Penerapan Ospf *Routing*, *De-Militarized Zone*, Dan *Firewall* Pada Mikrotik *Routerboard*tm Dinas Komunikasi Dan Informatika Depok

[1] Saleh Dwiyatno, [2] Gunardi Wira Putra, [3]Erni Krisnaningsih
Manajemen Informatika Politeknik Piksi Input Serang
Teknik Informatika Universitas Serang Raya
salehdwiyatno@gmail.com[1] , gunardiwiraputra@gmail.com[2], erni_krisnaningsih@yahoo.co.id[3]

ABSTRAKS
Penelitian ini bertujuan untuk mengaplikasikan konfigurasi dari Routing, De-Militarized Zone dan Firewall pada alat jaringan MikroTik RouterBoard yang berada pada Dinas Komunikasi dan Informatika Depok dan membuat jalur data pada jaringan memiliki kinerja yang lebih baik. Penelitian dilakukan dengan menggunakan metode wawancara, observasi, dan studi literatur yang dimulai dengan wawancara kepada pegawai yang bekerja di divisi IT internal Dinas Komunikasi dan Informatika Depok dilanjutkan dengan observasi memantau tata letak jaringan internal baik yang sudah ada maupun yang akan dibangun, serta mencari hal-hal dalam literatur yang bisa diterapkan untuk membantu meningkatkan kinerja jarigan. Hasil dari penelitian ini adalah terbentuknya koneksi antar jaringan dalam topologi beserta suksesnya fungsi dari firewall dan bekerjanya rule untuk area DMZ. Keberhasilan dalam pengaplikasian diuji kembali dengan melakukan beberapa metode serangan yang akan ditanggulangi oleh konfigurasi yang telah diterapkan pada alat jaringan beserta server.

Kata kunci : DMZ(De-Militarized Zone), firewall, jaringan, routing, server

1. PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan data yang melalui suatu jaringan adalah salah satu hal yang menjadi tanggung jawab DISKOMINFO, oleh karena itu DISKOMINFO harus membatasi pengguna yang bisa mengakses ke jaringan DISKOMINFO. DISKOMINFO juga bertanggung jawab terhadap pembentukan jaringan yang memungkinkan komunikasi antar alat dalam jaringan sehingga terjadi pertukaran informasi. Oleh sebab itu dalam penelitian ini akan dibahas mengenai Penerapan OSPF *Routing*, *De-Militarized Zone*, dan *firewall* pada MikroTik *Router*BOARD™ DISKOMINFO.

Beberapa masalah jaringan yang sering muncul adalah penyebaran virus, Trojan, dan pencurian data oleh *hacker* yang ingin memaksa masuk ke jaringan DISKOMINFO demi mendapatkan koneksi "gratis". Sering nya terjadi koneksi yang tidak stabil (*Request Time Out* / RTO) karena *traffic* jaringan yang tidak diatur dalam *device* jaringan pendukung seperti *Router* dan *Switch*. Jika permasalahan-permasalahan tersebut tidak segera diatasi, maka akan menghambat jalannya operasional sehari-hari.

1.2 Identifikasi Masalah

a. Jaringan DISKOMINFO Depok memiliki kelemahan yakni kecepatannya sering terganggu karena, banyaknya gangguan dari luar berupa percobaan masuk dengan meng-*input* kan *password* yang secara *random*, hak akses *user-client* yang belum ada, belum adanya keamanan jaringan yang memadai pada konfigurasi *device* dan *routing protocol* yang masih *static*.
b. Selain daripada gangguan yang berasal dari luar gangguan juga berasal dari dalam yakni padatnya paket data yang bergerak di dalam *traffic* jaringan biasa nya berupa pertukaran data seperti *download* dan *upload* atau bahkan virus yang dibawa oleh Trojan. *Device* jaringan pun sering diuji kemampuannya oleh para *hacker* yang berusaha masuk ke dalam jaringan untuk mendapatkan akses gratis ke internet, baik dengan cara memasukkan *random password* secara terus menerus, maupun dengan menggunakan aplikasi-aplikasi *hacking*. Banyak nya *client* yang mencoba melakukan "ping" ke *server* untuk mengetest koneksi jaringan.

1.3 Pembatasan Masalah

Bahasan dalam penelitian ini hanya akan membahas permasalahan:

a. Pembahasan mengenai *Routing* OSPF dalam MikroTik. Untuk mencegah terjadinya *hacking*.
b. Pembahasan mengenai fungsi dan pengertian DMZ beserta cara kerjanya. Dalam mencegah terjadinya *hacking*.
c. Pembahasan mengenai fungsi dan pengertian *firewall* serta contoh penyerangan dengan jenis serangan *port scanner* dan *brute force*.

1. 4 Perumusan Masalah

Adapun rumusan masalah yang akan diselesaikan dalam penelitian ini adalah

a. Apa yang menyebabkan jaringan berjalan lambat ?
b. Konfigurasi apa saja yang diperlukan untuk menangani penyebab lambat nya jaringan ?
c. Mengapa konfigurasi *default* harus diubah ?

d. Hasil apa yang didapati setelah konfigurasi untuk pencegahan serangan dan perbaikan transfer data jaringan diterapkan ?

1. 5 Tujuan Penelitian

Tujuan penelitian ini adalah membangun koneksi jaringan yang berpusat di DISKOMINFO, dan menerapkan beberapa metode keamanan pada *firewall rules*, serta membangun *access list* untuk keamanan *server* pada seluruh perangkat MikroTik *Router*BOARD™ agar tercipta bentuk topologi jaringan yang aman dan baik digunakan oleh khalayak.

