Міністерство освіти і науки України
Національний авіаційний університет
Факультет кібербезпеки, комп'ютерної та програмної інженерії
Кафедра комп'ютеризованих систем управління

Лабораторна робота № 1.6
з дисципліни «Захист інформації в комп'ютерних системах»
на тему «Налаштування міжмережевих екранів»

Виконав:
студент ФККПІ
групи СП-425
Клокун В. Д.
Перевірила:
Супрун О. М.

Київ 2019

1. Мета роботи

Ознайомитись з основними принципами функціонування міжмережевих екранів та їх настроювання.

2. Завдання роботи

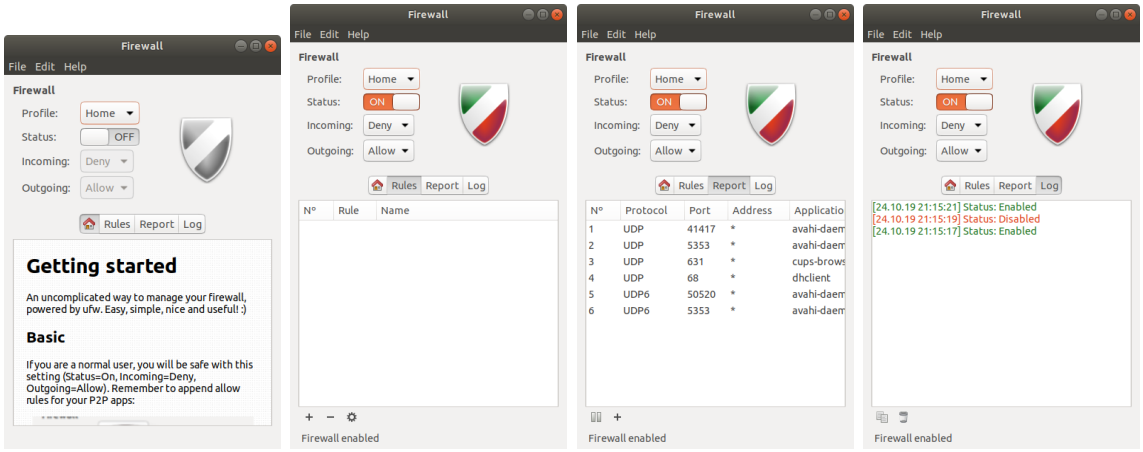
Встановити та настроїти програмне забезпечення міжмережевого екрану; сконфігурувати програмне забезпечення `iptalbes` для раціональної обробки мережевих пакетів.

3. Хід роботи

Щоб розпочати роботу, необхідно встановити програму `gufw` — інтерфейс для програми `iptables`. Для цього виконуємо таку команду:

```
sudo apt install gufw
```

Коли команда завершить роботу, в операційній системі буде встановлена програма `gufw`. Розглянемо встановлену програму. Для цього запустимо її і ознайомимось з інтерфейсом (рис. 1).

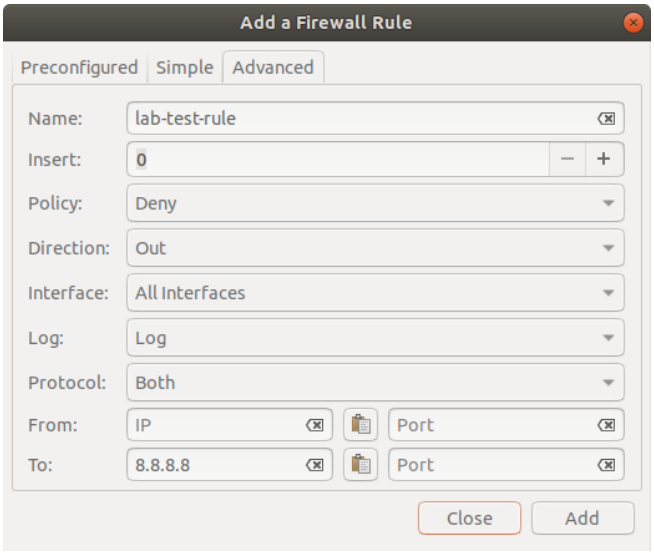


а) б) в) г)

