
**IMPLEMENTASI BLOCKING WEBSITE MENGGUNAKAN
7 LAYER PROTOKOL BERBASIS MIKROTIK RB 750**



**PROGRAM STUDI TEKNIK LISTRIK D-III
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
2011**

LEMBAR PERSETUJUAN

IMPLEMENTASI BLOCKING WEBSITE MENGGUNAKAN
7 LAYER PROTOKOL BERBASIS MIKROTIK RB 750



TUGAS AKHIR

*Disusun dan Diajukan Untuk Melengkapi dan
Memenuhi Syarat-syarat Guna Mencapai Gelar Diploma Tiga*

Disusun Oleh :

Kuncoro Cahyo Wicaksono
NIM : 07. 52. 517

Diperiksa dan Disetujui :

Dosen Pembimbing I


Ir. Eko Nur Cahyo
NIP.1028700172

Dosen Pembimbing II


Sonny Prasetyo, ST,MT
NIP.10310004433

Ketua Program Studi
Teknik Listrik DIII


Ir. Taufik Hidayat, MT
NIP. Y. 1018700151

PROGRAM STUDI TEKNIK LISTRIK D III
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
2011

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Allah Yang Maha Kuasa, karena berkat rahmat dan hidayahnya dapat memberi kesabaran, bimbingan dan perlindungan sehingga penulis dapat menyelesaikan tugas akhir dengan judul **IMPLEMENTASI BLOCKING WEBSITE MENGGUNAKAN LAYER 7 PROTOKOL BERBASIS MIKROTIK RB 750**

Pembuatan tugas akhir ini disusun guna memenuhi persyaratan kelulusan jenjang Diploma III di Institut Teknologi Nasional Malang. Dalam penulisan akhir ini, penulis mendapat banyak bantuan serta dukungan baik moril maupun materiil, saran dan dorongan semangat dari berbagai pihak, untuk itu penulis sangat – sangat mengucapkan terimakasih kepada:

1. Bapak Prof. Dr. Abraham Lomi, MSEE., selaku rektor ITN Malang.
2. Bapak Ir. Sidik Noerjahjono., selaku Dekan Fakultas Teknologi Industri.
3. Bapak Ir. H. Taufik Hidayat, MT, sebagai ketua jurusan Teknik Elektro D-3.
4. Bapak Ir. Eko Nur Cahyo selaku dosen pembimbing I.
5. Bapak Sonny Prasetyo. ST,MT dosen pembimbing II

5. Bapak Ir. Bambang Prio H, MT, selaku sekretaris jurusan Teknik Elektro D-3.
6. Dan untuk teman – teman serta semua pihak yang telah membantu terselesaikannya tugas akhir ini.

Penulis menyadari bahwa laporan ini masih banyak yang perlu disempurnakan. Oleh sebab itu kritik dan saran yang membangun sangat diharapkan dari berbagai pihak.

Akhir kata , penulis mohon maaf kepada semua pihak apabila selama penyusunan tugas akhir ini penyusun melakukan kesalahan secara sengaja dan semoga tugas akhir ini dapat bermanfaat bagi kita semua.

Malang, Februari 2011

Penulis

ABSTRAK

“IMPLEMENTASI BLOCKING WEBSITE MENGGUNAKAN LAYER 7 PROTOKOL BERBASIS MIKROTIK RB 750”

(Kuncoro Cahyo Wicaksono, 0752517, Teknik Komputer DIII, 51 halaman)

(Dosen pembimbing I : Ir. Eko Nur Cahyo)

(Dosen Pembimbing II : Sonny Prasetyo.ST,MT)

Suatu sistem di *internet* memungkinkan siapapun bisa menyediakan informasi. Dengan menggunakan teknologi tersebut, informasi dapat diakses selama 24 jam dan dikelola oleh mesin. Situs jejaring social Facebook akhir-akhir ini sangat cukup terkenal dan sangat digemari oleh banyak orang bahkan anak kecil yang masih Sekolah Dasar pun sudah tau apa itu facebook.

Untuk itu para pimpinan mulai resah atas perilaku kinerja karyawan yang kurang efektif, terjadilah dialog antara pimpinan dan admin jaringan untuk mencari solusi yang terbaik. Munculah suatu kebijakan untuk menutup akses facebook dari pukul 08.00-15.00 Wib dengan memberikan kesempatan karyawan untuk mengakses situs jejaring selama 1 jam sebelum pulang kerja.

Tadinya kami berniat untuk block ip perblok tetapi ini tidak efektif karena takut ada ip lain yang terkena block, akhirnya mencobalah block menggunakan layer 7 ini. Oleh sebab itu saya membuat Implementasi blocking website menggunakan layer 7 protokol berbasis mikrotik RB 750 sehingga dapat membantu kinerja admin untuk lebih mudah dan efektif.

DAFTAR ISI

| | Halaman |
|--|----------|
| HALAMAN JUDUL | i |
| HALAMAN PERSETUJUAN | ii |
| HALAMAN PENGESAHAN | iii |
| KATA PENGANTAR | iv |
| ABSTRAK | v |
| DAFTAR ISI | vi |
| DAFTAR GAMBAR | xii |
| | |
| BAB I PENDAHULUAN | 1 |
| 1.1 Latar Belakang..... | 1 |
| 1.2 Rumusan Masalah..... | 2 |
| 1.3 Tujuan..... | 2 |
| 1.4 Batasan Masalah..... | 2 |
| 1.5 Metodologi Penelitian..... | 3 |
| 1.6 Sistematika Penulisan..... | 5 |
| | |
| BAB II TINJAUAN PUSTAKA | 7 |
| 2.1 Pengertian mikrotik router..... | 6 |
| 2.2 Pengertian mikrotik router OS..... | 6 |

| | | |
|------|------------------------------------|----|
| 2.3 | Sejarah mikrotik router OS | 8 |
| 2.4 | Jenis- jenis mikrotik | 9 |
| 2.5 | Fitur – fitur mikrotik | 10 |
| 2.6 | 7 Layer Protokol | 12 |
| 2.7 | Pengertian Sistem Operasi | 13 |
| 2.8 | Pengertian Jaringan Komputer | 14 |
| 2.9 | Gateway | 17 |
| 2.10 | Proxy Server | 17 |
| | 2.10.1 Firewall | 18 |
| | 2.10.2 Virtual LAN..... | 18 |

BAB III PERANCANGAN DAN ANALISA BLOCKING WEBSITE 19

| | | |
|-----|---|----|
| 3.1 | Diskripsi Mikrotik | 19 |
| 3.2 | Alur perancangan system | 20 |
| 3.3 | Proses Instalai WinBox..... | 25 |
| 3.4 | Firewall..... | 28 |
| | 3.4.1 Ganti Pasword Admin..... | 28 |
| | 3.4.2 Tambahkan User pada Mikrotik..... | 29 |
| | 3.4.3 Set Up Packet Filtering | 29 |

| | |
|---|-----------|
| BAB. IV IMPLEMENTASI DAN PEMBAHASAN..... | 36 |
| 4.1 Sistem Konfigurasi Awal | 36 |
| 4.2 Seting Dasar mikrotik | 36 |
| 4.3 Langkah Setting Mikrotik dengan Win Box | 37 |
| 4.4 Pengujian system | 52 |
| BAB. V PENUTUP | |
| 5.1 Kesimpulan | 53 |
| 5.2 Saran | 54 |
| DAFTAR PUSTAKA..... | 55 |

DAFTAR GAMBAR

| | |
|---|----|
| 1. Gambar 2.1 Mikrotik routerboard..... | 8 |
| 2. Gambar 2.2 Jaringan Local Area Network (LAN)..... | 15 |
| 3. Gambar 2.3 Jaringan Metropolitan Network (MAN)..... | 15 |
| 4. Gambar 2.4 Jaringan Wide Area Network (WAN)..... | 16 |
| 5. Gambar 3.1 Folder yang berisi WinBox.exe..... | 26 |
| 6. Gambar 3.2 Tampilan Login WinBox..... | 26 |
| 7. Gambar. 3.3 Tampilan WinBox Setelah Login..... | 27 |
| 8. Gambar. 2.4 Ganti password Admin..... | 28 |
| 9. Gambar. 2.5. Form untuk membuat grup baru..... | 29 |
| 10. Gambar. 3.6. Filterisasi rule..... | 32 |
| 11. Gambar 3.7 Urutan Chart foward..... | 35 |
| 12. Gambar 3.2 Tampilan proses awal instalasi Macromedia dreamweaver..... | 35 |
| 13. Gambar 4.1 Tampilan login WinBox..... | 37 |
| 14. Gambar 4.2 Tampilan WinBox setelah login..... | 38 |
| 15. Gambar 4.3 Tampilan untuk mensetting layer 7 protokol..... | 38 |
| 16. Gambar 4.4 Form name and regexp..... | 39 |
| 17. Gambar 4.5 Form setting mangle..... | 40 |
| 18. Gambar 4.6 Form advance..... | 40 |
| 19. Gambar 4.7 Form action..... | 41 |
| 20. Gambar 4.8 Form mangle rule..... | 41 |
| 21. Gambar 4.10 Tab action..... | 42 |

| | |
|--|----|
| 22. Gambar 4.11 Form mangle List..... | 42 |
| 23. Gambar 4.12 Form general | 43 |
| 24. Gambar 4.13 Form tab action..... | 44 |
| 25. Gambar 4.14 Form general..... | 44 |
| 26. Gambar 4.15 Aktifkan option log..... | 45 |
| 27. Gambar 4.16 Form Add Rules | 45 |
| 28. Gambar 4.17 Form tab action..... | 46 |
| 29. Gambar 4.18 Form Add rules..... | 46 |
| 30. Gambar 4.19 Form Advance List | 47 |
| 31. Gambar 4.20 Form Action List..... | 47 |
| 32. Gambar 4.21 Form coment for firewall rule..... | 48 |
| 33. Gambar 4.22 Open script for access..... | 49 |
| 34. Gambar 4.23 Form script filter rule..... | 49 |
| 35. Gambar 4.24 Form to sceedhule..... | 50 |
| 36. Gambar 4.25 Form Script blacking | 50 |
| 37. Gambar 4.26 Form Address List | 51 |



BAB I

PENDAHULUAN

1.1. LATAR BELAKANG

Di era kompetisi global seperti sekarang ini kenyamanan, keamanan serta efisiensi waktu dalam mengakses informasi merupakan suatu hal yang sangat diperlukan. Bahkan sistem informasi yang tersedia pada suatu perusahaan menjadi salah satu ukuran kompetitif atau tidaknya suatu perusahaan. Teknologi internet sudah terbukti merupakan salah satu media informasi yang efektif dan efisien dalam penyebaran informasi yang dapat diakses oleh siapa saja, kapan saja dan dimana saja. Teknologi internet mempunyai efek yang sangat besar pada manusia . Oleh karena itu banyak sekali hal yang akan ditimbulkan, mulai dari positif dan negatifnya. Oleh sebab itu saya membuat suatu implementasi blogging website menggunakan layer 7 protokol yang berbasis mikrotik RB 750 guna membatasi akses kebeberapa website yang diinginkan.

