

**Федеральное государственное автономное образовательное учреждение  
высшего образования**  
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ  
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»**

Московский институт электроники и математики им. Тихонова  
Департамент электронной инженерии

**ОТЧЕТ  
О ПРАКТИЧЕСКОЙ РАБОТЕ №10**

по дисциплине «Программные и аппаратные средства защиты информации»  
**«Программные межсетевые экраны»**

Вариант 4

Студент гр. БИБ201  
Шадрунов Алексей  
Дата выполнения: 16 июня 2023 г.

Преподаватель:  
Перов А. А.  
«\_\_» \_\_\_\_\_ 2023 г.

Москва, 2023

## **Содержание**

<b>1 Цель работы</b>	<b>3</b>
<b>2 Ход работы</b>	<b>3</b>
2.1 Private Firewall . . . . .	3
2.2 Настройки межсетевого экрана . . . . .	3
2.2.1 Main menu . . . . .	4
2.2.2 Applications . . . . .	4
2.2.3 Process monitor . . . . .	6
2.2.4 Firewall Log . . . . .	8
2.2.5 Port tracking . . . . .	8
2.3 Создание сетевых соединений и правил . . . . .	10
2.3.1 Git . . . . .	10
2.3.2 Windows Media Player . . . . .	12
2.3.3 ssh . . . . .	14
2.4 Сканирование системы . . . . .	17
<b>3 Выводы о проделанной работе</b>	<b>20</b>

## 1 Цель работы

Цель: изучение и приобретение навыков работы с программными межсетевыми экранами.

Задачи:

- Изучение возможностей персональных межсетевых экранов;
- Конфигурирование персонального межсетевого экрана;
- Управление соединениями с помощью персонального межсетевого экрана.

## 2 Ход работы

### 2.1 Private Firewall

Загрузим программу по ссылке <https://www.comss.ru/download/page.php?id=790>. Установим Private Firewall на виртуальную машину. Окно программы приведено на рисунке 1.

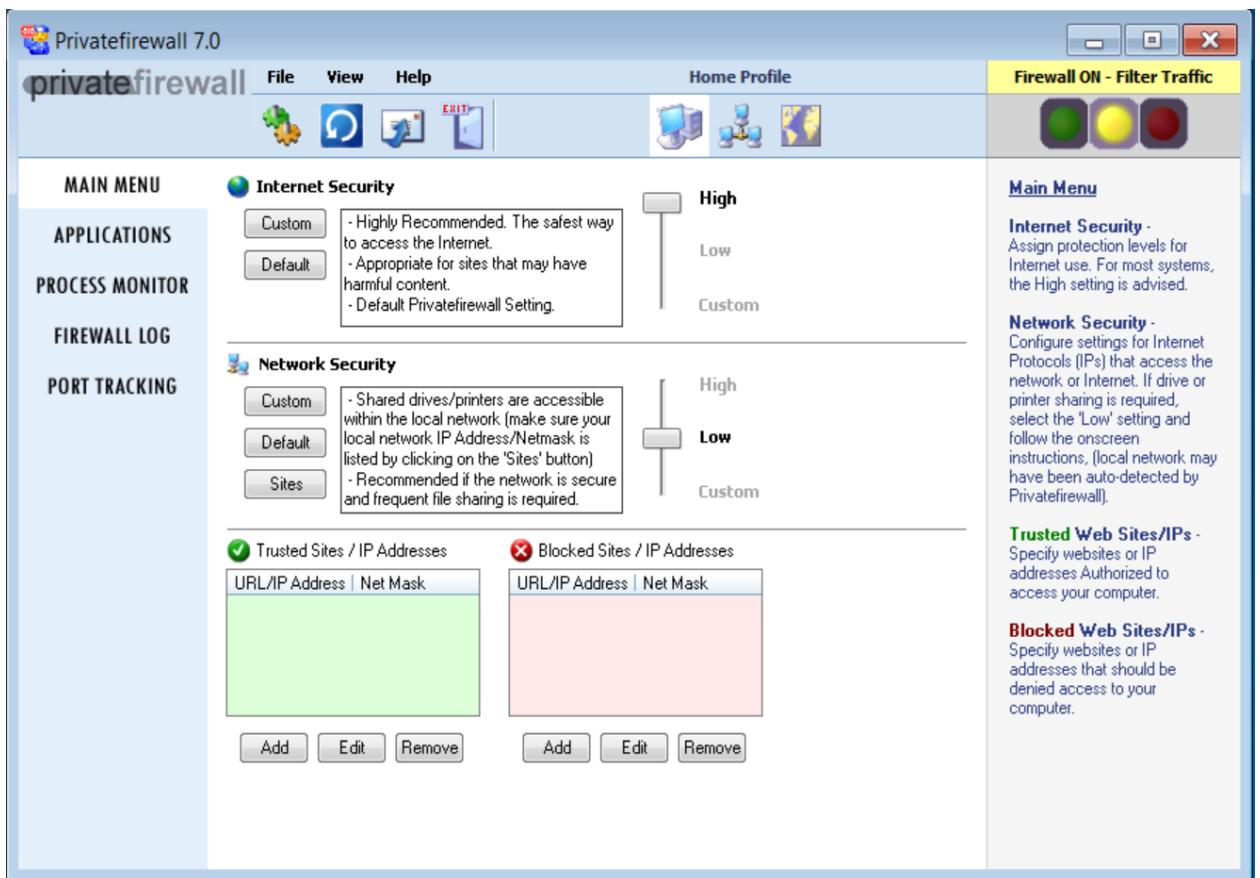


Рисунок 1 – Окно программы

### 2.2 Настройки межсетевого экрана

В верхнем углу есть основной переключатель режимов работы межсетевого экрана. При нажатии на зелёную кнопку весь трафик разрешается, при нажатии на красную — блокируется. В жёлтом режиме трафик фильтруется по правилам, которые можно настроить ниже.

В окне программы есть пять подменю для настройки правил.

### 2.2.1 Main menu

- Доступ в интернет — уровень защиты при работе в интернете. Высокий уровень (рекомендуемый) — подходит для небезопасной среды, отключает все протоколы, использование которых не предусмотрено в интернете. Низкий уровень — для использования интернета в безопасной среде. Также можно самостоятельно задать разрешения (и посмотреть, что отключено в High) в пользовательском режиме.

- Безопасность в сети — уровень защиты при работе в интернете и локальной сети. Нужен для настройки работы сетевых дисков и принтеров. Низкий уровень (рекомендуемый) — устройства в локальной сети доступны (адрес локальной сети можно задать дополнительно). Высокий уровень — многие протоколы отключены в локальной сети, может привести к проблемам в сетевом взаимодействии.

- Доверенные IP/сайты — сайты и адреса, с которых разрешён доступ к компьютеру. Можно задать адрес устройства, подсеть или URL.

- Заблокированные IP/сайты — сайты и адреса, с которых запрещён доступ к компьютеру.

### 2.2.2 Applications

В разделе перечислен список приложений, которые пытались подключиться к интернету. Для каждого приложения существует список правил, которые можно настроить через контекстное меню. Также можно временно включить или отключить фильтрацию трафика для приложения (Рисунок 2).

