Infortech, Vol. 8, No. 1, June 2026, E-ISSN: 2715-8160, Page. 35-40
Published: LPPM Universitas Bina Sarana Informatika

JURNAL INFORTECH

website: http://jurnal.bsi.ac.id/index.php/infortech/

Implementation of Local Network Access Restriction security on L2TP VPN with Firewall Filter Method

Tommi Alfian Armawan Sandi[1], Firmansyah[2], Eka Kusuma Pratama[3],Rian Septian Anwar[4]

[1,2,3]Informatika, Fakultas Teknik dan Informatika, Universitas Bina Sarana Informatika, Jakarta
[4]Teknik Elektro, Fakultas Teknik dan Informatika, Universitas Bina Sarana Informatika, Jakarta

ARTICLE INFORMATION

Artikel History:
Received: 05-05-2026
Revised: 08-05-2026
Accepted: 15-06-2026
Available Online: 22-06-2026

Keyword:

VPN
Inteconnection
Mobile Network
Firewall Strategy
Network Security

ABSTRACT

The use of L2TP/IPSec-based Virtual Private Networks (VPNs) has become a common solution for providing remote access to local networks. However, VPN implementations without adequate access restrictions can potentially pose security risks, such as unauthorized access to internal resources, including shared directories on servers. This study aims to implement and analyze a local network access restriction strategy using a firewall filter with an accept-few-drop-any approach on an L2TP VPN network. The research method used is an experiment with the PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) model approach. Testing was conducted in two scenarios: before and after the firewall filter implementation. The parameters analyzed included security aspects (access to shared directories) and network performance (latency, throughput, and packet loss). The results showed that before the firewall filter implementation, VPN users could access shared directories without restrictions. After the whitelisting strategy was implemented, access to file sharing services was effectively blocked, while other network services continued to run normally. In terms of performance, the firewall filter implementation did not have a significant impact on network performance.

Corresponding Author:

Tommi Alfian Armawan Sandi,
Informatika,
Universitas Bina Sarana Informatika, Jakarta,
Email: tommi.taf@bsi.ac.id

INTRODUCTION

Reliability in supporting mobile device connectivity has become an essential requirement in modern office environments, where network accessibility from anywhere is increasingly needed to support daily operational activities. One of the most widely adopted technologies for connecting local networks with remote users is the implementation of a Virtual Private Network (VPN) (Fauzan Prasetyo Eka Putra, Yogi Setiawan, Samsul Arifin, & Wahyu Hidayatullah, 2025). VPN technology provides secure communication through encrypted tunnels, making it a preferred solution for remote access implementation (Gunawan & Wardhana, 2023) (Budiyanto & Gunawan, 2023) . Among various VPN protocols, Layer 2 Tunneling Protocol (L2TP) is widely utilized due to its stable interconnection capabilities and compatibility across multiple operating systems such as Windows, Linux, macOS, and Android (Tymoshchuk & Karnaukhov, 2024) (Nugroho & Sutanto, 2025)

Despite the advantages offered by VPN technology, its implementation also introduces significant security challenges. VPN tunnels not only facilitate remote access and data exchange within private networks (Tomi Defisa, Thomas Budiman, & Sianipar, 2025) (Fassl, Ponticello, Dabrowski, & Krombholz, 2023), but also increase the risk of unauthorized access to internal resources. In many cases, users connected through VPN services are automatically granted broad access to internal network resources, including shared directories and file servers, without sufficient access restrictions. This condition may lead to data leakage, unauthorized access, and lateral movement attacks within the internal network (Abbas et al., 2023) (Khantamonthon, Patpituck, &

DOI: https://doi.org/10.31294/infortech.v8i1.

Chimmanee, 2025). Furthermore, Rytilahti & Holz (2024) explained that improperly secured VPN infrastructures can unintentionally expose internal organizational networks and other connected clients to security threats.

