### **Задание 1: Настройка базовых правил фаервола с использованием iptables**

1. **Открыть терминал:**

sudo -i

1. **Просмотреть текущие правила iptables:**

iptables -L -v -n

1. **Разрешить входящий трафик на порт 22 (SSH):  
   3.**  iptables -A INPUT -p tcp --dport 22 -j ACCEPT
2. **Разрешить входящий трафик на порт 80 (HTTP):  
   4.**  iptables -A INPUT -p tcp --dport 80 -j ACCEPT
3. **Заблокировать весь остальной входящий трафик:**

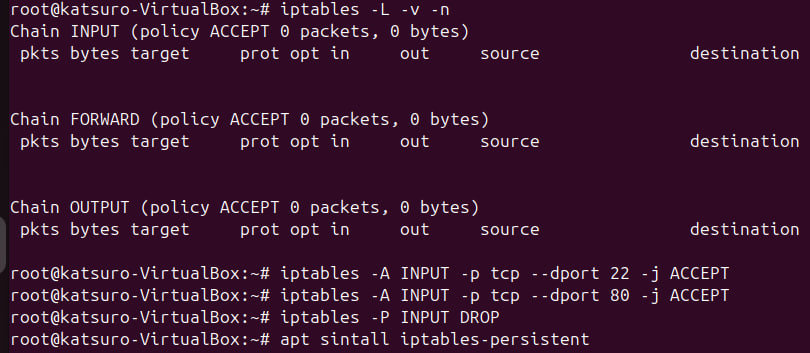
iptables -P INPUT DROP

1. **Сохранить правила:**

apt install iptables-persistent

netfilter-persistent save

Или сохраните вручную:  
 iptables-save > /etc/iptables/rules.v4

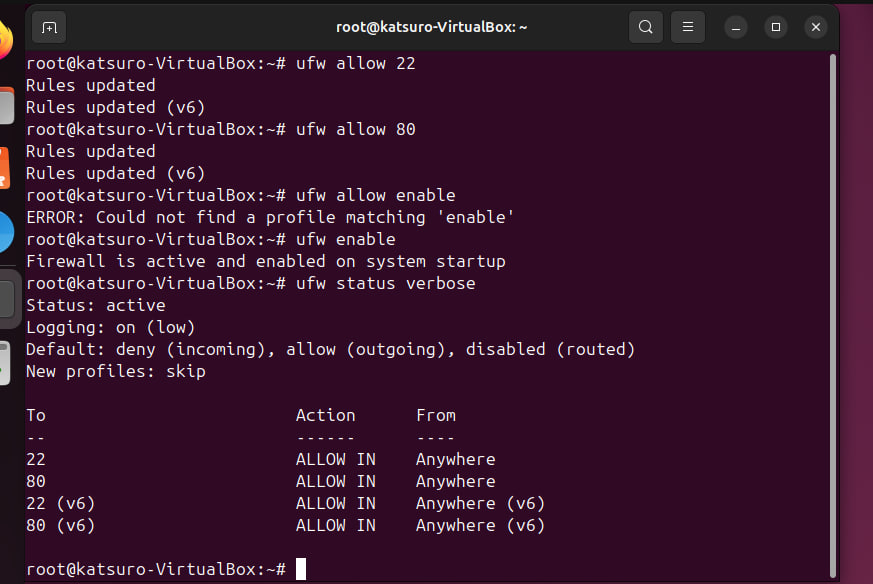


### **Задание 2: Настройка фаервола с использованием ufw**

1. **Установить ufw (если не установлен):** sudo apt update

sudo apt install ufw

1. **Разрешить входящий трафик на порт 22 (SSH):** sudo ufw allow 22
2. **Разрешить входящий трафик на порт 80 (HTTP):** sudo ufw allow 80
3. **Включить ufw:** sudo ufw enable
4. **Просмотреть текущие правила:** sudo ufw status verbose



### **Задание 3: Настройка правил для управления исходящим трафиком**

1. **Разрешить исходящий трафик на порт 80 (HTTP):**

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

1. **Заблокировать весь остальной исходящий трафик:**

iptables -P OUTPUT DROP

1. **Сохранить правила (аналогично Заданию 1, шаг 6).**

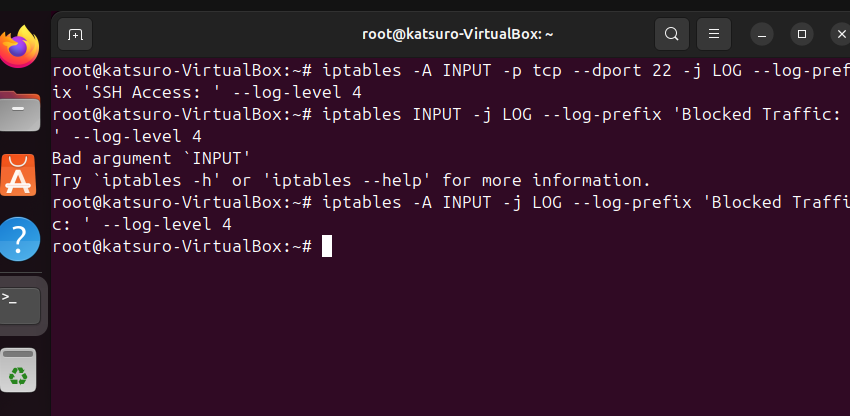
### **Задание 4: Настройка логирования трафика с использованием iptables**

1. **Логирование входящего трафика на порт 22 (SSH):**

iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix "SSH Access: " --log-level 4

1. **Логирование заблокированного трафика:**

iptables -A INPUT -j LOG --log-prefix "Blocked Traffic: " --log-level 4



### **Задание 5: Настройка правил NAT с использованием iptables**

1. **Включить форвардинг IP-пакетов:**

Отредактируйте /etc/sysctl.conf:  
 echo "net.ipv4.ip\_forward = 1" >> /etc/sysctl.confsysctl -p

1. **Настроить правило для преобразования исходящих IP-адресов (SNAT/MASQUERADE):** iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
2. **Сохранить правила (аналогично Заданию 1, шаг 6).**

### **Задание 6: Проверка и тестирование правил фаервола**

1. **Просмотреть текущие правила фаервола:**

Для iptables:

iptables -L -v -n

Для ufw:  
sudo ufw status verbose

1. **Проверить доступность сервисов (например, SSH, HTTP):**

Используйте telnet:  
telnet <IP-адрес> 22

Или curl:  
curl http://<IP-адрес>

1. **Убедиться, что нежелательный трафик блокируется:**Попробуйте доступ к закрытым портам или сервисам с других устройств.