

Методичні вказівки  
до лабораторної роботи №5  
**«Встановлення та конфігурування систем Firewall  
(в ОС Windows та Ubuntu)»**  
з навчальної дисципліни вільного вибору  
**«Основи інформаційної та кібербезпеки»**

**Зміст практичного заняття:** Вивчення міжмережових екранів для захисту даних в комп'ютерних мережах.

### Загальні відомості

**Міжмережевий екран** (брандмауер від нім. *brandmauer* – міцна стіна; *файрвол* від англ. *firewall* – вогняна стіна) – програмне забезпечення, розташоване на комп'ютері з метою захисту його інформаційних ресурсів або ресурсів корпоративної мережі від доступу із зовнішніх мереж.

За допомогою брандмауерів можна значно підвищити мережеву безпеку і зменшити ризик для комп'ютера шляхом фільтрації небезпечних за своєю природою служб. При використанні файрволу комп'ютер (або локальна мережа) буде піддаватись меншому числу небезпек, оскільки міжмережевий екран пропускатиме тільки безпечні протоколи. Принцип захисту комп'ютера в локальній мережі з використанням брандмауера показаний схематично на Рис. 1:

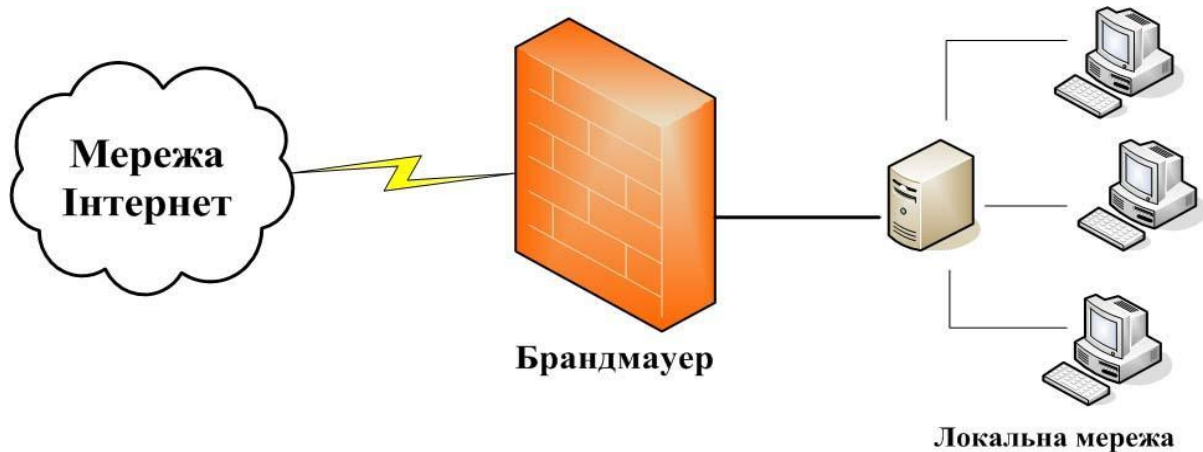


Рис. 1. Використання брандмауера

**Міжмережеві екрани** (файрволи чи брандмауери) є додатковою лінією оборони мереж, за допомогою яких забезпечуються всі з'єднання комп'ютера із зовнішнім світом, захист локальних мереж і окремих комп'ютерів від несанкціонованого доступу з боку зовнішніх мереж шляхом фільтрації двостороннього потоку повідомлень. Вони поділяються на дві великі групи:

**персональні файрволи** (брандмауери) – екрани, встановлені безпосередньо на захищувані персональні комп'ютери, та

**файрволи** (брандмауери) для захисту локальних (і корпоративних) мереж, що також називаються міжмережевими екранами.

Здебільшого, міжмережевий екран – це стратегія захисту ресурсів організації, доступних з Інтернету. При цьому він відіграє роль варті між небезпечним Інтернетом і більш надійними внутрішніми мережами.

Фактично міжмережеві екрани – це "урізані" VPN-агенти для здійснення лише фільтрації без тунелювання, оскільки в них не використовуються криптографічні методи для захисту даних.

Однак, крім фільтрації, міжмережеві екрани виконують ряд додаткових функцій, зокрема: антивірусне сканування, контроль коректності пакетів, контроль коректності з'єднань (наприклад, встановлення, використання і розриву TCP-сесій), контент-контроль. Вони можуть працювати з **FTP** (порт 21), **e-mail** (порт 25), **HTTP** (порт 80), **NNTP** (Network News Transmission Protocol, RFC 977) – протокол читання мережеских новин із багатетапним передаванням даних (порт 119), **Telnet** (порт 23), Gopher – назва походить від англ. *go for* – система пошуку даних в мережі Інтернет (порт 70), **SSL** (Secure Socket Layer [Level] – рівень захищених сокетів) – протокол безпечних з'єднань (порт 443) і деякими іншими відомими протоколами.

За допомогою брандмауерів забезпечують кілька типів захисту:

- блокування небажаного трафіку;
- направлення вхідного трафіку лише до надійних внутрішніх систем;
- приховування вразливих систем, які не можна убезпечити від атак з Інтернету іншим способом;
- протоколювання трафіку у внутрішню мережу та з неї;
- приховування даних, такі як імена систем, топологія мережі, типи мережеских пристроїв і внутрішні ідентифікатори користувачів, від Інтернету;
- забезпечення більш надійної аутентифікації, ніж та, що надається через стандартні програмні додатки.

## 1. Основи IP- адресації

Для організації міжмережеских з'єднань, необхідний відповідний протокол. Усі параметри, від швидкості передачі даних і до методів адресації при транспортуванні окремих повідомлень визначаються і задаються протоколами, що використовуються в даній конкретній мережі.

Протокол Інтернету – це просто сукупність погоджень, що визначає обмін даними між різними програмами. Протоколи задають способи передачі даних, повідомлень, обробку помилок мережі.

В Інтернеті базовим протоколом є протокол **TCP/IP** (Transmission Control Protocol/Internet Protocol). IP відповідає за доставку повідомлень за необхідною адресою.

В мережі TCP / IP існують адреси трьох типів: фізична (MAC-адреса), мережева (IP-адреса) і символічна (DNS-ім'я).

Отже для кожного пристрою у мережах IP можна говорити про адреси трьох рівнів:

- Фізична адреса пристрою (точніше - визначеного інтерфейсу). Для пристроїв у мережах Ethernet – це **MAC-адреса** мережної карти або порту маршрутизатора. Ці адреси призначаються виробниками обладнання. Фізична адреса має шість байтів: старші три байти – ідентифікатор фірми-виробника. Молодші три байти призначаються самим виробником;
- **IP-адреса**, що складається з чотирьох байтів. Ця адреса застосовується на мережному рівні еталонної моделі OSI;
- Символьний ідентифікатор – ім'я. Цей ідентифікатор може призначатися адміністратором довільно.

Internet, базуючись на профілі TCP/IP, представляє собою з'єднання маршрутизаторами (роутерами) окремих IP-мереж (які більш точно треба називати IP-підмережами, або первинні мережі, або приватні мережі). IP-мережа повинна мати унікальну IP-адресу, а вузол (хост, робоча станція тощо) в такій мережі повинен мати адресу (номер) в мережі.

Отже, **IP-адреса** є парою (**Адреса\_мережі**, **Адреса\_вузла\_в\_мережі**). Ще використовується термінологія для такої пари (Префікс, Суфікс), тобто префікс адреси є адресою мережі, а суфікс, відповідно, адресою вузла в мережі. Також адресація передбачає множину адрес спеціального призначення, інтерпретація котрих має особливості, зокрема, такі адреси "працюють" лише в первинній мережі та за межі її не повинні взагалі "виходити".

IP-адреса має довжину 4 байти (32 біти) і звичайно записується у вигляді чотирьох чисел, що представляють значення кожного байта в десятковій формі, і розділених крапками, наприклад:

128.10.2.30 – традиційна десяткова форма представлення адреси,

10000000 00001010 00000010 00011110 - двійкова форма представлення цієї ж адреси.

Яка частина адреси відноситься до номера мережі, а яка до номера вузла, визначається значеннями перших бітів адреси:

Якщо адреса починається з 0, то мережа відноситься до **класу А**, і номер мережі займає один байт, інші 3 байти інтерпретуються як номер вузла в мережі. Мережі класу А мають номери в діапазоні від 1 до 126. (Номер 0 не використовується, а номер 127 зарезервований для спеціальних цілей, про що буде сказано нижче.) У мережах класу А кількість вузлів повинно бути більше  $2^{16}$ , але не перевищувати  $2^{24}$ .

Якщо перші два біти адреси рівні 10, то мережа належить до **класу В** і є мережею середніх розмірів з числом вузлів  $2^8 - 2^{16}$ . У мережах класу В під адресу мережі і під адресу сайту відводиться по 16 бітів, тобто по 2 байти.

Якщо адреса починається з послідовності 110, то це мережа **класу С** з числом вузлів не більше  $2^8$ . Під адресу мережі відводиться 24 біта, а під адресу сайту – 8 біт.

Якщо адреса починається з послідовності 1110, то вона є адресою **класу D** і позначає особливий, групова адреса – multicast. Якщо в пакеті як адресу призначення вказана адреса класу D, то такий пакет повинні отримати всі вузли, яким присвоєно цю адресу.

Якщо адреса починається з послідовності 11110, то це адреса **класу Е**, він зарезервований для майбутніх застосувань.

Саме тому, що перший байт адреси 129.54.65.3 потрапляє в діапазон 128 -191, ми можемо сказати, що ця адреса відноситься до класу В, а значить, номером мережі є перші два октети, доповнені двома нульовими байтами – 129.54.0.0, а номером вузла – 0.0.65.3.

Адреса **127.0.0.1** зарезервована для організації зворотного зв'язку при тестуванні роботи програмного забезпечення вузла без реального відправлення пакета по мережі. Ця адреса має назва loopback.

Альтернативою цієї традиційної схеми є використання іншої ознаки, за допомогою якої можна більш гнучко встановлювати межу між номером мережі та номером вузла. Такою ознакою є маска – 32-розрядне число, яке використовується в парі з IP-адресою. Двійковий запис маски містить одиниці у тих розрядах, які повинні в IP-адресі інтерпретуватись як номер мережі. Оскільки номер мережі є цільною частиною адреси, одиниці у масці повинні являти собою неперервну послідовність.

Для стандартних класів IP-адрес маски мають такі значення:

- Клас А – 11111111. 00000000. 00000000. 00000000 (255.0.0.0);
- Клас В – 11111111. 11111111. 00000000. 00000000 (255.255.0.0);
- Клас С – 11111111.11111111.11111111.00000000 (255.255.255.0).

Супроводжуючи кожну IP-адресу маскою, можна відмовитися від понять класів адрес і зробити більш гнучкою систему адресації. Наприклад, якщо адресу 129.54.170.164 асоціювати з маскою 255.255.255.0 – номером мережі (а точніше підмережі) буде 129.54.170.0 (а не 129.54.0.0, як це визначено системою класів), якщо з маскою 255.255.248.0 – то 129.54.168.0, а якщо з маскою 255.255.255.224 – то 129.54.170.160.

Механізм масок широко використовується в IP-маршрутизації, причому маски можуть використовуватись з різною метою. За їх допомогою адміністратор може структурувати свою мережу, не вимагаючи від постачальника послуг додаткових

номерів мереж. На основі цього ж механізму постачальники послуг можуть об'єднати адресні простори декількох мереж шляхом введення так званих “префіксів” з метою зменшення об'єму таблиць маршрутизації та підвищення за рахунок цього продуктивності роботи маршрутизаторів.

**IPv6** (англ. Internet Protocol version 6) – нова версія протоколу IP, покликана вирішити проблеми, з якими зіткнулася попередня версія (IPv4) при її використанні в Інтернеті, за рахунок використання довжини адреси 128 біт замість 32. Адреси розділяються двокрапками (наприклад, fe80:0000:0000:0000:2000:f8ff:fe21:67cf). Велика кількість нульових груп може бути пропущена за допомогою подвійної двокрапки (fe80::200:f8ff:fe21:67cf). Такий пропуск має бути єдиним в адресі.

Минула версія протоколу підтримувала два варіанти для користувача IP-адрес:

- **статична** адреса, яка була незмінним ідентифікатором;
- **динамічна**, змінювалася при кожному новому підключенні до мережі.

У шостій версії протоколу було вирішено залишити тільки варіант **статичної** адреси. Таке рішення було обумовлено тим, що, в перспективі кожному пристрою в підмережі будь-якого рівня буде доступний свій унікальний ідентифікатор (IP-адреса).

### ***Утиліти ОС, пов'язані з IP-адресацією***

Як мінімум, потрібно вміти користуватися утилітами (командами) **ipconfig**, **ping** та **tracert** (в MS Windows, або аналогічними для Unix/Linux).

**ipconfig** – утиліта командної стрічки ipconfig відображає конфігурацію IP-адресації хоста.

**ping** – утиліта дозволяє встановити існування певної IP-адреси, відсиленням до неї певної кількості ехо-пакетів (Echo-Request). Вузол-адресат має дати відповідь на кожний отриманий ехо-пакет. Відсутність відповіді означає або відсутність адреси, або неможливість дати відповідь (перевантаженість, відключенням ехо-пакетів на сервері тощо).

**tracert** – утиліта дозволяє побачити маршрут проходження пакету до заданої адреси (IP чи доменної) вузла. Враховуючи, що профіль TCP/IP використовується в дейтаграмних пакетних мережах, що означає індивідуальну маршрутизацію кожного пакета (дейтаграми). Тому два запуски підряд tracert можуть відрізнитися маршрутами! Утиліта використовує хоп-метрику мережі, в якій проходження вузла (тут буде маршрутизатора) = 1 хопу. Отже результатом буде відстань в хопх до вказаної адреси та адреса кожного хопу (стрибка) і час очікування хопу.

## 2. Типи брандмауерів

Залежно від технічного виконання і виконуваних функцій брандмауери поділяються на брандмауери з фільтрацією пакетів, брандмауери на основі машин, під'єднаних до двох мереж, брандмауери з ізольованим хостом і брандмауери з ізольованою підмережею.

**Брандмауер з фільтрацією пакетів** є найпоширенішим і найпростішим при реалізації для маленьких мереж із простою структурою. Проте він має ряд недоліків і менш бажаний, ніж інші приклади брандмауерів. Як правило, брандмауер з фільтрацією пакетів встановлюється на маршрутизаторі з фільтрацією пакетів, через який відбувається з'єднання з Інтернет (або підмережею), на якому конфігуруються правила фільтрації пакетів, що дозволяє блокувати або фільтрувати пакети на підставі протоколів і адрес. Звичайно, з машин внутрішньої мережі надається повний доступ до Інтернету, а доступ з боку Інтернету до всіх або майже до всіх систем внутрішньої мережі блокується. Проте за допомогою маршрутизатора можна допускати вибірковий доступ до систем і сервісів (це залежить від політики). Зазвичай, блокуються такі потенційно небезпечні сервіси, як NIS, NFS і X Windows.

**NIS** (Network Information Service, мережева інформаційна служба) та **NFS** (Network File System, розподілена мережева файлова система або інколи в літературі: "система мережевих файлів", розроблена компанією Sun Microsystems Inc.; існує також: однойменний протокол підтримки мережевих файлових систем) – це сервіси, за допомогою яких можна значно зменшити час, що відводиться на конфігурування хостів, управляти рядом баз даних, таких як файли паролів, за допомогою віддаленого доступу до них забезпечувати можливість спільного використання файлів і даних. Вони спеціально розроблені для зменшення витрат на адміністрування в локальній мережі.

**X Windows** (або X-Windows) — графічний інтерфейс, використання якого дозволяє користувачам працювати зі своїми обчисленнями та з системою у графічному режимі. Віконну систему із назвою "X" (англійською саме так правильно називати систему "X window system" – "віконна система X", а не "X-Window") створила група молодих дослідників і програмістів з Массачусетського технологічного інституту.

**Брандмауер на основі машини, під'єднаної до двох мереж** – краща альтернатива, ніж брандмауер на базі маршрутизатора з фільтрацією пакетів. Він складається з хосту, що має два мережеві інтерфейси, у якого відключено функцію маршрутизації IP-пакетів з одного інтерфейсу на інший (тобто з хоста не можна маршрутизувати пакети між двома мережами). Крім того, можна помістити маршрутизатор з фільтрацією пакетів між мережею і цим хостом для забезпечення додаткового захисту. Це допоможе створити внутрішню ізольовану підмережу, яка зможе бути використана для розміщення спеціалізованих систем, таких як інформаційні сервери і модемні пули (це певна кількість модемів, об'єднаних в одному корпусі (для одночасної організації кількох процесів)). На відміну від

маршрутизатора з фільтрацією пакетів за допомогою брандмауера даного типу можна цілком блокувати передавання трафіка між Інтернетом і мережею, що захищається.

