Subject: Implementation of Host Firewalls on Linux Servers

To Management,

I am writing to report on the implementation of host firewalls on our Linux servers. The objective of this implementation was to control inbound packets to only permit those that are expected.

In order to achieve this objective, I used the iptables firewall tool on each Linux server. I created firewall policies using the following command: “sudo iptables -A INPUT -s 172.20.242.101 -p tcp --destination-port 22 -j DROP”

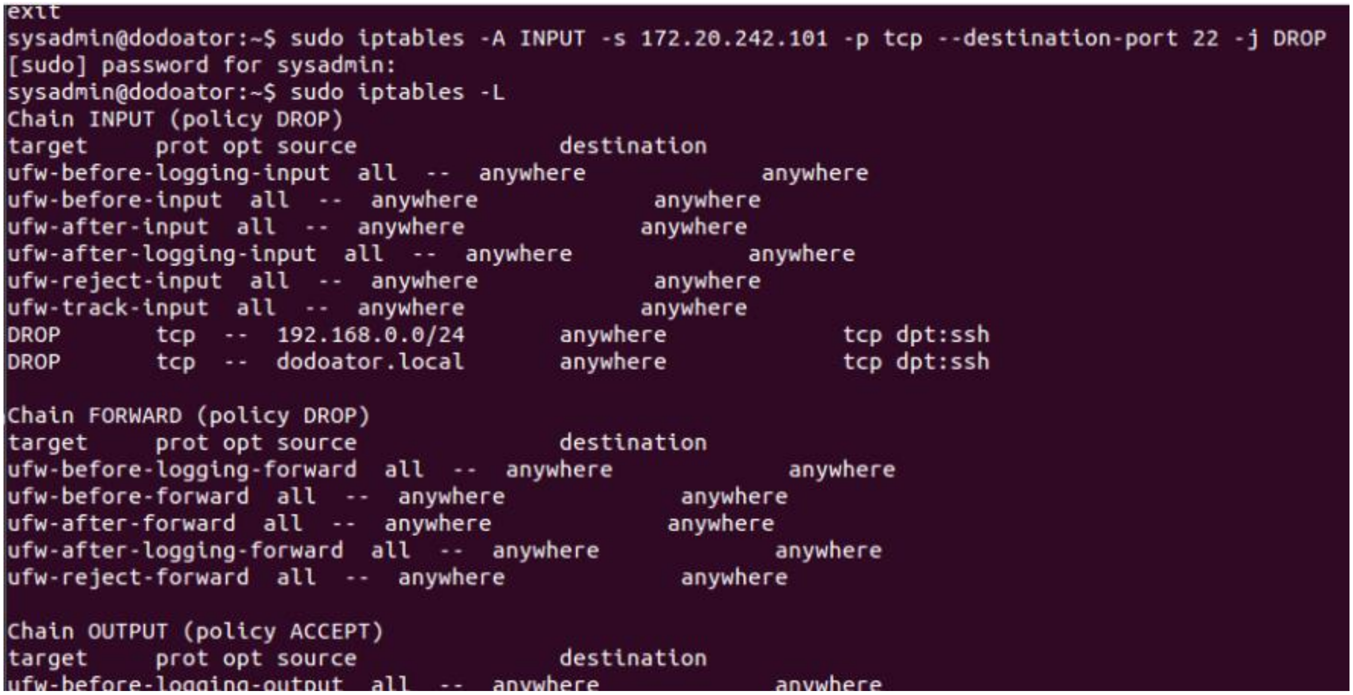
This command blocks inbound SSH (port 22) packets from IP address 172.20.242.101. All other inbound packets are permitted.

Please find attached screenshots of the server configuration used to implement these firewall policies, as well as log entries showing packets not fitting the profile being denied.

If you have any questions or need further information, please do not hesitate to reach out to me.

Best regards,

Group 9



```
exit
sysadmin@dodoator:~$ sudo iptables -A INPUT -s 172.20.242.101 -p tcp --destination-port 22 -j DROP
[sudo] password for sysadmin:
sysadmin@dodoator:~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ufw-before-logging-input  all  --  anywhere             anywhere
ufw-before-input  all  --  anywhere             anywhere
ufw-after-input  all  --  anywhere             anywhere
ufw-after-logging-input  all  --  anywhere             anywhere
ufw-reject-input  all  --  anywhere             anywhere
ufw-track-input  all  --  anywhere             anywhere
DROP       tcp  --  192.168.0.0/24       anywhere             tcp dpt:ssh
DROP       tcp  --  dodoator.local       anywhere             tcp dpt:ssh

Chain FORWARD (policy DROP)
target     prot opt source               destination
ufw-before-logging-forward  all  --  anywhere             anywhere
ufw-before-forward  all  --  anywhere             anywhere
ufw-after-forward  all  --  anywhere             anywhere
ufw-after-logging-forward  all  --  anywhere             anywhere
ufw-reject-forward  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ufw-before-logging-output  all  --  anywhere             anywhere
```