# Implementasi *Wireshark* Dan *Firewall* Untuk Mendukung Trafik Keamanan Jaringan

M. IKHSAN[1], Aswandi[2], Nanda Saputri[3]

[1,2,3] *Jurusan Tekniknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
*Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA*
[1]mikhsan102002@gmail.com
[2]aswandi@pnl.ac.id (penulis korespondensi)
[3]nandasaputri24@gmail.com

***Abstrak*—Kemajuan teknologi telah meningkatkan kompleksitas dan frekuensi ancaman keamanan jaringan, seperti peretasan, *malware*, dan aktivitas jaringan berbahaya. Penelitian ini bertujuan untuk menganalisis sistem keamanan *JJLink* dan mengidentifikasi kelemahan yang perlu diperbaiki. Alat analisis lalu lintas jaringan yang digunakan adalah *Wireshark*, sementara *firewall* diimplementasikan untuk menyaring paket data dan memblokir *website* yang tidak aman. Metode yang digunakan dalam penelitian ini adalah *Quality of Service (QoS)*, yang mengukur dan menganalisis kinerja jaringan berdasarkan parameter seperti *delay*, *jitter*, *throughput*, dan *packet loss*. Hasil penelitian menunjukkan adanya perbedaan performa dalam dua percobaan yang dilakukan. Pada percobaan menggunakan laptop, sistem berhasil memblokir 100% dari 20 *website* yang tidak aman, sementara 40% dari 15 *website* yang aman tidak terblokir. Sebaliknya, pada percobaan menggunakan *handphone*, hanya 40% dari 20 *website* yang tidak aman berhasil terblokir, dan 40% dari 15 *website* yang aman tidak terblokir. Temuan ini menunjukkan bahwa laptop memiliki kinerja yang lebih baik dalam memblokir *website* tidak aman dibandingkan dengan *handphone*.**
**Kata kunci—*firewall*, keamanan jaringan, *Wireshark*, Analisis *Traffic, QoS.***

***Abstract*—Technological advances have increased the complexity and frequency of network security threats, such as hacking, malware, and malicious network activity. This study aims to analyze the JJLink security system and identify weaknesses that need to be fixed. The network traffic analysis tool used is Wireshark, while a firewall is implemented to filter data packets and block unsafe websites. The method used in this study is Quality of Service (QoS), which measures and analyzes network performance based on parameters such as delay, jitter, throughput, and packet loss. The results showed a difference in performance in the two experiments conducted. In the experiment using a laptop, the system successfully blocked 100% of 20 unsafe websites, while 40% of 15 safe websites were not blocked. In contrast, in the experiment using a cellphone, only 40% of 20 unsafe websites were successfully blocked, and 40% of 15 safe websites were not blocked. These findings indicate that laptops perform better in blocking unsafe websites compared to cellphones.**
***Keywords—Firewall*, *Network Security*, *Wireshark*, *Traffic Analysis*.**

## I. PENDAHULUAN

Perkembangan teknologi yang pesat telah meningkatkan kompleksitas ancaman terhadap keamanan jaringan, termasuk serangan peretasan, *malware*, dan aktivitas berbahaya lainnya yang dapat mengancam ketersediaan, integritas, serta kerahasiaan data. Dalam menghadapi ancaman ini, pemahaman yang mendalam mengenai lalu lintas jaringan menjadi sangat penting untuk mengidentifikasi pola-pola anomali dan aktivitas mencurigakan. Pemantauan aktif terhadap lalu lintas jaringan, didukung dengan penggunaan *firewall*, merupakan salah satu langkah utama untuk melindungi jaringan dari akses tidak sah dan ancaman siber yang berkembang.

*Wireshark*, sebagai alat analisis lalu lintas jaringan, mampu memberikan pandangan yang mendalam terhadap berbagai aktivitas yang terjadi dalam jaringan. Melalui analisis yang mendalam, *wireshark* dapat membantu mendeteksi serangan siber dan potensi kerentanan keamanan yang mungkin tidak teridentifikasi oleh sistem perlindungan tradisional. Analisis ini juga mencakup evaluasi terhadap efektivitas *firewall* dalam mengelola lalu lintas jaringan dan mencegah akses yang tidak diinginkan. Penggunaan *wireshark* di JJLink berpotensi mengungkap kelemahan keamanan dan memberikan wawasan yang lebih dalam mengenai kebutuhan untuk memperkuat perlindungan jaringan.

Penggabungan antara penggunaan *wireshark* dan *firewall* sebagai metode keamanan jaringan diharapkan mampu meningkatkan tingkat proteksi secara signifikan. Dengan melakukan pemantauan lalu lintas jaringan secara proaktif, konfigurasi *firewall* yang tepat, dan deteksi dini terhadap aktivitas mencurigakan, solusi ini dapat memungkinkan tindakan pencegahan yang lebih cepat dan efisien. Hasil dari implementasi ini diharapkan tidak hanya meningkatkan keamanan jaringan, tetapi juga menjaga kinerja optimal dengan meminimalkan gangguan pada lalu lintas yang sah.