Several previous studies have focused primarily on strengthening VPN security through encryption mechanisms and protection against packet sniffing attacks. These studies demonstrated that VPN tunneling can secure communication channels and reduce the risk of data interception during transmission. However, most existing research emphasizes protection at the communication layer and authentication process, while limited attention has been given to internal access control after users successfully connect to the VPN network. As a result, authenticated users may still access sensitive internal services without granular restrictions. This limitation indicates a research gap in implementing fine-grained network access control mechanisms specifically for VPN-connected users.

In practice, firewall filtering mechanisms are commonly implemented to protect network perimeters based on IP addresses, ports, and protocols (Putra, Dafid, & Syafi'i, 2025) (Bodipudi, 2024). Nevertheless, existing implementations generally focus on filtering external traffic and have not been optimally utilized to restrict internal VPN user access to specific local network resources (Christanto, Cholillah, & Hirzan, 2025). Consequently, organizations still face difficulties in limiting access to confidential services such as Server Message Block (SMB)-based directory sharing while maintaining normal network communication for legitimate users.

To address this issue, this study proposes the implementation of a firewall filter strategy using a whitelist-based approach, namely accept few, drop any. This strategy allows only predefined traffic while rejecting all other unauthorized access by default. Compared to blacklist approaches, whitelist mechanisms are considered more secure because network access is denied unless explicitly permitted (Alfian, Purwaningsih, & Wicaksono, 2024) (Bechtel, Müller, Menth, & Heer, 2025). Through this approach, access to sensitive internal services such as shared directories can be effectively restricted without significantly affecting other permitted network services.

Therefore, this research aims to analyze the implementation of firewall filter rules on an L2TP VPN network to limit local resource access, particularly shared directories on file servers. In addition, this study evaluates the effectiveness of the accept few, drop any strategy from both security and network performance perspectives. The results of this research are expected to contribute to the development of a more secure and efficient VPN access control model for organizational network environments.

RESEARCH METHOD

This research uses an experimental research method using a network engineering approach. The experiment was conducted to test the effectiveness of implementing a firewall filter on an L2TP VPN network that would restrict access to local file sharing servers, particularly SMB on the server. The approach model used in this research refers to the PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) (Octaviyana & Soewito, 2023) network cycle model, which is commonly used in designing and managing network infrastructure. As shown in the figure 1,

Figure 1. Research Stage PPDIOO

The stages in the PPDIOO model are as follows:

1. Preparation Stage: In conducting this research, the author identified the needs and problems that formed the basis of the research, including a literature review on L2TP/IPSec VPN, firewall filtering, and access control in networks.
2. Planning Stage: The author conducted technical planning for the network to be implemented, including determining the devices to be used, determining test parameters, and developing test scenarios.
3. Design Stage: This stage includes the design, including the topology and firewall policies.
4. Implementation Stage: The author implemented the network design, using virtualization/simulation to achieve desired results.
5. Operate Stage (Testing and Operation): The author tested the implemented network using scenarios, both without and with a firewall filter. Therefore, the parameters tested for security included server directory access status (success/failure) and latency (ping) performance.
6. Optimize Stage: The author analyzed and evaluated the test results, including comparing results before and after firewall

implementation and evaluating the impact on network performance.

Data collected in this study included direct observation of network access and configuration results, network testing, and documentation of test results and router configurations..

RESULTS AND DISCUSSION

Based on the PPDIOO method, preparation is the first step before continuing research. Therefore, preparation begins with a preliminary analysis of both the observed research objects and the documentation of log activity. For the research objects, the author observed traffic activity through the L2TP VPN and copied the IP addresses used for both clients and network devices, as shown in Table 1.

Table 1. Addressing Table

Device	Initial	Int	IP	Gateway
Router	Core-Router-A	Eth1	182.xxx.xxx.x10	
		Eth2	10.168.68.254/30	
		Eth3	30.30.30.1/25	
		Eth4	40.40.40.1/24	
NAS Server 1	Server1	Gig0/1	10.168.68.24	10.168.68.254
NAS Server 2	Server2	Fa0/1	30.30.30.249	30.30.30.1

The following topology is simulated to support research needs and this stage enters the topology design stage.

