|Jurnal Jaringan Komputer dan Keamanan |JJKK|Vol. 6| No. 2|June|Year 2025|
This is an Open Access article, published by Institute of Information Technology and Social Science (IITSS), Indonesia

Implementation of a Network Security System Against SYN Flood Attacks and Unauthorized Access Blocking Using Firewall Filtering in the IT Service Department of PT Pupuk Sriwidjaja Palembang

M. Syaiful Huda Mubarok[1*]

Abstract

The Information Technology Services Department of PT Pupuk Sriwidjaja (PUSRI) Palembang relies heavily on internet network access to support a wide range of operational activities and to provide Information Technology (IT) services for various departments within the company. However, internet access within the IT Services Department must be tightly regulated and secured. One of the network security mechanisms applied is the firewall filtering method. Firewall filtering is used to protect network systems from SYN Flood attacks, prevent unauthorized access, and block potential threats from hacker activities. The firewall filtering mechanism inspects all incoming TCP connections, opens or blocks network ports such as ports 22 and 80, and filters source IP addresses, port ranges, and suspicious traffic patterns. By implementing a network security system against SYN Flood attacks, the network becomes more stable and secure and can operate normally without concerns about SYN-based disruptions or other forms of illegal access.

Keywords

Mikrotik, firewall filtering, network security, SYN Flood.

Article History
Received 15 April 2025
Accepted 23 June 2025

How to Cite

Ardiansyah. (2025). Implementation of a Network Security System Against SYN Flood Attacks and Unauthorized Access Blocking Using Firewall Filtering in the IT Service Department of PT Pupuk Sriwidjaja Palembang. ***Jurnal Jaringan Komputer dan Keamanan**, 6*(2), 78-86.

[1*] Universitas Bina Darma, Indonesia, Corresponding email: syaifulhuda@gmail.com

Introduction

The internet has evolved into a fundamental backbone for global information technology development, enabling seamless connectivity across individuals, corporations, and government institutions. Its widespread adoption has transformed how people access information, communicate, and operate digital services across numerous sectors. Daily activities—ranging from online transactions and cloud computing to data sharing and remote work—depend heavily on stable and secure network infrastructures. However, alongside these advances, substantial risks have emerged, particularly in the realm of cybersecurity. Threats such as data breaches, malware infections, unauthorized intrusions, and large-scale service disruptions illustrate the growing complexity of cyberattacks in the digital age.

In Indonesia, the increasing reliance on the internet is reflected in the rising number of internet users. The Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) reported that by 2024, internet penetration had reached 221.563 juta pengguna, marking an increase of 1.4% from the previous year. While this growth supports digital transformation across sectors, it simultaneously expands the potential attack surface for cybercriminals. Reports from the Badan Siber dan Sandi Negara (BSSN) indicate that Indonesia continues to experience numerous cyberattacks, with significant incidents of data loss recorded between January and August 2021. These findings underscore persistent gaps in public awareness and institutional readiness regarding network security (Nuroji et al., 2023).

Among the various cyber threats, the SYN Flood attack is recognized as one of the most common and disruptive forms of Distributed Denial-of-Service (DDoS) attacks. A SYN Flood attack works by sending massive volumes of spoofed SYN requests to a server to exhaust its resources and prevent legitimate connections. These attacks can destabilize network performance, overwhelm firewalls, and even render critical systems inoperable. As highlighted by Indar Parawansa et al. (2024), such disruptions do not merely affect digital operations—they also create severe economic, social, and organizational repercussions. In sectors such as healthcare, transportation, and public security, the consequences may escalate toward threats to human safety.

Recognizing these risks, implementing strong and effective network security mechanisms has become essential. Core protections, including firewalls, intrusion detection systems, antivirus solutions, and robust authentication protocols, act as defensive layers to maintain the confidentiality, integrity, and availability of information systems. These measures are also designed to prevent unauthorized access, detect suspicious traffic behavior, and minimize the risk of operational failures. However, the sophistication of modern attacks requires continuous enhancement of defensive technologies and proactive monitoring strategies.