### *A. Jaringan Komputer*

Jaringan komputer adalah kelompok komputer otonom yang terhubung satu sama lain. Dalam bahasa sehari-hari, jaringan komputer adalah kumpulan komputer dan perangkat lain seperti *printer*, *hub*, dan lainnya yang terhubung melalui media perantara. Media perantara dapat berupa kabel dan nirkabel. Media informasi nirkabel adalah data yang dikirimkan dari satu komputer ke komputer lain dengan cara

ini setiap komputer dapat berbagi perangkat keras atau bertukar data[1].

Ada empat hubungan yang berbeda antara keamanan jaringan komputer dan ancaman terhadap keamanan jaringan komputer. Ancaman terhadap keamanan jaringan komputer terdiri dari empat bentuk utama ancaman: penyalahgunaan informasi *Internet of Things*, penolakan layanan serangan latar belakang, kerusakan pada integritas lingkungan jaringan komputer, dan kebocoran informasi pada komputer[2].

*B. Wireshark*

Aplikasi ini biasanya digunakan sebagai alat pemecahan masalah pada jaringan yang bermasalah. Ini juga banyak digunakan untuk pengujian perangkat lunak karena dapat membaca isi lalu lintas paket apa pun. *Wireshark* mendukung banyak format file untuk pengambilan/pelacakan paket, termasuk *.cap* dan *.erf*. Selain itu, alat dekripsi internal memungkinkan Pengguna melihat paket data terenkripsi dari berbagai protokol yang umum digunakan di *internet* saat ini, seperti *WEP* dan *WPA/WPA2*. Pengembangan dan distribusi lintas *platform Wireshark* memberikan banyak keuntungan. Pengguna sistem operasi Mac dan Linux dapat menginstal dan menggunakan fitur aplikasi Wireshark. [1].

*C. Firewall*

*Firewall* berfungsi sebagai *filter* antara komputer *internal* dan *eksternal* dan berfungsi untuk melindungi data dari orang yang tidak berhak mengaksesnya. Selain itu, *firewall* juga melakukan tugas mengatur dan mengontrol lalu lintas data yang diizinkan untuk masuk ke jaringan *private*. Ini melakukan ini dengan mempertimbangkan alamat *IP* sumber, *port TCP/UDP* sumber dan tujuan, serta alamat *IP* tujuan dan informasi *header* yang disimpan dalam paket data. Salah satu fungsi *firewall* sebagai *filter* adalah ia dapat mencegah *traffic* mengalir ke *subnet* jaringan, sehingga pengguna tidak dapat berbagi *file* rahasia[3].

*D. Traffic Keamanan Jaringan*

*Traffic* keamanan jaringan adalah proses pemantauan dan pengendalian lalu lintas ke dan dari jaringan komputer. Tujuan dari *Traffic* keamanan jaringan adalah untuk memastikan bahwa hanya data yang sah dan aman yang masuk dan keluar dari jaringan dan untuk mencegah akses tidak sah yang dapat mencuri data. *Traffic* keamanan jaringan mengambil langkah-langkah seperti pemantauan lalu lintas, pemantauan konten, pemantauan log. memastikan bahwa jaringan komputer terlindungi dari akses tidak sah dan tetap aman[4]

*E. MikroTik*

*MikroTik RouterOS* adalah perangkat lunak dan sistem operasi yang dapat digunakan untuk mengubah *PC* konvensional atau perangkat keras *MikroTik Routerboard* menjadi *router*. *MikroTik* pertama kali dikembangkan di Latvia sekitar tahun 1996 oleh John Truly dan Arnis Riekstins. *MikroTik* tersedia dalam dua versi, versi perangkat lunak yang dapat diinstal pada komputer pribadi dan versi perangkat keras yang diintegrasikan dan dikenal sebagai *RouterBoard*. Karena biaya lisensi yang lebih rendah daripada perangkat lunak serupa, *MikroTik* menjadi pilihan yang tepat.[5].

*Mikrotik* memiliki dua jenis, yang dapat dijelaskan sebagai berikut:

1) *Mikrotik RouterOS*

MikroTik RouterOS adalah perangkat lunak dan sistem operasi yang dapat mengubah komputer menjadi router yang dapat diandalkan yang memiliki semua fitur yang diperlukan untuk jaringan IP dan nirkabel. Ini cocok untuk ISP.

2) *Mikrotik RouterBoard*

MikroTik RouterBoard adalah router terintegrasi dalam satu papan yang memiliki prosesor, RAM, ROM, dan memori flash. Dengan RouterOS, perangkat ini mengelola bandwidth, jaringan, proxy server, DHCP, dan DNS server*[6]*.

