УДК 004.77

Д. С. Антропов[1], Ю. Н. Ханбекова[1]*

Испытательный стенд для проведения исследований технологий построения виртуальных защищенных каналов связи

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: a.Danila2001@yandex.ru

Аннотация. В статье представлен собственный испытательный стенд для проведения исследований технологий построения виртуальных защищенных каналов связи. Описывается один из возможных способов организации взаимодействия клиента и сервера с автоматизированной настройкой установления соединения, последующим анализом и классификацией полученного трафика, опираясь на современные решения быстрой организации систем и функций взаимодействия клиента с представленным решением. В качестве протоколов, которые возможно настроить на стенде и провести их исследование, представлены популярные решения, такие как IPSec+L2TP/IKEv2, OpenVPN (+ Stunnel), WireGuard, ShadowSocks, Trojan, Xray. Приведенное исследование предметной области может использоваться для анализа фильтрации виртуальных защищенных корпоративных каналов, а также для создания новых протоколов безопасного обмена информацией при помощи шифрования.

Ключевые слова: VPN, виртуальные защищенные каналы, виртуальные частные сети, виртуальная инфраструктура, стек протоколов TCP/IP, классификация информационных потоков

D. S. Antropov[1], J. N. Khanbekova[1]*

Test Bench for Conducting research on technologies for Constructing Virtual Secure Communication Channels

[1] National Research Nuclear University MEPhI, Moscow, Russian Federation
* e-mail: a.Danila2001@yandex.ru

Abstract. The article presents its own test bench for conducting research on technologies for constructing virtual secure communication channels. Describes one of the possible ways to organize interaction between a client and a server with automated setup of connection establishment and subsequent analysis and classification of received traffic subsequently, based on modern solutions for quickly organizing systems and functions for client interaction with the presented solution. Popular solutions such as IPSec+L2TP/IKEv2, OpenVPN (+ Stunnel), WireGuard, ShadowSocks, Trojan, Xray are presented as protocols that can be configured at the stand and conducted research. The presented research of the subject area can be used to analyze the filtering of virtual secure corporate channels, as well as the creation of new protocols for the secure exchange of information using encryption.

Keywords: VPN, virtual secure channels, virtual private networks, virtual infrastructure, TCP/IP protocol stack, classification of information flows

Введение

Развитие информационно-коммуникационных технологий, в число которых входят виртуальные защищенные каналы связи, приводит к возрастанию атак на различные области этой сферы. Так, зафиксирована тенденция увеличения количества атак в России с использованием технологии VPN [1]. Причиной является

быстрое развитие различных видов рассматриваемого решения. Это подчеркивает необходимость разработки новых методов и систем, которые позволят исследовать и анализировать передаваемый трафик внутри туннелей виртуальных защищенных каналов связи.

На сегодняшний день существует широкий набор методов обнаружения виртуальных защищенных каналов связи, что обеспечивает возможность изучения различных технологий их создания. Группа зарубежных ученых Hua Wu, Yujie Liu, Guang Cheng, Xiaoyan Hu занимается исследованием виртуальных защищенных каналов связи с использованием глубокого обучения нейронных сетей [2, 3]. Однако в этом разнообразии методов отсутствуют эффективные подходы, способные учитывать современные тенденции в создании таких каналов с использованием разнообразных методов маскировки, что порождает необходимость в исследовании данных технологий. Исследованием технологий виртуальных защищенных каналов связи в рамках маскировки, например, обфускации, занимается научная школа «Сетевая информационная безопасность» под руководством Басыни Е. А. [4, 5].

Согласно Приказа № 168 от 8 ноября 2023 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) [6] и на законодательном уровне наблюдается активность в рамках регулирования технологий в условиях маскировки, что акцентирует внимание на их обнаружении.

Таким образом, возрастает актуальность разработки решений, позволяющих провести новые исследования в области сетевого взаимодействия через защищенные каналы связи при помощи шифрования и маскировки.

Постановка задачи

Целью работы является проектирование и реализация стенда сбора и анализа трафика виртуальных защищенных каналов связи с использованием автоматизированных средств организации виртуального испытательного стенда, а также обеспечение мониторинга всей системы для полного наблюдения за всеми компонентами.

Предлагаемое решение

Для достижения поставленной цели разрабатывается стенд, обеспечивающий передачу данных внутри организованной сети и сбор данных трафика с последующим анализом полученного объема информации. Также разрабатывается конечное решение, автоматизирующее процессы развертки и конфигурирования выбранного программного стека.