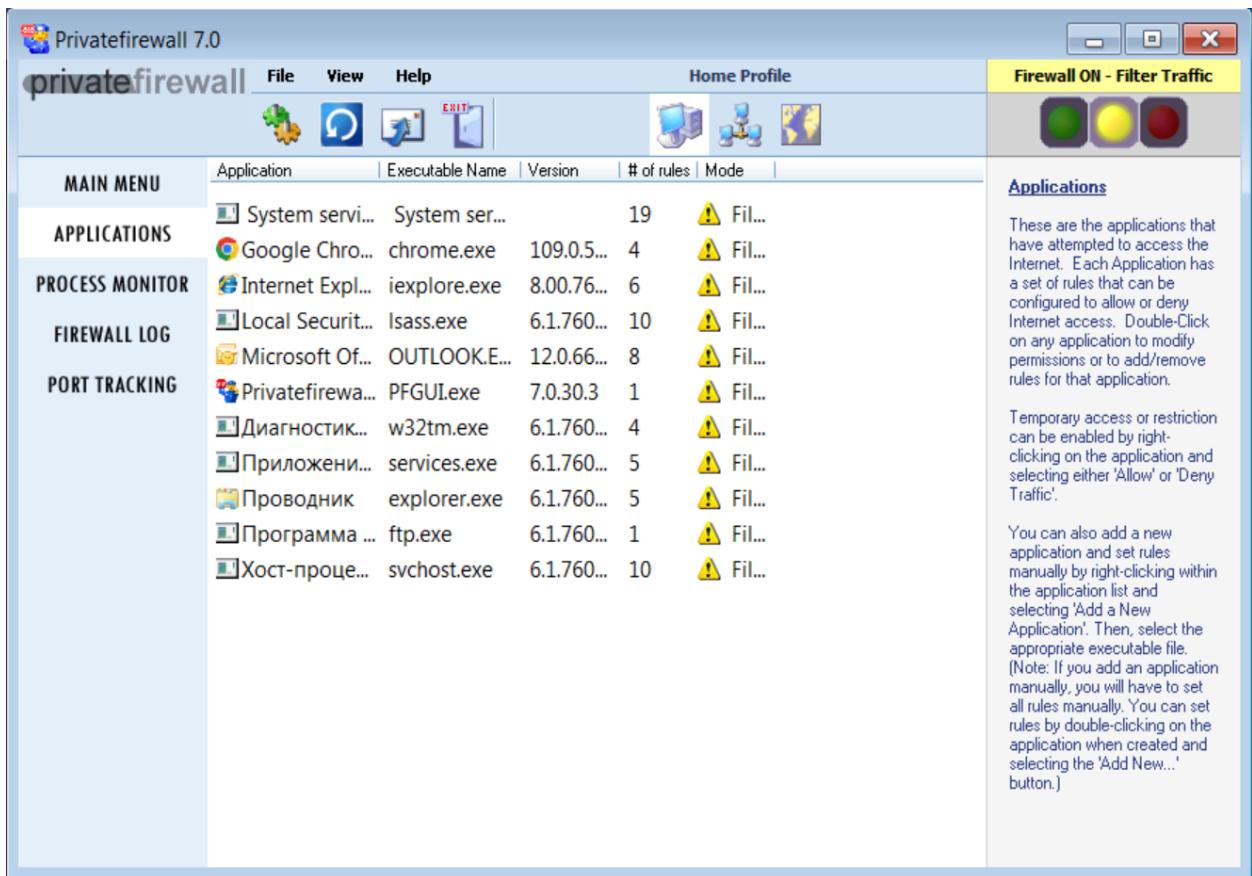


Рисунок 2 – Applications

При добавлении правила можно указать очерёдность применения правил, устанавливать тип правила, протокол, локальные и удалённые порты, а также в какой режим работы добавить данное правило (Рисунок 3).

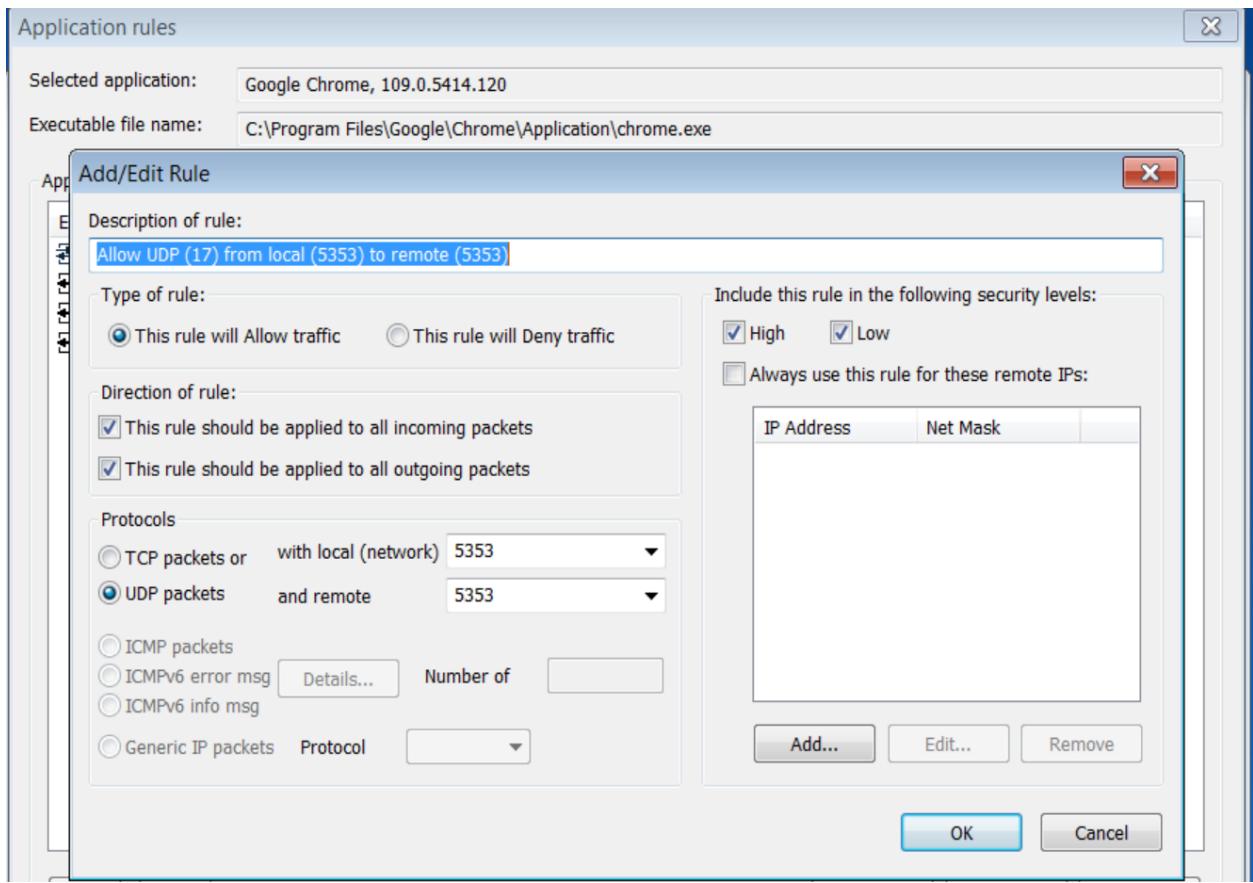


Рисунок 3 – Applications

### 2.2.3 Process monitor

Раздел позволяет мониторить процессы, запущенные в системе, и отслеживать системные вызовы. Для каждого процесса можно настроить правила, по которым одни системные вызовы буду доступны, а другие нет. Можно выбрать уровень защиты: в среднем режиме будут отслеживаться только процессы, относящиеся к приложениям, перечисленным в предыдущем меню программы, в высоком режиме будут отслеживаться все процессы в системе (Рисунок 4). Доступные системные вызовы перечислены на рисунке 5.

