1 Устанавливаем Glasswire (один из приведенных персональных межсетевых экранов по списку ниже, вариант 5 (( 16 mod 6 ) + 1)):

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Изображение выглядит как текст, снимок экрана, Операционная система, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Устанавливаем русский язык в настройках приложения:

Изображение выглядит как текст, программное обеспечение, Значок на компьютере, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

2 Изучаем и подробно описываем настройки межсетевого экрана (поварьировать настройки политик, конфигурацию, журналирование и тд):

2.1 Основный вид брандмауэра “GlassWire защита” имеет следующий вид:

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Контент, сгенерированный ИИ, может содержать ошибки.

Здесь отображены приложении, их версии, входящий и исходящий трафик. Также можно заблокировать подключение определенного приложения к сети:



После настройки:

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Также имеется функция оценки безопасности GlassWire:

Изображение выглядит как текст, снимок экрана, Шрифт, число

Контент, сгенерированный ИИ, может содержать ошибки.

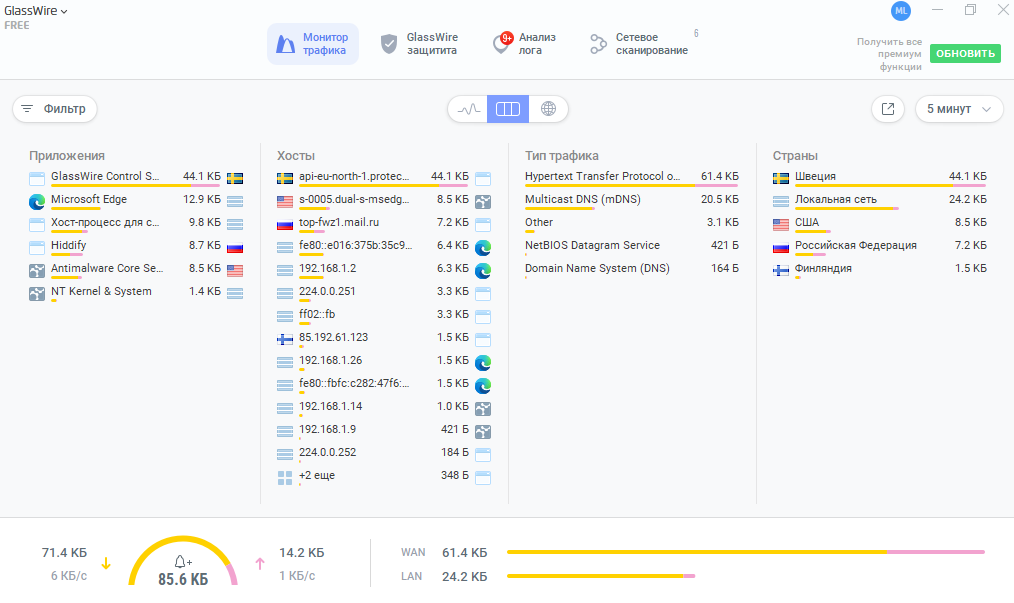
А также присутствует возможность проверить файл с помощью API VirusTotal:



Результат:



2.2 Ещё одна из основных функций – монитор трафика, где с помощью графика или таблицы можно отобразить активность приложений в сети за последние 5 минут / 3 часа / 1день:



Например, попробуем подключиться к прокси-серверу через приложение hiddify, видим в мониторе трафике следующие изменения:

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Контент, сгенерированный ИИ, может содержать ошибки.

Также попробуем загрузить страницу интернет-ресурса “Яндекс дзен”, видим в мониторе трафике следующие изменения:

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Контент, сгенерированный ИИ, может содержать ошибки.

2.3 GlassWire также позволяет сделать сетевое сканирование:

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Запустим ещё одну виртуальную машину в локальной сети и после ещё одного сканирования видим ещё одного пользователя:

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Контент, сгенерированный ИИ, может содержать ошибки.

2.4 Также существует некоторые платные функции безопасности:

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

На этом возможности бесплатной версии GlassWire заканчиваются. Для выполнения следующих заданий будем использовать встроенный в операционную систему Windows Defender Firewall.

3 Создаём не менее трёх сетевых соединений, помимо существующих (загрузка через браузер, удаленный доступ, доступ к веб страницам, доступ по FTP и др.):  
3.1 Создаём подключение по FTP с помощью FileZilla

Скачиваем FileZilla с официального сайта:

Изображение выглядит как текст, снимок экрана, Шрифт, число

Контент, сгенерированный ИИ, может содержать ошибки.

Устанавливаем соединение:

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Контент, сгенерированный ИИ, может содержать ошибки.

Подключаемся к серверу и пробуем передать файлы на виртуальную машину:

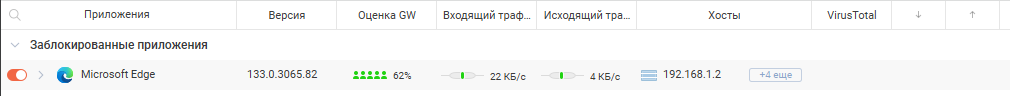
Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Контент, сгенерированный ИИ, может содержать ошибки.

