Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN: 2548-964X
Vol. 6, No. 1, Januari 2022, hlm. 394-401 http://j-ptiik.ub.ac.id

Penerapan *Authentication, Authorization, and Accounting* untuk Pengamanan Jaringan *Small Office/Home Office*

Moh. Fazriyal Audy

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: moh.fazriyal.audy@gmail.com

Abstrak

Small Office/Home Office (SOHO) adalah istilah mengacu pada bisnis kecil atau perkantoran skala kecil. Infrastruktur jaringan pada *SOHO* umumnya menggunakan konfigurasi default dari pabrikan seperti, aktifnya mode *WPS* dan penggunaan *same key*. Karena itu, tugas akhir ini menerapkan implementasi *Authentication, Authorization and Accounting (AAA)* sebagai model pengamanan akses pada jaringan SOHO. Perangkat utama dalam penerapan AAA pada jaringan SOHO, yaitu server *AAA* dan *Wi-Fi Router*. Server *AAA* menjadi pusat autentikasi pengguna, pengaturan hak akses dan *monitoring* aktivitas *user*, sedangkan *Wi-Fi Router* digunakan sebagai penyedia layanan akses *Wi-Fi* dan *DHCP server*. Untuk mendukung penerapan AAA pada jaringan SOHO, khususnya layanan akses Wi-Fi, maka perlu menerapkan *WPA Enterprise*. *WPA Enterprise* memerlukan perangkat dalam melakukan autentikasi secara terpusat yang disebut *Radius server* yang merupakan servis pada AAA. Pada tugas akhir ini telah berhasil menerapkan AAA pada contoh infrastruktur jaringan SOHO. Pengujian latensi untuk proses autentikasi pada perangkat *Windows* sebesar 170,750 *ms* dan *Android* sebesar *753,434 ms*. Penerapan pembagian pengguna dalam grup dengan hak akses yang berbeda dikelompokkan dalam 3 grup (IT, Manajemen, dan Sales). Ketiga grup tersebut dibedakan waktu akses selama *weekday* dan *weekend*. Server AAA dapat juga mencatat aktivitas log-in dan log-out serta durasi waktu pengguna terkoneksi ke dalam jaringan SOHO.

Kata kunci: *SOHO, AAA, WPA Enterprise, Radius*

Abstract

Small Office/Home Office (SOHO) is a term that refers to a small business or small-scale office. The network infrastructure in SOHO generally uses the default configuration from the manufacturer, such as active WPS mode and the use of the same key. Therefore, this final project implements Authentication, Authorization and Accounting (AAA) as a model for securing access on a SOHO network. The main perangkats in implementing AAA on a SOHO network are AAA servers and Wi-Fi Routers. The AAA server is the center for user authentication, setting access rights and monitoring user activity, while the Wi-Fi Router is used as a servis provider for Wi-Fi access and DHCP server. To support the implementation of AAA on SOHO networks, especially Wi-Fi access serviss, it is necessary to implement WPA Enterprise. WPA Enterprise requires a centralized authentication perangkat called the Radius server which is a servis on AAA. In this final project, we have successfully implemented AAA on an example of a SOHO network infrastructure. The latensi *test for the authentication process on Windows perangkats is 170.750 ms and Android is 753.434 ms. The implementation of sharing users in grups with different access rights is gruped into 3 grups (IT, Management, and Sales). The three grups have different access times during weekdays and weekends. AAA servers can also log log-in and log-out activities as well as the duration of time a user is connected to the SOHO network.*

Keyword*: SOHO, AAA, WPA Enterprise, Radius*

1. PENDAHULUAN

Small Office Home Office (SOHO) merupakan istilah yang mengacu pada bisnis atau usaha kecil. Tingginya mobilitas dan terbatasnya jarak dan waktu membuat rumah digunakan sebagai pilihan untuk melakukan bisnis atau usaha dengan nilai strategis yang

tinggi (Akmal, 2013). *SOHO* bersifat sederhana baik secara infrastruktur maupun layanan. Infrastruktur jaringan *SOHO* sederhana karena infrastruktur jaringannya berskala kecil. Jaringan *SOHO* membutuhkan satu perangkat yaitu wireless router yang dapat melakukan pengaturan lalu lintas komunikasi, penyedia layanan wireless, dan mengakses layanan broadband jaringan internet. Jaringan yang digunakan pada *SOHO* bertipe *peer-to-peer* yang digunakan untuk *file sharing, internet access,* dan *perangkat sharing* (Afrianto dkk., 2017).