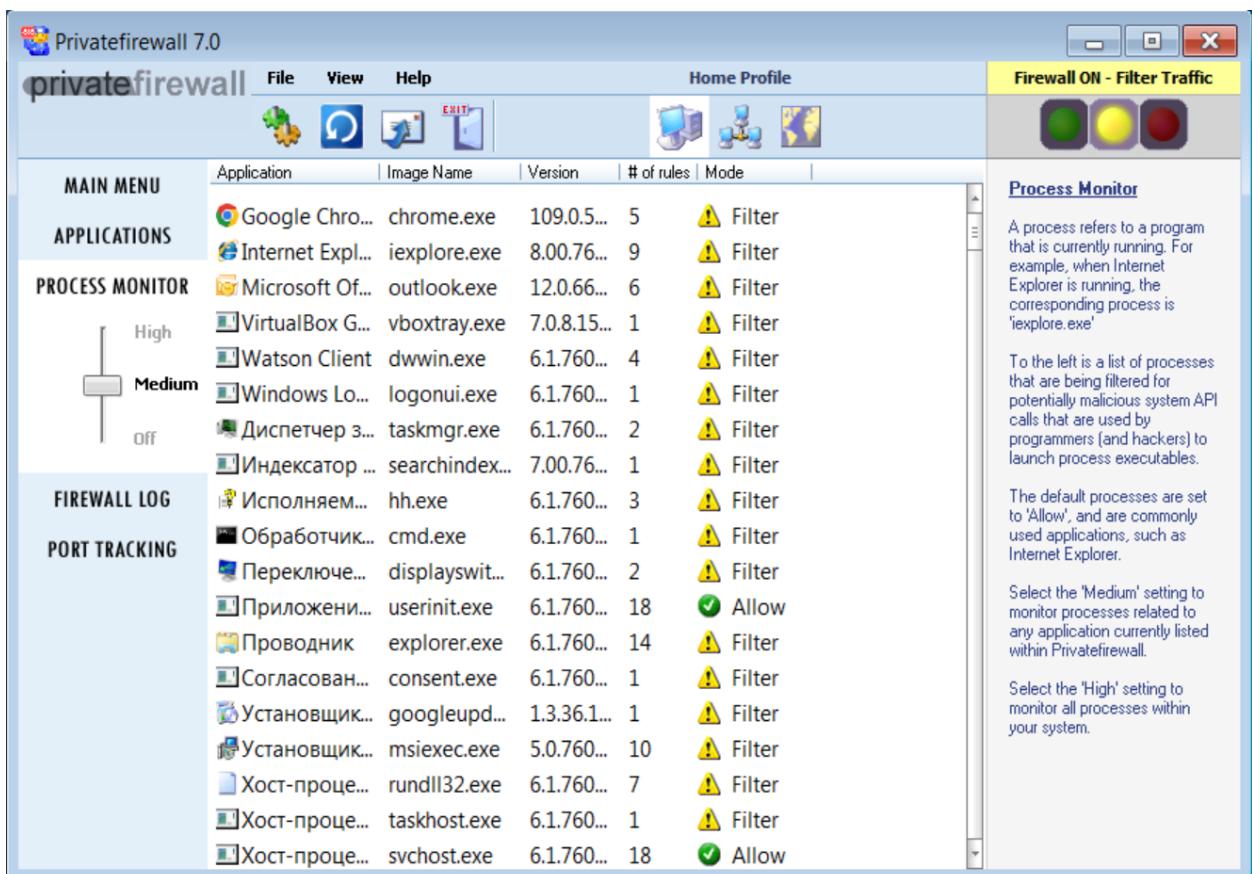


Рисунок 4 – Process monitor

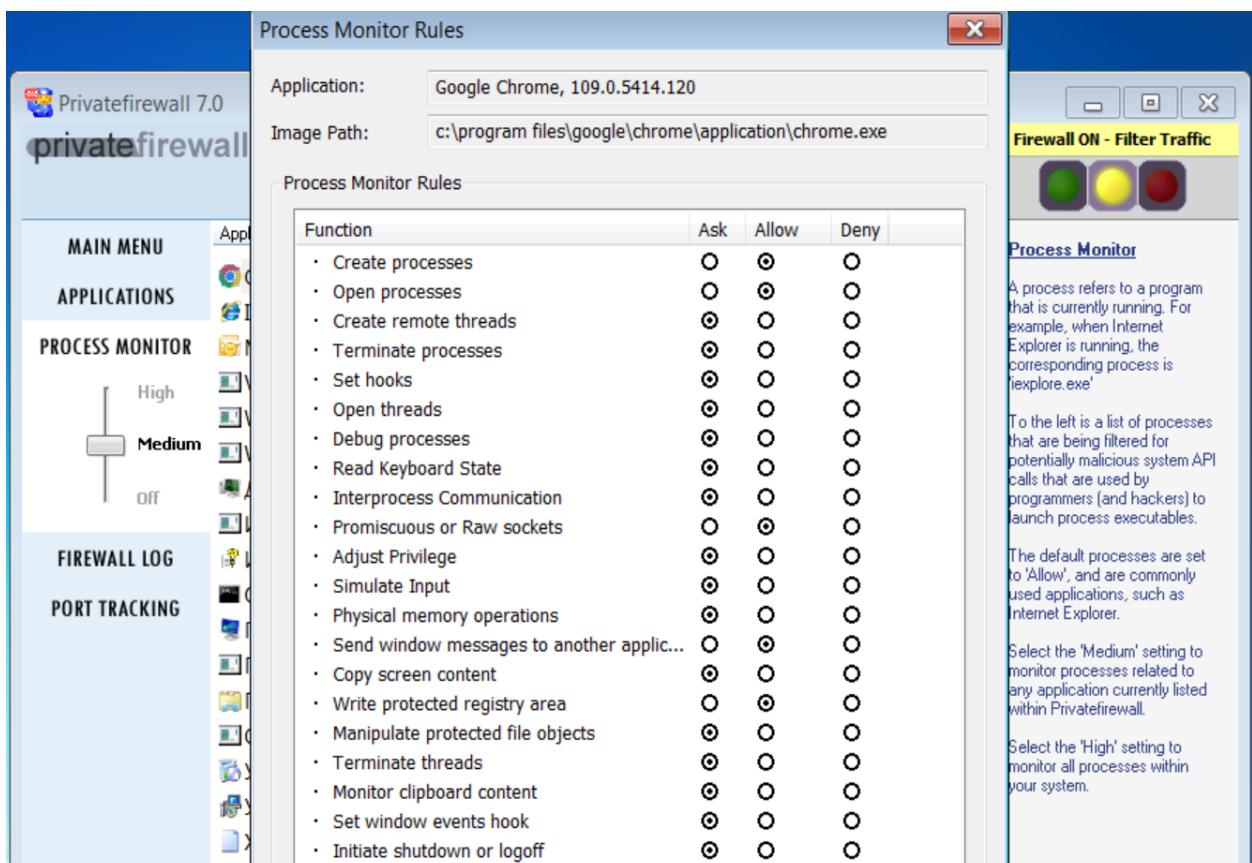


Рисунок 5 – Process monitor

## 2.2.4 Firewall Log

Раздел отображает входящие и исходящие пакеты, которые были заблокированы межсетевым экраном. В списке отображаются время и дата, локальный IP, удалённый IP, протокол и приложение, к которому относится пакет. Также указано, в каком направлении следовал пакет (Рисунок 6).

The screenshot shows the Privatefirewall 7.0 interface. The main window title is "Privatefirewall 7.0". The menu bar includes "File", "View", "Help", and "Home Profile". On the right, there's a status bar with "Firewall ON - Filter Traffic" and three colored icons (green, yellow, red). The left sidebar has a tree view with nodes: "MAIN MENU", "APPLICATIONS", "PROCESS MONITOR", "FIREWALL LOG" (which is selected), and "PORT TRACKING". Under "FIREWALL LOG", there's a dropdown menu with options: "High", "Medium", "Low", and "Off". The main content area displays a table of log entries:

	Time/Date	Local IP	Remote IP	Protocol	Application
[1]	21:45:28 ...	10.0.2.15:13...	10.0.2.255:1...	UDP ...	System
[1]	21:41:56 ...	[fe80::2c3c:...	[ff02::fb]:53...	UDP ...	
[1]	21:41:56 ...	10.0.2.15:53...	224.0.0.251:...	UDP ...	C:\Prog...
[1]	21:41:51 ...	10.0.2.15:49...	216.58.210....	TCP (...	C:\Prog...
[1]	21:41:51 ...	10.0.2.15:56...	216.58.210....	UDP ...	C:\Prog...
[1]	21:41:51 ...	10.0.2.15:65...	192.168.43....	UDP ...	C:\Prog...
[1]	21:41:51 ...	10.0.2.15:13...	10.0.2.255:1...	UDP ...	System
[1]	21:41:50 ...	10.0.2.15:60...	216.58.210....	UDP ...	C:\Prog...
[1]	21:41:50 ...	10.0.2.15:53...	216.58.209....	UDP ...	C:\Prog...
[1]	0:40:59 1...	10.0.2.15:13...	10.0.2.255:1...	UDP ...	System
[1]	0:37:27 1...	10.0.2.15:13...	10.0.2.255:1...	UDP ...	System
[1]	0:35:59 1...	10.0.2.15:13...	10.0.2.255:1...	UDP ...	System
[1]	0:33:27 1...	10.0.2.15:13...	10.0.2.255:1...	UDP ...	System
[1]	0:30:15 1...	10.0.2.15:13...	10.0.2.255:1...	UDP ...	System
[1]	0:28:43 1...	10.0.2.15:13...	10.0.2.255:1...	UDP ...	System
[1]	0:28:37 1...	10.0.2.15:13...	10.0.2.255:1...	UDP ...	System

The right side of the interface contains a "Firewall Log" section with explanatory text and icons:

- Firewall Log**: This report displays incoming or outgoing packets that have been blocked by the firewall.
- Packet Details**:
  - Time/Date - When the packet was detected.
  - Local/Remote IP - These are the local and remote Internet Addresses.
  - Protocol - The type of network connection used to send the packet.
  - Application Name - The file name to which the packet was attempting to be sent, (if any).
  - Blocked events for which no rule has yet been created are marked with the red icon to reflect incoming packets [1] or the blue icon to reflect outgoing packets [1]. Packets blocked based on existing rules are marked with gray icons.

Рисунок 6 – Firewall Log

## 2.2.5 Port tracking

Раздел отслеживает все порты в системе и защищает их от незапланированного проникновения. Кроме того, фаервол скрывает порты, делая их невидимыми для внешних устройств (Stealth). В таблице отображаются имя приложения, PID, протокол и адреса (Рисунок 7).

