



Mikrotik VPN Shielding E-Link Health Reports: Strengthening Data Security at Madiun Health Office

Bintang Agung Gumelar¹, Guruh Darma Setiya Putra², Dwi Nor Amadi³

^{1,2,3}Manajemen Informatika, Universitas Merdeka Madiun, Madiun, Indonesia
Email: ¹bintangagunggumelar@gmail.com, ²putrarasta21@gmail.com, ³dwinor@unmer-madiun.ac.id

Abstract

Advances in Information and Communication Technology have led to revolutionary changes in computer networking, especially in Indonesia, which has witnessed significant technological growth over the last four years. Despite this progress, inter-agency data exchange, particularly in governmental organizations, remains vulnerable to security risks. This study focuses on enhancing the security measures for the Electronic Health Information Report (E-Link) system at Madiun District Health Office by implementing a Virtual Private Network (VPN) using MikroTik. A multi-method approach, comprising direct observation, interviews, and literature review, was adopted for this investigation. The findings confirm that the utilization of Point-to-Point Tunneling Protocol (PPTP) via MikroTik substantially elevates the security and governs controlled access to the E-Link application. Therefore, the implementation of a VPN not only fortifies the security but also improves the accessibility of health data systems.

Keywords: VPN, Virtual Private Network, Network Security

1. INTRODUCTION

In the modern era, the unprecedented growth of Information and Communication Technology (ICT) has fundamentally reshaped computer networking landscapes. Indonesia stands as a case in point, demonstrating marked improvements across key metrics in technology, information, and communication [1]. Given that computer networks are now an indispensable medium for government agencies to exchange information, the demand for efficient, secure, and reliable data transmission has never been higher.

At the core of this issue is the Madiun District Health Office, which operates a web-based application to manage clinical health information reports. However, this digital convenience is not without risk. Web-based platforms are prime targets for various cyber-attacks, including but not limited to SQL Injection, Phishing,



and Cross-Site Scripting (XSS) [2]. One viable countermeasure to bolster cybersecurity is the deployment of Virtual Private Networks (VPNs) over public or internet frameworks.

A VPN is a specialized technology designed to create an isolated, secure network within the confines of a broader public network [3]. Its main advantage lies in its exclusivity: unauthorized parties cannot access the internal Application Server. Moreover, organizations can monitor VPN activities, enhancing data confidentiality and integrity. VPNs use encryption and tunneling protocols to facilitate secure data exchanges over a public telecommunication infrastructure [4]. The distinguishing factor of a VPN is not its network topology but the security mechanisms and procedures that permit specific user access [5].

This segues into the role of MikroTik RouterOS, a product by a renowned router manufacturer known for its reliability [6]. MikroTik offers robust VPN solutions, employing advanced tunneling, authentication, and encryption algorithms to create secure virtual transmission channels over public networks. The VPN options available are diverse, including OpenVPN, PPTP, L2TP, and IPSec, among others. The latter three are commonly preferred for their ease of integration into existing network infrastructures [7]. MikroTik routers are also lauded for their versatility, frequent updates, user-friendly interfaces, multiple access and control options, simple installation procedures, and an extensive range of features [8].

In this investigative milieu, we successfully developed and implemented VPN solutions within an organizational context to improve the efficacy and security of frequent data exchanges, primarily using MikroTik devices. Therefore, a comprehensive evaluation of IT governance is paramount to quantify the impact of these technological implementations in fulfilling organizational objectives [9].

The aim of this study is to evaluate the effectiveness of deploying MikroTik RouterOS-based VPN solutions in enhancing cybersecurity measures for the Madiun District Health Office's web-based application. Specifically, the study seeks to assess how these VPN technologies impact data transmission speed, reliability, and security, while also examining the return on investment (ROI) and alignment with organizational objectives. By conducting a multi-faceted analysis, this research aspires to provide actionable insights for government agencies to make informed decisions about network security solutions."

2. METHODS

This research procedure consists of five stages, as illustrated in Figure 1.

