P-ISSN: 2656-1743 | E-ISSN: 2656-1735 **JURNAL RISET INFORMATIKA**
DOI: https://doi.org/10.34288/jri.v7i3.367 Vol. 7, No. 3. Juni 2025
Accredited rank 4 (SINTA 4), excerpts from the decision of the DITJEN DIKTIRISTEK No. 230/E/KPT/2023

EVALUATION OF TWO-FACTOR AUTHENTICATION METHOD IN IMPROVING AUTHENTICATION SECURITY ON SSL VPN (Case Study of PT. Kanmo Group)

Muhamad Akbar Prasetyo[-1], Nur Chalik Azhar[-2]

Informatics Engineering
Prof. Dr. Hamka Muhammadiyah University
akbarprasetyo17@gmail.com

Abstract

The increasing use of remote access in corporate environments through Virtual Private Networks (VPNs) requires additional security measures to protect corporate data and systems from cyber threats. In Indonesia, several data leakage cases involving large companies have revealed vulnerabilities in existing security systems, highlighting the importance of stronger data protection. At PT Kanmo Group, the VPN used is still vulnerable to security threats such as brute force attacks and credential theft, because it has not implemented 2FA in increasing its security. To overcome this problem, this research aims to improve SSL VPN security by implementing 2FA as an additional layer in the user authentication process. The research methodology includes problem identification, literature study, implementation, and simulation of system testing using an experimental approach. The results showed that the implementation of 2FA significantly improved VPN access security, reduced the risk of credential leakage, and provided a basis for recommendations for companies in strengthening their security systems. This research is expected to be a reference for the development of a more reliable remote access security system in the corporate environment.

Keywords: SSL VPN, two-factor authentication (2FA), network security, remote access, PT. Kanmo Group, data security, VPN.

Abstrak

Peningkatan penggunaan akses jarak jauh di lingkungan perusahaan melalui Virtual Private Network (VPN) memerlukan langkah-langkah keamanan tambahan untuk melindungi data dan sistem perusahaan dari ancaman siber. Di Indonesia, beberapa kasus kebocoran data yang melibatkan perusahaan besar telah mengungkapkan kerentanan pada sistem keamanan yang ada, menyoroti pentingnya perlindungan data yang lebih kuat. Pada PT. Kanmo Group, VPN yang digunakan masih rentan terhadap ancaman keamanan seperti serangan brute force dan pencurian kredensial, karena belum mengimplementasikan 2FA dalam meningkatkan keamanannya. Untuk mengatasi permasalahan ini, Penelitian ini bertujuan untuk meningkatkan keamanan SSL VPN dengan mengimplementasikan 2FA sebagai lapisan tambahan dalam proses autentikasi pengguna. Metodologi penelitian meliputi identifikasi masalah, studi literatur, implementasi, serta simulasi pengujian sistem menggunakan pendekatan eksperimental. Hasil penelitian menunjukkan bahwa penerapan 2FA secara signifikan meningkatkan keamanan akses VPN, mengurangi risiko kebocoran kredensial, serta memberikan dasar rekomendasi bagi perusahaan dalam memperkuat sistem keamanannya. Penelitian ini diharapkan dapat menjadi acuan pengembangan sistem keamanan akses jarak jauh yang lebih andal di lingkungan perusahaan.

Kata Kunci: SSL VPN, autentikasi dua faktor (2FA), keamanan jaringan, akses jarak jauh, PT. Kanmo Group, keamanan data, VPN.

INTRODUCTION

In today's digital age, some companies have implemented a Work From Home (WFH) system (Pratama & Putra, 2022), where the use of a Virtual Private Network (VPN) is essential to enable secure remote access to company systems (Afifi Al-Atsari & Suharjo, 2023). The use of remote access to

company systems makes network security a critical issue, especially given the increasing risks of data theft and cyberattacks (Raka Herdiantoro et al., 2023). However, access to local applications on company systems remains vulnerable to various threats (Pongoh et al., 2023). Issues such as suboptimal configuration, weak credential usage, and potential exploitation of security vulnerabilities in applications are major challenges (Efendi et al., 2024).

According to a report published by the Shadowserver Foundation (2022), brute force attacks are one of the significant threats contributing to network security issues. The main targets of brute force attacks include protocols such as Secure Shell (SSH) and Remote Desk Protocol (RDP), which serve as entry points for network intrusions. Attacks on RDP servers increased by 325% in 2021, reflecting the growing risk for companies that rely on remote access, as reported by Microsoft (Shadowserver Foundation, 2022).

