**Харківський національний економічний університет**

**імені Семена Кузнеця**

**ЗВІТ**

**З ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ № 5**

**за дисципліною: *“*** **Корпоративні мережі та системи доступу**”

**на тему: “Налаштування політик IP-безпеки. Брандмауер”**

**Варіант №4**

**Виконав: студент факультету Інформаційних технологій**

**3 курсу, спец. Кібербезпека,**

**групи 6.04.125.010.21.2**

**Бойко Вадим Віталійович**

**Перевірив:**

**Чугай Андрій Михайлович**

**ХНЕУ ім. С. Кузнеця**

**2023**

**Завдання:**

Виконати налаштування базових політик безпеки.

За допомогою вбудованих політик IP-безпеки потрібно налаштувати

доступ до окремих протоколів та портів передачі даних.

Налаштувати блокування всіх вхідних та вихідних з'єднань, крім

HTTP (порт 80) та HTTPS (порт 443); налаштувати дозвіл на внутрішні

з'єднання у мережі, але блокування зовнішніх з'єднань.

Створити правила для різних типів програм.

Налаштувати журналування всіх подій брандмауера для подальшого

аналізу.

Налаштувати моніторинг мережевої активності для виявлення

аномалій.

Оскільки, заборона дозволу для різних протоколів відбувається

однотипним чином, то пропонується, для лабораторної роботи,

використовувати протокол ICMP. Відповідно до виданого варіанту,

вибирати діапазон IP-адрес для дозволу проходження пакетів протоколом

ICMP, проходження пакетів із інших адрес повинно бути заборонено.

Також у кожного діапазону є додаткова IP-адреса. Якщо вказана адреса

входить до первинного діапазону, то потрібно додатково заборонити

надходження запитів із вказаної адреси, якщо адреса не входить до

вказаного діапазону, то, навпаки, дозволити доступ із додаткової IP-адреси.

|  |  |
| --- | --- |
| Діапазон для дозволу доступу | Додаткова адреса |
| 192.168.1.192-192.168.1.255 | 192.168.1.153 |

**Контрольні питання**

1. Які існують типи мережевих екранів, чим вони відрізняються?

2. Яке призначення мережевого екрану, де він повинен бути встановлений?

3. Яке призначення протоколу ICMP?

4. Функціонування мережевого екрану із пакетною фільтрацією.

5. Основні принципи роботи мережевого екрану прикладного рівня.

6. Які наявні рішення мережевих екранів і яких компаній Ви можете назвати?

7. Яким чином здійснюється доступ до налаштувань IP-політик в

операційній системі Windows?

8. Які переваги персональних мережевих екранів перед вбудованими IP політиками ви можете назвати?

9. Які додаткові функціональні можливості мережеві фільтри можуть

запропонувати користувачеві?

10. Які персональні мережеві екрани Ви можете назвати?

