JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 12 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v12i3.4716

PENGEMBANGAN MANAJEMEN KEAMANAN JARINGAN NIRKABEL (WIFI) MENGGUNAKAN ROUTERBOARD MIKROTIK DAN FIREWALL PADA SMK KRISTEN PALOPO

Eben[1], Mukramin[2],Hisma Abduh[3]

[1,2]Teknik Informatika/Universitas Andi Djemma; Jl. Tandipau, Kota Palopo;

Received: 1 Juli 2024
Accepted: 31 Juli 2024
Published: 7 Agustus 2024

Keywords:
Jaringan Nirkabel (wifi), Routerboard Mikrotik, Firewall, SMK Kristen Palopo.

Corespondent Email:
eben22715@gmail.com

Abstrak. Penggunaan jaringan nirkabel (WiFi) semakin meluas, termasuk di lingkungan pendidikan seperti SMK Kristen Palopo. Namun, meningkatnya keterhubungan juga meningkatkan risiko keamanan informasi. Skripsi ini bertujuan untuk mengembangkan manajemen keamanan jaringan nirkabel di SMK Kristen Palopo menggunakan Routerboard Mikrotik dan firewall. Pendekatan pengembangan sistem melibatkan analisis kebutuhan keamanan, desain sistem, implementasi, dan evaluasi. Fokus penelitian adalah mengidentifikasi kerentanan keamanan dalam infrastruktur jaringan WiFi sekolah dan merancang solusi yang efektif dengan memanfaatkan perangkat Routerboard Mikrotik dan konfigurasi firewall yang disesuaikan. Hasil penelitian menunjukkan peningkatan signifikan dalam keamanan jaringan nirkabel, dengan mengurangi risiko serangan dan meningkatkan perlindungan terhadap data sensitif. Penelitian ini diharapkan dapat memberikan panduan praktis bagi SMK Kristen Palopo dalam meningkatkan keamanan jaringan nirkabel mereka dan juga dapat diterapkan pada institusi pendidikan lainnya.

Abstract. *The use of wireless networks (WiFi) is increasingly widespread, including in educational environments such as the Palopo Christian Vocational School. However, increasing interconnectedness also increases information security risks. This thesis aims to develop wireless network security management at Palopo Christian Vocational School using a Mikrotik Routerboard and firewall. The system development approach involves security requirements analysis, system design, implementation, and evaluation. The focus of the research is to identify security vulnerabilities in the school WiFi network infrastructure and design an effective solution by utilizing Mikrotik Routerboard devices and customized firewall configurations. The research results show significant improvements in wireless network security, by reducing the risk of attacks and increasing protection of sensitive data. It is hoped that this research can provide practical guidance for Palopo Christian Vocational Schools in improving the security of their wireless networks and can also be applied to other educational institutions.*

1. PENDAHULUAN

Perkembangan Perkembangan teknologi informasi, terutama internet, berdampak signifikan pada interaksi antara perusahaan dan karyawan melalui jaringan komputer. Namun, risiko muncul ketika informasi penting dapat diakses oleh pihak yang tidak berwenang. Ada dua jenis media transmisi dalam jaringan komputer: kabel dan nirkabel[1].

Teknologi jaringan komputer berkembang sangat cepat, meningkatkan kebutuhan akan berbagai jenis informasi. Internet, sebagai sumber informasi utama, memungkinkan aktivitas seperti browsing, chatting, dan

blogging semakin umum di kalangan pengguna di seluruh dunia.

Teknologi nirkabel, yang menggunakan frekuensi radio untuk mentransfer data, berkembang pesat. Banyak penyedia layanan seperti ISP, warnet, dan institusi pendidikan telah mengadopsi teknologi wifi. Namun, sedikit yang memperhatikan keamanan jaringan nirkabel, membuatnya rentan terhadap serangan hacker.

SMK Kristen Palopo, di Kota Palopo, Sulawesi Selatan, menggunakan jaringan internet nirkabel yang masih menggunakan pengaturan standar (default). Jaringan ini digunakan untuk akses internet, data online, dan kebutuhan pendidikan lainnya. Kekhawatiran muncul karena pengaturan standar rentan terhadap serangan. Sistem keamanan yang digunakan adalah WPA-PSK, dengan satu password dan username untuk 25 pengguna. Hal ini menyebabkan jaringan mudah diretas dan mengalami overload, mengakibatkan penggunaan bandwidth yang berlebihan dan kecepatan menurun.

Kekurangan karyawan IT memaksa sekolah memanggil teknisi eksternal dengan biaya besar untuk konfigurasi jaringan. Untuk mengatasi masalah ini, diperlukan sistem keamanan berbasis mikrotik dan firewall. Sistem ini akan mengontrol dan memantau lalu lintas data, melindungi jaringan dari serangan, dan mengurangi risiko kebocoran password serta overload jaringan.

Penulis memutuskan melakukan penelitian dengan judul "Pengembangan Manajemen Keamanan Jaringan Nirkabel (Wifi) Menggunakan Routerboard Mikrotik dan Firewall pada SMK Kristen Palopo," dengan harapan meningkatkan keamanan jaringan komputer di sekolah tersebut.

2. TINJAUAN PUSTAKA

2.1. Konsep Keamanan Jaringan

Keamanan jaringan adalah konsep yang bertujuan untuk mencegah akses oleh pengguna yang tidak sah ke dalam sistem jaringan komputer. [2].

Komputer berharga bagi kita karena memudahkan berbagai tugas seperti mengirim email, menelusuri web, dan menulis makalah, yang akan sulit dilakukan tanpa komputer. Kita juga mengandalkan integritasnya untuk memastikan dokumen dan foto tetap sama seperti saat disimpan atau diterima[3].

Dari pendapat di atas dapat disimpulkan bahwa keamanan jaringan sangat penting untuk mencegah akses tidak sah dan melindungi sistem komputer dari serangan.

2.2. Jaringan Komputer

Jaringan komputer merupakan hubungan koneksi antara dua atau lebih sistem komputer yang saling bertukar data melalui media komunikasi[4].

Jaringan komputer adalah sebuah sistem yang terdiri dari beberapa komputer dan perangkat jaringan lainnya yang bekerja sama untuk mencapai tujuan yang sama[5].

Dapat disimpulkan bahwa dengan berkembangnya teknologi komputer dan komunikasi, penggunaan model komputer tunggal dalam organisasi telah digantikan oleh jaringan komputer.

2.3. Klasifikasi Jaringan

Jaringan dapat diklasifikasikan berdasarkan jarak dan cakupannya menjadi beberapa jenis, yaitu Local Area Network (LAN) yang mencakup area kecil seperti kantor atau sekolah, Metropolitan Area Network (MAN) yang mencakup area lebih besar seperti kota, Wide Area Network (WAN) yang mencakup area sangat luas seperti negara atau benua, internet yang merupakan jaringan global mencakup berbagai jenis jaringan, dan jaringan nirkabel (Wireless) yang menggunakan teknologi nirkabel untuk mentransfer data tanpa kabel fisik[6].

2.4. Topologi Jaringan

Topologi jaringan didefinisikan sebagai hubungan fisik antara setiap anggota jaringan komputer, termasuk koneksi (links), node, dan lainnya. Setiap node, yang bisa berupa modem, hub, bridge, atau komputer, umumnya terhubung dengan satu atau lebih node lainnya melalui koneksi. Pemetaan hubungan antara setiap node dalam jaringan komputer ini membentuk sebuah topologi jaringan[7].

2.5. Wireles

Wi-Fi adalah teknologi populer yang memanfaatkan peralatan elektronik untuk bertukar data secara nirkabel melalui jaringan komputer, termasuk akses internet berkecepatan tinggi, menggunakan gelombang radio. Menurut definisi dari Wi-Fi Alliance, Wi-Fi adalah "produk jaringan lokal nirkabel (WLAN) apapun yang didasarkan pada standar

Institute of Electrical and Electronics Engineers (IEEE) 802.11". Karena sebagian besar WLAN saat ini mengikuti standar tersebut, istilah "Wi-Fi" telah menjadi sinonim umum untuk teknologi jaringan nirkabel[8].

2.6. Router

Router adalah perangkat yang berfungsi untuk mengirimkan paket data IP dari satu jaringan ke jaringan lainnya menggunakan metode addressing dan protokol tertentu. Dalam sebuah jaringan, router-router yang saling terhubung membentuk algoritma routing yang menentukan jalur terbaik yang harus dilalui oleh paket data IP untuk mencapai tujuannya[9].

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

Transmission Control Protocol/Internet Protocol (TCP/IP) adalah standar komunikasi data yang fundamental digunakan oleh komunitas internet untuk pertukaran data antara komputer dalam sebuah jaringan. TCP/IP mendefinisikan bagaimana data dikemas, diarahkan, dan dikirim melalui jaringan, memungkinkan komunikasi yang efisien dan andal antara perangkat-perangkat yang terhubung ke internet[10].

2.8. Firewall

Firewall adalah solusi perlindungan penting dalam jaringan komputer yang berfungsi untuk mencegah serangan dan penyusupan yang dapat membahayakan kerahasiaan data serta merusak infrastruktur jaringan. Metode-metode umum dalam firewall meliputi circuit level gateway, application level gateway, dan packet filtering firewall. Circuit level gateway bekerja pada lapisan sesi OSI untuk mengontrol koneksi antara dua jaringan, sementara application level gateway memonitor dan mengontrol aplikasi tertentu yang melewati firewall[11].

2.9. MikroTik

MikroTik adalah sistem operasi mandiri berbasis Linux yang khusus dirancang untuk komputer yang berfungsi sebagai router. Dirancang dengan fokus pada kemudahan penggunaan, MikroTik sangat cocok untuk keperluan administrasi jaringan komputer, baik untuk sistem jaringan skala kecil maupun kompleks[12].

2.10. Winbox

Winbox adalah sebuah utilitas yang digunakan untuk konektivitas dan konfigurasi perangkat MikroTik menggunakan Media Access Control Address (MAC) atau protokol IP. Ini menyediakan antarmuka grafis (GUI) yang memungkinkan pengguna untuk dengan cepat dan mudah mengatur MikroTik RouterOS. [13].