Jaringan *SOHO* tindak pengamanan sangat minimum karena umumnya masih menggunakan konfigurasi bawaan (*default configuration*) dari *vendor* dengan mode *WPS*. Konfigurasi ini meliputi pengaturan *SSID*, *IP Address*, *Remote* manajemen, *DHCP enable*, Kanal frekuensi hingga *password* (Supriyadi, 2006). Dengan menggunakan mode *WPS* untuk model pengamanan jaringan wireless pada jaringan *SOHO*, proses autentikasi akses jaringan sangat sederhana dengan model berbagi *password* yang sama sehingga membuat jaringan menjadi sangat rentan terjadi serangan (Garcia dkk., 2018).

Teknologi *nirkabel* merupakan teknologi yang menghubungkan dua perangkat atau lebih tanpa penggunaan kabel, yang sering dikenal dengan istilah *wireless*. *Wireless* menggunakan sinyal elektromagnetik untuk pengiriman data (Pratama, 2015). *Wireless* merupakan sebuah alternatif komunikasi dan pelengkap jaringan kabel agar membuat proses transfer data menjadi lebih praktis (Garcia dkk., 2018). *Wireless* memberikan aspek aksesibilitas dan fleksibilitas bagi penggunanya. *Wireless* lebih fleksibel untuk dipakai di berbagai perangkat mobile dan juga elektronik dibandingkan teknologi kabel. Aspek aksesibilitas memberikan kemudahan untuk *user* dalam mendapatkan atau mengakses suatu jaringan komputer. Kemudahan *user* yang di tawarkan menjadi daya tarik bagi *user* komputer untuk mengakses suatu jaringan dan internet (Pratama, 2015).

Kejahatan komputer menyebabkan kerugian dari pengelola sistem jaringan komputer. Khususnya berhubungan dengan sejumlah data-data yang merupakan informasi yang sangat penting dan bersifat rahasia, yang hanya diperbolehkan untuk diketahui oleh orang-orang tertentu di dalam suatu organisasi atau perusahaan (Pratama, 2015). Oleh karena itu, keamanan jaringan harus lebih diperhatikan untuk melindungi suatu sistem, dari berbagai ancaman serangan yang kemungkinan bisa terjadi. Pada jaringan *SOHO* serangan yang kemungkinan dilakukan dengan *brute force attack* (Garcia dkk., 2018).

Berdasarkan permasalahan pada jaringan *SOHO*, maka diperlukan suatu sistem pengamanan jaringan untuk memastikan keamanan pada jaringan *SOHO*. Solusi itu berupa penerapan *framework AAA. AAA* merupakan istilah untuk *framework* yang digunakan untuk mengontrol akses secara cerdas ke sumber daya komputer yang kita gunakan, kebijakan *user*, keperluan audit, serta menyediakan informasi yang diperlukan untuk layanan yang ada (Trisnio , 2017)

Penggunaan *AAA* terdapat tiga perangkat perantara, yaitu *End Perangkat*, *Wireless router* dan server AAA. *AAA* digunakan untuk mengontrol akses secara cerdas ke sumber daya komputer, kebijakan *user*, keperluan audit, serta menyediakan informasi yang diperlukan untuk layanan yang ada. Pada *AAA* dilakukan tiga proses yaitu proses *authentication, authorization,* dan *accounting* (Trisnio, 2017). *Wi-Fi Router* menjadi perangkat yang di dalamnya diterapkan *WPA Enterprise* untuk model pengamanan pada jaringan *SOHO*. Selain itu, perangkat *Wi-Fi Router* memberikan layanan sebagai penyedia *DHCP server & client, wireless,* dan *Radius client.*

2. KAJIAN KEPUSTAKAAN

Penelitian ini merujuk pada penelitian sebelumnya berjudul *"Perancangan Sistem Otentikasi Radius Pada Pengguna Jaringan Wireless untuk Meningkatkan Keamanan Jaringan Komputer"* yang ditulis oleh Eko Agus Darmadi. Pada penelitian tersebut membahas mengenai masalah keamanan jaringan yang dihadapi dalam menerapkan model *wireless*. Masalah keamanan pada penelitian ini tentang akses *user* yang umumnya tidak menggunakan autentikasi pengguna, karena tidak adanya autentikasi pengguna maka jaringan *wireless* dapat dengan mudah diakses oleh siapapun saat pengguna tersebut bergabung ke dalam jaringan. Dalam penelitian ini model pengamanan jaringan *wireless* menggunakan *Wired Equivalent Privacy (WEP)*. Saat ini *WEP* dapat dengan mudah dipecahkan oleh berbagai cara seperti *brute force*.

Dengan kemajuan teknologi, muncul model pengamanan jaringan *wireless* baru yaitu

Wireless Protected Access (WPA) sebagai kunci keamanan sementara untuk menggantikan *WEP*. Akan tetapi, *WPA* juga dapat dipecahkan dengan menggunakan metode *dictionary attack* secara *offline*. *WPA* memerlukan kunci yang disebut *key WPA* yang dapat mengkonfigurasi kunci setiap *access point (AP)* dan *client AP* itu sendiri. Hal ini dapat mempersulit administrator, karena harus mendatangi dan mengkonfigurasi *key WPA* dari setiap *AP*. Namun muncul masalah apabila terdapat kegiatan *password sharing user* legal dan ilegal. Dan dapat disimpulkan bahwa, siapapun yang memiliki *password* yang valid dapat mengakses jaringan tersebut.

Penelitian selanjutnya berjudul *"Hardening Applied Over a WLAN SOHO Environment for Mitigation of Vulnerabilities"* yang ditulis oleh Magnolia A.G dan kawan-kawan. Paper ini menjelaskan mengenai perbandingan tingkat keamanan pada protokol keamanan teknologi *nirkabel* pada jaringan *SOHO* diantaranya *Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA)* dan *Wi-Fi Protected Access 2(WPA2)*. Dengan melakukan perbandingan sistem autentikasi dari setiap protokol tersebut, dari enkripsi yang digunakan dan tipe *key* yang digunakan dari ketiga protokol tersebut. Dalam penelitiannya perangkat yang berperan sebagai server autentikasi yaitu menggunakan *access point (AP)*.

Dari penelitian ini didapat kelemahan dari jaringan *wireless SOHO* adalah aktifnya mode *Wi-Fi Protected Setup (WPS),* autentikasi bersama, dan konfigurasi bawaan (*Default configuration)*. Dengan mode *WPS*, *user* dapat dengan mudah melakukan proses autentikasi dengan menggunakan 8-digit PIN yang tertera pada perangkat *Wi-Fi*. Selain menggunakan PIN tersebut, *user* dengan mudah terhubung ke jaringan *wireless* dengan menekan tombol *WPS* ada perangkat *Wi-Fi*, dan *user* akan terhubung tanpa menggunakan PIN tersebut. Dengan aktifnya mode ini, resiko terjadi serangan pada jaringan *wireless* yaitu adanya *brute force attack* yang dilakukan oleh *user* ilegal.

Penelitian selanjutnya berjudul *Penerapan Model* Protokol *AAA (Authentication, Authorization, Accounting) Pada Pengamanan Jaringan Komunikasi WAN (Wide Area Network)*" yang ditulis oleh Abdul Sani S. Penelitian ini membahas tentang pengamanan perangkat jaringan *WAN* dengan menggunakan *Stateful Packet Inspection (SPI)* dan *Network Address Translation (NAT)* menggunakan media kabel. Sistem tersebut diimplementasi pada perangkat *Router Cisco*. Dalam penelitian ini didapat masalah pada jaringan komputer yaitu eksploitasi perangkat sistem, pengaksesan informasi, perubahan informasi dan penghapusan informasi oleh pihak yang tidak memiliki wewenang dalam mengakses informasi pada jaringan komputer.

Penerapan *NAT* dapat menimbulkan *delay switching* apabila diimplementasikan pada jaringan *WAN*. Selain itu penggunaan *NAT* dapat mengurangi hingga menghilangkan kemampuan *traceability* atau kemampuan dalam melakukan identifikasi. Penelitian ini hanya melakukan pengamanan terhadap akses ke dalam perangkat router saja dan *username* dan *password* dapat dengan mudah di sebar ke pihak yang tidak berwenang.

