PENERAPAN SISTEM KEAMANAN JARINGAN SMK NEGERI 1 INDRALAYA UTARA DENGAN MIKROTIK

Suryayusra[1], Imam Solikin[2], Maria Ulfa[3]
Universitas Bina Darma
Jalan Jenderal Ahmad Yani No.3 Palembang
Sur-el: suryayusra@binadarma.ac.id[1], imamsolikin@binadarma.ac.id[2], maria.ulfa@binadarma.ac.id[3]

Abstract: *SMK Negeri 1 Indralaya Utara is a public vocational high school that has implemented internet network as part of all activities and learning media. Computer network security system using LAN and WLAN management has implemented network security applications on access point on the network, some problems that often occur network performance becomes slow and sometimes not connected properly. It caused by several factors such as intruder attacks from the local network or the internet or viruses that exist on each computer used. From these problems will be developed existing network security system to improve network quality and performance. Mikrotik router is one solution that will be used in this research because mikrotik router has features of network security system complete and easy to use. Implementation of network security system with firewall and web proxy on network, very help network administrator in arranging access of network user in using internet service.*

Keywords: *Network Security System, Mikrotik, Computer Network*

Abstrak : *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, Sistem keamanan jaringan komputer yang ada, dalam memanajemen jaringan LAN dan WLAN telah menerapkan aplikasi keamanan jaringan pada perangkat acces point yang digunakan, permasalahan pada jaringan yaitu kinerja jaringan menjadi lambat dan terkadang tidak terkoneksi, disebabkan beberapa faktor antara lain serangan penyusup dari jaringan lokal maupun internet atau virus yang ada pada komputer. 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 solusi yang akan digunakan pada penelitian ini karena memiliki fitur-fitur sistem keamanan jaringan yang lengkap dan mudah digunakan, penerapan beberapa sistem keamanan tersebut dapat meningkatkan kinerja jaringan SMK Negeri 1 Indralaya Utara menjadi lebih optimal dan efisien dalam penggunaanya.*

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. Jaringan internet yang maha luas ini diibaratkan suatu komunitas yang terhubung antara satu dengan yang lain secara virtual. 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 computer (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 acces *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 penulis memberikan 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 memanajemen 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. Tujuan penelitian ini adalah Membangun sistem keamanan jaringan komputer dengan menerapkan sistem, *firewall*, *proxy* serta *Radius server* pada jaringan komputer SMK Negeri 1 Indralaya Utara, baik didalam jaringan *LAN* (*Local Area Network*) maupun jaringan *WLAN* (*Wireless Local Area Network*).

Manfaat penelitian ini adalah: (1) Membantu *Administrator* jaringan SMK Negeri 1 Indralaya Utara dalam meningkatkan sistem keamanan jaringan computer; (2) Mempermudah dalam memanajemen sistem keamanan jaringan LAN (*Local Area Network*) maupun jaringan WLAN (*Wireless Local Area Network*); (3) Mempermudah dalam *monitoring* dan *maintenance* jaringan apabila dalam kondisi tidak terkoneksi atau rusak; (4) Dapat mengontrol kegiatan para siswa, guru dan pegawai TU (Tata Usaha) dalam menggunakan Internet.

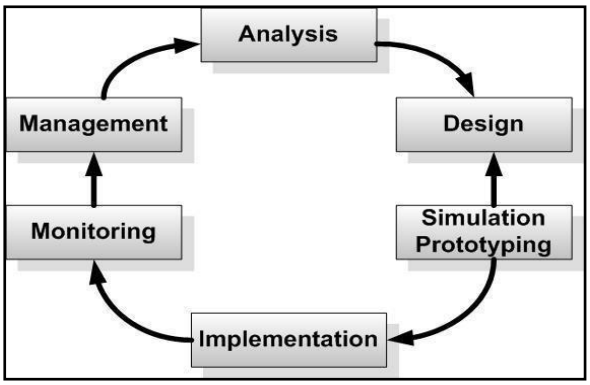
2. METODOLOGI PENELITIAN

2.1 Waktu dan Tempat Penelitian

Waktu penelitian ini akan dilaksanakan dari bulan Januari 2017 sampai dengan bulan Oktober 2017. Adapun tempat penelitian yaitu pada SMK Negeri 1 Indralaya Utara yang beralamatkan di Jalan Raya Tanjung Baru Kecamatan Indralaya Utara Kabupaten Ogan Ilir**.**

2.2 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).