2. LANDASAN TEORI

2.1 Jaringan

Network atau jaringan secara umum adalah suatu sistem saluran yang terinterkoneksi, seperti jalur telepon untuk komunikasi atau kereta bawah tanah untuk transportasi. Kita menggunakan jaringan transportasi tiap hari untuk beberapa hal yang berbeda tujuannya, contohnya saja kita menggunakan kereta untuk ekspedisi sehari-hari, kita berjalan kaki untuk pulang-pergi ke tempat kerja, dan pesawat atau penerbangan untuk perjalanan yang lebih jauh. Dalam bidang *Computer and Information Technology* (IT), sebuah *network* atau jaringan didefinisikan sebagai sekelompok komputer dan menghubungkan fungsi sirkuit dengan cara tertentu. Sedangkan definisi dari transportasi jaringan adalah sebuah sistem penyebrangan atau rute interkoneksi, seperti jalan atau trek kereta bawah tanah (Castelli, 2004: 8).

2.2 Pengenalan MikroTik

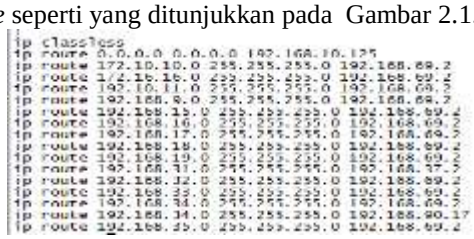
MikroTikls Ltd, yang dikenal sebagai MikroTik secara internasional, adalah produsen Latvia yang menjual perangkat jaringan komputer. Perusahaan ini didirikan pada tahun 1995, dengan maksud meraup pasar penjualan nirkabel. Pada tahun 2007 perusahaan ini memiliki lebih dari 70 karyawan dan terus berkembang. MikroTik memiliki beberapa jenis produk, yaitu:

a. *RouterOS*. Produk utama dari MikroTik ini berbasiskan sistem operasi Linux, dan dikenal dengan nama MikroTik RouterOS™. Sistem operasi ini membuat *user* bisa menggunakan PC sebagai mesin yang bekerja seperti *router* dan memiliki beberapa fitur, seperti *firewall*, VPN *server* dan *client*, *bandwidth shaper Quality of Service*(QoS), *wireless access point*, dan berbagai jenis fitur untuk *routing* dan koneksi jaringan lainnya.
b. *RouterBOAR* adalah kombinasi antara sistem operasi dan *hardware* yang dibuat oleh perusahaan MikroTik Ltd, yang dipasarkan di beberapa I*Internet service providers* kecil hingga menengah. Alat ini populer di beberapa negara, seperti Republik Czech dan Brazil.

2.3 *Router* & *Routing*

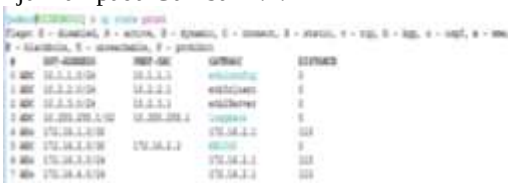
Router adalah sebuah alat jaringan yang meneruskan paket *downstream* (hilir) ke target tujuan. *Router* membuat keputusan *forwarding* berdasarkan pengetahuan tentang ke dua buah *network* yang berhubungan langsung, dan *network* yang didapatkan dari informasi *routing* dengan *router* lain. Sebuah *router* dapat terdiri dari beberapa *interface network* yang menyediakan konektifitas ke entitas jaringan lainnya, termasuk sesama *router*, *host*, *network segment* dan lainnya (Schudel & Smith, 2008:18).

Routing adalah lapisan kedua atau ketiga, tergantung model yang digunakan. Tugas *routing* adalah membagi informasi antara *router* atau *network* yang berbeda, supaya antara *network* bisa berhubungan satu sama lain (Parkhurst, 2005: 16). Ada beberapa jenis *routing* yang biasa digunakan dalam konfigurasi jaringan, yakni *static route* dan *dynamic route*. *Static route* adalah *routing* yang dimasukkan oleh *admin* secara manual, dengan persyaratan admin harus mengetahui pola atau topologi jaringan yang ada. Contoh konfigurasi *static route* seperti yang ditunjukkan pada Gambar 2.1.



Gambar 2.1 Konfigurasi *static route* pada sebuah perangkat *router*

Sedangkan *dynamic route* terbagi lagi beberapa jenis, yakni EBGP, EIGRP, IGRP, OSPF, IS-IS, RIP, IBGP, dan BGP. Tiap *routing* pun memiliki *administrative distance* (tingkat kepercayaan) masing-masing, contoh konfigurasi salah satu *dynamic route* ditunjukkan pada Gambar 2.2.



Gambar 2.2 *Routing* OSPF pada MikroTik

2.4 OSPF *Routing*

Open Shortest Path First (OSPF), lebih baik, lebih kuat, lebih cepat dari pendahulu nya. OSPF adalah hirarki *link-state* interior IP *Routing Protocol* yang di rancang untuk melampaui kemampuan dari keterbatasan *distance vector routing protocols*. *Open* artinya OSPF adalah salah satu basis standar protokol yang dijelaskan pada *Request For Comment* (RFC) atau kamus teknologi. Hirarki, berarti jaringan OSPF dapat dibagi menjadi beberapa area. *Distance vector routing protocols* (RIP dan EIGRP), adalah *single-area routing protocols*. *Single area* berarti seluruh *router* yang ada dalam satu area akan di ketahui informasi nya oleh *router* lain yang ada dalam area yang sama. Bertepatan dengan bertambahnya *router* di sebuah area, maka akan bertambah pula informasi yang harus dimiliki oleh *router* pada area yang sama dalam waktu yang sama, untuk jaringan yang besar hal ini tidak tepat sehingga harus dibatasi oleh beberapa area supaya tidak terjadi penyempitan data karena data

yang mengalir hanya informasi data mengenai *router* saja, maka OSPF lah yang paling tepat untuk *routing* (Parkhurst, 2005: 195).

