Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет информационных технологий и управления

Кафедра интеллектуальных информационных технологий

ОТЧЁТ

по лабораторной работе №6

по дисциплине

Средства и методы защиты информации в интеллектуальных системах

“Межсетевое экранирование”

|  |  |
| --- | --- |
| Выполнил | Робилко Т. М. гр. 2217011701 |
| Проверил | Захаров В. В. Н.В |

Минск 2024

**Задание:**

1. Создать папку с общим доступом на одной из виртуальных машин.
2. Настроить брандмауэр, применив различные политики:

2.1. доступ к разделяемому ресурсу разрешен только по заданным портам;

2.2. доступ к виртуальной машине разрешен только по заданным портам (например, www или ftp) и только компьютерам с данным IP-адресом (адресами);

2.3. доступ к внешним ресурсам разрешен только конкретным программам;

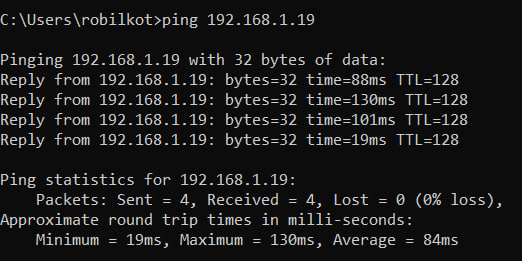
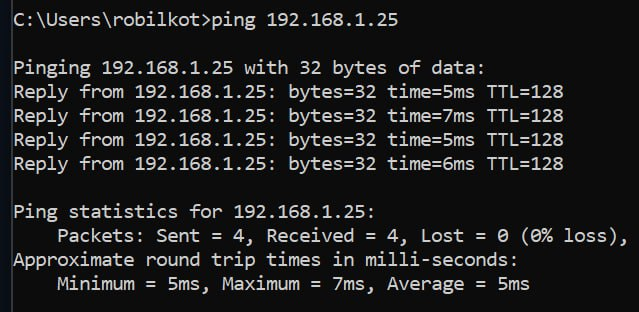
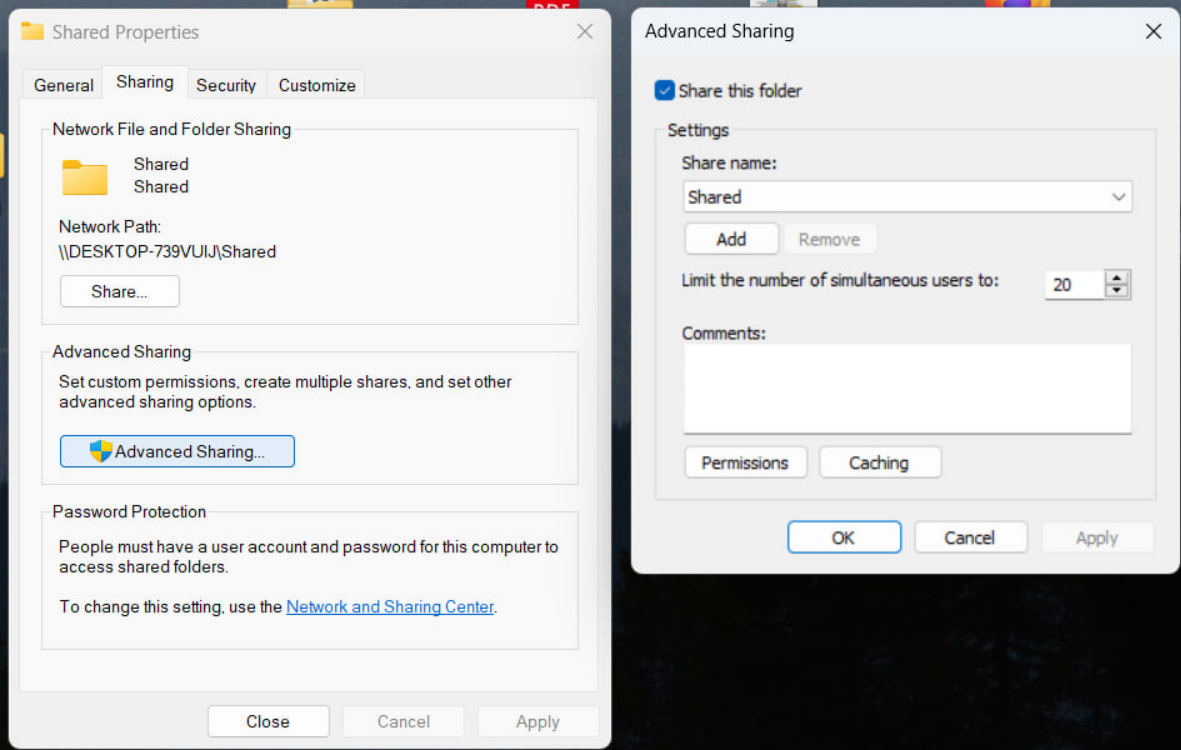
2.4. конкретной программе разрешен доступ к ресурсам удаленного компьютера с данным IP-адресом по заданному порту;

2.5. запретить запрос входящего эха (ICMP).

