JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika

[E-ISSN 2656-0321]
[Vol 15 No 1]
[Januari 2021]

OPTIMALISASI KEAMANAN WIRELESS MENGGUNAKAN *FILTERING* MAC *ADDRESS*

Firmansyah [a,1,*], Rachmat Adi Purnama [b,2], Rachmawati Darma Astuti [c,3]
[1]Sistem Informasi
[2]Teknologi Komputer, Fakultas Teknologi Informasi
[3]Teknologi Informasi, Fakultas Teknologi Informasi
[1]Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri
[2, 3]Universitas Bina Sarana Informatika
Firmansyah.fmy@nusamandiri.ac.id, rachmat.rap@bsi.ac.id, rachmawati.rcd@gmail.com

ARTICLE INFO

Keywords
Filtering MAC Address
Hotspot Login
Wireless Security

ABSTRACT

The use 802.11 wireless-based network services have become one of the most widely used network services, this will be directly proportional to the security holes that are in the wireless network. The rise of access rights theft in wireless networks is due to the large number of software and tools available on the internet to read encryption in wireless security. To minimize the occurrence of theft of access rights in wireless networks can use a layered security system by implementing security Hotspot login and MAC Address Filtering. This layered wireless network security is able to block users who try to access the network. This is because the wireless network security system has verified access rights 2 (two) times by matching the username and password in the hotspot login with the physical address or MAC address of the client. From the research results obtained by clients who use a username and password with different devices can not access the computer network. So every client who wants to connect to the internet network must use a device that has registered its MAC Address and in accordance with user access rights and passwords in the Hotspot login.

1. Pendahuluan

Beberapa tahun terakhir ini, Wireless LAN berbasis 802.11 telah menjadi hal yang umum dilingkungan perkantoran dan dunia kampus [1] . Perkiraan terbaru menunjukan lebih dari 10 miliar perangkat WiFi telah terjual secara total dan lebih dari 4,5 miliar perangkat tersebut digunakan saat ini. Pada jaringan nirkabel, masalah keamanan memerlukan perhatian yang lebih serius, mengingat media transmisi datanya adalah gelombang radio yang bersifat broadcast [2] [3]. Hal ini merupakan salah satu alasan rentannya keamanan didalam jaringan wireless. Kebijakan otentikasi diadopsi untuk mengamankan akses, penyalahgunaan, modifikasi, serta melakukan penolakan terhadapa layanan didalam jaringan dan sumber daya lainnya [4]. Banyak pengguna jaringan wireless tidak mengetahui jenis bahaya apa yang sedang menghampiri mereka saat terhubung kedalam Jaringan Wireless Access Point (WAP), misalnya seperti sinyal WLAN yang dapat disusupi oleh hacker [5]. Standar keamanan yang digunakan untuk koneksi dari user ke access point adalah WPA Personal, dimana WPA Personal ini bisa dikatakan sangat lemah karena untuk setiap SSID akan menggunakan user dan password yang sama untuk semua pengguna [6]. Keamanan wireless WEP (Wired Equivalent Privacy) merupakan standart dari keamanan wireless yang sebelumnya mampu meminimalisir pembatasan hak akses kedalam jaringan wireless. Namun kini keamanan wireless menggunakan WEP sudah mudah dipecahkan dengan berbagai tools yang tersedia didalam jaringan

https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 15 No 1]
[Januari 2021]

internet [7]. Tingkat keamanan pada jaringan wireless LAN tidaklah sama dengan jaringan kabel LAN [8].

Jaringan nirkabel IEEE 802.11 telah menjadi salah satu jaringan yang paling banyak digunakan [9]. Karena sifat media nirkabel yang terbuka, peretas dan penggangu dapat memanfaatkan internet untuk menemukan celah keamanannya. Kegiatan yang mengancam keamanan jaringan wireless dapat dilakukan dengan cara Warchalking, WarDriving, WarFlying, WarSpamming, atau WarSpying. Walaupun memiliki sitem keamanan, jaringan wireless masih dapat di diserang oleh para attacker [10]. Untuk memilimalisir pengguna layanan jaringan tanpa melakukan pembayaran dan membatasi akses kedalam jaringan dapat menggunakan sistem keamanan MAC Address Filtering. Metode security MAC Address dapat diimplementasikan menggunakan metode Filter Rule. Metode ini dapat bekerja melakukan filtering terhadap perangkat yang mencoba melakukan akses kedalam jaringan komputer.