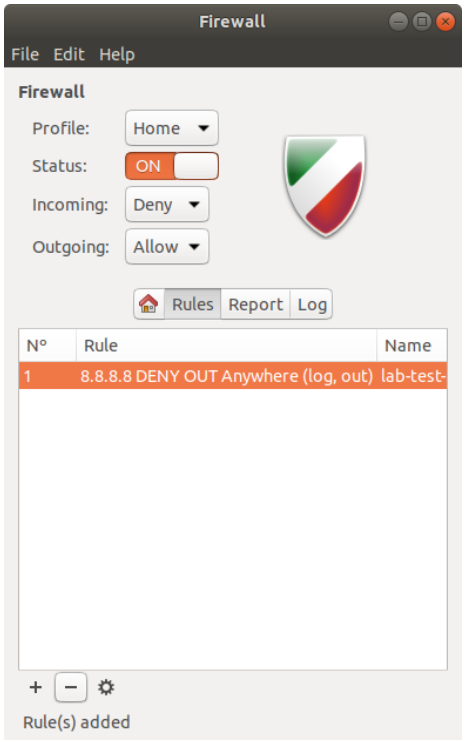
Рис. 1: Інтерфейс програми `gufw`

Основними елементами головного вікна програми є чотири вікна: «Домашня сторінка», «Правила», «Звіт» та «Логи». На домашній сторінці розказано, як користуватись програмою. Вкладка «Правила» містить правила міжмережевого екрана. На вкладці «Звіт» показані вхідні підключення, які намагались встановити ззовні. На вкладці «Логи» міститься інформація про роботу з міжмережевим екраном: включення, виключення, зміни правил та інші події.

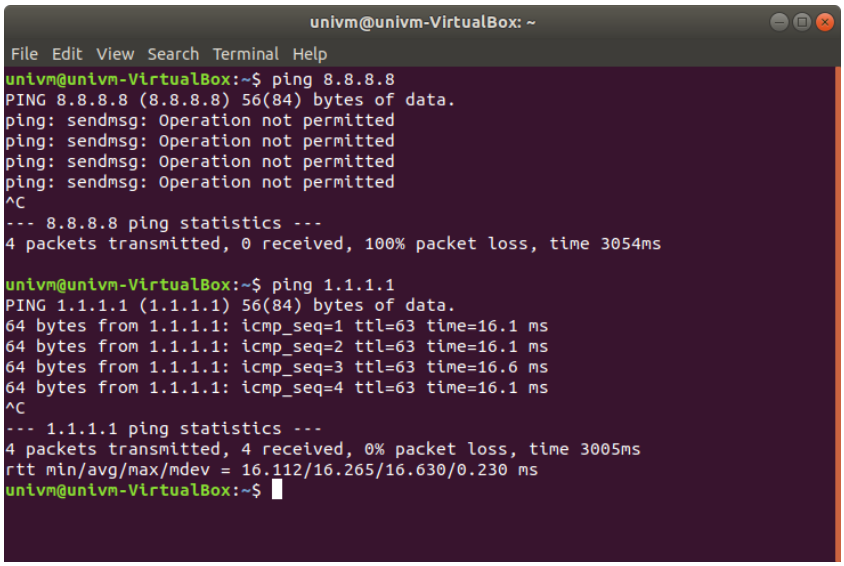
Щоб перевірити роботу встановленого інтерфейсу до міжмережевого екрану, створимо правило, яка блокуватиме вихідні підключення до вузла з IP-адресою 8.8.8.8 (рис. 2).



а)



б)

