РусКрипто

КОМПАНИЯ АКТИВ

Сравнение эксплуатационных характеристик протоколов безопасности сетевого уровня IPsec и WireGuard в некоторых сценариях

Илья Аркадьев
Антон Васин
Игорь Дудка

Евгений Мироненко
Кирилл Павлишин
Владислав Сапегин
Даниил Чугунов

Компания «Актив»

Wireguard и набор протоколов IPSec

Wireguard, IPSec - протоколы безопасности для защиты сетевого уровня для защиты IP-пакетов.

IPSec

- состоит из протокола обмена ключами IKEv2 и протокола защиты информации ESP;
- универсальный протокол с поддержкой различных сценариев;
- допускает широкое конфигурирование.

Wireguard

- handshake основан на паттерне Noise;
- фиксированные криптографические наборы;
- минимальная конфигурация.

Основные отличия протоколов

Wireguard	**IPSec**
Фиксированный криптонабор	Криптонабор согласуется в рамках IKEv2
Аутентификация с использованием ассиметричных ключей	Сертификаты, PSK
Открытые ключи предварительно распределены	Сертификаты абонентов могут пересылаться в рамках IKEv2
2 пересылки на этапе рукопожатия	4 пересылки в протоколе IKEv2
Фиксируется диапазон допустимых IP-адресов	Диапазон IP-адресов согласуется
Обновление сессионных ключей требует нового рукопожатия	Допускается обновлять Child SA в рамках существующего IKE SA

Цель исследования

Общая цель

Провести количественное и качественное сравнение эксплуатационных характеристик протоколов IPsec и WireGuard при различных сетевых условиях на разных аппаратных платформах.

Основной подход

- оценка структурных влияний протоколов, а не специфики конкретных реализаций;
- максимально единообразная настройка, обеспечивающая одинковые криптографические и сетевые характеристики.

Результат

Преимущества протокола в зависимости от аппаратной платформы и сетевых условий.

Обзор исследований

Michaelides et al. (2025) Assessing the Latency of Network Layer Security in 5G Networks

- тестируются задержки в сетях 5G в топологии peer-to-peer
- strongswan ipsec, wireguard linux kernel
- криптонаборы в ipsec: DH Group 19, AES-GCM, AES-CBC-HMAC, AES-NI инструкции

Gentile et al. (2022) A VPN Performances Analysis of Constrained Hardware Open Source Infrastructure Deploy in IoT Environment

- исследовалась пропускная способность без сетевых сценариев в топологиях s2s, s2multisite, road warrior
- Raspberry Pi 2, мобильных устройства, Mikrotik 7, Windows клиенты
- ограничение сети 100 Мбит/с
- strongswan ipsec, wireguard linux kernel
- криптонаборы в ipsec: aes256-sha256-modp2048, aes256-sha1

Обзор исследований

Sipahioglu (2024) Modernizing Deep Space Network Security

- исследовалась пропускная способность, задержка, нагрузка CPU
- сеть дальней космической связи
- peer-to-peer с 4-х и 2-х ядерным процессором
- strongswan ipsec, wireguard linux kernel
- результаты вряд ли корректны, в некоторых случаях пропускная способность Wireguard выше, чем без протокола, что говорит об ошибках в конфигурации и статистической обработке данных

Dekker E., Spaans P. (2021) Performance comparison of VPN implementations WireGuard, strongSwan, and OpenVPN in a 1 Gbit/s environment.

- strongswan ipsec, wireguard linux kernel
- ограничение сети 1 Гбит/с
- в некоторых случаях пропускная способность WireGuard выше, чем без него, что говорит об ошибках в конфигурации и статистической обработке данных

Обзор исследований

Osswald et al. (2020) Performance Comparison of VPN Solutions

- peer-to-peer, укаждого абонента по 4 ядра
- различные криптонаборы в ipsec, в том числе ChaChaPoly1305
- strongswan 5.6.2 ipsec (не поддерживает многопоточность), wireguard linux kernel

Demirdelen et al. (2025) Performance Evaluation of WireGuard and IPSec Protocols in Various Network Configurations

- strongswan ipsec, wireguard linux kernel
- не указаны используемые криптонаборы
- ограничение сети 1 Гбит/с
- peer-to-peer, у абонентов многоядерные процессоры
- показано, что ipsec на базе strongswan не поддерживает многопоточность
- данные вряд ли статистически значимые

Обзор исследований

Основные проблемы:

- пропускная способность ограничивается каналом связи, в этом случае выводы о преимуществах того или иного протокола некорректны;
- отсутствует статистический анализ данных;
- преимущество в пропускной способности Wireguard объясняется многопоточностью;
- сравниваются протоколы с разными криптонаборами;
- не везде рассматриваются помехи канала связи, другие сетевые параметры;
- отсутствует сравнение протоколов на низкоресурсной аппаратой платформе.

Основные свойства безопасности

Протокол Wireguard и сконфигурированный определённым образом IPSec обеспечивают:

- аутентифицированная выработка сторонами общего ключа с явным подтверждением выработки ключа;
- стойкость при компрометации сеансовых ключей, эфемерных закрытых ключей;
- защита от чтения назад;
- защита от повротов;
- конфиденциальность и целостность данных.

Реализации, используемые в тестировании

1. Тестирование на уровне ядра (kernel space) Linux
   - IPsec на базе strongSwan 6.0.2: libcharon (user space) для IKEv2 и XFRM ESP в рамках модуля ядра;
   - Wireguard как модуль ядра.
2. Тестирование на микроконтроллере
   - реализация IPsec на базе библиотеки CycloneIPSEC v 2.6.0 от Oryx Embedded;
   - Wireguard - адаптированная реализация WireGuard-C.

Используемые параметры IKEv2. Обмен IKE_SA_INIT

Инициатор		**Ответчик**
HDR, SAi1, KEi, Ni	$\longrightarrow$	
	$\longleftarrow$	HDR, SAr1, KEr, Nr

- **HDR**: значения по умолчанию [RFC 7296];
- **SAi1**/**SAi2**: определяется единственный криптонабор;
- **Секция (Notify)**: для аутентификации в фазе IKE_AUTH фиксируется алгоритм хеширования.

Используемые параметры IKEv2. Обмен IKE_AUTH

Инициатор		**Ответчик**
HDR, SK IDi, AUTH, SAi2, TSi, TSr	$\longrightarrow$	
	$\longleftarrow$	HDR, SK IDr, AUTH, SAr2, TSi, TSr

- **HDR**: значения по умолчанию [RFC 7296];
- **IDi** / **IDr**: любой допустимый тип идентификатора;
- **SAi2** / **SAr2**: определяется единственный proposal для протокола ESP;
- **Сертификаты**: не пересылаются в рамках обмена сообщениями IKE (CERT и CERTREQ payloads отсутствуют);
- **TSi** / **TSr**: задают ровно один селектор для каждой стороны. Тип селектора — $TS\_IPV4\_ADDR\_RANGE$;
- **Паддинг**: не требуется.

Используемые параметры протокола ESP

1. **Режим**: туннельный.
2. **Обработка ошибок**.

Пакеты, не прошедшие какую-либо проверку должны отбрысываться без уведомления отправителя.

Проверки:

- поиск SA в SAD по значению SPI;
- проверка номера полученного пакета;
- проверка ICV;
- проверка режима инкапсуляции;
- проверка селекторов трафика.

3. **Поле Padding**

- TFC Padding не должен использоваться;
- Обязательный паддинг Padding должен быть минимальной необходимой длины.

Параметры узлов

Peer-To-Peer Два абонента устанавливают между собой защищённое соединение.
Звезда Несколько абонентов устанавливают защищённое соединение с центральным узлом.
Параметры абонентов с высокопроизводительными процессорами.

- тактовая частота ядра 4.5 ГГц;
- количество ядер: 1 для топологии peer-to-peer, 2/4 для топологии звезда;
- оперативная память - 2 ГБ;
- операционная система Debian 14, версия ядра 6.19.

Параметры абонента с низкопроизводительным микроконтроллером.

- тактовая частота 800 МГц;
- количество ядер: 1;
- оперативная память - 1,5 МБ;
- операционная система реального времени RT-Thread v 5.2.2 + lwip.

Сценарии тестирования

Исследовались характеристики:

- пропускная способность;
- RTT;
- время установления соединения.

Топологии:

- **Peep-to-peer**. При тестировании пропускной способности обеспечивалась нагрузка CPU 100% на двух абонентах.
- **Звезда**. Вычислялась суммарная пропускная способность по 8 абонентам, RTT и время установления соединения тестировались под нагрузкой: 7 из 8 абонентов отсылали TCP трафик.

Сценарии тестирования

Сценарии с высокопроизводительными узлами

В качестве транспортного использовался протокол TCP, по умолчанию размер полезной нагрузки 512 байт, MTU сети 1500. Исследовались сценарии:

- задержка: 20 мс, 30 мс, 30 мс, 40 мс, 50 мс, 100 мс, 150 мс;
- задержка с джиттером: 20 мс с 5 мс, 30 с 5, 40 с 10, 50 с 10, 100 с 20, 150 с 30;
- потери пакетов: 1%, 2%;
- размер полезной нагрузки: 90, 512, 1398, 1600.

Сценарии с низкопроизводительным узлом

- задержка: 5 мс, 10 мс, 15 мс;
- задержка с джиттером: 5 мс с 1 мс, 10 с 2, 15 с 3;
- потери пакетов: 1%, 2%;
- размер полезной нагрузки: 1398.

Статистический анализ данных

Маленькие интервалы (до сотых долей секунды): нелинейная зависимость

- переполнение буферов сетевой карты;
- изменение окон TCP (cwnd и rwnd изменяются алгоритмом CUBIC);
- объединение маленьких пакетов алгоритмом Нейгла;
- прерывания на уровне ядра.

