Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th February 2025. Vol. 4. No. 2; e-ISSN: 2808-4519

Applying Sticky and Violation Shutdown Mode on Security Port Switch for Security Wan Infrastructure Network

Ikhsan Prasetya Ritonga[1]*, Ilham Faisal[2], Tengku Mohd.Diansyah[3]

[1,2,3] *Universitas Harapan Medan*
ghcikhsan@gmail.com [1*]

Abstract

Network security is a crucial aspect of managing information technology infrastructure. The risk of network threats, such as data theft and operational disruptions, increases as access points proliferate. One technique to mitigate these risks is port security. This study aims to implement and evaluate the effectiveness of switch port security in enhancing security within a Wide Area Network (WAN) infrastructure. The port security feature is configured using sticky mode and violation shutdown, allowing the recognition and authorization of legitimate devices based on their Media Access Control (MAC) addresses. A simulation using Cisco Packet Tracer was conducted to test this approach, where port security was applied to prevent unauthorized access. The results show that switch port security with sticky mode and violation shutdown effectively identifies and blocks unauthorized devices. When a device with an unknown MAC address attempts to access the network, the switch automatically disables the corresponding port, ensuring that only authorized devices can connect. The process of recovering disabled ports also proved to be quick and straightforward for network administrators. In conclusion, the implementation of switch port security in WAN infrastructure significantly strengthens network security, protects data from unauthorized access, and ensures optimal network availability and performance.

Keywords: *Switch Port Security, Sticky Mode, Violation Shutdown, Network Security, WAN Infrastructure*

1. Introduction

In the increasingly advanced digital era, network security has become a very important aspect in managing information technology infrastructure. A Wide Area Network (WAN) network that connects various geographic locations of different companies, educational institutions, or organizations, enabling fast and efficient data exchange and communication. There are several techniques that can be attempted to minimize the level of crime in the network, including port blocking and firewall filtering methods[1]. Implementing network security with switch port security on WAN infrastructure is a strategic step to strengthen network defense. Switch port security is a feature available on network switches that allows administrators to control what devices can connect to the network via switch ports. By configuring this feature, administrators can prevent unauthorized access and reduce the risk of attacks from unknown devices. This research will utilize Cisco Packet Tracer as a simulation tool to implement and test switch port security on WAN infrastructure.

Cisco Packet Tracer is network simulation software that allows users to create, configure, and test computer networks without the need for physical hardware. The use of Cisco Packet Tracer allows this research to simulate real-world scenarios in a controlled and secure environment. Through this simulation, research will evaluate the effectiveness of switch port security in preventing unauthorized access and identify potential problems that may arise during the implementation process. It is hoped that the results of this simulation can provide practical guidance for network administrators in improving network security and reliability. Thus, this research aims to address the critical need for reliable network security in WAN infrastructure, which will ultimately support safer and more efficient operations for organizations that adopt this technology.

2. Theoritical Basic

2.1. Basic Network Concepts

Computer network security as part of a system is very important to maintain the validity and integrity of data and ensure the availability of services for its use. A computer network is an absolute thing in building a network. Basically, the security system owned by the operating system is not enough to secure a computer network[2].Therefore, we need a system that can overcome threats that may occur optimally quickly and automatically so that it allows administrators to access the system even if network malfunctions occur. This will speed up the process of dealing with disruptions and restoring systems or services.

2.2. Network Devices

Network devices are all computers and additional devices connected to a computer network system to carry out data communications. The network devices used in this research include network cables, switches and routers. Further details regarding the network devices used in this research will be explained in the next sub-chapter.

2.3. TCP/IP Protocol

Universal computer language standards have been developed since 1969, consisting of a series of communication protocols called Transfer Control Protocol (TCP) which is responsible for controlling data packet transmission, error correction and data compression and Internet Protocol (IP) which is responsible for identifying and introducing data packet to the destination address[3]. The network protocol that is widely used today is the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol, which is a group of protocols that regulate computer data communication on the internet. Computers connected to the internet communicate using TCP/IP, because they use the same language, differences in computer type and operating system are not a problem. So if a computer uses the TCP/IP protocol and is connected directly to the internet, then that computer can connect to any computer connected to the internet[4].