Cyber attacks can damage, steal, or even destroy data and systems, potentially causing significant losses for companies (Wijoyo et al., 2023). Remote access via Secure Socket Tunneling Protocol (SSTP VPN) poses significant security issues for PT. Kanmo Group, particularly in relation to credential theft and brute force attacks (Badeges & Fauzi, 2023). These threats can expose the company's personal information and endanger the entire system. Network security involves not only protecting hardware and software but also a series of measures and practices to maintain the integrity, confidentiality, and availability of data (Syahputri et al., 2023).

Thus, the need to implement additional security measures, such as two-factor authentication (2FA), is becoming increasingly urgent, especially in the context of remote access via a Virtual Private Network (VPN). The effective implementation of two-factor user authentication (2FA) can enhance the security of remote access and help protect sensitive information from potential vulnerabilities on remote devices (Yeboah-Boateng & Kwabena-Adade, 2020).

Based on previous research, various methods have been applied to enhance VPN security, such as the use of RSA algorithms to strengthen public key encryption (Pariddudin & Syawaludin, 2021). Additionally, VPN implementation using the PPTP method employs authentication methods like PAP, CHAP, and MS-CHAP in VPN network implementation (Laksono & Alamin, 2025) ,as well as the combination of L2TP and IPSec protocols that provide protection through encryption and authentication (Prayogi Wicaksana et al., 2021). Additionally, the integration of on-premise servers with cloud servers is also done to enhance network security (Afifi Al-Atsari & Suharjo, 2023). The application of VPN in Star Topology is also implemented to enhance data security (Tiara Pramesti Wulandari et al., 2024), and other research on VPN security is enhanced through the use of SSL certificates as an important encryption layer in ensuring data transmission security (Affandi, 2022). However, these studies have not explored the integration of Two Factor Authentication (2FA) in SSL VPNs.

Although some studies focus on improving VPN security through encryption and protocol changes such as RSA (Pariddudin & Syawaludin, 2021) and L2TP/IPSec (Prayogi Wicaksana et al., 2021), none of these studies have explored the implementation of Two-Factor Authentication (2FA) specifically for SSL VPN. There are still few studies that explore additional security enhancements in access rights authentication.

This study aims to enhance VPN access security by evaluating Two-Factor Authentication (2FA) using SSL VPN at PT. Kanmo Group. The research focus includes evaluating 2FA and assessing risks that may arise at PT. Kanmo Group.

This research uses the Two-Factor Authentication (2FA) method because 2FA is an authentication method that requires users to provide two layers of verification before they can access a system (Nuryati et al., 2022). In addition, the 2FA method is commonly used in research related to security in login systems and corporate network access.

RESEARCH METHOD

This research involves several structured and systematic stages to achieve the goal of developingcomputer network security. The following is a flowchart diagram of the research stages:

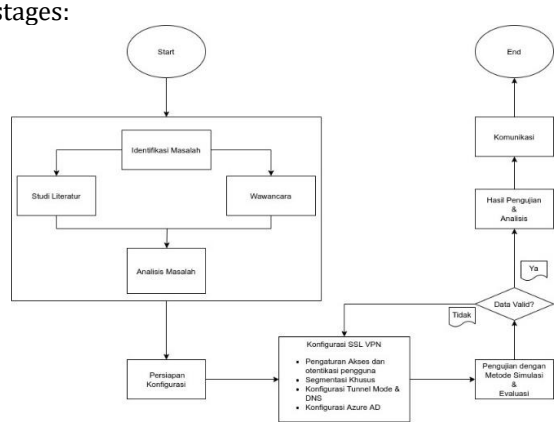

Figure 1. Research Methods

The research flow in Figure 1 is adopted from the study (Tahir et al., 2024), which provides a methodological framework for the implementation of network security based on the Experimental Method. From this method, adjustments were made to suit the needs of this study. This study aims to test the effectiveness of 2FA implementation on SSL VPN, so the author uses the Experimental Method as an appropriate approach. This method allows the author to conduct testing using simulation methods in a controlled environment, enabling the author to directly measure the impact of the 2FA method on authentication security.

Based on the flowchart in Figure 1, the stages began with the identification and analysis of problems through literature studies and interviews with the IT team at PT. Kanmo Group to understand the weaknesses of authentication in SSTP VPN. Next, the environment was prepared and configured, including the setup of software, hardware, and integration with the Azure Single Sign-On service.

The next phase is SSL VPN configuration, where the VPN system is developed and integrated with the 2FA mechanism. After configuration was complete, testing was conducted using simulation and evaluation methods, testing VPN authentication using prepared accounts. The evaluation was conducted to compare the effectiveness of the new system with the previous authentication method. The test results were analyzed to see the impact of implementing 2FA on improving security, particularly in reducing the risk of attacks such as brute force and credential theft.