1. Оформить отчет, подтверждающий применение указанных политик.

С учётом наличия двух физических компьютеров под управлением Windows 11, для выполнения работы будут использоваться именно они.

**Ход работы:**

1. Убедимся, что оба компьютера доступны в пределах локальной сети с помощью команды Ping. Ipv4 адреса компьютеров: 192.168.1.25 и 192.168.1.19 соответственно.
2. Создадим папку с общим доступом 

**Задание 2.1.** Настроить брандмауэр, применив различные политики. Доступ к разделяемому ресурсу разрешен только по заданным портам.

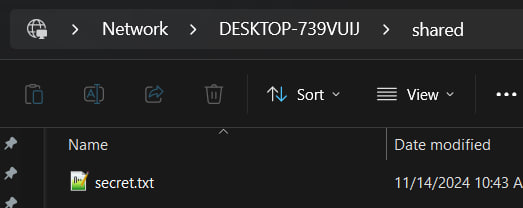


Рис. 2.1. - Доступ разрешен для первой машины

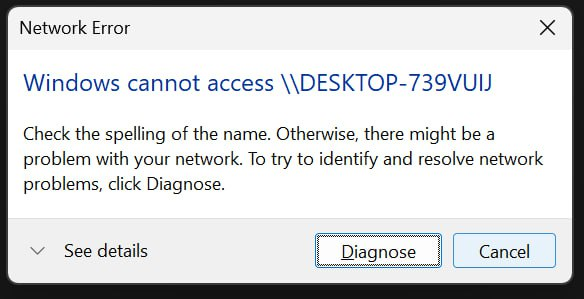
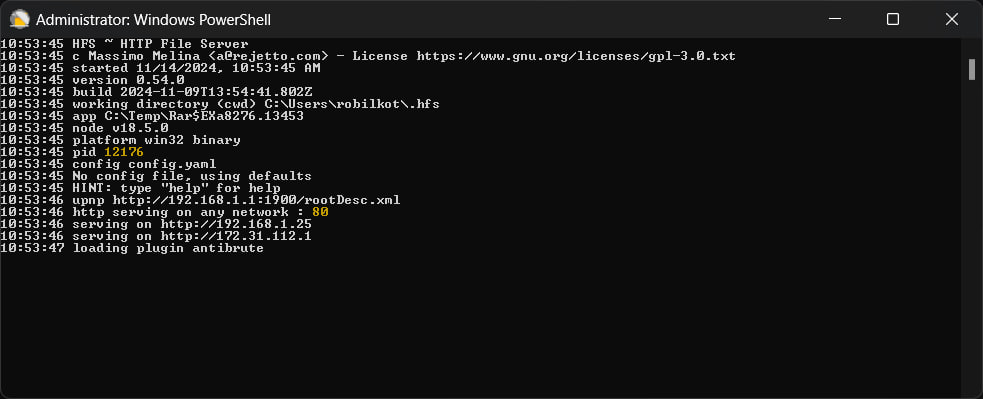


Рис. 2.1.1. - Доступ запрещен для второй машины

**Задание 2.2.** Настроить брандмауэр, применив различные политики. Доступ к виртуальной машине разрешен только по заданным портам (например, www или ftp) и только компьютерам с данным IP-адресом (адресами).

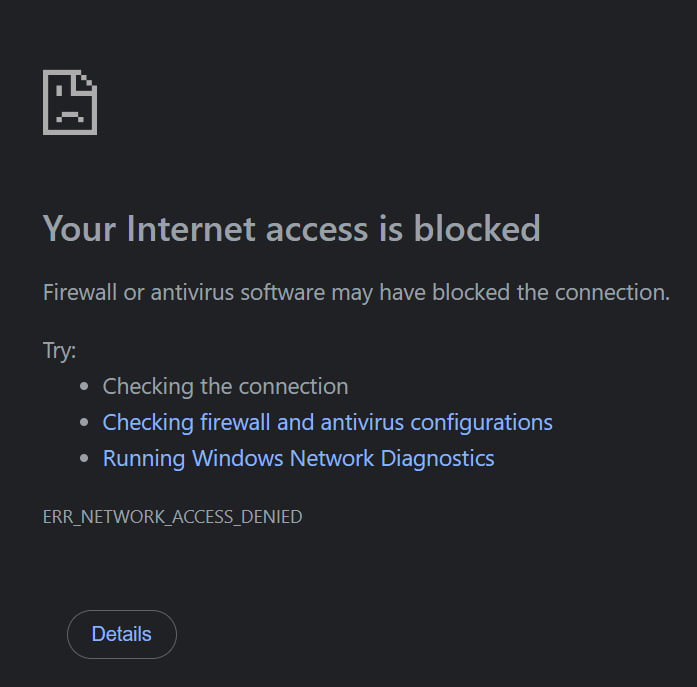
Для выполнения задания запустим http сервер на первой машине (слушает порт 80)



Для начала добавим правило, по которому доступ по 80 порту запрещен.