Средние интервалы (от десятых долей секунды до нескольких минут): линейная зависимость. Подтверждено, например, в работах:

- Silva et al. (2013) — *Computer Networks*
- Hernandez et al. (2001) — *Journal of Network and Systems Management*
- Elbiaze et al. (2005) — *13th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems*

Статистический анализ данных

Предварительное тестирование

Независимость

- Критерий Льюнга-Бокса для средних интервалов

Стационарность, однородность

- критерий Дики-Фуллера
- критерий Краскела-Уоллиса
- критерий Левене

Нормальность

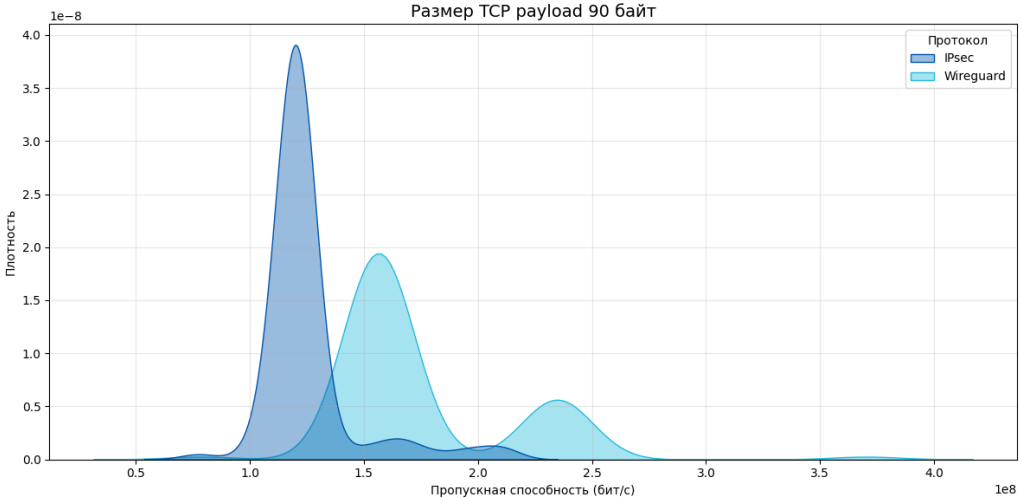
- часть замеров нормальна, часть — нет

Сравнение распределений

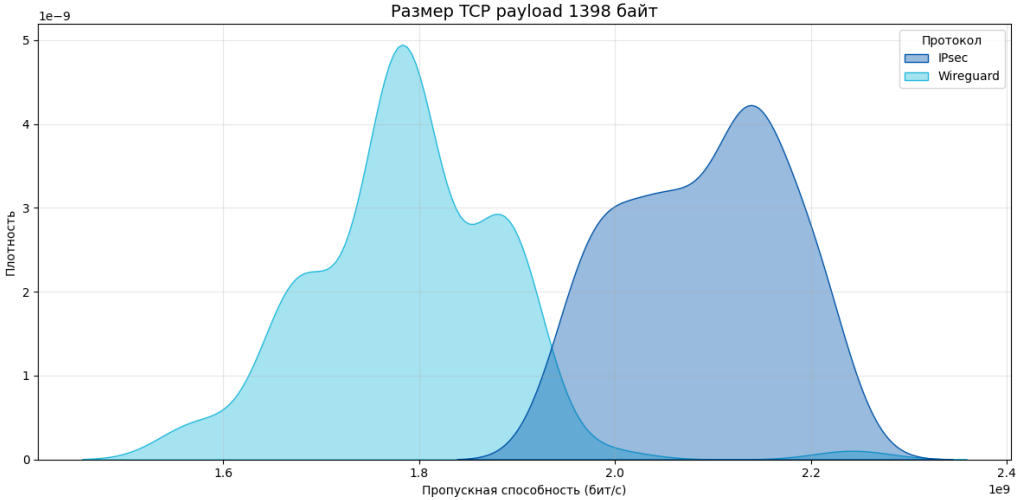
- сравнение распределений IPsec и Wireguard - критерий ван дер Вардена
- степень различия - коэффициент Коэна