*F. Winbox*

*Winbox* adalah sebuah utilitas yang sangat penting bagi pengguna *MikroTik*, memungkinkan mereka untuk melakukan *remote* ke *server MikroTik* melalui antarmuka grafis (*GUI*). Dalam situasi di mana konfigurasi *MikroTik* biasanya dilakukan melalui *mode* teks pada *PC* itu sendiri, *Winbox* menawarkan kemudahan dengan memungkinkan konfigurasi dilakukan melalui komputer klien dengan antarmuka yang lebih ramah pengguna. Fungsi utama dari *Winbox* adalah untuk mengelola dan mengatur berbagai pengaturan pada perangkat *MikroTik*, menjadikannya alat yang krusial dalam proses pengelolaan jaringan[7].

*G. Efektivitas*

Efektivitas adalah ukuran seberapa baik suatu pekerjaan dilakukan dan hasil yang dicapai sesuai dengan tujuan yang diharapkan. Efektivitas dicapai apabila suatu pekerjaan memberikan dampak positif dan menghasilkan output yang diharapkan sesuai dengan standar dan tujuan yang telah ditentukan. Menilai efisiensi tidak hanya mencakup pelaksanaan yang efektif dan sesuai rencana, tetapi juga hasil akhir. Sebuah pekerjaan dianggap efektif jika selesai tepat waktu, sesuai anggaran, dan memenuhi standar kualitas. Dalam hal ini, efektivitas berfungsi sebagai pengukur utama keberhasilan suatu usaha karena menunjukkan bahwa setiap langkah yang diambil telah memenuhi rencana dan menghasilkan hasil yang optimal[8].

Berikut ini adalah rumus dasar yang dapat digunakan:

$$Efektivitas = \frac{Jumlah\ hasil\ yang\ dicapai}{Jumlah\ hasil\ yang\ ditetapkan} \times 100\% \quad (1)$$

Keterangan:

- Jumlah hasil yang dicapai: Menunjukkan jumlah output yang dihasilkan.
- Jumlah Ancaman Total: menunjukkan total nilai yang ditetapkan[9].

### H. *QoS*

*Quality of Service (QoS)* adalah metode evaluasi kinerja jaringan dan upaya untuk menentukan karakteristik dan sifat suatu layanan. *QoS* digunakan untuk mengukur serangkaian atribut kinerja yang telah ditentukan sebelumnya yang terkait dengan suatu layanan [10]. Berikut penjelasan dari *throughput*, *packet loss, delay*, dan *jitter:*

1) *Throughput*

*Throughput* adalah kecepatan (*rate*) transfer data efektif, yang diukur dalam *bps (bit per second)*. Jumlah paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut dikenal sebagai throughput. Tabel I adalah tabel kategori *throughput.*

TABEL I
KATEGORI *THROUGHPUT*

| Kategori | *Throughput* | Indeks |
|---|---|---|
| Sangat Bagus | 100 | 4 |
| Bagus | 75 | 3 |
| Sedang | 50 | 2 |
| Jelek | <25 | 1 |

Sumber : (Hasbi & Saputra, 2021)

2) *Packet Loss*

*Packet loss* adalah sebuah parameter yang mengindikasikan jumlah paket yang dapat hilang secara total akibat dari tabrakan dan kepadatan lalu lintas pada jaringan. Tabel II adalah tabel kategori *packet loss.*

TABEL II
KATEGORI *PACKET LOSS*

| Kategori | *packet loss* | Indeks |
|---|---|---|
| Sangat Bagus | 0 | 4 |
| Bagus | 3 | 3 |
| Sedang | 15 | 2 |
| Jelek | 25 | 1 |

Sumber : (Hasbi & Saputra, 2021)

3) *Delay*

*Delay* merupakan waktu yang dibutuhkan data untuk menempuh jarak dari awal ke tujuan. *Delay* dapat disebabkan oleh congesti, waktu proses yang lama, jarak, media fisik dan jarak. Tabel III adalah tabel kategori *delay.*

TABEL III
KATEGORI *DELAY*

| Kategori | Besar *delay* | Indeks |
|---|---|---|
| Sangat Bagus | <150 ms | 4 |
| Bagus | 150 s/d 300 ms | 3 |
| Sedang | 300 s/d 450 ms | 2 |
| Jelek | >450 ms | 1 |

Sumber : (Hasbi & Saputra, 2021)

4) *Jittler*

*Jitter*, atau variasi kedatangan paket, disebabkan oleh perubahan pada panjang antrian, waktu pemrosesan data, dan waktu penggabungan ulang paket di akhir perjalanan. Dalam kaitannya dengan *latency*. *jitter*, yang juga disebut sebagai variasi *delay*, menunjukkan tingkat *delay* dalam transmisi data di jaringan. Tabel IV adalah tabel kategori *jitter.*

TABEL IV
KATEGORI *JITTLER*

| Kategori | *Jitter* (ms) | Indeks |
|---|---|---|
| Sangat Bagus | 0 ms | 4 |
| Bagus | 0 s/d 75 ms | 3 |
| Sedang | 75 s/d 125 ms | 2 |
| Jelek | 125 s/d ms | 1 |

Sumber : (Hasbi & Saputra, 2021)

## II. METODOLOGI PENELITIAN

### A. *Tahapan penelitian*

Gambar 1 merupakan tahapan penelitian untuk mendapatkan data penelitian. Untuk menyelesaikan masalah penyusunan penelitian ini, ada beberapa tindakan yang harus dilakukan. Gambar di bawah menunjukkan tahapannya.