4 Рассмотрим различные способы блокировки сетевых соединений (по порту, по приложению и иные) и выполним апробацию блокировки/разрешения соединений из задания 3:

4.1 Файрволл GlassWire представляет возможность блокировки сетевого трафика для конкретного приложения:

Блокируем трафик для браузера:

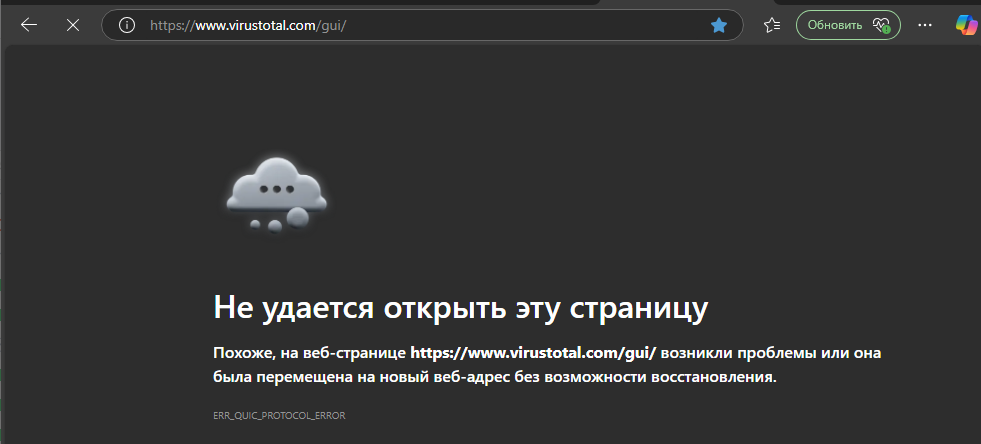


До включения настройки:

Изображение выглядит как текст, снимок экрана, программное обеспечение, мультимедиа

Контент, сгенерированный ИИ, может содержать ошибки.

После включения настройки:



4.2 Приведём примеры заблокированных/разрешенных соединений, инициированных в задании 3:

4.2.1 Заблокируем подключение по FTP. Создаём новое правило, запрещающие подключение по порту 21:

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

До включения настройки:

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

После включения настройки:

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Контент, сгенерированный ИИ, может содержать ошибки.

4.2.2 Заблокируем подключение по RDP:



Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

До включения настройки подключаемся через удалённый рабочий стол (mstsc):

Изображение выглядит как текст, программное обеспечение, снимок экрана, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Успешно подключаемся:

Изображение выглядит как текст, трава, компьютер, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

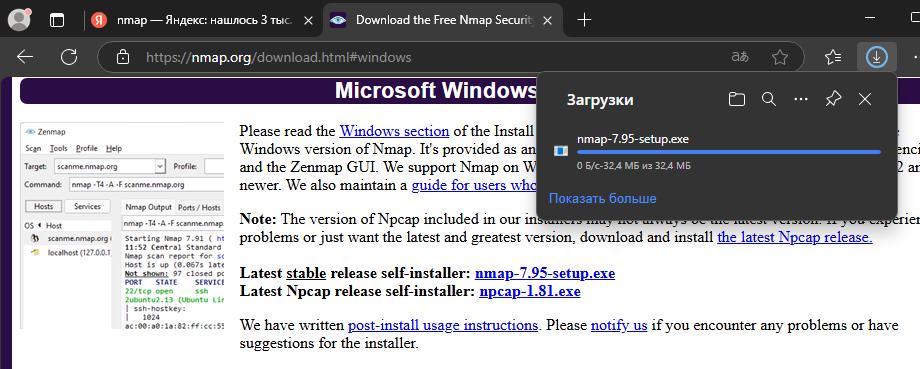
После включения правила:

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Контент, сгенерированный ИИ, может содержать ошибки.

5.1 Разворачиваем вторую виртуальную машину, настраиваем между ними сеть, выполняем сканирование виртуальной машины с межсетевым экраном при помощи nmap

Скачиваем программу nmap с официального сайта:



Проверяем подключение между двумя ВМ:

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Проводим сканирование с помощью Zenmap и в результате видим 4 открытых порта:

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Теперь включаем ранее подключенное правило “block rdp” и настраиваем новую блокировку 445 порта:

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Проводим снова сканирование с помощью zenmap и теперь не видим закрытые порты:

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

6 Напишем код на python, реализующее некоторые соединения:

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

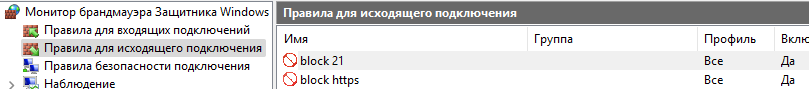
Контент, сгенерированный ИИ, может содержать ошибки.

Результат выполнения команды:

Изображение выглядит как текст, Шрифт, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Теперь применим правила брандмауэра, заданные заранее:



Выполняем код ещё раз и видим ошибки подключения:

