p-ISSN: 2301-6949
e-ISSN : 2715-5064


# Proteksi Internet Di SMK N 3 Pandeglang Menggunakan Firewall

**Hendra Permana [1*)], Singgih Mitro S[2]**
[1]Program Studi Informatika, Universitas Insan Cita Indonesia, Jakarta
[1]Jln. H,R Rasuna Said, Kota Jakarta Selatan, 12940, Indonesia
email: hendrapermana.m@gmail.com,[2]singgihmitro@uici.ac.id

***Abstract* − *In this digital era, internet security is a critical aspect in the educational environment. This research aims to investigate and implement internet protection strategies using a firewall at SMKN 3 Pandeglang. The firewall is employed to control and monitor internet access, including restrictions on specific websites. The research methodology includes the analysis of security needs, the selection of firewall devices, rule configuration, and evaluation of the implementation results. The research findings are expected to provide practical guidance for enhancing internet security in educational institutions.***

***Abstrak* − Dalam era digital saat ini, keamanan internet menjadi aspek kritis dalam lingkungan pendidikan. Penelitian ini bertujuan untuk menginvestigasi dan mengimplementasikan strategi proteksi internet menggunakan firewall di SMKN 3 Pandeglang. Firewall digunakan untuk mengontrol dan memantau akses internet, termasuk pembatasan pada situs web tertentu. Metodologi penelitian mencakup analisis kebutuhan keamanan, pemilihan perangkat firewall, konfigurasi aturan, dan evaluasi hasil implementasi. Temuan penelitian diharapkan dapat memberikan panduan praktis untuk peningkatan keamanan internet di lembaga pendidikan**
**Kata kunci - Jaringan Komputer, Internet, Firewall**

*) **penulis korespondensi**: **Hendra Permana**
Email: hendrapermana.m@gmail.com

## I. PENDAHULUAN

Penggunaan internet di lingkungan pendidikan, seperti Sekolah Menengah Kejuruan Negeri (SMKN) 3 Pandeglang, menjadi semakin penting seiring dengan perkembangan teknologi informasi. Namun, bersamaan dengan manfaatnya, internet juga membawa risiko keamanan yang signifikan. Sekolah-sekolah sering menjadi target serangan siber yang dapat merugikan integritas dan kerahasiaan data, serta mengancam kelangsungan proses pendidikan.

Salah satu solusi yang umum digunakan untuk melindungi jaringan dari ancaman siber adalah penggunaan firewall. Firewall berperan sebagai barisan pertahanan pertama, memonitor dan mengendalikan lalu lintas data yang masuk dan keluar dari jaringan. Meskipun firewall telah menjadi alat yang umum digunakan dalam lingkungan bisnis, penerapannya di lembaga pendidikan masih belum merata, terutama di SMKN 3 Pandeglang.

Dengan mempertimbangkan konteks tersebut, penelitian ini bertujuan untuk menginvestigasi penerapan proteksi internet menggunakan firewall di SMKN 3 Pandeglang. Fokus utama adalah menganalisis dampak penggunaan firewall terhadap ketersediaan layanan di lingkungan pendidikan dan pemblokiran akses ke situs-situs tertentu, seperti media sosial agar menjaga disiplin penggunaan internet pada saat pelajaran.

## II. PENELITIAN YANG TERKAIT

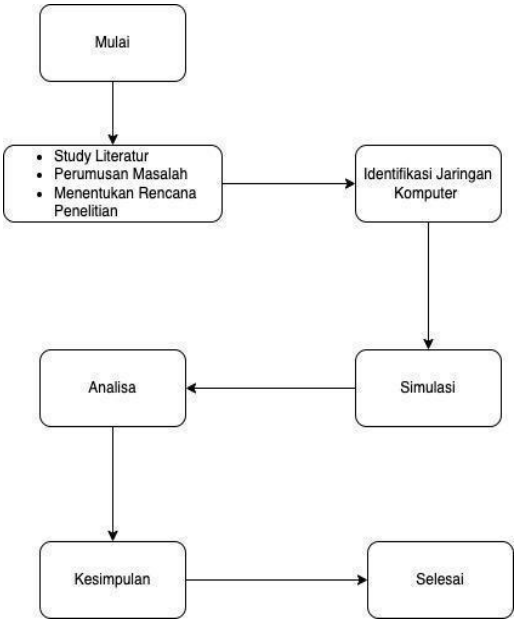
Beberapa penelitian terdahulu yang telah yang dilakukan oleh A. Muzakir & M. Ulfa yang judulnya "Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan Jaringan" tujuan penelitian yang telah dilakukan dalah untuk menyelidiki sistem keamanan dengan packet filtering [1]

Selanjutnya penelitian dari Sartomo & Wiwin S, berjudul "Network Security Model Utilizing Firewall Port Blocking," bertujuan untuk menjaga jaringan komputer agar aman dari serangan acaman eksternal maupun internal agar mencegah pencurian data [2]

Berdasarkan referensi yang telah ada diatas, maka penelitian ini akan difokuskan pada Proteksi Internet di SMKN 3 Pandeglang Menggunakan Firewall.

