JUPITER
Teknologi Informatika & Komputer
Vol. 5 No. 2 Agustus 2024
Institut Bisnis Muhammadiyah Bekasi
P-ISSN: 2798-3129 , E-ISSN: 2798-6187

OPTIMASI OTENTIKASI JARINGAN *WIRELESS* MENGGUNAKAN STANDAR PROTOKOL 802.1X DAN *PEAP*

Gunawan Wibisono[1], Bayu Anggoro Krisnamurti[2], Dany Candra Febrianto[1], Moniq Kartika Sari[2]

[1]Teknik Informatika, Institut Teknologi Telkom Purwokerto, gunawan@ittelkom-pwt.ac.id, danycandra@ittelkom-pwt.ac.id
[2]Sistem Informasi, Institut Teknologi Telkom Purwokerto, bayu.anggoro@ittelkom-pwt.ac.id, moniq@ittelkom-pwt.ac.id

ABSTRAK

Internet saat ini merupakan kebutuhan pokok dalam mengolah dan mengelola informasi, salah satu cara untuk terkoneksi dengan internet adalah menggunakan frekuensi dan transmisi radio sebagai media penghantarnya atau disebut juga dengan *WiFi*. *WiFi* memiliki banyak kelebihan dan keunggulan seperti ringkas dalam penggunaan dan kemudahan dalam perawatan, namun *WiFi* memiliki permasalahan yaitu data digital yang ditransfer melalui jaringan *wireless* (*WiFi*) mudah untuk dicuri atau diendus. Dibutuhkan standar protokol yang dapat menjamin keamanan koneksi *wireless* tersebut, standar protokol 802.1x dan *PEAP* dapat menjadi salah satu solusi terhadap permasalahan tersebut. Dalam implementasi standar protokol 802.1x dibutuhkan topologi yang melibatkan *server* radius sebagai tempat menyimpan akun pengguna, system otentikasi sebagai gerbang awal memvalidasi akun pengguna dan pengguna itu sendiri. Daloradius digunakan sebagai tool untuk memanajemen akun pengguna. Penelitian ini berhasil melakukan optimasi otentikasi pada jaringan *wireless* menggunakan standar protokol 802.1x dan *PEAP*.
Kata Kunci: daloradius, *PEAP*, protokol 802.1x, radius, *WiFi*

ABSTRACT

The internet is currently a basic need in processing and managing information, one way to connect to the internet is to use radio frequency and transmission as a delivery media or also called WiFi. WiFi has many advantages such as being concise in use and easy to maintain, but WiFi has a problem, namely digital data transferred via a wireless network (WiFi) is easy to steal or sniff. A protocol standard is needed that can guarantee the security of the wireless connection, the 802.1x protocol standard and PEAP can be one solution to this problem. In the implementation of the 802.1x protocol standard, a topology is needed that involves a radius server as a place to store user accounts, an authentication system as the initial gate to validate user accounts and the users themselves. Daloradius is used as a tool to manage user accounts. This study succeeded in optimizing authentication on wireless networks using the 802.1x and PEAP protocol standards.
Keywords: *daloradius, PEAP, protocol 802.1x, radius, WiFi*

PENDAHULUAN

Internet adalah fasilitas komunikasi yang dirancang untuk menghubungkan komputer-komputer sehingga dapat bertukar informasi digital (David D. Clark, 2018), internet menjadi kebutuhan pokok saat ini dalam mengolah dan mengelola informasi. Salah satu cara agar bisa terkoneksi internet adalah melalui jaringan WLAN (*Wireless Local Area Network*) atau *WiFi* (*Wireless Fidelity*) (Mahbub Hassan, 2022). Menurut

Lazarescu Teknologi *wireless* (*WiFi*) memiliki keunggulan yaitu mengurangi kerumitan dalam pengaturan kabel, dapat menghemat biaya dan kemudahan dalam perawatan (Bangsa & Setiyadi, 2021). *WiFi* juga memiliki kelebihan yaitu ringkas dalam penggunaannya terutama pada perangkat mobile seperti *smartphone*, tablet dan laptop.