Within this context, the IT Service Department of PT PUSRI Palembang faces a critical challenge. The department provides essential computer network access for employees and interns, supporting daily business operations across the organization. Yet, frequent service interruptions and periods of downtime have severely impacted performance and productivity. Initial assessments indicate that these disturbances are primarily triggered by SYN Flood attacks, which overload network resources and disrupt internal connectivity. As a result, employees experience slow response times, unstable services, and temporary loss of access to critical applications.

Given the significant implications of these disruptions, urgent improvements in network security and optimization are required. To prevent unauthorized access, mitigate SYN Flood attacks, and ensure stable network performance, the IT Service Department must strengthen its infrastructure with advanced protection mechanisms, including enhanced firewall filtering, traffic monitoring, and packet inspection. By reinforcing network defenses, the organization can preserve operational continuity, protect digital assets, and support a safer and more resilient technological environment.

Methodology

PPDIOO Method

The research applies the PPDIOO methodology, an acronym for Prepare, Plan, Design, Implement, Operate, and Optimize, developed by Cisco. This methodology provides a systematic sequence of steps for identifying and solving network-related problems (Novianto et al., 2022).

Prepare

This stage involves identifying and understanding SYN Flood attacks and illegal access mechanisms. Hardware and software requirements are also assessed, including Mikrotik routers, monitoring servers, switches, Winbox Tools, Zenmap, Pentmenu, Metasploit, and Kali Linux.

Plan

Data collection planning is carried out to evaluate network security conditions and determine the analysis scope.

Design

The network design phase includes creating testing schemes, configuring security mechanisms, and defining detection and response strategies for SYN Flood attacks in the IT Service Department.

Implement

Implementation is carried out according to the designed network architecture. This includes installing and configuring firewall filtering, SYN Flood protection, and access control mechanisms.

Operate

Operational testing is conducted to evaluate security performance under SYN Flood attack scenarios and to assess network stability.

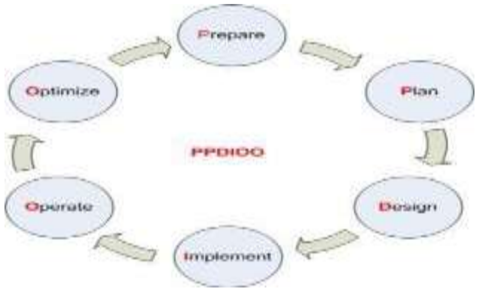


Figure 1. PPDIOO Method

Data Collection Methods

The study utilizes the following data collection techniques:

1. Observation, Direct observations were conducted to identify problems related to network instability and to monitor system behavior during attacks.
2. Interview, Discussions were held with IT Service staff at PT PUSRI Palembang to gather relevant information for the analysis.
3. Literature Review, Supporting literature was collected from books, journals, articles, and online sources related to SYN Flood attacks, firewall filtering, and network security.

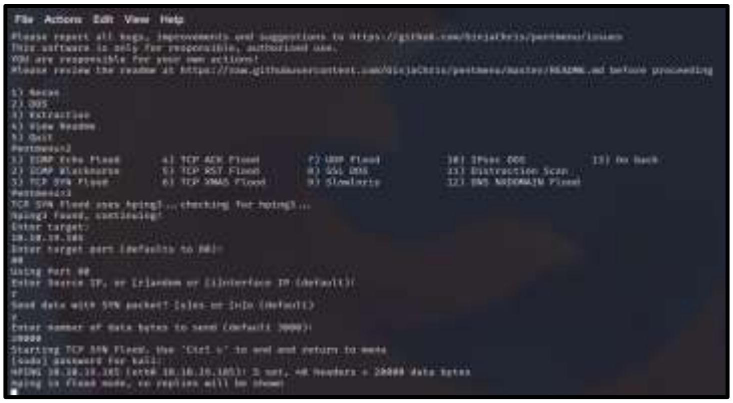
Research Design

Research design outlines the complete plan for the study, from preparation to evaluation. The following stages represent the attack testing scheme:

- Attackers perform port scanning to identify open ports.
- Open ports such as TCP, UDP, FTP, and SSH are identified.
- Attackers initiate SYN Flood attacks exploiting discovered open ports.
- SYN packets are sent to the router at IP Address 10.10.19.185/24.
- The attack results in severe router performance degradation and network instability.

