

P-34

RANCANG BANGUN SERVER AAA UNTUK MENGAkses SISTEM INFORMASI MANAJEMEN PNJ

DESIGN OF AAA SERVER FOR ACCESSING PNJ MANAGEMENT INFORMATION SYSTEM

Dandun Widhiantoro^{1*}, Maudy Rachma²

^{1,2}Politeknik Negeri Jakarta, Kampus UI Depok, Depok

*E-mail: dandun@elektro.pnj.ac.id

Diterima 09-10-2018	Diperbaiki 19-11-2018	Disetujui 05-12-2018
---------------------	-----------------------	----------------------

ABSTRAK

Server AAA (Authentication, Authorization, Accounting) merupakan salah satu metode untuk mengamankan jaringan WLAN agar hanya user tertentu saja yang dapat mengakses jaringan tersebut. Administrator jaringan mampu membatasi jumlah user, mengatur kapasitas bandwidth tiap user, membatasi akses user, serta melakukan pencatatan aktifitas user selama user terhubung ke jaringan WLAN. Pada penelitian kali ini dilakukan perancangan server AAA yang berisi data user untuk Dosen, Mahasiswa, dan Staff pada jaringan WLAN yang dirancang untuk mengakses SIMPNJ (Sistem Informasi Manajemen Politeknik Negeri Jakarta). Selain itu, pada server AAA juga ditambahkan fungsi web filtering yang berfungsi membatasi user untuk mengakses web lain. Server AAA menggunakan Mikrotik Router yang difungsikan juga sebagai router utama, router utama ini akan dihubungkan dengan Access Point dan ISP agar user dapat mengakses internet via jaringan WLAN. Analisis dilakukan dari data yang didapat saat pengujian sistem yang berupa fungsi Authentication, Authorization, dan Accounting server, performansi berupa bandwidth dan throughput, dan mekanisme backup database. Berdasarkan hasil pengujian server AAA mampu meningkatkan keamanan dengan adanya enkripsi password dengan MD5 saat user login dengan jaringan WLAN.

Kata kunci: *Captive Portal, Hotspot, Management User, RADIUS, Server AAA, WLAN*

ABSTRACT

AAA server (Authentication, Authorization, Accounting) is one method for securing a WLAN network so that only certain users can access the network. Network administrators are able to limit the number of users, adjust the bandwidth capacity of each user, limit user access, and record user activity as long as the user is connected to a WLAN network. In this thesis research carried out AAA server design which contains user data for Lecturers, Students, and Staff on WLAN networks designed to access SIMPNJ (Jakarta State Polytechnic Management Information System). In addition, the AAA server also adds a web filtering function which functions to limit the user to access other web. AAA server uses Mikrotik Router that is also used as the main router, this main router will be connected to the Access Point and ISP so that users can access the internet via the WLAN network. Analysis is carried out from the data obtained when testing the system in the form of Authentication, Authorization, and Accounting server functions, the performance in the form of bandwidth and throughput, and the mechanism of database backup. Based on the results of testing the AAA server is able to increase security by encrypting passwords with MD5 when the user logs in with a WLAN network.

Keywords: *Captive Portal, Hotspot, Management User, RADIUS, Server AAA, WLAN*

PENDAHULUAN

Politeknik Negeri Jakarta memiliki SIM (Sistem Informasi Manajemen) yang memerlukan *authentication* untuk mengaksesnya dan harus terhubung dalam jaringan lokal milik Politeknik Negeri Jakarta, sistem ini dapat diakses oleh mahasiswa, pegawai direktorat kampus, dan dosen melalui jaringan nirkabel WLAN atau dikenal juga dengan WiFi, yang memiliki standar IEEE 802.11 g dan n [1]. *Authentication* sendiri adalah suatu proses dimana *user* diidentifikasi oleh *server AAA* sebelum *user* menggunakan jaringan.[2][3]

Untuk permasalahan ini pihak kampus perlu memperhatikan dalam pemberian hak akses kepada user atau pengguna jaringan. *Authorization* penggunaan hak akses dapat memberikan nilai tambah dalam menjaga keamanan jaringan[2][3], sehingga pengguna jaringan yang tidak memiliki hak izin akses tidak dapat terhubung dengan jaringan, dan administrator jaringan kampus juga dapat membatasi apa saja yang dapat diakses oleh pengguna jaringan. Selain itu ada pencatatan (*Accounting*) merupakan proses pengumpulan data informasi seputar durasi *user* melakukan koneksi dan *billing time* yang telah dilalui selama pemakaian.[2][3] Untuk itu penggunaan jaringan WLAN pada kampus perlu dilakukan penyaringan dan pembatasan akses untuk mahasiswa dengan menggunakan “triple-A *server* atau *RADIUS server* sehingga dapat mencegah penggunaan *access point* secara ilegal[4][5][6].