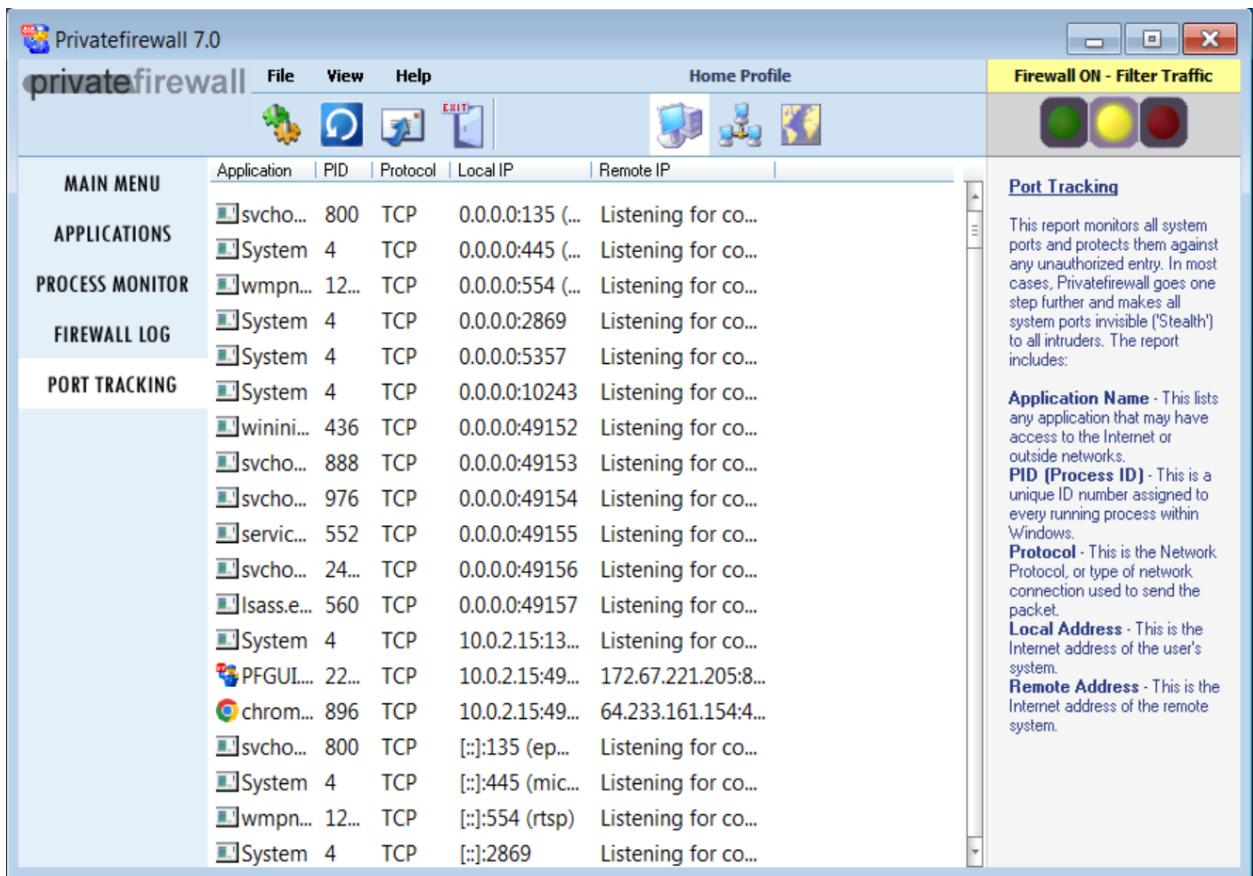


Рисунок 7 – Port tracking

## 2.3 Создание сетевых соединений и правил

Протестируем различные программы, использующие доступ к сети.

### 2.3.1 Git

Попробуем воспользоваться утилитой git, чтобы скачать репозиторий с гитхаба.

Запустим git bash и пронаблюдаем в логах фаервола, какие пакеты заблокированы.

На рисунке 8 видно, что это программа git-remote-https.exe.

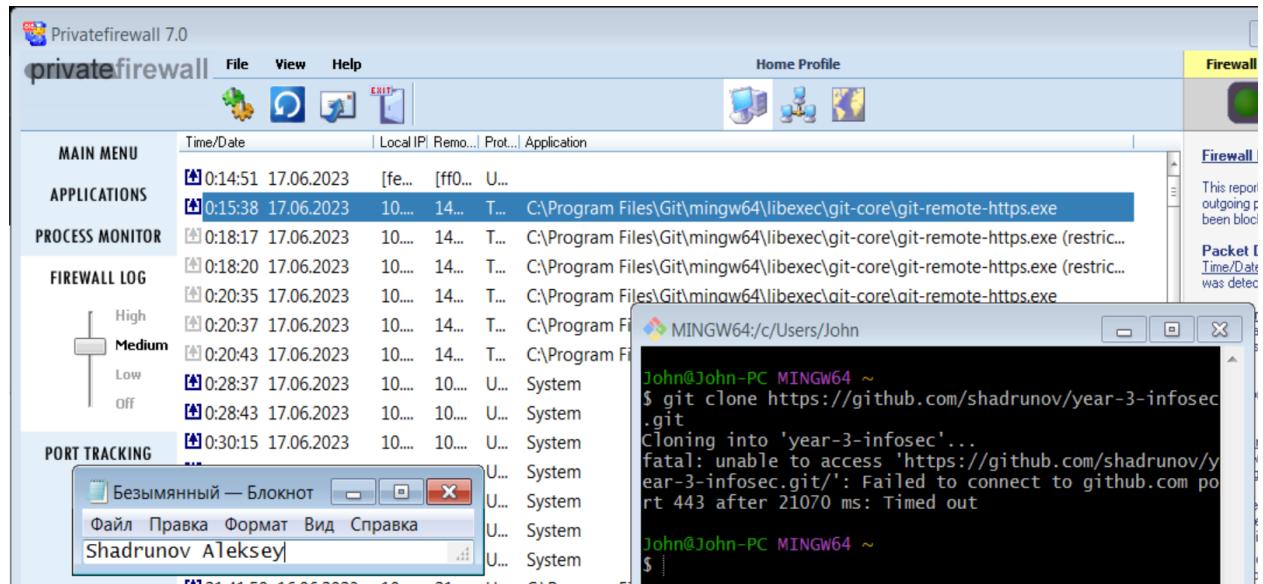


Рисунок 8 – Трафик запрещён

Создадим правило для разрешения трафика. Правило применим к нашему приложению (Рисунок 9).

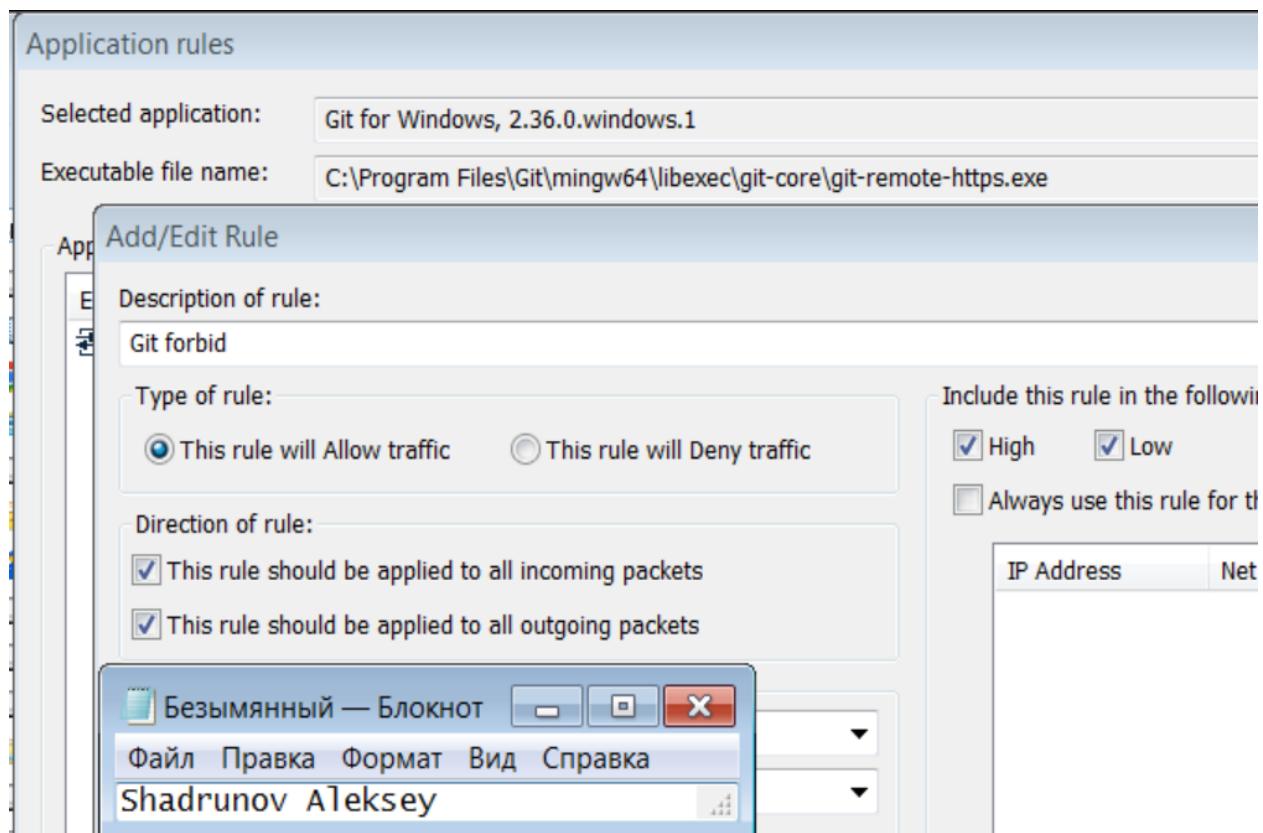


Рисунок 9 – Создание правила на приложение

После применения правила доступ к гитхабу появился и мы смогли загрузить репозиторий (Рисунок 10).

Рисунок 10 – Трафик разрешён

### 2.3.2 Windows Media Player

Попробуем воспользоваться приложением Windows Media Player. В нём встроен доступ к интернет-магазинам музыки. Открыв приложение, видим запрос на исходящий трафик, который перехватил фаервол (Рисунок 11).

