

***IMPROVING MIKROTIK ROUTER SECURITY AGAINST UDP
FLOOD, SYN FLOOD, AND ICMP FLOOD ATTACKS USING
RAW FIREWALL AT SMKN 3 BENGKALIS.***

Name : Muhammad Syofyan
Student Id Number : 6103211442
Supervisor : Lipantri Mashur Gultom, M.Kom

ABSTRACT

This issue is highly relevant at SMKN 3 Bengkalis, where the school's network frequently becomes a target of such attacks. The proposed solution in this study is the implementation of a raw firewall on MikroTik routers. This firewall is capable of filtering and monitoring incoming connections, allowing it to reject potentially harmful data traffic. The objective of this research is to enhance the security of MikroTik routers against UDP flood, SYN flood, and ICMP flood attacks by utilizing a raw firewall. Testing results indicate that before implementing the raw firewall, UDP flood, SYN flood, and ICMP flood attacks caused CPU load to reach 100% and memory usage to increase from 8.0 MiB to approximately 2996 KiB, leading to network downtime. After deploying the raw firewall, CPU load significantly decreased to around 5% to 9%, and memory remained stable at 10.8 MiB, demonstrating the effectiveness of the raw firewall in mitigating the impact of attacks and maintaining network service availability.

Keyword: MikroTik, Firewall, Udp flood, Syn flood, Icmp flood