Gambar 1. Tahapan penelitian

Berdasarkan kerangka kerja penelitian pada gambar 1 tahapan penelitian, pembahasan tentang masing-masing tahap penelitian dapat diuraikan sebagai berikut:

- Mengumpulkan informasi dan data tentang *Wireshark* dan *Firewall*, serta metode yang digunakan untuk mendukung keamanan jaringan.
- Pada tahap ini, data lalu lintas jaringan dianalisis menggunakan *wireshark*, sebuah alat untuk memantau dan menganalisis paket jaringan. Ini membantu memahami karakteristik dan pola lalu lintas yang perlu diatur oleh *firewall.*
- Membuat sistem yang akan mendukung keamanan jaringan dengan menggunakan *wireshark* dan *firewall.*
- Menggunakan *firewall* untuk mengonfigurasi lalu lintas jaringan pada perangkat *MikroTik*, yang memungkinkan untuk menerapkan kebijakan keamanan yang melindungi jaringan dari akses yang tidak sah. Aturan yang dapat dibuat berdasarkan *protocol*, *port*, dan *IP* memungkinkan *MikroTik* untuk lebih fleksibel dalam mengelola dan membatasi lalu lintas jaringan. Oleh karena itu, jaringan lebih aman dari serangan *DDoS* dan *malware*.
- Melakukan pengujian sistem *firewall* untuk memastikan bahwa sistem *firewall* yang telah diimplementasikan bekerja dengan baik dan dapat mendukung keamanan jaringan.
- Mengevaluasi hasil pengujian pada *wireshark* untuk menentukan seberapa baik implementasi sistem *firewall* yang dikonfigurasi pada *MikroTik* dapat mendukung keamanan jaringan.

*B. Rancangan Sistem*

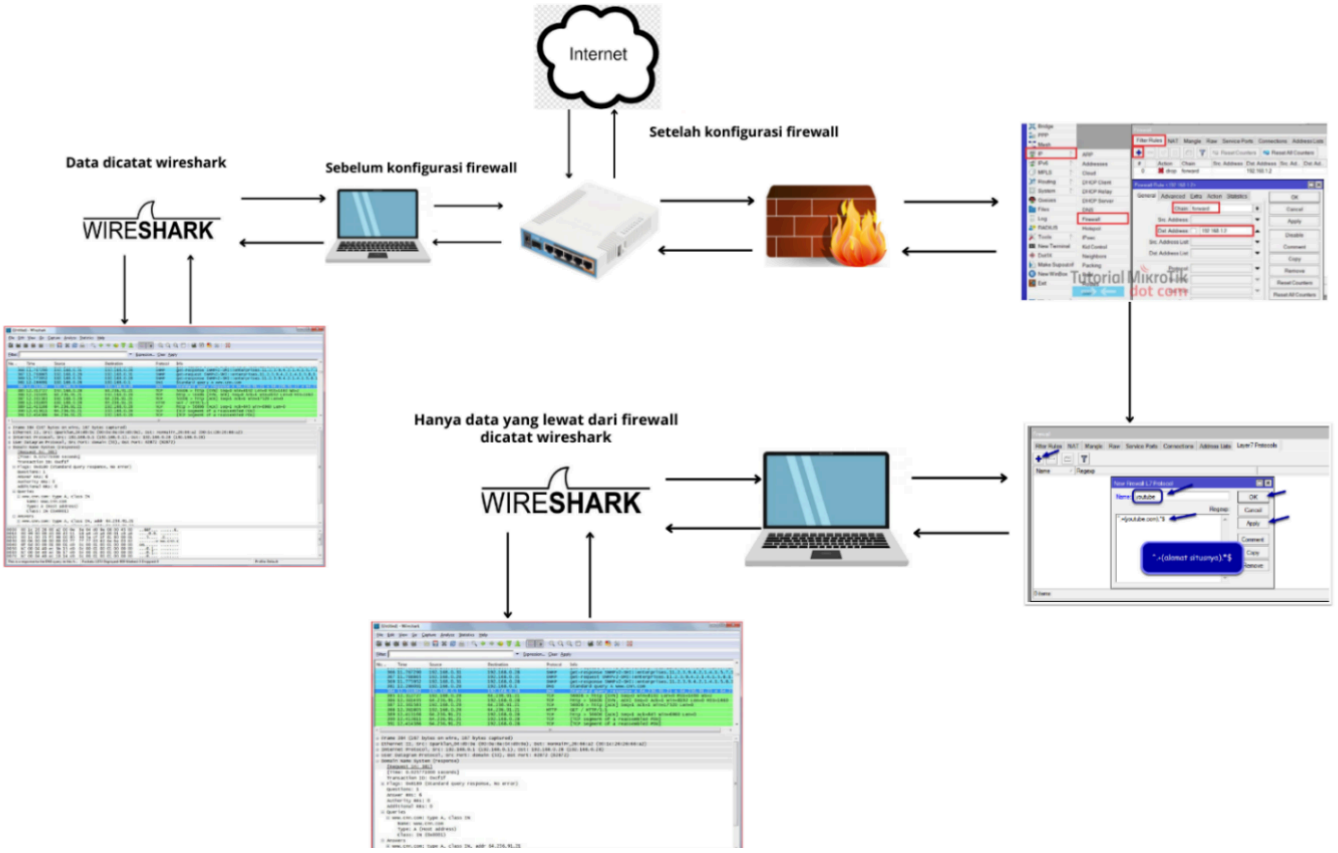
Gambar 2 menunjukkan rancangan sistem yang mengintegrasikan perangkat lunak dan perangkat keras untuk meningkatkan keamanan jaringan secara keseluruhan. Dengan menggunakan kemampuan *wireshark* sebagai alat pemantauan jaringan, sistem ini dapat menganalisis lalu lintas data secara *real-time* untuk menemukan ancaman potensial dan memetakan pola komunikasi yang mencurigakan.