RESULT AND DISCUSSION

Testing with Simulation and Evaluation Methods

This study successfully implemented an SSL VPN (2FA)-based network security system using Azure Active Directory (Azure AD). Testing was conducted through connection simulation using the FortiClient application in the PT. Kanmo Group network environment.

The authentication process was carried out in two stages. The first stage was the verification of the main credentials (username and password) that had been configured on the FortiGate and Azure AD systems. After the first credentials were successfully verified, the system requested a second verification in the form of an OTP (One-Time Password) code through the authenticator application, which acted as an additional security layer (Kurniawan et al., 2021).

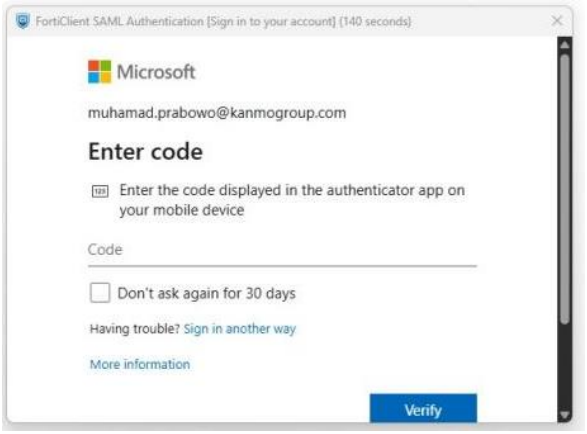

Figure 2. 2FA authentication screen through FortiClient

Users are required to enter an OTP code after initial login, as the second step in the two-factor authentication process.

Once both authentication steps have been successfully completed, users can establish a VPN connection with the status “VPN Connected” displayed on the FortiClient application. This indicates that a secure connection has been successfully established, and users have access to the company's internal network. This finding aligns with research by Cahyaningrum (2024), which states that the implementation of Multi-Factor Authentication significantly enhances system access security, particularly in minimizing the potential for unauthorized access by external parties (Cahyaningrum, 2024).

Figure 3. Successful VPN Connection Status (VPN Connected)

The connection status indicates that two-step authentication was successful and the user is connected to the internal network.

Evaluation of the system shows that the implementation of 2FA successfully adds a layer of

P-ISSN: 2656-1743 |E-ISSN: 2656-1735
DOI: https://doi.org/10.34288/jri.v7i3.367
Accredited rank 4 (SINTA 4), excerpts from the decision of the DITJEN DIKTIRISTEK No. 230/E/KPT/2023

protection against unauthorized access, while maintaining ease of access through the Single Sign-On (SSO) feature. Integration with Azure AD also ran stably and consistently during the simulation process. This mechanism has proven effective in preventing potential threats such as credential theft or brute force attacks, which were previously vulnerable in username-password-based authentication systems alone (Syahputri et al., 2023).

Thus, the system implemented in this study can be considered successful in terms of functionality and security, and is worthy of recommendation as a solution for strengthening remote VPN systems in corporate environments.

Comparison of SSTP VPN and SSL VPN (2FA)

To assess the effectiveness of the SSL VPN system integrated with Two-Factor Authentication (2FA), a comparison was made with the system currently used at PT. Kanmo Group, namely SSTP VPN. This comparison covers aspects of security, authentication, ease of access, and system integration. The results of the comparison are presented in Table 1.

Table 1. Comparison of SSTP VPN and SSL VPN (2FA)

Aspects	SSTP VPN	SSL VPN + 2FA
Authentication Method	Username & Password	Username, Password, OTP.
Safety Level	Low	High
Protocol	SSTP (port 443)	SSL (Port 443)
AD Integration	Yes	Yes (Azure AD + SSO)
Ease of Acces	High	High (SSO active)
Identity Protection	No MFA	App-based OTP

Based on Table 1, it can be seen that the authentication system implemented with SSL VPN and 2FA has a number of advantages over the SSTP VPN system used previously. One of the most significant differences lies in the authentication method. Whereas previously it relied solely on a username and password, the new system integrates two-factor authentication (2FA), which adds an additional layer of security in the form of an OTP code.

Single authentication methods that rely on only one factor, such as a username and password, still have a number of shortcomings in terms of security. One of the main weaknesses is vulnerability to phishing attacks, where users can be tricked into giving their credentials to unauthorized parties (Noorshalih et al., 2024).