Salah satu permasalahan yang ada pada koneksi *WiFi* sebagai jaringan publik adalah data digital yang ditransfer melalui jaringan *wireless* ini mudah untuk diendus oleh pihak yang tidak bertanggung jawab. Keamanan dalam jaringan *WiFi* menjadi aspek penting dalam pengelolaan internet, sistem otentikasi merupakan salah satu cara untuk memberikan keamanan terhadap koneksi internet. Sistem otentikasi pada jaringan *WiFi* yang dapat digunakan antara lain adalah sistem otentikasi standar protokol 802.11 dan standar protokol 802.1x, standar tersebut merupakan standar yang dikeluarkan oleh IEEE. Perbedaan standar protokol tersebut dijelaskan pada Tabel 1 berikut ini.

Tabel 1. Perbedaan 802.11 dan 802.1x

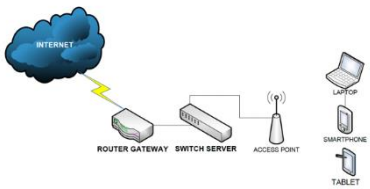
Atribut	802.11	802.1x
Standar	*Wireless* LAN	Network Access Control
Otentikasi	WPA, WPA2, WPA3	EAP, Radius
Enkripsi	WEP, TKIP, AES	EAP-TLS, *PEAP*, EAP-TTLS
Keamanan	Mac Filtering, SSID Hiding	Port Based, User Based
Otentikasi *Server*	-	Radius
Penggunaan	*Wireless* LAN	*Wireless* LAN dan Wired LAN

Standar protokol 802.1x saat ini memiliki tingkat keamanan paling baik dan paling canggih. protokol 802.1x menggunakan *server* otentikasi untuk memvalidasi koneksi klien untuk dapat terhubung ke internet. Validasi yang dimaksud adalah berupa nama pengguna (*username*) dan kata sandi (*password*) (Aznar Abdillah dkk., 2020). Penelitian ini bertujuan untuk meningkatkan sistem otentikasi koneksi *WiFi* pada jaringan publik dari standar protokol 802.11 menjadi standar protokol 802.1x, dengan penelitian ini diharapkan ada peningkatan keamanan terhadap lalu lintas data pada jaringan *WiFi* .

TINJAUAN PUSTAKA

Wireless LAN

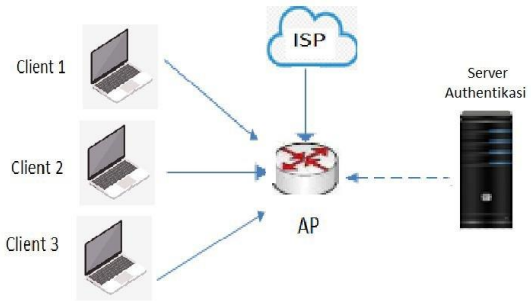
Wireless Local Area Network (*Wireless* LAN) merupakan teknologi LAN yang menggunakan frekuensi dan transmisi radio sebagai media penghantarnya pada area tertentu menggantikan fungsi kabel (H. Mukhtar, 2019). Pada jaringan *wireless* terdapat dua model yaitu Ad-Hoc dan infrastruktur, model Ad-Hoc merupakan model spontan atau langsung antar komputer secara *wireless* dan bersifat sementara, sedangkan model infrastruktur merupakan model yang membutuhkan *access point* sebagai penghubung antar perangkat komputer (Permadi dkk., 2020). Gambar 1 menjelaskan konfigurasi *WiFi* terdiri dari *access point* yang dihubungkan ke pengguna melalui media frekuensi dan transmisi radio.