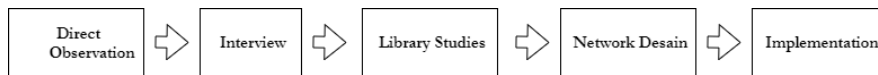


Figure 1. Research Procedures

The details procedures based on Fiture 1 as follow.

1. Observation and Interviews, Direct observation was conducted at the Health Office of Madiun District to understand the existing network infrastructure, its implementation, and current operations. Interviews were also worked with the IT team of the Health Office to gather detailed information about network configurations and security issues. The validity of research data was ensured through triangulation, a method of comparing data from observation, interviews, and documents to arrive at consistent conclusions. No additional data outside the scope of this research was utilized [10].
2. Literature Review, A comprehensive review of relevant literature was undertaken to explore previous research related to Virtual Private Networks (VPNs) and network security.
3. Network Development and Design, The initial network architecture at the Health Office of Madiun District relied on direct access to the E-Link server using a public IP address, which posed significant security risks. A site-to-site VPN using Point-to-Point Tunneling Protocol (PPTP) was proposed to enhance network security. Site-to-site VPNs are known to offer better service quality compared to networks without VPNs. This approach facilitated the protection of centralized data on the server.

3. RESULTS AND DISCUSSION

3.1 Network Development

The current network scheme at the Health Office of Madiun District directly utilizes a public IP to access the E-Link server. When a device has a public IP and is connected to the internet, that device can be accessed from anywhere via the internet [11]. This poses a significant and dangerous risk, as anyone can enter and access the E-Link server without any monitoring or detection from the IT team at the Health Office. It's crucial to develop a more secure network structure to enhance network security. One effective solution is implementing a Virtual Private Network (VPN) as a better security measure for the E-Link server. Only individuals with specific access or login credentials can connect to and access the E-Link server by using a VPN. Additionally, these activities can be monitored and tracked using MikroTik devices, enabling the IT team to see who is connected to or accessing the E-Link server.

3.1.1 Network Design

In the network design phase, the author proposes the development of a network with the implementation of a site-to-site VPN using the PPTP protocol. Networks that implement site-to-site VPN have better service quality than networks without VPN [12]. Computer network systems facilitate protecting centralized data on the server [13]. Using the site-to-site VPN method, not everyone can access the Madiun District Health Office server. Only authorized devices with the appropriate address, user credentials (username and password), and valid VPN connection can enter and access the server as if it were part of the local area network from the server.

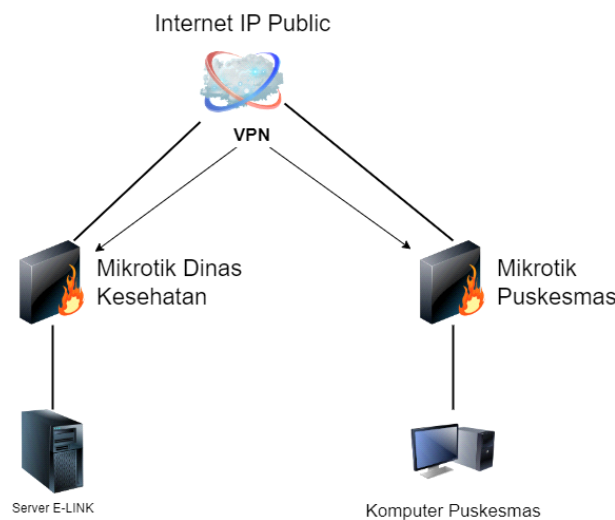


Figure 2. Proposed VPN Topology Diagram

The diagram shows better security than the direct use of the Public IP address to access the server.

3.1.2 Implementation

A. Setting up MikroTik at the Madiun District Health Office

VPN Server Configuration, log in to the Winbox application and click on the PPP menu to open the PPP window. Next, select PPTP Server, check the Enable box, and click OK. You have activated the PPTP VPN Server feature in MikroTik by doing this.