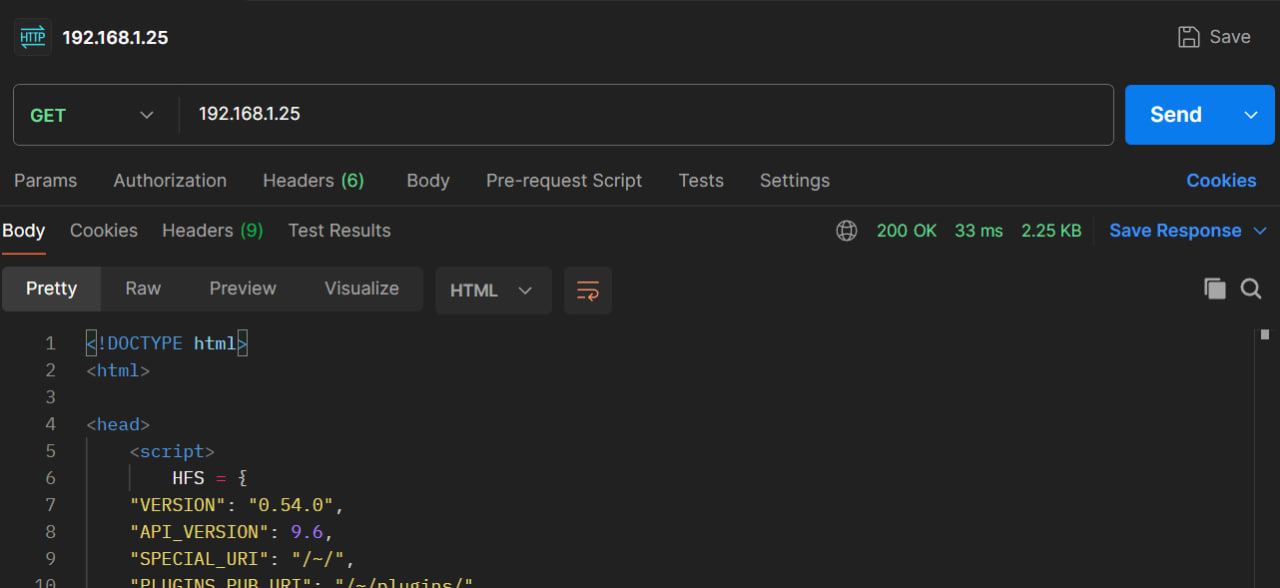
Проверим запрет соединения через браузер.



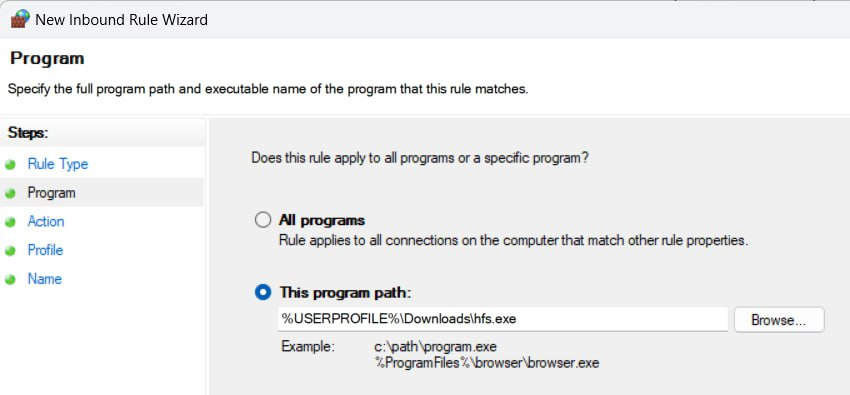
Теперь создадим другое правило, разрешающее соединение по 80 порту.



Через веб-браузер либо другой http клиент проверим наличие доступа к ресурсу.



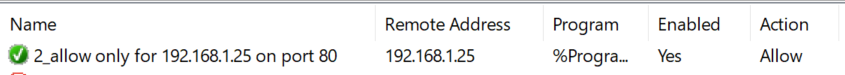
**Задание 2.3.** Настроить брандмауэр, применив различные политики. Доступ к внешним ресурсам разрешен только конкретным программам).

