УДК 004.056:004.7
МРНТИ 05.13.19

https://doi.org/10.55452/1998-6688-2025-22-4-209-218

[1]*Майлыбаев Е.К.,
PhD, ассоциированный профессор, ORCID ID: 0000-0002-1977-3690,
*e-mail: ersind@mail.ru
[2]Сейдалиева У.О.,
PhD, научный сотрудник, ORCID ID: 0000-0002-7190-6753,
e-mail: useidali@bu.edu

[1]Международный транспортно-гуманитарный университет, г. Алматы, Казахстан
[2]Университет Бостона, г. Бостон, США

ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННОГО СЕТЕВОГО ШЛЮЗА ДЛЯ ОБЛАЧНЫХ ПРИЛОЖЕНИЙ

Аннотация

Статья посвящена проектированию и настройке защищенного сетевого шлюза для облачных приложений на основе современных VPN-протоколов OpenVPN и WireGuard. В условиях активного развития облачных технологий и роста числа кибератак обеспечение защищенного удаленного доступа к сервисам становится ключевой задачей информационной безопасности. Рассматриваются актуальные угрозы, возникающие при передаче данных в облачных средах, и показана роль VPN-технологий в предотвращении атак. Подробно анализируются особенности OpenVPN и WireGuard: архитектура, криптографическая база, удобство настройки и производительность. В работе представлена архитектура шлюза, включающая сервер VPN, межсетевые фильтры и механизмы маршрутизации, обеспечивающие принудительное прохождение всего трафика через зашифрованный туннель. Эксперименты, проведенные в виртуализированной среде VMware Workstation, показали, что WireGuard демонстрирует более высокую скорость передачи данных и низкую задержку, тогда как OpenVPN отличается гибкостью и совместимостью с корпоративными системами. Совместное использование обоих протоколов позволяет повысить отказоустойчивость и адаптивность системы. Практическая значимость исследования заключается в возможности внедрения предложенной архитектуры в корпоративных и частных сетях для защиты облачных приложений, организации удаленного доступа сотрудников и повышения уровня безопасности информационных ресурсов.

Ключевые слова: облачные приложения, информационная безопасность, защищенный шлюз, шифрование, сетевые протоколы.

Введение

Современные облачные технологии предоставляют широкие возможности для хранения, обработки и передачи данных. Однако их использование сопряжено с рисками: перехват трафика, несанкционированный доступ, атаки типа «человек посередине». В этих условиях VPN (Virtual Private Network) остается одним из наиболее эффективных инструментов защиты коммуникаций [1].

Использование полной шифрации пакетов в VPN обеспечивает устойчивость к обнаружению и блокировкам, что подтверждает актуальность VPN как средства защиты коммуникаций [2]. OpenVPN и WireGuard являются двумя наиболее распространенными решениями в данной области [3, 4]. Первый отличается зрелостью и гибкостью, второй – высокой скоростью и минималистичной архитектурой. Ряд исследований подтверждает эти различия. Так, Jason и Donenfeld показали, что WireGuard превосходит традиционные VPN по пропускной способности и задержкам [5], а работы Joel Anyam и соавторов подчеркивают широкую применимость OpenVPN в корпоративных инфраструктурах благодаря богатой поддержке криптографических алгоритмов [6].

Несмотря на популярность обоих протоколов, недостаточно исследований, комплексно рассматривающих их совместное применение в архитектуре защищенного шлюза для облачных приложений. Цель статьи – восполнить данный пробел и предложить практическую модель шлюза, обеспечивающего баланс между безопасностью и производительностью.

Несмотря на то что основное внимание уделено построению защищенного шлюза для взаимодействия с облачными приложениями, реализация производилась в виртуализированной среде VMware Workstation. Это обусловлено ограничениями по бюджету и отсутствием доступа к коммерческим облачным платформам. Тем не менее вся архитектура решения и используемые протоколы сохраняют полную переносимость на облачные среды, такие как Microsoft Azure, Amazon EC2, DigitalOcean и др. Принципы построения VPN-туннеля, маршрутизации и фильтрации трафика остаются актуальными вне зависимости от среды развертывания.

