JOURNAL OF DATA SCIENCE | Vol.2024:40
eISSN:2805-5160

Data-Driven on Resilient Network Security Against SYN Flood Attacks at PT PUSRI

Misinem [1], M. Syaiful Huda Mubarok [2], Timur Dalipurwanto [3], Tamsir Ariyadi [4] and Nurul Adha Oktarini Saputri [5]

[1,2,3,4,5] Faculty of Vocation, Universitas Bina Darma, Palembang, Indonesia

[*]**Email:** misinem@binadarma.ac.id

Abstract

The PT PUSRI Information Technology Services Department plays a vital role in supporting operations and providing IT services across the company. To ensure secure internet access, robust security measures have been implemented, with firewall filtering as a key strategy. This study analyzes the effectiveness of firewall filtering in mitigating threats such as SYN flood attacks and unauthorized access by focusing on data-driven insights into traffic patterns and threat prevention. The firewall filtering system scrutinizes incoming TCP connections, manages critical ports (e.g., ports 22 and 80), filters IP address ranges, and continuously monitors suspicious network traffic patterns. Data analysis of network activity revealed a significant reduction in security incidents. By blocking illegitimate traffic and managing commonly targeted entry points, the system has minimized disruptions caused by SYN flood attacks and unauthorized access attempts. Filtering source IPs associated with malicious activities and analyzing traffic anomalies further strengthen network security. The results demonstrate increased network stability and enhanced operational efficiency at PT PUSRI, with data indicating fewer disruptions and threats. The department's ability to analyze traffic patterns has enabled proactive threat mitigation, contributing to a secure IT environment. This research highlights the strategic importance of integrating data analysis into firewall filtering to sustain and improve network security while supporting seamless operational activities.

Keywords

Mikrotik, Firewall Filtering, Network Security Syn Flood

Introduction

The Internet network has become the backbone for the development of information technology. Both individuals, companies, and government agencies rely on the Internet to access information, communicate, and run various digital services. The internet also carries significant security risks. The manuscript contains a letter containing Threats to internet network security that can come from a variety of sources, including complex and serious cyberattacks such as data hacks, malware

Submission: 24 July 2024; **Acceptance:** 28 October 2024

attacks, and internet network service disruptions, which can cause financial losses, loss of important data, or even compromise the safety of network users.

According to data released by the Indonesian Internet Services Association (APJII) in 2024, it shows that internet users in Indonesia have increased to 221,563 people, indicating an increase of 1.4 percent compared to the previous year, which reached 215.63 million internet users, the percentage of Internet users was 79.5% from the total population of Indonesia. According to data compiled by the State Cyber and Cryptography Agency (BSSN), it shows that in 2021 from January to August 2021, there were cyber-attacks in Indonesia that caused many cases of data loss; this indicates that there are still many people who do not know how important the internet network security is. Therefore, increasing vigilance and taking appropriate precautions to protect the network and data from cyberattacks (Nuroji, 2023).

One of the most common threats is attacks, including the SYN Flood attack, one of the most common DDoS attacks. In the SYN Flood attack, the attack is carried out by sending many fake SYN connection requests to the target server, thus causing network resources to become unavailable to legitimate users. The impact of an attack on internet network security can be devastating, both economically and socially. For example, attacks on a company's network infrastructure can disrupt business operations, lose sensitive data, and damage reputation. In the public sector, attacks on health or security services can endanger human lives (Parawansa & Nurhadi, 2024). Protection against attacks and other internet network security threats must be implemented effectively to protect digital infrastructure and maintain the continuity of people's activities in cyberspace.

The Information Technology Services Department of PT PUSRI has access to a Computer Network that Facilitates Network Services for Interns and Employees. However, currently, the IT service department network often experiences service interruptions or downtime. This affects the performance of the interns and employees in the room and causes their work to be disrupted and work slower. The main cause of this disruption is a network disruption caused by an attack on the network, namely a SYN attack. Therefore, network improvement or optimization is needed. To block and prevent the abuse of illegal network access by hackers, it is necessary to improve the security of existing networks (Tambunan & Neyman, 2024).

One of the ways the author applies to ensure internet access security in the IT service department of PT PUSRI is to implement network security with the firewall filtering method. Firewall filtering is one of the main ways to protect the network from various attacks, such as SYN Flood attacks, DDOS attacks, brute force, and MITM attacks. Firewalls can be used to monitor, restrict, and block suspicious or malicious network traffic; implementing network security can ensure that internet network access can be used safely and efficiently (Haeruddin, 2021).

