

Optimization Network Security Using Radius Server And ACL at Mandiri Global Vocational School

Susafa'ati¹, Mugi Raharjo², Ibnu Ansori³

Program Studi Informatika, Universitas Nusa Mandiri^{1,2,3}

susafa.suf@nusamandiri.ac.id, mugi.mou@nusamandiri.ac.id, 12170431@nusamandiri.ac.id

Abstract

Most educational units at this time that have utilized the internet network to support the learning system. However, there are still some obstacles that are often encountered in its implementation. Security or user authentication is needed in order to avoid unwanted things from other users who do not have the authority to enter the local network so that the internet network in schools gets good security. Several cases have occurred, such as the entry of unknown connections to network systems, breaches of school data that should be confidential in nature. Radius Server and Access List are authentication methods that can be used to secure local networks. By applying the RADIUS Server and Access List methods to the network router at SMK Global Mandiri Kota Tangerang, clients who want to connect to the network must first authenticate using usernames and passwords or can also match the MAC address of the device used, then match it with the data existing in the database. Before carrying out the design, the authors also carry out an analysis by scanning the entire network for security threats. RADIUS Server and Access List will be useful to determine whether the user is allowed to use services in the network or not. Based on this, it proves that the RADIUS Server and Access List security methods installed on the network router can block access by authenticating users who do not have authority or are not registered in the router database, so that the internet network becomes safer from security threats from outside the network. that are not recognized and the internet network and data at SMK Global Mandiri can be safe and run well.

Keywords: Network Security, RADIUS, Access List

Abstrak

Seperti kebanyakan satuan pendidikan pada masa ini yang sudah memanfaatkan jaringan internet untuk menunjang sistem pembelajaran. Namun masih ada beberapa kendala yang sering ditemui dalam pelaksanaannya. Keamanan atau autentikasi pengguna diperlukan agar menghindari hal-hal yang tidak diinginkan dari pengguna lain yang tidak memiliki wewenang untuk masuk kedalam jaringan lokal, sehingga jaringan internet di sekolah mendapatkan keamanan yang baik. Beberapa kasus yang telah terjadi seperti masuknya koneksi tidak dikenal ke sistem jaringan, terjadinya pembobolan data-data sekolah yang seharusnya sifatnya adalah rahasia. Radius Server dan Access List merupakan salah satu metode autentikasi yang dapat digunakan dalam mengamankan jaringan lokal. Dengan menerapkan metode RADIUS Server dan Access List pada router jaringan di SMK Global Mandiri Kota Tangerang, *client* yang ingin terhubung ke jaringan harus melakukan proses autentikasi terlebih dahulu menggunakan *username* dan *password* ataupun bisa juga dengan mencocokkan *MAC Address* dari perangkat yang digunakan, kemudian dicocokkan dengan data yang ada dalam *database*. Sebelum melakukan perancangan penulis juga melakukan analisis dengan melakukan *scanning* terhadap keseluruhan jaringan terhadap ancaman keamanan. RADIUS Server dan Access List akan berguna untuk menentukan apakah pengguna tersebut diizinkan menggunakan layanan dalam jaringan atau tidak. Berdasarkan hal tersebut membuktikan bahwa metode keamanan RADIUS Server dan Access List yang dipasang pada router jaringan dapat menghalangi akses dengan cara melakukan autentifikasi bagi pengguna yang tidak memiliki wewenang atau tidak terdaftar pada *database router*, sehingga jaringan internet menjadi lebih aman dari adanya ancaman keamanan dari luar jaringan yang tidak dikenali dan jaringan internet beserta data yang berada di SMK Global Mandiri dapat aman dan berjalan dengan baik.

