**Настройка сервиса блокирования сетевых портов iptables**

Конфигурация сетевого экрана iptables может быть сложной задачей, но следуя некоторым базовым правилам, мы можем с лёгкостью настроить правила блокирования портов в Linux.

**1.Создание правила блокирования порта**

Для создания правила блокирования порта в iptables, требуется выполнение следующей команды:

sudo iptables -I INPUT -p tcp --dport PORT\_NUMBER -j DROP

где PORT\_NUMBER - порт, который необходимо заблокировать.

Для примера, блокирование порта 80 (HTTP) должно выглядеть так:

sudo iptables -A INPUT -p tcp --dport 80 -j DROP

Блок INPUT — это входящие на сервер запросы, OUTPUT — исходящие.   
А FORWARD — перенаправление запросов на шлюз, на внутренний IP-адрес на определённом интерфейсе, т. е. маршрутизация пакетов в локальной сети.

Где атрибуты:

-I INPUT — для того, чтобы вставить новое правило в список

-i — через какой сетевой интерфейс

-p и --dport — описывает протокол и порт

-j — описывает цель правила (DROP, ACCEPT, REJECT)

Дополнительные атрибуты можно посмотреть [тут](https://www.opennet.ru/man.shtml?topic=iptables&category=8&russian=0).

**2.Сохранение правил iptables**

Чтобы сохранить правила iptables, нужно выполнить команду:

sudo iptables-save > /etc/iptables/rules.v4

Эта команда сохранит текущее состояние правил iptables в /etc/iptables/rules.v4.

**3.Настройка правил iptables для автозагрузки системы**

Нужно создать скрипт, чтобы выполнять сохранённое состояние iptables при загрузке системы.

Для этого:

1. Создайте новый файл в каталоге /etc/network/if-pre-up.d/ и назовите его, например, iptables-rules:

sudo nano /etc/network/if-pre-up.d/iptables-rules

1. Добавьте следующий код со ссылкой на файл, содержащий сохранённые правила iptables:

#!/bin/bash

iptables-restore < /etc/iptables/rules.v4

exit 0

1. Сохраните и закройте файл
2. Перезагрузите систему для применения настроек — они будут автоматически применены при загрузке системы
3. Проверьте успешность соединения с заблокированным портом

После перезагрузки системы можно использовать команду iptables -L для проверки действующих правил iptables. Если правила настроены правильно, соединение с заблокированным портом должно отбрасываться.

Конфигурация iptables может быть сложной, поэтому необходимо быть осторожным при изменении или удалении правил, чтобы не повредить работу сети. Желательно регулярно сохранять состояние правил и тестировать сетевые соединения после каждого изменения.