АНАЛИЗ ТЕХНОЛОГИИ WIREGUARD ДЛЯ РЕАЛИЗАЦИИ VPN

ANALYSIS OF WIREGUARD TECHNOLOGY FOR VPN IMPLEMENTATION

УДК 004.056.55: 621.391.7

РОСЛЯКОВ Александр Владимирович (доктор технических наук), **ЕФРЕМОВ** Даниил Алексеевич (студент)
(ПГУТИ)

В последние годы широкое распространение как в операторских мультисервисных сетях NGN, так и в инфокоммуникационной сети Интернет, получила технология виртуальных частных сетей VPN, которая позволяет безопасно передавать пакетные данные между заданными конечными пользователями.

Для реализации наложенных виртуальных сетей используется достаточно большой набор технологий и протоколов (PPTP, IPSec, L2TP+IPSec, SSTP, OpenVPN и др.), каждый из которых имеет свои особенности и области применения. Выбор оптимальной технологии в каждом конкретном случае является непростой многокритериальной задачей.

В статье проанализирована новая технология реализации VPN WireGuard, выявлены ее достоинства и недостатки и определены области возможного практического применения.

In recent years, the technology of virtual private networks VPN, which allows safe and high-quality transmission of packet data, has become widespread both in NGN operator multiservice networks and in the Internet infocommunication network.

To implement overlay virtual networks, a fairly large set of technologies and protocols is used (PPTP, IPSec, L2TP+IPSec, SSTP, OpenVPN, etc.), each of which has its own characteristics and applications. The choice of the optimal technology in each specific case is a difficult multi-criteria task.

The article analyzes a new VPN implementation technology — WireGuard, identifies its advantages and disadvantages, and identifies areas of possible practical application.

Ключевые слова: виртуальная частная сеть, технология WireGuard, одноранговая сеть, протокол UDP, криптографические протоколы, открытый/закрытый ключ.

Keywords: *virtual private network, WireGuard technology, peer-to-peer network, UDP protocol, cryptographic protocols, public/private key.*

Литература

1. Росляков А.В. Виртуальные частные сети: основы построения и применения. — М.: Эко-Трендз. 2006. 300 с.
2. WireGuard: fast, modern, secure VPN tunnel/ wireguard.com. [Электронный ресурс]. Дата обращения: 29.09.2022 г.
3. Abhilash T. Reliable user datagram protocol (RUDP)/ Kansas State University. Manhattan, Kansas. 2011. [Электронный ресурс]. Дата обращения: 29.09.2022 г.
4. Zhang X., Tsou T. IPsec Anti-Replay Algorithm without Bit Shifting/ IETF. January 2012. [Электронный ресурс]. Дата обращения: 29.09.2022 г.
5. Kent S., Atkinson R. Security Architecture for the Internet Protocol/ The Internet Society. November 1998. [Электронный ресурс]. Дата обращения: 29.09.2022 г.
6. Donenfild J.-A. WireGuard: Next Generation Kernel Network Tunnel/ wireguard.com. June 1, 2020. [Электронный ресурс]. Дата обращения: 29.09.2022 г.
7. WireGuard. Quick Start/ wireguard.com. [Электронный ресурс]. Дата обращения: 29.09.2022 г.
8. OpenVPN. How to Guide: Set Up & Configure OpenVPN Client/Server VPN/ openvpn.net. [Электронный ресурс]. Дата обращения: 29.09.2022 г.
9. Perrin T. The Noise Protocol Framework/ noiseprotocol.org. Rev. 34. 11.07.2018. [Электронный ресурс]. Дата обращения: 29.09.2022 г.