Deployment, management and comparative analysis of OpenVPN and L2TP Virtual Private Networks using MikroTik devices

Kehlibarova-Todorova D., Zhelyazkov Y. and Torlakov I.

***Abstract*—VPN is a technology that creates virtual network connectivity between a user and a remote resource such as a server or corporate network using the physical and software infrastructure of a larger public network most commonly the Internet. The purpose of this paper is to present an in-depth analysis of virtual private networks (VPNs) by examining the basic concepts of deployment and configuration, their advantages and disadvantages, and the specific characteristics of VPN technologies. Special attention will be paid to the OpenVPN and L2TP protocols, their features, applications and relevance in the modern digital world. A comparative analysis of their main characteristics will be carried out by implementing VPN connectivity using MikroTik RouterOS.**

***Keywords*— VPN, OpenVPN, L2TP, MikroTik, RouterOS**

I. Introduction

A virtual private network (VPN) provides a secure, encrypted connection over a less secure network, such as the Internet, allowing remote users to connect safely to a private network. The technology provides secure, encrypted communication, which is necessary when the user and the resource are located in different geographical locations [1]. The main applications of virtual private networks are as follows:

- Remote and secure access at work;
- Extended intranet networks – internal private networks of an organization, protected from access by unauthorized persons. They are used to store, share, and prioritize an organization's information;
- Extended extranet networks – private networks that use Internet protocols and networked computers. They use the public telecommunications system to securely share the organization's information and are aimed at users outside the company [2].

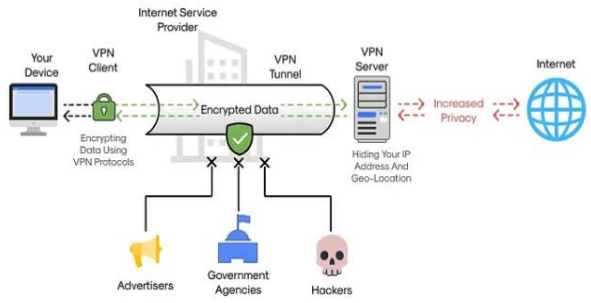

Fig. 1. Structure of VPN connectivity

A VPN is not just client-server communication - it includes many components such as tunnels, protocols, encryption, and authentication that provide security, stability, and functionality. Choosing the right components depends on the purpose of the VPN service - whether it is for business purposes, personal use, or corporate infrastructure connectivity.

The following main protocols are used to establish VPN communication: IPsec (Internet Protocol Security), OpenVPN, L2TP (Layer 2 Tunneling Protocol), L2F (Layer 2 Forwarding Protocol), PPTP (Point-to-Point Tunneling Protocol), WireGuard, SSTP (Secure Socket Tunneling Protocol), L2TP/IPsec, SoftEther VPN, IKEv2/IPsec (Internet Key Exchange version 2), SSL VPN (Secure Sockets Layer VPN), GRE (Generic Routing Encapsulation), MPLS VPN (Multiprotocol Label Switching VPN), Zero Trust Network Access (ZTNA) [1,3,4,5,7,8,9].

The advantages of using VPN connectivity are as follows: remote access, bypassing geographical restrictions, security and encryption, protection of public networks, network consolidation, traffic control, protection when using public Wi-Fi networks, and security when sharing files.

Despite the undeniable advantages of working with VPNs, they also have some disadvantages: increased network load, reduced performance, complexity of management, possible security issues with unreliable VPN providers, dependence on the Internet connection, and the need for maintenance and updates.

VPN is a powerful tool for accessibility, security, and anonymity, but choosing the right provider and protocol is crucial. Although it offers significant advantages, users should be aware of the potential drawbacks, especially those related to speed, reliability, and confidentiality.

MikroTik RouterOS [6], used for creating and managing VPN connectivity, is an operating system for routing and network administration developed by the Latvian company MikroTik. It offers a wide range of features for network management, routing, VPN, firewall protection, Quality of Service (QoS), network diagnostics, and much more. RouterOS is designed for use in both home and corporate networks and can be installed on various hardware platforms, including MikroTik RouterBOARD devices, which are specially optimized for this operating system. Configuring OpenVPN and L2TP VPN connectivity

OpenVPN is one of the most secure and commonly used protocols for creating VPN connections, using SSL/TLS encryption to protect data. This makes it particularly suitable for providing secure connectivity on public networks such as the Internet [10].

