Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.7.056(043.3)

КАПУСТО
Регина Александровна

ЗАЩИТА ДАННЫХ, ПЕРЕДАВАЕМЫХ ПО VPN ТУННЕЛЮ

Автореферат
на соискание степени магистра
по специальности 1-98 80 01 Информационная безопасность

_____

Научный руководитель
к.т.н., доцент, доцент кафедры ЗИ
БЕЛОУСОВА Елена Сергеевна

_____

Минск 2023

ВВЕДЕНИЕ

Ввиду распространенности передачи данных по незащищенным каналам и возможности их перехвата нарушителями, важной задачей на сегодняшний день является обеспечение защиты передаваемой информации за счет создания защищенного соединения по технологии Virtual Private Network (VPN). Таким образом, актуальность темы заключается в сравнительном анализе существующих VPN решений, разработке методик конфигурации и тестирования VPN туннелей и предложению рекомендаций по их использованию.

Объектом исследования является безопасность передачи данных. Предмет исследования – средства защиты передачи данных по VPN туннелю.

Цель диссертационного исследования состоит в разработке методик конфигурации и тестирования производительности VPN туннелей для оценки защиты передаваемых данных.

Для достижения цели необходимо последовательно решить следующие задачи:

– осуществить сравнительный анализ методов и протоколов организации защищенных соединений для обоснования выбора протоколов для конфигурации VPN туннелей;

– разработать модели сетей для конфигурации VPN туннелей;

– составить методики конфигурации и тестирования VPN туннелей;

– проанализировать передаваемые по VPN туннелям данные для определения их защиты;

провести апробацию составленных методик конфигурации и тестирования VPN туннелей.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами

Тема диссертационной работы соответствует пункту *6* приоритетных направлений научной, научно-технической и инновационной деятельности Республики Беларусь на 2021–2025 гг., утвержденных Указом Президента Республики Беларусь №156 от 7 мая 2020 г. «Обеспечение безопасности человека, общества, государства». Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Целью диссертационной работы является разработка методик конфигурации и тестирования производительности VPN туннелей для оценки защиты передаваемых данных.

Для достижения поставленной цели в диссертации решены следующие задачи:

1 Осуществить сравнительный анализ методов и протоколов организации защищенных соединений для обоснования выбора протоколов для конфигурации VPN туннелей.

2 Разработать модели сетей для конфигурации VPN туннелей.

3 Составить методики конфигурации и тестирования VPN туннелей.

4 Проанализировать передаваемые по VPN туннелям данные для определения их защиты.

5 Провести апробацию составленных методик конфигурации и тестирования VPN туннелей.

Личный вклад соискателя ученой степени

Личный вклад автора диссертации заключается в постановке и проведении экспериментов по исследованию криптографических характеристик VPN туннелей, а также показателей их производительности, обработке и анализе полученных результатов, формулировке выводов.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем к.т.н., доцентом, доцентом кафедры ЗИ Е. С. Белоусовой.

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты диссертационной работы докладывались и обсуждались на: XXVI Международной научно-технической конференции «Современные средства связи», 58-ой научной конференции аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Опубликование результатов диссертации

По результатам исследований, представленных в диссертации, опубликованы 2 печатные работы, в том числе: две статьи в сборниках материалов конференций.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, трех глав с выводами по каждой главе, заключения, библиографического списка, 4 приложений.

Общий объем диссертационной работы составляет 60 страниц, из них 46 страниц текста, 24 рисунка на 18 страницах, 6 таблиц на 5 страницах, список использованных библиографических источников (32 наименования на 2 страницах), список публикаций автора по теме диссертации (2 наименования на 1 странице), 4 приложения на 8 страницах, графический материал на 6 страницах.

Проверка на уникальность

Проведена экспертиза диссертации Капусто Регины Александровны «Защита данных, передаваемых по VPN туннелю» на корректность использования заимствованных материалов с применением сетевого ресурса «Антиплагиат» (адрес доступа: https://antiplagiat.ru) 10.06.2023 г. В результате проверки установлена корректность использования заимствованных материалов (оригинальность диссертационной работы составляет 80,66 %).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность выбранной темы диссертационного исследования, определяются цели и задачи, осуществляется выбор предмета и объекта исследования.

В **общей характеристике работы** показана связь работы с приоритетными направлениями научных исследований, цель и задачи исследования, личный вклад соискателя ученой степени, апробация результатов диссертации.