Материалы и методы

Рост интереса к построению защищенных сетевых шлюзов в современных условиях напрямую связан с увеличением числа пользователей, подключающихся к облачным сервисам из нестабильных или потенциально уязвимых сетей, будь то домашние подключения, публичные Wi-Fi сети или мобильный Интернет. В рамках данной работы ставится задача разработки практического решения, которое обеспечит безопасный обмен данными при взаимодействии с облачными приложениями, используя актуальные технологии VPN на базе протоколов OpenVPN и WireGuard.

В начальной фазе исследование ориентировано на определение характерных уязвимостей, связанных с передачей данных в облачной среде. При этом особое внимание уделяется сценариям, в которых конечные устройства пользователей подключаются к облачным платформам через ненадежные каналы связи, что делает необходимым внедрение дополнительного слоя защиты.

Следующий этап предполагает выбор технических решений, способных снизить указанные риски. В качестве приоритетных рассматриваются VPN-протоколы, предлагающие защищенный способ взаимодействия с удаленными ресурсами. В данном контексте OpenVPN выступает как проверенное временем решение с гибкой настройкой, тогда как WireGuard рассматривается как инновационная альтернатива, ориентированная на производительность и упрощение архитектуры. Оценка обоих протоколов проводится с учетом условий их интеграции в разнородные информационно-технические среды, а также способности противостоять распространенным угрозам.

Однако исследование не сводится исключительно к выбору программного обеспечения. Одной из важнейших задач становится формирование архитектурной модели шлюза, включающей маршрутизацию, механизмы шифрования, контроль трафика и способы аутентификации.

Исследование проводится в изолированной среде на базе виртуальных машин, что дает возможность моделировать реальные условия эксплуатации и воссоздавать потенциально нестандартные ситуации: обрыв соединения, попытку несанкционированного доступа, пиковую нагрузку. Это позволяет объективно проверить, насколько предложенное решение соответствует требованиям стабильности и защищенности.

Исследование строится не только на изучении теоретических основ. Его важной составляющей является практическая реализация и проверка работоспособности разрабатываемого шлюза. С одной стороны, проводится аналитический обзор литературных и нормативных источников, касающихся VPN, криптографических методов и архитектур безопасности. С другой – выполняется пошаговая настройка и отладка шлюза, включающая использование командной строки, работу с конфигурационными файлами, анализ логов и устранение ошибок. Такой подход позволяет получить всестороннее понимание не только логики работы системы, но и особенностей ее внедрения.

Различия между протоколами особенно заметны на этапе внедрения в реальные сети. OpenVPN отлично подходит для компаний с развитой инфраструктурой, нуждающихся в продвинутой маршрутизации, дифференцированных правах доступа и подключении к внутренним сервисам – LDAP, Active Directory и централизованным системам логирования. Он дает возможность гибкой настройки политик, включая ограничение по IP-диапазонам, времени активности и уровню доступа конкретных клиентов, что делает его мощным инструментом для администрирования.

WireGuard, напротив, оптимизирован под задачи, в которых ключевыми являются скорость и простота использования. Он показывает высокие показатели производительности даже на слабом оборудовании: одноплатных ПК, роутерах и IoT-устройствах. Подключения устанавливаются мгновенно, восстанавливаются автоматически при смене сетей и не требуют ручного вмешательства для обновления настроек. Эти свойства делают WireGuard привлекательным для мобильных решений, DevOps-инфраструктур и проектов, где ресурсы ограничены, а стабильность критична.

Для удобства восприятия ключевых различий между OpenVPN и WireGuard их характеристики представлены в таблице 1.

