УДК 004.057.4

В. Ю. Сапегин[1]*

Исследование технологий маскировки сетевого трафика

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: gvlad224@gmail.com

Аннотация. В статье исследуются методы и принципы, лежащие в основе технологий маскировки сетевого трафика корпоративной вычислительной сети, функционирующей на основе стека протоколов TCP/IP версии 4 и версии 6. В ходе исследования были классифицированы различные технологии маскировки по принципу их построения и целевому назначению. Были выделены преимущества и недостатки каждого класса методов маскировки, которые необходимо учитывать при выборе соответствующих технологий. Описаны существующие решения, комбинирующие методы маскировки трафика и обеспечивающие комплексную сетевую безопасность каналов связи. Приведенное исследование предметной области может использоваться при проектировании и конфигурировании решений обеспечивающих информационную безопасность каналов связи, а также исследование может быть полезно при разработке решений фильтрации сетевого трафика.

Ключевые слова: технологии маскировки, виртуальные защищенные каналы, VPN, стек протоколов TCP/IP, классификация информационных потоков, зондирование

V. Y. Sapegin[1]*

Research of Network Traffic Masking Technologies

[1] National Research Nuclear University MEPhI, Moscow, Russian Federation
* e-mail: gvlad224@gmail.com

Abstract. The article examines the methods and principles underlying the technologies of masking network traffic of a corporate computer network operating on the basis of the TCP/IP protocol stack version 4 and version 6. In the course of the study, various masking technologies were classified according to the principle of their construction and purpose. The advantages and disadvantages of each class of masking methods were highlighted, which must be taken into account when choosing appropriate technologies. The existing solutions combining traffic masking methods and providing comprehensive network security of communication channels are described. The above research of the subject area can be used in the design and configuration of solutions providing information security of communication channels, as well as the research can be useful in the development of network traffic filtering solutions.

Keywords: masking technologies, virtual secure channels, VPN, TCP/IP protocol stack, classification of information flows, probing

Введение

В современном цифровом мире обеспечение сетевой безопасности становится ключевой задачей. Технологии маскировки трафика играют важную роль в защите данных от киберугроз. Мониторинг сетевой активности и вмешательство в приватность становятся все более распространенными, подчеркивая важ-

ность эффективных методов защиты данных и анонимности в Интернете. Однако зачастую данные методы также применяются для обхода правил фильтрации на межсетевых экранах и совершения вредоносных действий. В данном исследовании мы рассмотрим современные методы и технологии маскировки сетевого трафика, анализируя их преимущества и недостатки.

Наиболее популярным направлением применения технологий сокрытия трафика являются сетевые кибератаки, использующие технологии построения виртуальных защищенных каналов связи, какими являются различные VPN (Virtual private network) технологии. Так согласно отчету F.A.C.C.T. за 2023 год [1] в Российской Федерации наиболее распространенным инструментом в совершении атак стали службы удаленного доступа (VPN), так как данные технологии маскируют свой трафик под легитимный и, тем самым, обходят правила на межсетевых экранах, установленных на периметре корпоративной вычислительной сети. Стоит отметить, что различные ученые как из зарубежных, так и из отечественных научных групп, занимаются исследованием проблематики обнаружения вредоносных виртуальных частных сетей. Среди зарубежных исследователей можно выделить группу, включающую Hua Wu, Yujie Liu, Guang Cheng, Xiaoyan Hu, которые специализируются на методах обнаружения VPN с использованием глубокого обучения нейронных сетей [2, 3]. Их научные труды демонстрируют успешные результаты в обнаружении существующих решений маскировки виртуальных защищенных каналов связи, включая семейство протоколов V2Ray. С другой стороны, отечественные ученые, такие как Канатьев К. Н., Шишкин С. Р., Нурмагомедов М. Д., аналогично исследуют данную проблему обнаружения виртуальных защищенных каналов связи в условиях их сокрытия [4, 5].

Еще одним направлением развития технологий маскировки сетевого трафика являются оверлейные сети, такие как Tor (от англ. The Onion Router) и I2P (от англ. Invisible Internet Project). Это связано с развитием методов фильтрации сетевого трафика в оверлейных сетях. В этой области научные исследования ведутся научной школой «Сетевая информационная безопасность» под руководством Басыни Е. А. [6-8].

Важно отметить, что современные технологии маскировки сетевого трафика оказывают влияние и на законодательную составляющую вопроса методов обнаружения. Так, согласно Приказа №168 от 8 ноября 2023 года Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) [9], необходима разработка Единого реестра для внесения VPN/Proxy сервисов, позволяющие обходить правила фильтрации на межсетевых экранах, тем самым получая доступ к информации, распространение которой в Российской Федерации запрещено.