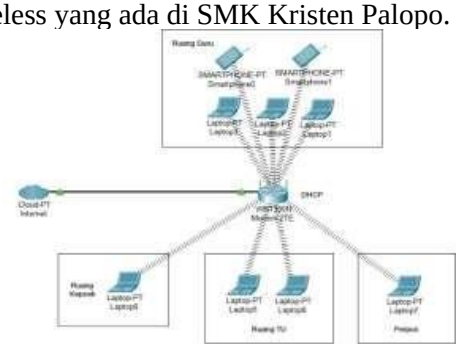
3. METODE PENELITIAN

3.1. Tahapan Penelitian

Model yang digunakan dalam penelitian pengembangan ini adalah model procedural, yang mengikuti serangkaian langkah-langkah untuk menghasilkan produk yang diinginkan. Langkah-langkah tersebut meliputi pengumpulan data melalui observasi, studi literatur, wawancara, dan kuisioner untuk memperoleh informasi yang diperlukan. Selanjutnya, dilakukan analisis kebutuhan untuk merancang sistem teknologi Augmented Reality sesuai dengan kebutuhan yang telah diidentifikasi. Tahap berikutnya adalah perancangan desain alat berdasarkan analisis yang telah dilakukan. Setelah desain selesai, dilakukan pengujian sistem untuk memastikan bahwa sistem memenuhi kebutuhan pengguna dan untuk mendeteksi gangguan atau kesalahan fungsi.

3.2. Analisis Sistem Yang Berjalan

Dari Selanjutnya adalah analisis sistem, pada tahap ini proses yang dilakukan yaitu melakukan analisis terhadap kemanan jaringan wireless yang ada di SMK Kristen Palopo.



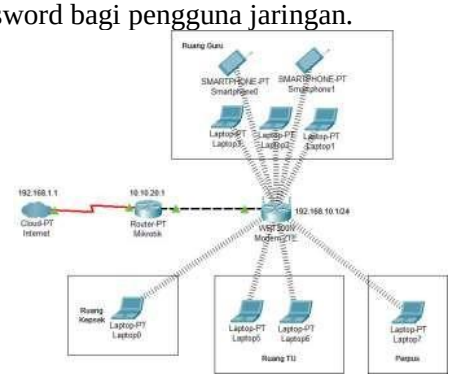
Gambar 1 sistem yang berjalan

Penggunaan jaringan di Sekolah Menengah Kejuruan (SMK) Kristen Palopo bersumber dari layanan IndiHome yang disediakan oleh PT. Telkom Palopo, berdasarkan hasil observasi yang dilakukan oleh penulis. Dalam lingkungan sekolah tersebut, topologi jaringan yang digunakan adalah topologi bintang (star), dan terdapat juga jaringan nirkabel atau wireless. Saat ini, penggunaan jaringan mengandalkan modem ZTE F-609. Modem tersebut bertugas mengirimkan data atau paket

ke access point untuk disebarkan ke seluruh jaringan. Jaringan yang dipancarkan melalui modem atau access point dilindungi dengan satu password, kemudian diterima oleh pengguna seperti kepala sekolah, staf administrasi, dan perpustakaan.

3.3. Analisis Sistem Yang Berjalan

Jaringan yang diterapkan di Sekolah Menengah Kejuruan (SMK) Kristen Palopo menggunakan topologi bintang. Penelitian ini bertujuan untuk melakukan analisis terhadap keamanan jaringan, serta merancang solusi keamanan jaringan dengan memanfaatkan perangkat MikroTik RB931-2nd-Hap Mini. Penggunaan perangkat MikroTik RB931-2nd-Hap Mini direncanakan untuk memberikan konfigurasi tambahan pada infrastruktur jaringan, seperti menyediakan hotspot dengan sistem login menggunakan username dan password bagi pengguna jaringan.



Gambar 2 Sistem yang Diusulkan

3.4. Tahapan NDLC

Penelitian ini mengawali dengan tahap analisis yang meliputi pengumpulan data melalui observasi, wawancara dengan pihak terkait seperti kepala sekolah SMK Kristen Palopo, studi kepustakaan, dan penggunaan kuesioner untuk mengumpulkan data dari responden. Setelah itu, data dianalisis untuk memahami kebutuhan dan masalah yang ada serta merancang desain topologi jaringan yang sesuai. Tahap selanjutnya adalah simulasi prototipe menggunakan VirtualBox untuk mengevaluasi kinerja jaringan sebelum implementasi. Implementasi dilakukan berdasarkan rencana yang telah disusun dengan teliti, diikuti dengan monitoring untuk memastikan jaringan berjalan sesuai tujuan.

3.5. Analisis Kebutuhan Sistem

Dalam pengembangan keamanan jaringan nirkabel di SMK Kristen Palopo, terdapat beberapa kebutuhan fungsional yang harus dipenuhi. Ini meliputi kemampuan jaringan nirkabel untuk memblokir beberapa port yang ada, mengontrol jaringan secara efektif, dan menyediakan langkah-langkah keamanan yang kuat. Selain itu, firewall harus dapat mengatur akses ke situs web, mengamankan port yang terbuka, serta memblokir akses ke game online. Dengan memenuhi kebutuhan ini, diharapkan sistem keamanan jaringan dapat diterapkan dengan efektif dan mengoptimalkan penggunaan infrastruktur jaringan di sekolah.

Kebutuhan non fungsional untuk pengembangan keamanan jaringan wireless di SMK Kristen Palopo melibatkan perangkat keras dan lunak yang spesifik. Perangkat keras yang diperlukan mencakup prosesor AMD Ryzen 3 dengan kecepatan 3,8 GHz, RAM 12 GB, SSD NVMe berkapasitas 1 TB, kartu grafis Radeon, modem ZTE F609, perangkat input dan output, kabel UTP, konektor RJ-45, tang crimping, MikroTik RB-931-2nd-hap-mini, dan LAN Tester. Sementara itu, untuk perangkat lunak, sistem operasi Windows 11 64-bit, aplikasi Speedtest, dan tools Nmap menjadi bagian integral dari infrastruktur keamanan yang diimplementasikan.

4. HASIL DAN PEMBAHASAN

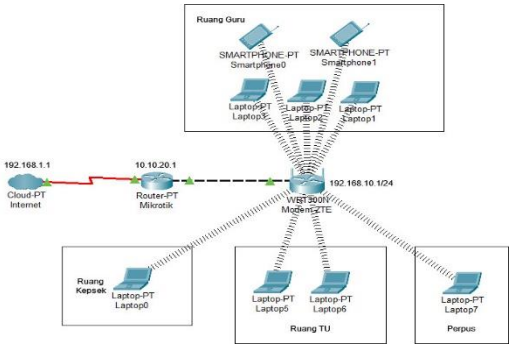
4.1. Hasil Penelitian

Hasil penelitian merupakan tahap di mana sistem keamanan jaringan yang telah dikembangkan oleh penulis dapat dijelaskan secara rinci. Dalam tahap ini, efektivitas jaringan yang dirancang dapat dievaluasi untuk menentukan apakah itu berhasil meningkatkan keamanan jaringan dan memperbaiki stabilitas koneksi internet di jaringan nirkabel SMK Kristen Palopo. Penelitian ini menerapkan metode NDLC (Network Design Life Cycle) mulai dari tahap Perencanaan dan Persiapan hingga tahap Pelaporan. Hasil penelitian ini mencakup pembahasan tentang pengumpulan data, desain jaringan, serta tahap pemantauan jaringan, dan memberikan langkah-langkah serta solusi untuk mengurangi kerentanan yang ditemukan dalam jaringan nirkabel SMK Kristen Palopo.

4.3. Design

Pada tahap desain ini, akan dibuat gambaran desain topologi jaringan interkoneksi yang akan dibangun. Desain ini mencakup struktur topologi, akses data, tata letak perkabelan, dan aspek lainnya yang memberikan gambaran

detail tentang jaringan yang akan dibangun. Selain itu, tahap ini juga akan mencakup analisis kebutuhan perangkat, kebutuhan pengguna, dan kebutuhan layanan yang diperlukan untuk memastikan bahwa desain jaringan memenuhi semua kebutuhan tersebut secara efisien.

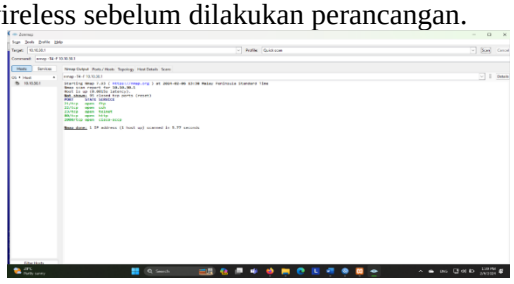


Gambar 3 Topologi Jaringan Yang Dirancang

Untuk memenuhi kebutuhan sistem keamanan jaringan di SMK Kristen Palopo, diperlukan sejumlah perangkat keras dan lunak. Secara spesifik, perangkat keras yang direkomendasikan mencakup laptop Acer Aspire dengan prosesor Intel 3,8 GHz, RAM 2 GB, dan HDD 500GB, serta perangkat jaringan seperti Modem ZTE F609, Mikrotik RB-931-2nd-hap-mini, dan perlengkapan tambahan seperti kabel UTP, tang crimping, LAN tester, dan konektor RJ-45. Sementara itu, perangkat lunak yang dianjurkan termasuk Winbox untuk konfigurasi Mikrotik, Speed Test CBN untuk menguji kecepatan internet, sistem operasi Windows 11 64 bit untuk kompatibilitas aplikasi, dan Tools Nmap untuk pemindaian jaringan. Kombinasi ini diharapkan dapat mendukung implementasi keamanan jaringan yang efektif dan optimal di lingkungan sekolah.

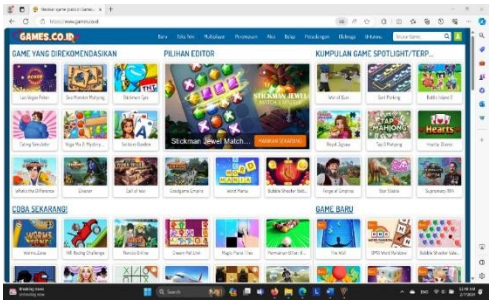
4.4. Simulation Prototype

Dari arsitektur dan topologi yang sudah penulis peroleh, pada tahap ini penulis akan melakukan simulasi penyerangan jaringan wireless menggunakan aplikasi Nmap untuk mengetahui port yang terbuka pada jaringan wireless sebelum dilakukan perancangan.



Gambar 4 Hasil Simulasi Scanning Prot Nmap

Berdasarkan gambar di atas hasil scanning port menggunakan aplikasi Nmap mendapatkan hasil 4 port yang terbuka antara lain, port 21 (FTP), 22 (SSH), 23 (TELNET), dan port 80 (HTTP). Port yang terbuka tersebut sangat rentan untuk diretas oleh hacker dikarenak port tersebut merupakan port service dari ISP. Selanjut untuk simulasi berikutnya adalah membuka game online pada jaringan wireless untuk mengetahui apakah website tersebut telah di blokir atau tidak oleh ISP.

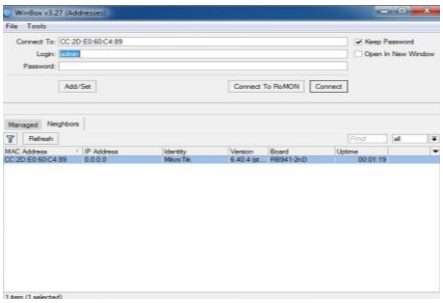


Gambar 5 Hasil Simulasi Game Online

Berdasarkan gambar di atas hasil simulasi game online dengan cara mengakses www.games.online.com, website tersebut dapat terbuka yang menendakan tidak adanya sistem keamanan jaringan yang memblokir website tersebut.

4.5. Implementation

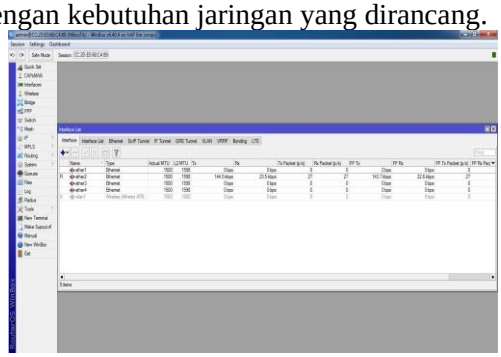
Langkah awal dalam proses penelitian ini adalah melakukan konfigurasi pada perangkat MikroTik.



Gambar 6 Tampilan Awal Winbox

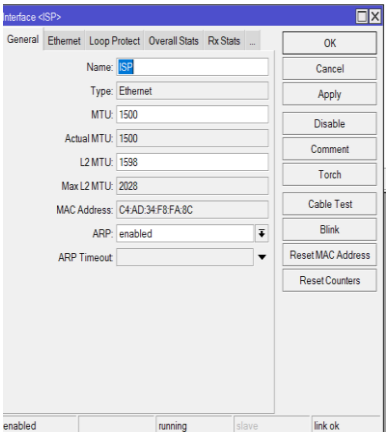
Langkah berikutnya adalah melakukan konfigurasi pada interface yang akan digunakan dalam penelitian ini. Terdapat tiga interface yang akan kami manfaatkan, yaitu ether1, ether2, dan wlan. Setiap interface memiliki fungsi yang berbeda. Ether1 berperan sebagai penghubung antara perangkat MikroTik dengan ISP (Internet Service Provider), sementara ether2 akan digunakan untuk konfigurasi jaringan LAN. Interface wlan akan dialokasikan untuk akses jaringan hotspot. Dengan demikian, pengaturan yang tepat pada setiap interface ini

akan memastikan fungsi yang optimal sesuai dengan kebutuhan jaringan yang dirancang.



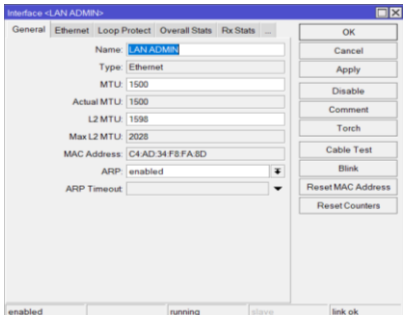
Gambar 7 Tampilan Menu Interface

Menu "Interface" adalah tampilan awal yang memungkinkan konfigurasi pada berbagai port dan wireless yang ada pada perangkat MikroTik yang digunakan. Pada tab ini, akan ditampilkan semua bagian dari port yang dimiliki oleh MikroTik, seperti ethernet (misalnya ether1, ether2, dll.), serta informasi tentang jaringan nirkabel (wireless) yang ada di perangkat MikroTik. Dari menu ini, pengguna dapat mengakses dan mengatur konfigurasi untuk setiap interface yang terhubung ke perangkat, baik itu untuk port kabel atau jaringan nirkabel, sesuai dengan kebutuhan jaringan yang sedang dikonfigurasi.



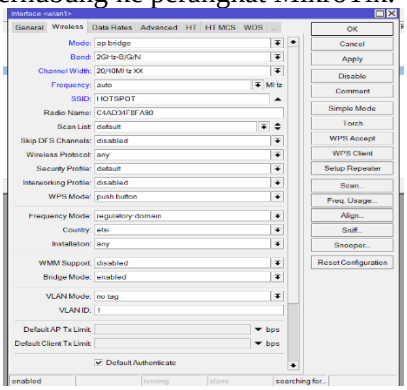
Gambar 8 Menu Interface ISP

Langkah ini merupakan langkah untuk nama atau pengenal kepada interface ethernet yang akan digunakan. Interface yang pertama, akan diberi nama "ISP". Interface ini bertugas untuk menerima kabel dari modem dan menjadi pintu masuk utama ke jaringan MikroTik. Dengan memberikan nama yang sesuai, memudahkan pengguna atau administrator jaringan dalam mengidentifikasi fungsi dan tujuan dari setiap interface yang terhubung ke perangkat MikroTik.



Gambar 9 Menu Interface LAN Admin

Langkah berikutnya adalah memberikan nama pada interface ether2 pada perangkat MikroTik. Interface ether2 akan diidentifikasi sebagai media kabel yang digunakan untuk koneksi administratif. Port ini akan digunakan oleh administrator untuk terkoneksi langsung dengan perangkat MikroTik. Dengan memberikan nama yang jelas pada interface ether2, administrator akan dapat dengan mudah mengenali dan mengelola koneksi administratif yang terhubung ke perangkat MikroTik.



Gambar 10 Menu Interface WLAN

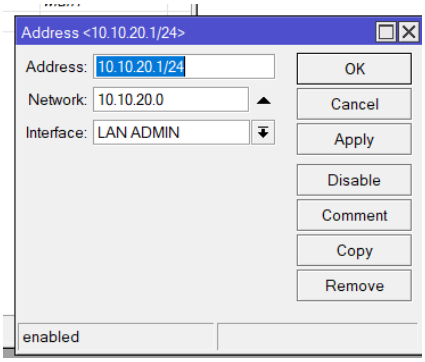
Setelah melakukan konfigurasi pada interface, langkah selanjutnya adalah mengatur konfigurasi alamat IP pada masing-masing ethernet. Untuk melakukan konfigurasi ini, Anda dapat menuju menu "IP" dan kemudian pilih submenu "Addresses".

Gambar 11 Konfigurasi IP Address

Pada tahap ini, Anda akan melakukan konfigurasi alamat IP untuk setiap ethernet yang sebelumnya telah diberi nama atau identitas. Tujuannya adalah untuk memberikan klasifikasi kelas alamat IP yang akan digunakan untuk masing-masing Ethernet.

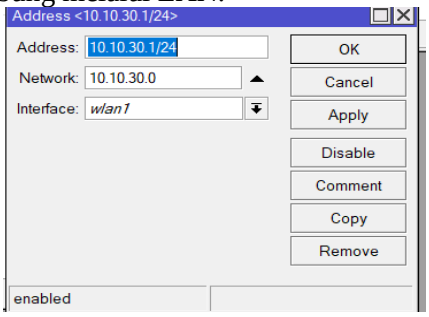
Gambar 12 IP Address ISP

Konfigurasi awal melibatkan pengaturan pada ether1-modem, di mana alamat IP yang diberikan berada dalam satu rentang dengan IP dari modem.



Gambar 13 IP Address LAN

Setelah itu, konfigurasi IP address pada LAN dilakukan untuk memberikan alamat IP yang akan digunakan oleh pengguna yang terhubung melalui LAN.

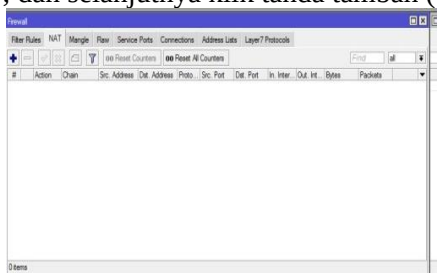


Gambar 14 IP Address WLAN

Setelah mengatur IP Address, langkah konfigurasi berikutnya adalah konfigurasi pada DNS Server. Untuk melakukannya, masuklah ke menu IP pada Winbox, lalu pilih opsi DNS. Masukkan DNS server sebagai 8.8.8.8 dan 8.8.0.0, kemudian centang opsi "allow remote request".

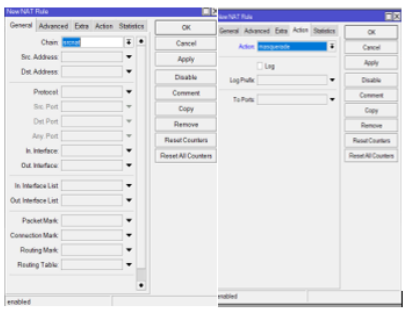
Gambar 15 konfigurasi DNS Server

Setelah melakukan konfigurasi pada DNS Server, langkah selanjutnya adalah konfigurasi firewall. Konfigurasi ini mencakup izin akses jaringan dari modem ke pengguna yang terhubung ke MikroTik, serta menu untuk pemblokiran akses ke situs-situs tertentu. Untuk melakukan konfigurasi firewall, langkah awal yang dilakukan adalah masuk ke menu IP, kemudian pilih firewall, lalu masuk ke menu NAT, dan selanjutnya klik tanda tambah (+).



Gambar 16 Konfigurasi firewall NAT

Setelah itu, pada menu general, pada opsi "out interface", pilih "ether-1" sebagai modem yang telah dikonfigurasi sebelumnya. Kemudian, pada tab "action", pilih opsi "masquerade".



Gambar 17 Konfigurasi NAT

Konfigurasi "out interface" digunakan untuk memberikan akses melalui firewall kepada modem yang menyediakan jaringan. Dengan

konfigurasi ini, MikroTik akan membaca akses dari modem dan memberikan izin akses sesuai dengan aturan yang ditetapkan dalam firewall.

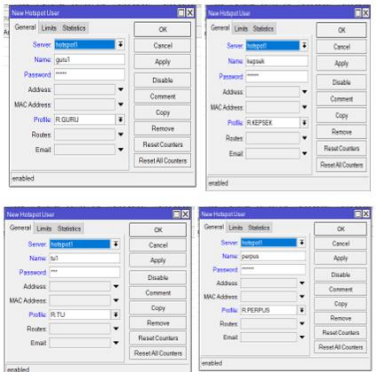
Setelah melakukan konfigurasi firewall, langkah selanjutnya adalah konfigurasi pada sistem hotspot. Konfigurasi ini bertujuan untuk membuat jaringan yang dapat diakses tanpa kabel, serta mengatur pengguna pada setiap media jaringan.

Gambar 18 Konfigurasi Hospot

Pemilihan interface dilakukan untuk menentukan ether yang akan digunakan sebagai akses jaringan hotspot, di mana ether yang dipilih biasanya adalah ether nirkabel (wireless). Selanjutnya, konfigurasi dilakukan pada DNS Name, yang bertujuan untuk memberikan alamat kepada pengguna saat mereka mengakses jaringan untuk memasukkan username dan password.