Gambar 1. Konfigurasi *WiFi*

PEAP

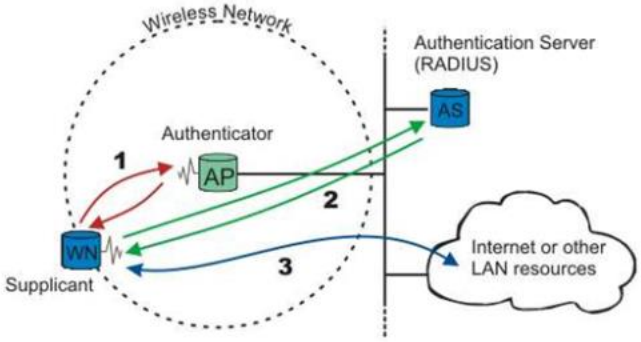
Protected Extensible Authentification Protocol (*PEAP*) merupakan salah satu metode *EAP* (*Extensible Authentification Protocol*), *PEAP* adalah protokol otentikasi yang menggunakan nama pengguna dan kata sandi. *PEAP* digunakan pada jaringan *wireless* ataupun jaringan kabel, *PEAP* menggunakan *server* otentikasi untuk memvalidasi pengguna yang akan terkoneksi ke jaringan internet yang kemudian diberikan akses terhadap internet. *PEAP* merupakan protokol otentikasi yang kompatibel dengan beberapa perangkat keras dari berbagai vendor (Hidayat & Riadi, 2021). Gambar 2 menjelaskan tentang topologi pada *PEAP*.



Gambar 2. Topologi *PEAP*

Protokol IEEE 802.1x

Institute of Electrical and Electronics Engineers (*IEEE*) merupakan organisasi yang memberikan standar protokol 802.1x, protokol yang dapat meningkatkan keamanan pada transmisi data. Kontrol akses jaringan berbasis port memungkinkan administrator jaringan untuk membatasi penggunaan titik akses (port) layanan LAN IEEE 802(R) untuk mengamankan komunikasi antara perangkat yang diautentikasi dan yang diotorisasi. Standar ini menetapkan arsitektur umum, elemen fungsional, dan protokol yang mendukung otentikasi timbal balik antara klien port yang terhubung ke LAN yang sama dan komunikasi yang aman antar port (IEEE, 2020). Gambar 3 menjelaskan tenang skema arsitektur protokol 802.1x.



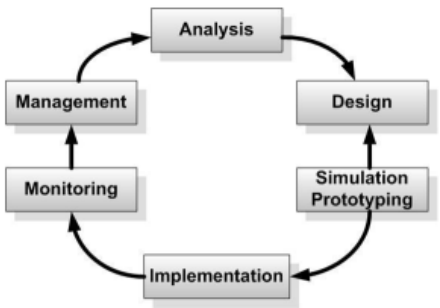
Gambar 3. Skema Arsitektur Protokol 802.1x

Radius

RADIUS (Remote Access Dial-in User Service) merupakan suatu protokol *client-server* yang dikembangkan untuk mekanisme akses kontrol yang memeriksa dan mengautentikasi pengguna berdasarkan protokol Autentikasi, Autorisasi, Akutansi atau dikenal dengan protokol AAA (Anhal dkk., 2020).

Network Development Life Cycle

Network Development Life Cycle (*NDLC*) adalah metode yang dapat digunakan untuk mengembangkan suatu jaringan komputer. Metode *NDLC* memiliki enam tahapan yang akan menjadi panduan dalam menerapkan *NDLC*. Adapun enam tahapan tersebut yaitu Analisa, Perancangan, Prototipe, Implementasi, *Monitoring* , dan Manajemen (Nurdadyansyah & Hasibuan, 2021).



Gambar 4. *NDLC*

METODE PENELITIAN

Metode penelitian yang digunakan pada penelitian ini yaitu *Network Development Live Cycle* (*NDLC*) meliputi beberapa tahap berikut ini

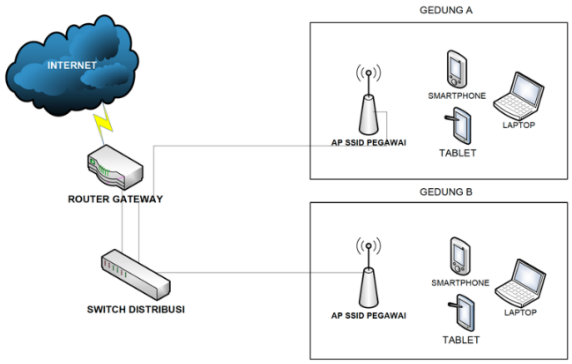
1. Analisa, pada tahap ini dilakukan analisa permasalahan yang muncul,dan analisa topologi jaringan yang digunakan.
2. Perancangan, perancangan yang dilakukan berupa membuat gambar jaringan interkoneksi yang telah dibangun dan design akses data.
3. Prototipe, pada tahap ini rancangan yang sudah dibuat disimulasikan menggunakan tool Cisco Packet Tracer untuk menguji apakah ada kekurangan dari rancangan jaringan yang dibuat.

