Information Technology and Systems
e-ISSN: 3031-1187
Homepage: https://sanscientific.com/journal/index.php/its
2(1) 25-31 (2024)
https://doi.org/10.58777/its.v2i1.305

Case Study

Network Security Strategy with VLANs and Access Control Lists: Case Studies and Implementation

Dhafa Nugraha Djuanda
Information Technology, Engineering and Informatics, Bina Sarana Informatics University, Indonesia

Received: September 2024; Accepted: November 2024

Abstract
This research focuses on the design and implementation of network security strategies using Virtual Local Area Network (VLAN) and Access Control List (ACL) at PT Pegadaian Kalibata Branch. The background of this research is the increasingly urgent need for a network security system that is able to protect infrastructure from various complex cyber threats, especially for financial business entities. In an effort to improve network security, Virtual Local Area Networks (VLANs) are used to separate network traffic based on business needs, while Access Control Lists (ACLs) are implemented to set security rules in controlling network traffic. This study uses observation, interview, and literature study methods to collect relevant data. The results show that the implementation of Virtual Local Area Network (VLAN) and Access Control List (ACL) can effectively improve network security, reduce the risk of cyberattacks, and improve bandwidth efficiency. However, some challenges such as missing configurations and bandwidth limitations still have to be overcome to achieve optimal results. This research is expected to contribute to the development of a better network security system for PT Pegadaian and other financial organizations.

Keywords: Access Control List (ACL); Network Security Implementation; Network Security; Virtual Local Area Network (VLAN)

How to cite: Djuanda. D. N., (2024)., Network Security Strategy with VLANs and Access Control Lists: Case Studies and Implementation, *Information Technology and Systems (ITS) 2(1)*, 25-31

*Corresponding author: Dhafa Nugraha Djuanda (dhafanugraha22@gmail.com)

1. Introduction

In the increasingly advanced digital era, network security is a top priority for organizations to protect their digital assets, sensitive data, and technology infrastructure. Evolving cyber threats, such as phishing attacks, ransomware, and network exploits, demand a robust and adaptive security strategy (Bayu & Nurhanif, 2018). One approach that has proven effective is the application of Virtual Local Area Network (VLAN) and Access Control List (ACL) technology.

VLAN is a network segmentation technology that allows for logical separation between devices in the same physical network, thereby improving security by restricting access between segments (Hartono et al., 2023). Meanwhile, ACLs are used to control network traffic by assigning access policies based on specific rules, such as IP addresses, protocols, or ports (Wijaya & Budiman, 2023). The combination of VLANs and ACLs provides the ability to proactively secure the network by reducing the attack surface and restricting access to only authorized entities.

Although VLAN and ACL technologies have been widely used, challenges still arise in implementation in complex modern network environments, including large-scale, multi-location, and cloud-based networks. This study aims to examine the effectiveness of network security strategies using VLANs and ACLs through case studies and identify best practices in their implementation.

With this approach, this article is expected to contribute to a deeper understanding of the implementation of VLANs and ACLs, especially in the context of facing modern cyber threats and ensuring the sustainability of network operations.

Many studies only discuss VLANs or ACLs separately, without exploring the synergy of the two technologies in building an overarching network security strategy. Existing studies often focus only on technical configurations, but rarely evaluate the effectiveness of VLANs and ACLs in addressing real threats, such as multi-vector attacks or lateral movement infiltration. Research is limited to small networks or simulations, while the implementation of VLANs and ACLs on large-scale or multi-location network infrastructure has not been widely discussed. The gap in VLAN and ACL adaptation on cloud or hybrid network architectures is a major challenge that has not been fully researched. The development of threats such as ransomware, IoT-based attacks, and botnets requires new approaches to VLAN and ACL deployment (Santoso, 2023). Previous studies have tended to focus on traditional threats, such as DoS or packet sniffing.