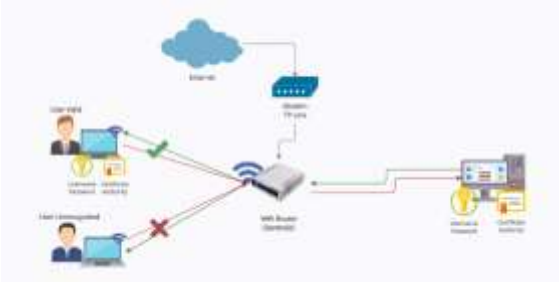
Penelitian selanjutnya berjudul Penelitian pertama berjudul *"Pemanfaatan Network Attached Storage (NAS) Sebagai Solusi Jaringan Small Office Home Office (SOHO)"* yang ditulis oleh Irawan Afrianto dan kawan-kawan. Penelitian tersebut menjelaskan bahwa tentang pemanfaatan *NAS* dalam mengamankan data, mengoptimalkan pengiriman data dan *monitoring memory usage* pada jaringan *SOHO*. Penelitian ini dibuat karena muncul isu dalam komunikasi data yaitu tentang inefisiensi waktu pengiriman data, ketersediaan data, dan keamanan data. Pada penelitian ini terdapat perbandingan antara jaringan *SOHO* sebelum dan sesudah menggunakan *NAS*. Dilakukan pengujian persentase keamanan yang berjalan menggunakan *NAS* menggunakan aplikasi *Nessus*. Untuk analisa trafik data, digunakan parameter *Quality of Servis (QoS). QoS* digunakan untuk mendapatkan kualitas kemampuan sebuah jaringan seperti aplikasi, host atau router untuk memberikan servis yang lebih baik dan terencana sehingga dapat memenuhi kebutuhan suatu layanan. Oleh karena itu penulis mengembangkan penelitian itu dengan mengimplementasikan *Radius server*. Di dalam *Radius server* pada penelitian ini menggunakan *NAS* sebagai port fisik. *NAS* ini nantinya bertugas yang akan digunakan untuk membangun *framework AAA* yang diimplementasikan pada server berbasis sistem operasi *Windows*.

3. *AUTHENTICATION, AUTHORIZATION AND ACCOUNTING (AAA)*

Dalam menerapkan *Authentication, Authorization and Accounting (AAA)* untuk pengamanan jaringan *Small Office/Home Office (SOHO),* diperlukan proses penyusunan rancangan dan implementasi.

3.1. Rancangan *Authentication, Authorization and Accounting (AAA)*

Rancangan *AAA* mencakup gambaran umum pada penelitian ini meliputi rancangan komunikasi pada jaringan *SOHO* dengan mengimplementasikan *AAA.*



Gambar 1 Arsitektur *AAA*

Gambar 1, merupakan arsitektur jaringan *SOHO* dengan mengimplementasikan *AAA.* Perancangan sistem pada penelitian ini terbagi menjadi empat proses, yaitu proses mengkonfirmasi *user* kepada administrator jaringan *SOHO.* Proses ini bertujuan untuk memastikan legalitas *user* sebelum terhubung ke jaringan *SOHO* dan untuk mendapatkan data *credential* dan *CA.* Proses kedua yaitu *authentication.* Proses ini digunakan untuk memastikan apakah data *credential user* tersebut autentik atau tidak Proses ketiga yaitu *authorization.* Proses ini menentukan hak akses kepada *user* yang terhubung ke jaringan *SOHO.* Hak akses *user* yang diberikan mengacu pada waktu *user* untuk dapat mengakses jaringan *SOHO* yang dapat dilihat pada tabel 1. Proses keempat yaitu *accounting.* Proses ini dilakukan server untuk mencatat aktivitas *user* dan durasi waktu *user* dalam mengakses jaringan *SOHO* yang disimpan pada direktori lokal server.

Tabel 1 *Network Policies*

No	Nama Grup	Hak akses
1	Secure Enterprise Wireless Connection IT (*User* IT)	All time
2	Secure Enterprise Wireless Connection Sales (*User* Sales)	*Weekday* (06:00-10:00 & 14:00-17:00)
3	Secure Enterprise Wireless Connection Manajemen (*user* manajemen)	*Weekday* (06:00-21:00)

3.2. Implementasi *Authentication, Authorization and Accounting (AAA)*

Implementasi *AAA* meliputi tahapan yang diperlukan dalam melakukan penyusunan sesuai dengan rancangan yang telah dilakukan sebelumnya. Tahapan yang diperlukan meliputi implementasi *Server AAA* & *Wi-Fi Router*.

Server AAA menggunakan *Windows Server 2012 R2*. Pada server *AAA* terdapat *Active Directory (AD), Event Viewer, Certificate Authority (CA),* dan *Network Policy Server (NPS). AD* digunakan untuk membuat *credential user* dan membuat grup *user* untuk mengelompokkan *user* sesuai dengan grup yang ditentukan yaitu grup *user* IT, Sales, dan Manajemen (Liberman, 2016). *Event Viewer* digunakan untuk melakukan monitoring aktivitas *log in* & *log out user* yang terhubung dengan melihat pada *network policies and access servis* yang dimiliki *Event Viewer*. *CA* dibuat sebagai *digital signature* yang di *broadcast* kepada *user*. *NPS* digunakan untuk membuat koneksi antara *Radius server* dan *Radius client*. *NPS* melakukan proses *authentication* dan menentukan *privilege user* terpusat untuk media *wireless*. Pada *NPS* dibuat *secure enterprise wireless connection properties* untuk setiap grup *user* untuk menentukan *privilege* untuk setiap grup dan metode *authentication* yang digunakan yang dapat dilihat pada tabel 2.

