

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ
Кафедра интеллектуальных информационных технологий

Отчёт по лабораторной работе №6
по дисциплине «Средства и методы защиты информации в
интеллектуальных системах»

Выполнил студент гр. 121701
Мулярчик Д.С.
Проверил
Сальников Д. А.

Минск 2023

Задача:

- 1) Создать папку с общим доступом на одной из виртуальных машин.
- 2) Настроить брандмауэр, применив различные политики:
 - а) доступ к разделяемому ресурсу разрешен только компьютеру с данным IP-адресом;
 - б) доступ к виртуальной машине разрешен только по заданным портам (например, www или ftp);
 - в) доступ к виртуальной машине разрешен только по заданным портам (например, www или ftp) и только компьютерам с данным IP-адресом (адресами);
 - г) доступ к внешним ресурсам разрешен только конкретным программам;
 - д) конкретной программе разрешен доступ к ресурсам удаленного компьютера с данным IP-адресом по заданному порту;
 - е) запретить запрос входящего эха (ICMP).

Реализация:

- а) доступ к разделяемому ресурсу разрешен только компьютеру с данным IP-адресом;

На данном рисунке можно увидеть, что правило может применять как для локальных IP-адресов, так и для удаленных, однако применено только для локальных адресов.

The screenshot shows the Windows Firewall rule configuration window. On the left, a sidebar lists the steps: Шаг 1, Тип правила, Программа, Протокол и порты, Область, Действие, Профиль, and Имя. The 'Область' (Scope) step is currently selected. The main area is titled 'Укажите локальные IP-адреса, к которым применяется данное правило.' (Specify local IP addresses to which this rule applies). Under this title, there are two radio buttons: 'Любой IP-адрес' (Any IP address) and 'Указанные IP-адреса:' (Specified IP addresses:). The 'Указанные IP-адреса:' option is selected. Below it, a text box contains the IP addresses '192.168.32.17' and '192.168.32.18'. To the right of the text box are three buttons: 'Добавить...' (Add...), 'Изменить...' (Change...), and 'Удалить' (Remove). Below the IP address section, there is a section for interface types with the title 'Настройка типов интерфейсов, к которым применимо данное правило:' (Configure interface types to which this rule applies). Under this title, there are two radio buttons: 'Любой IP-адрес' (Any IP address) and 'Указанные IP-адреса:' (Specified IP addresses:). The 'Любой IP-адрес' option is selected. Below it is an empty text box for specifying remote IP addresses. To the right of this text box are three buttons: 'Добавить...' (Add...), 'Изменить...' (Change...), and 'Удалить' (Remove). At the bottom right of the main area is a 'Настроить...' (Configure...) button.

- б) доступ к виртуальной машине разрешен только по заданным портам (например, www или ftp):

Допустим у нас есть в распоряжении порты начиная с 5000 до 5010. На рисунке можно увидеть, что мы ввели ограничения для портов с 5000-5008 и оставив для входа порты 5009 и 5010.

Шаги:

- Тип правила
- Протокол и порты
- Действие
- Профиль
- Имя

Укажите протокол, к которому будет применяться это правило.

☒ **Протокол TCP**
☐ **Протокол UDP**

Применять это правило ко всем удаленным портам или только к определенным удаленным портам?

☐ **Все удаленные порты**
☒ **Определенные удаленные порты:**

Пример: 80, 443, 5000-5010

На рисунке ниже можно увидеть, что мы можем неким портам как разрешить подключение, так и блокировать подключение.

Шаги:

- Тип правила
- Протокол и порты
- Действие
- Профиль
- Имя

Укажите действие, которое должно выполняться, когда подключение удовлетворяет указанным условиям.

☒ **Разрешить подключение**
 Включая как подключения, защищенные IPSec, так и подключения без защиты.

☐ **Разрешить безопасное подключение**
 Включая только подключения с проверкой подлинности с помощью IPSec. Подключения будут защищены с помощью параметров IPSec и правил, заданных в разделе правил безопасности подключений.

