JURNAL TEKNIK INFORMATIKA DAN TEKNOLOGI INFORMASI
Halaman Jurnal: https://ejurnal.politeknikpratama.ac.id/index.php/JUTITI
Halaman UTAMA: https://ejurnal.politeknikpratama.ac.id/index.php

MANAJEMEN KEBIJAKAN JARINGAN NIRKABEL MENGGUNAKAN *CLOUDPATH ENROLLMENT SYSTEM* DENGAN METODE RADIUS

Asep Supriadi [a], Hendra Supendar [b], Sulistianto Sutrisano Wanda[c]
[a] Teknologi Informasi / Informatika, asepsup1@gmail.com, Universitas Nusa Mandiri
[b] Teknik dan Informatika / Teknologi Informasi, hendra.hds@bsi.ac.id, Universitas BSI
[c] Teknologi Informasi / Informatika, sulistianto.sow@nusamandiri.ac.id, Universitas Nusa Mandiri

ABSTRAK

Many ways are used to make communication easier, One of the most notable changes to computer network communication technology is the use of wireless technology. The technology applied to this computer network is commonly called WLAN (Wireless LAN). WLAN is a local network of wireless areas that uses radio waves as a transmission medium. The conveniences contained in this technology are the triggers for choosing the use of technology in computer networks. Of all the conveniences offered by wireless, there is a weakness in the application of this technology, namely the security side, which still has many loopholes to be attacked by other parties. Many unauthorized clients can access hotspots, if this happens, it will directly or indirectly harm the ISP (Internet Service Provider). By implementing the Ruckus Cloudpath Application configuration and the use of RADIUS features on the user side. Based on the results of research, the best security system at this time uses the WPA RADIUS (Wireless Protection Autentication Remote Authentication Dial in User Services) method.
Keywords: Wireless, Cloudpath, RADIUS.

Abstrak

Banyak cara yang digunakan untuk membuat komunikasi semakin mudah, Salah satu perubahan paling menonjol pada teknologi komunikasi jaringan komputer adalah penggunaan teknologi *wireless*. Teknologi yang diterapkan pada jaringan komputer ini biasa disebut WLAN (*Wireless* LAN). WLAN adalah suatu jaringan lokal area tanpa kabel yang menggunakan gelombang radio sebagai media tranmisinya. Kemudahan-kemudahan yang terdapat pada teknologi ini yang menjadi pemicu pemilihan penggunaan teknologi pada jaringan komputer. Dari semua kemudahan-kemudahan yang ditawarkan wireless ini terdapat suatu kelemahan dalam penerapan teknologi ini yaitu sisi keamanan yang masih banyak terdapat celah untuk diserang oleh pihak-pihak lain. Banyak client yang tidak sah dapat mengakses hotspot, jika sampai hal ini terjadi maka secara langsung atau tidak langsung akan merugikan pihak ISP (*Internet Servis Provider*). Dengan menerapkan konfigurasi Aplikasi *Ruckus Cloudpath* dan penggunaan fitur RADIUS di sisi pengguna. Berdasarkan hasil penelitian sistem keamanan terbaik pada saat ini menggunakan metode WPA RADIUS (*Wireless Protection Autentication Remote Authentication Dial in User Services*).
Kata Kunci: *Wireless*, *Cloudpath*, RADIUS.

1. PENDAHULUAN

Kemajuan di bidang teknologi jaringan komputer memang sungguh luar biasa, baik menyangkut piranti keras (*hardware*), lunak (*software*) maupun *database* dari jaringan tersebut. Banyak cara yang digunakan untuk membuat komnunikasi semakin mudah, Salah satu perubahan paling menonjol pada teknologi komunikasi jaringan komputer adalah penggunaan teknologi *wireless* sebagai salah satu solusinya. Teknologi yang diterapkan pada jaringan komputer ini biasa disebut WLAN (*Wireless* LAN). WLAN adalah Suatu jaringan lokal area tanpa kabel yang menggunakan gelombang radio sebagai media transmisinya. Kemudahan-kemudahan yang terdapat pada teknologi ini yang menjadi pemicu pemilihan penggunaan teknologi pada jaringan komputer.

Beberapa tahun belakangan ini penggunaan teknologi ini mengalami kemajuan yang sangat pesat. Hal ini dibuktikan dengan banyaknya area hotspot yang dipasang pada tempat-tempat umum oleh pihak ISP (pihak Penyedia Jasa Layanan Internet), baik itu di mall, di pertokoan, perkantoran, tapi seiring dengan

berkembangannya teknologi, seiring itu pula kejahatan di bidang jaringan komputer terjadi, khusunya di bidang *wireles.*

Dari kejadian ini dapat kita ambil kesimpulan bahwa sudah banyak sekali penerapan teknologi ini di berbagai tempat untuk menyediakan informasi bagi tiap-tiap keperluan. Dari semua kemudahan-kemudahan yang ditawarkan wireless ini terdapat suatu kelemahan dari penerapan teknologi ini yaitu sisi keamanan yang masih banyak terdapat celah untuk diserang oleh pihak-pihak lain. Banyak client yang tidak sah (*illegal*) dapat mengakses hotspot, jika sampai hal ini terjadi maka secara langsung atau tidak langsung akan merugikan pihak ISP (Internet Servis Provider).

Dengan menerapkan konfigurasi Aplikasi Ruckus Cloudpath dan penggunaan fitur RADIUS di sisi pengguna, diharapkan dapat .melindungi Jaringan komputer kita dari pihak-pihak yang akan melakukan pengrusakan (jaringan atau data-data). Karena sistem keamanan itu sangat penting baik.

Berdasarkan hasil penelitian sistemm keamanan terbaik pada saat ini menggunakan metode WPA RADIUS (*Wireless Protection Autentication Remote Authentication Dial in User Services*).

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

2.1.1. Implementasi Keamanan Jaringan *Wireless Enterprise* Menggunakan *Remote Autentication Dial In User Service*

Penelitian yang dilakukan oleh dilakukan oleh Nanang Sadikin dari Universitas Islam Attahitirah. Berdasarkan penelitian tersebut terdapat perbedaan pada ruang lingkup penelitian dengan penelitian yang dilakukan, ruang lingkup penelitian yang dilakukan membahas mengenai Konfigurasi sistem keamanan dan manajemen akses masuk ke jaringan komputer dengan Secure WPA2-*Enterprise Encryption* menggunakan Aplikasi Ruckus Cloudpath, sedangkan penelitian oleh Nanang membahas mengenai mengamankan jaringan wireless menggunakan metode WPA2 Entrerhpire [11].

2.1.2. Manajemen Jaringan *Wireless* Mengunakan *Server Radius*

Penelitian yang sebelumnya dilakukan oleh Raymond Powes Tenggario dan Jonathan Lukas dari Universitas Bina Nusantara. dari penelitian tersebut dan topik penelitian yang memiliki persamaan yaitu keamanan jaringan berbasis RADIUS [12].

2.2. Landasan Teori

2.2.1. Pengertian Jaringan Komputer

Menurut Gitakarma dan Ariawan (2014:1), jaringan adalah sebuah kemampuan dari dua buah komputer atau lebih untuk dapat saling mengetahui keberadaan satu dengan yang lainnya sehingga dapat melakukan pertukaran data. Dalam era internet, yang dimaksudkan dengan pertukaran data antara dua buah komputer bisa menjadi hal yang sangat luas, sebagai contoh: perjalanan sebuah e-mail dari satu server ke server yang lain, sebuah web browser yang men-download halaman HTML, sebuah PC men-download film dari HTTP server, peer-to-peer MP3 sharing, dan masih banyak lagi [4].