Kata kunci: Keamanan Jaringan, RADIUS, Access List

I. PENDAHULUAN

Jaringan internet pada masa ini sangat berkembang dengan pesat. Oleh karena itu jaringan internet sudah menjadi sesuatu yang tidak bisa dipisahkan dari kehidupan sehari-hari, namun tidak jarang kita menemui permasalahan-permasalahan ketika kita mengakses jaringan internet. Salah satu faktor

yang perlu diperhatikan dalam sebuah jaringan internet ataupun *hotspot* yang digunakan oleh banyak pengguna adalah manajemen user/pengguna. Jaringan menjadi tulang punggung bagi setiap organisasi. Karena jaringan menyediakan berbagai fasilitas kepada pengguna. Penting untuk menjaga jaringan lebih aman dari luar, karena banyak perangkat heterogen seperti *desktop*, *laptop*, *tablet pc* dan

smartphone terhubung di jaringan.[1] Memberikan Manajemen pengguna pada sebuah layanan hotspot sangat diperlukan untuk dapat menjalankan layanan secara optimal, namun manajemen tersebut harus juga didukung oleh kebijakan/aturan dari penyedia layanan sebagai dasar dalam pengaturan layanan [2]. Berdasarkan penelitian [3] dengan adanya sistem keamanan *wireless security* berbasis *radius server*, para pengguna tidak sembarangan mengakses jaringan *wi-fi* karena pengguna harus memiliki *username* dan *password* yang telah terdaftar pada *database radius server* pada saat *authentication login* di jaringan.

Hal tersebut pun sesuai dengan penelitian yang dilakukan oleh [4] Beberapa kendala yang ditemui seperti akses internet yang lambat akibat banyak nya pengguna yang menggunakan jaringan internet sekolah secara bersamaan tanpa adanya kontrol atau manajemen pada sisi router. Berdasarkan permasalahan diatas, penulis melihat adanya kesamaan kondisi permasalahan di lokasi penelitian, sehingga penulis memberikan usulan untuk menerapkan manajemen jaringan menggunakan metode *Radius Server* dan *Access List* untuk mengatasi permasalahan yang ada. Penelitian yang dilakukan oleh Agus Didi Purwanto dan Mohammad Badrul di PT. Usaha *Entertainment* Indonesia, dapat disimpulkan bahwa dengan menambahkan metode *Access List* pada keamanan jaringan PT. *Firewall* adalah sistem keamanan pada jaringan komputer yang bertugas untuk melindungi komputer dari serangan virus, malware, dan jenis serangan lainnya yang dapat berpotensi membahayakan.[5] konfigurasi *firewall* dapat meningkatkan keamanan dan konektifitas jaringan[6] , Usaha *Entertainment*, lalu lintas atau *traffic* jaringan menjadi lebih efisien. Dan dengan metode tersebut akan meningkatkan kemampuan pada sisi keamanan jaringan serta dapat menghindari adanya akses data yang tidak diperlukan didalam jaringan. [7] *Access Control List* adalah salah satu tipe teknologi pengawasan paket yang paling umum dan paling lama. Dia memulai dengan memeriksa isi paket dan mengaplikasikan aturan untuk menentukan apakah paket itu ditolak atau diizinkan.[8]

II. METODE PENELITIAN

Berikut ini adalah metode pengumpulan data yang dilakukan oleh penulis:

a. Wawancara

Dalam penyusunan penelitian ini untuk mendapatkan informasi secara lengkap terkait permasalahan jaringan yang ada, maka penulis melakukan metode tanya jawab dengan staf terkait yang bertugas mengatur jaringan internet serta warga sekolah yang lain untuk mengetahui permasalahan yang ada pada jaringan internet di SMK Global Mandiri Kota Tangerang.

b. Observasi

Penulis melakukan pengamatan langsung terhadap topologi jaringan yang digunakan pada SMK Global Mandiri Kota Tangerang. Metode ini dilakukan karena diperlukannya keakuratan dan kebenaran dalam pengumpulan data sebagai bahan pembahasan dalam penyusunan penelitian ini.

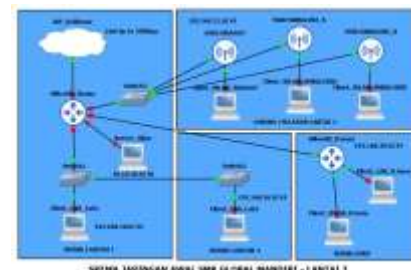
c. Studi Pustaka

Metode ini juga penulis gunakan untuk melengkapi penyusunan penelitian serta memperkuat landasan teori mengenai manajemen jaringan. Penulis mencari data dengan mempelajari penelitian terdahulu terkait permasalahan yang ada pada latar belakang, serta melalui literatur-literatur atau referensi-referensi yang ada dipergustakaan .