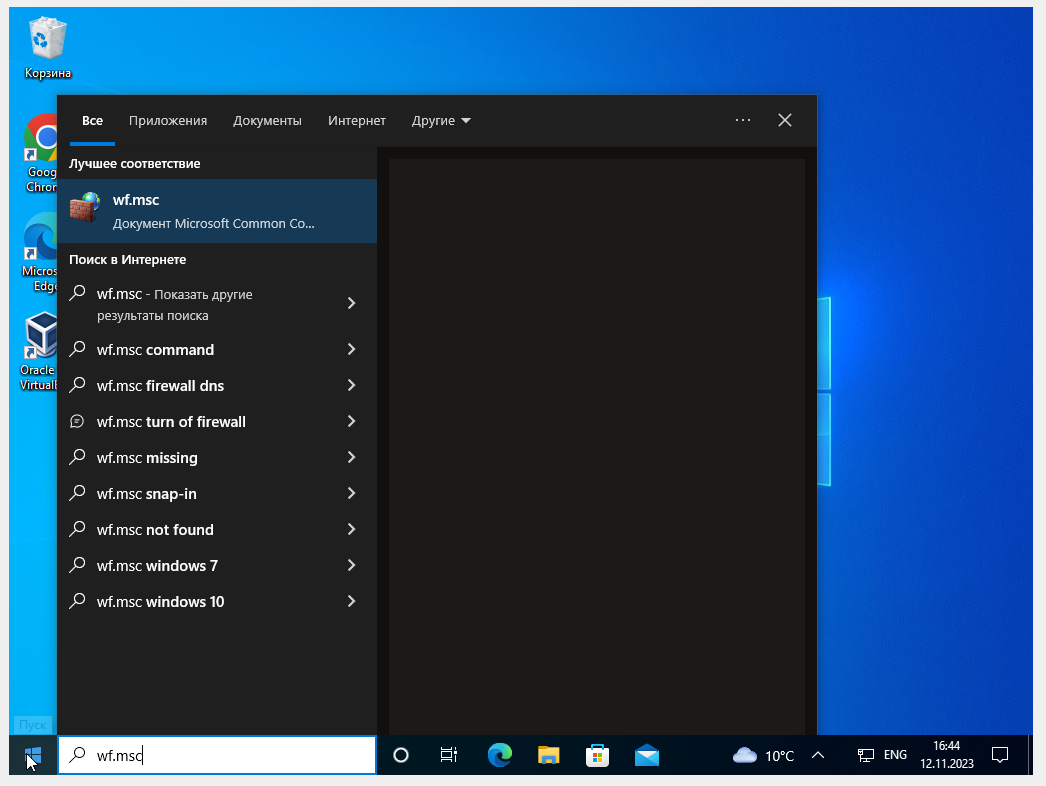
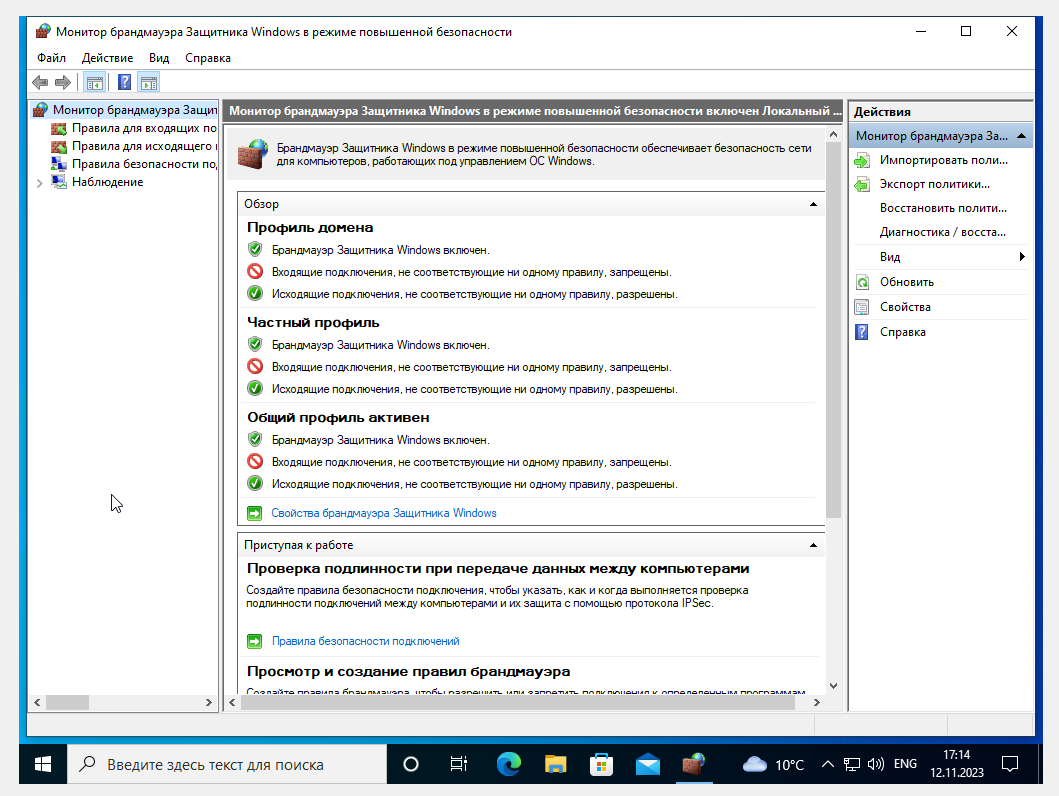
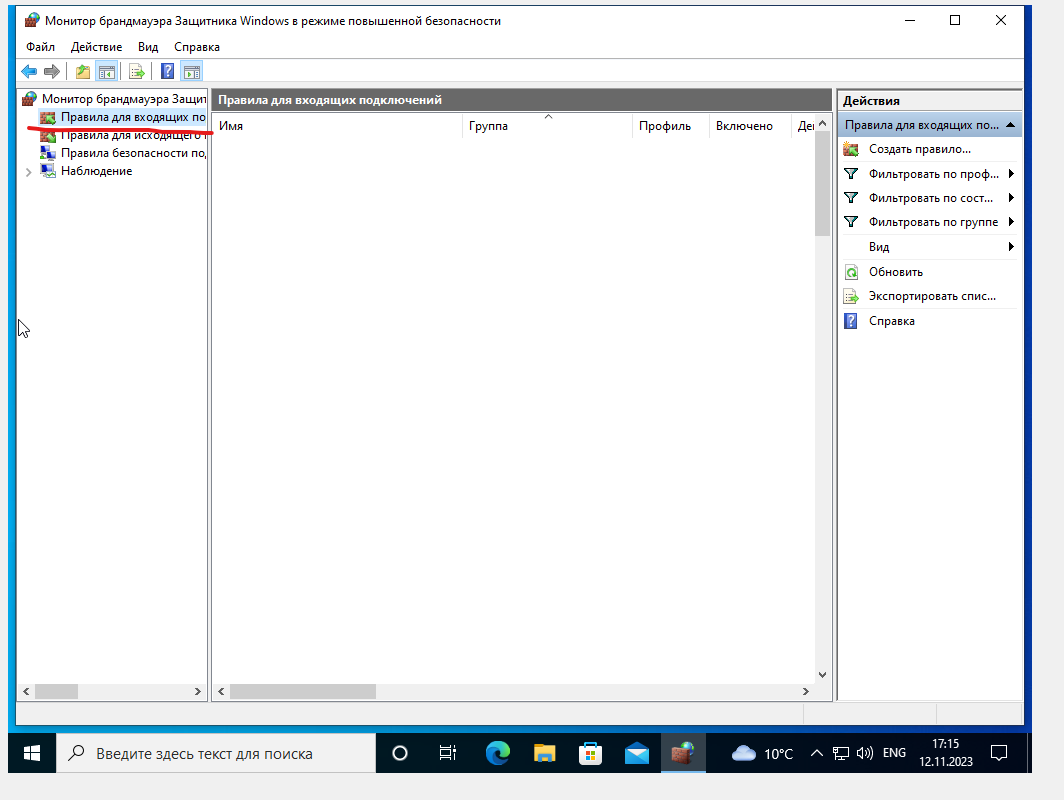
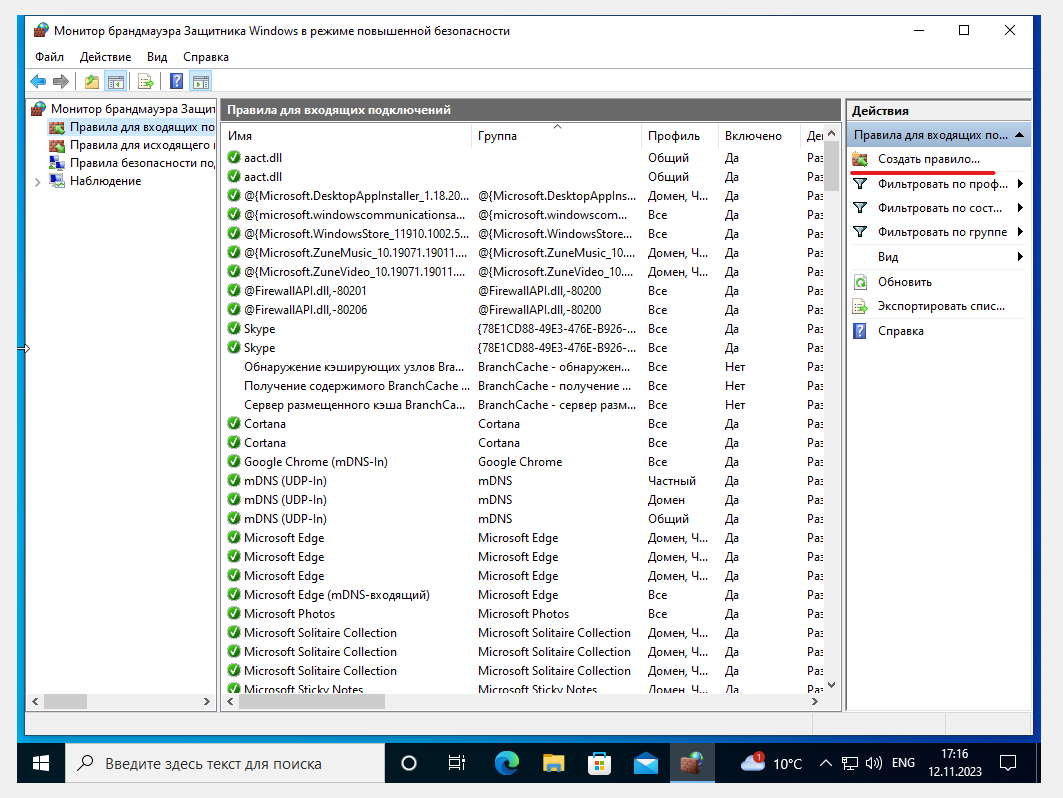
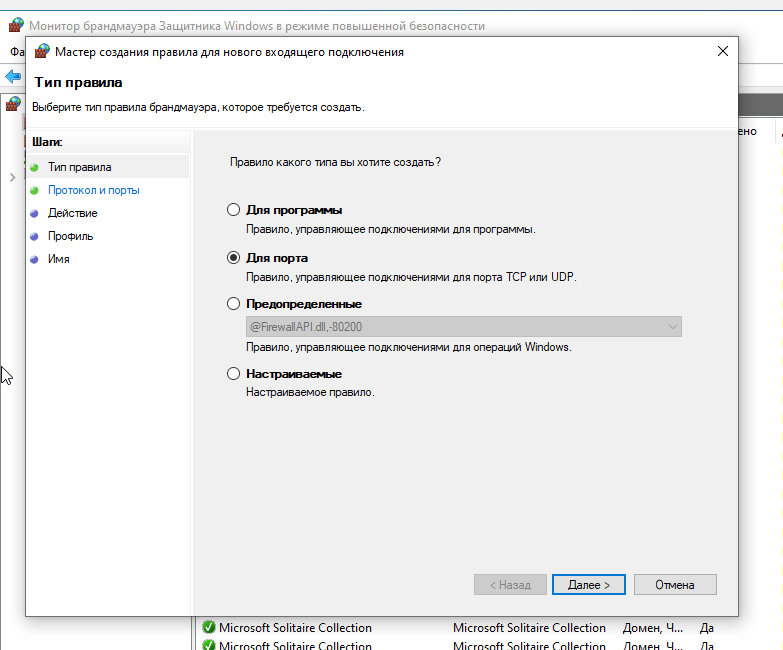
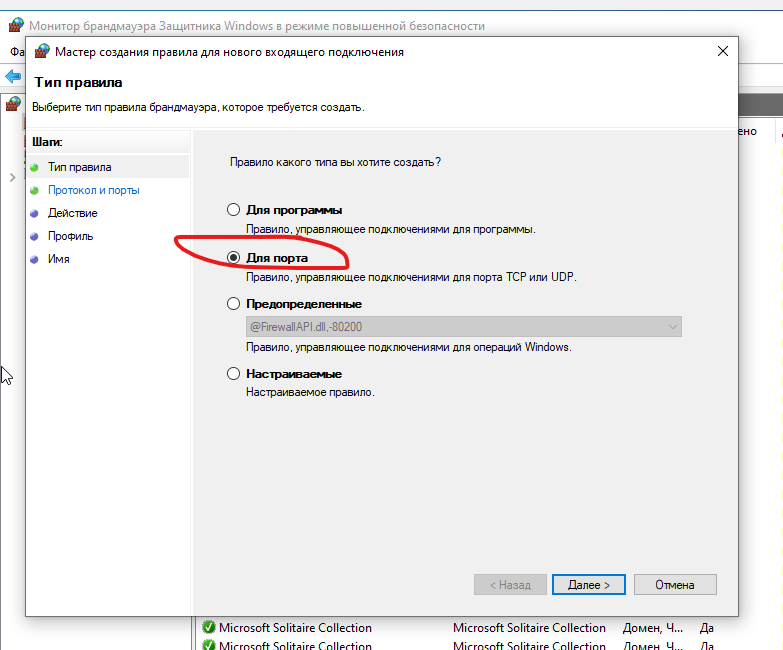
