

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ И АНАЛИЗ СЕТЕВОГО ТРАФИКА ПРОТОКОЛА SMB OVER QUIC В ИНФРАСТРУКТУРЕ WINDOWS SERVER 2025

Аннотация. В условиях роста объемов передаваемых данных и популярности удаленной работы обеспечение безопасности файловых ресурсов становится критической задачей. Традиционный протокол SMB over TCP (порт 445) уязвим к пассивному перехвату трафика и часто блокируется межсетевыми экранами. В статье рассматривается протокол SMB over QUIC, инкапсулирующий SMB-трафик в защищенный туннель QUIC поверх UDP (порт 443) с обязательным шифрованием TLS 1.3. Целью работы является практическая проверка методики развертывания данного протокола и сравнительный анализ его сетевого трафика с классическим SMB. В ходе эксперимента была развернута изолированная лабораторная среда на базе Windows Server 2025 (версия 24H2, сборка 26100.32230) и Windows 11 Pro (версия 25H2, сборка 26200.7840). С помощью анализатора Wireshark 4.6.8 был перехвачен и исследован трафик обоих протоколов. Результаты показали, что в сеансе SMB over QUIC анализатор отображает полезную нагрузку исключительно как Protected Payload, не декодируя команды протокола или имена файлов. В контрольном сеансе классического SMB over TCP (при настройках по умолчанию без принудительно включенного SMB Encryption) те же операции (Create Request, Read, Close) и имя файла test.txt (размер 1 КБ) отображаются в открытом виде. Сделан вывод, что SMB over QUIC является потенциальной альтернативой классическим VPN-решениям исключительно для защищенного файлового доступа, при условии корректной настройки инфраструктуры открытых ключей (PKI), строгой аутентификации и аудита, однако не заменяет полноценный VPN для маршрутизации всего сетевого трафика. Ограничения исследования включают использование самоподписанного сертификата и лабораторной сети без моделирования реальных условий эксплуатации.

Ключевые слова: SMB over QUIC, Windows Server 2025, сетевая безопасность, Wireshark, TLS 1.3, протокол QUIC, общий файловый ресурс.

Введение

Современные корпоративные ИТ-системы стремительно меняются: объемы данных растут, сотрудники всё чаще работают удаленно, а на периферию сетей выходят мобильные устройства. При этом информация постоянно передается по открытым глобальным каналам [1]. Для обмена файлами между клиентами и серверами по-прежнему незаменим протокол SMB, который ценят за надежность и стабильность [2]. Однако в условиях центра обработки данных (далее ЦОД) главная задача – защитить эти данные от несанкционированного доступа и перехвата [3].

Ответом на эти вызовы стал SMB over QUIC от Microsoft. В этой реализации файловый протокол инкапсулируется в QUIC (работающий поверх UDP на порту 443) и обязательно шифруется с помощью TLS 1.3. Поддержка новинки уже появилась в Windows Server 2022 (Azure Edition), Windows Server 2025 и Windows 11 [4, 5].

Что это дает на практике? Во-первых, обязательное шифрование TLS 1.3 и инкапсуляция в QUIC создают эффект защищенного туннеля. В сценариях файлового доступа администраторы могут рассмотреть SMB over QUIC как альтернативу классическим VPN-решениям, а встроенное шифрование снижает необходимость в дополнительной защите на сетевом уровне. Во-вторых, использование порта UDP 443 позволяет снизить вероятность блокировки трафика: провайдеры и межсетевые экраны часто закрывают "родной" порт SMB (TCP 445), тогда как порт UDP 443 в современных сетевых политиках зачастую имеет меньше ограничений на прохождение, при условии, что правила межсетевого экрана корректно настроены именно для UDP-трафика, а не только для классического HTTPS по TCP [4].

Такой подход отлично вписывается в современные тренды сетевых технологий. Стандартизация QUIC консорциумом IETF (RFC 9000, RFC 9001) решила проблему head-of-line blocking, свойственную TCP, а установка TLS-соединения по UDP происходит заметно быстрее [6, 7, 8]. Однако если обратиться к научной литературе, создается ощущение, что QUIC создан исключительно для веба. Большинство исследований посвящены HTTP/3 и

сравнению его производительности с классическим HTTP/1.1 и HTTP/2 (оба работают по TCP). Применению QUIC в файловых протоколах, в частности в SMB, уделено мало внимания [9, 10, 4]. Существующие материалы сводятся либо к официальной документации вендора [2, 4], которая описывает лишь общие принципы, либо к поверхностным упоминаниям без глубокого анализа механизмов защиты в реальных условиях.

В отличие от общей документации Microsoft [4, 5] и стандартов IETF [6, 7], описывающих теоретические основы протокола, вклад данного исследования заключается в практической верификации развертывания SMB over QUIC в изолированной лабораторной среде без использования доменной инфраструктуры Active Directory. Автором разработан и апробирован конкретный сценарий настройки: от генерации самоподписанного сертификата с SAN до принудительной привязки к порту UDP 443 и перехвата трафика. Полученные файлы захвата pcapng и сравнительный анализ декодируемости команд в Wireshark дополняют официальную документацию наглядным доказательством механизмов сокрытия полезной нагрузки в реальных условиях, а также выявляют специфические ограничения, требующие учета при переходе от лабораторного стенда к промышленной эксплуатации.

Объект исследования – современные сетевые файловые протоколы и инфраструктура Windows Server, обеспечивающие совместный доступ к данным в корпоративных средах.

Предмет исследования – механизмы обеспечения информационной безопасности, структура сетевого трафика и практические аспекты развертывания протокола SMB over QUIC в сравнении с классическим протоколом SMB over TCP в среде Windows Server 2025 и Windows 11.

Цель исследования – разработать и на практике проверить методику безопасного развертывания файлового сервера на базе SMB over QUIC, а также сравнить уровень защиты передаваемых данных с классическим подходом.

На практике это означает настройку инфраструктуры открытых ключей (PKI) для корректной проверки сертификатов, конфигурацию серверной и клиентской частей ОС Windows, а также перехват и детальный разбор сетевого трафика с помощью анализатора Wireshark.

Итогом работы станет готовое к использованию конфигурационное решение. В ходе эксперимента будет доказано, что полезная нагрузка трафика шифруется по стандарту TLS 1.3, и выявлены ключевые отличия нового протокола от классического SMB. Результаты исследования покажут, как с помощью SMB over QUIC можно организовать защищенный доступ к файловым ресурсам в качестве альтернативы классическим VPN-решениям (при соблюдении требований к PKI и аутентификации). Эти наработки будут полезны системным администраторам и специалистам по ИБ при модернизации корпоративной ИТ-инфраструктуры.

Литературный обзор

File share (общий файловый ресурс SMB) – это сетевой ресурс, предоставляющий пользователям доступ к файлам и каталогам, размещенным на удаленном сервере. В корпоративных информационных системах общие файловые ресурсы SMB играют ключевую роль: они обеспечивают централизованное хранение данных, совместную работу сотрудников над документами, резервное копирование и разграничение прав доступа. Типичный корпоративный общий файловый ресурс включает в себя серверную часть (файловый сервер), клиентскую часть (рабочие станции пользователей) и сетевой протокол, обеспечивающий передачу данных между ними.

В экосистеме Windows стандартом де-факто для реализации общих файловых ресурсов является протокол SMB (Server Message Block). Его история насчитывает несколько десятилетий: от первой реализации SMB1 (также известного как CIFS – Common Internet File System) до современных версий SMB2 и SMB3 [11]. Протокол SMB3, представленный в Windows 8 и Windows Server 2012, добавил поддержку шифрования данных, многоканальности и непрерывной доступности, что сделало его пригодным для использования в корпоративных средах с высокими требованиями к надежности [2].

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Появление протокола QUIC (Quick UDP Internet Connections), стандартизированного рабочей группой IETF в документе RFC 9000 в 2021 году [6], предложило новую парадигму построения защищенных соединений. Протокол был изначально разработан компанией Google в 2012 году как экспериментальная замена TCP для веб-трафика, но быстро завоевал популярность благодаря своим преимуществам: уменьшению времени установления соединения, устранению проблемы блокировки начала очереди (head-of-line blocking) за счет независимых потоков внутри одного соединения и встроенной защите от анализа трафика [9, 10].

Современные научные исследования активно изучают преимущества и особенности протокола QUIC. В работе М. М. Адживапаева [1] проводится подробный сравнительный анализ транспортных протоколов TCP, UDP и QUIC, где автор подчеркивает, что QUIC эффективно устраняет проблему блокировки начала очереди и ускоряет установление соединения. Автор отмечает, что QUIC сочетает в себе функции транспорта и криптографии, обеспечивая надёжную доставку, управление потоком и шифрование в едином протоколе. И. А. Смирнов [10] рассматривает QUIC как фундамент для HTTP/3, отмечая его высокую криптографическую стойкость и перспективы применения в высоконагруженных сервисах. В статье проводится сравнительный анализ HTTP/3 и HTTP/2, а также QUIC и TCP, обсуждаются сложности развёртывания и перспективы дальнейшего развития протоколов. Н. С. Андреев [3] в своем исследовании клиент-серверных протоколов подтверждает, что внедрение QUIC существенно повышает отказоустойчивость и безопасность сетевых соединений за счет встроенных механизмов шифрования и криптографической аутентификации. Автор подчеркивает, что каждый пакет QUIC содержит часть информации, передаваемой между клиентом и сервером, и может быть независимо обработан, что повышает надежность передачи данных.

Вопросы информационной безопасности при использовании новых протоколов требуют отдельного внимания. А. Ю. Симачев [9] исследует возможности формирования скрытых каналов в протоколе QUIC, что указывает на необходимость глубокого практического анализа его сетевого трафика с использованием специализированных анализаторов. В статье показано, что даже современные защищенные протоколы могут иметь скрытые уязвимости, требующие постоянного мониторинга и анализа. В контексте файловых систем А. В. Галимуллина [11] описывает особенности использования SMB, подчеркивая важность корректной настройки протокола для предотвращения несанкционированного доступа. Автор отмечает, что SMB-клиент-серверный протокол предназначен для получения доступа к файлам, каталогам и сетевым ресурсам, и его неправильная конфигурация может привести к серьезным проблемам безопасности.

Официальная документация Microsoft [2, 4] позиционирует SMB over QUIC как своеобразный “SMB VPN”, позволяющий безопасно передавать файлы через интернет по стандартному порту UDP 443, эффективно минуя традиционные блокировки порта TCP 445 интернет-провайдерами и межсетевыми экранами. Протокол требует наличия действительного сертификата X.509 с альтернативным именем субъекта (SAN), что обеспечивает криптографическую аутентификацию сервера. Шифрование осуществляется на базе TLS 1.3, который является последним стандартом Transport Layer Security и обеспечивает высокую скорость установления соединения благодаря механизму 0-RTT (Zero Round Trip Time) [7, 5].

Инфраструктура открытых ключей (PKI) играет важную роль в развёртывании SMB over QUIC. Сертификат сервера должен быть выпущен доверенным центром сертификации (CA) и содержать правильное альтернативное имя субъекта (SAN), соответствующее DNS-имени сервера [4]. Использование самоподписанных сертификатов возможно в тестовых средах, но требует их ручного импорта в хранилище доверенных корневых центров сертификации на клиентских устройствах. Неправильная настройка PKI является одной из наиболее частых причин проблем с подключением по SMB over QUIC.

Анализ сетевого трафика с использованием специализированных инструментов, таких как Wireshark, позволяет детально изучить механизмы работы протокола. Анализ трафика

Рубрика 2. Методы и системы защиты информации, информационная безопасность

- сравнение структуры пакетов: оценка видимости метаданных (имен файлов, команд протокола) и наличия шифрования (открытый текст против Protected Payload);
- анализ конфигурации: проверка состояния служб и привязки сертификата с помощью командлетов PowerShell (Get-SmbServerConfiguration, Get-NetUDPEndpoint, Get-ChildItem Cert:\LocalMachine\My).

