Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Кафедра автоматизації проектування

 енергетичних процесів і систем

**Звіт**

**з циклу лабораторних робіт**

**з дисципліни**

**„Безпека та приватність в Інтернеті”**

Лабораторна  робота № 2

Мережеві екрани. Робота з VPN.

Виконала: **Юрченко Богдана**

Студентка групи:   **ТВ-01 мп**

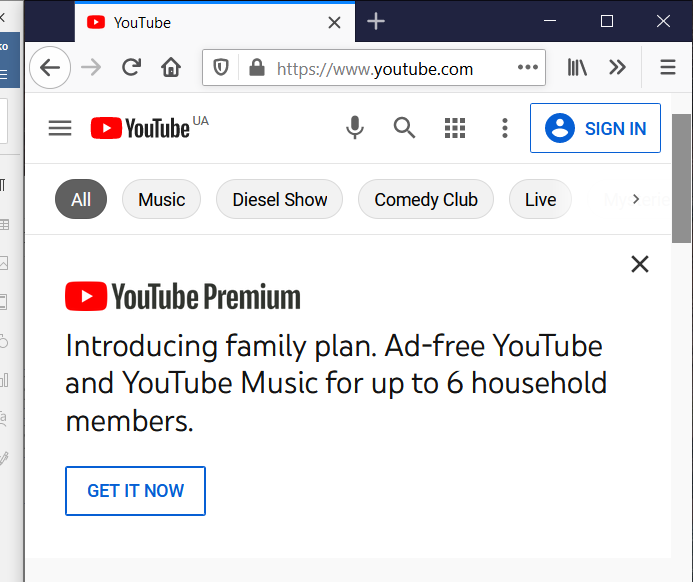
Перевірив викладач: **проф. Гаврилко Є. В.**