Berikut ini merupakan gambaran atau skema jaringan internet yang digunakan di SMK Global Mandiri Kota Tangerang :



Gambar 1. Skema Jaringan Lantai 1 SMK Global Mandiri



Gambar 2. Skema Jaringan Lantai 2 SMK Global Mandiri

Berdasarkan penelitan yang dilakukan Herman Kuswanto, dengan menerapkan sistem autentikasi *hotspot* menggunakan *Radius Server* pada jaringan *wireless*, terbukti dapat meningkatkan keamanan pada jaringan, setiap *user* yang akan terkoneksi ke jaringan *wireless* harus terdaftar terlebih dahulu di *Database Radius*, penggunaannyapun dapat dibatasi seperti pembatasan akses berdasarkan waktu dan pembatasan jumlah *user* dalam satu *user login*, hal ini dapat lebih menyulitkan *user* yang tidak mempunyai hak akses. Penerapan sistem autentikasi *hotspot* juga sangat membantu bagi admin jaringan untuk mengelola dan memonitoring semua *user* yang terkoneksi ke jaringan *hotspot* [9].

Penelitian yang dilakukan Arief Agung Gumelar menyimpulkan bahwa dengan menerapkan *Radius Server* pada jaringan *hotspot* dapat memudahkan manajemen *bandwidth* maupun manajemen *user* pada jaringan

hostpot tersebut, serta dapat memudahkan administrator jaringan untuk melakukan segmentasi jaringan antar divisi pada lingkup area jaringan *hotspot* tersebut [10].

III. HASIL PENELITIAN

Setelah penulis melakukan riset lapangan dan menganalisa sistem jaringan internet yang berjalan di SMK Global Mandiri Kota Tangerang, penulis memulai dengan melakukan wawancara terhadap pihak yang berwenang dalam IT di sekolah, hanya saja ada beberapa sektor yang menurut penulis masih belum efektif salah satunya pada sisi keamanan jaringan dan manajemen jaringan. Penulis mencoba melakukan penelusuran dengan *vulnerability assessment* dengan melakukan *Network Scanning* Melakukan scanning terhadap keseluruhan network dengan menggunakan aplikasi monitoring. Melihat *Log Activity service port* yang digunakan disemua jaringan. mengusulkan beberapa usulan untuk meningkatkan kualitas jaringan internet khususnya pada bagian keamanan jaringan yang sudah ada. Penulis mengajukan usulan untuk menambahkan konfigurasi *RADIUS Server* dan *Access List* pada router utama lantai 1 dan lantai 2 SMK Global Mandiri Kota Tangerang agar memberikan keamanan yang lebih efektif. Penulis juga mengusulkan untuk menambahkan konfigurasi manajemen bandwidth serta manajemen *hotspot user* agar meningkatkan kualitas jaringan SMK Global Mandiri Kota Tangerang menjadi lebih baik dan efektif.

1. Topologi Jaringan



Gambar 3. Topologi Jaringan SMK Global Mandiri

Pada rancangan topologi jaringan yang digunakan oleh SMK Global Mandiri Kota Tangerang, penulis tidak memiliki usulan atau tidak akan merubah bentuk topologi yang sudah ada. Hal ini dikarenakan topologi jaringan yang sudah diterapkan di SMK Global Mandiri Kota Tangerang sudah tergolong cukup baik, dengan menggunakan topologi extended star sehingga dapat mencakup beberapa area dan dapat memenuhi kebutuhan akses di SMK Global Mandiri Kota Tangerang. Hanya saja yang perlu diperhatikan

adalah memperbaiki peletakan perangkat jaringan agar lebih aman dan kinerjanya menjadi efektif.