Описание процедуры проведения исследования

Эксперимент проводился в следующей последовательности:

- подготовка ролей и сертификата. На сервере установлены роли файлового сервера и службы сертификации. С помощью PowerShell сгенерирован самоподписанный сертификат X.509 с альтернативным именем субъекта (SAN) командой: `New-SelfSignedCertificate -DnsName "SRV-QUIC.local" -CertStoreLocation "Cert:\LocalMachine\My" -KeyAlgorithm RSA -KeyLength 2048 -HashAlgorithm SHA256`;
- настройка SMB over QUIC. Сертификат привязан к порту UDP 443 командой `New-SmbServerCertificateMapping`. Поддержка протокола включена командой `Set-SmbServerConfiguration -EnableSMBQUIC $true`. Служба LanmanServer перезапущена;
- настройка клиента. Сертификат сервера импортирован в хранилище доверенных корневых центров сертификации (Cert:\LocalMachine\Root) на клиенте. В файле hosts прописано соответствие имени и IP-адреса;
- захват трафика SMB over QUIC. На клиенте запущен Wireshark с фильтром `udp.port == 443`. Подключение к ресурсу выполнено с явным указанием транспорта QUIC командой: `New-SmbMapping -LocalPath 'Z:' -RemotePath '\\SRV-QUIC.local\QUICShare' -TransportType QUIC`. Это позволило принудительно использовать QUIC вместо стандартного TCP-подключения. Произведено открытие и чтение тестового файла test.txt (размер 1 КБ);
- захват трафика классического SMB. Для чистоты эксперимента поддержка QUIC на клиенте временно отключена (`Set-SmbClientConfiguration -EnableSMBQUIC $false`). Фильтр Wireshark изменен на `tcp.port == 445`. Подключение и операции с файлом повторены;
- сравнительный анализ. Захваченный трафик (файлы 25u19t3.pcapng для SMB over QUIC и 2ieu5t3.pcapng для SMB over TCP) проанализирован на предмет декодируемости команд протокола и шифрования полезной нагрузки.

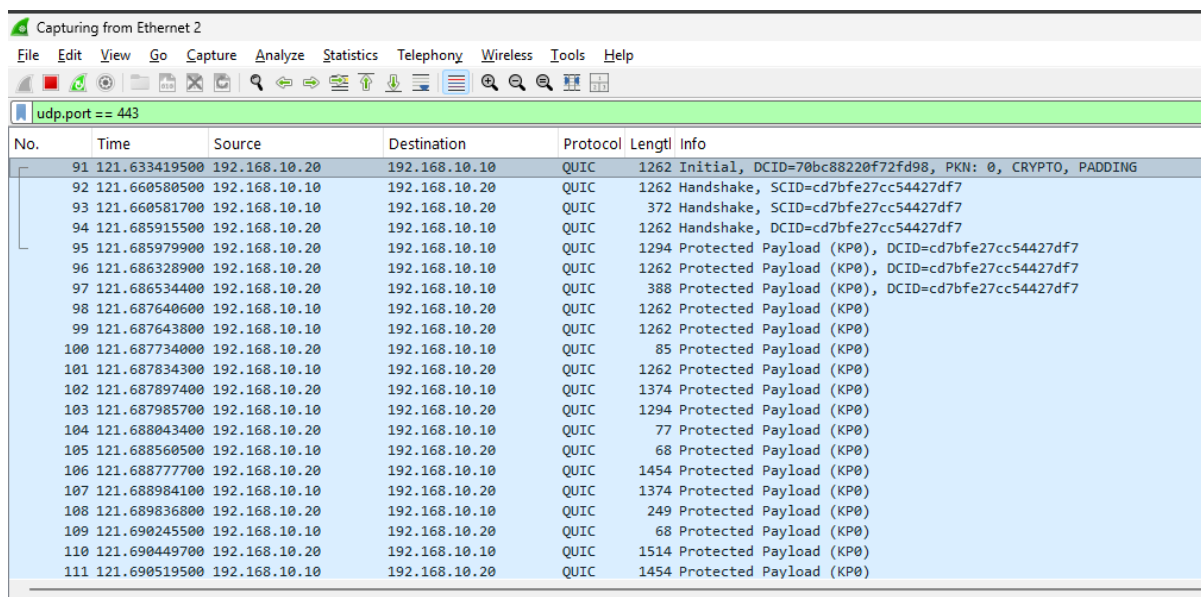
Результаты исследования

В ходе эксперимента была успешно развернута клиент-серверная инфраструктура с поддержкой SMB over QUIC. На сервере SRV-QUIC (Windows Server 2025) установлены роли файлового сервера и службы сертификации, сгенерирован самоподписанный сертификат X.509 с альтернативным именем субъекта (SAN) SRV-QUIC.local. Сертификат привязан к порту UDP 443 командой `New-SmbServerCertificateMapping`, после чего поддержка протокола активирована через `Set-SmbServerConfiguration -EnableSMBQUIC $true`.

На клиентской машине (Windows 11 Pro 25H2) сертификат импортирован в хранилище доверенных корневых центров сертификации, что обеспечило корректную валидацию при подключении. Подключение к общему файловому ресурсу `\\SRV-QUIC.local\QUICShare` прошло успешно, файлы открывались и читались без ошибок.

Следовательно, гипотеза 1 подтверждена полностью: развертывание файлового сервера с поддержкой SMB over QUIC в изолированной среде технически реализуемо при корректной настройке PKI и привязке сертификата к порту UDP 443.

Для анализа структуры сетевого трафика на клиентской машине был запущен анализатор Wireshark 4.6.8 с фильтром `udp.port == 443`. В ходе захвата были зафиксированы пакеты протокола QUIC, инкапсулирующего SMB-трафик.



