JISTI: Jurnal Ilmu Komputer, Sistem Informasi dan Teknologi Informasi
ISSN 3090-0174 (Media Online)
Vol 1, No 2, Juli 2025 | Hal 79–86
https://newjurnal.itbi.ac.id/index.php/JISTI

Implementasi Keamanan Jaringan Firewall Filtering Berbasis Mikrotik

Mutiarani Sinaga[1], Periman Lafau[1], Erna Simbolon[1], Santi Rosalinda Sihombing[1], David JM Sembiring[2,*]

[1]Fakultas Sains dan Teknologi, Program Studi Sistem Informasi, Institut Teknologi dan Bisnis Indonesia, Medan, Indonesia
[2]Fakultas Sains dan Teknologi, Program Studi Teknik Informatika, Institut Teknologi dan Bisnis Indonesia, Medan, Indonesia
Email: [1]mutiaranisinaga12345@gmail.com, [2]perrylafau@gmail.com, [3]simbolone037@gmail.com, [4]santisihombing2002@gmail.com, [5,*]davidjmsembiring@gmail.com
Email Penulis Korespondensi: davidjmsembiring@gmail.com

Abstrak-Perkembangan teknologi jaringan telah beralih dari kabel ke Wireless Local Area Network (WLAN), memungkinkan perangkat terhubung dan mengakses internet tanpa kabel, memberikan fleksibilitas lebih. Penggunaan internet meluas ke berbagai sektor, seperti pemerintah, perusahaan, dan sekolah, memudahkan aktivitas. Namun, penggunaan internet yang tidak bijak dapat menyebabkan dampak negatif, seperti mengakses situs tidak relevan atau masuk ke server ilegal, yang mengganggu keamanan jaringan dan kinerja, seperti di Adam Net. Untuk mengatasi masalah ini, diperlukan penerapan Firewall Filtering menggunakan router Mikrotik, yang dapat mengontrol lalu lintas jaringan dan membatasi akses ke situs tertentu, meningkatkan keamanan jaringan di Adam Net.

Kata Kunci: Keamanan Jaringan; WLAN; Firewall; Filtering; Mikrotik

Abstract-The development of network technology has shifted from cables to Wireless Local Area Networks (WLAN), allowing devices to connect and access the internet without cables, providing more flexibility. Internet use extends to various sectors, such as governments, companies and schools, making activities easier. However, unwise use of the internet can cause negative impacts, such as accessing irrelevant sites or logging into illegal servers, which compromise network security and performance, such as on Adam Net. To overcome this problem, it is necessary to implement Firewall Filtering using a Mikrotik router, which can control network traffic and limit access to certain sites, increasing network security on Adam Net

Keywords: Network Security; WLAN; Firewall; Filtering; Mikrotik

1. PENDAHULUAN

Dengan pesatnya perkembangan teknologi informasi di era digital saat ini, sistem teknologi informasi menjadi sangat penting dan, secara bersamaan, menjadi target utama ancaman keamanan. Dalam konteks ini, keamanan jaringan menjadi aspek krusial bagi perusahaan karena data dan infrastruktur yang dikelola harus dilindungi dari potensi serangan. Teknologi informasi mempermudah proses pertumbuhan perusahaan serta perlindungan data, dan meningkatkan signifikansi infrastruktur jaringan, yang semakin kompleks dan vital. Pertumbuhan teknologi informasi juga membawa dampak positif yang signifikan terhadap jangkauan dan hubungan antara pengguna, serta memperkuat keamanan di lingkungan digital. Salah satu komponen penting dari keamanan jaringan adalah firewall filtering, yang berfungsi untuk mengontrol dan memantau lalu lintas data di jaringan. Firewall filtering ini membantu mencegah akses yang tidak sah dan melindungi sistem dari berbagai ancaman dengan memeriksa dan mengatur data yang masuk dan keluar dari jaringan.

Jaringan WLAN (Wireless Local Area Network) yang digunakan oleh Adam Net menyediakan fasilitas untuk menghubungkan berbagai komputer secara nirkabel dan anonim. Ini berarti pengguna dapat terhubung ke jaringan tanpa harus mengungkapkan identitas mereka atau tanpa memerlukan kabel fisik, yang memberikan tingkat fleksibilitas dan kemudahan akses yang tinggi. Adam Net beroperasi sebagai penyedia layanan internet (ISP) skala kecil, dan sebagai ISP kecil, mereka memiliki kapasitas untuk menawarkan layanan yang lebih personal dan mungkin lebih terjangkau bagi pelanggannya. Namun, karena skala yang relatif kecil dan sifat dari jaringan nirkabel yang memungkinkan koneksi anonim, Adam Net juga menghadapi risiko tertentu. Jika jaringan ini tidak dikelola dengan baik atau digunakan secara tidak bertanggung jawab, dapat menimbulkan masalah serius.

Seiring dengan meningkatnya jumlah pengguna internet yang memanfaatkan layanan ini, muncul tantangan tambahan. Banyak individu mulai mencoba mengakses server Adam Net secara ilegal atau menggunakan layanan internet tanpa membayar biaya langganan yang sah. Hal ini meningkatkan risiko penyalahgunaan jaringan dan potensi kerugian bagi Adam Net, baik dari segi keamanan data maupun dari segi finansial. Dengan demikian, penting bagi Adam Net untuk mengimplementasikan langkah-langkah keamanan yang efektif untuk melindungi jaringan mereka dari penyalahgunaan dan memastikan bahwa layanan mereka tetap aman dan dapat diandalkan bagi pelanggan yang membayar dengan sah.

