iptables:

iptables -A(APPEND) input -p tcp --dport 22 -j accept (accept packet ssh)

iptables -i(INSERT) input 1 -p tcp --dport 22 -j accept

iptables --policy input drop (all packet, if no rule match to theme, drop)

iptables -A input -p tcp -s 192.168.1.1 --dport 22 -i(input interface) ens33 -j drop( all packet from ip(192.168.1.1) and port(22) drop)

iptables -A input -p tcp --syn --dport 22 -m connlimit --connlimit\_above 2 -j drop

-m iprange --src-range 192.168.1.100-192.168.1.120

-m time --timestart 09:00 --timestop 18:00 --days mon,tue,wed,thu,fri

what's different between DROP and REJECT:

- In REJECT we show message to client but not in DROP

iptables -A input -p tcp -s ipaddr --dport portno -j log

 ham log giri ham drop

iptables -A input -p tcp -s ipaddr --dport portno -j drop

iptables-save > path\_to\_save\_file

iptables-restore < read\_path\_save\_file-iptables

echo 1 > /proc/sys/net/ipv4/ip-forward enable-routing

iptables -t nat -A postrouting -s ipaddr\_out\_side -o adapter-outside -j masqurade

iptables -A forward -i input\_adapter-with-internet -o output\_adapter-without-internet -j accept