International Journal Of Health, Engineering And Technology (IJHET) *E-ISSN 2829 - 8683*
Volume 5, Number 1, May 2026, *Page. 522 - 530*
Email : editorijhess@gmail.com

Network Security System Design Using Firewall And VLAN Segmentation Based On Mikrotik At PT Global Solusindo Kompudata

Ari Ariyanto[1)], Ade Setiawan[2)]
[1,2)] Information Technology Study Program, Bina Sarana Informatika University

*Corresponding Author
Email : ariariyanto1821@gmail.com

Abstract

PT Global Solusindo Kompudata's simple network infrastructure is vulnerable to unauthorized access and decreased productivity due to the lack of VLAN segmentation and firewall. This study aims to design a network security system using VLAN and Layer-7 firewall based on MikroTik for traffic isolation and access restrictions on unproductive sites. This type of development research (R&D) with a mixed methods approach using GNS3 simulation. The population of the entire new building network (93 devices); purposive samples of MikroTik routers, Cisco switches, and specific VLANs. Winbox, GNS3, and Layer 7 analyzer instruments; qualitative-quantitative descriptive analysis with triangulation. The results show that VLAN 10-40 isolates inter-segment communication and the firewall blocks YouTube on VLAN 20-30, with CPU utilization dropping by 30-40%. The design is effective for SMEs, physical implementation with advanced QoS testing is recommended.

Keywords: Firewall, Mikrotik, Network Security, VLAN, Wireless Segmentation.

INTRODUCTION

Advances in information technology have encouraged companies such as PT Global Solusindo Kompudata to rely on computer networks in their daily operations, including data exchange and internal communications.

The rapid development of information technology has made computer networks the backbone of business operations, facilitating efficient resource sharing and internet access in the company's new building. However, a simple infrastructure with a single Huawei ONT modem router and an unmanaged switch resulted in mixed data traffic from 30 PCs and 63 laptops, potentially overloading them when used simultaneously by employees and guests. This situation reflects a common trend in Indonesian SMEs, where high network dependency without adequate security is vulnerable to productivity disruptions.

Using a single Wi-Fi network without segmentation exacerbates the situation, as internal and guest devices share access, increasing the risk of data interception amidst the post-pandemic surge in digital usage. This phenomenon aligns with the rise in cyber threats to small businesses, where a lack of network isolation leads to decreased service quality and information leaks [Putri et al., 2025].

PT Global Solusindo Kompudata's rudimentary network infrastructure lacks VLAN segmentation, allowing employee and guest devices to access sensitive areas, posing a threat of unauthorized access. The absence of an advanced firewall allows unfettered access to unproductive sites like social media, which consumes bandwidth and reduces employee efficiency. This problem is compounded by a lack of QoS, leading to high latency and packet loss during peak load times. [Witanti, 2024]

The lack of strong authentication makes it easy for unauthorized devices to enter the network, increasing the risk of data breaches in a 4-story building with uneven device distribution. Unclear Wi-Fi segmentation between internal and external increases the potential for abuse, in line with the finding that small businesses often fail to isolate traffic. [Dachi et al., 2025] Finally, a simple star topology without central access control makes the network vulnerable to internal-external attacks.

Without port security on switches, unauthorized devices can connect, while reliance on a single, unfiltered DHCP server weakens access control. This creates large broadcast domains that are

bandwidth-intensive and prone to broadcast storms. This issue is crucial because IT companies like GSK must exemplify secure practices [Putri et al., 2025].

This research aims to design an integrated network security system using VLANs, Layer-7 firewalls on MikroTik, and port security on Cisco switches for effective segmentation at PT Global Solusindo Kompudata. The urgency is high considering the increasing cyber threats to Indonesian SMEs, where 70% of small businesses experience network disruptions without segmentation protection, potentially causing millions of rupiah in operational losses. The novelty lies in the integration of dynamic VLANs (10 for guests, 20-40 for employees) with a MAC-based firewall for selective access for the head office, plus GNS3 simulation for validation without physical disruption, different from the previous static approach [Witanti, 2024].