L2TP is a tunneling protocol that is often used in conjunction with IPSec to provide encryption and security. L2TP itself does not provide encryption, so it is combined

with IPSec to add a layer of protection [3,11,12].

Before proceeding with the actual implementation of virtual private networks (VPNs), it is necessary to perform a complete manual configuration of the network device used. This method provides flexibility, higher security, and avoids configuration errors that are common with automated factory settings. The settings are made through WinBox, avoiding the use of Quick Set [13].

The configuration of the MikroTik device prior to setting up the VPN includes: initial access and basic preparation, creation of an internal network via Bridge, manual configuration of IP addresses, verification of Internet connectivity, configuration of the internal network, configuration of the DHCP server, configuration of NAT and wireless network settings [14,15].

The configuration of OpenVPN and L2TP VPN connectivity goes through the following stages: setting up and configuring the OpenVPN and L2TP server on MikroTik, generating server and client certificates, activating the OpenVPN and L2TP server, setting up the PPP Profile for clients, adding client accounts, monitoring VPN connections, Split Tunneling [16].

II. Testing OpenVPN and L2TP VPN connectivity

The purpose of this study is to conduct a comparative analysis between the two commonly used VPN protocols – OpenVPN and L2TP, with a focus on the following aspects:

- Efficiency and speed of data transmission;
- Connection reliability;
- Traffic protection level.

The measurements include ping tests to key points in the network (Gateway, DNS, independent server) and an overall assessment of connection speed and stability.

The tests were conducted via Windows Terminal on a client computer connected via both types of VPN connections to a MikroTik router with a configured VPN server. Identical test scenarios were used for each protocol in order to achieve objectivity in the comparative analysis.

A. Testing OpenVPN connectivity

1) In the Windows terminal window, use the "tracert" command to check for network and Internet connectivity via VPN.

OpenVPN uses the SSL/TLS protocol, which guarantees a high level of encryption and security, but often leads to slightly higher latency due to the complexity of tunneling.

Once the terminal checks have been performed and we are sure that our Internet connection is going through the VPN, we first test the Gateway, but with OpenVPN it is visually hidden on the physical adapter (LAN card).

In fact, when testing with tracert in the terminal, the Gateway is visible in the first position (192.168.5.76).

2) Ping to Gateway - we perform the test to the Gateway, which is actually the remote router (MikroTik) on which the VPN server is located.

- IP: 192.168.5.76;
- Parameters: ping -t -l 1470;
- Objective: Conduct a load test to the router.

This results in an average response time of 23 ms, during which the request goes to the VPN server gateway and returns to the VPN client.

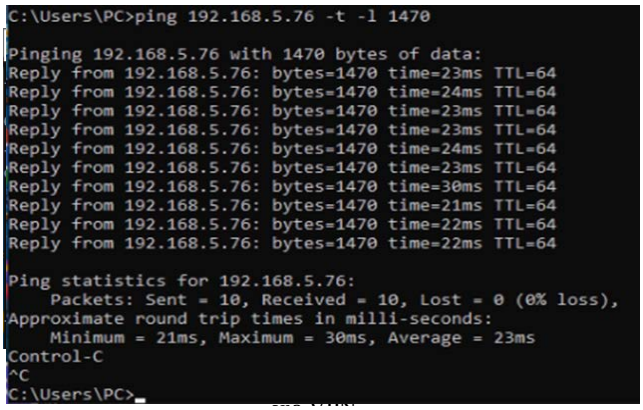

Fig. 3. Ping to the Gateway

3) Ping to DNS server – in this case, the DNS used is 8.8.8.8 (Google)

- Parameters: ping 8.8.8.8 -l 1400, 13 requests

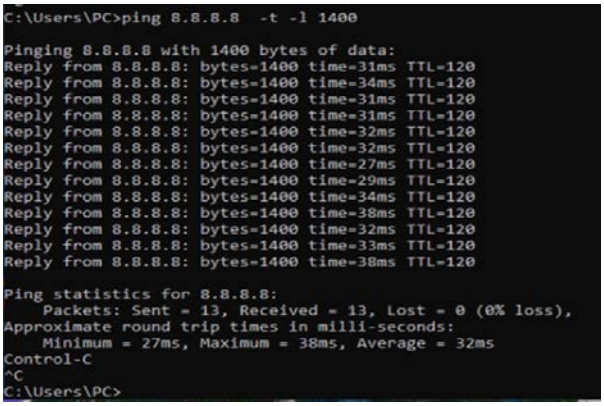

Fig. 4. Ping to DNS server (Google 8.8.8.8)

We send a Ping request with a load of 1400 packets and as a result we see an average response time of 32ms.