Selain itu, *firewall* berfungsi sebagai lapisan perlindungan yang secara aktif mengontrol akses dan mengontrol *traffic* yang masuk dan keluar dari jaringan. Kombinasi kedua komponen ini memungkinkan pengelolaan keamanan yang lebih dinamis dan responsif terhadap ancaman. Dengan menggabungkan kedua komponen ini, sistem tidak hanya dapat mendeteksi dan menganalisis ancaman secara menyeluruh, tetapi juga dapat merespons ancaman dengan cepat.

Berikut penjelasan dari rancangan sistem pada gambar 2:

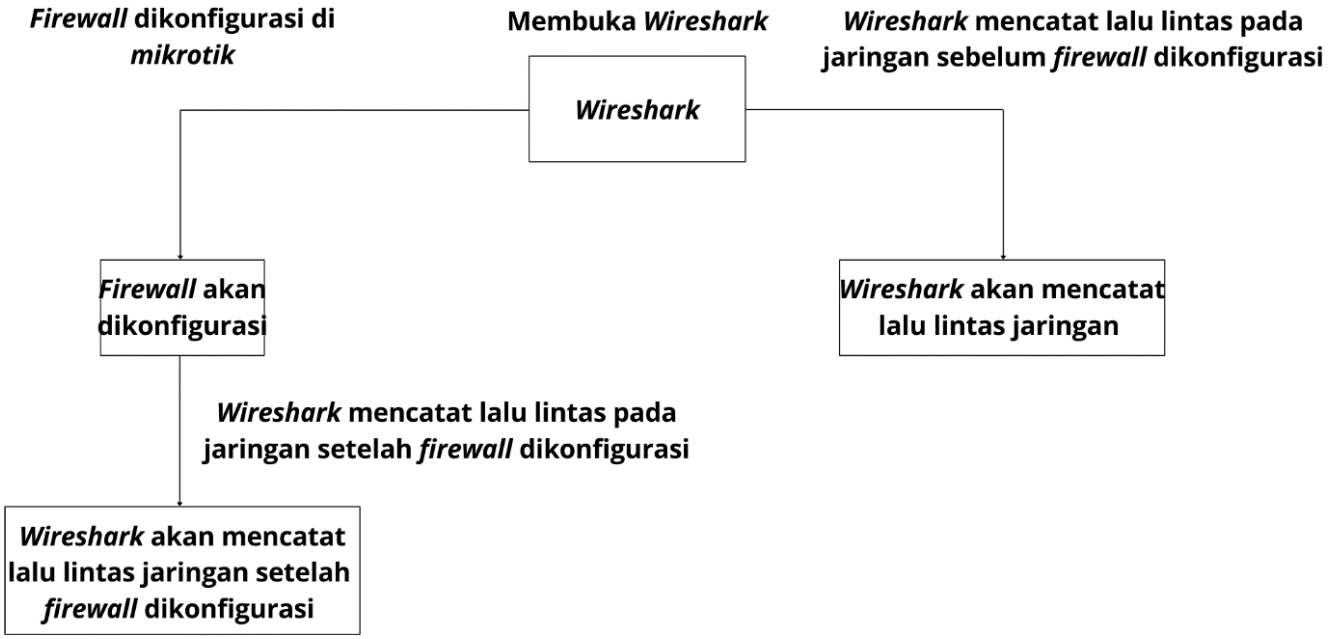
*Wireshark* mencatat lalu lintas jaringan sebelum mengaktifkan *firewall* di *MikroTik.*

- Semua paket data yang dikirim dan diterima dicatat oleh *Wireshark* tanpa batasan atau filter *firewall* apa pun.
- Setelah *firewall* diaktifkan dan dikonfigurasi di *MikroTik*, aturan keamanan yang telah ditentukan sebelumnya diaktifkan.
- *Wireshark* akan mencatat paket data pada lalu lintas jaringan setelah menerapkan aturan *firewall.*
- Hanya paket data yang memenuhi kriteria aturan *firewall* yang diizinkan atau diblokir, dan ini tercermin dalam data yang dicatat oleh *Wireshark*.