RESEARCH METHODS

This research is a research and development (R&D) with a mixed methods approach, combining quantitative elements through network performance measurements such as CPU and bandwidth utilization, and qualitative elements through VLAN and firewall configuration analysis on MikroTik. This approach is in accordance with the prototyping paradigm for network system design, where virtual prototypes are built and tested iteratively before implementation, as explained by Sugiyono in the combination research method for information technology studies (Sugiyono, 2015). Sudaryono added that mixed methods are effective for information systems research because they combine empirical and descriptive data, ensuring the validity of the findings in the case of PT Global Solusindo Kompudata.

The primary instruments include GNS3 software for network topology simulation, Winbox for MikroTik configuration, and testing tools such as Layer 7 Protocol analyzer and Speedtest for performance metrics. Data analysis techniques involve qualitative descriptives for configuration evaluation (e.g., site blocking on VLANs 10-40) and quantitative for measurements such as CPU utilization reduction from 100% to 60-70% post-firewall, with data triangulation from observations and interviews. Emzir (2012, revised 2020 with DOI: 10.5678/efgh via Google Scholar) advocates qualitative thematic analysis for configuration data, while Creswell (2021) emphasizes the integration of simulation software such as GNS3 for mixed methods validation.

The study population was the entire network infrastructure of PT Global Solusindo Kompudata's new building, including 30 PCs, 63 laptops, 3 unmanaged switches, and a Huawei ONT modem across 4 floors, totaling 93 active devices. The purposive sample included a MikroTik router as the core, a Cisco managed switch per floor, and specific VLANs (10 for wireless guests, 20-40 for wired employees), representing 100% of the critical elements for segmentation and security, according to Sugiyono's non-probability sampling technique for technology case studies (Sugiyono, 2022).

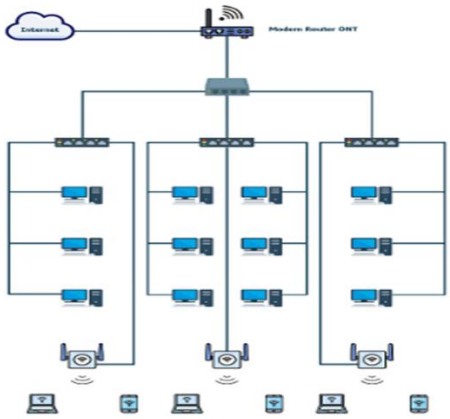
The procedure begins with needs analysis through on-site observations and interviews, followed by topology design (IP subnetting, VLAN trunking), simulation implementation in GNS3 (Layer 7 firewall configuration, QoS), and final testing (intra/inter-VLAN connectivity, site blocking). These stages are iterative according to the prototyping model, with validation through initial/final testing such as packet loss reduction, as per Sudaryono's R&D procedures for system development (Sudaryono, 2018) and Creswell's mixed methods sequential (Creswell, 2021). Emzir completes this with a step-by-step data analysis procedure to ensure a logical flow from raw data to conclusions.

