МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В. И. Ульянова (ЛЕНИНА)
Кафедра информационной безопасности

ОТЧЕТ

по лабораторной работе №6

по дисциплине «Компьютерные сети»

Тема: Доступ к ресурсам удаленной корпоративной сети

Студентки гр. 1361 _____ Токарева У.В.
_____ Галунина Е.С.
_____ Горбунова Д.А.
Преподаватель _____ Горячев А.В.

Санкт-Петербург
2024

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

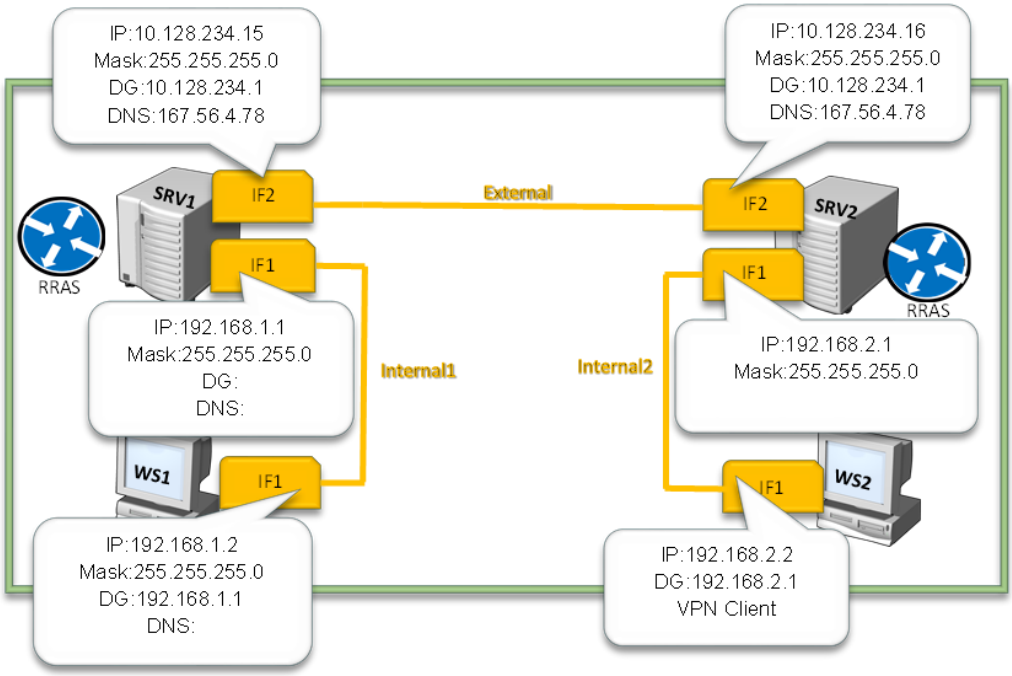


Рисунок 1 – Конфигурация стенда

ХОД РАБОТЫ

Доступ к ресурсам удаленной корпоративной сети.

1. Запустить две виртуальные машины (сервер и клиент). Убедиться с помощью программы Ping, что сервер доступен с клиентского компьютера.

2. Убедиться, что на сервере (SEV1) установлен анализатор пакетов (add/remove program – windows component – network monitor). Убедиться, что на обоих компьютерах отключен межсетевой экран.

3. Выключить на сервере RRAS.

4. Все действия контролировать сетевым анализатором на сервере. Будьте внимательны: периодически придется переключать сетевой анализатор на прием пакетов с внешнего интерфейса, и обратно.

Доступ к сети с помощью терминального сервиса.

1. Включаем на сервере удаленный доступ к рабочему столу, для чего в панели «свойства системы» в закладке «удаленное использование» включаем опция «Включить удаленный доступ к рабочему столу». Разрешение удаленного доступа к серверу показано на рисунке 2.