4. Implementasi merupakan tahap pengimplementasian rancangan jaringan yang sudah dibuat dan diuji pada tahap prototipe.
5. *Monitoring* , pada tahap ini dilakukan *monitoring* koneksi klien atau pengguna pada router.
6. Manajemen, pada tahap ini dilakukan pengelolaan pengguna melalui aplikasi Freeradius.

HASIL DAN PEMBAHASAN

Analisa

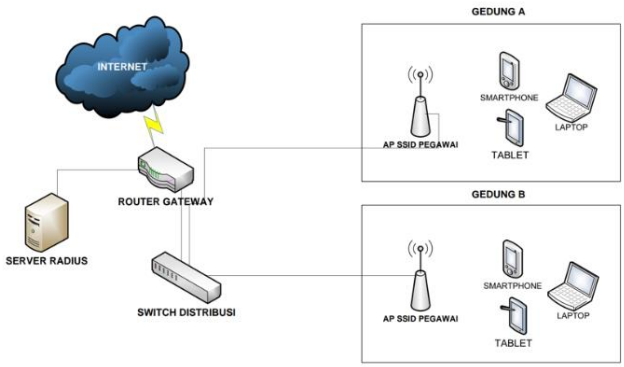
Topologi jaringan *wireless* yang ada dijelaskan pada Gambar 5 , SSID pegawai menggunakan protokol 802.11 sebagai sistem otentikasi agar dapat terhubung ke internet. SSID pegawai dapat digunakan pada perangkat mobile seperti laptop, *smartphone*, tablet, dll dengan memasukan *password* atau kata sandi dari *access point.*



Gambar 5. Topologi *Wireless*

Perancangan

Pada tahap perancangan dibuatlah topologi baru dengan menyertakan standar protokol 802.1x yaitu berupa adanya *server* radius sebagai *server* otentikasi. Untuk bisa menggunakan internet, pengguna setelah terhubung dengan *access point* harus memasukan nama pengguna (username) dan kata sandi (password). Gambar 6. menjelaskan rancangan topologi baru.

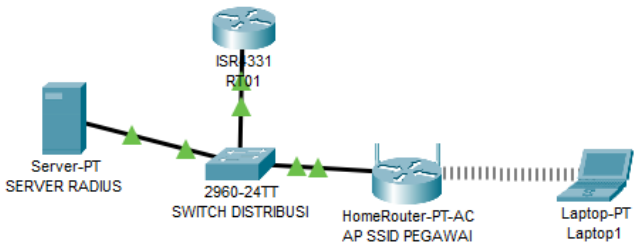


Gambar 6. Rancangan Topologi

Prototipe

Prototipe rancangan dibuat menggunakan tool cisco packet tracer, meliputi router, *server* radius dan perangkat mobile (laptop). Prototipe ini dibuat semirip mungkin dengan rancangan topologi baru untuk menguji apakah dengan rancangan topologi

tersebut penerapan standar protokol 802.1x bisa berjalan dengan baik. Gambar 7. menjelaskan hasil uji prototipe.



Gambar 7. Prototipe Rancangan jaringan

Implementasi

Pada tahap ini, penulis mempersiapkan *server* yang akan dipasang radius dan aplikasi freeradius sebagai aplikasi untuk manajemen penggunanya.

Instalasi *server* radius

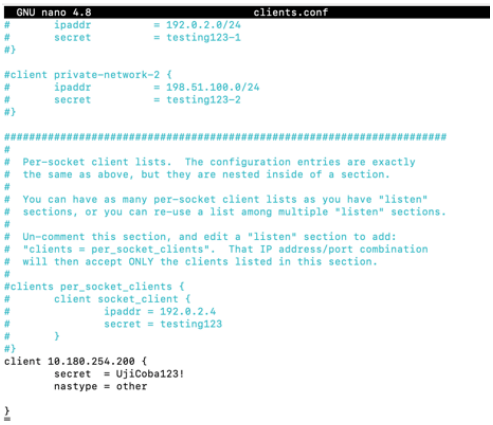
Aplikasi yang digunakan pada *server* radius adalah freeradius, aplikasi freeradius dapat diinstall pada *server* yang sudah memiliki sistem operasi. Penulis menggunakan sistem operasi ubuntu *server* versi 20 seperti pada Gambar 8. berikut ini.

```
root@radiusserver:~# cat /etc/os-release
NAME="Ubuntu"
VERSION="20.04.6 LTS (Focal Fossa)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 20.04.6 LTS"
VERSION_ID="20.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=focal
UBUNTU_CODENAME=focal
```

Gambar 8. Sistem Operasi

Freeradius yang penulis gunakan adalan versi 3.0, instalasi freeradius diawali dengan instalasi database menggunakan mariadb, kemudian membuat database yang akan digunakan oleh freeradius. Aspek penting yang perlu dilakukan adalah penentuan kata kunci atau *secret key* yang ada pada file clients.conf terletak pada /etc/freeradius/3.0/. *Secret key* yang digunakan oleh penulis dijelaskan pada Gambar 9, secret key digunakan untuk menghubungkan authenticator ke *server* radius.

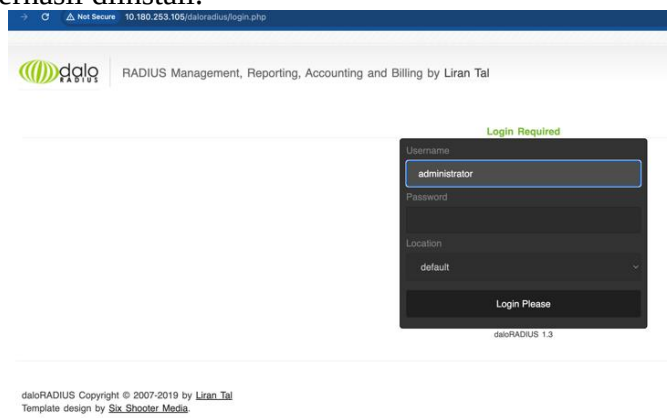
JUPITER
Teknologi Informatika & Komputer
Vol. 5 No. 2 Agustus 2024
Institut Bisnis Muhammadiyah Bekasi
P-ISSN: 2798-3129 , E-ISSN: 2798-6187



Gambar 9. Secret Key Freeradius

Instalasi Daloradius

Aplikasi selanjutnya yang diinstall oleh penulis adalah Daloradius, Daloradius akaan menjadi aplikasi yang digunakan untuk melakukan pengelolaan pengguna. Aspek penting yang perlu diperhatikan saat install daloradius adalah konfigurasi database yang perlu disesuaikan dengan konfigurasi database pada freeradius. Gambar 10 menjelaskan daloradius yang berhasil diinstall.



Gambar 10. Halaman Utama Daloradius

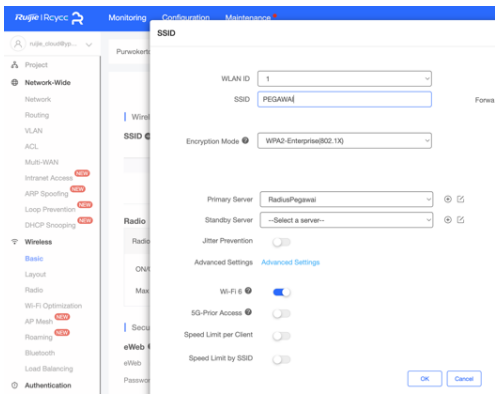
Konfigurasi pada *Access point*

Penulis menggunakan *access point* ruijie yang memiliki dashboard konfigurasi *cloud*, sehingga memudahkan proses konfigurasi. Gambar 11 menjelaskan konfigurasi penambahan *server* radius yang dilakukan pada dashboard cloud ruijie.

