УДК 004.056.53, 004.738.5

Методы обхода NAT и обеспечения безопасности при организации защищенного удаленного доступа к рабочим станциям

Н.А. Зенков, Л.А. Сазанова✉

Уральский государственный экономический университет, Екатеринбург, Россия

В данной работе рассматриваются подходы к организации защищенного удаленного доступа к вычислительным ресурсам и рабочим станциям. Авторами проведен сравнительный анализ проприетарных сервисов и частных VPN-решений и проанализированы ключевые методы преодоления сетевых ограничений. Описаны практический опыт построения защищенного канала связи с использованием протокола OpenVPN и статической адресации, а также современные методы обхода NAT в Mesh-сетях. Сделан вывод о необходимости использования, комплексного подхода, сочетающего метод туннелирования и настройку прав доступа, что обеспечит эффективность защиты рабочих станций в условиях ограничений и киберугроз.

Ключевые слова: информационная безопасность, удаленный доступ, NAT, VPN, OpenVPN, Tailscale, RDP.

Methods for NAT Traversal and Security When Organizing Secure Remote Access to Workstations

N.A. Zenkov, L.A. Sazanova✉

Ural State University of Economics, Yekaterinburg, Russia

This paper examines approaches to organizing secure remote access to computing resources and workstations. The authors conducted a comparative analysis of proprietary services and private VPN solutions and analyzed key methods for overcoming network restrictions. The paper describes practical experience in constructing a secure communication channel using the OpenVPN protocol and static addressing, as well as modern methods for bypassing NAT in mesh networks. A conclusion was made regarding the need to use a comprehensive approach combining tunneling and access rights configuration, which will ensure effective protection of workstations in the face of restrictions and cyber threats.

Keywords: information security, remote access, NAT, VPN, OpenVPN, Tailscale, RDP.

Введение и постановка проблемы

В условиях цифровой трансформации общества и перехода образовательных и рабочих процессов в гибридный формат вопрос обеспечения стабильного и безопасного удаленного доступа к вычислительным ресурсам становится критически важным. У конечных пользователей и ИТ-специалистов зачастую возникает необходимость работы с домашними рабочими станциями, обладающими высокой производительностью, без физического перемещения оборудования. Однако на пути решения данной задачи стоят две основные проблемы: преодоление сетевых барьеров, в частности, Network Address Translation (далее – NAT) и обеспечение должного уровня информационной безопасности передаваемых данных. Анализ подходов к решению данных проблем и составляет предмет данного исследования.

Результаты исследования

Главной преградой для установления прямого соединения между узлами в современной архитектуре TCP/IP [1] является дефицит IPv4-адресов. Для решения этой проблемы на уровне телекоммуникационных операторов повсеместно применяется технология CG-NAT (Carrier-Grade NAT) [2]. В отличие от классического NAT, она создает дополнительный уровень трансляции, объединяя за одним публичным IP-адресом не одну локальную сеть, а тысячи абонентских устройств. Схема этого процесса, часто называемая топологией NAT444 [3], приведена на рисунке. Такая многоуровневая трансляция критически усложняет сетевое взаимодействие: конечный узел получает «серый» адрес (обычно из диапазона 100.64.0.0/10), становясь невидимым для внешних инициаторов соединения. Без использования специализированных методов прохождения NAT (NAT Traversal и туннелирование), рабочая станция оказывается за изолированным барьером операторского шлюза, что исключает возможность прямого входящего доступа к её ресурсам. Технология NAT Traversal позволяет при использовании маршрутизатора устанавливать прямые сетевые соединения (VPN, VoIP, P2P) между устройствами, находящимися за NAT-маршрутизаторами (обычно за домашним роутером), скрывающими их локальные IP-адреса. При наличии барьера NAT происходит переключение соединения на протокол UDP. NAT Traversal и туннелирование, применяемые совместно, создают виртуальный канал для передачи данных: NAT Traversal создает доступ, а туннелирование создает защищенный канал внутри этого доступа.