## III. METODE PENELITIAN

Penelitian ini mengadopsi metodologi penelitian yang direpresentasikan melalui flowchart pada Gambar 1.




Gambar 1. *Flowchart* Penelitian

I. Jaringan Komputer

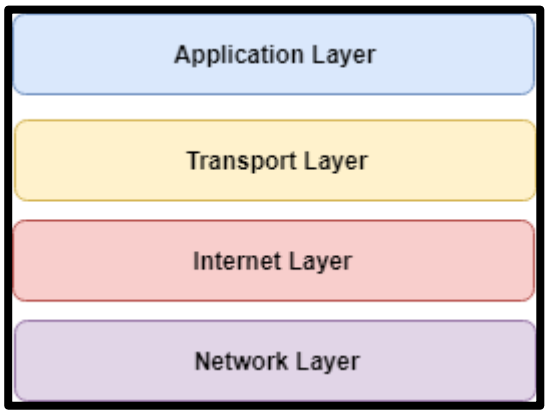
Jaringan komputer adalah suatu kumpulan perangkat elektronik yang saling terhubung, memungkinkan pertukaran data dan sumber daya di antara mereka [3]

II. Keamanan Jaringan

Keamanan jaringan merujuk pada serangkaian langkah dan tindakan yang diimplementasikan untuk melindungi sistem jaringan komputer dari ancaman dan risiko yang dapat merugikan integritas, kerahasiaan, dan ketersediaan data. [4]

III. TCP/IP (Transmission Control Protocol/Internet Protocol)

Suatu set protokol komunikasi yang digunakan untuk menghubungkan dan mentransfer data antar perangkat dalam suatu jaringan komputer, khususnya dalam konteks Internet . [5]




Gambar 2. TCP/IP Layer

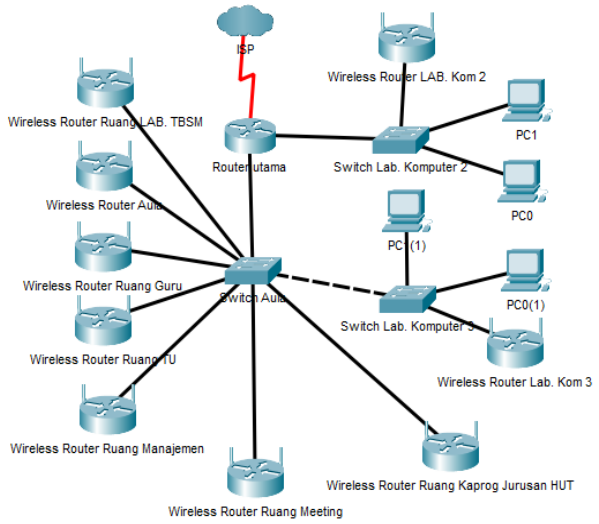
IV. Firewall

Firewall adalah sebuah sistem yang mampu melindungi perangkat ataupun user yang terhubung pada sebuah jaringan. Pada umumnya firewall dibuat untuk melindungi jaringan Local dari ancaman dan gangguan yang datang dari luar setelah jaringan tersebut terhubung dengan internet. [2]

## IV. HASIL DAN PEMBAHASAN

### 1. Identifikasi Jaringan

Berdasarkan hasil observasi, topologi yang digunakan adalah Star, dengan pusatnya berada pada Ruang Kepala Sekolah. Topologi ini memungkinkan komunikasi efisien antar-ruangan dan pusat kontrol yang terpusat.