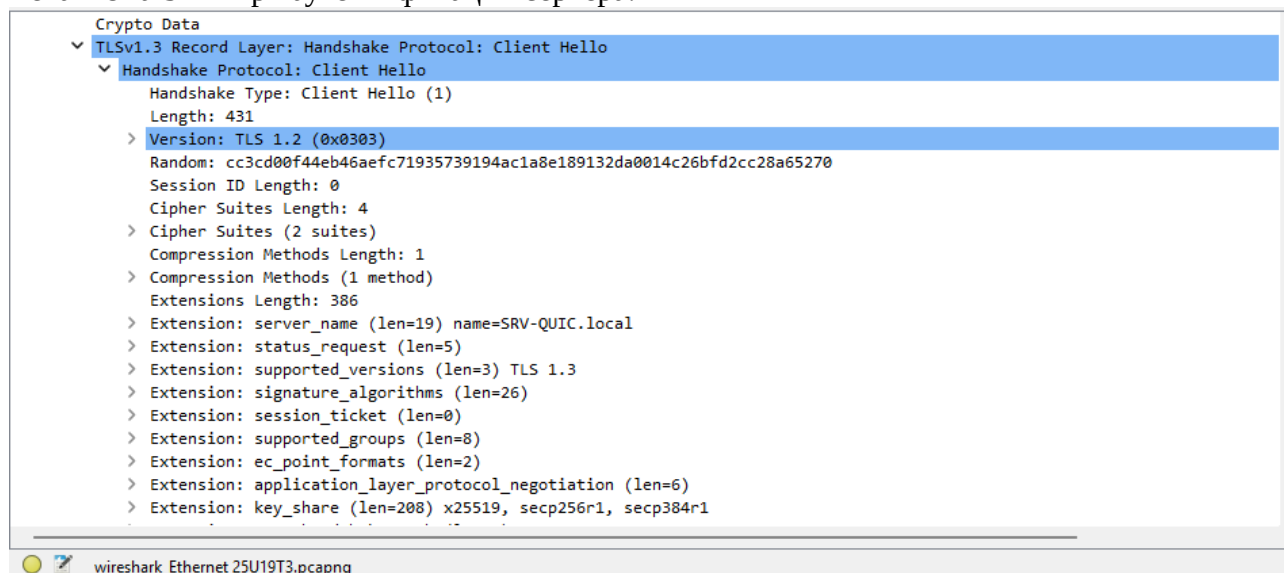
No.	Time	Source	Destination	Protocol	Length	Info
91	121.633419500	192.168.10.20	192.168.10.10	QUIC	1262	Initial, DCID=70bc88220f72fd98, PKN: 0, CRYPTO, PADDING
92	121.660580500	192.168.10.10	192.168.10.20	QUIC	1262	Handshake, SCID=cd7bfe27cc54427df7
93	121.660581700	192.168.10.10	192.168.10.20	QUIC	372	Handshake, SCID=cd7bfe27cc54427df7
94	121.685915500	192.168.10.20	192.168.10.10	QUIC	1262	Handshake, DCID=cd7bfe27cc54427df7
95	121.685979900	192.168.10.20	192.168.10.10	QUIC	1294	Protected Payload (KPB), DCID=cd7bfe27cc54427df7
96	121.686328900	192.168.10.20	192.168.10.10	QUIC	1262	Protected Payload (KPB), DCID=cd7bfe27cc54427df7
97	121.686534400	192.168.10.20	192.168.10.10	QUIC	388	Protected Payload (KPB), DCID=cd7bfe27cc54427df7
98	121.687640600	192.168.10.10	192.168.10.20	QUIC	1262	Protected Payload (KPB)
99	121.687643800	192.168.10.10	192.168.10.20	QUIC	1262	Protected Payload (KPB)
100	121.687734000	192.168.10.20	192.168.10.10	QUIC	85	Protected Payload (KPB)
101	121.687834300	192.168.10.10	192.168.10.20	QUIC	1262	Protected Payload (KPB)
102	121.687897400	192.168.10.20	192.168.10.10	QUIC	1374	Protected Payload (KPB)
103	121.687985700	192.168.10.10	192.168.10.20	QUIC	1294	Protected Payload (KPB)
104	121.688043400	192.168.10.20	192.168.10.10	QUIC	77	Protected Payload (KPB)
105	121.688560500	192.168.10.10	192.168.10.20	QUIC	68	Protected Payload (KPB)
106	121.688777700	192.168.10.20	192.168.10.10	QUIC	1454	Protected Payload (KPB)
107	121.688984100	192.168.10.10	192.168.10.20	QUIC	1374	Protected Payload (KPB)
108	121.689836800	192.168.10.20	192.168.10.10	QUIC	249	Protected Payload (KPB)
109	121.690245500	192.168.10.10	192.168.10.20	QUIC	68	Protected Payload (KPB)
110	121.690449700	192.168.10.20	192.168.10.10	QUIC	1514	Protected Payload (KPB)
111	121.690519500	192.168.10.10	192.168.10.20	QUIC	1454	Protected Payload (KPB)

Рис. 1. Общий вид захвата трафика SMB over QUIC в Wireshark. Файл: 25u19t3.pcapng, фильтр: udp.port == 443, диапазон пакетов 91–111. Видны пакеты QUIC Initial, Handshake и Protected Payload

На рисунке 1 отчетливо видна структура QUIC-соединения:

- QUIC Initial (пакет 91) — начальный пакет с параметрами соединения и началом TLS-рукопожатия;
- QUIC Handshake (пакеты 92–94) — обмен криптографическими параметрами и сертификатами;
- QUIC Protected Payload (пакеты 95–111 и далее) — зашифрованные данные SMB, которые Wireshark не может декодировать без ключей сессии.

Детальный разбор пакета QUIC Initial, показанный на рисунке 2, демонстрирует наличие расширения server_name со значением SRV-QUIC.local, что подтверждает корректную работу механизма SAN при аутентификации сервера.



Tree View	Details View
Crypto Data	
▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello	
▼ Handshake Protocol: Client Hello	Handshake Type: Client Hello (1) Length: 431
> Version: TLS 1.2 (0x0303)	Random: cc3cd00f44eb4aefc71935739194ac1a8e189132da0014c26bfd2cc28a65270 Session ID Length: 0 Cipher Suites Length: 4
> Cipher Suites (2 suites)	Compression Methods Length: 1
> Compression Methods (1 method)	Extensions Length: 386
> Extension: server_name (len=19) name=SRV-QUIC.local	
> Extension: status_request (len=5)	
> Extension: supported_versions (len=3) TLS 1.3	
> Extension: signature_algorithms (len=26)	
> Extension: session_ticket (len=0)	
> Extension: supported_groups (len=8)	
> Extension: ec_point_formats (len=2)	
> Extension: application_layer_protocol_negotiation (len=6)	
> Extension: key_share (len=208) x25519, secp256r1, secp384r1	

Рис. 2. Детальный разбор пакета QUIC Initial (пакет № 91, файл 25u19t3.pcapng). Видно расширение server_name = SRV-QUIC.local, подтверждающее использование SAN для аутентификации сервера

Все пакеты типа Protected Payload отображаются в Wireshark как зашифрованные, как показано на рисунке 3. Ни имена файлов, ни команды SMB (Create, Read, Write), ни содержимое файлов не поддаются декодированию. Это наглядно демонстрирует эффект сквозного шифрования TLS 1.3, встроенного в протокол QUIC.