Additionally, the new system also demonstrates improvements in user identity protection by implementing Azure AD-based Multi-Factor Authentication (MFA). This not only enhances security but also supports access efficiency through the Single Sign-On (SSO) feature. In terms of ease of access, the new system maintains user convenience while ensuring greater security (Nurhasanah & Harahap, 2022).

Thus, the results of this comparison indicate that the implementation of SSL VPN integrated with 2FA can be a safer and more effective solution to support the company's remote access needs without compromising user convenience.

CONCLUSION

This study successfully implemented a Two Factor Authentication (2FA) system on SSL VPN in the PT. Kanmo Group environment as a solution to improve remote access security. Simulation results show that the system functions effectively, with two layers of authentication (main credentials and OTP) that are effective in preventing unauthorized access. Additionally, the Single Sign-On (SSO) feature via Azure Active Directory supports easy access without compromising security.

From a practical perspective, this research provides a tangible contribution to improving corporate network security, particularly for organizations still using single authentication methods. From an academic perspective, this research enriches the study of 2FA technology implementation in the context of SSL-based VPNs, a topic previously not extensively discussed in the literature.

This research has limitations in the scope of testing, which was only conducted through simulations in a limited environment and did not include quantitative measurements of system performance (such as connection time, server load, or user satisfaction). Additionally, real-world cyberattack scenarios like brute force attacks have not been thoroughly tested.

For future research, it is recommended that testing be conducted in a broader environment, such as directly on production systems or active corporate networks. Additionally, it would be beneficial to measure system performance, for example, in terms of authentication time, connection speed, or user convenience. Future research could also consider the use of other more practical authentication methods, such as biometrics or passwordless authentication, to explore potential improvements in both security and ease of access.

REFERENCE

Affandi, M. (2022). IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) OPEN VPN DENGAN KEAMANAN SERTIFIKAT SSL PADA NETWORK ATTACHED STORAGE (NAS) FREENAS. *Jurnal Impresi Indonesia (JII)*, *1*(12). https://doi.org/https://doi.org/10.58344/jii.v1i12.748

Afifi Al-Atsari, H., & Suharjo, I. (2023). Integrasi Server On-Premise dengan Server Cloud Menggunakan Cloud VPN dan Mikrotik Ipsec Untuk Peningkatan Keamanan Koneksi. *Jurnal Syntax Admiration*, *4*(11), 1977–1996. https://doi.org/10.46799/jsa.v4i11.757

Badeges, W., & Fauzi, M. N. (2023). IMPLEMENTASI MULTI FACTOR AUTHENTICATION PADA PHPMYADMIN. *Jurnal Tiple A Pendidikan Teknologi Informasi Dan Teknologi Informasi*, *2*(1). https://jurnal.umj.ac.id/index.php/TripleA/article/view/17517

Cahyaningrum, Y. (2024). Evaluation of System Access Security in The Implementation of Multi-Factor Authentication (MFA) in Educational Institutions. *Journal of Practical Computer Science*, *4*(1). https://doi.org/https://doi.org/10.37366/jpcs.v4i1.4451

Efendi, R., Wahyono, T., & Widiasari, I. R. (2024). Uji kerentanan keamanan pada aplikasi berbasis web menggunakan metode Vulnerability Assessment. *AITI: Jurnal Teknologi Informasi*, *21*(Maret), 44–57. https://doi.org/https://doi.org/10.24246/aiti.v21i1.44-57

Kurniawan, D. E., Iqbal, M., Friadi, J., Hidayat, F., & Permatasari, R. D. (2021). Login Security Using One Time Password (OTP) Application with Encryption Algorithm Performance. *Journal of Physics: Conference Series*, *1783*(1). https://doi.org/10.1088/1742-6596/1783/1/012041

Laksono, I. A., & Alamin, M. M. (2025). IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) BERBASIS MIKROTIK MENGGUNAKAN METODE PPTP PADA JARINGAN INTERNET DI FAKULTAS ILMU KOMPUTER UNUSIDA. *Jurnal Mahasiswa Teknik Informatika)*, *9*(3). https://doi.org/https://doi.org/10.36040/jati.v9i3.13582

Noorshalih, P., Septiana, R., Nurul, I., & Afrianto, I. (2024). IMPLEMENTASI DUA FACTOR AUTHENTICATION DAN MONITORING TRANSACTION PADA APLIKASI PEMESANAN JASA FOTOGRAFI DAN VIDEOGRAFI DI PRIMAPICTURES. *INFOKOM : Journal of Information and Technology*, *17*(1), 52–57. https://jurnal.stikompoltekcirebon.ac.id/index.php/file_jurnal/article/view/112