Сравнение реализаций в ядре Linux

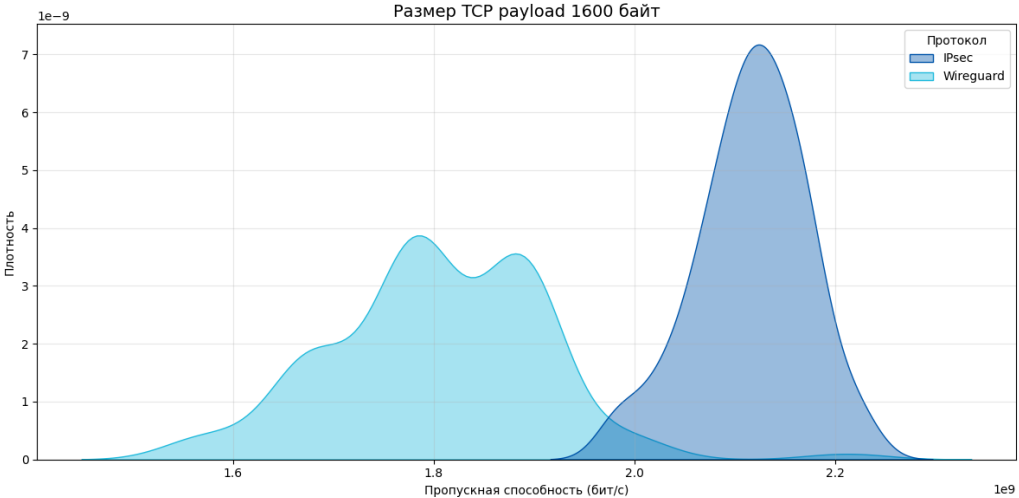
Топология Peer-To-Peer



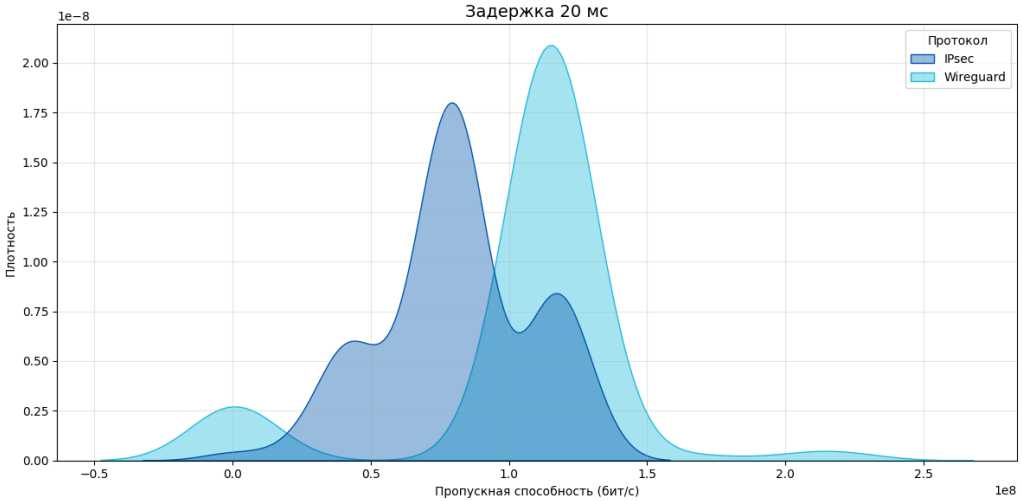
Топология Peer-To-Peer



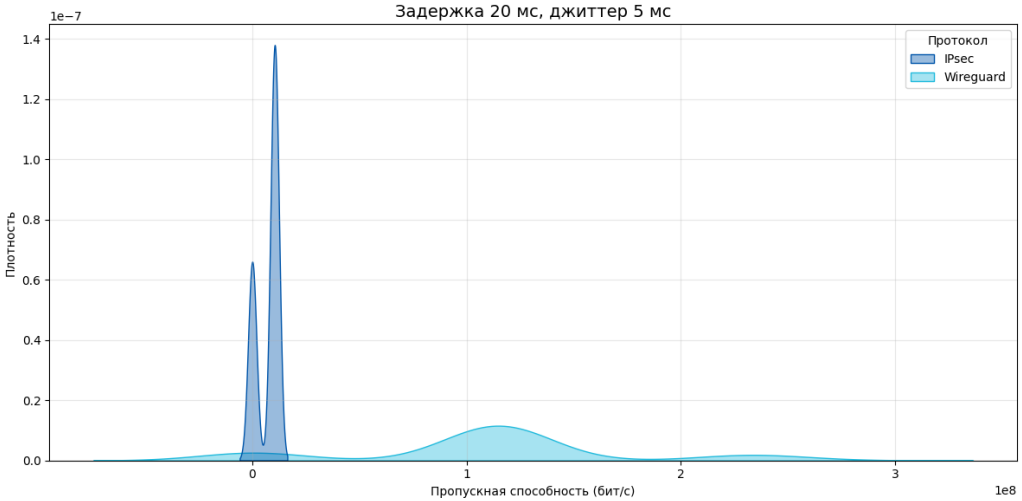
Топология Peer-To-Peer



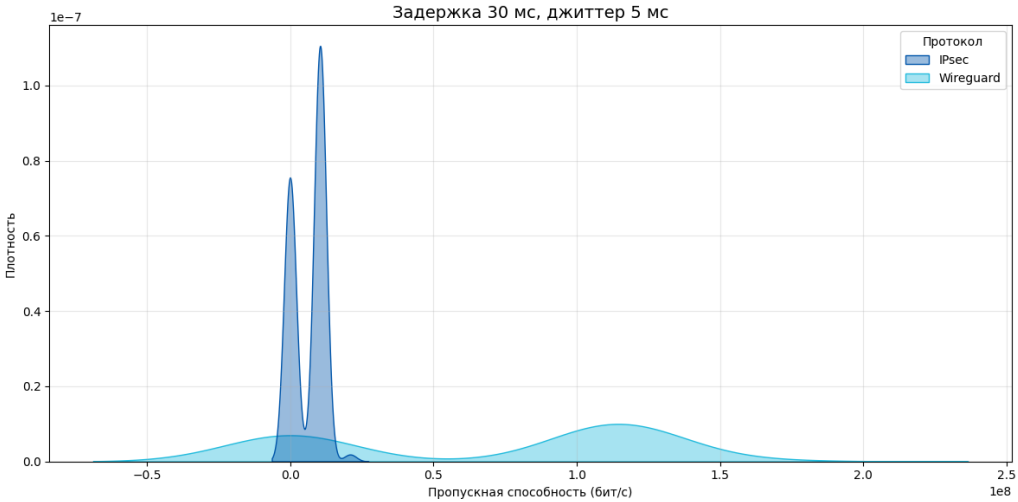
Топология Peer-To-Peer



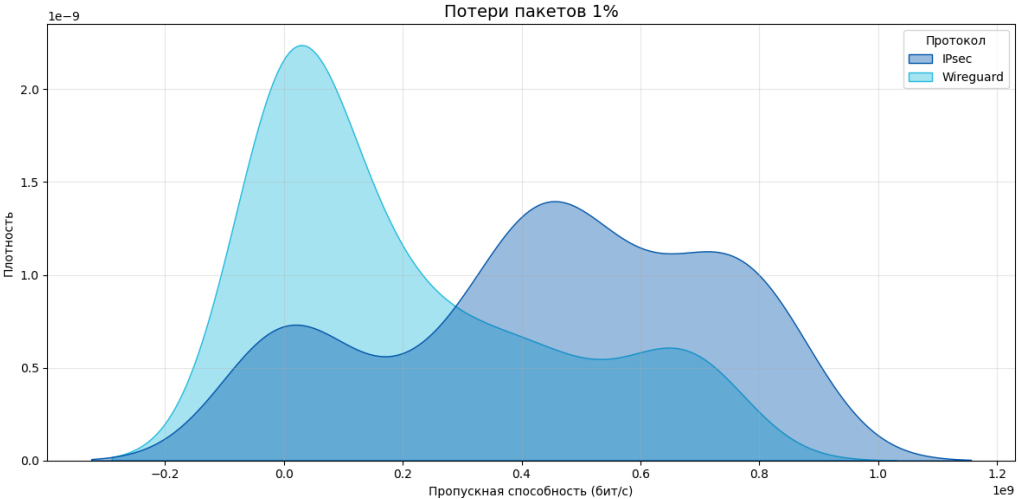
Топология Peer-To-Peer



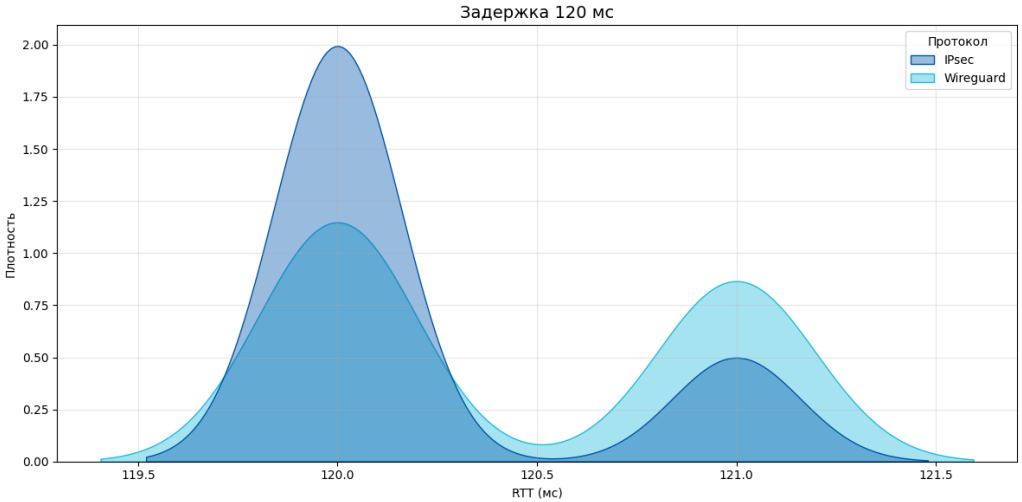
Топология Peer-To-Peer



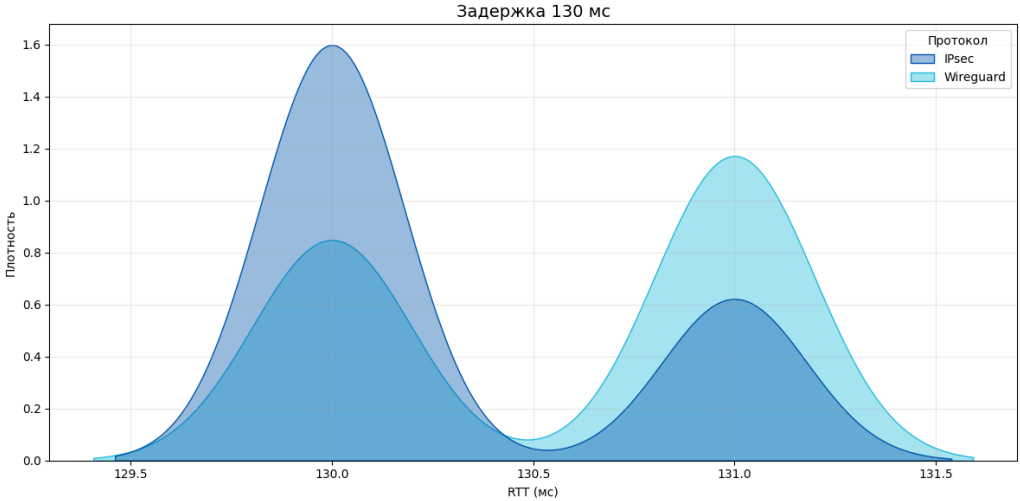
Топология Peer-To-Peer



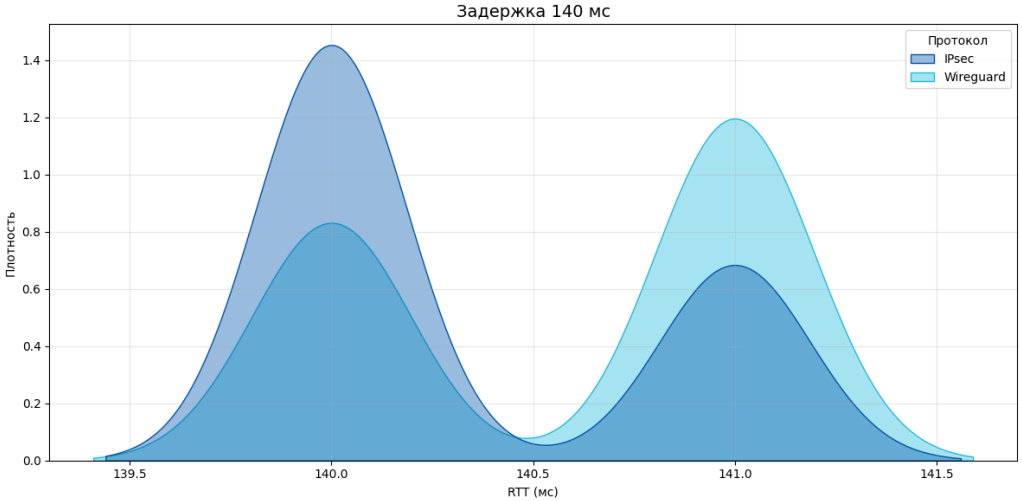
Топология Peer-To-Peer



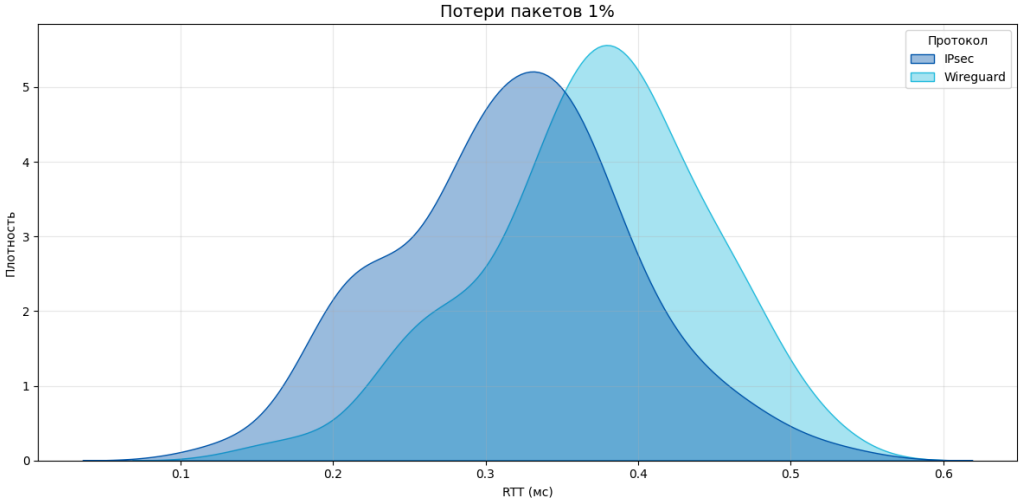
Топология Peer-To-Peer



Топология Peer-To-Peer

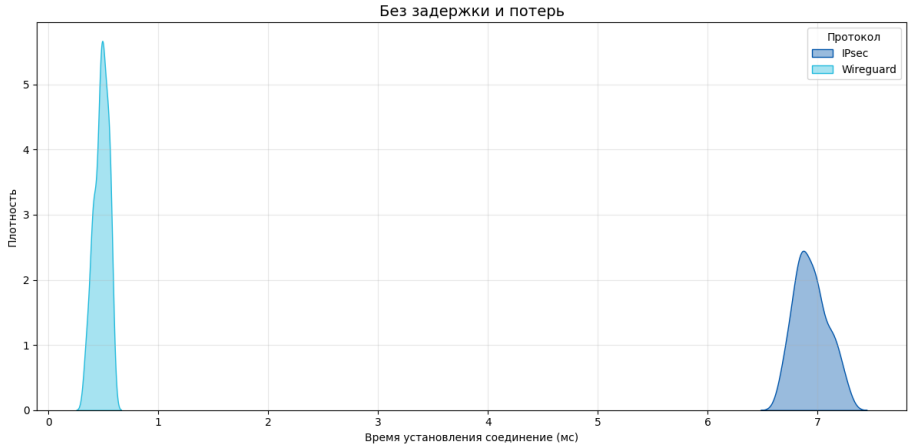


Топология Peer-To-Peer