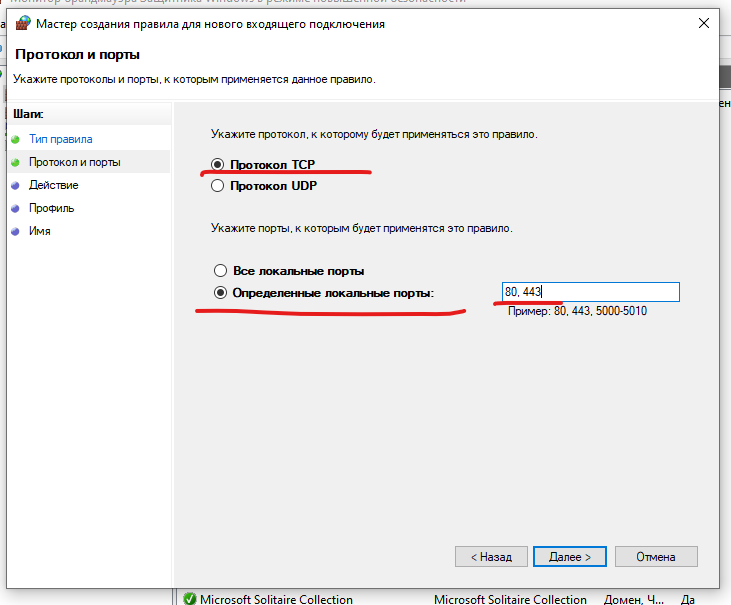
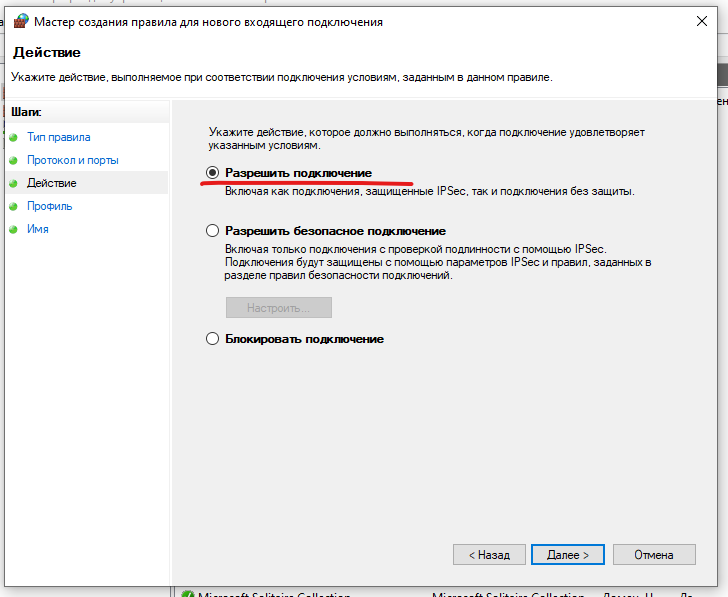
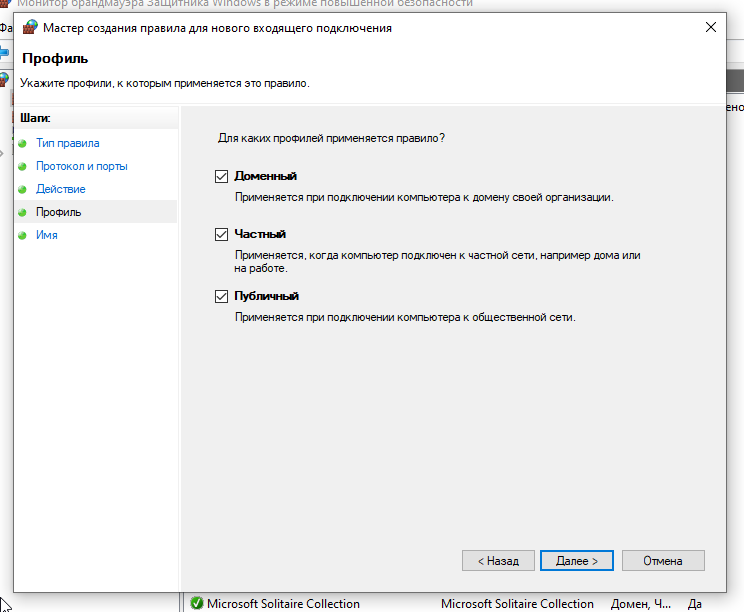
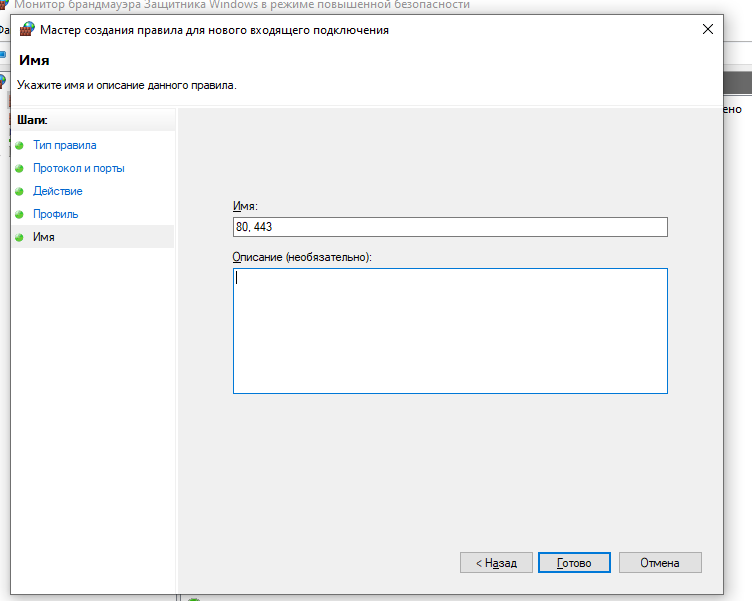
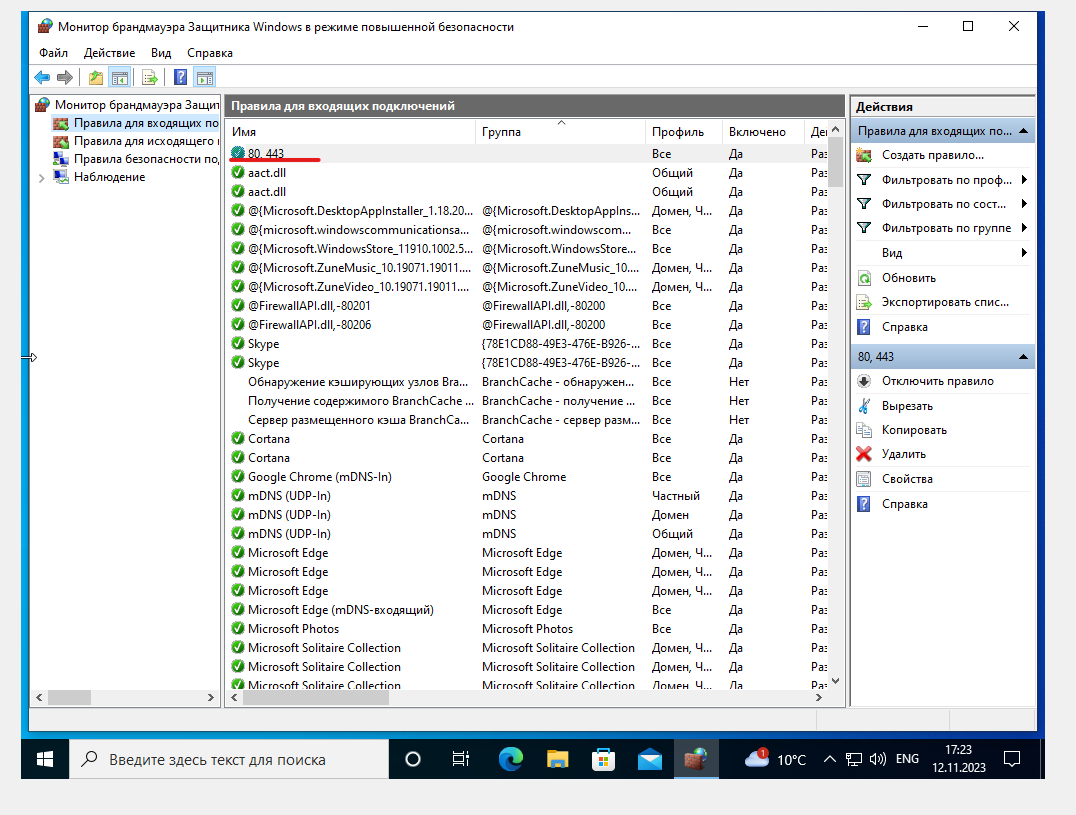
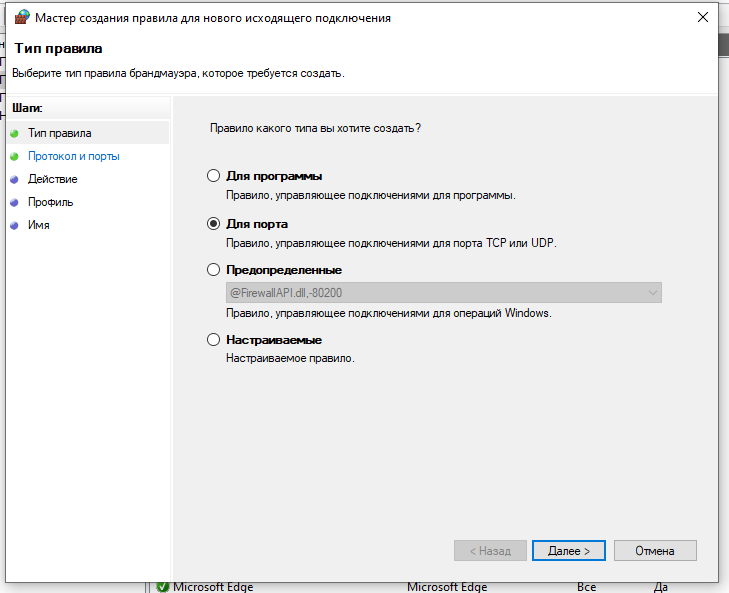
