

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Лабораторная работа №1

Выполнили студенты группы ИКТЗ-83:

Громов А.А., Миколаени М.С., Мазеин Д.С.

(Ф.И.О., № группы)

(подпись)

Проверил:

Казанцев А.А.

(уч. степень, уч. звание, Ф.И.О.)

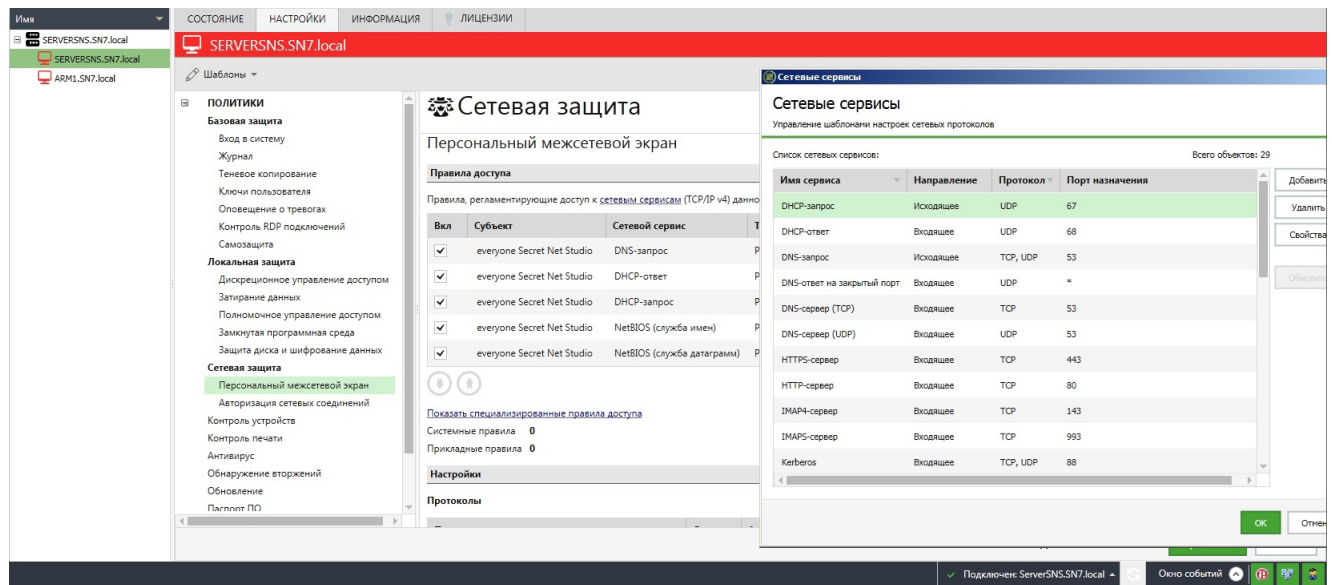
(подпись)

Санкт-Петербург

2021

Цель лабораторной работы:

Пункт 1 - Ознакомьтесь с параметрами настройки политик МЭ.



Настройки политик МЭ.

Пункт 3 - Добавление нового сетевого сервиса для доступа к серверу IIS по порту 8090

