НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Кафедра автоматизації проектування енергетичних процесів і систем

Лабораторна робота № 2

З дисципліни: «Безпека та приватність в Інтернеті»

**Виконав:**

студент 5 курсу

групи ТР-02мп, ТЕФ

Круглий Д.В.

**Перевірили:**

Касьянов А. / Гаврилко Є.В.

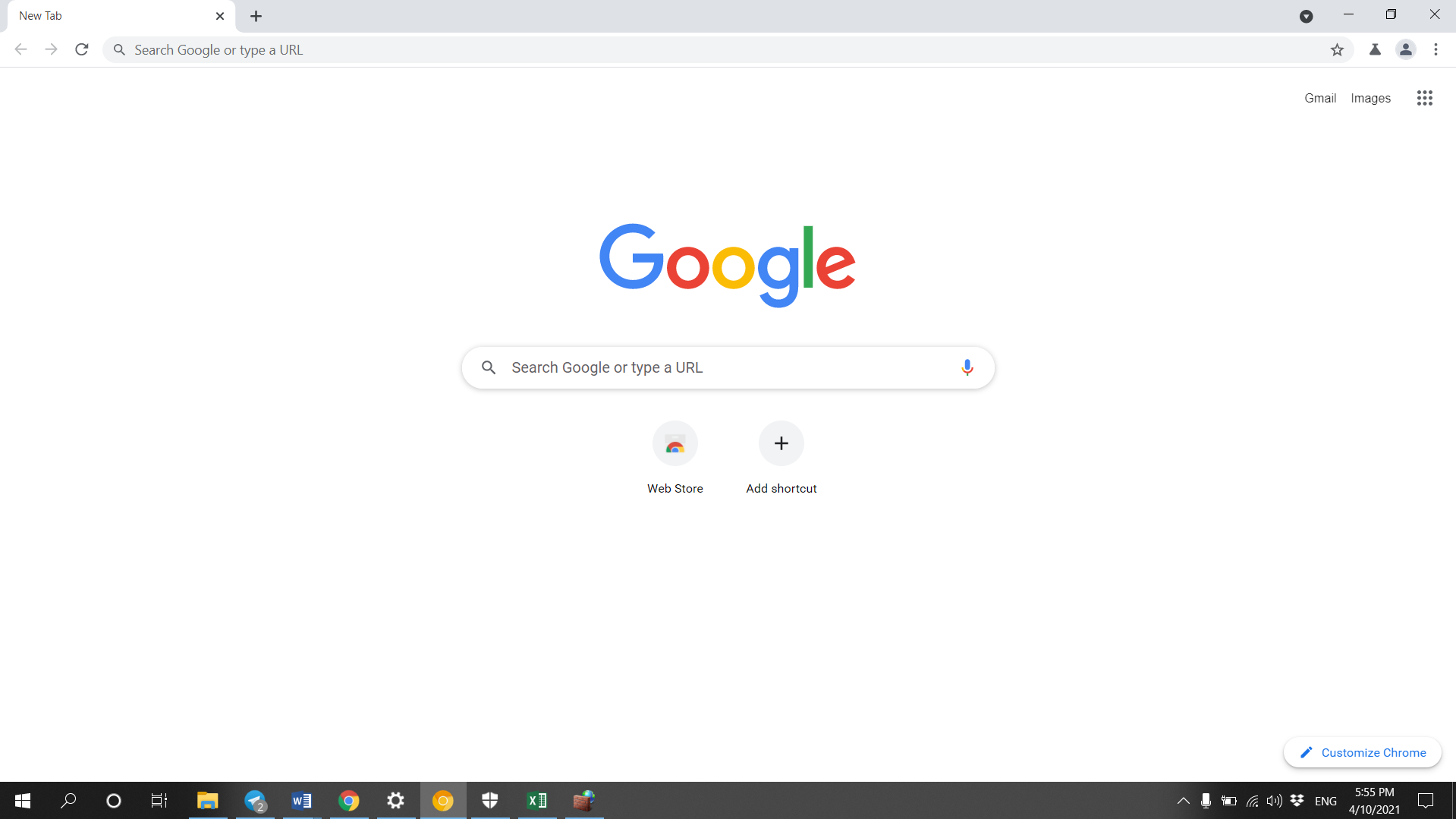
Київ – 2021

**Тема:** Мережеві екрани. Робота з VPN.

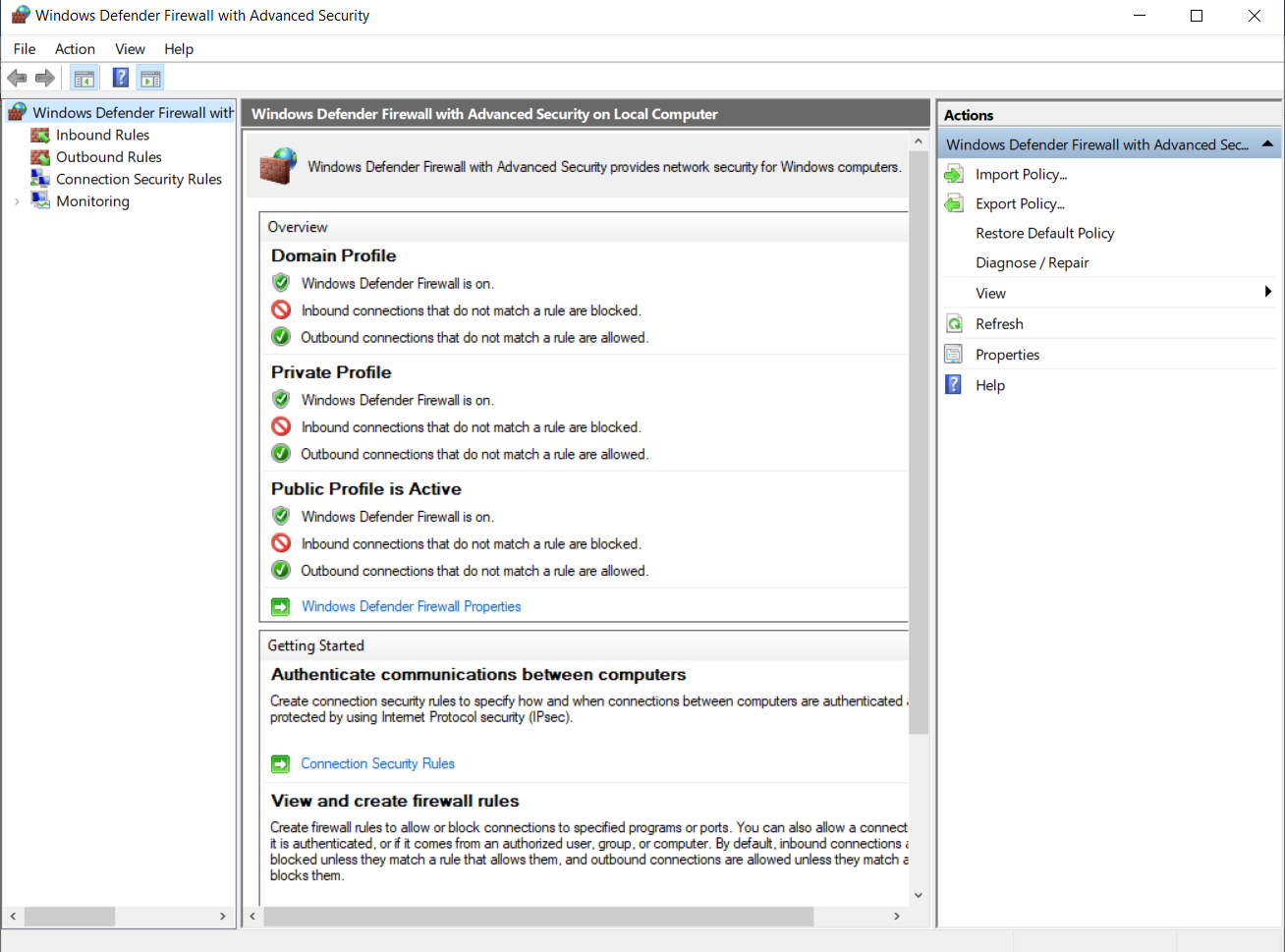
**Мета:** ознайомитись із мережевими екранами та навчитися працювати з ВПН.