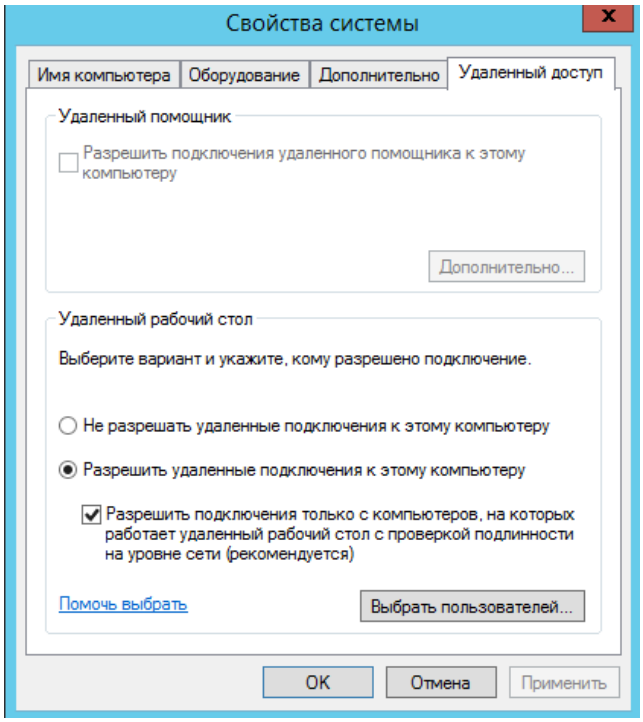


Рисунок 2 – Разрешение удаленного доступа к сервису

2. На WS1 запускаем клиента удаленного доступа (mstsc.exe или находим его в стартовом меню).

3. Раскрываем список параметров («показать параметры»).

4. Указываем адрес компьютера на закладке «общие» («SRV1» или его внутренний IP адрес). Подключение к удаленному рабочему столу представлено на рисунке 3.

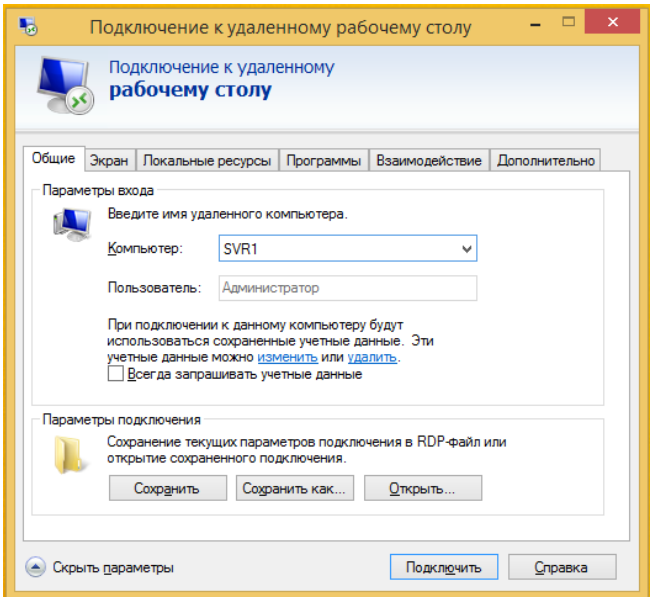


Рисунок 3 – Подключение к удаленному рабочему столу

5. Подключаем диск C:\ клиентского компьютера в закладке «Локальные ресурсы». Доступ SRV1 к диску C на WS1 показан на рисунке 4.

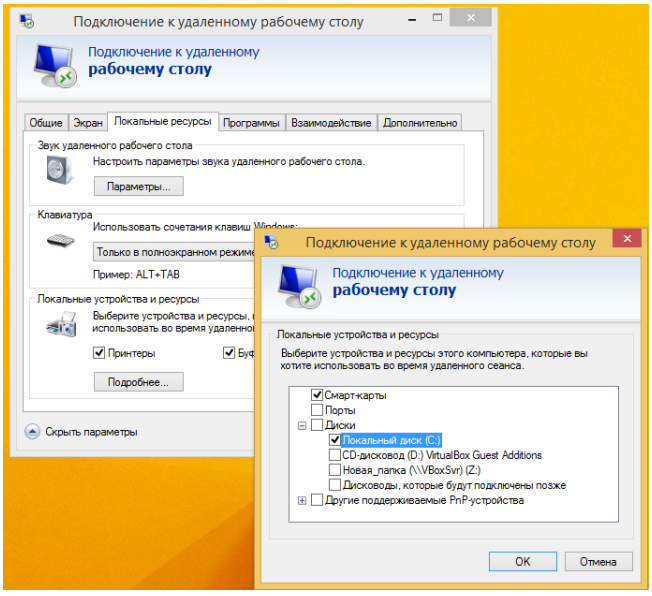


Рисунок 4 – Доступ SRV1 к диску C на WS1

6. Нажимаем клавишу OK и вводим реквизиты администратора сервера. Удаленный рабочий стол показан на рисунке 5.

