**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

**“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**

**імені ІГОРЯ СІКОРСЬКОГО”**

**ЗВІТ**

**з лабораторної роботи №4**

**з навчальної дисципліни “Інформаційне забезпечення безпеки**

**комп’ютерних систем”**

**Тема:**

Захист даних в комп’ютерних мережах

**Варіант 20**

**Виконав студент групи ТР–12**

Руденко Владислав\_\_\_\_\_\_\_\_\_

Лабораторну роботу захищено

з оцінкою \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Київ 2024**

**Мета роботи:** ознайомитися з основними поняттями комп’ютерних

мереж,навчитися використовувати програмні засоби для захисту даних в комп’ютерних мережах.

**Завдання на лабораторну роботу:**

1. На віртуальному комп’ютері завантажити та з’ясувати призначення програмного додатку

Центр безпеки (Панель керування) та компонентів, які входять до складу цього додатку.

1. Ознайомитися, налаштувати та продемонструвати роботу вбудованого брандмауера.
2. Продемонструвати увімкнення або вимкнення брандмауера Windows. Пояснити чим може загрожувати вимкнення брандмауера.

4. Перевірити проходження пакетів ICMP між комп’ютерами до і після відключення брандмауера (за допомогою команди ping).

5. Продемонструвати налаштування брандмауера Windows для різних типів мереж (приватна мережа, мережа спільного використання або мережа з доменами).

6. Продемонструвати надання програмі (будь-якій) дозволу на отримання даних через брандмауер.

7. Продемонструвати відкриття порту у брандмауері Windows.

**Хід виконання роботи**

1. **На віртуальному комп’ютері завантажити та з’ясувати призначення програмного додатку**

Брандмауер (Firewall) — це інструмент безпеки, що виконує роль бар'єра між локальною мережею або пристроєм і зовнішніми мережами, такими як Інтернет. Він контролює всі вхідні та вихідні підключення, пропускаючи лише ті, які відповідають заздалегідь заданим правилам. Завдяки цьому брандмауер забезпечує захист від несанкціонованого доступу та допомагає уникнути загроз, пов'язаних із небажаними мережевими з'єднаннями або шкідливими програмами.

Робота брандмауера базується на фільтрації трафіку за протоколами, портами, адресами або програмами. Він може дозволяти або блокувати доступ окремих програм до мережі, залежно від рівня довіри до них. Таким чином, система захисту забезпечує баланс між безпекою та функціональністю, дозволяючи налаштовувати політики доступу відповідно до потреб користувача чи організації.

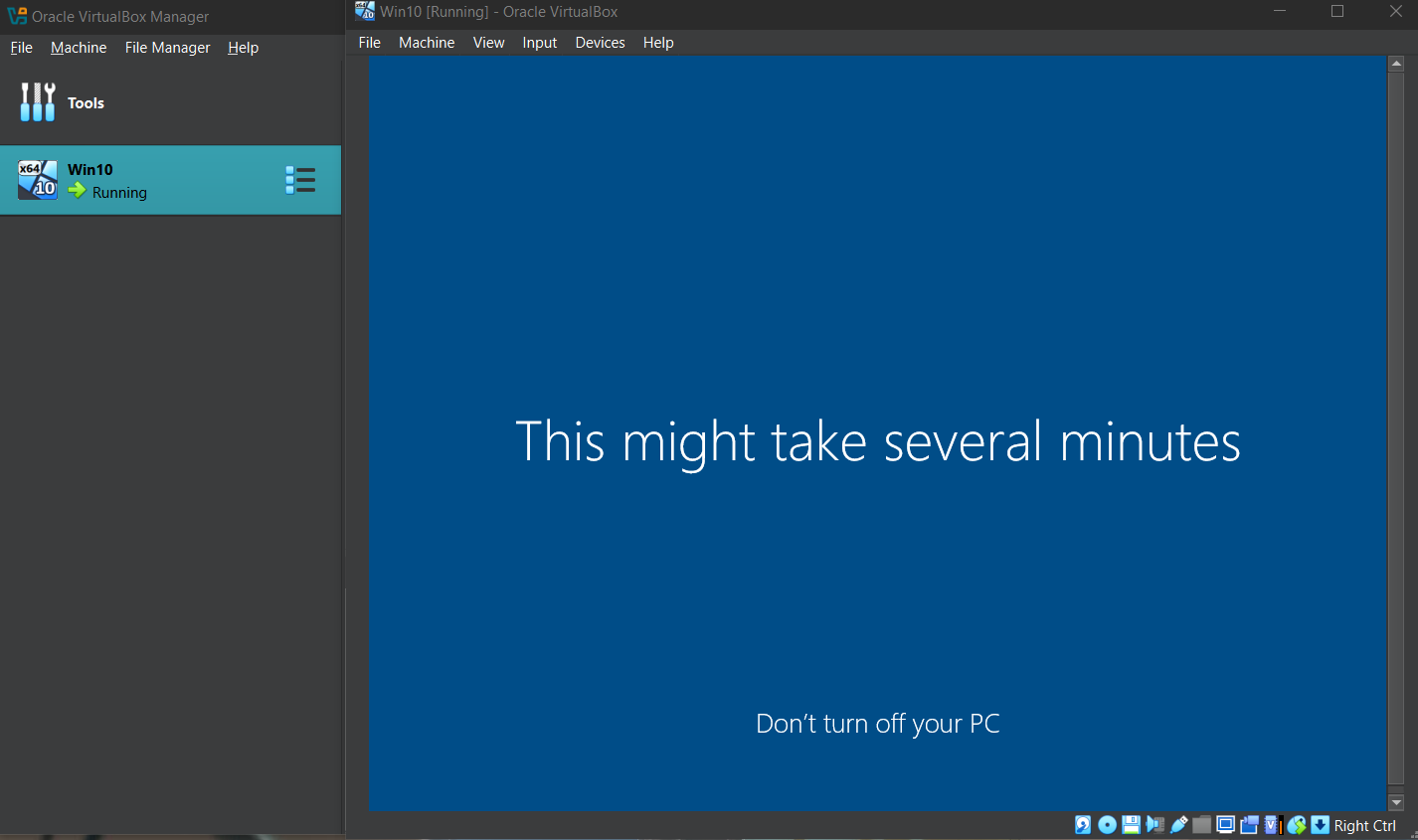


Table 1 Встановлення ОС на віртуальну машину

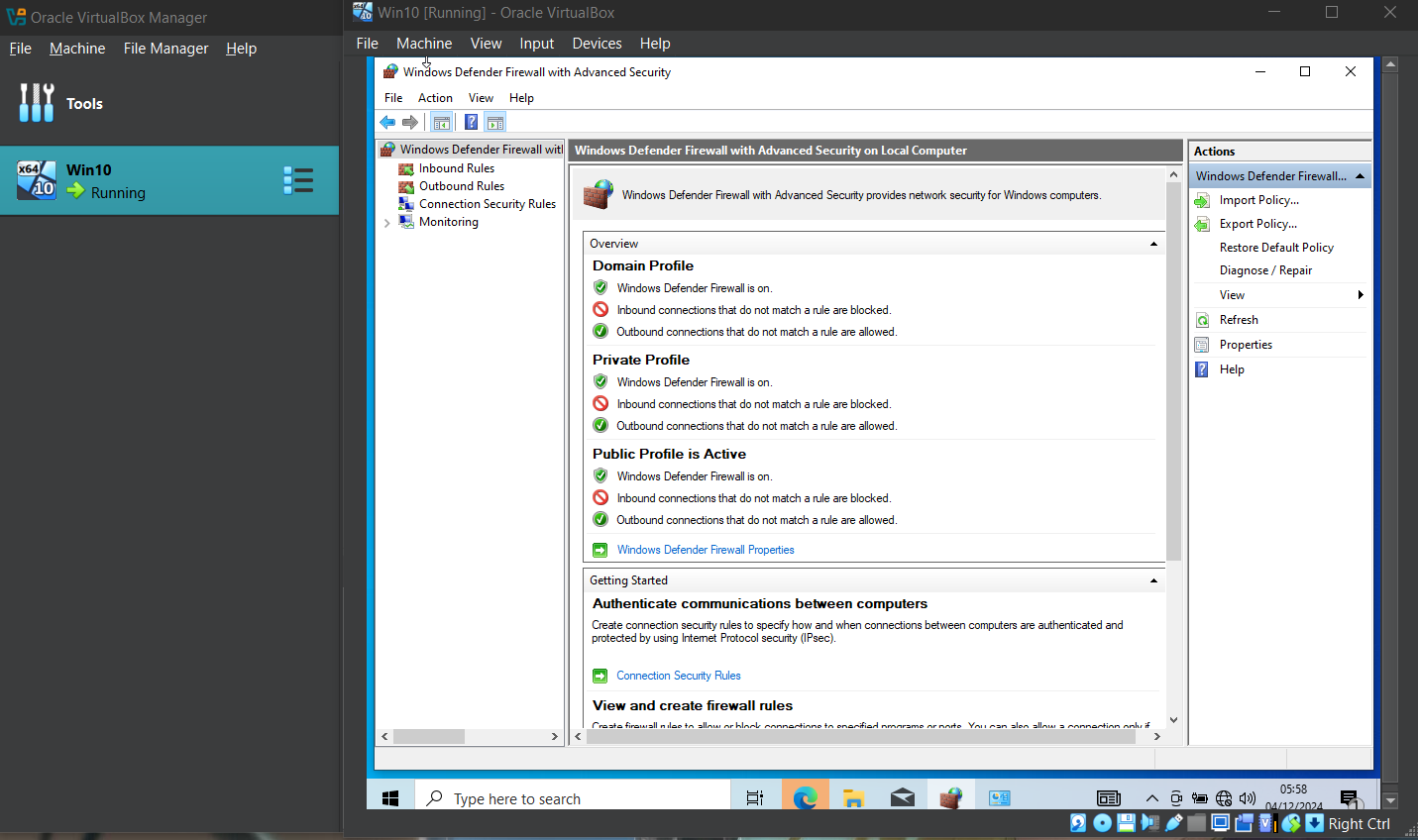


Table 2 Демонстрація наявності додатку

1. **Ознайомитися, налаштувати та продемонструвати роботу вбудованого брандмауера.**

Windows підтримує різні типи мереж, кожна з яких має унікальний рівень захисту. Доменні мережі використовуються в корпоративному середовищі з більш жорсткими вимогами до безпеки. Приватні мережі дозволяють взаємодію між довіреними пристроями, наприклад, для спільного використання ресурсів. У загальнодоступних мережах застосовується найвищий рівень захисту, що мінімізує ризики підключення до небезпечних чи невідомих джерел. Налаштування політик брандмауера здійснюється через монітор брандмауера, де створюються і редагуються правила для забезпечення потрібного рівня безпеки.