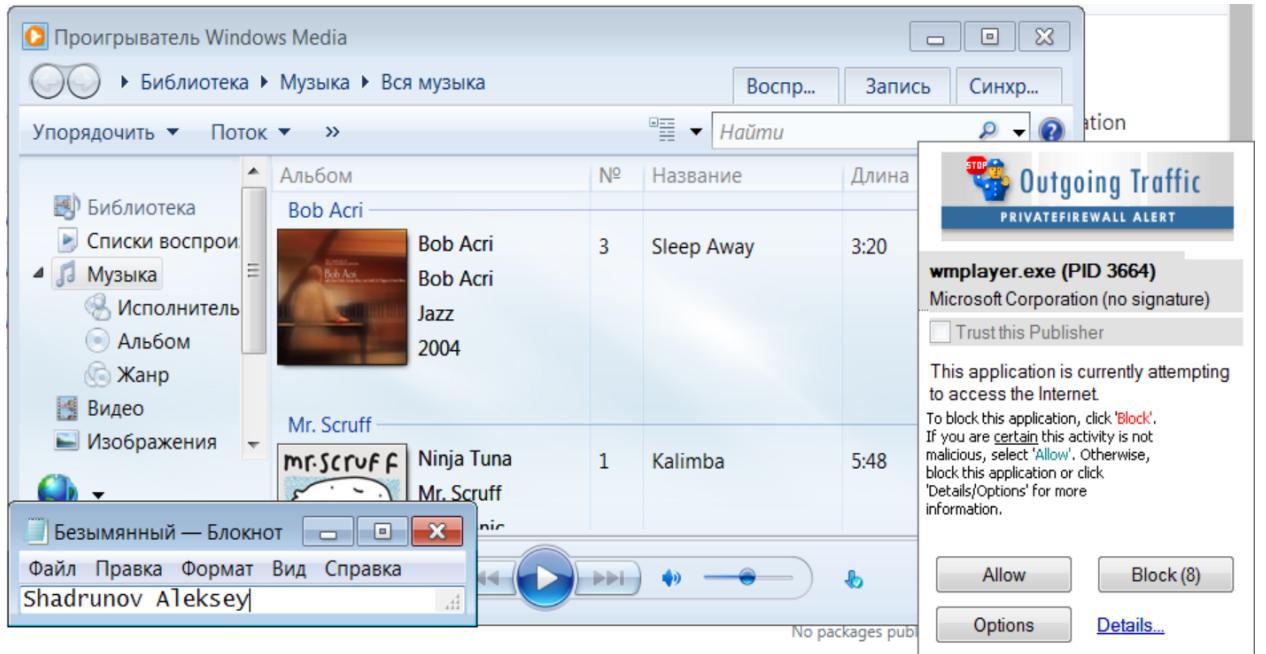


Рисунок 11 – Запрос на исходящий трафик

Создадим правило для разрешения трафика. Правило применим к нашему приложению. Настроим разрешение на порт 80, на котором расположен интернет-магазин (Рисунок 12). Видим, что в окне программы появилось сообщение, загруженное с сервера microsoft.com.

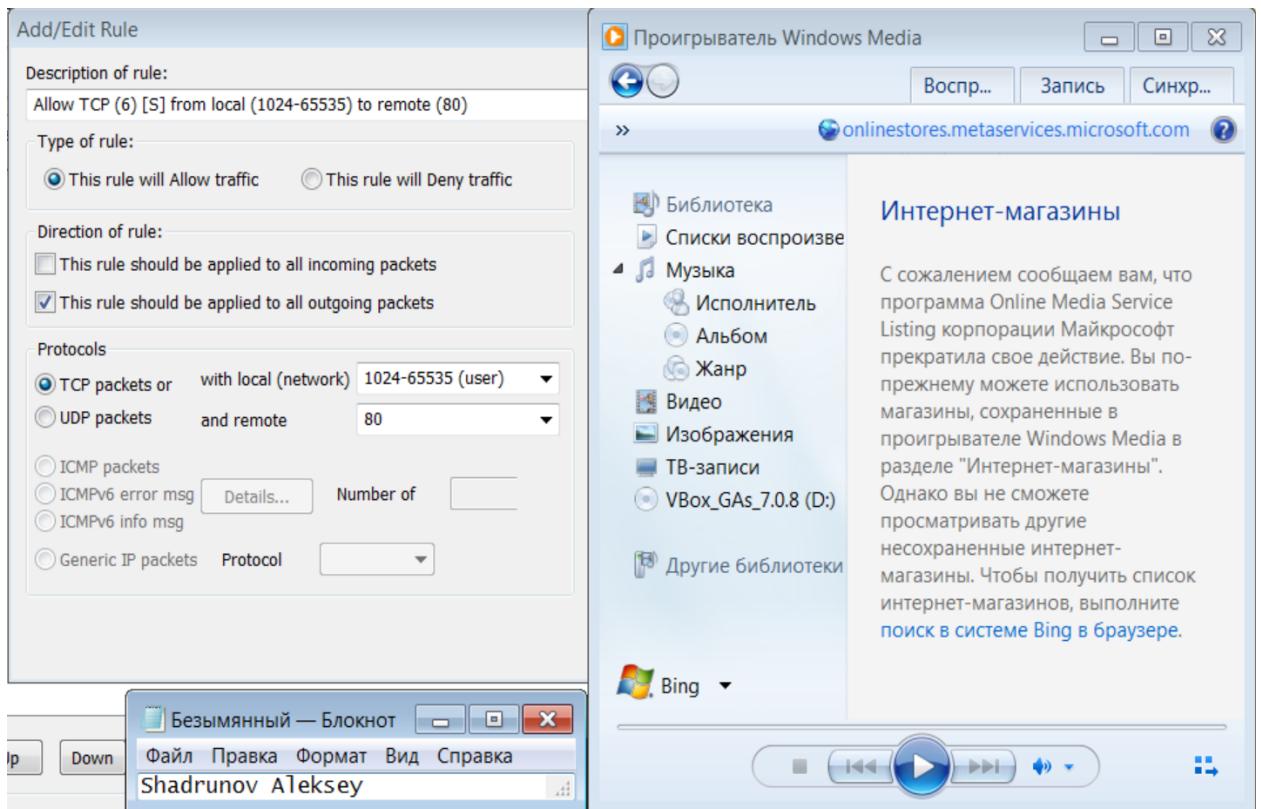


Рисунок 12 – Правило на порт

Теперь переведём правило в блокирующий режим (контекстное меню > блокировать). После применения правила доступ к интернет-магазину пропал (Рисунок 13).

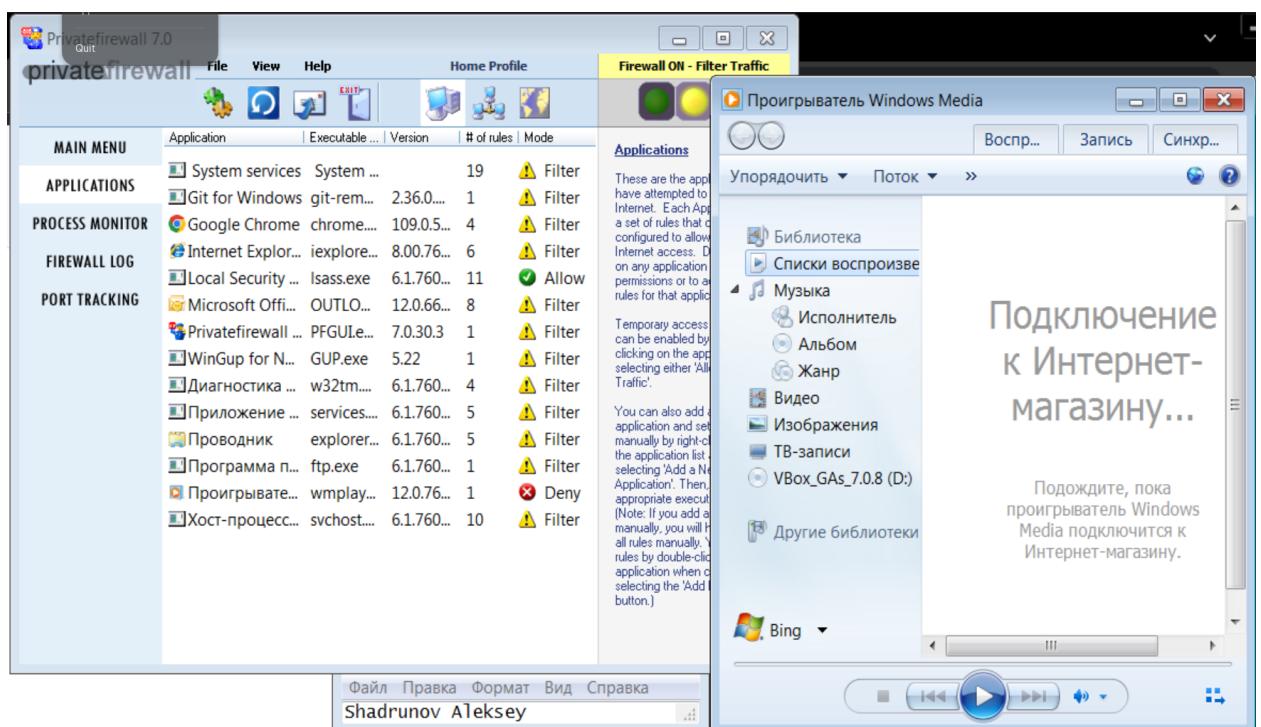


Рисунок 13 – Трафик заблокирован

### 2.3.3 ssh

Воспользуемся утилитой ssh для удалённого доступа к инстансу docker-playground. Для этого из git bash выполним команду ssh с адресом сервера (Рисунок 14). Видим, что в окне фаервола появилась строка ssh.exe (имя утилиты, которую мы запустили), а также что доступ к хосту у нас имеется (мы смогли сделать попытку установить сессию и сервер не принял наш ключ).