1.2. RUMUSAN MASALAH

Pada perancangan dan pembuatan Tugas Akhir ini masalah yang ditangani adalah bagaimana membatasi akses ke beberapa website dengan menggunakan layer 7 protokol berbasis mikrotik RB 750.

1.3. TUJUAN

Adapun tujuan dari pembuatan Tugas Akhir ini adalah untuk membatasi akses ke beberapa website yang diinginkan, khususnya digunakan di sekolah maupun suatu instansi guna memberikan batasan-batasan agar user tidak dapat mengakses website tertentu diluar kegiatan belajar mengajar ataupun suatu pekerjaan.

1.4. BATASAN MASALAH

Dalam bentuk pelayanan publik mencakup :

- Sekolah ataupun suatu instansi yang membutuhkan
- Kemitraan dalam membatasi maraknya website yang semakin menjamur di dunia maya

Disini saya akan mengaplikasikan project saya di SMP Negeri 02 Sumberpucung yang berada di Jl. TRIP.(TGP) No.2 Sumberpucung

Blogging website ini menggunakan layer 7 protokol

Hardware yang digunakan berbasis mikrotik RB 750

1.5. METODE PENELITIAN

Adapun metode penelitian yang digunakan dalam tugas akhir ini adalah sebagai berikut:

1. Studi Literatur

Pengumpulan data dan informasi mengenai hal-hal yang berkaitan dengan pembatasan situs website dengan mencari referensi dari berbagai sumber yang digunakan sebagai landasan teori untuk permasalahan yang dibahas.

2. Analisa Kebutuhan Sistem

Adalah suatu penggabungan, pernyataan dari dua atau lebih bagian-bagian komponen-komponen, atau sub - sub sistem yang interdependen

3. Perancangan Sistem.

Desain Sistem adalah langkah awal pembuatan sistem yang merupakan penjelasan hal -hal yang akan dilakukan pada saat pembuatan sistem sampai dengan sistem tersebut siap diaplikasikan.

4. Perancangan hardware

Pada Tahap ini kita memakai routerboard mikrotik RB750 untuk mengkonfigurasi/ memonopoli jaringan.

5. Eksperimen dan Evaluasi.

Pada tahapan Eksperimen dan evaluasi ini sistem informasi yang dibuat akan diuji coba berdasarkan fungsionalitas yang dibuat dan akan dilakukan pengoreksian dan penyempurnaan sistem jika diperlukan.

6. Penyusunan Buku

Menyimpulkan hasil perencanaan dan pembuatan system informasi serta penyempurnaan sistem dengan hasil pengujian, sehingga tersusunlah buku laporan Tugas Akhir.

1.6. SISTEMATIKA PENULISAN

Setelah dilakukan proses pembuatan dan perancangan system informasi pada Tugas Akhir ini, mulai dari studi literatur, perencanaan, pembuatan, pengujian dan perbaikan, serta analisa dan hasil – hasil yang didapat, maka untuk pembahasan selengkapnya diwujudkan dalam bentuk buku laporan Tugas Akhir ini dengan sistematika sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini membahas pendahuluan yang terdiri dari latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi penelitian dan sistematika penulisan Tugas Akhir.

BAB II : TINJAUAN PUSTAKA

Bab ini berisi tentang landasan teori mengenai permasalahan yang berhubungan dengan penelitian yang dilakukan.

BAB III : PERANCANGAN DAN ANALISA IMPLEMENTASI

Bab ini menjelaskan tentang perancangan dan analisa dari kebutuhan informasi yang diperlukan untuk system informasi yang akan dibuat.

BAB IV : PEMBUATAN DAN PENGUJIAN IMPLEMENTASI

Berisi tentang implementasi dari peancangan aplikasi yang telah dibuat serta pengujian terhadap aplikasi tersebut.

BAB V : PENUTUP

Pada bab ini berisikan kesimpulan dari keseluruhan pengerjaan Tugas Akhir dan juga saran saran serta masukan setelah melihat hasil analisa dari pengujian dari sistem informasi yang dibuat yang selanjutnya dapat digunakan sebagai pertimbangan untuk pengembangan penulisan selanjutnya.

1.7 Tinjauan Pustaka

Mikrotik routerOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer biasa menjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless. Fitur-fitur tersebut diantaranya : Firewall & Nat, Routing, Hotspot, Point to Point Tunneling Protocol, DNS server, DHCP server, Hotspot, dan masih banyak lagi fitur. Mikrotik dapat digunakan dalam 2 tipe, yaitu dalam bentuk perangkat keras dan perangkat lunak. Dalam bentuk perangkat keras, Mikrotik biasanya sudah diinstalasi pada suatu board tertentu, sedangkan dalam bentuk perangkat lunak, Mikrotik merupakan satu distro Linux yang memang dikhususkan untuk fungsi router. Umumnya pemblokiran URL / situs dapat dilakukan dengan layer7 Pada Mikrotik yang merupakan salah satu application firewall yang memiliki fungsi yang cukup bagus dalam melakukan Block situs /url pada Mikrotik Ver. 3.x sehingga dapat membantu para administrator jaringan untuk melakukan pemblokiran terhadap situs-situs yang menurunkan kinerja karyawan karena seringnya melakukan internetan ketimbang kerjaan misalnya situs facebook yang akhir-akhir ini cukup ngetren di kalangan baik anak2, remaja bahkan para keryawan dan karyawati sekalian.



BAB II

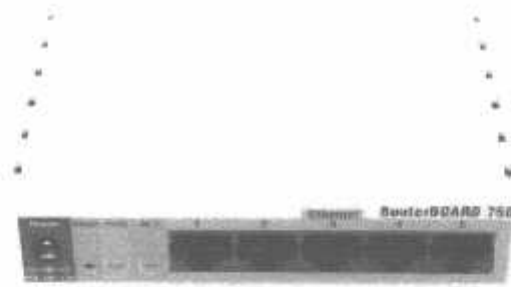
LANDASAN TEORI

2.1 Pengertian Mikrotik Router

Mikrotik Router adalah perangkat yang akan melewatkan paket IP dari suatu jaringan ke jaringan yang lain, menggunakan metode addressing dan protocol tertentu untuk melewatkan paket data tersebut. Router memiliki kemampuan melewatkan paket IP dari satu jaringan ke jaringan lain yang mungkin memiliki banyak jalur diantara keduanya. Router-router yang saling terhubung dalam jaringan internet turut serta dalam sebuah algoritma routing terdistribusi untuk menentukan jalur terbaik yang dilalui paket IP dari system ke system lain. Proses routing dilakukan secara hop by hop. IP tidak mengetahui jalur keseluruhan menuju tujuan setiap paket. IP routing hanya menyediakan IP address dari router berikutnya yang menurutnya lebih dekat ke host tujuan.

Fungsi :

- Membaca alamat logika / ip address source & destination untuk menentukan routing dari suatu LAN ke LAN lainnya.
 - Menyimpan routing table untuk menentukan rute terbaik antara LAN WAN.
 - Perangkat di layer 3 OSI Layer.
 - Bisa berupa "box" atau sebuah OS yang menjalankan sebuah daemon routing.
 - Interfaces Ethernet, Serial, ISDN BRI.
-



Gambar 2.1 Mikrotik routerboard

2.2 Pengertian MikroTik Router OS

MikroTik RouterOS™, merupakan sistem operasi Linux base yang diperuntukkan sebagai network router. Didesain untuk memberikan kemudahan bapenggunanya. Administrasinya dilakukan melalui Windows Application (WinBox). Selain itu instalasi dapat dilakukan pada Standard komputer PC (PersonalComputer). PC yang akan dijadikan router mikrotik pun tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway. Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan resource PC yang memadai.

2.3 Sejarah MikroTik RouterOS

MikroTik adalah sebuah perusahaan kecil 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 bejumpa dengan Arnis, Seorang darjana Fisika dan Mekanik sekitar tahun 1995. John dan Arnis mulai me-routing dunia pada tahun 1996 (misi MikroTik adalah me-routing seluruh dunia). Mulai dengan sistem Linux dan MS-DOS yang dikombinasikan dengan teknologi Wireless-LAN (WLAN) Aeronet berkecepatan 2 Mbps di Moldova, negara tetangga Latvia, baru kemudian melayani lima pelanggannya 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 eksperimen 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 staff 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.

2.4 JENIS-JENIS MIKROTIK

1. MikroTik RouterOS yang berbentuk software yang dapat di-download di www.mikrotik.com. Dapat diinstal pada kompuetr rumahan (PC).
 2. BUILT-IN Hardware MikroTik dalam bentuk perangkat keras yang khusus dikemas dalam board router yang didalamnya sudah terinstal MikroTik RouterOS.
-

2.5 FITUR-FITUR MIKROTIK

1. Address List : Pengelompokan IP Address berdasarkan nama
 2. Asynchronous : Mendukung serial PPP dial-in / dial-out, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, Radius, dial on demand, modem pool hingga 128 ports.
 3. Bonding : Mendukung dalam pengkombinasian beberapa antarmuka ethernet ke dalam 1 pipa pada koneksi cepat.
 4. Bridge : Mendukung fungsi bridge spinning tree, multiple bridge interface, bridging firewalling.
 5. Data Rate Management : QoS berbasis HTB dengan penggunaan burst, PCQ, RED, SFQ, FIFO queue, CIR, MIR, limit antar peer to peer
 6. DHCP : Mendukung DHCP tiap antarmuka; DHCP Relay; DHCP Client, multiple network DHCP; static and dynamic DHCP leases.
 7. Firewall dan NAT : Mendukung pemfilteran koneksi peer to peer, source NAT dan destination NAT. Mampu memfilter berdasarkan MAC, IP address, range port, protokol IP, pemilihan opsi protokol seperti ICMP, TCP Flags dan MSS.
 8. Hotspot : Hotspot gateway dengan otentikasi RADIUS. Mendukung limit data rate, SSL ,HTTPS.
 9. IPSec : Protokol AH dan ESP untuk IPSec; MODP Diffie-Hellmann groups 1, 2, 5; MD5 dan algoritma SHA1 hashing; algoritma enkripsi menggunakan DES, 3DES, AES-128, AES-192, AES-256; Perfect Forwarding Secresy (PFS) MODP groups 1, 2,5
-

10. ISDN : mendukung ISDN dial-in/dial-out. Dengan otentikasi PAP, CHAP, MSCHAPv1 dan MSCHAPv2, Radius. Mendukung 128K bundle, Cisco HDLC, x751, x75ui, x75bui line protokol.
 11. M3P : MikroTik Protokol Paket Packer untuk wireless links dan ethernet.
 12. MNDP : MikroTik Discovery Neighbour Protokol, juga mendukung Cisco Discovery Protokol (CDP).
 13. Monitoring / Accounting : Laporan Traffic IP, log, statistik graph yang dapat diakses melalui HTTP.
 14. NTP : Network Time Protokol untuk server dan clients; sinkronisasi menggunakan system GPS.
 15. Poin to Point Tunneling Protocol : PPTP, PPPoE dan L2TP Access Concentrator; protokol otentikasi menggunakan PAP, CHAP, MSCHAPv1 MSCHAPv2; otentikasi dan laporan Radius; enkripsi MPPE; kompresi untuk PPOE; limit data rate.
 16. Proxy : Cache untuk FTP dan HTTP proxy server, HTTPS proxy; transparent proxy untuk DNS dan HTTP; mendukung protokol SOCKS; mendukung parent proxy; static DNS.
 17. Routing : Routing statik dan dinamik; RIP v1/v2, OSPF v2, BGP v4.
 18. SDSL : Mendukung Single Line DSL; mode pemutusan jalur koneksi dan jaringan.
 19. Simple Tunnel : Tunnel IPIP dan EoIP (Ethernet over IP).
 20. SNMP : Simple Network Monitoring Protocol mode akses read-only.
-

21. Synchronous : V.35, V.24, E1/T1, X21, DS3 (T3) media types; sync-PPP, Cisco HDLC; Frame-Relay line protokol; ANSI-617d (ANDI atau annex D) dan Q933a (CCITT atau annex A); Frame Relay jenis LMI.
22. Tool : Ping, Traceroute; bandwidth test; ping flood; telnet; SSH; packet sniffer; Dinamik DNS update.
23. UPnP : Mendukung antarmuka Universal Plug and Play.
24. VLAN : Mendukung Virtual LAN IEEE 802.1q untuk jaringan ethernet dan wireless; multiple VLAN; VLAN bridging.
25. VoIP : Mendukung aplikasi voice over IP.
26. VRRP : Mendukung Virtual Router Redudant Protocol.
27. WinBox : Aplikasi mode GUI untuk meremote dan mengkonfigurasi MikroTik RouterOS.
28. Blocking website dan managemen

2.6 7 layer Protokol

Pada awal mulanya penutupan situs jejaring facebook dilakukan dengan memblok ip satu persatu menggunakan ip firewall filter, tetapi ini berlangsung hanya sekitar 2 bulan saja, selebihnya banyak karyawan yang sudah bisa mengaksesnya kembali, saya coba mengikuti list ip facebook.com satu persatu tetapi sangat banyak sekali, tadinya berniat untuk block ip perblok tetapi ini tidak efektif karena takut ada ip lain yang terkena block, ahirnya mencobalah block menggunakan layer 7 ini.

2.7 Pengertian Sistem Operasi

Sistem operasi adalah sekumpulan rutin perangkat lunak yang berada diantara program aplikasi dan perangkat keras (Bambang Hariyanto,2006,hal 25). Sistem operasi memiliki tugas yaitu mengelola seluruh sumber daya sistem komputer dan sebagai penyedia layanan. Sistem operasi menyediakan System Call (berupa fungsi-fungsi atau API=Application Programming Interface). System Call ini memberikan abstraksi tingkat tinggi mesin untuk pemrograman. System Call berfungsi menghindarkan kompleksitas pemrograman dengan memberi sekumpulan instruksi yang lebih mudah dan nyaman, sistem operasi juga sebagai basis untuk program lain dimana program aplikasi dijalankan diatas sistem operasi, program-program itu memanfaatkan sumber daya sistem komputer dengan cara meminta layanan sistem operasi mengendalikan sumber daya untuk aplikasi sehingga penggunaan sumber daya sistem komputer dapat dilakukan secara benar dan efisien.

Sistem operasi yang dikenal antara lain :

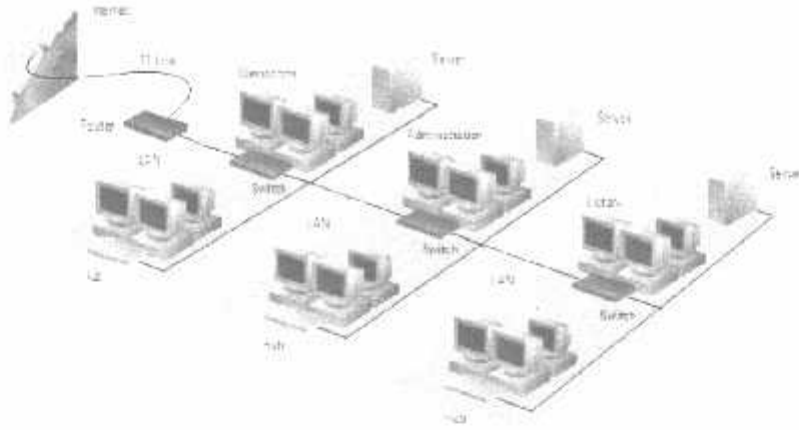
- ❖ Windows (95, 98, ME, 2000, XP, VISTA, SERVER, Windows7)
 - ❖ Linux (RedHat, Slackware, Ubuntu ,Fedora, Mikrotik, Debian, OpenSUSE)
 - ❖ UNIX
 - ❖ FreeBSD (Berkeley Software Distribution)
 - ❖ SUN (SOLARIS)
 - ❖ DOS (MS-DOS)
 - ❖ Machintosh (MAC OS, MAC OSX)
-

2.8 Pengertian Jaringan Komputer

Jaringan komputer merupakan sekelompok komputer otonom yang saling dihubungkan satu sama lainnya, menggunakan suatu media dan protocol komunikasi tertentu, sehingga dapat saling berbagi data dan informasi.(Deris Setiawan,2003,hal 1). Jaringan komputer memungkinkan terjadinya komunikasi yang lebih efisien antar pemakai (mail dan teleconference). Jaringan komputer adalah sekelompok komputer otonom yang saling menggunakan protocol komunikasi melalui media komunikasi (Dharma Oetomo(1),2003, hal 07) sehingga dapat berbagi data, informasi, program aplikasi dan perangkat keras seperti printer, scanner, CD-Drive maupun harddisk serta memungkinkan komunikasi secara elektronik. Sedangkan pada Aplikasi home user, memungkinkan komunikasi antar pengguna lebih efisien (chat), interaktif entertainment lebih multimedia (games, video,dan lain-lain).

