УДК 004.056

Исследование и системный сравнительный анализ протоколов туннелирования, устойчивых к атакам детектирования.

Коробейников Максим Алексеевич (ИТМО)
Научный руководитель - инженер ФБИТ Савков Сергей Витальевич (ИТМО)

Введение. В современных условиях стремительного темпа развития технологий и общего увеличения объемов передаваемой информации по каналам связи, вопросы безопасности и конфиденциальности данных становятся особенно актуальными. Протоколы туннелирования играют важную роль в обеспечении скрытной передачи информации, позволяя создавать защищенные каналы связи с инкапсуляцией полезной нагрузки в пакеты широко используемых протоколов и тем самым защищать данные от несанкционированного доступа. Однако с ростом популярности таких решений также увеличивается количество атак, направленных на их детектирование и блокировку.

Основная часть. Проведение исследования и системного сравнительного анализа протоколов туннелирования сопряжено с рядом задач, направленных на выявление слабых мест в безопасности каждого из протоколов:

1) Краткий обзор наиболее популярных протоколов туннелирования: Trojan [6], ShadowSocks [4], VLESS [3], VMESS [3], Wireguard [5], L2TP [7]. Для дальнейшего исследования и проведение анализа необходимо базовое ознакомление с существующими решениями и понимание специфики их функционирования.
2) Обзор современных методик детектирования туннелирования трафика. Важно знать не только о протоколах которые скрывают трафик, но и о методиках которые позволяют такой трафик выявлять [1].
3) Исследование слабых мест каждого из протоколов и условий их использований, повышающих вероятность детектирования. Механизмы работы рассматриваемых протоколов одинаковые по цели, но абсолютно разные по устройству. Для полноты картины необходимо понимать, где находятся слабые стороны у каждого протокола и что мешает протоколу повысить устойчивость к детектированию [2].

Выводы. Протоколы туннелирования играют важную роль в обеспечении конфиденциальности передаваемой информации. Понимание механизмов и специфик работы наиболее популярных из них позволяет выбирать наиболее подходящий протокол в зависимости от задач, целей, факторов, топологии сети и ее загруженности.

Список использованных источников:

1. A.I. Get'man, E.F. Evstropov, Y.V. Markin “Wirespeed network traffic analysis: survey of applied problems, approaches and solutions”
2. “Туннели и VPN, устойчивые к DPI” // URL: https://habr.com/ru/articles/415977/ (дата обращения: 17.01.2025)

3. XTLS Project. URL: https://xtls.github.io/ (дата обращения: 18.01.2025)
4. ShadowSocks Project. URL: https://shadowsocks.org/doc/what-is-shadowsocks.html (дата обращения: 20.01.2025)
5. Wireguard Project. URL: https://www.wireguard.com/protocol/ (дата обращения: 25.01.2025)
6. Trojan Project. URL: https://trojan-gfw.github.io/trojan/protocol.html (дата обращения: 26.01.2025)
7. IDM Docs. URL: https://www.ibm.com/docs/ru/i/7.3?topic=concepts-layer-2-tunnel-protocol (дата обращения: 29.01.2025)