2.4. DHCP Server

Implementing static IP addresses will have a negative effect on admin performance, which will take quite a long time if IP assignments are still done one by one. An effort to overcome this problem in reducing processing time is by implementing Dynamic Host Configuration Protocol (DHCP) to assign IP addresses automatically from the router. Network admins simply select DHCP or obtain IP address automatically when assigning an IP address[5]. A DHCP server is a network device that has the ability to provide or lend IP addresses to client computers connected to a network so that the computers can communicate. DHCP can help save on IP address usage because IP addresses no longer need to be assigned permanently to each client computer[6].

2.5. Network Security

Security is a very important element in computer networks. This is done in an effort to provide protection to computer networks to prevent threats, both internal and external, in an effort to prevent forced (unauthorized) data collection. A network security system needs to be built to control access to important assets, one of which is data, so that the access rights of each computer and user need to be regulated (Sartomo & Sulistyo, 2022).

2.6. Switch Port Security

Ports are the places where information enters and leaves a computer, port scanning identifies open doors to a computer. Ports have legitimate uses in managing networks, but port scanning can also be dangerous if someone is looking for weak access points to enter a computer[7]. The port itself is a part that can be said to be the entry and exit point for data on a computer[8].

2.7. Cisco Packet Tracer

Cisco Packet Tracer is an application created by the Cisco company located in San Francisco, California. Cisco was founded in 1984. Cisco Packet Tracer is a simulation tool used in learning computer networks, especially Cisco products. By using the Cisco Packet Tracer application, simulated network data can be used to provide information about the connection state of a computer in a network, if a problem occurs in the network interconnection[6].

3. System Analysis and Design

3.1. System Analysis

System analysis in this research is a crucial stage in network system development. This stage aims to understand in depth existing needs and problems, as well as to determine appropriate and effective solutions in overcoming various security threats. The main focus of this analysis is the implementation of network security through the use of switch port security on the WAN infrastructure. The main objective of this system analysis is to ensure that the proposed security solution, namely the implementation of switch port security, is able to meet the needs of the organization or company and functions effectively in protecting the network from potential security threats. Apart from that, this analysis is also intended to provide clear and structured guidance in the configuration and implementation process, so that it can make it easier for network administrators to secure the WAN infrastructure.

3.2. System Design

This section will discuss the planned network topology design from the implementation of sticky and violation shutdown modes on the port security switch for WAN infrastructure network security, as well as an explanation of the steps in the IP address distribution process and the port security switch configuration process at the city A branch office. and B city branch office.

3.2.1. Network Topology Design

Network topology design is an important step in implementing a secure and efficient network solution. In this research, we will use Cisco Packet Tracer to simulate the network topology implemented with Switch port security. This plan includes two main locations, namely the city A branch office and the city B branch office, which are connected via a WAN network, as shown in the figure 1.

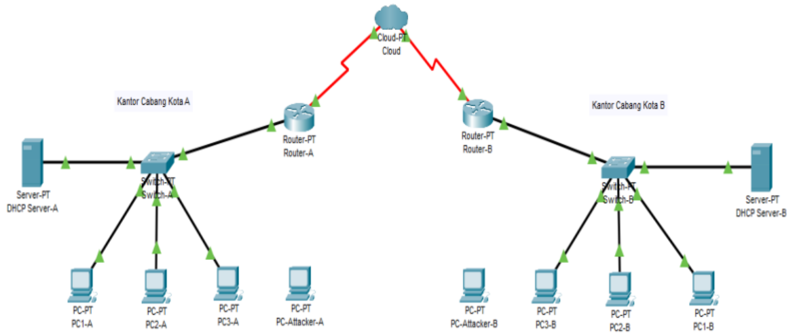

Fig. 1: Network Topology Design Used

Figure 1 shows the network topology that will be used in this research consisting of two cities, namely the city A branch office and the city B branch office, which are connected via a WAN (Wide Area Network) network represented by the cloud. Each city has a similar network infrastructure.

3.2.2. IP Address Configuration

Configuring the IP address on each device in the network topology in Figure 3.2 functions to ensure that each device has a unique identity and can communicate with other devices on the network. Referring to the network topology design explained in the previous chapter, at this stage, the IP address, subnet mask, and gateway are configured according to the planned network topology.

