IMPLEMENTASI *AAA* MENGGUNAKAN *RADIUS SEVER* PADA JARINGAN *VPN* (STUDY KASUS : PT. FORUM AGRO SUKSES TIMUR)

[1] Muhammad Zia Ul Haq (1310652015), [2] Taufiq Timur W., S.Kom., M.Kom., [3] Yulio Rahmadi., S.Kom., Jurusan Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jember

Email : siga_2@yahoo.com

ABSTRAK

Authentication, authorizing and accounting (AAA) adalah mekanisme verfikasi data pengguna yang berkaitan dengan user dan password, pemberian hak akses pada pengguna yang terverifikasi, dan pencatatan aktifitas pengguna terkain dengan alur data yang melewati sistem. Mekanisme tersebut telah banyak disediakan pada *protocol-protokol server* seperti *proxy* dan juga *protocol radius* yang memang khusus dibangun untuk memberikan service-service tersebut

VPN adalah mekanisme tunneling yang bersifat *private* karena mekanisme dari *VPN* adalah membuat *interface virtual* yang bersifat *private* yang tercipta dari *interface* fisik. Dengan memanfaatkan teknologi *VPN* ini maka bisa membuat suatu network local antaran 2 network yang berbeda yang bersifat private karena terhubung melalui tunneling *VPN*, sehingga monitoring dan management user dapat dilakukan secara terpusat.

Berdasarakan pengujian *centralisasi* mekanisme *authentication, authorizing and accounting* yang dilakukan, proses management otentikasi dapat dilakukan secara terpusat pada *radius server* dengan memanfaatkan teknologi *VPN* sebagai media untuk menghubungkan 2 *network* yang berbeda namun untuk *authorizing* masih dilakukan dimasing-masing *hotspot server*.

Kata kunci:*, Radius Server, Authentication, authorizing and accounting, VPN*

PENDAHULUAN

Teknologi internet saat ini semakin banyakn dan tidak terkontrol. Hal ini disebakan karena semakin banyaknnya pengguna akses internetnet di dunia. Dan dewasa ini hampir semua lapisan masyarakat mengetahui tentang adanya internet dan cara mengakses internet. Bahkan saat ini sudah banyak instansi-instansi memanfaatkan teknologi wireless untuk mengkoneksikan antara cabang. Hal ini membuat seorang administrator jarigan berfikir bagaiamana membangun sebuah koneksi yang bersifat secure dan private dengan memanfaatkan tunneling VPN dengan management pengguna menggunakan radius server

Radius server memberikan fungsi AAA (Authentication, Authorization, dan Accounting). Dengan ini seorang administrator jaringan mampu menambah sekuritas pada layanan internet karena setiap user yang akan berhubungan dengan *NAS (Network Access Server)* akan di tahan oleh *Radius Server* dan melakukan autentikasi. Radius juga memaksimalkan performance dari jaringan dengan meanfaatkan fungsi *Accounting* dengan cara menyimpan log aktifitas setiap user, sehingga seorang administrator jaringan mampu mengambil keputusan hak akses yang perlu diberikan kepada setiap users selain itu juga server *AAA* juga dapat memberikan fungsi *Authorize* yang mana seorang administrator mampu memberikan hak akses dan kewenangan pada setiap users yang ada, sehingga Acces *user* atau *client* dapat dibatasi oleh administrator jaringan. Sedangkan VPN Server dalam hal ini adalah sebagai tunneling antara kantor A dan kantor B yang nantinya di intregrasikan dengan *radius server* yang bertindak sebagai server *AAA* yang terintregasi dengan *UAM server* portal akses user terhadap internet.

PT. Forum Agro Sukses Timur merupakan perusahaan retail yang bergerak di bidang kebutuhan pertanian, dan saat ini sudah memiliki banyak cabang di seluruh daerah jawa timur. Dan penggunaan akses internet pada kantor pusat sendiri sudah memilki 80 client lebih yang mana terpisah menjadi 2 gedung. Sehingga dieperlukan management dengan memanfaatkan fungsi *Authentikasi* dan *Authorisasi* users pada server *AAA* dengan membuat koneksi tunneling antara Gedung A danGedung B.

Berdasarkan uraian diatas, penulis berkeinginan untuk membuat suatu implementasi *server AAA* menggunkan *radius server* pada jaringan *VPN* yang menghubungakan Jaringan pada Kantor A dan Jaringan pada kantor B. Sehingga akses user pada *internet* terauthentikas pada satu *UAM server* sebagai QoS klien dan Server *AAA* sebagai managemen *AAA* dengan membuat tunneling VPN, sehingga gedung B tersebut dapat terkoneksi ke internet melalui tunneling VPN.