2.2.2. Tipe Jaringan Komputer

Tipe jaringan berdasarkan letak penempatannya adalah : LAN (*Local Area Network*), WAN (*Wide Area Network*), dan *Internet*.

a. LAN (*Local Area Network*)

Sebuah jaringan yang terdapat dalam satu bangunan gedung, bisa berupa : kantor, rumah, gudang atau tepat pendidikan. Pada LAN tidak terpaut pada jumlah perangkat yang terhubung dan digunakan, tetapi lebih kepada penempatan jaringan di tempat yang sama.

b. WAN (*Wide Area Network*)

Jaringan LAN, yang terletak pada wilayah geografis yang berbeda.

Bisa dikatakan apabila sebuah usaha memiliki beberapa jaringan LAN dibeberapa area yang berbeda (misal antar kota) dan terhubung satu sama lain secara internet dari sebuah perusahaan penyedia layanannya.

c. *Internet*

Sebuah cara dalam menghubungkan banyak jaringan, yang saling berkomunikasi satu sama lain.

2.2.3. Pengertian IP Address

Menurut Nugroho (2016: 30), IP (*Internet Protocol*) adalah sebuah protokol yang paling banyak digunakan sebagai sarana untuk melakukan mekanisme pengalamatan dalam sebuah jaringan. [9]

Perlu adanya mekanisme pengalamatan antar jaringan dan perangkat yang terhubung didalamnya agar bisa saling berkomunikasi dan bertukar data melalui switch atau router.

IP address yang digunakan dalam sebuah jaringan sesuai dengan aturan tertentu dan tidak boleh menggunakan IP Address yang sama yang digunakan sebagai identitas dari sebuah jalur dalam sebuah jaringan harus unik.

2.2.4. Topologi Jaringan Komputer

Menurut Gitakarma dan Ariawan (2014:2), Topologi fisik adalah sebuah cara untuk menyusun atau mengatur komputer-komputer dalam jaringan. Topologi fisik ini berkaitan dengan pola koneksi antar perangkat yang mengacu pada bagaimana bentuk jaringan kalau dilihat secara fisik (tampak terlihat bentuk fisik jaringan). [4]

2.2.5. Server

Menurut Khairil, dkk (2013:2) :

"*Server* adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. *Server* didukung dengan prosesor yang bersifat scalable dan RAM yang besar, juga dilengkapi dengan sistem operasi khusus, yang disebut dengan sistem operasi jaringan atau *network operating system*. *Server* juga menjalankan perangkat lunak administratif yang mengontrol akses terhadap jaringan dan sumber daya yang terdapat di dalamnya, seperti halnya berkas atau alat pencetak (*printer*), dan memberikan hak akses kepada *workstation* anggota jaringan." [6]

2.2.6. Web Server

Menurut Jhonsen dalam Nandari, dkk (2014:43) "*Web Server* adalah tempat anda mendapatkan halaman *web* dan data yang berhubungan dengan *website* yang anda buat, sehingga data dapat diakses dan dilihat oleh orang lain." [8]

2.3. Manajemen Jaringan

2.3.1. Pembagian *Subnet*

Menurut Winarto dan Zaki (2013:64) "*Subnetting* adalah teknik yang lazim dipakai oleh admin jaringan dengan memanfaatkan 32 bit yang ada di IP address dengan lebih efisien." [13]

Sedangkan menurut Nugroho (2016:51) "*Subnetting* artinya proses dalam membagi wilayah jaringan besar menjadi beberapa wilayah jaringan kecil." [9] Seperti pada kata "*sub-net*" artinya adalah bagian kecil, (*sub*) dari sebuah *network* (alamat jaringan). Dalam membagi wilayah jaringan menjadi beberapa wilayah jaringan kecil, cara yang dilakukan adalah dengan mengubah-ubah parameter pada nilai *subnetmask* yang digunakan. Tujuan dari adanya proses *subnetting* adalah untuk memperbanyak jumlah wilayah jaringan (*network*).

2.3.2. SNMP (*Simple Network Management Protocol*)

Menurut Gitakarma dan Ariawan (2014:132) "SNMP merupakan contoh dari layer 7 aplikasi yang digunakan oleh *network management system* untuk memonitor perangkat jaringan sehingga dapat memberikan informasi yang dibutuhkan bagi pengelolanya." [4]

2.3.3. NAT (*Network Address Translation*)

Menurut Gitakarma dan Ariawan (2014:118) "NAT adalah *protocol* yang menyediakan kemampuan untuk memetakan (mentranslasi) *inside IP address* yang digunakan dalam lingkungan *network local* ke lingkungan *network* luar." [4]

Beberapa keuntungan yang akan didapat dari NAT seperti berikut:

a. Memungkinkan sebuah private IP network untuk menggunakan bob-registered IP address untuk mengakses sebuah outsidenetwork, seperti internet.
b. Menyediakan kemampuan untuk kembali menggunakan *registered IP address* yang telah digunakan di *internet* untuk dipakai di *private network*.
c. Menyediakan koneksi *internet* di *network* yang tidak mempunyai *internet registered IP address* yang cukup.
d. Dapat men-*translate address* di dua *intranet* yang digabung seperti dua perusahaan yang bergabung.

2.4. Konsep Penunjang Usulan

2.4.1. Teknik Pengamanan Jaringan

Untuk mengamankan jaringan wireless dapat menggunakan beberapa model strategi, diantaranya adalah Pemfilteran MAC Address, Kunci Enkripsi WEP dan WPA, mD Filtering, dan penggunaan *Protocol Filtering*.

Menurut Arifin (2008:37) "Pemfilteran MAC *address* merupakan pemfilteran standar 802.11 untuk mengamankan suatu jaringan *wireless*. MAC *address* dari kartu jaringan adalah bilangan *hexadecimal* 12-digit yang unik satu sama lain. Karena masing-masing kartu jaringan *wireless* memiliki MAC *address* nya sendiri, access point dapat membatasi kapasitas pengguna hanya kepada MAC *address*

yang sudah diotorisasikan". [2]

Dalam pengimplementasiannya berbagai macam cara enkripsi yang digunakan untuk mengamankan suatu jaringan wireless diantaranya adalah ;

a. WEP (*Wired Equivalent Privacy*) pada standar 802.11 merupakan enkripsi opsional dan standar otentikasi yang diterapkan pada beberapa WNIC (*Wireless Network Interface Card*) dan didukung oleh beberapa *vendor access point*. WEP bersifat opsional karena standar enkripsi yang telah disetujui di konfigurasi sebelum koneksi pengguna *wireless* ke *access point*. Sesudah pengguna dikonfigurasi pada *access point* dan pengguna, semua komunikasi yang dikirim melalui udara, dienkripsikan sehingga menyediakan koneksi yang aman dan sulit untuk disusupi
b. WPA (*Wi-Fi Protected Access*) menawarkan enkripsi kunci yang dinamis dan otentikasi secara mutual. Beberapa *Vendor* telah mendukung WPA, sehingga mempermudah implementasinya. WPA menyediakan pengaturan dan implementasi yang cukup mudah tanpa melakukan perunbahan yang berarti pada desain hardware WLAN 802.11. Fitur-fitur kemanan yang lebih kuat sangat berhubungan dengan kekuatan pada metode enkripsinya.