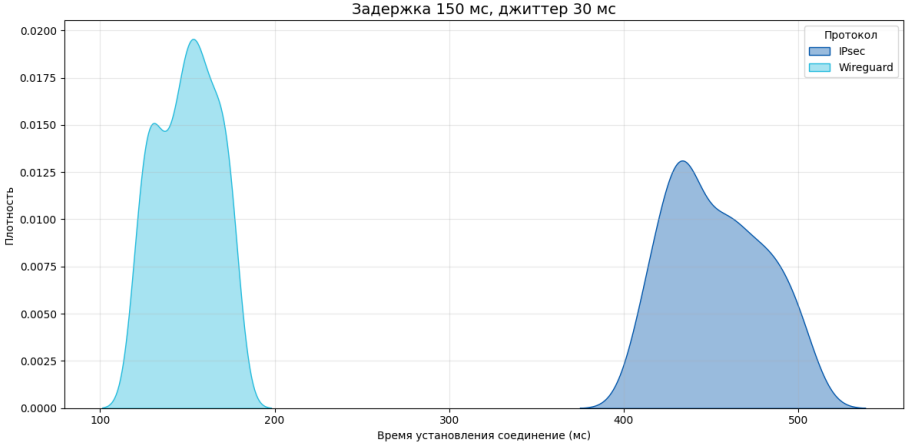
Топология Peer-To-Peer

Сертификаты не передаются в рамках протокола IKE



Топология Peer-To-Peer

Сертификаты не передаются в рамках протокола IKE

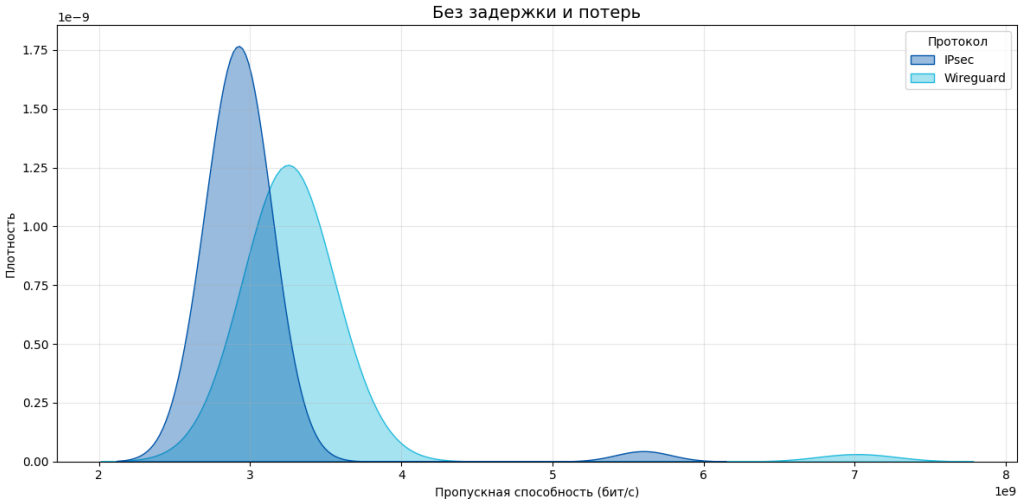


Топология Peer-To-Peer

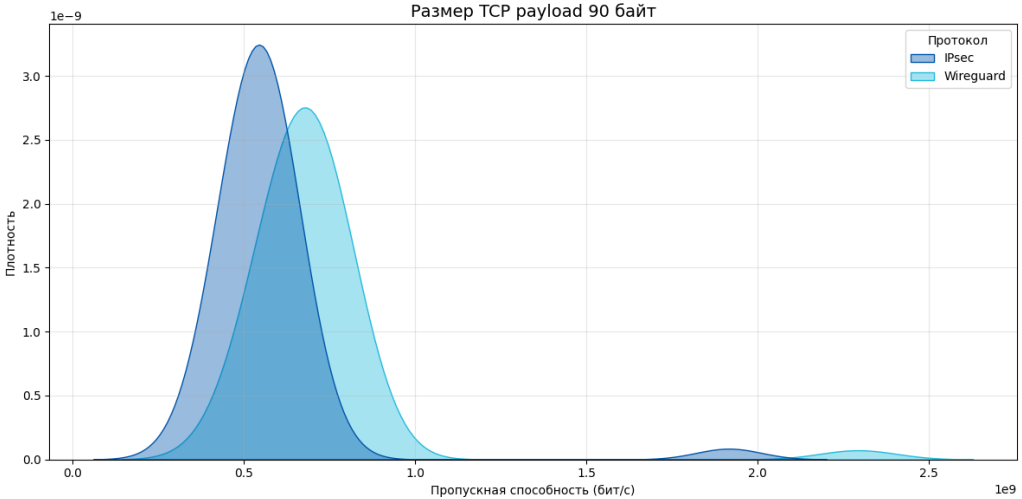
Сценарий	Протокол с преимуществом	Сценарий	Протокол с преимуществом
Пропускная способность		**RTT**	
TCP payload 90 байт	Wireguard	задержка 120 мс	IPsec
TCP payload 1398 байт	IPsec	задержка 130 мс	IPsec
TCP payload 1600 байт	IPsec	задержка 140 мс	IPsec
задержка 20 мс	Wireguard	потери пакетов 1%	IPsec
задержка 20 мс, джиттер 5 мс	Wireguard	**Время установления соединения**	
задержка 30 мс, джиттер 5 мс	Wireguard	все сценарии	Wireguard
потери пакетов 1%	IPsec		