Таблица 1 – Сравнение характеристик OpenVPN и WireGuard

Параметр	OpenVPN	WireGuard
Архитектура	Модульная, основана на TLS	Минималистичная, встроена в ядро Linux
Шифрование	AES-256, Blowfish, CAST5 и др.	ChaCha20, Curve25519 (фиксированные)
Настройка	Гибкая, но сложная	Простая, единый конфигурационный файл
Производительность	Средняя (зависит от параметров)	Высокая, особенно на Linux-платформах
Поддержка платформ	Широкая, включая Windows, MacOS, Linux	Ограничена на старых ОС, лучше всего работает на Linux
Совместимость с корпоративными политиками	Высокая	Требует адаптации
Применимость	Корпоративные сети, ЦОДы, сложная маршрутизация	Личные VPN, DevOps, мобильные устройства

В рамках статьи оба протокола рассматриваются как взаимодополняющие, а не конкурирующие решения. Их параллельное использование позволяет реализовать адаптивную архитектуру, в которой конечный пользователь самостоятельно выбирает наиболее подходящий вариант подключения. Такой подход расширяет возможности конфигурации, увеличивает гибкость системы и дает возможность более точного анализа эффективности каждого из протоколов в условиях реальной эксплуатации.

Результаты и обсуждение

Функциональная схема работы защищенного сетевого шлюза формируется вокруг четко организованного взаимодействия между центральной серверной частью и множеством клиентских устройств, объединенных в рамках логически замкнутой инфраструктуры. Основная задача этой системы заключается в создании устойчивого, безопасного и управляемого канала передачи данных, по которому весь пользовательский сетевой трафик проходит в зашифрованном виде. Центральным элементом в данной архитектуре выступает VPN-сервер, на котором реализуются функции шифрования, маршрутизации, управления сессиями и контроля по-

литик доступа. Визуальная структура взаимодействия всех компонентов шлюза представлена на рисунке 1.

Рисунок 1 – Общая схема работы защищенного сетевого шлюза

В результате формируется схема, в которой каждый этап – от подключения до контроля трафика – охватывается специализированным набором механизмов. Это позволяет выстраивать надежную и в то же время гибкую инфраструктуру, адаптируемую под различные сценарии эксплуатации. Шлюз не просто обеспечивает защищенную коммуникацию, но и формирует основу для построения более сложных сетевых решений, сохраняя при этом прозрачность конфигурации и управляемость.

Для реализации защищенного туннеля между клиентом и сервером необходимо предварительно установить и настроить OpenVPN.

Была выполнена полная настройка серверной части OpenVPN с использованием Easy-RSA 3.x. Реализованы все ключевые этапы криптографической подготовки: инициализация центра сертификации, выпуск серверного сертификата, генерация параметров шифрования и создание ключей безопасности. Также подробно рассмотрены процессы формирования и подписи клиентского сертификата, что обеспечило готовность инфраструктуры к безопасному взаимодействию между сервером и клиентами через VPN-туннель.

На рисунке 2 отображается подтверждение успешного подключения и факт маршрутизации трафика через установленное VPN-соединение. Это свидетельствует о корректной настройке и работоспособности всей криптографической инфраструктуры, развернутой с использованием Easy-RSA 3.x как на серверной, так и на клиентской стороне.