2. Keamanan Jaringan

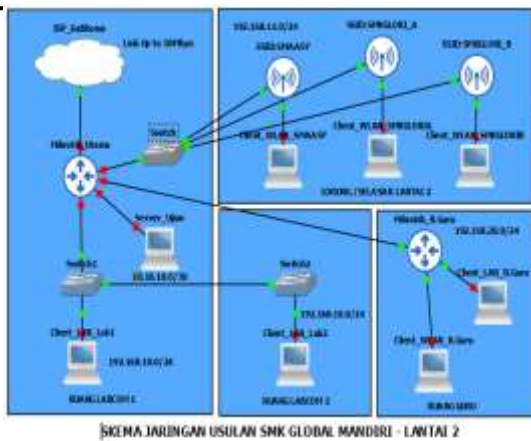
Keamanan jaringan yang diterapkan pada jaringan internet di SMK Global Mandiri sudah cukup baik, yaitu menggunakan protokol keamanan *WPA/WPA2 PSK* untuk mengamankan jaringan pada sisi jaringan nirkabel, sedangkan untuk keamanan pada sisi jaringan kabel hanya mengandalkan fitur *firewall* dan *program antivirus* dikomputer pengguna masing-masing. Namun protokol *WPA/WPA2 PSK* memiliki 1 kelemahan yaitu ketika ada *client* yang melakukan koneksi ke *access point* dan akhirnya terjadi proses *handshake*, maka *client* tersebut bisa melakukan *brute force* yang akan mencoba satu persatu *password* yang ada dengan didapatkan dari proses *handshake*.

Berdasarkan hal tersebut keamanan jaringan yang dapat penulis usulkan yaitu dengan menambahkan konfigurasi *RADIUS Server* dan *Access List* pada router mikrotik di lantai 1 dan 2 SMK Global Mandiri Kota Tangerang. Dengan menggunakan metode *RADIUS Server*, *client* yang ingin terhubung ke jaringan harus melakukan proses autentikasi terlebih dahulu menggunakan *user* dan *password*, kemudian dicocokkan dengan data yang ada dalam *database RADIUS Server* apakah *user* tersebut diizinkan menggunakan layanan dalam jaringan atau tidak. Dan dengan metode *Access List*, router mikrotik dapat melakukan *filtering/pembatasan* terhadap koneksi dari perangkat *client* berdasarkan *MAC Address* maupun *signal strength range*.

Berikut ini adalah skema jaringan usulan yang digunakan pada jaringan internet di SMK Global Mandiri Kota Tangerang:



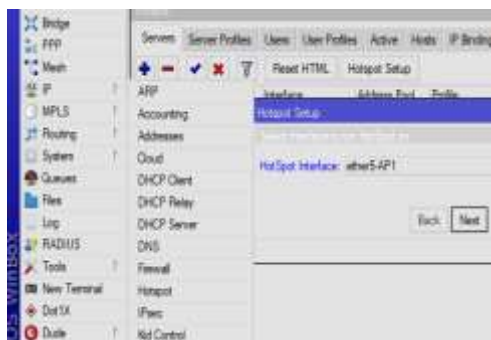
Gambar 4. Skema Jaringan Lantai 1



Gambar 5. Skema Jaringan Lantai 2

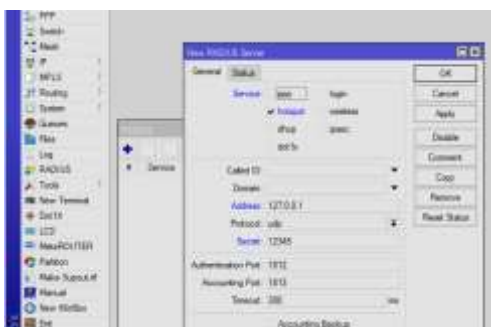
3. Rancangan Aplikasi

Pada tahap rancangan aplikasi ini, penulis melakukan konfigurasi pada *router* utama untuk mengimplementasikan metode keamanan jaringan menggunakan *RADIUS Server* dan *Access List*. Tahapan konfigurasinya adalah sebagai berikut:



Gambar 6. Konfigurasi Hotspot

Selanjutnya pada tahapan pembuatan *user* admin, silahkan isi *user* dan *password* yang diinginkan.

