

PENGEMBANGAN SISTEM KEAMANAN JARINGAN KOMPUTER BERBASIS MIKROTIK PADA SMK NEGERI 1 INDRALAYA UTARA

COMPUTER NETWORK SECURITY SYSTEM DEVELOPMENT BASED ON MIKROTIK AT SMK NEGERI INDRALAYA UTARA

¹Imam Solikin, ²Suryayusra, ³Maria Ulfa

¹Fakultas Vokasi, ²Fakultas Ilmu Komputer, ³Fakultas Vokasi
Universitas Bina Darma

email : ¹imamsolikin@binadarma.ac.id, ²suryayusra@binadarma.ac.id, ³maria.ulfa@binadarma.ac.id

Abstract. Internet is now a major requirement so that almost all activities are done using internet network. SMK Negeri 1 Indralaya Utara is a public vocational high school that has currently implemented internet network as part of all activities and learning media existed in laboratory room, classroom, teacher room, principal room, and library. Computer network security system uses LAN (Local Area Network) and WLAN (Wireless Local Area Network) management and has implemented network security applications on access point and modem devices used. However, there are still a variety of problems in the network that often occur, such as slow network performance and sometimes not connected properly. This can be caused by several factors such as intruder attacks from the local network or the internet or viruses that exist on each computer used. Based on these problems, the existing network security system will be developed to improve network quality and performance at SMK Negeri 1 Indralaya Utara. Mikrotik router is a solution that will be used in this research because it has a complete features of network security system and easy to use. This research will be implemented firewall security system, web proxy, and user manager (radius server) with research method of NDLC (Network Development Life Cycle). The implementation of firewall and web proxy in network security system of SMK Negeri 1 North Indralaya would help network administrator in arranging access of network user, which are the teachers, clerk and student in using internet service.

Keywords: Network Security System, Mikrotik, NDLC (Network Development Life Cycle).

Abstrak. Internet saat ini menjadi kebutuhan yang utama sehingga hampir semua aktivitas dilakukan dengan jaringan internet. SMK Negeri 1 Indralaya Utara adalah sekolah menengah kejuruan negeri yang saat ini telah menerapkan jaringan internet sebagai bagian dari semua aktivitas dan media pembelajaran yang ada di ruang laboratorium, kelas dan pada bagian ruang kantor guru, kepala sekolah serta perpustakaan. Sistem keamanan jaringan komputer menggunakan manajemen jaringan LAN (Local Area Network) dan WLAN (Wireless Local Area Network) dan telah menerapkan aplikasi keamanan jaringan pada perangkat acces point maupun modem yang digunakan, pada jaringan saat ini masih menemukan berbagai permasalahan yaitu sering terjadi kinerja jaringan menjadi lambat dan terkadang tidak terkoneksi dengan baik, hal ini bisa disebabkan oleh beberapa faktor antara lain serangan penyusup dari jaringan lokal maupun internet atau virus yang ada pada masing-masing komputer yang digunakan. Dari permasalahan tersebut akan dikembangkan sistem keamanan jaringan yang ada guna meningkatkan kualitas dan kinerja jaringan pada SMK Negeri 1 Indralaya Utara. Mikrotik router adalah salah satu solusi yang akan digunakan pada penelitian ini karena mikrotik router memiliki fitur-fitur sistem keamanan jaringan yang lengkap dan mudah digunakan, pada penelitian ini akan diimplementasikan sistem keamanan firewall, web proxy dan user

manager (radius server) dengan metode penelitian menggunakan NDLC (Network Development Life Cycle). Penerapan sistem keamanan jaringan dengan firewall dan web proxy pada jaringan SMK Negeri 1 Indralaya Utara sangat membantu administrator jaringan dalam mengatur akses para pengguna jaringan yaitu guru, pegawai dan siswa dalam menggunakan layanan internet..

