Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.2 (May 2026)

PERANCANGAN SISTEM KEAMANAN JARINGAN WIRELESS MENGGUNAKAN FITUR RULES DAN ACCESS LIST PADA BIZNET BRANCH KEBON SIRIH

Rizky Ibnu Hartadi[1], Fitri Latifah[2*]

Program Studi Informatika[1], Program Studi Informatika[2]
Fakultas Teknologi Informasi[1], Fakultas Teknologi Informasi[2]
Universitas Nusa Mandiri[1], Universitas Nusa Mandiri[2]

*Correspondent Author: fitri.flr@nusamandiri.ac.id

Author Email: rizkiibnuhartadi@gmail.com[1],

Received: February 28, 2026**. Revised:** April 18, 2026**. Accepted:** April 26,2026**. Issue Period:** Vol.10 No.2 (2026), Pp. 522-531

Perkembangan teknologi jaringan wireless memberikan kemudahan dalam komunikasi dan pertukaran data di lingkungan organisasi. Namun, penggunaan jaringan wireless juga menimbulkan berbagai risiko keamanan seperti akses tidak sah yang berpotensi terjadinya kebocoran data. Penelitian ini bertujuan untuk merancang sistem keamanan jaringan wireless pada Biznet Branch Kebon Sirih dengan memanfaatkan fitur Firewall Filter Rules dan Access List pada perangkat MikroTik. Metode penelitian yang digunakan meliputi observasi, wawancara, dan studi pustaka untuk memperoleh informasi terkait kondisi jaringan yang berjalan. Hasil analisis menunjukkan bahwa sistem keamanan sebelumnya hanya menggunakan WPA2-PSK sehingga masih memiliki celah keamanan. Oleh karena itu, dilakukan perancangan sistem keamanan tambahan dengan menerapkan Access List untuk membatasi perangkat yang dapat terhubung ke jaringan serta Filter Rules untuk memblokir akses pengguna luar ke website internal perusahaan. Implementasi sistem ini diharapkan mampu meningkatkan keamanan jaringan wireless serta menjaga kerahasiaan data internal perusahaan.

Kata kunci: Keamanan Jaringan Wireless, Filter Rules, Access List

Abstract: *The development of wireless network technology provides convenience in communication and data exchange in organizational environments. However, the use of wireless networks also poses various security risks such as unauthorized access and potential data leaks. This study aims to design a wireless network security system at the Biznet Kebon Sirih Branch by utilizing the Firewall Filter Rules and Access List features on MikroTik devices. The research methods used include observation, interviews, and literature studies to obtain information regarding the running network conditions. The analysis results show that the previous security system only used WPA2-PSK so that it still has security gaps. Therefore, an additional security system was designed by implementing an Access List to limit devices that can connect to the network and Filter Rules to block external users' access to the company's internal website. The implementation of this system is expected to improve wireless network security and maintain the confidentiality of the company's internal data.*

DOI: 10.52362/jisamar.v10i2.2391

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.2 (May 2026)

Keywords: *Wireless Network Security, Rules Features, Access List*

I. PENDAHULUAN

Jaringan nirkabel merupakan bagian adri teknologi paling manarik dan revlolusiioner yang telah berkontribusi pada kemajuan dunia selama dua dekade terakhir, Prilakuk pola komunikasi dan orientasi bisnis individu di bergagai belajan dunia telah mengalami peningkatan sebagai akibatnya. Terutama dalam area yang didorong informasi, mobilitas, kenyamanan, kemudahan komunikasi, dan konektivitas tanpa hambatan telah menjadi keuntungan yang luar biasa dan signifikan secara alami. Saat ini, jaringan nirkabel atau wlan, telah menjadi norma untuk komunikasi data dan seluler bagi sebagian besar infrastruktur jaringan di kantor dan perusahaan besar[1]. Keamanan jaringan merupakan aspek yang sangat penting saat ini, khususnya pada jaringan hotspot WiFi. Sebagian besar ancaman yang menyerang jaringan berasal dari pengguna internal hotspot itu sendiri, sehingga keamanan jaringan nirkabel memerlukan perlakuan khusus[2]. Ketika jaringan mengalami serangan hingga menyebabkan kerusakan sistem, biaya yang dibutuhkan untuk perbaikan menjadi sangat besar. Terlebih lagi, apabila komputer server terhubung langsung dengan internet, potensi serangan akan semakin meningkat karena berbagai teknik serangan terus berkembang dan tidak dapat diabaikan. Oleh karena itu, diperlukan sistem keamanan jaringan yang mampu mengamankan serta meminimalkan ancaman terhadap jaringan dan server. Salah satu teknik yang dapat diterapkan adalah penggunaan Filter rules dan access list. Dengan Filter rules, pengguna yang terhubung ke WiFi gratis Biznet dapat dibatasi agar tidak mengakses website internal Biznet. Sementara itu, access list digunakan untuk mengatur pengguna yang diizinkan terhubung ke jaringan wireless. Dalam penerapannya, terdapat beberapa konfigurasi dasar yang dapat dilakukan dengan menggunakan aplikasi Winbox.