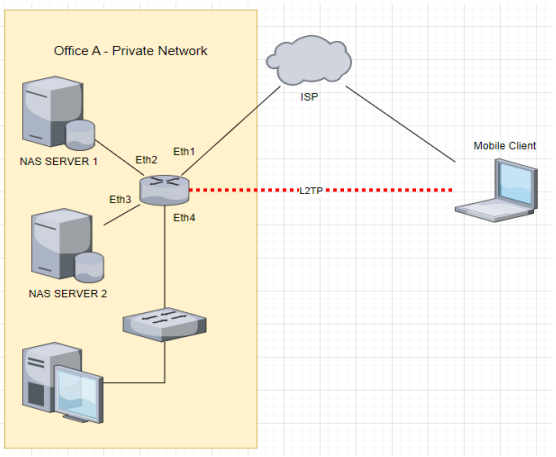

Figure 2. Topology Design

In the topology, it is concluded that the gateway router will be the gateway between the public network and the private network, with the ether 1 interface going to the ISP, Ether 2 going to NAS Server 1, Ether 3 going to NAS Server 2 and Ether 4 as the local network provider, for the interconnection that is formed, the gateway router will provide a public IP as the destination for mobile users and in the configuration that is formed, authentication in the form of IPSec and Encryption is also included. The devices used in the simulation include: Mikrotik RB1100 Hx router with 12 interfaces, NAS server with the code RackStation RS1221RP+, for mobile users using laptops and mobile hotspot connections.

1. L2TP Server Implementation

The implementation steps are applied to the Gateway and Client Routers. On the L2TP router, go to the PPP → L2TP Server menu, as shown in Figure 3. Enable L2TP Server. In this configuration, to enable L2TP Server tunneling, click Enable. Select the protocol used, then select the default profile = default-encryption. For double security protection, ensure Use IPSec = yes, and then create an IPsec Secret.

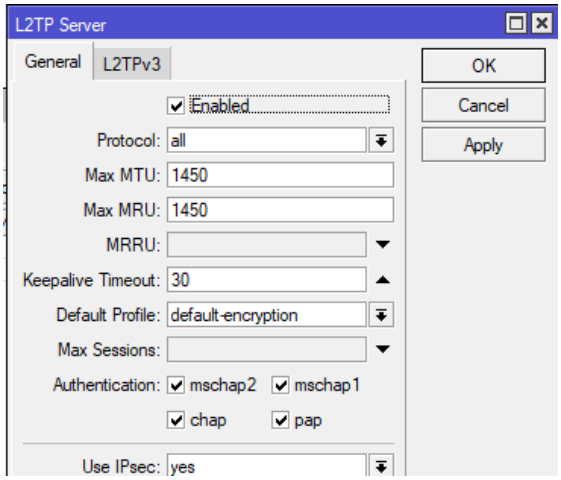

Figure 3. L2TP Server Setup

Next, create an L2TP account for the client in the Secret Tab, as shown in Figure 4, the PPP Secret Window, the most important part in creating a Secret is the username and password, service selection, profile = default-encryption, Local Address is used as the IP of the L2TP interface on the Server side, while the Remote Address will be used as the L2TP interface IP on the Client side.

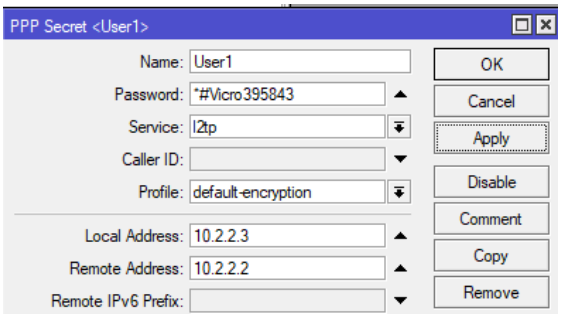

Figure 4. Create New User L2TP

2. Client Implementation

After creating the L2TP server, the next step is to implement it on the client, where the client uses a Windows operating system. The configuration is found in VPN Settings. The parameters to be configured include: Connection Name = ServerCore, Server name or address = Public IP of the ISP Server, VPN Type = L2TP/IPsec with pre-shared key, Pre-shared key = Secret IPsec, and then enter the username and password created on the server. Once completed, the user interface will appear as shown in Figure 5. VPN Client