В **первой главе** диссертации рассмотрены технология VPN и ее виды: «remote access», «site-to-site». Учитывая популярность «remote access» среди пользователей Интернета, данный вид VPN решений выбран для дальнейшего исследования. Чтобы обосновать выбор протоколов для построения «remote access» VPN туннелей, были изучены такие VPN протоколы, как PPTP, SSTP, L2TP/IPSec, IKEv2/IPSec, OpenVPN и WireGuard, выделены их достоинства и недостатки, выполнен сравнительный анализ. Для рассмотрения выбраны два VPN протокола: WireGuard и OpenVPN. По итогам сравнительного анализа криптографических параметров выбранных протоколов сделано заключение, что оба протокола являются надежными и безопасными VPN решениями.

Во **второй главе** диссертации разработаны модели сетей для создания безопасных туннелей с использованием VPN протоколов WireGuard и OpenVPN, на полученных моделях выполнена настройка VPN решений. Было приведено описание конфигурации WireGuard и OpenVPN, детально изучен процесс создания туннелей. С помощью программы Wireshark была осуществлена проверка, показавшая что данные, передающиеся по полученным туннелям, зашифрованы. На основе выполненных для настройки VPN решений действий составлены методики конфигурации защищенных VPN туннелей WireGuard и OpenVPN.

В **третьей главе** диссертации разработана методика тестирования параметров производительности VPN туннелей с помощью инструмента iPerf, проведена ее апробация на туннелях WireGuard и OpenVPN.

Первая часть тестирования – это TCP тест. По данным, полученным в результате тестирования, скорость OpenVPN ниже скорости WireGuard на 384 Мбит/с для локального сервера. Числовые данные представлены на рисунке 1 в виде графика.

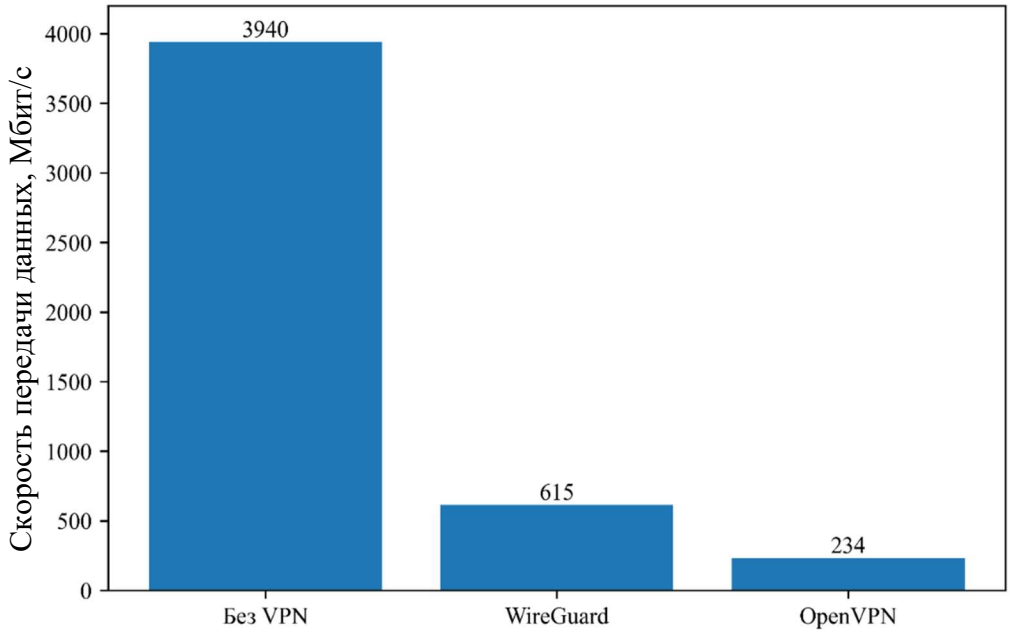

Рисунок 1 – Скорость передачи данных для локального сервера, Мбит/с

Для данного теста WireGuard оказался более быстрым VPN решением.

Вторым выполнен UDP тест без нагрузки. Для него значение джиттера WireGuard туннеля выше джиттера OpenVPN туннеля на 0,124 мс для случая с локальным сервером и на 0,082 мс для случая с общедоступным сервером. Результаты представлены в таблице 1.

Таблица 1 – Значение показателей для локального сервера

Параметр	Без VPN	WireGuard	OpenVPN
Джиттер, мс	0,094	0,195	0,071
Потеря пакетов, %	0	0	0

Скорость всех соединений достигла 10 Мбит/с, то есть своего целевого значения. Процент потери пакетов для всех соединений меньше 1 %. Сделан вывод, что оба решения достаточно стабильны.