Dengan demikian, penggunaan firewall filtering berbasis mikrotik dianggap sebagai solusi optimal untuk keamanan jaringan karena efektivitas dan popularitasnya, terutama dalam industri teknologi informasi. Firewall filtering ini bekerja dengan memeriksa dan mengontrol lalu lintas data yang masuk dan keluar dari jaringan, membantu melindungi sistem dari ancaman eksternal.

Mikrotik sebagai perangkat keras yang digunakan dalam firewall filtering, berfungsi sebagai router jaringan yang andal. Router ini memainkan peran penting dalam menghubungkan berbagai jaringan satu dengan yang lainnya. Mikrotik mengelola lalu lintas data dengan mengarahkan paket-paket informasi ke alamat IP yang tepat sesuai dengan aturan yang telah ditetapkan. Ini memastikan bahwa hanya data yang sah dan diizinkan yang dapat melewati jaringan, sementara data yang tidak diinginkan atau berpotensi berbahaya dapat diblokir atau ditangani sesuai kebutuhan.

Dalam konteks ini, penulis mengembangkan sebuah sistem keamanan jaringan dengan tujuan untuk menilai dan menguji efektivitas implementasi firewall filtering berbasis mikrotik pada jaringan Adam Net. Sistem keamanan ini dirancang untuk mengidentifikasi kekuatan dan kelemahan dari firewall filtering yang diterapkan, serta bagaimana hal

tersebut mempengaruhi keamanan keseluruhan jaringan. Dengan menggunakan sistem ini, penulis berharap dapat menemukan solusi yang tepat dan efektif untuk memperbaiki dan meningkatkan keamanan jaringan Adam Net. Tujuan utamanya adalah mengurangi risiko yang terkait dengan berbagai ancaman keamanan, seperti serangan malware yang dapat merusak sistem atau mencuri data sensitif. Melalui evaluasi yang mendalam dan penerapan solusi yang diusulkan, diharapkan jaringan Adam Net akan menjadi lebih aman dan terlindungi dari potensi ancaman di masa depan.

Terkait dengan Implementasi Keamanan Jaringan Firewall Filtering Berbasis Mikrotik Pada Adam Net, sudah pernah diteliti oleh peneliti sebelumnya antara lain : Fauzan Prasetyo Eka Putra, dkk (2023). Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking. Cara implementasi dari sistem keamanan jaringan Mikrotik ini menggunakan firewall filtering dan port knocking. Perbedaan yang terdapat pada skripsi yang dibuat oleh penulis dan yang dibuat oleh peneliti sebelumnya adalah penulis membuat sistem keamanan jaringan berbasis mikrotik menggunakan firewall filtering sedangkan peneliti sebelumnya menggunakan metode port knocking.

Deni Ahmad Jakaria (2020). Implementasi Firewall dan Web Filtering Pada Mikrotik Routeros Untuk Mendukung Internet Sehat dan Aman (INSAN). Dengan menggunakan Layer 7 firewall diharapkan dapat menyaring konten yang tidak pantas. Layer 7 firewall melakukan penapisan konten web berdasarkan kata kunci. Implementasi firewall Layer 7 dapat diterapkan diantaranya menggunakan perangkat routerboard mikroTik. Perbedaan yang terdapat pada skrispsi yang dibuat oleh penulis dan yang dibuat oleh peneliti sebelumnya adalah penulis menggunakan filtering IP Address sedangkan peneliti sebelumnya menggunakan web filtering.

Ridatu Ocanitra, Muhamad Ryansyah (2019). Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen. Dengan adanya sistem keamanan ini mampu untuk menjaga data perusahaan, serta untuk mengontrol dan mengintegrasikan semua penguna koneksi jaringan. Perusahaan ini dengan banyak karyawan dan divisi yang berbeda-beda sehingga sering dilakukan perpindahan tempat kerja atau adanya karyawan baru. Perbedaan yang terdapat pada skripsi yang dibuat oleh penulis dan yang dibuat oleh peneliti sebelumnya adalah penulis membuat sistem keamanan jaringan berbasis mikrotik menggunakan firewall filtering sedangkan peneliti sebelumnya menggunakan metode default atau static port security, port security dynamic learning dan sticky port security.

2. METODOLOGI PENELITIAN

2.1 Keamanan Jaringan

Keamanan jaringan komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Sistem keamanan jaringan komputer harus dilindungi dari segala macam serangandan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Sistem deteksi penyusup jaringan yang ada saat ini umumnya mampu mendeteksi berbagai jenis serangan tetapi tidak mampu mengambil tindakan lebih lanjut.

2.2 Jaringan Komputer

Jaringan komputer merupakan sistem yang terdiri atas dua atau lebih komputer serta perangkat-perangkat lainnya yang saling terhubung. Media pernghubung tersebut dapat berupa kabel atau nirkabel sehingga memungkinkan para pengguna jaringan komputer melakukan pertukaran informasi, seperti berbagi file, dokumen, data serta menggunakan perangkat keras dan perangkat lunak yang terhubung ke jaringan

2.3 Firewall Filtering

Firewall merupakan suatu cara / sistem / mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server. router, atau local area network (LAN)

3. HASIL DAN PEMBAHASAN

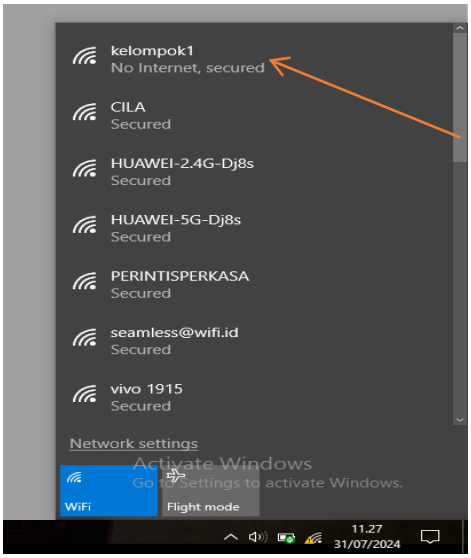
3.1 Analisa Masalah

Analisa jaringan yang berjalan adalah menganalisis jaringan yang sudah ada dan digunakan dalam objek penelitian dengan tujuan untuk mengidentifikasi permasalahan dan hambatan yang ada dalam jaringan tersebut serta memberikan usulan perbaikan atau pengembangan yang dapat diterapkan untuk meningkatkan kinerja dan efisiensi jaringan. Pada bagian ini peneliti menganalisa jaringan yang sudah digunakan pada Adam Net. Adam Net merupakan perusahaan berskala kecil yang menggunakan jaringan internet setiap harinya agar mempermudah aktivitas perusahaan yang didalamnya terdapat beberapa komputer atau PC yang saling terhubung satu sama lain serta memiliki suatu komputer yang dijadikan sebagai server. Server tersebut akan terhubung pada jaringan internet sehingga komputer yang lainnya yang terhubung dengan komputer server atau disebut client dapat terhubung secara bersamaan ke jaringan internet publik.

3.2 Penerapan Firewall

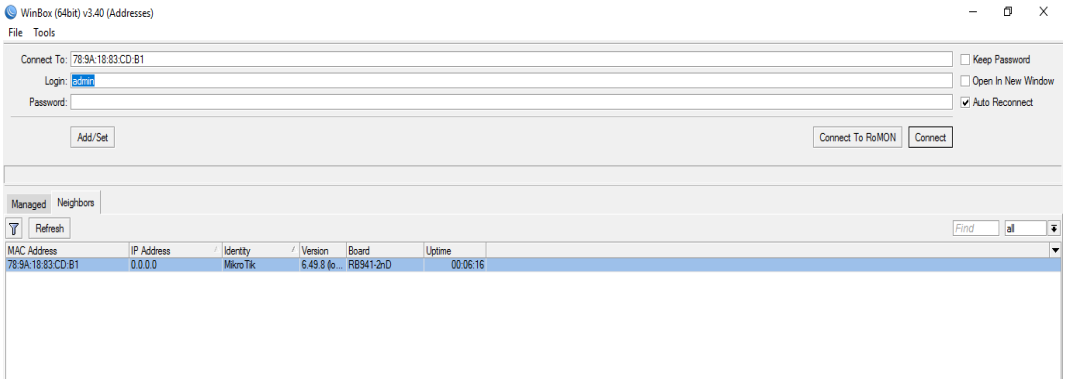
JISTI: Jurnal Ilmu Komputer, Sistem Informasi dan Teknologi Informasi
ISSN 3090-0174 (Media Online)
Vol 1, No 2, Juli 2025 | Hal 79–86
https://newjurnal.itbi.ac.id/index.php/JISTI

Sebelum mensetting mikrotik, kita perlu membuat jaringan wifi yang mana jaringan ini harus bisa ditangkap atau diakses oleh perangkat yang akan digunakan. Setelah jaringan Wifi berhasil dibuat dan di setting pada acces point, kita perlu menghubungkan perangkat (server) kita ke jaringan wifi tersebut. Setelah perangkat terhubung ke jaringan Wifi yang telah kita buat, kita bisa membuka aplikasi winbox.



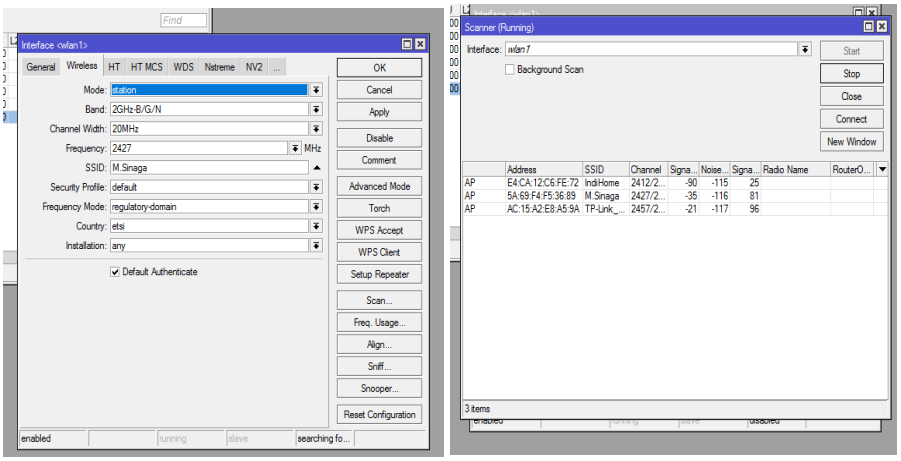
Gambar 1. Jaringan Wifi yang akan ditangkap oleh perangkat (client)

Ketika winbox dibuka, kita akan melihat perangkat mikrotik yang terhubung dengan IP address 0.0.0.0 dalam daftar perangkat yang terdeteksi.