TINJAUAN PUSTAKA

RADIUS

RADIUS menjalankan sistem administrasi pengguna yang terpusat, sistem ini akan mempermudah tugas administrator (Brislian, 2011). Dapat kita bayangkan berapa banyak jumlah pelanggan yang dimiliki oleh sebuah ISP, dan ditambah lagi dengan penambahan pelanggan baru dan penghapusan pelanggan yang sudah tidak lagi berlangganan lagi. Apabila tida ada suatu sistem administrasi yang terpusat, maka akan merepotkan administrator dan tidak menutup kemungkinan ISP akan merugi atau pendapatanya berkurang. Dengan sistem ini pengguna dapat menggunakan hotspot di tempat yang berbeda - beda dengan melakukan autentikasi ke sebuah RADIUS server.

Remote Access dial in user service (RADIUS), awalnya dikembangkan oleh Livingston Enterprise, adalah protocol *access-control* yang memverifikasi dan mengotentikasi pengguna yang umunya berdasarkan pada metode *challenge/response.* Sementara RADIUS memiliki tempat yang menonjol diantara penyedia layanan internet, hal itu juga termasuk dalam lingkungan di mana otentikasi terpusat, pengatur otorisasi, dan rincian *accounting* user, baik yang diperlukan atau diinginkan. Beberapa fitur key dari RADIUS adalah :

1. *Model Client/Server*

Sebuah *Network Access Server* (NAS) beroperasi sebagai RADIUS klien. Klien bertanggung jawab untuk menyampaikan informasi pengguna ke RADIUS serber yang ditunjuk, dan kemudian bekerja untuk mengembalikan respon.

RADIUS server bertanggung jawab untuk menerima permintaan koneksi pengguna, melakukan otentikasi pengguna, dan kemudian mengembalikan semua informasi konfigurasi yang diperlukan bagi klien untuk memberikan layanan kepada pengguna.

2. *Network Security*

Transaksi antara klien dan RADIUS server dikonfirmasi melalui pengunaan *shared secret,* yang tidak pernah dikirim melalui jaringan. Selain itu, setiap pengguna akan mengirimkan *password* yang telah dienkripsi antara klien dan RADIUS server, untuk menghilangkan kemungkinan bahwa seseorang mengintip di satu jaringan yang tidak aman dapat dengan menentukan password penggunanya.

3. *Flexible Authentication Mechanism*

RADIUS server dapat mendukung berbagai metode untuk otentikasi pengguna. Ketika disediakan dengan *username* dan *password* asli yang diberikan oleh pengguna, dapat mendukung PPP PAP atau CHAP, UNIX login, dan mekanisme otentikas lainnya

4. *Extensible Protocol*

Semua transaksi yang terdiri dari panjang variable-Length-Value 3-tuples. Nilai atribut baru dapat ditambahkan tanpa mengganggu implementasi protocol yang ada.

Pada awal pengembanganya, RADIUS menggunakan port 1645, yang ternyata bentrok dengan layanan “datametrics”. Sekarang, *port* yang dipakai RADIUS adalah *port* 1812.

Gambar 2.1 *Hardware Emulation*
(Source: IBM, 2006)

1. *Full Virtualization*

Full virtualization atau sering dikenal dengan *native virtualization* menggunakan sebuah *virtual machine* yang menghubungkan sistem operasi *guest* dengan *hardware native*. Beberapa instruksi terproteksi harus ditangkap dan ditangani dalam *hypervisor* karena *hardware* di bawahnya tidak dimiliki oleh sistem operasi *guest* melainkan dipakai bersama melalui *hypervisor*.

Full virtualization lebih cepat daripada *hardware emulation*, tapi kinerjanya masih kalah bila dibandingkan dengan akses langsung ke *hardware* karena adanya mediasi *hypervisor*. Keuntungan terbesar dari *full virtualization* adalah sebuah sistem operasi dapat dijalankan tanpa modifikasi. Satu-satunya batasan adalah sistem operasi harus mendukung *hardware* yang dipakai (misalnya, *PowerPC*).

Gambar 2.1 *Struktur Paket Data Radius*

FREERADIUS

Alasan utama kenapa memilih freeradius server adalah karena mahalnya harga RADIUS server komersial. Sebagai contoh : Interlink's secure.XS harganya mulai dari $2375 untuk 250 pengguna, Funk Odyssey server $2500, VOP Radius Small Business mulai dari $995 untuk 100 pengguna. Harga RADIUS server komersial diatas kebanyakan tidak terjangkau oleh pemilik hotspot ataupun perkantoran

Salah satu contoh RADIUS server yang non-komersial adalah freeradius server. *Free radius* server ini tidak kalah dengan RADIUS server komersial. Salah satu buktinya adalah freeradius server sudah mendukung beberapa *Access Point* (AP) / *Network Access Server* (NAS) :

1. 3com/USR Hiper Arc Total Control
2. 3com/USR netserver
3. 3com/USER TotalControl
4. Ascend Mas 4000 family
5. Cisco PortSlave
6. Cisron PortSlave
7. Computone PowerRack
8. Cyclades PathRAS
9. Livingston PortMaster
10. Multitech Commplete Server
11. Patton 2800 family

Freeradius dapat berjalan di berbagai sistem operasi, misalnya linux, FreeBSD, OpenBSD, OSF. Selain itu freeradius, ada beberapa RADIUS server non-komersial yang lain diantaranya adalah :