Kata Kunci: *Sistem Keamanan Jaringan, Mikrotik, NDLC (Network Development Life Cycle).*

1. Pendahuluan

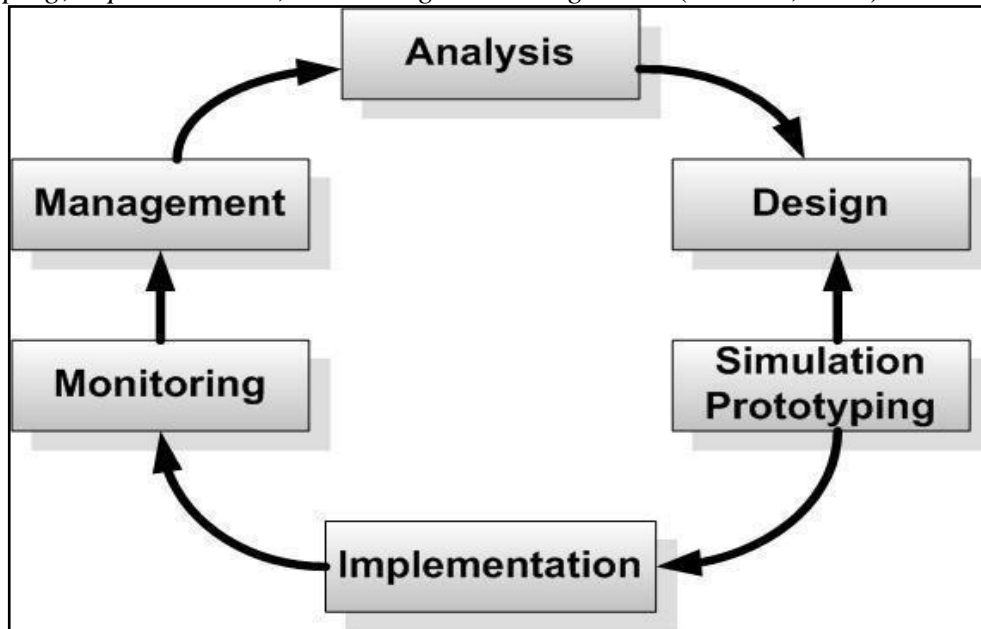
Perkembangan Jaringan internet yang begitu pesat menjadi salah satu hal yang menarik untuk dibahas, ada banyak sumber daya yang dapat dimanfaatkan dari internet seperti *email, newgroups, chatting, phone call, Internet Telephony (VOIP), real player streaming, internet radio broadcasting, streaming video, video conferencing* dan lain-lain).Keamanan saat ini menjadi suatu kebutuhan dasar karena komputasi global tidak aman, banyak negara sudah mulai menaruh perhatian pada keamanan komputer atau *internet security* dengan adanya hukum *cyber* atau hukum mengenal jaringan kejahatan komputer, dengan adanya hukum yang mengatur keamanan di bidang komputer, pelanggaran atau kejahatan dalam bidang ini tidak hilang sama sekali, tetapi setidaknya ada langkah yang akan diambil seandainya terjadi pelanggaran, akan tetapi sebenarnya masalah utama terletak pada pengguna atau user yang menggunakan komputer. (Stiawan,2005).

Pada bidang pendidikan kebutuhan akan layanan internet saat ini menjadi kebutuhan pokok, dimana pada beberapa kegiatan yang ada disekolah bergantung pada fasilitas jaringan internet yang digunakan, seperti pada SMK Negeri 1 Indralaya utara, jaringan internet sebagai media penggunaan website sekolah untuk mendapatkan informasi yang ada disekolah, media pembelajaran online berupa penggunaan e-learning, penggunaan website PSB (Penerimaan Siswa Baru), kegiatan yang ada dilaboratorium dalam proses belajar mengajar, diperpustakaan untuk mencari atau penggunaan *digital library* sehingga sistem keamanan jaringan yang ada perlu ditingkatkan dan diperhatikan.