II. ETODE DAN MATERI

1. Metode Penelitian

a. Metode Pengumpulan data
   1. Observasi
      Pada penelitian ini peneliti melakukan observasi langsung ke objek penelitian, observasi ini bertujuan agar peneliti pendapatkan gambagran secara langsung dan nyata bagaimana stuktur jaringan yang berjalan pada objek penelitian
   2. Wawancara
      Pada tahapan ini dilakukan bersamaan dengan observasi pada objek penelitian, pada tahapan ini peneliti melakukan pengembangan pengamatan sambil melakukan tanya jawab ke para personel yang menagani langsung sistem kerja jaringan yang berjalan pada objek penelitian.
   3. Studi Pustaka
      Untuk menunjang teoritis yang dilakukan maka peneliti juga menambahkan informasi dari beberapa bahan kajian dengan tujuan menambah muatan informasi pada penelitian ini.

b. Metode Penelitian
   Metode SDLC
   a. Tahapa Analisa
      Pada tahapan ini peneliti mempelajari cara kerja dari sistem jaringan yang selama ini di gunakan pada objek penelitian tujuan dari tahapan ini adalah untuk memahami permasalahan jaringan yang berjalan selama ini agar dapat menemukan solusi yang optimal dari permasalahan atau kendala pada sistem jaringan di obejek penelitian.
   b. Desain
      Pada tahapan ini peneliti merancang sistem keamanan jaringan wireless pada objek penelitian dengan menggunakan filter rules dan access list.
   c. Testing
      Pada tahapan ini testing yang dilakukan oleh peneliti dengan cara melakukan pengujian
   d. Implemetasi

DOI: 10.52362/jisamar.v10i2.2391

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.2 (May 2026)

Pada tahapan ini peneliti melakukan konfigurasi keamanan pada wareless dengan menggunakan filter rules dan access list yang telah terpasang

2. Konsep Penunjang Penelitian

Dalam menunjang pelaksanaan penelitian kali ini, peneliti mempelajari materi yang berkaitan baik langsung ataupun tidak langsung pada objek penelitian yang berkaitan langsung dengan permasalahan yang dihadapai objekpenelitian guna mendapatkan solusi yang optimal.

Beberapa perangkat yang peneliti gunakan untuk mendapatkan solusi dari permasalahan tentang keamanan jaringan wireless pada objek penelitian adalah sebagai berikut :

a. Mikrotik

MikroTik RouterOS adalah Suatu System operasi berbasis linux yang digunakan sebagai pengelola jaringan meliputi Routing, Firewall, Hotspot, VPN, dan lain sebagainya. Mikrotik sudah di-integrasikan dengan RouterOS. Router ini banyak digunakan.. MikroTik RouterOS adalah perangakt yang paling banyak digunakan karena fleksibilitas dan kemampuan mengelola berbagai jenis konfigurasi jaringan. Salah satu teknologi andalannya adalah PPPoE (Point-to-Point Protocol over Ethernet), yang memberikan kemampuan pengelolaan pengguna terpusat serta autentikasi yang terjamin[14].

Router Mikrotik merupakan suatu alatyang mampu memberikan kelebihan dalam sistem jaringan komputer, Karena dengan menggunakan Router Mikrotik maka jaringan bisa dibuat dengan lebih stabil dan mudah untuk dimonitoring. Filter – Filter Mikrotik – Mikrotik yang digunakan Router untuk mengoptimalkan Jaringan Wireless adalah :

1) Address list : Barisan Kelompok IP address berdasarkan nama
2) DHCP (Dynamic Host Configuration Protocol), Mendukung DHCP tiap antarmuka, diantaranya DHCP Relay, DHCP Client, Multiple network DHCP, static and dynamic DHCP leases.
3) Firewall dan NAT (Network Address Translation): Mendukung proses filtering koneksi peer to peer, source NAT dan destination NAT. Mampu melakukan proses filtering berdasarkan MAC address (Media Access Control Address), IP address, range port, protokol IP, pemilihan opsi protokol seperti ICMP (Internet Control Message Protocol), TCP Flags dan MSS.
4) Hotspot : Hotspot gateway dengan otentikasi RADIUS. Mendukung limit data rate, SSL, HTTPS.
5) Proxy : memiliki Filter Cache untuk FTP dan HTTP proxy server, HTTPS proxy meliputi transparent proxy, untuk DNS dan HTTP mendukung protokol SOCKS, mendukung parent proxy, dan static DNS.
6) Tool : Ping, Traceroute, bandwidth test, ping flood, telnet, SSH, packet sniffer, Dinamik DNS update.WinBox : Aplikasi mode GUI untuk meremote dan MikroTik RouterOS.

III. PEMBAHASA DAN HASIL

a. Jaringan Usulan

Setelah penulis melakukan riset pada jaringan berjalan di Biznet Networks. Penulis mengusulkan untuk membuat perancangan jaringan wireless dengan keamanan membatasi akses pengguna yang bukan karyawan Biznet. Dari hasil riset penulis di lapangan, penulis membuat perancangan jaringan usulan untuk memenuhi kekurangan atau permasalahan pada jaringan yang sudah ada.

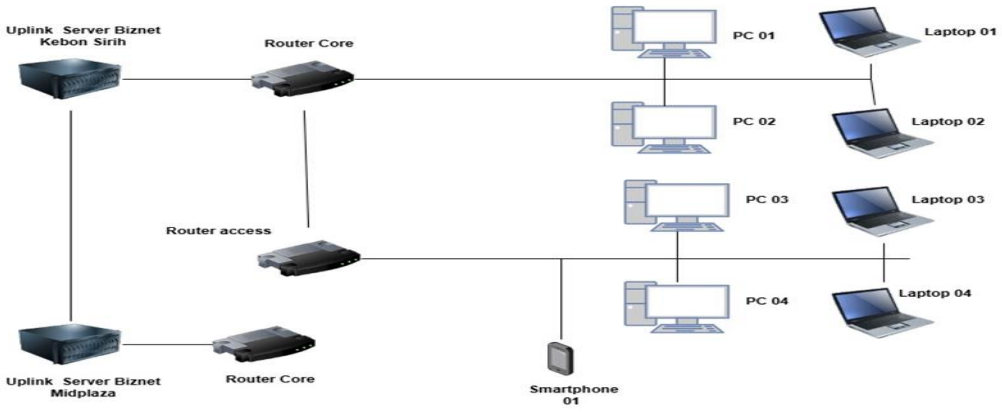
b. Topologi Jaringan

Dalam usulan topologi jaringan yang dipakai pada Biznet kebon sirih terdapat topologi hybrid terdiri dari topologi star dan topologi point to point yang berada pada perangkat uplink biznet dari jaringan yang sudah ada, karena terbatasnya akses dan kerahasian data perusahaan penulis tidak bisa meneliti lebih dalam terkait topologi jaringan keseluruhan yang perusahaan pada

c. Skema Jaringan

DOI: 10.52362/jisamar.v10i2.2391

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.2 (May 2026)



Gambar 3.1 Skema Jaringan yang dirancang

Sumber : Hail Penelitian tahun 2025

Skema jaringan yang pemulis usulankan memakai topologi hybrid yang terdiri dari Topologi Star dan Topologi point to point, untuk perangkat – perangkat keras yang digunakan yaitu : 2 unit Router Mikrotik seri RB941-2nd, 1 unit Router RB1100, 2 unit PC dan 2 Unit Laptop di Lantai 3, 2 unit PC , 2 unit laptop dan 1 Handphone.

d. Keamanan Jaringan

Keamanan yang digunakan pada Biznet Branch Kebon Sirih menggunakan WPA2-PSK yang diakses pada PC dan Laptop. Oleh karena itu penulis menambahkan Keamanan Jaringan menggunakan Firewall Filter rules dan access list untuk membatasi akses user dalam mengakses website internal Biznet