Правила в брандмауері визначають, який мережевий трафік дозволяється або блокується на основі встановлених критеріїв. Вони є ключовим механізмом для налаштування безпеки, оскільки дозволяють користувачеві або системному адміністратору точно контролювати поведінку програм і пристроїв у мережі. Правила можуть бути створені для вхідного та вихідного трафіку, окремо налаштовуючи доступ програм, портів, IP-адрес або мережевих протоколів.

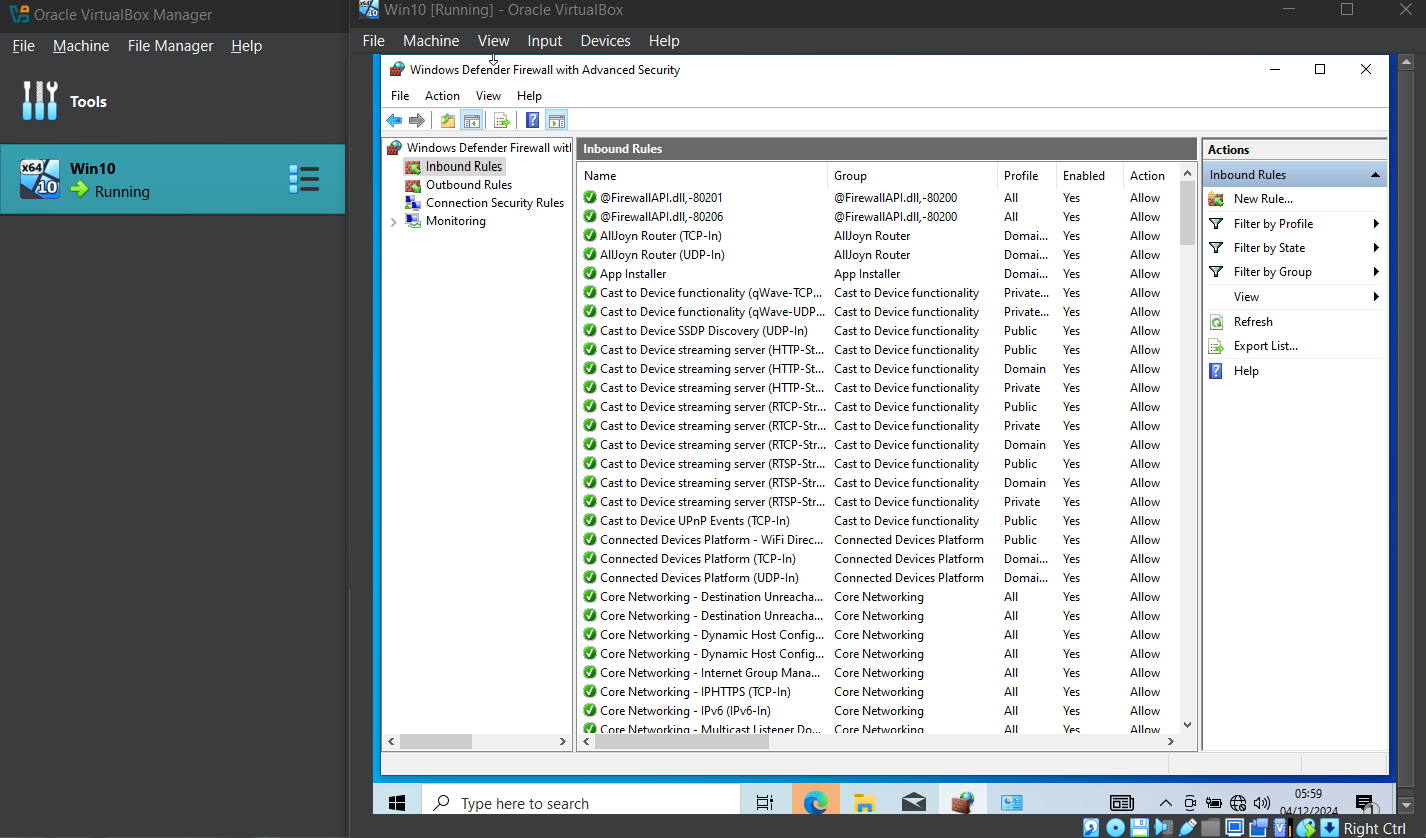


Table 3 Перелік правил на вхідний трафік

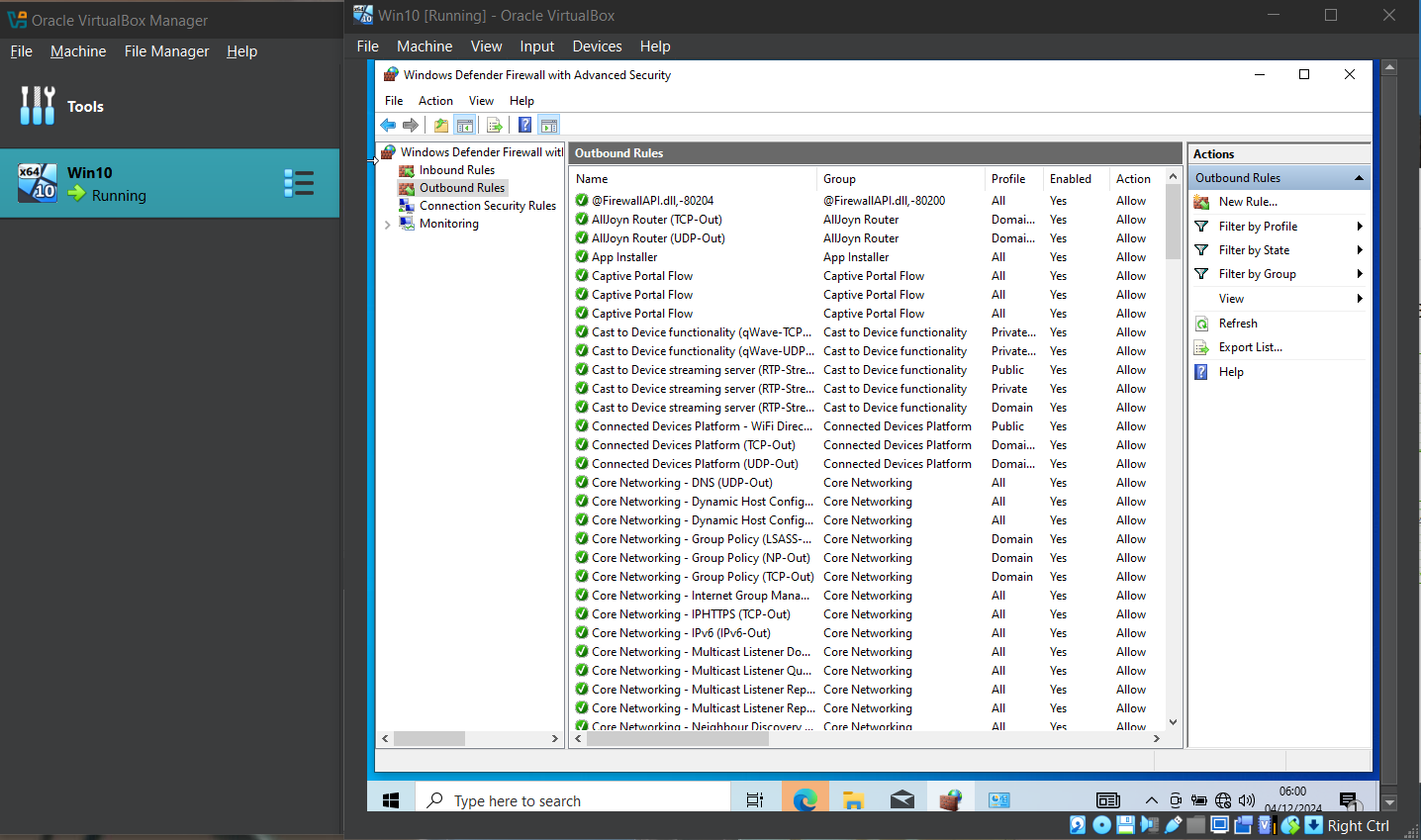


Table 4 Перелік правил на вихідний трафік

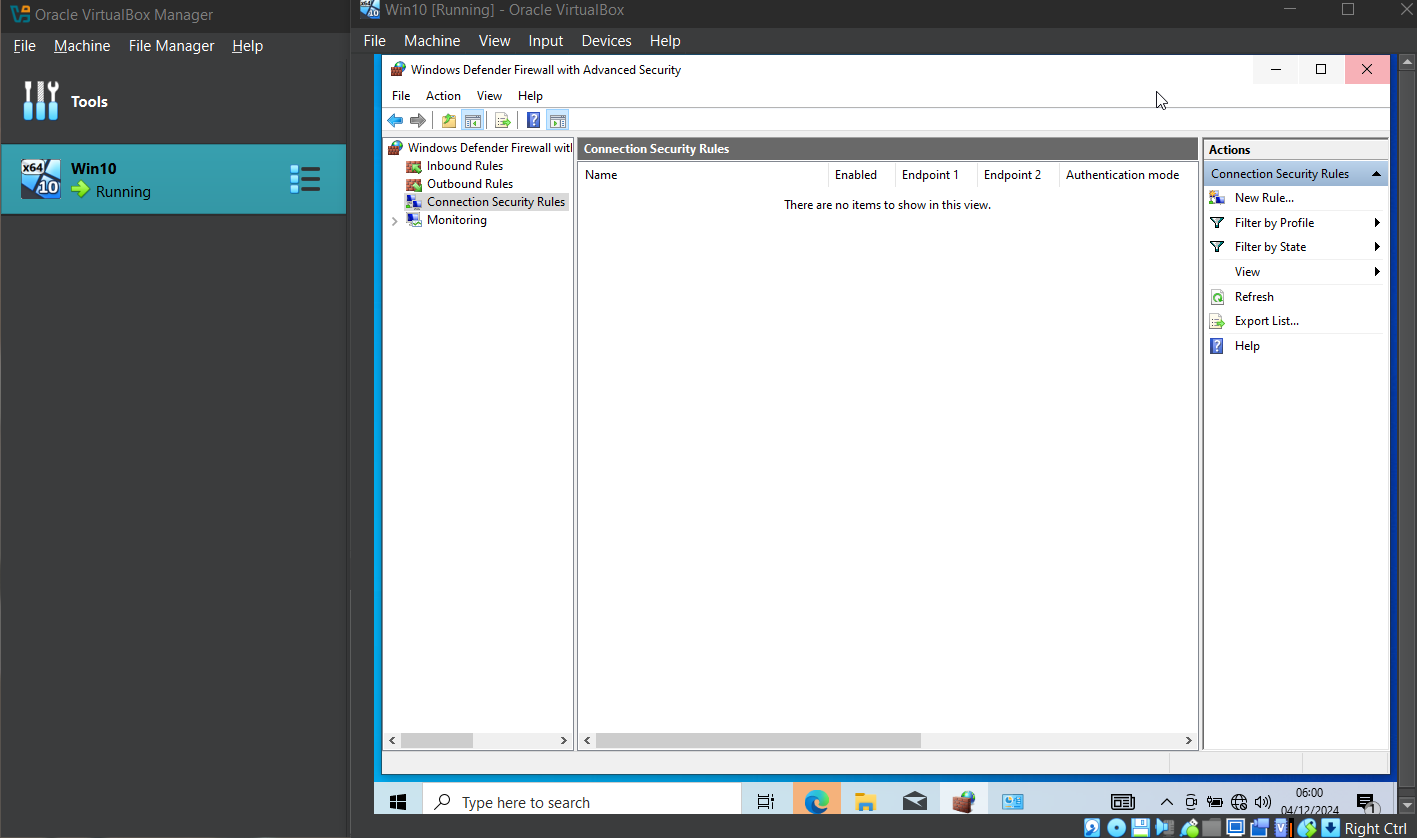


Table 5 Перелік правил безпеки підключення

1. **Продемонструвати увімкнення або вимкнення брандмауера Windows. Пояснити чим може загрожувати вимкнення брандмауера.**

Вимкнення брандмауера серйозно підвищує ризик безпеки, оскільки він припиняє фільтрацію вхідного та вихідного трафіку, що дозволяє зловмисникам здійснювати несанкціонований доступ до пристрою. Без брандмауера комп'ютер стає вразливим до мережевих атак, шкідливих програм та спроб викрадення даних. Це може призвести до зараження системи вірусами, крадіжки особистої інформації або втрати важливих даних через зловмисні підключення.