1. **Cistron RADIUS Server** dibuat oleh Miguel van Smoorenburg. Merupakan *free software* (dibawah lisensi GNU GPL). Cistron RADIUS dapat diperoleh di ftp://ftp.radius.cistron.nl/pub/radius dan http://www.radius.cistron.nl
2. **ICRADIUS** merupakan varian dari Cistron. Icradius menggunakan MySQL untuk menyimpan database nama-pengguna beserta *password.* Icradius sudah berbasis web, hal ini akan memudahkan administrator untuk mengelola server ini
3. **XtRADIUS** adalah freeware RADIUS server yang berbasiskan pada Cistron RADIUS server. Perbedaan utama antara Xtradius dengan RADIUS server yang lain adalah kita dapat mengeksekusi *skript* untuk menangani autentikasi
4. **Open RADIUS** server dapat berjalan di beberapa sistem operasi unix. OpenRADIUS juga merupakan *freesoftware,* bebas digunakan tanpa harus bayar, pengguna dapat melakukan modifikasi apabila dianggap perlu.
5. **YARD RADIUS** adalah singkatan dari *Yet Another Radius Daemon* RADIUS. Tulisanya yardradius, tetapi membacanya Y-A-R-D RADIUS. YARDRADIUS merupakan *freeware* yang berasal dari *open source* Livinston RADIUS Server 2.1.

6. **JRadius** Merupakan java plug-in untuk FreeRADIUS.

AAA (Authentication, Authorization, and Accounting)

1. Authentication

Authentication merupakan suatu proses untuk memverifikasi identitasi yang digunakan oleh pengguna (atau mesin) untuk kedalam suatu sistem atau service. Menggunakan kombinasi dari ID dan password (Brislian, 2011). Seperti yang kita ketahui bahwa password tersebut dapat diketahui oleh orang lain, maka hal tersebut akan menghancurkan metode authentication dimana seseorang yang tidak berhak dapat masuk kedalam suatu sistem. Dalam situs e-commerce dan situs-situs internet bisnis lainnya, membutuhkan authenticaticator yang lebih kuat dan lebih dapat dipercaya. Sertifikasi secara digital merupakan salah satu solusinya, dan mungkin 5 sampai 10 tahun mendatang sertifikasi secara digital akan menjadi dari *Public Key infrastructure* (PKI) yang akan menjadi rekomendasi *authenticator* di internet. Proses authentikasi diperlukan ketika kita mempunya kebutuhan untuk mebatasi siapa saja yang diperbolehkan masuk ke dalam jaringan remote access milik anda. Untuk memenuhi kebutuhan tersebut, pengguna yang ingin mengakses sebuah jaringan secara remote harus diidentifikasi terlebih dahulu. Pengguna yang ingin masuk kedalam jaringan pribadi tersebut perlu diketahui dahulu sebelum bebas mengkases jaringan tersebut. Pengenalan ini bertujuan untuk mengetahui apakah pengguna tersebut berhak atau tidak untuk mengakses jaringan.

Analogi sederhananya adalah seperti rumah anda. Apabila ada orang yang ingin berkunjung ke rumah anda, yang pertama kali dilakukan oleh pemilik rumahnya adalah mengidentifikasi siapa yang ingin datang dan masuk ke dalamnya. Jika anda tidak mengenal orang tersebut, bisa saja anda tolak permintaanya untuk masuk kerumah kita. Namun lain halnya ketika sudah kita kenal, maka anda mungkin akan langsung mempersilahkanya masuk. Demikian juga dengan apa yand dilakukan oleh perangakat *remote access* terhadapa user yang ingin bergabung ke dalam jaringan di belakangnya.

Pada umumnya, perangkat *remote access* telah dilengkapi dengan sebuah daftar yang berisikan siapa – siapa saja yang berhak masuk kejaringan di belakangnya. Metode yang paling umum digunakan untuk mengenali perngakses jaringan adalah login dan password. Metode ini juga didukung oleh banyak komponen lainnya, seperti metode *challenge* dan *response, messaging support,* dan *enskripsi*, tergantung pada protocol sekuriti apa yang anda gunakan,

2. Authorization (Otorisasi)

Authorization meliputi penggunaan aturan yang memutuskan apa yang dapat dilakukan oleh pengguna yang telah di authentikasi dalam suatu system (Brislian, 2011). Sebagai contoh, dalam kasus *ISP, ISP* memutuskan apakah akan memberikan alamat *IP Static* atau alamat *IP* dari hasil *DHCP*. Seorang sistem administrator yang harus mendefiniskan peraturan ini. Proses otorisasi merupakan langkah selanjutnya setelah proses otentikasi berhasil. Ketika pengguna yang ingin megakses jaringan anda telah dikenali dan termsuk dalam daftar yang diperbolehkan membuka akses, langkah berikutnya anda harus memberikan hak – hak apa saja yang akan diterima oleh pengguna tersebut.

Analogi dari proses ini dapat dimisalkan seperti perarutan-peraturan yang tertulis dikantor atau rumah kita. Isi dari peraturan tersebut biasanya akan membatasi para pengunjung agar mereka tidak dapat dengan bebas berkliling dirumah kita, tentu ada bagian yang privasi di rumah anda, bukan ? misalnya setiap pengunjung harus membuka alas kakinya ketika memasuki ruangan ibadah dan lain-lain yang membatasi setiap tamu di rumah anda.

Semua itu merupakan peraturan yang dapat dengan bebas anda buat di rumah anda. Begitu juga dengan apa yang terjadi pada proses pengamanan jaringan *remote access*. Perlu sekali adanya batasan untuk para pengguna jaringan remote karena kita tidak akan pernah tahu siapa yang inging masuk ke dalam jaringan kita tersebut, meskipun telah teridentifikasi dengan benar. Bisa saja orang lain yang tidak berhak menggunakan *username* dan *password* yang bukan miliknya untuk mendapatkan akses ke jaringan anda.bagaimana untuk membatasi masing – masing pengguna tersebut ?, banyak sekali metode untuk melakukan pembatasan ini, namun yang paling umum digunakan adalah dengan menggunakan seperangkat atribut khusus yang dirangkai untuk menghasilkan *policy* tenteng hak – hak apa saya yand dapat dilakukan si user. Atribut – atribut ini kemudian dibandingkan dengan apa yang dicatat dalah database

Setelah dibandingkan dalam informasi yang ada didatabase, hasilnya akan dikembalikan lagi kepada fasilitas *AAA* yang berjalan pada perangkat tersebut. Berdasarkan hasil ini. Perangkat *remote access* akan memberikan apa yang menjadi hak dari si pengguna tersebut. Apa saya yang bisa dilakukan dan apa saja yang dilarang sudah berlaku dalam tahap ini.

Proses otorisasi biasanya dilakuakn dalam banyak cara. Bisa dilakukan dengan cara one-time otorisasi yang memberikan seluruh hak dari si user hanya dengan satu kali proses otorisasi. Atau bisa juga dilakukan per service otorisasi yang membuat pengguna harus diotorisasi berkali-kali ketika ingin menggunakna layanan tertentu. Otorisasi juga dibuat per user berdasarkan daftar yang ada di server sekuriti, atau jika protokolnya mendukung otorisasi bisa diberlakuakn per group pengguna.

3. Accounting (Akunting)

Accounting merupakan bagian akhir dari kerangka kerja *AAA*, *accounting* dapat mengukur dan mencatat sumber daya yang telah digunakan, termasuk jumlah waktu atau jumlah data yang dikirim dan atau diterima selama pelanggan tersebut memanfaatkan sumber daya tersebut (Brislian, 2011).

Sistem Accounting terselenggara oleh pembukuan statistik sesi dan penggunaan informasi serta digunakan untuk kegiatan kendali pemberian hak (otoritas), billing, analisa trend (kecenderungan), pemanfaatan sumber daya dan rencana kapasitas. Data accounting mempunyai beberapa manfaat diantaranya :

1. Seorang administrator dapat menganalisa kesuksesan setiap permintaan dan memprediksi kebutuhan system kedepanya.

2. Seorang analis keamanan (security) dapat melihat setiap permintaan yang ditolak, dapat melihat pola yang sering muncul memungkinkan serangan dari hacker dan freeloader

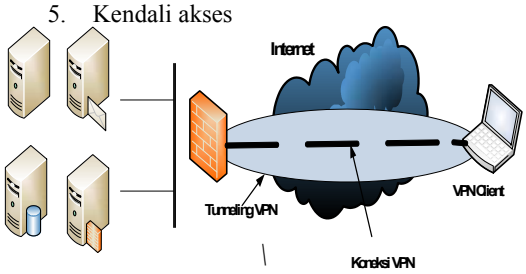
Seorang pengusaha dapat menjajaki waktu yang dibelanjakan atas service tertentu dan biaya yang harus dikeluarkan.

VPN (Virtual Private Network)

Virtual Private Network (VPN) adalah sebuah tekhnologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan public dan menggunakanya untuk dapat bergabung dengan jaringan local. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau LAN itu sendiri, walaupun sebenarnya menggunakna jaringan milik public.

Teknologi *VPN* menyediakan beberapa fungsi utama untuk penggunaanya. Fungsi – fungis utama terbut antara lain sebagai berikut.

1. Kerahasiaan
2. Keutuhan data
3. Autentikasi Sumber
4. Non-repudiation
5. Kendali akses



Gambar 2.2 Remote Access VPN

Teknologi *Tunneling*

Teknologi tunneling merupakan teknologi yang bertugas untuk manangani dan menyediakan koneksi point-to-point dari sumber ke tujuannya. Disebut tunnel karena koneksi point-to-point tersebut sebenarnya terbentuk dengan melintasi jaringan umum, namun koneksi tersbut tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya. Hal ini sama dengan seperti penggunaan jalur busway yang pada dasarnya menggunakan jalan raya, tetapi dia membuat jalur sendiri untuk dapat dilalui bus khusus. Koneksi point-to - point ini sesungguhnya tidak benar-benar ada, namun data yang dihantarkannya terlihat seperti benar-benar melewati koneksi pribadi yang bersifat point-to-point.