2.5 *Static Routing*

Static Routing adalah *routing* secara manual yang di inputkan oleh *admin* yang bertanggung jawab dalam pembuatan dan pengelolaan jaringan. *Routing* seperti ini adalah jenis *routing* yang tercepat ke dua setelah *directly connected* atau terhubung langsung dengan nilai *administrative distance* nya adalah satu (bisa dilihat pada Tabel Tabel 2.1). Kelemahan dari *static routing* adalah penginputan alamat-alamat yang terdapat dalam *router* secara manual, sehingga makin banyak *router* yang saling berhubungan akan semakin banyak pula alamat yang harus dimasukkan. Jenis *static routing* ini tidak cocok untuk jaringan dengan kapasitas yang cukup luas.

2.6 Telnet dan *WinBox*

Telnet adalah aplikasi *remote login internet*. Telnet digunakan untuk login ke komputer lain di jaringan luas dan mengakses berbagai macam layanan umum, termasuk katalog perpustakaan dan berbagai macam *database*. Telnet menggunakan dua program, yang salah satunya adalah *client* (telnet) dan *server* (telneted). *Client* adalah komputer yang meminta layanan telnet, sedangkan *server* adalah perangkat jaringan yang dihubungi lewat telnet yang dimintai layanan telnet. *WinBox* adalah sebuah *software* yang digunakan untuk memudahkan user masuk dan melakukan konfigurasi pada alat MikroTik baik dengan mode *Command Line Interface* (CLI) maupun mode *Graphical User InterfaceI* (GUI). Lewat *WinBox* kita bisa mengkoneksikan diri ke MikroTik *router* dengan alamat IP ataupun MAC *address* dari MikroTik tersebut.

2.7 *Firewall*

Firewall atau dinding api adalah suatu sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk bisa melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman. Umumnya, sebuah tembok-api diterapkan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (*gateway*) antara jaringan lokal dengan jaringan Internet. *Firewall* pada tingkatan paling dasar, mengontrol aliran lalulintas antara jaringan lokal (LAN) yang terpercaya dengan jaringan publik (Internet) yang bisa dibilang tidak terpercaya. *Firewall* yang digunakan saat ini berbasis *port* (*packet filtering*), *firewall* atau beberapa variasi (*stateful inspection*) dari jenis dasar *firewall*. *Firewall* semacam ini sangat populer, karena mereka relatif sederhana untuk operasional nya, murah, memiliki *throughput* yang baik, dan telah lazim digunakan dalam lebih dari dua dekade.

Banyak dari beberapa jenis *firewall* yang dikonfigurasi untuk mengizinkan seluruh kegiatan *traffic* yang datangnya dari jaringan terpercaya menuju ke jaringan yang tidak dipercaya, kecuali di blok oleh peraturan. Contoh nya *Simple Network Management Protocol* (SNMP) mungkin saja di blok untuk mencegah informasi jaringan yang keluar menuju jaringan luas (internet).

2.8 *De-Militarized Zone* (DMZ)

De-Militarized Zone (DMZ) merupakan mekanisme untuk melindungi sistem internal dari gangguan *hacker* atau pihak-pihak lain yang ingin memasuki sistem tanpa mempunyai hak akses. Sehingga karena DMZ dapat diakses oleh pengguna yang tidak mempunyai hak, maka DMZ tidak mengandung *rules*. Secara esensial, DMZ melakukan perpindahan semua layanan suatu jaringan ke jaringan lain yang berbeda. DMZ terdiri dari semua *port* terbuka, yang dapat dilihat oleh pihak luar. Sehingga jika *hacker* menyerang dan melakukan *cracking* pada *server* yang mempunyai DMZ, maka *hacker* tersebut hanya dapat mengakses *host* yang berada pada DMZ, tidak pada jaringan internal.

2.9 Teknik *Hacking* dan *Hacker*

Banyak aplikasi-aplikasi instant yang sudah siap untuk digunakan oleh *hacker* awam seperti untuk mencari *port* yang terbuka sebagai pintu masuk awal bisa dengan menggunakan aplikasi *port scanner*, sedangan untuk menerobos masuk ke *port* yang telah terdeteksi namun menggunakan password bisa memaksa masuk dengan menggunakan aplikasi *brute force*.

a. *Port Scanner* adalah sebuah aplikasi yang bisa mendeteksi port mana saja yang terbuka dari IP *address* yang akan di serang, *port scanner* merupakan *basic* dari *hacking*. Jenis *port scanner* yang biasa digunakan adalah "*free port scanner*" tampilan dari *user interface*-nya terlihat pada Gambar 2.4. Untuk penggunaanya, penyerang hanya perlu memasukkan ip *address* dari target yang akan di serang, dan TCP *port* yang diinginkan contoh nya *port* 21 adalah FTP, *port* 23 adalah telnet dan lain-lain.

