**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**Лабораторная работа № 2**

на тему «Блокировка сетевых соединений: политика IP-безопасности,

брандмауэр Windows»

|  |
| --- |
| Выполнил: студент группы ВКБ43 |
| Ковалев Данил Петрович |
| (Фамилия, имя, отчество) |
| Проверил: доцент |
| Скляров Алексей Викторович |
| (Фамилия, имя, отчество) |

## **Цель:**

* Изучить способы создания локальных учетных записей пользователей и групп и настройки их свойств;
* Изучить возможности настройки локальных политик безопасности для установки требований к паролям и учётным записям, блокировки нежелательных программ и сетевых соединений.

**Ход выполнения работы:**

**Задание № 2.** Настроить две виртуальные машины Virtual Box, которые будут находиться в 1 рабочей группе и имеющие общую маску подсети.

Для выполнения лабораторной работы было создано 2 виртуальные машины на основе Windows 10, так как на момент 2025 года тяжело достать образы таких старых операционных систем. На рисунке 1 представлены 2 виртуальные машины.

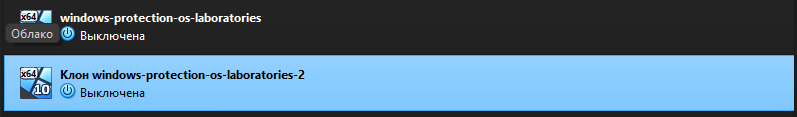


Рисунок 1 – созданные 2 виртуальные машины

Теперь перейдем к настройке виртуальных машин, для 1 первой виртуальной машины настроем адаптер NAT. Обязательно нужно выбрать, чтобы был подключен виртуальный кабель. Настройка представлена на рисунке 2.

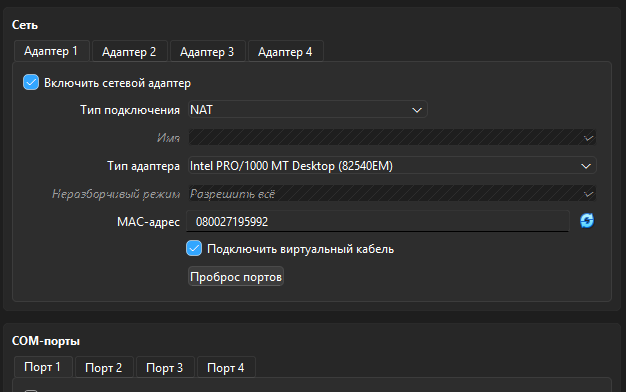


Рисунок 2 – настройка “Адаптер 1” для 1 виртуальной машины

Теперь перейдем к настройке “Адаптер 2”, выбрав режим “Внутренняя сеть”. Конфигурация представлена на рисунке 3.

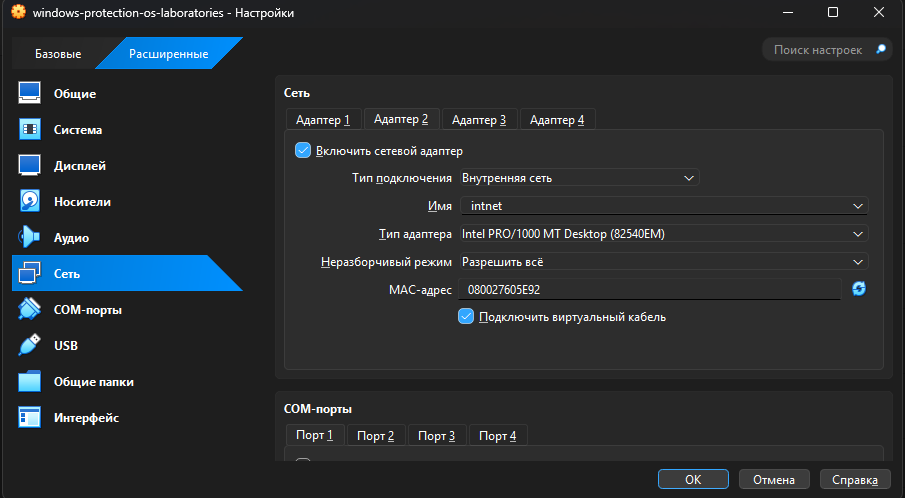


Рисунок 3 – настройка “Адаптер 2” для 1 виртуальной машины

Теперь остается настройке второй виртуальной машины, здесь нам требуется тоже выбрать “Внутренняя сеть”, но только для “Адаптер 1”. Конфигурация представлена на рисунке 4.