Teknologi ini dapat dibuat di atas jaringan dengan pengaturan *IP Addressing* dan *IP Routing* yang sudah matang. Maksudnya, antara sumber tunnel dengan tujuan tunnel telah dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP. Apabila komunikasi antara sumber dan tujuan dari tunnel tidak dapat berjalan dengan baik, maka tunnel tersebut tidak akan terbentuk dan *VPN* pun tidak dapat dibangun. Apabila tunnel tersebut telah terbentuk, maka koneksi point-to-point "palsu" tersebut dapat langsung digunakan untuk mengirim dan menerima data. Namun, di dalam teknologi VPN, tunnel tidak dibiarkan begitu saja tanpa diberikan sistem keamanan tambahan. Tunnel dilengkapi dengan sebuah sistem enkripsi untuk menjaga data-data yang melewati tunnel tersebut. Proses enkripsi inilah yang menjadikan teknologi VPN menjadi mana dan bersifat pribadi.

Jenis Implementasi *VPN*

1. *Remote Acces VPN*

Pada umumnya implementasi VPN terdiri dari 2 macam. Pertama adalah *remote access* VPN, dan yang kedua adalah *site-to-site* VPN. *Remote access* yang biasa juga disebut *virtual private dial-up network* (VPDN), menghubungkan antara pengguna yang *mobile* dengan *local area network* (LAN).

Jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan khusus perusahaannya dari berbagai lokasi yang jauh (*remote*) dari perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerjasama dengan *enterprise service provider* (ESP). ESP akan memberikan suatu *network access server* (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan *software* klien untuk komputer-komputer yang digunakan pegawai perusahaan tersebut.

Untuk mengakses jaringan lokal perusahaan, pegawai tersebut harus terhubung ke NAS dengan men-*dial* nomor telepon yang sudah ditentukan. Kemudian dengan menggunakan *sotware* klien, pegawai tersebut dapat terhubung ke jaringan lokal perusahaan.Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan *remote access* VPN untuk membangun WAN. VPN tipe ini akan memberikan

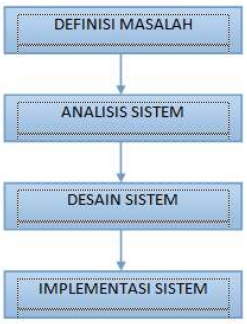
keamanan, dengan mengenkripsi koneksi antara jaringan lokal perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi

2. *Side To Side VPN*

Jenis implementasi VPN yang kedua adalah *site-to-site* VPN. Implementasi jenis ini menghubungkan antara 2 kantor atau lebih yang letaknya berjauhan, baik kantor yang dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkansuatu perusahaan dengan perusahaan lain (misalnya mitra kerja, *supplier* atau pelanggan) disebut ekstranet. Sedangkan bila *VPN* digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis intranet *site-to-site VPN*.

METODOLOGI PENELITIAN

Metode yang akan digunakna pada tugas akhir (TA) ini adalah metode *waterfall*. Adapun tahapan metode penelitian in dapat digambarkan pada gambar dibawah ini



Gambar 3.1 *Metode Waterfall*

Tahap definisi masalah

Tahap ini merupakan tahap penentuan hal – hal yang penting sebagai dasar permasalahan yang akan dianalisis dalam pembuatan server. Tahap ini merupakan tahap untuk mengkaji dan membatasi masalah yang akan diterapkan dalam system. Tahap define masalah ini dilakukan dengan cara mengumpulkan data – data secara tertulis maupun wawancara pada lokasi.

a. Studi literatur

Studi literature adalah suatu prose yang dilakukan penulis ketika akan menyelesaikan penelitian yang sedang dilakukan. Dalam hal ini penulis mencari dan mengumpulkan berbagai literature dari berbagai sumber sebagai bahan pendukung untuk menyelesaikan penelitian ini. Literature tersebut berupa jurnal paper maupun bacaan – bacaan yang berkaitan dengan tekhnologi jaringan computer seperti *radius, Mikrotik,* serta lainya yang berhubungan dengan system yang akan diterapakan dalam perusahaan tersebut.

Tahap analisis system

Analisa kebutuhan system dilakukan untuk mengetahui kebutuhan apa saja yang dibutuhkan oleh system yang akan dibuat dengan cara pengumpulan data – data yang berkaitan dan berhubungan dengan jaringan computer.

a. Observasi

Observasi yang penulis lakukan yaitu melakukan pengamatan terhadap system jaringan yang berlaku diperusahaan tersebut serta kebutuhan yang di butuhkan oleh user pada perusahaan tersebut. Dari pengamatan yang dilakukan penulis ditemukan beberapa masalah yang didapat yang kemudian dicarikan solusi. Solusi tersebut terancang dalam sebuah rancangan system yang akan diteliti lebih lanjut dan dilakukan peninjauan kembali apakah system yang dibuat ini memberikan manfaat.

Tahap desain system

Tahap ini merupakan tahap untuk mendesain topologi jaringan yang digunakan untuk menentukan posisi *server radius* di dalam jaringan. Desain topologi menggunakan aplikasi GNS3.

Server komunikasi NAS diletakkan pada server farm yang digunakan untukn penyimpanan database opsional *radius server.* Tahap yang dilakukan setelah melihat gambar topologi adalah instalasi terbagi menjadi beberapa bagian diantaranya :

- System operasi

  System operasi yang digunakan adalah ubuntu server versi 12.04. system operasi yang merupakan GPL (General Public License) atau open source
- Freeradius

  Freeradius membawa protocol radius yang digunakan sebagai server AAA. Freeradius mampu melakukan komunikasi dengan server AAA lain dengan menggunakna protocol NAS.
- Database server (MySql)

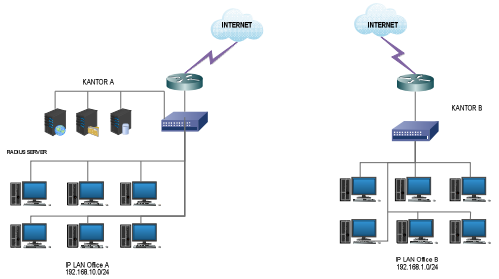
  Mysql mampu menangani sekita 15.000.000.000 record sehingga bisa menampung user pada proses otentikasi. Mysql adalah database server yang ringan dan cepat sehingga menjadi solusi dari masalah yang ada.
- UAM Server / Captive portal

  Captive portal adalah suatu tekhnik otentikasi dan pengamanan data yang lewat dari internal network ke network ekxternal. Captive portal sebenarnya merupakan mesin router atau gateway. Dalam hal ini captive portal yang digunakan fitur hotspot dari *RB450G.*

a. Konsep Perancangan

Konsep perancangan adalah sebuah gambaran yang akan diimplemetasikan pada

penelitian yang akan dilakukan. Konsep ini menggambarkan perancangan *RADIUS server* dalam jaringan *VPN*



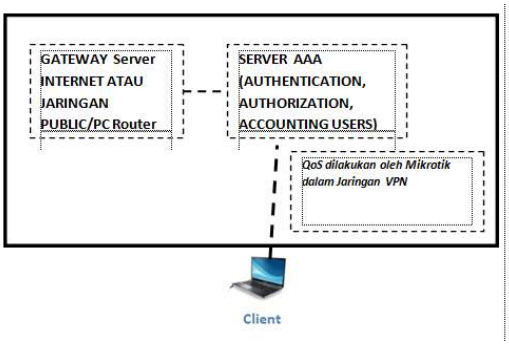
Gambar 3.2. Design awal Topologi Perushaan

Tahap Implementasi System

Tahap implementasi merupakan tahap pembuatan server yang dilakukan dengan cara mentranformasikan hasil analisis yang didapat dari tahap desain system sebelumnya. Dalam hal ini implementasi system dilakukan dengan mengkonfigurasi ubuntuk server dan mengkombinasikan dengan aplikasi freeradius, *mikrotik* untuk membangun *server hotspot* sebagai *system otorisasi* akses user melauli tunneling jaringan *vpn* antara kantor A dan kantor B .

Setelah system selesai dibuat maka tahap selanjutnya adalah tahap uji coba. Uji coba dilakukan dengan menggunakan dua metode testing, yaitu *functional testing* dan *Error Handling Testing.* Setelah system melalui tes uji coba, maka tahap selanjutanya adalah dilakukan *instalasi* system. Dimana pengguna mencoba fasilitas internet menggunakan user yang telah dibuat pada *server radius,* sehingga apabila terjadi kekurangan atau kesalahan dapat diperbaiki dan disesuaikan sampai terjadi kesepakatan antara administrator dan pengguna internet.

a. Gambaran System



Gambar 3.3 Gambaran Sistem Server RADIUS

Penelitian yang dilakukan penulis yaitu perancangan *virtual private server* sesuai dengan topologi di atas. *Host* server merupakan komputer server tunggal yang sistem operasi *Centos 6.2*. Di dalam *Host* server dibuat 4 (empat) *virtual private server* dengan sistem operasi yang berbeda-beda. Untuk memanajemen *virtual private server* yang berada pada *host* server maka diinstal aplikasi bernama *OpenVZ Web Panel*. *OpenVZ Web Panel* adalah *control panel VPS* yang dapat digunakan oleh administrator maupun *client* dalam melakukan *control* terhadap mesin virtual. *Client* merupakan komputer yang akan digunakan untuk mengakses masing-masing mesin virtual. Berikut ini merupakan detail pengalamatan *IP* dan sistem operasi yang digunakan:

Perancangan Gateway Server dan Server *AAA*

Perancangan Gateway server merupakan tahap awal yang dilakukan untuk menerapkan server *AAA*. Gateway server juga berfungsi sebagai *captive portal* akses internet untuk klien, *gateway server* menggunakna *Router Board* mikrotik dengan tipe *RB450G* . Untum mempermudah managemen Router Board berbasis GUI dapat menggunakna aplikasi pendukung yaitu winbox. Dengan aplikasi ini, admin jaringan bisa dengan mudah mengkofigurasi Router Board sebagai gateway server serta sebagai captive portal

Setting *Captive Portal* pada *router* A

Router board menyediakan system operasi yang dibutuhkan sesuai dengan system yang akan diterapakan di perusahaan tersebut. Tahap awal adalah memastikan bahwa router board sudah terkoneksi ke jaringan *public* dengan baik. Setelah router board sudah terkoneksi dengan jaringan public maka langkah selanjutnya adalah mebuat *NAT*, pada *router board* yang nantinya jaringan local pada kantor A dapat terkoneksi dengan jaringan public.

Captive portal atau yang familiar disebut hotspot disetting pada *router board* pada kantor A yang mana hotspot ini memilika *IP pool* dengan range ip yang ditentukan oleh administrator serta hotspot dengan *range ip* 192.168.10.2-192.168.10.50 *range* ip inilah yang akan dibuat oleh administrator sebagai hotspot client nantinya.

Setting *Captive Portal* pada *router* B

Tahap ini tidak berbeda dengan tahap yang dilakukan pada konfirugari *hotspot* pada *router* A. yang membedakan adalah user otentikasi login yang terpusat pada *server radius* yang ada pada kantor A.

Hotspot pada router B sebagai otentikasi client yang ada pada kantor B dengan user yang telah d create pada *server radius* pada kantor A.

Tahap Installasi dan Setting freeradius

Installasi dan setting *freeradius* dilakukan pada system operasi ubuntu dengan menginstall beberapa paket pendukung *freeradius* versi 2.0. Host server ini berada pada kantor A yang nantinya bertindak sebagai server radius dan di intregasikan dengan Router A atau *RB450G* pada kantor A.

Setelah installasi dan setting untuk freeradius pada ubuntu selesai dilakukan, ada beberapa tahap yang dilakukan untuk mengetahui bahwa installasi dan setting freeradius berjalan dengan baik, yaitu dengan cara test pengiriman paket dari client ke server radius. Melakukan ping antara *NAS* terhadap *radius server.*

Intregasi *freeradius* dan *mikrotik RB450G*

Tahap ini dilakukan ketika installasi dan setting *freeradius* dan *RB450G* berhasil dan berjalan normal. Sebelumnya antara *mikrotik* dan *freeradius* harus bisa terhubung dengan melakukan ping antara 2 *host server* tersebut. Mikrotik memanfaatkan proses otentikasi pada freeradius ini. Jadi user otentikasi dilakukan oleh *ubuntu server 12.04.*

Setting *VPN PPTP Server* pada mikrotik *RB450G*

Setting VPN PPTP dilakukan pada router di kantor A. user VPN ini berfungsi sebagai tunneling untuk share koneksi internet, sehingga nanti client pada kantor B dapat terkoneksi dengan jaringan public dengan melakukan tunneling terlebih dahulu sehingga nanti antara kantor A dan B dapat menjadi satu network, namun sebelum melakuakn tunneling antara Router A dan Router B halus melakukan static routing terlebih dahulu, agar jaringan pada kantor B dapat mengkases *PPTP server* pada jaringan A.

Pada *pptp server* juga terdapat ip pool yang diberikan oleh administrator pada client VPN yang nantinya setiap *client VPN* mendapatkan *IP* sesuai dengan *IP* yang administrator mapping pada IP pool saat mengkonfiguras *PPTP server*

Setting *VPN PPTP client* pada *router* B

Setting *VPN PPTP* pada *router* B dilakukan sebagai *tunneling* antara *router* A dan *router* B. Sehingga akan terbentuk koneksi tunneling yang berfungsi sebagai media penghubung agar nantinya dapat berkomunikasi antar kantor A dan kantor B.

Setting Static routing antara router A dan router B

Tahap ini diperlukan, karena tunneling yang dilakukan antara kantor A dan kantor B melakukan tunneling ip local yang ada pada router A, sehingga diperlukannya static route agar client pada *router B* dapat terhubung dengan *server PPTP* yang ada pada *router A*

Pengujian Sistem

Setelah tahap perancangan dan implementasi *Server radius* pada penelitian ini selesai, selanjutnya akan dilakukan pengujian terhadap system yang telah dibuat. Beberapa pengujian yang dilakukan adalah sebagai berikut:

Uji *log in hotspot client* pada kantor A dan kantor B

Uji log in hotspot ini dilakukan untuk mengetahui apakah portal login hotspot juga mengcover client yang ada pada kantor B, sehingga nantinya client pada kantor B harus melakukan otentikasi terlebih dahulu sebelum mengakses *resource* yang ada pada *router* pada kantor A misalnya *tunneling VPN* yang harus dilakukan agar mampu terkoneksi dengan jaringan luar/*public*. Jadi client pada kantor B harus melakukan otentikasi terlebih dahulu sebelum melakukan *tunneling VPN.*