Київ - 2021

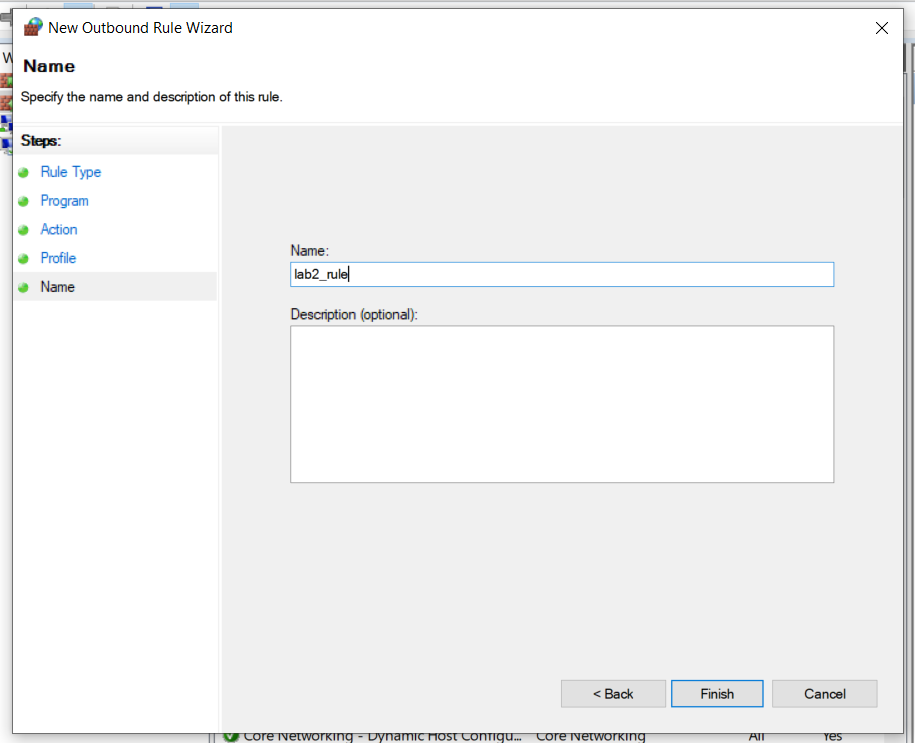
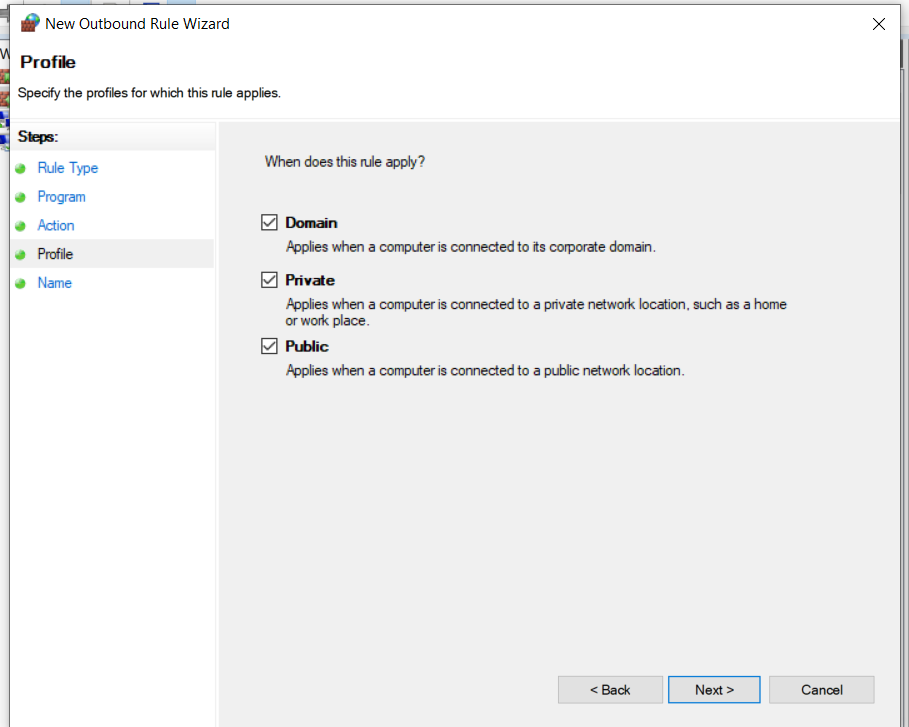
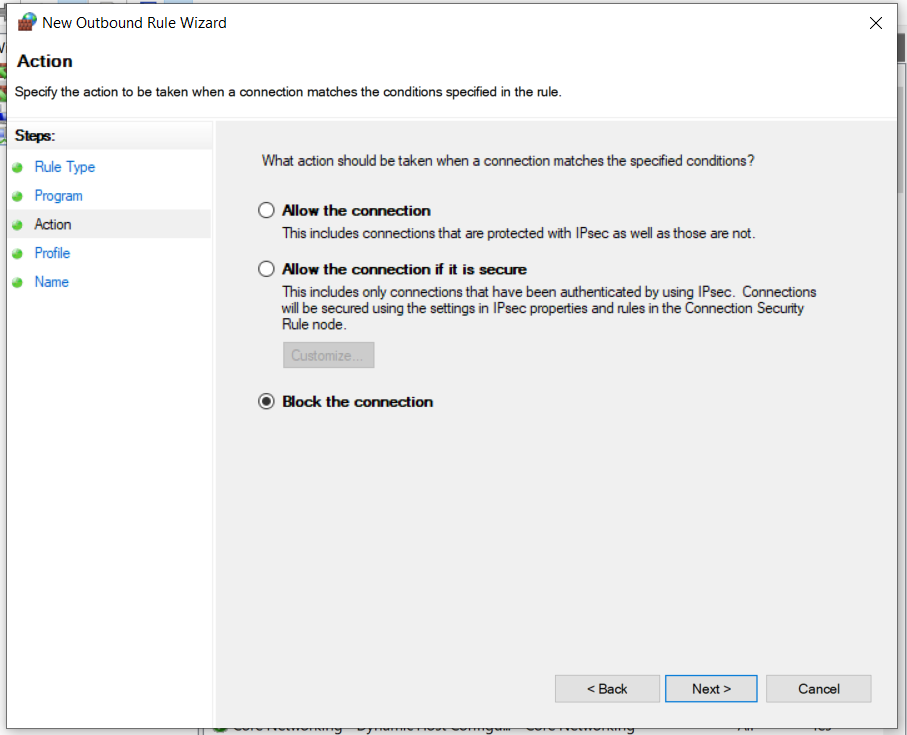