Таблица 1: Статистически значимые различия, P2P, высокопроизводительные ядра

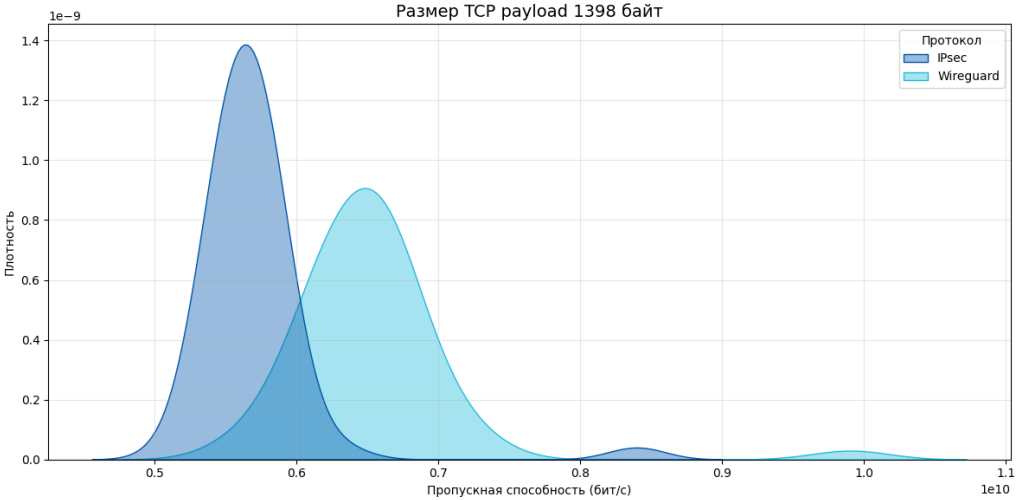
Топология Звезда, 2 ядра



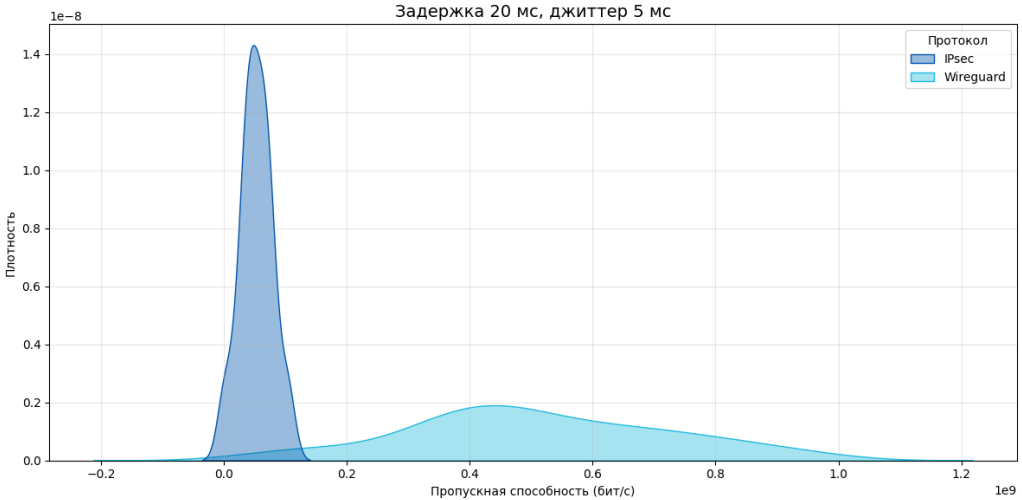
Топология Звезда, 2 ядра



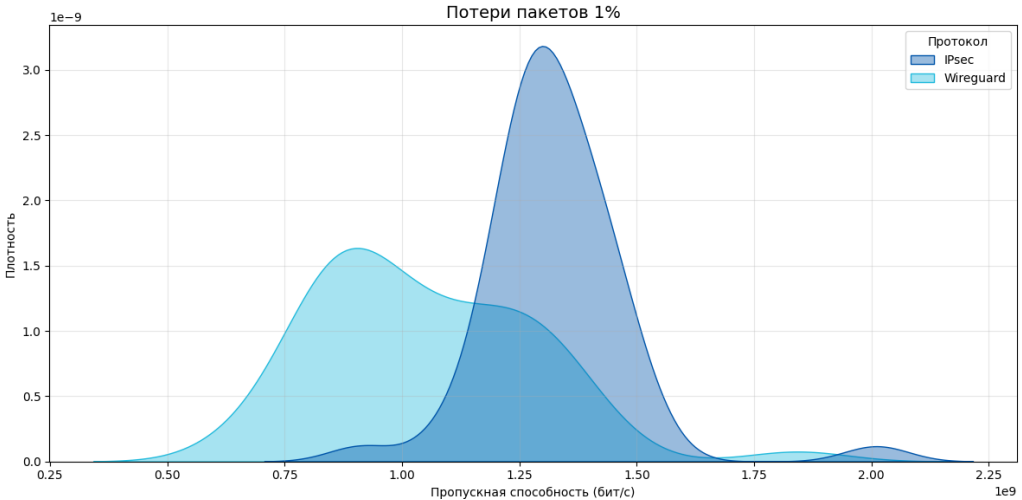
Топология Звезда, 2 ядра



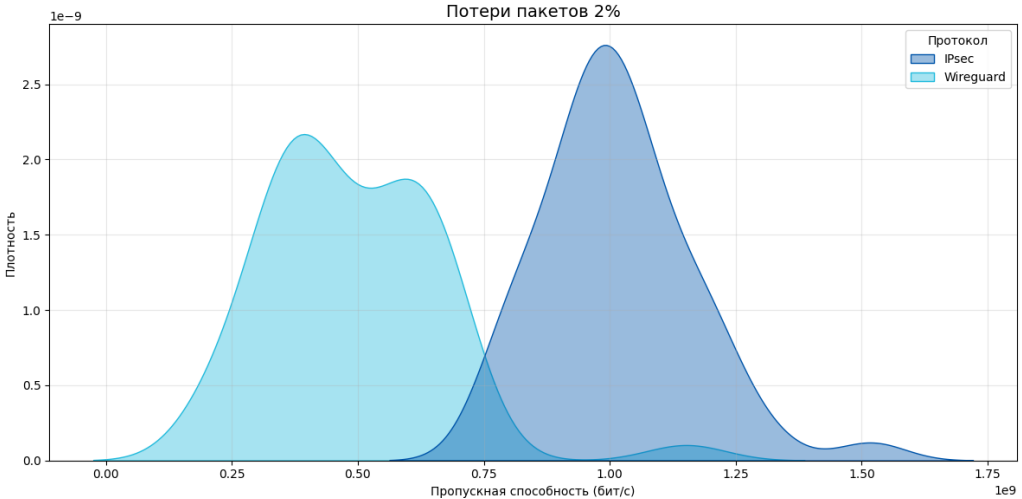
Топология Звезда, 2 ядра



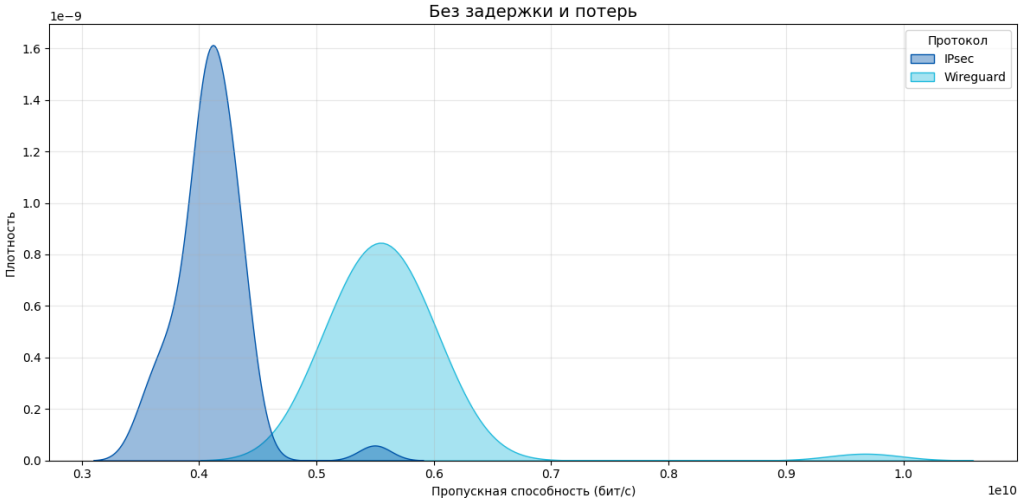
Топология Звезда, 2 ядра



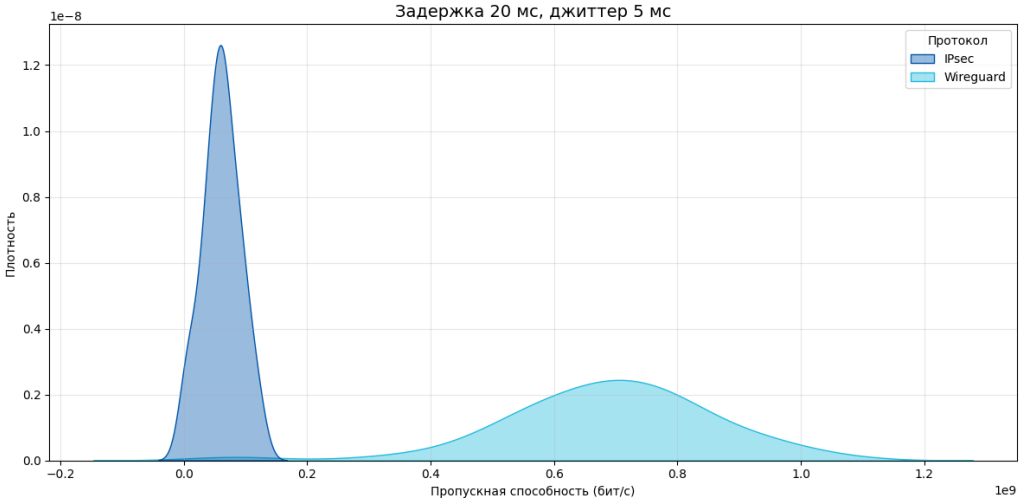
Топология Звезда, 2 ядра



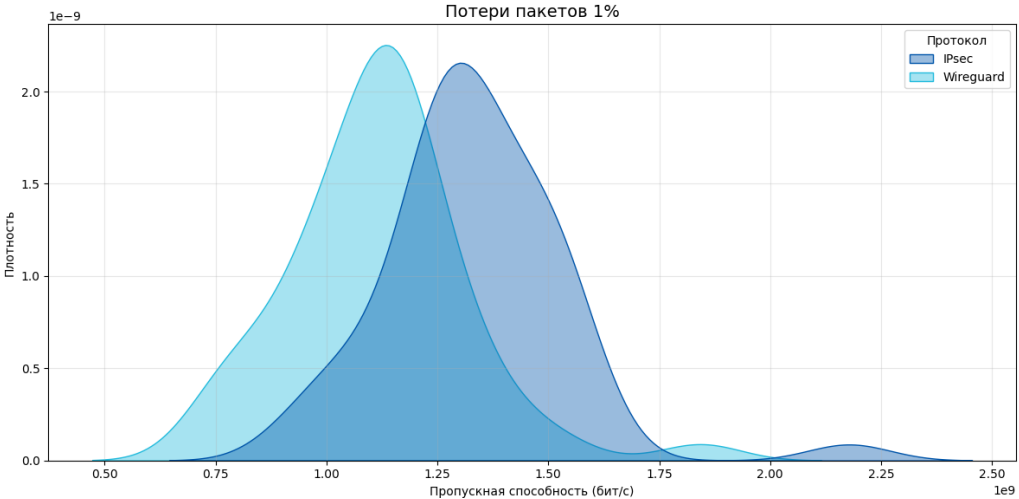
Топология Звезда, 4 ядра



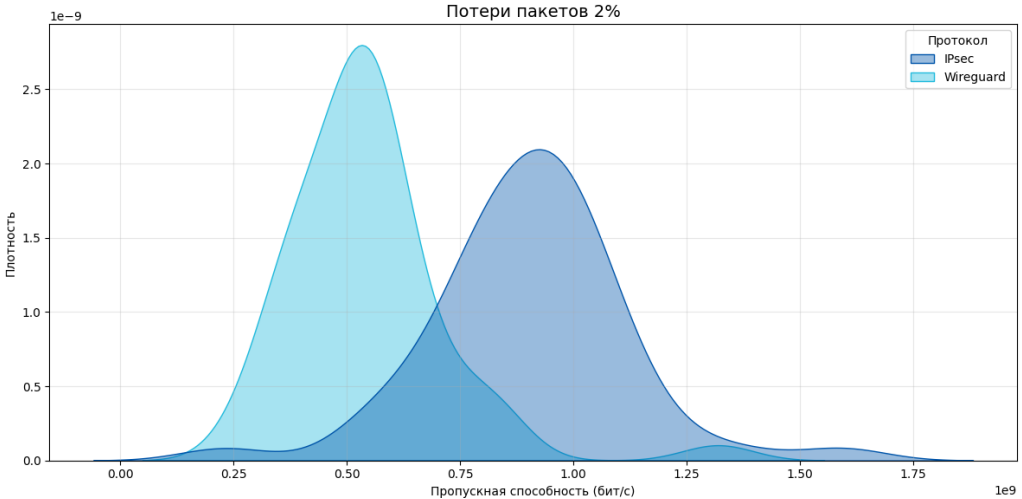
Топология Звезда, 4 ядра



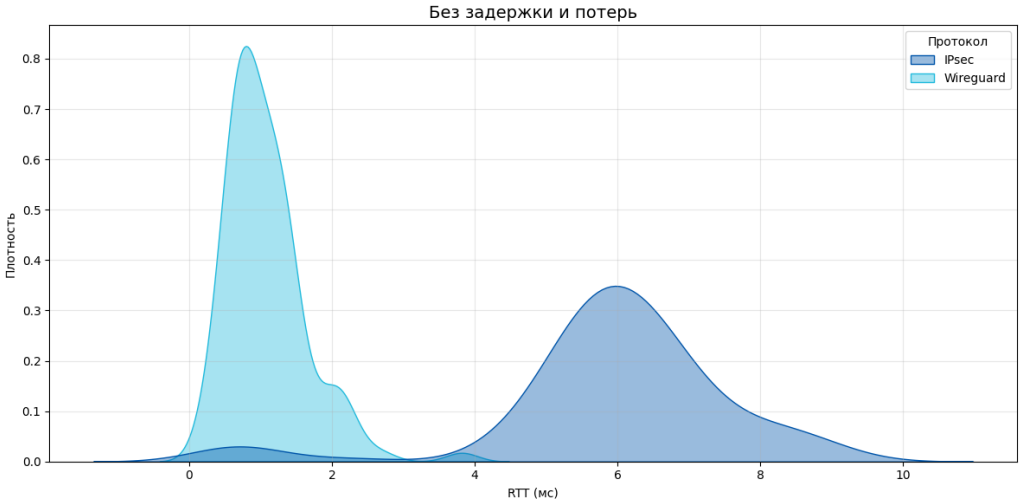
Топология Звезда, 4 ядра



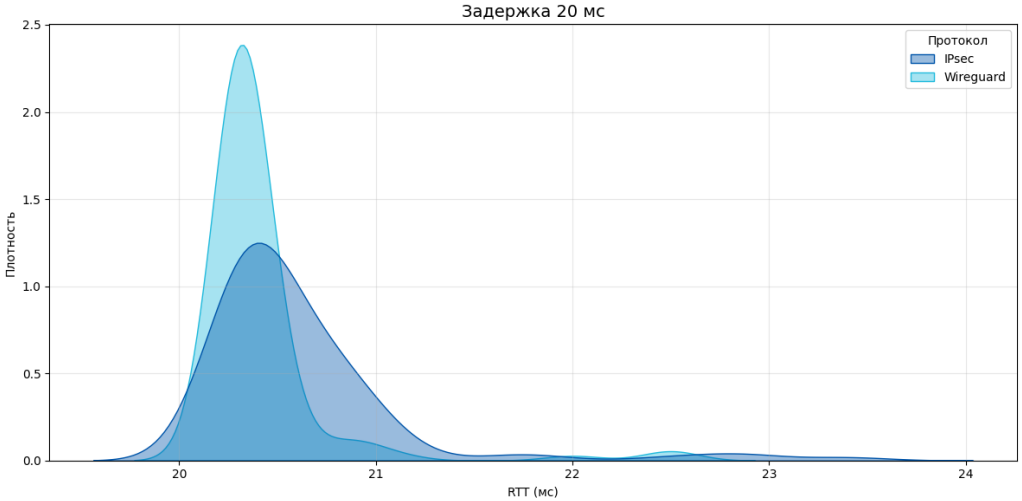
Топология Звезда, 4 ядра



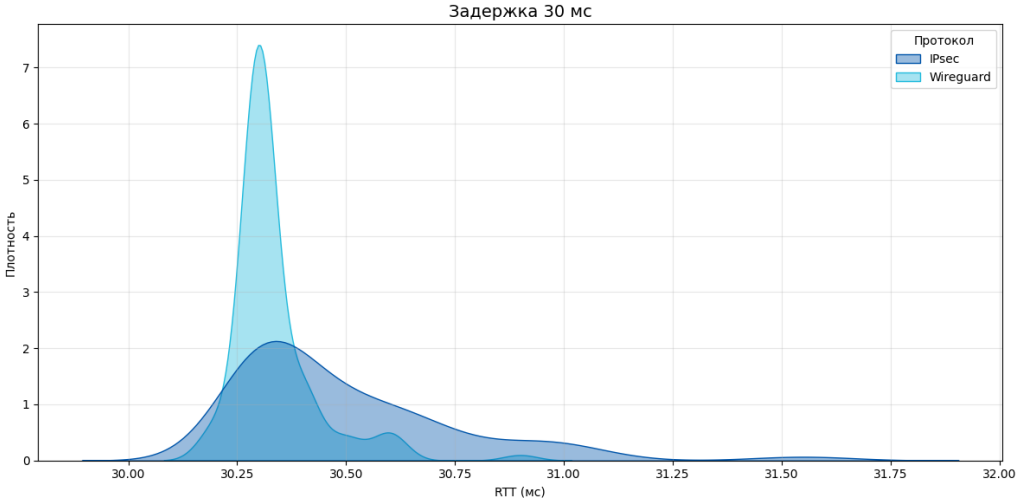
Топология Звезда, 2 ядра



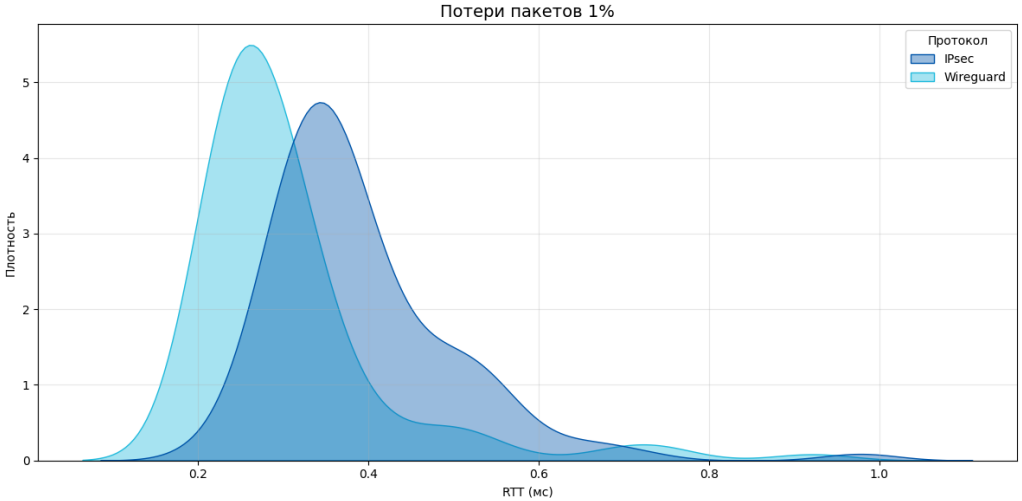
Топология Звезда, 2 ядра



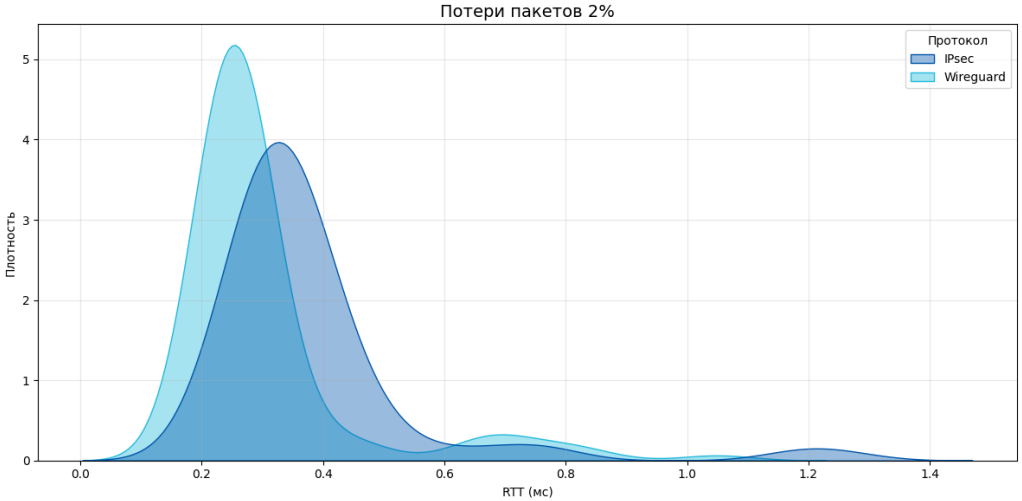
Топология Звезда, 2 ядра