Таким образом, подчеркивается актуальность разработки методов, позволяющих обнаруживать факт маскировки сетевых протоколов и предотвращать обход правил фильтрации на межсетевых экранах.

Постановка задачи

Целью настоящей работы является исследование предметной области, которое включает в себя анализ и классификацию существующих технологий маскировки сетевого трафика.

Исследование предметной области

Существует огромное количество различных технологий маскировки сетевого трафика. Все их можно разбить на два отдельных больших класса, представленных на рис. 1, в зависимости от их целевого назначения.

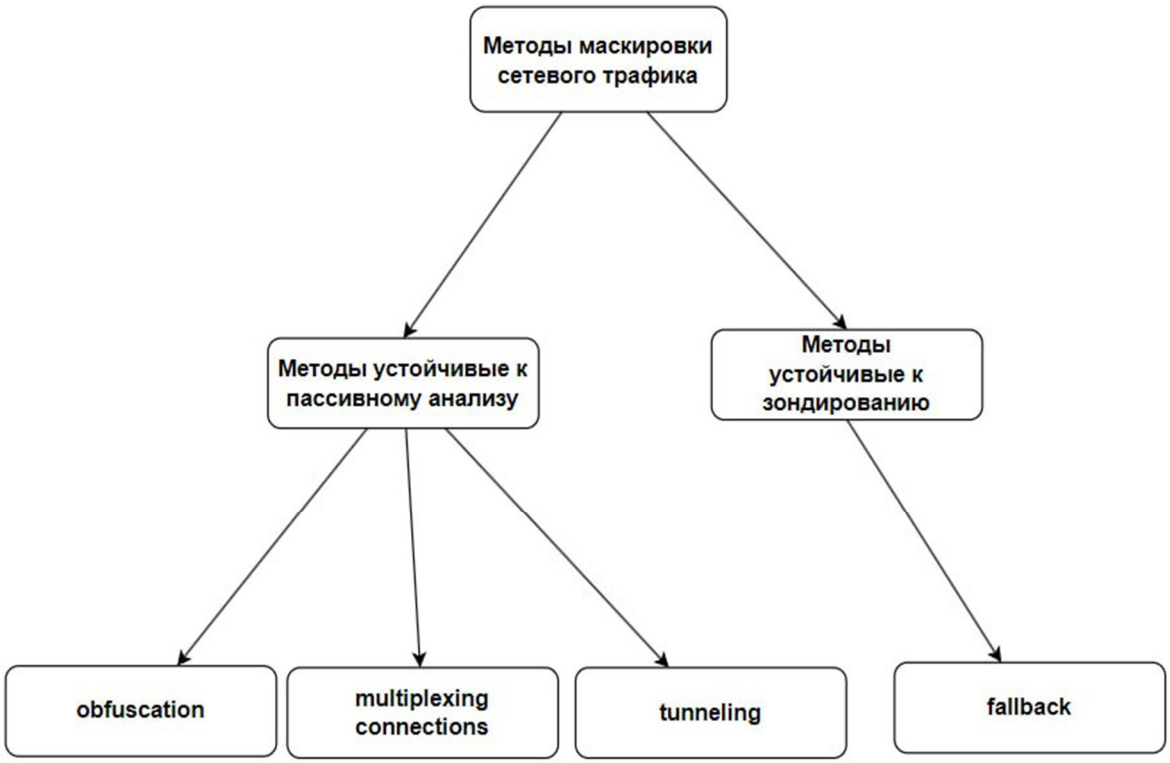

Рис. 1. Классификация методов маскировки сетевого трафика стека протоколов TCP/IP v4/v6

Первый класс – это методы маскировки, противодействующие пассивному анализу соединения. Под пассивным анализом понимается анализ пакетов, захваченных в неразборчивом режиме (sniffing пакетов), в рамках которого формируются логические информационные потоки из захваченных пакетов, и на основе данных потоков строится классификация сетевого трафика. Решением проблемы пассивного анализа соединения являются такие технологии, как обфускация (от англ. obfuscation), мультиплексирование соединений (от англ. multiplexing connections), туннелирование протоколов (от англ. tunneling).

Обфускация – это технология маскировки посредством преобразования полезной нагрузки транспортных протоколов, а именно – полное ее шифрование на первом же этапе соединения. Со стороны пакеты выглядят случайными, и при

пассивном анализе их нельзя соотнести с конкретными сетевыми протоколами. Яркими представителями технологии обфускации являются obfs4 [10], используемый в оверлейной сети Tor для подключений к сетевым мостам и, тем самым, для обхода блокировок по IP входных node сети и Shadowsocks [11], используемый для обфускации сетевого трафика прокси-протокола socks5.

