

Prototipe Manajemen Keamanan Jaringan di Pesantren (Study Kasus Pesantren Madinatunnajah)

Abdul Majid
IAIN Pekalongan
Abdulmajid1183@gmail.com

Abstract

Networking today is a much needed service. Existing problems include user authentication, user management hotspot, bandwidth management, as well as any unwanted intruders. It is necessary the development of a network system that can provide security for user authentication and bandwidth management. Network development means developing new systems and will replace the old system or repair the existing system. Particularly the issue of authentication and bandwidth. This type of research is the Applied Research with the development of systems using NDLC (Network Development Life Cycle). Data collection method using interviews, observation and study of literature. This research resulted in the network security system has a good quality with a percentage of 82.5% and meet the needs of the organization at pesantren Madinatunnajah.

Keyword : *Bandwidth Management, Mikrotik, User Manager, Hotspot.*

Abstrak

Saat ini jaringan merupakan suatu layanan yang sangat dibutuhkan. Masalah yang ada antara lain adalah otentikasi user, manajemen user hotspot, pengaturan bandwidth, serta adanya penyusup yang tidak diinginkan. Maka perlu pengembangan sistem jaringan yang dapat memberi keamanan otentikasi bagi user dan pengelolaan bandwidth. Pengembangan jaringan berarti menyusun sistem baru dan akan menggantikan sistem lama atau memperbaiki sistem yang telah ada. Khususnya masalah otentikasi dan bandwidth. Jenis penelitian ini adalah Applied Research dengan pengembangan sistem menggunakan metode NDLC (Network Development Life Cycle). Metode Pengumpulan data menggunakan Wawancara, Observasi dan studi kepustakaan. Penelitian ini menghasilkan sistem keamanan jaringan memiliki kualitas baik dengan prosentase sebesar 82,5% dan memenuhi kebutuhan organisasi di Pondok Pesantren Madinatunnajah.

Kata Kunci: *Bandwidth Management, Mikrotik, User Manager, Hotspot.*

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini, menjadikan proses komunikasi data semakin mudah. Jaringan komputer saat ini merupakan suatu layanan yang sangat dibutuhkan. Jaringan komputer memungkinkan pemakaian secara bersama-sama baik berupa perangkat lunak dan perangkat keras. Sehingga sebuah kelompok kerja dapat berkomunikasi lebih efektif. Hotspot adalah salah satu wujud dari perkembangan teknologi informasi yang menjadi tren di kalangan masyarakat dikarenakan kemudahan yang diberikan.

Seperti lembaga pada umumnya, Pesantren Madinatunnajah memiliki sistem jaringan komputer dan internet sebagai penunjang kegiatan kepesantrenan dan kegiatan belajar mengajar di sekolah. Pesantren Madinatunnajah memiliki sebuah sistem jaringan yang menghubungkan seluruh unit lembaga seperti ruang kantor Madrasah (RA, MI, MTs, MA), kantor Pengasuhan Putra, Pengasuhan Putri, kantor BMT, rumah Pimpinan dan Laboratorium Komputer yang digunakan para Siswa dalam kegiatan belajar mengajar mulai dari tingkat RA (Raudhatul Athfal) hingga Sekolah Tinggi Madinatunnajah serta para Guru dan Tamu melalui jaringan hotspot. Jaringan ini juga difasilitasi akses internet, sehingga semua unit dapat terhubung ke Jaringan dan dapat mengakses internet.

Jumlah user yang mengakses jaringan di Pondok Pesantren Madinatunnajah berkisar antara 5 sampai 50 user, maka diperlukan adanya sebuah pengembangan sistem keamanan di dalam jaringan baik yang menangani Authentication,

Authorization dan Accounting (AAA) serta mengatur bandwidth jaringan. Jaringan tanpa keamanan bagaikan rumah tanpa pintu, membiarkannya terbuka dan semua orang dapat masuk ke dalam dengan bebas dan dapat berbuat apa saja yang dikehendakinya.

Berdasarkan identifikasi serta batasan masalah di atas maka rumusan masalahnya adalah Bagaimana Desain dan Implementasi teknologi Authentication system pada jaringan komputer di Pondok Pesantren Madinatunnajah menggunakan Remote Authentication Dial in User Service (RADIUS) dan penerapan Bandwidth management

Manfaat penelitian ini secara teoritis yaitu untuk memberikan informasi tentang teknik pengamanan jaringan komputer khususnya dalam hal otentikasi dengan menggunakan RADIUS dan Bandwidth management, Sedangkan manfaat penelitian ini secara praktis yaitu manajemen jaringan komputer di Pondok Pesantren Madinatunnajah.

2. KERANGKA TEORI

Menurut Yohan Jati ^[14] jaringan komputer diartikan sebagai sebuah rangkaian yang terdiri dari dua atau lebih komputer. Komputer-komputer ini akan dihubungkan satu sama lain dengan sebuah system komunikasi. Dengan jaringan komputer ini, setiap pengguna komputer yang terjaring di dalamnya akan dapat saling tukar menukar data, program dan sumber daya computer lainnya seperti media penyimpanan, printer dan lain-lain.