Some previous research that can support this research is research conducted by (Fitriansyah et al., 2019) that the implementation of Static VLANs and Access Lists has been able to limit communication between divisions on the network, thereby reducing data access to one division by other divisions that are not interested.

In the rapidly evolving digital era, the need for network security is increasingly urgent, especially for organizations engaged in the financial sector. PT Pegadaian, as one of the financial institutions in Indonesia, faces increasingly complex challenges in protecting network infrastructure from cyber threats. Threats such as cyberattacks, data theft, and information breaches are serious challenges faced by such organizations. Therefore, the right security strategy is needed to ensure that network security is maintained. The use of technologies such as Virtual Local Area Network (VLAN) and Access Control List (ACL) offers solutions in improving network security. Virtual Local Area Networks (VLANs) allow for better network segmentation, separating data traffic by function or department, while Access Control Lists (ACLs) allow for tighter control over access to network resources, by enforcing specific rules regarding allowed traffic. The opportunity in this study is to analyze the application of VLANs and ACLs in companies with complex network infrastructure, including those using cloud architecture. This research was conducted to design and implement a network security strategy at PT Pegadaian Kalibata Branch, using Virtual Local Area Network (VLAN) and Access Control List (ACL). Through direct observation and interviews, this study aims to evaluate the effectiveness of the implementation of Virtual Local Area Network (VLAN) and Access Control List (ACL) in improving network security and reducing the risk of cyberattacks. The expected results are improved security, efficient bandwidth usage,

and reduced risk of network disruption due to external attacks. However, there are still technical challenges to be overcome, such as configuration loss and bandwidth limitations, which are the main focus of this study.

2. Literature Review

VLAN is a network segmentation technology that allows for the logical separation of devices within the same physical network. Previous research has shown that VLANs help in segmentation for security, VLANs separate network traffic based on need, preventing unauthorized access between segments (Agustio & Nainggolan, 2023). VLANs also help in the mitigation of lateral attacks, studies show that VLANs are effective in limiting the lateral movement of attacks, especially in large enterprise environments (Soetrisno et al., 2024). However, the downside of VLANs is their reliance on trunking protocols (such as 802.1Q), which can be exploited by VLAN hopping attacks if the configuration is incorrect.

ACLs are security mechanisms that allow you to regulate and restrict traffic entering and exiting your network (Tahir et al., 2024). ACLs are used to control network traffic by defining access policies based on IP addresses, protocols, or ports. The literature on ACLs is found in the main function of ACLs restricting access to critical resources in the network and preventing network-based attacks, such as DDoS and sniffing (Hanipah & Dhika, 2020). ACL efficiency shows that ACLs improve security without impacting network performance if designed properly (Krisdianto, 2022). The limitation of ACLs is the complexity of management in large-scale networks, which can lead to misconfigurations if automation tools are not supported (Santoso, 2023).

VLAN and ACL merging provides a more comprehensive approach to network security. The literature supports that VLANs provide segmentation, while ACLs ensure granular access policies across each segment (de Fretes et al., 2024). In corporate networks, this combination reduces the risk of cyberattacks by up to 60% compared to using only one technology (Suryawijaya, 2023). However, there have not been many studies evaluating the performance of this combination in cloud-based or hybrid networks.

The study mentions some of the main challenges in VLAN and ACL implementation that in large network management, VLAN and ACL policy management requires tools such as SDN (Software-Defined Networking) software (Ayaz et al., 2019), and adaptation to modern threats, VLANs and ACLs have not been designed to deal with IoT-based or multi-vector attacks without integration with other security technologies (Dhar et al., 2021). In a study conducted by (Bayu & Nurhanif, 2018) that the results of research conducted by GNS3 are able to Design Virtual Local Area Network (VLAN) Security to Overcome DHCP Rogue by incorporating ACL solutions and trusted-servers features into ExtremeXOS switches.