Далее был выполнен UDP стресс-тест. Скорость OpenVPN туннеля оказалось выше скорости WireGuard на 19 Мбит/с для теста с локальным сервером и на 0,3 Мбит/с для теста с публичным сервером. Увеличение скорости OpenVPN сочеталось с уменьшением стабильности, так как при этом повысились показатели джиттера и процента потери пакетов. Численные значения отражены в таблице 2.

Таблица 2 – Значение показателей для локального сервера

Параметр	Без VPN	WireGuard	OpenVPN
Джиттер, мс	0,051	0,052	0,126
Потеря пакетов, %	0,0019	0,02	2,4

Джиттер OpenVPN больше соответствующего параметра WireGuard на 0,074 мс для теста с локальным сервером и на 0,545 мс для теста с общедоступным сервером. Разница процента потери пакетов OpenVPN туннеля и WireGuard туннеля равнялась 2,38 %.

В результате сравнения принципов работы VPN туннелей WireGuard и OpenVPN сделан вывод, что WireGuard является более быстрым VPN решением. При стресс-тестировании OpenVPN менее стабилен, чем WireGuard.

В **заключении** подведены итоги диссертационного исследования, изложены его основные выводы и обобщающие результаты.

ЗАКЛЮЧЕНИЕ

На основе изучения статистики по использованию VPN туннелей, установлено что данная технология получила широкое распространение в связи с тем, что она помогает защитить данные, передающиеся по сети Интернет, путем создания безопасного туннеля.

Обоснован выбор «remote access» VPN туннеля в виду его распространенности среди пользователей Интернет по сравнению с «site-to-site». Для обоснования выбора протоколов построения VPN туннелей «remote access» были изучены такие VPN протоколы, как PPTP, SSTP, L2TP/IPSec, IKEv2/IPSec, OpenVPN и WireGuard. По результатам изучения протоколов выполнен их сравнительный анализ и обоснован выбор WireGuard и OpenVPN.

По результатам сравнительного анализа выбранных VPN протоколов сделан вывод, что WireGuard и OpenVPN по праву считаются безопасными и надежными VPN решениями, так как выигрывают у своих конкурентов в области по ряду определенных параметров.

Для тестирования производительности выбранных протоколов VPN разработаны модели сетей для конфигурации WireGuard и OpenVPN туннелей, выполнена настройка виртуальных машин. С помощью программы Wireshark проверено, что данные, передающиеся по полученным туннелям зашифрованы. На основе осуществленной конфигурации протокола OpenVPN составлена методика, которая может быть использована специалистами в области информационной безопасности для организации защищенных соединений между удаленными сотрудниками и корпоративными сетями. Методика конфигурации WireGuard может быть использована для получения доступа к веб-ресурсам.

На основе составленной методики тестирования VPN туннелей проведено тестирование, которое состояло из следующий этапов: TCP тест, UDP тест без нагрузки, UDP стресс-тест. По результатам TCP теста WireGuard проявил себя как более быстрое VPN решение, так как его скорость была выше скорости OpenVPN на 384 Мбит/с для локального сервера и на 1,7 Мбит/с для публичного сервера. При UDP тестировании без нагрузки значение скорости всех соединений достигло целевого значения 10 Мбит/с, процент потери пакетов оказался меньше 1 %, поэтому оба решения можно считать достаточно стабильными. Хотя для UDP стресс-теста скорость OpenVPN оказалась выше скорости WireGuard на 19 Мбит/с, его процент потери пакетов превысил соответствующий показатель WireGuard туннеля на 2,38 %. Это указывает на меньшую стабильность OpenVPN туннеля в сравнении с WireGuard туннелем в условиях превышения пределов нормального функционирования.

На основании проведенного исследования сделан вывод, что каждый из рассмотренных протоколов VPN является адекватным решением вопроса защиты передаваемых данных для различных вариантов использования: WireGuard подходит для простых задач, таких как удаленный доступ к веб-серверам и обмен файлами; протокол OpenVPN подходит для организации удаленного доступа к корпоративной сети компании.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

Статьи конференций

1–А. Капусто, Р. А. Обзор криптографической безопасности vpn-протоколов / Р. А. Капусто // Современные средства связи: материалы XXVI междунар. науч.-техн. конф., 21-22 окт. 2021 года, Минск, Респ. Беларусь; редкол. : А. О. Зеневич [и др.]. – Минск : Белорусская государственная академия связи, 2021. – С. 112–113.

2–А. Капусто Р. А. Показатели безопасности VPN-сервиса / Р. А. Капусто // 58-я научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 18-22 апреля 2022 г., БГУИР, Минск, Беларусь: сборник материалов. – Мн. – 2022. – С. 32–33.