Gambar 1. Metode NDLC (*Network Development Life Cycle*)

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;

1) Wawancara, dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke level bawah, agar mendapatkan data yang konkrit dan lengkap.
2) Survey langsung kelapangan, pada tahap analisis juga biasanya dilakukan survey langsung kelapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya sebelum masuk ke tahap *design*.
3) Membaca manual dokumentasi, pada *analysis* awal ini juga dilakukan dengan mencari informasi dari manual dokumentasi yang mungkin pernah dibuat sebelumnya.
4) 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 analysis ini adalah; (a) *User* atau pengguna: jumlah user, kegiatan yang sering dilakukan, level teknis *user;* (b) Media *hardware* dan *software*: peralatan yang ada, status jaringan, ketersedian data yang dapat diakses dari peralatan, aplikasi (*software*) yang digunakan; (c) Data: jumlah pengguna, jumlah sistem aplikasi yang digunakan, sistem keamanan yang sudah ada dalam mengamankan data; (d) *Network*: konfigurasi jaringan, *volume* trafik jaringan, *protocol*, *monitoring network* yang ada saat ini, harapan dan rencana pengembangan kedepan; (e) Perencanaan fisik: masalah listrik, tata letak, ruang khusus, sistem keamanan yang ada, dan kemungkinan akan pengembangan kedepan.

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.

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.

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.

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 (pewaktuan, *latency*, *packet loss*, *troughput)*; (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 utuh.

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.

2.3 Keamanan Jaringan Komputer

Masalah keamanan komputer merupakan salah satu aspek penting dari sebuah sistem informasi. Seringkali masalah keamanan berada di urutan kedua atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu performa sistem, seringkali keamanan dikurangi atau bahkan ditiadakan. Informasi pada era ini sudah menjadi komoditas yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah "*information-based society*". Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual. Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi.

Terhubungnya LAN (*Local Area Network*) atau komputer ke internet membuka potensi adanya lubang keamanan (*security hole*) yang tadinya bisa ditutup dengan mekanisme keamanan secara fisik. Ini sesuai dengan pendapat bahwa kemudahan mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri, semakin tinggi tingkat keamanan, semakin sulit untuk mengakses informasi. (Sukmaaji, 2008).

2.4 Kejahatan Komputer

Kejahatan komputer dapat digolongkan dari sangat berbahaya sampai mengesalkan (*annoying*). Banyak cara yang dilakukan oleh penjahat komputer untuk memenuhi keinginannya. Untuk mengatisipasi kondisi tersebut perlu ditingkatkan sistem pengamanan. Dalam teknologi komputer keamanan dapat diklasifikasikan menjadi empat yaitu: (Rahardjo, 2002): (1) Keamanan yang bersifat fisik, termasuk akses orang ke gedung, peralatan dan

media yang digunakan; (2) Keamanan yang berhubungan dengan orang, termasuk identifikasi dan profil risiko dari orang yang mempunyai akses (pekerjaa), seringkali kelemahan sistem informasi bergantung kepada manusia (pemakai dan pengelola); (3) Keamanan dari data dan media serta teknik komunikasi, yang termasuk didalam kelas ini adalah kelemahan dalam software yang digunakan untuk mengelola data; (4) Keamanan dalam operasi, termasuk prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setelah serangan.

2.5 Aspek-Aspek Keamanan Komputer

Keamanan komputer melingkupi empat aspek, yaitu *privacy, integrity, authentication* dan *availability*, selain keempat hal diatas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu access control dan *non-repudiantion* (Rahardjo, 2002).

1) *Privacy/Confidentiality:* adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Privacy lebih ke arah data-data yang sifatnya privat, sedangkan confidentiality biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu.
2) *Integrity*: adalah aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, trojan horse atau pemakai lain yang mengubah informasi tanpa izin merupakan contoh masalah yang harus dihadapi.

2.6 Sejarah Mikrotik

Mikrotik adalah sebuah perusahaan kecil yang berkantor pusat di Latvia, bersebelahan dengan Rusia. Pembentukannya diprakarsai oleh John Trully dan Arnis Riekstins. John Trully adalah seorang berkewarganegaraan Amerika yang berimigrasi ke Latvia. Di Latvia ia bertemu dengan Arnis, Seorang sarjana Fisika dan Mekanik sekitar tahun 1992.