Table 1: IP Address Configuration

Device	***IP Address***	***Subnet mask***	***Gateway***
Kantor Cabang Kota A			
DHCP Server-A	192.168.1.1	255.255.255.0	192.168.1.254
Router-A (LAN)	192.168.1.254	255.255.255.0	-
Router-A (WAN)	10.0.0.1	255.255.255.252	10.0.0.2
PC1-A	192.168.1.2	255.255.255.0	192.168.1.254
PC2-A	192.168.1.3	255.255.255.0	192.168.1.254
PC3-A	192.168.1.4	255.255.255.0	192.168.1.254
PC-Attacker-A	192.168.1.5	255.255.255.0	192.168.1.254
Kantor Cabang Kota B			
DHCP Server-B	192.168.2.1	255.255.255.0	192.168.2.254
Router-B (LAN)	192.168.2.254	255.255.255.0	-
Router-B (WAN)	10.0.0.2	255.255.255.252	10.0.0.1
PC1-B	192.168.2.2	255.255.255.0	192.168.2.254
PC2-B	192.168.2.3	255.255.255.0	192.168.2.254
PC3-B	192.168.2.4	255.255.255.0	192.168.2.254
PC-Attacker-B	192.168.2.5	255.255.255.0	192.168.2.254

With this IP address configuration, the networks at the city A branch office and city B branch office will be able to communicate well via the WAN network, and each device will have an appropriate IP address configuration. Referring to figure 1, the network topology design designed for the city A office and city B office aims to provide a safe and efficient network using switch port security. With a structured physical and logical topology, as well as the implementation of appropriate security policies, networks in both locations can function properly and be protected from potential security threats. Implementation and testing will be carried out through simulation using Cisco Packet Tracer to ensure all configurations work optimally.

3.2.3. Implementation of Switch Port Security

A network security system using switch port security will be implemented on switches at each location. Switch port security policies include limiting the number of MAC addresses allowed for each port, as well as determining actions to be taken if a violation occurs, such as blocking the port. To simplify the explanation regarding the implementation of switch port security, a flowchart is used. A flowchart is a graphical representation of a process or workflow that shows the steps or decisions that must be taken to achieve a result. In implementing switch port security, flowcharts are very useful because they provide a clear and structured visual guide regarding how the network configuration and security process is carried out. By using flowcharts, the implementation process can be carried out more efficiently, accurately and systematically, ensuring that all security aspects are implemented correctly and the network is protected from threats.

3.2.4. Configure Switch Port Security

After the IP address configuration is complete, the next step is to implement network security using switch port security. Switch port security is a feature that allows network administrators to control access to the network by limiting the number and type of devices that can connect to the switch. To increase network security, switch port security configuration was carried out on the switches used in both branch offices. This implementation of switch port security aims to prevent unauthorized access to the network by only allowing known devices to connect. This is very important in maintaining network integrity and security, especially in a WAN environment that connects several different locations. Thus, system implementation includes IP address configuration steps to ensure effective communication between devices, as well as implementing switch port security to ensure that the network can be protected from unauthorized device access.

4. System Implementation and Testing

4.1. Implementation of System Requirements

Implementation of system requirements includes hardware and software. Implementation of these system requirements ensures that all elements needed to support the switch port security function have been prepared correctly, so that the main goal can be achieved, namely increasing network security on the WAN infrastructure. Implementation of this system requires a network switch device that supports port security features, a router that is compatible with the WAN infrastructure, as well as client and server computers for simulation. Each device must have adequate specifications to support the security features that will be implemented. In addition to hardware, software used for simulation and testing is also identified. Cisco Packet Tracer was chosen as the main tool for carrying out network simulations and testing switch port security configurations. The software allows visualization and testing of various scenarios, including access attempts by unauthorized devices.

4.1.1. Hardware Requirements

In implementing a network security system simulation with switch port security using Cisco Packet Tracer, adequate hardware is required. The hardware requirements used in this research consist of one computer/laptop unit for simulation and simulation network device requirements (in Cisco Packet Tracer). The following are the specifications for the hardware required:

1. Computer For Simulation
   The computer/laptop used to run Cisco Packet Tracer must meet minimum specifications to ensure optimal performance. The recommended specifications are as follows:
   a. Processor : Intel Core I3 or higher
   b. RAM : 4 GB or higher
   c. Memory : 2 GB or higher
   d. Graphic Card : VGA with a minimum screen resolution of 1366x768 or higher
   e. USB Port : for software installation or data storage if necessary.