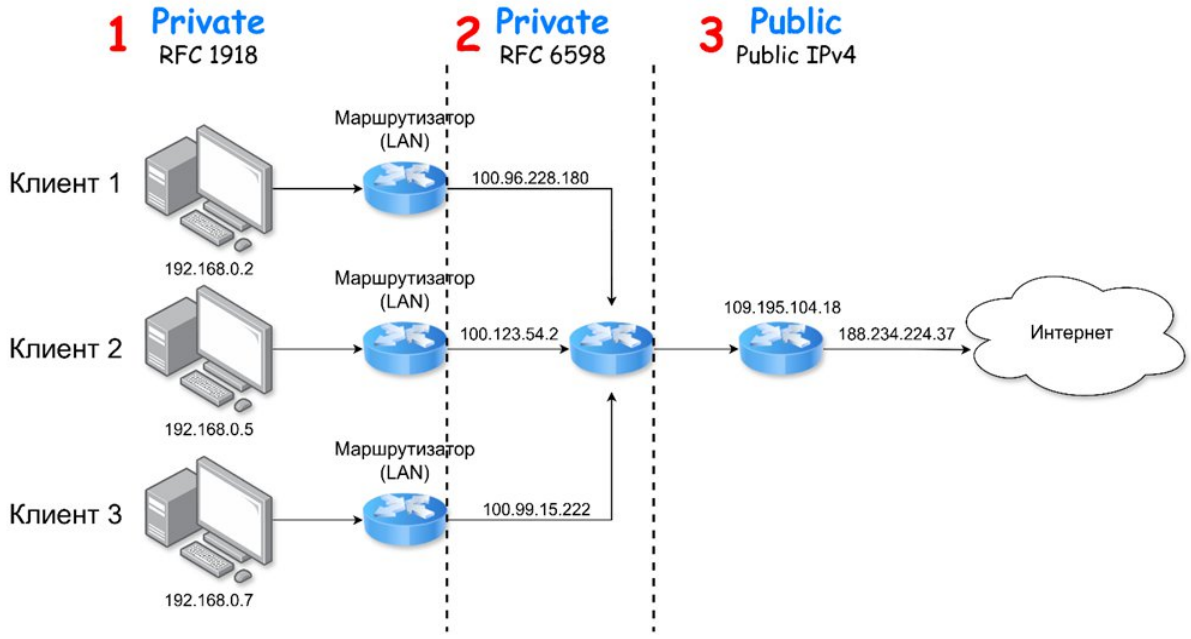

Рисунок. Схема многоуровневой трансляции адресов (NAT444) с использованием технологии CG-NAT

Параллельно с сетевыми ограничениями, критическим аспектом является обеспечение информационной безопасности. При организации удаленного сеанса управления передаваемые данные (включая учетные записи и экранные формы) проходят через публичные каналы связи, что делает их уязвимыми для атак типа «человек посередине». В случае такой кибератаки злоумышленник тайно внедряется в канал связи между сторонами (например, пользователем и сайтом), перехватывая и при

необходимости изменяя передаваемые данные. При этом жертвы считают, что общаются напрямую, но на деле информация проходит через хакера. Таким образом, выбор метода удаленного доступа должен основываться на балансе между пропускной способностью канала и криптографической стойкостью используемых алгоритмов.

Наиболее распространенным и доступным решением для конечного пользователя являются проприетарные облачные сервисы удаленного рабочего стола, такие как AnyDesk или TeamViewer. Механизм их работы основан на использовании промежуточного сервера-ретранслятора, который выступает в роли «посредника», позволяя обоим узлам установить исходящее соединение и тем самым миновать ограничения NAT. Однако, несмотря на низкий порог вхождения, данные системы обладают рядом критических недостатков с точки зрения требований информационной безопасности и производительности. Во-первых, весь трафик сессии проходит через сторонний сервер, что создает потенциальные риски перехвата или компрометации данных на стороне посредника. Во-вторых, использование трансляции видеопотока экрана (растровой передачи) при нестабильном интернет-соединении приводит к значительным задержкам и снижению четкости изображения, что затрудняет работу в специализированном инженерном ПО. Кроме того, например, сессия AnyDesk дублирует изображение на физическом мониторе удаленного хоста, что делает действия пользователя видимыми для посторонних лиц и снижает уровень конфиденциальности.

Альтернативным и более профессиональным подходом является использование протокола удаленного рабочего стола Remote Desktop Protocol (RDP) внутри защищенного VPN-туннеля. В отличие от видеостриминга, RDP оперирует графическими примитивами интерфейса операционной системы, что значительно снижает нагрузку на канал связи и обеспечивает быстрый отклик интерфейса. При этом сессия RDP блокирует локальный экран рабочей станции, исключая визуальный перехват информации.