Tabel 2 *Radius Attribute*

No	Nama	*Value*
1	Tunnel-Medium-Type	IPv4
2	Tunnel-Pvt-Grup-ID	20
3	Tunnel-Type	*Generic Route Encapsulation (GRE)*

Tunnel Medium Type merupakan nilai enumerasi yang menunjukkan media transportasi yang digunakan saat membuat tunnel berdasarkan protokol yang dapat mendukung beberapa jenis tunnel (Calhoun dkk, 2003). Tunnel type merupakan tipe *enumerated* yang berisi protokol *tunneling* yang digunakan dalam permintaan Authorization (Calhoun dkk, 2003). *GRE* dapat melakukan enkapsulasi berbagai protokol yang dibuat untuk kebutuhan sebuah link virtual *Peer To Peer* (Warman dan Hanafi, 2019). Tunnel-Pvt Grup-ID menentukan

ID Grup untuk melakukan sesi *tunneled*.

Wi-Fi Router pada penelitian ini menggunakan produk *MikroTik* tipe RB751u-2HnD. Pada *Wi-Fi Router* dilakukan konfigurasi *DHCP server*, *DHCP client*, *Security profile WLAN*, dan *Radius client*. *Secure profile WLAN* menggunakan *WPA2 EAP* sebagai tipe *authentication*. Selanjutnya konfigurasi *Radius client* ini bertujuan agar *Wi-Fi Router* dapat berkomunikasi secara *peer-to-peer* terhadap server, dengan atribut sebagai berikut.

IP Address : 192.168.20.3
Servis : wireless
Shared key : 123456789*********
Authentication port : 1812
Accounting port : 1813

4. EVALUASI

Pada penelitian ini dilakukan penyusunan parameter pengujian, dan analisis hasil pengujian untuk mendapatkan evaluasi dari sistem yang telah dibangun.

4.1. Parameter Pengujian

A. Pengujian *Authentication*

Pengujian untuk menilai apakah server dapat melakukan proses autentikasi pada *user* dan dapat memvalidasi *user* dengan menggunakan *credential* dan *CA* dengan kondisi sebagai berikut:

a. *User* melakukan proses autentikasi hanya menggunakan *credentia*l valid saja.
b. *User* melakukan proses autentikasi hanya menggunakan *certificate authority* valid saja.

Pengujian ini menguji *time-lapse* latensi yang diberikan server untuk melakukan autentikasi terhadap *user* dengan kondisi tanpa adanya hambatan. Pengujian ini dilakukan pada *Windows* dan *Android*. Selanjutnya, setelah proses autentikasi berhasil dilakukan, maka dilakukan pengujian dengan melakukan proses autentikasi dengan data dan waktu yang sama pada perangkat yang berbeda

B. Pengujian *Authorization*

Pengujian untuk menilai apakah server dapat memberikan hak akses yang sesuai pada setiap *user*. Pengujian dilakukan pada *weekend* dan *weekday* dengan skala waktu akses *user* yang dapat dilihat pada tabel 3.

Tabel 3 Pengujian *Authorization*

Day/Time	**00: 00**	**06: 00**	**……**	**16: 00**	**23: 59**
Sunday					
Monday					
Tuesday					
Wednesday					
Thursday					
Friday					
Saturday					

Selanjutnya, pengujian ini dilakukan untuk mengetahui bagaimana respon server apabila terdapat *user* melakukan proses autentikasi di luar waktu (hak akses).

C. Pengujian *Accounting*

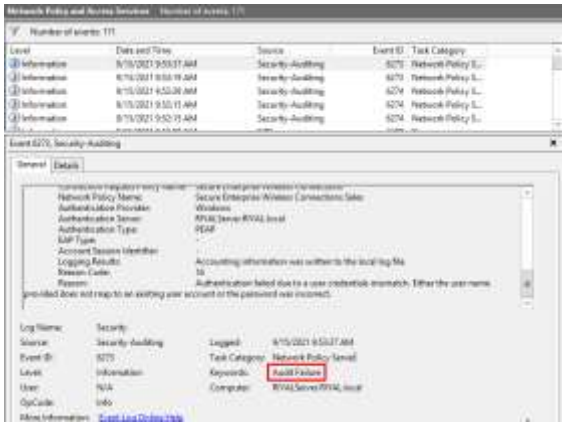
Pengujian ini bertujuan untuk mengetahui bahwa server dapat mencatat aktivitas *user* dan durasi waktu *user* yang disimpan pada *database server*. Pengujian ini dilakukan pada fitur *Event Viewer* dan *accounting* pada server. Kedua fitur tersebut merupakan tempat dimana segala aktifitas user tercatat dan disimpan.