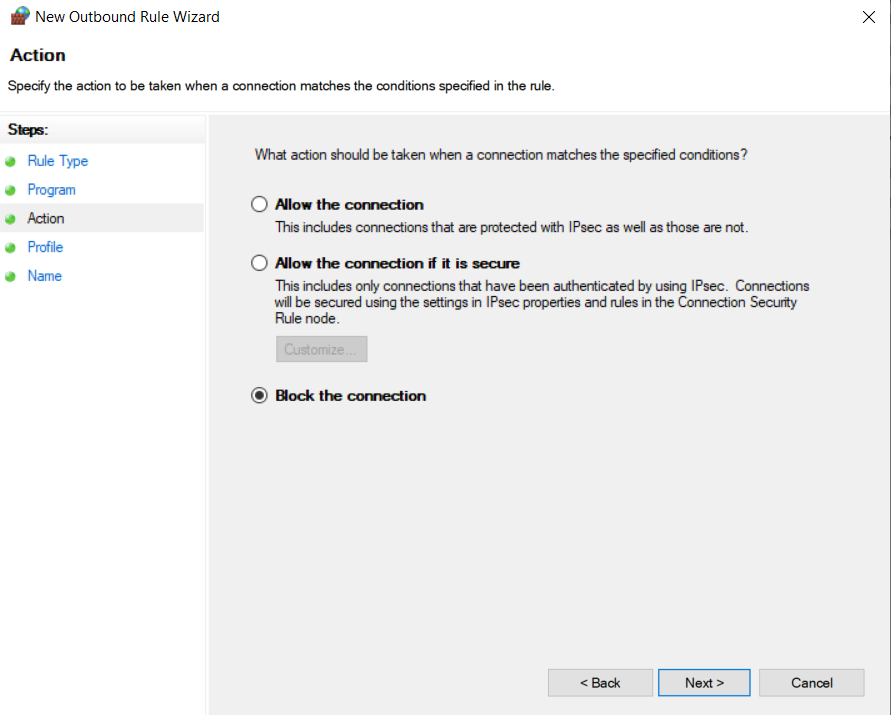
**Хід роботи**

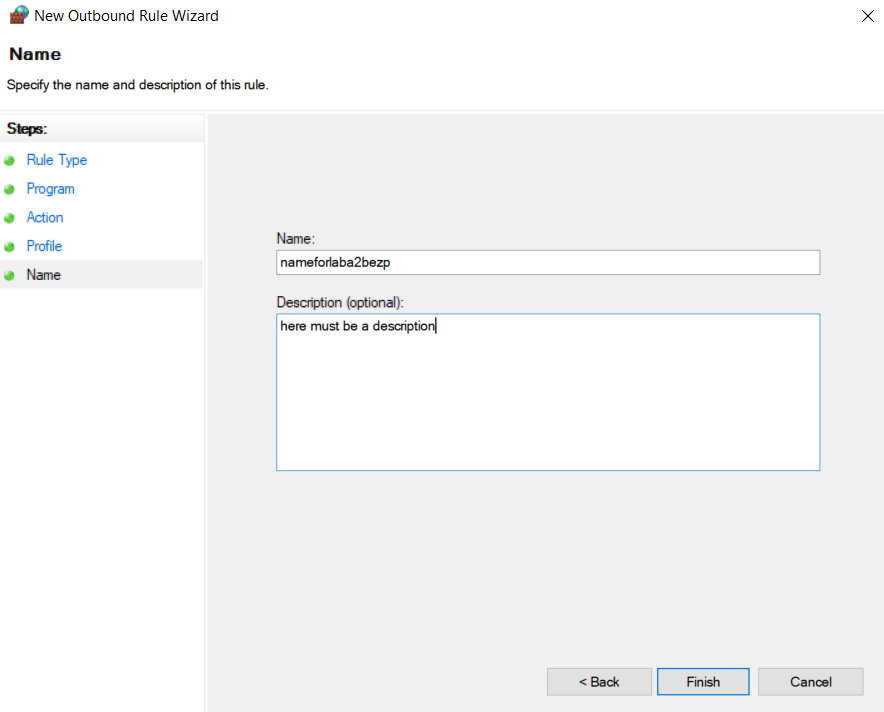
1. Завантажили окремий браузер *Google Chrome Canary* для виконання лабораторної роботи.