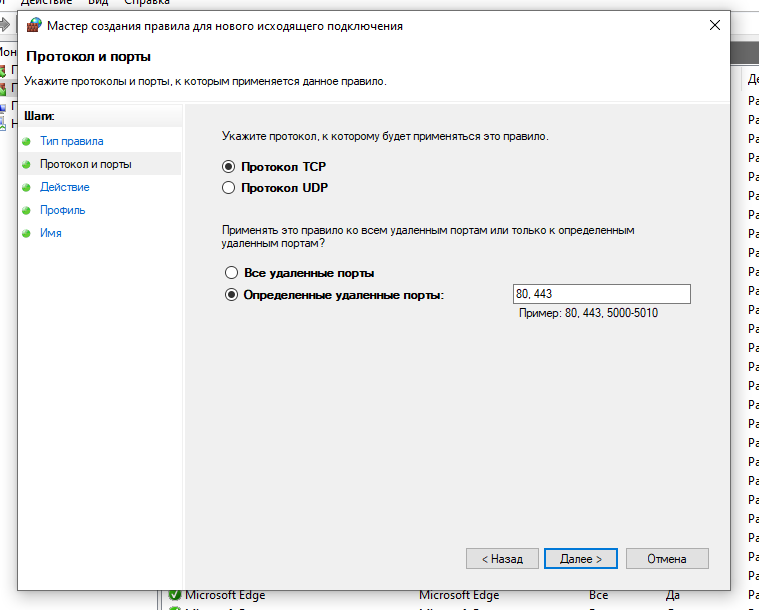
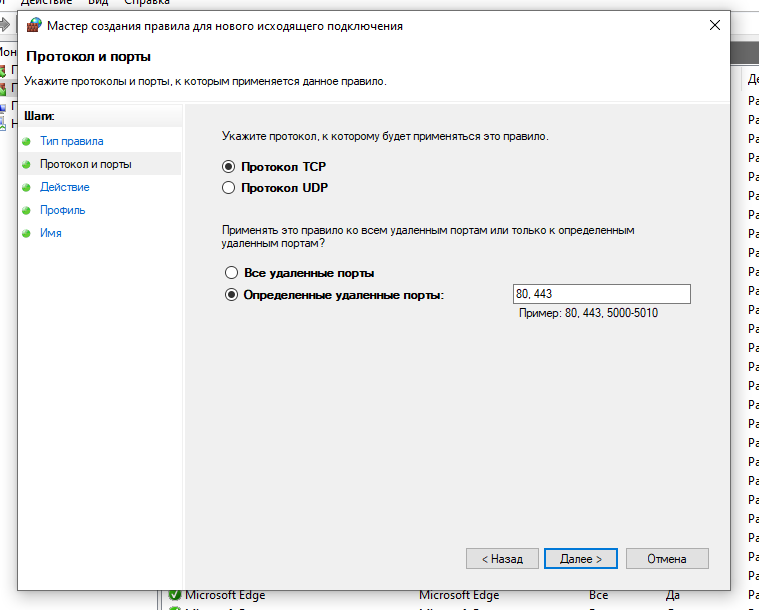
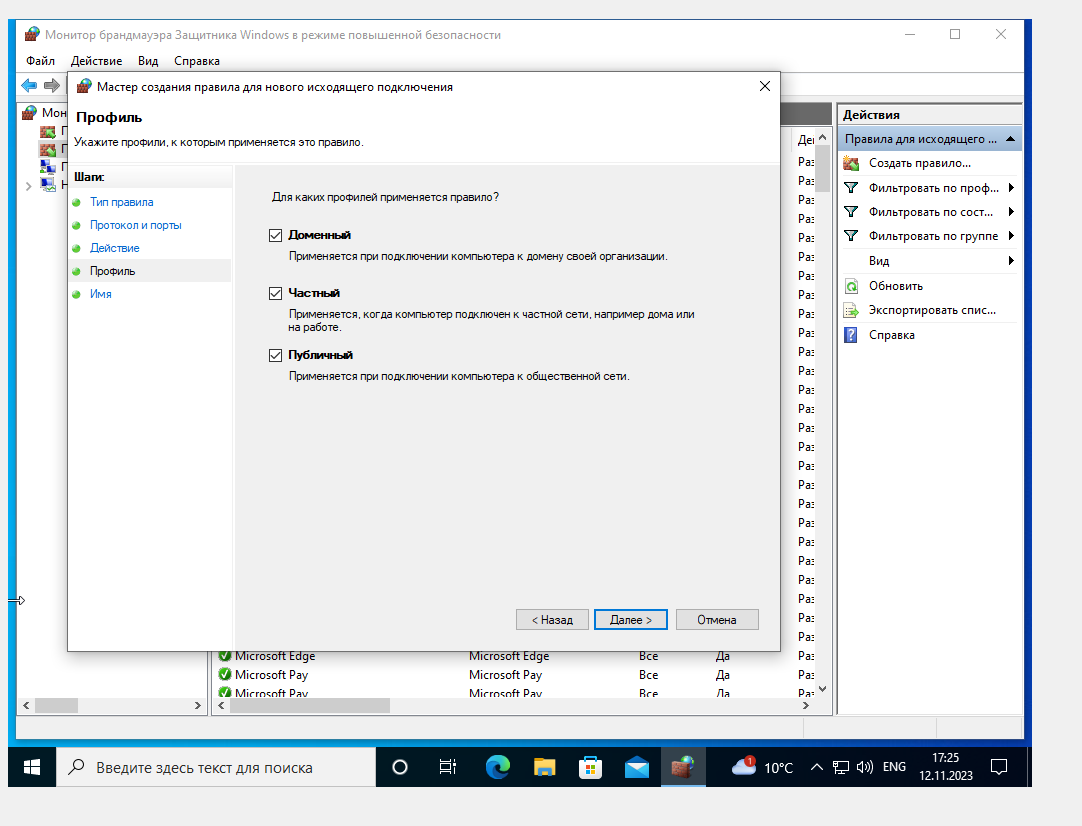
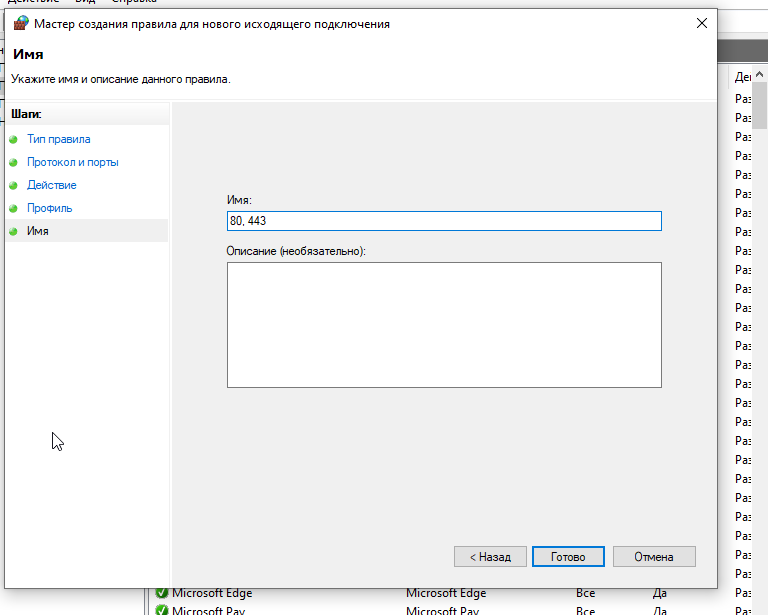
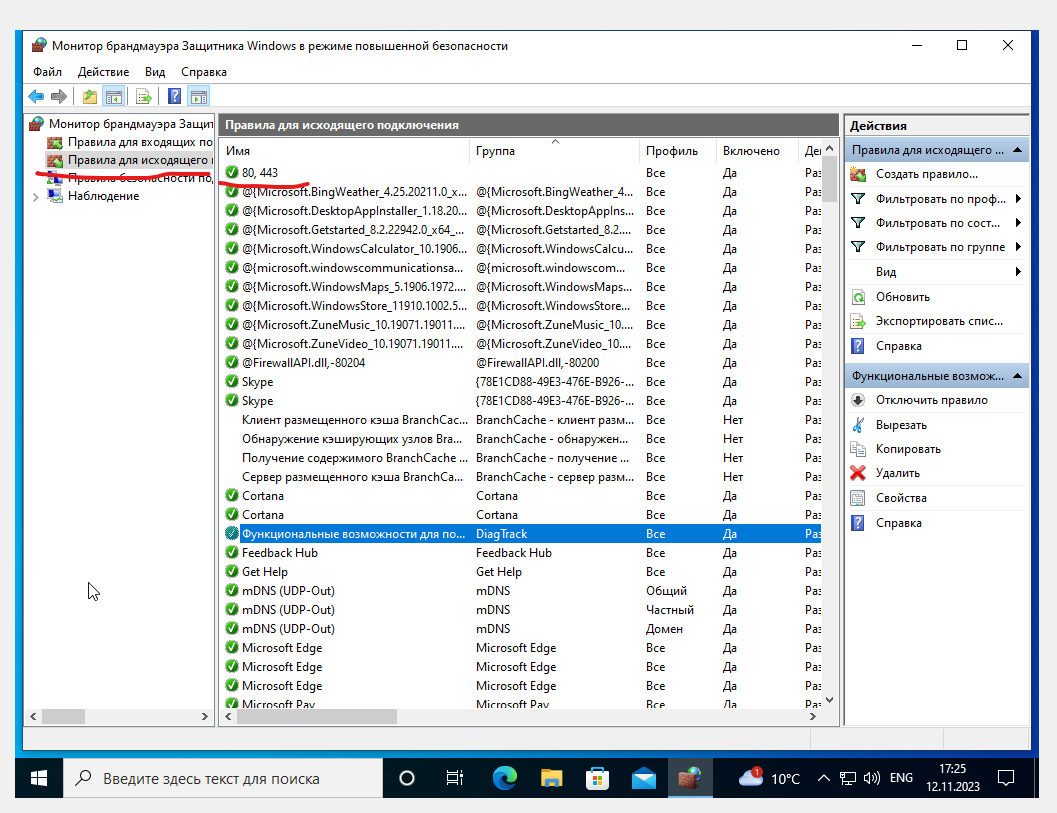
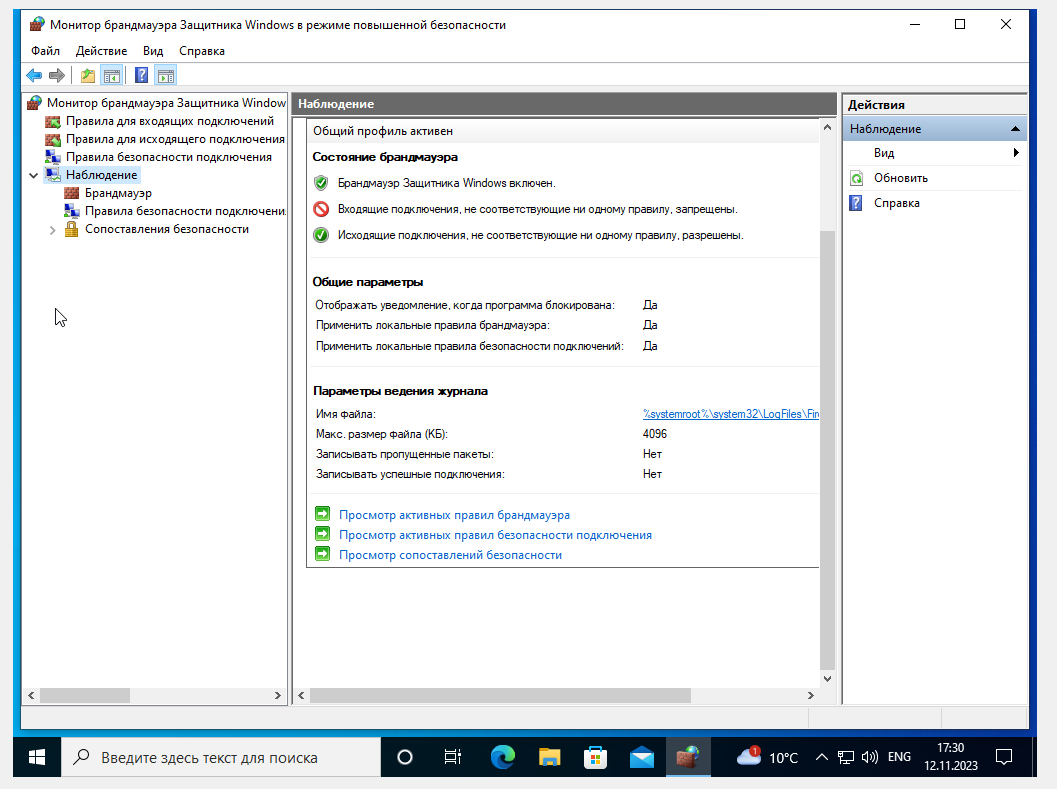