Gambar 2.3 Tampilan *port scanner*

b. Brute Force adalah sebuah aplikasi dan metode untuk *hacking* yaitu menyerang dengan memasukkan *password* secara *random* secara terus menerus. *Brute Force* akan berhenti jika *password* yang dimasukkan memiliki status "*match*". Jenis *brute force* yang di gunakan adalah "Brutus AET2". Untuk penggunaan nya, penyerang hanya perlu memasukkan alamat dari perangkat yang ingin di serang, lalu pada menu *type* dipilih jenis *protocol* yang akan digunakan oleh *brute force* untuk penyerangan. Tampilan *brute force* tampak pada Gambar 2.5.

Gambar 2.4 Tampilan *brute force* Brutus AET2

3. ANALISA DAN PERANCANGAN SISTEM

3. 1 Analisa Masalah

Pada tahapan analisa masalah, dilakukan perumusan masalah yang berkaitan mengenai cakupan jaringan yang dibicarakan dengan instansi dan perihal-perihal yang diperlukan untuk keamanan jaringan tersebut, serta alat jaringan yang digunakan. Setelah menetapkan beberapa permasalahan maka dicarilah solusi yang tepat untuk pemecahan masalah-masalah tersebut.

3. 2 Analisa dan Teknik Pengumpulan Data

Beberapa analisa dan teknik pengumpulan data yang dilakukan yaitu:

a. Wawancara adalah sebuah proses tanya-jawab dengan pihak yang berkaitan, maka wawancara dilakukan kepada penanggung jawab jaringan di instansi DISKOMINFO Depok. Hal-hal yang ditanyakan menyangkut permasalahan jaringan dan prospek ke depan dari DISKOMINFO Depok sendiri. Pada tahapan ini mendapatkan data berupa alat-alat yang digunakan dan aplikasi-aplikasi pembantunya, serta alamat IP *address* yang digunakan dalam jaringan.
b. Observasi adalah pengamatan langsung pada kegiatan. Melakukan *mapping* pada jaringan yang telah ada dengan melihat langsung dan menerapkan secara langsung pada perangkat jaringan. Hal-hal yang diterapkan adalah penerapan *firewall rules*, DMZ *server*, dan *routing* OSPF pada perangkat MikroTik. Penerapan langsung baru bisa dilakukan setelah mengetahui permasalahan apa saja yang bisa dijadikan latar belakang pembentukan jaringan baru. Pada tahapan ini mendapatkan data berupa topologi jaringan yang bisa di aplikasikan serta mengetahui *routing* dasar dan jenis *routing* yang digunakan serta awal untuk menerapkan konsep dasar yang akan dilakukan dalam penelitian.
c. Studi Literatur adalah pembelajaran mengenai materi yang berhubungan dengan penelitian dan penerapan secara langsung (observasi). Studi literatur dilakukan setelah observasi. Pencarian materi yang berhubungan diambil dari berbagai sumber, seperti *e-book*, *datasheet*, buku manual, *slide* perkuliahan, buku teks, dan *browsing* dari Internet. Pada tahapan ini mendapatkan data yang digunakan dalam teori serta *datasheet* dan tabel yang digunakan dalam penelitian.

3. 3 Analisa dan Metode Pengembangan Sistem

Analisa dan Metode pengembangan sistem yang digunakan adalah metode *prototyping*, dengan jenis *design prototyping*. *Prototyping* sendiri sebenarnya adalah metode pengembangan untuk perangkat lunak/*software* namun dapat digunakan di dalam pengembangan jaringan karena memiliki siklus yang bersifat *continue*. Alasan penggunaan metode ini karena metode ini biasa digunakan di dunia nyata dan keseluruhan metode ini mengacu kepada kepuasan *user*, tahapan-tahapan dari metode *design prototyping* yaitu:

a. Pemilihan fungsi yang berkenaan dengan pengambilan bahasan penelitian dan kebutuhan dari instansi terkait. Fungsi yang telah disetujui oleh instansi adalah fungsi dari keamanan pada *router*, dan fungsi konektivitas jaringan.
b. Penyusunan sistem jaringan bertujuan memenuhi permintaan kebutuhan akan tersedianya *prototype*. Penyusunan jaringan dimulai dari membentuk topologi yang akan dibuat dan konfigurasi yang mungkin akan dibutuhkan.
c. Evaluasi adalah bentuk penyempurnaan, yakni membahas permasalahan yang terjadi ketika proses pengerjaan *project* hingga selesai nya *project*, hal tersebut untuk membuat pihak *client* selanjutnya puas dengan menghilangkan kesalahan-kesalahan sekecil apapun yang terjadi sebelumnya.
d. Penggunaan selanjutnya adalah prospek kedepan dari *project* yang telah terbentuk untuk pemeliharaan dan pengembangan kedepannya.

3. 4 Analisis Perangkat Keras (*Hardware*)

Pada fase analisis ini hal-hal yang dilakukan adalah menganalisa data dari perangkat jaringan yang digunakan, disesuaikan dengan kebutuhan dari pihak instansi, baik dalam hal spesifikasi alat maupun harga. Untuk alat-alat yang dibutuhkan antara lain adalah, *embeded* RB433AH (A+G)20dbi atau *router* RB1100AHx2 dan alat yang telah ada dan bisa digunakan antara lain *router* RB1000-1U, *router* RB 750, dan *router* RB1100 AHx1

Kabel *cross*, kabel *fiber optic* dan *converter fiber to ethernet* yang bisa dilihat pada Lampiran 1.

3. 5 Analisis Perangkat Lunak (*Software*)

3. 5.1 Analisis Aplikasi *WinBox* dan Telnet

Dalam tahapan analisis ini, didapatkan data bahwa aplikasi *WinBox* memiliki lebih banyak keunggulan dibandingkan dengan Telnet.

