**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Вычислительные сети»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

«Настройка межсетевого экрана»

**Выполнили:**

Ахраров Али, студент группы N3350

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

(подпись)

**Проверил:**

Бучаев Абдулхамид Яхъяевич

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

Содержание

[1 Настройка межсетевого экрана 4](#_Toc192268750)

[1.1 Введение 4](#_Toc192268751)

[1.2 Схема лабораторного стенда 4](#_Toc192268752)

[1.3 Конфигурация межсетевого экрана 4](#_Toc192268753)

[1.3.1 Предварительная настройка 4](#_Toc192268754)

[1.3.2 Блокировка исходящего трафика (разрешены только порты SSH, HTTP, HTTPS) 4](#_Toc192268755)

[1.3.3 Фильтрация пакетов по размеру и TTL 5](#_Toc192268756)

[1.3.4 Настройка трансляции адресов (NAT) 5](#_Toc192268757)

[1.3.5 Защита от brute-force атак на SSH 5](#_Toc192268758)

[1.3.6 Скриншот конфигурации 5](#_Toc192268759)

[1.4 Результаты тестирования 5](#_Toc192268760)

[1.5 Выводы 6](#_Toc192268761)

# ****Настройка** **межсетевого** **экрана****

## Введение

Целью лабораторной работы является изучение принципов работы межсетевого экрана (firewall) на примере netfilter/iptables в Linux. В ходе работы необходимо:

* Настроить лабораторный стенд, включающий локальный сервер (Firewall), клиент и удалённый сервер;
* Организовать маршрутизацию проходящего трафика на локальном сервере;
* Выполнить настройку правил межсетевого экрана согласно заданию (блокировка исходящего трафика, фильтрация пакетов по размеру и TTL, настройка трансляции адресов, защита от brute-force атак на SSH);
* Провести тестирование настроенных правил и зафиксировать результаты.

## Схема лабораторного стенда

В лабораторном стенде используется следующая топология:

* **Firewall-1** – сервер Linux, выполняющий функции межсетевого экрана, имеет два интерфейса:
  + Внешний интерфейс с IP-адресом 192.168.100.1 (подключён к сети External);
  + Внутренний интерфейс с IP-адресом 10.0.0.1 (подключён к сети Internal).
* **External-1** – клиент с IP-адресом 192.168.100.2, подключённый к внешней сети.
* **Internal-1** (и/или Server-1) – внутренний сервер с IP-адресом 10.0.0.2 (или 10.0.0.3), подключённый к внутренней сети.

Стенд реализован в среде GNS3, где подключение между виртуальными машинами осуществляется через L2-свитчи.

## Конфигурация межсетевого экрана

На Firewall-1 выполнена настройка iptables в соответствии с вариантом задания (вариант 1). Ниже приведён перечень основных команд настройки:

### Предварительная настройка

# Включение маршрутизации

sudo sysctl -w net.ipv4.ip\_forward=1

echo "net.ipv4.ip\_forward=1" | sudo tee -a /etc/sysctl.conf

### Блокировка исходящего трафика (разрешены только порты SSH, HTTP, HTTPS)

sudo iptables -F

sudo iptables -t nat -F

sudo iptables -P INPUT ACCEPT

sudo iptables -P FORWARD ACCEPT

sudo iptables -P OUTPUT DROP

sudo iptables -A OUTPUT -p tcp --dport 22 -j ACCEPT

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

sudo iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT

sudo iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

### Фильтрация пакетов по размеру и TTL

sudo iptables -A INPUT -m length --length 601:65535 -m ttl --ttl-gt 10 -j DROP

sudo iptables -A FORWARD -m length --length 601:65535 -m ttl --ttl-gt 10 -j DROP

### Настройка трансляции адресов (NAT)

sudo iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE

Примечание: если NAT не требуется, этот шаг можно пропустить.