John dan Arnis mulai me-routing dunia pada tahun 1996 (misi mikrotik adalah me-*routing* seluruh dunia). Mulai dengan system *Linux* dan *MS-DOS* yang dikombinasikan dengan teknologi *Wireless-LAN* (WLAN) Aeronet berkecepatan 2 Mbps di Moldova, Negara tetangga Latvia, baru kemudian melayani lima pelanggan di Latvia. Prinsip dasar mereka bukan membuat *Wireless ISP* (W-ISP), tetapi membuat program *router* yang handal dan dapat dijalankan diseluruh dunia. Latvia hanya merupakan tempat eksprimen John dan Arnis, karena saat ini mereka sudah membantu Negara-negara lain termasuk Srilanka yang melayani sekitar 400 pengguna.

Linux yang pertama kali digunakan adalah Kernel 2.2 yang dikembangkan secara bersama-sama dengan bantuan 5-15 orang staf *Research and Development* (R&D). Mikrotik yang sekarang menguasai dunia *routing* di Negara-negara berkembang. Menurut Arnis, selain staf di lingkungan *Mikrotik*, mereka juga merekrut tenaga-tenaga lepas dan pihak ketiga yang dengan intensif mengembangkan *Mikrotik* secara marathon (Towidjojo, 2008)

3. HASIL

3.1 Perancangan Sistem Keamanan Jaringan SMK Negeri 1 Indralaya Utara

Dalam proses perancangan jaringan untuk menerapkan sistem keamanan menggunakan mikrotik router, perlu dilakukan redesain ulang terhadap jaringan yang telah ada karena akan berpengaruh pada kualitas jaringan yang akan dibangun nantinya. Redesain ulang yang akan dilakukan ini sebelum di implementasikan pada jaringan sebenarnya harus dilakukan ujicoba terlebih dahulu, dalam pengembangan sistem keamanan jaringan *LAN* dan *WLAN* SMK Negeri 1 Indralaya Utara ada beberapa tahapan yang akan dilakukan di antaranya: desain topologi jaringan, pemetaan IP *Address*, instalasi dan konfigurasi mikrotik sebagai server, konfigurasi sistem keamanan yang akan digunakan yaitu *firewall*, *web proxy* (*proxy*) dan *user manager* (*radius server*).

3.2 Topologi Sistem Keamanan Jaringan SMK Negeri 1 Indralaya Utara

Perancangan topologi jaringan yang akan dibangun dengan melihat hasil analisis yang telah dilakukan pada tahapan desain dari topologi jaringan sebelumnya. Desain topologi jaringan baru yang dilakukan merupakan salah satu upaya untuk pengembangan jaringan komputer SMK Negeri 1 Indralaya Utara. Perancangan topologi sistem keamanan jaringan ini dibangun secara dinamis, hal ini memungkinkan apabila terjadi suatu perubahan atau ingin mengupdate sistem maupun perangkat jaringan dengan resiko biaya yang tidak terlalu mahal.

Dalam perancangan topologi pengembangan sistem keamanan jaringan SMK Negeri 1 Indralaya Utara, dimana terdapat pendambahan 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 dibeberapa *access point* yang ada di jaringan SMK Negeri 1 Indralaya Utara.

3.3 Pemetaan IP Address pada Jaringan SMKN 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. Pembagian IP *Address* dapat dilihat seperti pada table 1 dan 2.

Tabel 1. Pemetaan *IP Address* pada Jaringan LAN SMKN 1 Indralaya Utara

No	Nama	*Network*	*Range IP Adrress*	*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

Tabel 2. Pemetaan IP *Address* pada Jaringan WLAN SMKN 1 Indralaya Utara

No	Nama	*Network*	*Range IP Adrress*	*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

3.4 Simulasi *Prototype* Sistem Keamanan Berbasis Mikrotik SMKN 1 Indralaya Utara

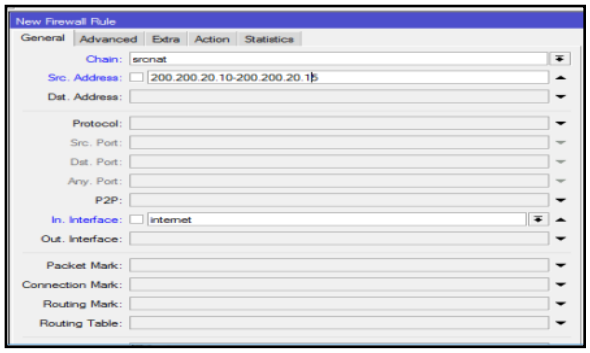
Proses simulasi yang dilakukan sebelum implementasi langsung pada jaringan SMK Negeri 1 Indralaya Utara, hal ini untuk melihat kinerja dari mikrotik *routerboard* dalam penerapan sistem keamanan jaringan yang akan dibangun, dalam simulasi *prototype* ini dilakukan beberapa ujicoba terhadap sistem keamanan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

3.4.1 Sistem Keamanan *Firewall*

1) 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. Pada konfigurasi perintah di atas dapat dilihat pada gambar 2.



