УДК 004

К. Ю. Копыл[1]✉

Распределенная система построения виртуальных защищенных каналов связи

[1]Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: kikopyl3@gmail.com

Аннотация. Обеспечение информационной безопасности корпоративных сетей является одной из ключевых задач управления современными информационными системами. Виртуальные защищенные каналы связи играют важную роль в обеспечении безопасности и конфиденциальности передаваемой информации. Построение физически распределенной системы защищенных каналов связи, в свою очередь, позволяет повысить отказоустойчивость, производительности и надежность системы, предоставляя тем самым безопасность и удобство для работы удаленных сотрудников. На обзор выносится разработанная распределенная система построения виртуальных защищенных каналов связи, обеспечивающая конфиденциальность сетевого взаимодействия. Построение физически распределенной системы защищенных каналов связи позволяет повысить отказоустойчивость и надежность системы. Разработанное решение может быть применено в задачах распределенного сетевого взаимодействия, в том числе в условиях географически разнесенных филиалов компании.

Ключевые слова: конфиденциальность, распределенная система, docker, openvpn, wireguard, vpn

K. Y. Kopyl[1]✉

Distributed system for establishing virtual secure communication channels

[1]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Moscow, Russian Federation
e-mail: kikopyl3@gmail.com

Abstract. Ensuring the information security of corporate networks is one of the key tasks in managing modern information systems. Virtual private communication channels play a crucial role in ensuring the security and confidentiality of transmitted information. The construction of a physically distributed system of secure communication channels, in turn, enhances the fault tolerance, performance, and reliability of the system, thereby providing security and convenience for remote employees. This paper presents a developed distributed system for establishing virtual secure communication channels that ensures the confidentiality of network interactions. The establishment of a physically distributed system of secure communication channels allows for increased fault tolerance and reliability of the system. The proposed solution can be applied to tasks involving distributed network interactions, including in the context of geographically dispersed company branches.

Keywords: confidentiality, distributed system, docker, openvpn, wireguard, vpn

Введение

Развитие информационных технологий привело к увеличению количества сотрудников, работающих удаленно [1], во многих компаниях. Ключевой зада-

чей корпоративных информационных систем стало обеспечение конфиденциальности передаваемой информации.

Обоснование запросов государства и общества подтверждается рядом нормативно-правовых актов. Например, Федеральный закон № 152-ФЗ «О персональных данных» обязывает организации предпринимать меры по защите персональных данных, в том числе при их передаче по сети. Кроме того, Указом Президента РФ № 899 «Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации» информационно-телекоммуникационные системы выделяются как приоритетное направление развития науки.

С целью решения поставленной проблематики научным обществом проводятся исследования в указанной области [2, 3]. Количество ежегодных публикаций, посвященных виртуальным каналам связи, значительно выросло. Если в 2018 году было опубликовано 54 работы, то в 2024 году это число выросло в 4 раза и составило уже 223 публикации, что свидетельствует об актуальности и значимости данной области исследований.

Приведенные факты указывают на растущую потребность в разработке решений для построения распределенных систем виртуальных защищенных каналов связи.

Моделирование предметной области

В рамках разработки распределенной системы построения виртуальных защищенных каналов связи проведено исследование существующих технологических решений [4] и подходов к обеспечению безопасного сетевого взаимодействия [5, 6]. По результатам исследования разработана концептуальная схема работы системы (рис. 1).