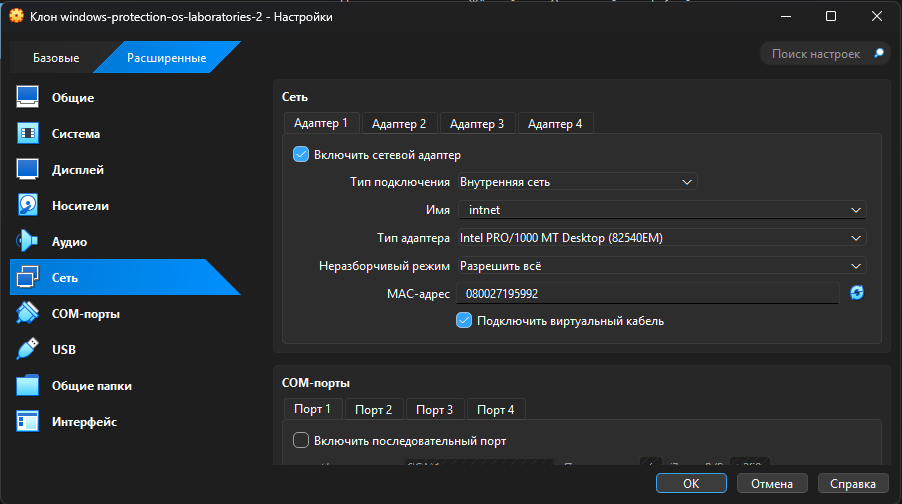


Рисунок 4 – настройка “Адаптер 1” для 2 виртуальной машины

Теперь настроим сетевые адаптеры в самих операционных системах. Для этого в случае Windows надо открыть данный гайд - <https://2kom.ru/for_subscribers/instruction/instruction_internet/134/> - и выполнить все до 9 пункта, а потом вставить данные, которые представлены в методическом материале. Настройка представлена на рисунке 5.

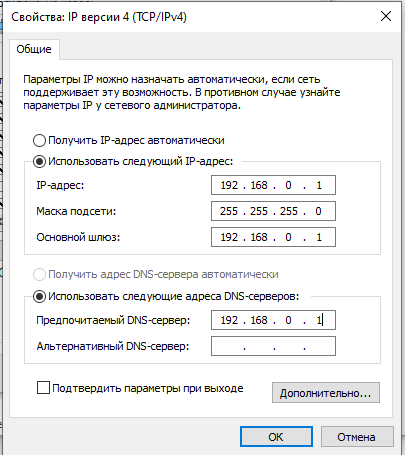


Рисунок 5 – настройка сети для 1 виртуальной машины

Теперь произведем настройку сети для 2 виртуальной машины, настройка представлена на рисунке 6.

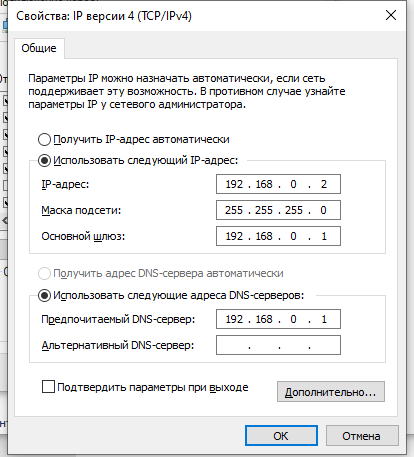


Рисунок 6 – настройка сети для 2 виртуальной машины

После удачной настройки в Windows должно вылететь уведомление, чтобы машины подключились к общей сети, данное уведомление будет справа. На двух машинах нужно будет дать согласие, чтобы все корректно работало.