Topologi adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Topologi yang saat ini banyak digunakan adalah bus,

token-ring, star dan tree network. Masing-masing topologi ini mempunyai ciri khas, dengan kelebihan dan kekurangannya sendiri. [12].

Topologi jaringan sendiri terbagi menjadi dua yaitu physical dan logical. Physical Merupakan gambaran fisik dari hubungan antara perangkat (komputer, server, hub, switch, dan kabel jaringan) yang membentuk suatu pola khusus. Sedangkan logical merupakan gambaran bagaimana suatu perangkat dapat berkomunikasi dengan perangkat lainnya.

a) Bus

Topologi bus merupakan topologi dimana semua perangkat keras terhubung melalui kabel tunggal yang kedua ujungnya tidak tertutup dan masing-masing ujungnya menggunakan sebuah perangkat terminator. Jika alamat perangkat sesuai dengan alamat pada informasi yang dikirim, maka informasi akan diterima dan diproses. Jika tidak, maka informasi akan diabaikan

b) Token-Ring

Topologi ring merupakan topologi dimana setiap perangkat dihubungkan sehingga berbentuk lingkaran. Setiap informasi yang diperoleh akan diperiksa alamatnya oleh perangkat jika sesuai maka informasi akan diproses sedangkan jika tidak maka informasi diabaikan.

c) Star

Dalam topologi *star*, semua kabel dihubungkan dari komputer-komputer ke lokasi pusat (central location), dimana semuanya terhubung ke suatu alat yang dinamakan hub.

d) Mesh

Topologi *mesh* dapat dikenali dengan hubungan *point-to-point* atau satu-satu ke setiap komputer. Setiap komputer terhubung ke komputer lain melalui

kabel, bisa menggunakan kabel *coaxial*, *twisted pair*, bahkan serat *optic*. Topologi *mesh* cocok digunakan pada jaringan yang sangat kritis. Pada awalnya jaringan *mesh* dikembangkan untuk keperluan militer. Apabila salah satu atau beberapa kabel putus masih tersedia rute alternative melalui kabel yang lain.

Jaringan Wireless.

a. Wireless Wide Area Network (WWANs).

Koneksi ini dapat mencakup jangkauan yang luas seperti pada sebuah kota atau Negara, melalui beberapa antena atau sistem satelit yang digunakan oleh penyelenggara jasa telekomunikasi.

b. Wireless Metropolitan Area Network (WMANs).

Degan teknologi ini akan memungkinkan pengguna untuk membuat koneksi nirkabel antara beberapa lokasi dalam satu daerah metropolitan misalnya antara gedung-gedung yang berbeda dalam satu kota atau dalam satu kampus atau satu universitas.

c. Wireless Local Area Network (WLANs).

Teknologi WLAN akan mengijinkan pengguna membangun jaringan nirkabel dalam satu daerah local, misalnya dalam lingkungan satu kantor, gedung, hotel, bandara.

d. Wireless Personal Area Network (WPANs)

Pada teknologi ini membolehkan pengguna membangun jaringan nirkabel untuk piranti-piranti sederhana, antara lain PDA (Personal Digital Assistant), HP/ telepon selular atau laptop. Hal ini dapat dilakukan pada sebuah ruang operasi personal (Personal Operating Space atau POS). Sebuah POS dalah sebuah ruang yang bisa mencapai 10 meter. Dua teknologi yang banyak dipakai dalam penerapan

WPANs adalah bluetooth dan infrared [13]

Hotspot

Menurut Onno [10] Hotspot adalah sebuah wilayah terbatas yang dilayani oleh satu atau sekumpulan Access Point wireless LAN standar 802.11 a/b/g, di mana user dapat masuk ke dalam Access point secara bebas dan mobile menggunakan perangkat sejenis notebook, laptop, PDA dan sebagainya. Biasanya hotspot dioperasikan di tempat umum seperti Cafe, Mall dan Kampus.

Otentikasi

Menurut Jonathan Hassel [3], otentikasi adalah proses pengesahan identitas pengguna (end user) untuk mengakses jaringan. Proses ini diawali dengan pengiriman kode unik misalnya, username, password, pin, sidik jari oleh pengguna kepada server. Di sisi server, sistem akan menerima kode unik tersebut, selanjutnya membandingkan dengan kode unik yang disimpan dalam database server. Jika hasilnya sama, maka server akan mengirimkan hak akses kepada pengguna. Namun jika hasilnya tidak sama, maka server akan mengirimkan pesan kegagalan dan menolak hak akses pengguna.

Captive Portal

Captive Portal adalah suatu teknik otentikasi dan pengamanan data yang melewati network internal ke network eksternal. Captive Portal sebenarnya merupakan router atau gateway yang memproteksi atau tidak mengizinkan adanya trafik, hingga user melakukan registrasi. Biasanya Captive Portal ini digunakan pada infrastruktur wireless seperti hotspot area, tapi tidak menutup kemungkinan diterapkan pada jaringan kabel. Cara kerja dari captive portal yaitu Pada

saat seorang pengguna berusaha untuk melakukan browsing ke Internet, captive portal akan memaksa pengguna yang belum terotentikasi untuk menuju ke Authentication web dan akan di beri prompt login termasuk informasi tentang hotspot yang sedang dia gunakan.