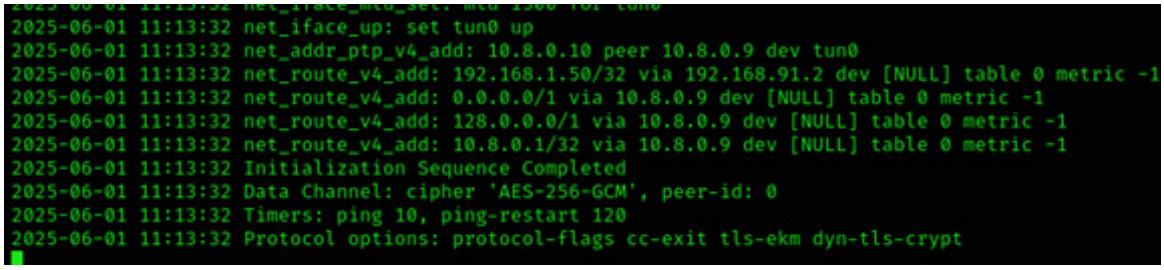

Рисунок 2 – Запуск и проверка состояния сервиса OpenVPN

Для реализации второго VPN-протокола в рамках защищенного шлюза используется WireGuard. Он отличается компактной архитектурой, высокой производительностью и простотой конфигурации. В отличие от OpenVPN, данный протокол не требует развертывания центра сертификации, а использует статические ключи, что делает его особенно удобным в условиях ограниченных вычислительных ресурсов.

Завершающим этапом настройки VPN-сервера является активация механизма переадресации IP-трафика, необходимого для обеспечения маршрутизации клиентских данных через защищенный туннель. Этот параметр позволяет передавать пакеты от подключенных клиентов во внешние сети, действуя как маршрутизатор. Включение данной функции выполняется путем изменения системной сетевой конфигурации, отвечающей за пересылку IPv4-пакетов между интерфейсами. Проверка активности соединения производится командой «sudo wg show», результат которой представлен на рисунке 3.

```
kalmar@kalmar-VMware-Virtual-Platform:~$ sudo wg
interface: wg0
  public key: 0FYMzmQ/EivNsi8YLXvawKTAcD2mLsUVpZ8z2irITno=
  private key: (hidden)
  listening port: 51820

peer: KHiIRGMJAGpL2WD5bJb5XPCVjxI7CWwrc1IaAX2UuWA=
  endpoint: 192.168.1.17:61869
  allowed ips: 10.10.10.2/32
  latest handshake: 25 seconds ago
  transfer: 12.21 KiB received, 764 B sent
kalmar@kalmar-VMware-Virtual-Platform:~$
```

Рисунок 3 – Проверка состояния соединения WireGuard

Реализация механизма сетевой фильтрации в рамках защищенного шлюза осуществляется с использованием UFW (Uncomplicated Firewall) – утилиты, предоставляющей упрощенный интерфейс для управления встроенным в систему инструментом iptables. Данный подход позволяет значительно упростить настройку базовых политик межсетевого экранирования, не снижая при этом уровня безопасности. В соответствии с принятой моделью «запрет по умолчанию» все входящие подключения блокируются, за исключением явно разрешенных правил. В данной конфигурации открываются только те порты, которые необходимы для функционирования туннельных протоколов OpenVPN и WireGuard. Это обеспечивает ограничение внешнего доступа к инфраструктуре, минимизируя возможные точки входа.

Помимо портовой фильтрации, важным аспектом является принудительная маршрутизация всего клиентского трафика исключительно через VPN-туннель. Такая мера позволяет полностью исключить вероятность обхода защищенной инфраструктуры и утечки данных в открытый Интернет. Для пользователей OpenVPN данная функция активируется с помощью параметров конфигурации, перенаправляющих весь трафик через виртуальный интерфейс сервера. Аналогичный эффект достигается в WireGuard путем указания маршрутов в параметре, который задает полный перечень IP-адресов, доступных только через шлюз. В результате весь пользовательский трафик направляется строго через VPN, обеспечивая централизованную фильтрацию, контроль и защиту. Схематическое представление архитектуры маршрутизации и фильтрации приведено на рисунке 4.

Хотя практическая реализация осуществлялась в локальной лабораторной среде, полученные результаты и структура решения позволяют утверждать, что оно может быть адаптировано для использования в публичных или частных облаках. Это делает предложенный подход универсальным и применимым в реальных условиях эксплуатации защищенных удаленных подключений.