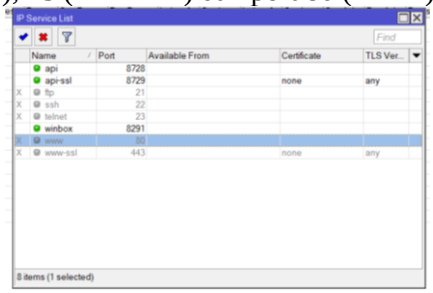
Gambar 19 Membuat Hospot User

Setelah konfigurasi hotspot profile selesai, tahapa berikutnya penulis membuat hotspot user Dimana fungsi dari konfigurasi ini adalah untuk membebagi user berdasarkan username dan password masing-masing.



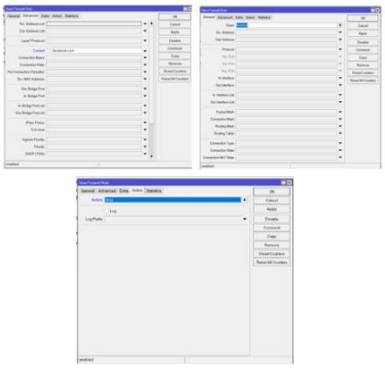
Gambar 20 Konfigurasi Hospot User

Setelah selesai mengkonfigurasi hotspot selesai kemudian penulis melakukan konfigurasi Blokir Port Service untuk memblokir port yang terbuka sebelumnya dengan aplikasi Nmap pada tahap simulasi. Port yang ditutup antara lain port 21 (FTP), 22 (SSH), 23 (TELNET) dan port 80 (HTTP).



Gambar 21 Konfigurasi Blokir Port Service

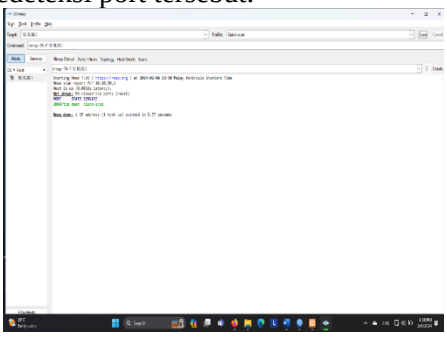
Pada konfigurasi ini penulis memblokir beberapa website yang sering digunakan pada saat jam kerja antara lain facebook.com, Instagram.com, tiktok.com dan game online. Untuk pemblokiran website dengan ekripsi https penulis menggunakan fiter rule pada firewall, dengan cara melakukan drop pada koneksi website agar tidak dapat di akses oleh user.



Gambar 22 Konfigurasi Blokir Website

Hasil Monitoring Port Menggunakan NMAP Berdasarkan gambar di bawah port yang

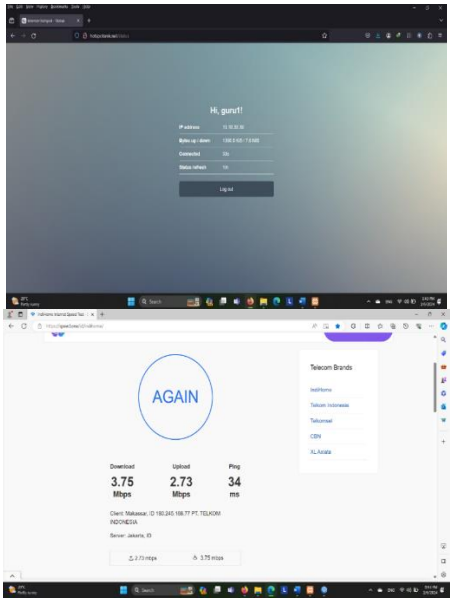
sebelumnya terbuka pada saat penulis melakukan simulasi dapat tertutup dengan sempurna sehingga aplikasi Nmap tidak dapat menedeteksi port tersebut.



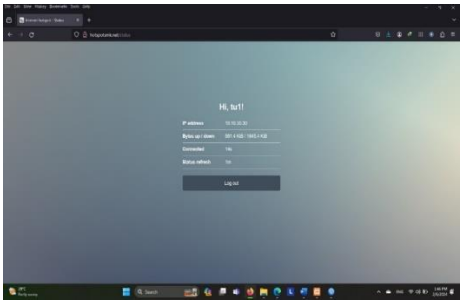
Gambar 23Scanning Port Nmap

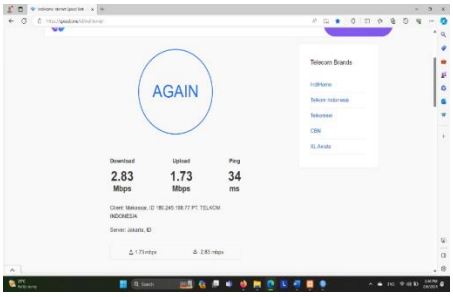
Hasil Monitoring Speed Test

Pada tahap ini, peneliti menguji kecepatan internet setelah menyelesaikan konfigurasi mikrotik dengan menggunakan speedtest CBN. Hasil pengujian tersebut dapat dilihat pada gambar di bawah ini.