Создадим правило для входящих соединений. Как следствие, только http сервер сможет принять запрос на 80 порту.

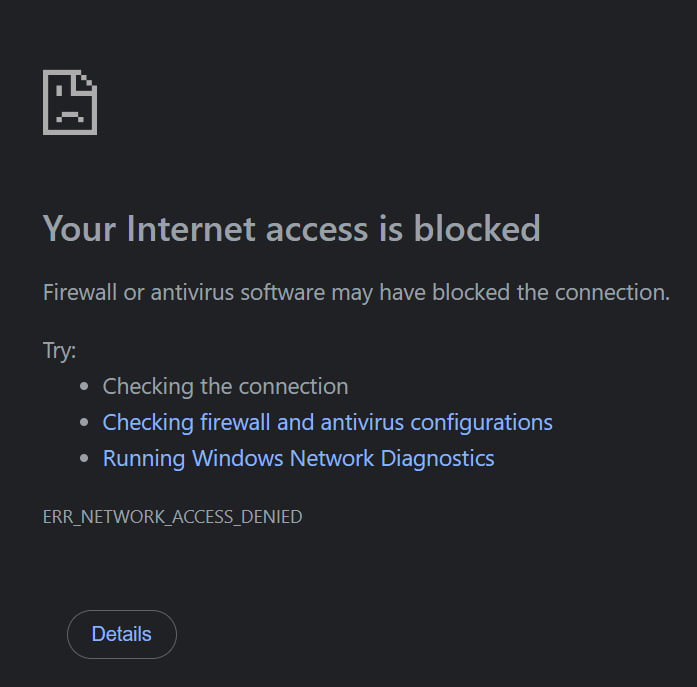
Результат до и после применения правила оказывается аналогичен пункту 2.2.

**Задание 2.4.** Настроить брандмауэр, применив различные политики. Конкретной программе разрешен доступ к ресурсам удаленного компьютера с данным IP-адресом по заданному порту.

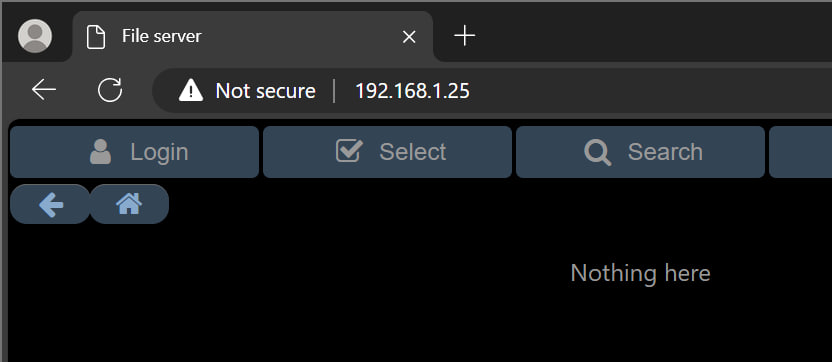
Создадим правило, согласно заданному условию



В результате становится невозможным получить доступ к внешним ресурсам через google chrome и другие приложения



Однако доступ через Microsoft edge будет разрешен

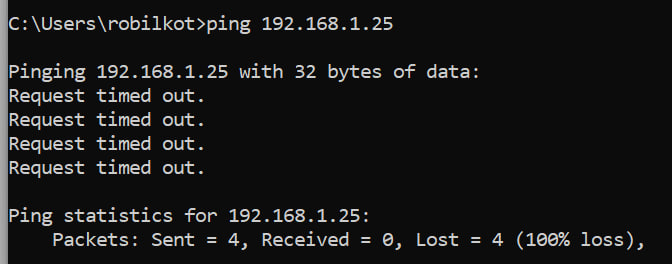


**Задание 2.5.** Настроить брандмауэр, применив различные политики. Запретить запрос входящего эха (ICMP).

Выключим правило, разрешающее ICMP запрос на первой машине.



Со второй машины выполним запрос, убедимся в отсутствии доступа.



**Вывод:**

В ходе выполнения данной лабораторной работы был рассмотрен комплекс программно-аппаратных средств межсетевой защиты, позволяющий реализовать частную политику безопасности.

Брандмауэр помогает предотвратить атаки или внедрение и запуск вредоносного программного обеспечения на компьютере через сеть, а также помогает предотвратить отправку вредоносных программ на другие компьютеры.

Настроенные правила показали свою состоятельность в ограничении доступа и контроле взаимодействия сетевых приложений, что является основой для обеспечения безопасности в локальной сети.