MEMANFAATKAN FITUR *FIREWALL RULES* PADA MIKROTIK UNTUK KEAMANAN JARINGAN DI HOTEL LENORA BANDUNG

Sendythias Pratama Putra[1], Yudi Ramdhani[2]

[1]Universitas Adhirajasa Reswara Sanjaya
Jalan Sekolah Internasional No. 1-2 Antapani Bandung
e-mail: Sendythias@gmail.com

[2]Universitas Adhirajasa Reswara Sanjaya
Jalan Sekolah Internasional No. 1-2 Antapani Bandung
e-mail: yudi@ars.ac.id

Abstrak

Jaringan Komputer semakin berkembang dengan adanya *Internet*. Dengan *Internet,* banyak manfaat yang didapat dengan jaringan komputer raksasa yang saling berinteraksi. Dalam beberapa hal, terhubung dengan *Internet* bisa menjadi suatu ancaman bahaya. Banyak kemungkinan serangan yang dapat terjadi, baik dari dalam maupun dari luar lingkup jaringan. Keamanan jaringan merupakan salah satu hal penting dalam implementasi jaringan komputer. Salah satu metode keamanan jaringan yang dapat diterapkan yaitu dengan memanfaatkan fitur – fitur pada Mikrotik. Dari pengujian yang dilakukan, *firewall* terbukti dapat melindungi jaringan dengan melakukan *filtering* yang bertujuan untuk mengoptimalkan sistem. Dengan sistem informasi perhotelan yang sudah terintegrasi dengan *cloud,* peluang rusak/hilangnya data semakin terbuka. Dengan memanfaatkan fitur *Firewall Rules* pada mikrotik, kita dapat melakukan pencegahan terhadap traffic – traffic penyerangan baik dari dalam maupun dari luar lingkup jaringan. Kita dapat melakukan *Drop Ftp Bruteforcers, Drop Ssh Bruteforcers, dan Drop Telnet Bruteforcers.* Sehingga dengan memanfaatkan fitur *Firewall Rules* pada Mikrotik, kita mendapatkan fasilitas Keamanan jaringan yang memadai dan Operasional Hotel Lenora Bandung pun bisa lancar tanpa gangguan.

Kata Kunci: *Internet, Keamanan Jaringan, Firewall Rules, Mikrotik, Drop Bruteforcers.*

Abstract

Computer networks are growing with the Internet. With the Internet, there are many benefits obtained from giant computer networks that interact with each other. In some ways, connecting to the Internet can be a threat. Many possible attacks can occur, both from within and from outside the network scope. Network security is one of the important things in implementing computer networks. One of the network security methods that can be applied is by utilizing the features of Mikrotik. From the tests conducted, the firewall is proven to be able to protect the network by filtering which aims to optimize the system. With a hospitality information system that is integrated with the cloud, opportunities for data damage / loss are increasingly open. By utilizing the Firewall Rules feature on Mikrotik, we can prevent attack traffic from both inside and outside the network scope. We can do Drop Ftp Bruteforcers, Drop Ssh Bruteforcers, and Drop Telnet Bruteforcers. So that by utilizing the Firewall Rules feature on Mikrotik, we get adequate network security facilities and Lenora Hotel Bandung operations can run smoothly without interruption.

Keyword: *Internet, Network Security, Firewall Rules, Mikrotik, Drop Bruteforcers.*

1. Pendahuluan

Sejak tahun 1940 sampai dengan saat ini perkembangan jaringan komputer cukup signifikan. Pada tahun 1940 menggunakan *Batch Processing*, pada tahun 1950 pengembangan TSS (*Time Sharing System*), *Distribution Processing* pada tahun 1960, penggunaan TCP/IP untuk standarisasi jaringan pada tahun 1980, lahirnya *World Wide Web* pada tahun 1990, hingga tahun 2000 CISCO menggunakan teknologi *Artificial Intelligence* (Inkofar, 2019).