3. 5.2 Analisis Aplikasi *Hacking* (*Port Scanner* dan *Brute Force*)

Dalam tahapan analisis ini setelah melakukan observasi dari metode –metode gangguan yang sering terjadi pada jaringan DISKOMINFO adalah penggunaan aplikasi *Brute Force* hanya saja penyerangan ini dilakukan oleh beberapa pihak yang bisa dibilang *hacker* dalam tingkat *Lamer* untuk tingkatan *hacker* bisa dilihat pada Tabel 3.6.

Tabel 3.1 Perbandingan *WinBox* dan Telnet

Tingkat	Istilah	Kemampuan	Keterangan
5	Elite	Basic, Networking, Programing, Scripting (PRO)	Mampu menyusun jaringan, membuat aplikasi hacking sendiri dan kemampuan tingkat profesional dalam bidang hacking

4	Semi Elite	Basic, Networking, Programing, Scripting (MID)	Mampu menyusun jaringan, membuat aplikasi hacking sendiri dan kemampuan tingkat menengah dalam bidang hacking
3	Developed Kiddie	Basic, Networking, GUI Users	Mengetahui dasar pengetahuan jaringan dan programing, lebih banyak menggunakan aplikasi yang telah ada untuk hacking dalam bidang jaringan
2	Script Kiddie	Basic, GUI Users	Mengetahui dasar pengetahuan jaringan, lebih banyak menggunakan aplikasi yang telah ada untuk hacking dalam bidang jaringan
1	Lamer	GUI Users	Biasa di sebut dengan orang yang "wanna-be-a-hacker" pengetahuan sangat minim dalam hacking hanya melakukan hacking dengan aplikasi bantuan hacking

Para *hacker* biasa menggunakan *Brute Force* oleh karena itu mereka pasti memiliki aplikasi tambahan untuk mengetahui *Port* yang digunakan dalam jaringan DISKOMINFO oleh sebab itu dalam analisa ini digunakan program tambahan yaitu *Port Scanner*.

3. 6 Analisis Konfigurasi Sistem

3. 6.1 Analisis Sistem yang Sedang Berjalan

Berdasarkan data yang didapatkan dari hasil wawancara dan observasi, yang telah dilakukan di DISKOMINFO Depok, bahwa sistem jaringan internal banyak mengalami gangguan dari pihak luar, juga jalur data yang telah ada cukup padat, sehingga membuat performa jaringan kurang baik, selain itu dibutuhkan konfigurasi ulang untuk topologi jaringan baru yang akan digunakan untuk saling berhubungan antara internal jaringan DISKOMINFO Depok. Dalam jaringan yang telah adapun memiliki kelemahan yaitu kurang nya performa pertahanan diri dari serangan-serangan baik berupa serangan eksternal maupun serangan dari pihak internal, sehingga dibutuhkan konfigurasi tambahan pada jaringan yang telah ada dan pada jaringan baru yang akan dibuat.

3. 6.2 Analisis Sistem Baru

Fungsi utama dari sebuah jaringan adalah menghubungkan beberapa perangkat sebagai satu kesatuan agar dapat melakukan pertukaran data untuk membantu operasional sehari-hari dan mempermudah komunikasi antara bagian dalam DISKOMINFO Depok. Berikut adalah analisa sistem yang akan diterapkan dalam jaringan baru DISKOMINFO Depok untuk performa yang lebih baik :

3. 6.2.1 Analisis Konfigurasi Dasar pada MikroTik dengan *WinBox*

Konfigurasi akan dilakukan pada *Router* MikroTik yang digunakan sebagai alat pemisah jaringan antar bagian. *WinBox* digunakan sebagai aplikasi pembantu untuk masuk ke dalam konfigurasi MikroTik menggantikan telnet dengan kelebihan-kelebihan seperti yang dapat dilihat pada Tabel 3.1 sub bab 3.5.1 Analisis Aplikasi *WinBox* dan Telnet. Konfigurasi dasar yang akan dilakukan berupa mengubah *user default* dan *password default* untuk keamanan jaringan, dan pengalamatan IP *address* tiap *gateway* yang berhubungan langsung antar *router*.

3. 6.2.2 Analisis Konfigurasi DMZ *Server* pada MikroTik

DMZ *Rules* yang akan diterapkan adalah hubungan *client-server* dimana hak akses *client* akan dibatasi, yaitu *echo request* "ping" tidak dibolehkan, karena hanya akan membebani *server*, "ping" hanya bisa dilakukan oleh admin yang masuk lewat *router* untuk memeriksa koneksi antar jaringan jika terjadi gangguan, tidak langsung dari pihak *client*. Terbebannya jaringan dengan *request* "ping" adalah hal yang paling sering terjadi dalam gangguan jaringan.

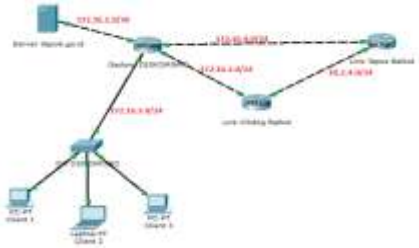
3. 6.2.3 Analisis Konfigurasi *Hacking Prevented* pada MikroTik

Hacking yang akan dicegah dalam gangguan jaringan ini adalah metode dengan *hacking Brute Force* dan *Port Scanner*. Untuk melakukan pemblokiran jenis-jenis *hacking* lain bisa dilakukan dengan menambahkan konfigurasi pada MikroTik dengan memasukkan perintah-perintah pemblokiran lain yang akan di bahas pada bab selanjutnya. Konsep pencegahan ini biasa disebut dengan *firewall* atau dinding api yang mencegah terjadinya gangguan-gangguan yang akan merusak performa jaringan.