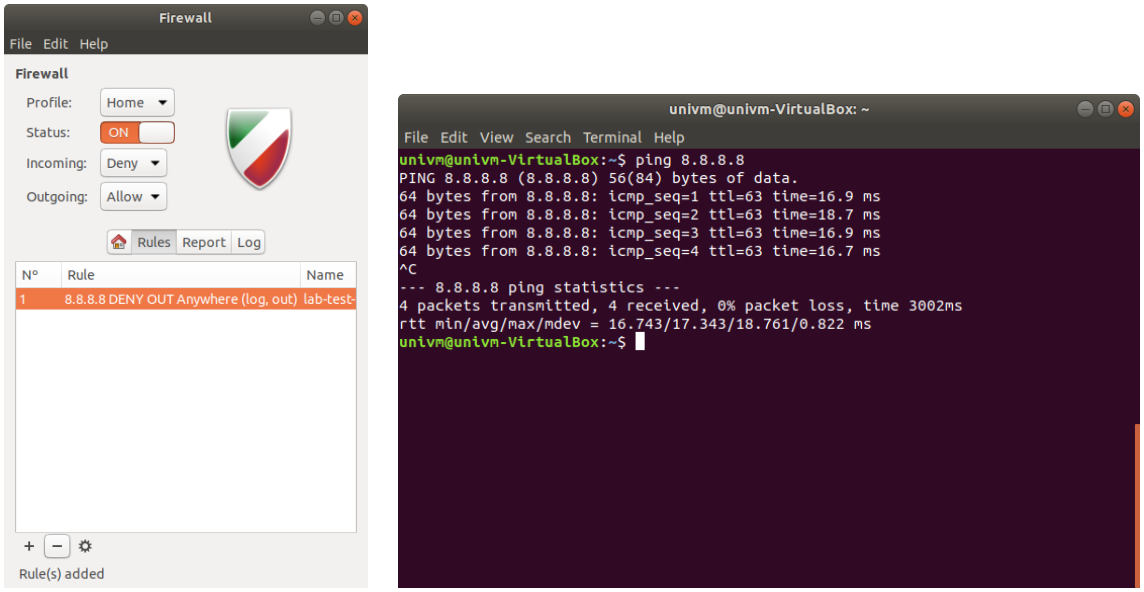


в)

Рис. 2: Створення правила для міжмережевого екрана у програмі `gufw`

Після створення правила спроба підключитись до заблокованого вузла відхиляється і закінчується невдачею, а для дозволеного виконується успішно.

Видалимо правило і перевіримо, чи можна тепер підключитись до раніше заблокованого вузла. Як бачимо, після видалення правила підключення проходить успішно (рис. 3).



а) б)

Рис. 3: Спроба підключення після видалення правила у програмі `gufw`

Перевіривши справність роботи правил, переглянемо, які правила діють у міжмережевому екрані на даний момент. Для цього виконаємо таку команду:

```
sudo iptables -L
```

Після завершення роботи команди на екран будуть виведені усі правила, знайдені у налаштуваннях міжмережевого екрана (рис. 4).

Отже, тепер ми навчились працювати з міжмережевим екраном за допомогою графічного інтерфейсу `gufw`. Переходимо до налаштування міжмережевого екрану на комп'ютері під управлінням операційної системи Windows.

В операційній системі Windows міжмережевий екран прийнято називати «брандмауером». Щоб його налаштувати, необхідно відкрити Панель керування і обрати елемент «Брандмауер Windows», а потім у боковому меню натиснути на надпис «Додаткові параметри». В результаті відкриється вікно налаштувань брандмауера (рис. 5).

У з'явившомуся вікні вмикаємо брандмауер для поточного домену, приватного та загального профілів і підтверджуємо вибрані налаштування. Після