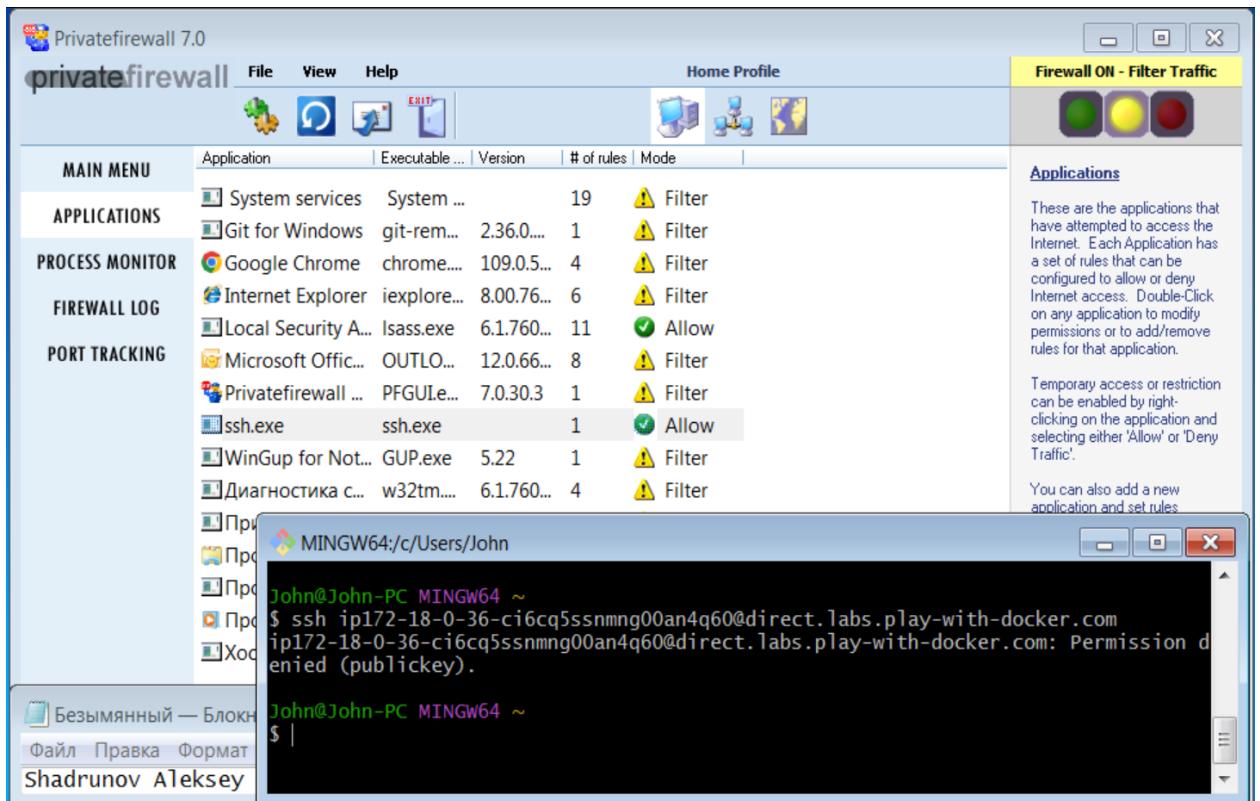


Рисунок 14 – Трафик разрешён

Переключим правило в режим Deny. Запустим ssh с флагом -v для просмотра расширенных логов. Видим, что соединение с сервером не может быть установлено (Рисунок 15).

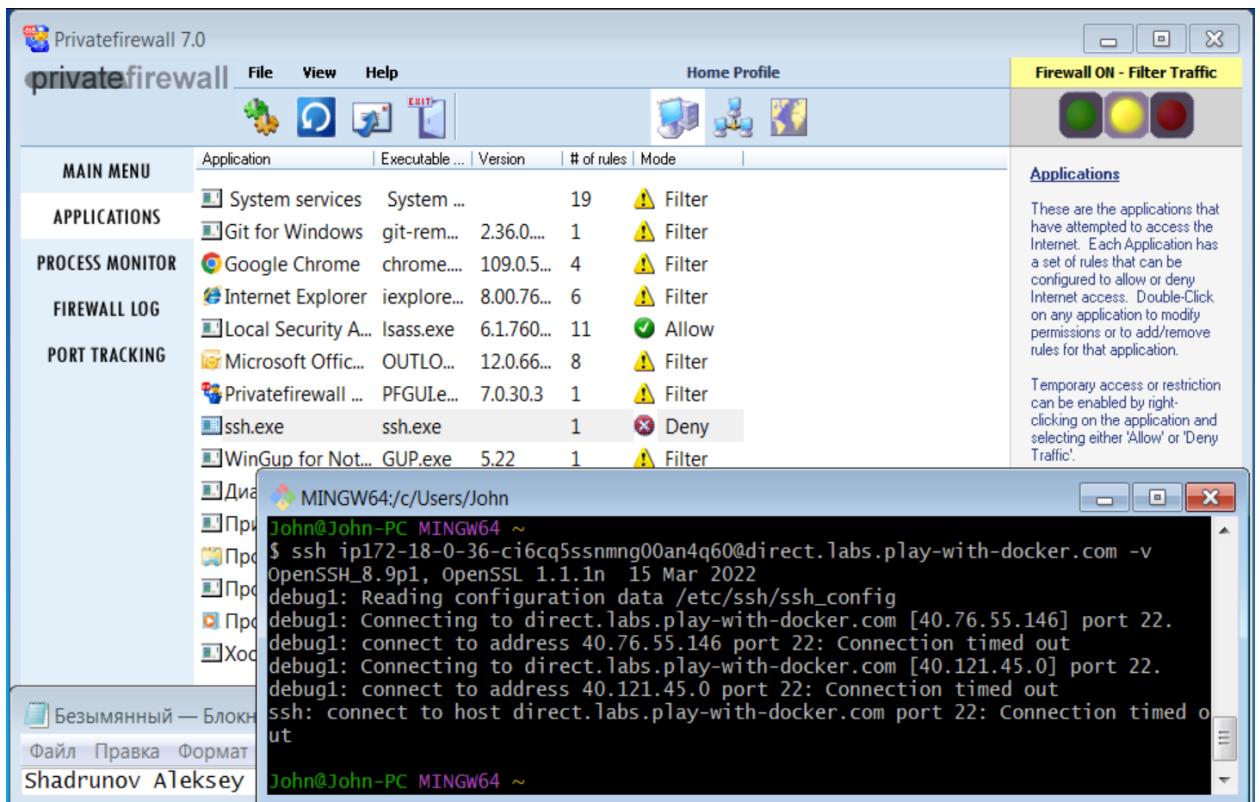


Рисунок 15 – Трафик запрещён

Откроем правило и настроим фильтрацию, разрешающую доступ к порту 22, который является стандартным для протокола (Рисунок 16). После этого доступ к серверу вновь появился.