После проведения указанных действий нужно теперь проверить работоспособность локальной сети с использованием консольной команды ping и убедиться в появлении компьютеров локальной сети в папках «Сетевое окружение» обоих виртуальных ОС. Для этого с виртуальной машины 2 сделаем запрос на виртуальную машину 1. В моем случае ping не доходил до обоих машин, что говорит нам о том, что методический материал является уже неактуальным.

В следствии этого, нам нужно будет поменять настройки сети виртуальных машин. В нашем случае для распределения доступа к сети буду использовать иную настройку, в которой будет использовать NAT Network. Конфигурация была взята с видео по ссылке - <https://youtu.be/DzmUOeFdc-w?si=9FKRXZaI4GryfNuR>.

Теперь проверим, что для обоих ПК есть возможность сделать ping запросы. Результат ping со 2 виртуальной машины на 1 представлен на рисунке 7.

Изображение выглядит как текст, электроника, компьютер, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 7 – пинг с 2 машины на 1

**Задание 2.1.** Блокировка сетевых соединений.

Создадим локальную политику безопасности для первой виртуальной машины. Для этого переходим в “Локальная политика безопасности”, набрав все в нижней панели. Само приложение и начальный этап создания политики представлен на рисунке 8.

Изображение выглядит как текст, снимок экрана, программное обеспечение, компьютер

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 8 – создание политики IP – безопасности

Теперь выполним настройку, как предложено в методическом материале. Создадим просто политику с названием “Политика 1”, добавим к ней описание, как предложено в методическом материале. Конфигурация представлена на рисунке 9.

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 9 – задание имя политики

Выставим также правила, как и предложено в методическом материале. Конфигурация представлена на рисунке 10.

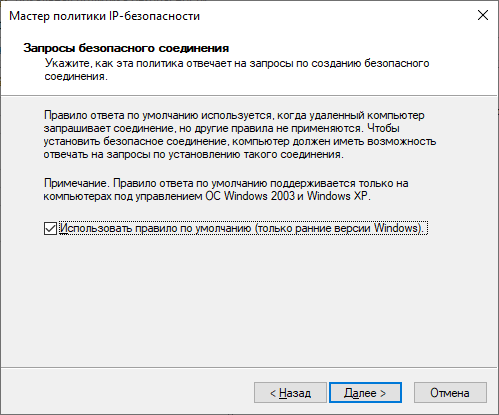


Рисунок 10 – правила по умолчанию для запросов

Теперь выберем настройку безопасности, используя протокол Kerberos. Kerberos - это сетевой протокол аутентификации, который позволяет безопасно идентифицировать пользователей и узлы в незащищенных сетях. Он действует как доверенная третья сторона, используя симметричную криптографию для выдачи "билетов" (тикеты) пользователям и серверам, подтверждающих их подлинность и обеспечивающих взаимное подтверждение личности. Конфигурация была сделана, как в методическом материале и представлена на рисунке 11.

В моем случае после настройки вылетело предупреждение, что может быть неактивно, мы должны автоматически согласиться. Чтобы все было нормально.

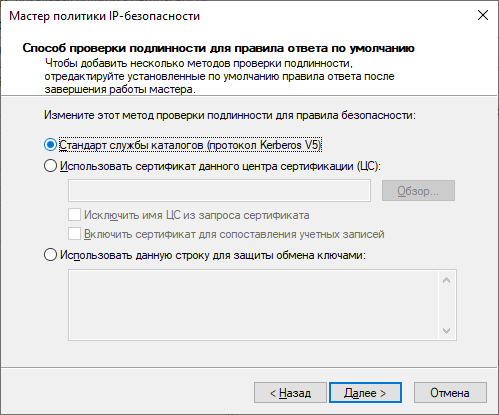


Рисунок 11 – настройка политики с использованием протокола Kerberos

В конце нас встретит фото, что нужно завершить настройку работы мастера. Результат представлен на рисунке 12.