Мультиплексирование соединений – это технология маскировки посредством создания ограниченного числа TCP соединений с сервером VPN/Proxy. Таким образом, все отдельные соединения, открываемые клиентом, будут передаваться через заранее созданные соединения. Мультиплексирование соединений позволяет перемешивать различные соединения между собой, усложняя пассивный анализ отдельно взятых соединений. Например, сложнее становится классифицировать тип контента, передаваемого в рамках соединения клиента. Одним из существующих решений маскировки, поддерживающих технологию мультиплексирования, является Cloak [12].

Туннелирование сетевых протоколов – это технология маскировки посредством инкапсулирования сетевых пакетов одного фильтруемого протокола в другой легитимный протокол. Наиболее распространенный вид туннелирования – туннелирование через протокол TLS, в ходе которого прокси-протоколы или протоколы обфускации инкапсулируются в полезную нагрузку протокола TLS. Важно отметить, что в случае туннелирования уже зашифрованного трафика, например, трафик Shadowsocks [11], дополнительного шифрования не происходит, потому что повторное шифрование может увеличить энтропию шифртекста и, тем самым, может быть раскрыт факт маскировки сетевого трафика детекторами. Одной из самых известных пар протоколов туннелирования является OpenVPN [13] + Stunnel [14], но данная связка не поддерживает большое количество новых возможностей существующих протоколов туннелирования. Например, Stunnel не поддерживает режим отключения повторного шифрования данных. Наиболее популярными новыми представителями протоколов туннелирования являются Trojan [15], Xray [16], связка Shadowsocks [11] + Cloak [12], которые поддерживают туннелирование TLS без повторного шифрования данных, а также технологию fallback.

Второй большой класс – это методы маскировки, противодействующие активному анализу соединений, а именно зондированию. Под зондированием понимается тестирование соединения внешним наблюдателем, привносящим различные задержки в соединения, повторения отправки пакетов, изменения порядка пакетов, а также отправки собственно собранных видов пакетов. Наиболее популярной технологией противодействия зондированию является fallback на серверах VPN/Proxy.

Fallback – это технология маскировки сервера под легитимный сервис для не аутентифицированных пользователей. Аутентификация пользователя происходит по заранее сгенерированной ключевой паре и UID (от англ. User Identifier) клиента. Публичные ключи и UID распространяются между клиентами. Клиент на первом этапе подключения к серверу генерирует эфемерные ключи, после чего на основе публичного ключа, полученного от сервера и эфемерной пары

вырабатывается общий секрет. UID шифруется на общем секрете и заносится в пакет TLS Client Hello, после чего сервер при получении запроса вырабатывает общий секрет и расшифровывает поле, содержащее UID. Если UID совпадает, то происходит проксирование соединения, иначе происходит переброс входного TLS Client Hello пакета на легитимный запасной сервис, функционирующий в рамках того же IP адреса, если это CDN (от англ. Content distribution network) узел, или же на заранее подготовленный веб-сервис. Описанный алгоритм представлен на рис. 2.

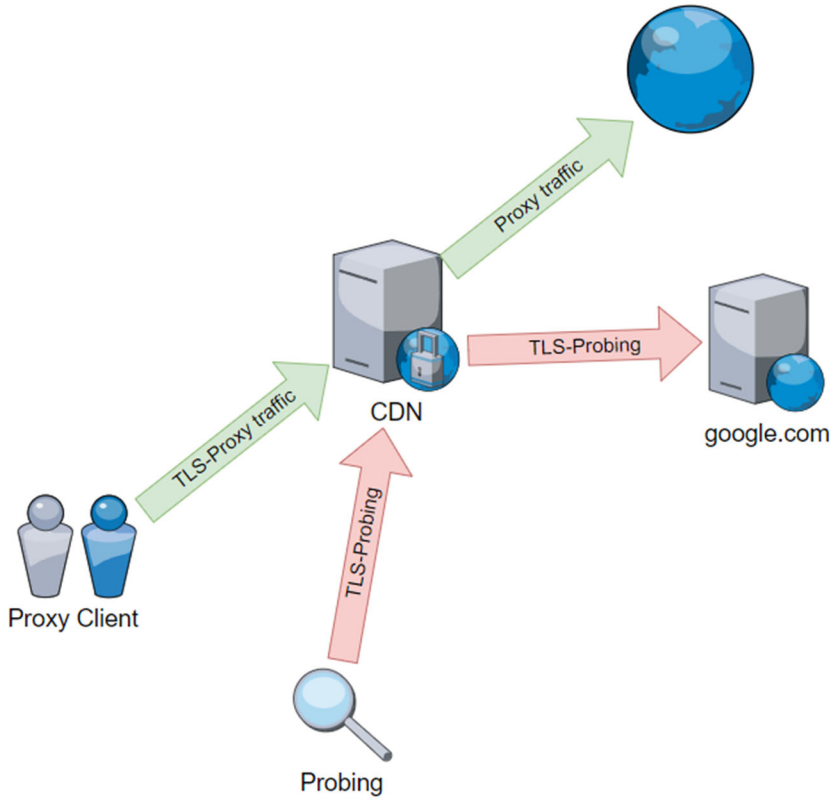

Рис. 2. Пример работы технологии fallback

Наиболее популярными решениями, поддерживающими данную технологию, являются Cloak [12], Trojan [15], Xray [16].