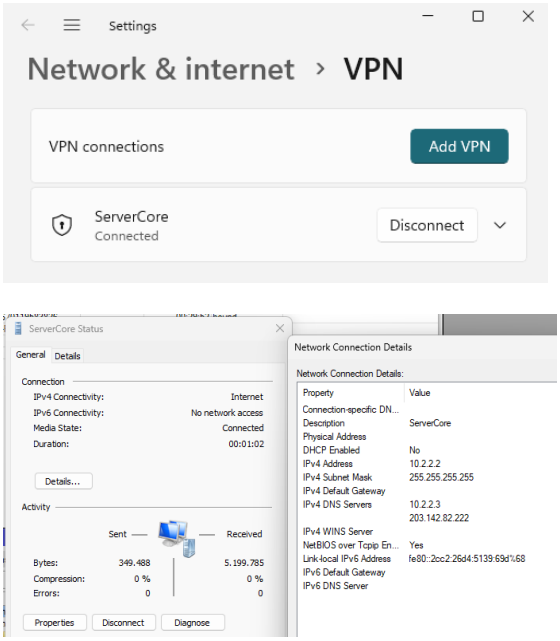

Figure 5. Connection VPN Client (Successful)

3. Connectivity Test

In this stage, the connectivity test is performed to verify that the main server network and the client on the different network are receiving VPN service by pinging the server on the network, as shown in Figure 6.

```
C:\Users\tomtom notebook>ping 30.30.30.249

Pinging 30.30.30.249 with 32 bytes of data:
Reply from 30.30.30.249: bytes=32 time=43ms TTL=127
Reply from 30.30.30.249: bytes=32 time=29ms TTL=127
Reply from 30.30.30.249: bytes=32 time=28ms TTL=127
Reply from 30.30.30.249: bytes=32 time=72ms TTL=127

Ping statistics for 30.30.30.249:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 28ms, Maximum = 72ms, Average = 43ms
```

Figure 6. Ping to Server (Reply)

Then Test the Connection using Network Credentials and SMB, as shown in Figure 7,8.

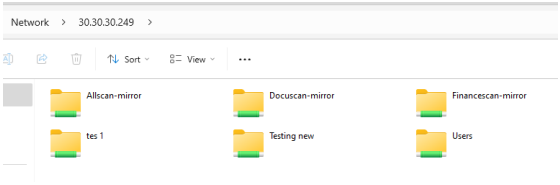

Figure 7. SMB Server

```
C:\Users\tomtom notebook>net use
New connections will be remembered.

Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           A:        \\30.30.30.249\Testing new
                                                 Microsoft Windows Network
OK                     \\30.30.30.249\tes 1      Microsoft Windows Network
OK                     \\30.30.30.249\IPC$       Microsoft Windows Network
The command completed successfully.
```

Figure 8. Show Credential Network Status (OK)

And also on the main Router side there is an Active Connections Tab, in Figure 9 it shows user 1 in an active state with Client IP 27.124.95.181 with L2TP interface IP 10.2.2.2.

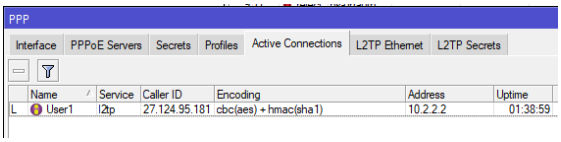

Figure 9. User VPN Status (Active)

4. Implementing a Firewall Filter Strategy

When implementing L2TP, connecting to a private network makes the internal network visible to users. In this case, not all mobile clients have permission to access directories or other services. Therefore, the author implemented a security strategy with "Accept few, drop any." In the implementation, the author will create a scenario where user 1 with the IP address 10.2.2.2 is allowed to access NAS Server 1 with the IP address 30.30.30.249. However, they are not allowed to access NAS Server 2 with the IP address 10.168.68.24. Therefore, there will be three firewall rules in the Filter Rule, configured as shown in Table 2.

