iptables -A FORWARD -p tcp --syn -m limit --limit 1/second -j ACCEPT

#Regole prevenzione port-scanner
iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/second -j ACCEPT

#Nat degli IP della LAN per uscire in Internet. Serve per mascherare gli IP locali della LAN, i cui pacchetti altrimenti sarebbero droppati dal primo router incontrato in Internet.
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE

#Abilito la connessione ssh con max 1 connessione al minuto, per limitare eventuali attacchi a "forza bruta" finalizzati a trovare la password eseguendo tutti i tentativi.
iptables -A INPUT -p tcp --dport 22 -m limit --limit 1/minute --limit-burst 1 -j ACCEPT

#Accetto in uscita connessioni nuove e già stabilite, in entrata solo le stabilite
iptables -A FORWARD -o eth1 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -i eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT

#Giro il traffico indirizzato alla porta 80 sulla porta 80 di un server nella LAN. In questo caso necessito di permettere l'attraversamento del firewall ai dati.
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to 10.0.0.10:80
iptables -A FORWARD -i eth1 -p tcp --dport 80 -d 10.0.0.10 -j ACCEPT

#Giro la porta 80 sulla porta 80 del server web che e' in DMZ. In questo caso non c'è bisogno di permettere il FORWARD perché i dati rimbalzano sulla scheda di rete esterna del firewall senza attraversarlo.
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to 192.168.1.101:80
```