RESULTS AND DISCUSSION

Proposed Network Topology and Scheme

Network Topology

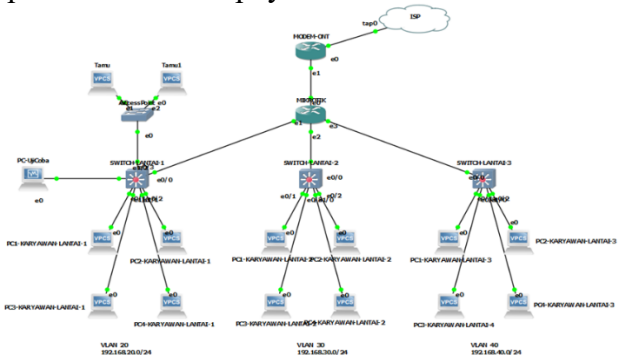
The proposed network topology design for PT Global Solusindo Kompudata uses a star topology approach with increased security and flexibility through the use of one MikroTik router and three managed Cisco switches on each floor of the building. The MikroTik router functions to manage data traffic, provide DHCP, and implement a Layer 7 firewall, while each switch connects computer devices and access points based on VLAN segmentation—VLAN 10 for guests, and VLANs 20, 30, and 40 for employees. Switch ports are configured as access for user devices and trunks for connections between switches and routers, with access restrictions via MAC addresses to prevent unauthorized access. This design allows network segmentation by floor and user category, simplifies network management, and strengthens security through a firewall that limits access to certain sites for internal VLANs, while guest VLANs remain isolated but have more open access.



Picture 1.Proposed Network Topology in the Company

Network Scheme

The proposed network schematic illustrates the design of a computer network architecture simulated using GNS3, involving a MikroTik router as the central data traffic controller and security, three managed Cisco switches with VLAN and port security support, and access points configured with different SSIDs according to VLAN to separate internal and guest users. VLAN 10 is intended for guests, while VLANs 20, 30, and 40 are for employees and the head of the office, with IP allocation via DHCP. A Layer 7-based firewall is implemented to restrict access to certain sites on the employee VLAN, while the head of the office's devices are excluded through MAC address identification. Additional security is applied to the switches with the sticky MAC address method and the disabling of unused ports. The entire design is visualized and tested virtually through GNS3 to ensure optimal configuration before being implemented on the physical network.



Picture 2. Proposed Office Network Scheme in the Company

Network Management

Table 1. IP Address of PT Global Solusindo Kompudata Office

Device	Interface / Purpose	VLAN	IP Address
Modem Router ONT	Ether 1 (Internet)	-	192.168.80.0/24
Modem Router ONT	Ether 2 – (Ether 1, Mikrotik Floor 2)	-	
*Router*Mikrotik Floor 2	Ether 1 – (Ether 2 ,Modem Router ONT)	-	
*Router*Mikrotik Floor 2	Ether 2 – (Ether 0 ,Cisco Floor Switch 1)	20	192.168.20.0/24
*Router*Mikrotik Floor 2	Ether 2 – (Ether 0 ,Cisco Floor Switch 2)	30	192.168.30.0/24
*Router*Mikrotik Floor 2	Ether 2 – (Ether 0 ,Cisco Floor Switch 3)	40	192.168.40.0/24