Брандмауер на основі хоста, під'єданого до двох сегментів мережі – це, фактично, брандмауер із двома мережевими платами, кожна з яких під'єднана до окремої мережі. Наприклад, одна мережева плата з'єднана із зовнішньою або небезпечною мережею, а інша – із внутрішньою або безпечною мережею. У цій конфігурації ключовим принципом забезпечення безпеки є заборона прямої маршрутизації трафіка з недовіреної мережі в довірену – брандмауер завжди повинен бути при цьому проміжною ланкою.

**Брандмауер з ізольованим хостом** – більш гнучкий брандмауер, ніж той, що побудований на основі шлюзу з двома інтерфейсами, хоча гнучкість досягається ціною деякого зменшення безпеки. Брандмауер такого типу доречний для мереж, яким потрібна більша гнучкість, ніж та, яку може дати використання брандмауера на основі шлюзу з двома інтерфейсами. Брандмауер даного типу складається з маршрутизатора із фільтрацією пакетів і прикладного шлюзу, розміщеного в захищеній підмережі.

**Брандмауер із ізольованою підмережею** – це об'єднання шлюзу з двома інтерфейсами і брандмауера з ізольованим хостом.

Якщо прослідкувати історію розвитку технологій міжмережевих екранів, то можна виділити кілька їх поколінь: фільтри пакетів, міжмережеві екрани рівня з'єднання, міжмережеві екрани прикладного рівня, міжмережеві екрани з динамічною фільтрацією пакетів, міжмережеві екрани інспекції станів, міжмережеві екрани рівня ядра, персональні міжмережеві екрани, розподілені міжмережеві екрани.

Пакетний фільтр – спрощений варіант міжмережевого екрану лише для фільтрації пакетів без додаткових функцій.

Спочатку **технологія фільтрації пакетів** застосовувалась на мережевому рівні і фільтрації піддавались лише IP-адреси. Зараз аналіз мережевого трафіка при фільтрації пакетів проводиться і на транспортному рівні. Кожен IP-пакет досліджується на відповідність певній множині правил. За цими правилами встановлюють дозвіл зв'язку за змістом заголовків мережевого і транспортного рівнів моделі TCP/IP, аналізується і напрямок передавання пакету.

За допомогою міжмережевих **екранів рівня з'єднання** перевіряють факт, що пакет є або запитом на TCP-з'єднання, або подаються дані, що мають відношення до вже встановленого з'єднання, або відноситься до віртуального з'єднання між двома транспортними рівнями.



За допомогою міжмережевих **екранів прикладного рівня** оцінюють мережеві пакети на відповідність певному прикладному рівню перед встановленням з'єднання. За їх допомогою досліджують дані всіх мережевих пакетів на прикладному рівні та встановлюють стан повного (завершеного) з'єднання і послідовних даних. Крім того, за допомогою міжмережевих екранів можна перевіряти інші параметри безпеки, що містяться всередині даних прикладного рівня (паролі, запити служб).

Брандмауери прикладного рівня повинні конфігуруватися так, щоб весь вихідний трафік здавався таким, що виходить від брандмауера (тобто щоб лише брандмауер було видно із зовнішніх мереж). У такий спосіб буде заборонений прямий доступ до внутрішніх мереж. Усі вхідні запити від різних мережесервісів, таких як Telnet, FTP, HTTP, RLOGIN, і т.д., незалежно від того, який внутрішній хост запитується, повинні проходити через відповідний проксі-сервер на брандмауері. Прикладні шлюзи потребують проксі-серверів для кожного сервісу (FTP, HTTP і т.д.), підтримуваного через брандмауер.

Англійське слово "proxy" означає "посередник, повноважний представник". **Проксі-сервер** – це програма-посередник між користувачем та Інтернетом, яка встановлюється на комп'ютері-шлюзі, що має доступ як до Інтернет, так і до замкненої локальної мережі. Призначення проксі-серверів – ретранслювати пакети відповідної служби (наприклад, FTP чи HTTP) в Інтернет і перевіряти (а у випадку необхідності обмежувати) права доступу клієнта. Для всіх популярних служб Інтернет існують свої проксі-сервери.

**Telnet-протокол** (Network Terminal Protocol) є протоколом програмного додатку, де використовується транспортний протокол TCP і забезпечуються взаємозв'язки термінального пристрою та термінал-орієнтованого процесу, а також може використовуватись для організації зв'язку ("термінал-термінал") і розподілених обчислень ("процес-процес"). По суті використання Telnet надає можливість під'єднання віддаленого клієнта в режимі текстового терміналу до головного комп'ютера через мережу. При використанні Telnet, зазвичай, вимагається надсилання пари ім'я-пароль до мережесервісів у незашифрованому вигляді — це серйозне уразливе місце.

**HTTP** – HyperText Transfer Protocol – протокол роботи з гіпертекстовими документами в Інтернет

**HTTPS** – захищений шифруванням аналог HTTP.

TCP портом за замовчуванням для HTTPS є 443, для HTTP — 80.

Використання міжмережесервісів **екранів з динамічною фільтрацією пакетів** дозволяє здійснювати модифікацію бази правил "на льоту" (on fly). Це реалізується для протоколу UDP. У цьому випадку через міжмережесервісний екран проводиться узгодження всіх UDP-пакетів, що проходять через віртуальне з'єднання, перетинаючи периметр безпеки. Якщо генерується пакет відповіді і передається до джерела запиту, то встановлюється віртуальне з'єднання, і пакет може надіслатися до серверу



міжмережевого екрану. Дані, асоційовані з віртуальним станом, запам'ятовуються на короткий проміжок часу, тому якщо пакет відповіді не отримано, то з'єднання вважається закритим.

Технологія динамічної фільтрації пакетів використовується не лише для протоколу UDP і прикладних протоколів, що спираються на нього, тому її можна назвати технологією встановлення віртуального з'єднання або віртуального сеансу.

**Технологією інспекції станів** (stateful inspection) проводиться аналіз пакетів на трьох вищих рівнях. Цей підхід використовується багатьма розробниками, але, оскільки найменування запатентоване компанією Check Point, вони змушені надавати йому різні найменування (крім stateful inspection використовуються expert inspection, smart filtering, adaptive screening, multilevel inspection та ін.).

За допомогою пристрою інспекції станів здійснюється аналіз пакетів і формування даних про «стан віртуального з'єднання». З'єднання може знаходитись у стані встановлення, передавання або від'єднання. У кожному з цих станів є можливість інтерпретувати комунікаційні дані певним способом.

В підсистемі безпеки міжмережевих **екранів**, що функціонують на **рівні ядра** (Kernel Proxy), використовується багато елементів з розглянутих технологій міжмережевих екранів. Вона включає: ядро безпеки, модуль управління хостом, модуль управління каналами зв'язку міжмережевого екрану, агент реєстрації входів, агент аутентифікації.

Основним модулем є ядро безпеки, за допомогою якого аналізується кожний вхідний і вихідний пакет, і яке функціонує усередині ядра операційної системи. Це дозволяє забезпечити високу продуктивність міжмережевих екранів.

Розглянуті види міжмережевих екранів, особливо міжмережеві екрани прикладного рівня і рівня ядра, є надзвичайно складними та дорогими продуктами, тому для захисту комп'ютерів окремих користувачів стали розроблятися персональні міжмережеві екрани. **Персональні міжмережеві екрани** (їх називають також вбудованими, embedded) є програмними продуктами, що розташовуються всередині комп'ютера на нижчому рівні операційної системи – між мережевими платами і всіма протокольними стеками (TCP/IP, NetBEUI, IPX і т.д. для Windows ).

За допомогою персональних файрволів (брандмауерів) забезпечують фільтрацію вхідного та вихідного трафіка, перевірку цілісності програмних додатків, шифрування даних, захист електронної пошти від вірусів, захист комп'ютера від шпигунських програм, а також багато інших функцій, за допомогою можна убезпечити комп'ютерні інформаційні ресурси.

**Фільтрація**, зазвичай, відбувається на чотирьох рівнях OSI (Open System Interconnection – еталонної моделі взаємозв'язків відкритих систем, в якій реалізовано

концепцію шарів, що стала основною архітектурною моделлю для передавання міжкомп'ютерних повідомлень): каналному (Ethernet), мережевому (IP), транспортному (TCP, UDP), прикладному (FTP, Telnet, HTTP, SMTP і т.д.).

Після встановлення на комп'ютері файрволу, як правило, відразу помічається велика кількість спроб різноманітних дивних програм, «вирватись» в Інтернет, використовуючи для цього незвичайні порти. Це може бути шкідливе програмне забезпечення, встановлене в системі різними способами, через яке у найгіршому випадку персональний комп'ютер використовується під контролем третьої особи, що знаходиться десь в Інтернеті. Антивірусні програми часто не виявляють такого типу шкідливих програм. Встановлення файрволу на комп'ютері, під'єднаному до Інтернету, дозволить упередити всі спроби за допомогою різного шпигунського програмного забезпечення одержати доступ до даних, що зберігаються в комп'ютері.

Найпопулярнішими на сьогодні брандмауерами є Outpost Firewall, ZoneAlarm Pro, Comodo, TinyWall, Bitdefender Total Security, Norton Personal Firewall та ін.

Якщо у вас є маршрутизатор wifi, ви, ймовірно, вже маєте захист від вторгнення у вигляді вбудованого апаратного брандмауера. Крім того, у вас може бути вбудований програмний брандмауер у вашу операційну систему, наприклад, Windows Defender для користувачів Windows. Однак ці брандмауери не є ідеальними, і вам може знадобитися додатковий захист. І це не тільки користувачів Windows. Жодна операційна система не захищена від атаки, тому ніхто не повинен скаржитися на вразливість своїх підключених до Інтернету пристроїв.

Дискусія про якість та захист, запропоновані брандмауером Windows, триває і, ймовірно, буде продовжуватись ще впродовж багатьох років. Незважаючи на те, що протягом багатьох років він стабільно вдосконалювався і тепер пропонує хороший рівень вхідного захисту, він все одно робить мало дій із вихідним трафіком.

За замовчуванням брандмауер Windows дозволяє весь вихідний трафік, якщо ви не створили правило для керування ним. Це означає, що будь-яке шкідливе програмне забезпечення або троянський кон'юнктурний сервер, який потрапив на ваші комп'ютери, має вільні можливості спілкуватися зі своїм хост-сервером та надсилати йому всі ваші дані. Саме з цієї причини спеціалісти не радять повністю покладатись на брандмауер Windows, навіть незважаючи на те, що рівень вхідного захисту зараз хороший.

## 2. Брандмауер захисника Windows з розширеною безпекою

Спочатку давайте уточнимо назву. Брандмауер у Windows має назву брандмауера **Windows Defender** у Windows 10 та 11, тоді як у Windows 7 та Windows 8.1 він зберігає стару назву Брандмауер Windows. Аналогічно, інструмент, який ми охоплюємо у цих методичних вказівках, має назву **Windows Defender Firewall з розширеною безпекою** в Windows 10 та 11, брандмауер Windows з розширеною безпекою в Windows 7 та Windows 8.1. Інструмент виглядає та функціонує однаково у

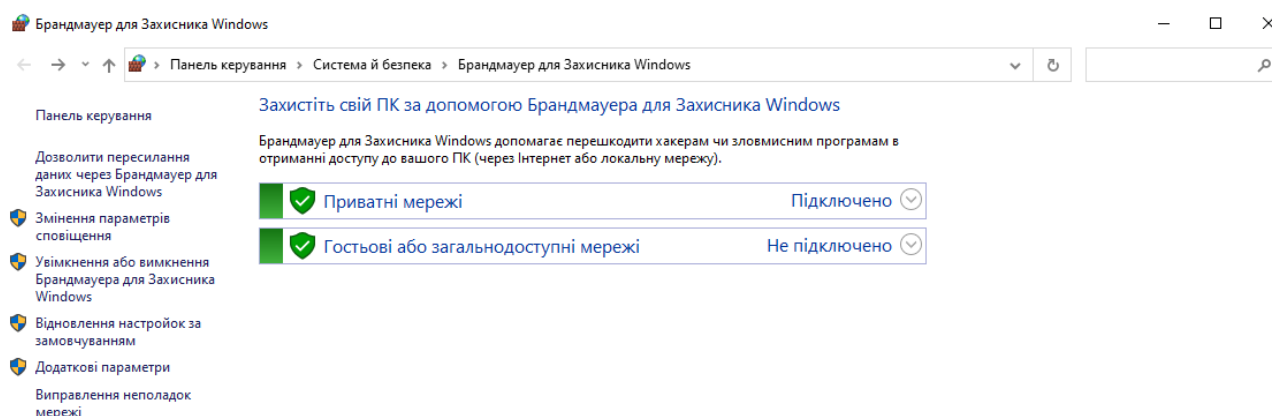
всіх чотирьох версіях Windows. Тут ми використовуємо скріншоти з Windows 10 та використовуємо ім'я брандмауера Windows Defender з розширеною безпекою, але описане дійсне для всіх чотирьох версій Windows.

### ***Що ви можете зробити з брандмауером Windows Defender із розширеною безпекою?***

Інструмент надає вам доступ до всіх функцій брандмауера Windows Defender . Ось деякі переваги його використання:

- **Зменшує ризик атак безпеки на мережу.** Брандмауер Windows Defender не є повноцінним рішенням безпеки, але це зменшує шанси на успішну мережеву атаку.
- **Підтверджує доступ до вашого пристрою.** Це можна зробити за допомогою IPsec (Internet Protocol Security), що забезпечує цілісність даних та захищає конфіденційність.
- **Забезпечує можливість брандмауера без додаткових інвестицій.** Брандмауер Windows Defender є частиною Windows.

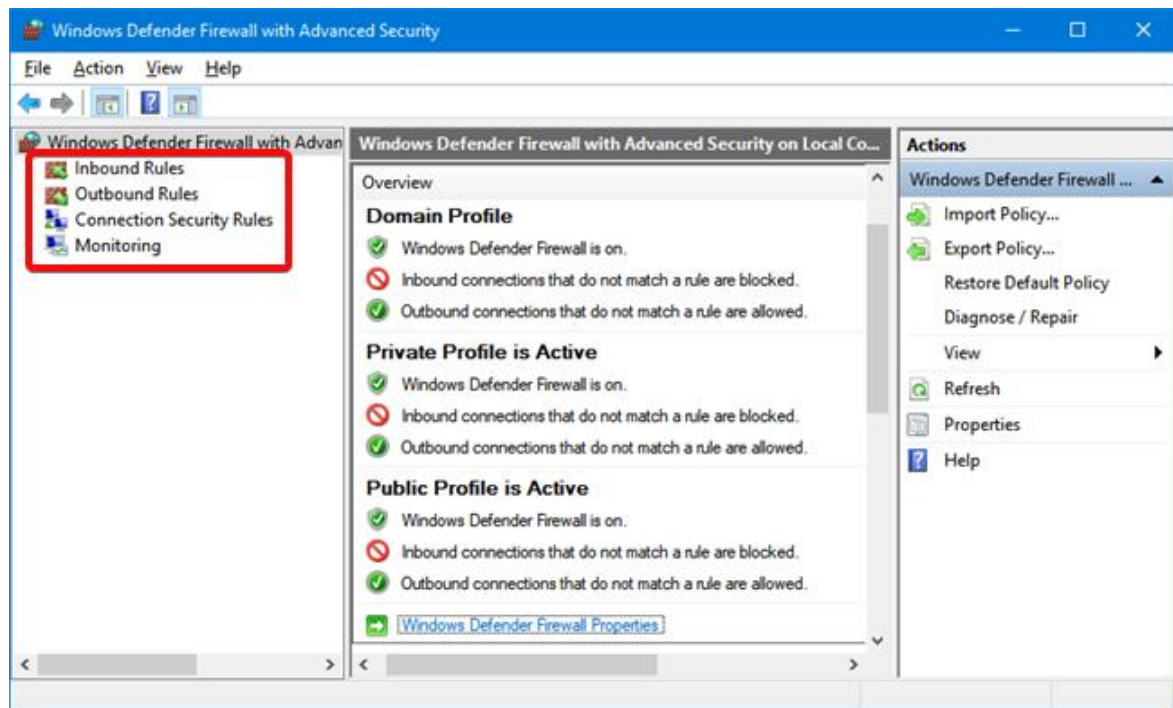
Відкрийте меню **Пуск**, введіть фразу **Брандмауер для Захисника Windows** і виберіть відповідний пункт у списку результатів пошуку.