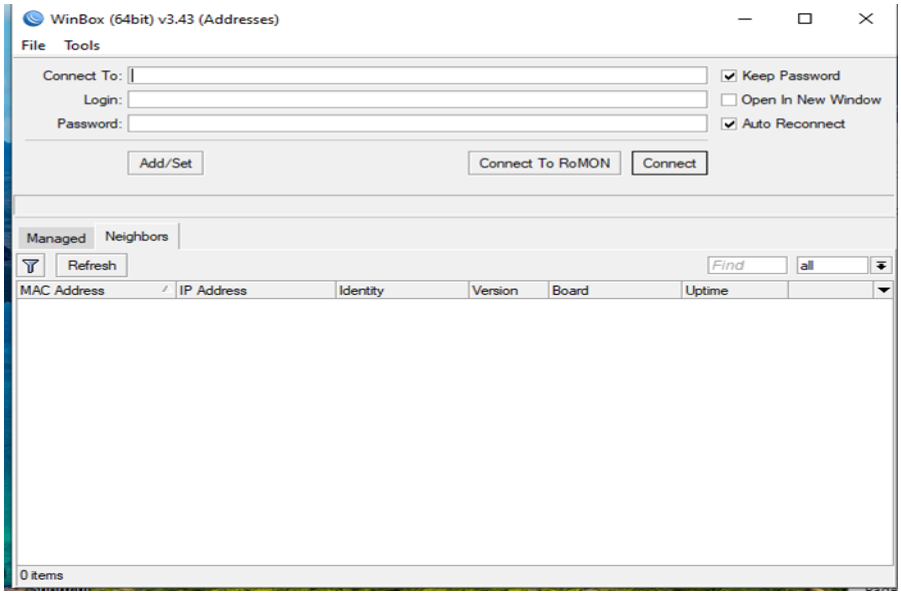
e. Rancangan Aplikasi

Dalam Perancangan aplikasi ini, penulis melakukan penelitian speksifikasi jaringan yang sudah berjalan dari mulai perangkat keras dan perangkat lunak di Biznet Branch Kebon sirih, membuat perancangan jaringan wireless dan menambahakan keamanan jaringan. Adapun tahapan-tahapan yang dilakukan penulis dalam melakukan perancangan jaringan yang diusulkan sebagai berikut :

1. Download dan install software Winbox version 3.43.
2. Menyalakan router mikrotik sebagai Router core di Lantai 3, sambungkan kabel utp port 1 ke jaringan ISP, untuk port 2 mikrotik sambungkan ke perangkat PC atau laptop yang sudah terintall software Winbox.
3. Pada menu winbox klik tombol refresh sampai muncul devuce mikrotik yang terbaca, username : admin dan password kosong, dan klik login

DOI: 10.52362/jisamar.v10i2.2391

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.2 (May 2026)



Gambar 3.2 WinBox

Sumber Hasil Penelitian 2025

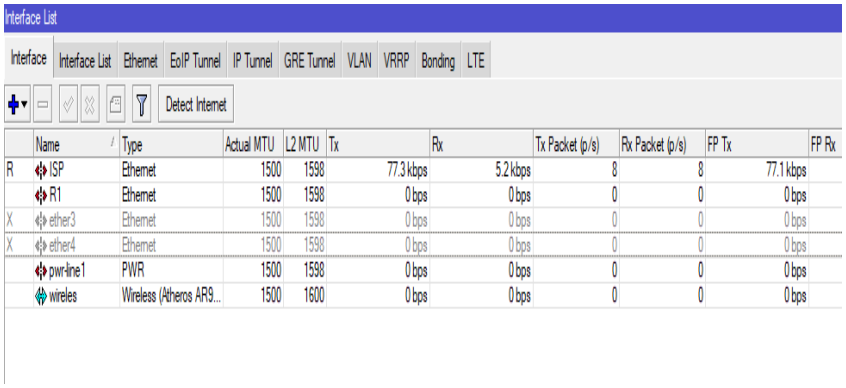
4. Cari Menu Terminal dan konfigurasi
5. Membuat identity dan name baru sebagai security untuk login mikrotik

```
[admin@MikroTik] > system identity set name=Operation
[admin@Operation] > user add name=IT password=biznetnetworks group=full
[admin@Operation] > user pr
Flags: X - disabled
 #    NAME                                                    GROUP
 0    ;;; system default user
      admin                                                   full
 1    IT                                                      full
[admin@Operation] > user remove numbers=0
[admin@Operation] > user pr
Flags: X - disabled
 #    NAME                                                    GROUP
 0    IT                                                      full
[admin@Operation] >
```

Gambar 3.3. Identify Router1

Sumber Hasil Penelitian 2025

6. Interface pada router core yang dipakai : ISP, R1, dan wireless



Gambar 3.4 Interface Router 1

Sumber hasil penelitian 2025

DOI: 10.52362/jisamar.v10i2.2391

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.2 (May 2026)

7. Membuat Lokasi IP baru

```
[IT@Operation] > interface pr
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                TYPE       ACTUAL-MTU L2MTU  MAX-L2MTU MAC-ADDRESS
 0  R  ISP                                 ether            1500  1598       2028 08:55:31:98:04:F5
 1     R1                                  ether            1500  1598       2028 08:55:31:98:04:F6
 2  X  ether3                              ether            1500  1598       2028 08:55:31:98:04:F7
 3  X  ether4                              ether            1500  1598       2028 08:55:31:98:04:F8
 4     pwr-line1                           ether            1500  1598       2028 08:55:31:98:04:F9
 5     wireles                             wlan             1500  1600       2290 08:55:31:98:04:FA
[IT@Operation] > ip add add address=192.168.18.2/24 interface=ISP
[IT@Operation] > ip add add address=172.168.32.1/24 interface=R1
[IT@Operation] > ip add add address=192.168.100.1/24 interface=wireless
input does not match any value of interface
[IT@Operation] > ip add add address=192.168.100.1/24 interface=wireles
[IT@Operation] > ip route add gateway=192.168.18.1
[IT@Operation] > ip dns set servers=192.168.18.1,8.8.8.8 allow-remote-requests=yes
[IT@Operation] > ip firewall nat add chain=srcnat action=masquerade out-interface=ISP
[IT@Operation] > ping google.com
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 216.239.38.120                             56 116 20ms
    1 216.239.38.120                             56 116 20ms
    2 216.239.38.120                             56 116 20ms
```

