Install iptables

“Sudo apt install iptables”

Set default policies

“sudo iptables -P INPUT DROP”

“sudo iptables -P FORWARD DROP”

“sudo iptables -P OUTPUT ACCEPT”

Allow incoming traffic on port 80 (HTTP)

“sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT”

Allow incoming traffic onn port 443 (HTTP)

“sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT”

Allow established and related connections

“sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT”

Save set rules.

“sudo iptables-save | sudo tee /etc/iptables/rules.v4”

Use the following command to ALLOW SSH access (port 22) only from 192.168.1.5 used for administration.

“sudo iptables -A INPUT -p tcp -s 192.168.1.5 --dport 22 -j ACCEPT”

Use the following command to allow specific application.

“sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT”

Use the following commands to allow ping request (ICMP Echo Request)

“sudo iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT”

Use the following command to allow printing traffic only from 192.168.1.5

“sudo iptables -A INPUT -p tcp -s 192.18.1.5 --dport 9100 -j ACCEPT”