У боковому меню навігації виберіть пункт **Додаткові параметри**. Імовірно, знадобиться ввести пароль адміністратора або підтвердити вибір.

Брандмауер Windows Defender з розширеною безпекою забезпечує переваги за допомогою цих функцій:

- Правила вхідних та вихідних даних
- Правила безпеки підключення
- Моніторинг



### ***Які вхідні та вихідні правила?***

Щоб забезпечити необхідну безпеку, брандмауер Windows Defender має стандартний набір вхідних та вихідних правил, які вмикаються залежно від місця підключеної мережі.

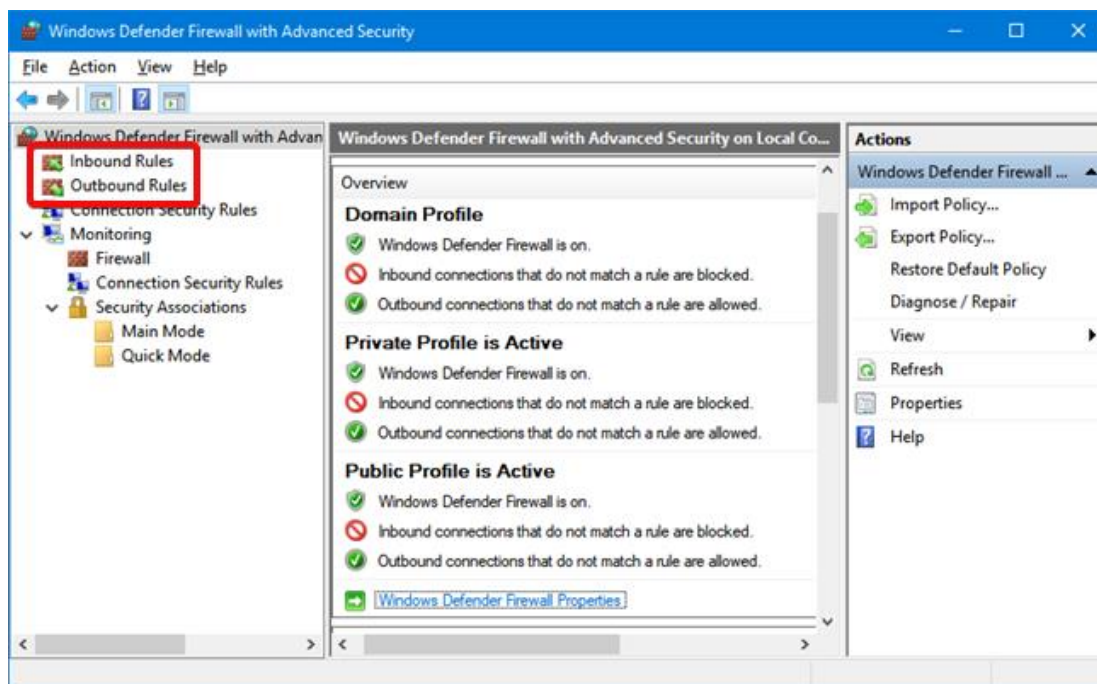
**Правила вхідних даних** застосовуються до трафіку, який надходить з мережі та Інтернету на комп'ютер або пристрій Windows. Вихідні правила застосовуються до трафіку з комп'ютера в мережу чи Інтернет.

Ці правила можна налаштувати так, щоб вони були специфічними для комп'ютерів, користувачів, програм, служб, портів або протоколів. Ви також можете вказати, до якого типу мережного адаптера (наприклад, бездротової, кабельної, віртуальної приватної мережі) або профілю користувача він застосовується.

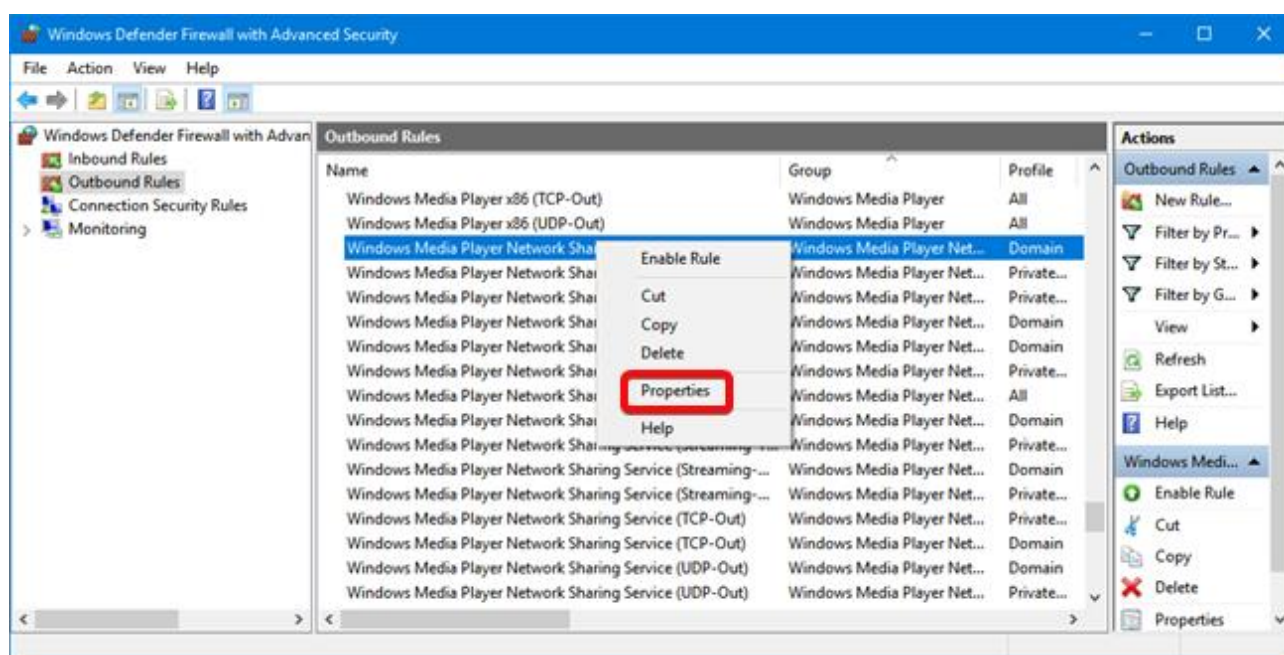
У брандмауері Windows Defender з розширеною безпекою ви можете отримати доступ до всіх правил та редагувати їх властивості. Все, що вам потрібно зробити, це натиснути або натиснути відповідний розділ на панелі зліва.

Правила, використовувані брандмауером Windows Defender, можна ввімкнути або вимкнути. Увімкнені або активовані позначені зеленою галочкою у стовпці *Ім'я*.

Виберемо в якості прикладу одне з правил для сервісу мережевого обміну Windows Media Player. Якщо ви керуєте медіа-бібліотекою на своєму пристрої Windows за допомогою медіапрогравача Windows, ви можете вирішити поділитися ними по мережі. Правила для цієї мети вимкнено за замовчуванням (зелений прапорець поруч із їх іменами відсутній).

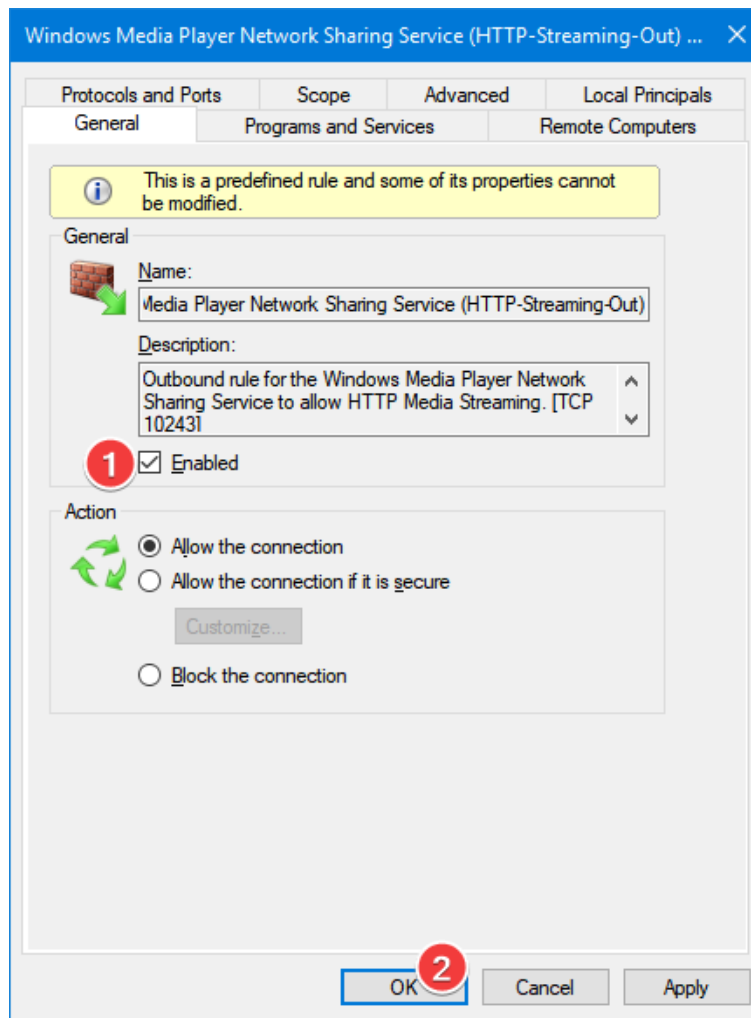


Якщо ви хочете дізнатися більше про певне правило та побачити його властивості, клацніть правою кнопкою миші та виберіть "Властивості" або виберіть його та натисніть "Властивості" у стовпці праворуч, у якому перераховані дії, доступні для вашого вибору.



У вікні "Властивості" ви знайдете повну інформацію про вибране правило, що воно робить і коли воно застосовується. Ви також можете редагувати його властивості та змінювати будь-який із доступних параметрів. Щоб увімкнути правило в нашому прикладі, позначте прапорець Увімкнено і натисніть кнопку ОК .

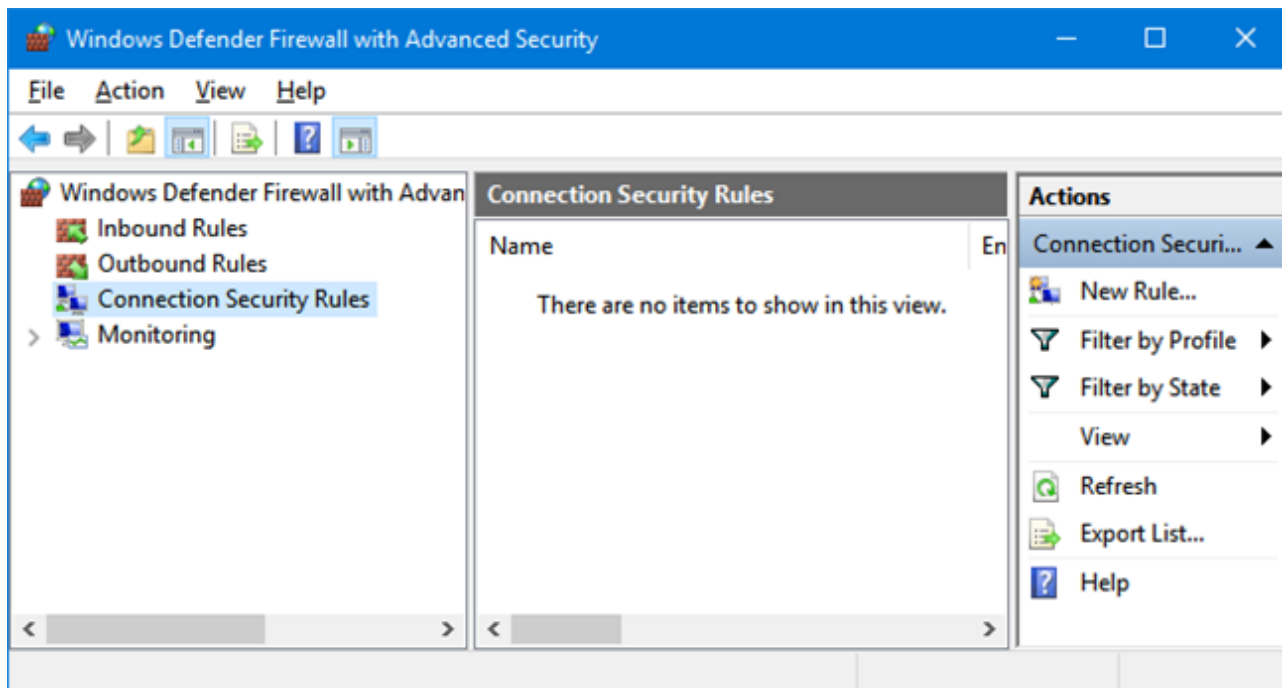




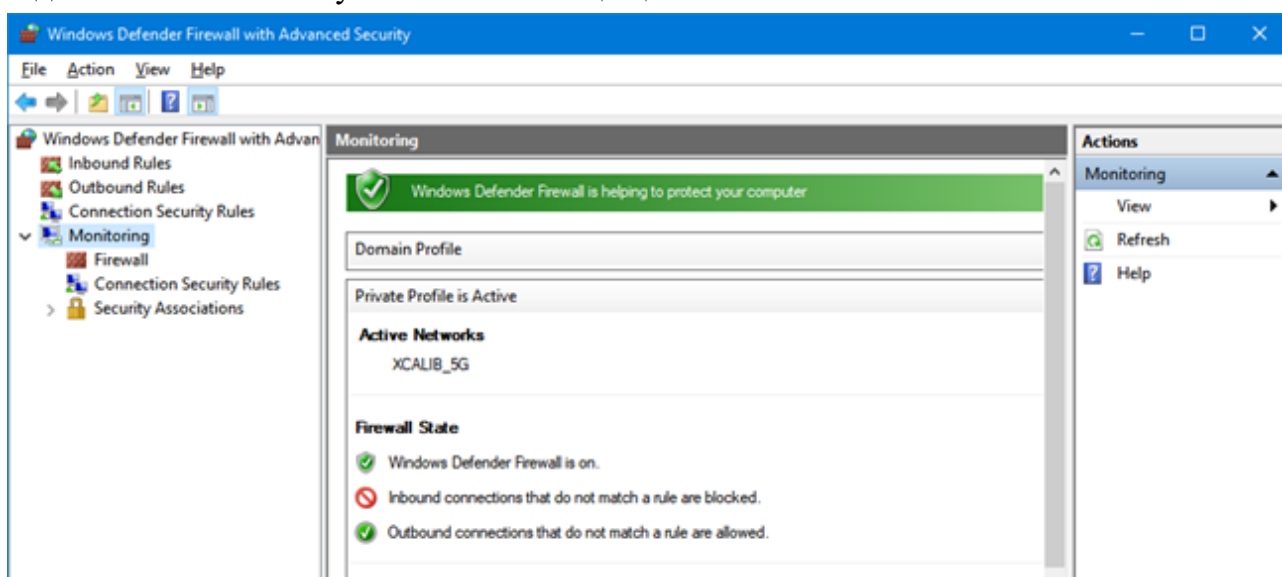
### ***Які правила безпеки підключення?***

Правила безпеки з'єднання використовуються для забезпечення трафіку між двома комп'ютерами під час перетину мережі. Одним із прикладів може бути правило, яке визначає, що з'єднання між двома конкретними комп'ютерами повинні бути зашифровані. Ці правила визначають, як і коли автентифіковано комп'ютери за допомогою **IPsec** (протокол безпеки Internet).

Хоча правила вхідного та вихідного характеру застосовуються лише до одного комп'ютера, правила безпеки з'єднання вимагають, щоб обидва комп'ютери були визначені та включені однакові правила. Якщо ви хочете дізнатися, чи є на вашому комп'ютері такі правила, натисніть або торкніться "Правила безпеки з'єднання" на панелі зліва. За замовчуванням на комп'ютерах та пристроях Windows таких правил не визначено. Вони, як правило, використовуються в бізнес-середовищах, і адміністратор мережі встановлює такі правила.



Брандмауер Windows Defender з розширеною безпекою також включає деякі функції моніторингу. У розділі "**Моніторинг**" ви можете знайти таку інформацію: активні правила брандмауера (як вхідні, так і вихідні), активні правила безпеки підключення та чи існують активні асоціації безпеки.