Jaringan komputer terdapat di hampir setiap negara maju maupun negara berkembang. Jaringan komputer digunakan untuk memperlancar arus informasi di dalam pemerintahan negara tersebut. Internet adalah suatu jaringan komputer raksasa yang merupakan jaringan komputer yang terhubung dan dapat saling berinteraksi. Dalam beberapa hal terhubung dengan internet bisa menjadi suatu ancaman bahaya. Banyak kemungkinan serangan yang dapat terjadi baik dari luar maupun dari dalam jaringan komputer itu sendiri (Purwaningrum, 2018).

Jaringan Komputer adalah interkoneksi antara 2 komputer *autonomous* atau lebih, yang terhubung dengan media transmisi kabel (*wired*) atau tanpa kabel (*wireless*). *Autonomous* merupakan kondisi apabila sebuah komputer melakukan kontrol terhadap komputer lain dengan akses penuh, sehingga dapat membuat komputer lain *restart*, *shutdown*, kehilangan *file* atau kerusakan sistem. Dalam definisi *networking* yang lain, *autonomous* dijelaskan sebagai jaringan yang independent dengan manajemen sistem sendiri, memiliki topologi jaringan, *hardware* dan *software* sendiri, dan dikoneksikan dengan jaringan *autonomous* yang lain. *Internet* merupakan contoh kumpulan jaringan *autonomous* yang sangat besar (Wongkar, 2015).

Keamanan jaringan merupakan salah satu hal terpenting dalam implementasi jaringan komputer. Kelalaian pengelola jaringan dalam membangun sebuah jaringan komputer dapat menyebabkan berbagai masalah. Kelalaian tersebut dapat membuka peluang bagi para *hacker* untuk meretas bahkan merusak jaringan yang dibangun. Untuk mengantisipasi terjadinya penyalahgunaan jaringan oleh para *hacker*, maka diperlukan peningkatan keamanan pada jaringan yang akan dibangun (Amarudin, 2018).

Dari pengujian yang dilakukan, *firewall* terbukti dapat melindungi suatu jaringan dengan melakukan *filtering* yang bertujuan untuk mengoptimalisasikan sistem. *Firewall* dapat membatasi siapa yang berhak dan tidak berhak mengakses internet dalam suatu jaringan. *Firewall* juga dapat menyaring siapa yang harus diizinkan dan tidak diizinkan untuk melewati suatu jaringan. *Firewall* merupakan sebuah fitur keamanan jaringan yang memperkenankan berbagai bagian ruas jaringan untuk melakukan komunikasi antar jaringan sesuai dengan definisi kebijakan keamanan yang telah diterapkan sebelumnya (Purwaningrum, 2018).

Firewall merupakan suatu mekanisme yang diterapkan pada *hardware* maupun *software* dengan tujuan untuk melindungi, membatasi, menyaring, bahkan menolak suatu kegiatan suatu segmen pada jaringan lokal dengan jaringan luar yang bukan ruang lingkupnya. *Firewall* bertugas memastikan bahwa tidak ada tambahan di luar ruang ingkup yang diizinkan (Khasanah, 2016).

Penerapan teknologi informasi yang baik dan aman dalam membangun sebuah jaringan komputer sangat penting. Salah satu metode keamanan jaringan yang dapat diterapkan yaitu dengan memanfaatkan fitur – fitur pada Mikrotik. MikroTikls Ltd yang dikenal sebagai Mikrotik secara umum, merupakan produsen Latvia yang menjual perangkat jaringan komputer. Didirikan pada tahun 1995, perusahaan ini bermaksud ingin meraup pasar penjualan nirkabel/*wireless*. Pada tahun 2007 perusahaan ini semakin terus berkembang dengan memiliki 70 karyawan lebih (Dwiyatno, Putra, & Krisnianingsih, 2015).

Fitur *Firewall Rules* yang terdapat pada Mikrotik dapat diterapkan pada sistem keamanan jaringan komputer. *Firewall Rules* merupakan sekelompok sistem yang menetapkan kebijakan kendali akses antara dua jaringan, dengan prinsip sepasang mekanisme memblok lalu lintas, dan mengizinkan lalu lintas jaringan. Dengan menggunakan *firewall*, pengelola jaringan dapat membatasi hak akses terhadap *IP-Address* yang dianggap kurang baik bagi pengguna jaringan.