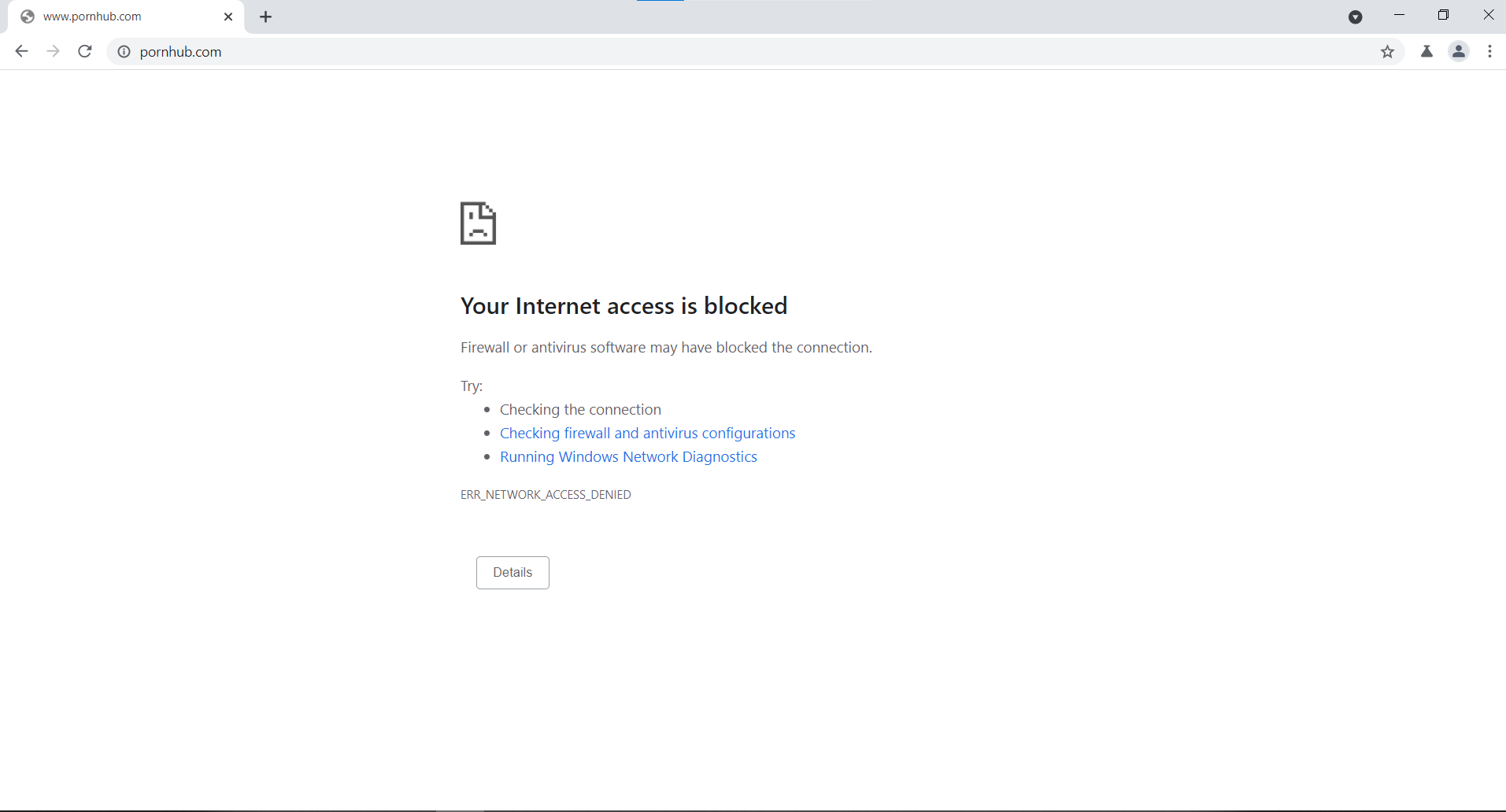


1. Відконфігурували мережевий екран Windows. Додайли правило, яке забороняє підключення для виконуємого файлу завантаженого браузера. Перевірили правильність роботи створеного правила.