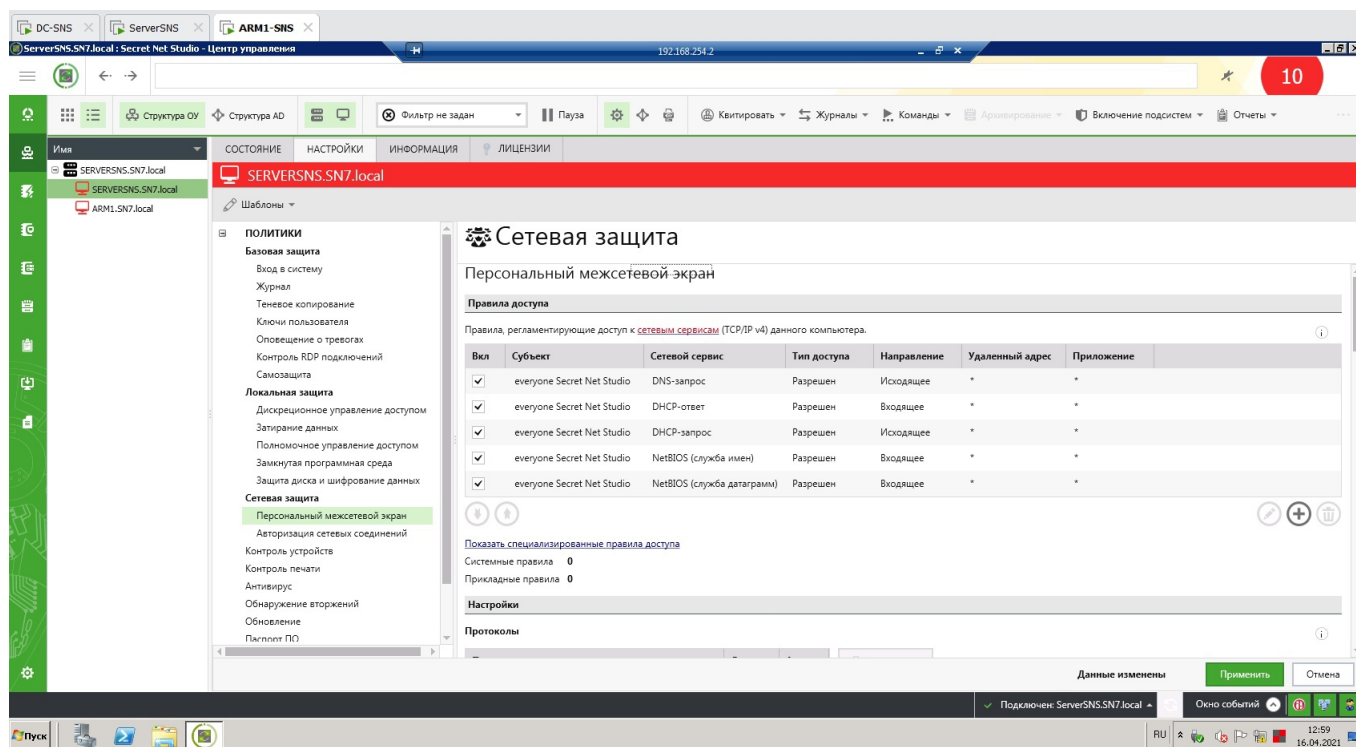
Список сетевых сервисов:

Всего объектов: 29

Имя сервиса	Направление	Протокол	Порт назначения
POP3-сервер	Входящее	TCP	110
RDP-сервер	Входящее	TCP, UDP	3389
RPC-сервер	Входящее	TCP	135
SMB-сервер	Входящее	TCP	139, 445
SMTPS-сервер	Входящее	TCP	465
SMTP-сервер	Входящее	TCP	25
Telnet-сервер	Входящее	TCP	23
WINS-репликация	Входящее	TCP, UDP	42
Все входящие (UDP, TCP)	Входящее	TCP, UDP	*
IIS-сервер 8090	Входящее	TCP	8090

Список сетевых сервисов.

Пункт 5 - Проверка доступа RDP-подключения



RDP-соединение.

Пункт 13 - Создание правила запрета подключения по RDP к ServerSNS

Вкл	Субъект	Сетевой сервис	Тип доступа	Направление	Удаленный адрес	Приложение
<input checked="" type="checkbox"/>	everyone Secret Net Studio	RDP-сервер	Запрещен	Входящее	192.168.254.21	*
<input checked="" type="checkbox"/>	everyone Secret Net Studio	DNS-запрос	Разрешен	Исходящее	*	*
<input checked="" type="checkbox"/>	everyone Secret Net Studio	DHCP-ответ	Разрешен	Входящее	*	*
<input checked="" type="checkbox"/>	everyone Secret Net Studio	DHCP-запрос	Разрешен	Исходящее	*	*
<input checked="" type="checkbox"/>	everyone Secret Net Studio	NetBIOS (служба имен)	Разрешен	Входящее	*	*
<input checked="" type="checkbox"/>	everyone Secret Net Studio	NetBIOS (служба датаграмм)	Разрешен	Входящее	*	*

Список правил.

Пункт 16 - Правила фильтрации доступа к сетевому сервису IIS-сервер 8090

Вкл	Субъект	Сетевой сервис	Тип доступа	Направление	Удаленный адрес	Приложение
<input checked="" type="checkbox"/>	everyone Secret Net Studio	IIS-сервер 8090	Разрешен	Входящее	192.168.254.21	*
<input checked="" type="checkbox"/>	everyone Secret Net Studio	IIS-сервер 8090	Запрещен	Входящее	*	*
<input checked="" type="checkbox"/>	everyone Secret Net Studio	RDP-сервер	Запрещен	Входящее	192.168.254.21	*
<input checked="" type="checkbox"/>	everyone Secret Net Studio	DNS-запрос	Разрешен	Исходящее	*	*
<input checked="" type="checkbox"/>	everyone Secret Net Studio	DHCP-ответ	Разрешен	Входящее	*	*
<input checked="" type="checkbox"/>	everyone Secret Net Studio	DHCP-запрос	Разрешен	Исходящее	*	*
<input checked="" type="checkbox"/>	everyone Secret Net Studio	NetBIOS (служба имен)	Разрешен	Входящее	*	*
<input checked="" type="checkbox"/>	everyone Secret Net Studio	NetBIOS (служба датаграмм)	Разрешен	Входящее	*	*

Список правил.