Gambar 11. Konfigurasi Penambahan *Server* Radius

JUPITER
Teknologi Informatika & Komputer
Vol. 5 No. 2 Agustus 2024
Institut Bisnis Muhammadiyah Bekasi
P-ISSN: 2798-3129 , E-ISSN: 2798-6187

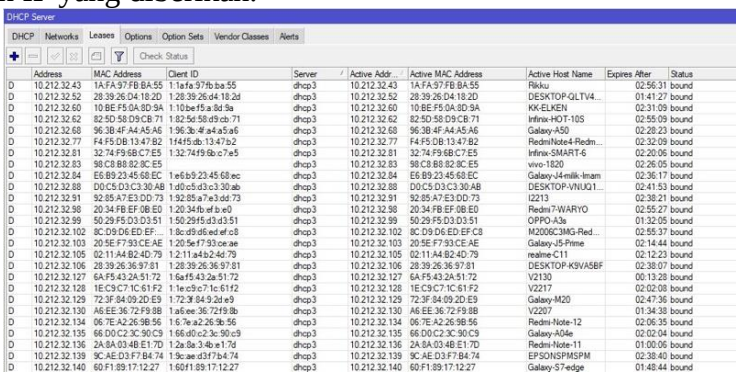
Gambar 12 menjelaskan tentang konfigurasi penambahan SSID Pegawai pada *access point*.



Gambar 12. Konfigurasi Penambahan SSID Pegawai

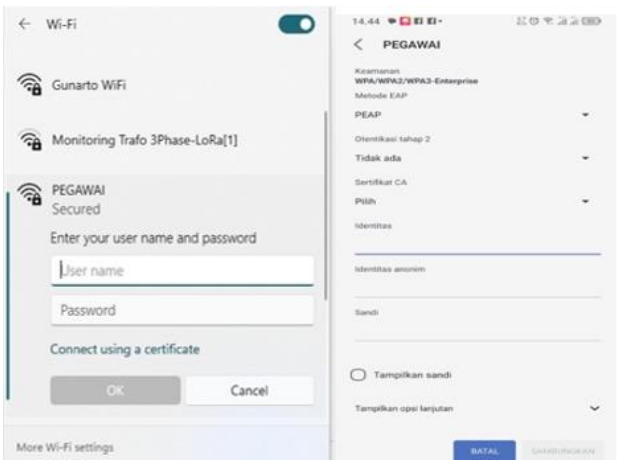
Monitoring

Monitoring dilakukan melalui router yang digunakan, penulis menggunakan mikrotik sebagai router. Penulis melakukan *monitoring* melalui IP DHCP yang diberikan oleh router. Gambar 13 menjelaskan detail klien atau pengguna yang terkoneksi yaitu mac address dan IP yang diberikan.



Gambar 13. *Monitoring* Koneksi

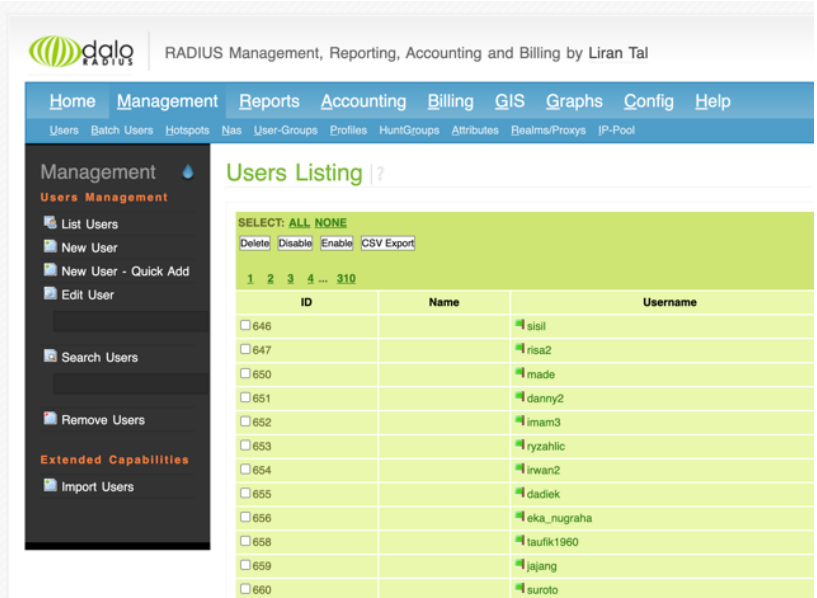
Penulis juga melakukan *monitoring* dari sisi pengguna berupa tampilan SSID di laptop atau *smartphone*, Gambar 14 menjelaskan tampilan SSID pada laptop dan smartphone.