Рубрика 2. Методы и системы защиты информации, информационная безопасность

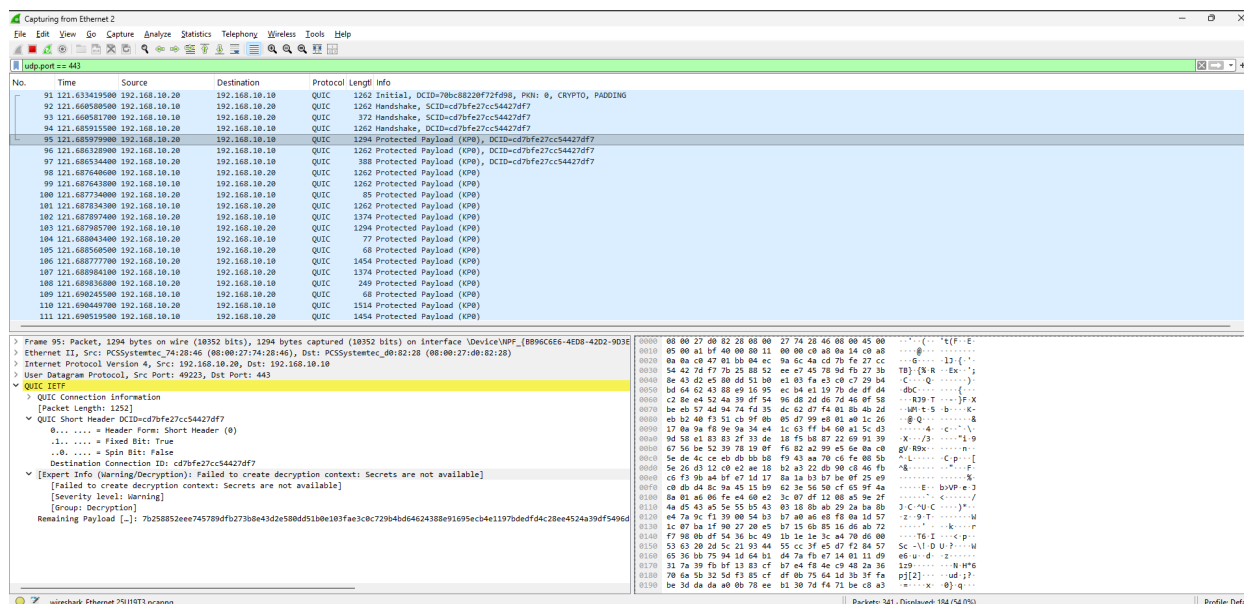


Рис. 3. Пакет QUIC Protected Payload (пакеты №95–111, файл 25u19t3.pcapng). Полезная нагрузка отображается как зашифрованная, декодирование команд SMB и имён файлов невозможно без ключей сессии TLS 1.3

Для сравнения был проведен повторный эксперимент с отключенной поддержкой QUIC на клиенте (Set-SmbClientConfiguration -EnableSMBQUIC \$false). Фильтр Wireshark изменен на tcp.port == 445. Важно отметить, что в данной контрольной конфигурации SMB Encryption на стороне сервера не был включён принудительно, что соответствует настройкам по умолчанию. Подключение и операции с файлом test.txt были повторены в идентичных условиях.

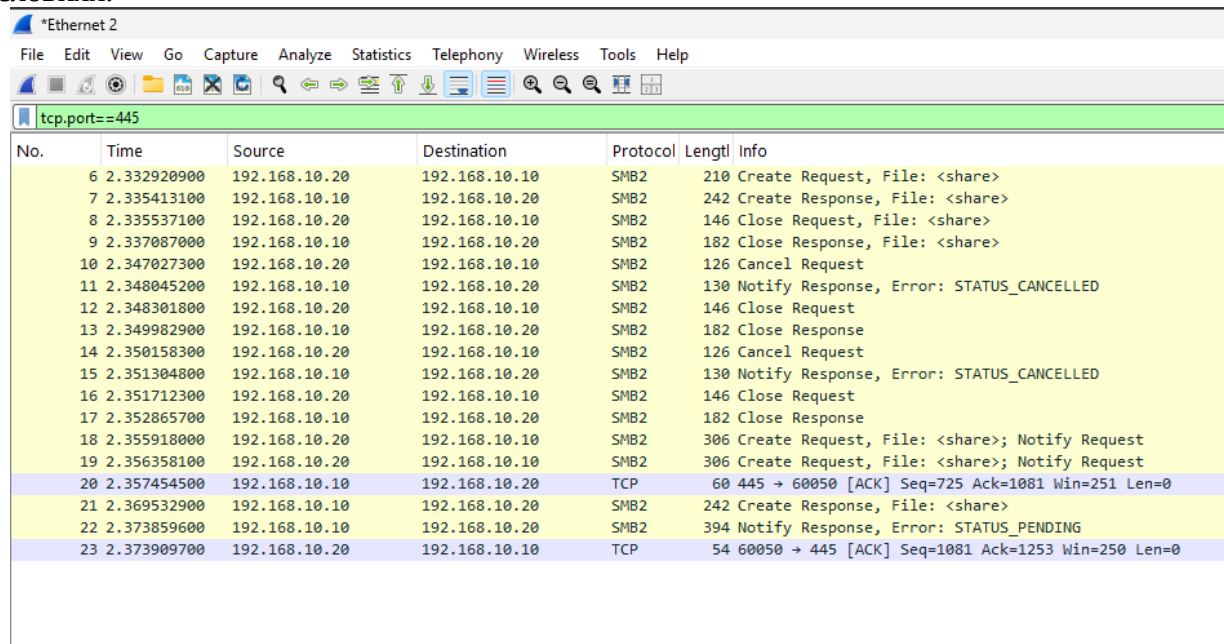


Рис. 4. Общий вид захвата трафика классического SMB over TCP в Wireshark. Файл: 2ieu5t3.pcapng, фильтр: tcp.port == 445, диапазон пакетов 9–20. Видны декодируемые пакеты SMB2

На рисунке 4 отчетливо видны пакеты протокола SMB2 с полностью читаемыми командами: Create Request, Close Request, Notify Request, Read Request. Wireshark успешно декодирует структуру каждого пакета, включая имена файлов и параметры операций.

Детальный разбор пакета SMB2, представленный на рисунке 5, показывает, что в открытом виде передаются:

- имя файла: test.txt;
- команды протокола: Create, Read, Close;

- параметры доступа: Read, Write, Delete;
- временные метки и атрибуты файла.