MAC Address merupakan sebuah identifikasi unik yang terdiri dari berbagai bilangan byte yang ditugaskan untuk sebagian besar adapter jaringan atau Network Interface Card (NIC) [11]. Setiap perangkat jaringan memiliki MAC Address yang berbeda satu dengan lainnya. Maka dengan menerapkan security MAC Address setiap pengguna layanan jaringan yang ingin terhubung kedalam jaringan harus melakukan pendaftaran MAC ddressnya. Hal ini dapat digunakan untuk meminimalisir pengguna layanan jaringan yang seharusnya tidak mendapatkan akses. *Firewall filtering* MAC Address telah dikembangkan untuk memberikan perlindungan terhadap pelayanan jaringan wireless. Penggunaan filtering MAC Address mampu membatasi beberapa komputer yang dapat terhubung kedalam wireless hotspot dengan mempertimbangkan IP Address dan MAC Address yang terdaftar [12] [13]. Diharapkan pengimplementasian keamanan secara ganda mampu meningkatkan keamanan didalam jaringan komputer. Karena pemakaian frekwensi yang sifatnya lebih terbuka dibanding dengan menggunakan kabel, maka kerentanan keamanan jalur komunikasi akan lebih berbahaya dibandingkan menggunakan kabel. Untuk itu perlu dilakukan penanganan keamanan yang lebih ekstra pada jaringan wireless. Penelitian sebelumnya, celah keamanan yang terdapat didalam hotspot login dapat dimanfaatkan oleh client yang tidak berhak untuk mengganggu kestabilan insfratruktur jaringan bahkan sampai keamanan privasi client yang digunakan hak aksesnya [14]. Hal inilah yang mendorong untuk pengimplemetasian keamanan jaringan wireless secara berlapis dengan menggunakan keamanan hotspot login dan filtering MAC address. Jadi setiap perangkat yang ingin terhubung kedalam jaringan internet harus didaftarkan MAC Addressnya terlebih dahulu [15] . Dengan kata lain, client bias terkoneksi jika MAC-address sudah terdaftar. Bagi MAC-address yang belum terdaftar, tidak dapat terkoneksi [16].

2. Metodologi Penelitian

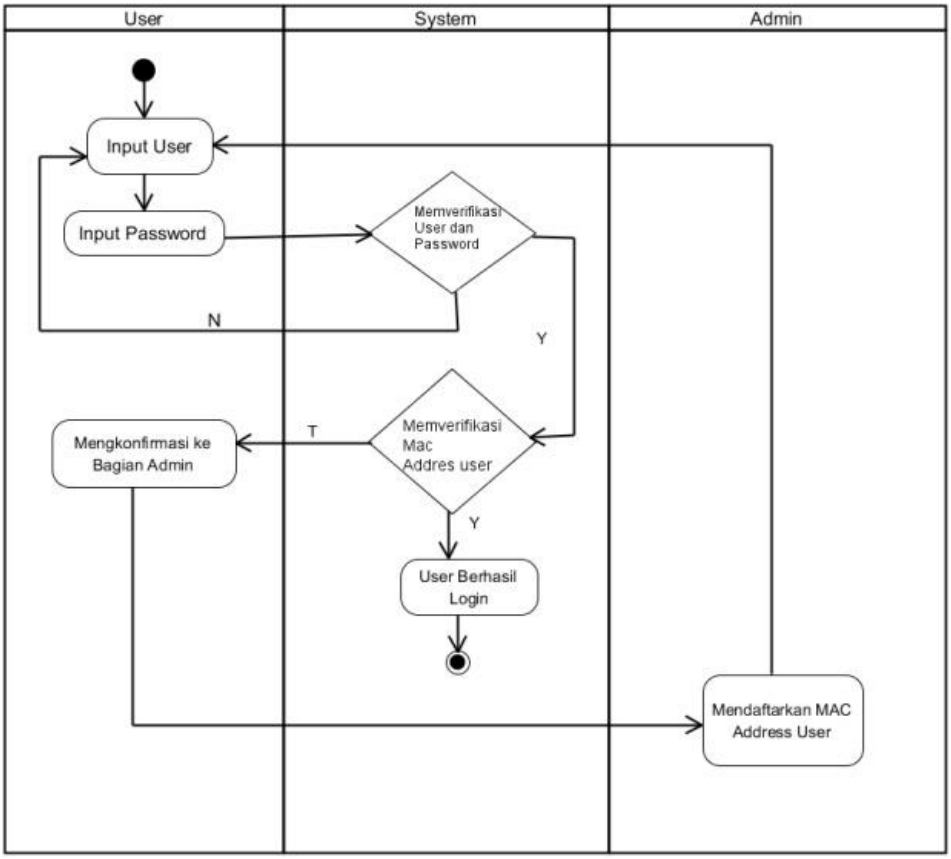
Dalam melakukan penelitian Optimalisasi Keamanan Wireless Menggunakan Filtering MAC Address penulis menggunakan bantuan perangkat mikrotik routerboard 951Ui-2HND yang diimplementasikan menggunakan dua (2) mode access point baik mode station untuk terhubung kedalam jaringan internet dan mode ap bridge untuk menghubungkan dengan jaringan lokal untuk melakukan uji konektifas terhadap keamanan jaringan yang digunakan. Dengan menggunakan keamanan wireless *two factor*, hotspot login dan filtering MAC Address diharapkan mampu melakukan pencegahan dari pengguna asing yang tidak diizinkan untuk melakukan akses kedalam jaringan wireless. Metode penelitian yang digunakan dalam penelitian ini menggunakan *The Security Policy Development Life Cycle (*SPDLC), yang memiliki enam (6) tahapan, yaitu:

a. Identifikasi, digunakan untuk melakukan pengidentifikasian terhadap permasalahan keamanan didalam jaringan wireless.
b. Analisis, pada tahapain ini penulis melakukan percobaan untuk mengetahui resiko dan ancaman didalam keamanan jaringan wireless.
c. Perancangan, tahapan ini penulis melakukan perancangan keamanan jaringan wireless menggunakan filtering MAC Address.

https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 15 No 1]
[Januari 2021]

d. Implementasi, penulis melakukan konfigurasi keamanan jaringan wireless dan melakukan tahapan uji konektifitas terhadap keamanan jaringan wireless.
e. Audit, digunakan untuk melakukan pemeriksaan terhadap system keamanan yang telah diimplementasikan.
f. Evaluasi, melakukan evalusi system keamanan yang telah diterapkan.



Gambar 1. Activity Diagram

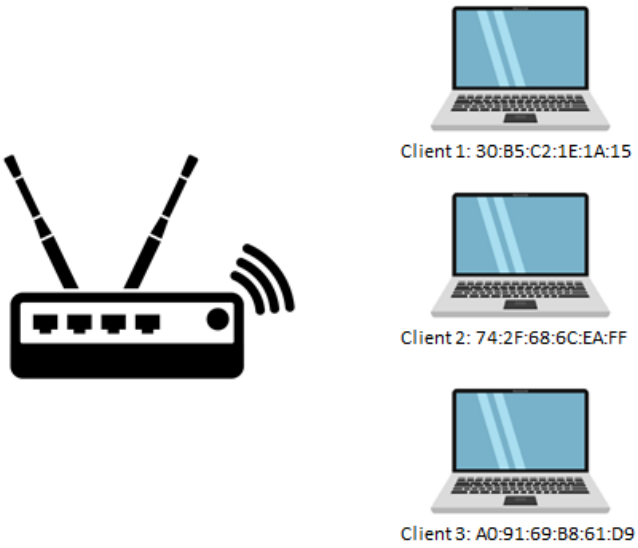
Terlihat pada gambar 1 merupakan alur flowchart yang digunakan dalam penilitan Optimalisasi Keamanan Wireless Menggunakan Filtering MAC Address. Client yang akan melakukan akses kedalam jaringan internet harus melewati verifikasi keamanan sebanyak 2 (dua) kali. Baik keamanan menggunakan user dan password pada hotspot login serta verifikasi terhadap MAC address yang digunakan.

3. Hasil dan Pembahasan

Untuk mengimplementasikan Optimalisasi Keamanan Wireless Menggunakan Filtering MAC Address penulis menggunakan skema jaringan yang terlihat pada gambar 2 dengan spesifikasi IP *Address* yang terlihat pada Tabel 1.

https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 15 No 1]
[Januari 2021]



Gambar 2. Skema Jaringan

Terlihat pada gambar 2 merupakan skema jaringan yang digunakan didalam penelitian, client 1 menggunakan MAC Address 30:B5:C2:1E:1A:15, sedangkan client 2 menggunakan MAC Address 74:2F:68:6C:EA:FF serta client 3 menggunakan MAC Address A0:91:69:B8:61:D9. Nantinya setiap client akan mendapatkan hak akses kedalam jaringan dengan melakukan verifikasi didalam Hotspot login dengan menggunakan user dan password yang berbeda diantara client.

Tabel 1 Spesifikasi IP Address

Interface	IP Address	Network
Wlan1 (to Public)	192.168.43.1	192.168.43.0
Ether2 (to Local)	192.168.2.1	192.168.2.0
Wlan2 (to Local)	192.168.10.1	192.168.10.0
Client 1	DHCP Client	192.168.10.0
Client 2	DHCP Client	192.168.10.0
Client 3	DHCP Client	192.168.10.0

Terlihat pada Tabel 1, Interface WLAN 1 dengan alokasi IP Address 192.168.43.1 digunakan sebagai IP Address yang terhubung dengan IP Publik, sedangkan interface ether2 dengan alokasi IP Address 192.168.2.1 digunakan sebagai gateway untuk jaringan lokal yang terhubung menggunakan media kabel serta interface Wlan2 dengan alokasi IP Address 192.168.10.1 digunakan sebagai gateway pada jaringan lokal wireless.

Tabel 2 Spesifikasi User dan Password

MAC Address	User	Password
30:B5:C2:1E:1A:15	FMY	FMY2020
74:2F:68:6C:EA:FF	RAP	RAP2020
A0:91:69:B8:61:D9	RCD	RCD2020

Dijelaskan pada Tabel 2 merupakan hak akses dari client untuk melakukan koneksi kedalam jaringan wireless. User FMY dengan password FMY2020 nantinya hanya dapat digunakan oleh

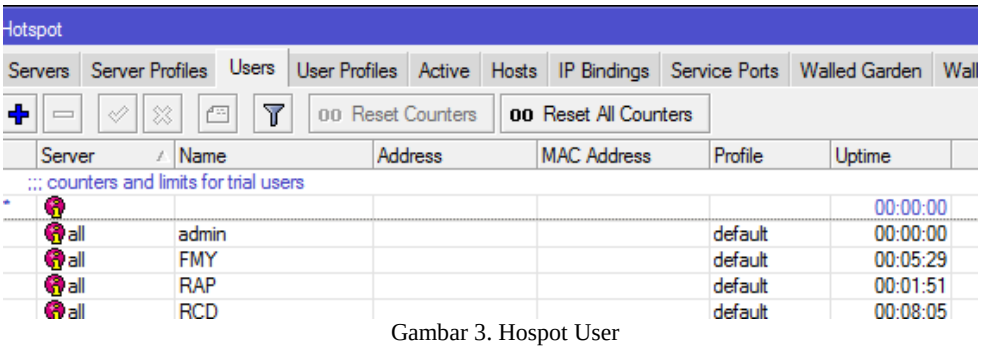
https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 15 No 1]
[Januari 2021]

Client dengan MAC Address 30:B5:C2:1E:1A:15 saja dan User RAP dengan password RAP2020 hanya dapat digunakan oleh client dengan MAC Address 74:2F:68:6C:EA:FF saja sedangkan client User RCD hanya dapat digunakan untuk client dengan MAC Address A0:91:69:B8:61:D9 saja. Terdapat 2 (dua) model skenario pengujian untuk melakukan Optimalisasi Keamanan Wireless Menggunakan Filtering MAC Address nantinya. Scenario pertama semua client dapat melakukan akses kedalam jaringan dengan menggunakan user dan password secara bebas sedangkan skenario pengujian kedua ialah melakukan pembatasan akses berdasarkan user, password dan MAC addressnya.

3.1 Uji Konektifitas Skenario 1

Didalam uji konektifitas skenario 1 peneliti akan melakukan uji koneksi terhadap keamanan jaringan wireless menggunakan Hostpot Login. Terlihat pada gambar 3 merupakan User Hotspot yang dapat terhubung kedalam jaringan wireless. Terdapat 3 (tiga) user yang telah mendapatkan hak akses untuk melakukan konektifitas kedalam jaringan wireless menggunakan keamanan wireless hotspot login.

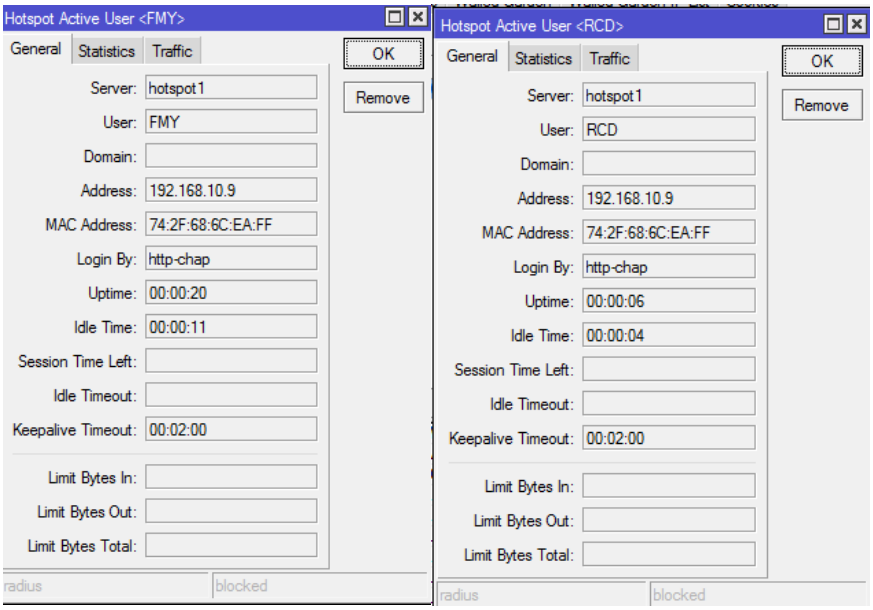


Gambar 3. Hospot User

Dengan mengimplementasikan keamanan jaringan wireless menggunakan hotspot login mampu membatasi pengguna layanan berdasarkan user dan password yang diberikan oleh seorang network administrator didalam jaringan. Namun, keamanan jaringan wireless menggunakan model hotspot login ini pun masih mengalami sebuah kerentanan seperti terlihat pada gambar 4 terdapat sebuah client dengan menggunakan MAC Address 74:2F:68:6C:EA:FF mampu melakukan login dengan menggunakan user FMY dan RCD yang seharusnya client dengan MAC Address digunakan untuk user RAP.

https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 15 No 1]
[Januari 2021]



Gambar 4. Hotspot Active User

Pada tabel 3 dijelaskan terdapat sebuah celah keamanan dari pengimplementasian keamanan jaringan wireless yang hanya menggunakan hotspot login. Ketika terdapat salah satu client yang telah mengetahui user dan password dari client lainnya. Client tersebut dapat menggunakan user dan password client lain untuk melakukan konektifitas kedalam jaringan Wi-Fi. Dijelaskan pada tabel 3, client 1 dengan MAC Address 30:B5:C2:1E:1A:15 mampu melakukan login baik menggunakan user FMY, RAP dan RCD, sedangkan client 2 dengan MAC Address 74:2F:68:6C:EA:FF pun mampu melakukan hal yang sama untuk login dengan user FMY, RAP dan RCD. Serta client 3 dengan MAC Address A0:91:69:B8:61:D9 yang seharusnya digunakan untuk user RCD dapat melakukan konektifitas kedalam jaringan wireless menggunakan user FMY maupun RAP.

Tabel 3. Spesifikasi Security Hotspot Login

MAC Address	USER	PASSWORD	KONEKTIFITAS
30:B5:C2:1E:1A:15	FMY	FMY2020	OK
	RAP	RAP2020	OK
	RCD	RCD2020	OK
74:2F:68:6C:EA:FF	FMY	FMY2020	OK
	RAP	RAP2020	OK
	RCD	RCD2020	OK
A0:91:69:B8:61:D9	FMY	FMY2020	OK
	RAP	RAP2020	OK
	RCD	RCD2020	OK

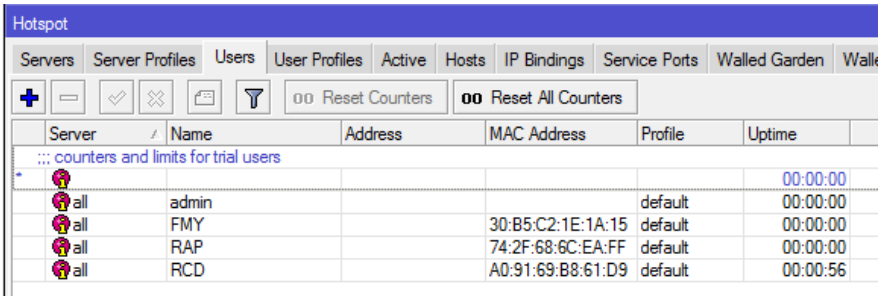
https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 15 No 1]
[Januari 2021]

Celah keamanan yang terdapat didalam hotspot login dapat dimanfaatkan oleh client yang tidak berhak untuk mengganggu kestabilan insfratruktur jaringan bahkan sampai keamanan privasi client yang digunakan hak aksesnya.

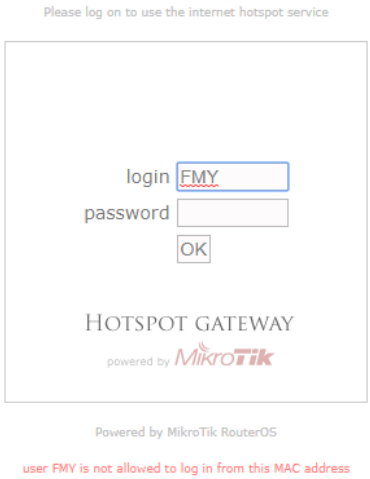
3.2 Uji Konektifitas Skenario 2

Skenario pengujian jaringan wireless yang ke dua ialah melakukan komparasi keamanan jaringan wireless menggunakan hostpot login dengan filtering MAC address. Hal ini digunakan untuk meminimalisir terjadinya hal seperti tabel 3 semua user dan password dapat digunakan oleh siapupun selama mengetahui user dan passwordnya. Dijelaskan pada gambar 5 setiap user yang akan terkoneksi kedalam jaringan wireless akan didaftarkan MAC Addressnya kedalam Hotspot User. Hal ini bertujuan agar user FMY hanya dapat digunakan oleh perangkat dengan MAC Address 30:B5:C2:1E:1A:15 saja, dan user RAP hanya dapat digunakan oleh perangkat dengan MAC Address 74:2F:68:6C:EA:FF, serta user RCD hanya dapat digunakan oleh perangkat dengan MAC Address A0:91:69:B8:61:D9 saja



Gambar 5. Hotspot User dengan MAC Address

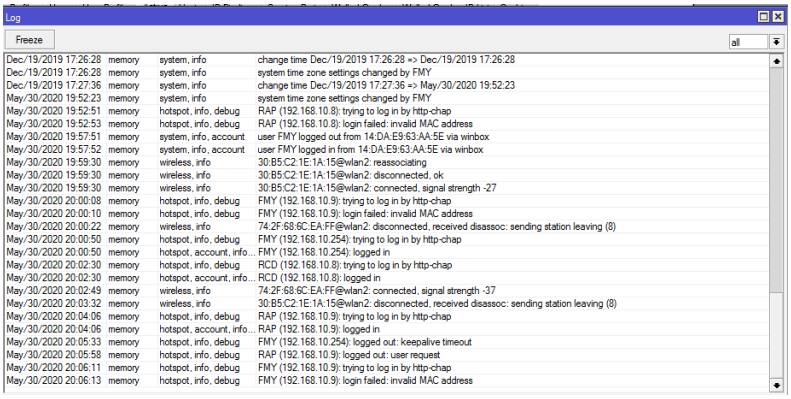
Ketika terdapat client yang melakukan percobaan akses kedalam jaringan dengan menggunakan user dan password yang berbeda, maka MikroTik RouterBoard secara otomatis akan menolaknya, seperti terlihat pada gambar 6. Dijelaskan pada gambar 6 dan gambar 7, terdapat client dengan MAC address yang berbeda melakukan percobaan akses kedalam jaringan wireless dengan menggunakan user FMY dan hasilnya client dengan perangkat yang berbeda tersebut tidak dapat terhubung kedalam jaringan komputer.



Gambar 6. Login Beda MAC Address

https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 15 No 1]
[Januari 2021]



Gambar 7. Log Percobaan Login Beda MAC Address

Terlihat pada TABEL IV merupakan uji konektifitas terhadap jaringan wireless menggunakan hostpot login dengn filtering MAC address. Jika sebelumnya, semua client dapat menggunakan user dan password siapapun. Ketika telah pengimplementasian filtering MAC address, user FMY hanya dapat digunakan oleh perangkat dengan MAC Address 30:B5:C2:1E:1A:15 saja, dan user RAP hanya dapat digunakan oleh perangkat dengan MAC Address 74:2F:68:6C:EA:FF

Tabel 4. Uji Konektifitas

MAC Address	USER	PASWD	KONEKTIFITAS	
			AFTER	BEFOR
30:B5:C2:1E:1A:15	FMY	FMY2020	OK	OK
	RAP	RAP2020	OK	BLOCK
	RCD	RCD2020	OK	BLOCK
74:2F:68:6C:EA:FF	FMY	FMY2020	OK	BLOCK
	RAP	RAP2020	OK	OK
	RCD	RCD2020	OK	BLOCK
A0:91:69:B8:61:D9	FMY	FMY2020	OK	BLOCK
	RAP	RAP2020	OK	BLOCK
	RCD	RCD2020	OK	OK

4. Kesimpulan

Dengan pengimplementasian keamanan jaringan wireless menggunakan filtering MAC address mampu melakukan block terhadap user yang melakukan percobaan akses kedalam jaringan. Model keamanan jaringan wireless secara berlapis ini dengan menggunakan hotspot login dan kombinasi filtering MAC address dapat mengoptimalkan keamanan jaringan baik untuk insfrastruktur jaringan maupun terhadap keamanan pengguna layanan jaringan. Hal ini dikarenakan sistem keamanan jaringan wireless telah melakukan verifikasi hak akses sebanyak 2 (dua) kali dengan mencocokan username dan password didalam hotspot login dengan physal address ataupun MAC address dari client tersebut. Jadi setiap client yang ingin terhubung kedalam jaringan internet haruslah menggunakan perangkat yang telah didaftarkan MAC Addressnya dan sesuai dengan hak akses user dan password didalam Hotspot login.

https://doi.org/10.47111/JTI

JURNAL TEKNOLOGI INFORMASI
Jurnal Keilmuan dan Aplikasi Bidang Teknik Informatika
[E-ISSN 2656-0321]
[Vol 15 No 1]
[Januari 2021]

Daftar Pustaka

[1] F. Wamser, R. Pries, D. Staehle, K. Heck, And P. Tran-Gia, "Traffic Characterization Of A Residential Wireless Internet Access," *Telecommun Syst*, Vol. 48, No. 1, Pp. 5–17, 2011.