В рамках практической деятельности авторами была реализована следующая схема доступа на базе открытого протокола OpenVPN. Для преодоления барьера NAT был использован метод прямой конфигурации сетевого шлюза с применением статической IP-адресации. Техническая реализация включала настройку перенаправления портов для UDP-порта 1194 домашнего маршрутизатора на целевой хост и развертывание инфраструктуры открытых ключей (PKI) для генерации индивидуальных криптографических сертификатов. Использование режима туннелирования уровня L3 позволило обеспечить минимальные затраты при инкапсуляции пакетов и применить стойкое шифрование по стандарту AES-256 [4]. Недостатками данного подхода являются сравнительно высокий порог вхождения и сложность конфигурации. В отличие от готовых P2P-решений (например, Tailscale), данный метод требует не только финансовых затрат на аренду статического IP-адреса, но и проведения ряда низкоуровневых манипуляций: ручной настройки таблиц NAT на маршрутизаторе, корректировки политик безопасности (firewall) и реестра операционной системы для корректной маршрутизации трафика.

Данные ограничения стимулируют поиск альтернативных подходов, основанных на технологиях Mesh-сетей [5] и построении туннелей без использования статических адресов. Одним из наиболее эффективных решений является сервис Tailscale, использующий протокол WireGuard и механизмы NAT Traversal. В отличие от классических облачных решений, Tailscale минимизирует риски компрометации на стороне посредника за счет использования сквозного шифрования (end-to-end шифрования) на базе протокола WireGuard. Централизованный сервер здесь выполняет

лишь функцию координации и обмена публичными ключами, в то время как закрытые ключи остаются исключительно на конечных узлах пользователя. Это исключает возможность дешифровки трафика даже в случае полной компрометации инфраструктуры сервис-провайдера.

Рассмотренные выше подходы к организации удаленного доступа существенно различаются по уровню безопасности, архитектурной сложности и качеству сетевого взаимодействия. Для выбора оптимального решения в условиях работы через CG-NAT необходимо провести сопоставление их ключевых характеристик. Чтобы наглядно оценить баланс между удобством развертывания системы и защищенностью передаваемого трафика, проведем сравнительный анализ технических характеристик исследуемых решений (табл.).

Таблица

Сравнительный анализ технологий удаленного доступа

Критерий сравнения	Облачные сервисы (AnyDesk/TeamViewer)	VPN с перенаправлением портов (статический IP + OpenVPN)	Mesh-сети (Tailscale)
Метод прохождения NAT	Реле-сервер	Статический проброс	NAT Traversal (STUN/ICE)
Тип шифрования	Проприетарное (закрытое), заявлено как AES-256	AES-256 (OpenSSL)	ChaCha20-Poly1305 (WireGuard)
Сложность настройки	Низкая (ID + пароль)	Высокая (NAT, PKI, перенаправление портов)	Средняя (авторизация узлов)
Зависимость от посредника	Полная (весь трафик через сервер)	Требуется поддержка провайдера (статический IP)	Минимальная (только координация ключей)
Задержка	Зависит от загрузки серверов вендора	Минимальная (прямой канал)	Минимальная (P2P-туннель)
Конфиденциальность	Риск перехвата на стороне вендора	Высокая (полный контроль)	Высокая (end-to-end шифрование)

Различия в архитектуре и методах реализации определяют целевую аудиторию каждого из подходов. Проприетарные решения (AnyDesk, TeamViewer) ориентированы на сегмент конечных пользователей, не обладающих глубокими знаниями в области сетевых технологий. Данный подход оправдан, например, при необходимости разового оказания технической поддержки или в сценариях, где скорость развертывания критичнее уровня защищенности и стабильности канала. Однако отсутствие механизмов блокировки локальной сессии и зависимость от внешней инфраструктуры делают этот метод неприемлемым для постоянной профессиональной эксплуатации.

Напротив, классическая связка OpenVPN и прямого проброса портов является инструментом опытных пользователей и системных администраторов. Данный метод требует от специалиста владения навыками администрирования сетевого оборудования, понимания принципов работы PKI-инфраструктуры и готовности к самостоятельному управлению безопасностью. Это выбор в пользу максимальной защищенности данных и независимости от глобальных облачных сервисов, что критически важно в рамках

импортозамещения и обеспечения безопасности критической информационной инфраструктуры.