Protokol AAA

Menurut Jonathan Hassel [3] Konsep kerja server otentikasi dikenal dengan AAA (authentication, authorization, and accounting). Yang terdiri dari Otentikasi, Otorisasi, dan Pendaftaran akun pengguna. Konsep AAA mempunyai fungsi yang berfokus pada tiga aspek dalam kontrol akses user, yaitu :

a. Authentication

Otentikasi adalah proses verifikasi untuk menyatakan suatu identitas. Bentuk umum yang biasa digunakan untuk melakukan otentikasi menggunakan kombinasi username dan password, jika kombinasi keduanya benar maka client dapat mengakses ke sumber daya jaringan tertentu. Proses otentikasi dapat dianalogikan seperti seorang tamu yang datang ke rumah anda, sebelum tamu tersebut diperbolehkan masuk, tentu anda harus mengetahui tamu itu terlebih dahulu, jika anda kenal dengan tamu tersebut, maka tamu tersebut pastinya akan anda persilahkan masuk dan sebaliknya.

b. Authorization

Otorisasi melibatkan penggunaan seperangkat aturan-aturan yang berlaku untuk memutuskan aktifitas apa saja yang dizinkan dalam sistem atau sumber daya jaringan tertentu untuk pengguna yang terotentikasi. Proses Authorization merupakan lanjutan dari proses Authentication. Proses Authorization dapat

dianalogikan sebagai berikut: jika anda sudah mengizinkan tamu untuk masuk kerumah anda, tentu anda mempunyai aturan-aturan yang ditempel di dinding rumah anda, misalnya tamu hanya boleh masuk sampai dengan ruang tamu. Dengan aturan seperti ini tentu akan memudahkan seseorang untuk melakukan kontrol terhadap sumber daya jaringan tertentu.

c. Accounting

Proses Accounting merupakan proses dimana terdapat proses pencatatan waktu user saat koneksi ke jaringan. Data dan informasi ini sangat berguna baik untuk pengguna maupun administrator, biasanya laporan ini digunakan untuk melakukan audit, membuat laporan pemakaian, membaca karakteristik jaringan, dan pembuatan billing tagihan. jadi pada intinya proses accounting berguna untuk mengetahui apa saja yang dilakukan oleh client dan servis apa saja yang dilakukan oleh client. Analogi sederhananya adalah mesin absensi dikantor, ia akan mencatat waktu datang dan waktu pulang, dengan demikian petugas dapat memonitoring karyawan dengan mudah.

Remote Authentication Dial-In User Service (RADIUS)

RADIUS merupakan singkatan dari Remote Acces Dial in User Service. Pertama kali di kembangkan oleh Livingston Enterprises. Merupakan network protokol keamanan komputer yang digunakan untuk membuat manajemen akses secara terkontrol pada sebuah jaringan yang besar. *RADIUS* didefinisikan di dalam RFC 2865 dan RFC 2866. *RADIUS* biasa digunakan oleh perusahaan untuk mengatur akses ke internet bagi client. *RADIUS* melakukan otentikasi, otorisasi, dan pendaftaran akun pengguna secara terpusat untuk

mengakses sumber daya jaringan. Sehingga memastikan bahwa pengguna yang mengakses jaringan adalah pengguna yang sah. *RADIUS* berstandar IEEE 802.1x. Sering disebut "port based authentication". *RADIUS* merupakan protokol client - server yang berada pada layer aplikasi pada OSI layer. Dengan protokol transport berbasis UDP. [3].

Firewall

Menurut Sukmaaji [2] : Firewall merupakan suatu cara atau mekanisme yang diterapkan terhadap *hardware, software*, ataupun sistem dengan tujuan untuk melindungi. Perlindungan dapat dilakukan dengan menyaring, membatasi, atau bahkan menolak (*access control policy*) suatu atau semua hubungan/kegiatan dari suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Tugas *firewall* adalah untuk memastikan bahwa tidak ada tambahan diluar ruang lingkup yang diizinkan. *Firewall* bertanggung jawab untuk memastikan bahwa *access control policy* yang diikuti oleh semua pengguna di dalam jaringan tersebut.

Firewall bekerja dengan mengamati paket IP (*internet protocol*) yang melewatinya. Berdasarkan konfigurasi dari *firewall* akses dapat diatur berdasarkan *IP address, port* dan arah informasi.

Firewall terbagi menjadi tiga jenis. yakni sebagai berikut yaitu *Packet Filtering Router, Application Level Gateway dan Circuit Level Gateway*. Ketiga dari jenis firewall adalah *circuit level gateway*. *Circuit level gateway* sistem yang dapat berdiri sendiri atau bias merupakan suatu fungsi yang melakukan dengan *application level gateway* untuk aplikasi. *Circuit level gateway* pintu

gerbang tidak mengizinkan *end to- end* koneksi tcp, satu diantaranya adalah kumpulan dua koneksi satu diantaranya gateway dan sebuah server user tcp diluar host. [2]
Perbedaan penulis dengan penelitian terdahulu adalah pada hardware yang

digunakan, software yang digunakan, metode dan pengembangan sistem yang digunakan serta obyek penelitian.