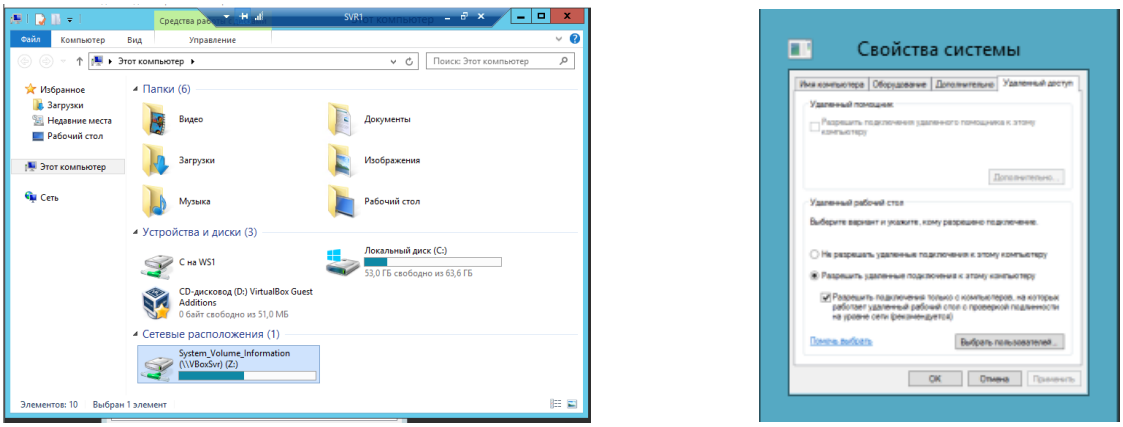


Рисунок 5 – Удаленный рабочий стол

После того, как мы подключились к удаленному рабочему столу SRV1 машины SRV1 и WS1 начали непрерывный обмен пакетами протоколов SSL (с 192.168.1.1 к 192.168.1.2) и RDPUDP (с 192.168.1.2 к 192.168.1.1). Также при совершении каких-либо действий (движение курсора) машины стали обмениваться пакетами протоколов TCP (с 192.168.1.1 к 192.168.1.2) и TLSv1.2 (с 192.168.1.2 к 192.168.1.1).

Протоколы SSL, RDPUDP, TCP, TLSv1.2 представлены на рисунке 6.

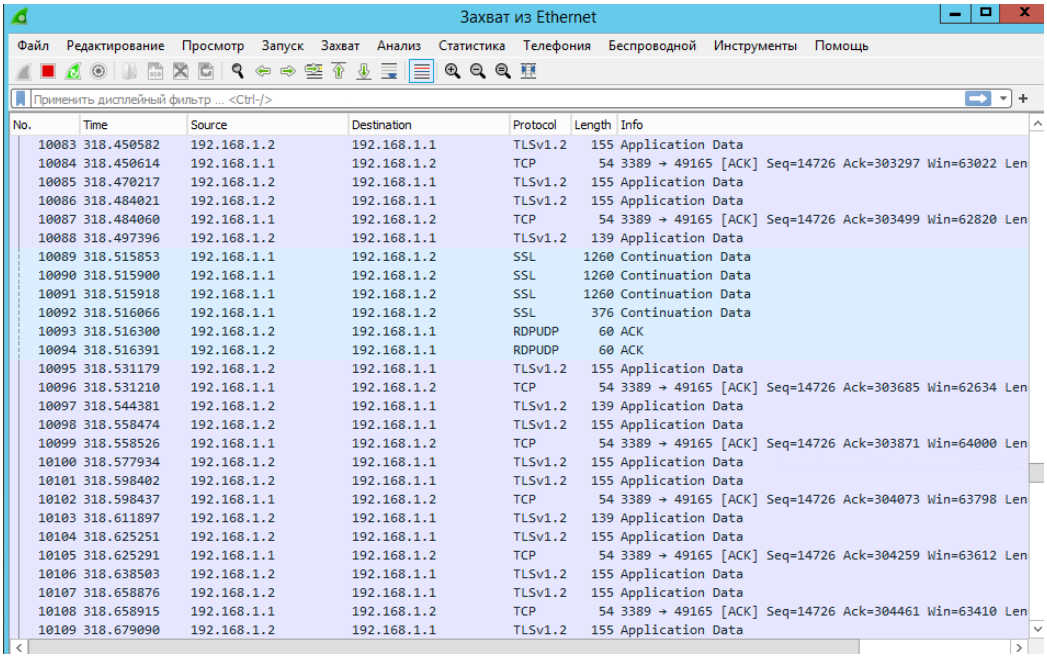


Рисунок 6 – Протоколы SSL, RDPUDP, TCP, TLSv1.2

7. Контролируем появление пользователя «Администратор» после появления рабочего стола сервера в диспетчере задач сервера – рисунок 7.