Вимкнення брандмауера також впливає на безпеку в різних типах мереж, таких як доменна, приватна та загальнодоступна. У доменній мережі, де зазвичай використовуються більш суворі політики безпеки, вимкнення брандмауера може дозволити несанкціонованим користувачам доступ до внутрішніх ресурсів. У приватних мережах, таких як домашні або робочі, це збільшує ризик атак з локальних пристроїв або через Інтернет. У загальнодоступних мережах, де комп'ютер підключається до незахищених або публічних Wi-Fi, вимкнення брандмауера дозволяє зловмисникам безперешкодно проникати в систему, що може призвести до серйозних наслідків для безпеки.

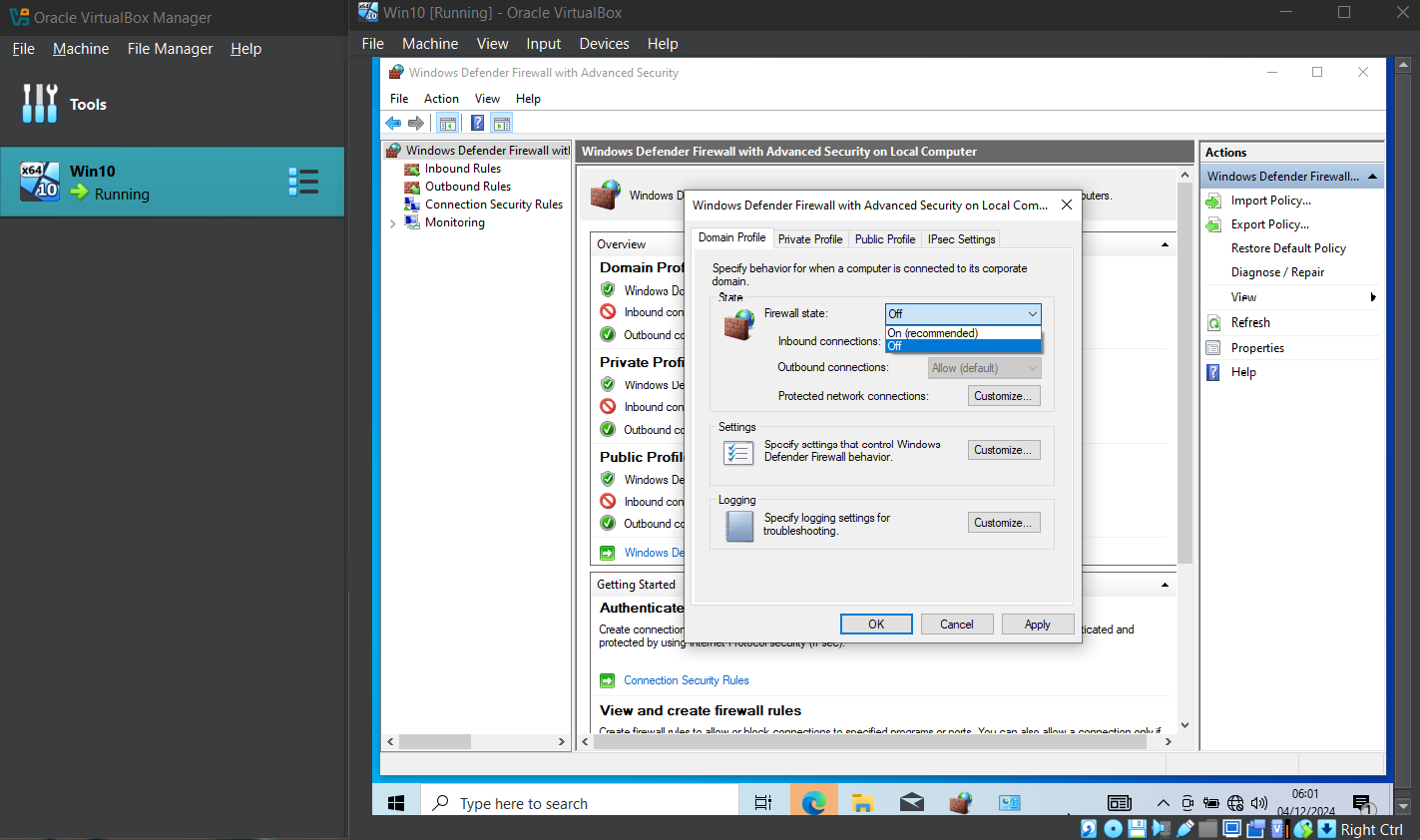


Table 6 Увімкнення брендмаузера

1. **Перевірити проходження пакетів ICMP між комп’ютерами до і після відключення брандмауера (за допомогою команди ping).**

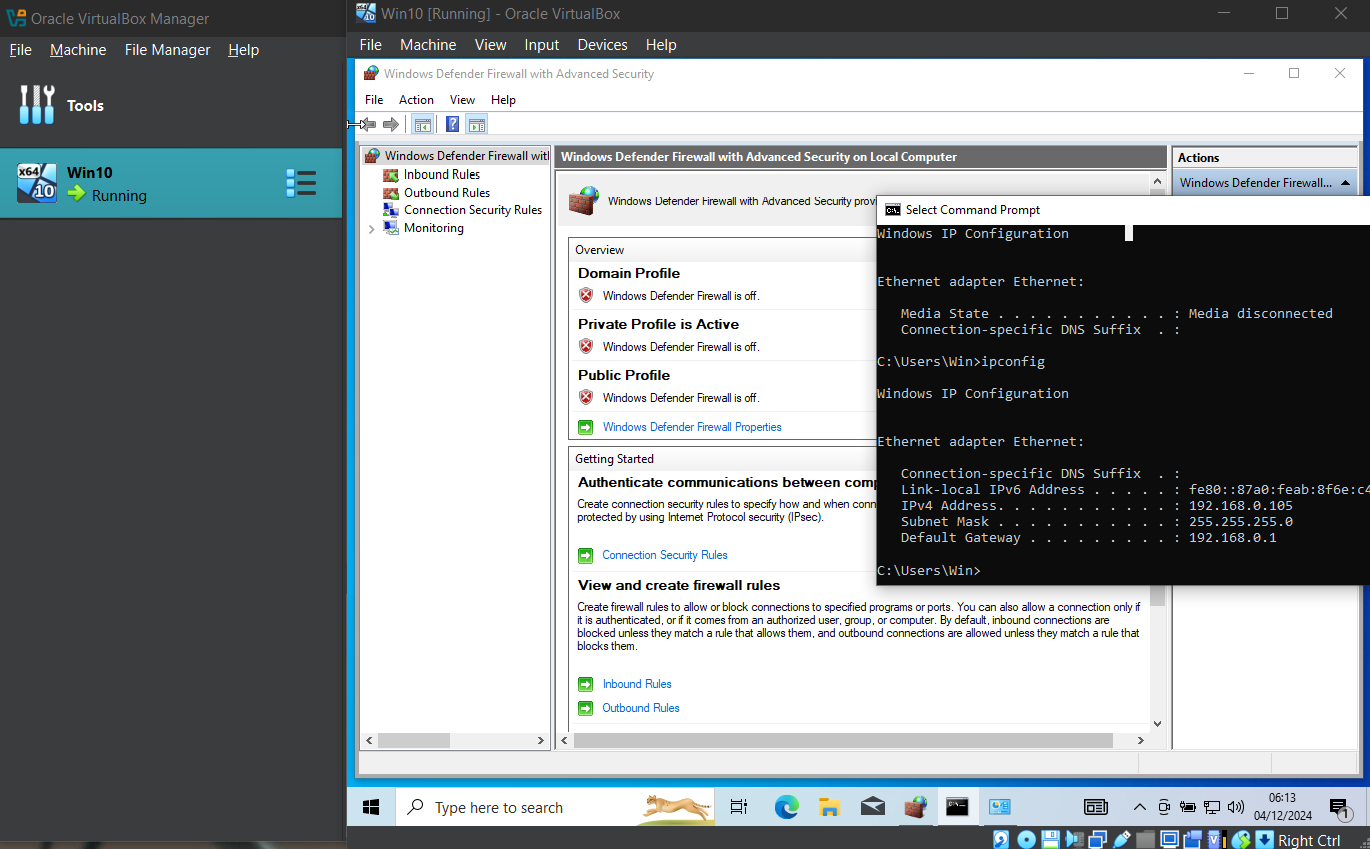


Table 7 Встановлення IP адресу машини в локальній мережі

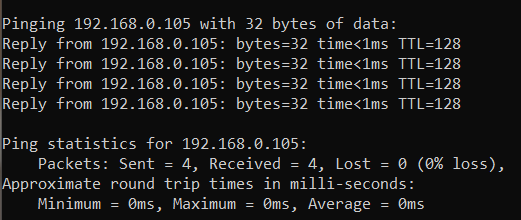


Table 8 Спроба виконання команди ping з хоста (вдачна)