Methodology

The present study used the Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) process as its methodology. Novianto et al. (2022) state that the PPDIOO approach is essentially

a methodical set of tasks for problem-solving. The stages of this research, based on the PPDIOO model proposed by Haris et al. (2022), are as follows.

PPDIOO Method

Prepare

At this stage, the researcher will identify and understand in depth the SYN Flood attack and illegal access blocking techniques, including how they work and the impact on the network, and define the system needs in the form of hardware to meet the needs of supporting needs such as Mikrotik router devices, switches and other supporting needs (Mulyana, 2023).

Plan

At this stage, researchers have planned the data collection necessary to evaluate network security.

Design

In the next stage, the researcher designs the network and designs a test scheme on the network and attack response detection.

Implement

Implementation will be based on the design in the previous phase, including implementing network security against SYN Flood attacks, creating planned access controls for blocking illegal access, and testing the system.

Operate

The SYN Flood attack was tested in monitoring and control at this stage. Some of the indicators measured include:

1. Attack volume, such as the number of packets sent by a SYN Flood attack
2. Increased CPU due to SYN Flood attack
3. decreased network performance and increased network traffic

Optimize

At this stage, HASL obtained from the testing process and system maintenance are evaluated and analyzed to ensure proper and optimal functioning.

Data Collection

In writing this final work, the researcher carried out the following data collection techniques:

1. Observation is a series of steps or processes to collect data by directly observing the studied Object or phenomenon. At this stage, the author is looking for problems regarding the data that the author wants to observe. At this stage, the author interacts with PT's IT service employees. PUSRI Palembang, regarding matters related to the research to be carried out (Azizah & Veritawati, 2021).
2. The author obtained and understood data from theories related to the topics discussed in the final project research paper. Authors derive theories from magazines, articles, books, the internet, and other sources.

Research Design

The design of the research is very important. A research design refers to a comprehensive plan regarding all stages of research, from planning to evaluation (Khanday & Khanam, 2023). The research design aims to clarify the research objectives, provide direction in conducting the research, and provide an overview of the planning process and the research (Awal & Gusman, 2023).

1 Open the WINBOX app and log in to your Mikrotik device by entering its IP and MAC addresses.
2 Name the interface as needed
3 Configure IP addresses for each interface
4 Enable the NAT firewall on the internet interface and give it a masquerade action.
5 Enter Google DNS to check if the network is properly connected and connected to the internet.
6 Configure firewall rules in Mikrotik
7 An interface attack scheme is carried out by scanning an open protocol port and testing an SYN Flood.
8 Testing a SYN Flood attack without using a firewall
9 Displays the results of a SYN Flood attack without using a firewall
10 Save configures and tests the result of an SYN Flood.
11 Monitoring access and testing
12 The configuration and afterward test the configuration that has been performed
13 Add firewall rules to block illegal network access
14 Save the configuration and test the configuration

Network Topology

The author will display the network topology of PT PUSRI's IT service department, as shown in Figure 1 in the image below.

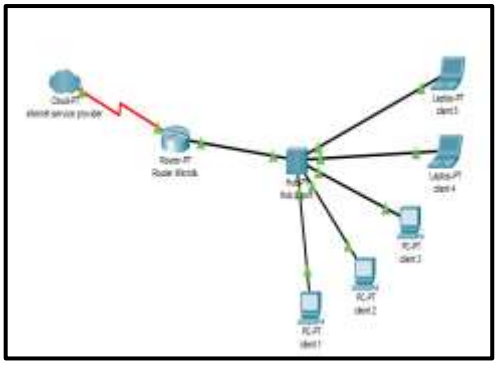

Figure 1 Network Topology

Topology and attack scheme

The topology and attack scheme in this study will be included in this study, which is intended so that the reader can understand the content of this study and make it easier to complete the research and as a guide for other research in referring to research studies (Khafif, 2021). The next stage will be an attack testing scheme, and IP addressing will be carried out, as shown in Figure 2.