Gambar 14. Tampilan SSID dan Login

Manajemen

Tahap manajemen, penulis menggunakan aplikasi daloradius untuk pengeloaan pengguna baik untuk menambahkan pengguna baru, ubah data atau hapus data pengguna. Fitur grouping pengguna juga tersedia pada aplikasi ini, grouping pengguna selain digunakan untuk mengkategorikan pengguna juga dapat mengatur besaran bandwidth yang diberikan kepada grup yang telah dibuat. Gambar 15 menjelaskan tentang aplikasi Daloradius.



Gambar 15. Manajemen pengguna pada aplikasi Daloradius

PENUTUP

Simpulan

Pengelola Internet wajib menyediakan koneksi internet yang handal namun juga harus memberikan koneksi yang aman dan mudah. Penggunaan koneksi internet sebelumnya yang mudah dilakukan perlu diteruskan namun harus ditingkatkan dari sisi keamanannya. Standar protokol koneksi *wireless* dioptimasi atau ditingkatkan untuk mencapai tujuan tersebut. Penggunaan standar protokol 802.1x memerlukan perubahan pada topologi serta membutuhkan perangkat *server* sebagai media untuk menyimpan akun pengguna. *Server* radius berhasil diimplementasikan dan dapat dihubungkan dengan konfigurasi *access point*, manajemen pengguna dijalankan melalui aplikasi daloradius. Implementasi standar protokol 802.1x pada jaringan *wireless* ini diharapkan dapat meningkatkan keamanan dalam transfer data selama menggunakan internet.

Saran

Pengujian keamanan terhadap penggunaan standar protokol 802.1x dapat dilakukan pada penelitian selanjutnya. Konfigurasi *lease time* pada router dapat diperpanjang sesuai kebijakan masing masing agar pengguna ketika hadir diarea yang tercover *WiFi* dapat langsung terkoneksi ke internet tanpa melakukan login atau otentikasi ulang.

REFERENSI

Anhal, S. D., Noh, J., & Hamid, M. (2020). Simulasi Protokol Authentikasi 802.1x Pada Jaringan Kabel di UMMU. *Jurnal Teknik Informatika (J-Tifa)*, *3*(2), 9–16. https://doi.org/10.52046/j-tifa.v3i2.1044

Aznar Abdillah, M., Yudhana, A., Fadil, A., & Dahlan Jl Soepomo, A. (2020). Sniffing Pada Jaringan *WiFi* Berbasis Protokol 802.1x Menggunakan Aplikasi Wireshark. *Jurnal Sains Komputer & Informatika (J-SAKTI*, *4*(1), 1–8. http://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Bangsa, B. P., & Setiyadi, D. (2021). Rancangan dan Implementasi Jaringan Komputer Antar Gedung Menggunakan Koneksi Nirkabel. *JUPITER : Journal of Computer & Information Technology*, *2*(2), 96–108. https://doi.org/10.53990/jupiter.v2i2.63

David D. Clark. (2018). *Designing an Internet*. The MIT Press.

H. Mukhtar. (2019). *Teknik Open Source*. Deepublish.

Hidayat, T. N., & Riadi, I. (2021). Optimation *Wireless* Security IEEE 802.1X using the Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-*PEAP*). *International Journal of Computer Applications*, *174*(11), 25–30. https://doi.org/10.5120/ijca2021920988

IEEE. (2020, Februari 28). *IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control*. IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control.

Mahbub Hassan. (2022). *Wireless and Mobile Networking*. CRC Press.

Nurdadyansyah, N., & Hasibuan, M. (2021). Perancangan Local Area Network Menggunakan *NDLC* Untuk Meningkatkan Layanan Sekolah. *Konferensi Nasional Ilmu Komputer*, 342–346.

Permadi, K. B., Seta, H. B., & Astriratma, R. (2020). Pengamanan Jaringan *Wireless* LAN Dengan Protokol EAP-TTLS Dan Otentikasi MSCHAPv2 Pada Fakultas Ilmu Komputer UPN Veteran Jakarta. *Informatik : Jurnal Ilmu Komputer*, *16*(2), 95. https://doi.org/10.52958/iftk.v16i2.1970