Keamanan data pada sistem informasi di bidang perhotelan yang digunakan Hotel Lenora Bandung harus terjamin. Dengan sistem informasi yang sudah terintegrasi dengan *cloud*, peluang

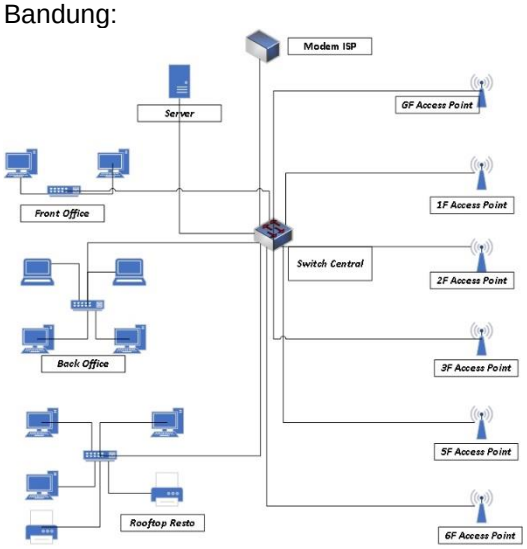
hilang/rusaknya data semakin terbuka. Banyak faktor yang bisa mengganggu operasional sistem perhotelan itu sendiri. Hal yang paling utama adalah faktor keamanan jaringan *LAN* (*Local Area Network*) pada komputer *server* hotel tersebut. Jaringan *LAN* hotel harus terhindar dari para penyusup, sehingga sistem bisa berjalan sesuai dengan yang diharapkan.

2. Metode Penelitian

2.1. Skema Jaringan Berjalan

Jaringan yang digunakan oleh Hotel Lenora Bandung menggunakan Jaringan *LAN* yang terkoneksi kepada *Internet* melalui vendor ISP (*Internet Service Provider*). Topologi Jaringan yang digunakan oleh Hotel Lenora Bandung menggunakan Topologi *Tree*. Topologi *Tree* merupakan penggabungan antara Topologi *Bus* dan Topologi *Star*. Topologi *Tree* dipilih karena selain fleksibel dalam pengembangannya topologi ini memiliki keuntungan manajemen yang jauh lebih mudah dari topologi lainnya sehingga mempermudah deteksi kesalahan pada jaringan yang ada.

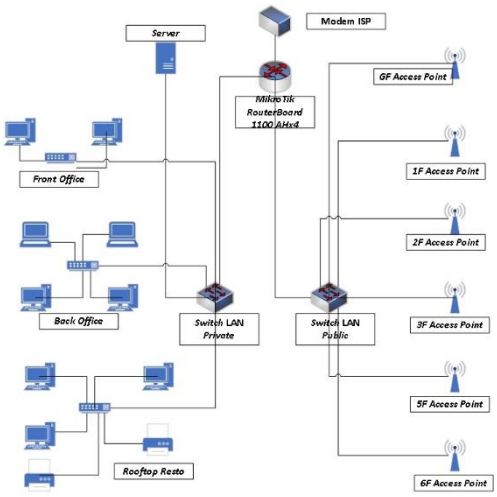
Berikut gambaran Topologi *Tree* pada Jaringan Komputer Hotel Lenora Bandung:



Gambar 1. Skema Jaringan Berjalan

2.2. Jaringan Usulan

Jaringan Usulan merupakan gagasan yang dirancang oleh penulis untuk menanggulangi masalah yang terjadi pada Jaringan Komputer Hotel Lenora saat ini. Dalam merancang Sistem Jaringan Usulan ini penulis memanfaatkan fitur – fitur *Firewall Rules* pada Routerboard Mikrotik untuk Keamanan Jaringannya. Penulis juga menggunakan fitur – fitur lain pada Routerboard Mikrotik demi terciptanya kelancaran Jaringan dan penggunaan *Internet* yang efisien pada Jaringan Komputer Hotel Lenora Bandung.



