## Лабораторна робота №14

## настройка брандмауера ОС Windows

**Метою роботи** є вивчення роботи та виконання операцій з налаштування деяких додаткових параметрів брандмауера ОС Windows.

**Технічне забезпечення занять**

1. Персональне робоче місце №1 студента (ПЕОМ на базі віртуальної машини) зі встановленим загальносистемним програмним забезпеченням ОС Windows 10.
2. Програмне забезпечення віртуалізації OracleVBox.
3. Програмне забезпечення ОС Window 10, встановлене на другої віртуальної машині (персональне робоче місце №2 студента).

**Питання, що відпрацьовуються на занятті**

1. Налаштування роботи брандмауера ОС Windows
2. Створення правил роботи з програмним забезпеченням за допомогою правил брандмауера ОС Windows.

**Приклад виконання завдань:**

1. На комп'ютері №1 натиснути правою кнопкою миші на робочому столі, далі вибрати **New > Folder (Создать> Папку)**. (рис.1). Задайте ім'я нової папки - Cisco.

|  |
| --- |
|  |

Рис.1 Створення нової папки

1. Натиснить правою кнопкою миші на папці **Cisco** і виберіть «**Share with > Advanced sharing > Advanced Sharing (Загальний доступ> Розширена настройка загального доступу> Розширена настройка загального доступу)**. Відкриється вікно **“Advanced Sharing”** («Розширена настройка загального доступу») - (Рис.2).

|  |
| --- |
|  |

Рис.2 Розширена настройка загального доступу

1. Надайте спільний доступ до цієї папки, використовуючи ім'я за замовчуванням **Cisco**.
2. На комп'ютері №2 натисніть кнопку **Start> (Пуск>)** , виберіть пункт **Control Panel > Network and Sharing Center > Network (Панель керування> Центр керування мережами і загальним доступом> Мережа)**. Двічі натисніть комп'ютер №1 та перевірте наявність папок у відповідності до рис 3.

|  |
| --- |
|  |

Рис.3 Вигляд папок загального доступу

1. Перейдіть до брандмауера на комп'ютері №1 ОС Windows.
2. Виберіть **Start > Control Panel > System and Security > Windows Firewall (Пуск> Панель керування>** Система і безпека> **Брандмауер Windows) –** рис. 4Індикатор брандмауера показує стан брандмауера. Стандартний режим **“ON” («Включено»).**

|  |
| --- |
|  |

Рис. 4 Вікно брандмауера на комп'ютері №1 ОС Windows.

1. Перейдіть за посиланням **Allow a program or feature through Windows Firewall** (Дозволити запуск програми або компонента через брандмауер Windows). – рис.5

|  |
| --- |
|  |

Рис. 5 Вікно брандмауера на комп'ютері №1 ОС Windows.

1. Відкриється вікно “Allowed Programs” ("Дозволені програми»). рис 6.

|  |
| --- |
|  |

Рис.6. Вікно брандмауера на комп'ютері №1 ОС Windows.

1. Для програм і служб, що не блокуються брандмауером Windows, будуть встановлені прапорці. Можна додавати застосунки до цього списку. Це може бути необхідно, якщо у клієнта є застосунок, який вимагає з'єднання з зовнішньою мережею, але з якоїсь причини брандмауер Windows не може виконати настройку автоматично. Для завершення даної процедури необхідно увійти в систему на цьому комп'ютері з правами адміністратора.
2. Перейдіть за посиланням **What are the risks of allowing a program to communicate? (**Які ризики становить дозвіл зв'язку для програми?).
3. Відкриється вікно **“Windows Help and Support” («Довідка та підтримка Windows»).** – див. рис. 7.

|  |
| --- |
|  |

Рис.7. Вікно довідки

1. Закрийте вікно **“Windows Help and Support”** («Довідка та підтримка Windows»).
2. З комп'ютера №1 виконайте наступні дії: натиснути вікно **“Allowed Programs**” ("Дозволені програми»), щоб активувати його. Рис.8.

|  |
| --- |
|  |

Рис. 8 Вид вікна «Дозволені програми»