### *Додавання виключень в брандмауері Windows 10*

Іноді виникає необхідність додати виключення або правило для додатка в брандмауер, зазвичай додавання відбувається автоматично, але і буває випадки коли потрібно зробити це вручну. При інсталяції нової програми, яка хоче взаємодіяти через брандмауер – Windows вам запропонує дозволити або заборонити йому доступ. Але що якщо ви заборонили додавати його в винятку, а в даний момент виникла потреба його додати? Або можливо ви хочете видалити його з винятків в брандмауері?



Пропустити програму через Брандмауер для Захисника Windows можна двома способами. Обидва вони є ризикованими.

- Менш ризикований спосіб полягає в додаванні програми до списку дозволених програм.
- Більш ризикований – у відкритті порту.

Коли ви відкриваєте порт у брандмауері Windows Defender, ви дозволяєте трафік на ваш пристрій, ніби ви просвердлили отвір у брандмауері. Це робить ваш пристрій менш захищеним та може створити можливості для хакерів і зловмисних програм, що можуть скористатися одним із цих "отворів" для доступу до ваших файлів або використати ваш пристрій для поширення зловмисних програм на інші пристрої.

Зазвичай безпечніше додавати програму до списку дозволених програм, аніж відкривати порт. Порт залишається відкритим, доки ви його не закриєте, а дозволена програма відкриває "отвір" лише за потреби.

Щоб зменшити ризик для безпеки, зробіть ось що.

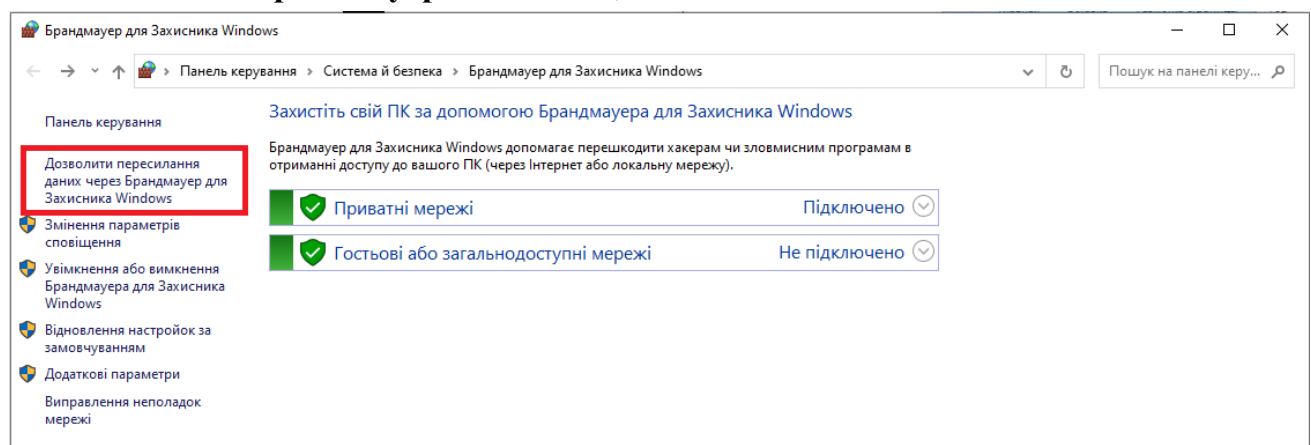
Додавайте програми до списку дозволених або відкривайте порти, лише якщо це дійсно необхідно, та виконуйте кроки з видалення програм зі списку дозволених або закриття портів, які більше не потрібні.

Ніколи не додавайте до списку дозволених ті програми, які не розпізнаються як програми, що передають дані через брандмауер.

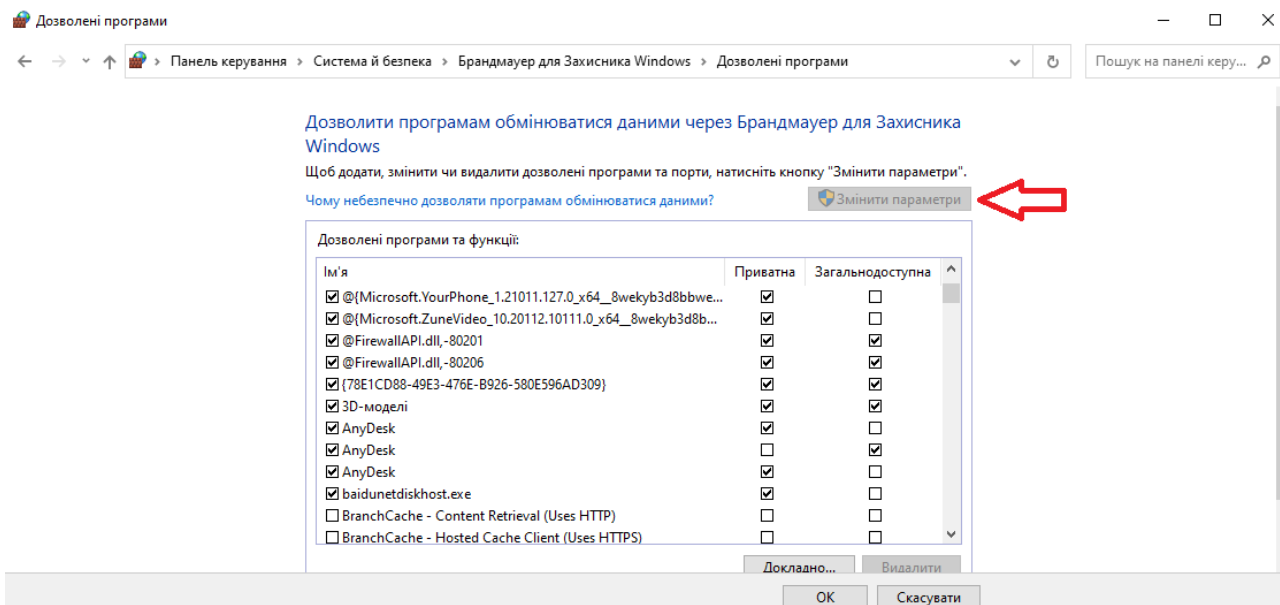
### Порядок дій:

1. **Відкрийте брандмауер:** один із способів – в рядку пошуку або в меню виконати введіть **firewall.cpl** і натисніть клавішу Enter.

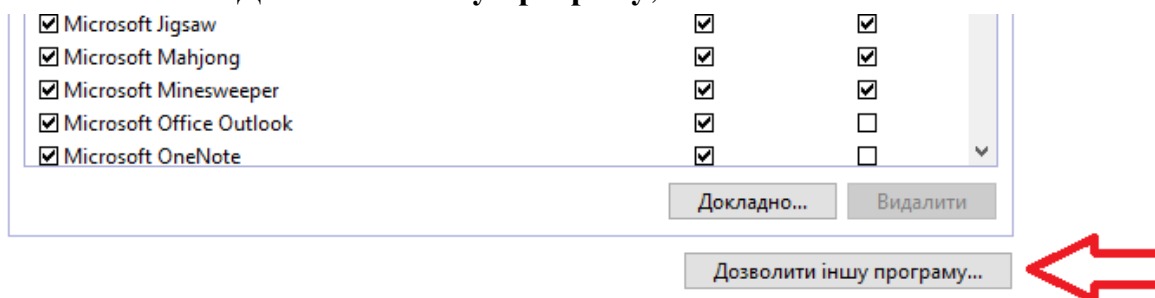
2. У лівій колонці натисніть на “Дозвіл взаємодії з додатком або компонентом в брандмауері Windows”;



3. Натисніть на “Змінити параметри”, якщо ви після завантаження Windows вже заходили в дані параметри, то кнопка буде не активна і можна просто переходити до наступного пункту;



4. Перед вами список додатків із заданими дозволами, якщо ваш додаток є в списку – поставте відмітки на потрібні поля і натисніть “ОК”, якщо його в списку немає – натисніть на **Дозволити іншу програму**;



5. Натисніть кнопку “**Огляд**”, щоб вказати шлях до потрібного додатку;
6. Через вікно, знайдіть додаток, який ви хочете дозволити, виберіть його і натисніть “**Відкрити**”;
7. Натисніть кнопку “**Типи мереж**”;
8. Поставте відмітки на мережах, в яких потрібно дозволити обмін даними з цим додатком, і натисніть “ОК”;
9. Натисніть кнопку “Додати”;
10. У цьому вікні підтвердіть дозволи для цього додатка, натиснувши на “ОК”.

Дозволені програми та функції:

Ім'я	Приватна	Загальнодоступна
<input type="checkbox"/> Secure Socket Tunneling Protocol	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Skype	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Skype	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> teams.exe	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> teams.exe	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Virtual Machine Monitoring	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Visual Studio 11 Beta Controller Listener Ports (devenv.exe)(6...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Visual Studio 11 Beta Controller Listener Ports (devenv.exe)(6...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Visual Studio 11 Beta Controller Listener Ports (devenv.exe)(6...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Visual Studio 11 Beta Controller Listener Ports (devenv.exe)(6...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Visual Studio 11 Beta Controller Listener Ports (devenv.exe)(6...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Visual Studio 11 Beta Controller Listener Ports (devenv.exe)(6...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Докладно... Видалити

Дозволити іншу програму...

ОК Скасувати

### 3. Встановлення фаєрволу в ОС Linux

У Linux є відмінна система управління мережевими пакетами на рівні ядра, яка називається iptables, яку можна налаштувати як безпосередньо з командного рядка, так і через різноманітні графічні інтерфейси адміністрування.

**Iptables** – це додаток / програма, яка дозволяє налаштовувати наданий ядром Linux міжмережевий екран, в якому користувач має можливість додавати або видаляти відповідні його вимогам правила безпеки.

Ця програма використовується для IPv4, **ip6tables** – для IPv6.

#### *Установка брандмауера*

Сьогодні міжмережевий екран вбудовується в кожне ядро Linux і у кожному відомому дистрибутиві Linux можна знайти його пребілд. У більшості лінуксових систем міжмережевий екран встановлений в папку /usr/sbin/iptables.

#### *Установка в Ubuntu або Debian:*

```
sudo apt-get install iptables
```

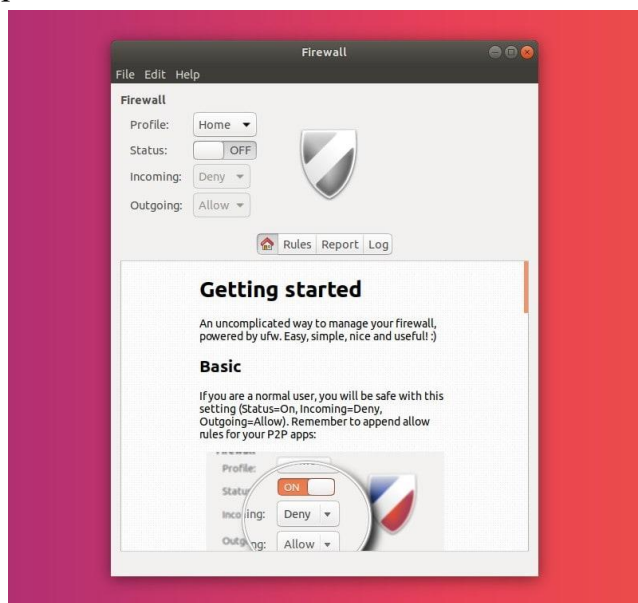
**Gufw** є графічною оболонкою до програми UFW (з англ. "Uncomplicated Firewall" – нескладний міжмережевий екран).

Для того щоб встановити Gufw, ви повинні підключити стандартний репозиторій. Для установки Gufw можна використовувати менеджер пакетів Synaptic або виконати в терміналі команду:

```
sudo apt-get install gufw
```

#### *Використання брандмауера*

Щоб отримати доступ до GUFW, перейдіть в Система→ Адміністрування→ Конфігурація брандмауера.



За замовчуванням брандмауер відключений.

Щоб увімкнути брандмауер, просто відзначте параметр "Увімкнути" після цього за замовчуванням будь-який доступ до комп'ютера буде заборонений.



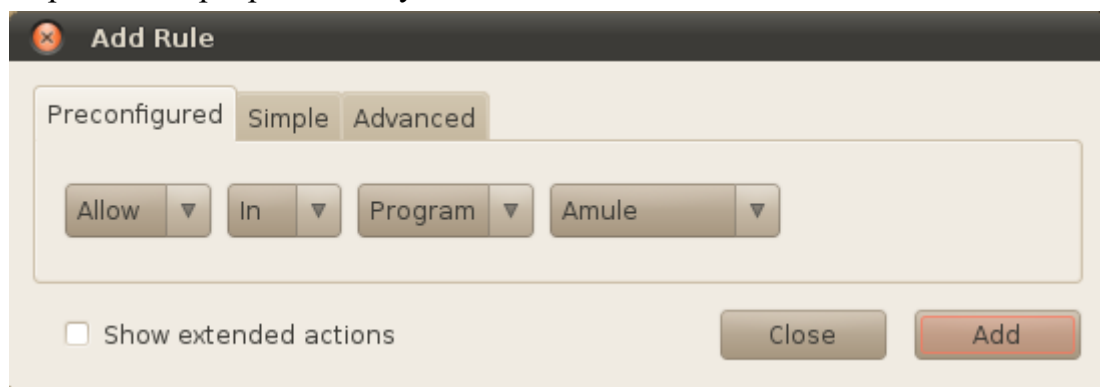
### *Додавання правил*

Щоб налаштувати брандмауер, ми додаємо свої правила. Просто натисніть кнопку Додати і з'явиться нове вікно. Детальніше про цю реалізацію, див. сторінку <https://help.ubuntu.com/community/UFW>. Правила можуть бути налаштовані для TCP і UDP портів, крім того, UFW має кілька попередньо налаштованих шаблонів для програм або послуг, щоб користувачеві було легше створити правила для цих програм або послуг.

Є такі варіанти правил "Дозволити", "Заборонити", "Відхилити", і "Обмежити":

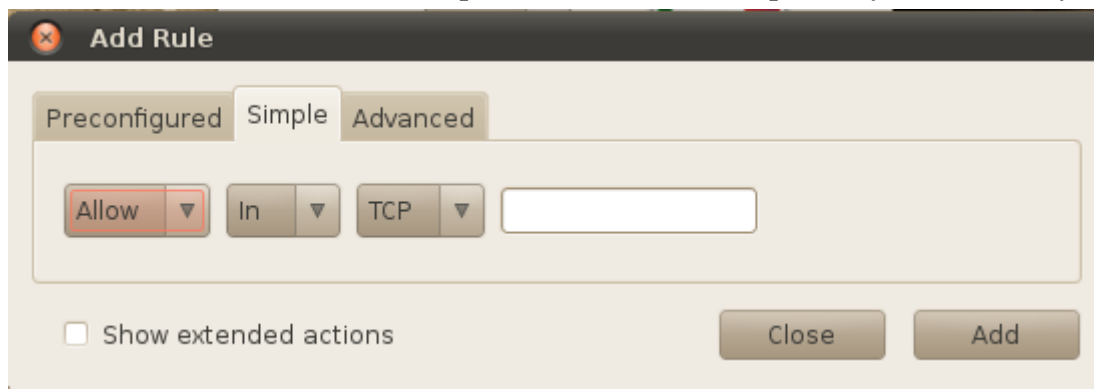
- Дозволити: система дозволить вхідний трафік через порт.
- Заборонити: система заборонить вхідний трафік на порт.
- Відхилити: система заборонить вхідний трафік на порт і повідомить запитувачу про відхилення запиту.
- Обмеження: система буде відхиляти з'єднання, якщо IP-адреса спробує ініціювати 6 або більше з'єднань за останні 30 секунд.

Шаблони створення правил дають можливість керування трафіком для найпоширеніших програм і послуг.



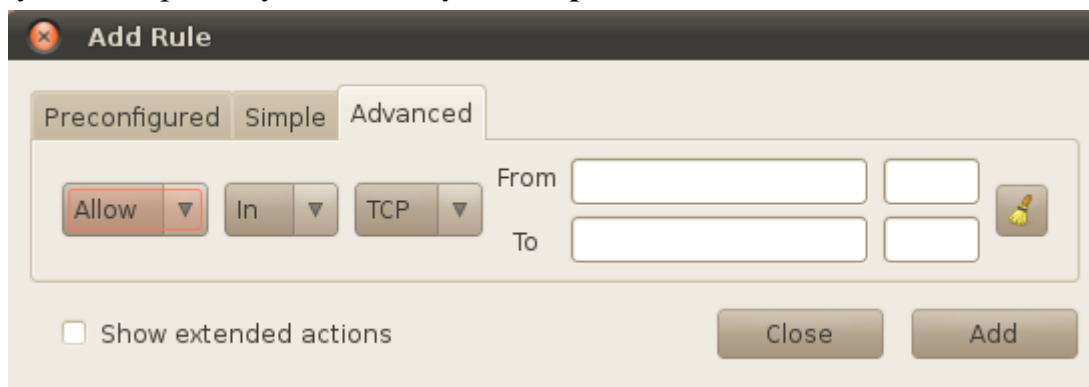
Прикладом є, представлена на сторінці <https://help.ubuntu.com/community/UFW>, інструкція, яка демонструє, як дозволити або заборонити доступ до комп'ютера по протоколу SSH, що використовує порт 22. Якщо ви виберете у спадному списку пункти "Дозволити", "Сервіс", "SSH", то брандмауер буде налаштований на прийняття трафіку по протоколу SSH.