2.4.2. WPA RADIUS (*Wireless Protection Autentication Remote Authentication Dial-In User Service*)

Menurut Arif dkk (2007:40) WPA RADIUS merupakan sistem keamanan pada jaringan *wireless* yang cukup terkenal dan banyak di pakai pada jaringan- jaringan internet untuk menghubungkan *client* pada jaringan. [1]

Pengamanan WPA RADIUS memerlukan *point* yang harus dipenuhi oleh administrator yaitu:

a. *Server*: Komputer *server* yang dituju oleh *akses point* yang akan memberi otontikasi kepada *client*. Aplikasi yang biasa digunakan antara lain *free*RADIUS, *open*RADIUS.
b. *Port,* Nomor *port* yang digunakan adalah 1812.
c. *Shared Secret* adalah kunci yang akan dibagikan ke komputer dan juga kepada *client* secara transparan.
d. Sertifikat Autentikasi ialah sertifikat yang dimiliki oleh *client* dan *server* sebagai authentikasi dalam jaringan.

2.4.3. Cloudpath Security and Management Platform

Cloudpath Enrollment System (ES) software "is a security and policy management platform that enables any IT organization to protect the network by easily and definitively securing users and their wired and wireless devices—while freeing those users and IT itself from the tyranny of passwords". [4]

Cloudpath adalah *platform* manajemen keamanan jaringan yang memungkinkan *user* untuk melindungi jaringannya baik jaringan kabel maupun nirkabel, serta mempermudah bagi penggguna dengan meniadakan *password*.

Ada dua komponen utama yang membentuk *Cloudpath*: *Secure Onboarding* and *Advanced Certificate Management*. Kombinasi kedua kemampuan ini memungkinkan cara baru yang kuat dalam mengamankan dan mengelola setiap perangkat yang terhubung ke jaringan, sekaligus membuatnya sangat dapat dipergunakan untuk pengguna akhir dan administrator.

Kombinasi ini memberikan *Automated Device Enablement* (ADE) pada industri.

Kemampuan *onboard* yang aman meliputi:

a. *Self-service automated onboarding* untuk beragam perangkat;
b. Akses BYOD, mitra, dan tamu;
c. Konfigurasi otomatis;
d. Keamanan WPA2-*Enterprise* dengan PEAP atau EAP-TLS;
e. Fleksibelitas pilihan pendaftaran - AD, LDAP, OAuth, Jaringan Sosial;
f. Pilihan sponsor, email, SMS, dan voucher;
g. Membangun *certificate authorities and Microsoft CA integration;*
h. Bekerja dengan infrastruktur Wi-Fi;
i. Otomatisasi sistem AV, firewall, NAC, proxy, dan perangkat lunak instalasi.

Kemampuan Manajemen Sertifikat Lanjutan meliputi:

a. Manajemen sertifikat per-perangkat yang unik;
b. Distribusi sertifikat secara otomatis;
c. Layanan pendaftaran izin dan instalasi;
d. Kebijakan dinamis berdasarkan pengguna, perangkat, kepemilikan (BYOD atau IT-*owned*), kebutuhan akses;

e. Mengelola aktivasi akses dan penghentian berdasarkan status karyawan;
f. Visibilitas ke setiap perangkat yang terhubung ke jaringan, pilihan pendaftaran, susunan faktor dan masa berlaku sertifikat menggunakan laporan otomatis ke dashboard;
g. Kebijakan kontrol perangkat, visibilitas, dan kontrol terhadap penggunaan.

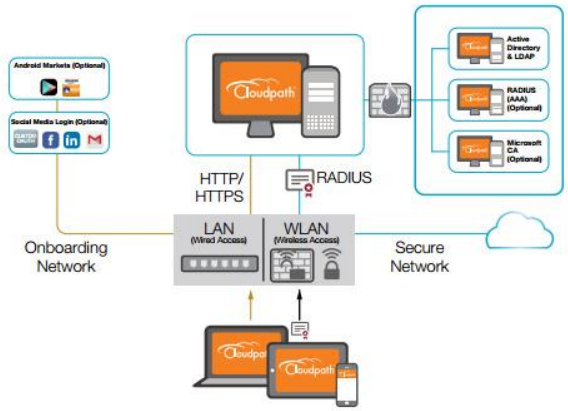
3. METODE PENELITIAN

3.1. Analisa Penelitian

3.1.1. Analisa Kebutuhan

Dalam penelitian ini dibutuhkan beberapa alat pendukung diantaranya:
a. Jaringan LAN;
b. *Server* RADIUS;
c. Software yang mendukung WPA-2 *Enterprise* via X.509 (*Ruckus Cloudpath*);
d. Perangkat *Accsess Point;*
e. DHCP *Server*;
f. Perangkat *End Point* (Laptop, Handhpone, Tablet).

3.1.2. Desain



Gambar 1. Desain Jaringan Internet
(Sumber : Cloudpath Security and Management Platform (commscope.com))

3.1.3. Testing

Testing yang dilakukan yaitu dengan cara percobaan akses dari pengguna untuk masuk ke dalam jaringan dengan metode memasukan akun media sosial, alamat email atau no telepon selular.

3.1.4. Implementasi

Sistem ini akan di jalankan di *Solution Center* PT. Ingran Micro Indonesia, dengan cara mengintegrasikan dengan jaringan di tempat tersebut.

4. HASIL DAN PEMBAHASAN

4.1. Topologi Jaringan

Penulis memberikan usulan Penambahan keamanan tambahan pada system koneksi nirkabel menggunakan sistem kemanan jaringan nirkabel WPA2 enterprised dari yang sebelumnya menggunakan WPA2-PSK yang rawan terhadap kebocoran.

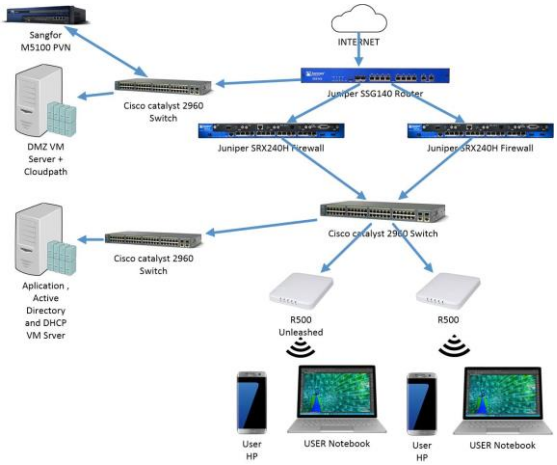
WPA2-PSK yang digunakan adalah *Ruckus Cloudpath Enrolment System* (ES). *CLoudpath ES* adalah platform manajemen keamanan dan kebijakan yang memungkinkan TEAm IT melindungi jaringan dengan mudah dan pasti mengamankan pengguna dan perangkat nirkabel dan kabel mereka - sambil membebaskan pengguna dan TI itu sendiri dari kerepotan memasukan *password*.

Software ini mengkonsolidasikan dan menyederhanakan penyebaran beberapa layanan yang biasanya berbeda dan kompleks untuk dikelola: Manajemen Sertifikat, Manajemen Kebijakan dan Pemberdayaan Perangkat

Ada dua komponen utama yang membentuk *Cloudpath*: *Secure Onboarding* dan *Advanced Certificate Management*. Kombinasi kedua kemampuan ini memungkinkan untuk mengamankan dan mengelola setiap perangkat yang terhubung ke jaringan,

4.2. Skema Jaringan

Adapun skema jaringan yang diusulkan menyesuaikan dengan kebutuhan jaringan usulan yang seperti gambar berikut:



Gambar 2. Skema Jaringan Usulan

Secara keseluruhan, perangkat keras dalam skema jaringan yang diusulkan tetap menggunakan perangkat keras yang ada, dalam hal ini penulis tidak mengubah susunan skema yang sudah berjalan. Adapun perubahan pada skema jaringan hanya terbatas pada penambahan VM Radius *server (Cloudpath ES)* yang akan digunakan sebagai penambahan kemanan pada jaringan nirkabel.

4.3. Keamanan Jaringan

Keamanan jaringan dari sisi *firewall*, *antivirus*, **internet** dan *email* tidak ada perubahan dari kondisi Awal.