Рисунок 7 – Появление пользователя «Администратор»

8. Попытаемся подключиться к диску C:\ (\\172.16.0.X\C$) по одному из внешних адресов к серверу коллег, убедимся в возможности скопировать с него какой-либо файл на диск нашей рабочей станции.

На SRV2 на диске C имеется файл TopSecretFile, он показан на рисунке 8.

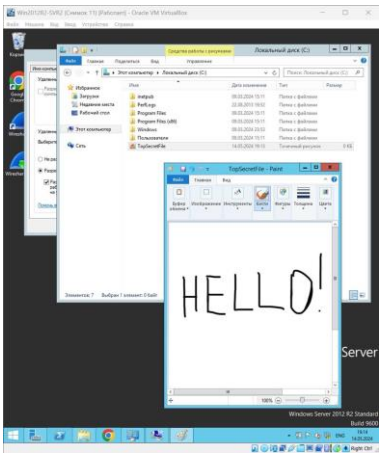
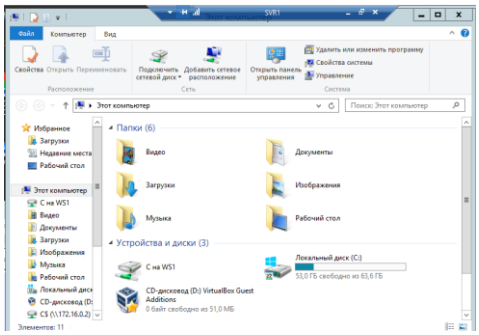


Рисунок 8 – TopSecretFile

Теперь создаем на SRV1 сетевой диск с адресом (\\172.16.0.2\C$) – рисунок 9.



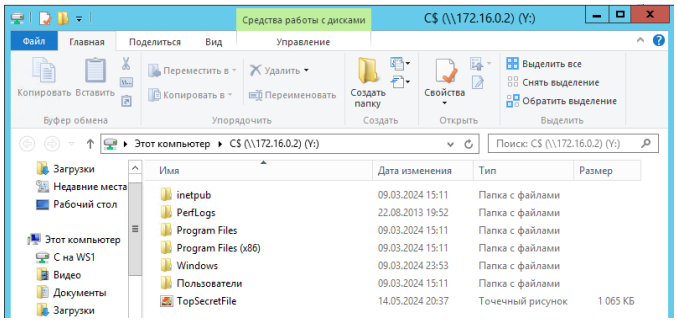


Рисунок 9 – Создание сетевого диска

При создании сетевого диска машины начинают обмениваться пакетами по протоколу SMB2. Причем, никакой информации о том, что действия на SRV1 ведутся через удаленный рабочий стол нет. Обмен пакетами при создании сетевого диска показан на рисунке 10.

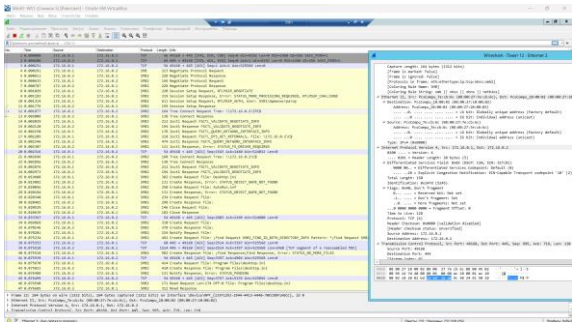


Рисунок 10 – Обмен пакетами при создании сетевого диска

Копируем нужный файл в доступный нам диск С на WS1. Перемещение файла на WS1 показано на рисунке 11.