Не всі програми доступні для конфігурації за допомогою готових шаблонів в Gufw, але ми все ж можемо додати правила для них, використовуючи вкладку **Прості**.



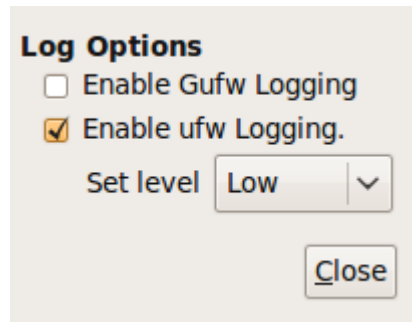
Знову ж таки, ми будемо використовувати в якості прикладу SSH – просто уявимо що для нього немає попередньо створеного шаблону. Щоб включити його у вкладці Прості, виберіть "Дозволити", "TCP", "22" і натисніть кнопку Додати.

Іноді ми хочемо налаштувати доступ на основі певних IP-адрес або діапазонів IP, тому ми використовуємо вкладку **Розширені**.



Наприклад, ми хочемо забезпечити доступ користувачів до локальної мережі, використовуючи діапазон IP-адрес 192.168.1.100 - 192.168.1.150. Вам потрібно буде вибрати варіанти "Дозволити", "TCP", 3: "192.168.1.100" / "22", ПО: "192.168.1.150" / "22".

Є два можливі налаштування в графічному модулі Gufw для ведення журналу, для цього треба зайти в Edit→ Preferences



Тут ви можете контролювати ведення журналу для UFW і Gufw. За замовчуванням, включити ведення журналу для UFW, і відключити ведення журналу для Gufw.



## Завдання до лабораторної роботи

### Завдання А. Використання правил брандмауера Windows.

#### **A1. Відкриття портів в брандмауері Windows.**

1. Відкрийте вікно управління брандмауером.
2. Створіть нове дозвоільне правило.
3. У звіті опишіть порядок виконання завдання.

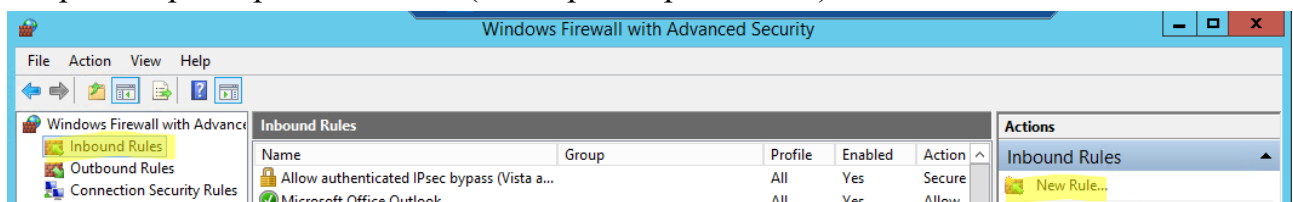
Таке завдання може виникнути якщо ви встановили якийсь, можливо не стандартний, сервіс на своєму комп'ютері і потрібно надати до нього доступ з мережі. Дуже часто потрібно відкрити порти до баз даних SQL Server (порти 1433 і 1434).

**Крок 1.** Відкрийте брандмауер: один зі способів – в рядку пошуку або в меню "Виконати" (виконати викликається клавішами Win + R) напишіть **firewall.cpl** та натисніть клавішу Enter.

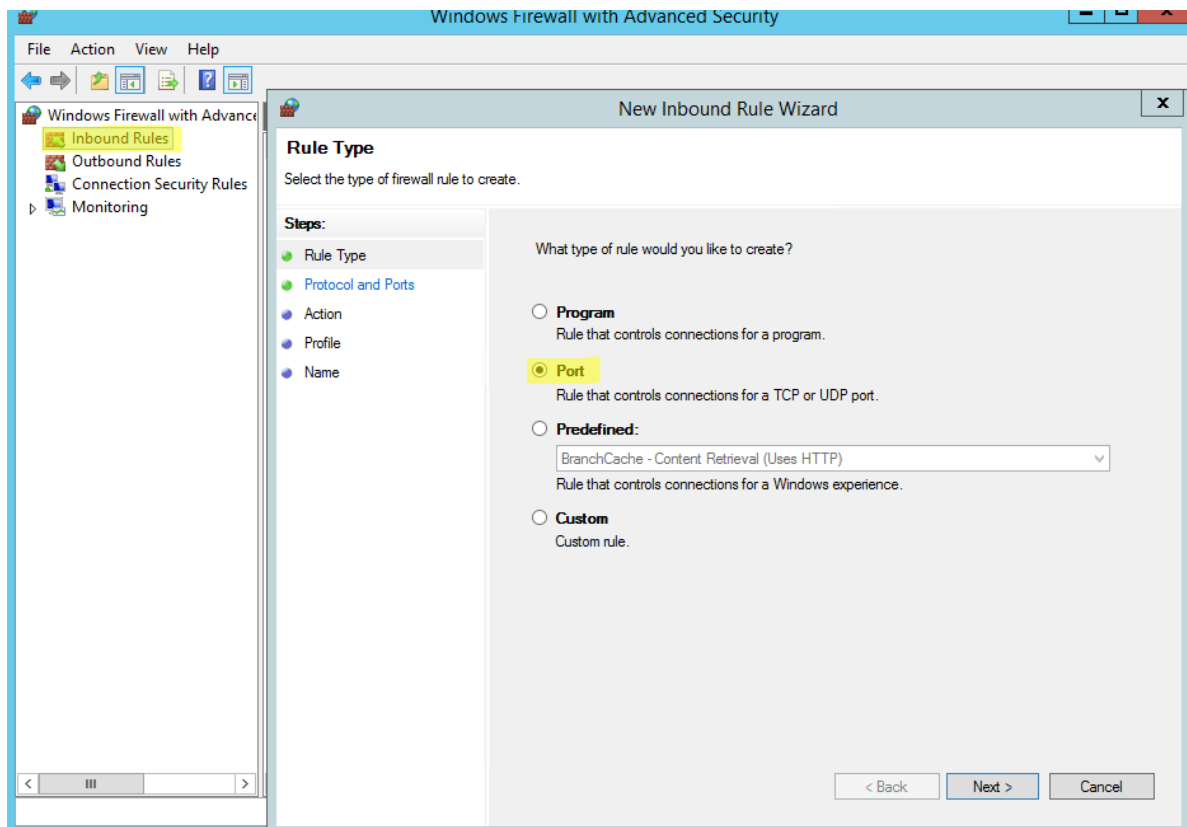
**Крок 2.** З лівого боку натисніть на "Додаткові параметри".

**Крок 3.** Ви відкриваєте порт для вхідних чи вихідних підключень? Вихідними називаються підключення, що ініціюються локальним комп'ютером, вхідні - ініціюються віддаленим комп'ютером. Якщо вам потрібно відкрити порт для вихідних підключень – з лівого боку виберіть "Outbound Rules" та продовжуйте робити написане далі. Якщо вам потрібно відкрити порт для вхідних підключень – з лівого боку виберіть "Inbound Rules".

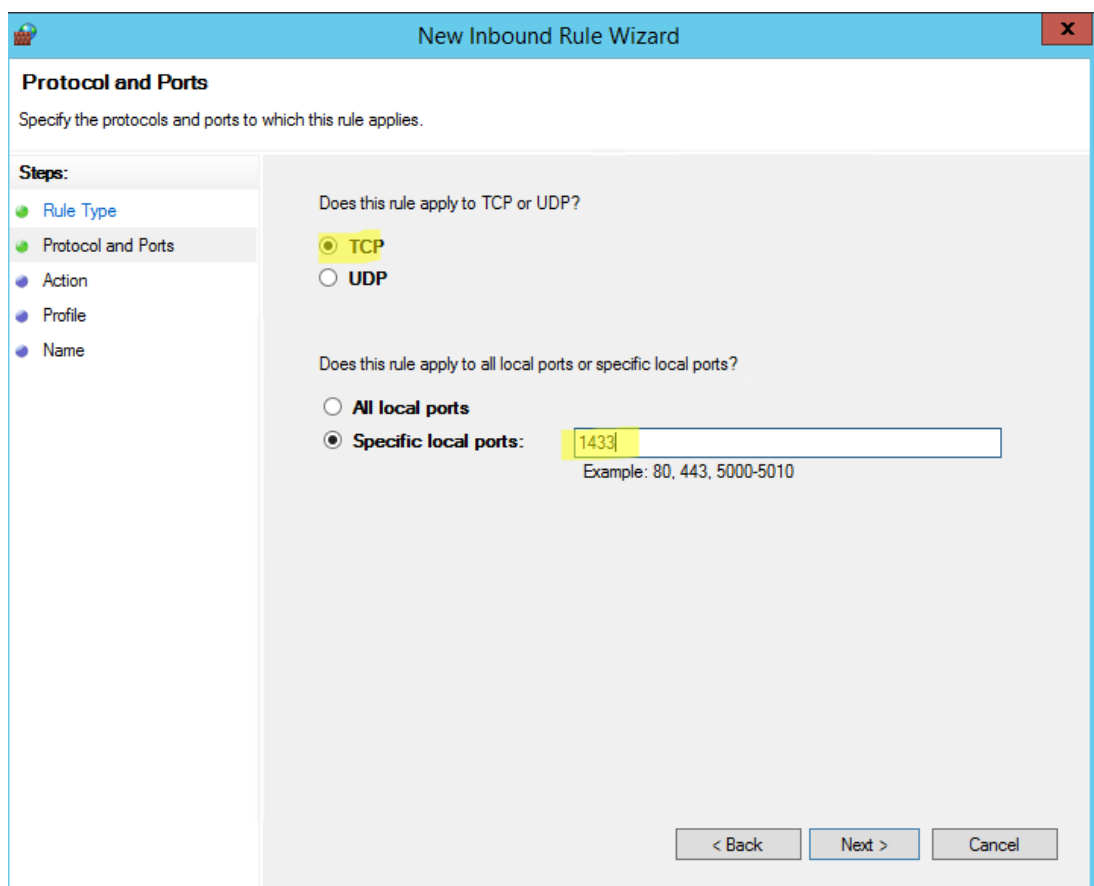
У нашому завданні необхідно натиснути правою кнопкою миші по гілці **Inbound Rules** («Правила для вхідних підключень»). У контекстному меню потрібно вибрати параметр **New Rule ...** («Створити правило ...»).



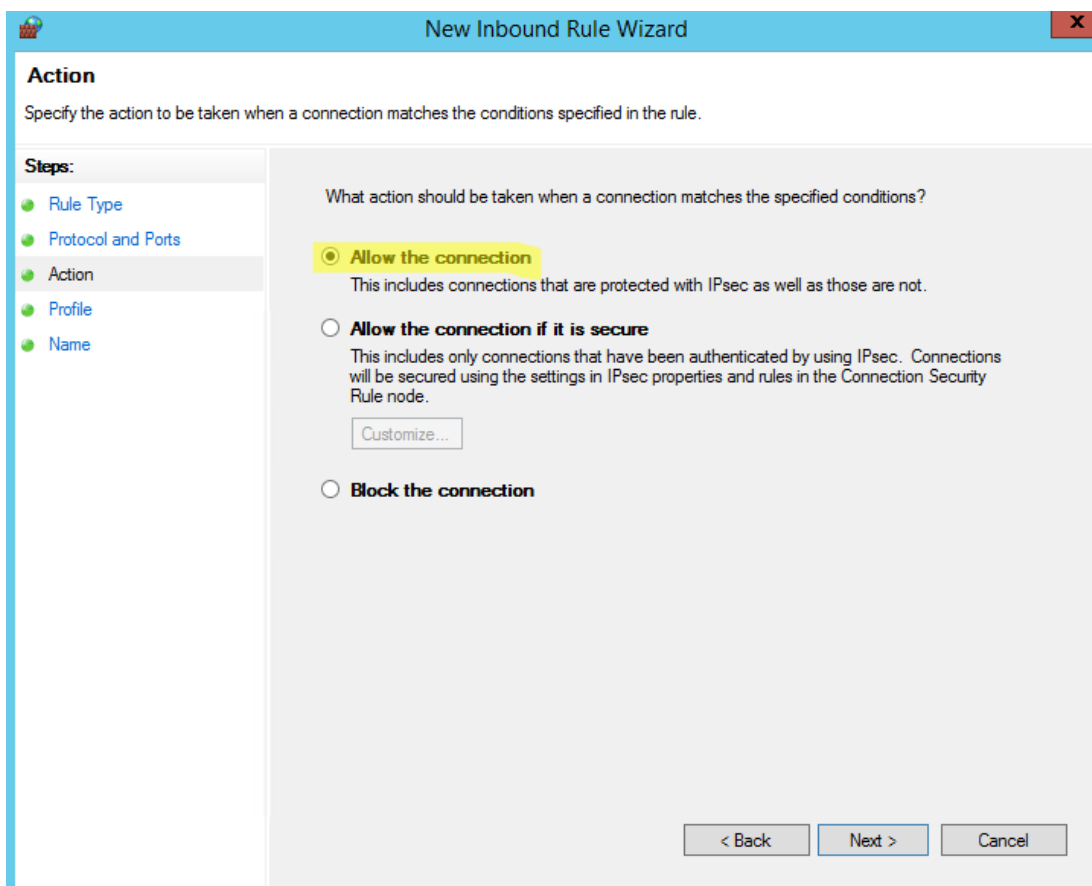
**Крок 4.** Поставте крапку напроти "Port" та натисніть на "Next".



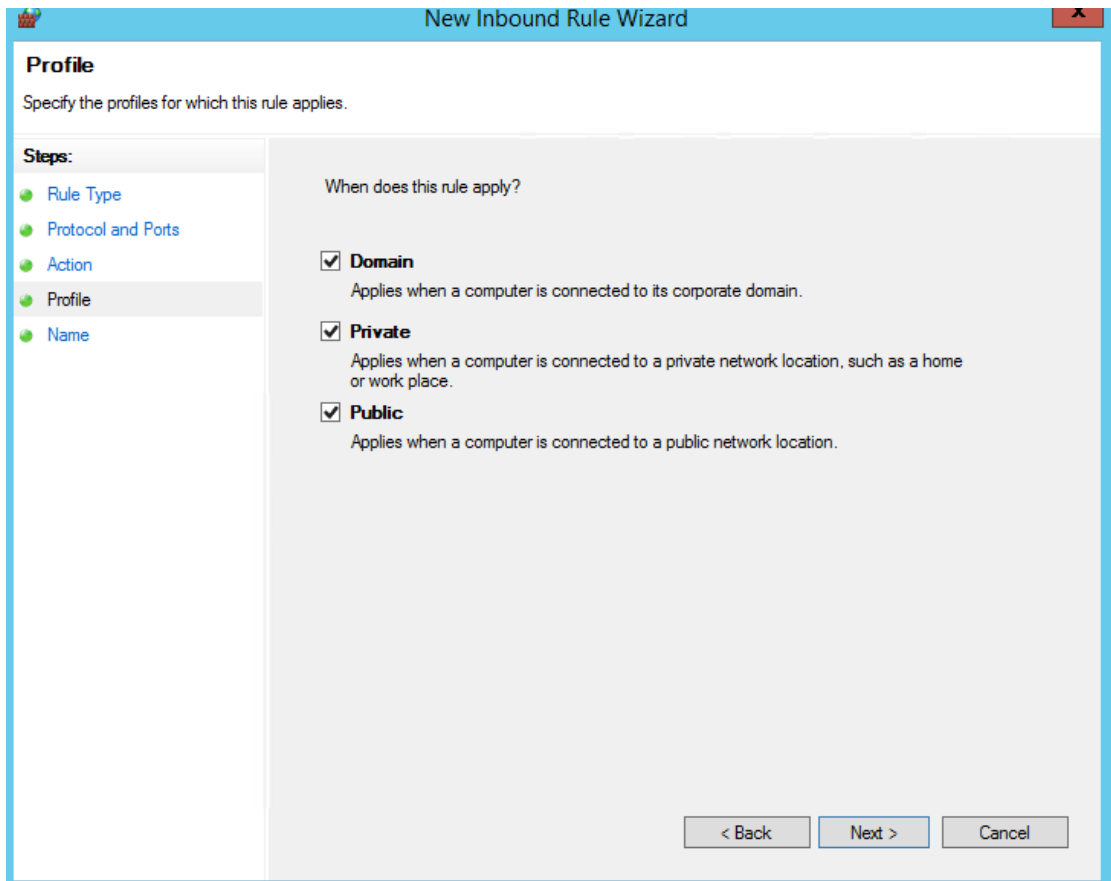
**Крок 5.** Біля "Specific local ports" введіть порт, який ви хочете відкрити та натисніть "Next".