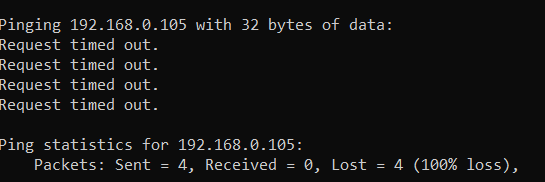


Table 9 Спроба виконання команди ping з хоста (НЕвдачна)

1. **Продемонструвати налаштування брандмауера Windows для різних типів мереж (приватна мережа, мережа спільного використання або мережа з доменами).**

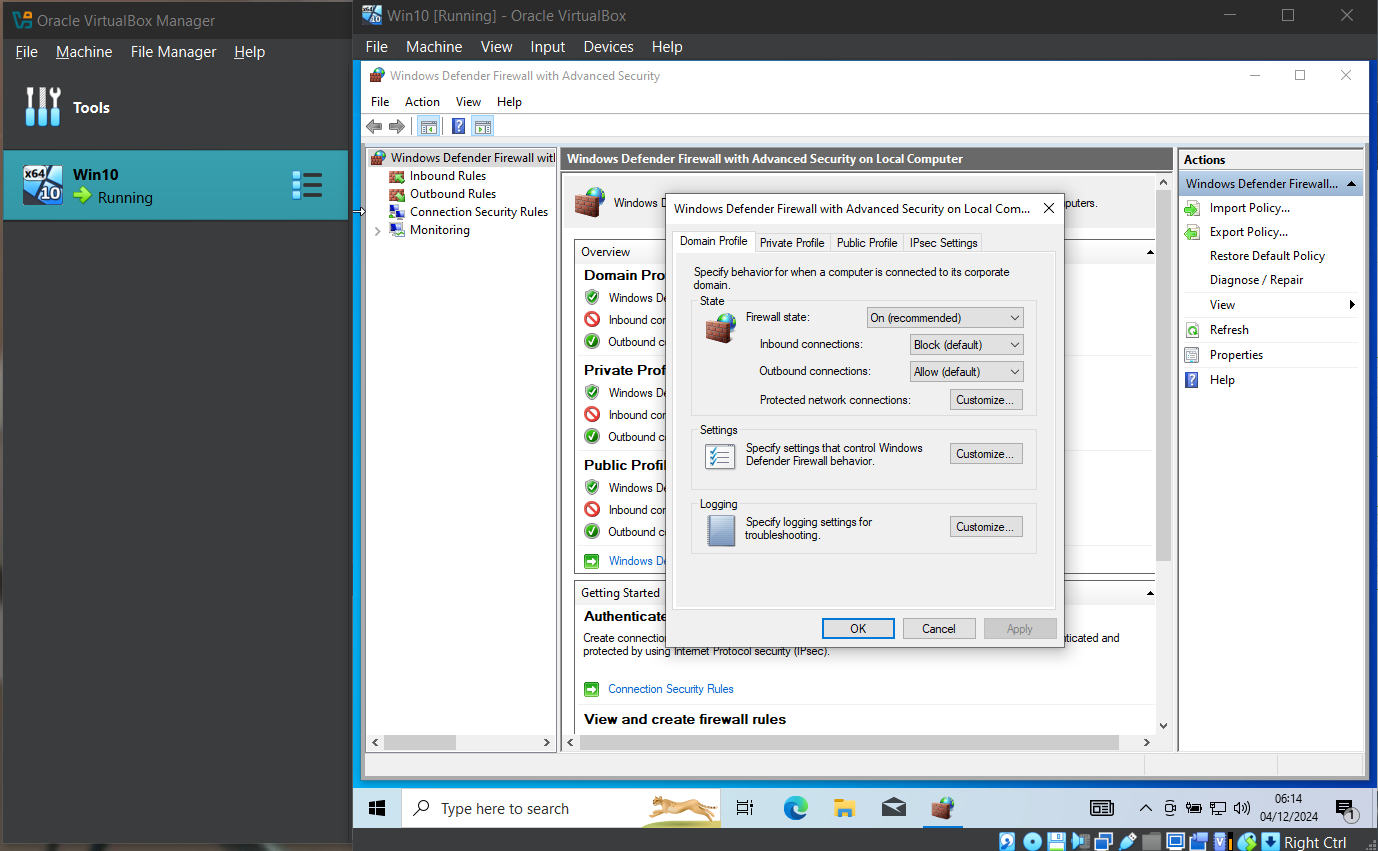


Table 10 Налаштування доступу Домейну

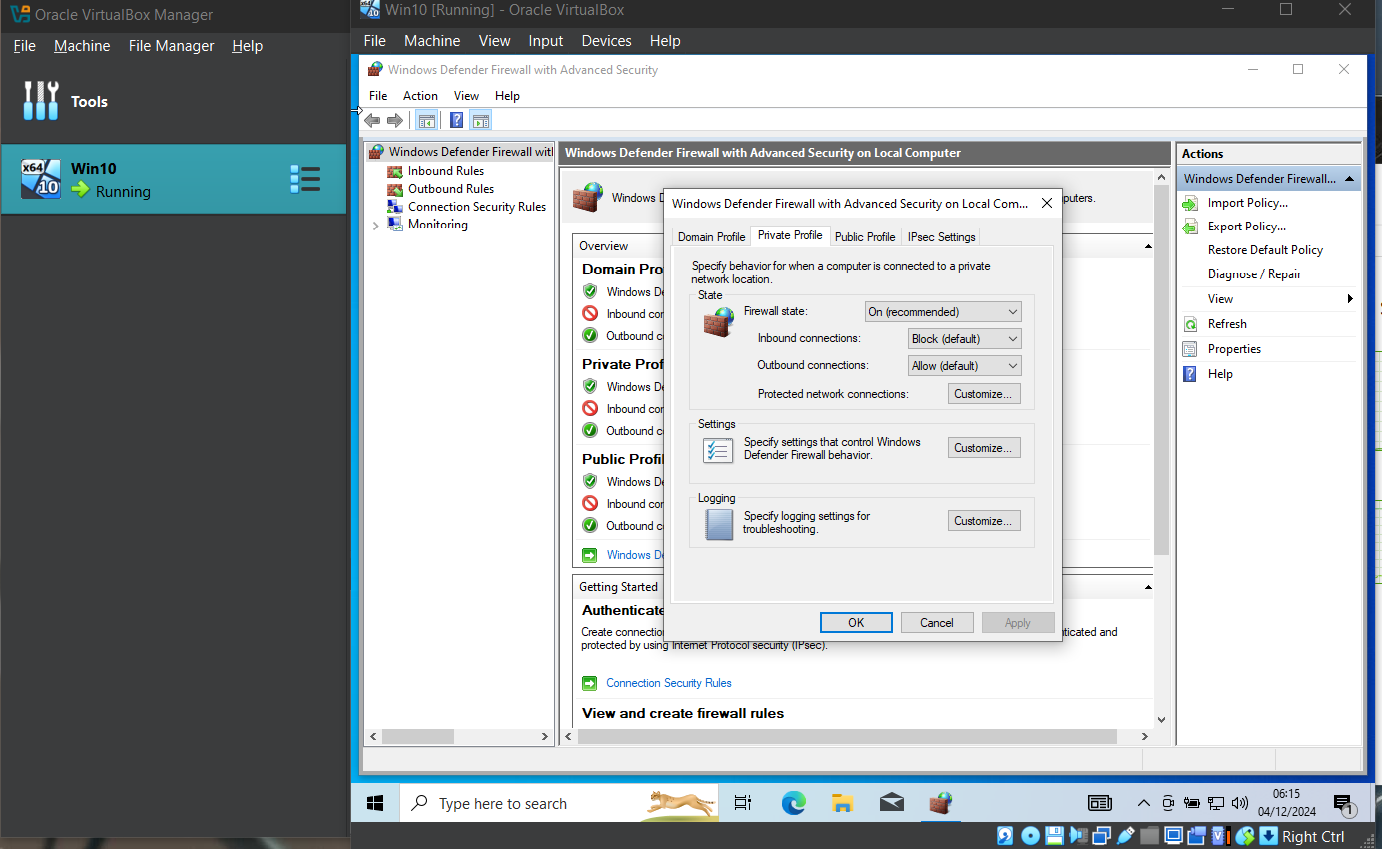


Table 11 Налаштування доступу Приватної мережі

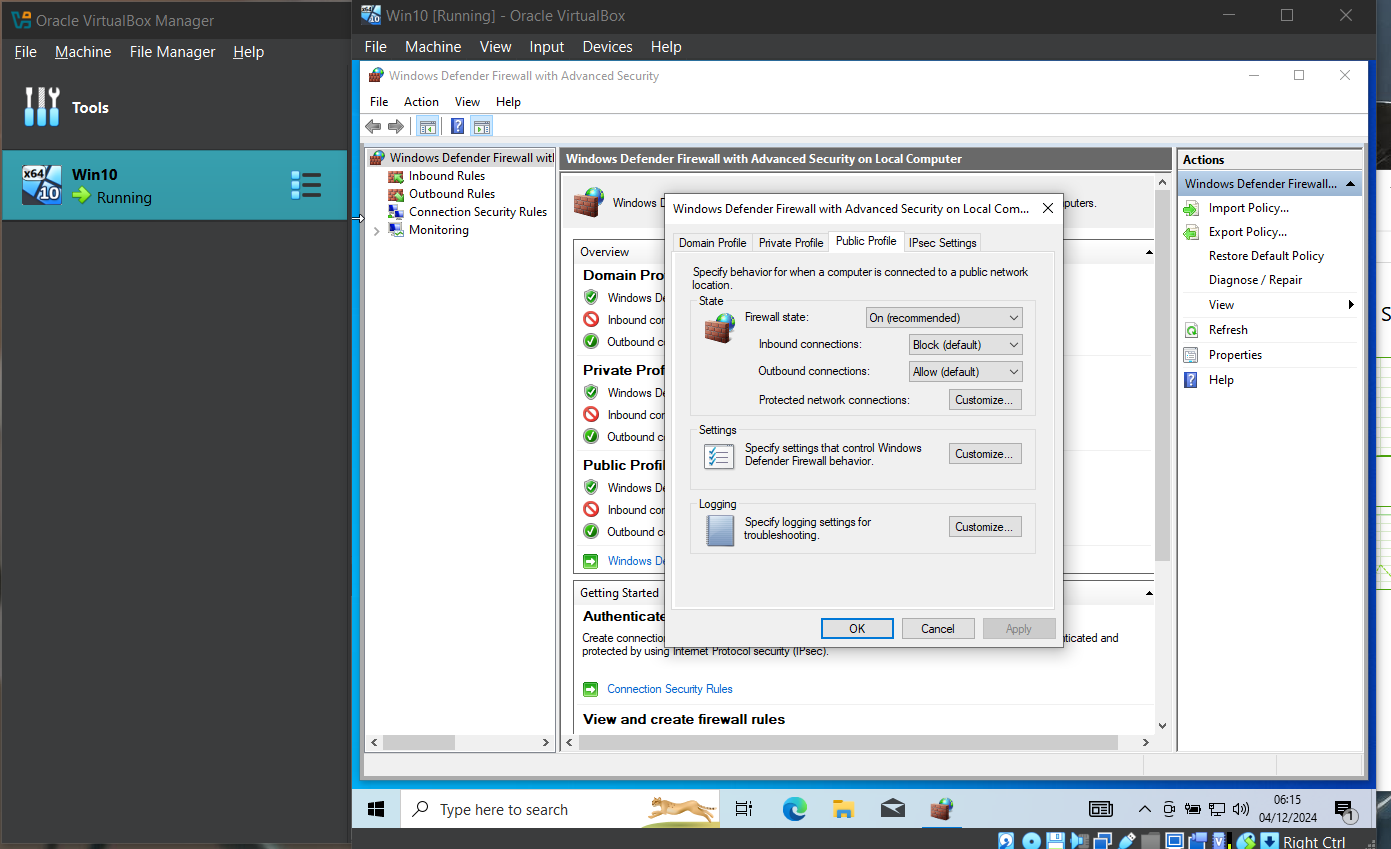


Table 12 Налаштування доступу публічної мережі

1. **Продемонструвати надання програмі (будь-якій) дозволу на отримання даних через брандмауер.**