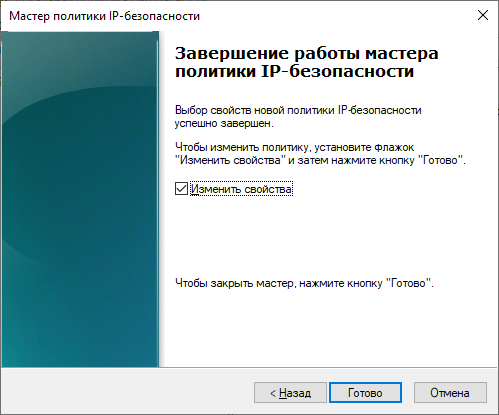


Рисунок 12 – завершение работы мастера политики

Теперь у нас открывается окно «Мастера создания новых правил IP-безопасности». В настройках «Конечная точка туннеля» нужно оставить значение по умолчанию «Это правило не определяет туннель», в «Тип сети» также оставить значение по умолчанию «Все сетевые подключения». На следующем шаге появится окно «Список IP-фильтров», которое по умолчанию пусто, т.к. ни одного списка еще добавлено не было. В моем случае я задал имя и описание. Конфигурация представлена на рисунке 13.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 13 – конфигурация списка IP - фильтров

Теперь произведем настройку, как предложено в методическом материале. В нашем случае только будет иной IP, потому что указания 2 для методического материала неактуальны для последней версии Virtual Box.

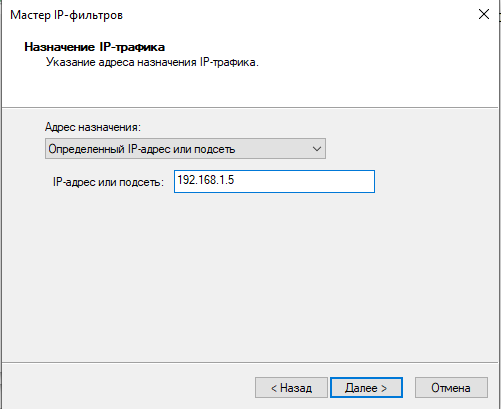


Рисунок 14 – назначение адреса назначения для 2 виртуальной машины

Теперь настроим действия фильтра, для выполнения данных целей нам нужно в приложении “Список IP-фильтров” выбрать фильтр и нажать “ОК”, после этого у нас откроется отдельное приложение, как представлено на рисунке 15.

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 15 – мастер правил безопасности

В результате вышло то, что представлено на рисунке 16.

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 16 – политика 1

Теперь, чтобы политика начала работать, нужно нажать в приложении “Локальная политика безопасности” на “Политика 1” с помощью ПКМ, а потом выбрать с помощью ЛКМ “Назначить”. Когда политика применилась, то будет все то же самое, как на рисунке 17.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 17 – результат настройки политики 1

Теперь попробуем проверить работоспособность нашей политики, попытавшись сделать запрос на другую виртуальную машину. Произведем в начале попытку с 1 виртуальной машины сделать запрос на 192.168.1.5. В результате получим то, что представлено на рисунке 18.

Изображение выглядит как текст, снимок экрана, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 18 – попытка сделать ping с 1 виртуальной машины на 2

**Задание 2.2.** Блокировка сетевых соединений: Брандмауэр Windows.

Для выполнения данной части лабораторной работы необходимо деактировать политики IP-безопасности, созданные при выполнении предыдущего задания. Для этого заходим обратно в “Локальная политика безопасности”.

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 19 – отмена политики

Теперь наша задача на виртуальной машине 1 создать папку и выдать доступ всем на просмотр.

Изображение выглядит как природа, на открытом воздухе, геология, пещера

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 20 – создание папки для задания

Теперь предоставим общий доступ к директории. Для этого с помощью ПКМ заходим в свойства -> доступ -> общий доступ, а дальше выбираем “Все”. В результате вышло то, что представлено на рисунке 21.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 21 – настройка доступа к сети к папке на 1 виртуальной машине

Теперь остается настроить расширенный доступ, указав, чтобы все видели директорию. Настройка представлена на рисунке 22.

Изображение выглядит как текст, снимок экрана, дисплей, число

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 22 – параметры расширенной настройки

Теперь проверим, что директория видна в сети, результат представлен на рисунке 23. Индикатор брандмауэра показывает его состояние, по умолчанию включен.