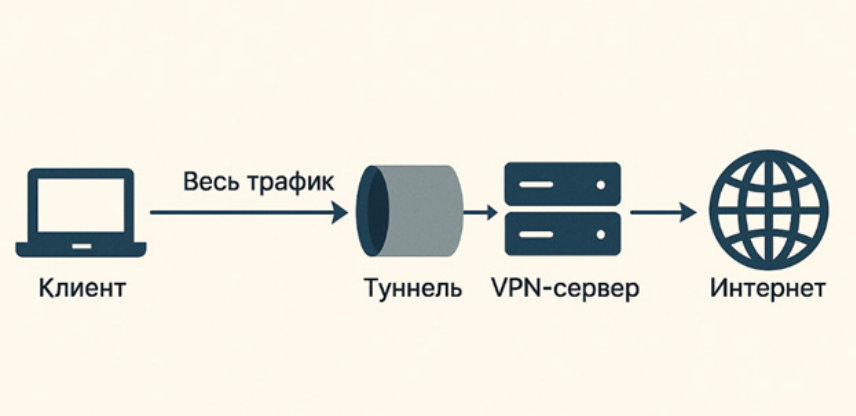

Рисунок 4 – Схема принудительной маршрутизации
всего трафика клиента через VPN

Таким образом, формируется логически замкнутая схема, в которой любые сетевые взаимодействия клиента происходят исключительно через контролируемый шлюз. Сам шлюз, в свою очередь, осуществляет мониторинг и управление всем трафиком, как входящим, так и исходящим. Такой подход особенно актуален в условиях использования публичных или ненадежных сетей, где критично обеспечить полное доверие только к одному – туннелированному каналу доступа.

Для повышения наглядности и ускорения процессов настройки в ходе тестирования использовались графические пользовательские интерфейсы (GUI), доступные в клиентских и серверных решениях для обеих технологий. Тестовая среда была развернута на виртуальных машинах, функционирующих под управлением операционных систем Ubuntu Desktop и Kali Linux. Виртуальные машины были соединены через комбинированную схему bridge-сетей, что позволило смоделировать как локальные, так и внешние подключения. Такая конфигурация обеспечивала достаточный уровень реализма для оценки поведения VPN в условиях, приближенных к реальной эксплуатации.

Сравнительные характеристики протокола WireGuard часто анализируются в сопоставлении с OpenVPN. Эти наблюдения особенно важны для оценки применимости технологии в высоконагруженных распределенных системах [7].

На основании результатов, полученных в ходе экспериментальной проверки работы VPN-шлюзов, выполнено сопоставление характеристик двух исследуемых протоколов – OpenVPN и WireGuard. В сравнении учитывались как количественные показатели (задержка, потери пакетов), так и качественные характеристики, фиксируемые визуально или через команды мониторинга.

Значения средней задержки при передаче пакетов в туннеле WireGuard оказались ниже и составили около 0.5 мс, в то время как для OpenVPN этот показатель находился в пределах 1 мс. Максимальная задержка у WireGuard также была ниже (1 мс против 2 мс у OpenVPN), что может свидетельствовать о более эффективной обработке трафика внутри ядра операционной системы. Потери пакетов при работе обоих протоколов отсутствовали, что демонстрирует их стабильность в контролируемой среде. Результаты эксперимента указаны в таблице 2.

Скорость установления соединения в WireGuard визуально выше: подключение происходило практически мгновенно, тогда как OpenVPN демонстрировал небольшую задержку при запуске. Мониторинг трафика с помощью утилиты nload показал наличие активности в обоих случаях, что подтверждает работоспособность туннелей. TTL в ответах на ICMP-запросы в обоих случаях составлял 64, что указывает на одноступенчатую маршрутизацию без промежуточных узлов.

Таблица 2 – Сравнительные характеристики OpenVPN и WireGuard по результатам тестирования

Метрика	OpenVPN	WireGuard
Средняя задержка (мс)	1	0.5
Максимальная задержка (мс)	2	1
Потери пакетов (%)	0	0
Загрузка CPU (%)	7	2.5
Криптоустойчивость (оценка)	4.5	5

Нагрузка на центральный процессор при функционировании VPN-соединения замерялась при помощи команды top. В процессе наблюдений средняя загрузка CPU при работе OpenVPN составила порядка 6–8%, в то время как у WireGuard данный показатель оказался значительно ниже и не превышал 2–3%. Это может быть связано с тем, что WireGuard реализован в пространстве ядра и обладает более компактной архитектурой.