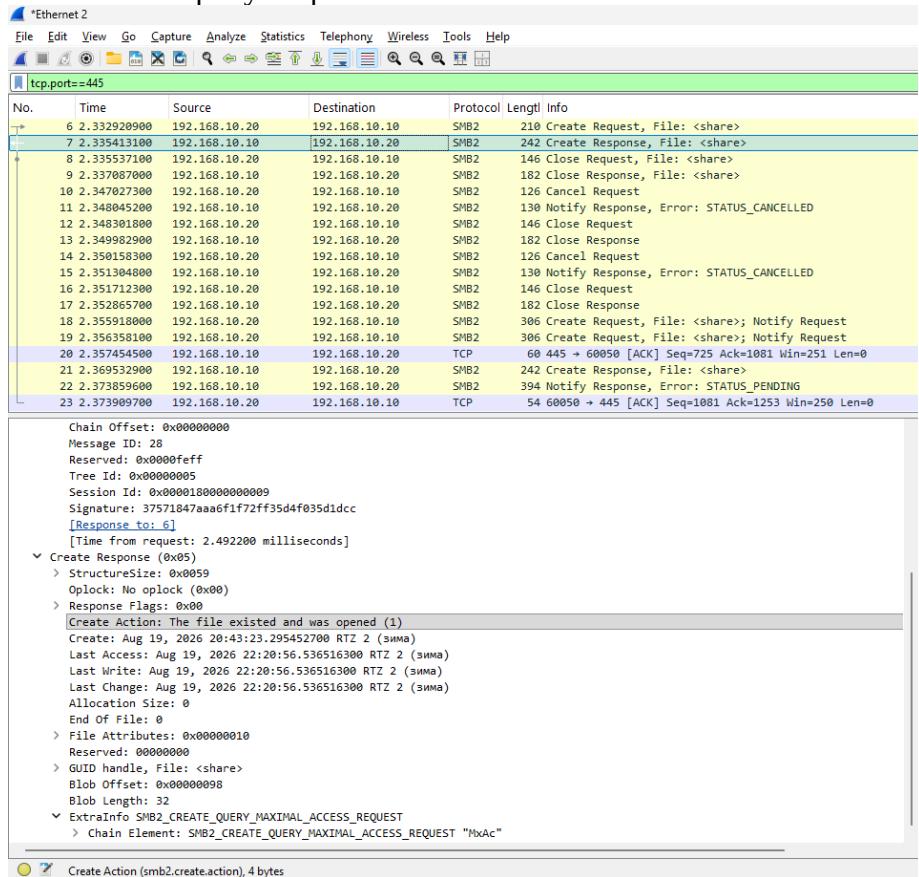


Рис. 5. Детальный разбор пакета SMB2 Create Request (пакет № 19, файл 2ieu5t3.pcapng). В открытом виде отображаются имя файла test.txt и параметры операции. Конфигурация: SMB over TCP без включённого SMB Encryption

Наиболее показательным является пакет SMB2 Read Response, как показано на рисунке 6, в котором содержимое файла передается в открытом виде. В поле данных четко читается текст "Test test test", что подтверждает отсутствие шифрования полезной нагрузки в классическом SMB over TCP при настройках по умолчанию.

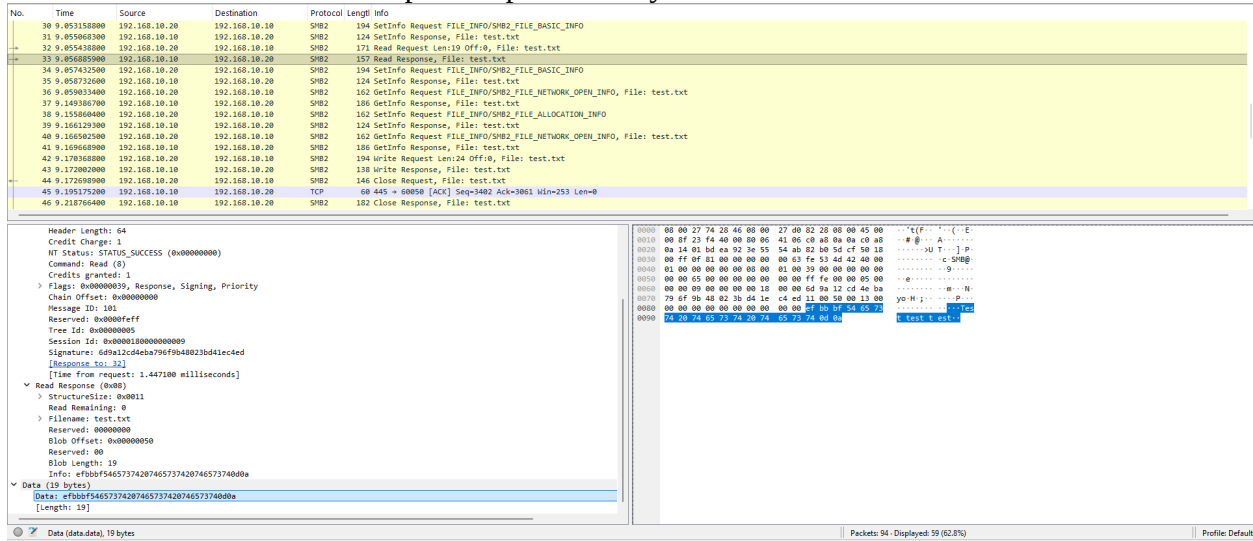


Рис. 6. Пакет SMB2 Read Response (пакет № 20, файл 2ieu5t3.pcapng). Содержимое файла test.txt ("Test test test") передается в открытом виде. Конфигурация: SMB over TCP без включённого SMB Encryption

Таким образом, гипотеза 2 подтверждена. В ходе эксперимента наблюдалось, что в сеансе SMB over QUIC анализатор Wireshark отображает полезную нагрузку исключительно как Protected Payload, не позволяя декодировать команды протокола или имена файлов. В

Рубрика 2. Методы и системы защиты информации, информационная безопасность

контрольном сеансе классического SMB over TCP (порт 445) при настройках по умолчанию (без принудительно включённого SMB Encryption) те же операции (Create Request, Read, Close) и имя файла test.txt отображаются в открытом виде. Наблюдаемое различие согласуется с документацией Microsoft [4] и стандартом RFC 9001 [7], согласно которым SMB over QUIC использует обязательное шифрование TLS 1.3. При этом сетевые метаданные (IP-адреса, порты, размеры пакетов) остаются видимыми в обоих случаях.

Для систематизации результатов исследования составлена таблица 2, отражающая ключевые различия между протоколами.

Таблица 2 – Сравнительный анализ SMB over QUIC и SMB over TCP

Критерий	SMB over QUIC	SMB over TCP
Транспортный протокол	UDP	TCP
Порт	443*	445
Шифрование	Обязательное (TLS 1.3)	Опциональное (по умолчанию отключено)**
Видимость команд SMB в Wireshark	Нет (Protected Payload)	Да (Create, Read, Write, Close)**
Видимость имен файлов	Нет	Да**
Видимость содержимого файлов	Нет	Да**
Аутентификация сервера	X.509 сертификат (SAN)	Kerberos/NTLM

*Доступность порта 443 по протоколу UDP в данной работе показана только в рамках изолированной лабораторной сети. Доступность HTTPS по TCP 443 не гарантирует прохождение UDP-трафика, необходимого для QUIC - в реальных сетях это требует отдельной проверки.