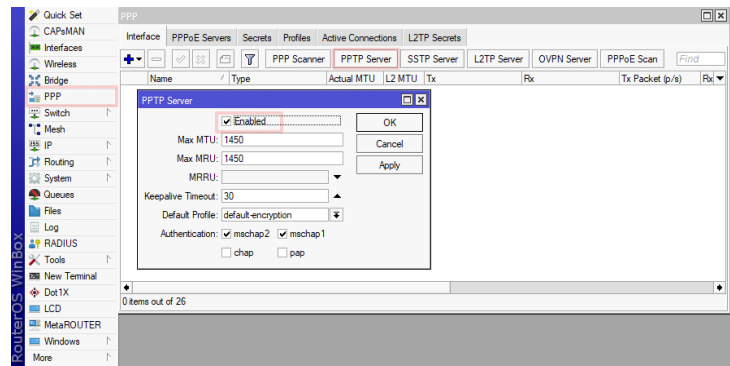


Figure 3. VPN Server Configuration

VPN Secret Configuration, Still, in the PPP menu, select Secret, then click the add button to create a new PPP Secret. Continue by filling in the following details:

- Name: Enter the desired Username for PPTP VPN.
- Password: Set the Password for PPTP VPN as desired.
- Service: Choose the service to be used; you can select PPTP or choose any.
- Local Address: Enter the IP address to be used by the PPTP VPN Server.
- Remote Address: Enter the IP address to be used by the PPTP VPN Client. Then click OK.

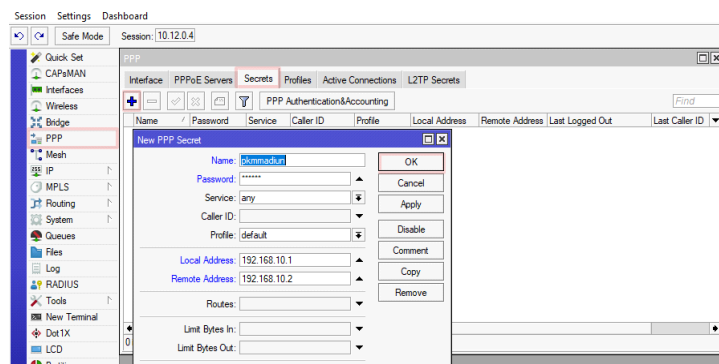


Figure 4. VPN Secret Configuration

B. Setting Up Mikrotik at the Puskesmas.

Configuring Dial Out PPTP, click on the PPP menu, and a PPP window will appear. Click the add (+) icon and select PPP Client. A New Interface window will appear then choose Dial Out and fill in the following details:

- Connect To: Fill in with the Public IP Address.
- Name: Enter the Username for the PPTP VPN as desired.

- c) Password: Enter the Password for the PPTP VPN as desired.
- d) Then click OK.

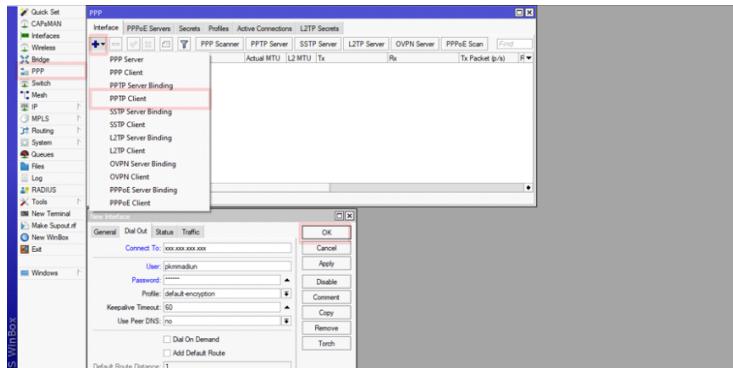


Figure 5. MikroTik Puskesmas Dial Out Configuration

Routing Configuration, Click on the IP menu and then select Route. A Route List window will appear. Click the add (+) icon, and a Route window will appear. Fill in the Dst Address with the Server IP and fill in the Gateway with the IP Gateway from the VPN Server's Gateway IP. Then click OK.