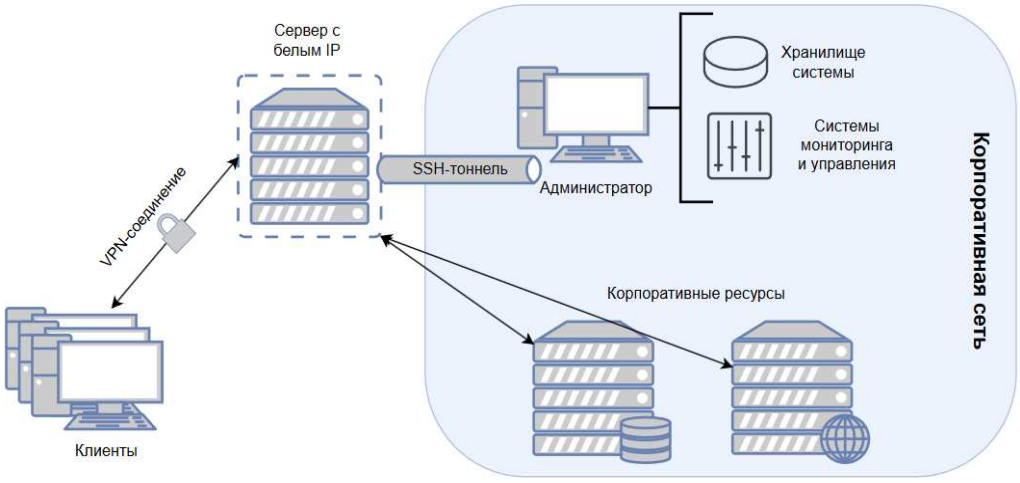

Рис. 1. Концептуальная схема работы системы

Схема включает в себя выделенный сервер с белым IP-адресом (англ. Internet Protocol), узел администратора, корпоративные ресурсы и узлы пользователей.

Узел администратора является центральным узлом системы, он имеет доступ к хранилищу системы и системам мониторинга и осуществляет управление и настройку системы, включая создание, изменение и удаление VPN-серверов (англ. Virtual Private Network). Доступ клиентов к корпоративным ресурсам обеспечивается через защищенное соединение, которое доступно благодаря сконфигурированным и запущенным VPN-серверам в виде контейнеров.

Постановка задачи

После формирования концептуальной схемы системы целью исследования поставлена разработка распределенной системы построения виртуальных каналов связи, обеспечивающей конфиденциальность сетевого взаимодействия.

В рамках декомпозиции цели выделены следующие задачи:

1) проектирование системы построения виртуальных каналов связи;
2) определение функциональности системы и выбор технологического стека;
3) разработка прототипа программного обеспечения системы;
4) создание виртуального стенда для эмуляции сетевой инфраструктуры;
5) интеграция разработанной системы в виртуальный стенд.

Результатом работы должен являться разработанный программный код системы, которая обеспечивает автоматическое создание и настройку контейнеров с VPN-серверами, а также поддерживает их распределение на несколько узлов и предоставляет гибкую настройку параметров безопасности.

Функциональность системы

На основе анализа концептуальной схемы работы системы сформирован перечень функциональных требований. Система должна обеспечивать автоматическое создание и настройку контейнеров с VPN-серверами, позволяя управлять контейнерами. Также требуется поддержка распределения контейнеров на несколько узлов, включая возможность автоматического определения доступных узлов и балансировки нагрузки.

Система должна обеспечивать гибкую настройку VPN-серверов, включая настройку протоколов, алгоритмов шифрования, аутентификации и других параметров безопасности. Необходимо реализовать мониторинг работоспособности и производительности VPN-серверов, логирование событий и обеспечение безопасного хранения конфигурационных данных.

На основании сформированного списка функциональных требований разработана UML-диаграмма [7] компонентов системы (рис. 2).