Gambar 3. Skema Diagram Jaringan

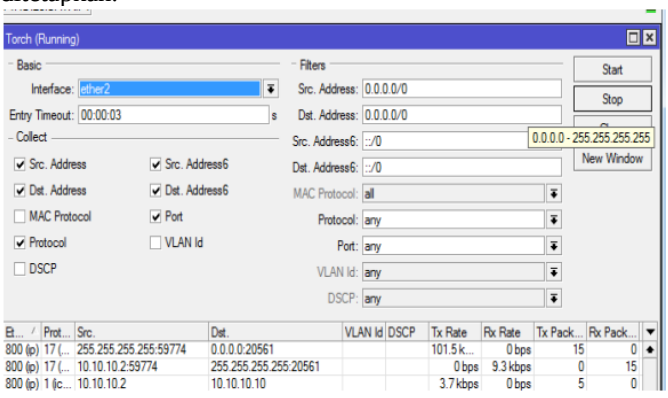
Pada skema jaringan SMKN 3 Pandeglang, terdapat Internet Service Provider (ISP). Sekolah berlangganan ISP IndiHome untuk Internet. Terdapat Router Utama/Modem yang menghubungkan jaringan ke internet. Switch Aula, Switch Lab. Switch Lab Komputer 2, dan Switch Lab. Komputer 3 bertindak sebagai perangkat penghubung di area khusus.

### 2. Tahap Implementasi

Berdasarkan skema jaringan yang telah diobservasi di SMKN 3 Pandeglang, langkah-langkah penguatan keamanan jaringan tidak hanya melibatkan penggunaan antivirus, tetapi juga melibatkan penerapan firewall filtering dengan menggunakan perangkat MikroTik. Proses instalasi sistem keamanan jaringan mencakup beberapa langkah, seperti:

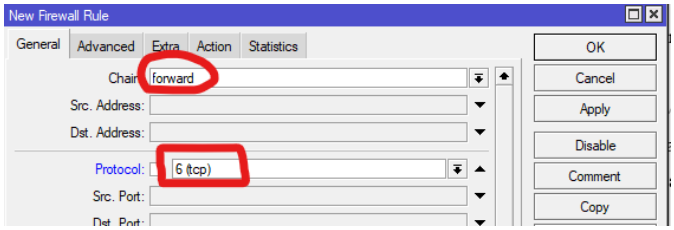
1. Konfigurasi Packet Filtering

a. Eksplorasi port digunakan untuk mengidentifikasi alamat IP permainan online dan platform media sosial yang akan disaring. Langkah ini bertujuan untuk mengetahui alamat IP yang terkait dengan permainan atau media sosial yang digunakan oleh pengguna. Informasi tersebut akan menjadi dasar untuk pelaksanaan pemblokiran dengan menyaring alamat IP tertentu, sehingga akses ke permainan atau platform media sosial tersebut dapat dikendalikan sesuai kebijakan yang ditetapkan.



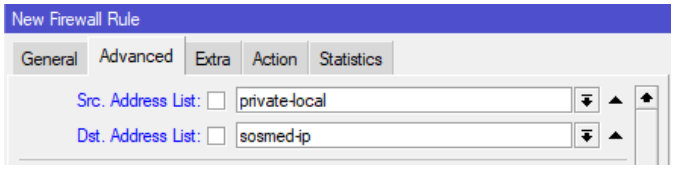

Gambar 4. Fasilitas torch

b. Mengatur chain pada protokol TCP.
Menyesuaikan urutan pada protokol TCP dilakukan untuk menetapkan kategori lalu lintas yang akan diatur melalui fitur firewall, terutama filter rule, pada level protokol TCP. Hal ini bertujuan untuk mengontrol dan mengelola lalu lintas jaringan berdasarkan protokol TCP, memungkinkan firewall untuk memberlakukan kebijakan keamanan yang spesifik terhadap jenis komunikasi yang menggunakan protokol tersebut. Dengan menyesuaikan urutan pada protokol TCP, organisasi dapat meningkatkan efektivitas pengaturan kebijakan keamanan dan memitigasi potensi risiko keamanan yang berkaitan dengan protokol tersebut.



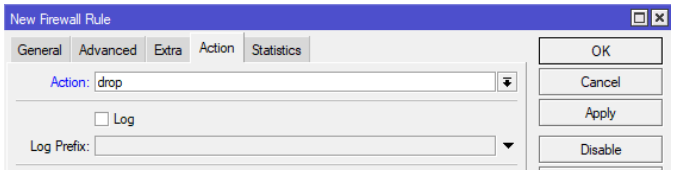
Gambar 5. Konfigurasi Filter Rule pada tab general

c. List daftar alamat yang ingin diblokir adalah langkah untuk mengkategorikan situs web atau aplikasi yang akan dilarang aksesnya. Tujuannya adalah untuk menyusun daftar alamat IP atau domain yang dianggap tidak diinginkan atau berpotensi membahayakan keamanan, privasi, atau produktivitas pengguna jaringan. Dengan langkah ini, firewall atau perangkat keamanan jaringan dapat dikonfigurasi untuk secara efektif memblokir akses ke alamat-alamat yang terdaftar sesuai dengan kebijakan keamanan yang ditetapkan oleh organisasi.