SMK Negeri 1 Indralaya Utara telah menerapkan sistem keamanan jaringan dengan menggunakan aplikasi yang ada pada perangkat jaringan seperti *access point* dan modem, akan tetapi sistem keamanan yang ada pada perangkat tersebut, masih memiliki banyak kelemahan dan keterbatasan dalam penggunaannya serta lebih rentan akan terjadinya kerusakan. Dari permasalahan di atas, pada penelitian ini diberikan solusi dengan melakukan pengembangan sistem keamanan jaringan berbasis mikrotik pada SMK Negeri 1 Indralaya Utara. Mikrotik dikenal sebagai router dimana dapat berupa sistem operasi atau perangkat (*routerboard*) yang memiliki fitur-fitur yang sangat lengkap dalam manajemen sistem keamanan jaringan. Dengan penerapan mikrotik pada jaringan SMK Negeri 1 Indralaya Utara diharapkan dapat memiliki sistem keamanan jaringan yang tidak rentan terhadap berbagai bentuk gangguan atau serangan baik dalam jaringan *local* maupun dari jaringan internet., desktop atau web”.

2. Metode Penelitian

Pada penelitian ini akan menggunakan metode *Network Development Life Cycle*(NDLC) merupakan sebuah metode yang terdiri dari *analysis, design, simulation prototyping, implementation, monitoring* dan *management*. (Stiawan, 2009).



(Sumber : Applied Data Communications, A business-Oriented Approach, James E. Goldman, Philips T. Rawles, Third Edition, 2001, John Wiley & Sons : 470)

Gambar1. Metode NDLC (Network Development Life Cycle)

1. Analysis : Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan user (pengguna), dan analisa topologi jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya;
 - a. Wawancara, dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke level bawah, agar mendapatkan data yang konkrit dan lengkap.
 - b. Survey langsung kelapangan, pada tahap analisis juga biasanya dilakukan survey langsung kelapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya sebelum masuk ke tahap *design*.
 - c. Membaca manual dokumentasi, pada *analysis* awal ini juga dilakukan dengan mencari informasi dari manual dokumentasi yang mungkin pernah dibuat sebelumnya.
 - d. Memahami setiap data yang didapat dari data-data sebelumnya, maka perlu dilakukan analisa data tersebut untuk masuk ke tahap berikutnya. Adapun yang bisa menjadi pedoman dalam mencari data pada tahap analisis ini adalah;
 - *User* atau pengguna : jumlah user, kegiatan yang sering dilakukan, level teknisi *user*
 - Media *hardware* dan *software* : peralatan yang ada, status jaringan, ketersediaan data yang dapat diakses dari peralatan, aplikasi (*software*) yang digunakan