☐ **Блокировать подключение**

в) доступ к виртуальной машине разрешен только по заданным портам (например, www или ftp) и только компьютерам с данным IP-адресом (адресами);

Настраиваем ip-address

Шаги:

- Тип правила
- Программа
- Протокол и порты
- Область**
- Действие
- Профиль
- Имя

Укажите локальные IP-адреса, к которым применяется данное правило.

☐ Любой IP-адрес

☒ Указанные IP-адреса:

192.168.32.17 Добавить...

Изменить...

Удалить

Настройка типов интерфейсов, к которым применимо данное правило: Настроить...

Укажите удаленные IP-адреса, к которым применяется данное правило.

☒ Любой IP-адрес

☐ Указанные IP-адреса:

Добавить...

Изменить...

Удалить

Выбираем параметры подключения

Шаги:

- Тип правила
- Программа
- Протокол и порты
- Область
- Действие**
- Профиль
- Имя

Укажите действие, которое должно выполняться, когда подключение удовлетворяет указанным условиям.

☒ **Разрешить подключение**
Включая как подключения, защищенные IPSec, так и подключения без защиты.

☐ **Разрешить безопасное подключение**
Включая только подключения с проверкой подлинности с помощью IPSec. Подключения будут защищены с помощью параметров IPSec и правил, заданных в разделе правил безопасности подключений.

Настроить...

☐ **Блокировать подключение**

Настраиваем порт

Шаги:

- Тип правила
- Протокол и порты
- Действие**
- Профиль
- Имя

Укажите протокол, к которому будет применяться это правило.

☒ **Протокол TCP**

☐ **Протокол UDP**

Применять это правило ко всем удаленным портам или только к определенным удаленным портам?

☐ Все удаленные порты

☒ **Определенные удаленные порты:**

Пример: 80, 443, 5000-5010

г) доступ к внешним ресурсам разрешен только конкретным программам;

Шаг:

- Тип правила
- Программа
- Действие
- Профиль
- Имя

Применять это правило ко всем программам или к определенной программе?

☐ **Все программы**
Правило применяется ко всем подключениям компьютера, отвечающим другим свойствам правила.

☒ **Путь программы:**
D:\OBS-Studio-29.1.3-Full-Installer-x64.exe Обзор...

Пример: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Шаг:

- Тип правила
- Программа
- Действие
- Профиль
- Имя

Укажите действие, которое должно выполняться, когда подключение удовлетворяет указанным условиям.

☒ **Разрешить подключение**
Включая как подключения, защищенные IPSec, так и подключения без защиты.

☐ **Разрешить безопасное подключение**
Включая только подключения с проверкой подлинности с помощью IPSec. Подключения будут защищены с помощью параметров IPSec и правил, заданных в разделе правил безопасности подключений.

Настроить...

☐ **Блокировать подключение**

Для каких профилей применяется правило?

☒ **Доменный**
Применяется при подключении компьютера к домену своей организации.

☐ **Частный**
Применяется, когда компьютер подключен к частной сети, например дома или на работе.

☐ **Публичный**
Применяется при подключении компьютера к общественной сети.

е) запретить запрос входящего эха (ICMP).

Шаги:

- Тип правила
- Программа
- Протокол и порты
- Область
- Действие
- Профиль
- Имя

Укажите порты и протоколы, к которым применяется это правило.

Тип протокола: ICMPv4

Номер протокола: 1

Локальный порт: Все порты

Пример: 80, 443, 5000-5010

Удаленный порт: Все порты

Пример: 80, 443, 5000-5010

Параметры протокола ICMP:

Настроить...

Настройка параметров ICMP

Применять это правило к следующим подключениям по протоколу ICMP:

☐ Все типы ICMP

☒ Определенные типы ICMP

- ☐ Пакет слишком велик
- ☐ Объект назначения недоступен
- ☐ Понижение скорости источником
- ☐ Перенаправить
- ☒ Эхо-запрос
- ☐ RA (Router Advertisement)
- ☐ Запрос маршрута
- ☐ Превышено время
- ☐ Ошибка параметра
- ☐ Запрос отметки времени
- ☐ Запрос маски адреса

Тип ICMP:

Тип: 0

Код: Любой

Добавить