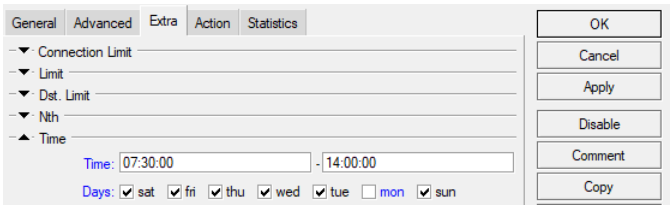
Gambar 6. Pengaturan Filter Rule pada tab general

d. Pilih "drop" sebagai tindakan bertujuan supaya router membuang paket yang telah diidentifikasi. Langkah ini memungkinkan implementasi kebijakan keamanan yang efektif, di mana paket-paket yang terkait dengan kategori atau kriteria tertentu akan secara otomatis ditolak dan tidak diteruskan melalui router. Hal ini bertujuan untuk meningkatkan kontrol terhadap lalu lintas jaringan, melindungi keamanan, dan mematuhi kebijakan keamanan yang telah ditetapkan oleh organisasi.



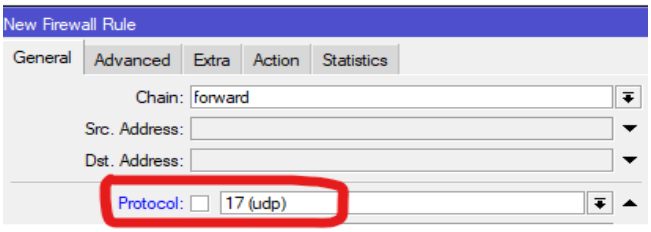
Gambar 7. Konfigurasi Filter Rule pada tab Action

e. Penetapan jadwal waktu efektif untuk pemblokiran dilakukan untuk mengatur periode di mana pemblokiran situs atau aplikasi diaktifkan dan kapan pemblokiran tersebut dinonaktifkan. Langkah ini bertujuan untuk memberikan fleksibilitas dalam implementasi kebijakan keamanan jaringan, sehingga pemblokiran dapat diatur sesuai dengan kebutuhan dan kebijakan spesifik pada waktu tertentu. Jadwal waktu efektif membantu organisasi dalam mengelola akses internet dan meningkatkan kontrol terhadap penggunaan jaringan selama periode yang telah ditentukan.



Gambar 8. Konfigurasi Filter Rule pada tab Extra

f. Pengaturan chain pada protokol UDP memiliki fungsi serupa dengan TCP, yaitu menggunakan protokol UDP untuk memblokir IP Addres. Pengaturan ini dilakukan di pada tools filter rule untuk memberlakukan kebijakan keamanan terhadap lalu lintas jaringan yang menggunakan protokol UDP. Tindakan ini membantu dalam meningkatkan kontrol dan keamanan jaringan dengan mengatur aturan yang spesifik terhadap komunikasi yang menggunakan protokol UDP, sehingga sesuai dengan kebijakan keamanan yang telah ditetapkan oleh organisasi.

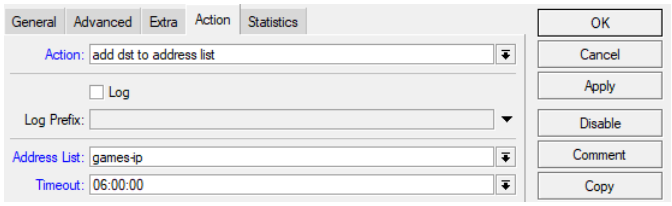


Gambar 9. Konfigurasi Filter Rule pada protocol UDP

g. Mengkonfigurasi halaman filter raw melibatkan penambahan IP Addres yang ditemukan menggunakan alat torch. Selain itu, menjadwalkan waktu efektif untuk pemblokiran bertujuan mengatur periode di mana pemblokiran situs atau aplikasi diaktifkan dan kapan pemblokiran tersebut dinonaktifkan. Langkah-langkah ini memberikan kontrol yang lebih baik terhadap kebijakan keamanan jaringan dengan menyesuaikan dan menyinkronkan tindakan pemblokiran sesuai dengan jadwal yang telah ditetapkan. Dengan demikian, organisasi dapat meningkatkan efisiensi dan fleksibilitas dalam mengelola akses internet dan memberlakukan kebijakan keamanan yang sesuai dengan kebutuhan.