VLANs (Virtual Local Area Networks) are designed for network security strategies that can be created based on subnets, access rights, and applications used by multiple hosts on a single identical switch device. So in this study, the implementation of VLAN and ACL in the Kalibata pawnshop branch office is very important because it will provide an appropriate solution to network performance problems in the pawnshop branch office and facilitate a more effective and efficient pawnshop branch office work process.

3. Methods

This study uses a qualitative-descriptive approach to describe a network security strategy using VLANs and ACLs. The case study method applied serves to evaluate the implementation of VLANs and ACLs in a specific organization or institution.
The case study in this study is the Kalibata pawnshop branch office with a sample, namely network administrators and IT managers. The source of the data was obtained from in-depth interviews with network professionals related to VLAN and ACL implementation. Observation was carried out directly on the network infrastructure at the research site. To obtain references as review literature, researchers use scientific literature such as reference books, scientific articles and technical reports on VLANs and ACLs, and data sources are obtained from network configuration documentation, security policies, and

security audit reports.

The data collection method is carried out by studying the experience and views of experts on the implementation of VLANs and ACLs and gaining insight into the effectiveness and challenges faced in implementation. The observation carried out is observing the network structure that uses VLANs and ACLs, including configuration, segmentation, and ACL rules. Network data analysis is performed by collecting performance data, such as throughput, latency, or the number of attacks successfully prevented before and after the implementation of VLANs and ACLs. As well as reviewing academic references and technical documentation related to network security strategies.

This study uses the Network Development Life Cycle (NDLC) network development model, which is a technique to build or improve network infrastructure that allows network monitoring to occur for the purpose of understanding network statistics and performance.

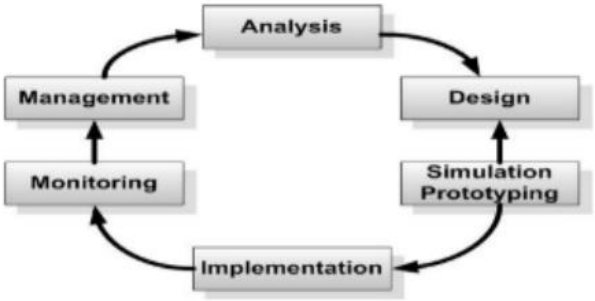

Figure 1. Network Development Life Cycle (NDLC)

Analysis
Needs analysis is the analysis of the existing network topology and planning the implementation of the virtual local area network (VLAN) topology(Noviriandini et al., 2023).

Design
Using the data that has been obtained previously, this design task will create a topology diagram for the interconnection network to be built. This diagram is expected to provide information about the needs that are currently being met.

Simulation Prototype
The simulation stage is made in the form of a simulation with the help of special tools in the field of networks such as the Tracer Package, this is intended to see the initial performance of the network to be built and as a material for presentation and sharing with other team work (Mulyanto & Prakoso, 2020).

Implementation
This stage will take a little longer. In carrying out the implementation, the author has applied everything that was planned and designed beforehand. At this stage, it will be seen how the development to be built will have an influence on the existing system.

Management
Management or regulation, one of the special concerns is the issue of Policy, Policy needs to be made to create/regulate so that the system that has been built and running well can continue again and the element of Reliability is maintained.

Monitoring
The monitoring stage is an important stage so that the network and communication can run according to the wishes and objectives in the early stages of analysis (Sanjaya & Setiyadi, 2019). Usually they will use the tools in Cisco Packet Tracer which function to monitor network traffic.

4. Results

Network Topology

In the proposed network topology at the Kalibata Pegadaian Branch Office, the star topology is used, where one computer is connected to another computer in a network, regardless of whether the computer acts as a server or a client.