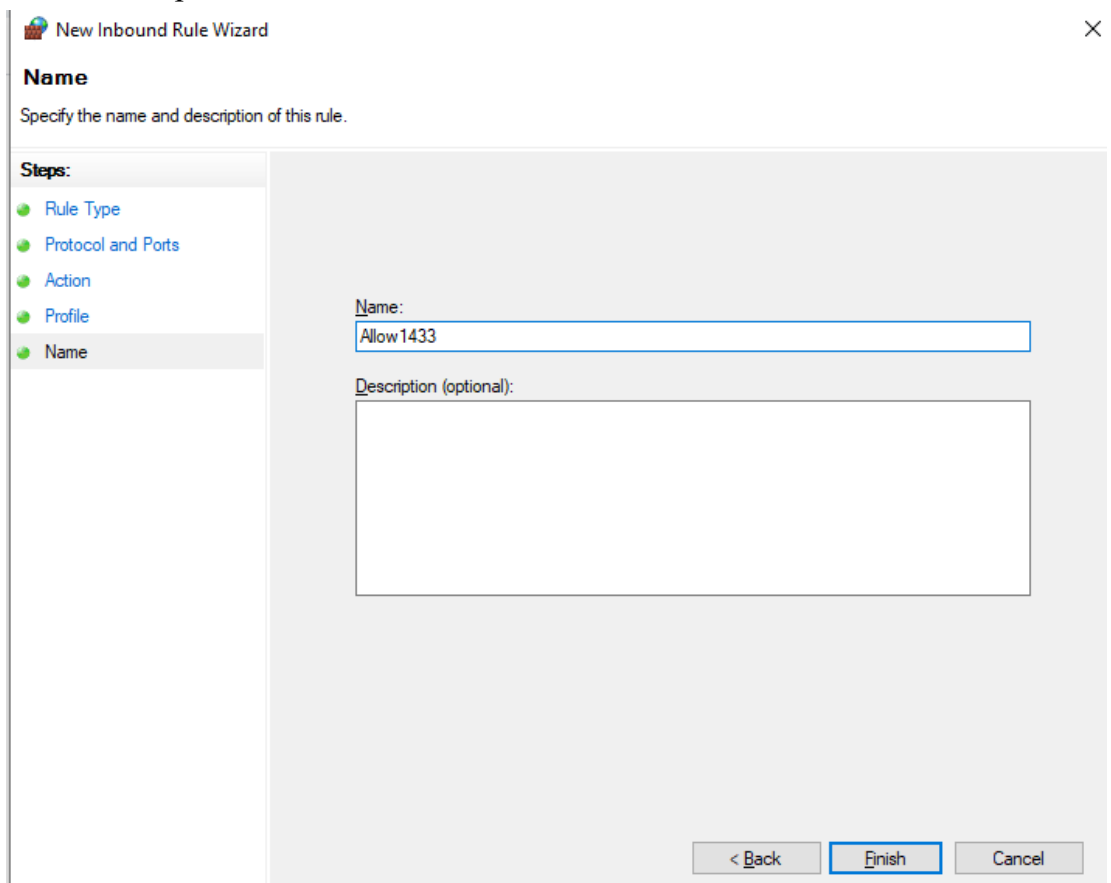
**Крок 6.** Поставте крапку біля "Allow the connection" та натисніть "Next". Якщо ви хочете більше налаштувань для даного порту – поставте крапку біля "Allow the connection if it is secure".



**Крок 7.** Виберіть для яких профілів мережі застосовувати правило та натисніть "Next".

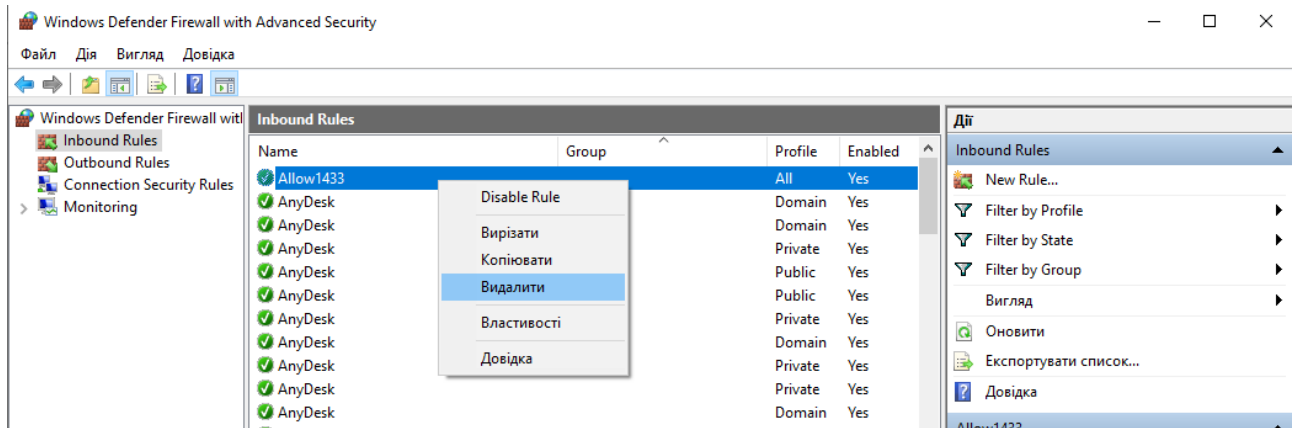


**Крок 8.** Придумайте та напишіть ім'я для створеного вами правила, щоб в майбутньому легше було його знайти, також ви можете додати опис, що не є обов'язковим. По завершенню натисніть **"Finish"** та закрийте брандмауер, правило створено та вже працює.



Після цього, ви побачите це правило буде створено та увімкнено за замовчуванням. Всі клієнтські програми можуть тепер підключатися до MS SQL Server по заданому порту.

Після виконання завдання A1 можна видалити створене правило.



## ***A2. Створення правила, яке забороняє відсилання істр-пакетів на заданий вузол.***

1. Знайдіть правило, яке дозволяє відсилання ICMP-пакетів echo request. Перевірте його роботу для якого-небудь вузла з локальної або зовнішньої мережі, використовуючи його ip-адресу (наприклад, командою ping 192.168.0.10 можна перевірити доступність комп'ютера з вказаними адресою). Якщо відповідь прийшла, можна переходити до другої частини завдання. Якщо відповіді немає, спробуйте знайти такий вузол, який надішле відповідь.
2. Вибравши кнопку **New Rule** створіть правило, яке забороняє відсилання істр-пакетів на даний вузол. Перевірте його роботу.
3. У звіті опишіть порядок виконання завдання.

ICMP (Internet Control Message Protocol) – це протокол, який мережеві пристрої (наприклад, маршрутизатори) використовують для генерування повідомлень про помилки, коли мережеві проблеми не дозволяють проникати IP-пакетам.

Хоча ви, можливо, не чули про ICMP, напевно, ви чули про одну з його особливостей: Ping. Ping – утиліта для перевірки з'єднань в мережах на основі TCP/IP, а також повсякденне найменування самого запиту. Утиліта відправляє запити (ICMP Echo-Request) протоколу ICMP зазначеному вузлу мережі й фіксує відповіді, що надходять (ICMP Echo-Reply). Час між відправленням запиту й одержанням відповіді (RTT, від англ. Round Trip Time) дозволяє визначати двосторонні затримки (RTT) за маршрутом і частоту втрати пакетів, тобто побічно визначати завантаженість на каналах передачі даних і проміжних пристроях.

У розмовній мові пінгом називають також час, витрачений на передачу пакету інформації в комп'ютерних мережах від клієнта до сервера і назад від сервера до клієнта.

Повна відсутність ICMP-відповідей може також означати, що віддалений вузол (або який-небудь з проміжних маршрутизаторів) блокує ICMP Echo-Reply або ігнорує ICMP Echo-Request.

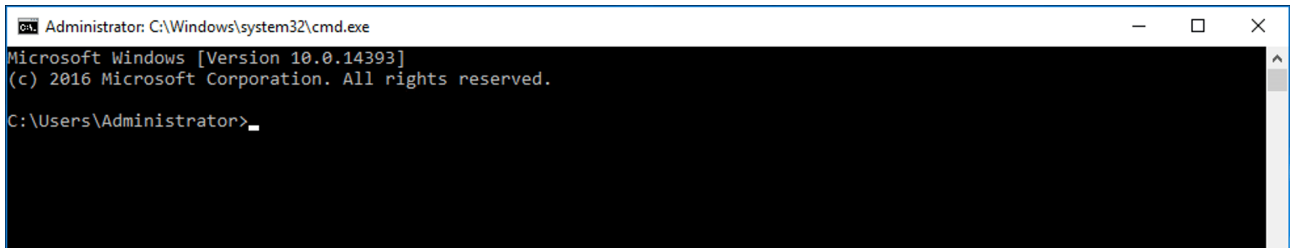
- Програма ping є одним з основних діагностичних засобів у мережах TCP/IP і входить у поставку всіх сучасних мережевих операційних систем.
- Практичне використання:
  - Можна дізнатися IP-адресу по доменному імені.
  - Можна дізнатися, чи працює сервер. Наприклад, системний адміністратор може дізнатися, чи лише завис веб-сервер або на сервері глобальні проблеми.
  - Можна дізнатися, чи є зв'язок з сервером. Наприклад, проблеми з налаштуванням DNS серверів на машині можна дізнатися, задавши в ping спочатку доменне ім'я, а потім IP-адресу.
  - Також можна дізнатися якість каналу, подивившись, скільки відповідей не прийшло. Це часто використовується гравцями в мережеві ігри, тому що якість зв'язку для них дуже важливо.

### **Крок 1. Перевірка пінгу.**

Для перевірки пінгу використовується однойменна команда `ping`, яку необхідно вводити в командному рядку. Запустити командний рядок можна у такий спосіб:

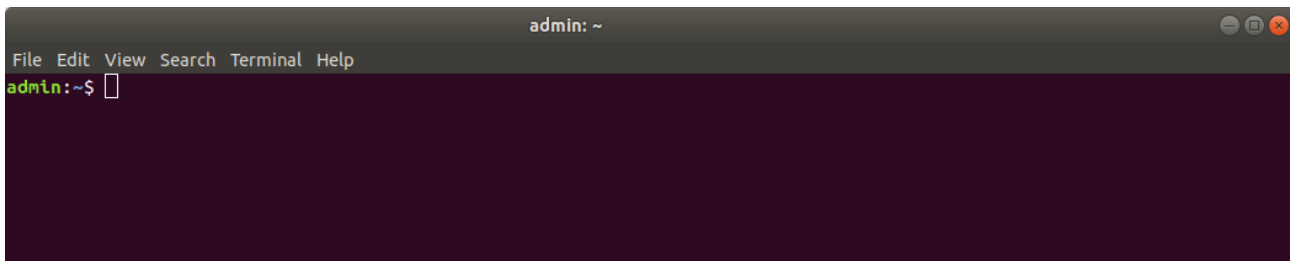
*Windows:*

- 1) Пуск -> Всі програми -> Стандартні -> Командний рядок
- 2) Пуск -> Виконати -> `cmd`

A screenshot of a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The window shows the Microsoft Windows version 10.0.14393 and the copyright notice for 2016. The current directory is C:\Users\Administrator>.

*Linux:*

У цій ОС є безліч терміналів. Для нашої мети підійде будь-який з встановлених на ПК. Зазвичай стандартний термінал можна запустити поєднанням клавіш CTRL+ALT+T.

A screenshot of a Linux terminal window titled "admin: ~". The window shows a menu bar with File, Edit, View, Search, Terminal, and Help. The prompt is admin:~\$.

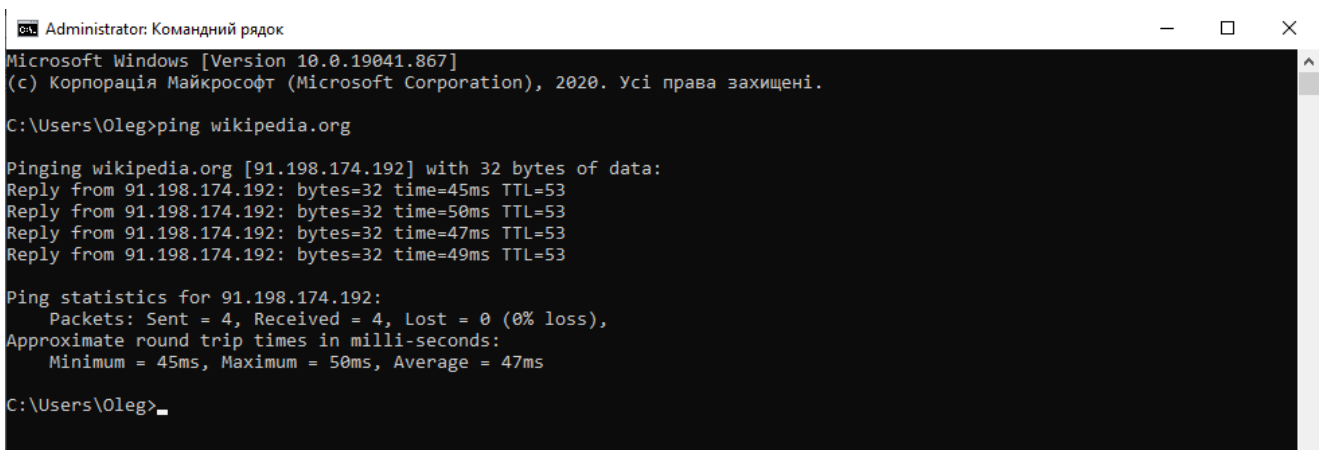
Отже, щоб пропінгувати певний сервер, необхідно виконати команду:

`ping <IP або домен>`

Наприклад, для пінга адреси 11.222.33.44 необхідно виконати команду:

`ping 11.222.33.44`

Пропінгуємо домен `wikipedia.org`, одночасно дізнаємось його ір-адресу 91.198.174.192

A screenshot of a Windows Command Prompt window titled "Administrator: Командний рядок". The window shows the Microsoft Windows version 10.0.19041.867 and the copyright notice for 2020. The user has entered the command `C:\Users\Oleg>ping wikipedia.org`. The output shows four successful replies from 91.198.174.192 with times ranging from 45ms to 50ms and TTL=53. The ping statistics show 4 packets sent, 4 received, and 0% loss, with an average round trip time of 47ms.