Table 1. IP Address Allocation

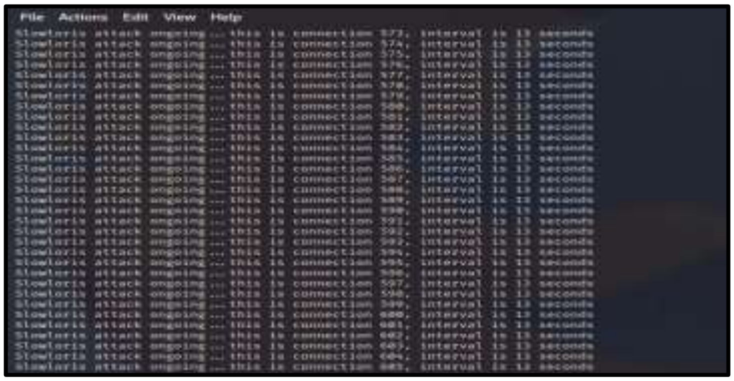
Device Name	Interface	IP Address	Network	Description
Router	Ether1	10.10.19.185/24	10.10.19.0/24	Internet
User 1	Ethernet	192.168.10.1/24	192.168.10.0/24	Wired Access
User 2	Wireless	192.168.1.1/24	192.168.1.0/24	Wi-Fi Access
Attacker 1	Ethernet	10.10.19.0/24	–	External Attacker
Attacker 2	Ethernet	192.168.10.0/24	–	Local Attacker



```
Please report all bugs, improvements and suggestions to https://github.com/GinjaChris/pentmenu/issues
This software is only for responsible, authorised use.
YOU are responsible for your own actions!
Please review the readme at https://raw.githubusercontent.com/GinjaChris/pentmenu/master/README.md before proceeding

1) Recon
2) DOS
3) Extraction
4) View Readme
5) Quit
Pentmenu>2
1) ICMP Echo Flood      4) TCP ACK Flood       7) UDP Flood          10) IPsec DOS            13) Go back
2) ICMP Blacknurse      5) TCP RST Flood       8) SSL DOS            11) Distraction Scan
3) TCP SYN Flood        6) TCP XMAS Flood      9) Slowloris          12) DNS NXDOMAIN Flood
Pentmenu>3
TCP SYN Flood uses hping3...checking for hping3...
hping3 found, continuing!
Enter target:
10.10.19.185
Enter target port (defaults to 80):
80
Using Port 80
Enter Source IP, or [r]andom or [i]nterface IP (default):
r
Send data with SYN packet? [y]es or [n]o (default)
y
Enter number of data bytes to send (default 3000):
20000
Starting TCP SYN Flood. Use 'Ctrl c' to end and return to menu
[sudo] password for kali:
HPING 10.10.19.185 (eth0 10.10.19.185): S set, 40 headers + 20000 data bytes
hping in flood mode, no replies will be shown
```