Gambar 2. Rancangan sistem

C. *Metode Penelitian*




Gambar 3. Blok diagram

Dalam penelitian ini, metode yang digunakan adalah *Quality of Service (QoS)*, di mana sistem kerjanya adalah mengukur dan menganalisis kinerja jaringan berdasarkan parameter-parameter *QoS* seperti *latency*, *jitter*, *throughput*, dan *packet loss*. Metode penelitian ini dimaksudkan untuk mendukung keamanan jaringan melalui penggunaan *firewall*

dan *Wireshark*. Implementasi metode ini mengharuskan *administrator* untuk menginstal *Wireshark* dan memantau lalu lintas jaringan yang ditangkap oleh *Wireshark*. Selain itu, metode ini juga memerlukan konfigurasi *firewall* untuk memastikan bahwa hanya pengguna yang berwenang yang memiliki akses, serta untuk memblokir akses yang mencurigakan atau berbahaya.

Berikut adalah penjelasan mengenai urutan langkah dalam gambar 3 blok diagram pada Implementasi *Wireshark* dan *Firewall* Untuk Mendukung Trafik Keamanan Jaringan.

1) *Membuka aplikasi Wireshark.*

2) *Wireshark mencatat lalu lintas sebelum firewall diaktifkan*.
- *Wireshark* adalah alat untuk menangkap dan menganalisis paket jaringan secara mendetail. Sebelum konfigurasi *firewall* diaktifkan, *Wireshark* digunakan untuk mencatat dan mengamati lalu lintas jaringan.
- Pada tahap ini, *Wireshark* menangkap semua paket yang melewati jaringan tanpa ada konfigurasi *firewall*. Ini memberikan gambaran awal tentang semua jenis lalu lintas, termasuk *website* yang tidak aman yang akan melalui jaringan.
- Gambar *Wireshark* di sebelah kanan menunjukkan tampilan standar *Wireshark* dengan berbagai informasi seperti *source*, *destination*, *protocol*, dan *info* dari paket yang ditangkap sebelum *firewall* diaktifkan. Ini menunjukkan data mentah yang tidak di *filter* oleh aturan *firewall*.

3) *Wireshark mencatat lalu lintas setelah firewall dikonfigurasi*.
- Setelah *firewall* di *MikroTik* dikonfigurasi dan diaktifkan, *Wireshark* kembali digunakan untuk mencatat lalu lintas jaringan.
- Pada tahap ini, *Wireshark* akan menunjukkan perubahan pada lalu lintas yang disebabkan oleh *firewall* yang telah dikonfigurasi.
- Setelah *firewall* diaktifkan, gambar *Wireshark* di kiri bawah menunjukkan tampilan *Wireshark* yang mencatat paket. Beberapa jenis lalu lintas telah berubah karena telah diblokir.

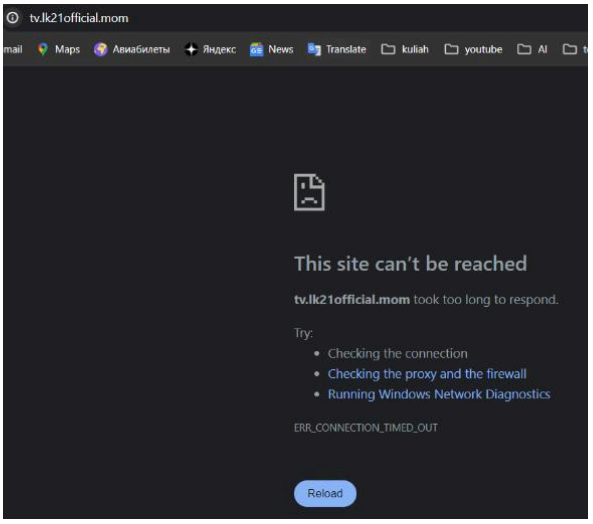
### *D. Teknik Pengujian*

Teknik pengujian *QoS* (*Quality of Service*) digunakan setelah data terkumpul guna mengevaluasi kinerja jaringan secara objektif. *QoS* merupakan parameter penting dalam menilai kualitas transmisi data, khususnya dalam hal keandalan dan efisiensi jaringan. Setelah konfigurasi *firewall* selesai, *Wireshark* akan dijalankan kembali untuk melakukan *capture* data dari *website* yang telah diblokir. Proses ini memastikan bahwa *firewall* berfungsi sesuai dengan yang diharapkan. Data yang diperoleh dari *Wireshark* akan dianalisis lebih lanjut menggunakan *metrix-metrix* utama *QoS* seperti *throughput*, *packet loss*, *delay*, dan *jitter*. *Metrix-metrix* ini memberikan gambaran menyeluruh mengenai performa jaringan setelah implementasi *firewall*, memastikan bahwa langkah-langkah keamanan yang diterapkan tidak mengorbankan kualitas layanan jaringan. Dengan demikian, pengujian ini tidak hanya mengonfirmasi keberhasilan blokir, tetapi juga menilai dampak konfigurasi *firewall* terhadap kualitas jaringan yang digunakan.