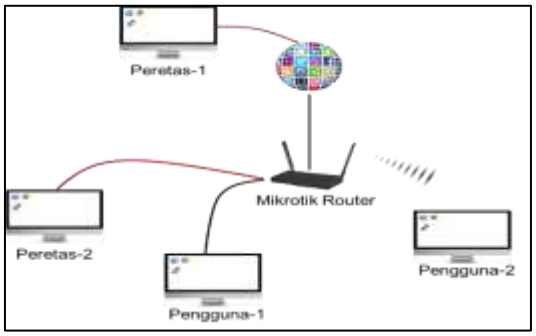

Figure 2. Attack Scheme

The following are the phases of the attack testing scheme in the IT services department as follow (Novianto et al., 2022):

1. The perpetrator will scan the open protocol port. Port scanning determines if a particular system port is open or closed. It lets users know if the system has open ports to access services such as TCP, UDP, FTP, and SSH (Jufri & Heryanto, 2021)
2. After scanning and getting information related to the open ports, the hackers will try to carry out a SYN Flood attack by utilizing the open tools and start targeting the target, namely on an internet router with an IP address of 10.10.19.185/2 and an IP address of 192.168.10.1.
3. The attacker sends an SYN packet to the router with an IP address of 10.19.185/24, continuously sending attack packets to flood the router's traffic.
4. After the network administrator realizes something is wrong with his network, he improves the network security system by creating a firewall, as shown in Table 2.

Table 2. IP Addressing

Device name	Interface	IP address	Description
Router	Either 1	10.10.19.185/24	Internet
User 1	Ethernet	192.168.10.1/24	Use with cable media
User 2	Wireless	192.168.1.1/24	Wireless media
Attacker 1	Ethernet		Hackers from the internet
Attacker 2	Ethernet		Hackers from local networks

Results and Discussion

This application is very necessary to know how the form of an attack from SYN Flood on network security and blocking illegal access, and the researcher will discuss the process of preventing and attacking Syn Flood (DDos Attack) on the network of the IT service department based on the Mikrotik OS router, in the prevention process the researcher uses the features in the Mikrotik router

by using the firewall filtering feature and For the attack process Researchers using the Linux operating (Sahren, 2021).

SYN Flood attack testing without a Firewall

At this stage, hackers will test the Syn Flood attack without using a firewall by targeting routers with IP addresses of 10.10.19.85/,24 and sending attack packages of 20000 data bytes. Here is the configuration: Open a Linux application running in a virtual box, enter the terminal, and type "./pentmenu." If you have entered the pentmenu tools view, select the dos > menu, select no 3, select SYN Flood, and then enter the desired target (Sahren, 2021), as shown in Figure 3.

Figure 3. PentMenu tools display

Figure 3 above shows that the hacker targeted the attack at *IP Address* 10.10.19.185 and then targeted port 80 by sending 20000 SYN attack data packets and 40 headers. This can cause the server to be unable to respond to requests quickly and become slow.

The results of the attack

Researchers will display the results of the SYN Flood attack before the firewall is applied. The results of the attack will be directly using the pentmenu tool. A SYN Flood attack is an attack that attacks packets on the network so that the network connection is disrupted, and the SYN Flood causes downtime by using a numbering attack, as shown in Figure 4.

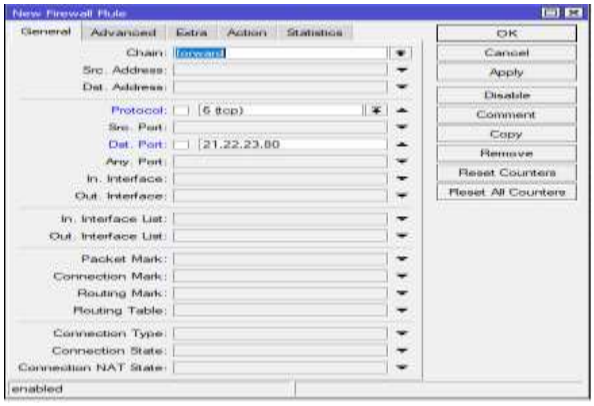

Figure 4. Network Improvement Chart

The network graph shows a significant increase at the time of the attack. It increased by 49.3 kbps to 174.2 kbps, increasing the CPU by up to 100%. The attack floods the server with SYN packets. Many SYN Flood attacks can disrupt the network, degrade server performance, and make it unresponsive.

