**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Вычислительные сети и контроль безопасности в компьютерных сетях»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4**

«Протоколы туннелирования»

**Выполнили:**

Кукелко Владислав, студент группы N3349

(подпись)

Молитвин Илья, студент группы N33Изображение выглядит как текст, соединитель

Контент, сгенерированный ИИ, может содержать ошибки.45

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

Коптяев Александр, студент группы N3345

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

**Проверил:**

Бучаев Абдулхамид Яхьяевич

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

Содержание

[Введение 3](#_Toc154111231)

[1 Ход работы 4](#_Toc154111232)

[1.1 Настройка лабораторного стенда 4](#_Toc154111233)

[1.2 Настройка IPSec на роутерах 6](#_Toc154111234)

[1.3 Измерение пропускной способности 9](#_Toc154111235)

[Заключение 11](#_Toc154111236)

[Список использованных источников 12](#_Toc154111237)

Введение

Цель работы – изучить основные протоколы туннелирования на примере настройки туннеля IPSEC.

Для достижения поставленной цели необходимо решить следующие задачи:

* настроить лабораторный стенд в GNS3, включающий следующие узлы:
  + шлюз IPSEC – 1;
  + шлюз IPSEC – 2;
  + промежуточный маршрутизатор для обмена трафиком между шлюзами;
  + клиентские устройства в локальной сети каждого шлюза - для тестирования работы туннеля;
* проверить взаимную доступность шлюзов;
* выполнить необходимые настройки туннеля IPSEC site-to-site в соответствии с заданием;
* убедиться в работоспособности туннеля и в том, что маршрутизация трафика настроена через туннель;
* изучить структуру заголовков для каждого протокола туннелирования;
* провести измерение пропускной способности канала без туннелирования и канала, использующего IPSEC, а также для каждого настроенного протокола. Сравнить полученные значения.

# Ход работы

## Настройка лабораторного стенда

Настроить лабораторный стенд в GNS3, включающий следующие узлы:

* Шлюз IPSEC - 1
* Шлюз IPSEC - 2
* Промежуточный маршрутизатор для обмена трафиком между шлюзами
* Клиентские устройства в локальной сети каждого шлюза - для тестирования работы туннеля

Изображение выглядит как текст, Графика, снимок экрана, логотип

Автоматически созданное описание

1. Лабораторный стенд

Изображение выглядит как текст, снимок экрана, диаграмма, линия

Автоматически созданное описание

1. Схема лабораторного стенда в GNS3

Настроим статичную маршрутизацию у маршрутизатора (Рисунок 3).

Изображение выглядит как текст

Автоматически созданное описание

1. Настройка центрального маршрутизатора

Настроим шлюз по умолчанию на роутерах IPSec-1-MikroTik (Рисунок 4) и IPSec-2-Cisco (Рисунок 5).

Изображение выглядит как текст

Автоматически созданное описание

1. Маршруты на роутере IPSec-1-MikroTik

Изображение выглядит как текст, квитанция

Автоматически созданное описание

1. Маршруты на роутере IPSec-2-Cisco

Проверим связь между устройствами PC1 и PC2 (Рисунок 6).

Изображение выглядит как текст

Автоматически созданное описание

1. Ping PC1 и PC2

## Настройка IPSec на роутерах

Настроим параметры IPSec для роутеров IPSec-1-MikroTik (Рисунок 7) и IPSec-2-Cisco (Рисунок 8).

Изображение выглядит как текст

Автоматически созданное описание

1. Параметры IPSec на роутере IPSec-1-MikroTik

Изображение выглядит как текст

Автоматически созданное описание

1. Параметры IPSec на роутере IPSec-2-Cisco

Проверим сигнал между конечными хостами с помощью утилиты ping (Рисунок 9). Видим, что пакеты доставляются без потерь.

Изображение выглядит как текст

Автоматически созданное описание

1. Пинг хоста

Отследим процесс создания туннеля с помощью утилиты Wireshark (Рисунок 10).

Изображение выглядит как текст, Шрифт, число, снимок экрана

Автоматически созданное описание

1. Построение туннеля, отслеженное через Wireshark

## Измерение пропускной способности

Осуществим проверку с помощью утилиты ping, будем отправлять пакеты размером 1000 байт командой *ping 192.168.10.2 -l 1000*. Повторяем данную процедуру 3 раза при настроенном туннеле (Рисунок 11) и без него (Рисунок 12).

Изображение выглядит как текст, квитанция

Автоматически созданное описание

1. Результат пинга без настроенного туннеля

Изображение выглядит как текст, квитанция

Автоматически созданное описание

1. Результат пинга с настроенным туннелем

Далее найдем среднее значение времени выполнения команды ping без туннеля и с туннелем. Среднее значение без туннелирования – 29.22 мс, с туннелированием – 35.64 мс. Как можем заметить, время отличается. Это связано с временными затратами на обработку зашифрованного пакета.

Заключение

В ходе выполнения лабораторной работы были решены следующие задачи:

* настроен лабораторный стенд в GNS3, включающий следующие узлы:
* проверена взаимная доступность шлюзов;
* выполнены необходимые настройки туннеля IPSEC site-to-site;
* проверена работоспособность туннеля;
* изучена структура заголовков для каждого протокола туннелирования;
* проведены измерение пропускной способности канала без туннелирования и канала, использующего IPSEC, а также для каждого настроенного протокола.

Таким образом, все поставленные задачи решены, цель достигнута.

Список использованных источников

1. IPsec в Cisco [Электронный ресурс] // Wiki XGU. – Режим доступа: <http://xgu.ru/wiki/IPsec_%D0%B2_Cisco>.
2. IPsec / MikroTik RouterOS [Электронный ресурс] // MikroTik Documentation. – Режим доступа: <https://help.mikrotik.com/docs/spaces/ROS/pages/11993097/IPsec>.
3. Site-to-Site IPsec using Pre-Shared Keys (PSK) [Электронный ресурс] // Netgate Docs. – Режим доступа: <https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-s2s-psk.html>.
4. How To Set Up an IKEv2 VPN Server with StrongSwan on Ubuntu 20.04 [Электронный ресурс] // DigitalOcean Community Tutorials. – Режим доступа: <https://www.digitalocean.com/community/tutorials/how-to-set-up-an-ikev2-vpn-server-with-strongswan-on-ubuntu-20-04>.