Задание:
Настройте правила iptables для создания базового файрвола на сервере. Разрешите доступ только к службам SSH (порт 22), HTTP (порт 80) и HTTPS (порт 443). Ограничьте доступ с определенных IP-адресов к вашему серверу, и запретите весь остальной входящий трафик. В качестве решения предоставьте список команд для настройки и продемонстрируйте вывод команды iptables -L

Очищаем правила iptables:

```
vagrant@ubuntu-jammy:~$ sudo iptables -F
vagrant@ubuntu-jammy:~$ sudo iptables -X
vagrant@ubuntu-jammy:~$ sudo iptables -Z
```

Вывод команды iptables -L до настройки:

```
vagrant@ubuntu-jammy:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Команды для настройки правил iptables:

```
vagrant@ubuntu-jammy:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
vagrant@ubuntu-jammy:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
vagrant@ubuntu-jammy:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
vagrant@ubuntu-jammy:~$ sudo iptables -A INPUT -s 192.168.20.111 -j DROP
vagrant@ubuntu-jammy:~$ sudo iptables -A INPUT -s 192.168.22.113 -j DROP
```

Вывод команды iptables -L после настройки:

```
vagrant@ubuntu-jammy:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
DROP       all  --  192.168.20.111       anywhere
DROP       all  --  192.168.22.113       anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
```

target prot opt source destination

Вывод команды iptables -L -n -v после настройки:

```
vagrant@ubuntu-jammy:~$ sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 84 packets, 4980 bytes)
 pkts bytes target     prot opt in     out     source               destination
   97  5912 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
    0     0 DROP       all  --  *      *       192.168.20.111       0.0.0.0/0
    0     0 DROP       all  --  *      *       192.168.22.113       0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```