4.2. Analisis Hasil Pengujian

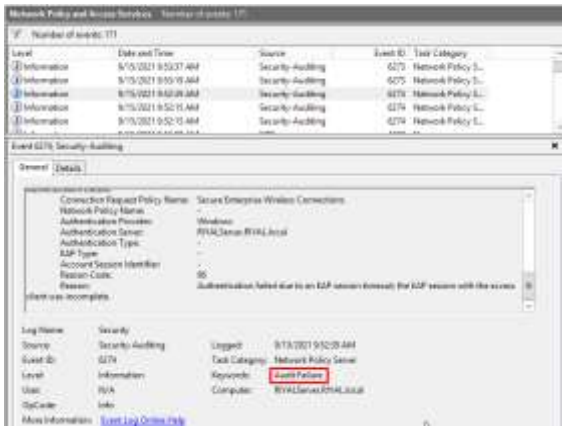
A. Pengujian *Authentication*

Proses autentikasi pada *Windows* mendapatkan nilai latensi sebesar 170,750 *ms* dan pada *Android* mendapatkan nilai latensi sebesar 753,434 *ms*. Nilai tersebut didapat pada aplikasi *Wireshark*. *Time-lapse* yang tercatat didapat dengan melakukan filtering untuk tipe protokol *RADIUS*.

Pengujian proses autentikasi hanya menggunakan *credential* atau *CA* mendapatkan hasil bahwa proses autentikasi mengalami kegagalan. Proses autentikasi yang gagal dicatat oleh server dengan status *audit failure* yang dapat dilihat pada gambar 2 dan gambar 3.



Gambar 2 Invalid Credential



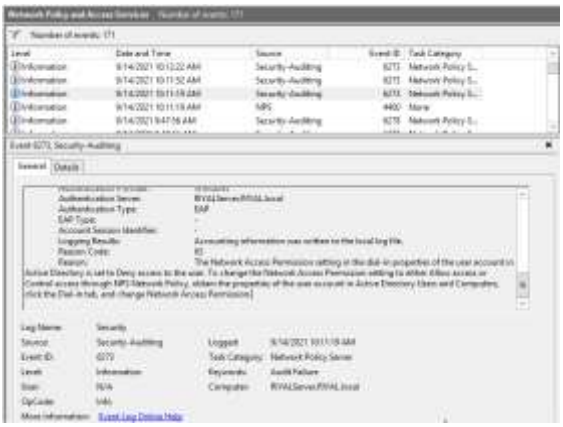
Gambar 3 Tanpa Instalasi *CA*

Reaksi server pada gambar 2 memberikan informasi bahwa proses autentikasi gagal karena terdapat ketidakcocokan *credential user*, baik *user*name yang diberikan tidak dipetakan ke akun pengguna yang ada atau kata sandi nya salah. Sedangkan, gambar 3 memberikan informasi bahwa *user* dalam melakukan autentikasi terdapat kekurangan dalam melakukan sesi *EAP* yang *user* tersebut tidak memiliki prosedur autentikasi yang lengkap.

Hasil pengujian melakukan autentikasi dengan menggunakan satu *credential* valid untuk dua perangkat yang berbeda mendapatkan hasil bahwa proses autentikasi dapat dilakukan pada beberapa perangkat dengan menggunakan data valid.

B. Pengujian *Authorization*

Pengujian *authorization* mendapatkan hasil bahwa setiap grup *user* berjalan sesuai dengan *network policy* yang telah dibuat dan ditentukan pada *NPS*. Pengujian ini dilakukan pada tiga grup *user* yaitu *user* IT, sales, dan Manajemen. Apabila terdapat kegiatan yang memaksa melakukan proses autentikasi di luar waktu aksesnya maka proses autentikasi *user* tersebut gagal atau mendapat penolakan dari server. Penolakan server dapat dilihat pada gambar 4.



Gambar 4 Reaksi Server

Reaksi tersebut memberikan informasi bahwa Permission oleh *user* tersebut mendapat penolakan dari server, karena permission *user* tersebut tidak sesuai pada NPS. Apabila *user* ingin mengakses ke jaringan, harus melakukan perubahan permission pada NPS.