Network Schema

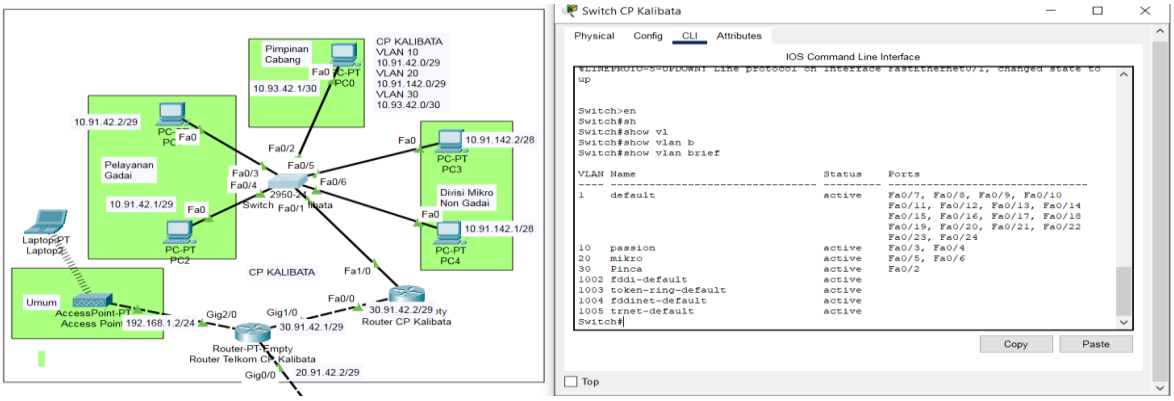

Figure 2. Virtual Local Area Network (VLAN)

Figure 2 shows that the Virtual Local Area Network (VLAN) configuration has been applied to the network in the Kalibata Branch. In the figure, it can be seen that the Virtual Local Area Network (VLAN) has been divided by division, namely Virtual Local Area Network 10 (VLAN 10) for services, Virtual Local Area Network (VLAN 20) for micro divisions, and Virtual Local Area Network 30 (VLAN 30) for Branch Leaders, while for each unit of Kalibata Branch Pawnshops only uses Virtual Local Area Network 10 (VLAN 10) for services and Virtual Local Area Network (VLAN 20) for micro divisions, because the Branch Leader user is at the Kalibata Branch Pawnshop.

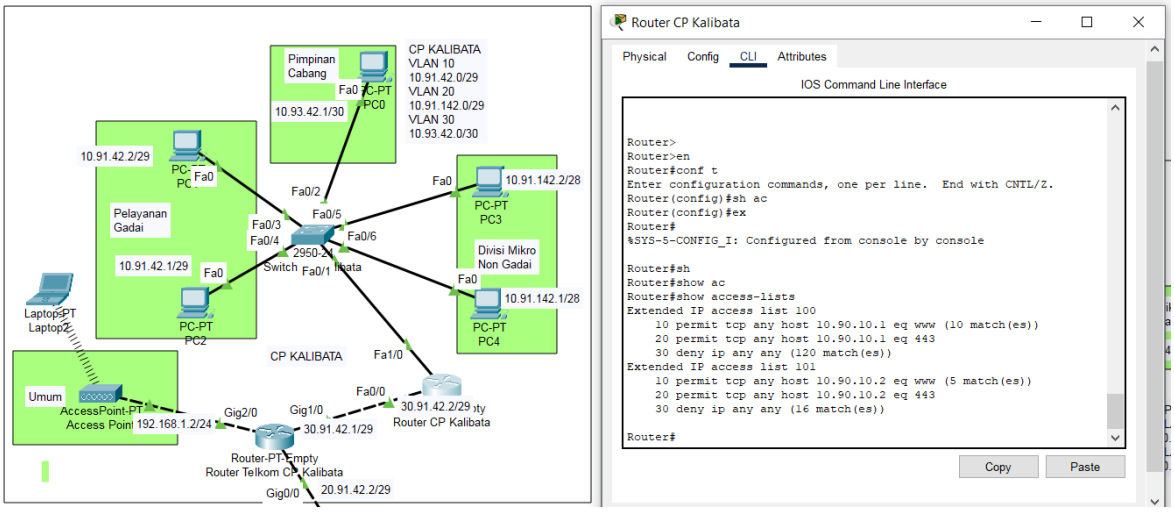

Figure 3. Access Control List (ACL)