## III. HASIL DAN PEMBAHASAN

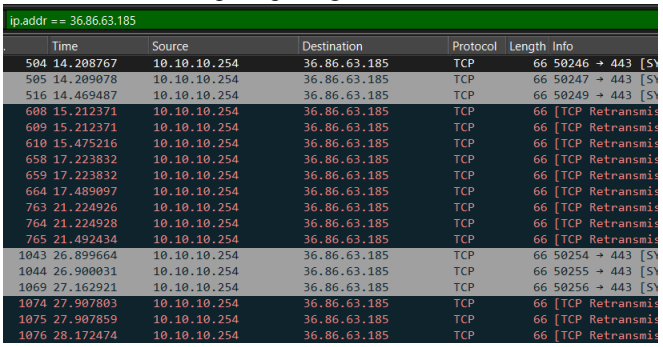
### *A. Hasil*

Setelah firewall dikonfigurasi di *mikrotik, website* yang tidak aman tidak akan terbuka karena *IP website* tersebut sudah terblokir di *firewall mikrotik*, seperti gambar 4.




Gambar 4. *Website* yang tidak aman

Saat menjalankan *wireshark, IP* website tersebut akan berubah menjadi merah karena *IP* tersebut sudah diblokir di *Firewall mikrotik*, seperti pada gambar 5.




Gambar 5. *IP* website yang dituju

1) *Hasil pengujian dengan QoS*

Standar THIPON menguji berbagai parameter utama untuk mengevaluasi kualitas layanan (*Quality of Service/QoS*) jaringan internet. *Throughput* yang mengukur kecepatan transfer data dalam jaringan, *Packet Loss* yang menunjukkan persentase data yang hilang selama transmisi, *Delay* yang mengukur waktu yang dibutuhkan data untuk berpindah dari satu tempat ke

tempat lain, dan *Jitter* yang mengukur variasi waktu keterlambatan pengiriman paket data. Standar THIPON menunjukkan kinerja dan keandalan jaringan internet melalui pengujian parameter ini. Tabel V menunjukkan hasil pengujian dari QoS.

TABEL V
HASIL PENGUJIAN QoS

| Qos | | | | | | | |
|---|---|---|---|---|---|---|---|
| *Throughput* | | *packet loss* | | *Delay* | | *Jittler* | |
| Rata-Rata | Index | Rata-Rata | Index | Rata-Rata | Index | Rata-Rata | Index |
| 1.972 Kbit | 4 | 2,6% | 4 | 270 ms | 3 | 0,387104012 ms | 4 |

*2) Hasil pengujian dengan rumus efektivitas*

Perhitungan yang menggunakan rumus efektivitas mendapatkan hasil yang berbeda dari 2 percobaan yang dilakukan. Percobaan yang menggunakan laptop menunjukkan hasil yang lebih baik dibandingkan dengan percobaan yang menggunakan *handphone.* Pada laptop, diperoleh nilai bahwa dari 20 *website* yang tidak aman, semuanya terblokir (100%), dari 15 *website* yang aman, hanya 6 yang tidak terblokir (40%). Sementara itu, pada *handphone*, dari 20 *website* yang tidak aman, hanya 8 yang terblokir (40%), dan dari 15 *website* yang aman, hanya 6 yang tidak terblokir (40%). Hal ini menunjukkan bahwa laptop memberikan performa yang lebih baik dalam hal blokir *website* tidak aman (100%) dibandingkan dengan *handphone*.

*B. Pembahasan*

*1) Menghitung nilai efektivitas dari percobaan yang menggunakan handphone*

- $Efektivitas = \frac{8}{20} \times 100\%$
  $= 40\%$

*Website* yang tidak aman tersebut dibuka di *handphone*, dan 8 di antaranya berhasil diblokir.

- $Efektivitas = \frac{6}{15} \times 100\%$
  $= 40\%$

*Website* yang aman tersebut dibuka di *handphone*, dan 6 di antaranya tidak terblokir.

*2) Menghitung nilai efektivitas dari percobaan yang menggunakan laptop*

- $Efektivitas = \frac{20}{20} \times 100\%$
  $= 100\%$

*Website* yang tidak aman tersebut dibuka di laptop dan berhasil diblokir 100%.

- $Efektivitas = \frac{6}{15} \times 100\%$
  $= 40\%$

*Website* yang aman tersebut dibuka di laptop, dan 6 di antaranya tidak terblokir.