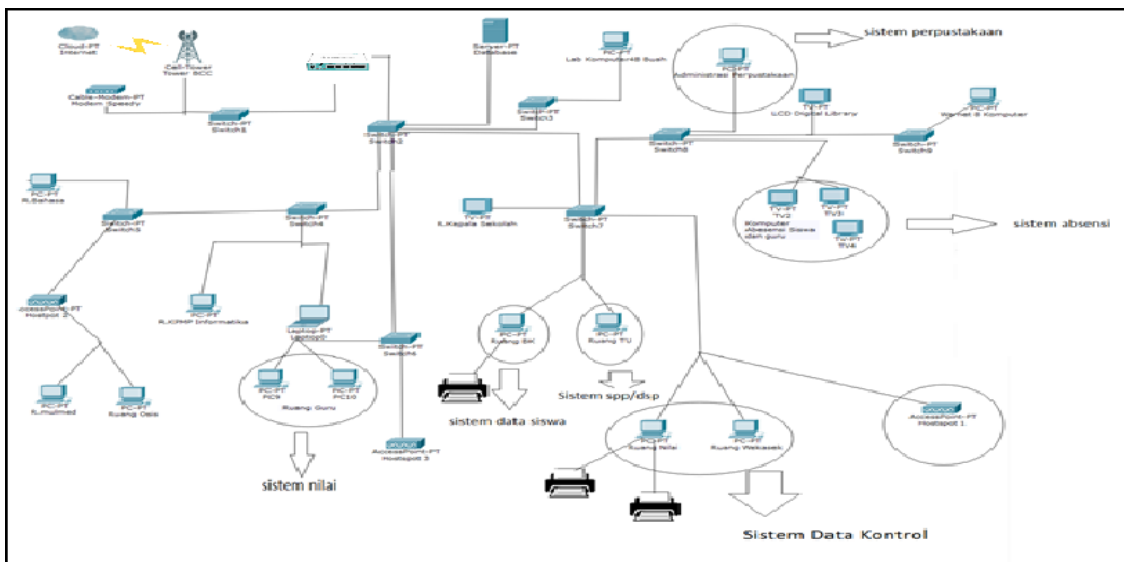
- Data : jumlah pengguna, jumlah sistem aplikasi yang digunakan, sistem keamanan yang sudah ada dalam mengamankan data.
 - *Network* : konfigurasi jaringan, *volume* trafik jaringan, *protocol*, *monitoring network* yang ada saat ini, harapan dan rencana pengembangan kedepan
 - Perencanaan fisik : masalah listrik, tata letak, ruang khusus, sistem keamanan yang ada, dan kemungkinan akan pengembangan kedepan.
2. *Design* : Dari data-data yang didapatkan sebelumnya, tahap *design* ini akan membuat gambar *design topology* jaringan interkoneksi yang akan dibangun, *design* bisa berupa *design struktur topology*, *design akses data*, *design tata layout* perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang *network* yang akan dibangun.
 3. *Simulation Prototype* : pada tahap ini membuat dalam bentuk simulasi dengan bantuan Tools khusus di bidang *network* dengan aplikasi virtualbox, hal ini dimaksudkan untuk melihat kinerja awal dari *network* yang akan dibangun.
 4. *Implementation* : di tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam tahap implementasi peneliti akan menerapkan semua yang telah direncanakan dan di *design* sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil atau gagalnya *network* yang akan dibangun.
 5. *Monitoring* : setelah implementasi tahapan *monitoring* merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari *user* pada tahap awal analisis, maka perlu dilakukan kegiatan *monitoring*. *Monitoring* bisa berupa melakukan pengamatan pada:
 - a. *Infrastruktur hardware* : dengan mengamati kondisi kehandalan sistem yang telah dibangun.
 - b. Memperhatikan jalannya packet data di jaringan (*pewaktu*, *latency*, *packet loss*, *throughput*)
 - c. Metode yang digunakan untuk mengamati kondisi jaringan. Pendekatan yang paling sering dilakukan adalah pendekatan *Network Management*, dengan pendekatan ini maka *network* dapat di monitor secara otomatis.
 6. *Management*, pada tahap manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah *Policy*, kebijakan perlu dibuat untuk membuat atau mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama.

3. Hasil dan Pembahasan

Rancangan Topologi

Dalam perancangan topologi pengembangan sistem keamanan jaringan SMK Negeri 1 Indralaya Utara, dimana terdapat penambahan perangkat jaringan yaitu sebuah mikrotik *routerboard* Rb951u 2HnD yang diletakkan diantara jaringan *local* dan jaringan internet, perangkat mikrotik *routerboard* dapat berperan sebagai penghubung sekaligus mengatur lalu lintas internet, baik yang masuk maupun keluar dari jaringan *local*, selain itu mikrotik *routerboard* memiliki beberapa *interface ethernet* dan memiliki sebuah *interface wireless*, pada *interface ethernet* yang terdapat pada mikrotik

routerboard dapat di fungsikan sebagai *port switch* biasa yang dapat dihubungkan langsung ke jaringan *local*, pada desain topologi jaringan ini satu *interface ethernet* terhubung ke modem internet dan sisa dari beberapa *interface ethernet* akan dihubungkan di beberapa *switch* yang terdapat pada jaringan SMK Negeri 1 Indralaya Utara sedangkan pada *interface wireless* dapat juga difungsikan sebagai *access point* pada jaringan *wireless* (wifi), yang nantinya akan dihubungkan di beberapa *access point* yang ada di jaringan SMK Negeri 1 Indralaya Utara.