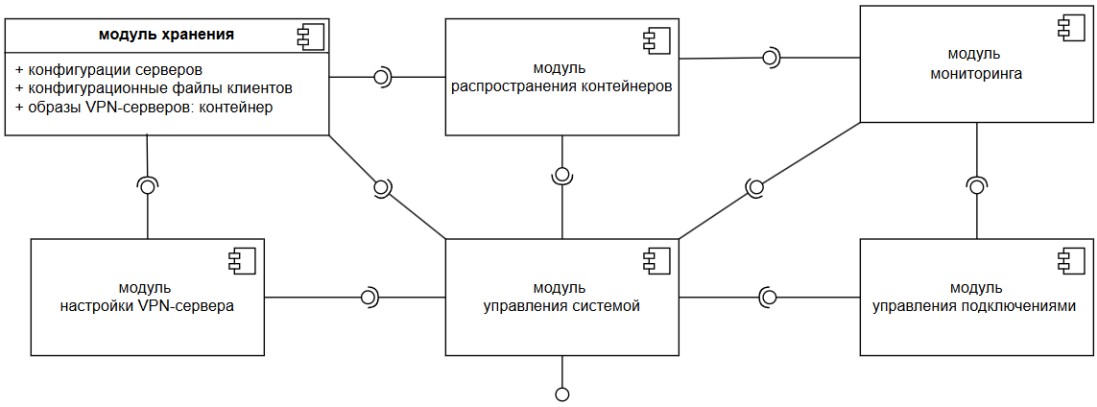

Рис. 2. UML-диаграмма компонентов системы

Диаграмма компонентов включает следующие модули: управление системой, настройка VPN-сервера, мониторинг, распространение контейнеров, хранение данных и управление подключениями.

Стек технологий

Для программной реализации функциональности системы построения виртуальных защищенных каналов связи определен стек технологий, который представлен в табл. 1.

Таблица 1

Стек технологий

Компонент системы	Выбор
модуль настройки VPN-сервера	Docker-образ Alpine
модуль управления системой, модуль распространения контейнеров	DockerSwarm
модуль управления подключениями	Nginx
модуль мониторинга	Portainer
модуль хранения данных	SFTP

Для модуля настройки VPN-сервера выбран Docker-контейнер [8] с базовым образом Alpine Linux. Docker обеспечивает изолированное выполнение приложений в контейнерах, что позволяет легко управлять зависимостями и конфигурациями. Alpine Linux, будучи одним из самых легковесных контейнеров, минимизирует затраты на ресурсы и ускоряет сборку и внедрение.

Для модулей управления системой и распространения контейнеров выбран Docker Swarm [9, 10]. Данная технология обеспечивает интеграцию с Docker и

предоставляет всю необходимую функциональность для реализации запланированных задач. Альтернативным решением являлось использование Kubernetes, но в рамках текущих требований его функциональность избыточна, что могло бы усложнить процесс разработки и администрирования.

Модуль управления подключениями реализован с использованием Nginx в качестве реверс-прокси. Эта технология позволяет распределять входящие запросы между несколькими контейнерами, обеспечивая высокую доступность и отказоустойчивость системы. Nginx способен обрабатывать большое количество одновременных соединений [11], что критично для стабильной работы при высоких нагрузках.

В качестве модуля мониторинга выбран Portainer [12]. Этот веб-интерфейс позволяет управлять и контролировать Docker-контейнеры, что упрощает процесс мониторинга и администрирования.

Решением для модуля хранения данных выбран сервер SFTP [13]. Данная технология обеспечивает шифрование данных на уровне протокола, что обеспечивает безопасность при передаче и хранении конфиденциальной информации.

В качестве протоколов VPN выбраны протоколы OpenVPN [14] и WireGuard [15], обеспечивающие высокий уровень безопасности благодаря поддержке современных алгоритмов шифрования, а также оба протокола поддерживают работу через NAT (англ. Network Address Translation).

Программное обеспечение реализуемой системы

В рамках разработки создана система, использующая Docker для автоматизации сборки контейнеров и их последующего распространения с помощью Docker Swarm. Docker Compose использован для описания конфигурации стека в формате YAML (англ. YAML Ain't Markup Language), что соответствует принципам инфраструктуры как код (англ. IaC, Infrastructure as code).

Для обеспечения безопасного доступа к корпоративным ресурсам разработаны скрипты, автоматически настраивающие контейнеры с VPN-серверами. Для упрощения процесса внедрения и эксплуатации системы подготовлено руководство README.md по настройке и запуску системы.