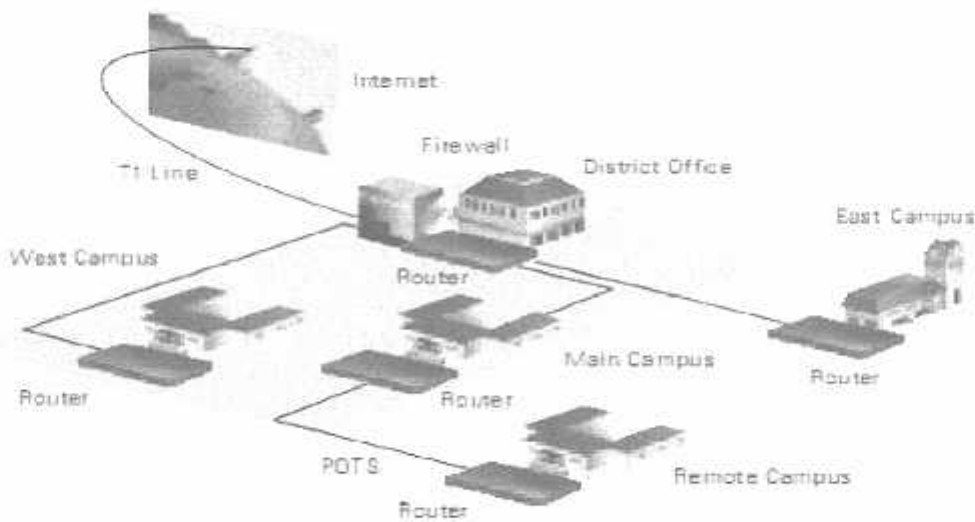
Klasifikasi Jaringan Komputer :

- ❖ LAN (Local Area Network) : Jaringan komputer yang saling terhubung ke suatu komputer server dengan menggunakan topologi tertentu, biasanya digunakan dalam kawasan satu gedung atau kawasan yang jaraknya tidak lebih dari 1 km.
-



Gambar 2.1 Jaringan Local Area Network

- ❖ MAN (Metropolitan Area Network) : Jaringan komputer yang saling terkoneksi dalam satu kawasan kota yang jaraknya sampai lebih dari 1 km. Pilihan untuk membangun jaringan komputer antar kantor dalam suatu kota, kampus dalam satu kota.



Sumber : www.cisco.com

Gambar 2.2 Jaringan Metropolitan Area Network (MAN)

- ❖ WAN (Wide Area Network) : Jaringan komputer yang menghubungkan banyak LAN ke dalam suatu jaringan terpadu, antara satu jaringan dengan jaringan lain dapat berjarak ribuan kilometer atau terpisahkan letak geografi dengan menggunakan metode komunikasi tertentu.



Gambar 2.3 Jaringan WAN

Secara garis besar ada beberapa tahapan dalam membangun jaringan LAN :

- ❖ Menentukan teknologi tipe jaringannya (Ethernet, Fast Ethernet, Token Ring, FDDI)
 - ❖ Memilih model perkabelan (Fiber, UTP, Coaxial)
 - ❖ Menentukan bentuk topologi jaringan (Bus, Ring, dan Star)
 - ❖ Menentukan teknologi Client/Server atau Peer to Peer
 - ❖ Memilih Sistem Operasi Server (Windows NT, 2000, XP, atau Linux)
-

2.10.1 Firewall

Sistem keamanan yang menggunakan device atau sistem yang diletakkan di dua jaringan dengan fungsi utama melakukan filtering terhadap akses yang akan masuk. Berupa seperangkat hardware atau software, bisa juga berupa seperangkat aturan dan prosedur yang ditetapkan oleh organisasi. Firewal juga dapat disebut sebagai system, atau perangkat yang mengizinkan lalu lintas jaringan yang dianggapnya aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan local dan jaringan lainnya. Firewall juga umumnya digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari hak luar. Saat ini, istilah firewall menjadi istilah generic yang merujuk pada sistem yang mengatur komunikasi antar dua jaringan yang berbeda. (PC MILD edisi 13/2008)

2.10.2 Virtual LAN

VLAN berupa suatu software dari device switch yang berfungsi untuk mengelompokkan user berdasarkan fungsional, 1 broadcast domain (1 VLAN) dan antar VLAN dapat terkoneksi dengan router. Teknologi VLAN adalah suatu cara yang memisahkan segmen-segmen pada switch dimana antara 1 segmen dengan segmen lain tidak dapat terkoneksi, koneksi dapat dilakukan dengan menggunakan router. Dalam satu switch akan berbeda network-id-nya dan berbeda broadcast domainnya.



BAB III

INSTALASI DAN PERANCANGAN SISTEM

3.1 Deskripsi mikrotik

Instalasi mikrotik dapat dilakukan pada Standard computer PC. PC yang akan dijadikan router mikrotikpun tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway.

Berikut spec minimal nya :

1. CPU and motherboard – bisa pake P1 ampe P4, AMD, cyrix asal yang bukan multi-prosesor.
2. RAM – minimum 32 MiB, maximum 1 GiB; 64 MiB atau lebih sangat dianjurkan, kalau mau sekalian dibuat proxy , dianjurkan 1GB... perbandingannya, 15MB di memori ada 1GB di proxy.
3. HDD minimal 128MB parallel ATA atau Compact Flash, tidak dianjurkan menggunakan UFD, SCSI, apa lagi S-ATA Very Happ
4. NIC 10/100 atau 100/1000

Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit dll) disarankan untuk mempertimbangkan pemilihan resource PC yang memadai.

3.2 Alur Perancangan Sistem

Layer 7 protokol adalah suatu arsitektur komunikasi yang digunakan untuk menghubungkan komputer-komputer dari vendor-vendor yang berbeda. Layer ini berada pada urutan ketujuh model Open System Interconnection (OSI) yang menggunakan protocol dan format data yang berbeda-beda.

Alur perancangan system menggunakan 7 layer protocol dapat dikategorikan sangat sistematis, karena gatewaynya berada pada layer ini, sehingga dapat melakukan pekerjaan yang sama seperti sebuah router.

Perancangan sistem yang diterapkan layer 7 protokol ini akan dikonfigurasi dalam mikrotik untuk membangun sebuah jaringan sederhana sebagai gateway servernya. Alur dan perancangan sistemnya sebagai berikut :

1. Langkah pertama adalah install Mikrotik RouterOS pada PC atau pasang DOM.
2. Login Pada Mikrotik Routers melalui console :
MikroTik v2.9.7
Login: admin
Password: (kosongkan)

Sampai langkah ini kita sudah bisa masuk kedalam penerapan system dengan menggunakan mikrotik. User default adalah admin dan tanpa password, tinggal ketik admin kemudian tekan tombol enter.

4. Mengganti nama Mikrotik Router, pada langkah ini nama server akan diganti menjadi "becouz" (nama ini sih bebas2 aja mo diganti)

```
[admin@Mikrotik] > system identity set name=becouz  
[admin@becouz] >
```

5. Melihat interface pada Mikrotik Router

```
[admin@becouz] > interface print  
Flags: X – disabled, D – dynamic, R – running  
# NAME TYPE RX-RATE TX-RATE MTU  
0 R ether1 ether 0 0 1500  
1 R ether2 ether 0 0 1500  
[admin@becouz] >
```

6. Memberikan IP address pada interface Mikrotik. Misalkan ether1 akan kita gunakan untuk koneksi ke Internet dengan IP 192.168.0.1 dan ether2 akan kita gunakan untuk network local kita dengan IP 172.16.0.1

```
[admin@becouz] > ip address add address=192.168.0.1  
netmask=255.255.255.0 interface=ether1  
[admin@becouz] > ip address add address=172.16.0.1  
netmask=255.255.255.0 interface=ether2
```

7. Melihat konfigurasi IP address yang sudah kita berikan

```
[admin@becouz] > ip address print  
Flags: X – disabled, I – invalid, D – dynamic
```

```
# ADDRESS NETWORK BROADCAST INTERFACE
```

```
0 192.168.0.1/24 192.168.0.0 192.168.0.63 ether1
```

```
1 172.16.0.1/24 172.16.0.0 172.16.0.255 ether2
```

```
[admin@becouz] >
```

8. Memberikan default Gateway, diasumsikan gateway untuk koneksi internet adalah 192.168.0.254

```
[admin@becouz] > /ip route add gateway=192.168.0.254
```

9. Melihat Tabel routing pada Mikrotik Routers

```
[admin@becouz] > ip route print
```

```
Flags: X – disabled, A – active, D – dynamic,
```

```
C – connect, S – static, r – rip, b – bgp, o – ospf
```

```
# DST-ADDRESS PREFSRC G GATEWAY DISTANCE INTERFACE
```

```
0 ADC 172.16.0.0/24 172.16.0.1 ether2
```

```
1 ADC 192.168.0.0/26 192.168.0.1 ether1
```

10. Tes Ping ke Gateway untuk memastikan konfigurasi sudah benar

```
[admin@becouz] > ping 192.168.0.254
```

```
192.168.0.254 64 byte ping: ttl=64 time
```

11. Setup DNS pada Mikrotik Routers

```
[admin@becouz] > ip dns set primary-dns=192.168.0.10 allow-remoterequests=no
```

```
[admin@becouz] > ip dns set secondary-dns=192.168.0.11 allow-remoterequests=no
```

12. Melihat konfigurasi DNS

```
[admin@becouz] > ip dns print  
primary-dns: 192.168.0.10  
secondary-dns: 192.168.0.11  
allow-remote-requests: no  
cache-size: 2048KiB  
cache-max-ttl: 1w  
cache-used: 16KiB  
[admin@becouz] >
```

13. Tes untuk akses domain, misalnya dengan ping nama domain

```
[admin@becouz] > ping yahoo.com  
216.109.112.135 64 byte ping: ttl=48 time=250 ms  
10 packets transmitted, 10 packets received, 0% packet loss  
round-trip min/avg/max = 571/571.0/571 ms  
[admin@becouz] >
```

Jika sudah berhasil reply berarti seting DNS sudah benar.

14. Setup Masquerading, Jika Mikrotik akan kita pergunakan sebagai gateway server maka agar client computer pada network dapat terkoneksi ke internet perlu kita masquerading.

```
[admin@becouz]> ip firewall nat add action=masquerade outinterface=  
ether1 chain:srcnat  
[admin@becouz] >
```

15. Melihat konfigurasi Masquerading

```
[admin@becouz]ip firewall nat print
```

```
Flags: X – disabled, I – invalid, D – dynamic
```

```
0 chain=srcnat out-interface=ether1 action=masquerade
```

```
[admin@becouz] >
```

Setelah langkah ini bisa dilakukan pemeriksaan untuk koneksi dari jaringan local. Dan jika berhasil berarti kita sudah berhasil melakukan instalasi Mikrotik Router sebagai Gateway server. Setelah terkoneksi dengan jaringan Mikrotik dapat dimanage menggunakan WinBox yang bisa di download dari Mikrotik.com atau dari server mikrotik kita.