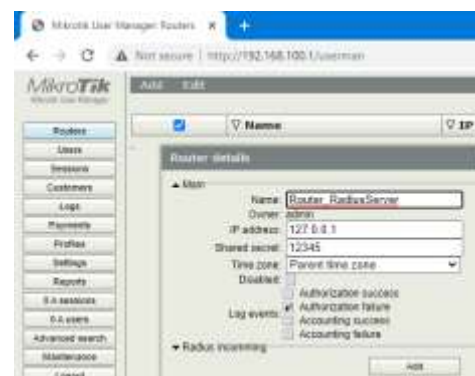


Gambar 7. Konfigurasi Radius Server 1

Tahap awal untuk mengaktifkan fitur *Radius Server*, pilih menu *Radius* -> klik "+" -> lalu pilih *Service Radius* yang diinginkan, setelah itu masukan IP Address router mikrotik yang dijadikan sebagai *Radius Server* dan juga masukan *secret* nya. Jika sudah selesai klik *Apply & Ok*. Melakukan konfigurasi pada sisi *Userman*



Gambar 8. Konfigurasi Radius Server 2



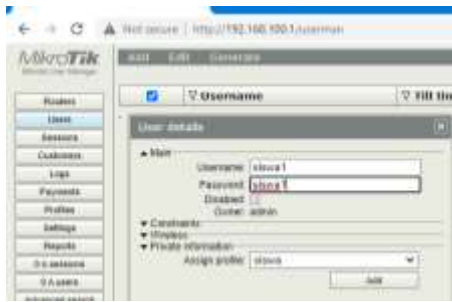
Gambar 9. Konfigurasi Radius Server 3

Setelah itu tambahkan *device* router yang dijadikan sebagai *Radius Server* kedalam *Userman* dengan cara sebagai berikut, pilih menu *Routers* -> lalu klik tombol *Add* -> selanjutnya mengisikan informasi untuk menambahkan Router yang dijadikan sebagai *Radius Server* -> jika sudah, klik tombol *Add* untuk menambahkan pengaturan tersebut..



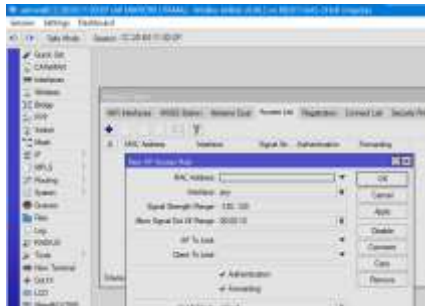
Gambar 10. Konfigurasi Radius Server 4

Langkah selanjutnya adalah menambahkan *profile* yang akan digunakan untuk pembuatan akun *login user* dengan cara sebagai berikut, pilih menu *Profiles* -> kemudian isikan pengaturan *Profile* yang ingin ditambahkan -> jika sudah klik tombol *Save Profile*.



Gambar 11. Konfigurasi Radius Server 5

Setelah membuat *profile*, langkah selanjutnya yaitu membuat akun *user* untuk login ke dalam jaringan. Langkah-langkahnya sebagai berikut, pertama klik menu *Users* -> lalu klik tombol *Add* -> selanjutnya isi kan *username* dan *password* yang diinginkan -> lalu pilih *profile* yang ingin digunakan untuk akun *user* tersebut -> jika sudah, klik tombol *Add* untuk menyimpan dan menambahkan pengaturan akun *user* tersebut. Melakukan konfigurasi *Access List*.