**Наблюдение относится к контрольной конфигурации SMB over TCP без принудительно включённого SMB Encryption.

Эксперимент показал, что SMB over QUIC успешно работает по порту UDP 443 в рамках изолированной лабораторной сети. Важно отметить, что работоспособность в данной работе продемонстрирована только в лабораторных условиях. Доступность HTTPS по TCP 443 не гарантирует прохождения UDP-трафика на порт 443, так как это разные транспортные протоколы, которые могут обрабатываться межсетевыми экранами по-разному, что требует отдельной проверки на конкретном сетевом оборудовании.

В лабораторных условиях было продемонстрировано, что SMB over QUIC может обеспечивать защищенный доступ к файловым ресурсам без необходимости развертывания классических VPN-решений. Однако важно отметить ограничения данного вывода:

- эксперимент проводился в изолированной среде с самоподписанным сертификатом;
- в производственной среде требуется инфраструктура PKI с доверенным центром сертификации;
- SMB over QUIC не заменяет полноценный VPN для доступа ко всем сетевым ресурсам, а только к общим файловым ресурсам SMB.

Таким образом, гипотеза 3 подтверждена частично: использование SMB over QUIC по порту UDP 443 позволяет обойти стандартные ограничения на порт TCP 445 и обеспечивает защищенный доступ к файловым ресурсам, но полная замена VPN-решений требует учета дополнительных факторов (PKI, аутентификация, политики доступа).

Заключение

В ходе исследования была разработана и экспериментально проверена методика безопасного развертывания файлового сервера с поддержкой протокола SMB over QUIC в изолированной лабораторной среде. Был проведен сравнительный анализ структуры сетевого трафика SMB over QUIC и классического SMB over TCP с использованием анализатора Wireshark.

На основе полученных результатов проведена проверка сформулированных гипотез:

Гипотеза 1 подтверждена полностью. Эксперимент доказал техническую реализуемость развертывания SMB over QUIC в изолированной среде без полноценной инфраструктуры Active Directory. Ключевым условием успешной настройки является корректная генерация самоподписанного сертификата X.509 с обязательным указанием альтернативного имени субъекта (SAN), его импорт в доверенное хранилище на клиенте и явная привязка к порту UDP.

Гипотеза 2 подтверждена. Экспериментально наблюдалось, что в сеансе SMB over QUIC анализатор Wireshark отображает полезную нагрузку как Protected Payload, не декодируя команды протокола или имена файлов. В контрольном сеансе классического SMB over TCP при настройках по умолчанию (без включенного SMB Encryption) операции Create Request, Read, Close и имя файла test.txt отображаются в открытом виде. При этом сетевые метаданные (IP-адреса, порты, размеры и временные метки пакетов) остаются видимыми в обоих случаях.

Гипотеза 3 подтверждена частично. Использование порта UDP 443 действительно позволяет успешно обходить стандартные ограничения межсетевых экранов на порт 445, создавая эффект защищенного туннеля. Однако утверждение о том, что SMB over QUIC является универсальной заменой классическим VPN-решениям, требует существенного уточнения. Данный протокол защищает исключительно трафик файлового доступа (SMB), но не обеспечивает маршрутизацию всего сетевого трафика, как это делает полноценный VPN. Кроме того, его безопасное применение в производственной среде невозможно без развернутой инфраструктуры открытых ключей с доверенным центром сертификации, строгой настройки политик аутентификации и аудита.

Перспективные направления дальнейших исследований включают: проведение сравнительного нагрузочного тестирования SMB over QUIC и классического SMB over TCP с принудительно включенным SMB Encryption в условиях высокой интенсивности трафика, исследование механизмов интеграции SMB over QUIC с полноценными корпоративными инфраструктурами открытых ключей (в частности, Active Directory Certificate Services) и сценариев автоматического обновления сертификатов, а также анализ устойчивости соединения QUIC при миграции клиента между разнородными сетями (например, при переходе с Wi-Fi на мобильный интернет) с количественной оценкой времени восстановления сессии. Особый интерес представляет изучение влияния обязательного шифрования TLS 1.3 на производительность файловых операций в высоконагруженных средах, что позволит определить оптимальные сценарии применения протокола. Результаты данной работы могут быть использованы системными администраторами и специалистами по информационной безопасности при проектировании защищенных сценариев удаленного доступа к файловым ресурсам в современных гибридных ИТ-инфраструктурах.

Библиографический список

1. Адживапаев, М. М. Современные транспортные протоколы: TCP, UDP и QUIC Текст научной статьи по специальности «Компьютерные и информационные науки» / М. М. Адживапаев // Информационные технологии и вычислительные системы. – 2025. – [Электронный ресурс] // КиберЛенинка: [сайт]. – URL: <https://cyberleninka.ru/article/n/sovremennyye-transportnye-protokoly-tcp-udp-i-quic> (дата обращения: 18.08.2026).
2. Безопасность SMB. – [Электронный ресурс] // Microsoft Learn: [сайт]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/smb-security> (дата обращения: 22.08.2026).
3. Андреев, Н. С. Исследование клиент-серверных протоколов для повышения отказоустойчивости и безопасности соединения / Н. С. Андреев // Вестник науки и образования. – 2024. – [Электронный ресурс] // КиберЛенинка: [сайт]. – URL: <https://cyberleninka.ru/article/n/issledovanie-klient-servernyh-protokolov-dlya-povysheniya-otkazoustoychivosti-i-bezopasnosti-soedineniya> (дата обращения: 21.08.2026).
4. SMB over QUIC. – [Электронный ресурс] // Microsoft Learn: [сайт]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/smb-over-quic> (дата обращения: 21.08.2026).