2. Simulation Network Devices (In Cisco Packet Tracer)
   The component requirements used to simulate in Cisco Packet Tracer include:
   a. Router : 2 unit.
   b. Switch : 2 unit.
   c. PC : 6 unit.
   d. DHCP Server : 2 unit.
   e. Cable : Cable straight-through and crossover.

By meeting the hardware requirements above, the simulation of implementing switch port security in Cisco Packet Tracer can run well and effectively. Simulation using Cisco Packet Tracer allows testing and validation of configurations before deployment in real environments.

4.1.2. Software Requirements

In implementing a network security system simulation with switch port security using Cisco Packet Tracer, adequate software is also needed. The software requirements used in this research consist of Operating System software, Cisco Packet Tracer software, and supporting software. The following is an analysis of the software requirements required :

1. Operating System
   The computer/laptop used for the simulation must be running an operating system that is compatible with Cisco Packet Tracer. Microsoft Windows 11 (64-bit) will be used as the operating system in this research.
2. Cisco Packet Tracer
   Cisco Packet Tracer is the main software used for network simulation and Switch port security configuration. The recommended version is Cisco Packet Tracer 7.3.1 or a newer version.
3. Supporting Software
   For documentation and report creation purposes, the supporting software required includes Microsoft Word for report creation and documentation. Microsoft Visio for creating network topologies and flowcharts.

A summary of system requirements which includes software requirements in implementing network security using switch port security in this research can be presented in table 2.

Table 2: Software Requirements Summary

Need	Specs	Recommendation Specs
Operating System	*Windows* 7/8/10	*Windows* 11-64 *bit*
Cisco Packet Tracer	Versi 7.3.1	Versi 8.2.2
Word Processor	*Microsoft Word*	*Microsoft Word 2013*
Diagram and *Flowchart*	*Microsoft Visio*	*Microsoft Visio 2007*

By fulfilling the software requirements above, the simulation of implementing switch port security in Cisco Packet Tracer can run well and effectively.

4.2. Initial Network Testing

Initial network testing was carried out using the ping command by experimenting with network connections between each device at the city A branch office and devices used by different computers at the city B branch office. In this initial test, Cisco Packet Tracer software was used which had been routed and switched. Switches that are configured without using a security port. Test connected to the network and test ping to ensure every device on the network can communicate with each other. The expected result is that each device can respond to pings from other devices.

4.3. Test Results

Referring to the tests described previously in evaluating the effectiveness of implementing sticky and violation shutdown modes on switch port security in securing the WAN infrastructure network, where the tests were carried out by simulating attacks from unauthorized devices (PC-Attacker-A and PC-Attacker-B) to various destinations on the network, both on a LAN (local) and WAN (cloud) scale. The results of port security testing using the ping command at the city A branch office can be presented in table 3.

Table 3: Port Security Test Results at City A Branch Office

No.	Source	Destination	Packet Send	Packet Received	Packet Lost	Time	Status
Jaringan LAN (*Local*)							
1.		*PC1-A*	4	0	4	0 ms	*Failed*
2.		*PC2-A*	4	0	4	0 ms	*Failed*
3.	*PC-Attacker-A*	*PC3-A*	4	0	4	0 ms	*Failed*
4.		*DHCP-Server-A*	4	0	4	0 ms	*Failed*
5.		*Router-A*	4	0	4	0 ms	*Failed*
Jaringan WAN (*Cloud*)							
6.		*Router-B*	4	0	4	0 ms	*Failed*
7.		*DHCP-Server-B*	4	0	4	0 ms	*Failed*
8.	*PC-Attacker-A*	*PC1-B*	4	0	4	0 ms	*Failed*
9.		*PC2-B*	4	0	4	0 ms	*Failed*
10.		*PC3-B*	4	0	4	0 ms	*Failed*

Table 3 is the result of port security testing which aims to evaluate the effectiveness of implementing sticky and violation shutdown modes on port security switches in securing the WAN infrastructure network. Testing is carried out by simulating attacks from unauthorized devices (PC-Attacker-A) to various destinations on the network, both on a LAN (local) and WAN (cloud) scale. On the LAN network, the test results show that all attempts to send data packets from PC-Attacker-A to other devices such as PC1-A, PC2-A, PC3-A, DHCP-Server-A, and Router-A failed (failed). No packets were successfully received by the target device, with a packet loss rate of 100% and an average delivery time of 0 ms (milli second). These results indicate that unauthorized devices cannot access devices in the LAN network that have been protected by switch port security.