Table 2. Firewall Strategy

#	Chain	Scr-Address	Dst-Address	Action	Strategy
1	Forward	10.2.2.2	30.30.30.249	Accept	Accept Few
2	Forward		30.30.30.249	Drop	Drop Any
3	Forward	10.2.2.2	10.168.68.24	Drop	Drop Few

After configuring the firewall filter, 3 rules will be formed as shown in Figure 10, where each strategy has been determined according to Table 2.

	;;; Accept Few NAS 2				
17		acc...	forward	10.2.2.2	30.30.30.249
	;;; Drop Any NAS 2				
18		drop	forward		30.30.30.249
	;;; Drop Few NAS 1				
19		drop	forward	10.2.2.2	10.168.68.24

Figure 10. Firewall Filter Rule

5. Testing Scenario 1

Scenario 1 testing involved uploading and downloading, sharing files from the server to the mobile client without firewall filter rules. The packet loss delay test results were also analyzed. Furthermore, the parameters used were the net use command on the client user, allowing them to view the status of the computer's connection or disconnection from the shared resource (Microsoft, 2016), as shown in Figure 11.

```
C:\Users\tomtom notebook>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK                     \\10.168.68.24\IPC$       Microsoft Windows Network
OK                     \\30.30.30.249\IPC$       Microsoft Windows Network
The command completed successfully.
```

Figure 11. Status OK both connection server

6. Testing Scenario 2

Testing with scenario 2 by carrying out upload and download activities, sharing files from the server to the mobile client with a firewall filter rule, from the results of the packet loss delay test it can be concluded that the NAS Server 2 connection that was formed was disconnected so that the user could not re-access the server directory that had previously been opened, as evidenced in Figure 12, the IP to NAS Server 2 10.168.68.24 has a disconnected status.

```
C:\Users\tomtom notebook>net use
New connections will be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
Disconnected           \\10.168.68.24\IPC$       Microsoft Windows Network
OK                     \\30.30.30.249\IPC$       Microsoft Windows Network
The command completed successfully.
```

Figure 12. Status Disconnected for NAS Server 2

CONCLUSION

Based on the experimental results conducted using the PPDIOO approach, the implementation of firewall filter rules on the L2TP VPN network using the accept few, drop any strategy significantly improved internal network access control. The proposed whitelist-based filtering mechanism successfully restricted unauthorized access to SMB-based shared directories while still allowing permitted network services to operate normally.

The testing results demonstrated that, prior to firewall implementation, VPN users had unrestricted access to internal file-sharing services after successful authentication. This condition indicated that the VPN authentication process alone was insufficient to protect sensitive local network resources. After applying the firewall filtering rules, access attempts to shared directories were consistently blocked according to the predefined policies, thereby reducing the possibility of unauthorized access and limiting potential lateral movement within the network environment.

From the network performance perspective, the implementation of firewall filtering showed minimal impact on overall network quality. Latency, throughput, and packet loss remained within stable operational ranges during testing, indicating that the security enhancement did not significantly degrade communication performance across the VPN infrastructure. These findings confirm that granular firewall filtering can be integrated into L2TP VPN environments without sacrificing service reliability.

The main contribution and novelty of this research lie in the application of a whitelist-based firewall filtering strategy specifically designed for post-authentication access control within L2TP VPN networks. Previous studies mainly focused on VPN encryption mechanisms and protection against external attacks, whereas this study emphasizes internal access restriction after VPN connectivity has been established. By combining VPN tunneling with selective firewall filtering, this research provides a practical and lightweight security model for controlling user access to sensitive local network resources.

Overall, the results indicate that the accept few, drop any strategy is an effective approach for strengthening VPN network security, particularly in protecting shared directory services from unauthorized access while maintaining acceptable network performance.