Топология Звезда, 2 ядра



Топология Звезда, 2 ядра



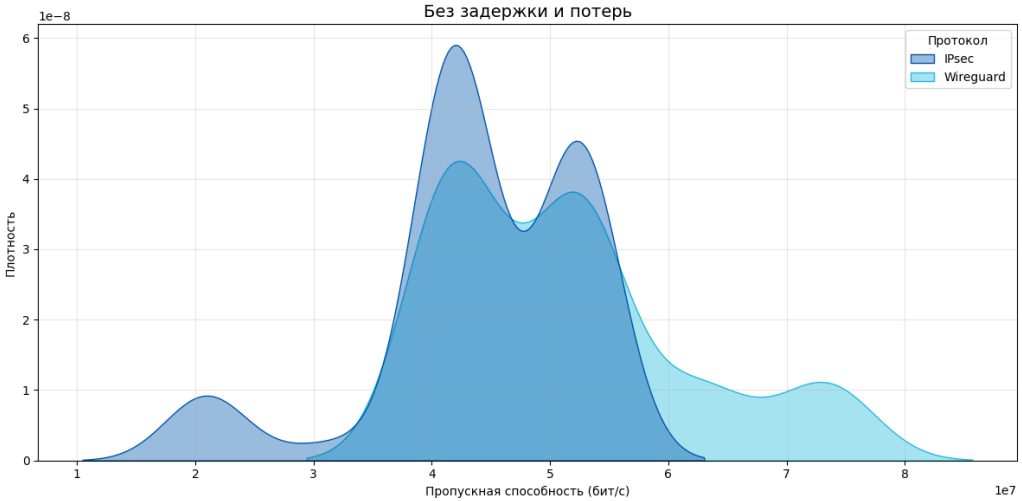
Топология Звезда

Сценарий	Протокол с преимуществом	Сценарий	Протокол с преимуществом
Пропускная способность, 2 ядра		**RTT**	
TCP payload 90 байт	Wireguard	Без задержки и потерь	Wireguard
TCP payload 1398 байт	Wireguard	задержка 20 мс	Wireguard
TCP payload 1600 байт	Wireguard	задержка 30 мс	Wireguard
задержка 20/30/40/50/200/150 мс, джиттер 5/5/10/10/20/30 мс	Wireguard	потери пакетов 1%	Wireguard
потери пакетов 1% , 2%	IPsec	потери пакетов 2%	Wireguard
Пропускная способность, 4 ядра		**Время установления соединения**	
TCP payload 90 байт	Wireguard	все сценарии	Wireguard
TCP payload 1398 байт	Wireguard		
TCP payload 1600 байт	Wireguard		
задержка 20/30/40/50/200/150 мс, джиттер 5/5/10/10/20/30 мс	Wireguard		
потери пакетов 1%, 2%	IPsec		

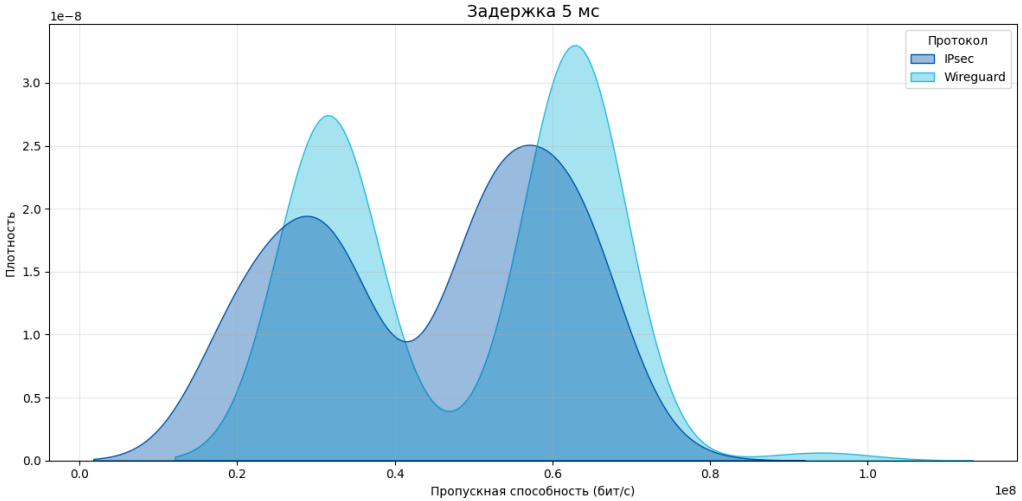
Таблица 2: Статистически значимые различия, Звезда, высокопроизводительные ядра