Gambar 2. Topologi Jaringan Usulan

Topologi pada Gambar 2 merupakan rancangan topologi jaringan usulan yang penulis usulkan dengan menggunakan tambahan Routerboard Mikrotik dan *Switch* baru sebagai keamanan jaringan dan pembagi dalam *network grouping*.

3. Hasil dan Pembahasan

3.1. Jenis Jaringan

Jaringan yang digunakan oleh Hotel Lenora Bandung hanya menggunakan satu jenis jaringan saja. Jenis jaringan yang digunakan yaitu jaringan jenis *LAN* (*Local Area Network*). Jaringan *LAN* tersebut dibagi menjadi dua bagian. Berikut penjelasan *Network Grouping* yang akan digunakan di area Hotel Lenora Bandung:

1. *LAN* (*Local Area Network*) *Public*

Jaringan *LAN Public* merupakan jaringan yang dialokasikan untuk tamu. Baik tamu Hotel (tamu yang akan menginap di hotel), tamu *back office* Hotel (Vendor – vendor hotel, maupun para Direksi yang sedang melakukan kunjungan ke hotel) dan Tamu Resto di *Rooftop* Hotel Lenora. Sama seperti namanya, LAN *Public* ini dialokasikan untuk umum. Media yang digunakan adalah *Wireless*, menggunakan *Wireless Access Point* di setiap lantai Hotelnya. Jaringan LAN *Public* harus terhubung ke internet selama 24 jam. Karena *free Wi-fi* atau *free internet*

merupakan salah satu bagian dari *service* Hotel Lenora.

2. *LAN* (*Local Area Network*) *Private*

Jaringan *LAN Private* merupakan jaringan yang dialokasikan untuk operasional Hotel. Jaringan ini diberi nama *LAN Private* karena jaringan ini statusnya lebih *privacy.* Media yang digunakan adalah *Wired,* sehingga akses kepada jaringan *LAN Private* ini lebih terbatas. Di dalamnya terdapat *Komputer Server* utama Hotel Lenora. Semua *device* yang digunakan para karyawan seperti Komputer, Laptop, Printer, dan *Scanner* untuk keperluan operasional Hotel berada di dalam jaringan kategori *LAN Private*. Oleh sebab itu keamanan jaringan pada *LAN Private* harus terjamin, karena operasional Hotel Lenora sangat bergantung kepadanya.

Tabel 1. Jenis Jaringan Hotel Lenora

No	Jenis Jaringan	Media Transmisi	Alokasi
1	LAN *Public*	*Wireless*	Untuk Umum/Tamu
2	LAN *Private*	*Wired*	Untuk Operasional Hotel

3.2. Keamanan Jaringan

Keamanan Jaringan yang penulis usulkan dapat menjadi solusi dari permasalahan keamanan di Jaringan Hotel Lenora Bandung. Pada sisi keamanan jaringan penulis mengusulkan untuk menambah kemanan jaringan tanpa mengurangi keamanan jaringan yang sudah ada. Berikut penulis jelaskan beberapa metode pengamanan jaringan pada Routerboard Mikrotik yang akan diimplementasikan pada Jaringan Hotel Lenora Bandung.

A. Merubah *User Admin Default* Mikrotik

Mikrotik membuat *user Admin* tanpa *password* dengan *full access* secara *default*. Salah satu cara untuk mengamankan *Router* Mikrotik adalah dengan menonaktifkan *user admin* dan membuat *user admin* baru dengan proteksi *password* dan membatasi *login* hanya bisa diakses dari jaringan tertentu saja.

B. Menonaktifkan *Service*

Secara d*efault, Router* Mikrotik mengaktifkan seluruh *service* yang ada agar *user* dapat mengakses dan mengatur fitur lainnya. Ada beberapa cara untuk *login* ke dalam sistem Mikrotik, diantaranya, melalui applikasi winbox, *http, ssh, telnet,* dan lainnya. Dengan menonaktifkan *service* yang tidak diperlukan, maka dapat memperketat Sistem Keamanan Jaringan Routerboard Mikrotik.