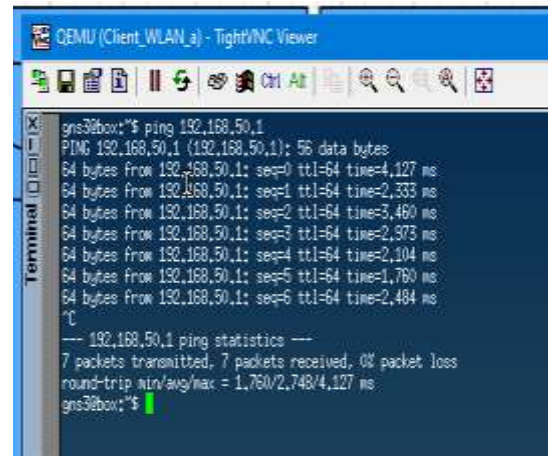


Gambar 12. Access List

Tahap awal dalam konfigurasi *Access List* yaitu pilih menu *Wireless* -> Pada *Wireless Tables* pilih tab *Access List*. Pada tampilan *Access Rule* diatas, kita dapat mendaftarkan perangkat yang ingin dimasukkan ke dalam *Access List* melalui kolom *MAC Address*. Kita juga bisa mengatur agar perangkat yang memiliki sinyal yang bagus saja yang dapat terhubung ke jaringan melalui kolom *Signal Strength Range*. Kita juga bisa membatasi akses kepada perangkat yang didaftarkan tersebut apakah dapat berkomunikasi dengan *client* lain yang ada di jaringan atau tidak menggunakan fitur *Forwarding*.

IV. PEMBAHASAN

Pada pengujian jaringan awal, penulis melakukan uji coba pada *client* yang terhubung melalui *access point* di lantai 1 dengan SSID WIFI_ASYGLORI.

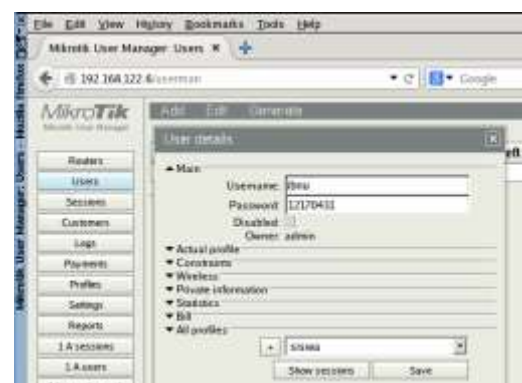


Gambar 13. Tes Ping dari Client Wlan ke Router

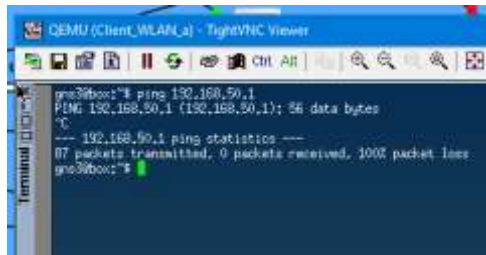
Hasil pengujian sebelum ditambahkannya konfigurasi *Radius Server* dan *Access List* dapat disimpulkan bahwa *client* yang sudah terhubung melalui *access point* yang ada, dapat langsung terhubung ke jaringan lokal dan dapat langsung mengakses internet. Hal ini memang wajar dikarenakan jaringan tersebut belum menambahkan metode autentikasi yang dapat mencegah *client* dapat langsung masuk kedalam jaringan. Hal ini pun berlaku pada segmen *network* yang lain yang ada pada *router* mikrotik tersebut.

1. Pengujian Jaringan Akhir

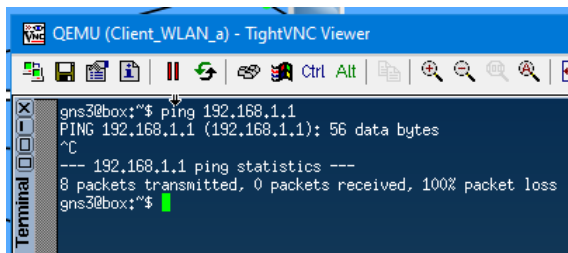
Pada tahap pengujian jaringan akhir ini, penulis melakukan pengujian dengan cara yang sama seperti sebelumnya yaitu dengan melakukan tes *ping* dan akses internet *client* yang terhubung melalui *access point* yang sama, namun kali ini *router* mikrotik sudah ditambahkan konfigurasi *RADIUS Server* dan *Access List* serta pada *database* sudah dibuatkan 1 akun pengguna dengan *username*=ibnu dan *password*=12170431.



Gambar 14. Database userman (RADIUS Server)



Gambar 15. Tes Ping dari Client Wlan ke Router (sebelum login)



Gambar 16. Tes Ping dari Client Wlan ke Router (sebelum login)

Pada gambar diatas, penulis melakukan uji konektifitas sebelum melakukan login ke jaringan menggunakan perintah *Ping* dari *client* menuju internet dengan *gateway* 192.168.1.1, dari 8 paket yang dikirim seluruhnya gagal atau *loss*.