Разработка виртуального стенда для эмуляции сетевой инфраструктуры

Для тестирования и демонстрации работы разработанной системы создан виртуальный стенд, обеспечивающий необходимую инфраструктуру для проверки функциональности VPN-контейнеров (рис. 3).

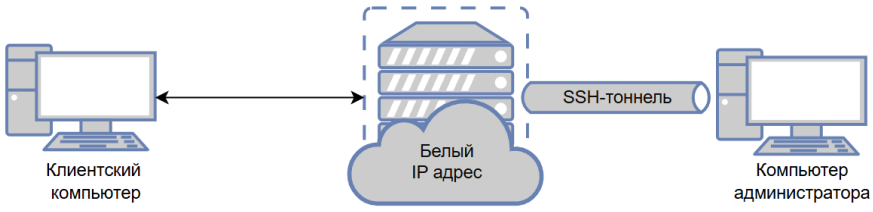

Рис. 3. Схема виртуального стенда

Основным компонентом стенда является сервер с белым IP-адресом, обеспечивающий доступ к VPN-сервисам из внешней сети. На этом сервере размещены контейнеры с VPN-серверами. Сетевые настройки сервера сконфигурированы для обеспечения корректной маршрутизации трафика и доступа к VPN-сервисам.

В качестве узла администратора использовался компьютер с подключением к серверу по SSH-соединению (англ. Secure Shell). Для проверки функциональности VPN-соединений использовался сторонний компьютер, подключающийся к VPN-серверу. Виртуальный стенд также использовался для мониторинга работы VPN-сервисов и выявления возможных проблем.

Интеграция разработанной системы в виртуальный стенд

Интеграция системы в виртуальный стенд осуществлена с использованием Docker и его инструментов оркестрации. Перед началом интеграции обновлена конфигурация сервисов системы, описывающая все необходимые сервисы, их зависимости и параметры.

Для интеграции использована команда sudo docker stack deploy <имя стека>, автоматически создающая все сервисы, указанные в конфигурационном файле. Docker Swarm обеспечил распределение контейнеров по заранее определенным узлам системы. Топология виртуального стенда после интеграции системы представлена ниже (рис. 4).

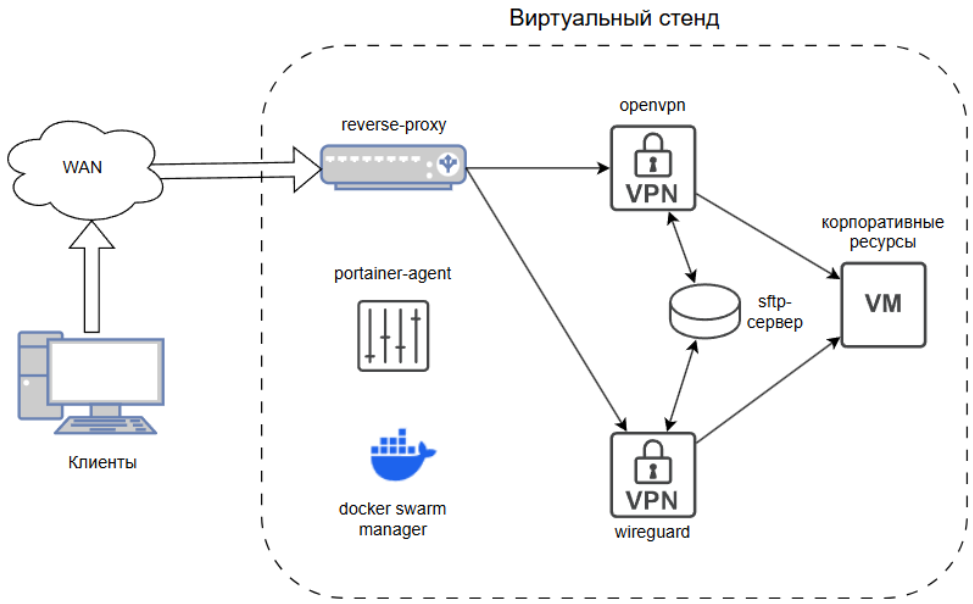

Рис. 4. Топология виртуального стенда

В разработанную систему заложена возможность масштабирования, позволяющая интегрировать ее в более комплексную сетевую инфраструктуру. Пример масштабирования (рис. 5) показывает, как система может быть расширена за

счет добавления новых узлов и перераспределения части сервисов между ними, что способствует повышению отказоустойчивости и производительности.