Misal Ip address servermikrotik kita 192.168.0.1, via browser buka <http://192.168.0.1> dan download WinBox dari situ. Jika kita menginginkan client mendapatkan IP address secara otomatis maka perlu kita setup dhcp server pada Mikrotik. Berikut langkah-langkahnya :

1. Buat IP address pool

```
/ip pool add name=dhcp-pool ranges=172.16.0.10-172.16.0.20
```

2. Tambahkan DHCP Network dan gatewaynya yang akan didistribusikan ke

client Pada contoh ini networknya adalah 172.16.0.0/24 dan gatewaynya

```
172.16.0.1
```

```
/ip dhcp-server network add address=172.16.0.0/24 gateway=172.16.0.1
```

3. Tambahkan DHCP Server (pada contoh ini dhcp diterapkan pada interface ether2)

```
/ip dhcp-server add interface=ether2 address-pool=dhcp-pool
```

4. Lihat status DHCP server

```
[admin@becouz]> ip dhcp-server print
```

```
Flags: X – disabled, I – invalid
```

```
# NAME INTERFACE RELAY ADDRESS-POOL LEASE-TIME ADD-  
ARP
```

```
0 X dhcp1 ether2
```

Tanda X menyatakan bahwa DHCP server belum enable maka perlu dienablekan terlebih dahulu pada langkah 5.

5. Jangan Lupa dibuat enable dulu dhcp servernya

```
/ip dhcp-server enable 0
```

kemudian cek kembali dhcp-server seperti langkah 4, jika tanda X sudah tidak ada berarti sudah aktif.

6. Tes Dari client

```
c:\>ping www.yahoo.com
```

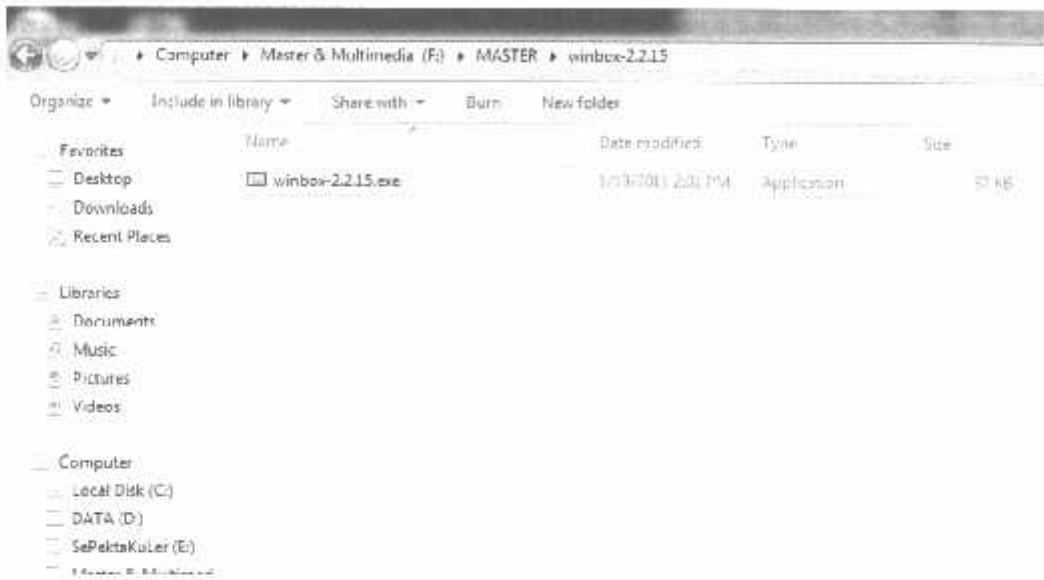
untuk bandwidth controller, bisa dengan sistem simple queue atau pun bisa

```
dengan mangle [admin@becouz] queue simple> add name=Komputer01
```

```
interface=ether2 target-address=172.16.0.1/24 max-limit=65536/131072
```

```
[admin@becouz] queue simple> add name=Komputer02 interface=ether2
```

3.3 Proses Instalasi WinBox



Gambar 3.1 Folder Yang Berisi WinBox.exe

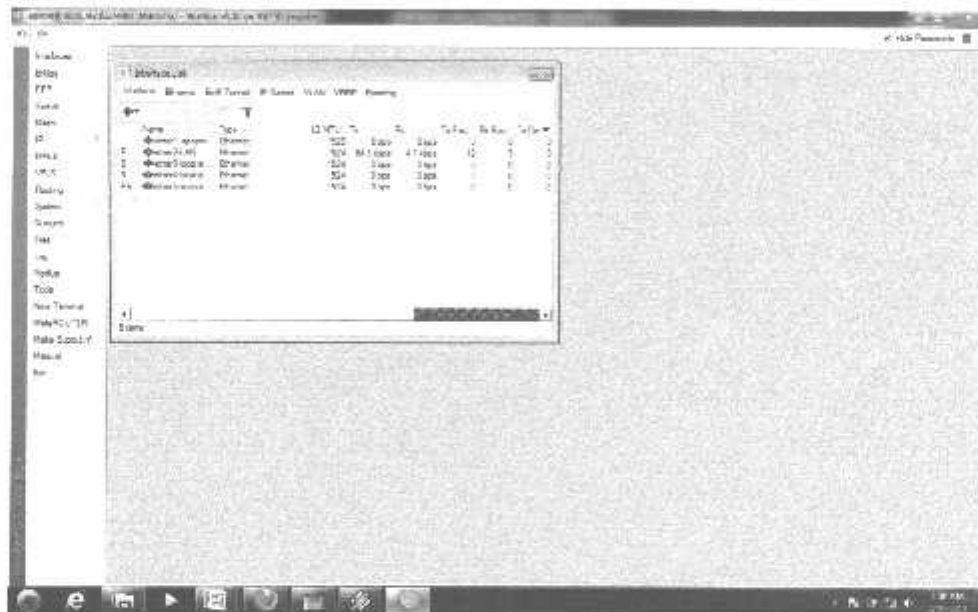
Tentukan *destination folder* atau *folder* yang akan dijadikan tempat menginstal Winbox dan kemudian klik tombol *Install*.



Gambar 3.2 Tampilan login WinBox

Kemudian akan muncul tampilan seperti di gambar 3.2. Apabila kita ingin membuat *shortcut* Winbox di *desktop* atau *start menu*, maka klik kanan pilih opsi *send to – Desktop*

Setelah muncul gambar 3.2 lalu konfigurasi dan aktifkan mikrotik, connect to 192.168.88.1 Default username , login : no password, sehingga muncul gambar seperti dibawah ini,



Gambar 3.3 Tampilan WinBox setelah Login

Instalasi WinBox Selesai, Mikrotik menggunakan WinBox siap di konfigurasi.

3.4 Firewall

Jika anda ingin mengamankan mikrotik router anda dari tangan-tangan jaii, kasus kali ini adalah cara simple mengamankan router anda, Ada beberapa langkah-langkah yang bias anda lakukan sebagai berikut :

3.4.1 Ganti password admin

Hanya mengganti di Password menu dengan winbox, contoh:



Gambar 3.4 Ganti password admin

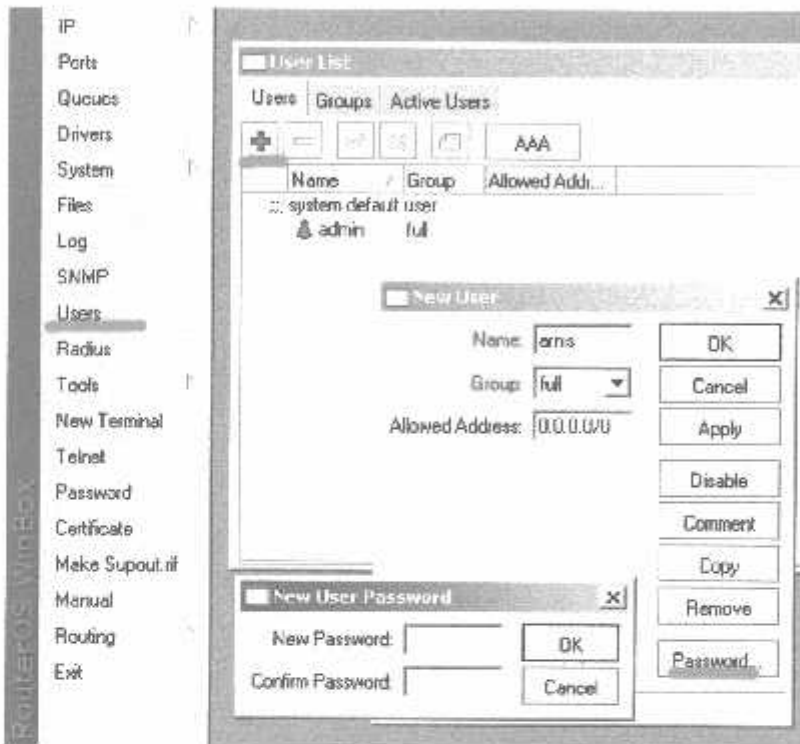
Atau, ketik command berikut di Terminal:

```
[admin@MikroTik] > / password
old password:
new password: *****
retype new password: *****
```

Ini akan mengganti default password admin. Yakinkan anda ingat password itu dan jika anda lupa, tidak ada untuk membalikannya. Anda butuh install ulang router anda.