4.4. Rancangan Aplikasi

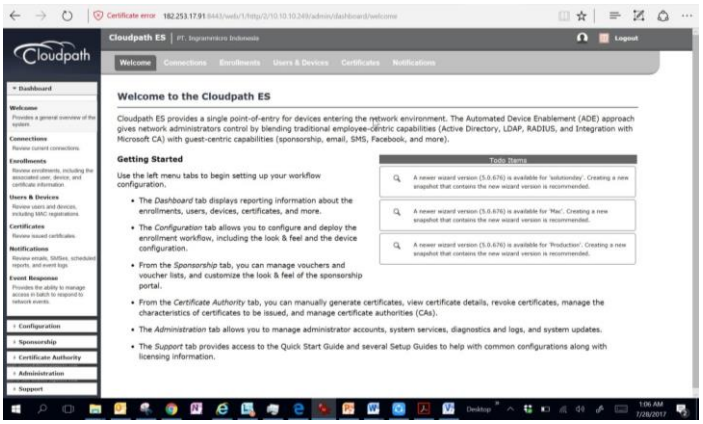
A. **Perancangan Awal**

1. Menjalankan *CLoudpath ES*

Pada perancangan awal ini penulis Menjalankan aplikasi *VM Cloudpath ES* pada *VMWARE* di server DMZ yang sudah tersedia, kemudian membuat IP *address standard* untuk akses lewat jaringan. IP *Address* untuk *server* ini di buat satu segmen dengan *server* lain yaitu 10.10.10.249.

2. Membuat akun Admin

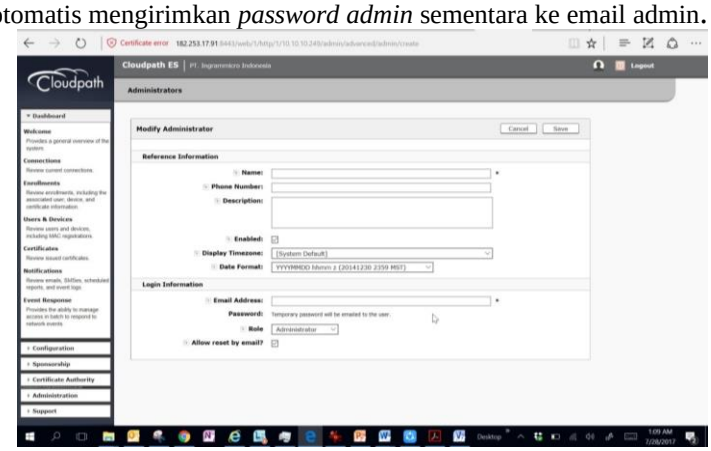
Setelah IP *Address* di buat, *Server* dapat dijalankan dari PC atau Laptop dengan memasukan alamat IP yang kita berikan ditambahkan dengan "admin", dengan ini kita akan memasukan 10.10.10.249/admin di *browser* yang ada di laptop dalam jaringan dan segment yang sama dengan *Server cloudpath.* Akan tampil antar muka seperti dibawah



Gambar 3. Tampilan *Cloudpath*

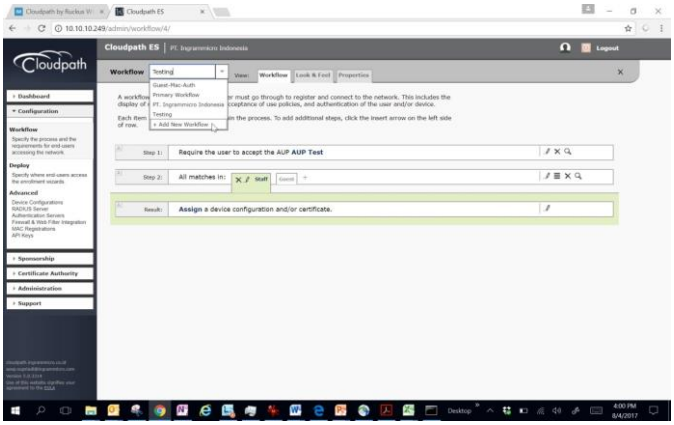
Kemudian masuk ke menu *Administration-Administrators-Add Admin*

Kemudian isi dengan lengkap semua kolom yang ada dan di save. Setelah disimpan maka sistem akan secara otomatis mengirimkan *password admin* sementara ke email admin.



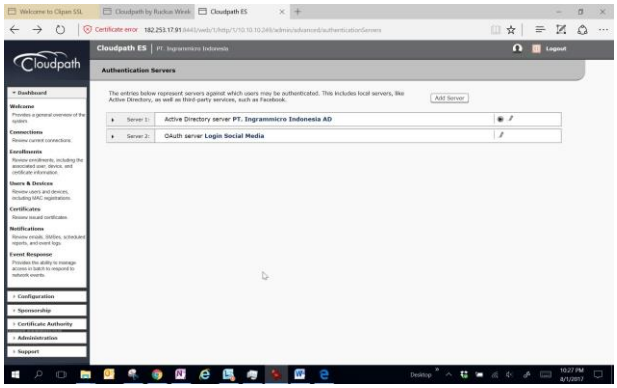
Gambar 4. Tampilan Administrasi

3. Membuat *captive portal* atau tampilan halaman awal.
Setelah membuat *password admin* silahkan *logout* dan *login* kembali dengan *password admin* yang kita buat. Proses pembuatan *captive portal* dengan cara masuk ke menu *Configuration-Workflow-add new workflow.*

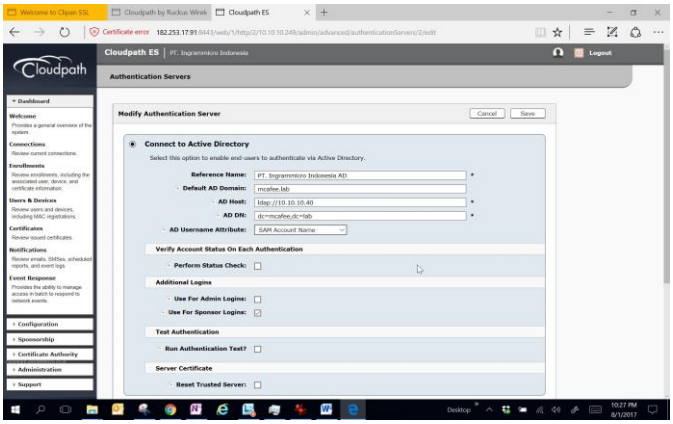


Gambar 5. Tampilan *Captive Portal*

B. Melakukan integrasi *server active directory* ke dalam sistem *Cloudpath ES*
Langkah selanjutnya yang harus dilakukan adalah memasukan *server active directory* agar karyawan bisa akses kedalam *cloudpath* tanpa harus memasukan *password* setiap kali masuk. Dalam menu *configuration- advanced- authentication server*, masukan nama *server active directory* yang kita punya.