Gambar 2. Topologi Sistem Keamanan Jaringan SMK Negeri 1 Indralaya Utara

Pemetaan IP Address pada JaringanSMKN 1 Indralaya Utara

Pada tahapan pemetaan IP Address yang akan diterapkan di jaringan LAN dan WLAN SMK Negeri 1 Indralaya Utara, terlebih dahulu dilakukan pembagian IP Address dengan menggunakan metode *subnetting*, dimana pada penelitian ini menggunakan teknik pembagian CIDR (*Classes Inter Domain Routing*), hal ini bertujuan untuk memudahkan *administrator* jaringan dalam melakukan pengelompokan IP Address berdasarkan kebutuhan pada setiap unit ruangan kerja SMK Negeri 1 Indralaya Utara

Table 1. Pemetaan IP Address pada Jaringan LAN SMKN

No	Nama	Network	Range IP Address	Host	Broadcast
1	Ruang Server	200.200.20.0/28	200.200.20.1 200.200.20.14	– 14	200.200.20.15
2	Ruang Guru	200.200.20.16/28	200.200.20.17 200.200.20.30	– 14	200.200.20.31
3	Ruang Pegawai TU	200.200.20.32/28	200.200.20.33 200.200.20.46	– 14	200.200.20.47
4	Ruang Laboratorium TKJ 1	200.200.20.48/28	200.200.20.49 200.200.20.62	– 14	200.200.20.63
5	Ruang Laboratorium TKJ 2	200.200.20.64/28	200.200.20.65 200.200.20.78	– 14	200.200.20.79
6	Ruang Laboratorium RPL 1	200.200.20.80/28	200.200.20.81 200.200.20.94	– 14	200.200.20.95

7	Ruang Laboratorium RPL 2	200.200.20.96/28	200.200.20.97 200.200.20.110	-	14	200.200.20.111
8	Ruang Laboratorium Teknik Mesin	200.200.20.112/28	200.200.20.113 200.200.20.126	-	14	200.200.20.127

Table 2. Pemetaan IP Address pada Jaringan WLAN

No	Nama	Network	Range IP Address	Host	Broadcast	
1	Ruang Server	200.200.20.128/28	200.200.20.129 200.200.20.142	-	14	200.200.20.143
2	Ruang Guru	200.200.20.144/28	200.200.20.145 200.200.20.158	-	14	200.200.20.159
3	Ruang Pegawai TU	200.200.20.160/28	200.200.20.161 200.200.20.174	-	14	200.200.20.175
4	Ruang Laboratorium	200.200.20.176/28	200.200.20.177 200.200.20.190	-	14	200.200.20.191
5	Ruang Perpustakaan	200.200.20.192/28	200.200.20.193 200.200.20.206	-	14	200.200.20.207
6	Ruang Kepala Sekolah	200.200.20.208/28	200.200.20.209 200.200.20.222	-	14	200.200.20.223