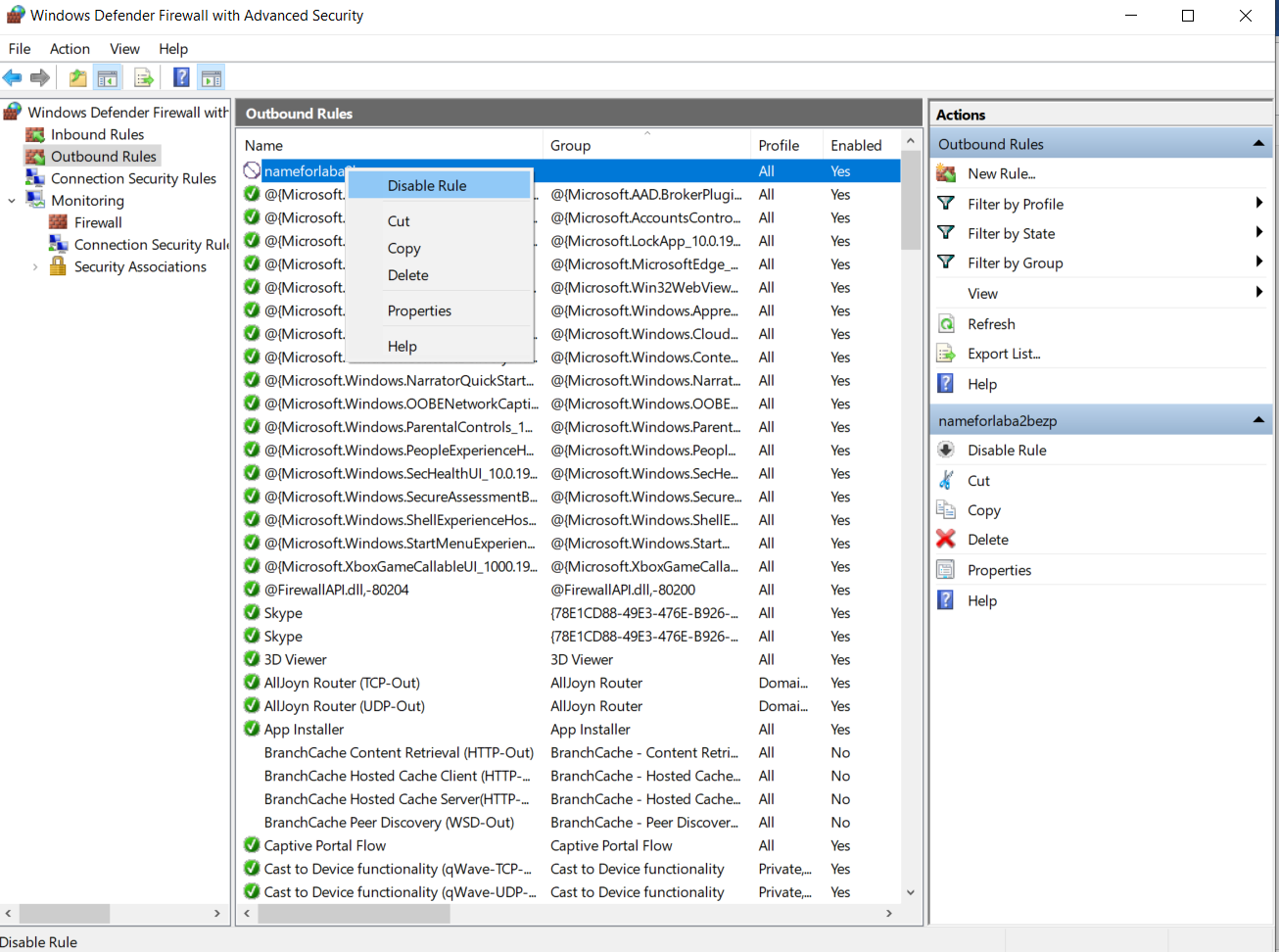


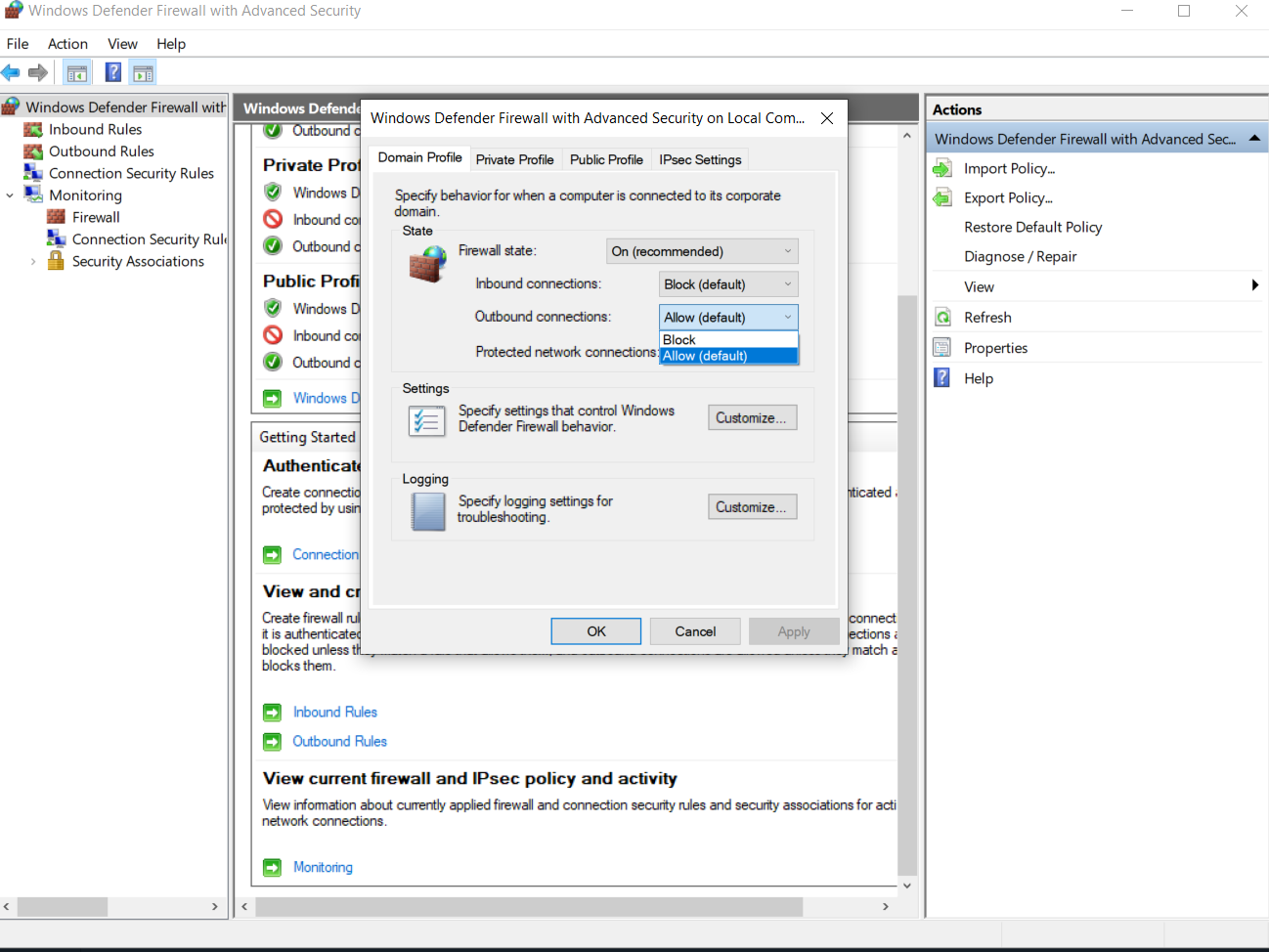




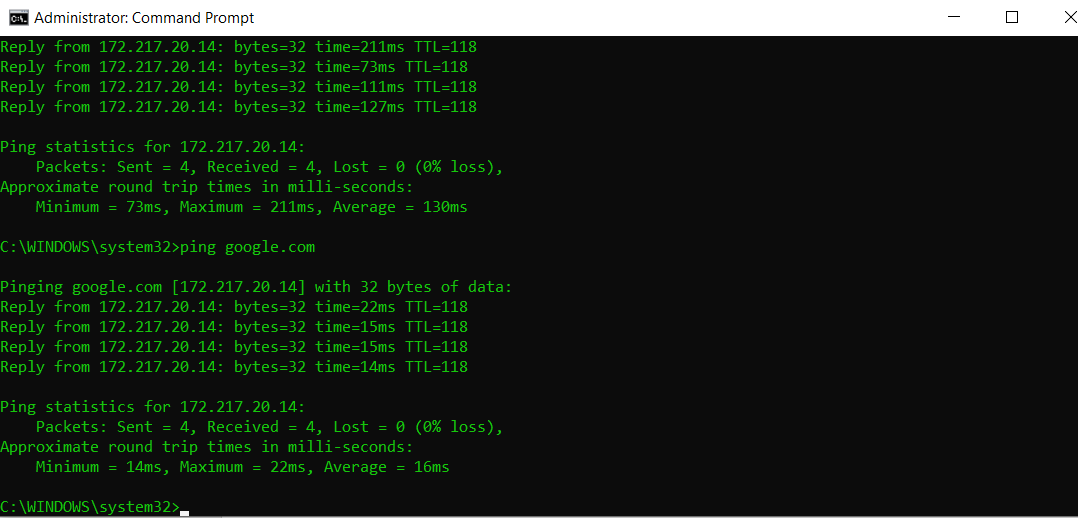


1. Зробили неактивним створене правило. Перевели режим мережевого екрану для поточного профілю підключення в режим "білого списку".