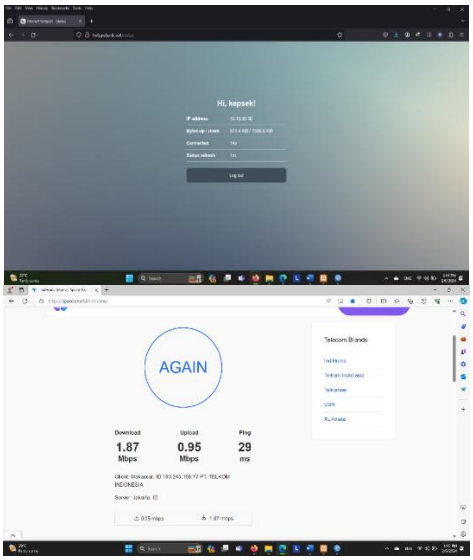


Gambar 24 Penguji Kecepatan Jaringan Internet Guru





Gambar 25 Penguji Kecepatan Jaringan Internet TU



Gambar 26 Penguji Kecepatan Jaringan Internet Kepala Sekola0068

5. KESIMPULAN

Penelitian tentang Pengembangan Manajemen Keamanan Jaringan Nirkabel (WiFi) menggunakan Routerboard MikroTik dan Firewall pada SMK Kristen Palopo menyimpulkan bahwa MikroTik efektif dalam mengatur dan mengamankan jaringan. MikroTik memungkinkan pembagian bandwidth teratur untuk setiap klien, penutupan port yang terbuka, pemblokiran akses ke situs web tertentu, dan kontrol jaringan melalui aplikasi WinBox. Dengan demikian, MikroTik memberikan solusi yang efisien dan aman untuk pengelolaan jaringan nirkabel, memastikan gangguan pada satu klien tidak mempengaruhi yang lain dan memberikan kontrol penuh kepada administrator.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak terkait yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] C. S. Saputri *et al.*, "Dampak Teknologi Informasi Mengenai Proses Audit : Teknologi Informasi Carina Serly Saputri Zulkarnain Zulkarnain Universitas Internasional Batam Korespondensi Penulis : 2242006.carina@uib.edu memperkuat sistem pengendalian internal . Melalui integrasi te," *J. Tek. Mesin, Ind. Elektro Dan Inform.*, vol. 3, no. 1, 2024.

[2] W. W. Purba and R. Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT," *Aiti*, vol. 17, no. 2, pp. 143–158, 2021, doi: 10.24246/aiti.v17i2.143-158.

[3] Maulana, *Keamanan Komputer*, vol. 5, no. 1. 2022.

[4] N. I. Febriyanto and I. A. Sobari, "Perancangan Jaringan Vpn Menggunakan Protokol L2Tp+Ipsec Sebagai Media Transmisi Data Pada Yayasan Sirajul Falah Indonesia," *J. Inform. dan Tek. Elektro Terap.*, vol. 12, no. 1, pp. 275–281, 2024, doi: 10.23960/jitet.v12i1.3703.

[5] A. V. Mananggel, A. Mewengkang, and A. C. Djamen, "Perancangan Jaringan Komputer Di Smk Menggunakan Cisco Packet Tracer," *Edutik J. Pendidik. Teknol. Inf. dan Komun.*, vol. 1, no. 2, pp. 119–131, 2021, doi: 10.53682/edutik.v1i2.1124.

[6] A. A. Muharram, "Analisis Quality Of Service Jaringan Wireless Virtual Local Area Network Pada UIN Syarif Hidayatullah Jakarta," 2021, [Online]. Available: https://repository.uinjkt.ac.id/dspace/handle/123456789/56366%0Ahttps://repository.uinjkt.ac.id/dspace/bitstream/123456789/56366/1/ABDUL AZIZ MUHARRAM-FST.pdf

[7] M. Ardhiansyah, S. Noris, and R. Andrianto, *Modul Jaringan Komputer Universitas Pamulang*, no. 1. 2020. [Online]. Available: http://dhoto.lecturer.pens.ac.id/publications/book/2008/Dhoto-JaringanKomputer2.pdf

[8] T. Destianti and U. M. Buana, "Implementasi Telekomunikasi, Internet, Dan Teknologi Nirkabel Pada Pt. Berito Pangan Makmur," no. April, 2021.

[9] A. S. Rifandi, *Pengukuran Kinerja Fhrp Menggunakan Etherchannel Dan Routing Protocol Ospfv2 , Eigrp Dan Bgpv4 Dengan Topologi Three-Tier Pengukuran Kinerja Fhrp Menggunakan Etherchannel Dan Routing Protocol Ospfv2 ,*. 2023.

[10] I. K. Anak Agung Ngurah Putra Gunawan., I. W. Supardi., Ilham., and M. S. Made Satriya Wibawa, *Dasar Ilmu Komputer dan Jaringan*, no. February. 2024. [Online]. Available: https://mii-press.com/2024/02/12/dasar-ilmu-komputer-dan-jaringan/

[11] M. R. Dwi Setiawan, Ridwansyah, "Perancangan Keamanan Jaringan Next-Generation Firewall Menggunakan Router Fortinet Pada Pt. Alodokter Teknologi Solusi," *J. Inform. Terpadu*, vol. 9, no. 1, pp. 34–39, 2023, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[12] Ahmad Iwan Fadli, "Analisis, Perancangan dan Implementasi Wireless HotspotManajemen Sistem Menggunakan Router Mikrotik Pada SMA Negeri 1 Prambanan Naskah Publikasi," 2020.

[13] Fadlan Abdillah Hasibuan and Subhiyanto, "Jaringan Komputer Berbasis Radius Server untuk Meningkatkan Pemanfaatan Internet di Madrasah Aliyah Al-Azhaar Ummu Suwanah," *J. Tek. Inform.*, vol. 7, no. 1, pp. 30–39, 2021, doi: 10.51998/jti.v7i1.349.