3.4.2. Tambahkan user pada mikrotik

Anda perlu menambahkan user tersendiri untuk login ke router dengan hak group masing-masing. Tambahkan user anda sendiri sebagai user dengan group full (sama untuk user admin). Contoh :



Gambar 3.5 Form untuk membuat group baru

Anda boleh membuat group baru untuk user dengan izin yang anda berikan.

3.4.3 Set up packet filtering

Semua paket dengan tujuan ke router adalah proses ip firewall filter **input** chain. Catatan, input chain tidak berpengaruh pada paket yang melewati router. Anda bisa mengikuti rules dibawah ini menggunakan chain **input** didalam **/ip firewall filter** (hanya copy paste ke router anda menggunakan Terminal Console atau menggunakan winbox)

Listing :

```
/ ip firewall filter
add chain=input connection-state=established comment="Accept
established connections"
add chain=input connection-state=related comment="Accept related
connections"
add chain=input connection-state=invalid action=drop comment="Drop
invalid connections"
add chain=input protocol=udp action=accept comment="UDP"
disabled=no
add chain=input protocol=icmp limit=50/5s,2 comment="Allow limited
pings"
add chain=input protocol=icmp action=drop comment="Drop excess
pings"
add chain=input protocol=tcp dst-port=22 comment="SSH for secure
shell"
add chain=input protocol=tcp dst-port=8291 comment="winbox"
# Ganti rules dibawah dengan IP anda! #
add chain=input src-address=192.168.0.0/24 comment="Dari jaringan
lokal"
add chain=input src-address=10.0.0.0/8 comment="Dari luar jaringan
lokal"
# akhir yang bisa dirubah #
add chain=input action=log log-prefix="DROP INPUT" comment="Log
everything else"
add chain=input action=drop comment="Drop everything else"
```

Gunakan `/ip firewall filter print input stats` command untuk melihat seberapa banyak paket yang diproses rules tersebut. Gunakan `reset-counters-all` command untuk mereset counter. Periksa system log file `/log print` untuk melihat paket yang telah di drop.

Catatan : jika anda salah mengkonfigurasi firewall dan memblock anda sendiri, anda bisa menggunakan **MAC telnet** dari router yang lain atau komputer dalam 1 jaringan yang terhubung dengan router tersebut untuk memperbaikinya.

Untuk melindungi jaringan client anda, kita harus mengecek semua trafik yang melewati router dan memblock yang tidak dikehendaki. Untuk trafik icmp, tcp, udp kita akan membuat chain, dimana semua paket yang tidak kita kehendaki akan di drop. Awal pertama, kita bisa copy paste command dibawah ini ke router terminal console.

Listing :

```
/ip firewall filter
add chain=forward connection-state=established comment="allow
established connections"
add chain=forward connection-state=related comment="allow related
connections"
add chain=forward connection-state=invalid action-drop
comment="drop invalid connections"
```

Kita tidak inginkan paket yg invalid, maka pada rules ketiga di drop.

| Action | Chain | Src. Address | Src. Port | In. Interface | Out. Address | Out. Port | Out. Interface | Proto. | Bytes | Packets |
|-------------------------------|-------|--------------|-----------|---------------|--------------|-----------|----------------|--------|----------|---------|
| allow established connections | input | | | | | | | | 262 41 4 | 513 |
| allow related connections | input | | | | | | | | 0 0 | 0 |
| drop invalid connections | input | | | | | | | | 0 0 | 0 |
| drop | input | | | | | | | | 0 0 | 0 |

Gambar 3.6 Filterisasi rules

Kita harus me filter dan drop semua paket yang tidak kita kehendaki yang terlihat seperti datang dari aktifitas virus. Kita bisa membuat chain baru untuk semua netbios yg tidak dikehendaki dan trafik yang hampir sama dengan aktifitas virus. Kita bisa memberikan nama untuk chain dengan nama "virus", anda bisa copy paste code dibawah ke terminal, jika anda dalam menu **/ip firewall filter** :

Listing ip firewall :

```
add chain=virus protocol=tcp dst-port=135-139 action=drop
comment="Drop Blaster Worm"
add chain=virus protocol=udp dst-port=135-139 action=drop
comment="Drop Messenger Worm"
add chain=virus protocol=tcp dst-port=445 action=drop
comment="Drop Blaster Worm"
add chain=virus protocol=udp dst-port=445 action=drop
comment="Drop Blaster Worm"
add chain=virus protocol=tcp dst-port=593 action=drop
comment="_____"
```

```
add chain=virus protocol=tcp dst-port=1024-1030 action=drop
comment="_____"

add chain=virus protocol=tcp dst-port=1080 action=drop
comment="Drop MyDoom"

add chain=virus protocol=tcp dst-port=1214 action=drop
comment="_____"

add chain=virus protocol=tcp dst-port=1363 action=drop
comment="ndm requester"

add chain=virus protocol=tcp dst-port=1364 action=drop
comment="ndm server"

add chain=virus protocol=tcp dst-port=1368 action=drop
comment="screen cast"

add chain=virus protocol=tcp dst-port=1373 action=drop
comment="hromgrafx"

add chain=virus protocol=tcp dst-port=1377 action=drop
comment="ciclid"

add chain=virus protocol=tcp dst-port=1433-1434 action=drop
comment="Worm"

add chain=virus protocol=tcp dst-port=2745 action=drop
comment="Bagle Virus"

add chain=virus protocol=tcp dst-port=2283 action=drop
comment="Drop Dumar.Y"

add chain=virus protocol=tcp dst-port=2535 action=drop
comment="Drop Beagle"

add chain=virus protocol=tcp dst-port=2745 action=drop
comment="Drop Beagle.C-K"

add chain=virus protocol=tcp dst-port=3127-3128 action=drop
comment="Drop MyDoom"

add chain=virus protocol=tcp dst-port=3410 action=drop
comment="Drop Backdoor OptixPro"
```

```

add chain=virus protocol=tcp dst-port=4444 action=drop
comment="Worm"

add chain=virus protocol=udp dst-port=4444 action=drop
comment="Worm"

add chain=virus protocol=tcp dst-port=5554 action=drop
comment="Drop Sasser"

add chain=virus protocol=tcp dst-port=8866 action=drop
comment="Drop Beagle.B"

add chain=virus protocol=tcp dst-port=9898 action=drop
comment="Drop Dabber.A-B"

add chain=virus protocol=tcp dst-port=10000 action=drop
comment="Drop Dumar.Y"

add chain=virus protocol=tcp dst-port=10080 action=drop
comment="Drop MyDoom.B"

add chain=virus protocol=tcp dst-port=12345 action=drop
comment="Drop NetBus"

add chain=virus protocol=tcp dst-port=17300 action=drop
comment="Drop Kuang2"

add chain=virus protocol=tcp dst-port=27374 action=drop
comment="Drop SubSeven"

add chain=virus protocol=tcp dst-port=65506 action=drop
comment="Drop PhatBot, Agobot, Gaobot"

```

Kita mendaftarkan semua port dan protocol yang biasanya digunakan beberapa trojan dan virus. Pekerjaan kita belum selesai hanya dengan kode diatas, kita tidak bisa menjalankan rules itu tanpa membuat 1 rules dengan chain forward action=jump. Ini command nya :

```

add chain=forward action=jump jump-target=virus comment="jump to
the virus chain"

```

Urutan chain forward akan terlihat seperti ini :

| Action | Chain | Src. Address | Src. Port | In. Inter. | Dst. Address | Dst. Port | Out. Int. | Proto | Bytes | Packets |
|-------------------------------|---------|--------------|-----------|------------|--------------|-----------|-----------|-------|----------|---------|
| allow established connections | forward | | | | | | | | 13903 KB | 5052 |
| allow related connections | forward | | | | | | | | 1248 B | 12 |
| drop invalid connections | forward | | | | | | | | 0 B | 0 |
| jump to the next chain | forward | | | | | | | | 468 | 1 |

Gambar 3.7 Urutan Chain Forward

Jika paket tidak sama dengan apa yang ada di chain virus, prosesnya akan dikembalikan ke chain forward. Pada point ini kita punya bermacam-macam pilihan, dan anda harus mempelajari ini lebih lanjut dengan membaca manual. Untuk contoh yang saya maksud kita mau mem block semua trafik kecuali beberapa yang boleh kita lewatkan. Contoh kita menginginkan untuk membolehkan trafik HTTP, SMTP, paket TCP, UDP, ICMP(ping)

Kita bisa menambahkan command untuk membolehkan trafik yang kita inginkan dan mendrop semua trafik selain paket yg kita lewatkan.

```
add chain=forward action=accept protocol=tcp dst-port=80
comment="Allow HTTP"
add chain=forward action=accept protocol=tcp dst-port=25
comment="Allow SMTP"
add chain=forward protocol=tcp comment="allow TCP"
add chain=forward protocol=icmp comment="allow ping"
add chain=forward protocol=udp comment="allow udp"
add chain=forward action=drop comment="drop everything else"
```




BAB IV

IMPLEMENTASI DAN PEMBAHASAN

4.1 Sistem Konfigurasi Awal

- a. Mengakses core router (maingw)
- b. Membuat Address List Exception

Ini untuk pengecualian, fungsinya apabila ada request pimpinan atau pejabat yang ingin mengakses facebook pada jam kerja.

Untuk mengakses Address List : IP>FIREWALL>ADDRESS LIST

4.2 Setting Dasar Mikrotik

Langkah awal dari semua langkah konfigurasi mikrotik adalah setting ip. Hal ini bertujuan agar mikrotik bisa di remote dan dengan winbox dan memudahkan kita untuk melakukan berbagai macam konfigurasi. Login sebagai admin dengan default password tidak usah diisi langsung enter. Gantilah dengan ip address anda dan interface yg akan digunakan untuk meremote sementara. Setting mikrotik ada 2 cara yaitu dengan TEXT dan Winbox. Di sini akan saya terangkan seting mikrotik dengan Winbox.