Gambar 3.5. Alokasi IP Adress

Sumber Hasil Penelitian 2025

Interface ISP alokasi ip : 192.168.18.2/24
Interface R1 alokasi ip : 172.168.32.1/24
Interface wireless alokasi ip : 192.168.100.1/24

8. Menambahkan konfigurasi DHCP server pada interface R1 dan Wireless.

```
[IT@Operation] > ip dhcp-server setup
Select interface to run DHCP server on

dhcp server interface: R1
Select network for DHCP addresses

dhcp address space: 172.168.32.0/24
Select gateway for given network

gateway for dhcp network: 172.168.32.1
Select pool of ip addresses given out by DHCP server

addresses to give out: 172.168.32.2-172.168.32.254
Select DNS servers

dns servers: 192.168.18.1,8.8.8.8
Select lease time

Lease time: 50m
[IT@Operation] > ip dhcp-server setup
Select interface to run DHCP server on

dhcp server interface: wireles
Select network for DHCP addresses

dhcp address space: 192.168.100.0/24
Select gateway for given network

gateway for dhcp network: 192.168.100.1
Select pool of ip addresses given out by DHCP server

addresses to give out: 192.168.100.2-192.168.100.254
Select DNS servers

dns servers: 192.168.18.1,8.8.8.8
Select lease time

Lease time: 50m
[IT@Operation] >
```

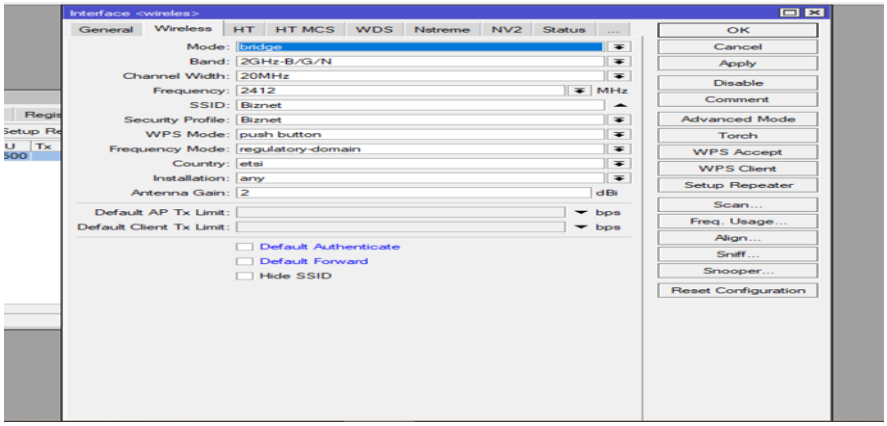
Gambar 3.6. Konfigurasi DHCP R1 dan wireless

Sumber Hasil Penelitian 2025

9. Menambahkan konfigurasi access list pada interface wireless

DOI: 10.52362/jisamar.v10i2.2391

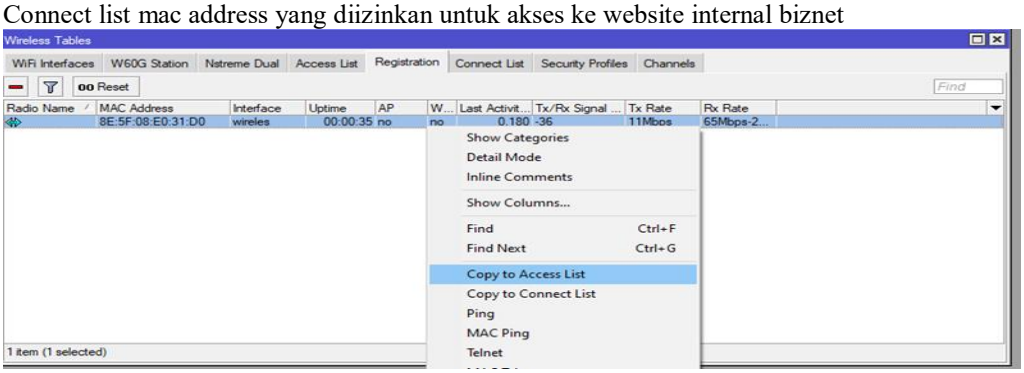
Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.2 (May 2026)