Otentikasi *client* pada kantor A dan kantor B

Uji akses ini dilakukan untuk menguji bahwa client sudah dapat log in hot spot dengan menggunakna user yang telah di buat oleh server radius. Client akan mendapatkan halaman otentikasi berbasis web yang telah disediakan oleh *RB450G*. untuk *client* pada kantor B harus melakukan log in hotspot terlebih dahulu sebelum tunneling *vpn pptp server* pada kantor A, setelah log in terverifikasi maka *client* pada kantor B baru bisa tunneling *pptp server.*

Uji otorisasi *client* pada kantor A dan Kantor B

Pengujian ini dilakukan untuk mengetahui sejauh mana otorisasi yang bisa dilakukan oleh *server AAA* baik itu client di kantor A (*LAN*) maupun client di kantor B (*Tunneling VPN*). Ada 3 pengujian pada uji otorisasi client ini, diantaranya

Otorisasi client dengan limit pemakaian bandwith

Otorisasi client dengan melimit bandwith berguna untuk mengontrol pemakaian bandwith antar user, sehingga tidak ada saling berebut bandwith diantara client karena telah dibagi sesuai dengan kebutuh *user* atau client pada kantor A maupun kantor B

Otorisasi client akses web tertentu tanpa melakukan otentikasi

Otorisasi client akses web tertentu tanpa melakukan otentikasi, jadi otorisasi ini bertujuan agar web-web tertentu tidak perlu melakukan otentikasi terlebih dahulu, missal aplikasi web *cloud.ptfast.co.id* yang sering digunakan user untuk transfer file atau beberapa situs-situs lain.

Otoriasasi client membatasi download user

Membatasi download *user* atau disebut juga dengan quota download user. Jadi ketikas user sudah melewati batas quota yang telah ditentukan, user tidak dapat melakukan akses lagi. Berbeda dengan limit pemakaian bandwith yang ada pada point pertama tadi.

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian yang dilakukan oleh penulis tentang "Implementasi *AAA*Menggunakan R*adius Sever*Pada Jaringan *VPN"* maka dapat ditarik beberapa kesimpulan sebagai berikut:

1. Implementasi *AAA menggunakan Radius Server* pada jaringan VPNberjalan sukses.
2. Otentikas internet terpusat pada satu side yaitu pada kantor A yaitu pada *freeradius server* yang telah di buat
3. Otorisasi masih dilakukan pada masing-masing router pada *router* A dan *router* B

5.2 Saran

Untuk mengembangkan hasil dari penelitian ini, ada beberapa saran yaitu sebagai berikut:

1. Untuk pengembangan proyek ini adalah dengan *centralisasi authorizing user* pada satu *side* saja yaitu pada kantor A
2. Management *user* pada *freeradius* masih dalam bentuk command line, penembangan dapat dilakukan dengan menambahkan *daloradius* sebagai *management user* pada *freeraius* atau *usemanager* pada *mikrotik*.

DAFTAR PUSTAKA

1. Mualimsan,(2013). Tutorial Wordpress Setup VPN PPTP, http://www.mualimsan.web.id/, (diakses 15 Mei 2015).
2. Rifqi, M., (2014). *Tutorial Installasi UGM Hotspot pada mikrotik., http://masrifqi.staff.ugm.ac.id/doc/Tutorial%20Instalasi%20UGM%20Hotspot%20Mikrotik.pdf,* (diakses 1 Juni 2015).
3. Retno, A., (2010). Rancang Bangun Radius Server Pada Jaringan VPN menggunakan IPV6. Skripsi Institut Teknologi Sepuluh Nopember, Surabaya
4. Solichin, A., (2010). Dasar MySQL 5 dari pemula hingga mahir., http://achmatim.net/download/21/, (diakses 31 Mei 2015).
5. Towidjojo, R., (2013). Mikrotik Kung fu jilid 2 panduan router mikrotik lengkap dan jelas. Jakarta: Jasakom.
6. Towidjojo, R., (2013). Mikrotik Kung fu kitab 1. Jakarta: Jasakom.
7. Yuliansayh, H., (2011). Optimalisasi radius server sebagai system otentikasi dan otorisasi untuk proses login multi aplikasi web berbasis php. Skripsi Universitas Ahmad Dahlan, Yogyakarta.
8. Wahyutomo, T., (2013). Analisis Perancangan dan Monitoring Hotspot Area. Skripsi STMIK AMIKOM Yogyakarta, Yogyakarta.
9. Wijaya, B., (2011). *Membangun Server AAA Menggunakan Protokol Remote Access Dial In User Service.* Diploma Polteknik Negeri Jember, Jember.
10. Nopriansyah, (2010). Desain dan Implementasi Authentifikasi User Pada jaringan Wireless TOP Komputer Palembang. Skripsi STMIK PalComTech, Palembang.