Рубрика 2. Методы и системы защиты информации, информационная безопасность

5. TLS 1.3 в Windows Server. – [Электронный ресурс] // Microsoft Learn: [сайт]. – URL: <https://learn.microsoft.com/ru-ru/windows-server/security/tls/tls-1.3> (дата обращения: 18.08.2026).
6. IETF RFC 9000. QUIC: A UDP-Based Multiplexed and Secure Transport. – [Электронный ресурс] // IETF: [сайт]. – URL: <https://www.rfc-editor.org/rfc/rfc9000.html> (дата обращения: 19.08.2026).
7. IETF RFC 9001. Using TLS to Secure QUIC. – [Электронный ресурс] // IETF: [сайт]. – URL: <https://www.rfc-editor.org/rfc/rfc9001.html> (дата обращения: 21.08.2026).
8. QUIC Working Group Documentation. – [Электронный ресурс] // IETF GitHub: [сайт]. – URL: <https://quicwg.github.io/> (дата обращения: 20.08.2026).
9. Симачев, А. Ю. Оценка скрытых каналов по памяти в протоколе QUIC и методы их обнаружения / А. Ю. Симачев // Информационная безопасность регионов России. – 2022. – [Электронный ресурс] // КиберЛенинка: [сайт]. – URL: <https://cyberleninka.ru/article/n/otsenka-skrytykh-kanalov-po-pamyati-v-protokole-quic-i-metody-ih-obnaruzheniya> (дата обращения: 20.08.2026).
10. Смирнов, И. А. HTTP/3 и протокол QUIC: будущее высокопроизводительных веб-сервисов / И. А. Смирнов // Молодой ученый. – 2025. – [Электронный ресурс] // КиберЛенинка: [сайт]. – URL: <https://cyberleninka.ru/article/n/http-3-i-protokol-quic-budushchee-vysokoproizvoditelnykh-veb-servisov> (дата обращения: 19.08.2026).
11. Галимуллина, А. В. Получение событий с клиента и статусе состояния клиентов средствами Samba AD / А. В. Галимуллина // Информационные технологии. – 2024. – [Электронный ресурс] // КиберЛенинка: [сайт]. – URL: <https://cyberleninka.ru/article/n/poluchenie-sobytiy-s-klienta-i-statuse-sostoyaniya-klientov-sredstvami-samba-ad> (дата обращения: 21.08.2026).

References

1. Adzhivapaev, M. M. (2025). Sovremennye transportnye protokoly: TCP, UDP i QUIC [Modern transport protocols: TCP, UDP and QUIC]. *Informatsionnye tekhnologii i vychislitel'nye sistemy*. <https://cyberleninka.ru/article/n/sovremennye-transportnye-protokoly-tcp-udp-i-quic>
2. Microsoft Learn. (n.d.). *SMB security*. <https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/smb-security>
3. Andreyanov, N. S. (2024). Issledovanie klient-servernykh protokolov dlya povysheniya otkazoustoychivosti i bezopasnosti soedineniya [Study of client-server protocols to improve fault tolerance and connection security]. *Vestnik nauki i obrazovaniya*. <https://cyberleninka.ru/article/n/issledovanie-klient-servernykh-protokolov-dlya-povysheniya-otkazoustoychivosti-i-bezopasnosti-soedineniya>
4. Microsoft Learn. (n.d.). *SMB over QUIC*. <https://learn.microsoft.com/ru-ru/windows-server/storage/file-server/smb-over-quic>
5. Microsoft Learn. (n.d.). *TLS 1.3 in Windows Server*. <https://learn.microsoft.com/ru-ru/windows-server/security/tls/tls-1.3>
6. IETF. (2021). *RFC 9000: QUIC: A UDP-Based Multiplexed and Secure Transport*. <https://www.rfc-editor.org/rfc/rfc9000.html>
7. IETF. (2021). *RFC 9001: Using TLS to Secure QUIC*. <https://www.rfc-editor.org/rfc/rfc9001.html>
8. IETF GitHub. (n.d.). *QUIC Working Group Documentation*. <https://quicwg.github.io/>
9. Simachev, A. Y. (2022). Otsenka skrytykh kanalov po pamyati v protokole QUIC i metody ikh obnaruzheniya [Assessment of memory covert channels in the QUIC protocol and methods for their detection]. *Informatsionnaya bezopasnost' regionov Rossii*. <https://cyberleninka.ru/article/n/otsenka-skrytykh-kanalov-po-pamyati-v-protokole-quic-i-metody-ih-obnaruzheniya>
10. Smirnov, I. A. (2025). HTTP/3 i protokol QUIC: budushchee vysokoproizvoditel'nykh veb-servisov [HTTP/3 and QUIC protocol: the future of high-performance web services]. *Molodoy*

uchenyy. <https://cyberleninka.ru/article/n/http-3-i-protokol-quic-buduschee-vysokoproizvoditelnyh-veb-servisov>

11. Galimullina, A. V. (2024). Poluchenie sobytiy s klienta i statuse sostoyaniya klientov sredstvami Samba AD [Obtaining events from the client and the status of clients using Samba AD]. *Informatsionnye tekhnologii*. <https://cyberleninka.ru/article/n/poluchenie-sobytiy-s-klienta-i-statuse-sostoyaniya-klientov-sredstvami-samba-ad>

Информация об авторе

Васильев Никита Сергеевич - студент кафедры "Безопасность информационных технологий", ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация, e-mail: nikita.vasilev.1901@list.ru

SECURITY RESEARCH AND NETWORK TRAFFIC ANALYSIS OF THE SMB OVER QUIC PROTOCOL IN WINDOWS SERVER 2025 INFRASTRUCTURE

Vasilev N. S.¹

¹ National University of Oil and Gas «Gubkin University», Moscow, Russian Federation

Abstract. With growing data volumes and remote work, file resource security has become critical. Traditional SMB over TCP (port 445) is vulnerable to passive traffic interception and is often blocked by firewalls. This article examines SMB over QUIC, which encapsulates SMB traffic into a secure QUIC tunnel over UDP (port 443) with mandatory TLS 1.3 encryption. The study aims to practically verify the deployment methodology of this protocol and to comparatively analyze its network traffic with classic SMB. During the experiment, an isolated laboratory environment based on Windows Server 2025 (version 24H2, build 26100.32230) and Windows 11 Pro (version 25H2, build 26200.7840) was deployed. Using Wireshark 4.6.8 analyzer, traffic of both protocols was intercepted and investigated. The results showed that in an SMB over QUIC session, the analyzer displays the payload exclusively as Protected Payload, without decoding protocol commands or file names. In a control session of classic SMB over TCP (with default settings without forcibly enabled SMB Encryption), the same operations (Create Request, Read, Close) and the file name test.txt (size 1 KB) appear in plain text. It is concluded that SMB over QUIC is a potential alternative to classic VPN solutions exclusively for secure file access, provided that the Public Key Infrastructure (PKI), strict authentication, and auditing are correctly configured, but it does not replace a full-fledged VPN for routing all network traffic. The limitations of the study include the use of a self-signed certificate and a laboratory network without modeling real operating conditions.

Keywords: SMB over QUIC, Windows Server 2025, network security, Wireshark, TLS 1.3, QUIC protocol, file share.

Information about the author

Vasilev Nikita Sergeevich - Student, Department of Information Technology Security, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russian Federation, e-mail: nikita.vasilev.1901@list.ru