Изображение выглядит как текст, Прямоугольник, дизайн, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 23 – Lab3-Win10

Теперь на виртуальной машине 1 включим брандамуэр. Для этого делаем пуск > панель управления > Брандмауэр Windows (в поиске). Теперь мы должны выключить то, что представлено на рисунке 24.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 24 – отключение общего доступа к файлам

Теперь для виртуальной машины 2 попробуем подключиться. В моем случае даже с виртуальной машины 1 не видно. На рисунке 25 представлен результат.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 25 – вывод настройки отображения сети

Теперь с виртуальной машиной 1 включить компонент «Общий доступ к файлам и принтерам» и нажать кнопку «OК», проверить доступность папки Lab3\_Win10, сделать скриншот результата, объяснить его. На рисунке 26 представлен корректный результат. Если не будет видно так в сети, то нужно выполнить WIN + R и вставить туда путь к папке.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 26 - результат отображения при включении брандмауэра

**Задание 3.** Блокирование исходящего трафика.

Для блокирования исходящего трафика необходимо нажать ссылку «Дополнительные параметры» в окне брандмауэра. Откроется окно «Брандмауэр Windows в режиме повышенной безопасности», в котором необходимо нажать кнопку «Свойства». В открывшемся окне свойств перейти на вкладку с настройками общественной сети (общественная сеть > общий профиль). В разделе Исходящие подключение из выпадающего меню выбирать «Блокировать» и нажать кнопку «ОК» (или «Применить» > «ОК»). После нажатия конпки «ОК» произойдет переход в окно «Брандмауэр Windows в режиме повышенной безопасности», в котором необходимо нажать кнопку «обновить». Настройка представлена на рисунке 27.

Изображение выглядит как текст, снимок экрана, компьютер, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 27 – свойства монитора браундмауэра

Используя консольную команду ping проверим, что брандмауэр защищает. Если в результате пинга весь трафик проходит, то нужно сбросить и настройки и заново включить. Результат представлен на рисунке 28.

Изображение выглядит как текст, электроника, компьютер, снимок экрана

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 28 - неудачная попытка установить соединение с VM1

**Задание 4.** Создания правил разрешения для программ

После блокирования исходящих подключений необходимо настроить правила доступа для конкретных программ, например, браузеру Internet Explorer, являющемуся браузером по умолчанию в ОС Windows. Для этого необходимо перейти в левой части окна «Брандмауэр Windows в режиме повышенной безопасности» на ссылку «Правила для исходящего подключения» и в колонке «Действия» нажать кнопку «Создать правило…». Интерфейс для настройки представлен на рисунке 29.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 29 – интерфейс для создания нового правила

Откроется окно мастера создания правила для нового исходящего подключения, выбирать «Для программы»> «Далее». Интерфейс представлен на рисунке 30.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 30 – выбор пункта для программы

C помощью кнопки «Обзор…» указать путь к программе, для которой создается правило (Internet Explorer (C:\Program Files\Internet Explorer\iexplore.exe)) и нажать кнопку «Далее». Результат выбора представлен на рисунке 31.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 31 – путь к программе

На следующем шаге необходимо выбрать «Разрешить подключение»> «Далее». Выбор данного пункта представлен на рисунке 32.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 32 – разрешить подключение

После нажатия кнопки «Далее» необходимо определить для каких профилей данное правило будет применяться (профиль «Публичный»> «Далее») и указать имя и описание правила, нажать «Готово». Конфигурация представлена на рисунке 33.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 33 – выбор профиля

После настройки правила для браузера проверяем, что работает хорошо. Результат представлен на рисунке 34.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 34 – результат отображения для браузера

**Задание 5.** Разрешения для служб и системных программ Windows

Далее, на примере службы «Обновление Windows», показано, как создать правило для системных служб Windows. Что бы предоставить доступ в интернет службе «Обновление Windows» необходимо выполнить шаги, которые представлены ниже.