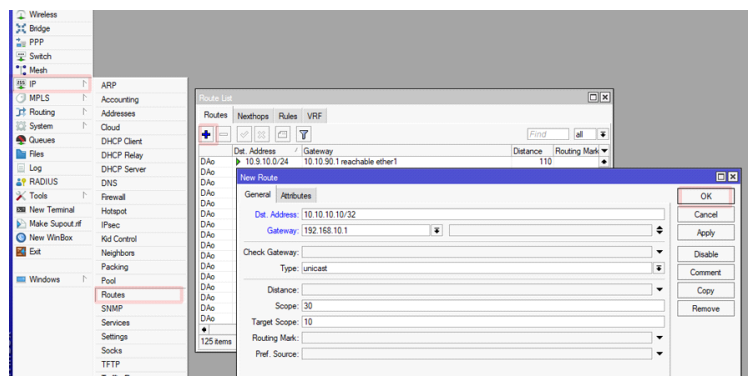


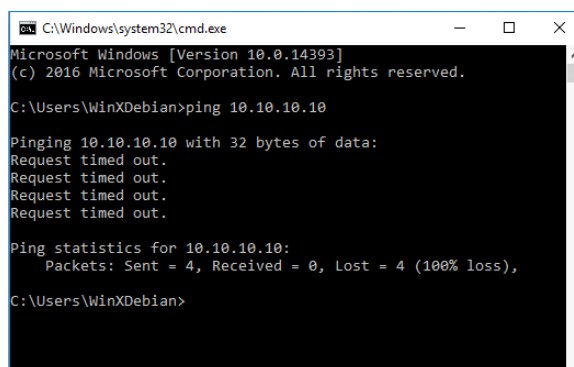
Figure 6. Static Routing Configuration for Local E-Link Server IP

3.2 Test Results

The testing was conducted to determine whether the created VPN network functions effectively. In network testing, two stages are carried out to ensure optimal outcomes, particularly in VPN technology design: Initial Network Testing and Final Network Testing [10].

3.2.1 Initial Network Testing

In this stage, testing is performed by pinging the local IP address of the E-Link server (10.10.10.10) from the Puskesmas, the technical implementation unit of the District Health Office of Madiun Regency. Before the implementation of the VPN configuration, Puskesmas could not establish a connection to the local IP address of the E-Link server. Figure 7 displays the testing results using the 'ping' command to the local IP address of the E-Link server. In this initial phase, the Puskesmas cannot connect to the local IP address of the E-Link server due to the absence of a VPN configuration.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\WinXDebian>ping 10.10.10.10

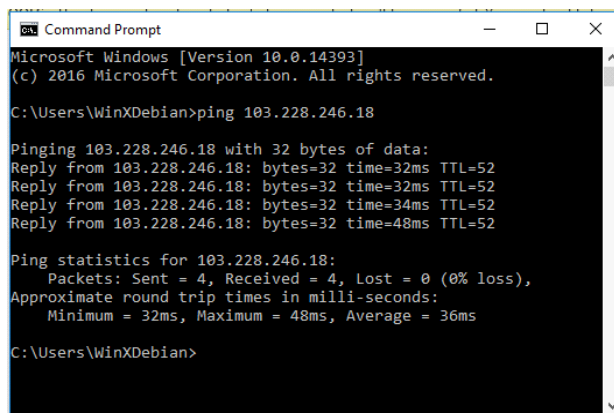
Pinging 10.10.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\WinXDebian>
```

Figure 7. Testing Results of Local IP E-Link using cmd

However, despite this, the Puskesmas can still access the E-Link server via the server's public IP address, which can be vulnerable to cyberattacks. Figure 8 illustrates the testing results of accessing the E-Link server through its public IP address. This outcome indicates that in the initial phase, the Puskesmas can still access the E-Link server using its public IP address.