Заключение

В рамках статьи был проведено исследование предметной области технологий маскировки сетевого трафика стека протоколов TCP/IP версии 4 и версии 6, в ходе которого были проанализированы и классифицированы существующие методы маскировки трафика по принципу работы и назначению, а также были детально рассмотрены наиболее популярные технологии маскировки сетевого трафика. Кроме того, представлены недостатки и преимущества каждой технологии, а также приведены существующие решения, реализующие рассмотренные методы маскировки сетевого трафика.

Значимость работы заключается в том, что результаты проведенного исследования могут использоваться в дальнейшем для проектирования систем и разработки методов фильтрации маскированного сетевого трафика стека протоколов TCP/IP версии 4 и версии 6.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Универсальный шифровальщик: количество кибердиверсий в России в 2023 году выросло на 140% // F.A.C.C.T. – URL: https://www.facct.ru/media-center/press-releases/cyberattacks-2023/ (дата обращения: 21.04.2024).

2. Wu H. et al. Real-time identification of VPN traffic based on counting Bloom filter and chained hash table from sampled data in high-speed networks //ICC 2022-IEEE International Conference on Communications. – IEEE, 2022. – С. 5070-5075.

3. Wu H. et al. RT-CBCH: Real-time VPN Traffic Service Identification based on Sampled Data in High-speed Networks //IEEE Transactions on Network and Service Management. – 2023.

4. Обзор методов обнаружения VPN и DNS-анализ для классификации на примере Hotspot Shield Free / К. Н. Канатьев, С. Р. Шишкин, И. И. Басыров [и др.] // Инновации и инвестиции. – 2023. – № 10. – С. 215-219.

5. Передовые методы обнаружения и обфускации VPN-трафика: углубленный анализ OpenVPN и его уязвимостей в современную цифровую эпоху / К. Н. Канатьев, М. Д. Нурмагомедов, А. А. Гребенщиков [и др.] // Инновации и инвестиции. – 2023. – №10. – С. 211-214.

6. Басыня Е. А. Система самоорганизующегося виртуального защищенного канала связи / Е. А. Басыня // Защита информации. Инсайд. – 2018. – № 5 (83). – С. 10–15.

7. System of a self-organizing virtual secure communication channel based on stochastic multilayer encryption and overlay technologies / E. A. Basinya, Z. B. Akhayeva, D. H. Omarkhanova, G. B. Tolegenova [et al.] // Journal of Theoretical and Applied Information Technology. – 2022. – Vol. 100, iss. 16. – P. 4918-4927.

8. Басыня Е. А. Программная реализация и исследование системы интеллектуально-адаптивного управления информационной инфраструктурой предприятия / Е. А. Басыня // Вестник Самарского государственного технического университета. Серия: Технические науки. – 2020. – Т. 28, № 1 (65). – С. 6-21.

9. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций "О внесении изменений в Критерии оценки материалов и (или) информации, необходимых для принятия Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций решений, являющихся основаниями для включения доменных имен и (или) указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет", а также сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", в единую автоматизированную информационную систему "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено", утвержденные приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27 февраля 2023 г. N 25" от 08.11.2023 № 168 // Собрание законодательства Российской Федерации. 01.12.2023 г.

10. obfs4 [Электронный ресурс]. – URL: https://gitlab.com/yawning/obfs4 (дата обращения: 21.04.2024).

11. Shadowsocks. – URL: https://github.com/shadowsocks/shadowsocks-rust (дата обращения: 21.04.2024).

12. Cloak. – URL: https://github.com/cbeuw/Cloak (дата обращения: 21.04.2024).

13. OpenVPN. – URL: https://openvpn.net/ (дата обращения: 21.04.2024).
14. Stunnel. – URL: https://www.stunnel.org/ (дата обращения: 21.04.2024).
15. Trojan. – URL: https://github.com/trojan-gfw/trojan (дата обращения: 21.04.2024).
16. Xray. – URL: https://github.com/XTLS/Xray-core (дата обращения: 21.04.2024).