Gambar 2. Perangkat mikrotik dengan IP Address 0.0.0.0

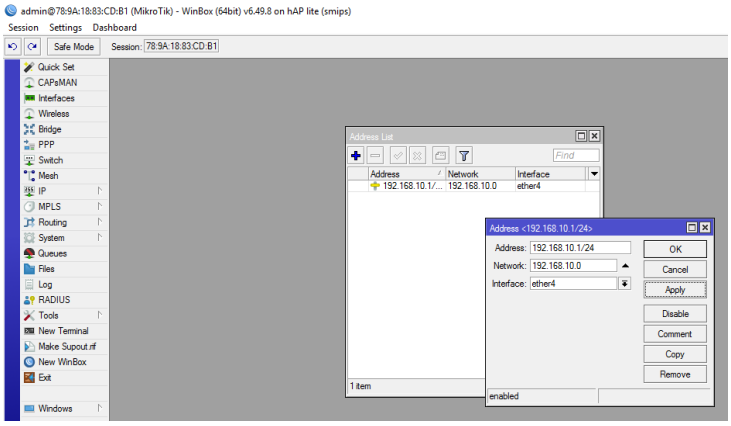
Setelah itu, mulai dengan menghubungkan (connect) ke perangkat mikrotik yang terdeteksi. Setelah berhasil terhubung, aktifkan WLAN dengan cara memindai (scan) hotspot yang tersedia. Double klik pada WLAN diantar muka Mikrotik – pilih opsi Scan - Klik “start” untuk memulai pemindaian hotspot – cari dan pilih hotspot yang ingin digunakan – klik connect untuk mengubungkan ke hotspot tersebut.



Gambar 3. Mengaktifkan WLAN dan pilih hotspot

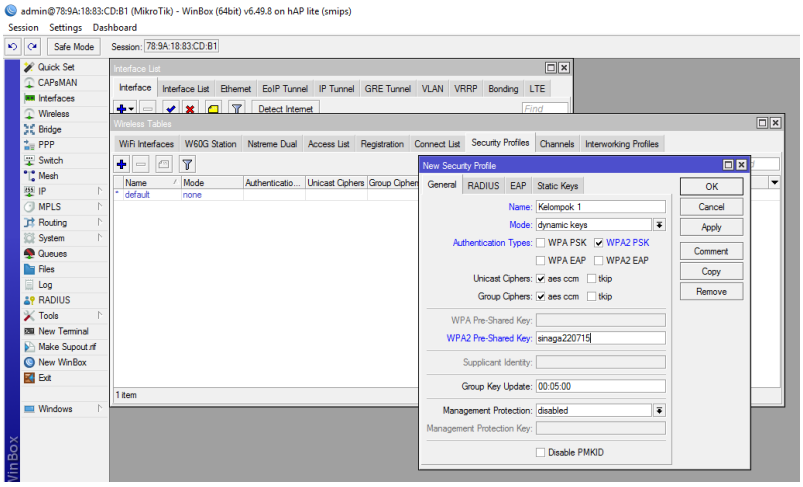
JISTI: Jurnal Ilmu Komputer, Sistem Informasi dan Teknologi Informasi
ISSN 3090-0174 (Media Online)
Vol 1, No 2, Juli 2025 | Hal 79–86
https://newjurnal.itbi.ac.id/index.php/JISTI

Setelah terhubung ke hotspot, tentukan IP address untuk ethernet yang aktif, klik menu IP – address – add – isikan dengan IP address 192.168.10.1/24 – interface: ether yang aktif.



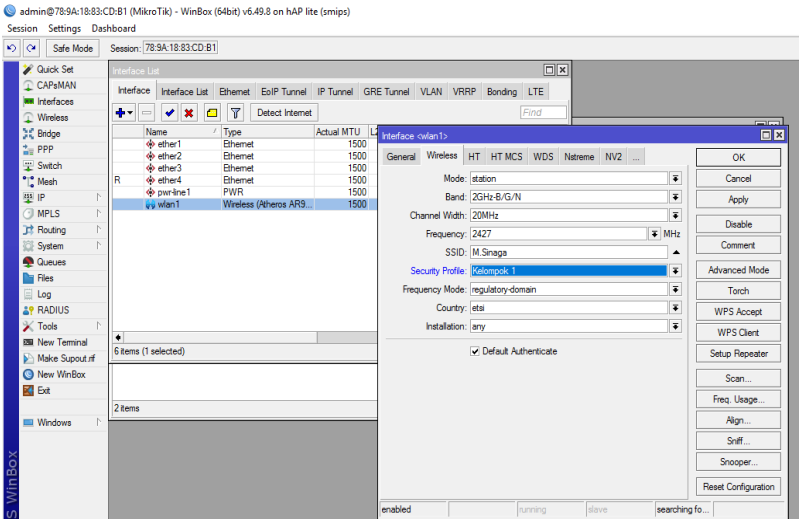
Gambar 4. Setting IP address

Setelah IP address untuk ethernet yang aktif telah di atur, setting security profile dengan cara : klik menu "Wireless" – pilih "security profile"- add – ganti nama profile dengan nama yang diinginkan – Mode : dynamic keys – Authentic Types : WPA2 PSK – Pre shared key isikan password – Apply – Ok.



Gambar 5. Setting security profile

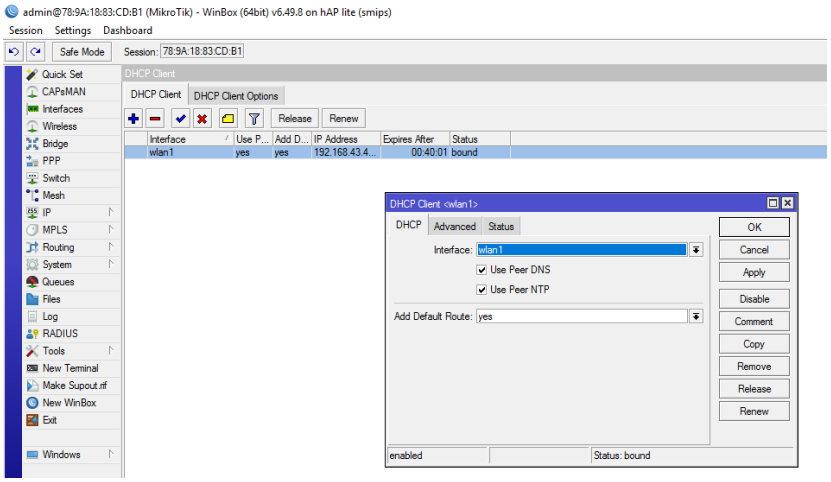
Setelah itu, kembali ke menu interface – klik WLAN – ganti security profile menjadi nama profile yang telah dibuat tadi – Apply –Oke.



Gambar 6. Ganti security profile

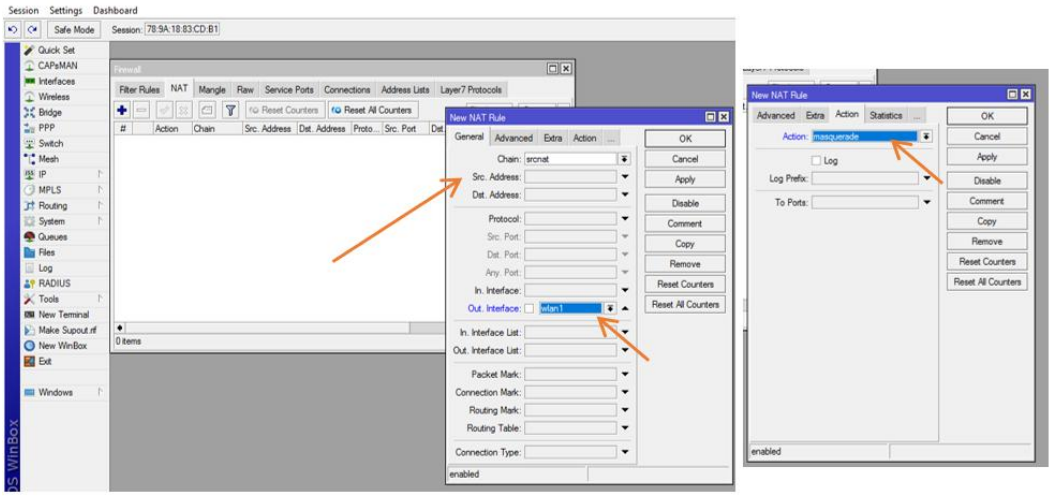
Setelah itu setting DHCP Client dengan cara : Menu IP – DCHP Client – add – interface : Wlan 1 – Apply – Ok.

JISTI: Jurnal Ilmu Komputer, Sistem Informasi dan Teknologi Informasi
ISSN 3090-0174 (Media Online)
Vol 1, No 2, Juli 2025 | Hal 79–86
https://newjurnal.itbi.ac.id/index.php/JISTI



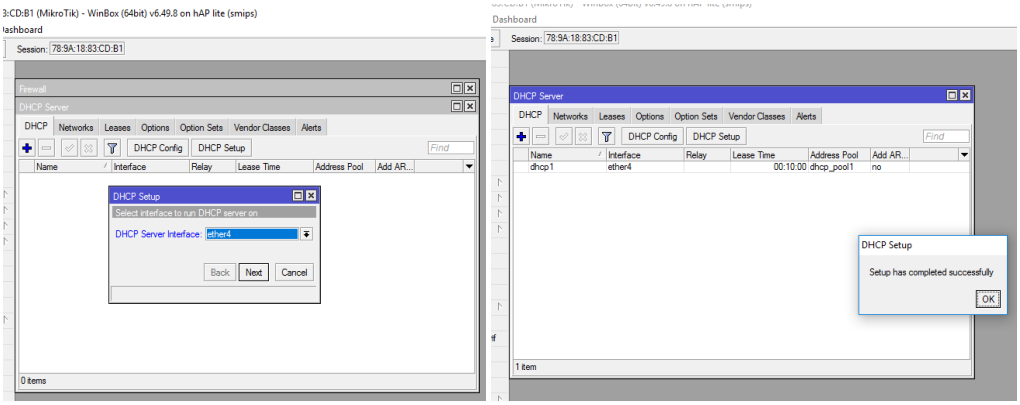
Gambar 7. Interface dari DHCP Client diubah menjadi Wlan1

Selanjutnya adalah setting Firewall dengan cara klik menu IP – Firewall – NAT – General - pilih Chain : scrnat – Out interface : Wlan1 – klik Action pilih masquerade – Apply – Ok.



Gambar 8. Setting Firewall

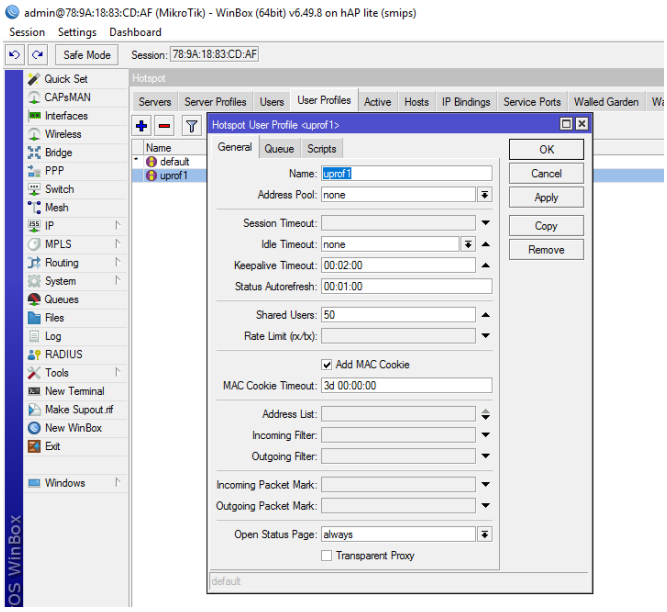
Selanjutnya setting DHCP Server dengan cara : klik menu IP – DHCP Server – klik DHCP Setup – tentukan DHCP Server Interface yang aktif – klik Next sampai DNS Server berhasil dibuat.