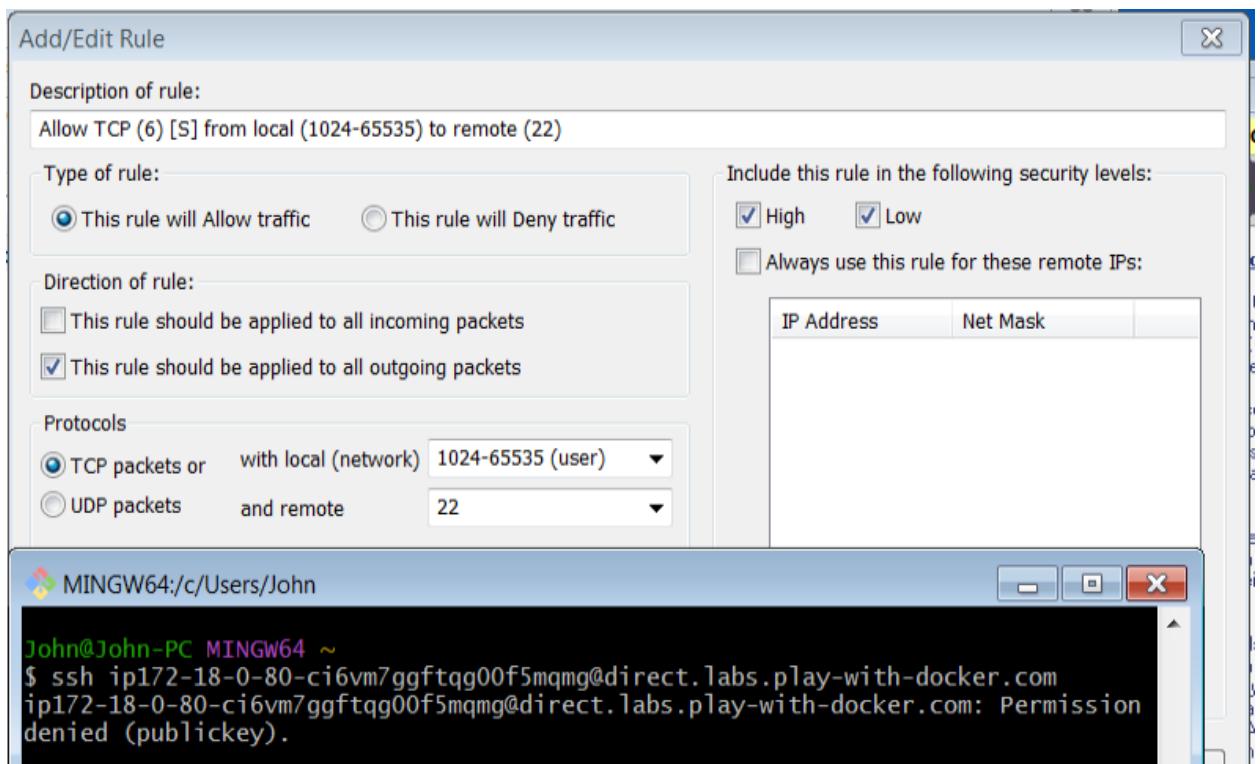


Рисунок 16 – Трафик разрешён

Снова заблокируем доступ на порт 22. Результат виден на рисунке 17.

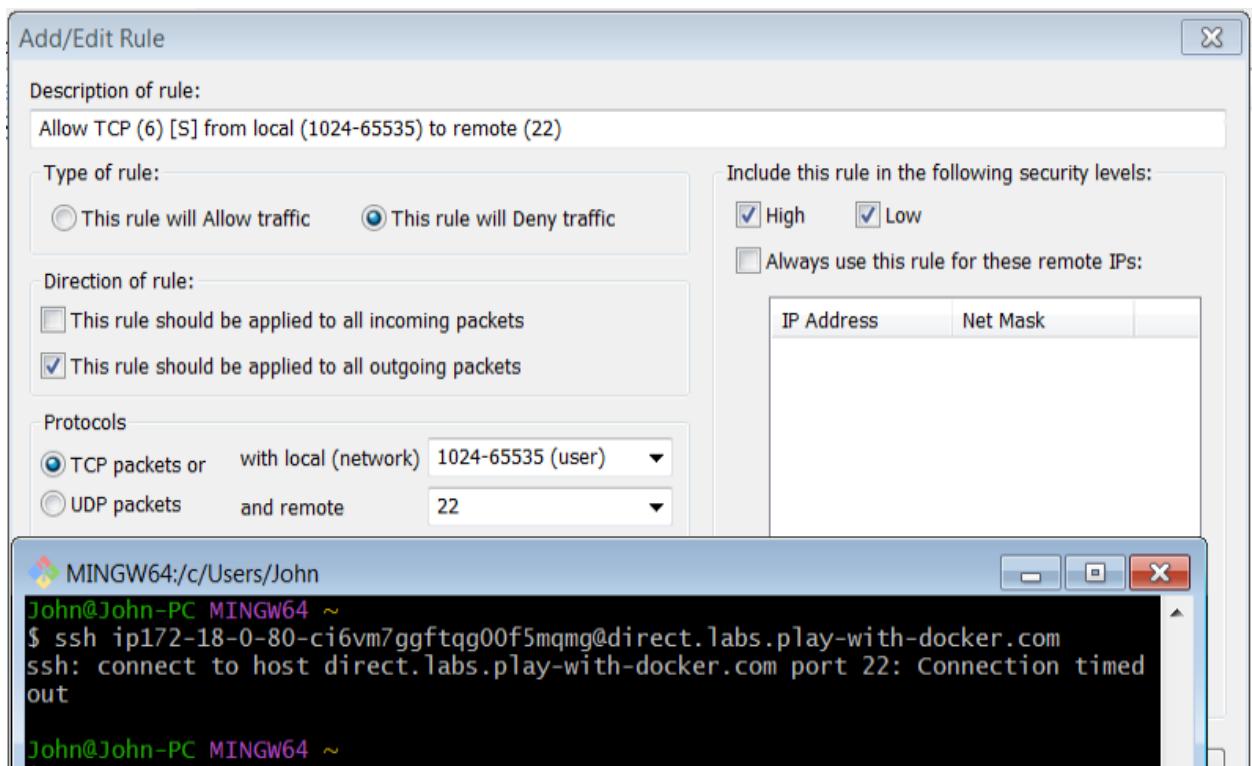


Рисунок 17 – Трафик заблокирован

## 2.4 Сканирование системы

В качестве дополнительного задания выполним сканирование виртуальной машины, защищённой фаерволом, с помощью утилиты nmap.

При первом запуске сканирования (nmap 192.168.56.101) видим, что сканер не смог выполнить пинг до хоста. Делаем вывод, что фаервол блокирует входящие ICMP-запросы. После запуска сканирования с ключом -Pn видим, как фаервол отобразил запрос на входящее соединение (Рисунок 18).

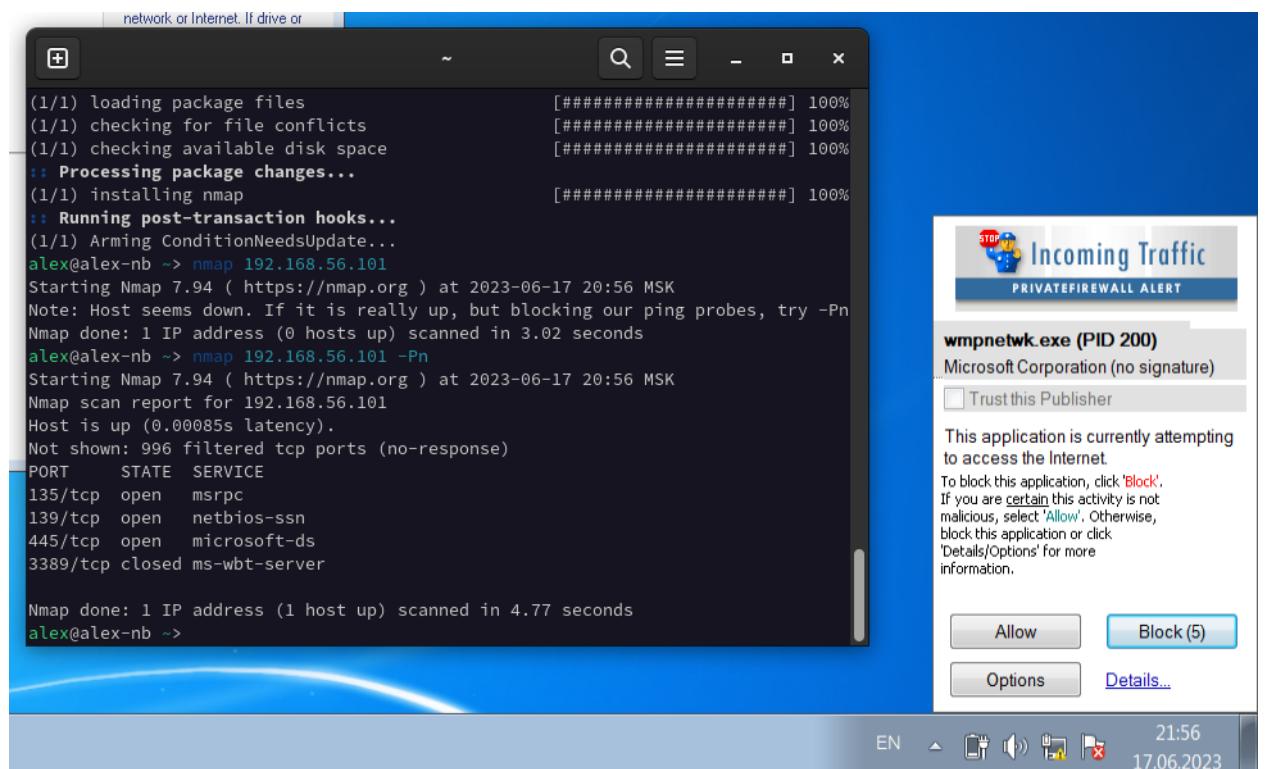


Рисунок 18 – Запросы

После запрета на эти запросы повторяем сканирование. В результате сканер видит 4 открытых порта и 1 закрытый.