```
Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\WinXDebian>ping 103.228.246.18

Pinging 103.228.246.18 with 32 bytes of data:
Reply from 103.228.246.18: bytes=32 time=32ms TTL=52
Reply from 103.228.246.18: bytes=32 time=32ms TTL=52
Reply from 103.228.246.18: bytes=32 time=34ms TTL=52
Reply from 103.228.246.18: bytes=32 time=48ms TTL=52

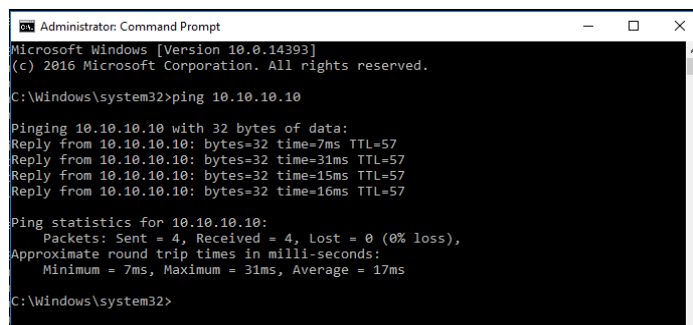
Ping statistics for 103.228.246.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 32ms, Maximum = 48ms, Average = 36ms

C:\Users\WinXDebian>
```

Figure 8. Testing Results of Public IP E-Link using cmd

3.2.2 Final Network Testing

After the VPN configuration is implemented, Puskesmas successfully accesses the local IP address of the E-Link server securely, even if it is not within the local network of the Madiun Regency Health Office. Furthermore, the time taken to access the E-Link server has significantly increased. Figure 9 presents the network testing results of the local IP address of the E-Link server after the connection between the Puskesmas and the Madiun Regency Health Office is established through the PPTP VPN method. This display indicates that after the VPN configuration, Puskesmas can securely connect to the local IP address of the E-Link server using the PPTP method.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 10.10.10.10

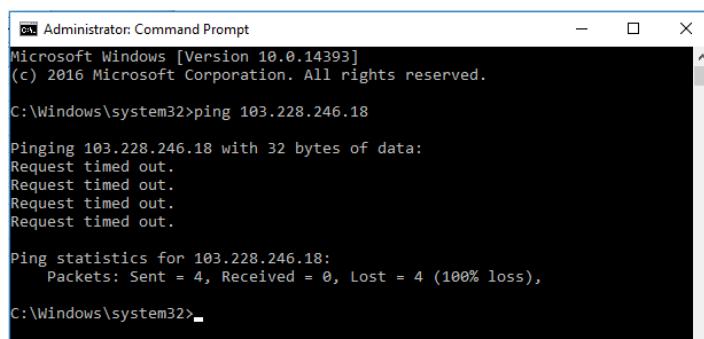
Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time=7ms TTL=57
Reply from 10.10.10.10: bytes=32 time=31ms TTL=57
Reply from 10.10.10.10: bytes=32 time=15ms TTL=57
Reply from 10.10.10.10: bytes=32 time=16ms TTL=57

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 31ms, Average = 17ms

C:\Windows\system32>
```

Figure 9, Network Test Results of Local IP E-Link, connected via PPTP VPN

Furthermore, the public IP address of the E-Link server, which was initially active, was disabled, rendering the server inaccessible through the Internet network. Figure 10 illustrates the view after the public IP address of the E-Link server was deactivated. This display demonstrates that once the public IP address of the E-Link server was disabled, the Puskesmas facility could not reconnect to the server E-Link through the internet network.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 103.228.246.18