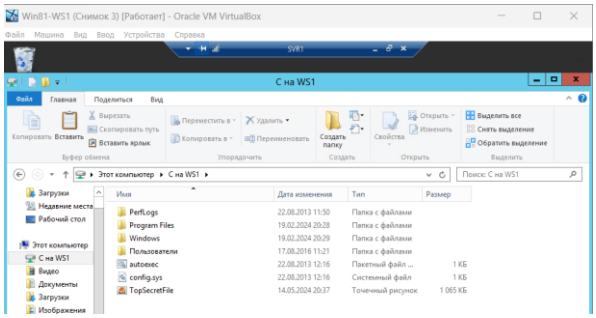


Рисунок 11 – Перемещение файла на WS1

9. Теперь закрываем терминальное соединение. Проверка наличия нового файла на диске С WS1 представлено на рисунке 12.

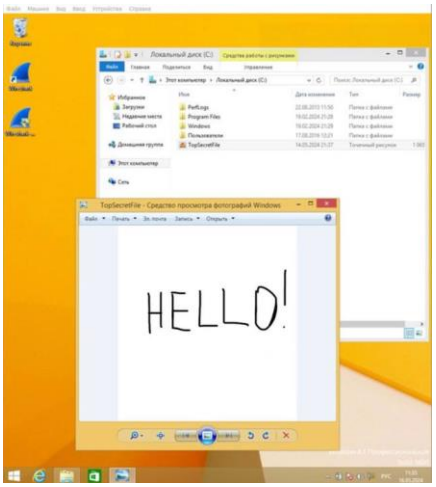


Рисунок 12 – Проверка наличия нового файла на диске С WS1

При закрытии терминального соединения в сети появляются два особых пакета протокола TCP. Закрытие терминального соединения показано на рисунке 13.

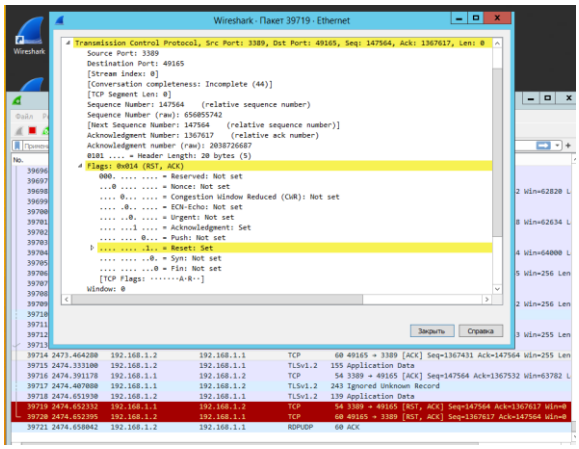


Рисунок 13 – Закрытие терминального соединения

Настройка VPN соединения.

1. Отключаем RRAS на сервере.

2. Включаем RRAS снова, выбираем в визарде пункт «Удаленный доступ (VPN или модем)».

3. Устанавливаем опцию «Доступ к виртуальной частной сети (VPN)». Настройка сети показана на рисунке 14.

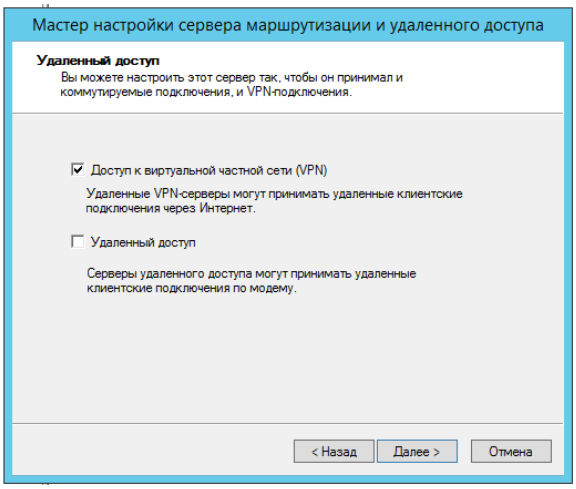


Рисунок 14 – Настройка сети

4. Выбираем в качестве интерфейса, подключенного к Интернету, внутренний интерфейс сервера (192.168…).

5. Задаем из «Заданного диапазона» IP n адрес.

6. Назначаем диапазон 192.168.X.30 – 192.168.X.40. Диапазон адресов показан на рисунке 15.