Gambar 9. Setting DHCP Server

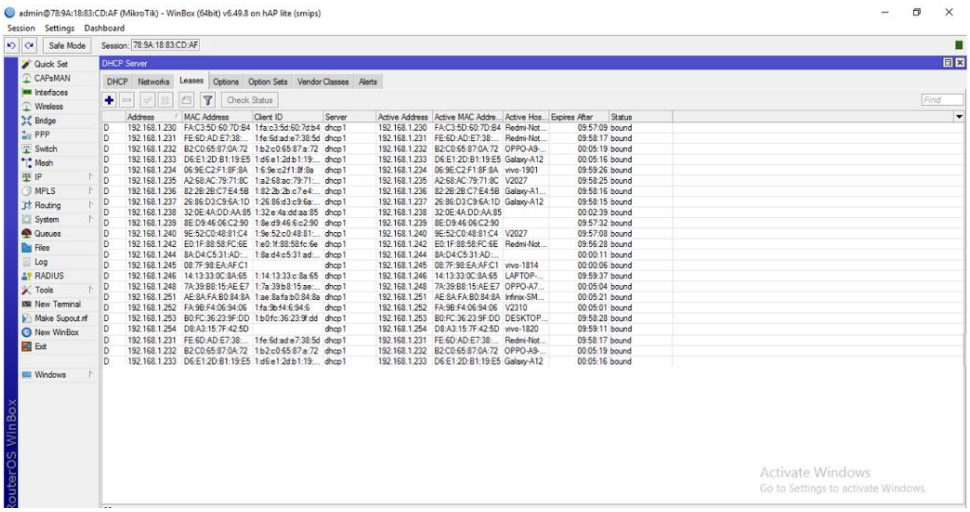
Selanjutnya Koneksi Wifi akan terhubung dengan mikrotik, tes koneksi di New Terminal atau bisa juga dengan melakukan pencarian (searching) di google. Setelah koneksi Wifi terhubung, perangkat lain akan masuk ke jaringan dan akan di filtering menggunakan firewall dengan cara klik menu IP – DHCP Server – Leases. Dalam penelitian ini penulis membatasi perangkat yang akan masuk ke dalam jaringan sebanyak 30 (tiga puluh) perangkat (client). Cara untuk membatasinya yaitu dengan mengklik menu IP – Hotspot – double klik User Profiles – Add – General – Shared User : sebanyak 30 (tiga puluh) – Apply – Oke.

JISTI: Jurnal Ilmu Komputer, Sistem Informasi dan Teknologi Informasi
ISSN 3090-0174 (Media Online)
Vol 1, No 2, Juli 2025 | Hal 79–86
https://newjurnal.itbi.ac.id/index.php/JISTI



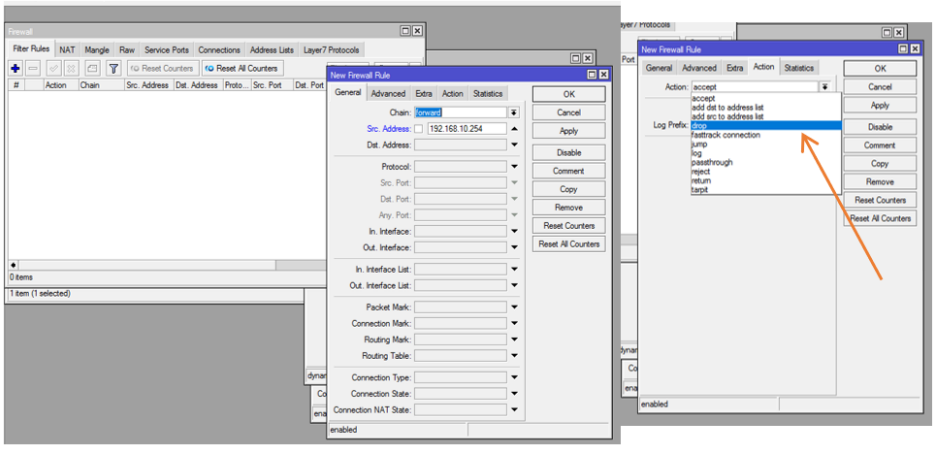
Gambar 10. Membatasi perangkat yang masuk kedalam jaringan

Didalam menu leases perangkat yang masuk kedalam jaringan akan tertera seperti gambar di bawah ini.



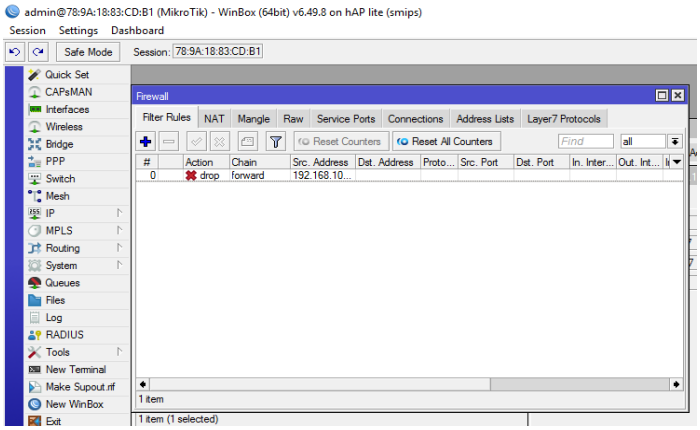
Gambar 11. Perangkat-perangkat yang terhubung kedalam jaringan.