Dengan terciptanya suasana jaringan yang terkendali akan memudahkan tiap pengguna jaringan dan mengamankan data yang lewat pada jaringan tersebut sehingga prosesi tukar menukar data akan lebih aman dan nyaman bagi pengguana jaringan.

3. 7 Perancangan Sistem

Seluruh konfigurasi dan analisis tersebut diaplikasikan kedalam sebuah topologi jaringan seperti yang bisa dilihat pada Gambar 3.1.



Gambar 3.1 Topologi Jaringan Baru DISKOMINFO Depok

4. HASIL DAN IMPLEMENTASI

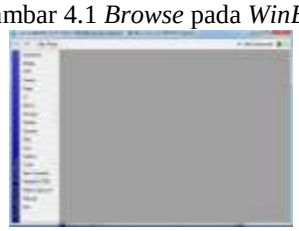
4.1 Implementasi Sistem

Penelitian dilaksanakan dan diimplementasikan di jaringan DISKOMINFO Depok. Hal-hal yang diimplementasikan adalah konfigurasi dasar MikroTik *router*, OSPF *routing* pada MikroTik, penerapan *firewall* pada MikroTik, penerapan DMZ *rules* pada sistem *client-server*, dan percobaan dengan aplikasi serangan pada perangkat yang telah dikonfigurasi.

4.1.2 Konfigurasi Dasar MikroTik

a. Login dengan *WinBox*. Untuk melakukan login pada alat MikroTik, menu *browse* yang ada dekat dengan tombol *connect* dipilih, maka bentuk pilihan *browse* bisa dilihat pada Gambar 4.1, setelah berhasil mengkoneksikan diri ke dalam *router* MikroTik maka akan tampil menu-menu dalam MikroTik seperti pada Gambar 4.2.

Gambar 4.1 *Browse* pada *WinBox*



Gambar 4.2 Menu utama MikroTik pada *WinBox* dan *New Terminal*

b. Konfigurasi *Users*, *host name*, dan *password* pada MikroTik. Untuk kemanan *router* harus dibuat beberapa ketentuan, dengan orang-orang tertentu yang bisa mengakses *router*.
   1. Dalam MikroTik bisa diciptakan *user* baru dengan perintah-pertintah seperti yang ditunjukkan pada Gambar 4.3.

Gambar 4.3 Penambahan *user* baru pada MikroTik

   2. Dalam MikroTik *host name* bisa diganti untuk memudahkan *admin* mengingat dan mengelola tiap-tiap alat jaringan MikroTik dengan perintah-perintah seperti yang ditunjukkan pada Gambar 4.4.

Gambar 4.4 Ganti *host name* pada MikroTik

   3. Dalam MikroTik untuk menjaga keamanan dan hanya memberikan akses kepada orang-orang tertentu dilakukan dengan cara mengganti *password* dari router MikroTik dengan perintah-perintah seperti yang ditunjukkan pada Gambar 4.5.

```
[gunardi@RB750LinkTaposBalkot] > password
old password:
new password: ****************
retype new password: ****************
```

Gambar 4.5 Ganti *password* pada MikroTik

c. Konfigurasi *Interface* dan IP *address* pada MikroTik. *Interface* pada tiap *ethernet* di MikroTik bisa diubah, untuk memudahkan mengingat tiap-tiap konfigurasi yang menggunakan *interface* berbeda dengan IP *address* yang berbeda. Untuk bentuk-bentuk konfigurasi nya seperti yang terlihat pada Gambar 4.6 dan Gambar 4.7.
   1. Konfigurasi mengganti *interface*.

Gambar 4.6 *Interface* pada MikroTik

   2. Konfigurasi menambahkan IP *address*.

Gambar 4.7 IP *address* pada MikroTik

4.1.3 OSPF *Routing* pada MikroTik

Beberapa hal yang perlu dikonfigurasi adalah, konfigurasi area OSPF pada menu *routing*/OSPF/*instance*. Dalam hal ini, area dibiarkan dalam keadaan default kecuali pada bagian "redistribute-connected = no" harus dikonfigurasi menjadi "redistibute-connected = as-type-1". Maksud dari "*redistibute-connected = as-type-1*" adalah perintah untuk *router* agar mendistribusi kan *network* yang terhubung langsung dengan *router* pada *router* lainnya. Tampilan menu *routing*/OSPF/*instance* terlihat seperti pada Gambar 4.8.

Gambar 4.8 Menu *router*/OSPF/*instance*

Setelah itu *network* yang akan dikirim oleh *router* ke *router* lain dimasukkan. Karena perintah "redistibute-connected = as-type-1" telah dikonfigurasi, maka *router* akan menyebarkan informasi tentang *network* yang terkoneksi langsung pada *router*, sehingga *network-network* tersebut harus di daftarkan. Untuk mendaftarkan *network-network* tersebut, menu *routing*/OSPF/*network* dipilah dan *network-network* yang *directly connected* dimasukkan dengan perintah *add*. Tampilan memasukkan *network* tampak seperti pada Gambar 4.9.

Gambar 4.9 Menu *routing*/OSPF/*network*

Ketika *network* dimasukkan, *router* membutuhkan waktu beberapa saat untuk membuat tabel *routing* baru, dan akan segera mendapatkan informasi mengenai *network* yang berada di seberangnya. Untuk tampilan pada menu ip/*routing* , di mana *router* telah mendapat kan pengalamatan dari *router* lain, nampak pada Gambar 4.10.