Дополнительный критерий анализа – уровень криптографической защищенности. Протокол OpenVPN применяет такие проверенные алгоритмы, как AES-256, TLS, и инфраструктуру открытых ключей (PKI), что обеспечивает высокий уровень криптостойкости. Однако высокая гибкость настройки сопровождается риском ошибок конфигурации. В отличие от него, WireGuard использует современный стек алгоритмов: ChaCha20, Curve25519, Poly1305 и BLAKE2s, реализуемых в виде минималистичной схемы. Такая структура снижает вероятность конфигурационных уязвимостей и повышает общее доверие к безопасности соединения.

Для наглядного представления различий между протоколами по числовым показателям – задержке, загрузке CPU и криптостойкости – построена сравнительная диаграмма (рисунок 5).

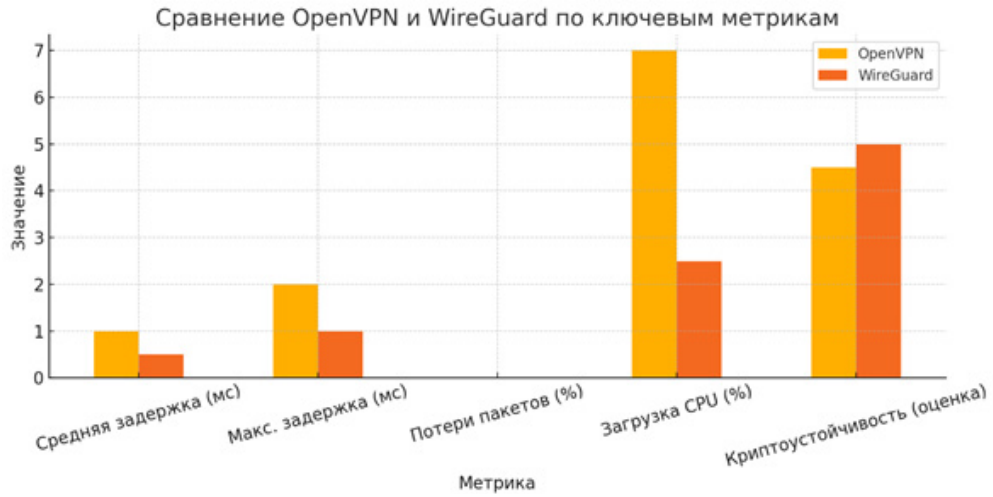

Рисунок 5 – Диаграмма различий между OpenVPN
и WireGuard по ключевым метрикам

На основании совокупности вышеуказанных наблюдений можно сделать вывод, что протокол WireGuard демонстрирует лучшие результаты по ряду ключевых показателей, включая контрольный трафик, стабильность и криптографическую надежность, при этом оставаясь более простым в конфигурации и эксплуатации.

Таким образом, несмотря на идентичный функционал – создание защищенного туннеля, протоколы OpenVPN и WireGuard показали различия в скорости установления соединения, нагрузке на систему и сложности конфигурации. В условиях ограниченной инфраструктуры и необходимости быстрого развертывания предпочтительным решением можно считать WireGuard, однако выбор должен основываться на политике безопасности организации и инфраструктурных возможностях.

Заключение

В ходе исследования были выполнены проектирование, реализация и комплексная настройка защищенного сетевого шлюза на основе протоколов OpenVPN и WireGuard, а также проведена всесторонняя проверка его работоспособности и безопасности. Достигнуты результаты, подтверждающие эффективность предложенного решения в условиях ограниченных вычислительных ресурсов и повышенных требований к защите трафика.