Figure 2. SYN Flood Attack Scenario on Target IP



```
Slowloris attack ongoing... this is connection 573, interval is 13 seconds
Slowloris attack ongoing... this is connection 574, interval is 13 seconds
Slowloris attack ongoing... this is connection 575, interval is 13 seconds
Slowloris attack ongoing... this is connection 576, interval is 13 seconds
Slowloris attack ongoing... this is connection 577, interval is 13 seconds
Slowloris attack ongoing... this is connection 578, interval is 13 seconds
Slowloris attack ongoing... this is connection 579, interval is 13 seconds
Slowloris attack ongoing... this is connection 580, interval is 13 seconds
Slowloris attack ongoing... this is connection 581, interval is 13 seconds
Slowloris attack ongoing... this is connection 582, interval is 13 seconds
Slowloris attack ongoing... this is connection 583, interval is 13 seconds
Slowloris attack ongoing... this is connection 584, interval is 13 seconds
Slowloris attack ongoing... this is connection 585, interval is 13 seconds
Slowloris attack ongoing... this is connection 586, interval is 13 seconds
Slowloris attack ongoing... this is connection 587, interval is 13 seconds
Slowloris attack ongoing... this is connection 588, interval is 13 seconds
Slowloris attack ongoing... this is connection 589, interval is 13 seconds
Slowloris attack ongoing... this is connection 590, interval is 13 seconds
Slowloris attack ongoing... this is connection 591, interval is 13 seconds
Slowloris attack ongoing... this is connection 592, interval is 13 seconds
Slowloris attack ongoing... this is connection 593, interval is 13 seconds
Slowloris attack ongoing... this is connection 594, interval is 13 seconds
Slowloris attack ongoing... this is connection 595, interval is 13 seconds
Slowloris attack ongoing... this is connection 596, interval is 13 seconds
Slowloris attack ongoing... this is connection 597, interval is 13 seconds
Slowloris attack ongoing... this is connection 598, interval is 13 seconds
Slowloris attack ongoing... this is connection 599, interval is 13 seconds
Slowloris attack ongoing... this is connection 600, interval is 13 seconds
Slowloris attack ongoing... this is connection 601, interval is 13 seconds
Slowloris attack ongoing... this is connection 602, interval is 13 seconds
Slowloris attack ongoing... this is connection 603, interval is 13 seconds
Slowloris attack ongoing... this is connection 604, interval is 13 seconds
Slowloris attack ongoing... this is connection 605, interval is 13 seconds
```

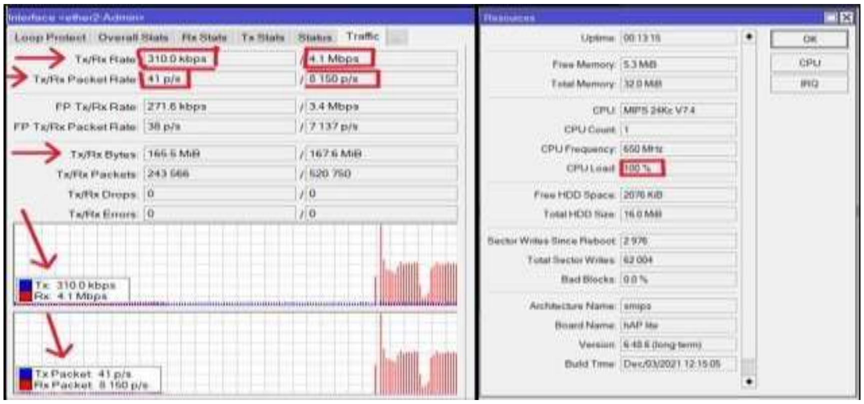
Figure 3. SYN Packet Transmission by Attacker

Attackers targeted port 80 on IP 10.10.19.185 and sent 20,000 SYN packets with 40 headers, overwhelming the server.

Results

SYN Flood Attack Activity

SYN Flood attacks caused significant increases in network traffic. As shown: Tx/Rx rate increased from 310.0 kbps to 4.1 Mbps. Incoming packets rose from 41 p/s to 8,150 p/s. CPU usage reached 100%, indicating system overload.



Tx/Rx Rate: 310.0 kbps / 4.1 Mbps
Tx/Rx Packet Rate: 41 p/s / 8 150 p/s
FP Tx/Rx Rate: 271.6 kbps / 3.4 Mbps
FP Tx/Rx Packet Rate: 38 p/s / 7 137 p/s
Tx/Rx Bytes: 166.5 MiB / 167.6 MiB
Tx/Rx Packets: 243 566 / 520 750
Tx/Rx Drops: 0 / 0
Tx/Rx Errors: 0 / 0
Tx: 310.0 kbps
Rx: 4.1 Mbps
Tx Packet: 41 p/s
Rx Packet: 8 150 p/s