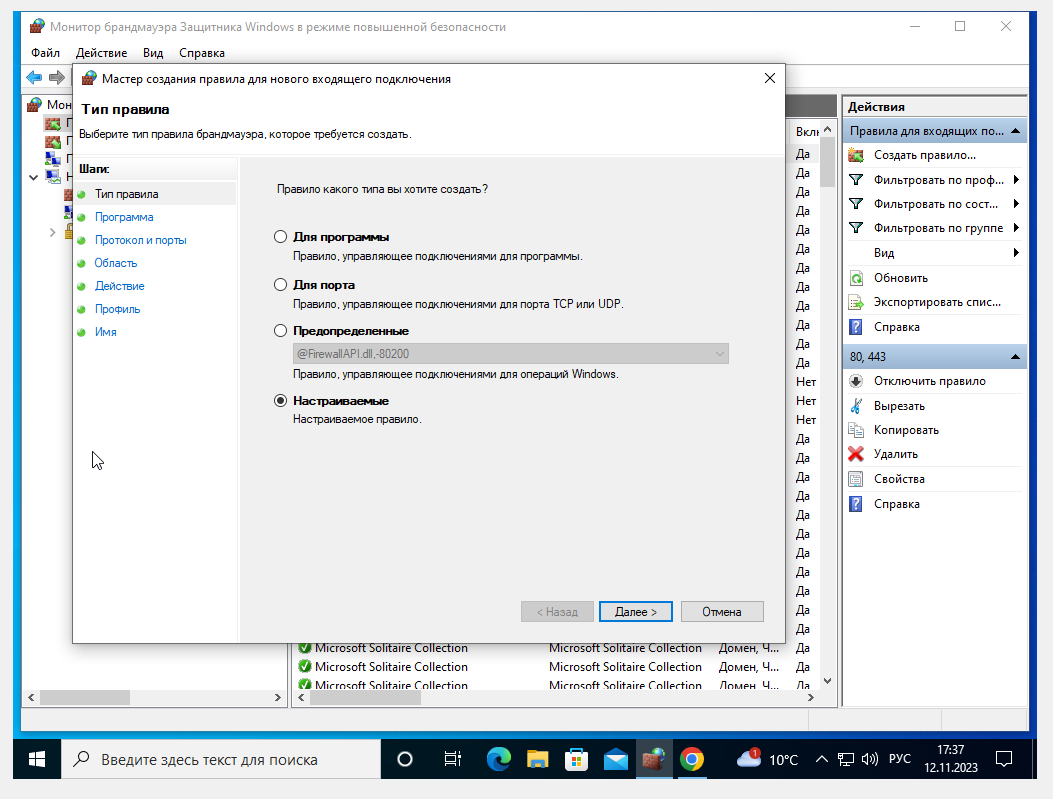
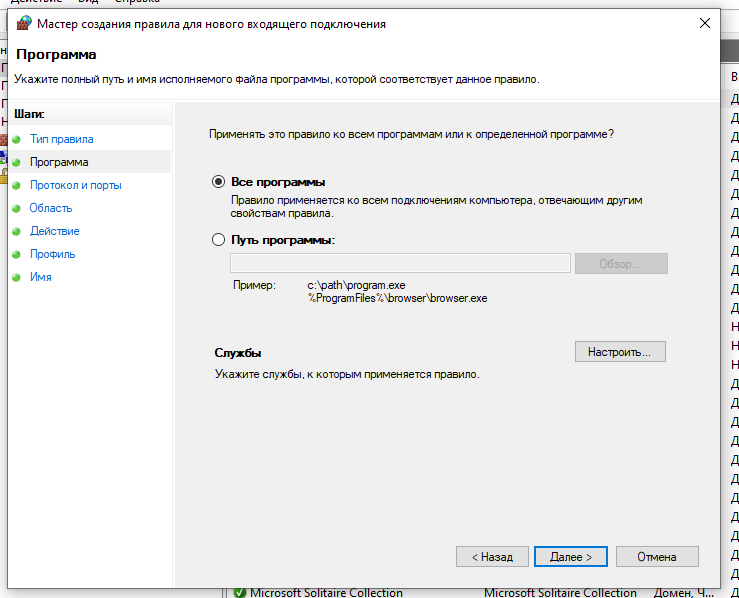
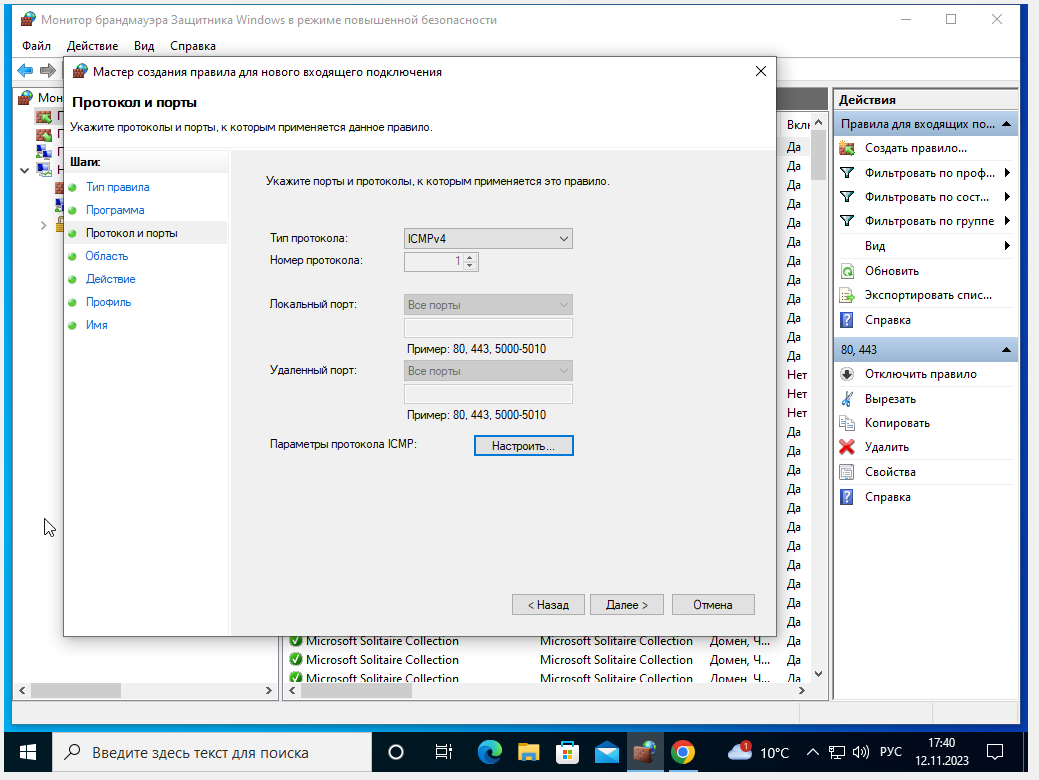
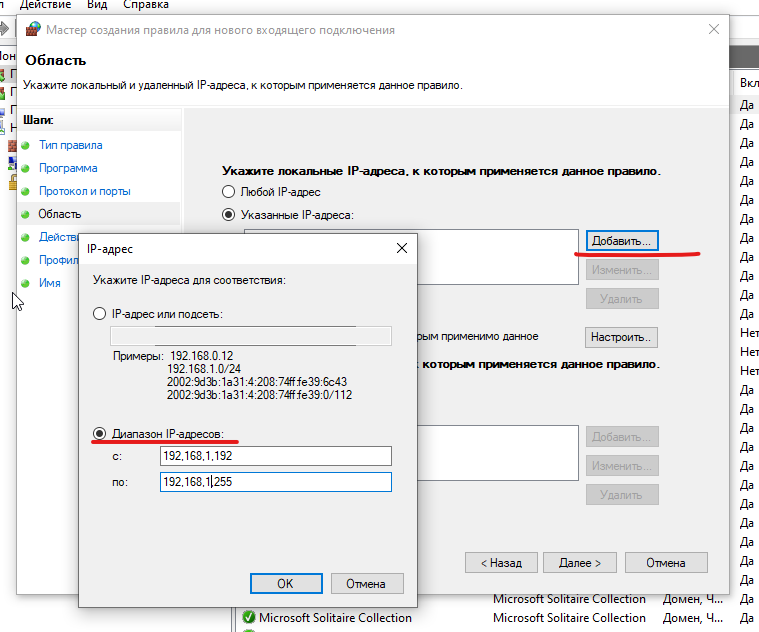
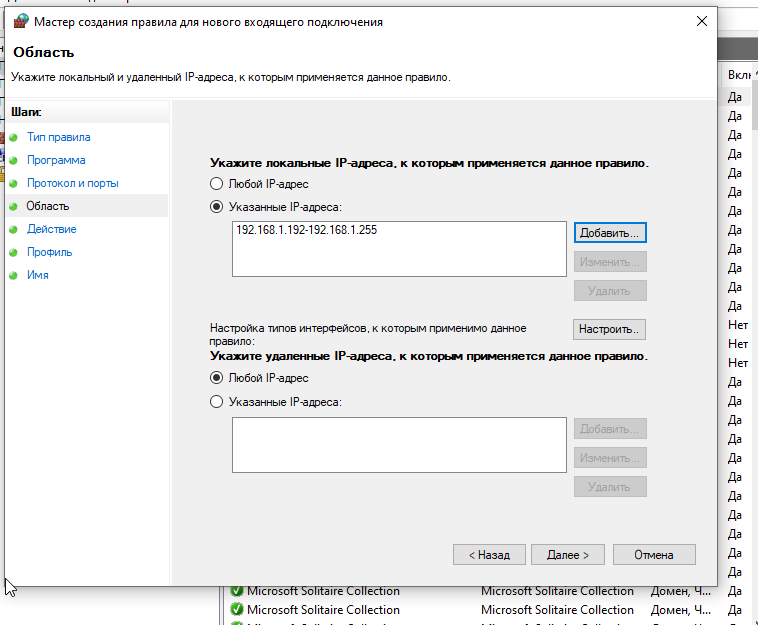
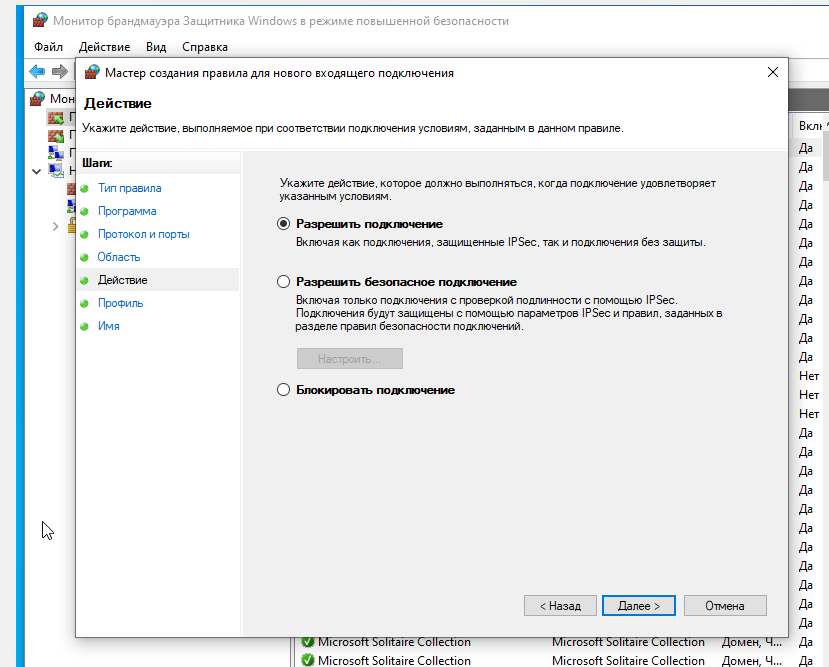