Пункт 17 - Специализированные правила доступа

Правила доступа

Системные правила контролируют соединения с данным компьютером по протоколам семейства TCP/IP v4. Имеют более **высокий приоритет**, чем правила доступа к сервисам и прикладные правила.

Вкл	Протокол	Тип доступа	Удаленный адрес
-----	----------	-------------	-----------------

Прикладные правила регламентируют доступ субъектов к общим папкам и именованным каналам (TCP/IP v4) данного компьютера. Имеют минимальный приоритет.

Вкл	Субъект	Прикладной сервис	Объект доступа	Тип доступа	Удаленный адрес
-----	---------	-------------------	----------------	-------------	-----------------

Специализированные правила доступа.

Пункт 18 - Пример настройки запрета доступа к серверу ServerSNS по RDP-протоколу.

Создание системного правила

Системное правило

Укажите тип доступа и другие параметры.

Доступ: ☒ Разрешить ☐ Запретить

Протокол: TCP

Номер протокола: 6

Маска фильтра:

Удаленный адрес: 192.168.254.21

Локальный адрес: *

Правило действует на всех адаптерах

- Адаптер Microsoft ISATAP #2
- Адаптер Microsoft ISATAP
- Сетевое подключение Intel(R) PRO/1000 MT
- Сетевое подключение Intel(R) PRO/1000 MT #2

☒ Включить аудит

☐ Отключить правило

Применить Отмена

Создание системного правила

Системное правило

Укажите тип доступа и другие параметры.

Доступ: ☐ Разрешить ☒ Запретить

Протокол: TCP

Номер протокола: 6

Маска фильтра:

Удаленный адрес: *

Локальный адрес: *

Правило действует на всех адаптерах

- Адаптер Microsoft ISATAP #2
- Адаптер Microsoft ISATAP
- Сетевое подключение Intel(R) PRO/1000 MT
- Сетевое подключение Intel(R) PRO/1000 MT #2

☒ Включить аудит

☐ Отключить правило

Применить Отмена

Окно настройки правила.

Пункт 19 - Создание прикладного правила

Прикладные правила регламентируют доступ субъектов к общим папкам и именованным каналам (TCP/IP v4) данного компьютера. Имеют минимальный приоритет.

Вкл	Субъект	Прикладной сервис	Объект доступа	Тип доступа	Удаленный адрес
<input checked="" type="checkbox"/>	everyone Secret Net Studio	Общие папки	user_files	Запрещен	192.168.254.21



Правила доступа

Правила, регламентирующие доступ к сетевым сервисам (TCP/IP v4) данного компьютера.

Вкл	Субъект	Сетевой сервис	Тип доступа	Направление	Удаленный адрес	Приложение
<input checked="" type="checkbox"/>	everyone Secret Net Studio	SMB-сервер	Разрешен	Входящее	192.168.254.21	*

Прикладное правило.