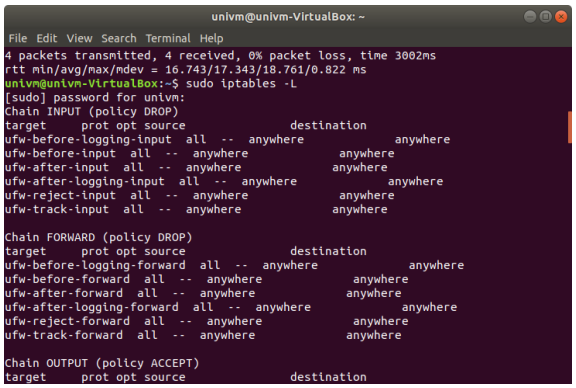


Рис. 4: Список активних правил міжмережевого екрана

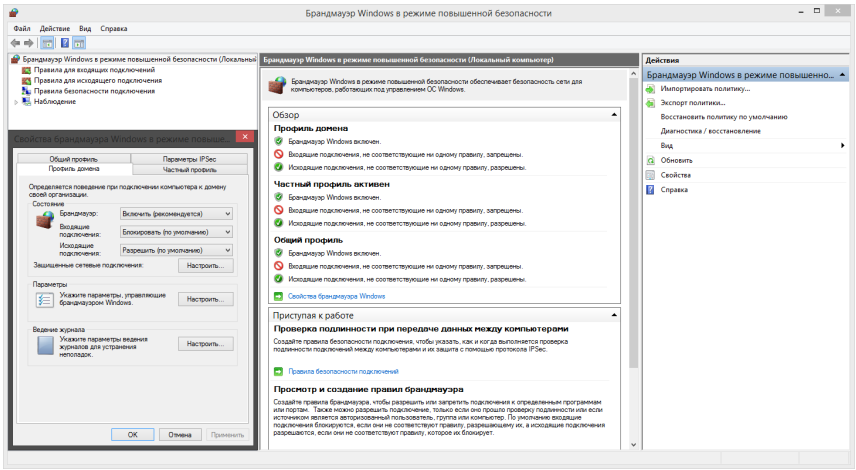
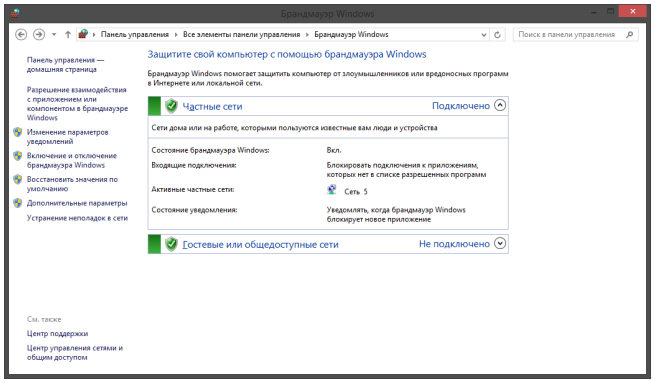
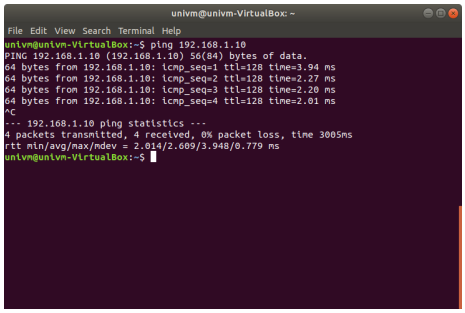


Рис. 5: Вікно налаштування брандмауера Windows

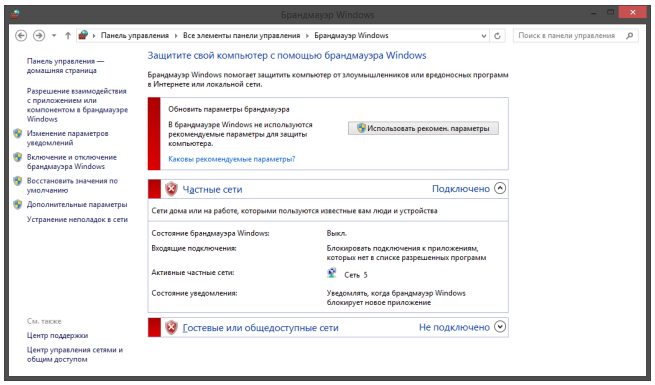
цього брандмауер налаштований. Перевіримо його роботу. Для цього спробуємо підключитись від імені комп'ютера під управлінням операційної системи GNU/Linux до комп'ютера під управлінням Windows спочатку коли брандмауер увімкнений, а потім — вимкнений (рис. 6).



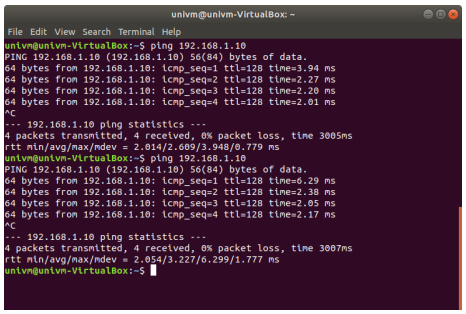
а)



б)



в)



г)

Рис. 6: Спроби підключення до комп'ютера під управлінням Windows з різними налаштуваннями брандмауера

Отже, ми ознайомились з можливостями, особливостями і налаштуваннями міжмережевого екрана в операційній системі Windows.