Pinging 103.228.246.18 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 103.228.246.18:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>
```

Figure 9. Network Test Results of Public IP E-Link, disconnected after disabling

These testing results show that the VPN configuration has successfully enhanced the security and accessibility of the E-Link server while reducing its vulnerability to attacks through its public IP address.

4. CONCLUSION

In summary, implementing a site-to-site VPN using the PPTP protocol at the Madiun District Health Office has yielded positive results. This VPN solution enhances the security of the E-Link server, ensuring that only authorized VPN users can access it. Network testing demonstrates that Puskesmas can access the E-Link server securely and swiftly via VPN, even outside the Madiun District Health Office's local network after configuration.

REFERENCES

- [1] D. Ferdiansyah, A. R. Kamal, S. A. Majapahit, and F. Mulyanto, "Pengujian Multicore Pada Processor Terhadap Performansi Server Virtualisasi Menggunakan Metode Load Testing," *J. Inf. Syst. Informatics*, vol. 3, no. 4, pp. 698–710, 2021, doi: 10.51519/journalisi.v3i4.193.
- [2] F. Yudha, A. Muhammad, and P. Muryadi, "CyberSecurity dan Forensik Digital Perancangan Aplikasi Pengujian Celah Keamanan Pada Aplikasi Berbasis Web," vol. 1, no. 1, pp. 1–6, 2018.
- [3] S. Ikhwan and A. Amalina, "Analisis Jaringan VPN Menggunakan PPTP dan L2TP (Studi Kasus: Dinhubkominfo Kabupaten Banyumas)," *J. Infotel*, vol. 9, no. 3, pp. 265–270, 2017.
- [4] S. Hendra, "Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik," *Bina Insa. ICT J.*, vol. 3, no. 1, pp. 85–98, 2016.
- [5] Lia Umaroh, Machsun Rifauddin, "Implementasi Virtual Private Network (VPN) Di Perpustakaan Universitas Islam Malang, SK Dirjen Risbang - Kemristekdikti No 21/E/KPT/2018(Peringkat 2 SINTA).
- [6] Tanda Budimulya, Maryanah Safitri, Faridi, "Perancangan VPN Sebagai Pendukung Sistem Informasi Kepegawaian Pada Kantor Kementerian Kesehatan RI", *JIKA (Jurnal Informatika) Universitas Muhammadiyah Tangerang*, Tangerang, Juni 2022.
- [7] B. Santoso, A. Sani, T. Husain, and N. Hendri, "Vpn Site To Site Implementation Using Protocol L2Tp and Ipsec," *Teknokom*, vol. 4, no. 1, pp. 30–36, 2021, doi: 10.31943/teknokom.v4i1.59.
- [8] H. G. Ardiansyah Taufiq A.; Afdhal, Afdhal, "Pengaturan Pemakaian Bandwidth Menggunakan Mikrotik Bridge," *J. Rekayasa Elektr.*, vol. 9, no. Vol 9, No 2 (2010), pp. 69–76, 2010.
- [9] D. Putra and M. I. Fianty, "Capability Level Measurement of Information Systems Using COBIT 5 Framework in Garment Company," *J. Inf. Syst.*

- Informatics*, vol. 5, no. 1, pp. 333–346, 2023, doi: 10.51519/journalisi.v5i1.454.
- [10] Afit Muhammad Lukman, Yusuf Bachtiar, “Analisis Sistem Pengelolaan, Pemeliharaan Dan Keamanan Jaringan Internet Pada IT TELKOM Purwokerto”, *Jurnal Evolusi*, vol. 6, no 2, 2018.
- [11] R. Azhar, “Analisa Qos Pada Jaringan Site To Site Vpn,” *Anal. Qos Pada Jar. Site To Site Vpn Menggunakan Protoc. Sstp*, pp. 52–60, 2017.
- [12] N. K. Dewi and A. S. Putra, “Pengembangan Sistem Jaringan Menggunakan Local Area Network Untuk Meningkatkan Pelayanan (Studi Kasus di PT . ARS Solusi Utama),” *TEKINFO Vol. 22, No. 1, April 2021*, vol. 22, no. 1, pp. 66–81, 2021.
- [13] E. Mufida, D. Irawan, and G. Chrisnawati, “Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta,” *J. Matrik*, vol. 16, no. 2, p. 9, 2017, doi: 10.30812/matrik.v16i2.7.