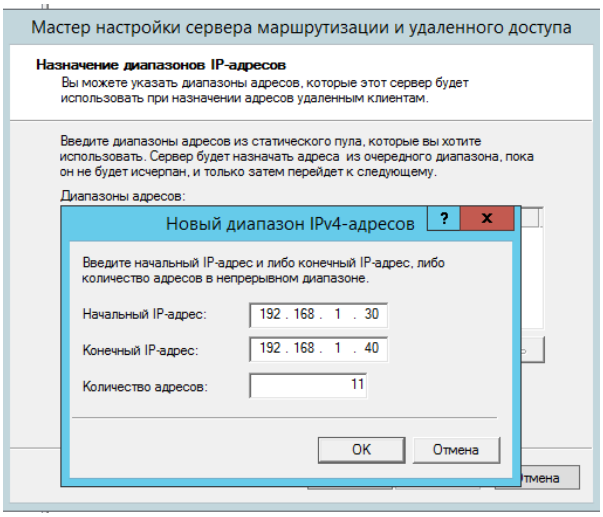


Рисунок 15 – Диапазон адресов

7. Используем для проверки доступа маршрутизацию и удаленный доступ (НЕ RADIUS!).

8. Завершение настройки сети представлено на рисунке 16.

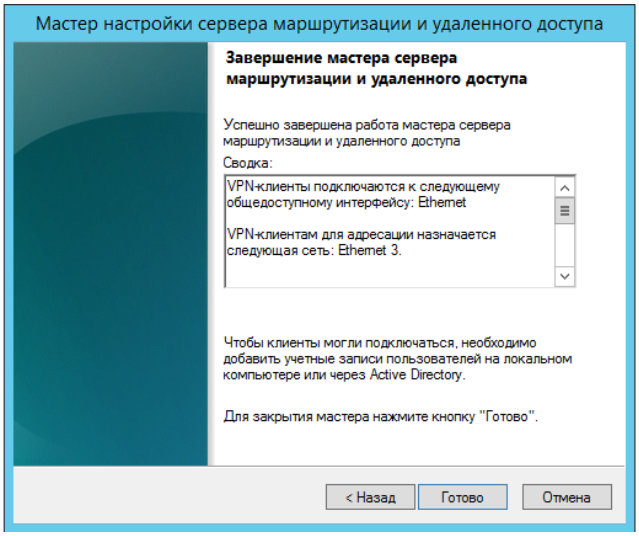


Рисунок 16 – Завершение настройки сети

9. Открываем «Управление компьютером», выбираем пользователя «Администратор», в его свойствах в закладках «Входящие звонки» разрешаем удаленный доступ к VPN. Разрешение удаленного доступа к VPN показано на рисунке 17.

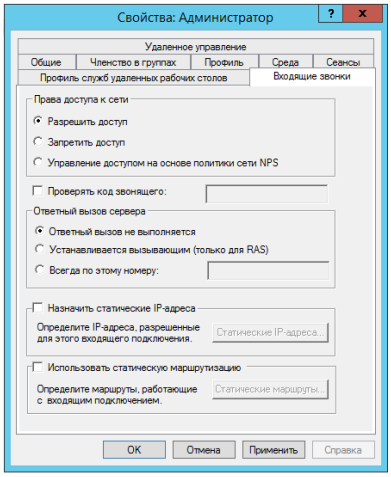


Рисунок 17 – Разрешение удаленного доступа к VPN

10. Переходим на рабочую станцию.

11. В «Сетевых подключениях» запускаем «Мастер новых приключений», выбираем «Подключение к сети на рабочем месте». Подключение к рабочему месту показано на рисунке 18.

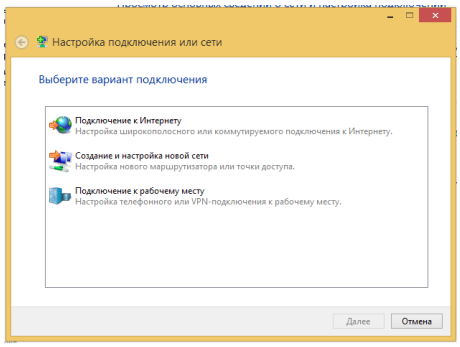


Рисунок 18 – Подключение к рабочему месту

12. Выбираем «Подключение к виртуальной частной сети».

13. Указываем имя сервера (SRV1) или его IP адрес (192.168.X.1) – рисунок 19.