Hasil pengujian *authorization* terdapat pada tabel 4 dan tabel 5. Tabel 4 meruapkan hasil pengujian pada *weekday* atau hari kerja sedangkan tabel 5 merupakan hasil pengujian pada *weekend*. Pada tabel tersebut kolom bersisi tanda centang (✓) menunjukkan bahwa *user* tersebut dapat mengakses internet pada jaringan *SOHO* dan pada kolom yang bersisi tanda silang (×) *user* tersebut tidak dapat mengakses ke jaringan *SOHO* pada waktu pada tabel.

Tabel 4 *Secure Enterprise Wireless Connection at Weekday*

Grup User\Waktu	**01:00-05:00**	**06:00-10:00**	**11:00-13:00**	**14:00-17:00**	**18:00-21:00**	**22:00-00:00**
User IT	✓	✓	✓	✓	✓	✓
User Manajemen	×	✓	×	✓	×	×
User Sales	×	✓	✓	✓	✓	×

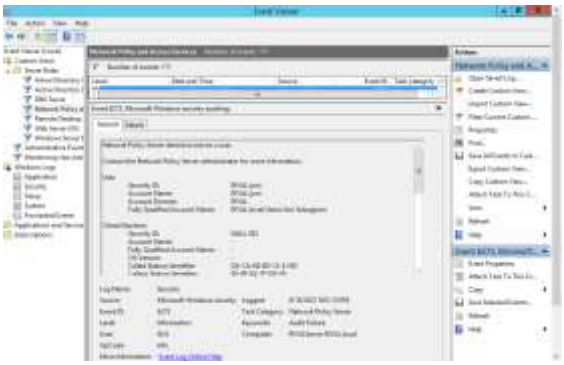
Tabel 5 *Secure Enterprise Wireless Connection at Weekend*

Grup User\Waktu	**01:00-05:00**	**06:00-10:00**	**11:00-13:00**	**14:00-17:00**	**18:00-21:00**	**22:00-00:00**
User IT	✓	✓	✓	✓	✓	✓
User Manajemen	×	×	×	×	×	×
User Sales	×	×	×	×	×	×

C. Pengujian *Accounting*

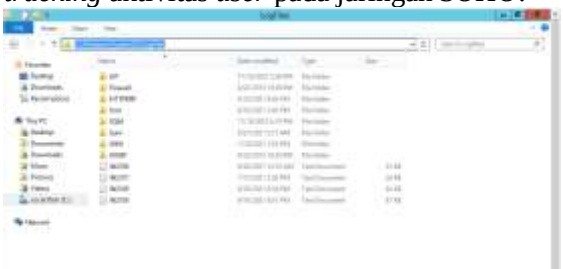
Hasil pengujian ini menghasilkan bahwa server dapat mencatat aktivitas dan durasi waktu *user* dalam mengakses jaringan *SOHO*. Pada gambar 8 dan 9 merupakan log aktifitas *user* yang tercatat pada sisi server. Gambar 5 merupakan log aktifitas *user* yang berhasil melakukan proses autentikasi dengan mendapatkan status "*Audit Success*". Gambar 6 merupakan log aktifitas *user* yang gagal dalam melakukan proses autentikasi dengan mendapatkan status "*Audit Failure*".

Gambar 5 *User Audit Success*



Gambar 6 *User Audit Failure*

Hasil pengujian ini digunakan untuk keperluan *tracking* aktivitas *user* pada jaringan *SOHO*.



Gambar 7 *Data Accounting*

Gambar 7 merupakan lokasi direktori lokal server, yaitu C:\Windows\System32\Log*File*s sebagai tempat menyimpan data *accounting*. Pada gambar 7 terdapat 4 *file .txt*, yaitu IN2106, IN2107, IN2108 dan IN2109 yang secara default diberikan oleh sistem pada server. *File* tersebut berisi informasi waktu kapan *user* memulai dan mengakhiri sesi untuk terhubung ke jaringan *SOHO*. Dengan 4 *file* tersebut dapat dilakukan analisa untuk mengetahui informasi *user* dan waktu user dalam mengakses jaringan *SOHO*. Tabel 6 merupakan hasil analisa ang dilakukan pada keempat *file* tersebut.