Configure SYN Flood attack using a Firewall

At this stage, the researcher configured firewall filtering to prevent SYN Flood attacks. The preventive impact of SYN Flood attacks is positive, including improving network security, high service availability, accelerating network performance, and improving service quality.

Configure firewall filter rules by using the following configuration:
Select the IP > firewall menu > + select the general tab: chain, select forward, protocol, select 6 TCP, etc. port type 22, 80, connection state, select New, > advanced tab, Src address list, type DDoser, and select dst address list, type DDosed, > then enter the action menu, enter the Drop command, then click Apply and OK, as shown in Figure 5.

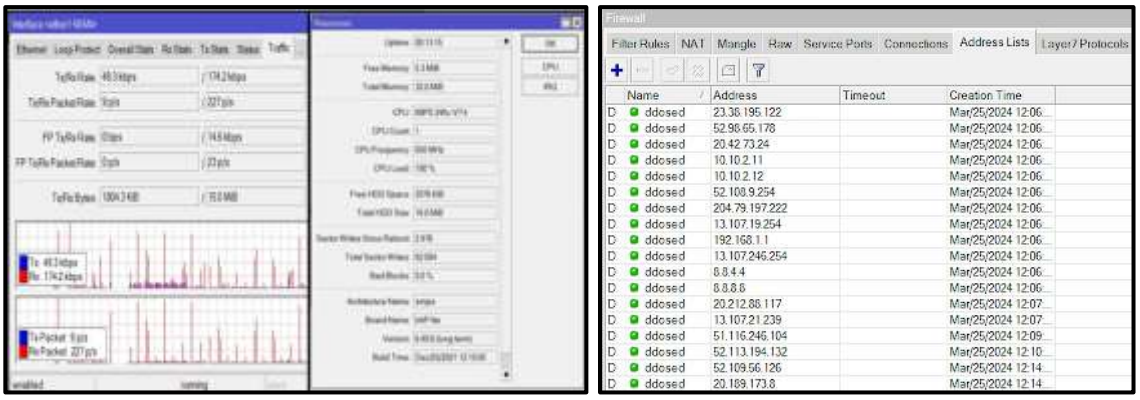

Figure 5. Firewall Filter Configuration

The image above displays the firewall filter rules configuration implemented into the firewall filtering network, which can overcome, block, and monitor the source of attacks accurately and precisely.

In Figure 5, select the advanced menu, select New, > the advanced tab, select Src address list, type DDoser, select dst address list, type DDosed, then enter the action menu, enter the Drop command, then click Apply and OK. The src address list menu is part of the firewall configuration in Mikrotik that allows you to create a list of specific source IP addresses that can be used in firewall rules. Using the src address list menu can specify a list of IP addresses that can be blocked. While the DST address menu is a list of destination IPs to be accessed, with firewalls, this list can filter and supervise data traffic entering the network.

With the above rule, when an attack occurs, and there is an abnormal SYN packet, the list address will combine the SYN packet with the names dosed and dose. Once the attacker's IP address and destination are successfully captured, the IP address will be dropped or blocked by the firewall that has been created. This way, client devices such as servers can be protected from SYN Flood attacks, and irresponsible actors can block illegal access.

Testing of SYN Flood using a Firewall

A SYN Flood attack will be tested after the firewall configuration is carried out on the IT service department's network. The attacker will attack the LAN network with the IP address 192.168.10.1 by entering the target port of 80 and the attack distribution of 2000 bytes of data.

This is a process of attack by a hacker that attacks a network. The hacker successfully carried out the attack. The image above shows that the hacker sent a SYN package of 2000 data bytes. The target IP Address was 192.168.10.1, and the hacker entered the target port 80.

Displays the IP address list of attackers

After the SYN Flood attack package is carried out, the author will display the results of capturing the attacker's IP address. This means that the network security configuration that has been created has been successful and is running well, as shown in Figure 6.