4) Ping to an external site

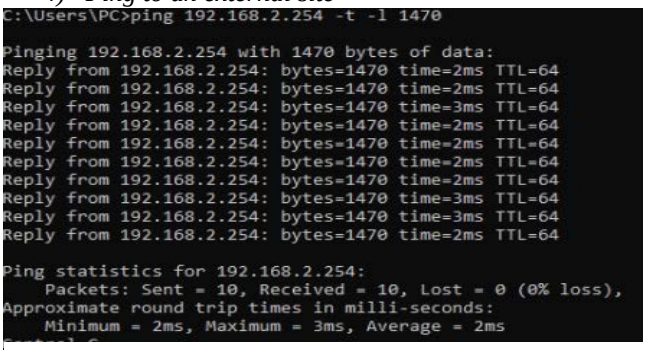

Fig. 9. Ping to Gateway

- Parameters: request ping nov.tu-sliven.com -l 10000

• Objective: Simulating heavy traffic to a site with lower network capacity

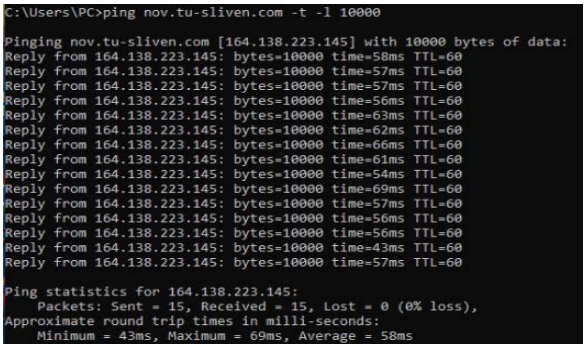

Fig. 5. Ping to an external site (nov.tu-sliven.com)

In this case, the site of TU-Sofia, EPF-Sliven, was selected. We performed a test with a buffer size of 10,000 bytes, and the results show that the average time for receiving the packets is 58 ms.

5) SpeedTest – the test was conducted with a major provider in Sofia (Neterra).

• A test was performed to the Neterra server.

Fig. 6. SpeedTest to provider (Neterra)

B. Testing L2TP connectivity

L2TP is a lighter protocol that is often used with IPSec for security. In this case, tests show that without specific encryption settings, the connection is much faster – at the expense of a lower level of protection.

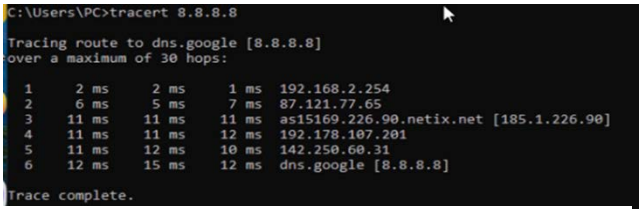

Fig. 7. Test for established connection and Internet access via VPN

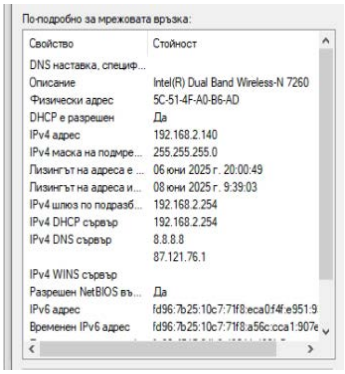

Fig. 8. Checking the Gateway via the client LAN card

1) Ping to Gateway 192.168.2.254

As a result, you get really low latency of 2ms, where the request goes to the VPN server's gateway and comes back to the VPN client.