Nurhasanah, S., & Harahap, A. A. (2022). EVALUASI TINGKAT KESIAPAN PENGGUNA SISTEM SINGLE SIGN ON PADA PORTAL UNIVERSITAS ALMA ATA MENGGUNAKAN METODE TECHNOLOGY READINESS INDEX (TRI). *Indonesian Journal of Business Intelligence (IJUBI)*, *5*(1), 1. https://doi.org/10.21927/ijubi.v5i1.2126

Nuryati, N., Lasambouw, C. M., Djatnika, D., Meilinda, L. L., Agoes, F., Sholahuddin, M. R., & Harika, M. (2022). Two Factor Authentication Sistem Inventarisasi Barang dan Manajemen Dana Bantuan Operasional Sekolah Dinas Pendidikan Nasional. *Building of Informatics, Technology and Science (BITS)*, *4*(2). https://doi.org/10.47065/bits.v4i2.2297

Pariddudin, A., & Syawaludin, M. (2021). Penerapan Algoritma Rivest Shamir Adleman Untuk Meningkatkan Keamanan Virtual Private Network. *Jurnal Ilmiah Teknologi - Informasi & Sains*, *11*, 73–84. https://doi.org/10.36350/jbs.v11i2

Pongoh, D. S., Eksan, S., Pairunan, T., & Manado, P. N. (2023). Analisis Keamanan Perangkat Lunak Terhadap Serangan Melalui Jaringan WiFi Publik. *Jurnal Komputasi Terdistribusi*, *6*(4). https://oaj.jurnalhst.com/index.php/jkt/article/view/2813

Pratama, F., & Putra, P. (2022). PENGEMBANGAN SISTEM PRESENSI UNTUK WORK FROM HOME (WFH) DAN WORK FROM OFFICE (WFO) SELAMA PANDEMI COVID-19. *Jurnal Sains, Nalar, Dan Aplikasi Teknologi*

Informasi, *1*(2). https://doi.org/10.20885/snati.v1i2.9

Prayogi Wicaksana, Hadi, F., & Aulia Fitrul Hadi. (2021). Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan. *Jurnal KomtekInfo*, 169–175. https://doi.org/10.35134/komtekinfo.v8i3.128

Raka Herdiantoro, H., Reza Redo Islami, M., Informatika, T., Dharma Wacana Metro Jl Kenanga No, S., Metro Bar, K., & Metro, K. (2023). *IMPLEMENTASI TWO-FACTOR AUTHENTICATION (2FA) DAN FIREWALL POLICIES DALAM MENGAMANKAN WEBSITE*. *4*(1), 1–9. https://doi.org/https://doi.org/10.24127/ilmukomputer.v4i1.3300

Shadowserver Foundation. (2022). *Honeypot Brute Force Events Report*. https://www.shadowserver.org/wp-content/uploads/2022/06/Honeypot_Brute_Force_Events_March_2022.pdf

Syahputri, N. I., Harahap, H., Siregar, R., & Tommy, T. (2023). Penyuluhan Pentingnya Two Factor Authentication dan Aplikasinya Di Era Keamanan Digital. *Jurnal Pengabdian Masyarakat Bangsa*, *1*(6), 768–773. https://doi.org/https://doi.org/10.59837/jpmba.v1i6.256

Tahir, M., Hariyanto, H., Firdausi, M. I., Saim, S., Nuriyah, N., & Maimunah, M. (2024). Peningkatan Keamanan Jaringan LAN dan WLAN Melalui Standard Acces Control List. *Digital Transformation Technology*, *4*(1), 607–614. https://doi.org/10.47709/digitech.v4i1.4261

Tiara Pramesti Wulandari, Novaldi Ramdani Reza, Errisa Zulqa Deswana, Muhammad Rifqi Adillah, & Didik Aribowo. (2024). Penerapan VPN Dalam Topologi Star Untuk Keamanan Pengiriman Data. *Neptunus: Jurnal Ilmu Komputer Dan Teknologi Informasi*, *2*(2), 63–70. https://doi.org/10.61132/neptunus.v2i2.93

Wijoyo, A., Rosadi, A., Hanafi, M., & Sidik, R. (2023). *Keamanan Jaringan Melindungi Sistem dari Serangan Luar*. https://jurnalmahasiswa.com/index.php/jrijin/article/view/407

Yeboah-Boateng, E. O., & Kwabena-Adade, G. D. (2020). Remote Access Communications Security: Analysis of User Authentication Roles in Organizations. *Journal of Information Security*, *11*(03), 161–175. https://doi.org/10.4236/jis.2020.113011