Untuk *routing* yang terdapat pada *router* lain bisa dimasukkan dengan perintah seperti pada Lampiran 2

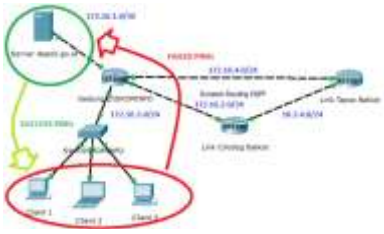
Gambar 4.10 Menu ip/*routing* RB750 Tapos

4.1.4 DMZ *Rules*

Untuk memasukkan *rule* baru bisa dengan perintah *add* pada menu ip/*firewall*/*filter*. Untuk *rule* yang sudah dimasukkan akan tampak seperti pada Gambar 4.11.

Gambar 4.11 DMZ *rule* pada menu ip/*firewall*/*filter*

Action yang terdapat pada *rule* tersebut adalah *accept* dan *reject*. Masih banyak pilihan dalam perintah *action*, yang bisa dilihat pada Lampiran 3 tentang *property* dan *description* pada menu *firewall. Protocol* memiliki fungsi untuk menentukan jenis *packet* yang melewati *router* tersebut menggunakan jenis *protocol* yang telah ditentukan pada *rule* dan akan dikenai *rule* yang telah dikonfigurasi. Src dan dst *address* juga dst-port menentukan asal mula *packet* dan tujuan tempat *packet* akan dikirim. Pada *rule* 0 bisa diartikan seperti berikut : "paket yang melalui *router* dengan *protocol* tcp yang berasal dari alamat 172.16.3.0/24 dengan *port* 80 dan akan dikirim ke alamat tujuan 172.16.1.0/30 akan dibiarkan atau diizinkan melewati *router*". Untuk lengkapnya deskripsi dan isi dari menu pada *firewall*/*filter* bisa dilihat pada Lampiran 4 tentang *property* dan *description* pada menu *firewall*. Skema konfigurasi yang telah dilakukan bisa dilihat seperti pada Gambar 4.12.



Gambar 4.12 DMZ *Server Rules*

4.1.5 *Firewall* pada MikroTik

Berikut adalah penerapan konfigurasi *firewall* pada MikroTik untuk penanganan jenis serangan *brute force* dan *port scanner* :

a. *Brute Force Prevention*. *Brute force* bekerja pada berbagai macam jenis *protocol* tergantung dengan *software* dari *brute force* tersebut. Untuk mencegah *brute force router* bisa dikonfigurasi pada menu ip/*firewall*/*filter*.

b. *Drop port scanner.* Untuk mencegah serangan *port scanner* pada *router* di menu ip/*firewall*/*filter* dapat dilakukan konfigurasi.

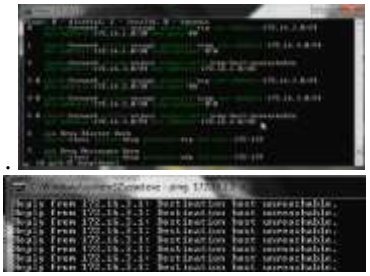
4.2 Pengujian Sistem

Dalam tahapan pengujian sistem ini, yang diuji adalah keberhasilan dari penerapan uji kelayakan DMZ *rules* serta *firewall* untuk menahan bentuk serangan dari *brute force* dan *port scanner*. Berikut adalah tahapan-tahapan yang dilakukan.

4.2.1 Uji Kelayakan DMZ *Rules*

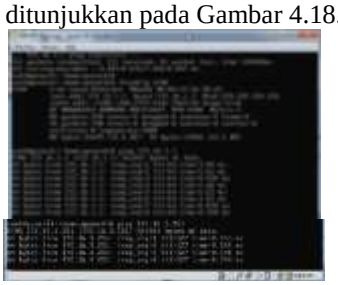
DMZ *rule* dikatakan layak jika *rule* yang diterapkan sebelumnya telah berjalan dengan semestinya. *Rule* tersebut adalah : "Seluruh *user* (172.16.3.251/24) hanya bisa mengakses web yang ada pada *server*(172.16.1.2/30) dan tidak bisa melakukan 'ping' pada *server*, namun *server* bisa melakukan 'ping' pada tiap *user* yang ada di jaringan".

Berdasarkan *rule* 2 maka ping dari *user* ke *server* akan gagal, seperti yang ditunjukkan pada Gambar 4.17



Gambar 4.17 Gagal ping dari *user*

a. Test ping dari *server* ke *user.* Dengan *rule* yang sama, berdasarkan *rule* nomor 1, maka ping dari *server* ke *user* seharusnya berhasil, seperti yang ditunjukkan pada Gambar 4.18.



Gambar 4.18 Berhasil ping dari *server* ke *user*

b. Tes membuka web dari *user*/*client.* Berdasarkan *rule* yang sama dan *rule* tersebut sedang aktif (*enable*) maka seharusnya *user* bisa membuka web yang ada pada *server*. *Rule* tersebut ada pada *rule* nomor 0 dan 1, maka hasil nya akan tampak seperti pada Gambar 4.19.

Gambar 4.19 *Default web* berhasil di buka dari *user*

4.2.2 Uji Keberhasilan *Firewall*

Akan digunakan dua buah IP *address* untuk melakukan simulasi penyerangan, berikut adalah IP *address* penyerang seperti yang terlihat pada Gambar 4.20 dan Gambar 4.21.