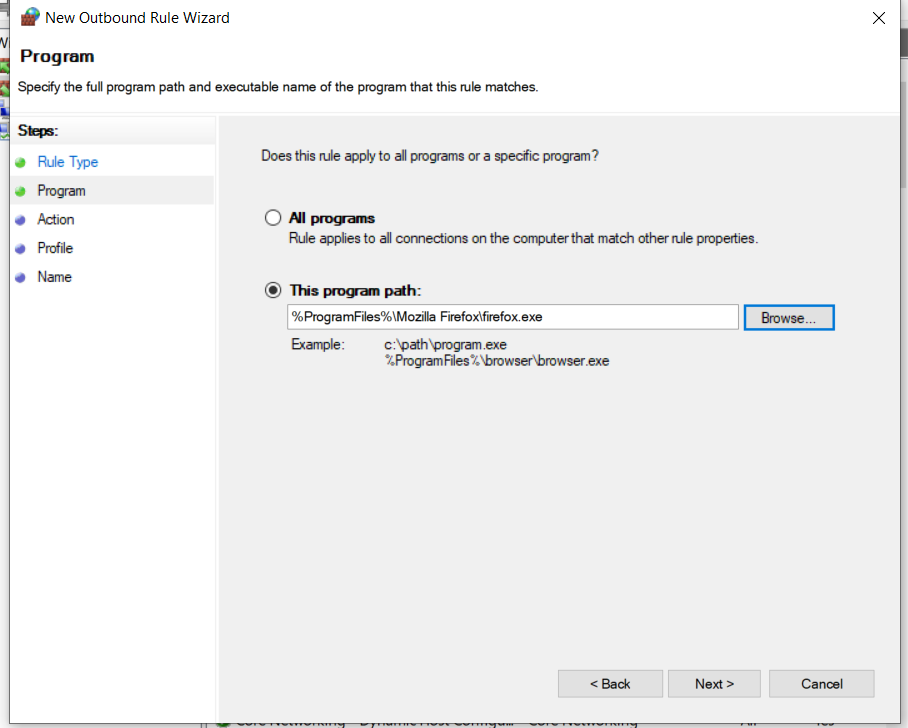
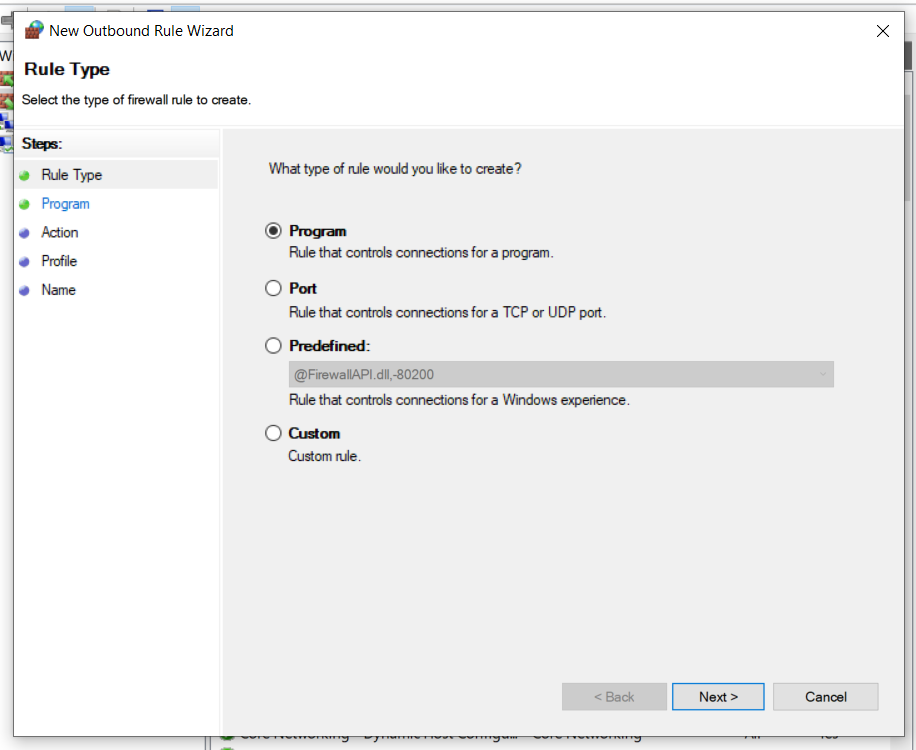
## Кроки виконання лабораторної роботи та завдання.