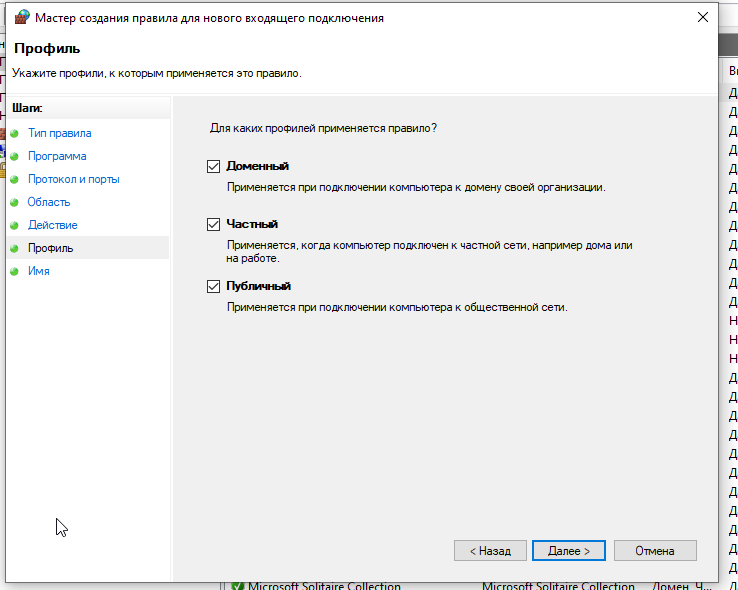
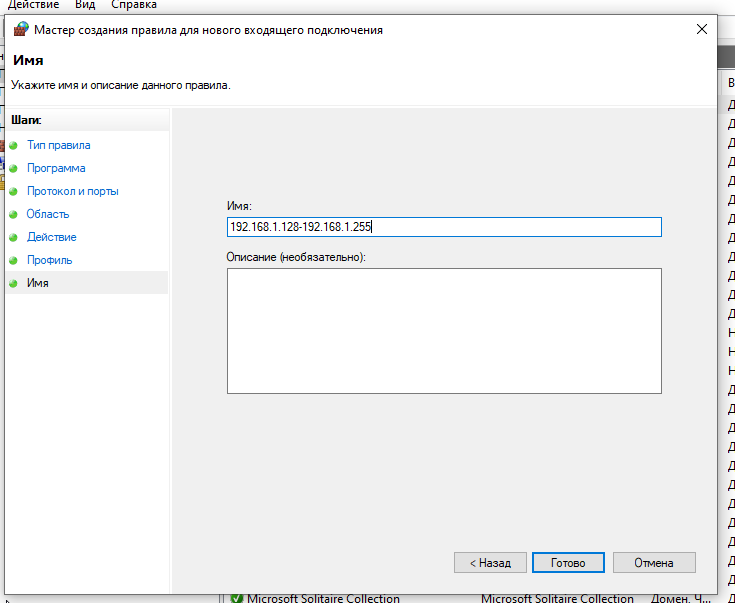
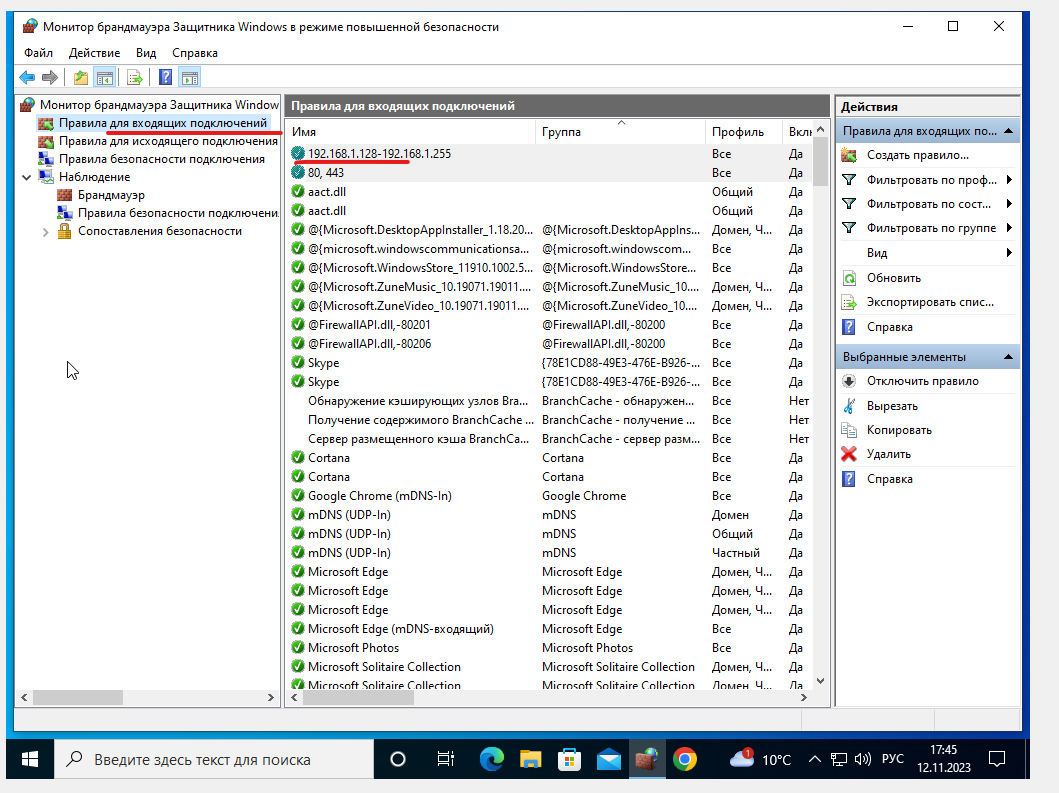
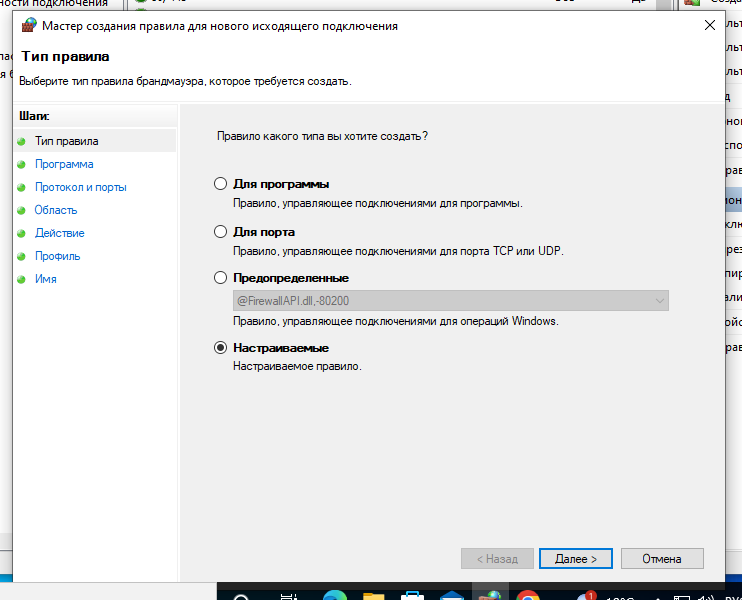
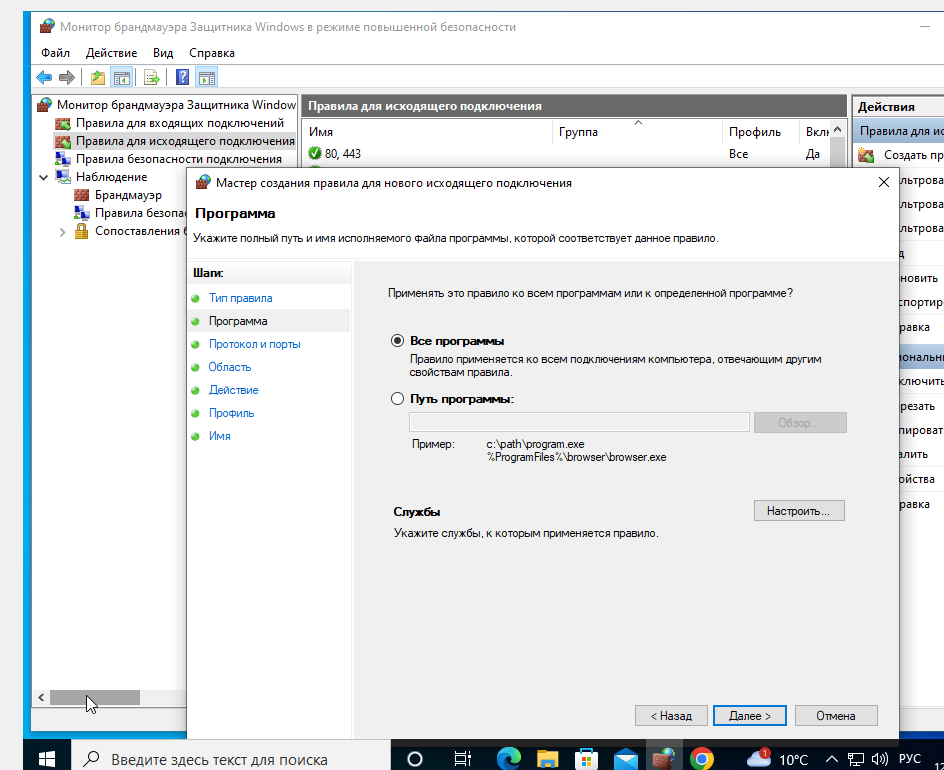
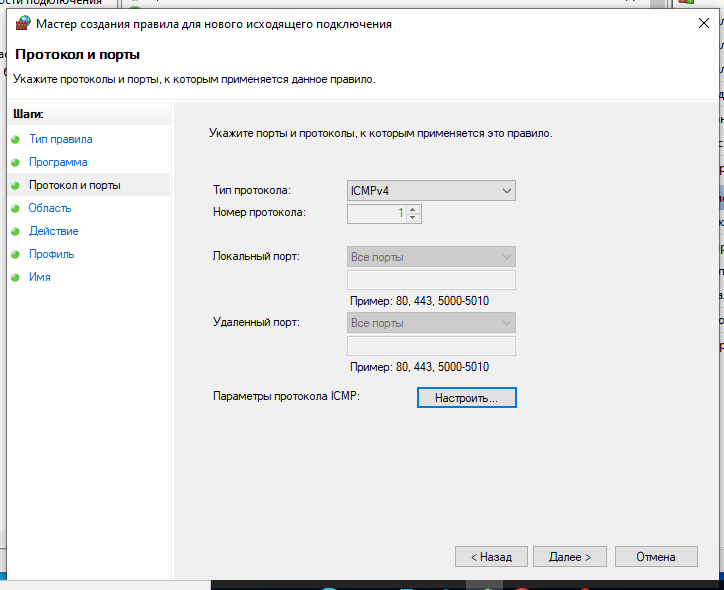