Повернемось до міжмережевого екрана в операційній системі GNU/Linux. Вимкнемо правила, встановлені програмою `gufw` і переглянемо активні правила, які залишились (рис. 7).

Заблокуємо вхідні, вихідні і транзитні пакети, тобто зробимо так, щоб жоден пакет не проходив через мережеві інтерфейси. Для цього виконаємо такі команди:

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

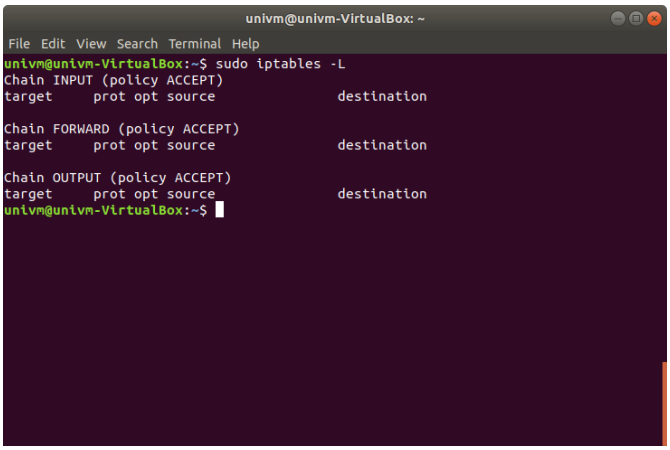
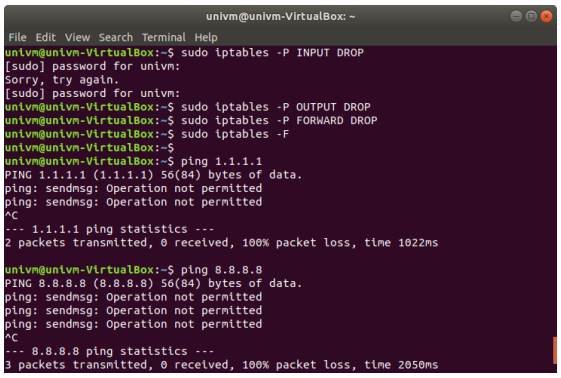


Рис. 7: Активні правила міжмережевого екрана за замовчуванням

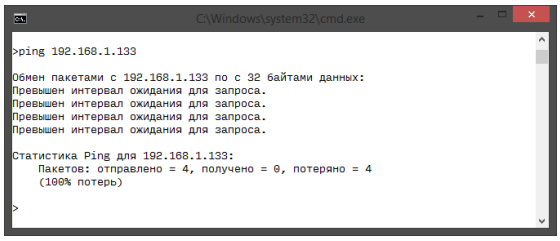
В результаті виконання команди всі пакети будуть заблоковані і жоден не зможе пройти крізь будь-який мережевий інтерфейс. За умовами завдання збережемо поточні правила міжмережевого екрана. Для цього виконаємо таку команду:

```
sudo iptables-save > uni/iptables-01.txt
```

Після того, як правила збережені, переглянемо список активних правил і переконаємось у цьому на практиці (рис. 8).



а)



б)

Рис. 8: Спроби підключення до комп'ютера під управлінням GNU/Linux із повною забороною пропуску пакетів

Як бачимо, ні внутрішні, ні зовнішні пакети не можуть пройти крізь мережеві інтерфейси комп'ютера, в якому міжмережевий екран налаштований на відторгнення усіх пакетів.

Зазвичай `iptables` використовують з ключем `-P`, який позначає створення нової політики міжмережевого екрану. Також використовують ключ `-L`, щоб ви-

вести список усіх активних правил, а також ключ `-F`, щоб очистити і оновити усі активні правила міжмережевого екрана.

4. Висновок

Виконуючи дану лабораторну роботу, ми ознайомились з основними принципами функціонування міжмережевих екранів та їх настроювання.