Selanjutnya yaitu double klik salah satu perangkat yang tidak diinginkan lalu copy IP Addressnya.Kemudian klik menu IP – Firewall – Filter Rules – Add – klik General. Pastekan IP Address yang sudah di copy di Src.Address, lalu klik Action pilih action : drop.



Gambar 12. Setting Firewall untuk memblokir perangkat

Firewall berhasil dibuat dan perangkat yang sudah diblok tadi tidak dapat mengakses internet.



Gambar 13. Perangkat yang tidak diinginkan berhasil di blok

3.2 Pembahasan

Dari penelitian yang telah kami lakukan, firewall filtering merupakan salah satu metode keamanan jaringan yang berfungsi untuk memfilter lalu lintas jaringan berdasarkan aturan yang ditentukan. Analisis yang dilakukan dalam penelitian ini mengungkapkan bahwa penerapan firewall filtering mampu meningkatkan keamanan jaringan dengan melakukan beberapa fungsi utama, antara lain:

1. Pemblokiran Akses Ilegal: Firewall memblokir akses ke port dan protokol yang tidak diizinkan, mencegah pengguna tidak sah mengakses sumber daya internal.
2. Pemantauan Lalu Lintas: Firewall mampu memantau dan mencatat lalu lintas masuk dan keluar, memungkinkan administrator untuk mengidentifikasi aktivitas yang mencurigakan.
3. Pengaturan Kebijakan Akses: Penerapan aturan filtering memungkinkan untuk mengontrol akses berdasarkan alamat IP, protokol, dan aplikasi, memberikan fleksibilitas dalam pengelolaan keamanan.

Proses perancangan jaringan firewall filtering dimulai dengan identifikasi kebutuhan keamanan dan karakteristik jaringan yang akan dilindungi. Langkah awal perancangan melibatkan analisis komponen jaringan, seperti server, router, dan perangkat pengguna akhir, untuk memahami jenis lalu lintas yang harus diamankan. Setelah itu, kebijakan keamanan disusun berdasarkan hasil analisis potensi ancaman. Kebijakan ini mencakup pemblokiran port tertentu, pembatasan akses, serta prioritas pada lalu lintas yang dianggap penting bagi kelancaran operasional jaringan.

Langkah selanjutnya adalah pemilihan tipe firewall yang sesuai dengan kebutuhan jaringan. Setelah itu, aturan filtering disusun untuk mengizinkan atau menolak lalu lintas berdasarkan berbagai parameter, seperti alamat IP, protokol, dan nomor port, dengan Access Control List (ACL) sebagai landasan utama.

Implementasi firewall filtering dilakukan melalui beberapa langkah penting. Langkah pertama adalah penerapan konfigurasi firewall, di mana kebijakan keamanan dan aturan filtering yang telah disusun sebelumnya diterapkan pada perangkat firewall. Proses ini mencakup memasukkan aturan filtering ke dalam Access Control List (ACL) yang ada di perangkat firewall, memastikan semua aturan berjalan sesuai dengan desain awal. Setelah konfigurasi selesai, dilakukan uji coba untuk memastikan firewall bekerja dengan baik. Uji coba ini melibatkan simulasi serangan serta pengujian akses legal dan ilegal terhadap jaringan, dengan pemantauan real-time lalu lintas jaringan untuk mengevaluasi efektivitas firewall.

Setelah uji coba selesai, kami melakukan penyesuaian dan optimasi berdasarkan hasil pemantauan untuk memastikan firewall berfungsi lebih optimal. Dalam penelitian ini, kami berusaha menguji kapasitas dan kinerja jaringan dengan menghubungkan 30 (tiga puluh) perangkat (client) ke dalam sistem. Namun, selama pengujian, kami menemukan bahwa jaringan dan peralatan yang digunakan memiliki batasan tertentu. Secara khusus, sistem kami hanya mampu menampung maksimal 23 (dua puluh tiga) perangkat secara bersamaan. Kendala ini muncul akibat keterbatasan infrastruktur jaringan, termasuk keterbatasan kapasitas router dan kemampuan manajemen perangkat lunak yang tidak cukup memadai untuk menangani lebih dari 23 (dua puluh tiga) perangkat.

Setelah 23 (dua puluh tiga) perangkat berhasil terhubung ke jaringan, kami segera mengambil langkah-langkah untuk memutus akses mereka. Tindakan yang dilakukan meliputi penerapan aturan firewall yang lebih ketat dan pengaturan kebijakan akses yang lebih spesifik. Dengan langkah-langkah ini, perangkat yang telah masuk ke jaringan tidak lagi memiliki akses untuk menggunakan jaringan atau melakukan aktivitas apapun, sehingga jaringan kami tetap aman dan terlindungi dari potensi gangguan.