**1. Завантажте окремий браузер для лабораторної роботи. Впевніться в можливості цього браузера підключатися до інтернету на вашій основній системі.**

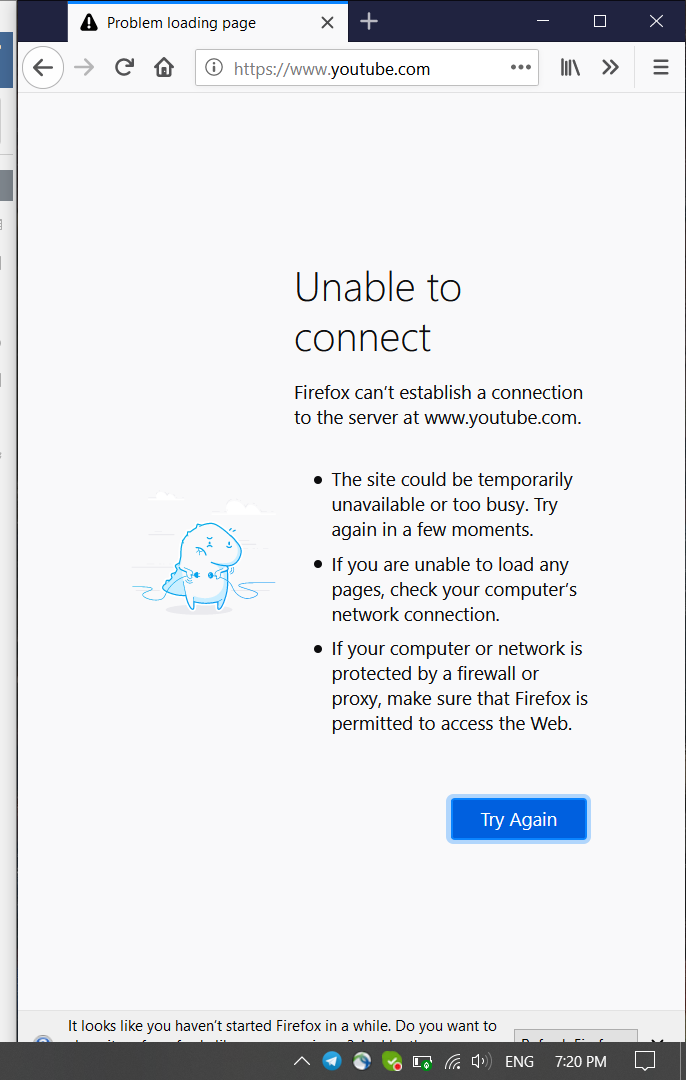
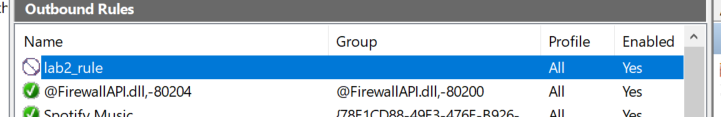
Для виконання роботи було встановлено новий браузер Firefox



**2. Відконфігуруйте мережевий екран Windows. Додайте правило, яке забороняє підключення для виконуємого файлу завантаженого браузера. Перевірте правильність роботи створеного правила.**



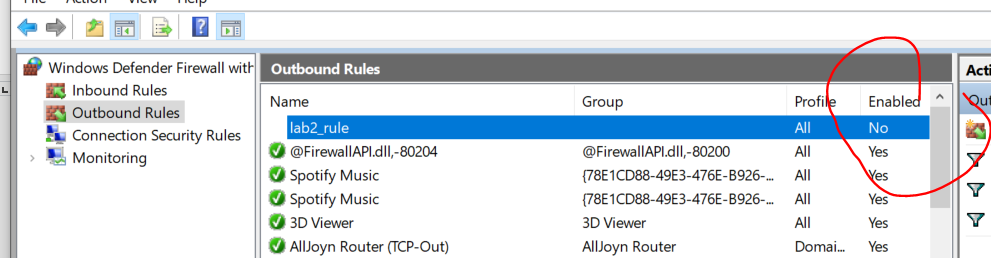
Відразу після створення правила, сторінка в браузері була рефрешнута. Браузер не зміг підключитися і відобразити сторінку.