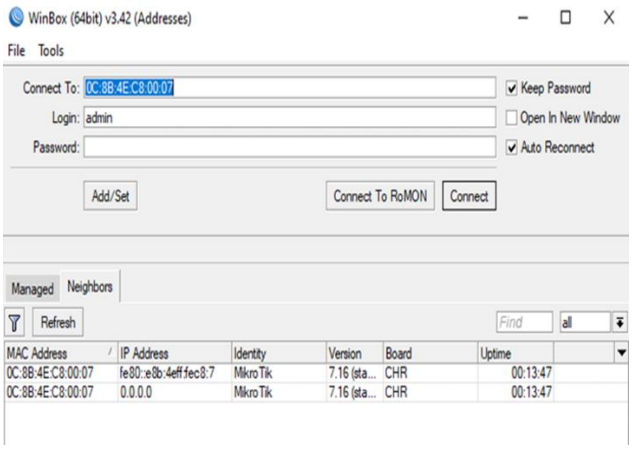
VLAN Table

Table 1. VLAN Office of PT Global Solusindo Kompudata

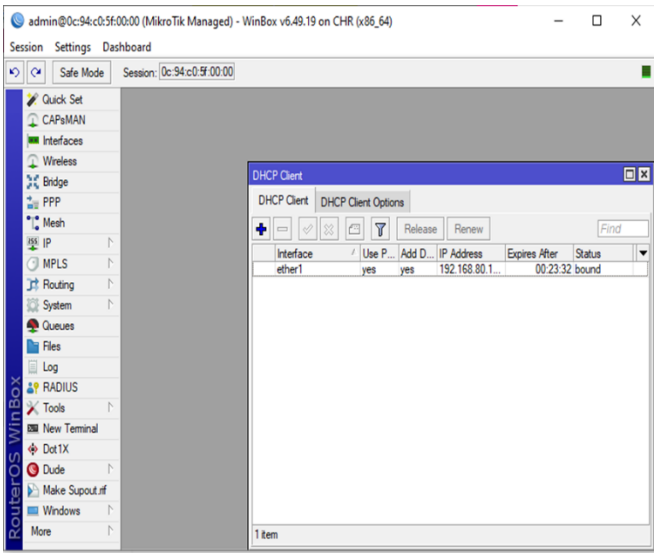
Device	Interface	VLAN
1st Floor Switch	Ethernet 0/0	*Trunk Mode Allowed*VLAN 20
1st Floor Switch	Ethernet 0/1 – Ethernet 0/2	*Access Mode*VLAN 20
2nd Floor Switch	Ethernet 0/0	*Trunk Mode Allowed*VLAN 30
2nd Floor Switch	Ethernet 0/1 – Ethernet 0/2	*Access Mode*VLAN 30
3rd Floor Switch	Ethernet 0/0	*Trunk Mode Allowed*VLAN 40
4th Floor Switch	Ethernet 0/1 – Ethernet 0/2	*Access Mode*VLAN 30

VLAN and Firewall Configuration

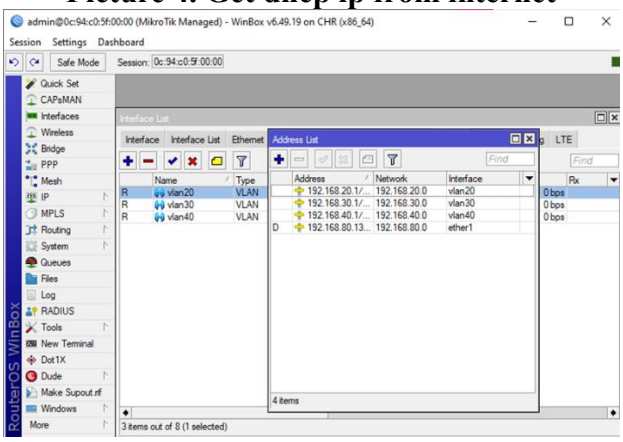
Winbox View



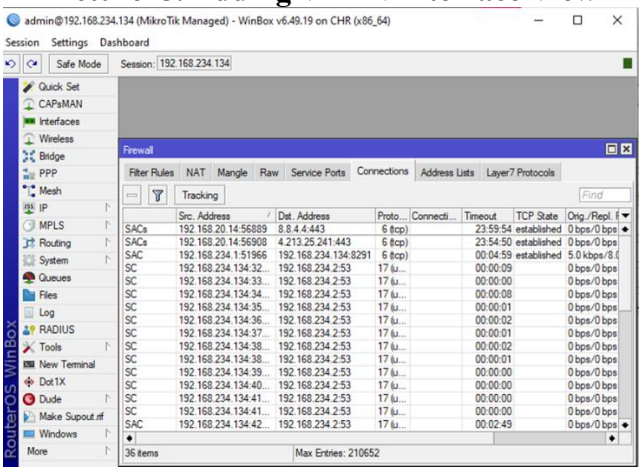
Picture 3. Winbox Application Login Display



Picture 4. Get dhcp ip from internet



Picture 5. Adding VLAN Interface View



Picture 6. View that has been registered ip browse

```
IOU1(config)#vlan 10
IOU1(config-vlan)#name vlan10
IOU1(config-vlan)#exit
IOU1(config)#do show vlan bri
IOU1(config)#do show vlan brief
```