Сравнение реализаций на низкоресурсном микроконтроллере

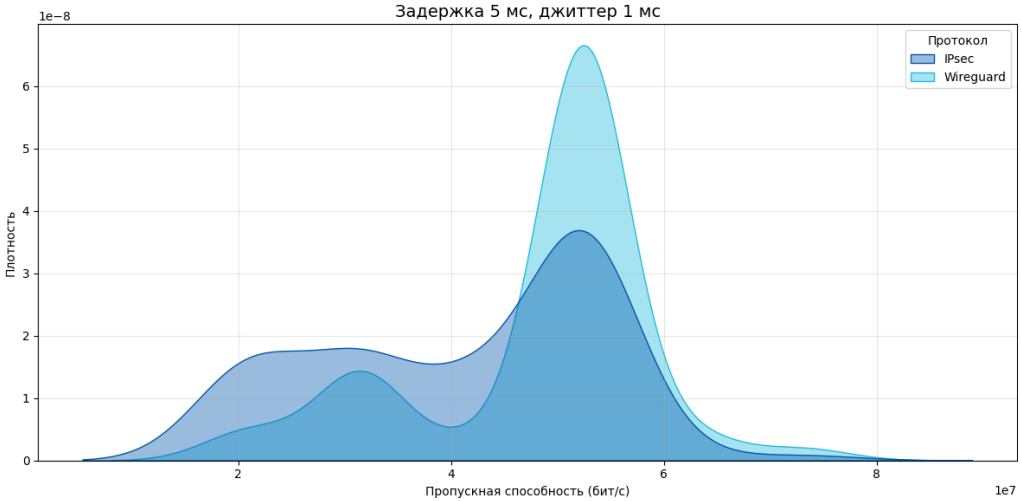
Топология Peer-To-Peer



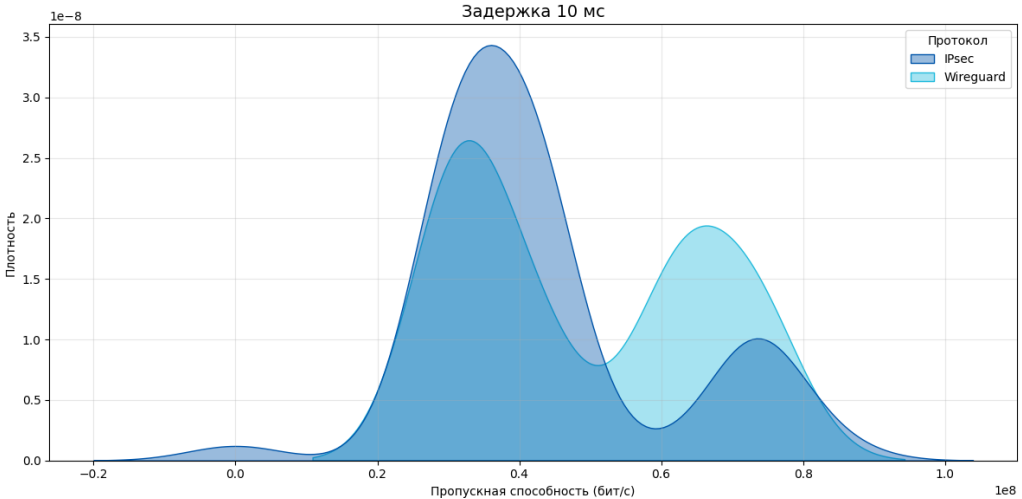
Топология Peer-To-Peer



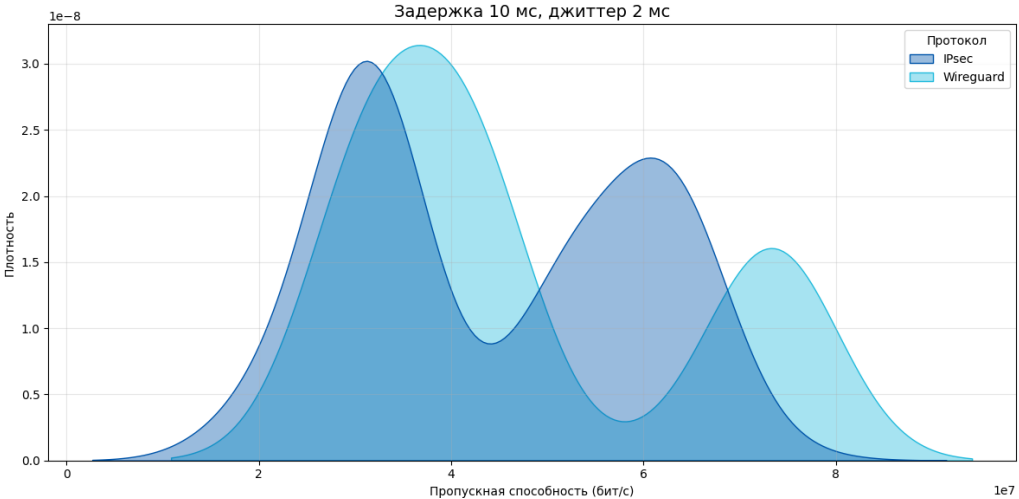
Топология Peer-To-Peer



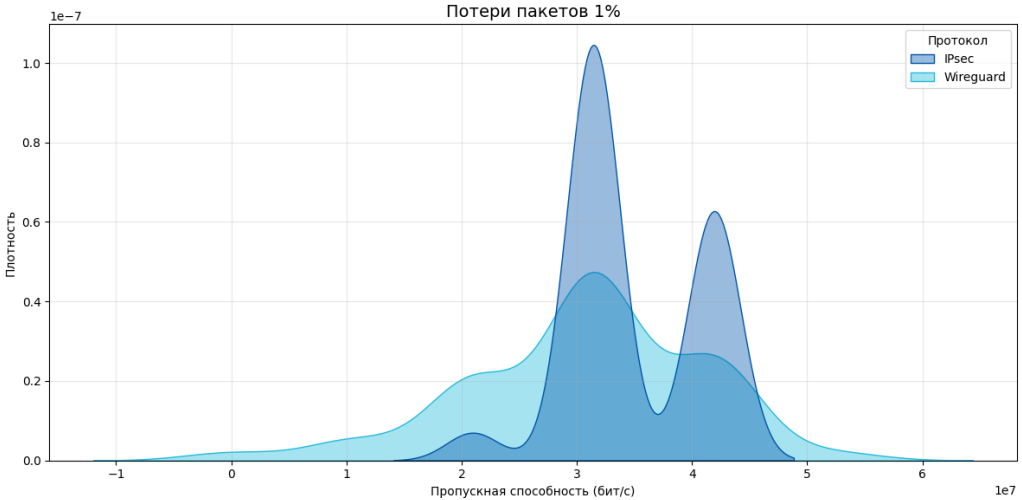
Топология Peer-To-Peer



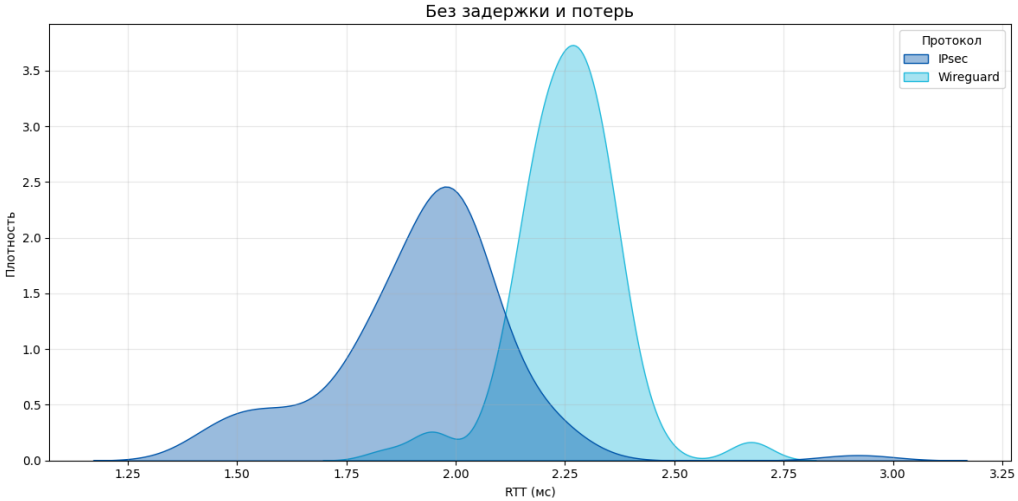
Топология Peer-To-Peer



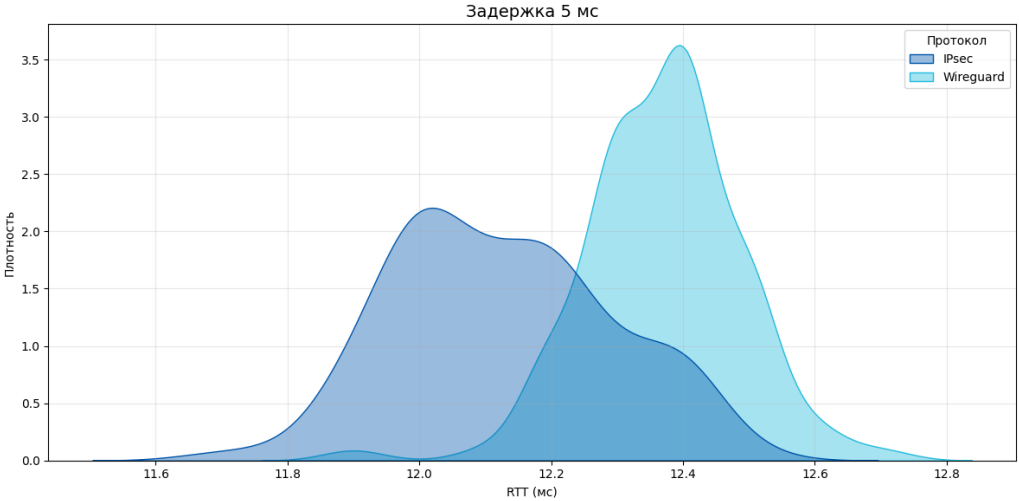
Топология Peer-To-Peer



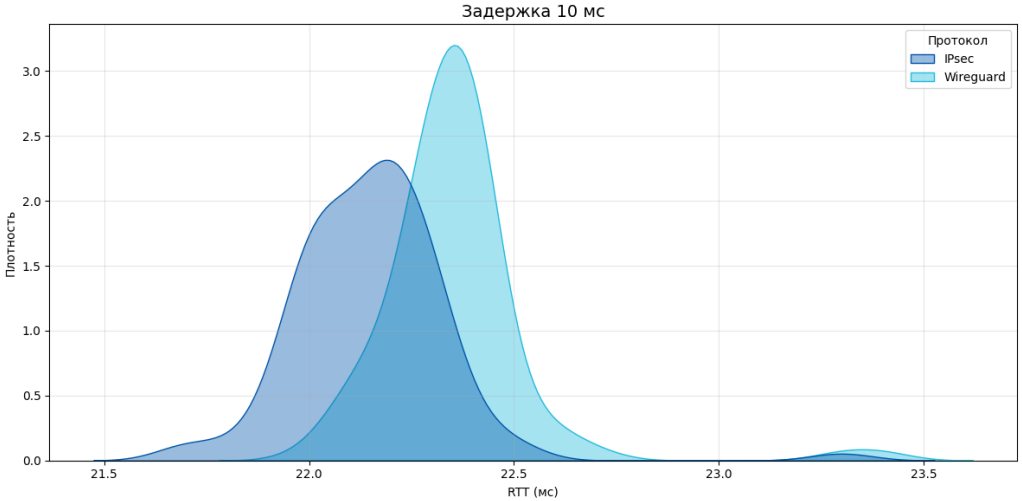
Топология Peer-To-Peer



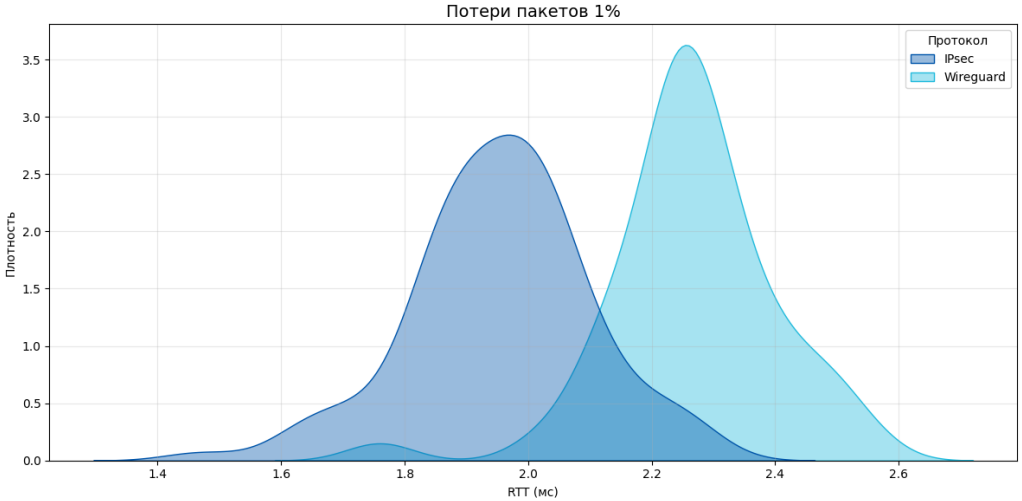
Топология Peer-To-Peer



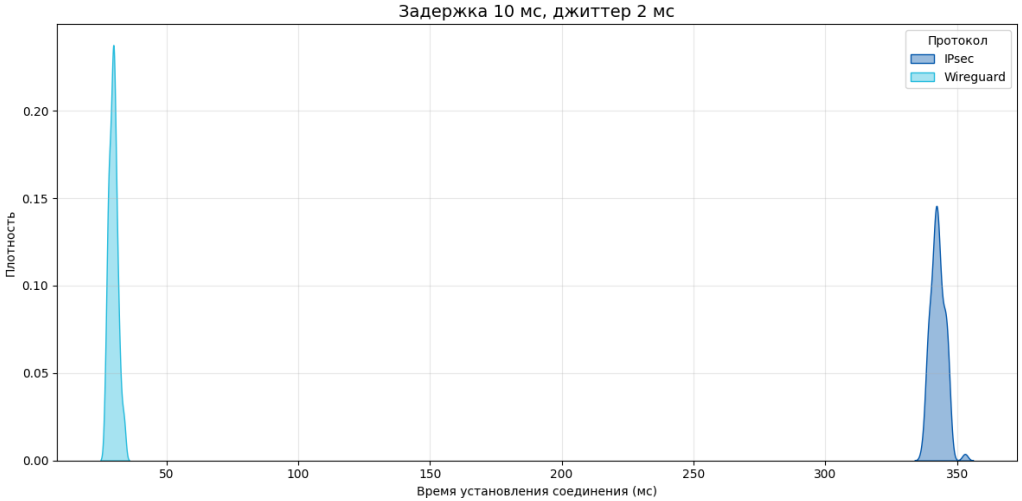
Топология Peer-To-Peer



Топология Peer-To-Peer



Топология Peer-To-Peer

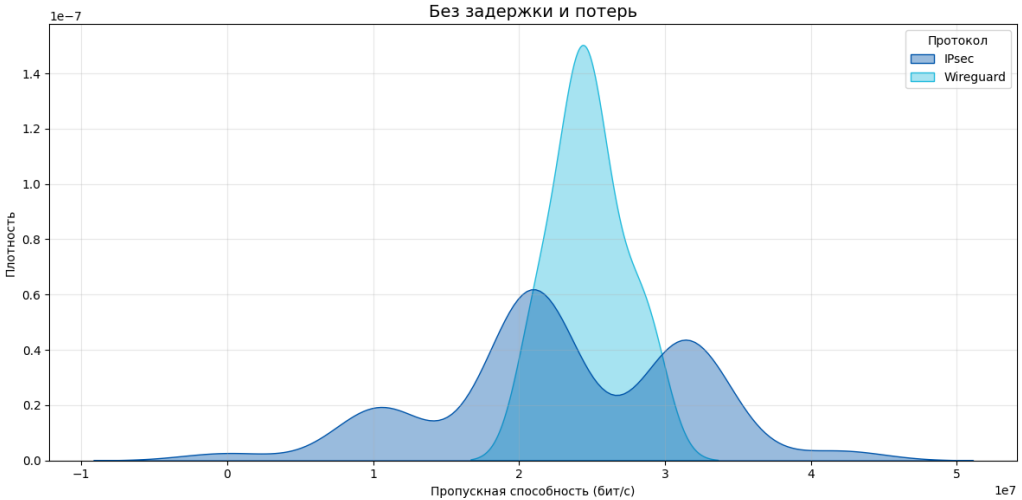


Топология Peer-To-Peer

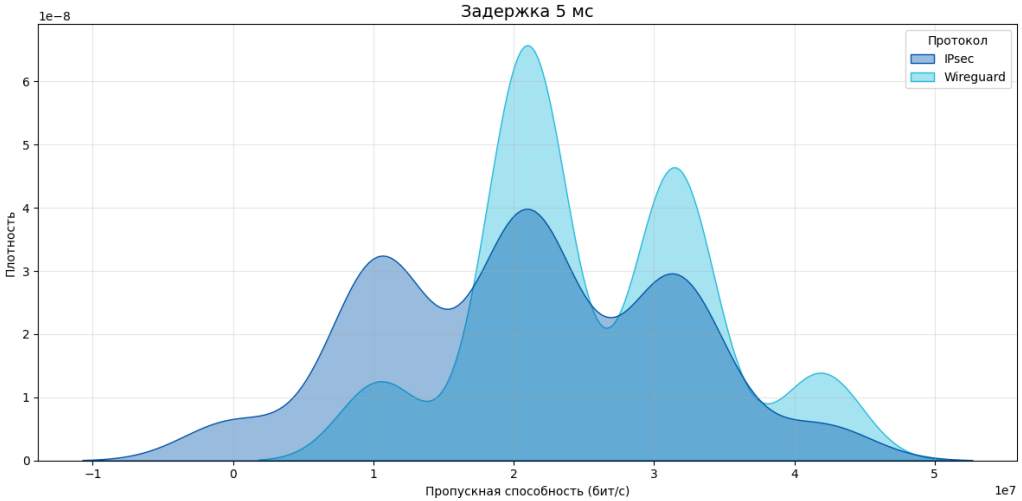
Сценарий	Протокол с преимуществом	Сценарий	Протокол с преимуществом
Пропускная способность		**RTT**	
TCP payload 1398 байт	Wireguard	Без задержек и потерь	IPsec
Задержка 5 мс	Wireguard	задержка 5 мс	IPsec
задержка 5 мс, джиттер 1 мс	Wireguard	задержка 10 мс	IPsec
задержка 10 мс	Wireguard	потери пакетов 1%	IPsec
задержка 10 мс, джиттер 2 мс	Wireguard	**Время установления соединения**	
потери пакетов 1%	IPsec	все сценарии	Wireguard

Таблица 3: Статистически значимые различия, P2P, низкоресурсный МК

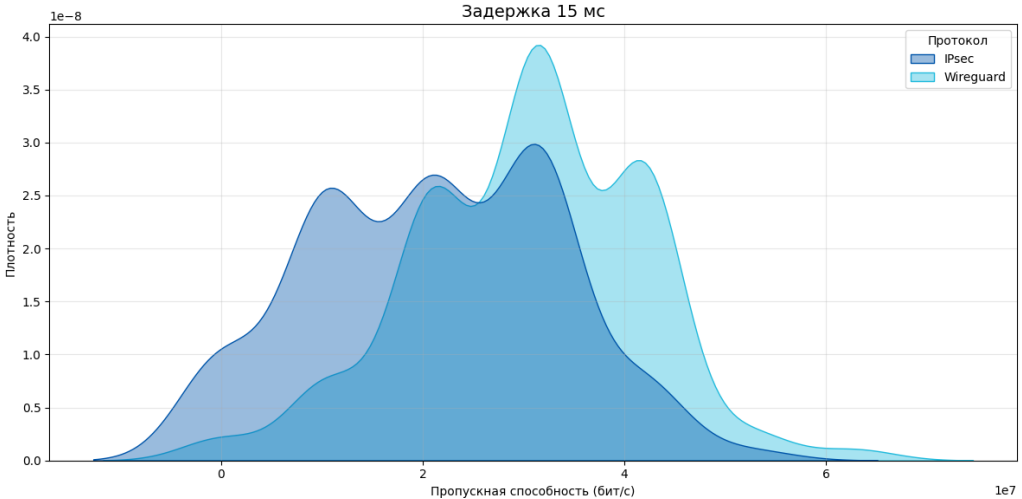
Топология Звезда



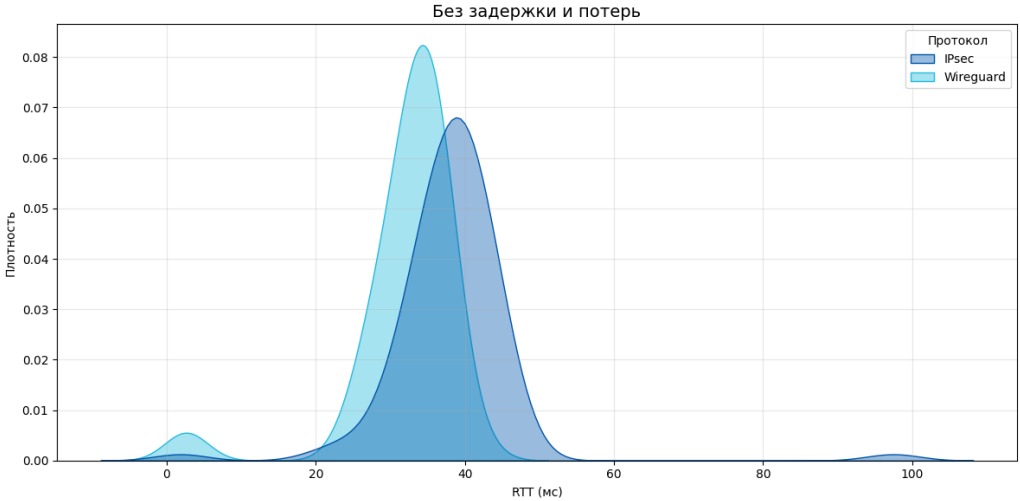
Топология Звезда



Топология Звезда



Топология Звезда



Топология Звезда