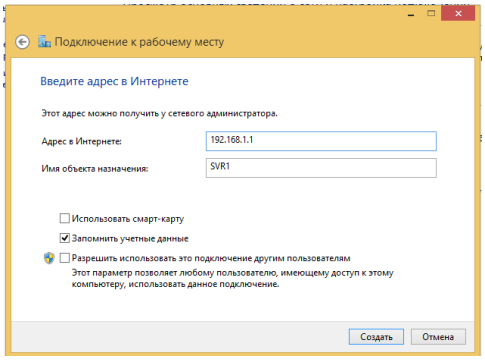


Рисунок 19 – Указание данных сервера

14. Указываем реквизиты администратора сервера в окошке запроса реквизитов.

15. Находим новый отключенный адаптер в окне «Сетевые подключения и открываем его свойства. Создание нового адаптера показано на рисунке 20.

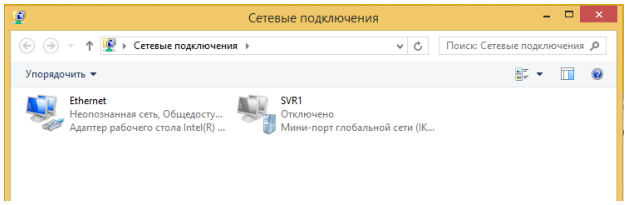


Рисунок 20 – Создание нового адаптера

16. Устанавливаем тип VPN «PPTP VPN» в закладке «Сеть». Настройка типа VPN показана на рисунке 21.

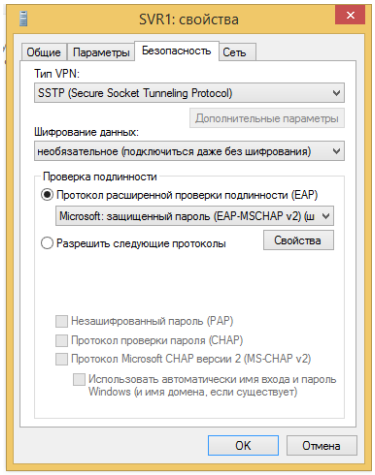


Рисунок 21 – Настройка типа VPN

17. Включаем этот интерфейс. Прохождение аутентификации на WS1 и подключенный интерфейс показаны на рисунке 22 и 23 соответственно.

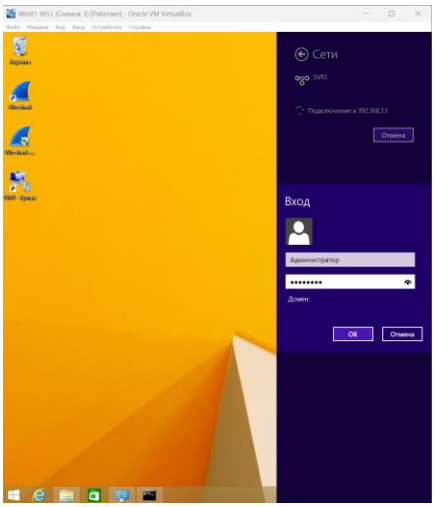


Рисунок 22 – Прохождение аутентификации на WS1

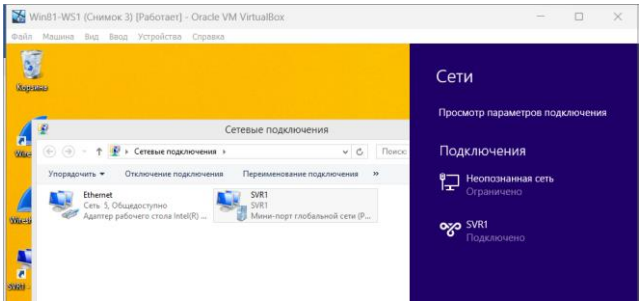


Рисунок 23 – Подключенный интерфейс

18. С помощью команды Ipconfig просматриваем сетевую конфигурацию рабочей станции. Команда Ipconfig -all представлена на рисунке 24.

Рисунок 24 – Команда Ipconfig -all

19. Фиксируем изменения в таблице маршрутизации с помощью Rout Print – рисунок 25.

Рисунок 25 – Команда Round Print

20. Попытаемся получить данные от внешнего (172.16…) интерфейса сервера. Доступ ко внешнему интерфейсу SRV1 с WS1 показан на рисунке 26.