Dari penelitian-penelitian tersebut dapat disimpulkan dalam sebuah tabel di bawah ini :

| NO | JUDUL | METODE | HASIL |
|----|---|---|--|
| 1 | Rancang Bangun Radius Server Pada Jaringan Vpn Menggunakan Ipv6 | Perancangan dan konfigurasi Radius dan VPN serta pengalamatan menggunakan Ipv6 menggunakan freeradius | Membangun Koneksi client-server dengan client yang berbeda OS dan Interkoneksi antara VPN dengan Ipv6 dengan menggunakan key yang sama yang dibuat oleh server sebagai sertifikat |
| 2 | Implementasi Sistem Otentikasi Pada Pengguna Jaringan Hotspot Di Universitas Kanjuruhan Malang Guna Meningkatkan Keamanan Jaringan Komputer | Perancangan menggunakan freeradius dan Mikrotik pada universitas kanjuruhan malang | Hasil dari penelitian ini adalah system otentikasi pengguna jaringan pada jaringan hotspot yang ada di Universitas Kanjuruhan Malang yang dapat memberikan keamanan user hotpsot. |
| 3 | Implementasi Radius Server Pada Jaringan Virtual Private Network | Analisis dan Perancangan | Merancang radius server dengan VPN menggunakan OpenVpn dengan hasil bahwa Radius server dapat terkoneksi dengan jaringan VPN melalui jaringan lokal dan dapat memberi keamanan otentikasi pada jaringan VPN. |

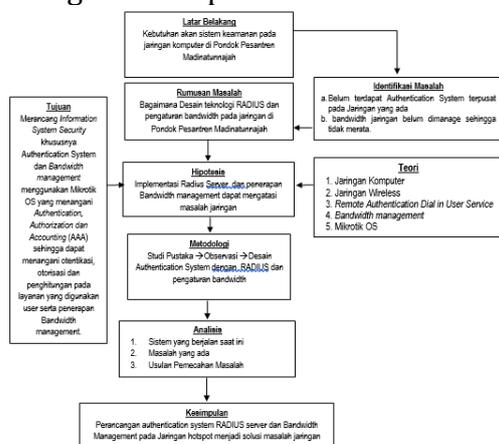
| | | | |
|---|---|---------------------------------------|--|
| 4 | Prototipe Manajemen Keamanan Jaringan di Pesantren : Studi kasus pesantren Madinatunnajah | Network Development Life Cycle (NDLC) | Merancang User Mangement dengan Radius Server Mikrotik dan mengatur layanan user serta pengaturan Bandwidth. |
|---|---|---------------------------------------|--|

Tinjauan Obyek Penelitian

Pesantren Madinatunnajah adalah lembaga pendidikan Islam yang mendidik para santrinya untuk siap memimpin umat dan bangsa. Madinatunnajah adalah sebuah nama pemberian dari seorang ulama yang berarti "Kota Kesuksesan". Pada tanggal 14 Februari 1997 Pondok Pesantren Madinatunnajah didirikan oleh Almurkarrom Drs. KH Mahrus Amin di lahan milik pribadinya seluas 2 (dua) hektar terletak di Jombang Ciputat Tangerang. Dan dilakukan peresmian oleh Almarhum KH. Shoiman Lukmanul Hakim salah satu Pimpinan Pondok Modern Darussalam Gontor pada tanggal 20 September 1997. Visi Pesantren Madinatunnajah adalah "Ya Tuhanku, tambahkanlah kepadaku ilmu pengetahuan".

Dari latar belakang yang ada di Pondok Pesantren Madinatunnajah yaitu belum adanya sistem otentikasi pada jaringan di pesantren dan belum adanya *bandwidth management*, dari latar belakang tersebut kemudian diidentifikasi masalah yang ada yaitu belum adanya beberapa system manajemen jaringan yang ada di Pesantren Madinatunnajah terutama masalah otentikasi dan juga pengaturan bandwidth. Dari masalah tersebut maka dengan metode pengumpulan data melalui observasi dan studi pustaka kemudian dilanjutkan langkah penelitian yang direncanakan seperti Analisis masalah dan sebagainya diharapkan bahwa penerapan Radius dan pengaturan bandwidth dapat menjadi solusi pada masalah jaringan di Pesantren Madinatunnajah.

Kerangka Konsep



Hipotesis Penelitian

Berdasarkan kerangka konsep yang telah dikemukakan maka pernyataan hipotesis dirumuskan sebagai berikut : Diduga bahwa Desain Authentication Sytem pada hotspot menggunakan *Remote Authentication dial in User Service* serta *Bandwidth management* dapat memberikan solusi sistem manajemen jaringan di Pesantren Madinatunnajah.