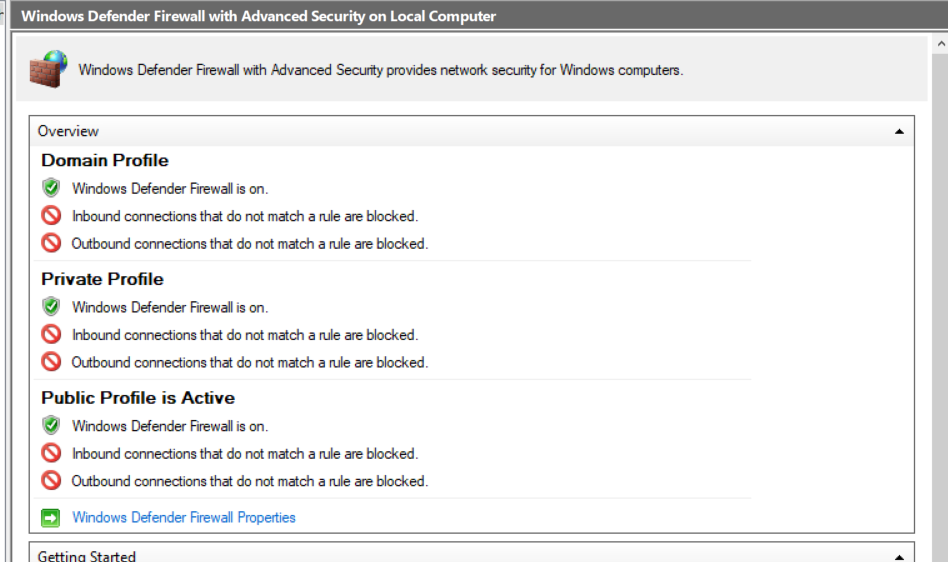
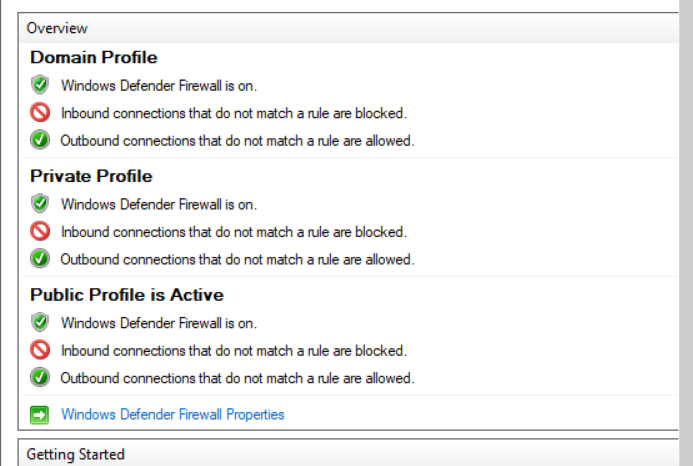
**3. Зробіть неактивним створене правило. Переведіть режим мережевого екрану для поточного профілю підключення в режим "білого списку".**

**Для цього змініть налаштування для поточного профілю із "Вихідні підключення, що не відповідають жодному правилу, дозволені" на "Вихідні підключення, що не відповідають жодному правилу, заборонені".**

**Впевніться у роботі нових налаштувань - спробуйте відкрити будь-яку сторінку у браузері. Також спробуйте запустити команду ping з командної строки на адресу google.com.**

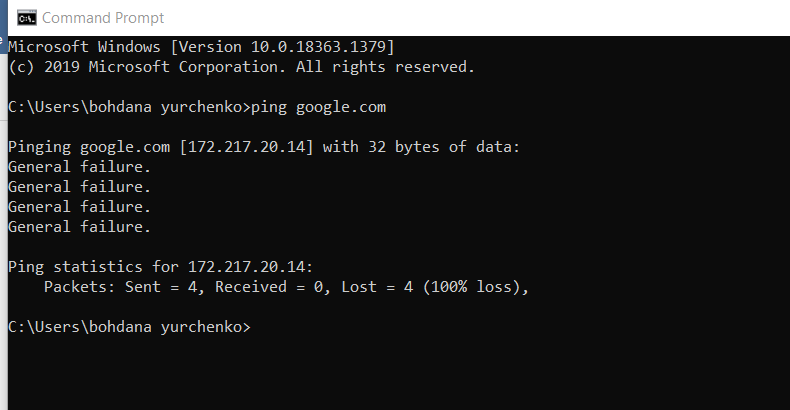


Після цього сторінка [YouTube.com](http://YouTube.com) стала знову доступною в браузері.



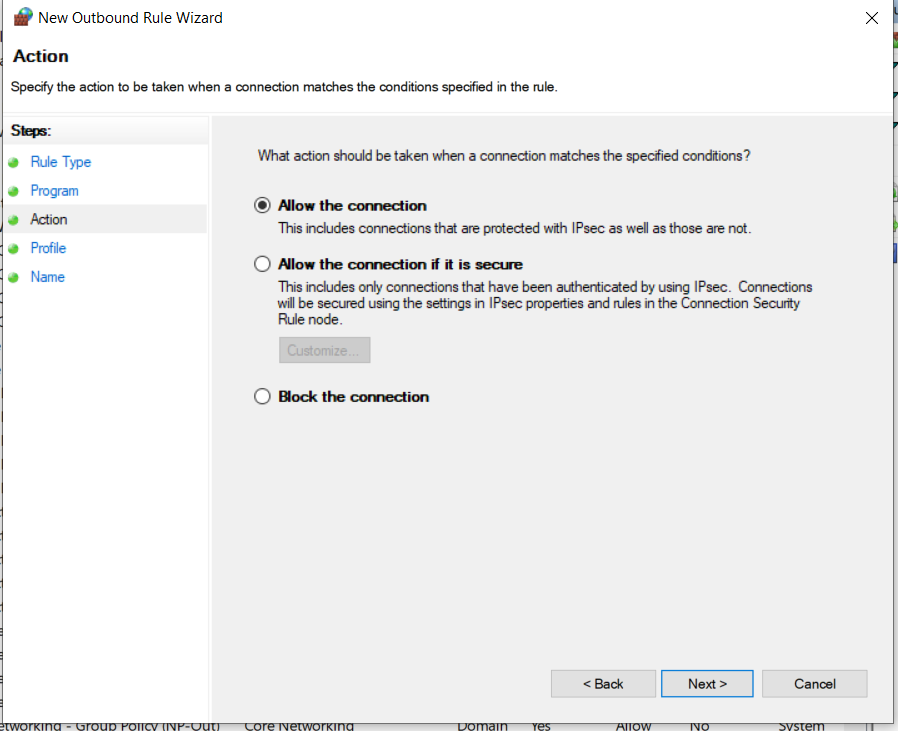
Після цього сторінка [YouTube.com](http://YouTube.com) стала знову НЕ доступною в браузері.