Были проанализированы существующие подходы к построению VPN-сетей, изучены особенности архитектуры OpenVPN и WireGuard, а также проведен сравнительный обзор их функциональных возможностей. Основное внимание было уделено характеристикам безопасности, способам аутентификации, принципам маршрутизации и механизму защиты от атак.

Развернут шлюз в виртуальной среде с последовательной настройкой каждого из VPN-сервисов, внедрение механизма сетевой фильтрации и реализации политики «только через туннель». Проведенные тесты позволили выявить различия в производительности, времени подключения, отклике системы на сбои и потреблении ресурсов. WireGuard продемонстрировал лучшую эффективность по всем ключевым метрикам, в то время как OpenVPN обеспечил более широкие возможности управления и интеграции.

Безопасность предложенного решения была подтверждена серией испытаний, в ходе которых проверялась корректность изоляции, туннелирования трафика, устойчивость к несанкционированным подключениям и сбоям. Все тесты показали соответствие реализованной схемы базовым принципам защищенного сетевого взаимодействия. В частности, была достигнута полная недоступность внутренних ресурсов вне VPN-туннеля, а также устойчивость к подмене ключей, отказам соединения и попыткам обхода фильтрации.

Таким образом, исследование имеет прикладной характер и может быть адаптировано для использования в реальных условиях – как в учебных лабораториях, так и в корпоративных средах, где требуется построение надежного канала удаленного доступа с минимальной нагрузкой на инфраструктуру. Полученные результаты подтверждают целесообразность применения предложенного подхода при проектировании безопасных коммуникационных решений в облачной среде.

ЛИТЕРАТУРА

1 Mahmood, Z. Virtual Private Networks: Fundamentals, security issues and solutions, pp. 1–7 (2023). https://doi.org/10.20944/preprints202306.1105.v1.

2 Parker, A. Efficacy of Full-Packet Encryption in Mitigating Protocol Detection for Evasive Virtual Private Networks, pp. 1–6 (2024) https://doi.org/10.48550/arXiv.2412.17352.

3 Xue, D., Ramesh R., Jain A., Kallitsis M., Halderman J., Crandall J., Ensafi R. Roya. OpenVPN is Open to VPN Fingerprinting. Communications of the ACM, pp. 79–87 (2024). https://doi.org/10.1145/3618117.

4 Farooq, I., Ahmed Syed., Ali, A., Warraich, M., Aqeel, M., Khan, H. Enhanced Classification of Networks Encrypted Traffic: A Conceptual Analysis of Security Assessments, Implementation, Trends and Future Directions. The Asian Bulletin of Big Data Management, pp. 500–522 (2024). https://doi.org /10.62019/abbdm.v4i4.287.

5 Donenfeld, J. WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium, pp. 1–12 (2017). https://doi.org/10.14722/ndss.2017.23160.

6 Joel, A., Rajiv, S., Hadi, L., Anand, P. Empirical Performance Analysis of WireGuard vs. OpenVPN in Cloud and Virtualised Environments Under Simulated Network Conditions. Computers., pp. 1–52 (2025). https://doi.org/10.3390/computers14080326.

7 Mackey, S., Mihov, I., Nosenko, A., Vega, F., Cheng, Y. A Performance Comparison of WireGuard and OpenVPN., pp. 162–164 (2020). https://doi.org/10.1145/3374664.3379532.