Gambar 3.7 Konfigurasi Wereless

Sumber Hasil Penelitian 2025

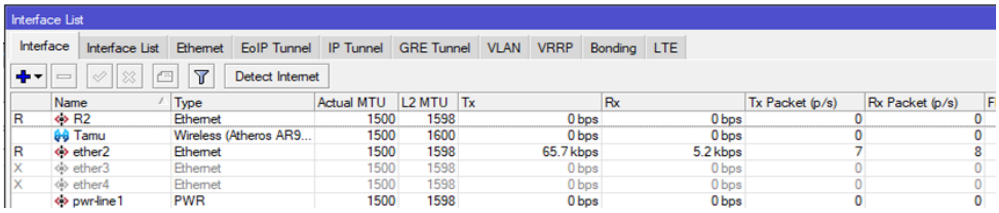
10. Connect list mac address yang diizinkan untuk akses ke website internal biznet



Gambar 3.8. Connect list macc address

Sumber Hasil Penelitian 2025

11. Menyalakan router mikrotik 2 sebagai Router access pada Lantai 1, sambungkan port 2 Router core ke Port 1 Router access sebagai WAN.
12. Interface pada Router access yang dipakai : R2 dan Tamu



Gambar 3.9 Interface Router 2

Sumber Hasil Penelitian 2025

13. Membuat identity dan name yang sama dengan router core.

```
/command          Use command at the base level
[admin@MikroTik] > system identity set name=Operation
[admin@Operation] > user add name=IT password=biznetnetworks group=full
[admin@Operation] > user pr
Flags: X - disabled
 #    NAME                GROUP                ADDRESS              LAST-LOGGED-IN
 0    ;;; system default user
      admin               full                                      jan/02/1970 00:07:36
 1    IT                  full
[admin@Operation] > user remove numbers=0
[admin@Operation] > user pr
Flags: X - disabled
 #    NAME                GROUP                ADDRESS              LAST-LOGGED-IN
 0    IT                  full
[admin@Operation] >
```

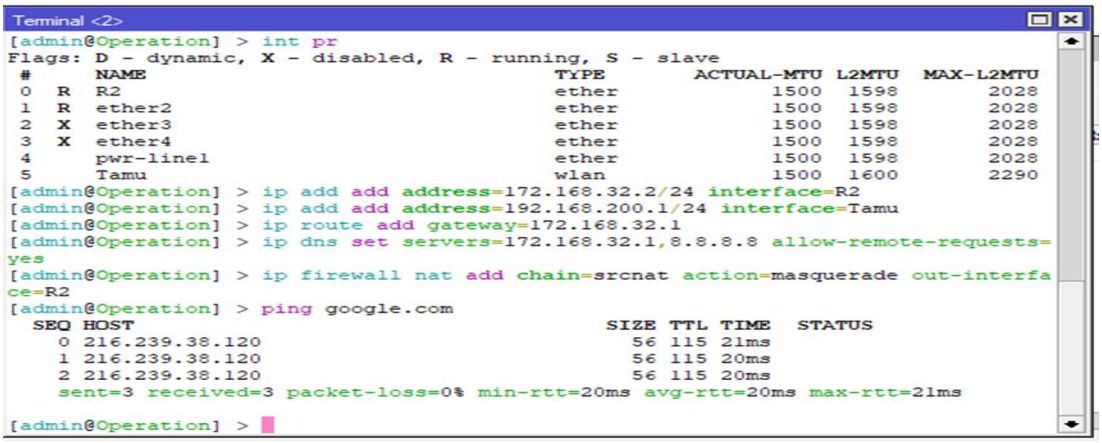
DOI: 10.52362/jisamar.v10i2.2391

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.2 (May 2026)

Gambar 3.10 Skema Jaringan Usulan

Sumber Hasil Penelitian 2025

14. Membuat alokasi ip address pada 2 interface

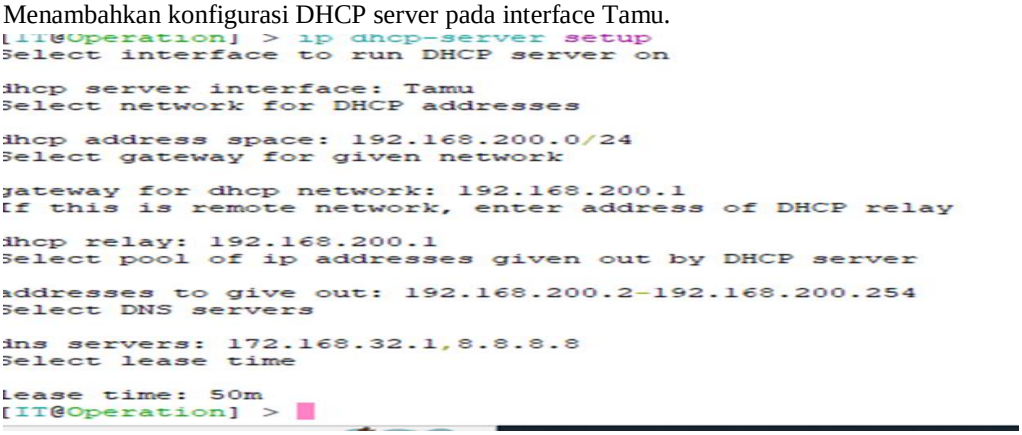


Gambar 3.11 Konfigurasi Ip address Router 2

Sumber Hasil Penelitian

Interface ISP alokasi ip : 172.168.32.2/24
Interface R1 alokasi ip : 192.168.200.1/24