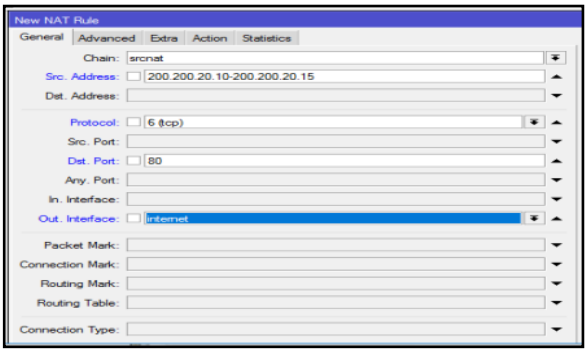
Gambar 2. Konfigurasi *Firewall* NAT

Kemudian dengan *masquerade* juga dapat melakukan pembagian *IP Address* pada jaringan *local* yang diizinkan dapat mengakses internet, sehingga dapat membatasi pengguna internet pada jaringan *LAN* maupun *WLAN* SMK Negeri 1 Indralaya Utara. Pada gambar 3 berikut ini komputer *client* yang berhasil koneksi internet:

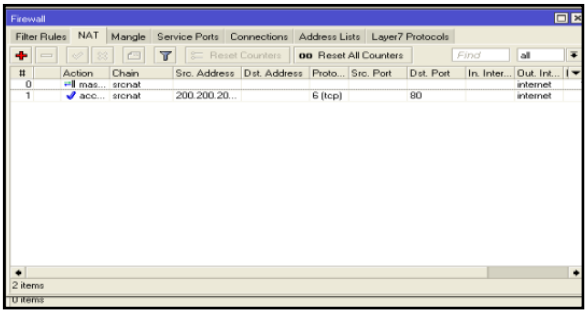
Gambar 3. Komputer *client* yang mengakses Internet

2) Sistem *Firewall* untuk Aplikasi tertentu

Tahap selanjutnya adalah jika *administrator* jaringan SMK Negeri 1 Indralaya Utara menginginkan komputer *client* hanya mendapatkan layanan internet tertentu saja misalnya pengguna hanya di izinkan untuk melakukan akses *browsing*, maka yang harus dilakukan adalah dengan menambahkan *opsi protocol* dan *destination port* pada baris perintah konfigurasi *masquerade*, dapat dilihat pada gambar 4 dan 5.



Gambar 4. Konfigurasi *Firewall* untuk Aplikasi tertentu



Gambar 5. Komputer *Client* Hanya Diizinkan Melakukan *Browsing*

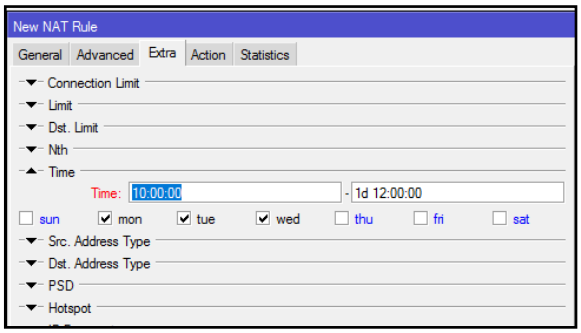
3) Sistem *Firewall* untuk waktu tertentu

Kemudian dapat juga melakukan proses membatasi akses layanan internet berdasarkan hari dan jam tertentu, jika *administrator* jaringan SMK Negeri 1 Indralaya Utara ingin memberikan izin untuk para pengguna guru, pegawai dan siswa dapat mengakses internet hanya pada jam 10.00 – 12.00 untuk hari senin, selasa dan rabu maka konfigurasi yang dapat dilakukan seperti pada gambar 6.