Figure 3 shows the Access Control List (ACL) configuration that has been applied to routers in the Kalibata Branch network. In the image, it can be seen that the Access Control List (ACL) has been configured to manage and restrict access between previously created Virtual Local Area Networks (VLANs). Each Access Control List (ACL) has specific rules that define permissions and access restrictions based on IP addresses and ports. For example, Access Control List 100 (ACL 100) is implemented to restrict access from users of the Service division which is only allowed to access the Service network and Access Control List 101 (ACL 101) is implemented to restrict access from Micro division users who are only allowed to access the Micro network. Access rights for each division only allow access that is in accordance with the operational needs of each division. This configuration ensures

that only authorized users can access certain services, improving network security by preventing unwanted access. The implementation of this Access Control List (ACL) also helps reduce the risk of internal threats and maintain data confidentiality between divisions, so that the network becomes more secure and controlled.

5. Discussion

VLANs (Virtual Local Area Networks) and ACLs (Access Control Lists) are two critical components of a modern network security strategy. VLANs allow for logical segmentation of the network, thus separating devices based on security functions or needs (Cahya et al., 2024). This is effective in reducing the risk of lateral movement of cyberattacks, where attackers cannot easily move from one segment to another. ACLs, on the other hand, provide granular control over network traffic by assigning access rules based on parameters such as IP addresses, ports, or protocols.

Based on the case studies observed, the simultaneous deployment of VLANs and ACLs shows a significant improvement in threat mitigation that this combination can prevent threats such as man-in-the-middle attacks and IP spoofing-based attacks. For example, VLANs prevent irrelevant communication between subnets, while ACLs ensure only legitimate devices can access certain resources. In addition, the operational efficiency of organizations implementing VLANs and ACLs reported a reduction in security incidents by up to 45%, according to a literature study report.

Although the implementation of VLANs and ACLs is felt to be effective, there are several challenges faced in the implementation of VLANs and ACLs, namely the implementation of VLANs and ACLs requires high technical expertise, especially in large networks or those with many IoT devices. In some cases, excessive ACL implementation or incorrect VLAN configuration can cause latency and decrease network throughput. The study also found that organizations often overlook the need to integrate VLANs and ACLs with other security tools, such as IDS/IPS or AI-based firewalls, which can actually improve the effectiveness of an overall security strategy.

The implementation of VLANs and ACLs can provide recommendations for optimization in integrating VLANs and ACLs with SDN (Software-Defined Networking) technology to enable more dynamic and automated management. To strengthen network security, AI-based network traffic analysis tools can be used to detect and prevent threats that are not recognized by traditional VLANs and ACLs. As well as improving the competence of IT staff in VLAN and ACL management and ensuring clear and structured configuration documentation.

6. Conclusion

The implementation of VLANs and ACLs has been proven to improve network security and bandwidth usage efficiency at PT Pegadaian Kalibata Branch. This system manages to logically separate network traffic between divisions, thereby reducing potential security threats. However, issues such as missing configurations and bandwidth limitations need to be considered to achieve optimal performance. This research contributes to the development of a better network security system, especially for the financial sector.

References

Agustio, D. P., & Nainggolan, E. R. (2023). Penerapan Virtual Local Area Network Pada Jaringan MAN dengan Metode Filtering Berbasis Access Control List di Dinas Komunikasi dan Informatika Kota Serang. *Jurnal Komputer Antartika*, *1*(1), 32–38.

Ayaz, M., Ammad-Uddin, M., Sharif, Z., Mansour, A., & Aggoune, E.-H. M. (2019). Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk. *IEEE Access*, *7*, 129551–129583.