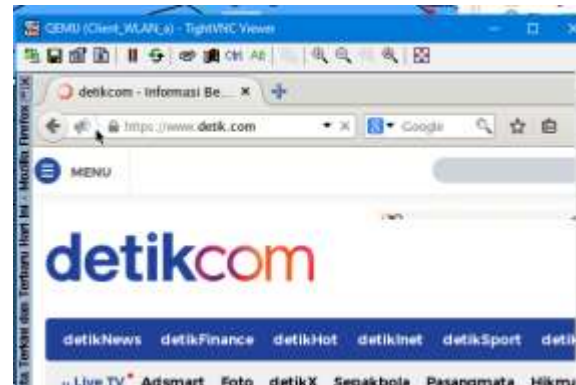
Gambar 17. Akses detik.com terblokir

Pada gambar diatas, penulis melakukan uji coba *client* yang sudah terhubung ke jaringan untuk mengakses website detik.com melalui browser. Berdasarkan uji coba diatas, website detik.com dialihkan ke halaman *login* mikrotik karena *client* belum melakukan *login* menggunakan akun yang sudah dibuat di *database Radius Server*.



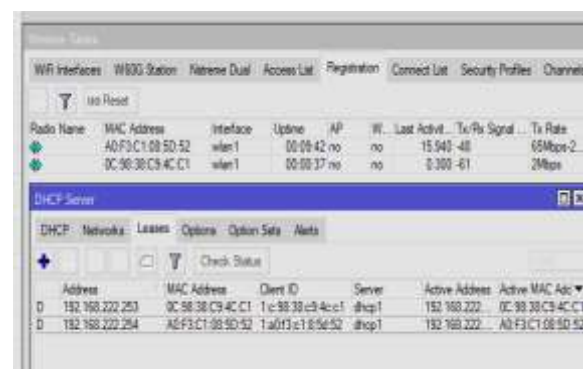
Gambar 18. Status Login Hotspot

Pada gambar diatas, *client* sudah melakukan *login* menggunakan akun yang sudah terbuat di *database Radius Server*.

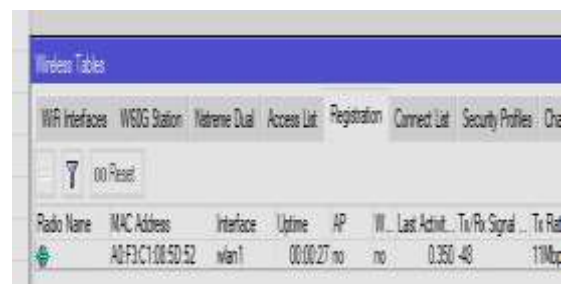


Gambar 19. Akses detik.com terhubung

Pada gambar diatas, *client* sudah melakukan *login* menggunakan akun yang sudah terbuat di *database Radius Server* dan berhasil mengakses website detik.com.



Gambar 20. Daftar client wireless sebelum ACL



Gambar 21. Access Rule

Pada gambar diatas, sebelum ditambahkan rule pada *Access List* di router *client* dapat langsung terhubung ke jaringan secara langsung setelah melakukan autentikasi. Lalu setelah ditambahkan *rule* pada *Access List*, hanya perangkat dengan kekuatan sinyal antara -50 sampai 120 saja yang bisa terkoneksi, maka hasil yang didapatkan yaitu hanya 1 perangkat yang berhasil

terhubung karena kekuatan sinyal perangkat tersebut sesuai dengan *rule* yang ada pada *Access List*.

Dari hasil pengujian diatas dapat disimpulkan bahwa konfigurasi yang diterapkan berjalan sesuai dengan yang diharapkan. Pengguna yang ingin terhubung kedalam jaringan diharuskan melakukan proses autentikasi terlebih dahulu menggunakan akun yang sudah terdaftar di database *Radius Server*, setelah itu router baru akan mengizinkan pengguna tersebut terhubung kedalam jaringan. Lalu perangkat jaringan yang tidak sesuai ataupun tidak terdaftar pada *rule* yang ada di *Access List* juga tidak dapat terhubung.