Результати пінгування

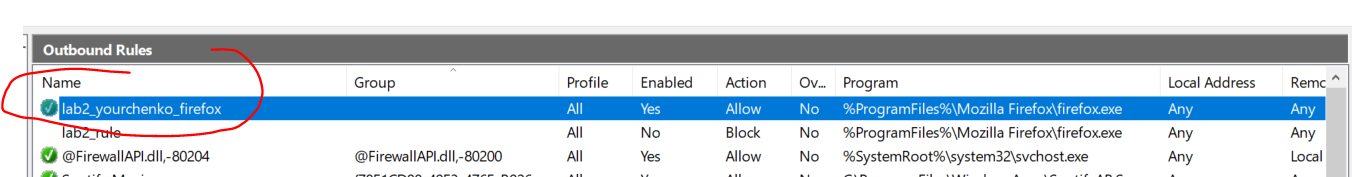


**4. Тепер мережевий екран працює в режимі білого списку. Не змінуючи налаштувань профілю, додайте правило, що дозволяє підключити ваш браузер до інтернету.**

Створення нового рула для виконуючого файлу Firefox

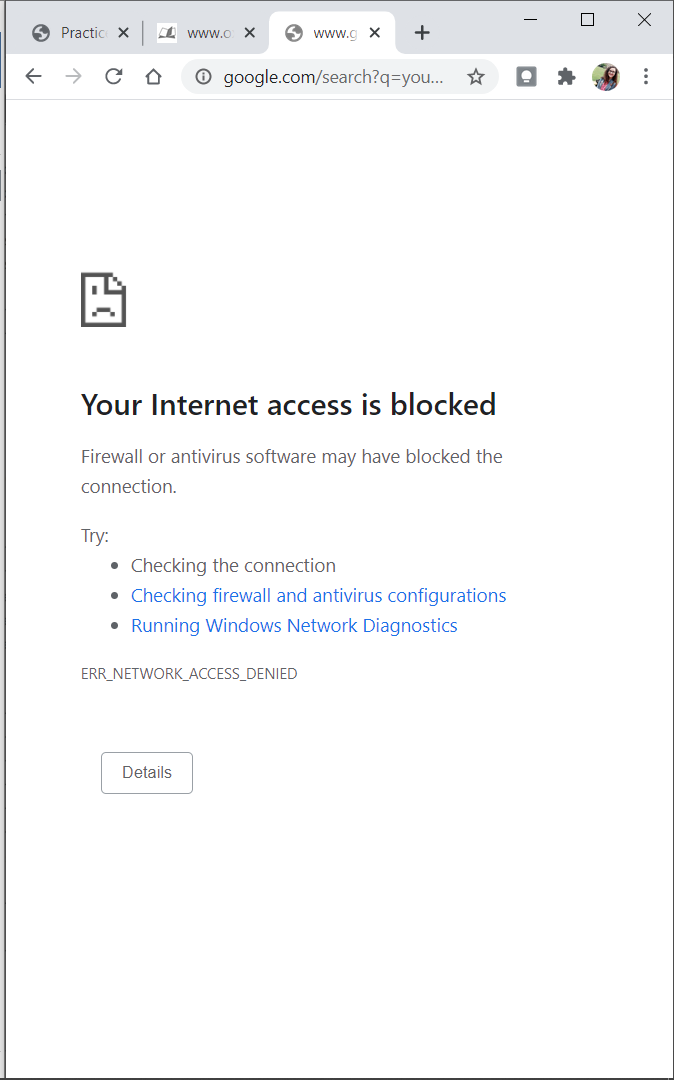


Новий рул

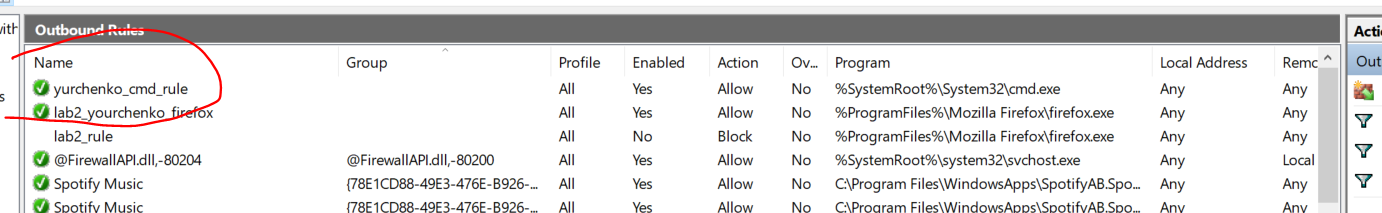
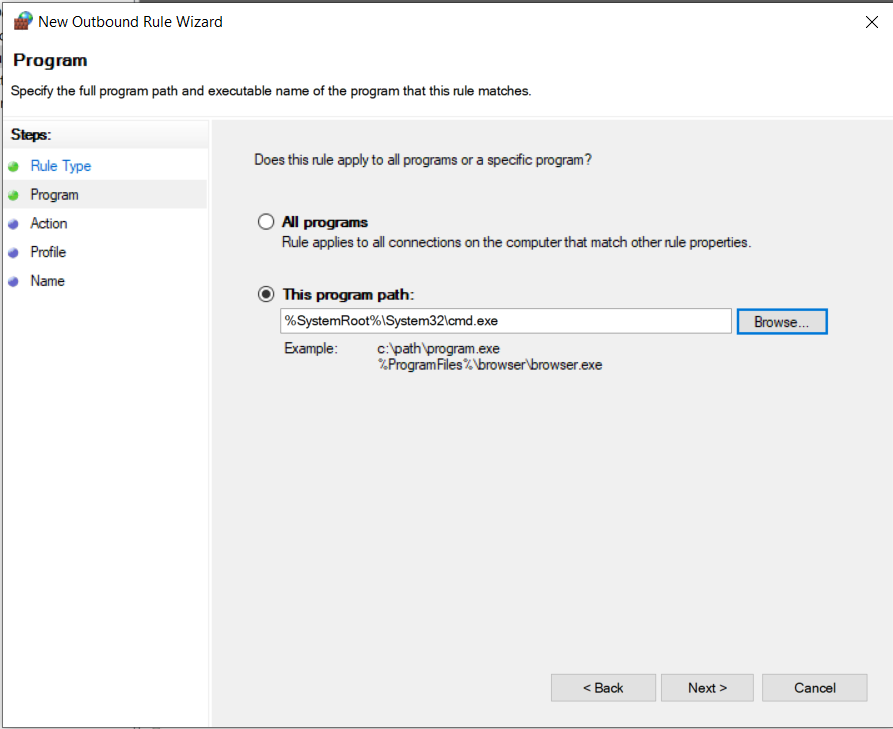


Після цього інтернет сторінки із браузера Firefox знову стали доступними.

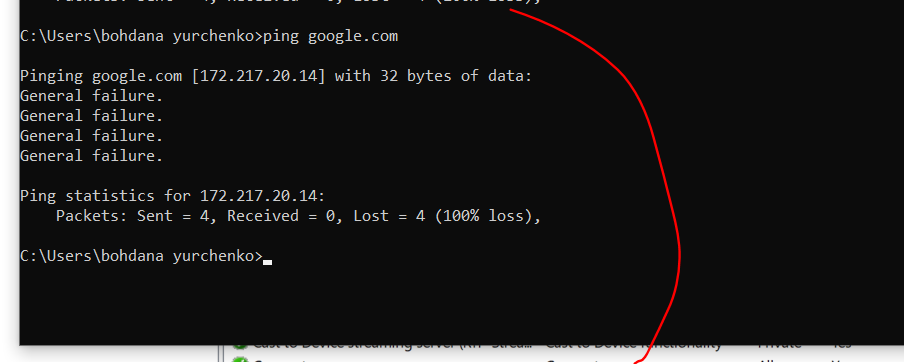
В той же час, інтернет сторінки із іншого браузера ( Google Chrome ) стали недоступні



**5. Спробуйте додати до правил таке, що дозволить підключення командної строки Windows, після чого знову спробуйте запустити команду ping на адресу google.com. Опишіть отриманий результат. Чому саме ви отримали такий результат?**

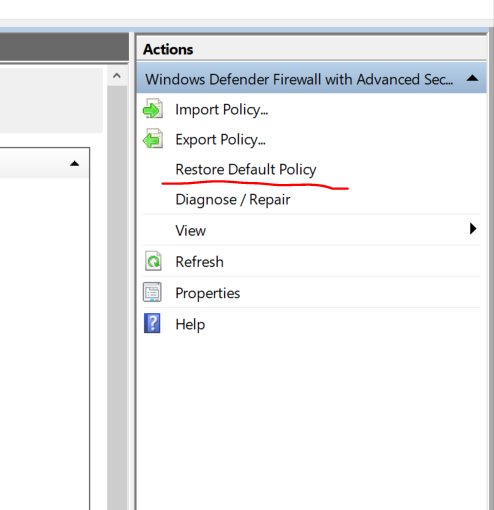


Результати після додавання нового правилу для [cmd.exe](http://cmd.exe) Пінг все іще не проходить. Не проходить тому, що ping - це окрема від cmd програма, і для неї ніякого правилу не існує.