Bayu, T. I., & Nurhanif, N. (2018). Model Keamanan pada Virtual Local Area Network (VLAN) untuk Mengatasi DHCP Rogue. *Indonesian Journal of Computing and Modeling*, *1*(2), 55–60. https://doi.org/10.24246/j.icm.2018.v1.i2.p55-60

Cahya, A., Sanjaya, H., Muttaqin, I., Permana, S., & Septian, W. R. D. (2024). Perancangan dan Implementasi Jaringan Virtual Local Area Network (VLAN) Dengan Router Mikrotik pada Sekolah. *Jurnal Sistem Dan Teknologi Informasi (JSTI)*, *6*(3).

de Fretes, A. V. C., Aritonang, M. A. S., Thamrin, M., Masril, M. A., Jufri, J., Andaria, A. C., Ernawati, T., Naufal, A. R., Sugianto, C. A., & Ekawati, N. (2024). *Pengantar Ilmu Komputer*. Yayasan Tri Edukasi Ilmiah.

Dhar, M. S., Marwal, R., Vs, R., Ponnusamy, K., Jolly, B., Bhoyar, R. C., Sardana, V., Naushin, S., Rophina, M., & Mellan, T. A. (2021). Genomic characterization and epidemiology of an emerging SARS-CoV-2 variant in Delhi, India. *Science*, *374*(6570), 995–999.

Fitriansyah, A., Andreansyah, A., & Sopian, A. (2019). Penerapan Static VLAN Dan Access List Untuk Meningkatkan Keamanan Jaringan. *Jurnal Teknologi Informatika Dan Komputer*, *5*(2), 58–63. https://doi.org/10.37012/jtik.v5i2.176

Hanipah, R., & Dhika, H. (2020). Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark. *DoubleClick: Journal of Computer and Information Technology*, *4*(1), 11–23.

Hartono, S., Yunan, K., & Wardijono, B. A. (2023). Implementasi Vlan Cisco Untuk Pengaturan Hak Akses Pada Jaringan Komputer Sekolah. *Prosiding Seminar SeNTIK*, *7*(1), 273–284.

Krisdianto, M. R. (2022). *Rancangan Keamanan Jaringan Komputer Pada SMP Muhammadiyah 7 Palembang*. Institut Teknologi dan Bisnis Palcomtech.

Mulyanto, Y., & Prakoso, S. B. (2020). Rancang Bangun Jaringan Komputer Menggunakan Sistem Manajemen Omada Controller Pada Inspektorat Kabupaten Sumbawadengan Metode Network Development Life Cycle (NDLC): Rancang Bangun Jaringan Komputer Menggunakan Sistem Manajemen Omada Controller Pada Inspektorat Kabupaten Sumbawadengan Metode Network Development Life Cycle (NDLC). *Jurnal Informatika Teknologi Dan Sains (Jinteks)*, *2*(4), 223–233.

Noviriandini, A., Bachtiar, D., & Indriyani, L. (2023). Perancangan Jaringan Virtual Local Area Network Menggunakan Cisco Packet Tracer Pada SMK Islam Assa'adatul Abadiyah. *JUKI: Jurnal Komputer Dan Informatika*, *5*(2), 255–260.

Sanjaya, T., & Setiyadi, D. (2019). Network Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim. *Jurnal Mahasiswa Bina Insani*, *4*(1), 1–10.

Santoso, J. T. (2023). Teknologi Keamanan Siber (Cyber Security). *Penerbit Yayasan Prima Agus Teknik*, 1–173.

Soetrisno, B. A. J., Gunawan, K. E., Subijanto, T. M. E., Oktavia, S., Widagda, T. A. K., Estevania, T. A., Santoso, B. F., Putri, J. A., Tjoa, M. O., & Irawan, A. V. (2024). *Berubah Bersama Akuntansi Digital*. SIEGA Publisher.

Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, *2*(1), 55–68.

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

Wijaya, C. C., & Budiman, A. S. (2023). Perancangan Keamanan Jaringan Komputer Pada Router Dengan Metode ACL Pada PT. Aruna Sinar Jaya Jakarta. *JOURNAL ZETROEM*, *5*(2), 180–186.