Сценарий	Протокол с преимуществом
Пропускная способность	
Без задержки и потерь	Wireguard
задержка 5 мс	Wireguard
задержка 15 мс	Wireguard
RTT	
все сценарии	Wireguard

Таблица 4: Статистически значимые различия, Звезда, низкоресурсный МК

Память на низкоресурсном микроконтроллере

IPsec: 5 КБ + 8 КБ × количество пиров
Wireguard: 0,25 КБ + 0,79 КБ × количество пиров

Количество пиров	IPsec	WireGuard
1	13 КБ	1,04 КБ
2	21 КБ	1,83 КБ
3	29 КБ	2,62 КБ
5	45 КБ	4,20 КБ

Таблица 5: Сравнение потребления памяти IPsec и WireGuard (в килобайтах)

Выводы

- **P2P на высокопроизводительных ядрах**: у WG больше пропускная способность на маленьких пакетах и с небольшими помехами в канале, меньше время установления соединения; у IPsec больше пропускная способность на больших пакетах и при потерях пакетов, а также меньше RTT;
- **Звезда на высокопроизводительных ядрах** Wireguard демонстрирует преимущество почти во всех сценариях, IPsec выигрывает только в пропускной способности при потерях пакетов;
- **P2P на низкоресурсном микроконтроллере**: Wireguard демонстрирует преимущество почти во всех сценариях с пропускной способностью, IPsec показывает меньше RTT в некоторых сценариях;
- **Звезда на низкоресурсном микроконтроллере** Wireguard демонстрирует преимущество в пропускной способности в сценариях с небольшой задержкой, а также во всех сценариях у Wireguard меньше RTT.

Спасибо
за внимание!

КОМПАНИЯ АКТИВ

vasin@aktiv-company.ru

www.rutoken.ru
www.aktiv-company.ru

+7 495 925-77-90

РусКрипто