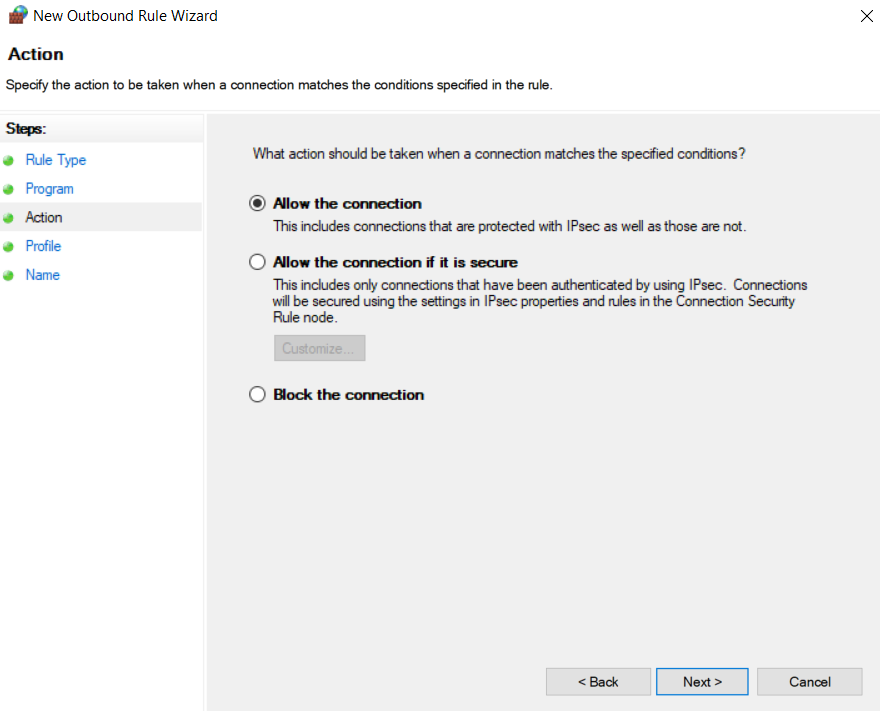




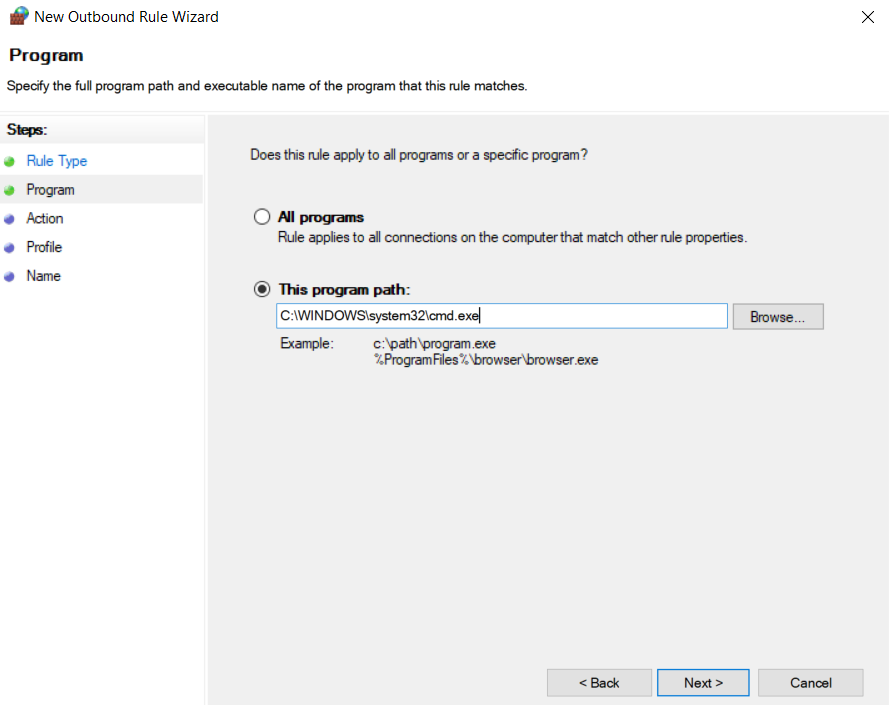
1. Пробуємо пропінгувати google.com .



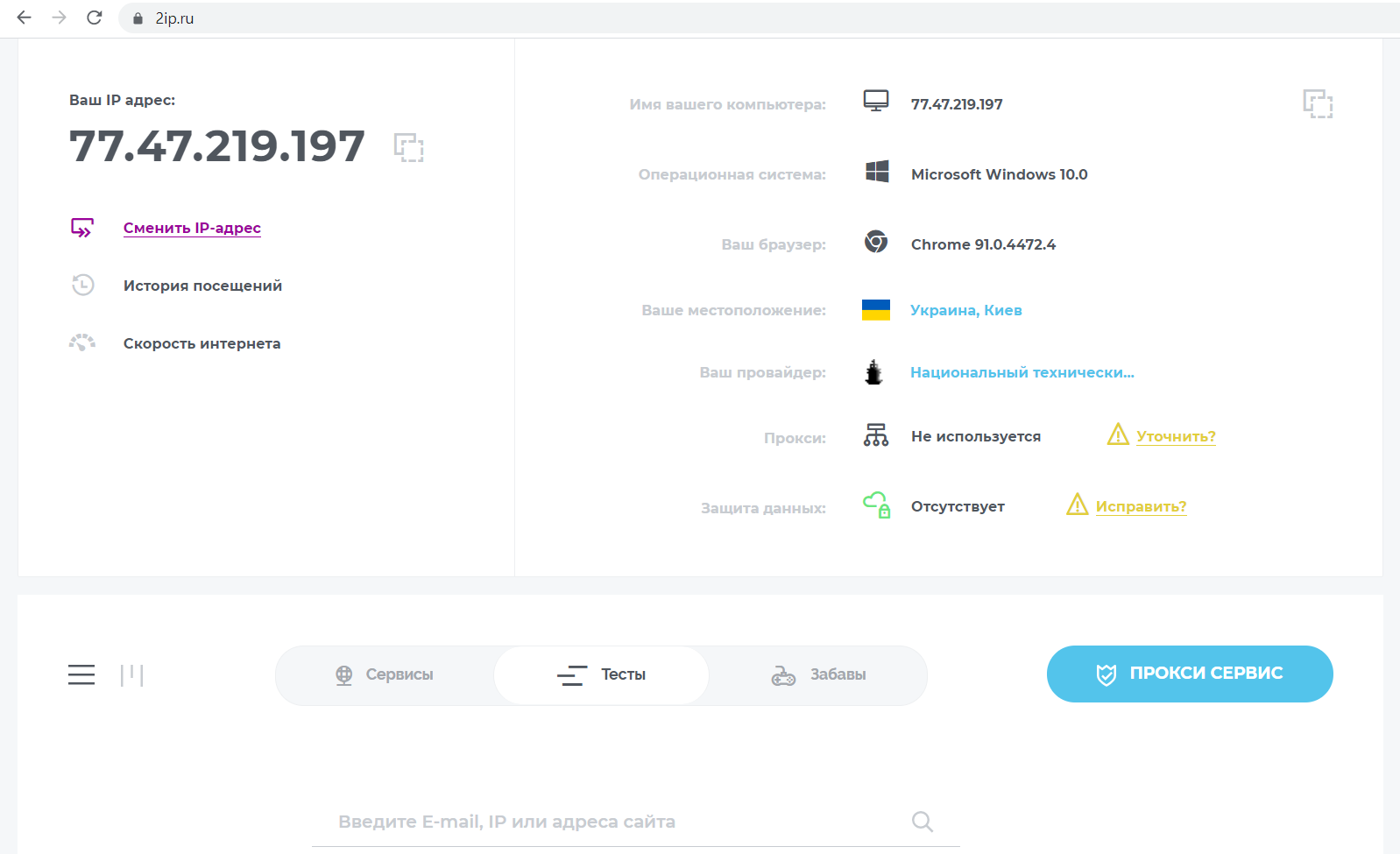
1. Не змінюючи налаштувань профілю, додаємо правило, що дозволяє підключити наш браузер до інтернету.