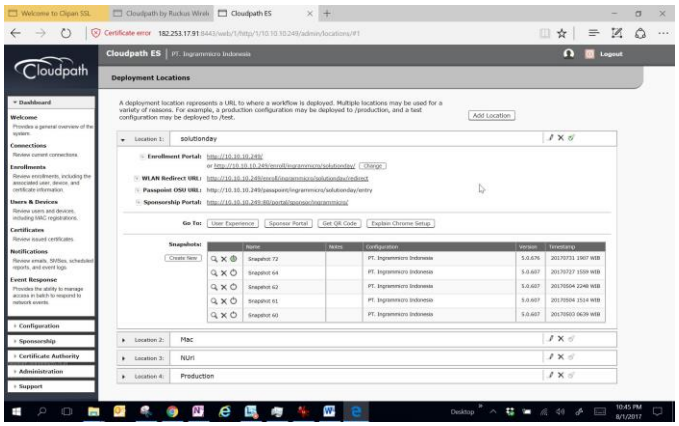


Gambar 6. Tampilan *Authentifiction Servers*



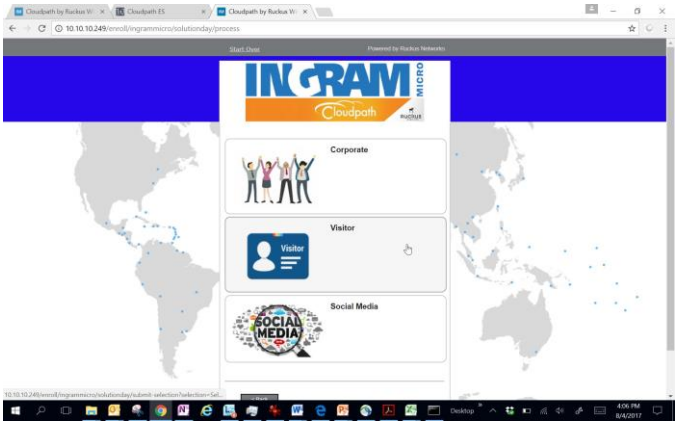
Ganmbar 7. Tampilan Modifikasi *Authentifiction Servers*

1. Melakukan tes tampilan dan sistem
   Sebelum di integrasikan dengan *system access point*, tampilan harus di tes dulu tampilannya secara lokal. Caranya dengan mengakses *configuration –deploy-user experience.*



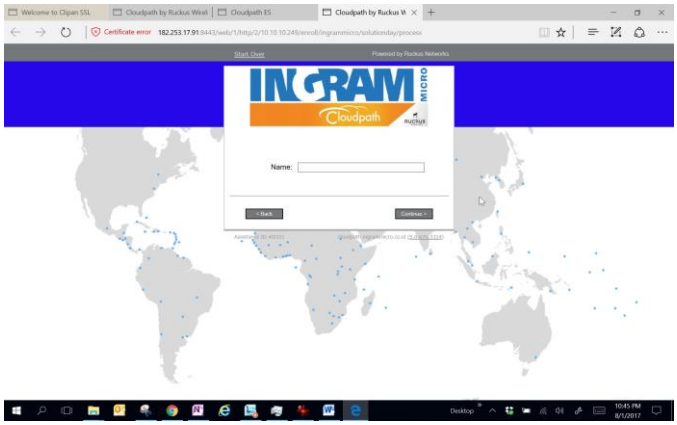
Gambar 8. Tampilan *Deployment Location*

Gambar 9. Tampilan Akses Welcome

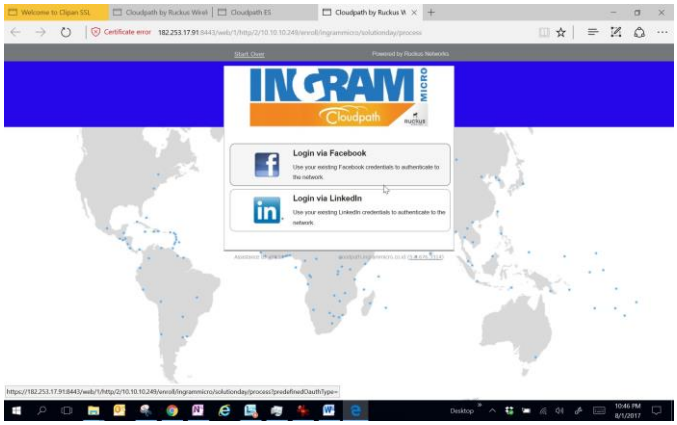


Gambar 10. Tampilan Pilihan Akses

Gambar 11. Tampilan Akses Masuk

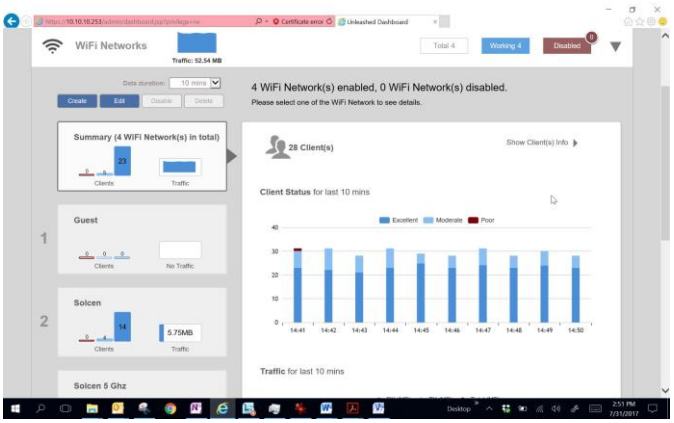


Gambar 12. Tampilan Pengguna

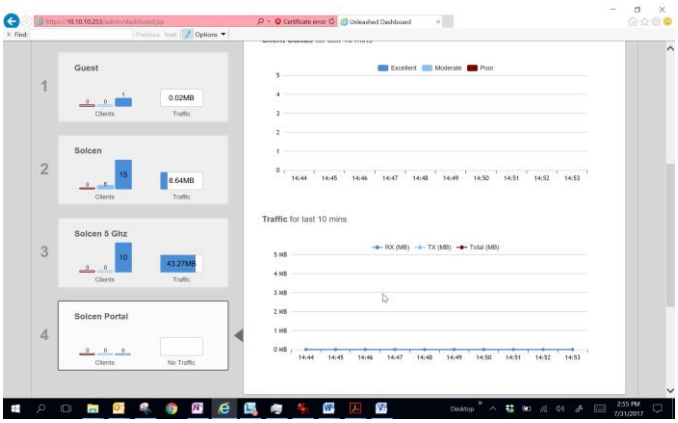


Gambar 13. Tampilan Pilihan

2. Melakukan Integrasi sistem *cloudpath* dengan *Acesss Point*
   Untuk melakukan integrasi Sistem *cloudpath* harus dilakukan pada antar muka *Unleashed Ruckus Access point conroler*, agar mengarahkan sistem koneksi melewati *server Cloudpath* sebelum masuk kedalam jaringan.
3. Membuat SSID baru
   Agar tidak menggangu sistem jaringan yang sudah ada maka kita akan membuat SSID baru pada Sistem *access point* yang ada. Caranya pada *menu* utama klik *access point-create*- masukan nama *access point* nya kemudia *save*. Pada kali ini diberi nama *solcen portal* untuk SSID yang baru ini.