Penjelasan :

3. METODOLOGI

Jenis penelitian ini merupakan jenis Penelitian Terapan (Applied Research). Dimana hasil penelitian dapat langsung diterapkan untuk memecahkan permasalahan yang dihadapi. Metode pemilihan sampel dalam penelitian tentang sistem keamanan Jaringan di Pondok Pesantren Madinatunnajah ini adalah purposive sampling.

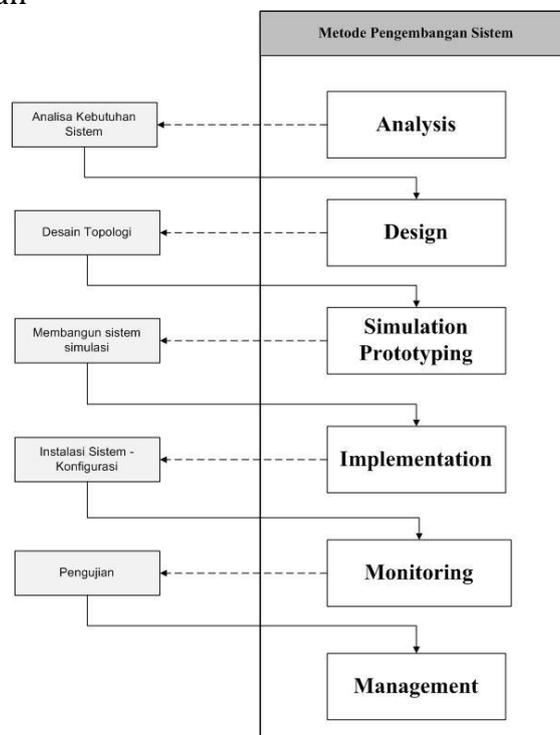
Metode Pengumpulan Data

- a. Studi Kepustakaan

- b. Observasi (pengamatan)
- c. *Interview* (wawancara)

Metode Pengembangan Sistem

Dalam penelitian ini akan menerapkan metode NDLC (Network Development Life Cycle) untuk pengembangan sistem dengan menggunakan *MikroTik*. Tiap tahap pada metode pengembangan sistem NDLC akan dijelaskan sebagai berikut.



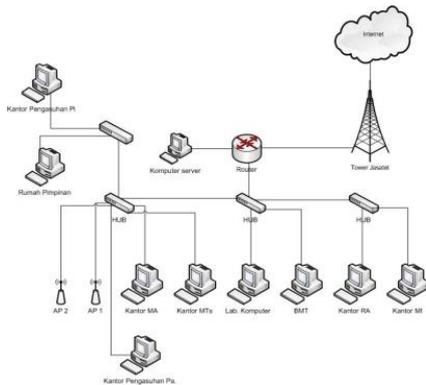
Gambar
Mekanisme Penelitian

1. **Analysis** : Analisa permasalahan yang muncul, analisa keinginan user, dan analisa topologi / jaringan yang sudah ada saat ini.
2. **Design** : Membuat gambar design topology jaringan interkoneksi yang akan dibangun.
3. **Simulation Prototyping** : membuat dalam bentuk simulasi dengan bantuan Tools khusus di bidang network
4. **Implementation** : Menerapkan semua yang telah direncanakan dan di design sebelumnya
5. **Monitoring**
6. **Management** : Membuat/mengatur agar sistem yang telah dibangun dan berjalan

dengan baik dapat berlangsung lama dan unsur reliability terjaga.

4. HASIL DAN PEMBAHASAN

Berikut adalah gambaran topologi jaringan Pesantren Madinatunnajah :



Mikrotik *routerOS* sebagai *router* dan *gateway* yang berfungsi sebagai penghubung antara jaringan lokal dan jaringan Internet. Mikrotik *routerOS* juga digunakan untuk pengaturan *addressing* atau pengalamatan untuk semua *client* / PC yang ada pada jaringan lokal.

| Eth | Address | Network |
|--------|-----------------|--------------|
| Lokal | 192.168.10.1/24 | 192.168.10.0 |
| Publik | 10.100.10.2/24 | 10.100.10.0 |

Tabel Pengalamatan Jaringan Pada Mikrotik

Dari hasil identifikasi kebutuhan fungsional bahawasanya pengguna jaringan hotspot di Madinatunnajah adalah semua civitas, karyawan, mahasiswa, siswa dan juga para tamu yang mana prioritasnya untuk akses internet bagi Guru-guru yang akan mempersiapkan materi pembelajaran dan juga bagi para Mahasiswa yang sedang menyusun Skripsi atau Tugas Akhir. Adapun bagi Siswa diberikan

akses internet pada saat pembelajaran Mata Pelajaran TIK.

Jaringan yang ada di Pesantren Madinatunnajah saat ini belum memiliki system keamanan baik yang berhubungan dengan otentikasi maupun yang berhubungan dengan pengaksesan jaringan internet. Untuk masalah otentikasi user, apabila user akan terkoneksi dengan jaringan hotspot yang ada di Pondok Pesantren Madinatunnajah, user cukup hanya dengan mengatur wireless card nya dengan mode *Dynamic Host Configuration Protocol* (DHCP), sehingga tanpa menggunakan otentikasi apapun user sudah dapat terkoneksi dengan hotspot yang ada di Pondok Pesantren Madinatunnajah. Hal ini tentu berbahaya dikarenakan jika ada user yang berusaha untuk masuk dan merusak sistem keamanan jaringan yang ada.