15. Menambahkan konfigurasi DHCP server pada interface Tamu.



Gambar 3.12 Konfigurasi DHCP Server interface Tamu

Sumber Hasil Penelitian 2025

16. Menambahkan konfigurasi firewall Filter rules pada interface Tamu.

Gambar 3.13 Konfigurasi Firewall Filter rules

DOI: 10.52362/jisamar.v10i2.2391

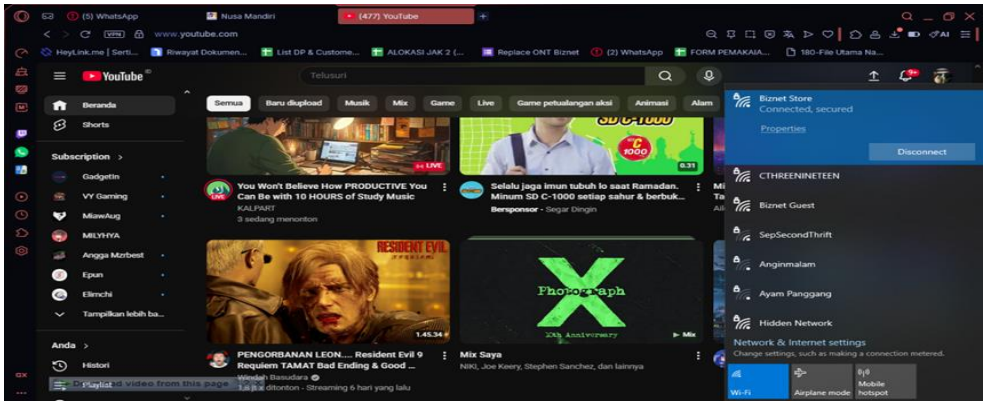
Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 10 No.2 (May 2026)

Sumber Hasil Penelitian 2025

f. Pengujian Jaringan

1. Pengujian Awal

Dalam tahap ini, pengujian dilakukan terhadap jaringan yang masih menggunakan jaringan wifi WPA2-PSK.. Tujuan dari pengujian ini adalah untuk mengetahui alur kerja jaringan yang di pakai dan keamanan jaringan yang sedang berjalan.

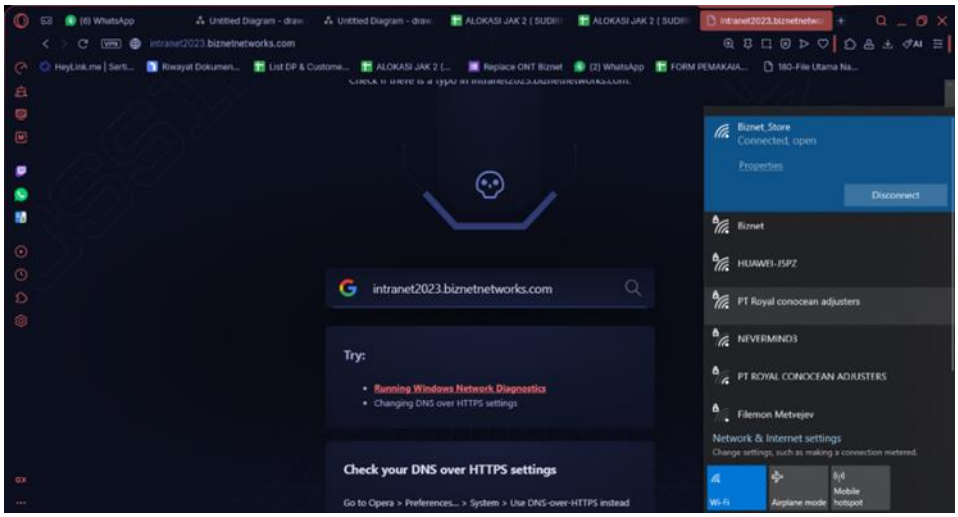


Gambar 3.14 Hasil Pengujian awal

Sumber Hasil Penelitian 2025

2. Pengujian Akhir

Pengujian ini dilaksanakan bersama dengan tim operasional pada objek penelitian guna memastikan performa dan kestabilan jaringan berjalan sesuai dengan standar yang diterapkan.