Simulasi Prototype Sistem Keamanan Berbasis Mikrotik

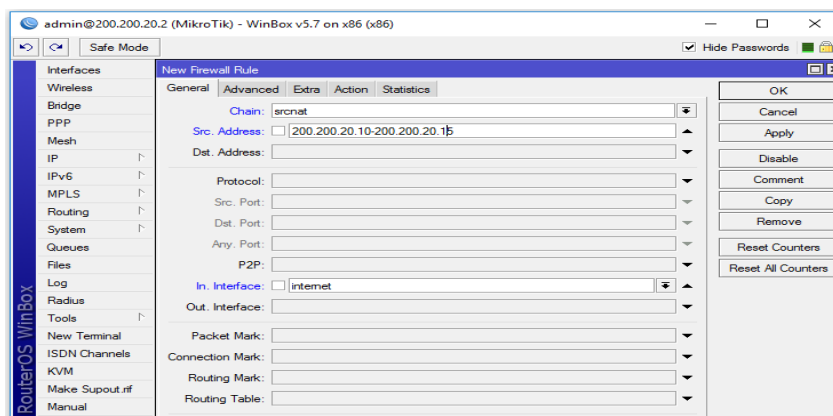
Proses simulasi yang dilakukan sebelum implementasi langsung pada jaringan SMK Negeri 1 Indralaya Utara, hal ini untuk melihat kinerja dari mikrotik *routerboard* dalam penerapan sistem keamanan jaringan yang akan dibangun, dalam simulasi *prototype* ini dilakukan beberapa ujicoba terhadap sistem keamanan jaringan diantaranya pada sistem keamanan *firewall*, sistem *proxy* (web-proxy) serta sistem *user manager* (radius server). Berikut adalah beberapa tahapan ujicoba yang akan dilakukan.

1. Sistem keamanan *firewall*

Dalam melakukan proses simulasi pada sistem *firewall* yang ada pada mikrotik *routerboard* yaitu ada dua bagian yang pertama NAT (*Network Address Translation*) yang bertugas untuk melakukan perubahan IP paket yang akan dikirim ke internet, NAT akan mengubah paket data yang berasal dari komputer *client* seolah-olah berasal dari *router* dan *filter* bertugas memeriksa paket data yang ditujukan bagi mikrotik *routerboard* sendiri. Berikut adalah tahapan simulasi sistem *firewall* :

2. Sistem *Firewall* untuk IP Address tertentu

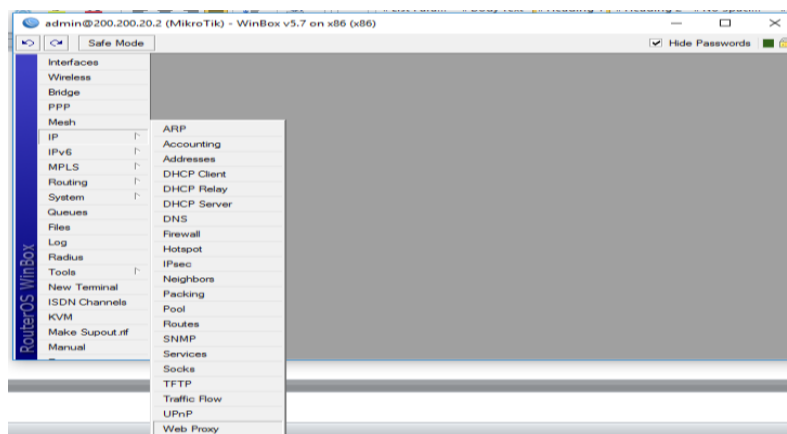
Pada mikrotik *routerboard* akan menjalankan NAT dengan mengaktifkan perintah `action=masquerade`, perintah ini menyebabkan server-server yang berada di internet tidak mengetahui bahwa sebenarnya yang mengakses adalah komputer *client* dengan IP Address *private* yang disembunyikan.