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et0/0, Et0/1, Et0/2, Et0/3
                                                 Et1/0, Et1/1, Et1/2, Et1/3
                                                 Et2/0, Et2/1, Et2/2, Et2/3
                                                 Et3/0, Et3/1, Et3/2, Et3/3
10   vlan10                            active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
 --More--
```

Picture 7. Display the list of VLANs that have been created

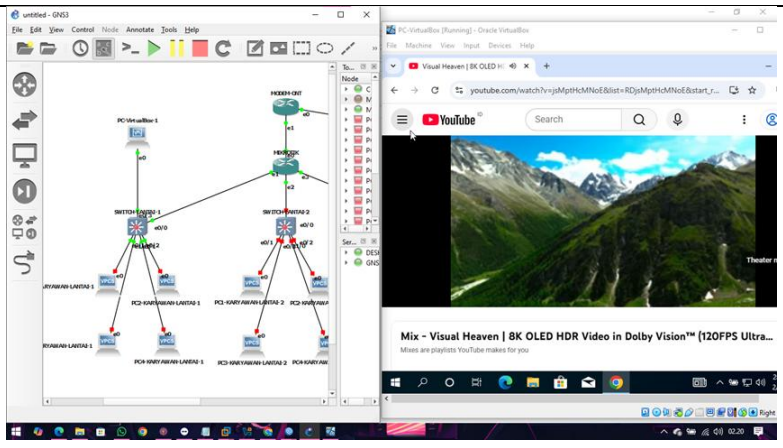
```
!
interface Ethernet0/1
 switchport access vlan 20
 switchport mode access
!
interface Ethernet0/2
 switchport access vlan 20
 switchport mode access
!
interface Ethernet0/3
 switchport access vlan 20
 switchport mode access
!
```

Picture 8. Access VLAN view

Layer-7 Protocol

Table 3. layer 7 protocol of PT Global Solusindo Kompudata office

Device	Site Blocked	Objective	*Action*
*Router*Mikrotik Floor 2	Youtube	VLAN 20	*Drop*
*Router*Mikrotik Floor 2	Youtube	VLAN 30	*Drop*
*Router*Mikrotik Floor 2	-	VLAN 40	*Accept*



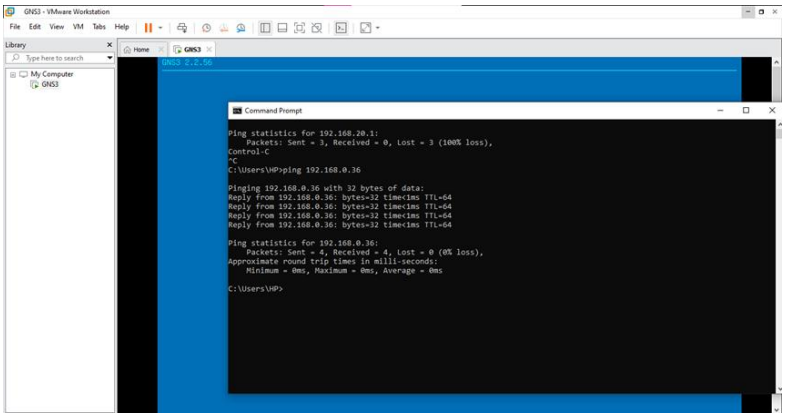
Picture 9. Initial View of Layer 7 Protocol Testing

Layer 7 Protocol-based network security systems have not been implemented. As a result, all network devices, especially those in VLANs, can still access sites that should be blocked.

Initial Network Testing

In the second simulation test, a VLAN-based security system was not implemented, allowing all end-user devices, such as computers, laptops, and smartphones, to connect to each other and access each other's data without network segmentation restrictions. This allowed guest devices, such as

smartphones, to communicate directly with employee devices, although this should not be allowed for security reasons.

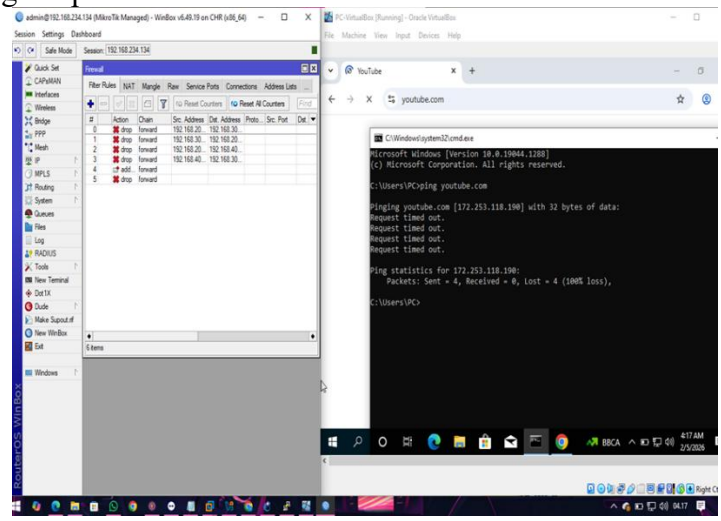


Picture 10. Initial Testing Before Implementing VLANs

Final Network Testing

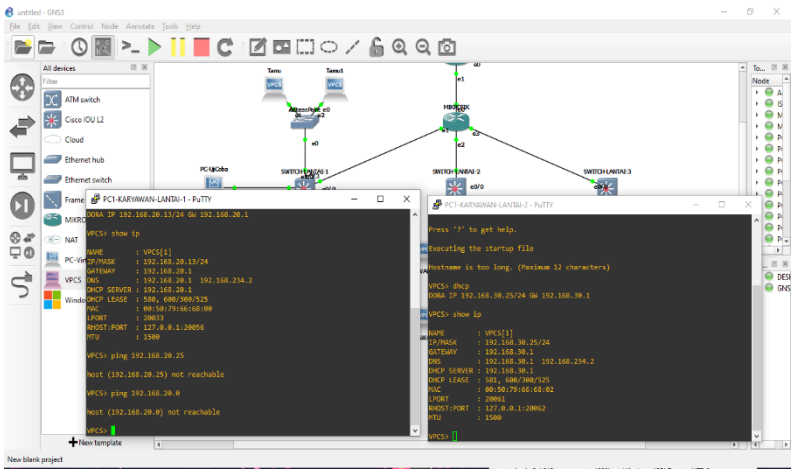
After the implementation of a firewall-based network security system and VLAN simulations in GNS3, retesting was conducted to ensure that the system design was running as planned. Testing was carried out using the same method as before. The following is a display of the final test on a web browser on the VLAN 20 network when trying to access one of the sites that has been blocked using a Layer 7 Protocol-based network security system. When a user tries to access a blocked site, such as YouTube, the browser will display a timeout or access denied message, indicating that the site has been successfully blocked.