Пункт 23.1 - Проверка команды ping с выключенной ICMP защитой

```
Администратор: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.
C:\Users\Администратор.SN7>ping 192.168.254.2
Обмен пакетами с 192.168.254.2 по 32 байтами данных:
Ответ от 192.168.254.2: число байт=32 время<мс TTL=128
Ответ от 192.168.254.2: число байт=32 время<мс TTL=128
Ответ от 192.168.254.2: число байт=32 время<мс TTL=128
Ответ от 192.168.254.2: число байт=32 время<мс TTL=128
Статистика Ping для 192.168.254.2:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
  Приблизительное время приема-передачи в мс:
  Минимальное = 0 мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

ICMP-защита

☐ Включить ICMP-защиту

Разрешить следующие типы ICMP-сообщений:

Описание	Тип	Код	Получение	Отправка
Эхо-ответ	0	Любой	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Адресат недоступен	3	Любой	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Перенаправление	5	Любой	<input type="checkbox"/>	<input type="checkbox"/>
Альтернативный адрес узла	6	Любой	<input type="checkbox"/>	<input type="checkbox"/>
Эхо-запрос	8	Любой	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Ходатайство маршрутизатора	10	Любой	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

☒ Заблокировать остальные типы ICMP-сообщений

Команда пинг и правила.

Пункт 23.2 - Проверка команды ping с включенной ICMP защитой

ICMP-защита

☒ Включить ICMP-защиту

Разрешить следующие типы ICMP-сообщений:

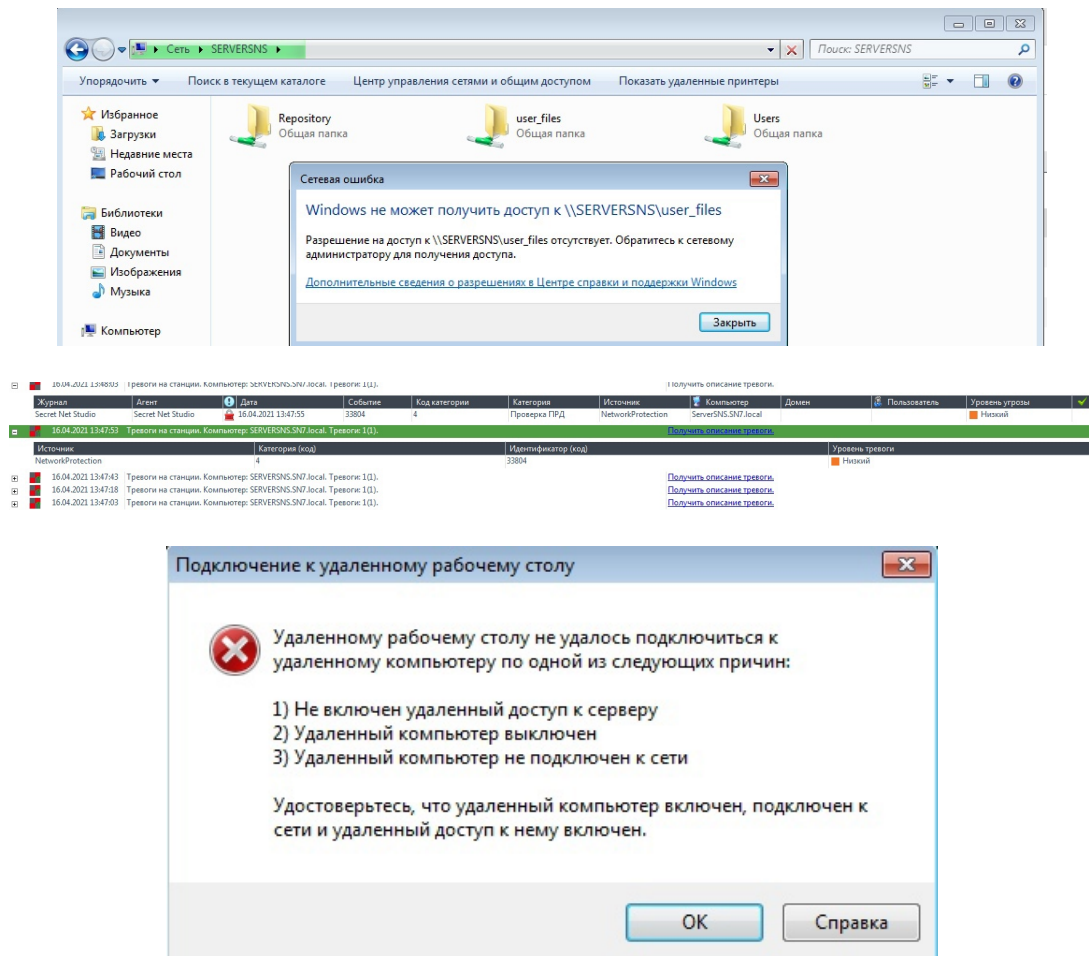
Описание	Тип	Код	Получение	Отправка
Эхо-ответ	0	Любой	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Адресат недоступен	3	Любой	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Перенаправление	5	Любой	<input type="checkbox"/>	<input type="checkbox"/>
Альтернативный адрес узла	6	Любой	<input type="checkbox"/>	<input type="checkbox"/>
Эхо-запрос	8	Любой	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Ходатайство маршрутизатора	10	Любой	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

☒ Заблокировать остальные типы ICMP-сообщений

```
Администратор: C:\Windows\system32\cmd.exe
C:\Users\Администратор.SN7>ping 192.168.254.2
Обмен пакетами с 192.168.254.2 по 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Статистика Ping для 192.168.254.2:
  Пакетов: отправлено = 4, получено = 0, потеряно = 4
  (100% потерь)
```

Команда пинг и правила.

Пункт 24 - Тестирование работы правил



Работа правил.