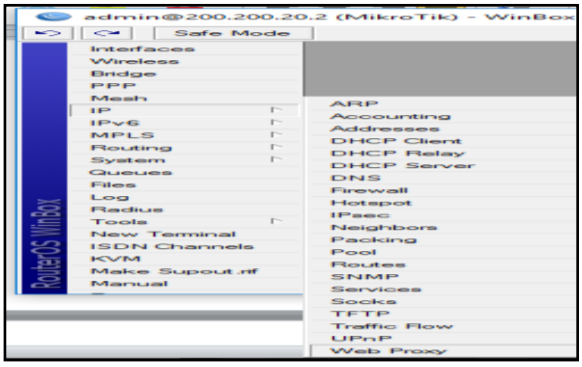
3.4.2 Sistem Keamanan *Web Proxy*

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

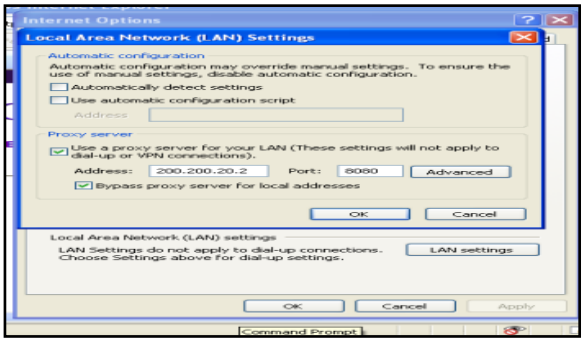
berbeda dengan *firewall*, dimana jika hanya menggunakan *firewall* maka mikrotik *routerboard* hanya akan meneruskan HTTP *request* yang dibuat oleh komputer *client* ke internet. Namun jika dikombinasikan juga menggunakan *proxy* maka mikrotik *routerboard* dapat memeriksa *content* dari HTTP *request* maupun respon secara keseluruhan. Untuk konfigurasi *web proxy* dapat dilihat seperti pada gambar 7 dan 8.



Gambar 6. Membatasi layanan Internet berdasarkan Hari dan Jam



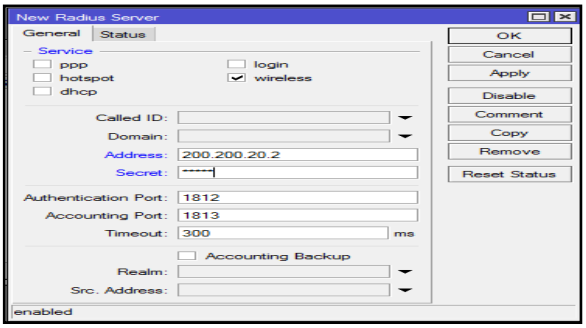
Gambar 7. Konfigurasi *Web Proxy* di *Mikrotik*



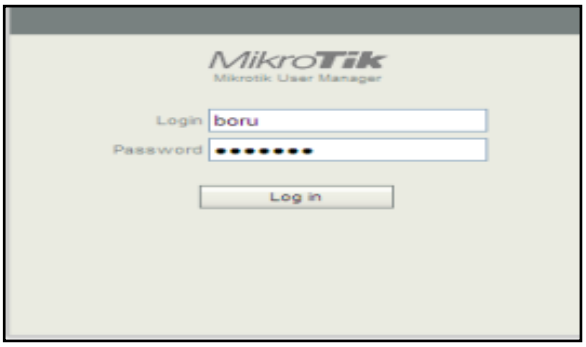
Gambar 8. Konfigurasi *Proxy* di Komputer *Client*

3.4.3 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. Konfigurasi user manager dapat dilihat pada gambar 9 dan gambar 10 adalah tampilan menu login layanan internet dan hasil ujicoba koneksi internet pada komputer *client* berikut ini.



Gambar 9. Konfigurasi *User Manager*



Gambar 10. Menu *Login User Manager*

4. SIMPULAN

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. 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 memanajemen 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 RUJUKAN

Rahardjo, Budi. 2002. *Keamanan Sistem Informasi Berbasis Internet*. [Online]. (Diakses; http://www.ilmukomputer.com, 10 Desember 2017).

Stiawan, Deris. 2009. *Internet Working Development and Design Life Cycle*. [Online]. (Diakses http.unsri.ac.id/upload/ arsip/network_development_cycles.pdf., 15 Desember 2017).

Stiawan, Deris. 2005. *Sistem Keamanan Komputer*. Elex Media Komputindo. Jakarta.

Sukmaaji, Anjik. Rianto. 2008. *Jaringan Komputer*. Andi Offset. Yogyakarta.

Towidjojo, Rendra. 2008. *Teori dan Implementasi Menggunakan Router Mikrotik*. Informatika. Bandung.