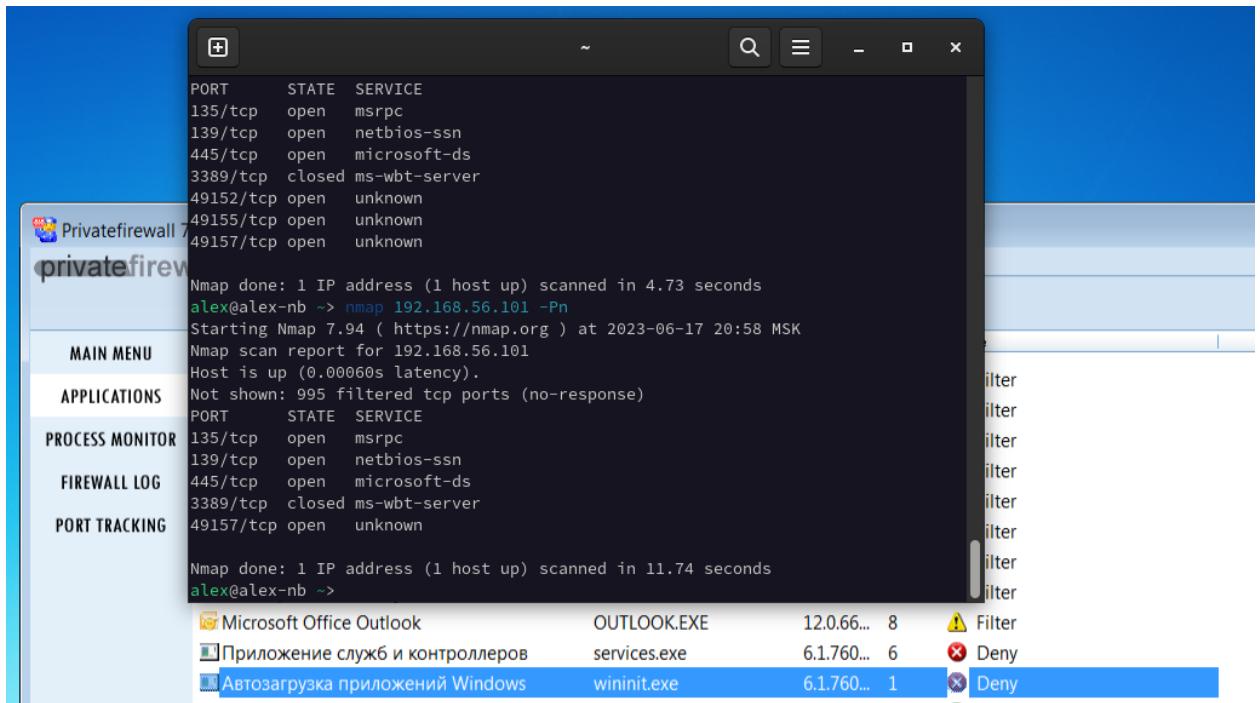


Рисунок 19 – Заблокированные сервисы

Переведём фаервол в зелёный режим — теперь весь трафик разрешён. Видим, что появились несколько новых открытых портов (Рисунок 20).

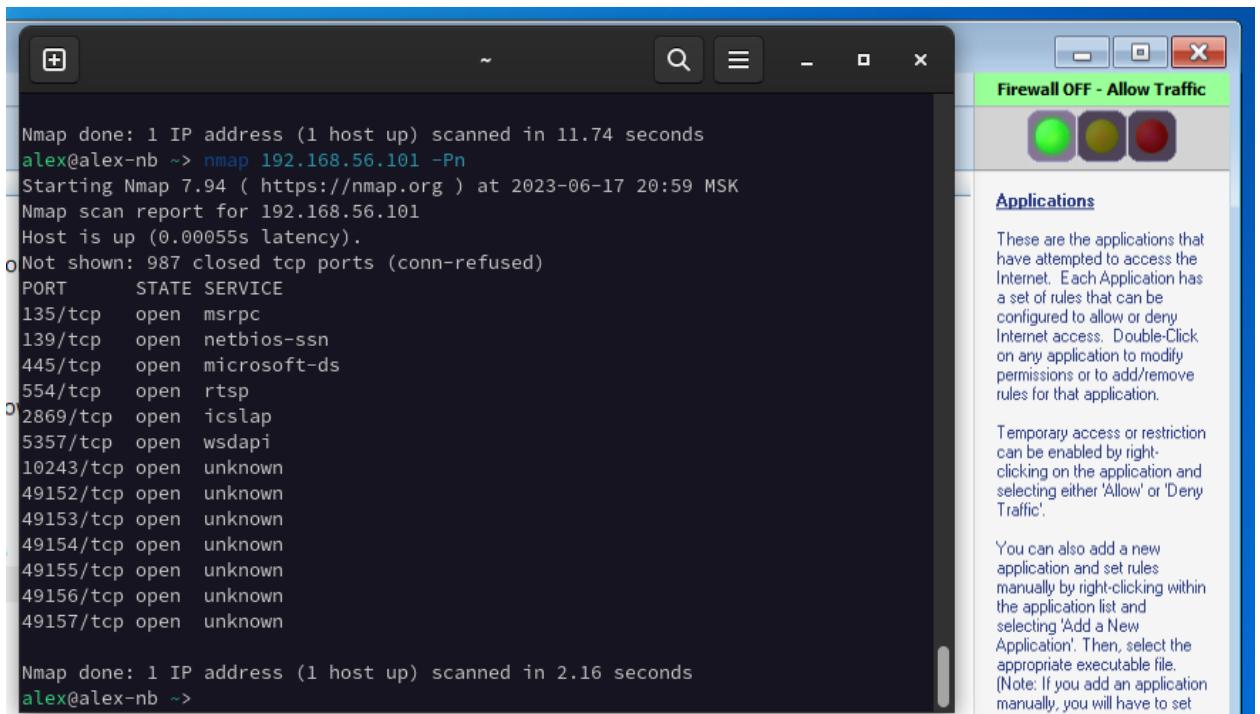
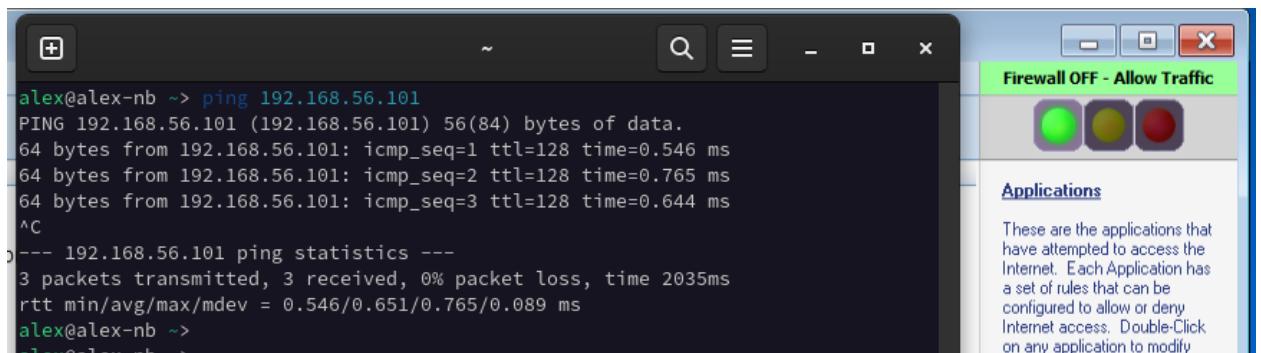


Рисунок 20 – Трафик разрешён

Команда ping также срабатывает в таком режиме (Рисунок 21).



```
alex@alex-nb ~> ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=128 time=0.546 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=128 time=0.765 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=128 time=0.644 ms
^C
--- 192.168.56.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2035ms
rtt min/avg/max/mdev = 0.546/0.651/0.765/0.089 ms
alex@alex-nb ~>
```

Рисунок 21 – Команда ping работает

Вернём фаервол в режим фильтрации. Команда ping больше не работает (Рисунок 22).

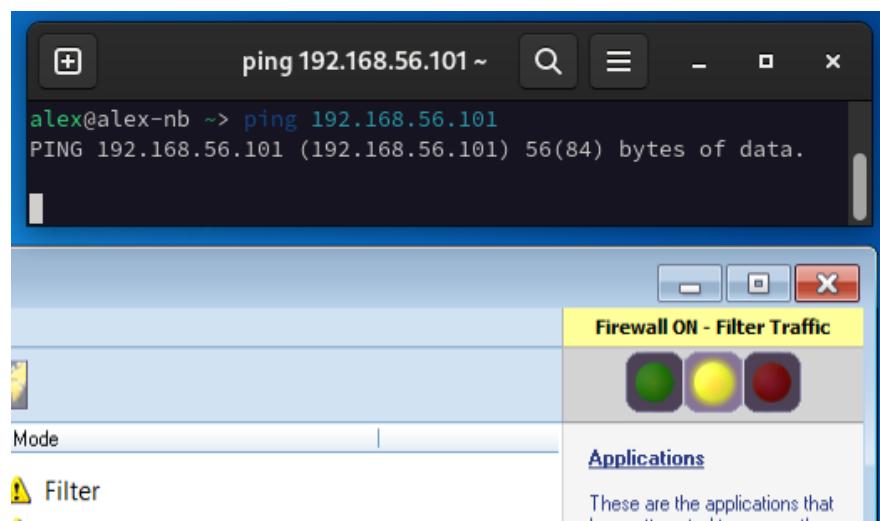


Рисунок 22 – Команда ping не работает

### **3 Выводы о проделанной работе**

Я изучил и приобрёл навыки работы с программными межсетевыми экранами, различные конфигурации персонального межсетевого экрана, а также управление соединениями с помощью персонального межсетевого экрана.