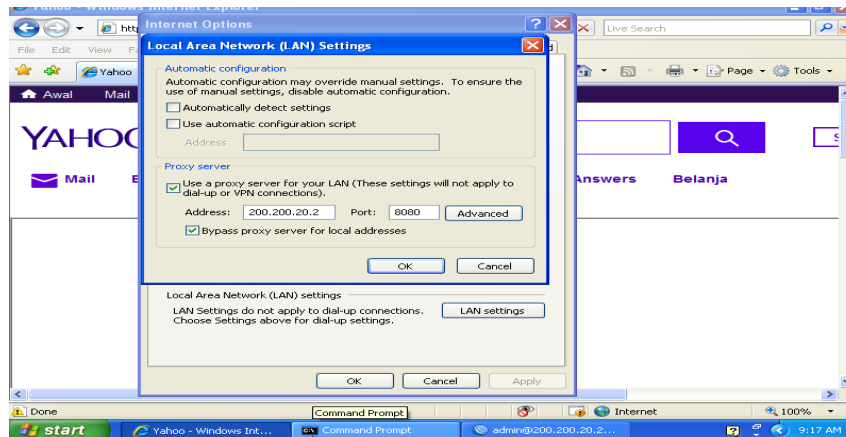
Gambar 3. Konfigurasi *Firewall* NAT

3. Sistem Keamanan *Web Proxy*

Web proxy merupakan salah satu fitur dari mikrotik *routerboard* yang bertugas sebagai perantara antara *browser* yang ada di komputer pengguna dengan web server yang berada di internet. Pada penerapannya *proxy* sangat berbeda dengan *firewall*, dimana jika hanya menggunakan *firewall* maka mikrotik *routerboard* hanya akan meneruskan HTTP *request* yang dibuat oleh komputer *client* ke internet. Namun jika dikombinasikan juga menggunakan *proxy* maka mikrotik *routerboard* dapat memeriksa *content* dari HTTP *request* maupun respon secara keseluruhan. Untuk konfigurasi *web proxy*.



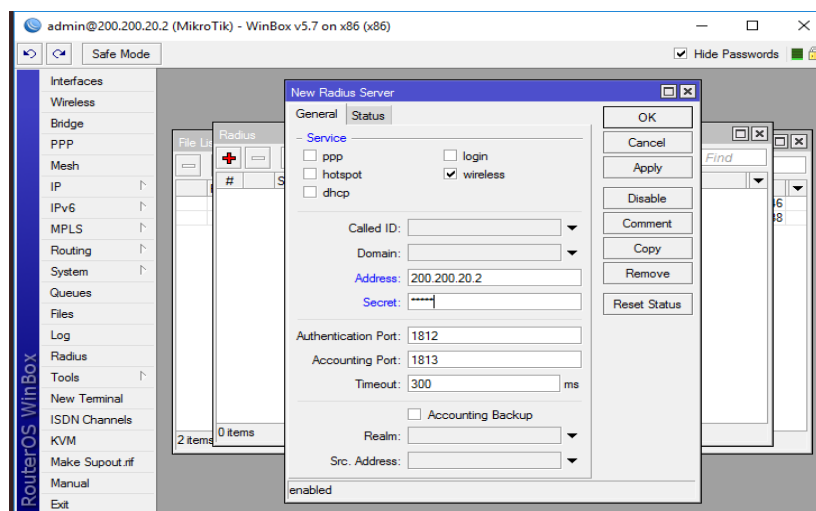
Gambar 4. Konfigurasi *Web Proxy* di Mikrotik



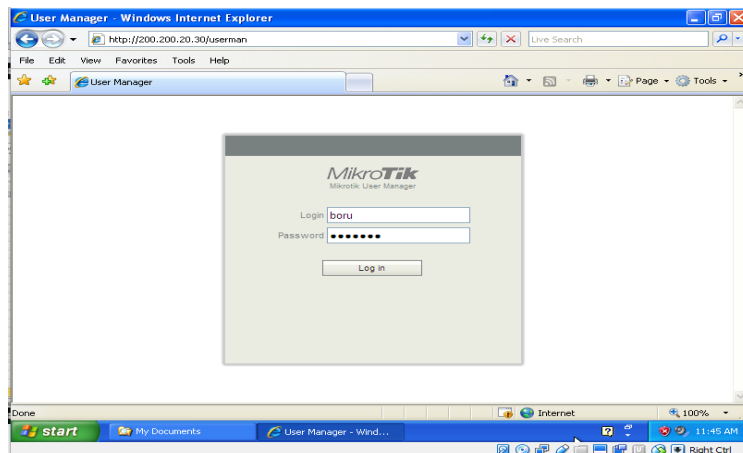
Gambar 5. Konfigurasi Proxy di Komputer Client