Untuk itu dirancang sistem dengan *server AAA*, agar penggunaan akses internet dapat efisien dalam mengakses SIM PNJ. Rancang bangun *server AAA* ini menggunakan router Mikrotik RB 750-R2 sebagai perangkat utamanya.[7][8][9] Router dikonfigurasi menjadi *RADIUS* (Remote Access Dial In User Service), yang menggunakan format RFC 2865 dan RFC 2866 sebagai dasar dari *RADIUS*. [5][6] Selain itu agar memudahkan user untuk mengakses SIM PNJ, digunakan web atau satu halaman untuk melakukan proses *authentication*, *authorization* dan *accounting* yang dinamakan *Captive Portal* atau bisa disebut halaman login.[10][11] Sistem keamanan jaringan juga diperhitungkan, untuk itu *firewall* di Mikrotik juga diaktifkan. Serta untuk enkripsi data digunakan MD5 yang dikenal relatif aman karena menggunakan hash satu arah.[9][12]



Gambar 1. Tampilan halaman login

Tampilan dari halaman *captive portal* untuk rancang bangun *server AAA* dapat dilihat di gambar 1.

METODOLOGI

Pada penelitian ini dilakukan pengujian *server AAA* pada jaringan WLAN untuk akses SIMPNJ. Pengujian sistem pada penelitian ini adalah metode kuantitatif. Data untuk metode kuantitatif dapat diperoleh dari hasil pengujian sistem yang dibangun. Data tersebut dapat berupa angka, tabel, dan grafik. [13][14] Terdapat 3 pengujian yang dilakukan yaitu dengan pengujian fungsi *AAA*, pada *server AAA*, performansi dari *server AAA*, dan Mekanisme *Backup Database server AAA*. [8][14][15].

Dalam penelitian kali ini instrumen penelitian yang digunakan adalah sebagai berikut: Perangkat Lunak (*Software*) Perangkat lunak yang digunakan dalam perancangan dan pengujian ini meliputi *software network analyzer* dan *software* pengukuran performansi, yaitu *wireshark* dan www.speedtest.net [12][15] Perangkat keras yang digunakan dalam perancangan ini meliputi perangkat komputer, dan perangkat jaringan, yaitu router Mikrotik RB750 R2 dan wireless router, serta gawai, switch, kabel jaringan dan lainnya. [7][8][9][11][14]

HASIL DAN PEMBAHASAN

Pengujian Server AAA

Pada analisis dari mekanisme pengujian membahas tentang hasil pembacaan *software Wireshark*. Analisis ini bertujuan untuk menunjukkan bahwa *server AAA* dapat meningkatkan keamanan pada jaringan *wireless LAN*, dengan adanya penggunaan MD5 (*Message-Digest*) yang melakukan enkripsi *password*.

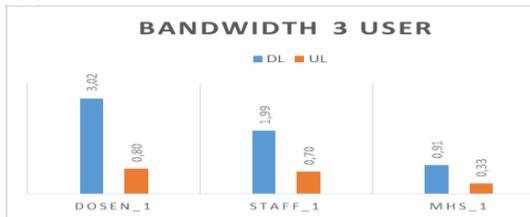


Gambar 2 Hasil Pembacaan Authentication dengan user Dosen

Password untuk setiap user yaitu “123456” dan yang terbaca oleh wireshark adalah 32 digit hexadecimal yang berbeda untuk setiap user hal ini terjadi karena adanya MD5 saat user melakukan login sehingga password dienkripsi saat dikirimkan ke server AAA.

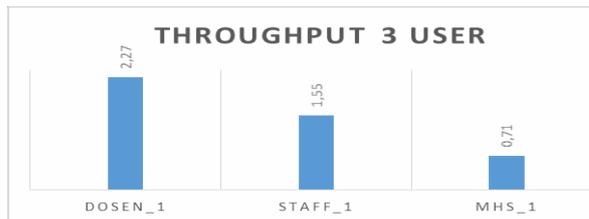
Performansi Bandwidth

Hasil pengujian bandwidth dengan 3 user sesuai dengan limitasi bandwidth yang sudah ditetapkan untuk setiap user yaitu sebesar ≤ 3 Mbps untuk user Dosen, ≤ 2 Mbps untuk user Staff, ≤ 1 Mbps untuk user Mahasiswa.



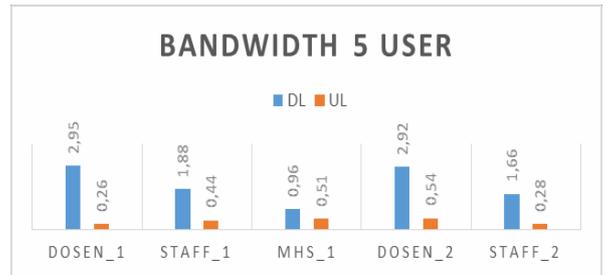
Gambar 3. Grafik Pengujian Bandwidth dengan 3 User

Hasil pengujian throughput dengan 3 user dikatakan BAIK karena nilai masih lebih dari 75% berdasarkan standar TIPHON.