Selain itu tidak ada kontrol terhadap user-user yang terkoneksi melalui hotspot. Meskipun kebanyakan staff pesantren yang menjadi user jaringan, tidak menutup kemungkinan ada user illegal yang dapat masuk ke jaringan, karena seperti hasil observasi langsung yang penulis lakukan bahwa koneksi yang ada saat ini sering mengalami down karena kelebihan beban jaringan.

Perancangan system keamanan jaringan komputer dengan membangun sistem keamanan seperti otentikasi dengan *Remote Authentication Dial-In User Service* (RADIUS). Penulis menggunakan Mikrotik OS dalam merancang system keamanan. Dengan adanya sistem otentikasi yang diterapkan, memudahkan administrator dalam memantau, mengontrol, dan melakukan bandwidth management terhadap user-user yang terhubung

pada jaringan komputer. Dan yang terpenting adalah *RADIUS* server memiliki protokol AAA (*Authentication, Authorization, Accounting*) yang dapat mengatur mekanisme bagaimana tata cara berkomunikasi, baik antara user ke jaringan maupun antar user dengan domain yang berbeda dengan tetap menjaga keamanan pertukaran data. Berikut ini adalah rincian dari sistem yang ada.

1. Sistem dari sisi Server, yaitu Hardware dan software yang digunakan sebagai pengatur jaringan.

| Hardware | Software |
|--|--|
| <p>PC dekstop sebagai Router</p> <p>Dengan spesifikasi : Memory 512 MB, HDD 8,2 GB, Processor Intel 3066 MHz,</p> | <p>MikroTik RouterOS Versi 5.20</p> |
| Kabel UTP Cat 5e | |
| Connector RJ45 | |
| HUB D-link | |

Pada tahap ini dibuat rancangan sistem manajemen keamanan jaringan komputer yang telah diusulkan mulai dari topologi infrastruktur, rancangan sistem keamanan jaringan hotspot (*RADIUS* server, Firewall, Manajemen bandwidth) yang akan diterapkan di jaringan Pesantren Madinatunnajah. Berikut ini dijelaskan mengenai perancangan fisik dan perancangan logik.

| | |
|--------------------------------|--|
| Acces Point TP-LINK TL-WA701ND | |
| Tower Triagle | |
| POE | |
| Routerboard | |

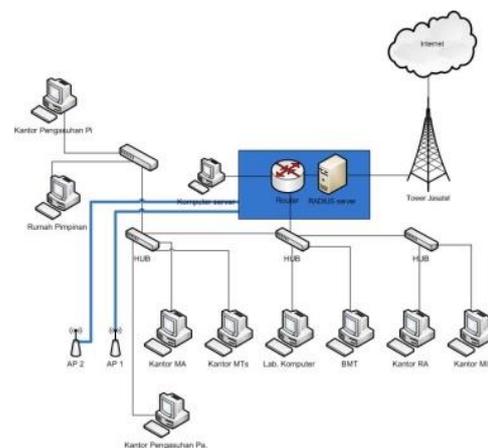
Tabel

Spesifikasi Sistem Server

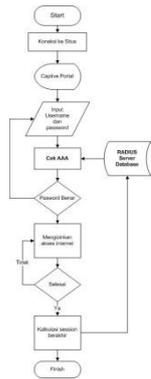
2. Sistem dari sisi Client, yaitu komputer yang digunakan untuk mengakses jaringan dan mengatur jaringan.

| Hardware | Software |
|--|---|
| <ul style="list-style-type: none"> Laptop TOSHIBA satellite L-310 | Windows 7-SP1 Google Chrome Mozilla Firefox |
| <ul style="list-style-type: none"> PC Dekstop Lenovo A70 All-In-One | Windows 7-SP1 Google Chrome Mozilla Firefox |
| <ul style="list-style-type: none"> PC Dekstop Acer Veriton M10 | Windows 7-SP1 Google Chrome Mozilla Firefox |

Tabel Spesifikasi Sistem Client



Gambar Rancangan usulan topologi sistem jaringan



Gambar Flow chart login user RADIUS

Perancangan Sistem RADIUS

a. Konfigurasi NAT, IP Address, Bridge, Hotspot

| Konfigurasi NAT | |
|-----------------|---|
| 1 | [admin@ROUTER MADINATUNNAJAH]> /ip firewall nat add action=masquerade out- interface=Publik chain=srcnat |
| 2 | [admin@ROUTER MADINATUNNAJAH]> /interface bridge port add bridge=bridge1 interface=Lokal |
| 3 | [admin@ROUTER MADINATUNNAJAH] > /ip pool add name=pool ranges=192.168.10.2- 192.168.10.254 |

Tabel IV-5, Konfigurasi NAT, Bridge, Pool, dan Hotspot

b. Menginstall NTP dan Package RADIUS Server (User Manager)