1. Для скасування винятку зніміть прапорець **File and Printer Sharing (Загальний доступ до файлів і принтерів)> OK.**
2. На комп'ютері №2 виконайте наступні дії: Відкрийте мережне підключення до комп'ютера №1.
3. Послідовно виберіть **Start > Control Panel > Network and Sharing Center > Network (Пуск> Панель керування> Центр керування мережами і загальним доступом> Мережа).** – рис.9.

|  |
| --- |
| Рис.9 Вікно мережі комп’ютеру №2 |

1. З комп'ютера №1 виконайте наступні дії: Для скасування винятку встановіть прапорець **«File and Printer Sharing (Загальний доступ до файлів» і принтерів)>** і натисніть OK.
2. На комп'ютері №2 виконайте наступні дії: Оновіть вікно **Network (Мережа)** та здійснити з’єднання до комп'ютера №1.
3. Виберіть **Start > Control Panel > System and Security > Administrative Tools > Windows Firewall** (Пуск> Панель керування> Система і безпека> Адміністрування> Брандмауер Windows) в режимі Advanced Security > Inbound Rules (Підвищена безпека> Правила для вхідних підключень). Рис 10.

|  |
| --- |
| Рис.10 Вікно «Правила для вхідних підключень» |

1. Розгорніть вікно, щоб можна було побачити повне ім'я правил для вхідних підключень. Знайдіть **Files and Printer Sharing (Echo Request – ICMPv4-In)**  («Загальний доступ до файлів і принтерів (ехо-запит - вхідний трафік ICMPv4)»). Натиснути правило правою кнопкою миші, виберіть **Properties > Advanced>** (Властивості> Додатково>) натисніть кнопку **Customize** (Налаштувати). – рис.11

|  |
| --- |
|  |

Рис.11. Вікно загального доступу до файлів і принтерів

1. На вкладці **Advance** («Додатково») відображається профіль, який використовується комп'ютером, а у вікні “**Customize Interface Types**” («Налаштування типів інтерфейсів» ) відображаються різні підключення, налаштовані на комп'ютері. Натисніть OK.
2. Перейдіть на вкладку **Programs and Services** (Програми та служби). Відкриється вікно “Customize Service Settings” («Налаштування параметрів служби»). – рис. 12.

|  |
| --- |
|  |

Рис.12. Вікно «Налаштування параметрів служби»

1. Перейдіть на вкладку **Protocols and Ports** (Протоколи і порти). Для настройки ICMP натисніть кнопку **Customize** (Налаштувати). Можна побачити меню, в якому налаштовуються винятки ICMP. –рис.13.

|  |
| --- |
|  |

Рис.13. Вікно настройки ICMP

1. У наведеному прикладі дозволяються вхідні ехо-запити, що дозволяє користувачам мережі перевіряти комп'ютер щодо визначення чи він в мережі. Це дає можливість відслідковувати, наскільки швидко передається інформація до комп'ютера і від нього.

**Завдання на виконання лабораторної роботи**

1. Перевірити працездатність операційної системи Windows ПЕОМ користувача на віртуальної машині №1 за допомогою програмного забезпечення **OracleVBox,** у разі необхідності здійснити налаштування її роботи.
2. Перевірити працездатність операційної системи Windows користувача на віртуальної машині №2 за допомогою програмного забезпечення OracleVBox.
3. Перевірити працездатність зв’язку між віртуальними машинами. У разі несправності усунути помилки.
4. Виконати пункти лабораторної роботи та здійснити перевірку роботи брандмауера операційної системи Windows.

**Контрольні питання (відповісти письмово)**

1. Призначення брандмауера операційної системи Windows.
2. Методика налаштування параметрів брандмауера операційної системи Windows на роботу щодо забезпечення доступу до ресурсів комп’ютера.
3. Опишіть основні вхідні та вихідні правила роботи брандмауера операційної системи Windows.
4. Призначення основного та швидкого режиму роботи брандмауера операційної системи Windows.
5. Призначення папки «Наблюдение» брандмауера операційної системи Windows.
6. Методика створення правил роботи брандмауера для програми.
7. Методика створення правил роботи брандмауера для порту.