4. Sistem Keamanan Radius Server (*User Manager*)

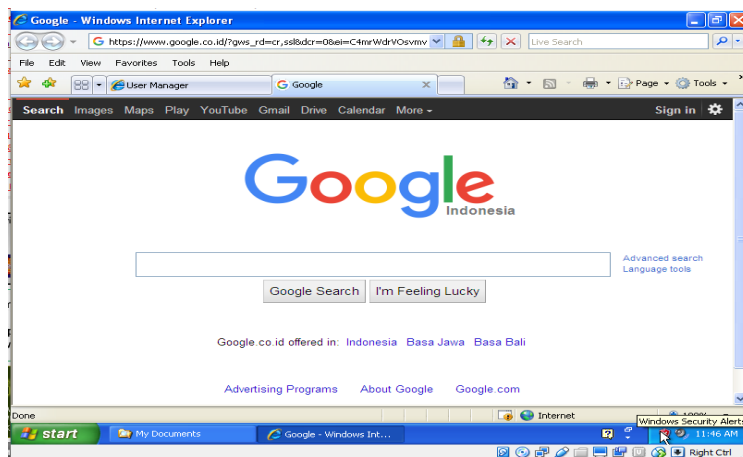
User manager dalam mikrotik adalah Radius server yang merupakan *protocol* jaringan yang menjalankan *service* manajemen *Authentication, Authorization, dan Accounting (AAA)* secara terpusat untuk pengguna (*client*) yang terkoneksi pada jaringan dan hendak menggunakan *resource* yang terdapat dalam jaringan LAN dan WLAN SMK Negeri 1 Indralaya Utara, sehingga peran dari *user manager* ini dapat menggantikan konfigurasi *static lease* di DHCP Server pada jaringan serta *Access List* pada *wireless* menjadi terpusat.



Gambar 6. Konfigurasi User Manager Tahap



Gambar 7. Menu Login Komputer client



Gambar 8. Hasil Ujicoba Koneksi Internet Komputer Client

4. Kesimpulan

Penerapan sistem keamanan jaringan dengan *firewalldan web proxypada* jaringan SMK Negeri 1 Indralaya Utara sangat membantu *administrator* jaringan dalam mengatur akses para pengguna jaringan yaitu guru, pegawai dan siswa dalam menggunakan layanan internet. Selain itu *administrator* jaringan SMK Negeri 1 Indralaya Utara dapat dengan mudah melakukan monitoring terhadap jaringan LAN (*Local Area Network*) maupun jaringan WLAN (*Wireless Local Area Network*) apabila terjadi masalah koneksi dan keamanan dalam jaringan. Dalam manajemen pengguna jaringan dengan menerapkan sistem *user manager* (radius server) *administrator* jaringan SMK Negeri 1 Indralaya Utara dapat memantau setiap pengguna (*user*) dengan mudah karena memiliki satu *accountlogin* yang sama dan dapat diterapkan secara bersamaan pada jaringan LAN maupun jaringan WLAN

Daftar pustaka

- Herlambang, Moch Lintang, Azis Catur. 2008. *Penduan Lengkap Menguasai Router Masa Depan Menggunakan Mikrotik OS*. Yogyakarta : Andi Offset.
- James E. Goldman, Philips T. Rawles, Third Edition, 2001, *Applied Data Communications, A business-Oriented Approach*, , John Wiley & Sons
- Rahardjo, Budi. 2002. Keamanan Sistem Informasi Berbasis Internet. Ilmu Komputer ; <http://www.ilmukomputer.com/>.
- Stiawan, Deris. 2005. *Sistem Keamanan Komputer*. Jakarta : ElexMedia Komputindo.
- Stiawan, Deris. 2009. Internetworking Development and Design Life Cycle. Unsri.ac.id/upload/arsip/network_development_cycles.pdf.
- Sukmaaji, Anjik. Rianto. 2008. Jaringan Komputer. Yogyakarta : Andi Offset.
- Towidjojo, Rendra. 2008. *Teori dan Implementasi Menggunakan RouteMikrotik*. Bandung : Informatika