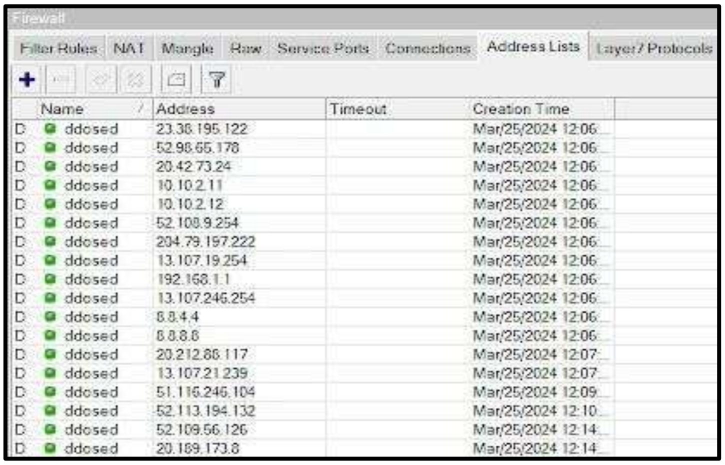
Uptime: 00:13:15
Free Memory: 5.3 MiB
Total Memory: 32.0 MiB
CPU: MIPS 24Kc V7.4
CPU Count: 1
CPU Frequency: 650 MHz
CPU Load: 100 %
Free HDD Space: 2076 KiB
Total HDD Size: 16.0 MiB
Sector Writes Since Reboot: 2 976
Total Sector Writes: 62 004
Bad Blocks: 0.0 %
Architecture Name: smips
Board Name: hAP lite
Version: 6.48.6 (long-term)
Build Time: Dec/03/2021 12:15:05

Figure 3.1. Network Traffic During SYN Flood Attack

These metrics indicate severe performance degradation and network instability.

Detection of Attacker IP Address

Firewall configuration successfully detected and recorded the attacker's IP address.



	Name	Address	Timeout	Creation Time
D	ddosed	23.38.195.122		Mar/25/2024 12:06
D	ddosed	52.98.65.178		Mar/25/2024 12:06
D	ddosed	20.42.73.24		Mar/25/2024 12:06
D	ddosed	10.10.2.11		Mar/25/2024 12:06
D	ddosed	10.10.2.12		Mar/25/2024 12:06
D	ddosed	52.108.9.254		Mar/25/2024 12:06
D	ddosed	204.79.197.222		Mar/25/2024 12:06
D	ddosed	13.107.19.254		Mar/25/2024 12:06
D	ddosed	192.168.1.1		Mar/25/2024 12:06
D	ddosed	13.107.246.254		Mar/25/2024 12:06
D	ddosed	8.8.4.4		Mar/25/2024 12:06
D	ddosed	8.8.8.8		Mar/25/2024 12:06
D	ddosed	20.212.88.117		Mar/25/2024 12:07
D	ddosed	13.107.21.239		Mar/25/2024 12:07
D	ddosed	51.116.246.104		Mar/25/2024 12:09
D	ddosed	52.113.194.132		Mar/25/2024 12:10
D	ddosed	52.109.56.126		Mar/25/2024 12:14
D	ddosed	20.189.173.8		Mar/25/2024 12:14

Figure 3.2. IP Address Captured After Firewall Configuration

The Address List feature allowed administrators to block malicious IP addresses efficiently.

Attack Indicators

Table 2. Attack Indicators Before and After Firewall Filtering

No	Indicator	Before Firewall	After Firewall
1	Packet Volume	High	Low

No	Indicator	Before Firewall	After Firewall
2	Server Response	Slow	Fast
3	CPU Load	High	Low
4	Network Traffic	High	Low
5	Bandwidth Usage	High	Normal
6	Network Performance	Slow	Fast

Before Firewall Filtering

- Packet volume extremely high
- Server overwhelmed and unable to respond
- CPU load excessive
- Network traffic significantly increased

After Firewall Filtering

- Packet volume drastically reduced
- Server responds rapidly
- CPU returns to normal condition
- Bandwidth stabilized
- Network improves and operates optimally

Discussion

The implementation of firewall filtering successfully mitigated SYN Flood attacks. After the filtering configuration:

- Malicious traffic was effectively blocked.
- CPU load decreased significantly.
- Network performance improved and stabilized.
- Unauthorized access attempts were prevented.