Tests on the WAN network also provide similar results. All attempts to send packets from PC-Attacker-A to devices at different locations, including Router-B, DHCP-Server-B, as well as PC1-B, PC2-B, and PC3-B, failed completely. No packets were successfully received by the destination device, which also indicates that port security is functioning effectively in preventing unauthorized access from the external network. Overall, the results of this test prove that implementing sticky and violation shutdown mode on switch port security is successful in protecting the network from the threat of unauthorized access, both on the LAN (local) network and the WAN (cloud) network. This implementation ensures that network security is maintained optimally.

The results of port security testing using the ping command at the city B branch office can be presented in table 4.

Table: Port Security Test Results at City B Branch Office

No.	*Source*	*Destination*	*Packet Send*	*Packet Recieved*	*Packet Lost*	*Time*	Status
Jaringan LAN (*Local*)							
1.		*PC1-B*	4	0	4	0 ms	*Failed*
2.		*PC2-B*	4	0	4	0 ms	*Failed*
3.	*PC-Attacker-B*	*PC3-B*	4	0	4	0 ms	*Failed*
4.		*DHCP-Server-B*	4	0	4	0 ms	*Failed*
5.		*Router-B*	4	0	4	0 ms	*Failed*
Jaringan WAN (*Cloud*)							
6.		*Router-A*	4	0	4	0 ms	*Failed*
7.		*DHCP-Server-A*	4	0	4	0 ms	*Failed*
8.	*PC-Attacker-B*	*PC1-A*	4	0	4	0 ms	*Failed*
9.		*PC2-A*	4	0	4	0 ms	*Failed*
10.		*PC3-A*	4	0	4	0 ms	*Failed*

Table 4 is the result of port security testing which aims to evaluate the effectiveness of implementing sticky and violation shutdown modes on port security switches in securing the WAN infrastructure network. Testing was carried out by simulating attacks from unauthorized devices (PC-Attacker-B) to various destinations on the network, both on a LAN (local) and WAN (cloud) scale. The port security test results at the city B branch office also gave similar results at the city A branch office. On the LAN network, the test results showed that all efforts to send data packets from PC-Attacker-B to other devices such as PC1-B, PC2-B , PC3-B, DHCP-Server-B, and Router-B failed. Tests on the WAN network also provide similar results. All attempts to send packets from PC-Attacker-B to devices at different locations, including Router-A, DHCP-Server-A, as well as PC1-A, PC2-A, and PC3-A, failed completely. No packets were successfully received by the destination device, which also indicates that port security is functioning effectively in preventing unauthorized access from the external network.

Based on the test results in table 3 and table 4, overall, the results of this test prove that the implementation of sticky and violation shutdown mode on switch port security is successful in protecting the network from the threat of unauthorized access, both on the LAN (local) network and the WAN (cloud) network). The overall results of this test indicate that the switch port security configuration using sticky and violation shutdown modes is effective in ensuring network security is maintained optimally.

4.4. Interpretation of Test Results

The interpretation of the results of network security testing by implementing sticky mode and shutdown violations on the WAN network infrastructure can be described as follows:

1. Violation Detection
   When PC-Attacker-A tries to connect to the port that has been configured for PC1-A, PC2-A, PC3-A and DHCP-Server-A, the Switch-A device will detect that the MAC address of PC-Attacker-A is different from Permitted MAC addresses (from PC1-A, PC2-A, PC3-A, and DHCP-Server-A). Likewise, when PC-Attacker-B tries to connect to the port that has been configured for PC1-B, PC2-B, PC3-B and DHCP-Server-B, the Switch-B device will detect the MAC address of the PC-Attacker. -B is different from the permitted MAC addresses (from PC1-B, PC2-B, PC3-B, and DHCP-Server-B). Thus, this is considered a port security violation.
2. Respons Switch
   In accordance with the violation mode shutdown setting, the switch device (Switch-A and Switch-B) will shut down the port that is experiencing the violation. The port will be in "err-disabled" (error-disabled) status, so it will not be able to send or receive any network traffic with all requests timed out, on the LAN (local) or WAN (cloud).
3. Port Status
   The breached port will be disabled and will need to be manually reactivated by the network administrator with the appropriate command, such as shutdown and then no shutdown.