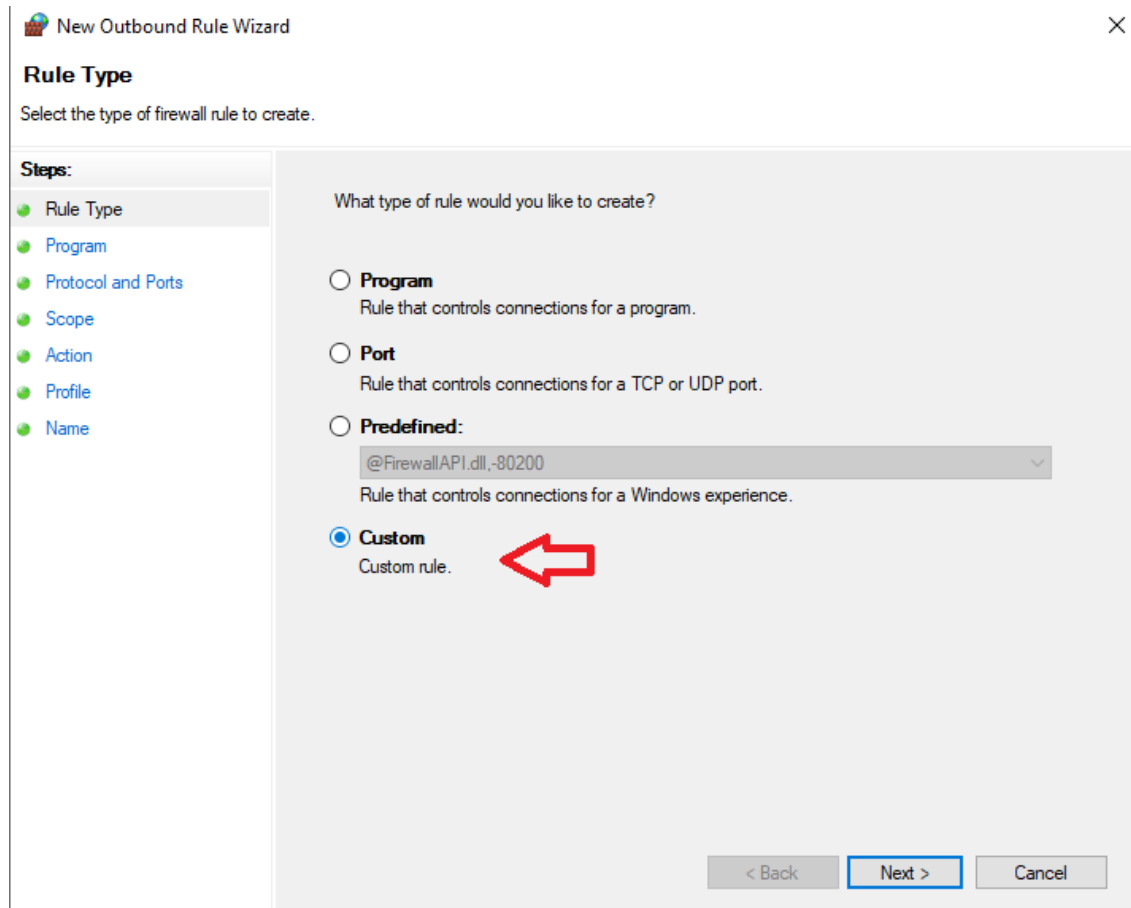


**Крок 2.** Створимо правило, яке забороняє відсилання істр-пакетів на даний вузол.

Відкрийте брандмауер. У нашому завданні необхідно натиснути правою кнопкою миші по гілці **Outbound Rules** («Правила для вихідних підключень»). У контекстному меню потрібно вибрати параметр **New Rule ...** («Створити правило ...»).

### Крок 3.

На сторінці "Тип правила" виберіть опцію "**Налаштовувані**". Натисніть "Далі"

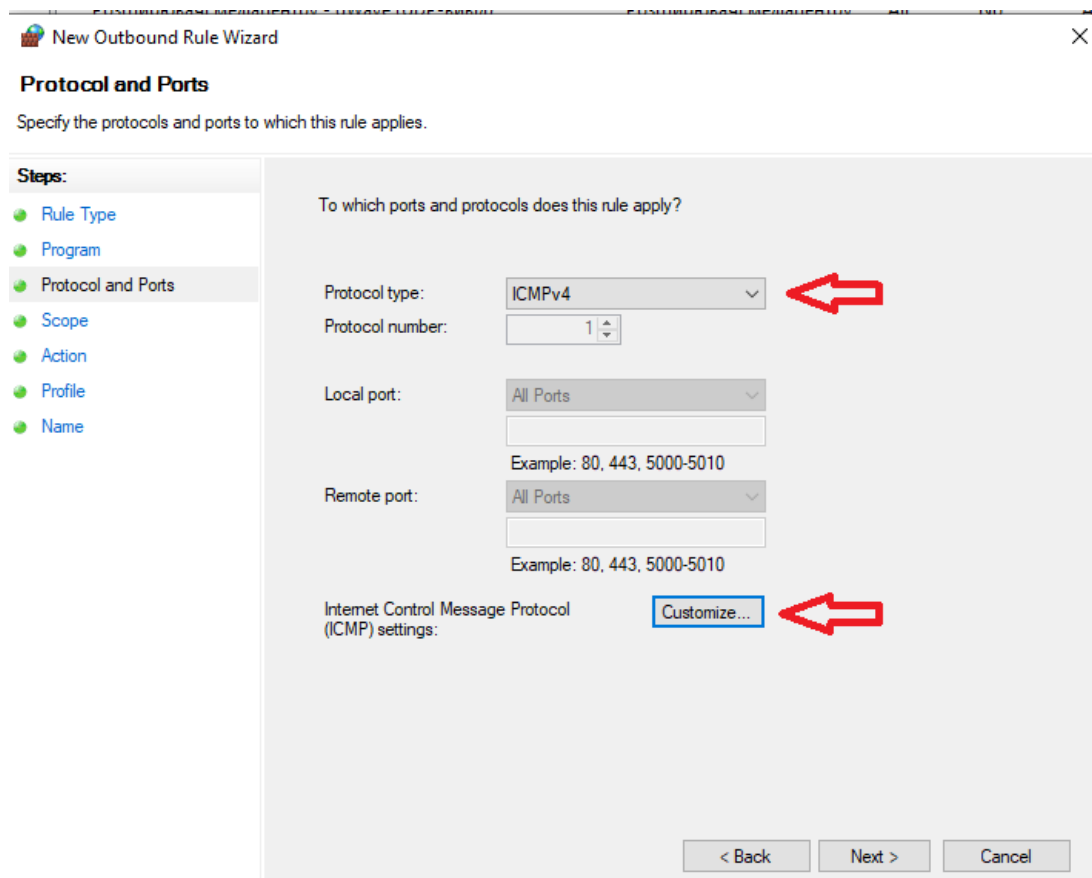


### Крок 4.

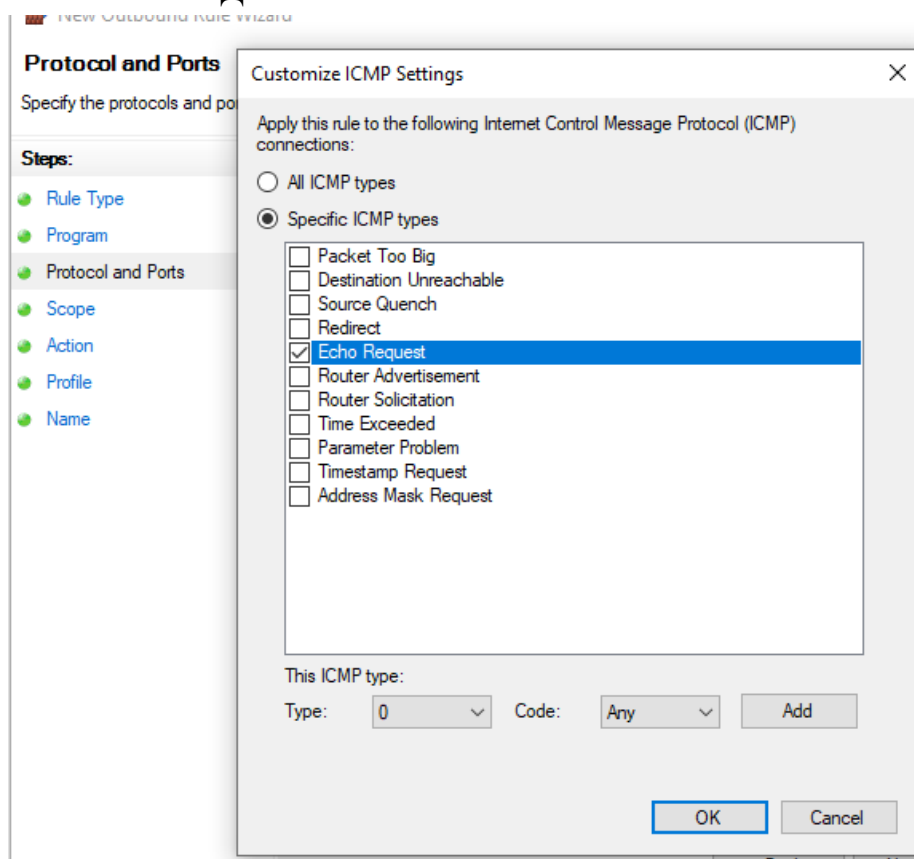
На сторінці "Програма" виберіть опцію "Всі програми" і натисніть "Далі".

### Крок 5.

На сторінці "Протокол і порти" натисніть по стрілці вниз у списку "Тип протоколу" і виберіть опцію "ICMPv4".



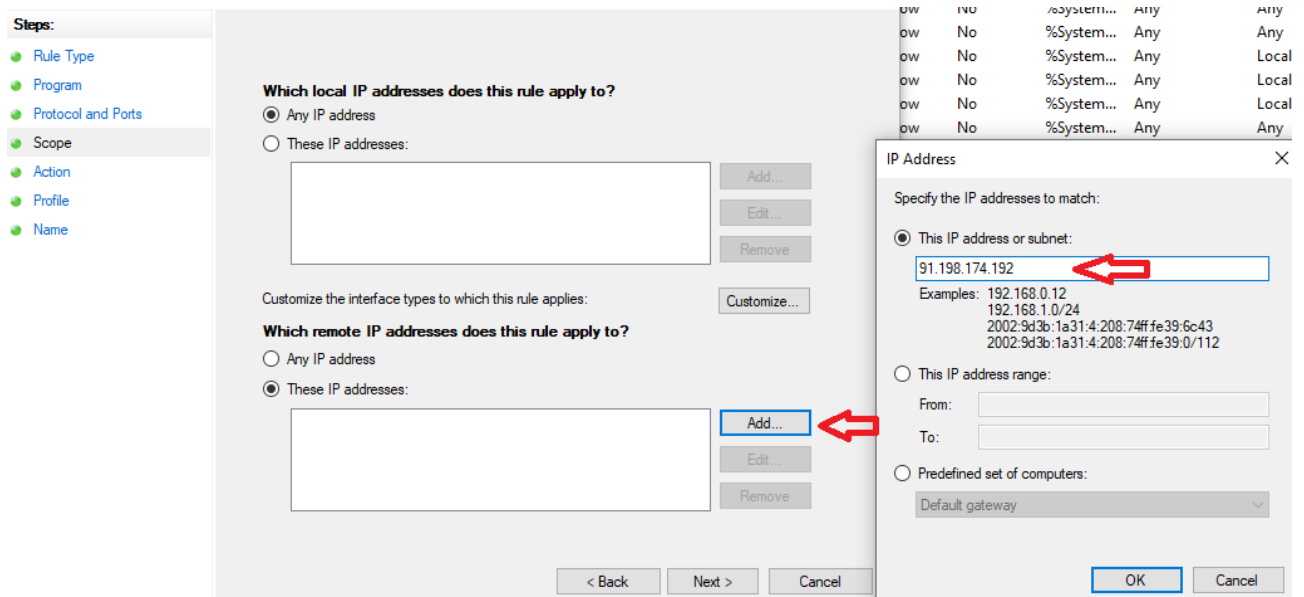
Потім натисніть кнопку "Налаштувати". У діалоговому вікні "Параметри налаштування ICMP" виберіть опцію "Певні типи ICMP". Потім поставте прапорець в рядку "Ехо запит". Натисніть Далі.



**Крок 6.**

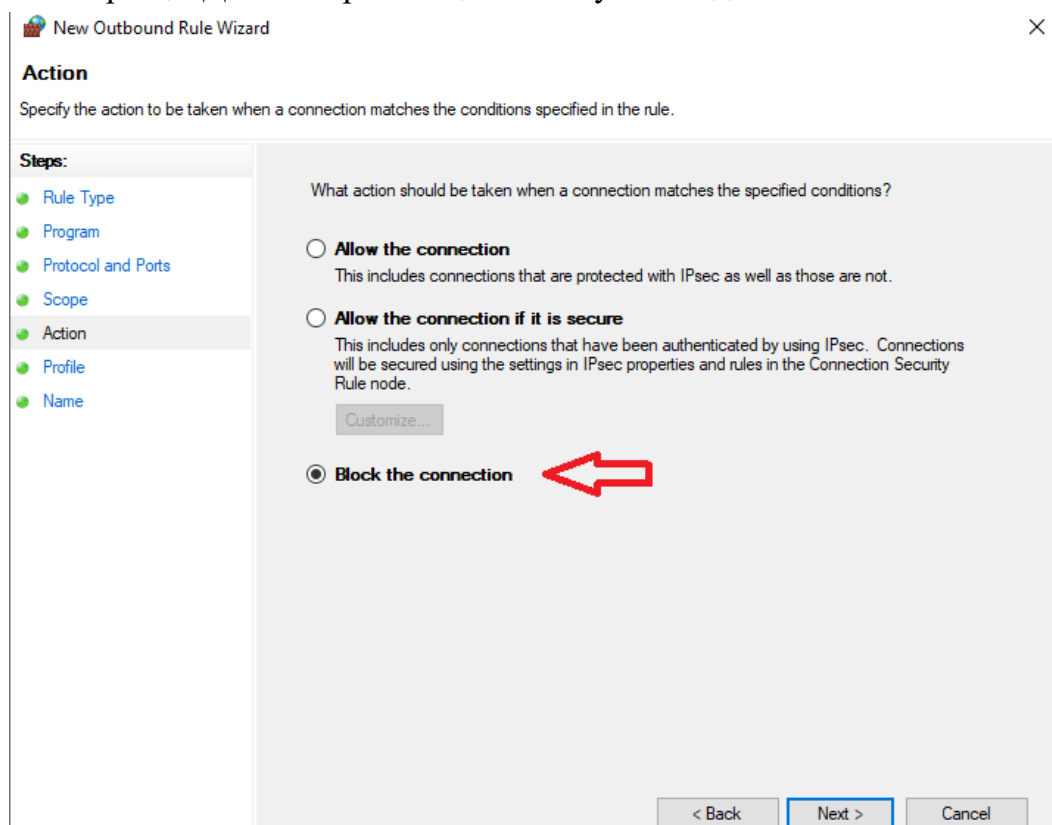
Натисніть Далі на сторінці Протокол і порти.

У діалоговому вікні "Область" для віддалених IP адрес, введіть адресу **91.198.174.192**. Натисніть "Далі".



## Крок 7.

На сторінці "Дія" виберіть опцію "Блокувати підключення" і натисніть "Далі".



**Крок 8.** На сторінці "Профіль" натисніть "Далі".

**Крок 9.** На сторінці "Ім'я" вкажіть назву правила. У цьому прикладі ми назвали правило "Блокувати пінг". Натисніть "Готово".

New Outbound Rule Wizard

**Name**

Specify the name and description of this rule.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name**

Name:  
BlockPing

Description (optional):

< Back Finish Cancel

Якщо ви зробили все правильно, то ви повинні побачити **"BlockPing"** в списку правил.

### Крок 10. Перевіряємо, чи працює створене блокування.

```
Administrator: Командний рядок
Microsoft Windows [Version 10.0.19041.867]
(c) Корпорація Майкрософт (Microsoft Corporation), 2020. Усі права захищені.

C:\Users\Oleg>ping wikipedia.org

Pinging wikipedia.org [91.198.174.192] with 32 bytes of data:
General failure.
General failure.
General failure.
General failure.

Ping statistics for 91.198.174.192:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Oleg>
```

### А3. Налаштування журналу в брандмауері Windows.

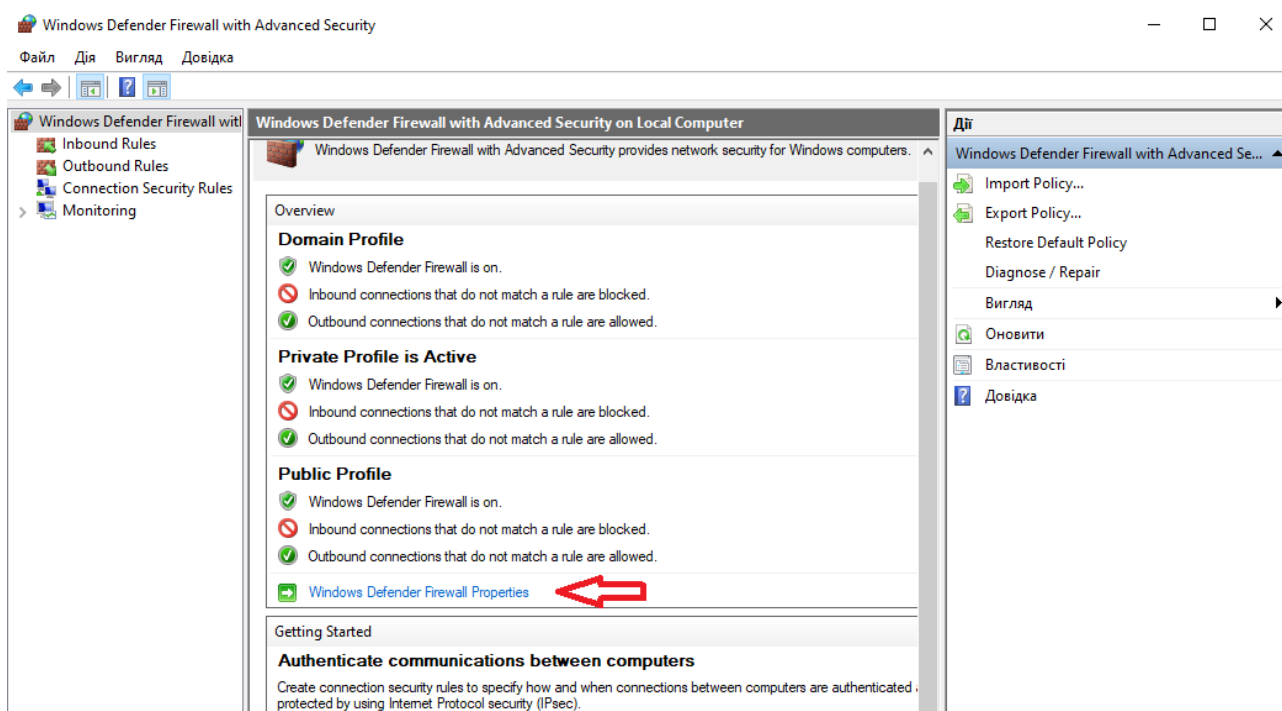
1. Активуйте ведення журналу.
2. Виконайте команду `ping` для вузла, для якого створювалося блокуюче правило.
3. Перевірте вміст файлу журналу.
4. У звіті опишіть порядок виконання завдання.

