

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 №2

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.)

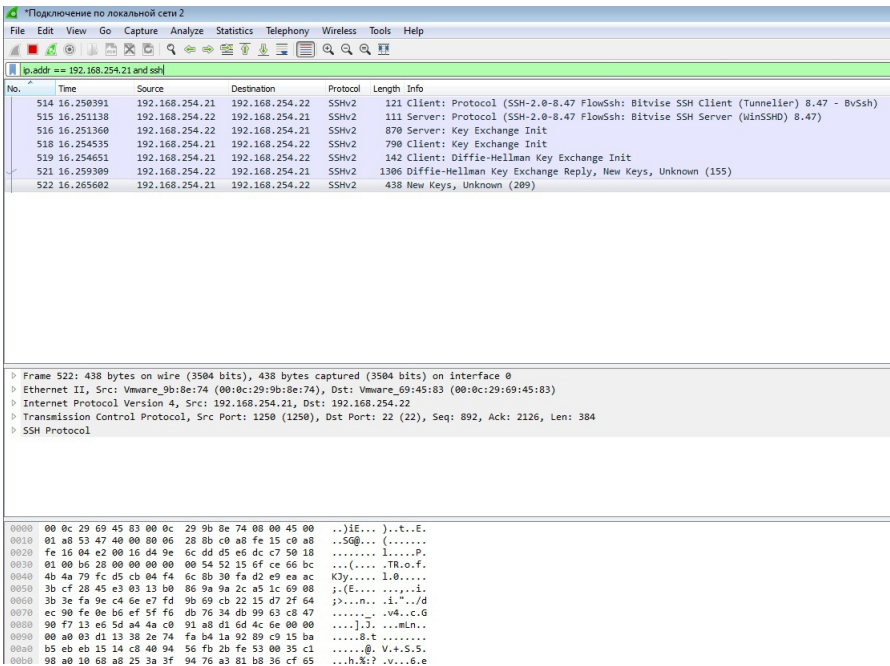
(подпись)

Санкт-Петербург

2021

Цель лабораторной работы:

Пункт 2 - Убедиться, что передается открытый трафик.



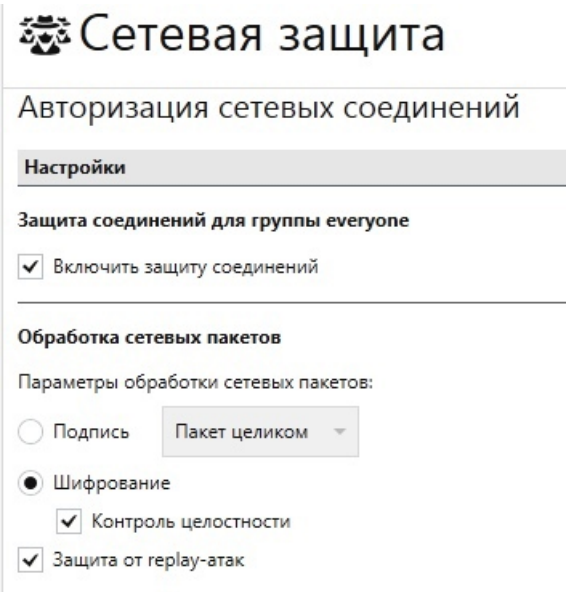
Открытый трафик.

Пункт 3 - Настройка правил доступа

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	Все входящие (UDP, TCP)	Разрешен	Входящее	*

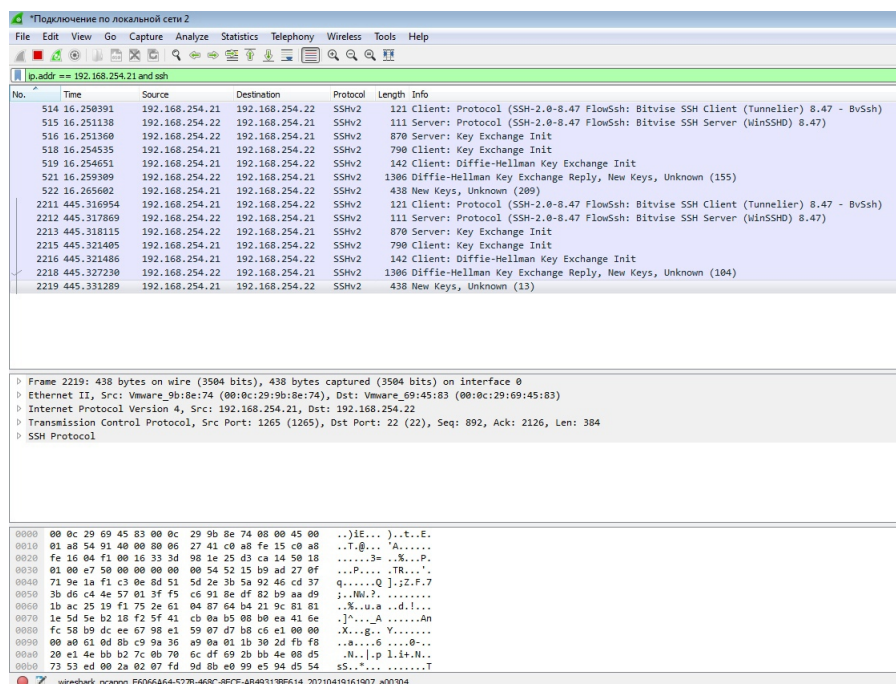
Парвило доступа.

Пункт 4 - Настройка режима защиты сетевых соединений



Экран настроек.

Пункт 5 - Убедиться, что передается зашифрованный трафик



Не удалось зашифровать трафик.

Пункт 7 - Настройка блокировки соединений для неавторизованных на СБ пользователей

Сетевая защита

Персональный межсетевой экран

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"/>	anonymouse Secret Net Studi	Все входящие (UDP, TCP)	Запрещен	Входящее	*	*

Правило доступа.

Ответы на контрольные вопросы.

1. В отличие от традиционных, ”периметровых” МЭ, реализованный в SNS распределенный межсетевой экран предназначен именно для защиты информации внутри сети организации, функционирует непосредственно на ее защищаемых объектах (сервер БД, рабочие места руководителей или сотрудников и т.д.) и обеспечивает их защиту от сетевых угроз со стороны внешнего и внутреннего нарушителей.
2. Правила доступа, прикладные правила, системные правила, сетевые протоколы.
3. Системные правила
4. Все IP-based протоколы (RDP)

5. Прикладные правила. Регламентируют доступ пользователей к сетевым сервисам защищаемого компьютера (например, общие папки).
6. Чем выше правило в таблице, тем больше его приоритет
7. 4 - 6 минут
8. Сетевой режим
9. Механизм авторизации сетевых соединений обеспечивает защиту взаимодействия только между авторизованными на СБ клиентами Secret Net Studio. Если на компьютере пользователя не установлен Secret Net Studio или пользователь по каким-либо причинам не прошел аутентификацию на СБ SNS (anonymous), то трафик между ним и авторизованным клиентом SNS не будет защищаться.
10. Средствами протоколов семейства IPsec, а именно АН (Authentication Header) - гарантирует аутентичность и целостность и ESP (Encapsulation Security Payload) - шифрование и контроль целостности.
11. Необходима лицензия на использование механизма авторизации сетевых соединений.
12. Если прохождение пакетов по протоколу SMB запрещается системными правилами или правилами доступа, то прикладные правила не работают, так как на транспортном уровне IP-пакеты блокируются.