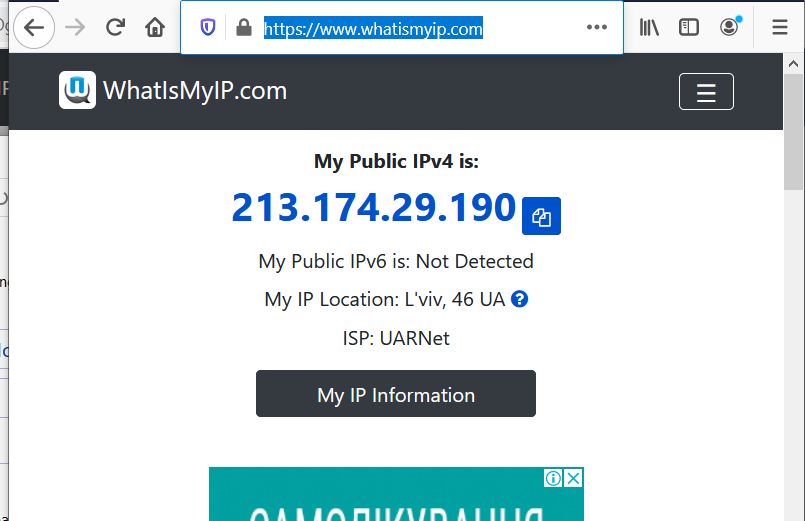
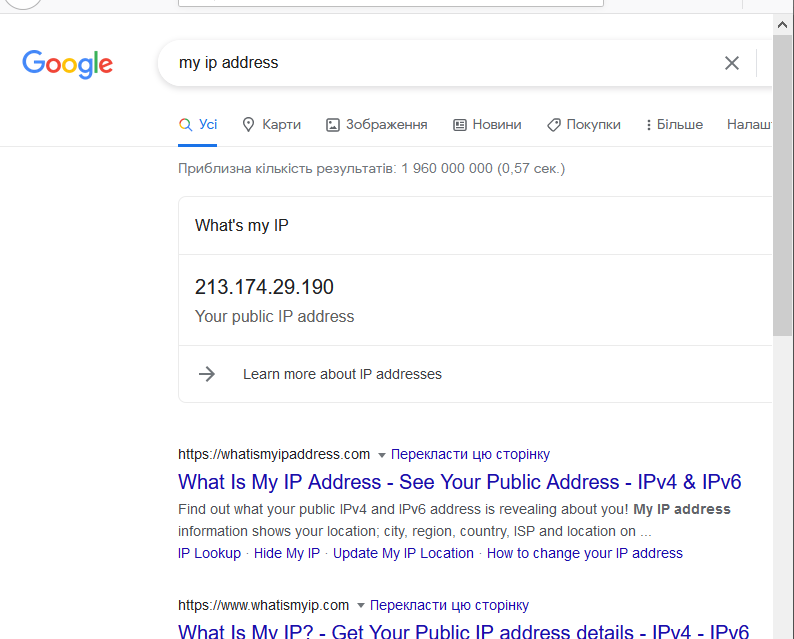


**6. Поверніть всі ваші налаштування мережевого екрану на налаштування за замовчуванням, видаліть або зробіть неактивними нові правила.**

Конфігурацію було повернено за допомогою функції

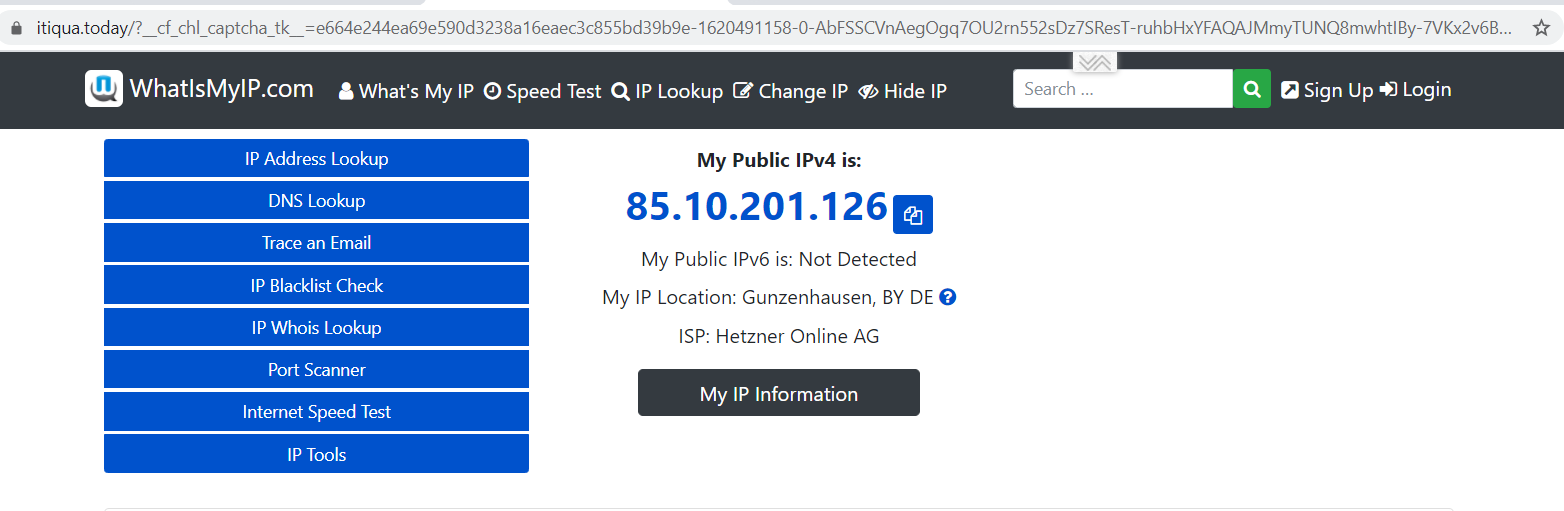


**7. Завантажте у браузері сторінку, яка відобразить вашу поточну IP-адресу.**



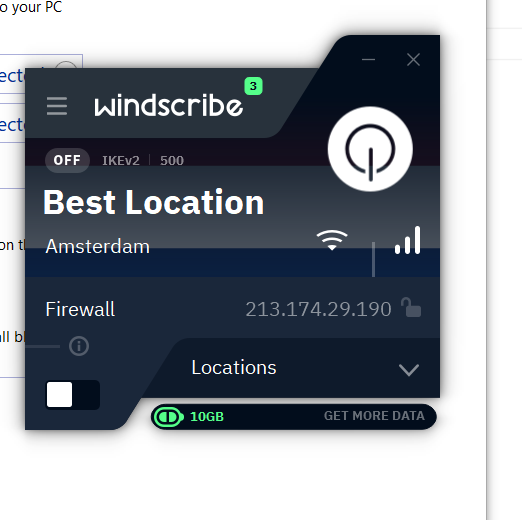
**8. Використайте проксі-сервер для підключення до тієї ж сторінки. Можете використовувати налаштування проксі у браузері із зазначенням IP-адреси і порту проксі-серверу (якщо маєте до такого серверу доступ), або використати онлайн web-проксі сервіс.**