2) Ping to DNS server – in this case, the DNS used is 8.8.8.8 (Google)

• Parameters: ping 8.8.8.8 -l 1400, 10 requests

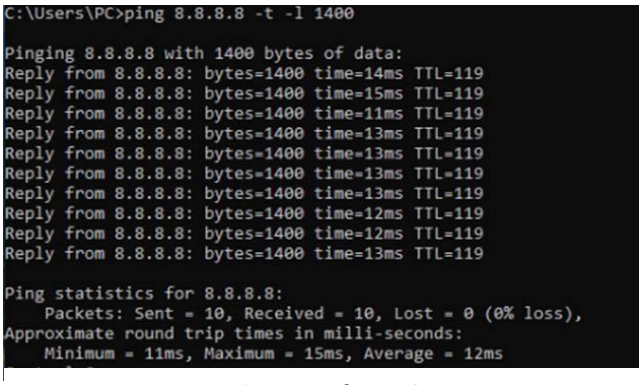

Fig. 10. Ping to the DNS server

This gives us an average latency of 12 ms.

3) Ping to an external site

• Parameters: nov.tu-sliven.com -l 10000

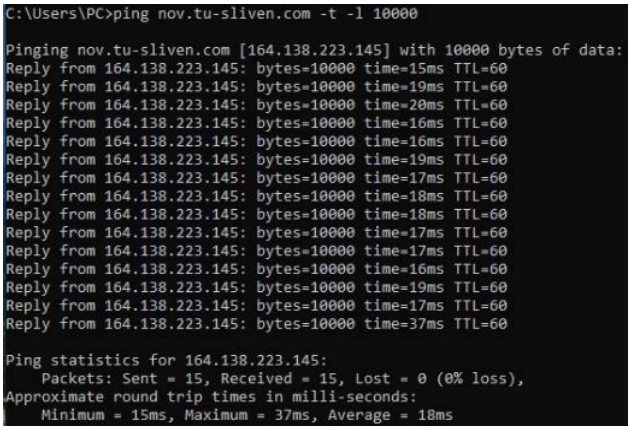

Fig. 11. Ping to an external website (nov.tu-sliven.com)

The test was again conducted at the EPF site in Sliven. The load during the test was with a size of 10,000 bytes, and the result was an average packet reception time of 18 ms.

4) SpeedTest – test to a major provider in Sofia (Neterra).

Fig. 12. SpeedTest to provider (Neterra)

L2TP passes through NAT and firewalls more easily, but in some networks it may be blocked if IPSec is not used.

III. STATISTICAL DATA OF OPENVPN AND L2TP VPN CONNECTIVITY

As a result of measurements of key metrics such as latency, connection stability, and security level, statistical analyses of OpenVPN and L2TP connectivity, two of the most popular VPN protocols, are presented through practical testing and performance measurement under actual communication and information exchange conditions.

TABLE I
SUMMARY OF ADVANTAGES BY METRICS

Metrics / Test	OpenVPN	L2TP	Advantage
Ping to Gateway	23 ms	2 ms	L2TP

Ping to DNS (8.8.8.8)	32 ms	12 ms	L2TP
Ping to site (EPF-Sliven)	58 ms	18 ms	L2TP
Gateway availability	Hidden	Visible	OpenVPN (for security)
SpeedTest	Good	Excellent	OpenVPN
Level of security	High (SSL/TLS)	Medium (depends on IPSec)	OpenVPN
Transmittance and response	Slower, stable	Faster, more sensible	Depends on the case

TABLE II
SUMMARY OF KEY ADVANTAGES

Criterion	Recommendation	Explanation
Quick action	L2TP	Significantly lower ping values, especially to Gateway and DNS.
Reliability	OpenVPN	It works stably, maintains more secure sessions, and hides the route.
Security	OpenVPN	It uses SSL/TLS encryption, which provides better data protection.
Use in a controlled network	L2TP	Suitable for local networks where security is not a priority.
Use in public/unknown networks	OpenVPN	Provides higher security and confidentiality.