[2] D. Yuniarto, "Keamanan Jaringan Wireless Lan Menggunakan Mac Address Di Smk Informatika Sumedang," *J. Infoman's*, Vol. 3, No. 1, Pp. 47–52, 2019.

[3] E. A. Darmadi, "Perancangan Sistem Otentikasi Radius Pada Pengguna Jaringan Wireless Untuk Meningkatkan Keamanan Jaringan Komputer," *Ikra-Ith Inform.*, Vol. 2, No. 3, Pp. 9–16, 2018.

[4] N. Ag And G. Shankar, "A Survey On Wireless Security Standards And Future Scope," *Int. J. Latest Res. Eng. Technol.*, Vol. 02, No. 08, Pp. 94–99, 2016.

[5] A. Tedyyana, "Rancang Bangun Jaringan Wirelless Di Politeknik Negeri Bengkalis Menggunakan Mac Filtering," In *Seminar Nasional Inovasi Dan Aplikasi Teknologi Di Industri (Seniati)*, 2016, Pp. 31–36.

[6] I. Wiratama, P. Sugiartawan, F. I. Komputer, And T. Informatika, "Peningkatan Keamanan Wireless Pada Jaringan Komputer Di Universitas Amikom Menggunakan Protokol Ieee802.1x," *J. Sist. Inf. Dan Komput. Terap. Indones.*, Vol. 2, No. 1, Pp. 21–30, 2019.

[7] M. I. Rusdi And D. Prasti, "Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux," In *Seminar Nasionalteknologi Informasi Dan Komputer*, 2019, Pp. 260–269.

[8] Jamaludin, "Teknik Keamanan Jaringan Wireless Lan Pada Warnet Salsabila Computer Net," *Jamaludin*, Vol. 1, No. 1, Pp. 67–74, 2016.

[9] M. Waliullah, A. B. M. Moniruzzaman, And M. S. Rahman, "An Experimental Study Analysis Of Security Attacks At Ieee 802.11 Wireless Local Area Network," *Int. J. Futur. Gener. Commun. Netw.*, Vol. 8, No. 1, Pp. 9–18, 2015.

[10] H. D. Sabdho And M. Ulfa, "Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor Pt . Mora Telematika Indonesia Regional Palembang," In *Seminar Hasil Penelitian Vokasi (Semhavok) Universitas Bina Palembang*, 2018, Pp. 15–24.

[11] F. Zuli And A. Priambodo, "Analisis Keamanan Jaringan Nirkabel Publik Dengan Radius (Studi Kasus Univeristas Satya Negara Indonesia – Fakultas Teknik," *J. Ilm. Fak. Tek. Limit's*, Vol. 13, No. 1, Pp. 8–18, 2017.

[12] R. D. Sari, Supiyandi, A. P. U. Siahaan, And M. Muttaqin, "A Review Of Ip And Mac Address Filtering In Wireless Network Security," *Ijsrst*, Vol. 3, No. 6, Pp. 470–473, 2017.

[13] D. M. Sari, M. Yamin, And L. M. B. Aksara, "Analisis Sistem Keamanan Jaringan Wireless (Wep, Wpapsk/Wpa2psk) Mac Address, Menggunakan Metode Penetration Testing," *Semantik*, Vol. 3, No. 2, Pp. 203–208, 2017.

[14] A. Supriyanto, "Analisis Kelemahan Keamanan Pada Jaringan Wireless," *J. Teknol. Inf. Din. Vol.*, Vol. Xi, No. 1, Pp. 38–46, 2006.

[15] R. A. Purnama, "Optimalisasi Keamanan Jaringan Wireless Menggunakan Firewall Filtering Mac Address," *Ijns.Org Indones. J. Netw. Secur.*, Vol. 8, No. 4, Pp. 43–47, 2019.

[16] Syaiful And C. Novia, "Perancangan Jaringan Internet Dengan Hotspot Mikrotik Dan Mac Address Filtering," *Cyber-Techn*, Vol. 12, No. 02, Pp. 13–24, 2018.

https://doi.org/10.47111/JTI