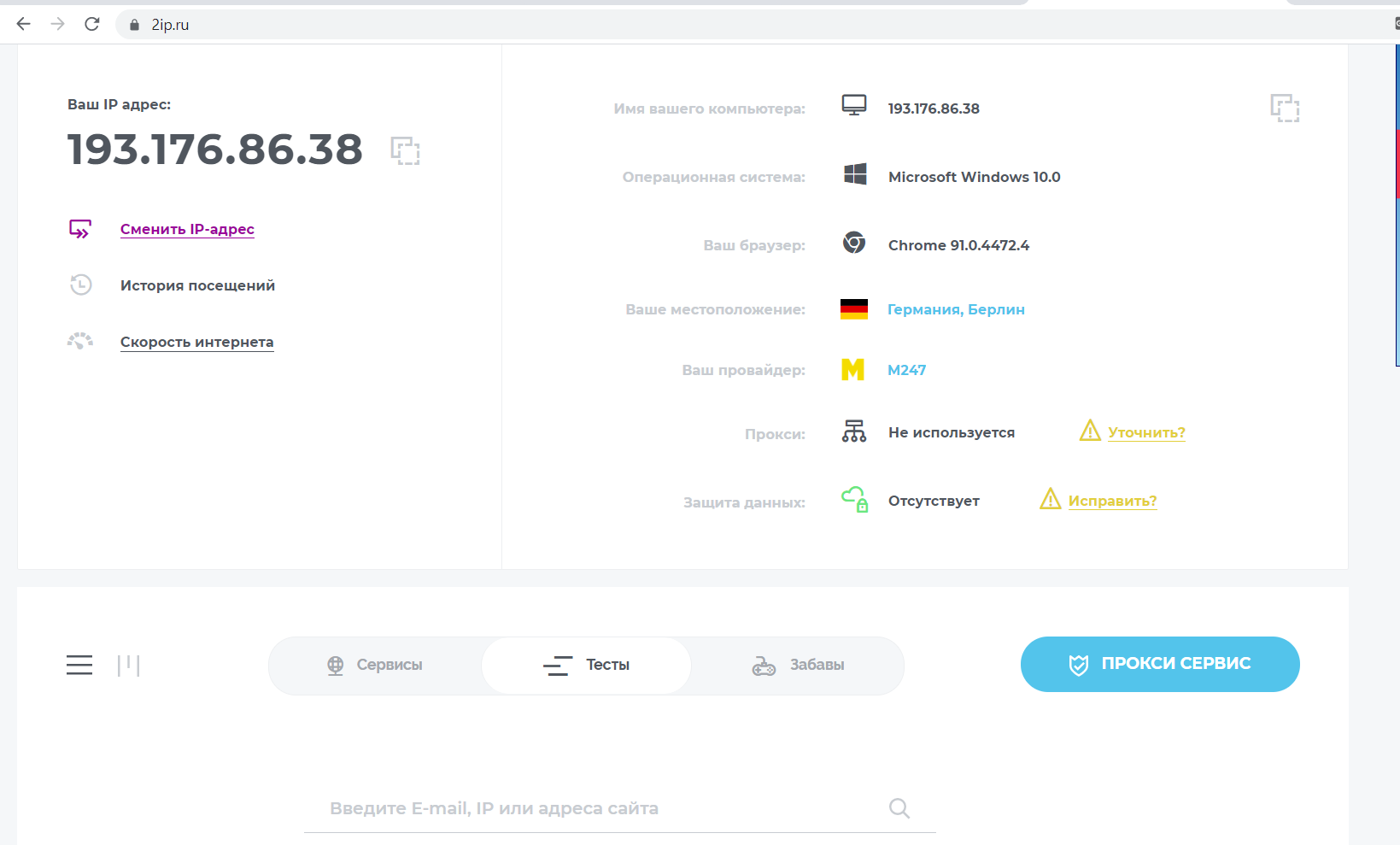
1. Пробуємо додати до правил таке, що дозволить підключення командної строки Windows, після чого знову пробуємо запустити команду ping на адресу google.com.



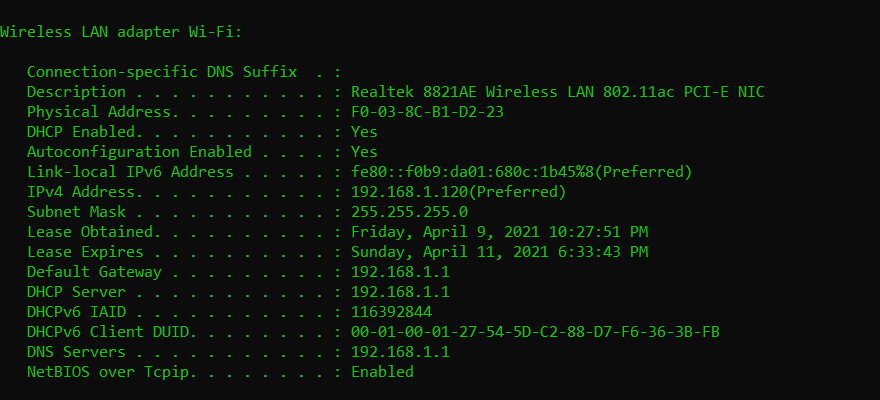
1. Повернули всі налаштування мережевого екрану та налаштування за замовчуванням, зробили неактивними нові правила.
2. Завантажили у браузері сторінку, яка відображає поточну IP-адресу.