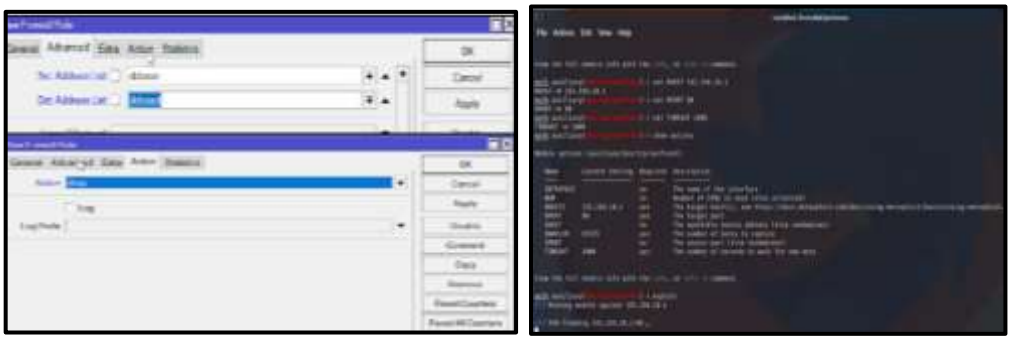

Figure 6. Captured IP address and listed IP address hacker

In the image above, the attacker's IP Address was successfully detected and caught after the firewall configuration was carried out. The address list feature allows network administrators to create a list of IP addresses considered the source of an attack if they are used to capture the IP addresses of a SYN Flood attack. Thus, administrators can easily block packets originating from those IP addresses, hindering SYN Flood attacks that can disrupt the network. With this feature, administrators can categorize IPs considered the source of attacks and block them effectively, reducing the likelihood of attacks and improving network security: display graphics and CPU.

Display graphic and CPU

Figure 7 shows that CPU usage decreased and network graphics improved after the firewall was implemented on the IT Services department's network.

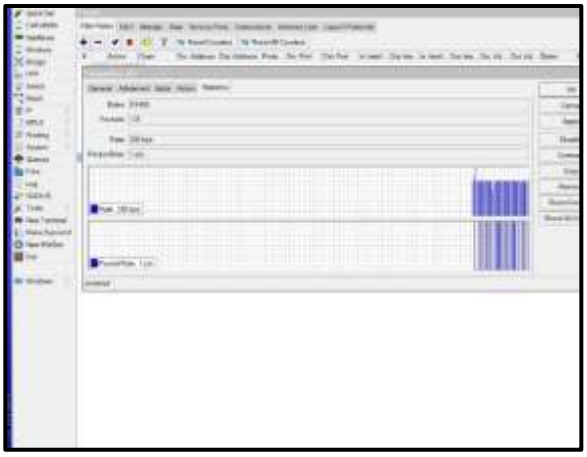

Figure 7. Display Network Graphics

Firewalls can help keep network performance stable and improve network security from unauthorized attacks by acting as filters that block unnecessary packets in a SYN Flood attack situation. The positive impact of the improved network graph and CPU with the firewall is that the network can continue to operate properly and not experience significant disruptions, allowing network usage to continue to function normally, as shown in Table 2.

Table 3. Attacking indicator

No	Indicator	Before using firewall	After using firewall
1	Volume packet	high	low
2	Server response	slow	fast
3	CPU		
4	Traffic network	high	low
5	Bandwidth	high	Low
6	Network	low	fast

Information:

- SYN Flood Attack Before Firewall Applies
- The volume of packets going to the server is very high
- causing the server to slow down and not be able to handle requests
- In addition, it makes CPU performance high up to 100%
- Making network traffic high due to attacks
- Bandwidth is also overused so that
- making network performance very slow and potentially network down or unavailable

Information:

- Syn Flood Attack After Firewall Applies
- The volume of packets entering the server is very low due to the implementation of the firewall.
- The server can respond to requests quickly.
- After applying the firewall, the CPU is getting better and running normally. The firewall causes network traffic to continue to operate properly and not experience significant disruptions,
- After applying the firewall, the bandwidth condition runs normally
- So that it makes network performance fast and optimal

Conclusion

The study highlights the effectiveness of firewall filtering in mitigating SYN Flood attacks and enhancing network security within PT PUSRI's IT services. By leveraging the firewall's capabilities to filter and monitor network traffic, the organization has successfully addressed vulnerabilities and reduced risks associated with unauthorized access and network disruptions. Integrating preventive measures, such as identifying and blocking suspicious IP addresses and managing critical ports, has significantly improved network performance and reliability. These advancements have ensured the availability of services and optimized resource utilization,

fostering a secure and efficient IT environment.

The findings emphasize the critical role of robust network security strategies in safeguarding digital infrastructure and mitigating cyber threats. Organizations are encouraged to adopt similar approaches to enhance their resilience against evolving cyberattacks, ensuring continuity and stability in their operations. Future research could further explore advanced techniques for automated threat detection and response to enhance network security systems.