### Защита от brute-force атак на SSH

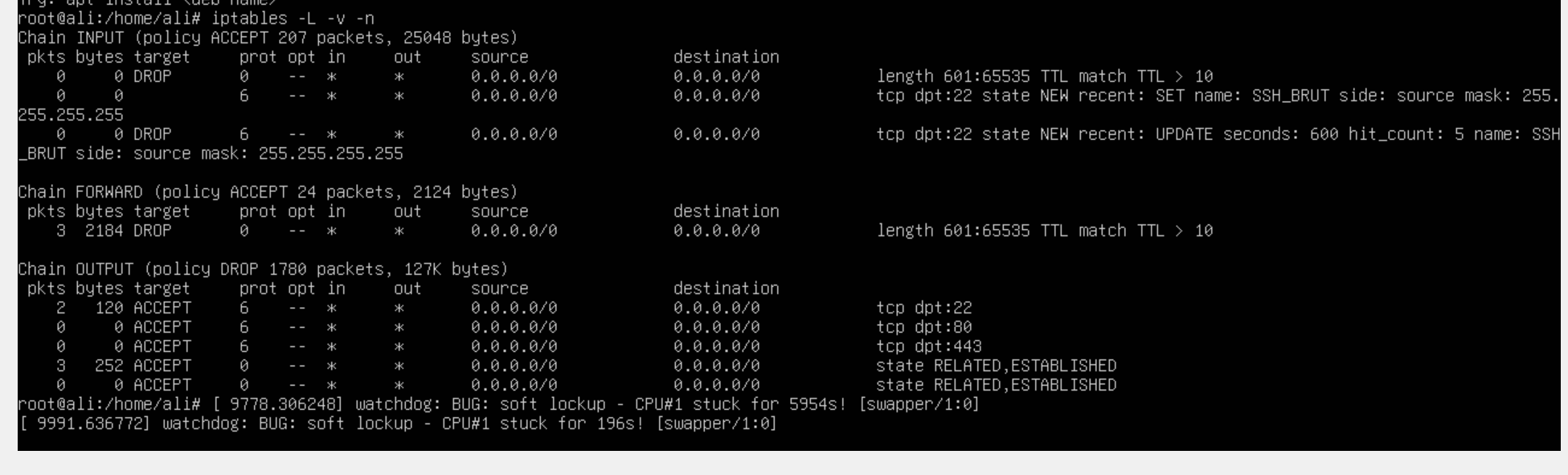
sudo iptables -N SSH\_BRUTE\_PROTECT

sudo iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set --name SSH\_ATTACK --rsource

sudo iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 600 --hitcount 5 --name SSH\_ATTACK --rsource -j DROP

### Скриншот конфигурации

sudo iptables -L -v -n && sudo iptables -t nat -L -v -n



1. Результат настройки iptables

## Результаты тестирования

В ходе тестирования выполнены следующие проверки:

* **Проверка исходящего трафика:**  
  Из Firewall-1 выполнены тесты подключения по SSH, HTTP и HTTPS, что подтвердило, что только разрешённые порты пропускаются, а остальные – блокируются (проверено с помощью curl и ssh).
* **Проверка фильтрации пакетов:**  
  С внешней и внутренней сетей отправлялись пакеты с увеличенным размером (более 600 байт) и высоким TTL (>10). Ответы на такие запросы отсутствовали, что подтверждает срабатывание правил.
* **Проверка защиты от brute-force SSH:**  
  При многократных попытках подключения по SSH с одного IP адреса Firewall-1 блокировал дальнейшие соединения в течение заданного интервала (10 минут).

## Выводы

В ходе лабораторной работы были изучены основные механизмы работы межсетевого экрана в Linux с использованием iptables. Выполненная настройка позволила:

* Ограничить исходящий трафик, разрешив только трафик для SSH, HTTP и HTTPS.
* Реализовать фильтрацию пакетов по размеру и TTL, что повышает защиту от определённых атак.
* Настроить NAT (трансляцию адресов) для обеспечения выхода внутренней сети во внешнюю.
* Обеспечить защиту от brute-force атак на SSH-сервис с помощью модуля recent.