REFERENCES

Abbas, H., Emmanuel, N., Amjad, M. F., Yaqoob, T., Atiquzzaman, M., Iqbal, Z., … Ashfaq, U. (2023). Security Assessment and Evaluation of VPNs: A Comprehensive Survey. *ACM Computing Surveys*, *55*(13s). https://doi.org/10.1145/3579162

Alfian, A., Purwaningsih, M., & Wicaksono, F. D. N. (2024). Pencegahan Kerentanan Keamanan Jaringan Komputer Mikrotik Menggunakan Metode Penetration Testing. *Jurnal Ilmiah FIFO*, *16*(2), 121. https://doi.org/10.22441/fifo.2024.v16i2.003

Bechtel, L., Müller, S., Menth, M., & Heer, T. (2025). Transforming the Network into a Filter: Distributed Firewall Rules for Time-Critical Traffic. *2025 IEEE 21st International Conference on Factory Communication Systems (WFCS)*, 1–8. IEEE. https://doi.org/10.1109/WFCS63373.2025.11077639

Bodipudi, A. (2024). Effective Firewall Review And Network Optimization by Data-Driven & Holistic approach. *Journal of Technological Innovations*, *5*(2). https://doi.org/10.93153/fh18nv35

Budiyanto, S., & Gunawan, D. (2023). Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol. *IEEE Access*, *11*, 60853–60865. https://doi.org/10.1109/ACCESS.2023.3286032

Christanto, F. W., Cholillah, P., & Hirzan, A. M. (2025). Optimizing Mikrotik-Based Network Security using Address List, Firewall Filter Rules, and Raw Firewall. *Revista de Informatica Teorica e Aplicada*, *32*(3), 66–76. https://doi.org/10.22456/2175-2745.142954

Fassl, M., Ponticello, A., Dabrowski, A., & Krombholz, K. (2023). Investigating Security Folklore: A Case Study on the Tor over VPN Phenomenon. *Proceedings of the ACM on Human-Computer Interaction*, *7*(CSCW2). https://doi.org/10.1145/3610193

Gunawan, M. A., & Wardhana, S. (2023). Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN (Virtual Private Network). *RESISTOR (Elektronika Kendali Telekomunikasi Tenaga Listrik Komputer)*, *6*(1), 69. https://doi.org/10.24853/resistor.6.1.69-78

Khantamonthon, N., Patpituck, P., & Chimmanee, K. (2025). Guidelines for Organizations on Protecting Against Cyber Threats through the use of Virtual Private Networks (VPN). *2025 9th International Conference on Information Technology (InCIT)*, 215–221. IEEE. https://doi.org/10.1109/InCIT66780.2025.11276011

Nugroho, H. D., & Sutanto, Y. (2025). Implementasi Keamanan Data Pada Jaringan Router MikroTik Menggunakan VPN L2TP Dan IPSec. *Journal of Electrical, Electronic …*, *4*(1). https://doi.org/https://doi.org/10.58991/at4tdq03

Octaviyana, R. A., & Soewito, B. (2023). Perancangan Ulang Topologi Jaringan Dengan Kerangka Kerja Ppdioo. *Jurnal Ilmiah Sistem Informasi*, *13(1)*(1), 34–41. Retrieved from https://doi.org/10.26594/teknologi.v13i1.3624

Putra, F. P. E., Dafid, M., & Syafi'i, I. (2025). Firewall Implementation as a Computer Network Security Strategy for Data Protection. *Brilliance: Research of Artificial Intelligence*, *5*(1), 291–297. https://doi.org/10.47709/brilliance.v5i1.6162

Tomi Defisa, Thomas Budiman, & Sianipar, A. Z. (2025). Model of Sharing Public IP Address Using Tunneling Protocol. *Journal of Advances in Information and Industrial Technology*, *7*(1), 95–104. https://doi.org/10.52435/jaiit.v7i1.691

Tymoshchuk, V., & Karnaukhov, A. (2024). *Using Vpn Technology To Create Secure Corporate Networks*. 166–170. https://doi.org/10.36074/logos-21.06.2024.034