Представленное решение для проведения исследований технологий построения ВЗКС (виртуальных защищенных каналов связи) включает в себя такие ключевые компоненты, как межсетевые экраны (firewall), базы данных, интерфейс взаимодействия пользователей со стендом и виртуальные машины, выступающие в роли клиента и сервера для реализации сетевого взаимодействия, приближенного к реальному общению узлов соединения (рис. 1).

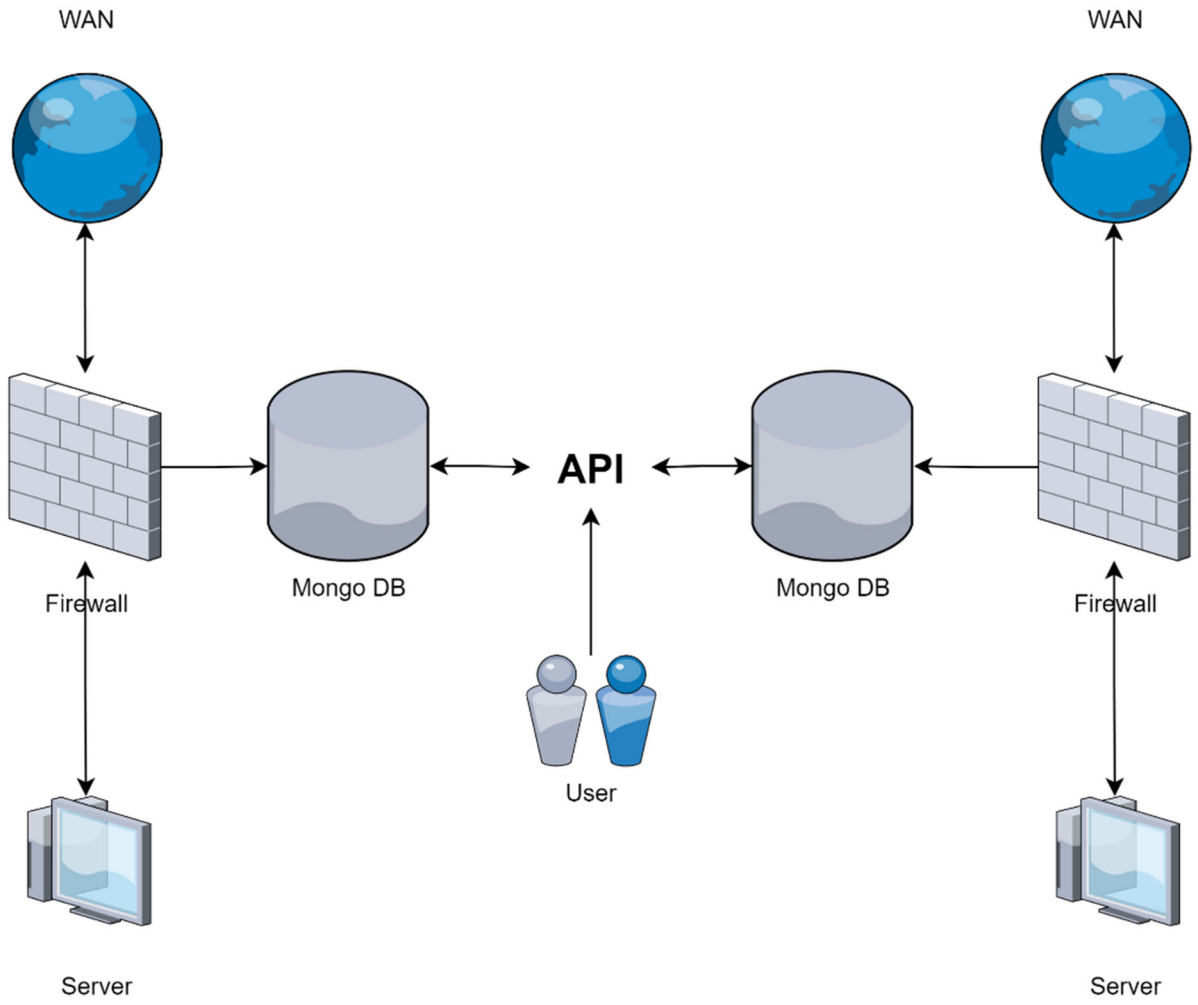

Рис. 1. Архитектура разработанного стенда

Технологии автоматизированной настройки стенда помогали обеспечить быструю организацию всех компонент для передачи пакетов между клиентом и сервером. В качестве таких технологий используются Vagrant, Ansible и Virtual Box (рис. 2).