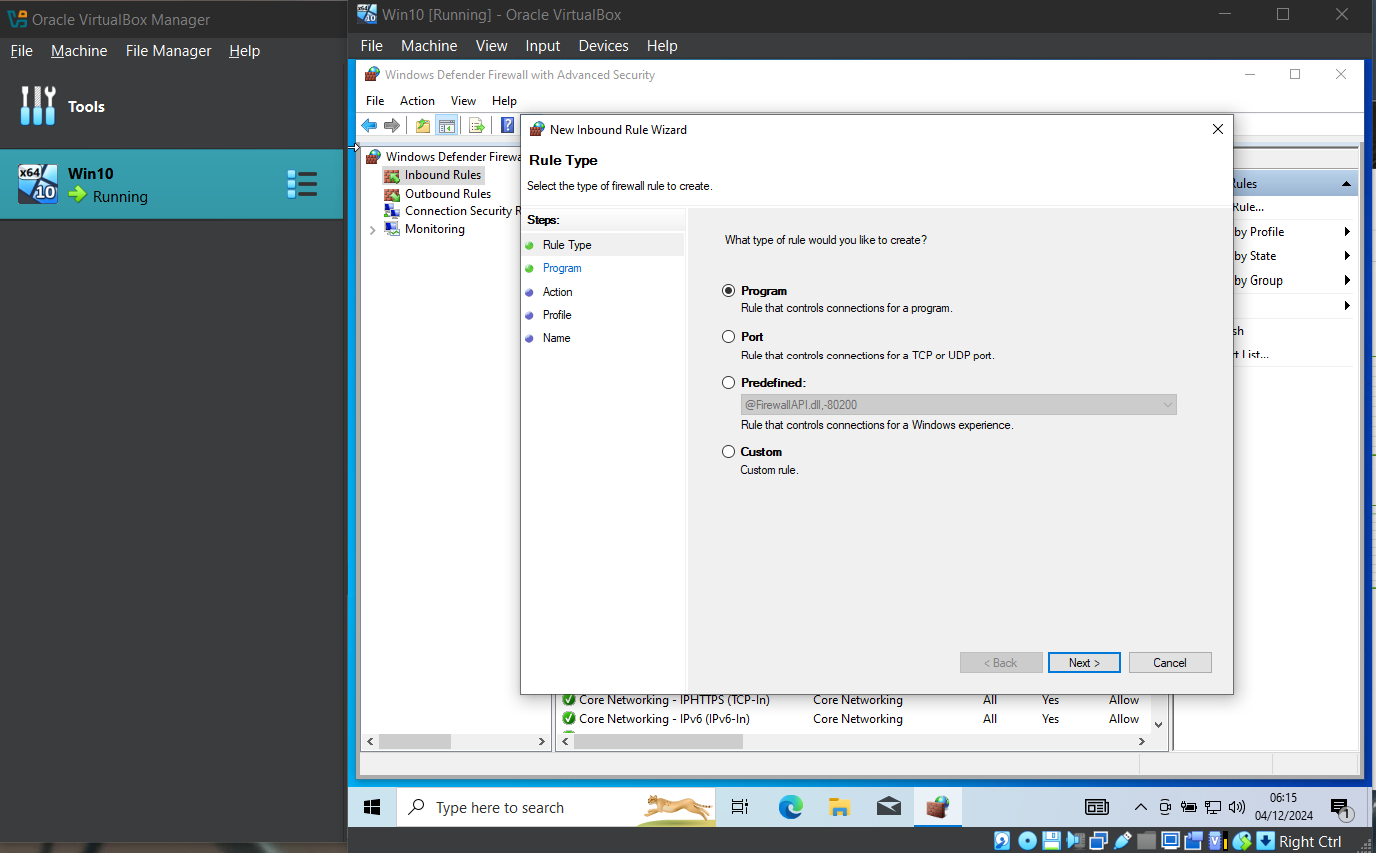


Table 13 Встановлення нового дозволу до програми

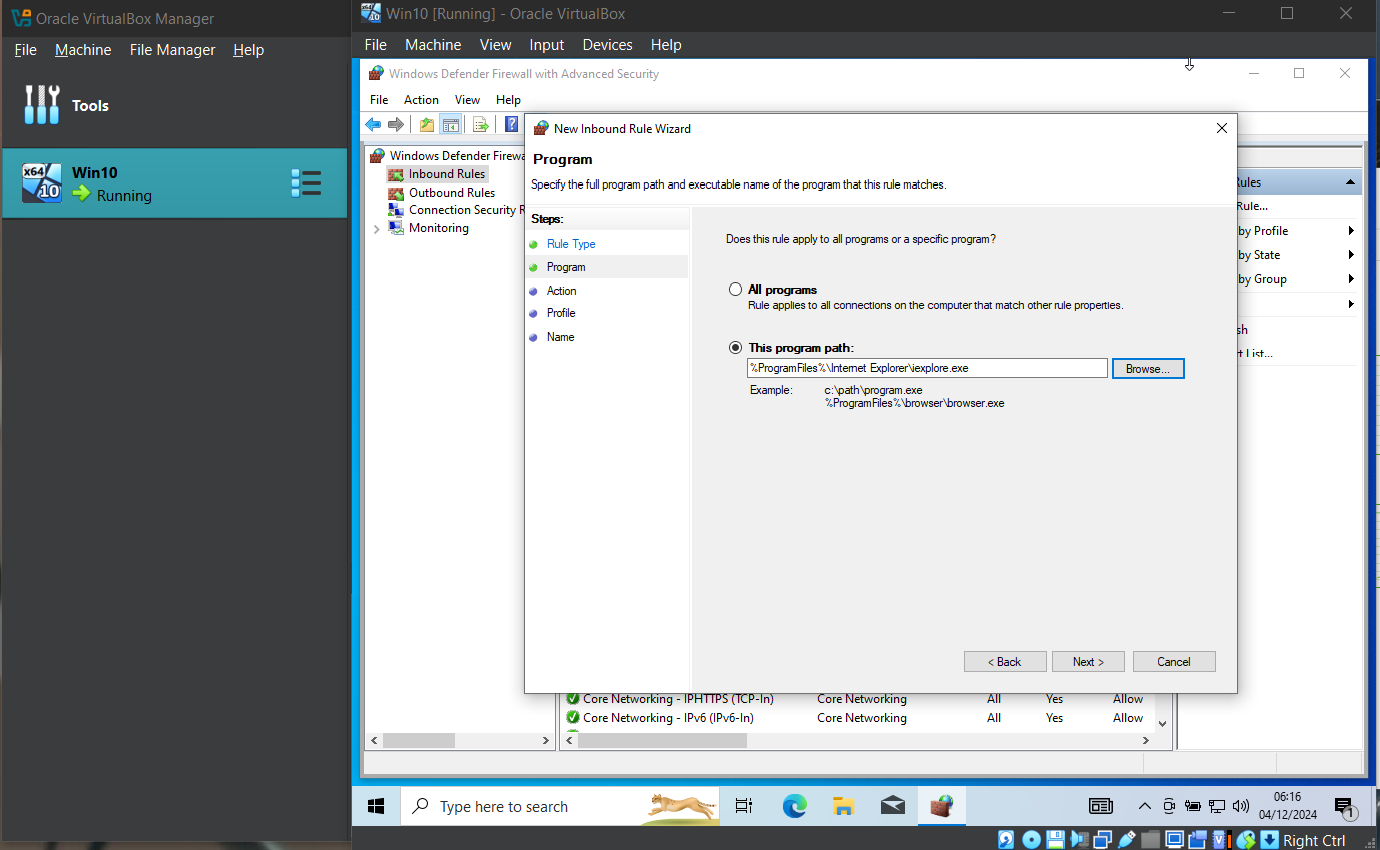


Table 14 Налаштування конкретизації програми

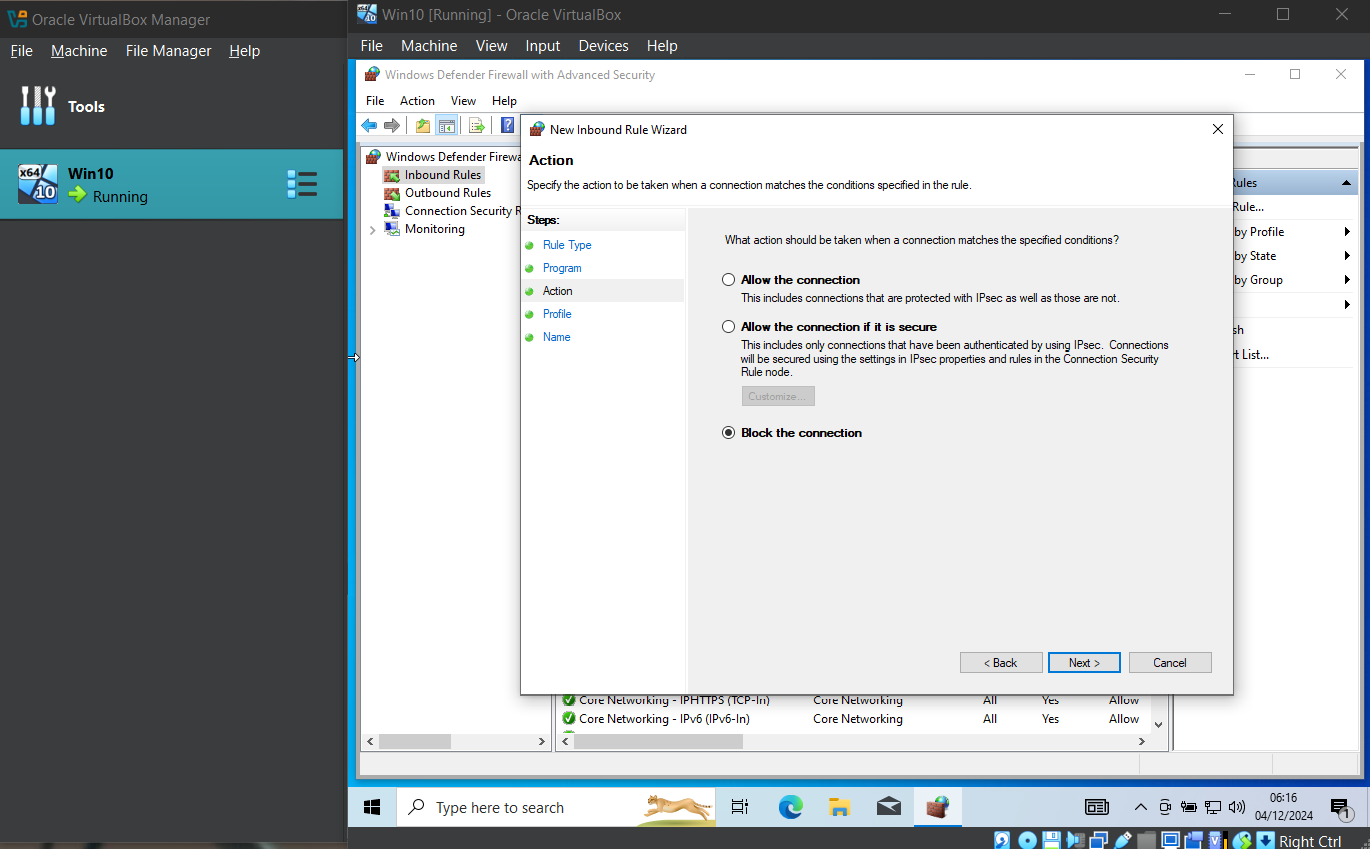


Table 15 Налаштування доступу

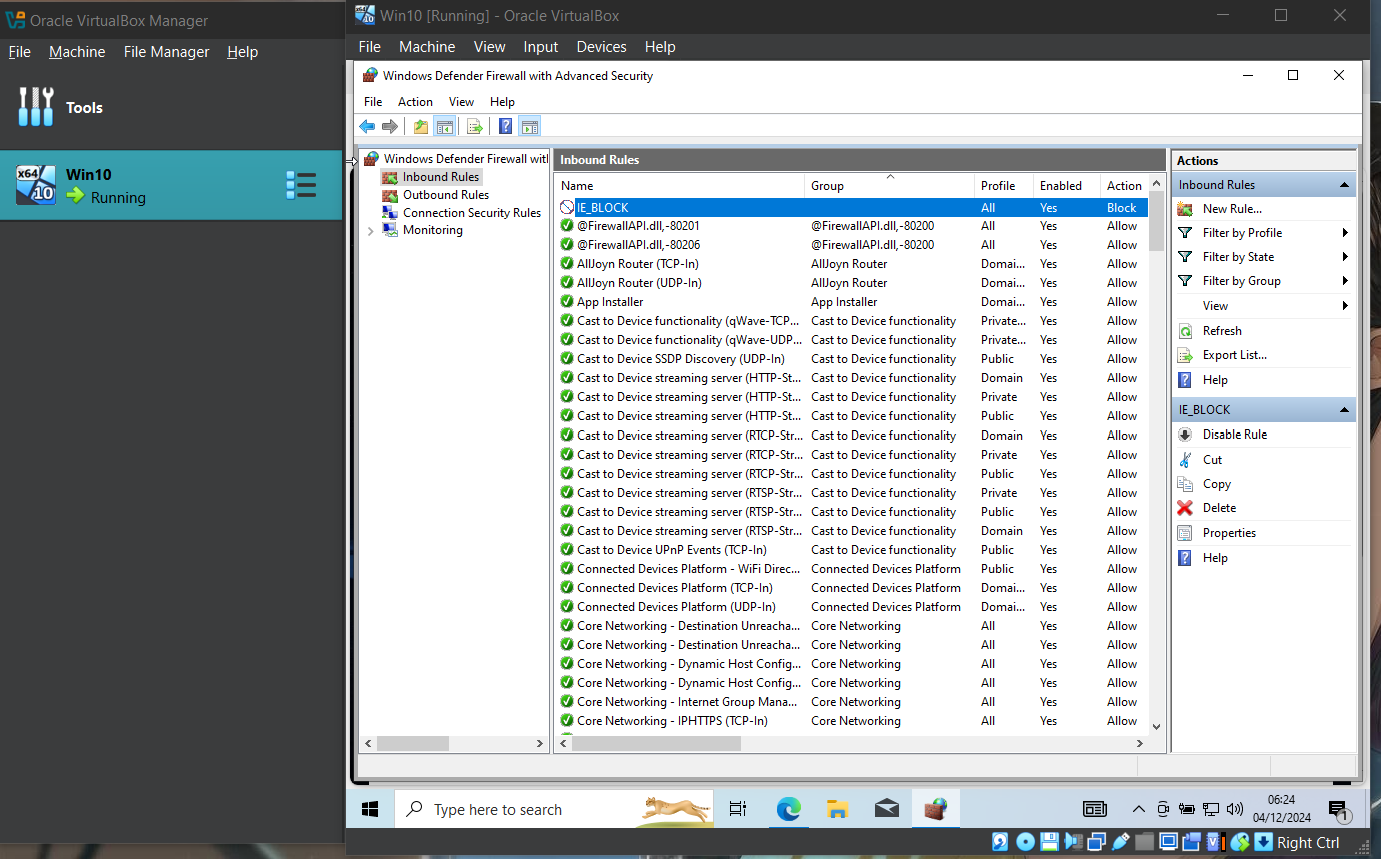


Table 16 Створене правило в контексті переліку Брєндмаузеру

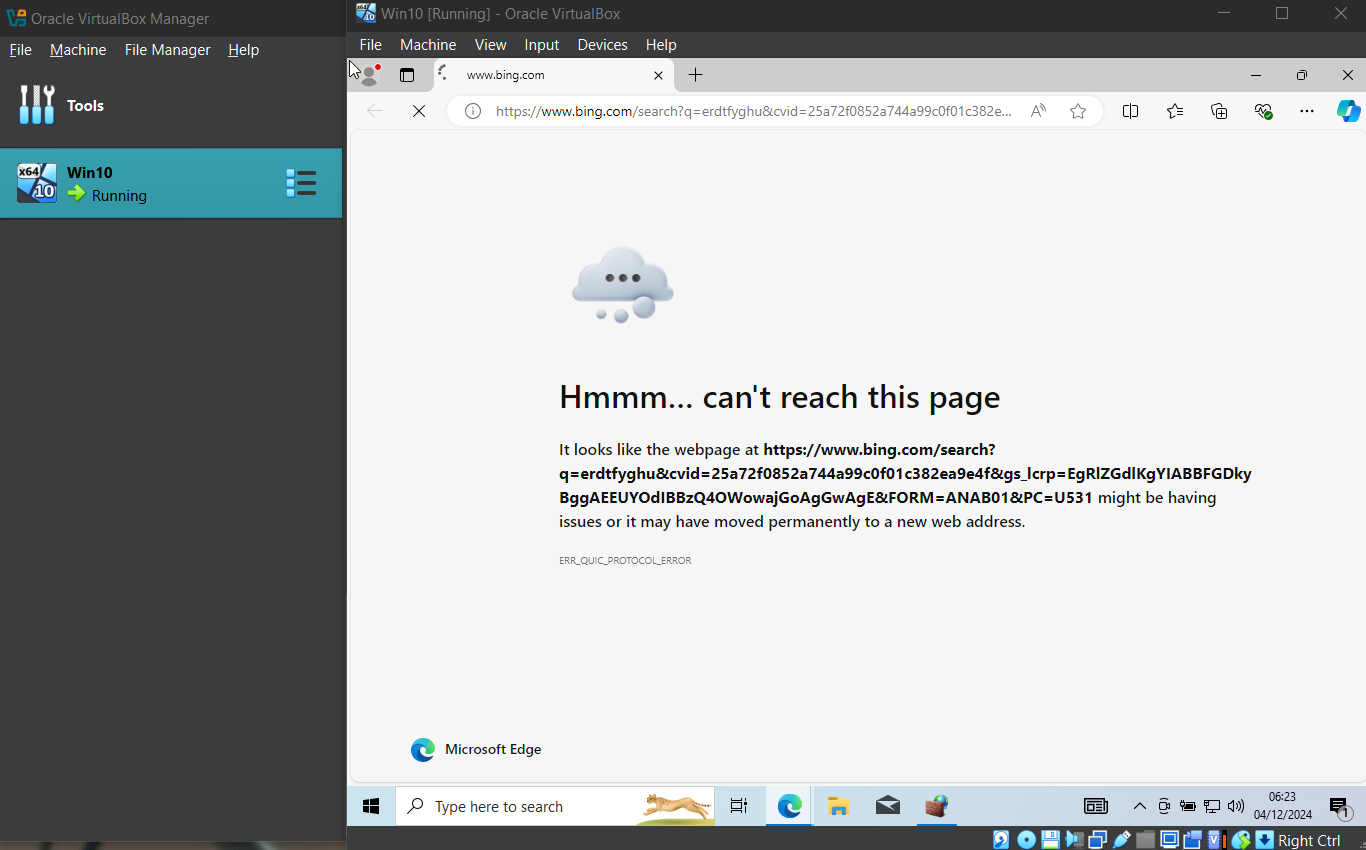


Table 17 Спроба користування додатком з увімкненим фільтром

1. **Продемонструвати відкриття порту у брандмауері Windows.**

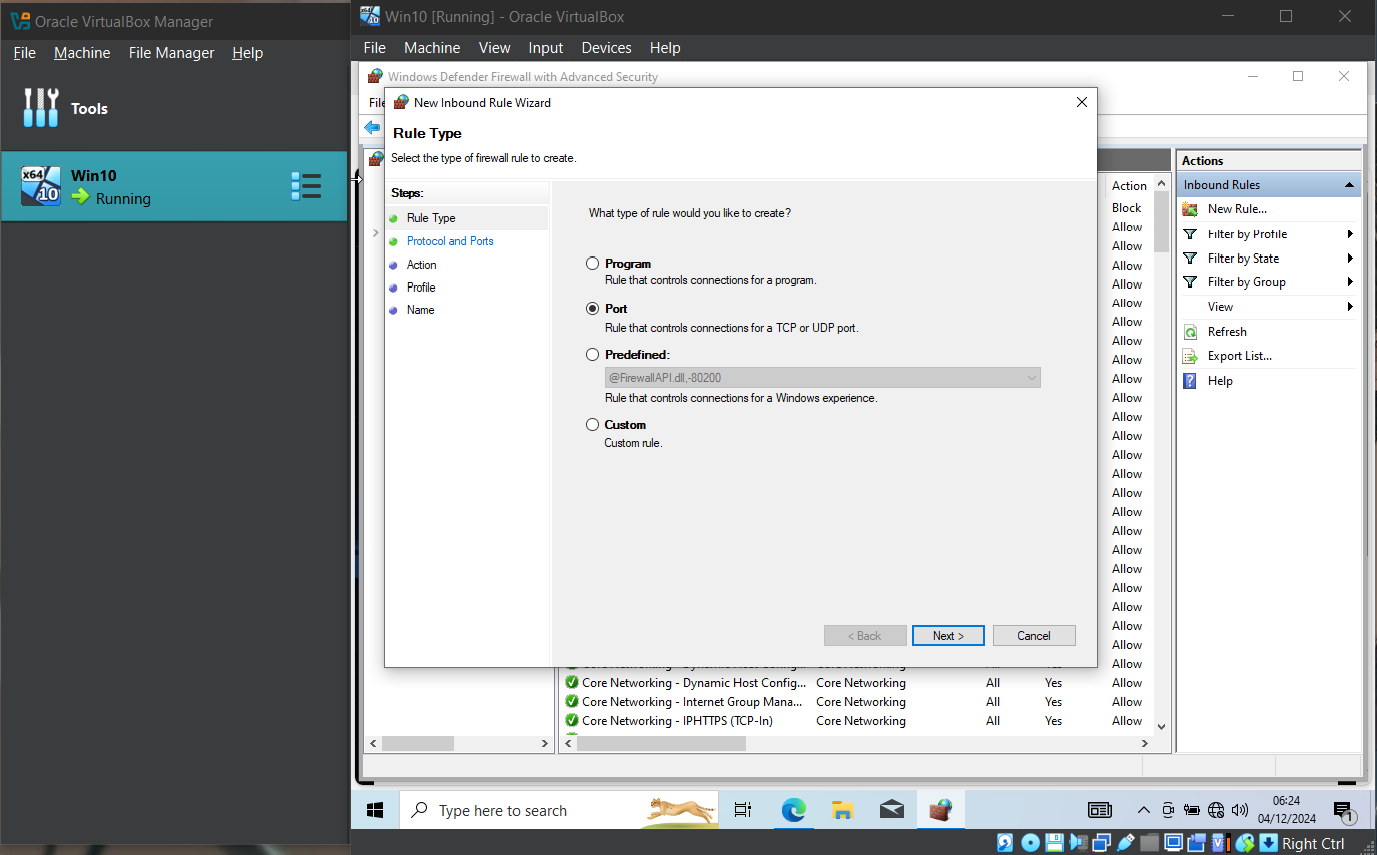


Table 18 Створення правила для порта

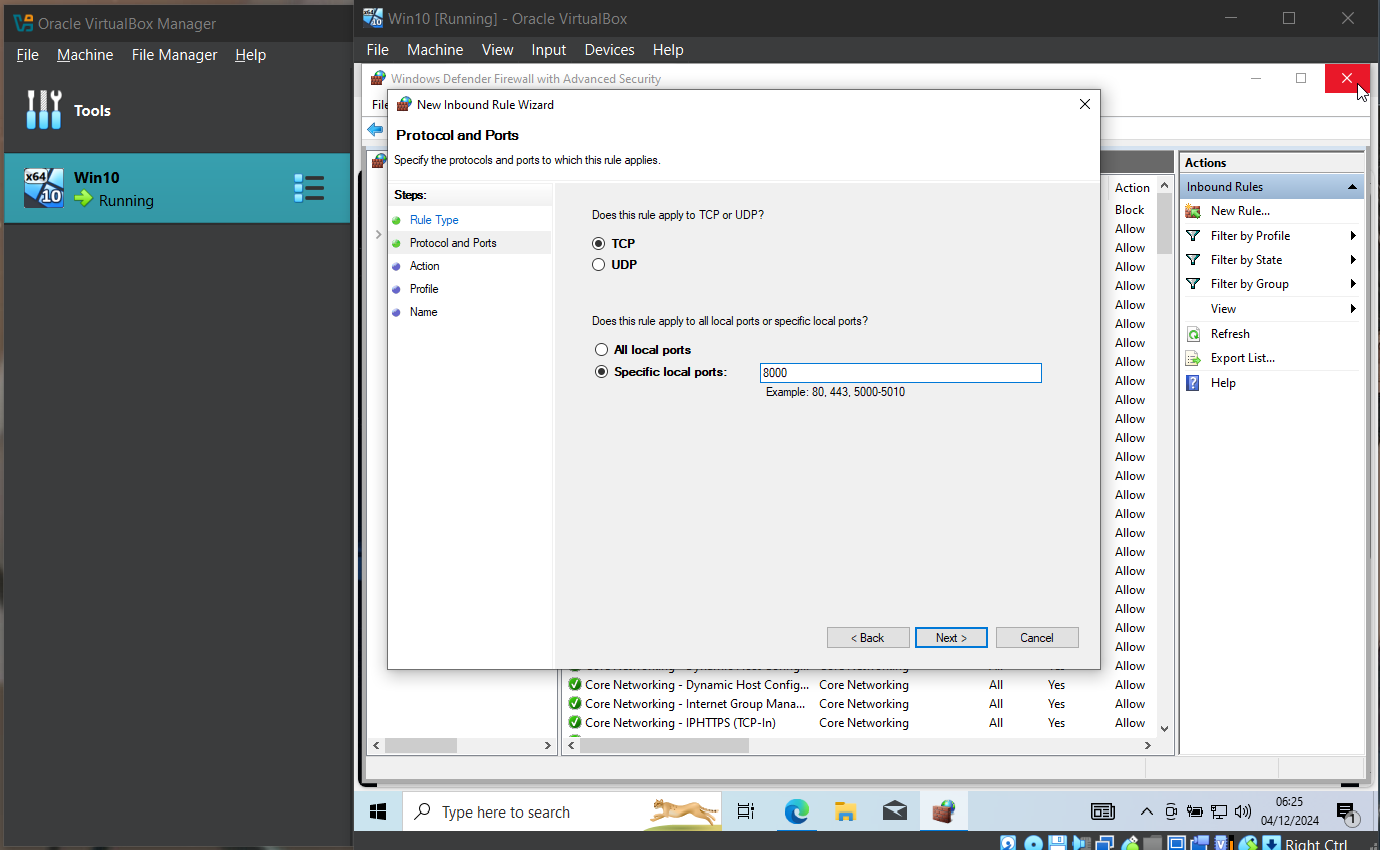


Table 19 Конкретизації порта

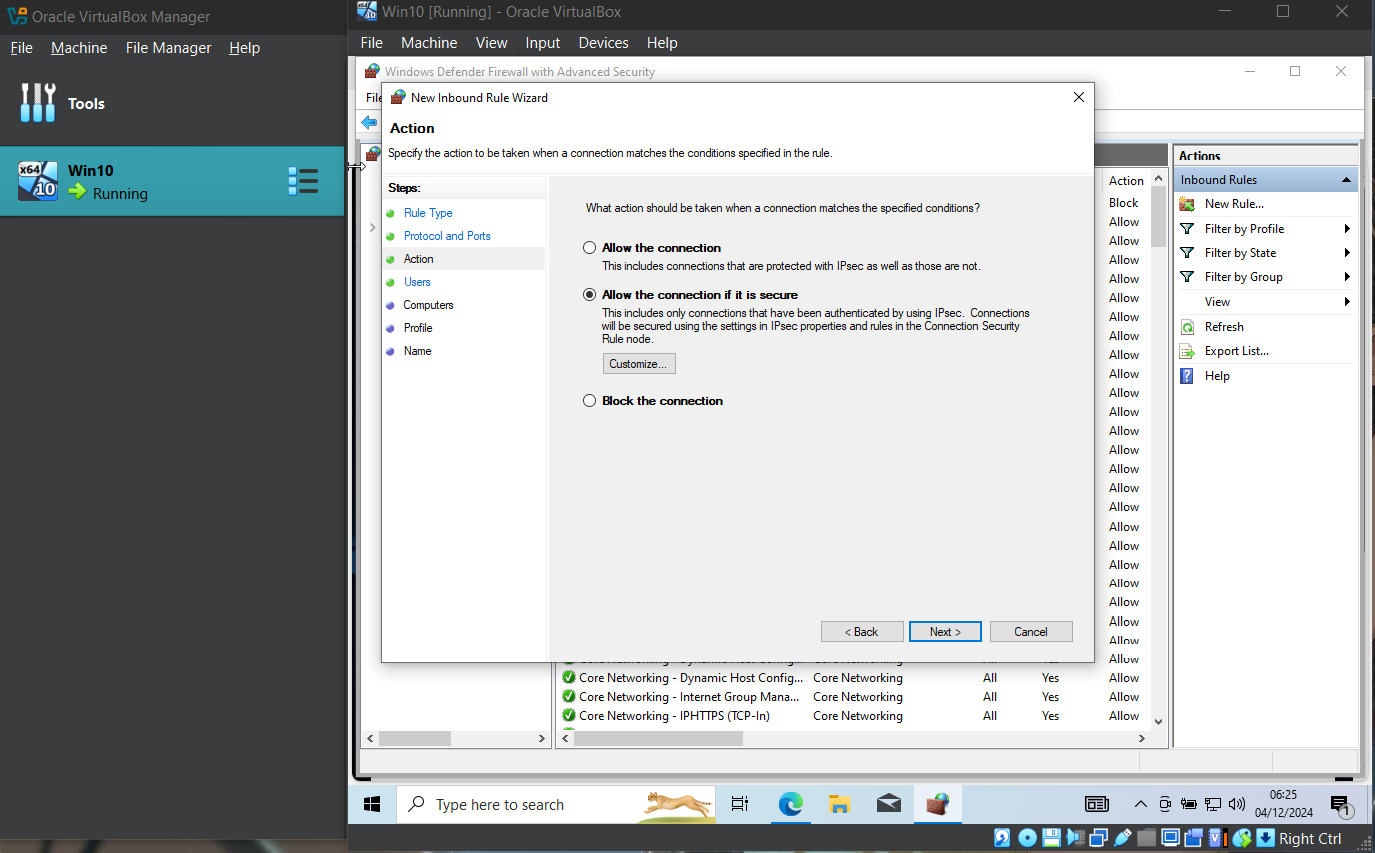


Table 20 відкриття порту

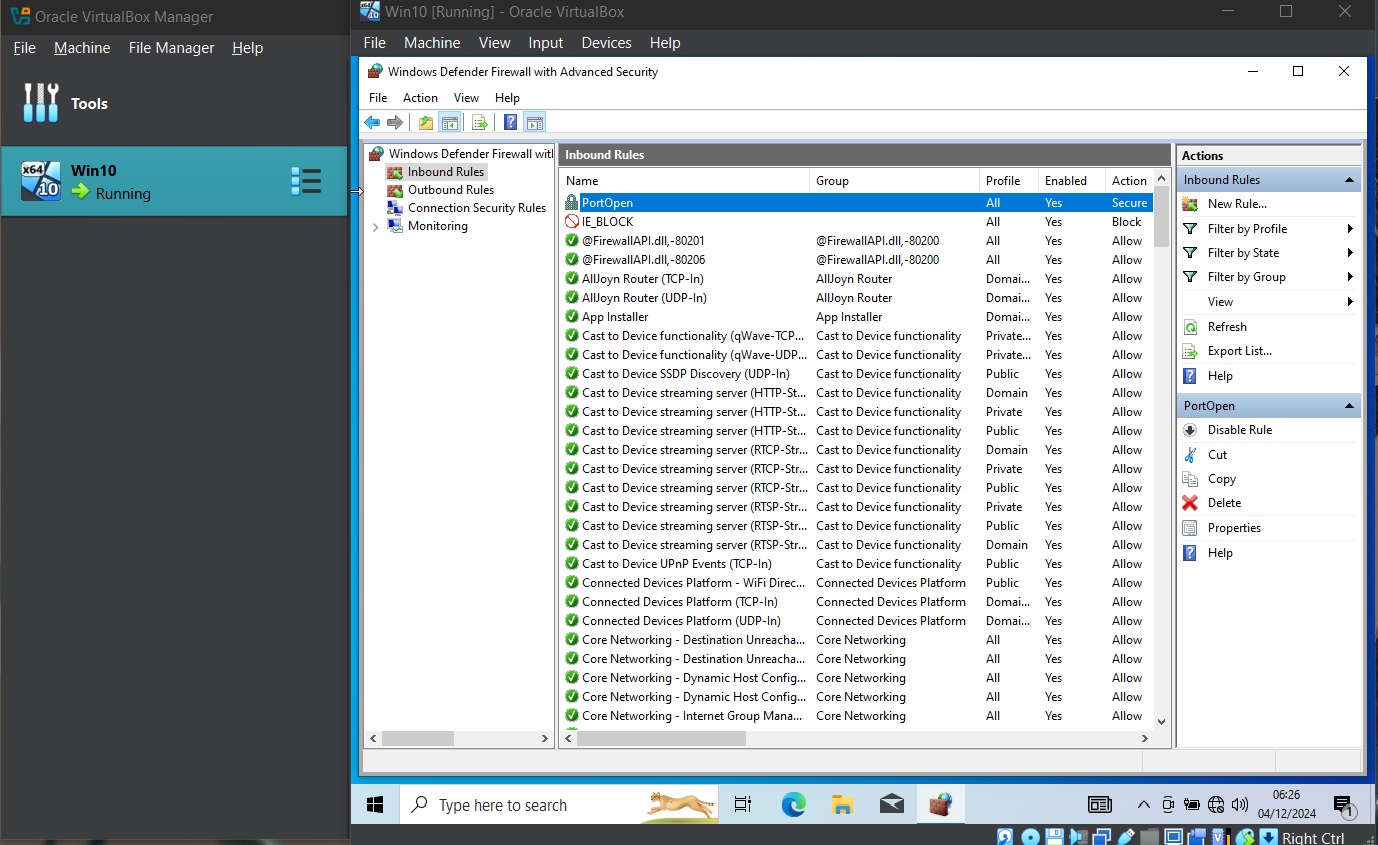


Table 21 Нове правило в переліку брєндмаузера

**Висновок:**

У ході лабораторної роботи досліджено механізми захисту даних у комп’ютерних мережах із використанням вбудованих інструментів Windows. Опановано налаштування брандмауера, створення правил для трафіку, перевірку ICMP-з’єднань і відкриття портів. Встановлено, що правильна конфігурація мережевих політик суттєво підвищує безпеку системи, знижуючи ризик атак та несанкціонованого доступу.