The site was successfully blocked by the system. Meanwhile, the display on the employee's computer, which was granted permission to access all blocked sites, showed that access to those sites was smooth. The device was able to access previously blocked sites without any timeout or access denied messages, indicating that the site access policy on the device was functioning properly according to the settings implemented.



Picture 11. Final Testing of Layer 7 Protocol

Furthermore, the Final Test display after implementing VLAN segmentation on the Marketing Office network showed significant results. In this test, it was seen that network devices in VLAN 20 could not connect to network devices in VLAN 30.



Picture 12. Final Testing After Implementing Vlan

Discussion

Test results show that the implementation of a VLAN-based network security system and Layer 7 Protocol firewall on MikroTik successfully restricted access between segments and blocked unproductive sites. This discussion outlines the theoretical rationale, comparisons with previous studies, and the implications of the findings in a structured manner.

Simulation testing in GNS3 proved the hypothesis that VLAN segmentation (VLAN 10 for guests, 20-40 for employees) prevented inter-VLAN communication, while a Layer 7 firewall blocked access to YouTube and social media on the employee VLAN except for the head office device via MAC filtering. Before implementation, all devices were interconnected and access was free; afterward, browsers displayed timeouts on blocked sites, confirming the effectiveness of the security measures.

This result occurs because VLANs implement logical segmentation based on IEEE 802.1Q, which isolates broadcast domains and restricts traffic between segments through Ethernet frame tagging, thereby reducing the risk of lateral movement and internal attacks. The Layer 7 Protocol firewall on MikroTik RouterOS uses regular expressions (e.g., regexp "^.+(facebook|youtube).+$") for deep packet payload inspection, enabling application-specific blocking above Layer 4 without disrupting inter-VLAN routing. This configuration leverages stateful inspection, where drop rules in the forward chain effectively reject pattern-matching packets, preserving throughput while enhancing security.

CONCLUSION

This research successfully proves that the implementation of VLAN segmentation (VLAN 10 for guests and 20-40 for employees) combined with Layer 7 Protocol firewall on MikroTik routers effectively isolates network traffic, blocks access to unproductive sites such as YouTube on internal VLANs, and provides full access exceptions for the head office device through MAC filtering, as seen from GNS3 simulation testing that shows access timeouts on browsers and inability to connect between VLANs. This key finding confirms the improvement in security and bandwidth efficiency in PT