[1]*Майлыбаев Е.Қ.,
PhD, қауымдастырылған профессор, ORCID ID: 0000-0002-1977-3690,
*e-mail: ersind@mail.ru
[2]Сейдалиева Ұ.Ө.,
PhD, ғылыми қызметкер, ORCID ID: 0000-0002-7190-6753,
e-mail: useidali@bu.edu

[1]Халықаралық көліктік-гуманитарлық университет, Алматы қ., Қазақстан
[2]Бостон университеті, Бостон, АҚШ

БҰЛТТЫҚ ҚОЛДАНБАЛАР ҮШІН ҚАУІПСІЗ ЖЕЛІ ШЛЮЗІН ЖОБАЛАУ

Аңдатпа

Мақала заманауи VPN-хаттамалары OpenVPN және WireGuard негізінде бұлтты қосымшаларға арналған қорғалған желілік шлюзді жобалауға және баптауға арналған. Бұлтты технологиялардың белсенді дамуы мен кибершабуылдардың көбеюі жағдайында қызметтерге қорғалған қашықтан қолжетімділікті қамтамасыз ету ақпараттық қауіпсіздіктің негізгі міндетіне айналуда. Бұлтты ортада деректерді беру кезінде туындайтын өзекті қатерлер қарастырылып, шабуылдардың алдын алуда VPN-технологиялардың рөлі ұсынылған. OpenVPN және WireGuard ерекшеліктері: архитектурасы, криптографиялық негізі, ыңғайлылығы мен өнімділігі жан-жақты талданған. Жұмыста VPN-серверді, брандмауэр сүзгілерін және барлық трафиктің шифрланған туннель арқылы міндетті өтуін қамтамасыз ететін маршрутизация механизмдерін қамтитын шлюз архитектурасы ұсынылған. VMware Workstation виртуалды ортасында жүргізілген тәжірибелер WireGuard деректерді беруде жоғары жылдамдық пен төмен кідірісті қамтамасыз ететінін, ал OpenVPN икемділігімен және корпоративтік жүйелермен үйлесімділігімен ерекшеленетіні көрсетілген. Екі хаттаманы бірлесіп пайдалану жүйенің сенімділігін және бейімделгіштігін арттыруға мүмкіндік береді. Зерттеудің практикалық маңыздылығы ұсынылған архитектураны корпоративтік және жеке желілерге енгізу мүмкіндігінде, бұлтты қосымшаларды қорғау, қызметкерлердің қашықтан қолжетімділігін ұйымдастыру және ақпараттық ресурстардың қауіпсіздік деңгейін арттыруда көрініс табады.

Тірек сөздер: бұлтты қосымшалар, ақпараттық қауіпсіздік, қорғалған шлюз, шифрлау, желілік хаттамалар.

[1]*Mailybayev Y.,
PhD, Associate Professor, ORCID ID: 0000-0002-1977-3690,
*e-mail: ersind@mail.ru
[2]Seidaliyeva U.,
PhD, Research Associate, ORCID ID: 0000-0002-7190-6753
*e-mail: useidali@bu.edu

[1]International University of Transport and Humanities, Almaty, Kazakhstan
[2]Boston University, Boston, USA

DESIGN OF A SECURE NETWORK GATEWAY FOR CLOUD APPLICATIONS

Abstract

The article is devoted to the design and configuration of a secure network gateway for cloud applications based on modern VPN protocols OpenVPN and WireGuard. In the context of the rapid development of cloud

technologies and the increasing number of cyberattacks, ensuring secure remote access to services has become a key task of information security. The paper discusses relevant threats arising during data transmission in cloud environments and highlights the role of VPN technologies in preventing attacks. The features of OpenVPN and WireGuard are analyzed in detail, including their architecture, cryptographic foundation, ease of configuration, and performance. The study presents a gateway architecture comprising a VPN server, firewall filters, and routing mechanisms that enforce mandatory transmission of all traffic through an encrypted tunnel. Experiments conducted in a virtualized VMware Workstation environment showed that WireGuard provides higher data transfer speeds and lower latency, while OpenVPN demonstrates flexibility and compatibility with corporate systems. The combined use of both protocols improves system resilience and adaptability. The practical significance of the research lies in the possibility of implementing the proposed architecture in corporate and private networks to protect cloud applications, organize secure remote employee access, and enhance the security level of information resources.

Keywords: cloud applications, information security, secure gateway, encryption, network protocols.

Дата поступления статьи в редакцию: 21.08.2025