References

Awal, H., & Gusman, A. P. (2023). Implementasi Intrusion Detection Prevention System Sebagai Sistem Keamanan Jaringan Komputer Kejaksaan Negeri Pariaman Menggunkan Snort Dan Iptables Berbasis Linux. *Jurnal Sains Informatika Terapan*, *2*(1), 38–44. https://doi.org/10.62357/JSIT.V2I1.184

Azizah, U., & Veritawati, I. (2021). IMPLEMENTASI MANAGEMENT BANDWIDTH MENGGUNAKAN METODE QUEUE TREE DENGAN PCQ (PER CONNECTION QUEUE). *Journal of Informatics and Advanced Computing (JIAC)*, *2*(1), 2021. https://journal.univpancasila.ac.id/index.php/jiac/article/view/2687

Haeruddin, H. (2021). Analisa dan Implementasi Sistem Keamanan Router Mikrotik dari Serangan Winbox Exploitation, Brute-Force, DoS. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *5*(3), 848–855. https://doi.org/10.30865/MIB.V5I3.2979

Haris, A., Riyanto, B., Surachman, F., & Ramadhan, A. (2022). Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. *Komputika : Jurnal Sistem Komputer*, *11*, 67–76.

Jufri, M., & Heryanto, H. (2021). PENINGKATAN KEAMANAN JARINGAN WIRELESS DENGAN MENERAPKAN SECURITY POLICY PADA FIREWALL. *JOISIE (Journal Of Information Systems And Informatics Engineering)*, *5*(2), 98–108. https://doi.org/10.35145/JOISIE.V5I2.1759

Khafif, F. (2021). PENINGKATAN PELAYANAN INTERNET MENGGUNAKAN MIKROTIK DAN SOFTWARE WINBOX DI PTIPD UIN WALISONGO SEMARANG. *Prosiding Seminar Nasional*, *3*(1), 264–267. https://e-journal.akpelni.ac.id/index.php/prosiding-nsmis/article/view/213

Khanday, S., & Khanam, D. (2023). *THE RESEARCH DESIGN*. *Journal Critical Reviews*, Vol.06(03), 376.

Mulyana, A., (2023). “PERANCANGAN WEB FILTERING DENGAN METODE FIREWALL FILTER RULES PADA JARINGAN KOMPUTER PT. INTI PAKET PRIMA BERBASIS MIKROTIK ROUTEROS,” *Incomtech*, vol. 12, pp. 1–10, Dec. 2023.

Novianto, D., Setiawan Japriadi, Y., Tommy, L., (2022). Implementasi Keamanan Akses Terhadap Website Menggunakan Wireguard VPN Di Routerboard Mikrotik. *Jurnal Ilmiah Informatika Global*, *13*(2). https://doi.org/10.36982/JIIG.V13I2.2308 https://doi.org/10.34010/komputika.v11i1.5227

Nuroji, (2023). Penerapan Intrusion Detection and Prevention System (IDPS) pada Jaringan komputer sebagaipencegahan serangan Port-Scanning, *Journal of Data Science and Information System (DIMIS)*, vol. 1, pp. 1–9, 2023, doi: 10.58602/dimis.v1i2.35.

Parawansa, K.I., Nurhadi, A., (2024). ANALISIS SYN FLOOD ATTACK MENGGUNAKAN METODE NIST 800-61 REV 2 PADA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM). *INFORMATIKA SAINS TEKNOLOGI*, *2*(1), 1–8. https://uia.e-journal.id/INSIT/article/view/3134

Sahren, S. (2021). *IMPLEMENTASI TEKNOLOGI FIREWALL SEBAGAI KEAMANAN SERVER DARI SYN FLOOD ATTACK | Sahren | JURTEKSI (Jurnal Teknologi dan Sistem Informasi)* Vol. 7(2). https://jurnal.stmikroyal.ac.id/index.php/jurteksi/article/view/933

Tambunan, M. R. H., & Neyman, S. N. (2024). Implementasi Firewall pada Linux untuk Pencegahan Dari Serangan DoS. *Journal of Technology and System Information*, *1*(4), 10–10. https://doi.org/10.47134/JTSI.V1I4.2648