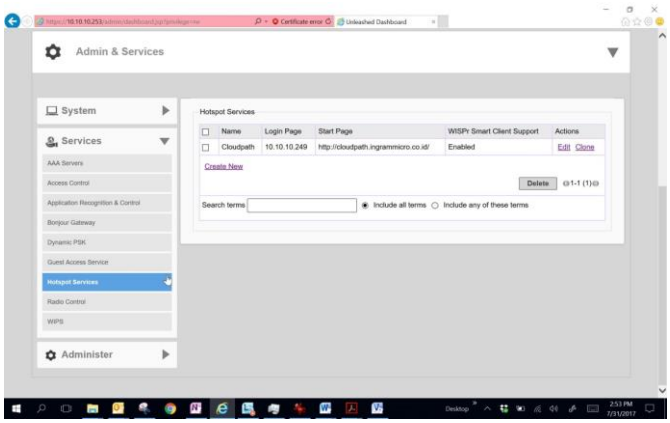


Gambar 14. Pemberian Nama *Solcen Portal* pada SSID



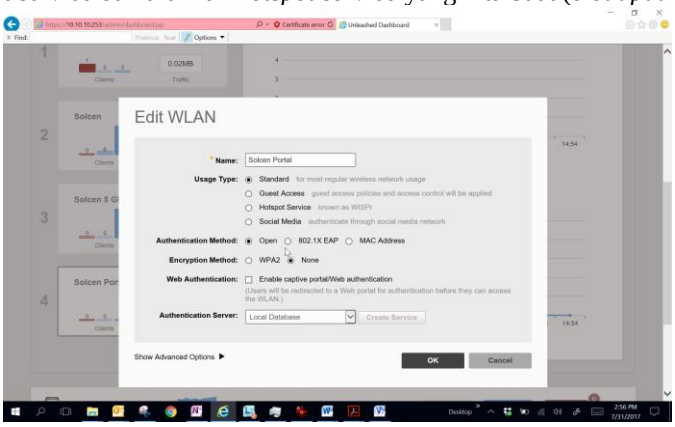
Gambar 15. Tampilan Mionitoring pada *Solcen Portal*

4. Mengintegrasikan SSID dengan *Cloudpath*
   Setelah SSID baru dibuat maka tahap yang kita lakukan selanjutnya adalah mengarahkan semua *user* yang terkoneksi dengan SSID tersebut masuk kedalam *server cloudpath*.
   Pada tahap awal masukan *IP server CLoudpath* kedalam sistem, *Ruckus unleashed access point*, dengan cara *pada menu admin&service-Services –Hotspot Servic*es.
   Pilih *create new* dan buat nama *Services* nya (*Cloudpath*) kemudian masukan IP dan *Start page cloudpath server*.

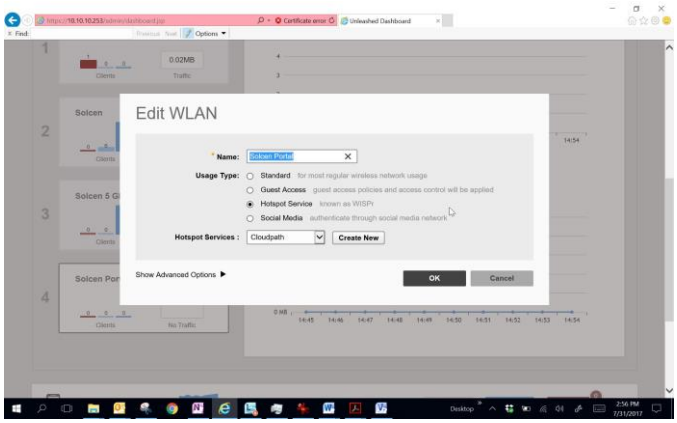


Gambar 16. Tampilan Integrasi SSID dengan *Cloudpath*

5. Tahap selanjutnya pada *Page Solcen Portal* (SSID yang baru) ubah *setting* nya dari *Standard Type* menjadi *Hotspot service* dan arahkan *hotspot service* yang kita buat (*cloudpath*).



Gambar 17. Tampilan Edit WLAN



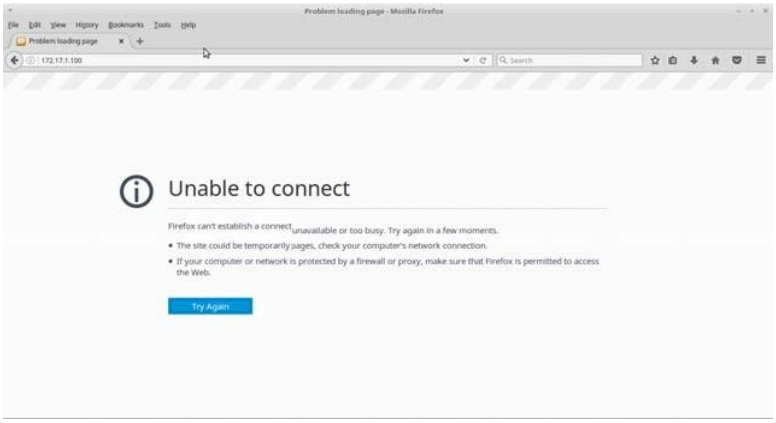
Gambar 18. Tampilan Edit WLAN Lanjutan

C. Pengujian Jaringan

Tujuan dari adanya pengujian jaringan awal dan pengujian jaringan akhir ini adalah untuk melihat perbedaan system koneksi yang menggunakan WPA2-*shared key standard* yang sebelumnya digunakan dengan WPA2-*Enterprise* yang kita gunakan sekarang.

1. Pengujian Jaringan Awal

Menggunakan WPA2-*Preshared key*

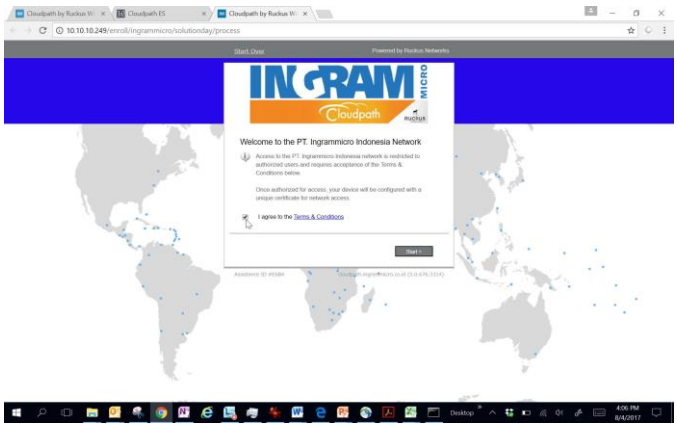


Gambar 19. Tampilan *User* gagal mengakses layanan *web* pada saat terjadi masalah.

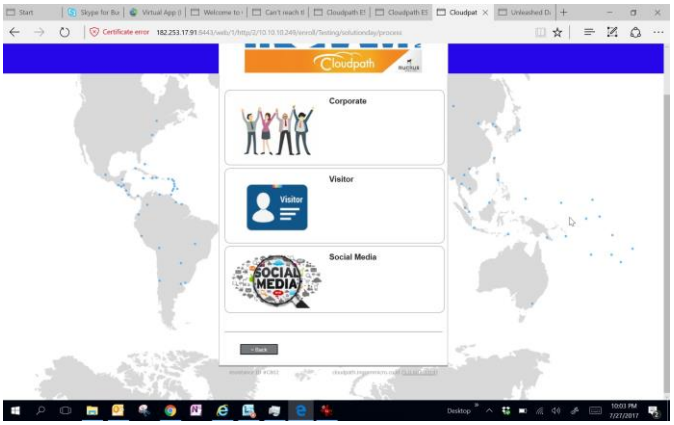
2. Pengujian Jaringan Akhir

a. Tampilan awal.