Mesh-сети, представленные технологией Tailscale, выступают в роли «золотой середины», сочетая в себе простоту интеграции пользовательских решений и высокий уровень безопасности корпоративного класса. Данный подход оптимален для ИТ-специалистов и пользователей, которым необходим быстрый, защищенный и отказоустойчивый доступ к распределенным ресурсам в условиях динамически меняющейся сетевой топологии. Использование принципов нулевого доверия в совокупности с современным криптографическим протоколом WireGuard позволяет организовать удаленное администрирование на профессиональном уровне без избыточных временных затрат на конфигурацию сетевого оборудования.

Важным техническим аспектом, определяющим применимость рассмотренных методов, является редакция операционной системы на целевой рабочей станции. В отличие от сторонних сервисов (AnyDesk, TeamViewer), работающих на уровне прикладного ПО и доступных в любой версии ОС, использование протокола RDP в связке с OpenVPN или Tailscale требует наличия определенной редакции ОС. Функция входящих подключений удаленного рабочего стола является привилегией профессиональных редакций – Windows Pro, Enterprise.

В домашних редакциях (Windows Home) служба удаленных рабочих столов ограничена и не позволяет принимать входящие RDP-сессии. Таким образом, организация защищенного канала через VPN или Mesh-сеть позиционируется как решение для корпоративного сегмента или продвинутых пользователей, готовых к системному администрированию инфраструктуры. Использование профессиональных редакций ОС также открывает доступ к расширенным политикам безопасности и групповым политикам, что позволяет дополнительно защитить RDP-хост, например, ограничив список разрешенных пользователей и их привилегий.

Заключение и выводы

В ходе проведенного исследования были проанализированы ключевые методы преодоления сетевых ограничений NAT и обеспечения безопасности при организации удаленного доступа. Сравнительный анализ показал, что выбор конкретной технологии напрямую зависит от квалификации пользователя и требований к конфиденциальности данных. Особое внимание следует уделять выбору операционной системы: если в среде Windows возможности удаленного доступа жестко привязаны к редакции ОС, то использование отечественных решений на базе Linux (например, Astra Linux) позволяет строить более гибкие и экономически эффективные системы удаленного администрирования. Таким образом, реализация защищенного удаленного доступа на базе открытых протоколов (OpenVPN, WireGuard) отличается кроссплатформенностью. В среде Linux-систем, включая отечественные дистрибутивы, такие как Astra Linux, организация удаленного рабочего стола не имеет искусственных ограничений по редакциям (в отличие от Windows Home/Pro). Переход на Linux-дистрибутивы снимает лицензионные барьеры для организации удаленной работы, сохраняя при этом высокий уровень безопасности за счет использования проверенных криптографических решений. В конечном итоге, комплексный подход, сочетающий надежное туннелирование и грамотную настройку прав доступа, является на сегодняшний день единственным эффективным способом защиты рабочих станций в условиях современных киберугроз.

СПИСОК ИСТОЧНИКОВ

1. Зенков Н.А. Уязвимости веб-приложений как вызов цифровому обществу: XSS-атаки и SQL-инъекции / Н.А. Зенков, Л.А. Сазанова // BI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов: Материалы XIII Международной научно-практической конференции. – Екатеринбург: Уральский государственный экономический университет, 2026. – С. 56–60.

2. Иванова А.А. Применение технологии NAT для повышения информационной безопасности компьютерных сетей / А.А. Иванова // Инжиниринг предприятий и управление знаниями (ИП&УЗ-2023): Сборник научных трудов XXVI Российской научной конференции (молодежная секция). – Москва: Российский экономический университет имени Г.В. Плеханова, 2024. – Т. 2. – С. 84–88.

3. Астуриас Д. CGNAT: Обходной путь в условиях истощения IPv4 [2026] / Д. Астуриас // RapidSeedBox [Электронный ресурс]. – URL: https://www.rapidseedbox.com/ru/blog/cgnat (дата обращения: 20.05.2026).

4. Жолудев Я.М. Методы и технологии для обеспечения всесторонней защиты данных / Я.М. Жолудев // Национальный вестник Республики Крым. – 2026. – № 13. – С. 306–310.

5. Прядкин А.М. Исследование вопросов производительности меш-сетей в системах связи специального назначения / А.М. Прядкин, И.С. Гришанов // Телекоммуникации и связь. – 2024. – № 2 (2). – С. 6–12.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Зенков Николай Андреевич, студент, Уральский государственный экономический университет, Екатеринбург, Россия.
e-mail: nikolaizenkov2005@gmail.com

Сазанова Лариса Анатольевна, кандидат физико-математических наук, доцент, Уральский государственный экономический университет, Екатеринбург, Россия.
e-mail: sazanovalarisa@rambler.ru