Untuk mengaktifkan fitur RADIUS Server yang ada pada Mikrotik RouterOS terlebih dahulu kita harus mengecek terlebih dahulu apakah ntp dan package RADIUS (user manager) sudah terintegrasi atau belum karena ntp dan user manager merupakan paket yang terpisah dari router OS Mikrotik.

c. Setup Parent Time Zone dan Radius Hotspot

Setelah kita menginstall ntp dan user manager, tentunya kita

pastikan bahwa parent time zone telah terupdate. Setelah itu membuat konfigurasi RADIUS melalui terminal pada Winbox.

| Script melalui Terminal | |
|-------------------------|--|
| 1 | [admin@ROUTER MADINATUNNAJAH]> /system ntp client set enabled=yes mode=unicast primary- ntp=203.114.224.252 secondary-ntp=218.93.250.18 |
| 2 | [admin@ROUTER MADINATUNNAJAH]> /ip hotspot profile set hsprof1 use- radius=yes |
| 3 | [admin@ROUTER MADINATUNNAJAH]> /radius add service=hotspot address=127.0.0.1 secret=123 |

d. Membuat daftar user profile pada User Manager

Pembuatan profil user jaringan pada RADIUS server adalah proses pendaftaran user agar dapat terhubung dengan jaringan. Termasuk di dalamnya adalah pembatasan bandwidth pada masing-masing profil pembatasan bandwidth ini akan diintegrasikan dengan pengaturan jaringan hotspot melalui Mikrotik

e. Membangun Captive Portal

Merubah tampilan login user menggunakan bahasa pemrograman web yaitu HTML dan PHP sehingga tampilannya berubah lebih menarik.



Captive Portal untuk login user

A. Pengujian RADIUS

- a. Apabila user name dan password yang diinputkan benar, maka user sudah dapat mengakses internet.
- b. Sedangkan apabila user tidak dapat masuk ke sistem, ada beberapa pesan kesalahan yang akan muncul seperti : internal-error, config-error, not-logged-in, ip pool-empty, shutting-down, user-session-limit, license-session-limit, wrong-mac-username, chap-missing, invalid-username, invalid-mac, uptime-limit, traffic-limit, radius-timeout, auth-in-progress, radius-reply.

B. Monitoring Melalui Winbox

Untuk memantau user jaringan bisa dengan menggunakan Winbox. Dari gambar terlihat apabila notifikasi R berarti user aktif terkoneksi oleh RADIUS server.

| Server | Server Profile | Users | User Profiles | Active | Hosts | IP Bindings | Service Ports | Walled Garden | Walled Garden IP List | Cookies |
|--------|----------------|-------|---------------|--------|----------------|-------------|---------------|---------------|-----------------------|----------|
| 1 | Hotspot | 1 | user1 | Active | 192.168.16.182 | 00:21:07 | 00:00:30 | 00:00:30 | 00:00:30 | 00:00:30 |
| 2 | Hotspot | 1 | user2 | Active | 192.168.16.182 | 00:23:16 | 00:00:30 | 00:00:30 | 00:00:30 | 00:00:30 |
| 3 | Hotspot | 1 | user7 | Active | 192.168.16.182 | 00:25:29 | 00:00:30 | 00:00:30 | 00:00:30 | 00:00:30 |

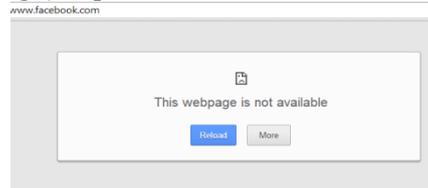
Monitor user melalui Winbox

C. Monitoring Melalui Browser

Selain melalui aplikasi winbox, dapat juga memantau user melalui fitur manajemen user manger yang ada di

Mikrotik yaitu dengan menggunakan Browser dan mengetikkan URL: IP_adress Mikrotik/userman.

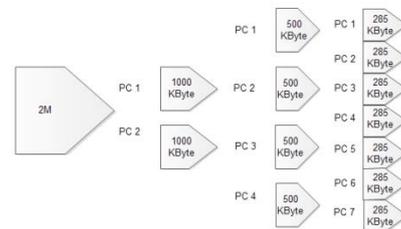
Pada manajemen selanjutnya adalah dengan melakukan penjadwalan akses terhadap situs – situs yang sudah dikelompokkan pada “jadwal-akses”. Pengujian dilakukan pada dua waktu yang berbeda, yakni pada jam sibuk kegiatan belajar mengajar pukul 07.00 – 13.00 WIB dan pada jam bebas kegiatan belajar mengajar pukul 13.00 – 07.00 WIB.



Gambar diatas menunjukkan bahwa facebook tidak bisa diakses pada jam waktu belajar. Karena jam tersebut filter rule untuk jadwal-akses berstatus aktif.