Menggunakan WPA2-*Preshared key*, setelah *User* masuk ke dalam SSID *Solcen Portal*, *User* langsung diarahkan ke *server* Cloudpath 10.10.10.249

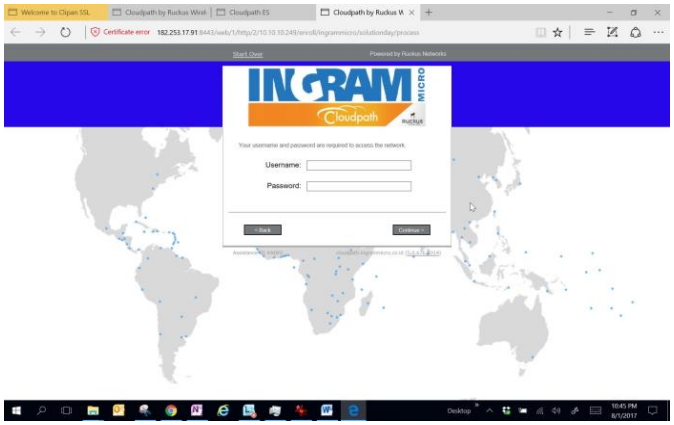


Gambar 20. Tampilan User yang sudah menggunakan Setingan Baru



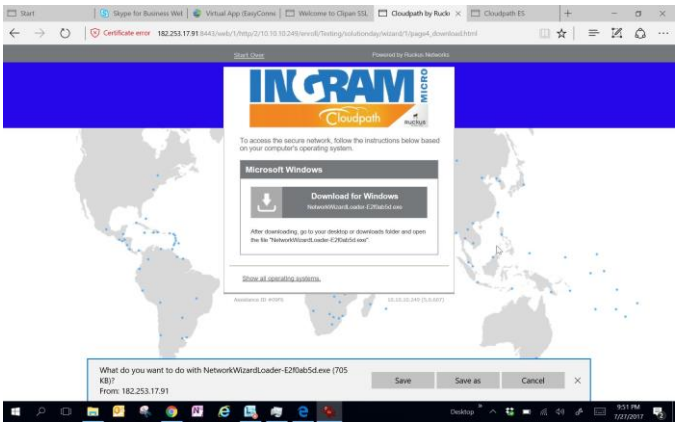
Gambar 21. Tampilan Pilihan untuk *User* yang sudah menggunakan Setingan Baru

b. Masuk dengan *Active directory*
Masuk dengan memilih *corporate*, kemuadian masukan *username* dan *password* yang sudah di daftarkan di *Active directory*



Gambar 22. Tampilan Akses Masuk *User* dengan *Active Directoery*

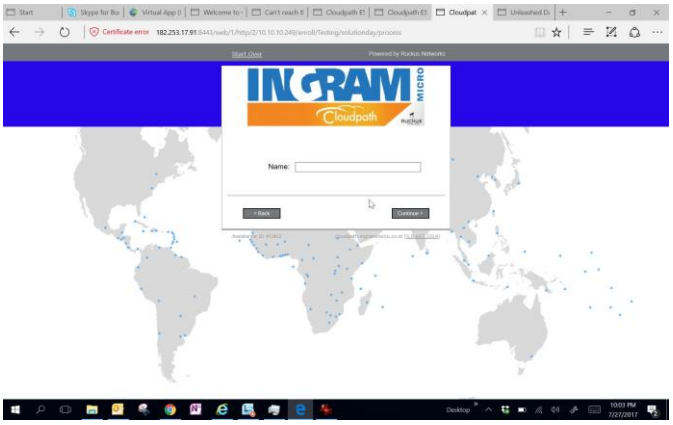
Setelah berhasil masuk, maka sistem akan meminta perangkat untuk meng *install certificate*, agar pada sesi berikutnya perangkat tersebut tidak perlu memasukan password kembali.



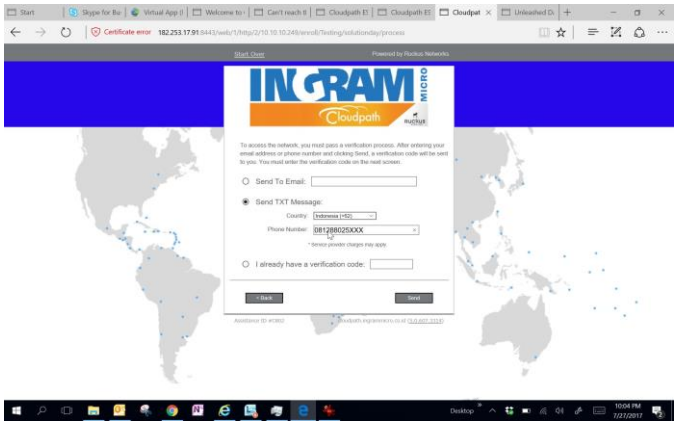
Gambar 23. Tampilan Akses Permohonan Sertifikat

c. Masuk sebagai *visitor* dengan alamat *email* atau SMS

Masuk dengan memilih *Visitor*, kemuadian masukan nama, pilih cara masuknya, mau mengunakan *Email* atau SMS, jika menggunakan *email* masukan alamat *email* kita kemudian secara otomatis sistem akan mengirimkan email code konfirmasi kepada kita.
jika menggunakan SMS, masukan no *Telephone* genggam milik *user* dan sistem akan mengirimkan SMS berisi kode konfirmasi yang harus kita masukan ke sistem setelah mendapat kode konfirmasi kemudian kita masukan data tersebut ke system.

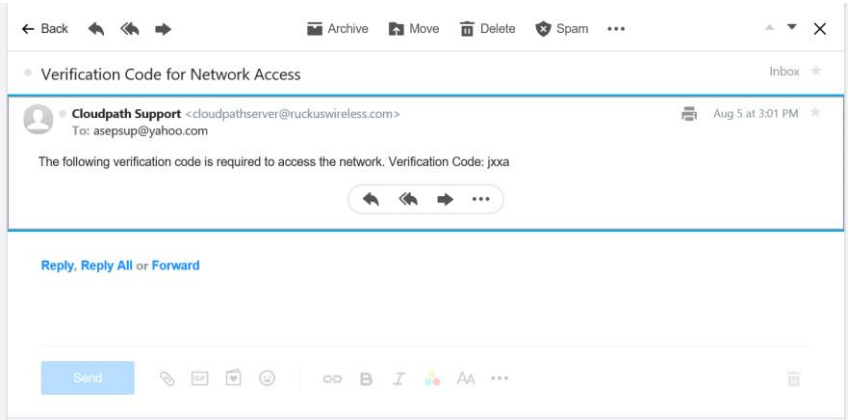


Gambar 24. Tampilan Akses bagi Pengunjung



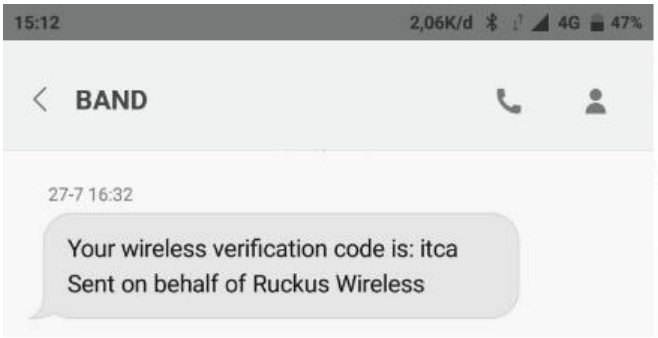
Gambar 25. Tampilan Akses dengan Konfimrasi Kode

Jika mengunakan email akan mendapat balasan seperti dibawah



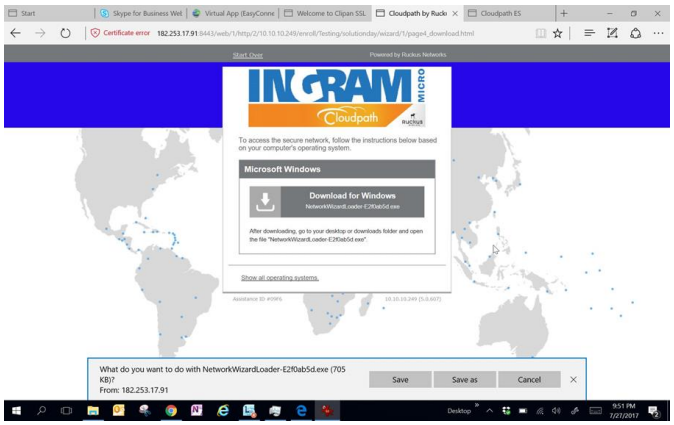
Gambar 26. Tamnpilan Informasi Balasan *via Email*