Нужно создать настраиваемое правило (перейти в левой части окна «Брандмауэр Windows в режиме повышенной безопасности» на ссылку «Правила для исходящего подключения» и в колонке «Действия» нажать кнопку «Создать правило…»). Выбор представлен на рисунке 35.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 35 – создание настраиваемого правила

Теперь указываем путь к программе %SystemRoot%\System32\svchost.exe, так как обновление ОС выполняется этим процессом. Конфигурация представлена на рисунке 36.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 36 – конфигурация для пути к программе

Теперь в разделе службы нажимаем «Настроить…», в появившемся окне выбирать «Применять к службе» и в списке выделить «Центр обновления Windows (краткое имя — wuauserv)», нажать ОК. Результат представлен на рисунке 37.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 37 – параметры для процесса

После нажатия кнопки «Далее» появится окно с предупреждением о возможных конфликтах при работе системы, нажать «Да». Результат представлен на рисунке 38.

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 38 – подтверждение настроек

В окнах «Протоколы и порты», «Область» оставить значения по умолчанию. В окне «Действие» выбрать «Разрешить подключение» > «Далее».

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 39 – параметры для разрешения подключения

В окне профиль выбрать все профили сетевого подключения (Доменный, частный, Публичный). Результат настройки представлен на рисунке 40.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 40 – настройки профиля

В окне «Имя» указать имя и описание правила, нажать «Готово». В результате должно выйти то, что представлено на рисунке 41.

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 41 – имя для правила

**Задание 6.** Создание разрешений для системных команд

Далее, на примере системной команды ping, показано, как создать правило для системных команд Windows. На предыдущем этапе рассматриваемой лабораторной работы было осуществлено блокирование всего исходящего трафика и попытки «пропинговать» ПК под управлением завершались неудачей. Результат представлен на рисунке 42.

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 42 – запрос к 192.168.100.4

Что бы разрешить взаимодействие ПК – VM1, так и VM2, по локальной сети необходимо выполнить следующие действия.

Нам нужно создать предопределенное правило (перейти в левой части окна «Брандмауэр Windows в режиме повышенной безопасности» на ссылку «Правила для исходящего подключения» и в колонке «Действия» нажать кнопку «Создать правило…», из выпадающего списка выбирать «Общий доступ к файлам и принтерам»> «Далее»). Выбор представлен на рисунке 43.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 43 – выбор предопределенных правил

В разделе «Правила» выбрать «Общий доступ к файлам и принтерам (эхо-запрос — исходящий трафик ICMPv4)» и нажать «Далее». Выбор конфигурации представлен на рисунке 44.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 44 – настройка доступа к файлам

В окне «Действие» выбрать «Разрешить подключение»> «Готово». Выбор параметра представлен на рисунке 45.

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 45 – создание правила

После настройки правила для служебной программы ping проверить его наличие в окне правил для исходящего подключения, проверить работоспособность («пропинговать» ПК под управлением Windows XP), сделать скриншот.

Изображение выглядит как текст, снимок экрана, компьютер, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Рисунок 46 - успешная попытка эхо-запроса на хост 192.168.0.2

**Контрольные вопросы**

1. Что такое политики IP-безопасности?

Политики IP – безопасности – это набор правил и фильтров, которые контролируют (ограничивают или разрешают) различные формы взаимодействия устройств в сети.

1. Для чего предназначен межсетевой экран?

Программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

1. Какие наиболее распространенные типы атак на сети TCP/IP известны?

Атаки на сетевом уровне (IP)

Эти атаки эксплуатируют недостатки протокола IP, в частности отсутствие встроенной аутентификации и шифрования.

* IP-спуфинг (IP Spoofing):
  + Суть: Злоумышленник подделывает IP-адрес источника в заголовке пакета, чтобы выдать себя за доверенную систему. Это основа для многих других атак.
  + Цель: Обход списков контроля доступа (ACL), основанных на IP-адресах, проведение атак типа "отказ в обслуживании" (DoS).
* Smurf-атака (устарела, но принцип важен):
  + Суть: Атакующий отправляет ICMP-пакеты (ping) с поддельным IP-адресом жертвы на широковещательный адрес сети. Все устройства в сети отвечают жертве, перегружая ее трафиком.
  + Цель: Отказ в обслуживании (DoS).
* ICMP-атаки:
  + Суть: Злоупотребление протоколом ICMP. Например, *ICMP Redirect* для перенаправления трафика через себя (атака "человек посередине") или *ICMP Echo Request (Ping)* для сканирования сети и проведения DoS-атак (Ping of Death — сейчас неактуальна из-за патчей).