TABLE III
SUMMARY OF ADVANTAGES IN TERMS OF APPLICATION

Scenario	Recommended protocol
High-speed connection in a secure LAN network	L2TP
Transfer of sensitive data	OpenVPN
Connecting to public Wi-Fi networks	OpenVPN
VPN for gaming or streaming	L2TP
VPN in a corporate network with high standards	OpenVPN

TABLE IV
SUMMARY OF ADVANTAGES IN TERMS OF PING TEST

Test	OpenVPN	L2TP
Ping to Gateway	23 ms	2 ms
Ping to DNS (8.8.8.8)	32 ms	12 ms
Ping EPF-Sliven (nov.tu-sliven.com)	58 ms	18 ms

IV. CONCLUSION

The results of the tests conducted show the following correlations:

• L2TP significantly outperforms OpenVPN in terms of speed and latency. In all ping tests - to the gateway, DNS server, and independent website - L2TP shows two to three times lower latency. These results clearly show that L2TP provides a faster connection, making it suitable for applications that require low latency;

• OpenVPN uses modern encryption methods based on SSL/TLS, hides routes, and provides a high level of security that is suitable for sensitive data and corporate use;

• L2TP, especially in combination with IPSec, offers a decent level of security, but it's vulnerable to certain attacks and is more often blocked by firewalls and NAT devices. In some cases, L2TP can be used without encryption, making it less suitable for critical situations where security is a priority.

• If speed is the main priority (e.g., for streaming, gaming, quick access to internal resources), L2TP is the better choice, provided that the network is protected in other ways.

• In cases of access via a public or risky network, as well as when transmitting sensitive information, OpenVPN remains the more reliable alternative.

Neither protocol is universally "better" - the choice depends on the specific goals and conditions of use. The balance between performance and security is the deciding factor when making a recommendation.

REFERENCES

[1] X. Tian, "A Survey On VPN Technologies: Concepts, Implementations, And Anti-Detection Strategies," International Journal of Engineering Development and Research, vol. 13, no. 1, pp. 85–96, Feb. 2025.

[2] M. T. Khan, J. DeBlasio, G. M. Voelker, A. C. Snoeren, C. Kanich, and N. Vallina-Rodriguez, "An Empirical Analysis of the Commercial VPN Ecosystem," in Proc. Internet Measurement Conf. (IMC), Boston, MA, USA, Oct. 2018, pp. 443–456

[3] Internet Engineering Task Force, "Security Architecture for the Internet Protocol," RFC 4301, Dec. 2005

[4] Internet Engineering Task Force, "Layer Two Tunneling Protocol 'L2TP'," RFC 2661, Nov. 1999

[5] B. Lipp, B. Blanchet, and K. Bhargavan, "A Mechanised Cryptographic Proof of the WireGuard Virtual Private Network Protocol," in Proc. IEEE European Symposium on Security and Privacy, Stockholm, Sweden, Jun. 17–19, 2019.

[6] MikroTik, "RouterOS," RouterOS Online Documentation, MikroTik, Riga, Latvia. Updated Jun. 26, 2025.

[7] MikroTik, "OpenVPN," RouterOS Virtual Private Networks, Artūrs C. Last updated Jul. 22, 2025.

[8] MikroTik, "L2TP," RouterOS Virtual Private Networks, Artūrs C. Last updated Dec. 16, 2024

[9] Gartner, "Market Guide for Zero Trust Network Access," Gartner, Stamford, CT, USA, Feb. 17, 2022.

[10] M. J. Hall, "Performance Analysis of OpenVPN on a Consumer Grade Router," arXiv:2504.19069, Apr. 2025

[11] D. A. P. Silva et al., "A VPN Performances Analysis of Constrained Hardware Open Source Solutions," Future Internet, vol. 14, no. 9, 2022, doi:10.3390/fi14090264

[12] Internet Eng. Task Force, "Securing L2TP using IPsec," RFC 3193, Nov. 2001.

[13] C. Formica, "Analysis and Characterization of the VPN Configuration Problem," M.Sc. thesis, Politecnico di Torino, Italy, 2023

[14] X. Tian, "A Survey On VPN Technologies: Concepts, Implementations, And Anti-Detection Strategies," Int. J. Eng. Dev. Res., vol. 13, no. 1, pp. 85–96, Feb. 2025

[15] IEEE, "IEEE Std. 802.11-2016: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 2016.

[16] W. Lin, "Tunneling and VPN," in Trends in Data Protection and Encryption Technologies, V. Mulder et al., Eds., Cham, Switzerland: Springer, 2023, ch. 26, pp. 441–466, doi:10.1007/978-3-031-33386-6_26.