Jika menggunakan SMS akan mendapatkan pesan seperti dibawah

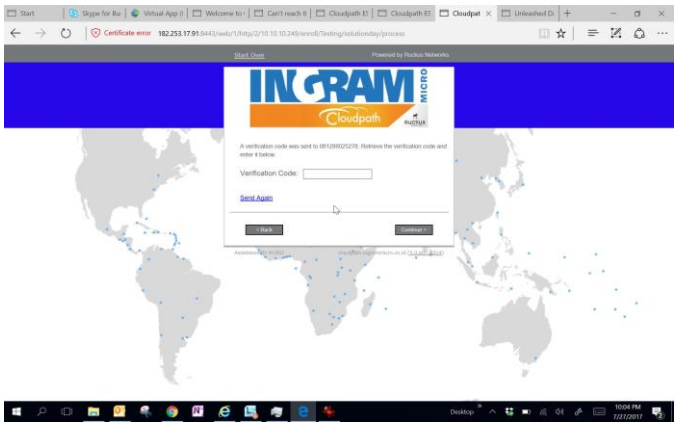


Gambar 27. Tampilan Informasi Balasan Via SMS

Masukan kodenya kedalam sistem



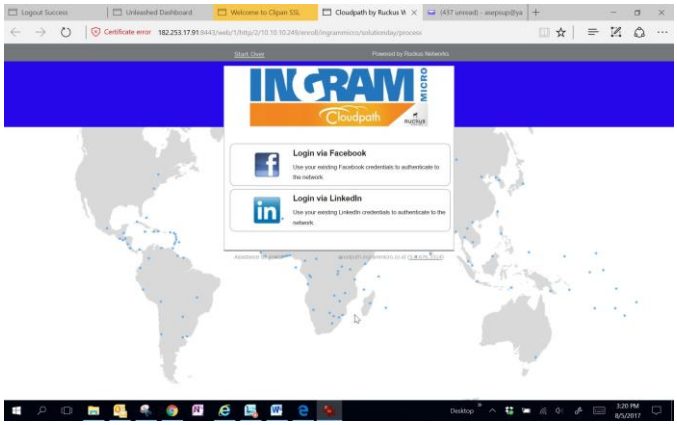
Gambar 28. Tampilan Perintah dari email atau SMS



Gambar 29. Tampilan Permintaasn Kode

Setelah berhasil masuk, maka sistem akan meminta perangkat untuk men *download* dan meng *install certificate* yang di *generate* oleh sistem.
Setelah *certificate* berjalan kita bisa langsung bisa berhubungan dengan koneksi di dalam jaringan.

d. koneksi dengan Sosial Media
Pilih menu sosial media, kemudian masukan sosial media yang kita miliki, masuk menggunakan *account* sosial media, kemudian langsung masuk



Gambar 30. Tamnpilan yang sudah Terhubung dan bisa Mengkses Sosial Media

5. KESIMPULAN DAN SARAN

Berdasarkan pembahasan pada bab-bab sebelumnya, maka dapat diambil beberapa kesimpulan, sebagai berikut:

1. Penggunaan system penggunaan WPA2-*Preshared Key* memungkinkan terjadinya kebocoran pada jaringan dengan bocornya *password* yang digunakan untuk masuk kedalam jaringan tersebut.
2. Untuk menghindari kebocoran jaringan dengan karena kebocoran *password* dapat diatasi dengan WPA2-*Enterprised* yang dapat melakukan pengelolaan dan pembatasan lebih baik terhadap perangkat yang dapat masuk kedalam jaringan.
3. *Ruckus Cloudpath* ES adalah salah satu sistem pengelolaan pengamanan jaringan nirkabel WPA2-*Enterprised* yang menggabungkan antara *Radius server*, *Active Directory* dan *Cloud server ruckus* untuk memberikan *activation code* kepada *user* yang menggunakan *Email* atau SMS.

Berdasarkan kesimnpulan tersebut, maka beberapa saran untuk pengembangan selanjutnya, antara lain:

1. WPA2-*Enterprised* adalah sistem pengelolaan yang digunakan hanya masuk masuk kedalam jaringan dengan menggunakan sistem nirkabel. Oleh sebab itu selain penggunaan sistem WPA2-*Enterprised* ini, harus ditambah juga sistem keamanan di dalam jaringan dengan *Antivirus* dan pengelolaan *User* yang lebih baik.
2. *Ruckus Cloudpath* ES adalah WPA2-*Enterprised* yang cukup mahal. Oleh karena hal tersebut Sistem tidak cocok jika digunakan untuk Perusahaan kecil atau *system network* yang tidak terlalu membutuhkan keamanan tinggi.
3. Jika perusahaan kecil ingin menggunakan WPA2-*Enterprised*, bisa dimulai dengan menggunakan *Server Radius* gratis yang disediakan *operating system Linux* yang mendukung EAP-TLS (*Extensible Authentication Protocol – Transport layer Security*)**.**

DAFTAR PUSTAKA

[1] Arif, T. Y., Syahrial, Zulkiram, (2007). Studi Protokol Autentikasi pada Layanan Internet Service Provider (ISP), Jurnal Rekayasa Elektrika, Vol. 6, No.1,

[2] Arifin, Z., Prabawati, A., (2008). Sistem Pengamanan Jaringan Wireless LAN Berbasis pada Protokol 802.1X & Sertifikat, Yogyakarta : Andi Offset.

[3] Gitakarma, M. S., Ariawan, K. U., (2014). Jaringan Komputer. Yogyakarta: Graha Ilmu.

[4] Juliharta, I. G. P. K., Supedana, W., Hostiadi, D. P., (2015). *High Availability Web Server* Berbasis *Open Source*. SEMNASTEKNOMEDIA, Vol. 3, No. 1, 31 – 36.

[5] Khairil, K., Riyanto, N. P., Rosmeri, R., (2013) MEMBANGUN WEBSERVER INTRANET DENGAN LINUX (Studi Kasus di Laboratorium Komputer SMP Negeri 38 Seluma Bengkulu Selatan), Jurnal Media Infotama, Vol. 9 No. 1, 1 – 24.

[6] Moniruzzaman, A. B. M., Waliullah, Rahman, S., (2014). *A High Availability Clusters Model*

Combined with Load Balancing and Shared Storage Technologies for Web Servers, International Journal of Scientific & Engineering Research, Vol. 5, Issue. 12.

[7] Nandari, B. A., Sukadi. (2014). Pembuatan *Website* Portal Berita Desa Jetis Lor, ijns.org, Vol. 3, No. 3. 43 – 47.

[8] Nugroho, K., (2016). Jaringan Komputer Menggunakan Pendekatan Praktis. Kebumen : Mediatera.

[9] Pribadi, P. T., (2013). Implementasi *High Availability VPN Client* pada Jaringan Komputer Fakultas Hukum Universitas Udayana, Jurnal Ilmu Komputer, Vol. 6, No. 1, 17 – 24.

[10] Sadikin, Nanang. (2015), Implementasi Keamanan Jaringan Wireless Enterprise Menggunakan Remote Authentification Dial in User Servicess, SEMNASTEKNOMEDIA, Vol. 3, No. 1, 7 – 12.

[11] Tenggario, R. P. Lukas, J. (2011) Manajemen Jaringan Wireless Menggunakan Server Radius, Jurnal Teknik Komputer, Universitas Binus. Vol. 19, No. 1, 80 – 87.

[12] Winarno, E., Zaki, A., SmitDev Community, (2013), Buku Sakti Pemrograman, Jakarta : Gramedia.