Сбор и анализ трафика обеспечивается использованием программы отслеживания пакетов Suricata. Данный выбор был сделан в пользу этого решения, так как Suricata является мощной системой обнаружения (IDS, от англ. Intrusion Detection System) и вторжения (IPS, от англ. Intrusion Prevention System), разработанной для анализа сетевого трафика в реальном времени. Технология имеет поддержку сигнатур и правил, позволяющих использовать гибкую настройку для обнаружения аномалий в сетевом трафике с последующей фиксацией этих событий и анализа собранных данных.

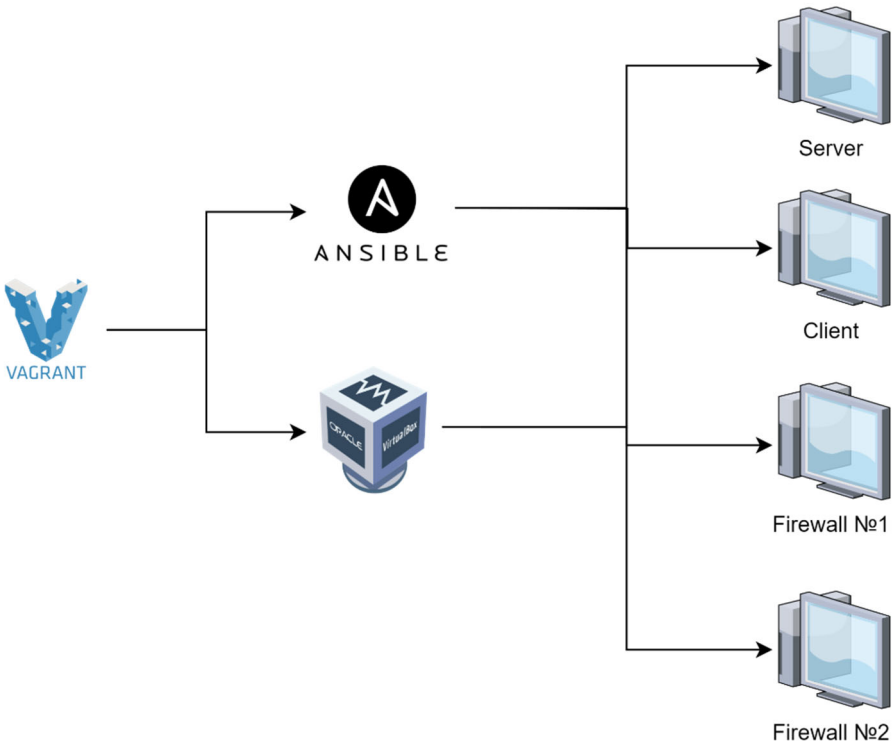

Рис. 2. Схема работы автоматизации организации стенда

Собранные данные сетевого трафика сохраняются в базе данных, к которой через запросы к API (от англ. application programming interface) может обратиться пользователь стенда.

Выполнение процессов, необходимых для удовлетворения запросов пользователей, является ключевой функцией предлагаемого стенда. Используя свои возможности, API инициирует запрос к базе данных (БД) для получения запрошенных данных сетевого пакета. В то же время база данных пополняется новыми данными о сетевых пакетах, обеспечивая актуальность и доступность данных для поиска. После того, как база данных заполнена информацией о пакетах, сервер извлекает необходимую информацию и проводит тщательный анализ, используя передовые методы обработки и агрегации. После получения необходимых данных формируется ответ и передается пользователю. Этот ответ может принимать различные формы, такие как описание или предоставление в базовом виде данных, обеспечивая пользователям ценную информацию для принятия обоснованных решений.

Предлагаемая архитектура системы включает программу анализа пакетов, разработанную на Python с использованием Scapy. Хранение сетевых пакетов обеспечивается сохранением в базы данных MongoDB благодаря ее гибкой конструкции без схемы и возможности горизонтального масштабирования. MongoDB поддерживает данные в формате JSON, что упрощает их хранение и извлечение, а документно-ориентированный подход упрощает манипулирование и анализ отдельных пакетов. В базе данных MongoDB присутствуют две коллек-

ции: «пакеты» и «счетчики». База данных развертывается в виде кластера в облачной сети MongoDB, обеспечивая высокую доступность и масштабируемость. Набор данных «пакетов» имеет поля для хранения идентификатора, слоев, отметки времени, имени пакета и данных. Набор данных «счетчики» имеет поля для хранения количества различных пакетов и меток времени, собранных во время установленного соединения.