Firewall filtering proved capable of identifying SYN packet patterns and blocking suspicious or abnormal traffic.

Conclusion and Recommendations

Based on the research titled "Implementation of a Network Security System Against SYN Flood Attacks and Unauthorized Access Blocking Using Firewall Filtering in the IT Service Department of PT PUSRI Palembang", the following conclusions are drawn:

1. Firewall filtering on Mikrotik routers effectively prevents SYN Flood attacks. The firewall filters and identifies SYN attack patterns, blocking or limiting access from suspicious IP sources.
2. Network performance becomes more stable and secure after applying firewall filtering. The network operates normally without concerns about SYN Flood attacks or unauthorized access.

Strengthening network security using firewall filtering is highly recommended to ensure user safety, maintain service continuity, and increase network reliability.

Disclosure Statement

The authors declare no conflicts of interest.

Acknowledgments

The authors express their gratitude to PT Pupuk Sriwidjaja Palembang and Universitas Bina Darma for their support, facilities, and contributions to this research.

References

Nuroji. (2023). *Implementation of Intrusion Detection and Prevention System (IDPS) on computer networks as prevention of port-scanning attacks. Journal of Data Science and Information System (DIMIS), 1*, 1–9. https://doi.org/10.58602/dimis.v1i2.35

Indar Parawansa, K., Nurhadi, A., et al. (2024). *Analysis of SYN Flood attack using NIST 800-61 Rev 2 on Security Information and Event Management (SIEM).* https://uia.e-journal.id/INSIT

Dermawati, R., & Hasim Siregar, M. (2020). *Implementation of honeypot on university laboratory networks using Dionaea for network security.*

Sahren, S. (2021). Implementation of firewall technology for server security against SYN Flood attacks. *JURTEKSI: Jurnal Teknologi dan Sistem Informasi, 7*(2), 159–164. https://doi.org/10.33330/jurteksi.v7i2.933

Novianto, D., Japriadi, Y. S., & Tommy, L. (2022). Implementation of secure access to websites using Wireguard VPN on Mikrotik Routerboard. *Jurnal Ilmiah Informatika Global, 13*(2). https://doi.org/10.36982/jiig.v13i2.2308

Haris, A. I., Riyanto, B., Surachman, F., & Ramadhan, A. A. (2022). Analysis of network security using Mikrotik routers against DoS attacks and their effect on performance. Komputika: Jurnal Sistem Komputer, 11(1), 67–76. https://doi.org/10.34010/komputika.v11i1.5227

Radiyah, U. (2022). Optimization of WAN security using raw firewall based on Mikrotik at PT Permata Graha Nusantara. *INTI Nusa Mandiri, 17*(1), 16–23. https://doi.org/10.33480/inti.v17i1.3401

Jayanto, R. D. (2019). *Network monitoring system design using Mikrotik RouterOS.*

Zainy, A., et al. (2023). *Installation of Mikrotik on VirtualBox and connection with Winbox at SMKS Teruna Padangsidimpuan.*https://jurnal.spada.ipts.ac.id/index.php/adam

Bumi, P., et al. (2021). Improving internet services using Mikrotik and Winbox software at PTIPD UIN Walisongo Semarang.

Rismawati, N., & Mulya, M. F. (2020). Network simulation design of MAN with EIGRP and DUAL algorithm using Cisco Packet Tracer.

Haeruddin, H. (2021). Analysis and implementation of Mikrotik router security from Winbox exploitation, brute force, and DoS attacks. *Jurnal Media Informatika Budidarma, 5*(3), 848. https://doi.org/10.30865/mib.v5i3.2979

Muharor, A., Panjiasmara, B., & Bonok, Z. (n.d.). *Analysis of fiber optic aerial transmission at 1310 nm wavelength from ODP to ONT.*

Biographical Notes

M. Syaiful Huda Mubarok is a researcher in computer networks and cybersecurity at Universitas Bina Darma. His research interests include network security, firewall systems, and cyberattack mitigation.