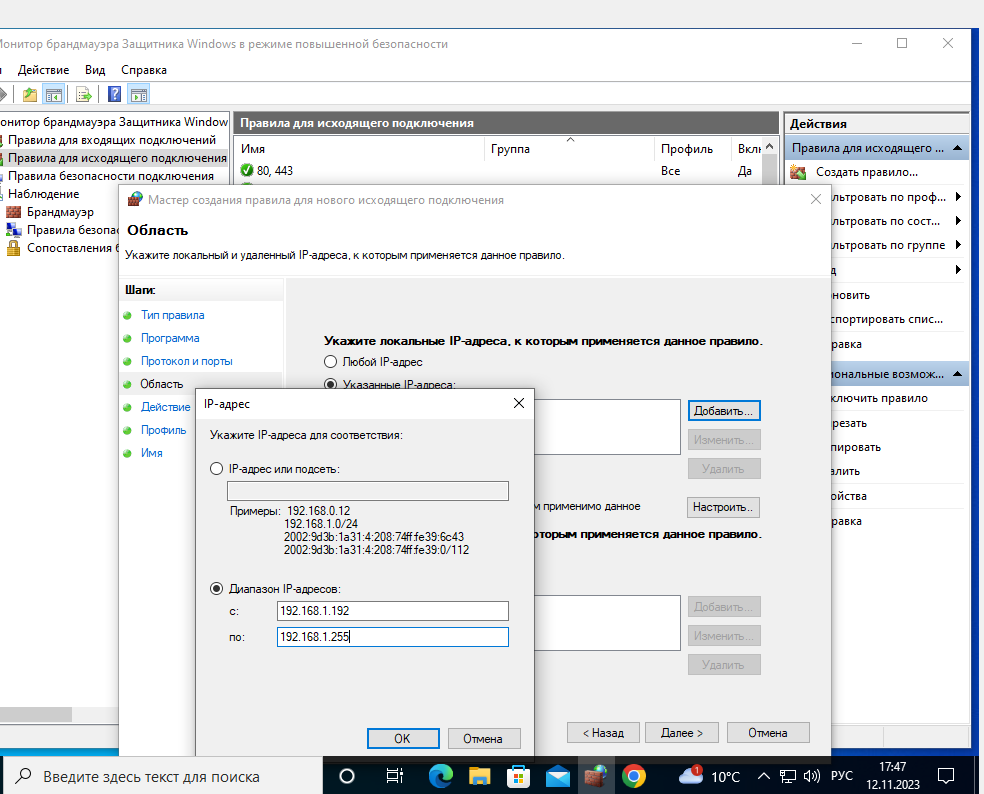
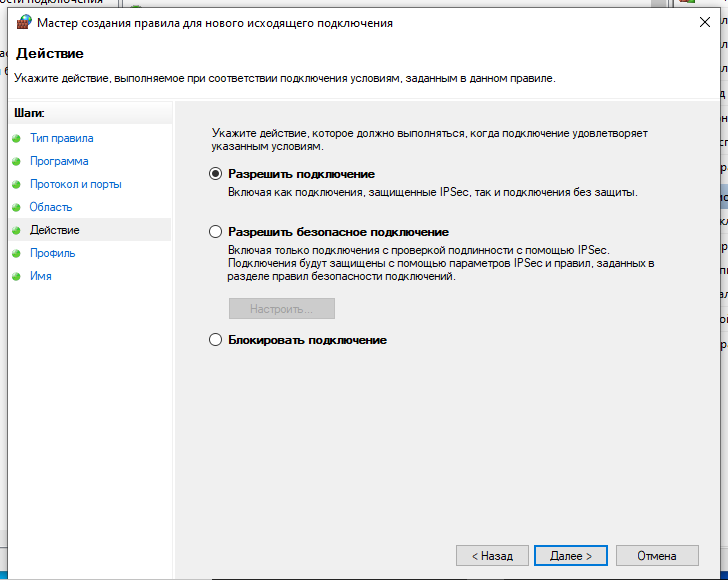
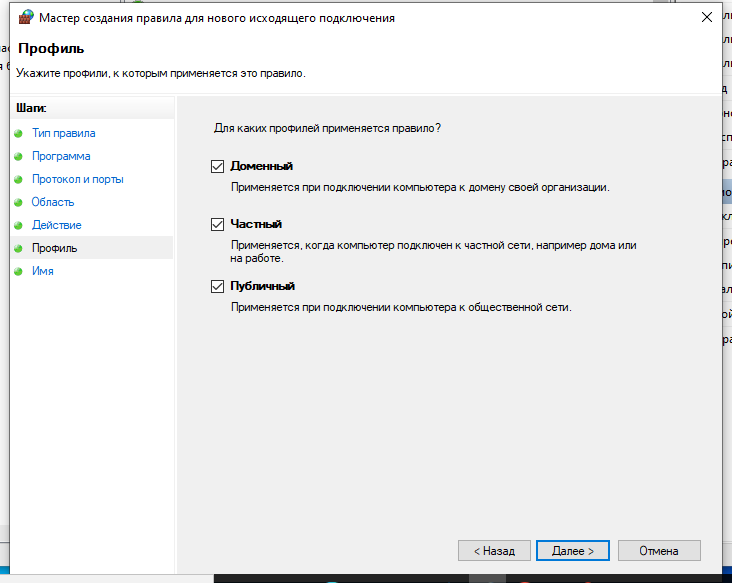
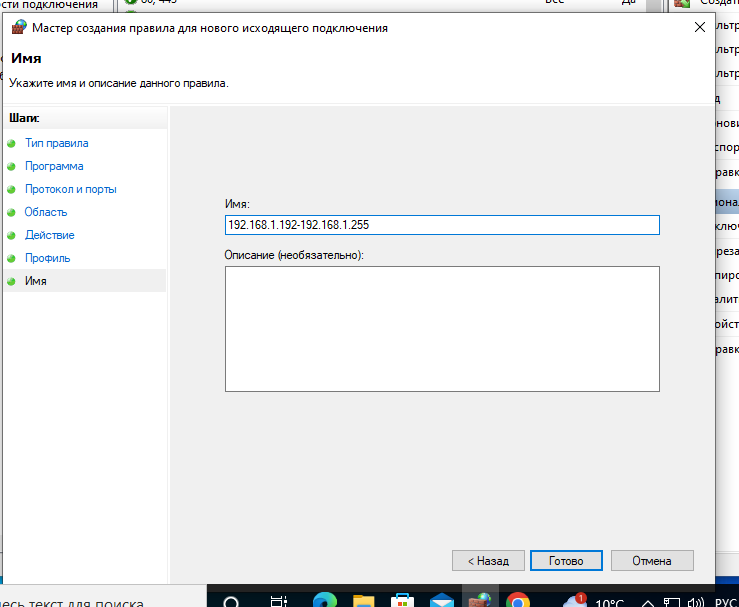
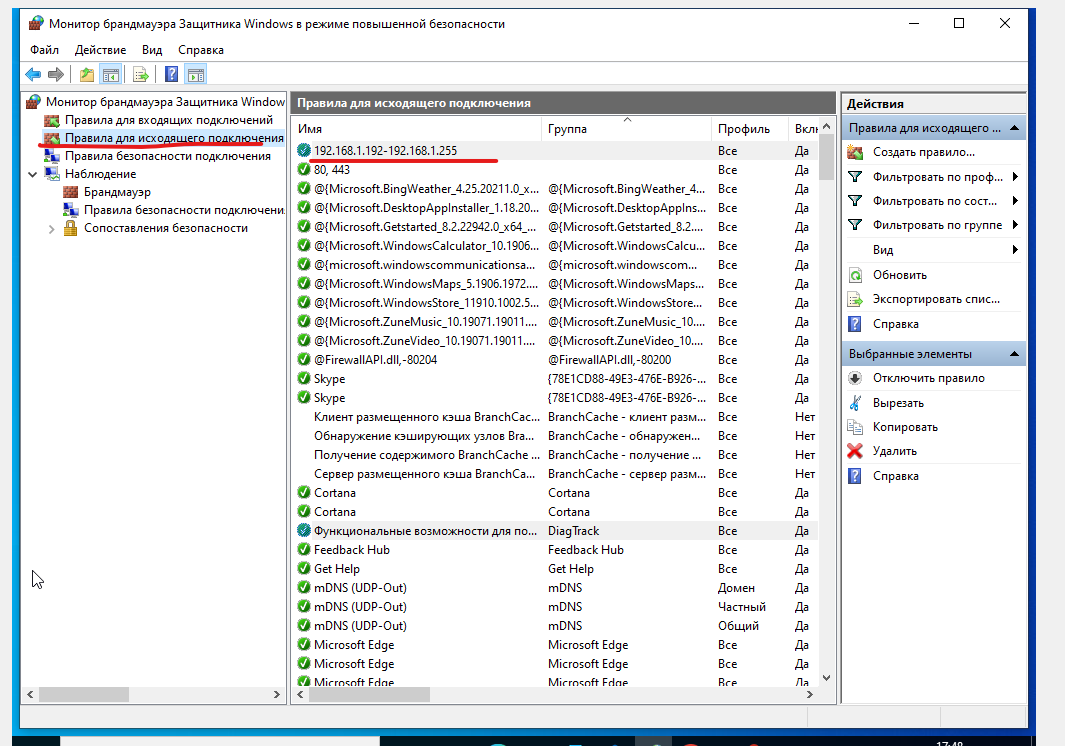
11. Яким чином можна здійснити розподіл мережі на підмережі за