В качестве базовых технологий ВЗКС были взяты IPSec+L2TP/IKEv2 [15], OpenVPN [16] и WireGuard [17]. Также для анализа технологий, которые обеспечивают передачу данных с шифрованием, был настроен Shadowsocks [18]. Взаимодействие сервера и клиента было организовано при помощи связки пары протоколов туннелирования OpenVPN [16] + Stunnel [21]. Однако не только эти технологии возможно настроить в рамках этого стенда. Популярные протоколы туннелирования Trojan [22], Xray [20] включаются в список технологий ВЗКС, для которых можно провести экспериментальные замеры скорости, анализа трафика, сбора данных и метрик во время соединения конечных узлов.

Заключение

В рамках данной работы был создан испытательный стенд для проведения исследований технологий построения виртуальных защищенных каналов связи с обеспечением сбора метрик и данных о сетевом взаимодействии.

Теоретическая значимость работы заключается в проектировании архитектуры и исследовании сетевого трафика технологий ВЗКС в рамках базового взаимодействия и в условиях маскировки, функционирующих на базе стека протоколов TCP/IP.

Практическая значимость заключается в сборе метрик и сетевых данных взаимодействия в рамках ВЗКС, что позволяет провести анализ полученных результатов и предложить решения по снижению риска утечек персональных данных и результатов интеллектуальной деятельности предприятий и организаций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Miller S., Curran K., Lunney T. Detection of virtual private network traffic using machine learning // International Journal of Wireless Networks and Broadband Technologies (IJWNBT). – 2020. – Т. 9. – №. 2. – С. 60-80.

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. Басыня Е. А., Французова Г. А., Гунько А. В. Самоорганизующаяся система управления трафиком вычислительной сети // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2014. – №. 1 (31). – С. 179-184.

5. Басыня Е. А. Метод управления трафиком на межсетевых узлах локальных вычислительных сетей // Известия Самарского научного центра Российской академии наук. – 2014. – Т. 16. – №. 4-3. – С. 507-511.

6. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций "О внесении изменений в Критерии оценки материалов и (или) ин-

формации, 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.

7. Wahanani H. E., Idhom M., Mandyartha E. P. Analysis of streaming video on VPN networks between OpenVPN and L2TP/IPSec //2021 IEEE 7th Information Technology International Seminar (ITIS). – IEEE, 2021. – С. 1-5.

8. Yuanxun W. et al. Performance Test and Analysis of Ground-Air Communication Network based on IPSec VPN //2021 IEEE 5th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). – IEEE, 2021. – Т. 5. – С. 1136-1142.

9. Praneeth B. et al. Remote Packet Monitoring: Real-Time Network Analysis from Anywhere //2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT). – IEEE, 2024. – С. 699-703.

10. Mamchenko M. Modeling the Performance of IEEE 802.11 ac WLAN Network for Remote Visual SLAM //2023 16th International Conference Management of large-scale system development (MLSD). – IEEE, 2023. – С. 1-5.

11. Budiyanto S. et al. Auto Discover Virtual Private Network Using Border Gateway Protocol Route Reflector //2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT). – IEEE, 2022. – С. 123-129.

12. Wei X. et al. Research and design of high performance VPN Security System Based on VPP //2021 7th International Conference on Computer and Communications (ICCC). – IEEE, 2021. – С. 2038-2041.

13. Aswad S. A., Sonuç E. Classification of VPN network traffic flow using time related features on Apache Spark // 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). – IEEE, 2020. – С. 1-8.

14. Bu Z. et al. Encrypted network traffic classification using deep and parallel network-in-network models // Ieee Access. – 2020. – Т. 8. – С. 132950-132959.

15. IPSec Overview [Электронный ресурс]. – URL: https://www.ciscopress.com/articles/article.asp?p=25470 (дата обращения: 22.04.2024).

16. OpenVPN. – URL: https://openvpn.net/ (дата обращения: 23.04.2024).

17. WireGuard. – URL: https://www.wireguard.com/ (дата обращения: 24.04.2024).

18. Shadowsocks. – URL: https://github.com/shadowsocks/shadowsocks-rust (дата обращения: 22.04.2024)

19. Cloak. – URL: https://github.com/cbeuw/Cloak (дата обращения: 23.04.2024)

20. Xray. – URL: https://github.com/XTLS/Xray-core (дата обращения: 23.04.2024)

21. Stunnel. – URL: https://www.stunnel.org/ (дата обращения: 25.04.2023).

22. Trojan. – URL: https://github.com/trojan-gfw/trojan (дата обращения: 25.04.2024)

23. В. Олифер, Н. Олифер. Компьютерные сети. Принципы, технологии, протоколы: юбилейное издание. – Санкт-Петербург : Питер, 2021. – 1008 с.