Penelitian ini bertujuan untuk mengevaluasi efektivitas implementasi perangkat ke dalam jaringan yang dirancang menggunakan mikrotik, dengan menggunakan metodologi perhitungan persentase keberhasilan. Dalam uji coba yang dilakukan, kami berusaha untuk mengukur persentase perangkat yang berhasil diintegrasikan ke dalam jaringan dari total perangkat yang diuji. Metode yang digunakan untuk menghitung persentase keberhasilan cukup sederhana namun efektif, yakni membandingkan jumlah perangkat yang berhasil terhubung dengan jumlah total perangkat yang diuji. Rumus yang digunakan adalah sebagai berikut :

$$\text{Persentase Keberhasilan} = \frac{\text{Jumlah Data yang Berhasil}}{\text{Jumlah data yang Diuji}} \text{ x } 100\% \quad (1)$$

Dengan rumus ini, kami memperoleh gambaran yang jelas mengenai performa jaringan dan kemampuan sistem dalam mengakomodasi sejumlah perangkat. Hasil penelitian menunjukkan bahwa dari 30 (tiga puluh) perangkat yang diuji, hanya 23 (dua puluh tiga) perangkat yang berhasil diintegrasikan dengan sukses.

Dengan menggunakan data tersebut, kami menerapkan rumus persentase keberhasilan untuk menghitung efektivitas keberhasilan perangkat ke dalam jaringan yaitu sebagai berikut :

$$\text{Persentase Keberhasilan} = \frac{23}{30} \text{ x } 100\% = 77\%$$

Persentase ini memberikan indikasi bahwa infrastruktur jaringan yang digunakan saat ini belum sepenuhnya optimal dalam menangani sejumlah perangkat yang lebih besar.

4. KESIMPULAN

Berdasarkan hasil penelitian dan implementasi yang telah dilakukan, dapat disimpulkan bahwa : Penelitian ini berhasil mengevaluasi efektivitas implementasi perangkat dalam jaringan yang dirancang menggunakan mikrotik dengan mengukur persentase keberhasilan integrasi perangkat. Dari total 30 (tiga puluh) perangkat yang diuji, hanya 23 (dua puluh tiga) perangkat yang berhasil terhubung, menghasilkan persentase keberhasilan sebesar 77% (tujuh puluh tujuh persen). Hasil ini menunjukkan bahwa meskipun jaringan dapat mengakomodasi sebagian besar perangkat, terdapat keterbatasan yang signifikan dalam infrastruktur yang ada. Penelitian ini mengindikasikan adanya keterbatasan dalam infrastruktur jaringan yang digunakan, yang tidak sepenuhnya mampu mendukung jumlah perangkat yang lebih besar. Beberapa faktor penyebab rendahnya persentase keberhasilan tersebut antara lain keterbatasan kapasitas jaringan, konfigurasi perangkat keras yang tidak optimal, pengaturan perangkat lunak yang kurang tepat, serta faktor eksternal yang dapat mempengaruhi performa jaringan.

REFERENCES

[1] Agustina. (2022). Universitas Pasundan. Diambil kembali dari repo unpas : http://repository.unpas.ac.id/56050/6/9.%20BAB%20III.pdf
[2] Busyairi Ahmad, M. S. (Jan-Jun 2020). Penerapan StudiI Lapangan Dalam Meningkatkan Kemampuan Analisis Masalah (Studi Kasus Pada Mahasiswa Sosiologi IISIP YAPIS BIAK). Jurnal Nalar Pendidikan , 65.
[3] Cahya Kamila Wilujeng, A. V. (Juni 2024). Implementasi Firewall Filteer Rules Sebagai Filtering Pada Jaringan Komputer Menggunakan Microtik Conten JATI (Jurnal Mahasiswa Teknik Informatika), 2680 - 2684.
[4] Cahyono, A. D. (Desember 2020). Studi Kepustakaan Mengenai Kualitas Pelayanan Terhadap Kepuasan Pasien Rawat Jalan Di Rumah Sakit. Jurnal Ilmiah Pamenang - JIP, Vol. 2 No. 2, 1-6.
[5] Habibi, A. (2020 , Juli 28). Jenis-jenis Jaringan Komputer Berdasarkan Fungsi Dan Skala. Diambil kembali dari Wordpress.com: https://aldihabibi15.wordpress.com.
[6] Jakaria, D. A. (2020). Implementasi Firewall dan Web Filtering Pada Mikrotik Routeros Untuk Mendukung Internet Sehat dan Aman (INSAN). JURNAL , 1.
[7] M.Parenreng, J. (2022). Pengantar Jaringan Komunikasi Nirkabel. Banyumas, Jawa Tengah : CV. ZT CORPORA.
[8] N.Nadila. (2023). Repostory STEI . Diambil kembali dari Repostory STEI: http://repository.stei.ac.id/10803/4/BAB%203.pdf
[9] Nurul Hayati, M. (Mei 2020). Buku Ajar : SISTEM KEAMANAN . Tanjung Pinang : Universitar Maritim Raja Ali Haji .
[10] Putra, F. P. (2023). Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking. JURNAL POLEKTRO, 1.
[11] Ridatu Ocanitra, M. R. (2019). Implementasi Sistem. Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen, 1.
[12] Sabara, M. A. (2020). Konfigurasi Manajemen Bandwith Menggunakan Router Mikrotik RB2011UiAS-RM Untuk Mengontrol Penggunaan Internet Di PT REKAN USAHA MIKRO ANDA TEGAL. Jurnal POLEKTRO: Jurnal Power Elektronik, Vol.9, No.2 : 44.
[13] Suprapto, S. (2018). Analisis Dan Implementasi Keamanan Jaringan Menggunakan Mikrotik Firewall. Universitas Putra Batam , 7-10.
[14] Susanto, R. (2020). Rancang Bangun Jaringan Vlan dengan Menggunakan Simulasi Cisco Packet Tracer . InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan , Vol.4 : 346.
[15] Usman, N. (2020). Konteks Implementasi Berbasis Kurikulum. Jakarta : Grasindo