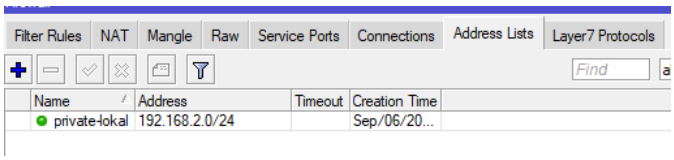
Gambar 10. Konfigurasi Filter Raw

h. Mengarahkan semua packet data ke list yang dibuat.




Gambar 11. Konfigurasi tab action pada filter raw

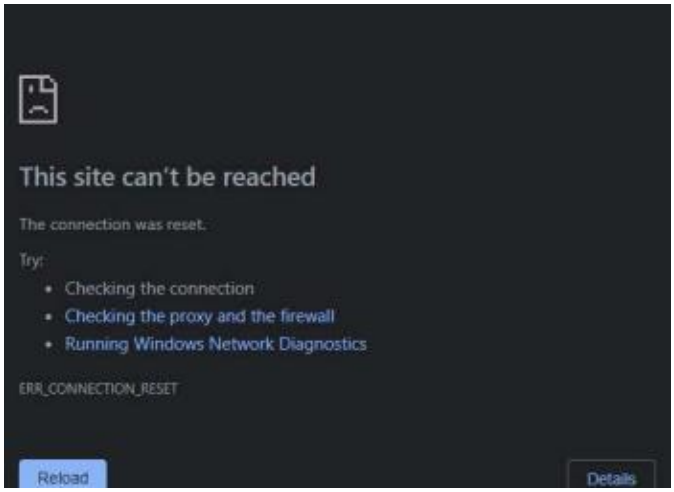
i. Untuk mengaktifkan koneksi internet user, buka tab address list dan inputkan network ID lokal yang akan digunakan oleh user seperti yang terlihat pada gambar 12. Dengan demikian, langkah ini memastikan bahwa pengguna dapat terhubung dengan internet menggunakan IP yang telah ditentukan, dan informasi hasil tangkapan IP dapat digunakan untuk memonitor akses ke sistus web media sosial.




Gambar 12. Membuat Network ID

j. Dalam pengaturan firewall rule, pilih chain forward untuk menandai trafik yang akan menuju router dengan cara memilih "IN" dan "OUT" pada pengaturan firewall rule, serta memasukkan src address 192.168.1.0/24. Tindakan ini bertujuan untuk mengubah source address dari paket data, sehingga MikroTik dapat membatasi semua perangkat (PC/hp) yang memiliki IP Address 192.168.1.0/24. Dengan demikian, langkah ini memungkinkan untuk menandai dan mengatur lalu lintas yang akan diarahkan ke router sesuai dengan kebijakan keamanan yang telah ditetapkan.

k. Hasil pengujian menunjukkan bahwa akses ke media sosial dan Facebook berhasil diblokir sesuai dengan kebijakan yang telah diimplementasikan.




Gambar 13. Facebook tidak bisa di akses

## V.KESIMPULAN DAN SARAN

Dari hasil penelitian tentang strategi proteksi internet di SMKN 3 Pandeglang menggunakan firewall, dapat disimpulkan bahwa implementasi firewall menjadi langkah yang efektif dalam mengelola dan melindungi akses internet di lingkungan sekolah. Penerapan firewall, khususnya dalam mengatur aturan filter, telah berhasil mengendalikan dan memonitor lalu lintas jaringan. Pemblokiran akses ke situs-situs tertentu, seperti media sosial, membuktikan efektivitas firewall dalam menjaga disiplin penggunaan internet.

## V. DAFTAR PUSTAKA

[1] A. Muzakir and M. Ulfa, "ANALISIS KINERJA PACKET FILTERING BERBASIS MIKROTIK ROUTERBOARD PADA SISTEM KEAMANAN JARINGAN," Jurnal SIMETRIS, vol. 10, no. 1, 2019.

[2]W. Sulistyo, "Krea-TIF: Jurnal Teknik Informatika Model Keamanan Jaringan Menggunakan Firewall Port Blocking," vol. 10, no. 1, pp. 10–18, 2022, doi: 10.32832/kreatif.v10i1.6678.

[3] Sofana, Iwan. 2013. Membangun Jaringan Komputer : Mudah membuat Jaringan Komputer (Wire & Wireless) untuk pengguna Windows dan Linux. Bandung: Informatika

[4] Ma'sum, M. S., Irwansyah, M. A., & Priyanto, H. (2017). Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter. Jurnal Sistem Dan Teknologi Informasi (JUSTIN), 5(1), 56–60.

[5] Bandhu Nath, P., & Uddin, M. (2015). TCP-IP Model in Data Communication and Networking. American Journal of Engineering Research (AJER), 4(10), 102–107. Retrieved from www.ajer.org