1. Використали проксі сервер для підключення до тієї ж сторінки.



1. Налаштували операційну систему на роботу з VPN. Відбулися зміни в API адресі.



**Відповіді на контрольні питання**

1. **Що таке мережевий екран?**

Мережевий екран — узагальнююча назва фізичних пристроїв чи програмних застосунків, сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати мережевий трафік між областями різної безпеки мережі згідно з бажаним набором правил безпеки. Фаєрвол може бути у вигляді окремого приладу (так званий маршрутизатор або роутер), або програмного забезпечення, що встановлюється на персональний комп'ютер чи проксі-сервер. Простий та дешевий фаєрвол може не мати такої гнучкої системи налаштувань правил фільтрації пакетів та трансляції адрес вхідного та вихідного трафіку (функція переадресації).

1. **Наведіть приклади вхідних та вихідних підключень, налаштування яких можуть регулюватися мережевим екраном.**

Дозвіл або заборона доступу фаєрволом здійснюється на основі заданих адміністратором параметрів. У тому числі можуть використовуватися такі параметри і їх комбінації:

- IP-адреси. За допомогою Firewall можна надати або заборонити отримання пакетів з певного адреси або задати перелік заборонених і дозволених IP-адрес.

- Доменні імена. Можливість установки заборони на пропуск трафіку з певних веб-сайтів.

- Порти. Завдання переліку заборонених і дозволених портів дозволяє регулювати доступ до певних сервісів і додатків. Наприклад, заблокувавши порт 80, можна заборонити доступ користувачів до веб-сайтам.

- Протоколи. МСЕ може бути налаштований таким чином, щоб блокувати доступ трафіку певних протоколів.

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

Профіль домену - для комп'ютера, підключеного до домену. Приватний профіль - використовується для підключень до приватної мережі, наприклад, робочої або домашньої. Загальний профіль - використовується для підключення до мережі до публічної мережі (Інтернет, публічна точка доступу Wi-Fi).

1. **Які бувають типи правил у мережевого екрану Windows? Які дії доступні для регулювання для будь-якого правила?**

Правила брандмауера визначають, які типи інтернет-трафіку є дозволеними або забороненими.

У кожному профілі брандмауера попередньо визначений набір правил брандмауера, які не можна змінити. В деякі профілі можна тільки додавати нові правила. У деяких профілях можна створювати власні правила. Також бувають профілі, які не містять заданих параметрів і дозволяють додавати власні набори правил. Обраний профіль брандмауера також впливає на пріоритет власних правил щодо попередньо визначених.

Правило брандмауера може застосовуватися для трафіку з Інтернету на ваш комп'ютер (входить) або з комп'ютера в Інтернет (вихідний). Правило також може застосовуватися для двох напрямків одночасно.

Правило брандмауера складається зі служб брандмауера, що вказують тип трафіку і портів, що використовують цей тип трафіку. Наприклад, правило з ім'ям Пошук в Інтернеті включає в себе службу HTTP, що використовує TCP і порт з номером 80.

Правила брандмауера також керують відображенням спливаючих повідомлень брандмауера про трафік, на який поширюється дія правил.

1. **Що таке проксі сервер?**

Проксі-сервер — сервер (комп'ютерна система або програма) в комп'ютерних мережах, що дозволяє клієнтам виконувати непрямі (через посередництво проксі-сервера) запити до мережевих сервісів. Спочатку клієнт з'єднується з проксі-сервером і запитує який-небудь ресурс (наприклад, e-mail), розташований на іншому сервері. Потім проксі-сервер або підключається до вказаного сервера та отримує ресурс у нього, або повертає ресурс з власного кешу (у випадках, якщо проксі має свій кеш). У деяких випадках запит клієнта або відповідь сервера може бути змінена проксі-сервером з певною метою. Також проксі-сервер дозволяє захищати клієнтський комп'ютер від деяких мережевих атак і допомагає зберігати анонімність клієнта.

1. **Які бувають основні типи проксі?**

Прозорий проксі — схема зв'язку, при якій трафік, або його частина, перенаправляється на проксі-сервер неявно (засобами маршрутизатора). При цьому клієнт може використовувати всі переваги проксі-сервера без додаткових налаштувань, але з іншого боку, не має вибору.

Зворотний проксі — проксі-сервер, який на відміну від прямого, ретранслює запити клієнтів із зовнішньої мережі на один або декілька серверів, логічно розташованих у внутрішній мережі. Часто використовується для балансування мережевого навантаження між декількома вебсерверами і підвищення їх безпеки, граючи при цьому роль міжмережевого екрану на прикладному рівні.

1. **Що таке VPN?**

VPN — узагальнена назва технологій, які дозволяють створювати віртуальні захищені мережі поверх інших мереж із меншим рівнем довіри. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному клієнту бути повноцінним учасником віддаленої мережі і користуватись її сервісами — внутрішніми сайтами, базами, принтерами, політиками виходу в Інтернет. 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. Багато провайдерів пропонують свої послуги як з організації VPN-мереж для бізнес-клієнтів, так і для виходу в мережу Інтернет. VPN є клієнт-серверною технологією.

1. **Чим проксі відрізняються від VPN?**

Для користувача відмінність полягає в тому, що VPN використовує наскрізне шифрування, передані дані знаходяться в безпеці від точки входу до точки виходу. А проксі - це менш захищена технологія, її не варто використовувати, якщо потрібна повна анонімність і захист цінних даних.

**Висновок:** виконавши дану лабораторну роботу, я навчився працювати та встановлювати мережеві екрани, налаштовувати проксі та впн.