Bandwidth Management

- a. Pembagian IP Address adalah tabel pengalamanan IP (*Internet Protocol*) pada Jaringan.
- b. PCQ (Per Connection Queue) Untuk lebih mudah memahami konsep PCQ, menggunakan analogi berikut ini :



Per Connection Queue (PCQ) Sebuah jaringan sebanyak 7 PC yang akan di bagikan bandwidth maksimal 2 Mb dan bandwidth minimal tiap PC 200 kb. Jika hanya

satu PC saya yang online maka dia akan dapat Bandwidth max 2 Mb, namun jika ada dua PC yang online Bandwidth dibagi 2, dan seterusnya hingga 7 dengan pembagian bandwidth yang merata.

Pengujian Kualitas Software

Kegiatan *Focus Group Discussion* dilaksanakan di ruang kantor pada tanggal 27 Juli 2015 pukul 16.00 – 17.00 WIB. Dihadiri oleh 5 peserta sebagai responden, 4 responden tersebut adalah Guru dan 1 respondennya adalah Staff. Memulai diskusi, peneliti melakukan presentasi dan demo sistem yang sudah dirancang. Peneliti menjelaskan setiap fungsi yang ada berdasarkan instrumen yang sudah disiapkan. responden diperkenankan untuk memberikan tanggapan dan persetujuan melalui form yang sudah disiapkan peneliti.

Pengujian Kualitas

Hasil pengujian kualitas terdiri dari pengujian kualitas masing-masing aspek berdasarkan empat karakteristik ISO 9126 dan pengujian keseluruhan dari empat karakteristik ISO 9126. Rumus untuk mengukur kualitas *software* menurut ISO 9126 berdasarkan jawaban responden sebagai berikut :

$$\% \text{ Skor Aktual} = \frac{\text{Skor Aktual}}{\text{Skor Ideal}} \times 100 \%$$

Keterangan :

1)Skor aktual yaitu jawaban seluruh responden mengenai kuesioner yang telah diberikan.

2) Skor ideal yaitu nilai tertinggi atau semua responden diasumsikan memilih jawaban dengan skor tertinggi.

Kesimpulan berdasarkan hasil pengujian dibuktikan bahwa kualitas perangkat lunak *system manajemen jaringan* yang dihasilkan jika diukur berdasarkan kualitas perangkat lunak dengan mengadopsi ISO 9126 dalam kriteria Baik dengan persentase tanggapan responden sebesar **82,5 %**.

5. PENUTUP

Kesimpulan yang diperoleh setelah melalui tahap-tahap pengembangan sistem keamanan jaringan pada Pondok Pesantren Madinatunnajah adalah sebagai berikut :

1. Pada sistem berjalan, sebelum diterapkannya sebuah system otentikasi maka keamanan jaringan rentan dari penyusup masuk ke dalam jaringan.
2. Dengan adanya sistem keamanan jaringan ini, memungkinkan adanya sistem otentikasi user dan monitoring serta manajemen terhadap user (Guru, Staff, Siswa dan tamu) yang terkoneksi dan lebih aman dalam menggunakan internet pada jaringan di Pesantren Madinatunnajah.
3. Sistem keamanan jaringan yang dirancang, dapat mengatur layanan apa saja yang berhak diakses oleh user dan apa saja yang tidak.

REFERENCE

- Al-Qutaish, Rafa, E. (2010) "Quality Models in Software Engineering Literature: An Analytical and Comparative Study." *Journal of American Science*, Vol. 6: 166-175.
- Anjik Sumkaaji, S. Kom & Rianto, S. Kom. (2008) *Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan*. Yogyakarta : Andi
- Hassel, Jonathan. (2002) *RADIUS*, Cambridge, Massachusetts : O'Reilly Media.
- Moch. Linto Herlambang, dkk. (2008) *Panduan Lengkap Menguasai Router Masa Depan Menggunakan MikroTik RouterOS*. Yogyakarta : ANDI
- Hoed, B.H, (1995) *Diskusi Kelompok Terfokus*, Jakarta :Fakultas Sastra Universitas Indonesia,.
- Sofana, Iwan. (2008) *Membangun Jaringan Komputer*. Bandung :Informatika,.
- Kajian Pustaka, (*Pengertian dan Jenis-jenis Topologi Jaringan*, www.kajianpustaka.com (diakses 30 Maret 2015)
- Krueger, RichardA, (1998) *Focus Group A Practical Guide for Applied Research*, Newbury Park, California: Sage Publication,Inc..
- Litosseliti,L,(2003) *Using Focus Group Discussion in Research*, London: Continum.
- Onno W. Purbo, (2006) *Buku Pegangan Internet Wireless dan Hotspot*, Jakarta: PT. Elex Media Komputindo.
- Presman, (2012) *Software Engineering: A Practitioner's Approach, 7th ed*. Dialih bahasakan oleh Adi Nugroho, J, Leopold Nikijuluw George dan et.al. Yogyakarta: Andi.
- Tanenbaum, Andrews S. (2000) *Jaringan Komputer. Jilid 1. Terjemahan Gurnita Priatna*. Jakarta: Prenhallindo.
- Utomo, Eko Priyo.(2011) *Membangun Jaringan Komputer dan Server Internet*, Yokyakarta: MediaKom,.
- Yohan Jati Waloeya,(2012) *Seri Belajar Kilat Computer Networking*, Yogyakarta: Elcom.