Pada laptop, 20 *website* tidak aman terblokir sepenuhnya (100%), tetapi 6 dari 15 *website* aman tidak terblokir (40 %). Pada *handphone*, 8 dari 20 *website* tidak aman terblokir (40%), dan 6 dari 15 *website* aman tidak terblokir (40%).

## IV. KESIMPULAN

Kesimpulan dari penelitian ialah sebagai berikut:

Sistem keamanan pengguna yang terhubung ke jaringan yang telah diimplementasi *firewall* cukup baik dalam menjaga integritas, kerahasiaan, dan ketersediaan data pada laptop dan *handphone*. Ketika membuka *website* yang tidak aman menggunakan laptop, *website* tersebut tidak bisa diakses, sementara di *handphone*, hanya 8 *website* tidak aman yang berhasil diblokir. Sedangkan membuka *website* yang aman pada laptop dan *handphone* sama-sama hanya 6 *website* yang terbuka.

Analisis *traffic* jaringan yang menggunakan *wireshark* cukup membantu untuk mendeteksi aktivitas mencurigakan karena *wireshark* menangkap *ip website* yang tidak aman. Setelah menangkap *IP website* yang tidak aman, *wirehark* akan menampilkan di *I/O Graphs* dalam bentuk bar warna merah.

*Firewall* efektif dalam mengelola lalu lintas jaringan pada laptop sedangkan cukup efektif dalam mengelola lalu lintas jaringan pada *handphone*. Dengan menggunakan rumus efektivitas, website yang tidak aman ketika dibuka di *hanphone* hanya 8/20 atau 40% *website* yang tidak aman yang tidak bisa dibuka sedangkan *website* yang tidak aman ketika dibuka di laptop 20/20 atau 100% *website* yang tidak aman tidak bisa dibuka. Sedangkan *website* yang aman ketika dibuka di laptop dan *handphone* sama-sama hanya 6/15 atau 40% *website* yang terbuka.

*Firewall* dapat mempengaruhi hasil percobaan yang dilakukan menggunakan laptop dan *handphone*. Dengan melihat hasil dari efektivitas dari kedua percobaan tersebut. Percobaan yang menggunakan laptop mendapatkan hasil 100% untuk *website* yang tidak aman, sedangkan percobaan yang menggunakan *handphone* hanya mendapatkan 40% untuk *website* yang tidak aman.

## REFERENSI

A. Wahid, M. E. Firdaus, and J. M. Parenreng, "Implementation of Wireshark and IPtables Firewall Collaboration to Improve Traffic Security on Network Systems," *Internet of Things and Artificial Intelligence*

*Journal*, vol. 1, no. 4, pp. 249–264, Oct. 2021, doi: 10.31763/iota.v1i4.509.

[2] zen Munawar and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data," Jun. 2020.

[3] G. H. A. Kusuma, "Perancangan Skema Sistem Keamanan Jaringan Web Server Menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19," *Journal of Informatics and Advanced Computing*, vol. 2, no. 2, pp. 1–4, 2021.

[4] S. Hidayat, A. Silvanie, A. Asistyasari, and Y. Nuryaman, "Optimalisasi Manajemen Trafik Dan Keamanan Data Pada Jaringan Intranet IBI-K 1957 DENGAN METODE USER BEHAVIOUR ANALYSIS," *Universitas Bina Sarana Informatika*, vol. 7, no. 2, pp. 312–321, Jul. 2023.

[5] D. A. Jakaria and A. Yulianeu, "Implementasi Firewall Dan Web Filtering Pada Mikrotik Routeros Untuk Mendukung Internet Sehat Dan Aman (INSAN)," *Jurnal Teknik Informatika*, vol. 8, no. 2, pp. 76–83, 2020.

[6] Anwar, Mursyidah, and W. Rahma, "Perancangan Jaringan Multi Protocol Label Switching Menggunakan Mikrotik Routerboard RB951Ui," *Jurnal Infomedia: Teknik Informatika, Multimedia & Jaringan*, vol. 6, no. 1, pp. 39–44, Jun. 2021.

[7] Sulasminarti and T. Gunawan, "Konfigurasi Gateway Server Pada Dinas Komunikasi Dan Informatika Kabupaten Pesawaran," *Jurnal Informatika Software dan Network*, vol. 02, no. 01, pp. 1–7, Apr. 2021.

[8] V. D. Lestari, "Implementasi Efektivitas Pengendalian Intern Pada Sistem Informasi Akuntansi Penggajian," 2023.

[9] A. P. Supriyadi and F. Ahmad, "Analisis Rasio Efektivitas PAD Terhadap Kinerja Keuangan Daerah Kota Jakarta Periode 2015-2019," *Jurnal Akuntansi dan Keuangan*, vol. 8, no. 1, pp. 39–43, May 2021.

[10] M. Hasbi and N. R. Saputra, "Analisis Quality Of Service (QoS) Jaringan Internet Kantor Pusat King Bukopin Dengan Menggunakan Wireshark," Jakarta, Sep. 2021.