У процесі фільтрації Інтернет-трафіку всі брандмауери мають певний тип реєстрації, який документує, як брандмауер обробляв різні типи трафіку. Ці журнали можуть надавати цінну інформацію, таку як IP-адреси джерела та призначення, номери портів та протоколи. Ви також можете використовувати файл журналу брандмауера Windows для моніторингу з'єднань TCP та UDP та пакетів, які заблоковані брандмауером.

За замовчуванням журнал відключено. Але якщо виникає підозра, що міжмережевий екран заважає встановленню якогось типу мережевих з'єднань, можна включити цю опцію і проаналізувати журнал.

#### Крок 1.

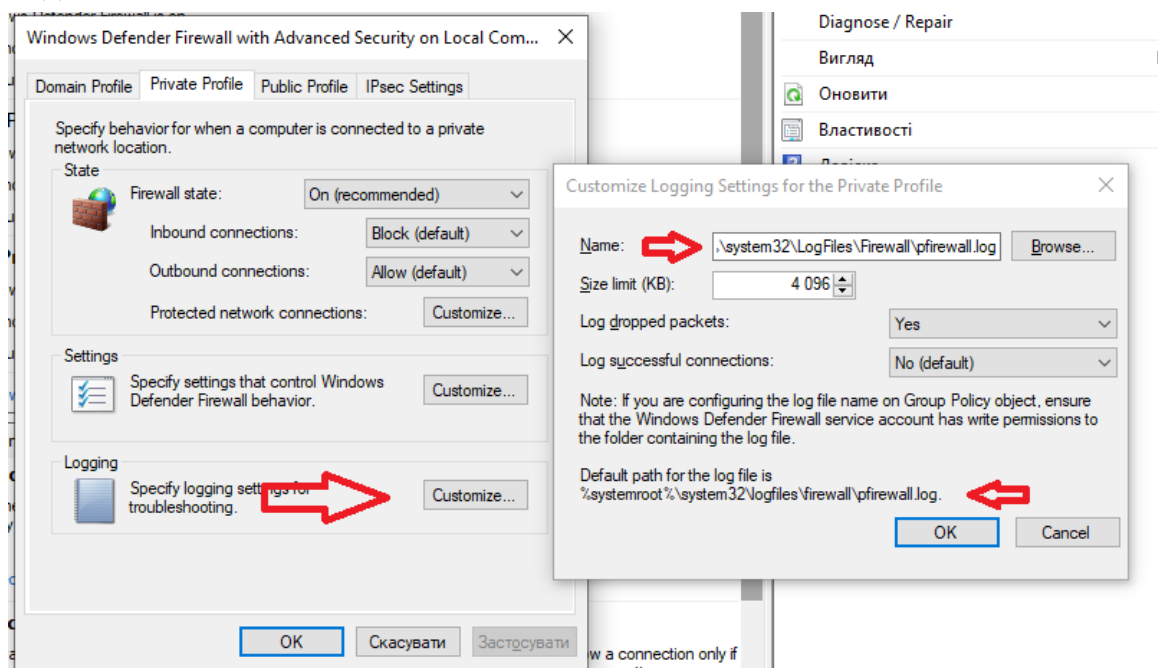
У головному вікні Windows Defender із розширеною безпекою вибираємо пункт Firewall Properties і активуємо ведення журналу відкинутих пакетів.



Для цього в групі Logging у вікні треба натиснути кнопку Customize і провести налаштування розміщення файлу журналу та його розміру.

Вказуємо ім'я і розташування файлу журналу і задаємо його максимальний розмір. Вибираємо, що саме буде записуватись – Log dropped packets (тільки

відкинуті пакети) або Log successfully connections (вдалі підключення), тиснемо OK і йдемо дивитися логи.



**Крок 2.** Відкрити файл журналу у відповідній папці і переписати його вміст (те що стосується блокування надсилання пакетів на домен сайту wikipedia.org) у звіт до лабораторної роботи.

#### **A4. Блокування доступу до певного веб-сайту з локальної мережі.**

1. Заблокуйте доступ до певного веб-сайту з локальної мережі.

Скористайтесь списком сайтів <https://www.stopfake.online/p/blog-page.html>

2. Перевірте, чи блокування працює.

3. У звіті опишіть порядок виконання завдання.

**Крок 1.** Спочатку визначимо IP-адресу потрібного нам веб-сайту.

В налаштуваннях правил не можна використовувати доменні імена, а можна вказати тільки IP-адреси. Один сайт може мати кілька різних IP-адрес (зазвичай це стосується великих ресурсів, таких як google.com та ін).

Один зі способів дізнатися IP-адресу сайту – використати команду

```
nslookup <ім'я веб-сайту>
```

Наприклад, в командному рядку операційної системи виконаємо команду:

```
nslookup bbc-ccnn.com
```

```
C:\Users\Oleg>nslookup bbc-ccnn.com
Server: my.router
Address: 192.168.1.1

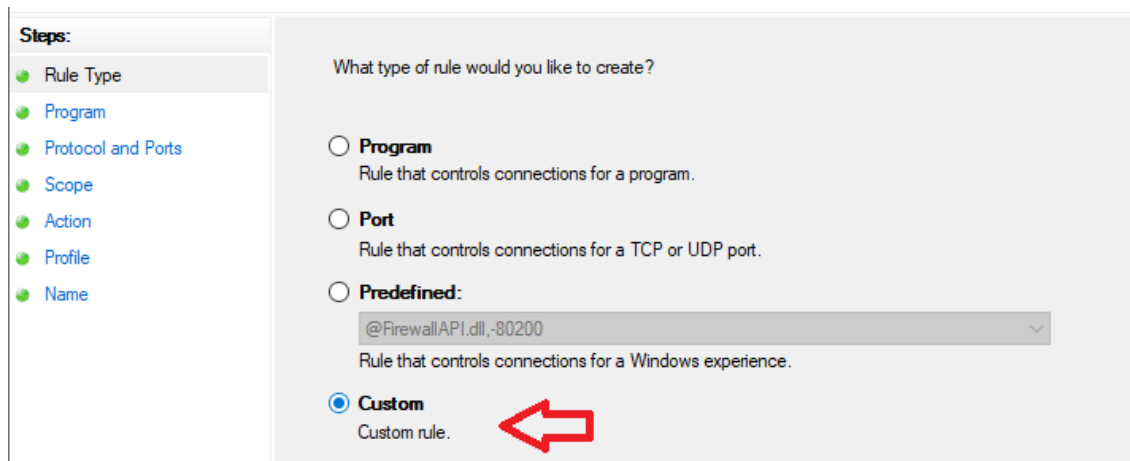
Non-authoritative answer:
Name:    bbc-ccnn.com
Addresses: 104.21.67.153
          172.67.177.135
```

Результат виконання зазначеної вище команди дозволить побачити IP-адреси, на яких розміщується веб-сайт (в нашому прикладі сайт використовує дві IP-адреси: 104.21.67.153 та 172.67.177.135).

**Крок 2.** Створюємо блокуючі правила, в якому вказуємо IP-адреси сайту призначення.

Відкрийте брандмауер. У нашому завданні необхідно натиснути правою кнопкою миші по гілці **Outbound Rules** («Правила для вихідних підключень»). У контекстному меню потрібно вибрати параметр **New Rule ...** («Створити правило ...»).

**Крок 3.** На сторінці "Тип правила" виберіть опцію "**Налаштовувані**".





#### Крок 4.

На сторінці "Програма" виберіть опцію "Всі програми" і натисніть "Далі".

#### Крок 5.

На сторінці "Протокол і порти" натисніть по стрілці вниз у списку "Тип протоколу" і виберіть опцію "Усі".

#### Крок 6.

У діалоговому вікні "Область" для віддалених IP адрес, введіть адресу **вибраного сайту**. Натисніть "Далі".

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope**
- Action
- Profile
- Name

**Which local IP addresses does this rule apply to?**

☒ Any IP address

☐ These IP addresses:

Add... Edit... Remove

Customize the interface types to which this rule applies: Customize...

**Which remote IP addresses does this rule apply to?**

☐ Any IP address

☒ These IP addresses:

104.21.67.153  
172.67.177.135

Add... Edit... Remove

< Back Next > Cancel

#### Крок 7.

На сторінці "Дія" виберіть опцію "Блокувати підключення" і натисніть "Далі".

**Action**

Specify the action to be taken when a connection matches the conditions specified in the rule.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action**
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

☐ **Allow the connection**  
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**  
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

Customize...

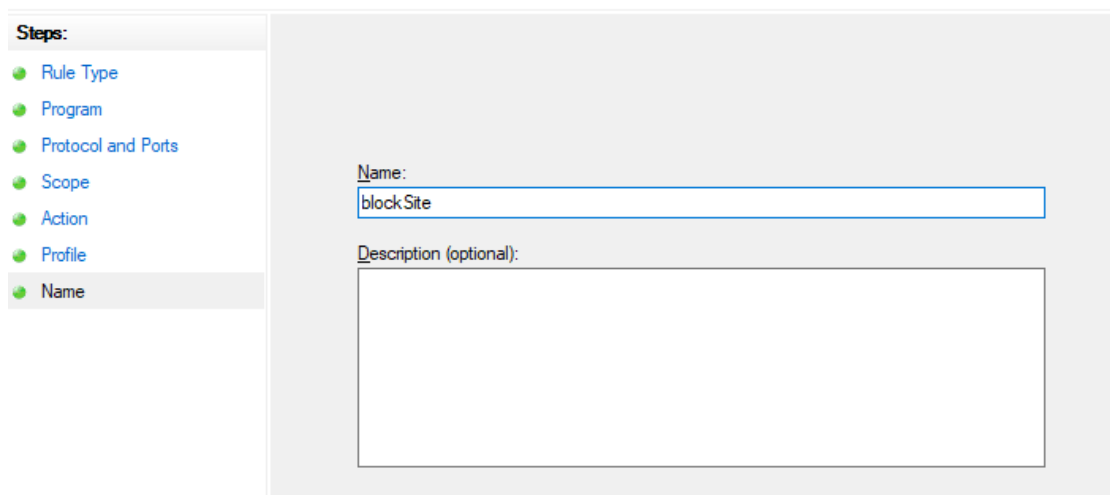
☒ **Block the connection**

**Крок 8.** На сторінці "Профіль" натисніть "Далі".

Необхідно вибрати, коли застосовується правило (за замовчуванням всі елементи відмічені). Ці елементи визначають, чи застосовується правило в залежності від того, чи ваш комп'ютер підключено до мережі, яку ви визначили, як загальнодоступну чи приватну мережу.

Припустимо ви використовуєте ноутбук вдома (в мережі, яку ви визначили, як конфіденційну), на роботі (в мережі під управлінням домену) і в кафе (мережа, яку ви визначили, як загальнодоступну). Якщо ви хочете, щоб правило застосовувалося і в кафе, і на роботі, і вдома, виберіть всі 3 опції. Якщо ви хочете, щоб правило застосовувалося тільки в одному з 3 випадків, вкажіть відповідну опцію.

**Крок 9.** На сторінці "Ім'я" вкажіть назву правила. У цьому прикладі ми назвали правило "Блокувати сайт". Натисніть "Готово".



Steps:

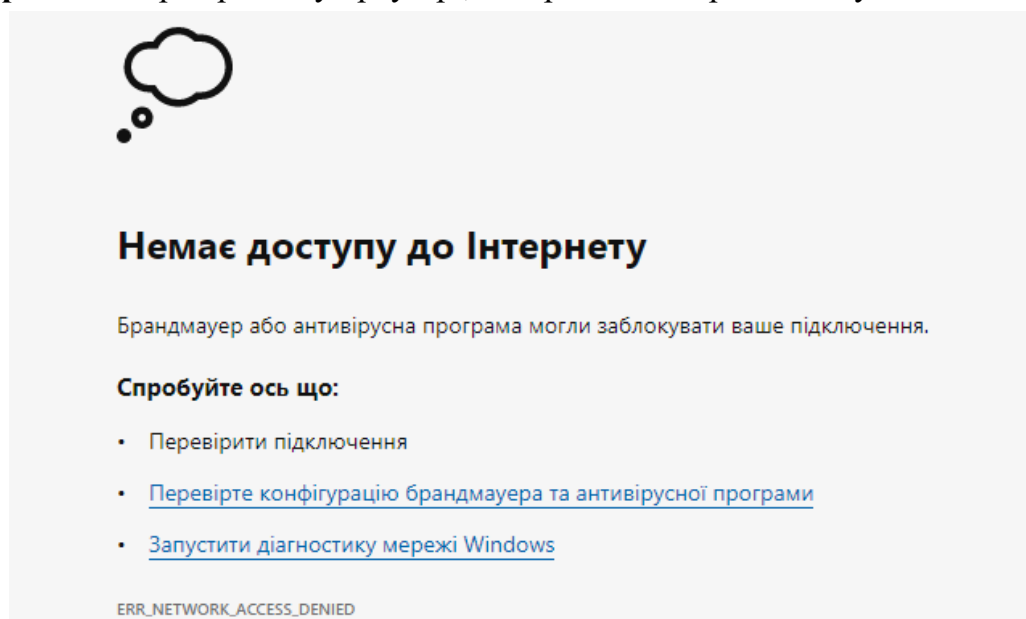
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Name:  
blockSite

Description (optional):

Якщо ви зробили все правильно, то ви повинні побачити **"blockSite"** в списку правил.

**Крок 10.** Перевіряємо у браузері, чи працює створене блокування.



Важливо! При перевірці працездатності правила потрібно враховувати наступне: коли сесія вже встановлена, а ПІСЛЯ цього застосована настройка правила мережевого екрану, що стосується трафіку в цій сесії, цю існуючу сесію мережевий екран не контролюватиме. Правило почне діяти після розриву поточної сесії - примусового або після закінчення часу життя сесії.

Якщо ви раніше заходили на сайти, щодо яких міняли налаштування, то відповіді DNS-серверів швидше за все, знаходяться в кеші браузера, клієнта DNS на локальному комп'ютері або кешуються DNS на роутері.

Для якнайшвидшого вступу в дію зміни налаштувань може знадобитися перезапустити браузер. У більшості випадків цього достатньо.

Якщо після перезапуску браузера змін немає, виконайте команду `ipconfig / flushdns` на локальному комп'ютері, яка очистить кеш DNS-клієнта Windows.

У ще більш рідкісних випадках може знадобитися очистити кеш DNS на роутері (досить буде перезапустити роутер).

**Завдання Б.** Установка віртуальної машини під ОС Linux і налаштування її брандмауера.

1. Завантажте інсталятор програми для роботи із віртуальною машиною Oracle VirtualBox, VMware або Microsoft Hyper-V.
2. Інсталюйте програму на комп'ютері та запустіть її.
3. Створіть нову віртуальну машину і встановіть на неї операційну систему Ubuntu (завантажити готовий образ віртуальної машини для VirtualBox можна на сайті <https://www.osboxes.org/ubuntu/>).
4. Встановіть та налаштуйте брандмауер gufw.