Та ж сама сторінка із використанням онлайн проксі сервісу



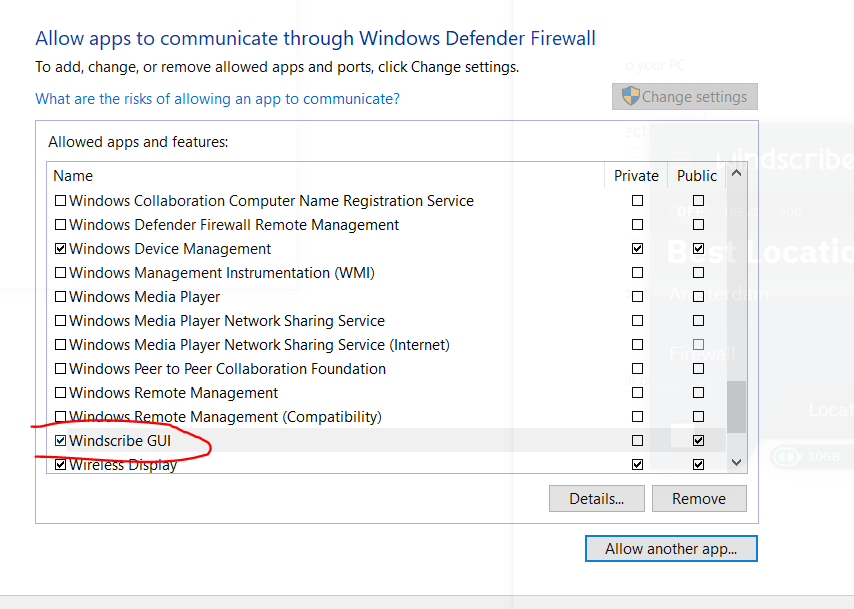
**9. Вимкніть налаштування проксі. Налаштуйте вашу операційну систему на роботу із VPN. VPN-провайдера оберіть самостійно (є безкоштовні варіанти з обмеженими функціями клієнту або перевірочним періодом). Перевірте правильність роботи VPN із декількома програмами (наприклад браузерами).**

В якості ВПН сервісу був обраний WIndscribe (має безкоштовний обмежений план), клієнти для різних операційних систем і розширення для браузерів.



**10. Налаштуйте мережевий екран таким чином, щоб доступ до інтернету для програм був доступним тільки під час роботи VPN.**

**Для цього може знадобитися змінити профілі активних підключень у Центрі управління мережами та спільним доступом, додати певні програми (виконуємі файли вашого VPN клієнту) до дозволених програм для всіх профілів, та змінити режим для доступу до інтернету для програм, яких немає у правилах для окремих профілів.**



## Відповіді на контрольні запитання

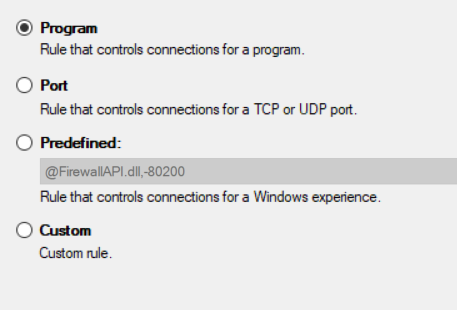
## **Що таке мережевий екран?**

Мережевий екран - це іще одна назва файрволла (firewall) або брандмауера. Це програмний продукт або комплекс, що захищає локальну мережу шляхом керування потоку даних між локальною мережею і зовнішнім світом.

## **Наведіть приклади вхідних та вихідних підключень, налаштування яких можуть регуляватися мережевим екраном.**

Підключення конкрерних програм, портів, кастомних.

Також рули можна налаштувати для роботи в конкретних мережах : приватній, публічній та доменній.



## **Що таке профіль домену, приватний профіль, загальний профіль у налаштуваннях мережевого екрану Windows?**

Профіль домену застосовується до мереж, де хост-система може аутентифікуватися на контролері домену.

Приватний профіль - це призначений користувачем профіль і використовується для позначення приватних або домашніх мереж.

Загальним профілем є загальнодоступний профіль, який використовується для позначення загальнодоступних мереж, таких як точки доступу Wi-Fi у кав'ярнях, аеропортах та інших місцях.

## **Що таке проксі сервер?**

Проксі-сервер - це будь-яка машина, яка перекладає трафік між мережами або протоколами. Це посередницький сервер, який відокремлює клієнтів-кінцевих користувачів від пунктів призначення, які вони переглядають. Проксі-сервери забезпечують різний рівень функціональності, безпеки та конфіденційності залежно від вашого випадку використання, потреб або політики компанії.

## **Які бувають основні типи проксі?**

Transparent Proxy

Anonymous Proxy

Distorting proxy

High Anonymity proxy

## **Що таке VPN?**

Virtual Private Network — віртуальна приватна мережа.

Технологія, що дозволяє створювати віртуальні захищені мережі поверх інших мереж із меншим рівнем довіри. Безпека передавання інформації через загальнодоступні мережі реалізована за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. Технологія VPN дозволяє об'єднати декілька географічно віддалених мереж (або окремих клієнтів) в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

## **Чим проксі відрізняються від VPN?**

VPN - підключення через віртуальну мережу, а проксі - підключення через сторонній сервер.

Якщо ви хочете дозволити своїй команді віддалено працювати із захищеним доступом до ресурсів компанії, налаштуйте та підтримуйте користувачів VPN для доступу до мережі за допомогою VPN.

Якщо ваші проблеми більше стосуються того, на які веб-сайти потрапляють мої користувачі, проксі-сервер є кращим інструментом.