Tabel 6 *Log Files Accounting*

File	Tanggal	*User*	Waktu	Durasi
IN2106	22/06/2021	riki	18:13:24 - 22:20:26	4jam 5menit 3detik
	23/06/2021		10:21:51 - 21:47:53	11jam 26menit 2detik
IN2107	13/07/2021	riki	12:06:54 - 15:30:12	3jam 23menit 18detik
IN2108	20/08/2021	riki	17:38:27 - 17:52:04	13menit 37detik
		joni	18:28:00 - 20:21:18	1jam 53menit 18detik
IN2109	05/09/2021	adi	19:40:02 - 21:24:27	1jam 44menit 25detik
	14/09/2021	rani	09:38:29 - 10:00:00	21menit 31detik
	15/09/2021		09:52:11 - 09:57:49	5menit 38detik
	16/09/2021	Joni	20:55:15 - 21:00:00	4menit 45detik

5. KESIMPULAN

Berdasarkan hasil dari proses perancangan, implementasi dan pengujian, maka penelitian ini menghasilkan kesimpulan sebagai berikut:

1. Arsitektur *AAA* yang diterapkan pada jaringan *SOHO* menggunakan dua perangkat utama yaitu *Wi-Fi Router* dan Server *AAA*. *Wi-Fi Router* memberikan layanan *Wi-Fi*, *DHCP server client* dan menjadi *Radius client*. Server *AAA* berperan menjadi perangkat *backend* yang bertugas dalam proses *authentication*, *authorization*, dan *accounting* jaringan *SOHO* secara terpusat.

2. Pengujian proses *authentication* menghasilkan bahwa, keberhasilan proses autentikasi dapat dilakukan dengan menggunakan data *credential* dan *CA*. apabila salah satu data tidak dipenuhi, maka proses autentikasi akan mengalami kegagalan. Dengan menggunakan data tersebut, *user* dapat melakukan proses autentikasi pada beberapa perangkat.
3. Berdasarkan hasil pengujian *authorization*, setiap grup mendapatkan hak akses yang sesuai pada *NPS*. Apabila *user* melakukan proses autentikasi di luar hak akses yang diberikan, maka *user* tersebut mengalami kegagalan dan mendapatkan penolakan dari server.
4. Berdasarkan hasil pengujian *accounting*, server dapat mencatat aktivitas dan durasi waktu *user* dalam mengakses jaringan *SOHO* pada fitur *Even Viewer* dan *accounting.*

6. DAFTAR PUSTAKA

Afrianto, I., Saputra, A. P. H. & Sufa'atin, 2017. Pemanfaatan Network Attachmed Storage (NAS) Sebagai Solusi Jaringan Small Office Home Office (SOHO).

Akmal, I. (2013). Seri Rumah Ide - SOHO Small Office Home Office. Jakarta: PT Gramedia Pustaka Utama.

Calhoun, P. R., Zorn, G., Spence, D., & Mitton, D. (2003). Diameter Network Access Server Application. *IETF*.

Darmadi, E. A., 2018. PERANCANGAN SISTEM OTENTIKASI *RADIUS* PADA PENGGUNA JARINGAN WIRELESS UNTUK MENINGKATKAN KEAMANAN JARINGAN KOMPUTER. ISSN, pp. 10-11.

Garcia, M. A., Martinez, D. J. S. & Castillo-Velazquez, J.-I., 2018. Hardening Applied Over a WLAN SOHO Environment for Mitigation of Vulnerabilities. IEEE.

Liberman, E. (2016). *Windows Server 2016: Active Directory Enterprise Infrastructure.* linkedin.com.

Pratama, I. P. A. E., 2015. Handbook Jaringan Komputer. 2nd ed. Bandung: Informatika Bandung.

Sembiring, A. S., 2020. Penerapan Model ProtokolAAA (Authentication, Authorization,Accounting) Pada Pengamanan Jaringan Komunikasi WAN

Supriadi, D., 2018. ANALISA DAN PERANCANGAN INFRASTRUKTUR JARINGAN WIRELESS LOCAL AREA NETWORK (WLAN) PADA DINAS PERINDUSTRIAN DAN PERDAGANGAN KABUPATEN LOMBOK TENGAH. JIRE (Jurnal Informatika & Rekayasa Elektronika) .

Trisnio, K., 2017. Binus University School of Information Systems. [Online] Available at: https://sis.binus.ac.id/2017/05/02/apa-itu-AAA-authentication-authorization-accounting/

Warman, I., & Hanafi, A. (2019). ANALISA PERBANDINGAN KINERJA GENERIC ROUTING ENCAPSULATION (GRE) TUNNEL DENGAN POINT TO POINT PROTOCOL OVER ETHERNET (PPPoE) TUNNEL MIKROTIK ROUTEROS. *Jurnal TEKNOIF*.

Akmal, I. (2013). Seri Rumah Ide - SOHO Small Office Home Office. Jakarta: PT Gramedia Pustaka Utama.