DOI: 10.37791/2687-0649-2022-17-5-88-101

Development of a secure neural traffic tunneling system with post-performance evaluation

A. Zaenchkovski[1]***, A. Lazarev***[1*]***, V. Sinyavskiy***[1]
[1]*Branch of the National Research University "MPEI" in Smolensk, Smolensk, Russia*
[*]*anonymous.prodject@gmail.com*

Abstract. Currently information exchange methods and means of communication development are being done a significant impact on the level of all industrial and economic entities innovation potential, which is also the same for their group formations, such as regional complexes. It is necessary to note high degree of integration and interdependence of all such systems elements and processes closely interconnected by different kind of networks. Among them, it is possible to highlight the interaction between participants of scientific and industrial cluster within the framework of innovative activities, which should provide possibility to transfer and receive various kinds of data, which could be both open and confidential type. At the current stage, there is not many applied tools for ensuring confidentiality in the implementation of these processes. For example, they partially solve the problem of traffic tunnelling systems based on OpenVPN or WireGuard tunnels, and other software solutions provide the potential of an extensible cloud (Nextcloud). However, analysing the functionality of these solutions, it is possible to identify shortcomings that do not allow their implementation in the complex production and economic systems processes of innovative development. Thus, existing traffic tunnelling solutions are not adapted for deployment on a corporate scale with a flexible organisational structure. In solutions based on Nextcloud, the complexity disadvantages of the server configuration and the cost of the primary software configuration are highlighted. To solve the above problems, in article has been proposed an intelligent traffic tunneling system, which is based on using additional means of primary automated OpenVPN connection initialization at neural module expense. A dynamic digital fingerprint distribution system with two-way key exchange was used as an authorization server. The developed software solution was tested and then compared with existing analogues. This experiment may to conclusion that the developed software solution is not inferior in a number of aspects to existing methods, and can subsequently be used to ensure secure information and communication exchange between industrial and economic entities in clusters during innovative processes implementation.

Keywords: traffic tunneling, two-factor authentication, scientific and industrial cooperation, neural network forecasting, traffic optimization, innovation process

For citation: Zaenchkovski A., Lazarev A., Sinyavskiy V. Development of a secure neural traffic tunneling system with post-performance evaluation. *Prikladnaya informatika*=Journal of Applied Informatics, 2022, vol.17, no.5, pp.88-101. DOI: 10.37791/2687-0649-2022-17-5-88-101

Разработка безопасной системы нейронного туннелирования траффика с постоценкой производительности работы

А.Э. Заенчковский[1]***, А.И. Лазарев***[1*]***, В.Ю. Синявский***[1]
[1]*Филиал ФГБОУ ВО «Национальный исследовательский университет «МЭИ» в г. Смоленске, Смоленск, Россия*
[*]*anonymous.prodject@gmail.com*

Аннотация. В настоящее время развитие средств коммуникации и способов обмена информацией оказывает существенное влияние на все стороны деятельности производственно-хозяйствующих субъектов, в том числе на их уровень инновационного потенциала. Также как следствие можно отметить высокую степень интеграции отдельных элементов и субъектов в рамках инновационной деятельности и взаимозависимость частей таких формирований, тесно взаимосвязанных сетью различных процессов. Усложнение самих инновационных процессов, их высокая стоимость, рискованность, комплексный характер, лежащие в самой природе инноваций, а также специализация отдельных субъектов на частных операциях и этапах реализации только усиливают данные тенденции. Можно выделить ряд существующих прикладных инструментов, направленных на обеспечение информационной безопасности при формировании и передаче данных различного рода, имеющих как открытый, так и конфиденциальный характер. Например, частично позволяют решить проблему системы туннелирования трафика на базе OpenVPN или WireGuard-туннелей, а другие программные решения предоставляют потенциал расширяемого облака (Nextcloud). Однако, проводя анализ функциональности данных решений, можно выделить недостатки, не позволяющие выполнить их внедрение в процессы инновационного развития сложных производственно-хозяйственных систем. Так, существующие решения туннелирования трафика не адаптированы для развертки в корпоративных масштабах с наличием гибкой оргструктуры. В решениях на базе Nextcloud выделяются недостатки сложности конфигурации сервера и затрат на первичную конфигурацию ПО. Для решения указанных выше проблем в статье предлагается разработанная интеллектуальная система туннелирования трафика с использованием дополнительных средств первичной автоматизированной инициализации соединения за счет нейронного модуля на базе OpenVPN. В качестве авторизирующего сервера использована динамическая система раздачи цифровых отпечатков с двухсторонним обменом ключами. Разработанное программное решение было протестировано, и приведено сравнение с существующими аналогами. В результате можно отметить, что разработанное решение не уступает существующим способам и впоследствии может быть использовано для обеспечения безопасного информационно-коммуникационного обмена между субъектами научно-промышленного кластера при реализации инновационных процессов.

Ключевые слова: туннелирование трафика, двухфакторная аутентификация, научно-промышленная кооперация, нейросетевое прогнозирование, оптимизация траффика, инновационный процесс

Для цитирования: *Заенчковский А.Э., Лазарев А.И., Синявский В.Ю.* Development of a secure neural traffic tunneling system with post-performance evaluation // Прикладная информатика. 2022. Т. 17. № 5. С. 88–101. DOI: 10.37791/2687-0649-2022-17-5-88-101