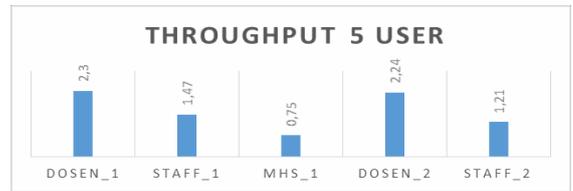
Gambar 4. Grafik Pengujian Throughput dengan 3 User

Hasil pengujian bandwidth dengan 5 user mengalami penurunan nilai bandwidth dari yang sudah ditetapkan untuk setiap user yaitu sebesar ≤ 3 Mbps untuk user Dosen, ≤ 2 Mbps untuk user Staff, ≤ 1 Mbps untuk user Mahasiswa.



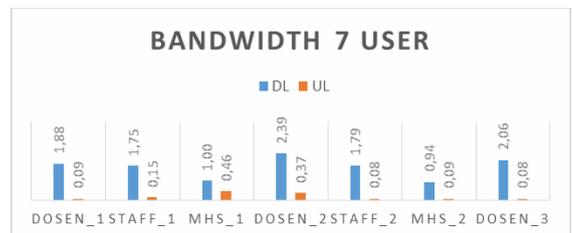
Gambar 5. Grafik Pengujian Bandwidth dengan 5 User

Hasil pengujian throughput dengan 5 user dikatakan BAIK karena nilai masih lebih dari 75% kecuali untuk user Staff_2 yang memiliki persentase 73% yang termasuk dalam kategori SEDANG.



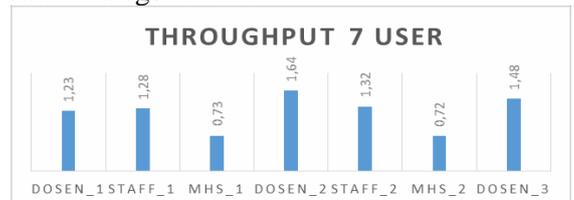
Gambar 6. Grafik Pengujian Throughput dengan 5 User

Hasil pengujian bandwidth dengan 7 user mengalami penurunan nilai bandwidth dari yang sudah ditetapkan untuk setiap user yaitu sebesar ≤ 3 Mbps untuk user Dosen, ≤ 2 Mbps untuk user Staff, ≤ 1 Mbps untuk user Mahasiswa.



Gambar 7. Grafik Pengujian Bandwidth dengan 7 User

Hasil pengujian throughput dengan 7 user dikatakan SEDANG karena nilai kurang dari 75% kecuali untuk user Mhs_2 yang memiliki persentase 77% yang termasuk dalam kategori BAIK.



Gambar 8. Grafik Pengujian Throughput dengan 7 User

Mekanisme Backup Server

Hasil pengujian pada mekanisme pengujian 3 yaitu log yang terdapat pada server AAA saat mengirimkan file *backup* database server AAA ke *Email address* admin. Log yang terdapat pada server AAA menunjukkan bahwa saat mengirim *email* terdapat protokol jaringan untuk keamanan yaitu TLS, pada *log* terdapat proses *handshake* antara server AAA dengan SMTP server milik Gmail untuk membangun TLS yang merupakan protokol keamanan seperti yang terlihat pada Gambar 9.

Aug/02/2018 19:20:24	memory	e-mail, debug	send STARTTLS
Aug/02/2018 19:20:25	memory	e-mail, debug	rcv: 220 2.0.0 Ready to start TLS
Aug/02/2018 19:20:26	memory	e-mail, debug	send EHLO [192.168.1.16]
Aug/02/2018 19:20:27	memory	e-mail, debug	rcv: 250-smtp.gmail.com at your service, [180.244.232.118]

Gambar 9. Log saat mengirim *email* pada serverAAA

KESIMPULAN

Berdasarkan hasil data dan analisis tentang rancang bangun server AAA untuk akses SIM PNJ dengan jaringan Wireless LAN ini, maka dapat disimpulkan sebagai berikut:

Server AAA (*Authentication, Authorization, dan Accounting*) memiliki 3 (tiga) cara untuk dapat meningkatkan keamanan jaringan WLAN yaitu adanya metode enkripsi untuk *password* dengan MD5 pada *Authentication*, membedakan hak akses dengan *Authorization*, dan pencatatan statistik *user* dengan *Accounting*.