4.3 Langkah setting Mikrotik dengan Winbox

Mari kita mulai dengan asumsi proses install sudah berhasil

1. Setelah install Mikrotik sudah OK, selanjutnya masukkan IP sembarang untuk remote.

Misal :

ip address add address 192.168.1.254 netmask 255.255.255.0 interface ether2

Kemudian buka browser dengan alamat IP tadi, dan download **Winbox**

2. Buka Winbox yang telah di download tadi

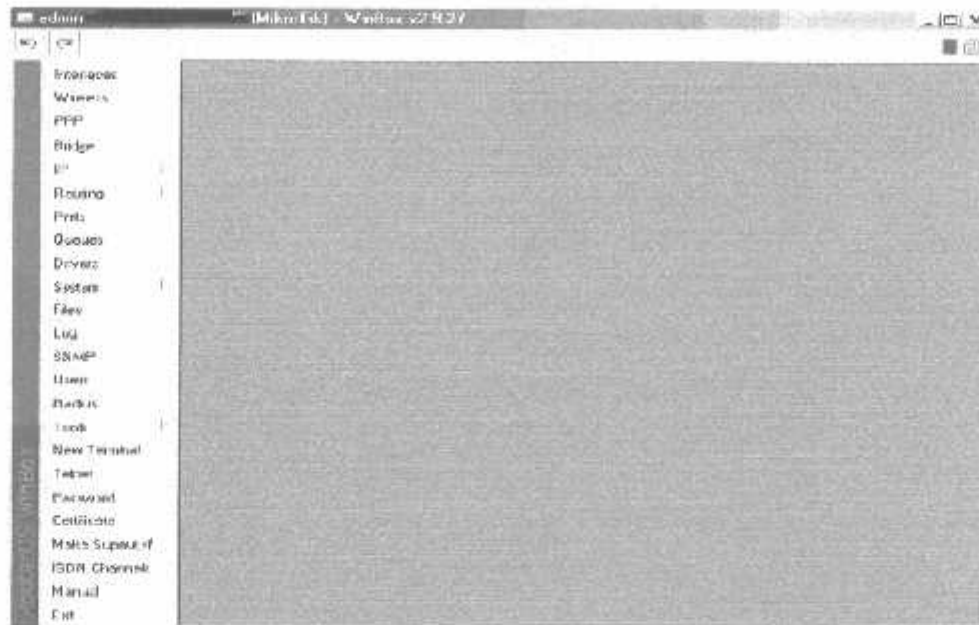


Gambar 4.1 Tampilan login winbox

3. Di tampilan **Winbox**, pada kolom **Connect To** masukkan no IP tadi (192.168.1.254) dengan

Login : **admin** password : **kosong**. Kemudian klik tombol **Connect**

4. Login ke Mikrotik Via Winbox berhasil



Gambar 4.2 Tampilan Winbox setelah login

5. Setting layer 7 untuk facebook.com

IP > FIREWALL > Layer 7 Protocols

Tampilannya akan seperti gambar dibawah ini



Gambar 4.3 Tampilan untuk mensetting layer 7 protokol

6. Kemudian untuk mendaftarkan satu persatu klik tanda plus berwarna merah kemudia akan muncul layar Firewall L7 Protocol kemudian isi Name dan Regexp seperti gambar dibawah ini.



Gambar 4.4 Form Name dan Regexp

7. Setting Mangle

Mangle disini adalah untuk mengelompokan, bahwa setiap akses yang menuju ke *www.facebook.com* akan dimasukan ke *illegal-url-connection*.

Untuk mengakses Mangle : `IP>FIREWALL>MANGLE`

Untuk menambahkan klik tanda + warna merah, kemudian lakukan seperti gambar dibawah ini.



Gambar 4.5 Form Setting Mangle

Kemudian klik Advance dan isi seperti gambar dibawah ini



Gambar 4.6 Form Advance

Kemudian klik Action dan isi seperti gambar dibawah ini :



Gambar 4.7 Form Action

Selanjutnya Klik ok

Kemudian klik tanda + kembali isi seperti gambar dibawah ini



Gambar 4.8 Form Mangle Rule

Kemudian klik tab Action kemudian isi seperti gambar dibawah ini :



Gambar 4.10 Tab Action

Setelah itu klik Ok

Kemudian akan muncul list seperti gambar dibawah ini



Gambar 4.11 Form Mangle List

8. Setting Filter Rule

Setelah pengelompokan menggunakan Mangle, saatnya sekarang pengaturan filter.

Untuk mengakses Filter Rules : `IP>FIREWALL>FILTER RULES`

Kemudian untuk menambahkan aturan klik tanda + disebelah kiri atas, untuk filter rules ada beberapa tahapan, yaitu :

Tahapan Pertama : Mengalihkan setiap koneksi yg mengakses illegal-url-connection

Lakukan step-step dibawah ini :

Klik tab General kemudian isi seperti gambar dibawah ini



Gambar 4.12 Form General

Klik tab Actions, kemudian isi seperti gambar dibawa ini



Gambar 4.13 Form Tab Action

Kemudian klik Ok

Tahapan Kedua : Menyimpan log setiap koneksi yang mengakses illegal-url-connection

Klik + untuk menambahkan rule, kemudian lakukan seperti gambar dibawah ini :



Gambar 4. 14 Form general

Kemudian klik Action kemudian lakukan seperti gambar dibawah ini :



Gambar 4.15 Aktifkan option Log

Setelah itu klik Ok.

Tahapan Ketiga : Melist address illegal-url-connection (disini akan terlihat list ip facebook yg terkena blok)

Klik tanda + untuk menambahkan rules, kemudian lakukan seperti gambar dibawah ini :



Gambar 4.16 Form Add Rules

Kemudian klik Action, lakukan seperti gambar dibawa ini :



Gambar 4.17 Form Tab Action

Klik ok

Tahap Ke Empat : Melakukan drop koneksi yg menuju ke illegal-url-connection

Untuk menambah rule baru klik tanda +, kemudian lakukan seperti gambar dibawah ini :



Gambar 4.18 Form Add Rule

Kemudian klik tab Advanced, kemudian lakukan seperti gambar dibawah ini :



Gambar 4.19 Form Advance List

Pada gambar diatas adalah perintah untuk tidak melakukan drop akses untuk group ip yang masuk ke group exception.

Kemudian klik Action, lakukan seperti gambar dibawah ini :



Gambar 4.20 Form action option

Kemudian klik comment dan isi seperti gambar dibawah ini (ini berfungsi untuk pengaturan waktu di scheduler)



Gambar 4.21 Form Coment for Firewall rule

Kemudian klik Ok.

9. Pengaturan waktu (cron job)

Disini untuk mengatur waktu block atau allow user untuk mengakses situs facebook, pada tulisan sebelumnya dijelaskan waktu untuk mengakses facebook dari pukul 08.00-15.00 Wib, berikut langkah-langkahnya :

Tahap pertama : membuat script untuk mengallow dan memblock

* Script untuk allow

Untuk mengakses script : klik System>Script

Script ini berjalan dengan mendisable filter rules yang memiliki comment facebook, berikut contohnya :



Gambar 4.22 Option Scrip For acces

Klik Ok

*Script untuk memblock

Script ini berjalan dengan meng enable filter rules yang memiliki comment facebook, , berikut contohnya :



Gambar 4.23 Form Script option filter rules

Tahap kedua : mengatur waktu pemblokian dan allow.

Untuk mengakses Scheduler : klik System>Scheduler

*Script untuk allow



Gambar 4.24. Form to scheduler

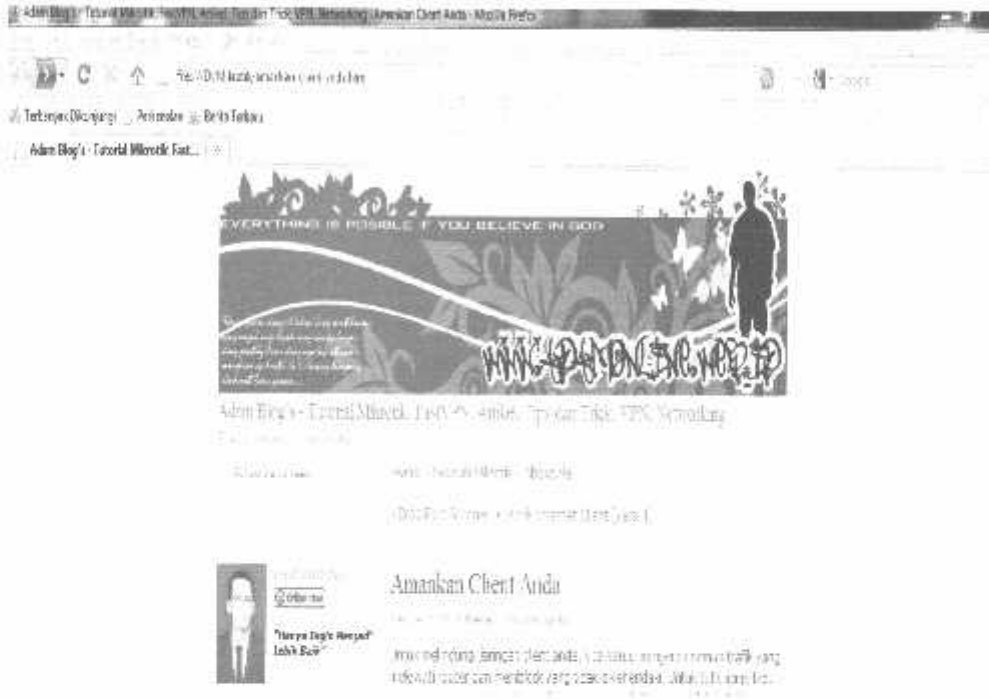
*Script untuk memblock



Gambar 4.25 Form Script blocking

4.4 Pengujian

Sebagai pengujian, kami mencoba membloking situs Adam Blog's, sebelum situs dibloking terlihat seperti gambar 4.27



Gambar. 4.27 Hasil Pengujian Sebelum situs dibloking

Setelah dilakukan pemblokiran, website terlihat seperti gambar 4.28 karena sudah tidak dapat diakses kembali.