Test results prove that port security with sticky and violation shutdown modes is effective in protecting the network from unauthorized devices. The switch device automatically disables the port when it detects a device with an unknown MAC address, preventing other devices (PC-Attacker-A and PC-Attacker-B) from accessing the network and communicating with other devices at the city A branch office and city B branch office , locally (on a LAN network) or cloud (on a WAN network). A completely failed ping test result confirms that the port has been successfully disabled by the port security feature.

This test shows the effectiveness of port security in protecting the network from unauthorized devices. With sticky mode, the switch learns and remembers the MAC addresses of authorized devices, and with violation mode shutdown, the switch ensures that only authorized devices can connect and operate through protected ports. If a breach occurs, the port will be disabled, thereby protecting network integrity and security. Thus, the use of port security is able to provide network security that can run well, so that if the device wants to reconnect, the MAC address on the switch must be deleted by the network administrator.

5. Conclusions and Suggestions

The conclusions that can be obtained from the results of implementation and testing of sticky and violation shutdown modes on switch port security for WAN infrastructure network security systems are as follows:

1. Implementing switch port security on WAN infrastructure has proven effective in increasing network security by limiting access to only authorized devices. By using the port security feature, each port on the switch can be configured to recognize and only allow devices with a certain MAC address. This will prevent unauthorized or unknown devices from accessing the network, reducing the risk of attacks such as unauthorized access.
2. Configuring switch port security with sticky and violation shutdown mode is an efficient way to secure the network. Sticky mode allows the switch to automatically learn and save the MAC address of the device first connected to the port, reducing the need for manual configuration. Meanwhile, violation mode shutdown shuts down ports automatically if a violation occurs, ensuring that unauthorized devices cannot communicate over the network. Configuration steps include: enabling port security on the switch, setting port security mode to sticky, setting violation action to shutdown, and configuring the maximum number of MAC addresses allowed.
3. The tests carried out show that implementing switch port security with sticky and violation shutdown modes is effective in preventing unauthorized access to the simulated WAN network infrastructure. When a device with an unknown MAC address tries to access the network, the switch automatically disables the port used by that device. This ensures that only authorized devices can operate within the network, maintaining the integrity and security of transmitted data. Simulations also show that after a breach, ports can be quickly restored by network administrators, ensuring network availability is maintained.

References

[1] D. Wicaksono, “Firewall Sistem Keamanan Jaringan Menggunakan Firewall dengan Metode Port Blocking dan Firewall Filtering,” *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 2, pp. 1380–1392, 2022, doi: 10.35957/jatisi.v9i2.2103.

[2] R. Hanipah and H. Dhika, “Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark,” *DoubleClick J. Comput. Inf. Technol.*, vol. 4, no. 1, p. 11, 2020, doi: 10.25273/doubleclick.v4i1.5668.

[3] R. Rahmat, R. Wiji Wahyuningrum, E. Haerullah, and S. Sodikin, “Analisis Monitoring Sistem Jaringan Komputer Menggunakan Aplikasi Spiceworks,” *PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 9, no. 1, pp. 44–52, 2022, doi: 10.30656/prosisko.v9i1.4671.

[4] A. Subki, M. N. Karim, and J. Juhartini, “PENGEMBANGAN JARINGAN HOTSPOT MENGGUNAKAN MIKROTIK ROUTERBOARD RB951Ui-2HnD PADA SMKN 2 SELONG,” *Explore*, vol. 10, no. 1, p. 14, 2020, doi: 10.35200/explore.v10i1.43.

[5] W. Sulistyo and S. Sartomo, "Model Keamanan Jaringan Menggunakan Firewall Port Blocking," *Krea-TIF J. Tek. Inform.*, vol. 10, no. 1, pp. 10–18, 2022, doi: 10.32832/kreatif.v10i1.6678.

[6] Z. Miftah, "Simulasi Keamanan Jaringan Dengan Metode Dhcp Snooping Dan Vlan," *Fakt. Exacta*, vol. 11, no. 2, p. 167, 2018, doi: 10.30998/faktorexacta.v11i2.2456.

[7] R. O. Nitra and M. Ryansyah, "Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen," *J. Sist. dan Teknol. Inf.*, vol. 7, no. 1, p. 52, 2019, doi: 10.26418/justin.v7i1.29979.

[8] K. Al Fikri and Djuniadi, "Keamanan Jaringan Menggunakan Switch Port Security," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 5, no. 2, pp. 302–307, 2021, [Online]. Available: http://bit.ly/InfoTekJar