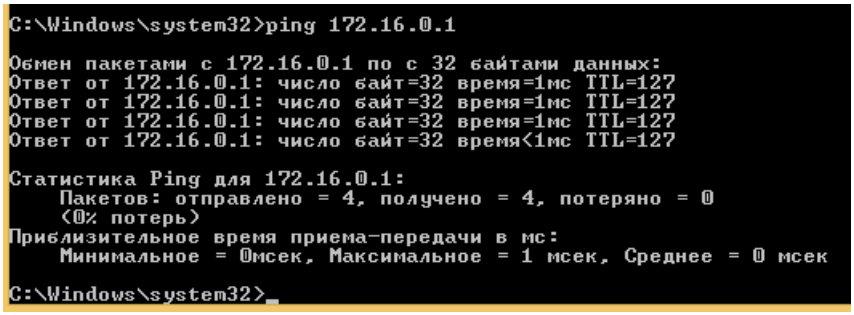


Рисунок 26 – Доступ ко внешнему интерфейсу SRV1 с WS1

21. Фиксируем типы появляющихся пакетов в анализаторе пакетов. В процессе настройки VPN соединения в сети были обнаружены следующие пакеты, представленные на рисунке 27.

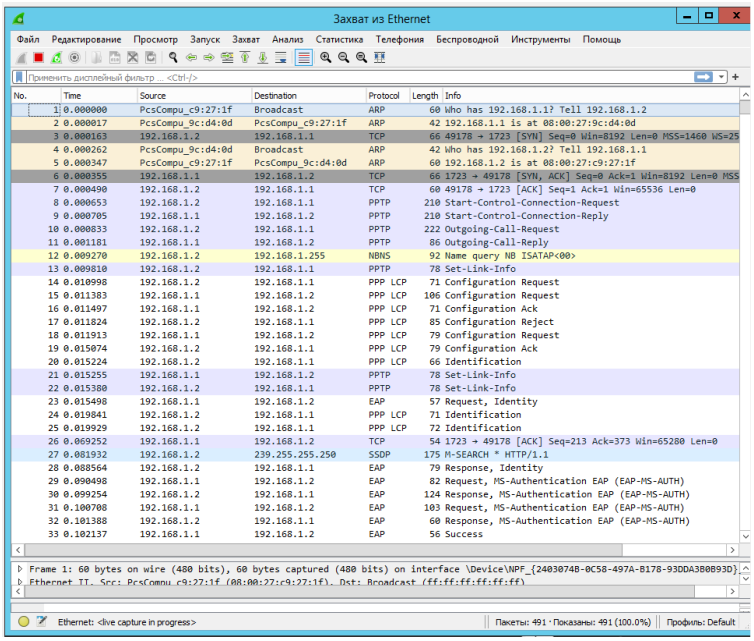


Рисунок 27 – Пакеты настройки VPN соединения

Видно, что для установления VPN-соединения сначала машины обмениваются пакетами протокола TCP для гарантии исправного обмена пакетами через это соединение. Затем с помощью пакетов протокола PPTP данное соединение становится защищенным за счет создания специального туннеля.

После установления туннеля связи идет обмен пакетами протоколов из семейства PPP (Point-to-Point Protocol), EAP (Extensible Authentication Protocol)

и GRE (Generic Routing Encapsulation). Основными целями такого обмена являются обеспечение аутентификации соединения, шифрование и сжатие данных.

ВЫВОД

В ходе выполнения данной лабораторной работы на практике были рассмотрены основные принципы реализации доступа к ресурсам удалённой корпоративной сети при помощи терминального сервиса и путем установления VPN-соединения.

Также рассмотрели основные характеристики составляющих машины, влияющие на возможность реализации того или иного механизма доступа к ресурсам сети. Особое внимание было уделено настройке и применению удалённого доступа к рабочему столу, механизму создания сетевых дисков и подключения к ним и настройке VPN соединения.

Кроме того, познакомились с новыми протоколами, используемыми при реализации VPN-соединения, такими как PPTP, PPP, EAP и GRE, и рассмотрели процесс настройки основных параметров сетевого взаимодействия компьютеров, необходимой для реализации доступа к ресурсам удалённой сети, на конкретном примере и рассмотрели возможности, доступные подключённой к удалённой корпоративной сети рабочей станции.

На протяжении выполнения работы были усвоены знания о принципах установления доступа к удалённой сети путем использования терминального сервиса и VPN-соединения при взаимодействии серверов и рабочих станций как компонентов нескольких локальных сетей.