**Контрольні запитання**

**Наведіть приклади класів електронної комерції і основні засоби їх безпеки.**  
Електронна комерція охоплює різні моделі взаємодії між бізнесами та споживачами. У моделі Business-to-Consumer (B2C) компанії продають товари кінцевим споживачам, і для забезпечення безпеки використовуються технології захисту платіжних даних, такі як SSL/TLS та стандарти PCI DSS, а також багатофакторна аутентифікація. У моделі Business-to-Business (B2B) компанії взаємодіють між собою, використовуючи VPN для забезпечення безпеки з’єднань і контроль доступу до корпоративних даних. Модель Consumer-to-Business (C2B) включає платформи, де споживачі пропонують послуги або товари бізнесу, і тут важливими є перевірка особистості та антифрод-системи для забезпечення безпеки транзакцій. У моделі Consumer-to-Consumer (C2C) споживачі продають товари іншим споживачам через платформи, де важливими засобами захисту є захист транзакцій через escrow-сервіси, а також система рейтингів та відгуків для оцінки репутації продавців і покупців.

**Наведіть приклади основних сервісів, що забезпечуються зв’язком з мережею Інтернет, і засоби їх безпеки.**  
Серед популярних сервісів, що працюють через Інтернет, можна виділити електронну пошту, хмарні сервіси, соціальні мережі та інтернет-банкінг. Для захисту електронної пошти використовуються технології шифрування, такі як TLS, а також засоби боротьби з фішингом і спамом. Хмарні сервіси забезпечують безпеку через шифрування даних як в стані спокою, так і під час передачі, а також резервне копіювання для відновлення даних. У соціальних мережах для захисту даних користувачів передбачено функції приватності, а також моніторинг порушень і шифрування повідомлень у месенджерах. В інтернет-банкінгу застосовуються SSL/TLS сертифікати, контроль транзакцій у реальному часі і використання одноразових паролів (OTP) для підвищення безпеки користувачів.

**Надайте ваше розуміння брандмауера.**  
Брандмауер (Firewall) – це засіб безпеки, який служить для контролю і фільтрації мережевого трафіку між різними пристроями або мережею і Інтернетом. Його основна мета – захистити комп'ютер або мережу від несанкціонованого доступу, мережевих атак та інших загроз. Брандмауер здійснює фільтрацію трафіку за різними критеріями, такими як IP-адреси, порти та протоколи, що дозволяє блокувати шкідливий трафік і забезпечувати безпеку. Він також допомагає реалізувати політики безпеки, наприклад, обмежуючи доступ до певних веб-ресурсів або сервісів, а також запобігає атакам типу DoS/DDoS.

**Які основні різновиди заміни мережевої адреси використовуються в брандмауерах?**  
У брандмауерах застосовуються різні методи заміни мережевих адрес, які відносяться до технології NAT (Network Address Translation). Статичний NAT призначає одну внутрішню IP-адресу для конкретної зовнішньої, що забезпечує постійний доступ до певних пристроїв, наприклад, вебсерверів. Динамічний NAT дозволяє використовувати пул зовнішніх адрес для тимчасової заміни внутрішніх IP-адрес. PAT (Port Address Translation) дає змогу кільком пристроям використовувати одну зовнішню IP-адресу, розрізняючи їх за портами, що допомагає зекономити зовнішні адреси. Зворотний NAT, або Reverse NAT, використовується для маршрутизації запитів з Інтернету до внутрішніх серверів за допомогою зовнішньої IP-адреси