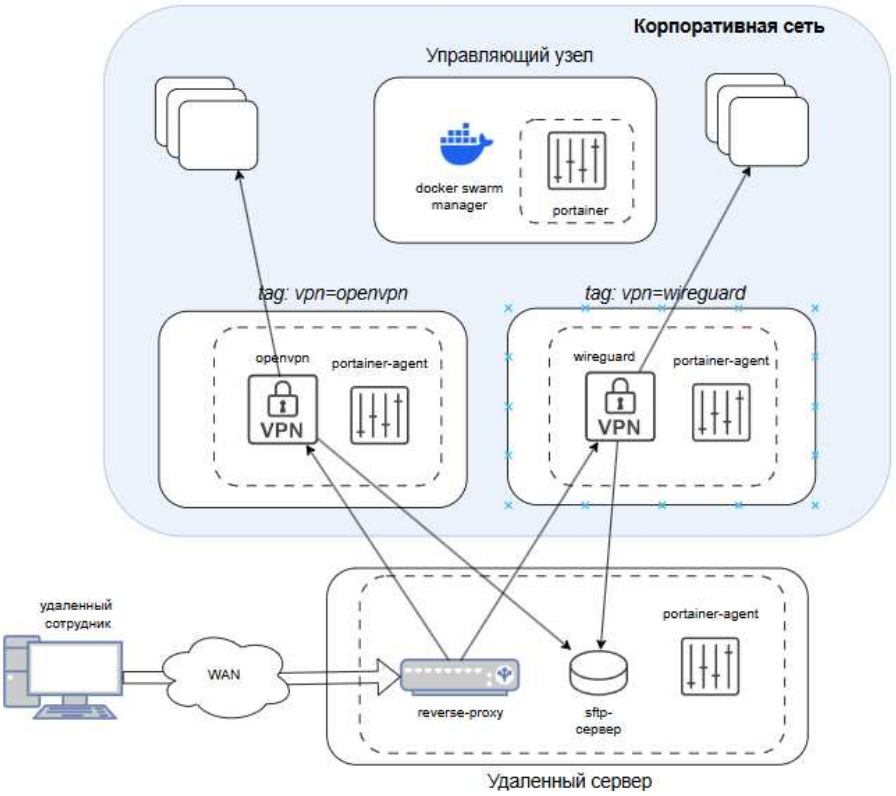

Рис. 5. Масштабирование системы на примере более комплексной сетевой инфраструктуры

После установки и настройки стека проведена проверка состояния всех контейнеров с помощью команд docker service ls и docker ps. Мониторинг осуществлялся с использованием Portainer.

После успешной интеграции системы проведен тест для проверки функциональности VPN-соединений, подтвердивший возможность доступа к ресурсам локальной сети стенда через VPN.

Заключение и обсуждение

В ходе научно-практических изысканий была разработана распределенная система построения виртуальных защищенных каналов связи, обеспечивающая конфиденциальность сетевого взаимодействия. Получившаяся в результате работы система является масштабируемой, что открывает возможность интеграции ее в более комплексную сетевую инфраструктуру, а также дополнения системы иными протоколами VPN, системами мониторинга, логирования и хранения информации.

Область применения полученного решения включает направления, связанные с обеспечением конфиденциальности сетевого взаимодействия в корпоративных сетях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Great Expectations: Making Hybrid Work Work—2022. – URL: https://www.microsoft.com/en-us/worklab/work-trend-index/great-expectations-making-hybrid-work-work/.

