**IP-Tables setup on Cent-OS**

Document Version 1.0  
Prepared by

**Lekshminarayanan K**

***Check the existing rules:***

iptables -S

***Enable SSH access for our IP***

iptables -A INPUT -s 192.168.4.13 -p tcp --dport 22 -j ACCEPT

iptables -A INPUT -s 192.168.4.0/32 -p tcp --dport 22 -j ACCEPT

***Accept all established inbound connections:***

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

***Allow HTTP and HTTPS inbound traffic:***

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -p tcp --dport 443 -j ACCEPT

***Allow DNS queries:***

iptables -A INPUT -p udp --dport 53 -j ACCEPT

iptables -A INPUT -p tcp --dport 53 -j ACCEPT

***At last, set the default policies:***

iptables -P INPUT DROP

iptables -P OUTPUT ACCEPT

iptables -P FORWARD DROP

***Delete rule by seeing its number.***

iptables -L --line-numbers

13 ACCEPT tcp -- 192.168.4.13 anywhere tcp dpt:ssh state NEW,ESTABLISHED

14 ACCEPT tcp -- 192.168.4.90 anywhere tcp dpt:ssh state NEW,ESTABLISHED

***If i need to delete the rule 13th i will just delete by below.***

iptables -D INPUT 20

***Work logs.***

iptables -A INPUT -s 192.168.4.13 -p tcp --dport 22 -j ACCEPT

iptables -A INPUT -i lo -j ACCEPT

iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP

iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

iptables -A INPUT -p tcp --dport 443 -j ACCEPT

iptables -A INPUT -p udp --dport 123 -j ACCEPT

iptables -A INPUT -p udp --dport 53 -j ACCEPT

iptables -A INPUT -p tcp --dport 53 -j ACCEPT

iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

iptables -A INPUT -i eth0 -p tcp -s 192.168.4.13 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

iptables -P INPUT DROP

iptables -P OUTPUT ACCEPT

iptables -P FORWARD DROP

iptables -A INPUT -i eth0 -p tcp -s 192.168.4.90 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A INPUT -i eth0 -p tcp -s 192.168.1.115 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -L --line-numbers

iptables -D INPUT 20

service iptables save

***If you want to make changes to an iptables configuration, it is always good idea to save the current configuration by typing the following commands:***

save

iptables-save > /root/working.iptables.rules

restore

iptables-restore < /root/working.iptables.rules