Hasil analisis pengujian *bandwidth limitation* didapat nilai untuk masing-masing *user* mendapat nilai sudah ditetapkan untuk setiap *user* yaitu sebesar $\leq 3\text{Mbps}$ untuk *user* Dosen, $\leq 2\text{Mbps}$ untuk *user* Staff, $\leq 1\text{Mbps}$ untuk *user* Mahasiswa.

Hasil analisis menunjukkan bahwa kualitas *throughput* menurun ketika ada 7 *user* mengakses secara bersamaan dengan persentase rata-rata sebesar 71,85%. *Throughput* termasuk kategori SEDANG berdasarkan standar TIPHON dengan sebelumnya rata-rata persentase sebesar $\geq 75\%$ ketika ada 5 *user* yang mengakses jaringan.

Backup database server AAA dapat dilakukan dengan 2 (dua) mekanisme, yang pertama yaitu dengan cara *download file* "logsqldb" dan "sqldb" pada Mikrotik. Mekanisme kedua yaitu dengan cara mengirim *backup database* berupa file

berformat .rsc melalui *email*.

SARAN

Sebaiknya pengujian untuk QoS dilakukan sehingga dapat dianalisis kinerja dari jaringannya. Sebaiknya dipadukan antara pengguna WLAN dan pengguna LAN, agar dapat diuji parameter QoS-nya.

UCAPAN TERIMA KASIH

Terima kasih kepada ketua jurusan Teknik Elektro PNJ, KPS dan program studi S1 Terapan Broadband Multimedia PNJ, sehingga penelitian ini dapat dilaksanakan. Ucapan terima kasih juga kepada staf laboratorium dan bengkel Telekomunikasi PNJ, telah membantu dalam pengambilan data. Serta tak lupa ucapan terima kasih kepada keluarga, atas pengertian terhadap pelaksanaan tri darma perguruan tinggi..

DAFTAR PUSTAKA

- [1] E. Orlando, "Pemanfaatan Protokol 802.11 Dilihat dari Sisi Kelemahan dan Keamanan," *J. Ilm. KOMPUTASI*, 2015.
- [2] Jamaludin, "Teknik Keamanan Jaringan Wireless LAN Pada Warnet Salsabila Computer Net," *J. Penelit. Tek. Inform.*, 2016.
- [3] Y. Herdiana, "Keamanan Pada Jaringan Wireless," *Isu Teknol. STT Mandala*, 2014.
- [4] M. Nakhjiri and M. Nakhjiri, *AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility*. 2006.
- [5] Y. N. Kunang and T. Ibadi, "Celah Keamanan Sistem Autentikasi Wireless Berbasis RADIUS," *CELAH KEAMANAN Sist. AUTENTIKASI Wirel. Berbas. RADIUS*, 2013.
- [6] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "RFC 2687 - Remote Authentication Dial In User Service (RADIUS)," *J. Chem. Inf. Model.*, 2013.
- [7] C. N. Infomedia, "Mikrotik Training Basic," <http://www.mikrotik.co.id>, 2010.
- [8] P. Eko, "Implementasi Jaringan Hotspot Dengan Menggunakan Router Mikrotik Sebagai Penunjang Pembelajaran," *J. Inf. Politek. Indonusa Surakarta*, 2015.

-
- [9] Ilham Eka Putra, “Perancangan Jaringan Hotspot Berbasis,” *Peranc. Jar. Hotspot Berbas. Mikrotik Router OS 3.3.0*, 2013.
- [10] B. K. A. Setyawan and M. Syafrizal, “Analisis Keamanan Jaringan Wireless yang Menggunakan Captive Portal (Studi Kasus : Warnet Fortran),” *Dasi*, 2012.
- [11] B. A. Masse and I. Iyan, “Membangun Jaringan Wireless Dengan Pengaturan Bandwidth Menggunakan Mikrotik RB951 Pada SMK Negeri 6 Palu,” *J. Elektron. Sist. Inf. dan Komput.*, 2016.
- [12] F. R. Doni, “Optimalisasi Jaringan Wireless Dengan Router Mikrotik Studi Kasus Kampus Bsi Tangerang,” *Evolusi*, 2014.
- [13] S. Amri, J. Triyono, and R. Y. R. K, “ANALISIS KINERJA WIRELESS ACCESS POINT (WAP) DAN VIRTUAL ACCESS POINT (VAP) PADA MIKROTIK RB951Ui-2HnD,” *JARKOM*, 2017.
- [14] M. Muhammad and I. Hasan, “Analisa dan Pengembangan Jaringan Wireless Berbasis Mikrotik Router OS V . 5.20 di Sekolah Dasar Negeri 24 Palu,” *J. Elektron. Sist. Inf. dan Komput.*, 2016.
- [15] A. Rahman and H. Havaluddin, “Implementation of Bandwidth Management Authentication,” *Int. J. Comput. Informatics*, 2016.