C. Merubah *Port* Winbox

Secara *default,* winbox menggunakan *port* 8291 dalam mengakses Mikrotik. Tetapi *port* tersebut dapat diubah sesuai dengan keinginan *Administrator* Jaringan. Hal ini dilakukan untuk menghindari serangan dari *remote access.* Bahkan untuk memperketat pembatasan hak akses *login*, Mikrotik dapat membatasi akses Winbox hanya diizinkan dari jaringan tertentu saja.

D. Merubah *Port Web*

Secara *default,* jalur akses Mikrotik via *Web* menggunakan *port* 80. Sama halnya dengan Winbox, *port Web* pada Mikrotik dapat diubah sesuai keinginan. Bahkan hak *access login* melalui *Web* pada Mikrotik bisa dibatasi hanya dari jaringan tertentu saja.

E. Menonaktifkan *Neighbour Discovery*

Mikrotik memiliki *protocol* yang dapat melakukan *broadcast domain* pada *layer* 2, sehingga membuat masing – masing *Router* dapat saling menemukan satu sama lain apabila berada di jaringan layer 2 yang sama. Mikrotik *Neighbor Discovey Protocol (MNDP)* dapat menemukan atau mengetahui informasi *Router* lain seperti informasi identitas *Router*, *MAC-Address*, dan *IP-Address*. Dengan dinontaktifkannya fitur ini, diharapkan dapat meningkatkan keamanan Routerboard Mikrotik, karena Routerboard Mikrotik menjadi tidak terdeteksi pada jaringan *layer* 2 yang sama.

F. Memanfaatkan fitur *Firewall Rules*

Pada Routerboard Mikrotik yang sudah *running* di sebuah jaringan, berbagai cara dilakukan oleh penyusup atau *hacker* untuk mencoba masuk kedalam *Router* tersebut. Salah satunya dengan menggunakan *Brute Force Attack*. Dalam

Kriptografi *Brute Force Attack* adalah penyerangan dengan mengirimkan banyak *password* atau frasa *password* dengan harapan pada akhirnya dapat menebak *password* yang benar. Dengan fitur *Firewall Rules* pada Mikrotik, *traffic* dari *Brute Force Attack* dapat disaring melalui *filtering* kemudian diblok.

4. Kesimpulan

Kondisi Keamanan Jaringan Hotel Lenora dapat lebih terjamin dari para penyusup yang mencoba login maupun pihak – pihak yang tidak diinginkan lainnya. Dibutuhkan fitur tambahan selain *Firewall Rules* pada Mikrotik untuk memastikan Keamanan Jaringan di Hotel Lenora Bandung lebih terjamin. Dengan fitur *Drop SSH Brute Forcers*, *Drop Telnet Brute Forcers*, dan *Drop FTP Brute Forcers*, Kerahasiaan Data pada Jaringan Komputer Hotel Lenora dapat lebih terjamin, karena kemungkinannya sangat kecil ada penyusup yang dapat memasuki Jaringan Komputer Hotel Lenora.

Referensi

Amarudin. (2018). Analisis dan Implementasi Keamanan Jaringan pada Mikrotik Router OS Menggunakan Metode Port Knocking. 1-7.

Dwiyatno, S., Putra, G. W., & Krisnianingsih, E. (2015). Penerapan OSPF Routing, De-Militarized Zone, dan Firewall Pada Mikrotik Routerboard Dinas Komunikasi dan Informatika Depok. 59-67.

Fajar Adhi Purwaningrum, A. P. (2018). Optimalisasi Jaringan Menggunakan Firewall. 17-23.

Khasanah, S. N. (2016). Keamanan Jaringan dengan Packet Filtering Firewall. 182-192.

Stefen Wongkar, A. S. (2015). Analisa Implementasi Jaringan Internet. 62-68.

Syifa Nur Rakhmah, I. M. (2019). Pengelolaan Jaringan Hotspot Menggunakan Mikrotik Router OS pada PT Arsen Kusuma Indonesia. 15-22.