Gambar 3.15 Hasil pengujian Akhir

Sumber Hasil Penelitian 2025

IV. KESIMPULAN

Dari hasil implementasi sistem kemanan jaringan wereless pada objek penelitian dapat diambil kesimpulan bahwa jaringan WLAN dengan menggunakan *acces list* dan *filter rules* telah berhasil dalam mendukung opersional jaringan pada objek penelitian, namun dalam praktek nya perlu secara rutin di adakan pemantauan dan pemeliharaan secara berkala terutama pada router mikrotik guna mengaantisipasi kerusakan atau kesalahan pada sistem router mikrotik dan untuk lebih mengoptimalkan pengamanan jaringan pada objek penelitian tentusaja diharuskan menggunakan standar opersional prosedur yang lebih baik lagi

REFERENASI

DOI: 10.52362/jisamar.v10i2.2391

[1] I. C. Emeto, U. W. Anthony, D. C. Elenwo, A. A. Galadima, C. O. Ajayi, and M. S. Hamza, "Security Vulnerabilities of Wlan Protocols : A Review," vol. 17, no. 9, pp. 13–26, 2024.

[2] R. Rajawali, N. Saifullah, L. S. Arum, and J. Maulindar, "Perancangan Sistem Keamanan Jaringan Hotspot / Microtik OS," … Nas. Teknol. Inf. …, no. 55, pp. 704–706, 2022, [Online]. Available: http://ojs.udb.ac.id/index.php/Senatib/article/download/1993/1576

[3] T. S. Juniarti, F. Teknik, T. Informatika, U. M. Bengkulu, and K. Bengkulu, "Jurnal Software Engineering and Information System (SEIS) STRATEGI PENERAPAN WIRELESS MESH NETWORK UNTUK," vol. 5, no. 2, pp. 98–107, 2025.

[4] S. E. Prasetyo and E. Tan, "Analisis Quality of Service (QoS) Jaringan Wireless 2.4 GHz dan 5 GHz di Dalam Ruangan dengan Hambatan Kaca," J. Ilm. Teknol. Inf. Asia, vol. 15, no. 2, pp. 103–114, 2021, doi: 10.32815/jitika.v15i2.609.

[5] M. D. Nurfaishal and Y. Akbar, "Analisis Efektivitas Keamanan Jaringan Layer 2 : Port Security , VLAN Hopping , DHCP Snooping Abstrak," vol. 5, no. 3, pp. 3278–3290, 2024.

[6] C. Kamila Wilujeng and A. Voutama, "Implementasi Firewall Filter Rules Sebagai Filtering Content Pada Jaringan Komputer Menggunakan Mikrotik," JATI (Jurnal Mhs. Tek. Inform., vol. 8, no. 3, pp. 2680–2685, 2024, doi: 10.36040/jati.v8i3.9530.

[7] F. Azmi, T. U. Kalsum, and H. Alamsyah, "Analysis and Application of Access Control List (ACL) Methods on Computer Networks Analisa dan Penerapan Metode Access Control List (ACL) pada Jaringan Komputer," vol. 2, no. 1, pp. 81–88, 2022.

[8] M. Tahir and M. I. Firdausi, "Peningkatan Keamanan Jaringan LAN dan WLAN Melalui Standard Acces Control List," vol. 4, no. 1, pp. 607–614, 2024.

[9] E. Saepudin et al., "IMPLEMENTASI BITDEFENDER CORPORATE SECURITY UNTUK," vol. 9, no. 2, 2022.

[10] V. Assyahdani and S. P. Ismoyo, "Pemanfaatan Jaringan Komputer LAN , MAN , dan WAN di Era," vol. 3, no. 7, pp. 1581–1585, 2025.

[11] R. Kaur, D. Kaur, and R. Kaur, "An Overview on Network Topologies," vol. 2, no. 4, pp. 40–43, 2023.

[12] A. G. Alenezi and M. F. Aldhamen, "A Comparative Study between IPv4 and IPv6," vol. 12, no. 3, pp. 52–55, 2023, doi: 10.17148/IJARCCE.2023.12310.

[13] R. K. Cahyawati, F. Fadwa, K. Agustin, and K. S. Arum, "Perancangan Keamanan Jaringan Menggunakan Metode Firewall Security Port," no. November, pp. 203–209, 2023.

[14] A. Samad and M. F. Adiman, "Jurnal Sistem dan Teknologi Informasi Indonesia Konfigurasi MikroTik RouterOS untuk Manajemen Jaringan pada Infrastruktur Jaringan RT / RW Net MikroTik RouterOS Configuration for Network Management in RT / RW Net Network Infrastructure," vol. 10, no. 2, pp. 118–125, 2025.

DOI: 10.52362/jisamar.v10i2.2391