2. Басыня Е. А. Самоорганизующаяся система управления трафиком вычислительной сети: удаленный сетевой доступ / Е. А. Басыня, Г. А. Французова, А. В. Гунько // Автоматика и программная инженерия. – 2014. – № 1(7). – С. 9-12. – EDN VIUOGP.

3. Колегов, Д. Н. Использование российских криптографических алгоритмов в протоколе безопасности сетевого уровня WireGuard / Д. Н. Колегов, Ю. Р. Халниязова // Прикладная дискретная математика. Приложение. – 2021. – № 14. – С. 81-84. – DOI 10.17223/2226308X/14/18. – EDN LIRYZL.

4. Kjorveziroski V. et al. Full-mesh VPN performance evaluation for a secure edge-cloud continuum //Software: Practice and Experience. – 2024. – Т. 54. – №. 8. – С. 1543-1564.

5. Карасев П. А. Информационная безопасность в корпоративных сетях // Таврический научный обозреватель. 2017. №3-1 (20).

6. Николахин А. Ю. Использование технологии vpn для обеспечения информационной безопасности // Экономика и качество систем связи. 2018. №3 (9).

7. Простакова А. А. Сравнительный анализ использования Plant UML и графических редакторов для создания диаграмм UML при проектировании программных продуктов / А. А. Простакова, Д. С. Трифанов // XXXVI Международные Плехановские чтения : Сборник статей участников конференции. В 4-х томах, Москва, 25–27 апреля 2023 года. – Москва: Российский экономический университет им. Г.В. Плеханова, 2023. – С. 226-231.

8. Дибиров С. М. Сравнительный анализ Docker, Podman и CRI-O: выбор оптимального инструмента контейнеризации // Актуальные исследования. – С. 28.

9. Захарченко, Д. В. Применение Docker-Swarm при построении кластеров / Д. В. Захарченко // Аллея науки. – 2018. – Т. 5, № 11(27). – С. 830-833. – EDN YWHXLV.

10. Чаплыгин Н. А. Технологии оркестровки Docker Swarm и Kubernetes / Н. А. Чаплыгин, В. С. Гридчин, В. А. Балаев // Перспективы развития и применения современных технологий : сборник статей III Международной научно-практической конференции, Петрозаводск, 16 декабря 2021 года. – Петрозаводск: Международный центр научного партнерства «Новая Наука» (ИП Ивановская И.И.), 2021. – С. 71-75. – EDN VHXXQL.

11. Никишин К. И. Балансировка нагрузки данных в распределенной сети через прок-сисервер Nginx / К. И. Никишин // Известия Юго-Западного государственного университета. – 2022. – Т. 26, № 3. – С. 98-111. – DOI 10.21869/2223-1560-2022-26-3-99-112.

12. Тохтаниязов А. А. Мониторинг и управление контейнерами Docker / А. А. Тохтаниязов // Научно-технический прогресс: актуальные и перспективные направления будущего : Сборник материалов Международной научно-практической конференции, Кемерово, 30 июня 2020 года. – Кемерово: Общество с ограниченной ответственностью "Западно-Сибирский научный центр", 2020. – С. 16-19. – EDN VNFSSE.

13. Дорофеев В. М. Автоматизация интеграции файлообменного решения в корпоративной вычислительной сети / В. М. Дорофеев // Интерэкспо Гео-Сибирь. – 2023. – Т. 7, № 1. – С. 186-192.

14. Бешков А. OpenVPN, или Кроссплатформенная частная сеть / А. Бешков // Системный администратор. – 2004. – № 8(21). – С. 4-12. – EDN REIMCB.

15. Ильичев В. Ю. Сравнительный анализ VPN-протоколов WireGuard и OpenVPN / В. Ю. Ильичев, В. Е. Драч // Системный администратор. – 2022. – № 5(234). – С. 86-89.