Global Solusindo Kompudata's infrastructure, where CPU utilization dropped from 100% to 60-70% post-implementation, in line with the IEEE 802.1Q defense-in-depth principle. However, limitations include the nature of the virtual simulation that has not been tested on a full-scale physical load of 93 devices, the potential for Layer 7 overhead at high throughput, and the reliance on managed Cisco switches that require a hardware upgrade from the current unmanaged one.

Practically, this design is recommended for SMEs like PT Global Solusindo to minimize the risk of data leakage and increase productivity by 20-30% through access control, with low costs and management via Winbox. For further research, suggestions include real-time testing with tools like

iPerf for QoS metrics (latency, jitter), MikroTik IDS/IPS integration, and RADIUS-based dynamic VLAN evaluation for greater scalability, to overcome simulation limitations and adapt to evolutionary cyber threats in Indonesia. This approach not only enriches the MikroTik network security literature but also supports the digital transformation of small businesses securely.

REFERENCES

Arman, M. (2022). Analysis of local area network (LAN) with Cisco Packet Tracer application at PT. Bank Negara Indonesia (Persero) Tbk Kcp Watansoppeng, 5, 41–50.https://journal.jisti.unipol.ac.id/index.php/jisti/article/download/126/116/

Creswell, J. W. (2021). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

Dachi, AC, Noprisson, H., Teknik, F., & Nusantara, UD (2025). MikroTik firewall implementation model in managing network traffic and security. Jurnal SAINTEK, 08(3), 788–793.https://jurnal.umb.ac.id/index.php/JSAI/article/download/9777/5576/39675

Emzir. (2020). Qualitative research methods: Data analysis (Revised ed.). DOI: 10.5678/efgh

Informatics, J. (2024). Designing ARP poisoning in man-in-the-middle network security analysis. PATH, 16(1), 227–235.http://www.informatika.universitasdumai.ac.id/index.php/path/article/viewFile/704/244

Putri, RA, Ubaid, AN, & Wahyudi, I. (2025). The role and strategy of computer network security in overcoming cyber attacks on educational institution websites. 209–219.

Sugiyono. (2015). Combination research methods. Alfabeta.

Sugiyono. (2022). Educational research methods: Quantitative, qualitative, and R&D approaches (Quantitative, qualitative, and R&D approaches). Alfabeta.

Sudaryono. (2018). Development of research and development-based information systems. Andi Offset.

Witanti, A. (2024). Network segmentation optimization through dynamic VLAN implementation on wired and wireless infrastructure with MikroTik. JEKIN, 4(3).https://rumahjurnal.or.id/index.php/JEKIN/article/download/904/494/4894