V. KESIMPULAN

Setelah mempelajari dan menganalisa sistem jaringan yang sudah ada, maka penulis dapat menyimpulkan bahwa jaringan internet yang sudah diterapkan di SMK Global Mandiri Kota Tangerang adalah sebagai berikut. SMK Global Mandiri Kota Tangerang menggunakan metode kabel dan nirkabel/*wireless* dalam mendistribusikan data/jaringan internet pada lantai 1 dan 2 yang didukung dengan perangkat jaringan yang tergolong cukup baik dan mumpuni, melihat kondisi saat ini yang mengharuskan sekolah memiliki sistem jaringan komputer ataupun internet yang dapat menunjang proses belajar mengajar. Keamanan jaringan yang digunakan oleh SMK Global Mandiri Kota Tangerang khususnya pada jaringan *wireless* masih menggunakan protokol keamanan *WPA/WPA2 PSK*, walaupun sudah tergolong baik namun protokol keamanan ini masih memiliki kelemahan yang dapat dimanfaatkan oleh pengguna/*user* lain yang tidak memiliki hak akses untuk memaksa masuk kedalam jaringan. Oleh karena itu penulis mengusulkan untuk menggunakan metode *Radius Server* dan *Access List* untuk melakukan pengamanan lebih terhadap jaringan internet di SMK Global Mandiri Kota Tangerang yang dimana sebagian besar pendistribusian data dilakukan melalui metode *wireless*. Dengan metode usulan ini sistem jaringan yang ada pada SMK Global dapat diamankan dari ancaman luar jaringan yang mencoba masuk ke dalam jaringan SMK Global Mandiri, dan keamanan data siswa pada SMK Global Mandiri menjadi lebih secure dari ancaman pembobolan data.

VI. REFERENSI

- [1] T. Rahman and R. M. Adha, "Keamanan Jaringan dengan Metode Access List Demilitarized Zone (DMZ) pada Cisco RV042," *INOVTEK Polbeng - Seri Inform.*, vol. 6, no. 2, p. 295, 2021.
- [2] S. Suryanto and F. A. Permadi, "Optimalisasi Jaringan Internet Hotspot Menggunakan User Manajemen Pada Pusat Pengembangan SDM Asuransi Indonesia," *J. Infotech*, vol. 1, no. 2, pp. 59–67, 2020.
- [3] R. N. Puspasari, L., & Dasmen, "Perancangan Dan Implementasi Radius Server Sebagai Wireless Security Di Rsup Dr. Mohammad Hoesin Palembang," *Pros. Semhavok*, vol. 2(1), pp. 153–159, 2020.
- [4] Z. Miftah, "Desain Keamanan Internet Hotspot Dengan Radius Server dan Manajemen Bandwidth Design of Internet Hotspot Security with Server Radius and Bandwidth Management," vol. 29, no. 1, 2019.
- [5] A. E. W. Wuryantai, "Digitalisasi Masyarakat: Menilik Kekuatan dan Kelemahan Dinamika Era Informasi Digital dan Masyarakat Informasi," *J. ILMU Komun.*, vol. 1, no. 2, pp. 131–142, 2013.
- [6] D. Kurnia, "Analisis Kinerja Optimasi Bandwidth Menggunakan Proxy Eksternal Squid Lusca Ubuntu Pada Jaringan Router Mikrotik," vol. 9, no. 3, pp. 43–50, 1978.
- [7] M. B. Agus Didi Purwanto, "Implementasi Access List Sebagai Filter Traffic Jaringan (Study Kasus Pt. Usaha Entertainment Indonesia)," *J. Tek. Komput. AMIK BSI*, vol. II, no. 1, pp. 78–88, 2016.
- [8] 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.
- [9] H. Kuswanto, "Sistem Autentikasi Hotspot Menggunakan Radius Server Mikrotik Router," *Informatics Educ. Prof.*, vol. 2, no. 1, pp. 43–50, 2017.
- [10] A. A. Gumelar, "Perancangan Jaringan Hotspot Berbasis Radius Server Untuk Manajemen Penggunaan Internet Di SMK Negeri 3 Pekalongan," *Semin. Nas. Teknol. Inf. dan Multimed.*, pp. 43–48, 2017.