Gambar 4.20 IP *address* penyerang dengan *port scanner*

Gambar 4.21 IP *address* penyerang dengan *brute force*

a. Penyerangan dengan *port scanner*. Penyerang hanya perlu memasukkan ip *address* dari target yang akan di serang, dan TCP *port* yang diinginkan contoh nya *port* 21 adalah FTP, *port* 23 adalah telnet dan lain-lain, setelah itu tombol *scan* dipilih, maka akan tampil *port* yang terbuka seperti terlihat pada Gambar 4.22.

Gambar 4.22 *Port* yang terdeteksi oleh *port scanner*

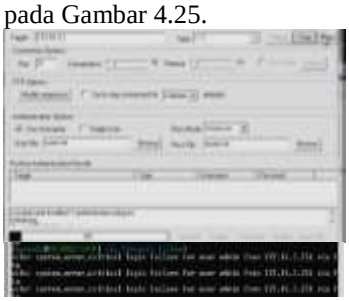
Jika *rule* mencegah *port scanner* telah diaktifkan, maka *port scanner* tidak akan bisa berjalan dan secara langsung ip *address* penyerang akan diblok dan dimasukkan ke dalam menu ip/*firewall*/*address-list. Rule* seperti yang dijalankan ditunjukkan pada Gambar 4.23.

Gambar 4.23 *Port scanner* menjadi tidak aktif dan ip penyerang masuk ke dalam menu ip/*firewall*/*address-list*

Tiap ip *address* yang masuk ke dalam menu ip/*firewall*/*address-list* akan diblok sehingga tidak bisa melakukan koneksi ke *router* MikroTik. Untuk koneksi *time out* di tunjukkan pada Gambar 4.24.

Gambar 4.24 Koneksi *time out*

b. Penyerangan dengan *brute force*. Penyerang hanya perlu memasukkan alamat dari perangkat yang ingin di serang, lalu pada menu *type* dipilih jenis *protocol* yang akan digunakan oleh *brute force* untuk penyerangan dan klik tombol *start* untuk memulai serangan. Tampilan untuk *brute force* yang sedang bekerja dan alat yang diserang tampak pada Gambar 4.25.



Gambar 4.25 *Brute force* yang melakukan penyerangan dan *device* yang diserang

Jika *rule* mencegah *brute force* telah diaktifkan, maka *brute force* Brutus AET2 tidak akan bisa berjalan dan secara langsung ip *address* penyerang akan diblok dan dimasukkan ke dalam menu ip/*firewall*/*address-list.* Jalannya *rule* ditunjukkan pada Gambar 4.26.

Gambar 4.26 *Brute force* menjadi tidak aktif dan ip penyerang masuk ke dalam menu ip/*firewall*/*address-list*

5. KESIMPULAN

a. Kecepatan transfer data yang lambat pada jaringan DISKOMINFO Depok yang disebabkan oleh serangan-serangan baik dari pihak luar maupun dalam jaringan karena belum adanya hak akses antara *client-server*. Permasalahan tersebut dapat teratasi oleh sistem *firewall rules* yang telah dikonfigurasi dalam alat jaringan MikroTik termasuk pengamanan *server* dengan DMZ *Rules*.
b. Routing *protocol* yang telah diubah dari *static* menjadi OSPF membuat jalannya jaringan data

menjadi lebih baik dan lebih cepat, serta admin dapat mengelola jaringan lebih baik dan mudah.

c. Keamanan jaringan menjadi lebih baik dengan adanya konfigurasi yang tidak sesuai dengan konfigurasi *default* pada awal ketika pembelian alat jaringan, admin pun dapat melakukan pengelolaan alat-alat jaringan yang saling terkoneksi dengan baik.

d. Hasil yang didapat setelah penerapan konfigurasi-konfigurasi yang dilakukan pada penelitian adalah seperti yang dijelaskan pada Tabel 5.1.

DAFTAR PUSTAKA

Castelli MJ. *LAN Switching First-Step*. Indianapolis: Cisco Press

Herlambang ML, L AC. *Panduan Lengkap Menguasai Router Masa Depan Menggunakan MikroTik RouterOS™*. Yogyakarta: Andi

[Ichsan N]. nurichsan.blog.unsoed.ac.id. 2010. [terhubung berkala]. http://nurichsan.blog.unsoed.ac.id/2010/11/19/metode-pengembangan-waterfall-prototyping/. [Maret 2014]

[MikroTik]. wiki.mikrotik.com. 2008. [terhubung berkala]. http://wiki.mikrotik.com/wiki/Bruteforce_login_prevention_(FTP_%26_SSH). [Februari 2014]

[MikroTik]. wiki.mikrotik.com. 2011. [terhubung berkala]. http://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter. [Februari 2014]

[MikroTik]. wiki.mikrotik.com. 2011. [terhubung berkala]. http://wiki.mikrotik.com/wiki/Manual:Routing/OSPF. [Februari 2014]

[Wikipedia]. id.wikipedia.org. 2012. [terhubung berkala]. http://id.wikipedia.org/wiki/MikroTik. [Maret 2014]

[Wikipedia]. id.wikipedia.org. 2012. [terhubung berkala]. http://id.wikipedia.org/wiki/Tembok_api. [Maret 2014]

Miller LC. *Next-Generation Firewall for Dummies*. Indianapolis: Wiley

Parkhurst B. 2005. *Routing First-Step*. Indianapolis: Cisco Press

Schudel G, Smith DJ. *Routing Security Strategies Securing IP Network Traffic Planes*. Indianapolis: Cisco Press

Stallings W. 2003. *Computer Organization & Architecture*. New Jersey: Pearson Educati.