Атаки на транспортном уровне (TCP/UDP)

Эти атаки нацелены на механизмы установления соединения и его поддержания.

* TCP SYN Flood (Полуоткрытая атака):
  + Суть: Атакующий отправляет жертве множество запросов на установление TCP-соединения (пакеты с флагом SYN), но не завершает handshake (не отправляет ACK). Сервер тратит ресурсы на ожидание и, в конечном итоге, перестает принимать новые соединения.
  + Цель: Отказ в обслуживании (DoS/DDoS).
* TCP Hijacking (Перехват сессии):
  + Суть: Атакующий, работающий "посередине", предсказывает или перехватывает номера последовательностей (sequence numbers) TCP-пакетов. Это позволяет ему "встроиться" в установленное соединение между двумя узлами и перехватить его.
  + Цель: Кража данных, получение несанкционированного доступа.
* UDP Flood:
  + Суть: Аналогична SYN Flood, но для протокола UDP. Атакующий отправляет на случайные порты жертвы множество UDP-пакетов. Система пытается найти приложение, работающее на этом порту, и в ответ генерирует пакет "Destination Unreachable". Большой объем такого трафика перегружает систему.
  + Цель: Отказ в обслуживании (DoS/DDoS).

Атаки на уровне приложений

Эти атаки нацелены на уязвимости в конкретных приложениях и сервисах (веб-серверы, DNS, почта).

* DNS-спуфинг / DNS Cache Poisoning (Отравление DNS-кэша):
  + Суть: Атакующий подделывает ответ от DNS-сервера, заставляя его сохранить в своем кэше неверную запись (например, сопоставить доменное имя example.com с IP-адресом злоумышленника). Все пользователи этого DNS-сервера будут перенаправлены на фальшивый сайт.
  + Цель: Фишинг, перехват трафика.
* HTTP-атаки:
  + Суть: Это огромный класс атак, включающий SQL-инъекции, XSS (Межсайтовый скриптинг), CSRF (Подделка межсайтовых запросов) и многие другие. Они exploit уязвимости в веб-приложениях, а не в самом протоколе HTTP, но используют его как транспорт.

1. На каком уровне модели OSI используется протокол IPSec?

Протокол IPSec работает на сетевой уровне модели OSI.

1. Какие протоколы включены в состав протокол IPsec?

Ядро IPsec составляют три протокола [3]:

* ***Authentication Header (АН)*** обеспечивает целостность передаваемых данных, аутентификацию источника информации и функцию по предотвращению повторной передачи пакетов.
* ***Encapsulating Security Payload (ESP)*** обеспечивает конфиденциальность (шифрование) передаваемой информации, ограничение потока конфиденциального трафика. Кроме этого, он может исполнять функции AH: обеспечить целостность передаваемых данных, аутентификацию источника информации и функцию по предотвращению повторной передачи пакетов. При применении ESP в обязательном порядке должен указываться набор услуг по обеспечению безопасности: каждая из его функций может включаться опционально.
* ***Internet Security Association and Key Management Protocol (ISAKMP)*** — протокол, используемый для первичной настройки соединения, взаимной аутентификации конечными узлами друг друга и обмена секретными ключами. Протокол предусматривает использование различных механизмов обмена ключами, включая задание фиксированных ключей, использование таких протоколов, как Internet Key Exchange, Kerberized Internet Negotiation of Keys (RFC 4430) или записей DNS типа IPSECKEY (RFC 4025).

1. По каким признакам можно классифицировать межсетевые экраны?

Различают следующие типы межсетевых экранов:

1. управляемые коммутаторы (канальный уровень);
2. сетевые фильтры (сетевой уровень);
3. шлюзы сеансового уровня (circuit-level proxy);
4. посредники прикладного уровня;
5. инспекторы состояния (stateful inspection), представляющие собой межсетевые экраны сеансового уровня с расширенными возможностями.