допомогою маски?

12. У якому випадку використання мережевого екрану буде

неефективним?

**Хід роботи**

1. Відкрию віртуальну ОС для виконання даної лабораторної роботи
2. Відкрию пуск та напишу “wf.msc”  
     
   та натискаю «Enter»
3. Відкрилось наступне вікно  
   
4. Для блокування «вхідного» трафіку відкриваю «Правила для входящего трафика»  
   
5. Для додавання правил, обираю «Создать правила»  
   
6. Відкриється наступне вікно  
   
7. Обираю правила «Для порта»  
     
   Та натискаю «Далее»
8. Наступним кроком прописую порти   
     
   Та натискаю «Далее»
9. У наступному вікні обираю «Разрешить подключения»  
     
   Та натискаю «Далее»
10. Далі натискаю «Далее», бо правила будуть задіяні для всі профілей  
    
11. У останньому вікні додам ім’я правила та натисну «Готово»  
     
12. В результаті бачимо, наше правило у списку   
    
13. Теж саме роблю для «Вихідного трафіку»  
      
      
      
      
      
    ****  
    ****
14. Наступним кроком додам журналювання
15. Для цього відкрию вкладку «Наблюдение»  
    ****
16. Можна побачити, що журналювання вже вімкнене
17. Наступним кроком дозволю трафік для певних ip адрес
18. Знову настисну на «Создать правило» та обираю «Настраиваемый»  
    ****
19. Обираю «Все программы» та натискаю далее  
    
20. Обираю протокол «ICMP» та натискаю «Далее»  
    
21. Наступним чином додаю правила для локальних адрес та прописую діапазон відповідно да завдання  
      
    ****  
    Та натискаю «Далее»
22. У наступному вікні натискаю «Далее»  
    
23. Профілі не змінюю  
    
24. Та дам ім’я для правила   
    ****
25. Бачимо правило у списку  
    
26. Теж саме зроблю для вихідного трафіку  
      
      
      
      
      
      
      
    

**Відповіді на контрольні питання**

1. Типи:
   1. Пакетні фільтри:
      1. Спрямовані на рівень мережі (Network Layer): Ці екрани аналізують та фільтрують трафік на основі інформації, яка міститься в заголовках мережевих пакетів, таких як IP-адреса та порт.
      2. Спрямовані на рівень транспортного протоколу (Transport Layer): Фільтрація виконується на основі інформації, що міститься в заголовках транспортних пакетів (наприклад, TCP або UDP).
   2. Мережеві екрани зі станом (Stateful Firewalls):
      1. Аналізують трафік на більш високому рівні, спостерігаючи за станом пакетів та використовуючи інформацію з попередніх пакетів для визначення того, чи є певний пакет частиною легітимного з'єднання.
   3. Проксі-сервери (Proxy Firewalls):
      1. Опосередковують з'єднання між внутрішньою та зовнішньою мережами, допомагаючи захищати інтернет-ресурси від прямого з'єднання із зовнішніми джерелами. Вони можуть фільтрувати трафік та виконувати інші функції безпеки.
   4. Програмні та апаратні мережові екрани:
      1. Програмні мережеві екрани працюють на рівні операційної системи, вбудовуючись у стек мережевих протоколів.
      2. Апаратні мережеві екрани є фізичними пристроями, вбудованими в інфраструктуру мережі.
   5. Cloud Firewalls:
      1. Розташовані в хмарних сервісах та призначені для захисту хмарних інфраструктур та ресурсів.
   6. Інтелектуальні мережеві екрани:
      1. Використовують алгоритми машинного навчання та аналізу трафіку для виявлення нестандартних патернів та потенційно шкідливих активностей.
2. Мережевий екран потрібен для:
   1. Фільтрації трафіку
   2. Блокування доступу
   3. Захист від атак
   4. Моніторинг та журналювання
3. ICMP (англ. Internet Control Message Protocol — міжмережевий протокол керуючих повідомлень) — мережевий протокол, що входить в стек протоколів TCP/IP. В основному ICMP використовується для передачі повідомлень про помилки й інші виняткові ситуації, що виникли при передачі даних. Також на ICMP покладаються деякі сервісні функції, зокрема на основі цього протоколу заснована дія таких загальновідомих утиліт як ping та traceroute.
4. Пакетні фільтри:
   1. Спрямовані на рівень мережі (Network Layer): Ці екрани аналізують та фільтрують трафік на основі інформації, яка міститься в заголовках мережевих пакетів, таких як IP-адреса та порт.
   2. Спрямовані на рівень транспортного протоколу (Transport Layer): Фільтрація виконується на основі інформації, що міститься в заголовках транспортних пакетів (наприклад, TCP або UDP).
5. Опосередковують з'єднання між внутрішньою та зовнішньою мережами, допомагаючи захищати інтернет-ресурси від прямого з'єднання із зовнішніми джерелами. Вони можуть фільтрувати трафік та виконувати інші функції безпеки.
6. Cloud flare – захист для веб сервісу   
   Firewall від компанії cisco можна налаштувати будь що
7. Переваги персональних мережевих екранів перед вбудованими:
   1. Гнучкість налаштувань
   2. Більш високий рівень безпеки
   3. Захист в режимі реального часу
   4. Можливості антивірусного та антишпигунського захисту
   5. Наявність додаткових функцій
   6. Спрощений інтерфейс
8. Обробка пакетів