Gambar 4.28 Hasil pengujian setelah situs diblocking



BAB V

PENUTUP

5.1 Kesimpulan

Setelah membuat perancangan dan pengujian sistem blocking website, akhirnya penulis dapat membuat kesimpulan sebagai berikut:

1. Blocking website menggunakan mikrotik sangat mudah dalam mengatur sistem dan pengoperasiannya.
 2. Dengan menggunakan layer 7 protokol didalam mikrotik kita tidak perlu memblock sata-persatu IP client, karena semua komputer yang terhubung dalam satu jaringan secara otomatis akan terblocking.
 3. Blocking Website menggunakan 7 layer protocol tidak membutuhkan waktu yang lama.
-

5.2 Saran

Dalam mengakhiri penulisan Tugas Akhir, penulis menguraikan beberapa saran antara lain:

1. Mikrotik routerboard RB750 cocok digunakan diberbagai instansi, kampus atau sekolah. Karena Selain banyak fitur, mikrotik juga terjangkau harganya.
 2. Untuk penggunaan setiap saat, lebih dihimbau untuk diberi pendingin, karena jika ada komponen yang rusak sulit untuk mendapatkan spartpart atau sevicenya
-



DAFTAR PUSTAKA

- (1) Wikipedia, Konsep Sistem Informasi 2009, [URL: http://id.wikipedia.org/wiki/Konsep_Mikrotik](http://id.wikipedia.org/wiki/Konsep_Mikrotik), 23 April 2010.
 - (2) Wikipedia, Basis Data, [URL: http://id.wikipedia.org/wiki/Jarkom](http://id.wikipedia.org/wiki/Jarkom), 25 April 2010.
 - (3) Untung Subagyo, Perancangan Terstruktur, [URL: http://WWW.mansuans.com/Perancangan_jaringan.pdf](http://WWW.mansuans.com/Perancangan_jaringan.pdf), 25 April 2010.
 - (4) Cahaya Suci, Internet dan Intranet, [URL: http://enengnurul.wordpress.com/2009/07/20/Pengertian-internet-dan-intranet](http://enengnurul.wordpress.com/2009/07/20/Pengertian-internet-dan-intranet), 25 April 2010.
 - (5) Amif, Pengertian dan Kelebihan web server, [URL: http://amif.wordpress.com/2008/07/25/pengertian-dan-kelebihan-web-server/](http://amif.wordpress.com/2008/07/25/pengertian-dan-kelebihan-web-server/), 26 April 2010.
 - (6) Kadir Abdul, 2003, "*Blocking situs menggunakan mikrotik*", Andi Offset, Yogyakarta.
 - (7) Peranginangin Kasiman, 2006, "*Aplikasi Win-box*", Andi Offset, Yogyakarta.
 - (8) Imam Hadi, Macromedia Dreamweaver, [URL: http://imanhadi88.blogspot.com/2009/05/pengertianlayer_protokol.html](http://imanhadi88.blogspot.com/2009/05/pengertianlayer_protokol.html), 26 April 2010.
 - (9) Budi Kumala, Macromedia Flash MX, URL: PT Elex Media Komputindo, Kelompok Gramedia Jakarta, 2004.
 - (10) Aninymous, Kamus Komputer dan Teknologi Informasi, <http://www.total.or.id/info.php?kk=Web.html>, 03 Februari 2011.
-



PERKUMPULAN PENGELOLAH PENDIDIKAN UMUM DAN TEKNOLOGI NASIONALA MALANG

INSTITUT TEKNOLOGI NASIONAL MALANG

PROGRAM STUDI TEKNIK LISTRIK D-III

FAKULTAS TEKNOLOGI INDRUSTI

Kampus I : Jl. Bendungan Sigura-gura No.2 Telp. (0341)551431, Fax. (0341)553015 Malang 65145

Kampus II : Jl. Raya Karanglo, Km 2 Telp. (0341)417636, Fax. (0341)417634 Malang 65145

**BERITA ACARA UJIAN TUGAS AKHIR
FAKULTAS TEKNOLOGI INDUSTRI**

Nama Mahasiswa : Kuncoro Cahyo Wicaksono
Nim : 07.52.517
Program Studi : Teknik Listrik D-III
Judul Tugas Akhir : Implementasi Blocking Website menggunakan layer 7
Protokol berbasis Mikrotik RB 750

Dipertahankan di hadapan Tim Penguji Tugas Akhir jenjang Program Diploma
Tiga (D-III)

Pada Hari : Selasa
Tanggal : 22 Februari 2011
Dengan Nilai : 80 (A)

PANITIA UJIAN TUGAS AKHIR

KETUA,



Ir. Taufik Hidayat, MT
NIP. Y. 1018700151

SEKRETARIS

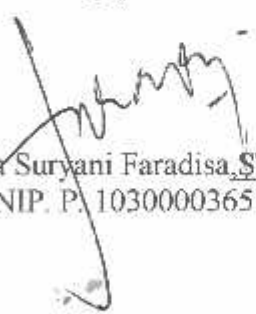

Bambang Prio Hartono, ST, MT
NIP. Y. 1028400082

ANGGOTA PENGUJI

Penguji I


Ir. Taufik Hidayat, MT
NIP. Y. 1018700151

Penguji II


Irmalia Suryani Faradisa, ST, MT
NIP. P. 1030000365

LEMBAR ASISTENSI

Nama : Kuncoro Cahyo Wicaksono
NIM : 0752517
Jurusan : Teknik Listrik D III
Konsentrasi : Teknik Komputer D III
Dosen Pembimbing : Sonny Prasetio ST,MT
Waktu Bimbingan : 01/01/2011 s/d 01/06/2011
Judul : Implementasi blocking website menggunakan layer 7 protokol
Berbasis Mikrotik RB 750

| No | Tanggal | Keterangan | Paraf |
|----|------------|--|-------|
| 1 | 01/01/2011 | BAB I : PENDAHULUAN • Pengaturan huruf dan spasi | Ah |
| 2 | 05/01/2011 | BAB II : TINJAUAN PUSTAKA • Huruf asing dicetak miring • Tambahan sejarah dari mikrotik | Ah |
| 3 | 26/02/2011 | BAB III : PERANCANGAN SISTEM • Perbaikan alur dan perancangan sistem | Ah |
| 4 | 26/02/2011 | BAB IV : IMPLEMENTASI DAN PENGUJIAN • Pengujian sistem dan keterkaitannya dengan alat • Penambahan keterangan instalasi winbox | Ah |
| 5 | 26/02/2011 | BAB V : PENUTUP • Revisi kesimpulan diambil dari hasil pengujian di BAB 4 • Penambahan saran | Ah |

Malang, 26 Februari 2011

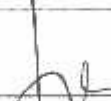
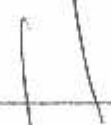
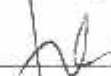


Dosen Penguji I



Ir. H. Taufik Hidayat, MT
NIP. Y. 101870051

LEMBAR ASISTENSI

Nama : Kuncoro Cahyo Wicaksono
NIM : 075251
Jurusan : Teknik Listrik D III
Konsentrasi : Teknik Komputer D III
Dosen Pembimbing : Sonny Prasetio, ST,MT
Waktu Bimbingan : 01/01/2011 s/d 01/06/2011
Judul : Implementasi Blocking Website Menggunakan layer 7 protokol
Berbasis Mikrotik RB 750

| No | Tanggal | Keterangan | Paraf |
|----|------------|---|---|
| 1 | 01/01/2011 | BAB I : PENDAHULUAN • Pengaturan huruf dan spasi |  |
| 2 | 05/01/2011 | BAB II : TINJAUAN PUSTAKA • Huruf asing dicetak miring • Tambahan Dasar Teori |  |
| 3 | 26/02/2011 | BAB III : PERANCANGAN SISTEM • Penambahan keterangan mengenai mikrotik |  |
| 4 | 26/02/2011 | BAB IV : IMPLEMENTASI DAN PENGUJIAN • Diuji sistem dan keterkaitannya dengan alat • Penambahan keterangan instalasi Win Box |  |
| 5 | 26/02/2011 | BAB V : PENUTUP • Kesimpulan diambil dari hasil pengujian di BAB 4 • Penambahan saran |  |

Malang, 26 Februari 2011

Dosen Penguji I


Irmalia Suryani Faradisa, ST.MT
NIP. P. 1030000365

LAMPIRAN

Listing program

1. Listing :
 2. / ip firewall filter
 3. add chain=input connection-state=established
comment="Accept established connections"
 4. add chain=input connection-state-related comment="Accept
related connections"
 5. add chain=input connection-state=invalid action=drop
comment="Drop invalid connections"
 6. add chain=input protocol=udp action=accept comment="UDP"
disabled=no
 7. add chain=input protocol=icmp limit=30/5s,2 comment="Allow
limited pings"
 8. add chain=input protocol=icmp action=drop comment="Drop
excess pings"
 9. add chain=input protocol=tcp dst-port=22 comment="SSH for
secure shell"
 10. add chain=input protocol=tcp dst-port=8291
comment="winbox"
 11. # Ganti rules dibawah dengan IP anda: #
 12. add chain=input src-address=192.168.0.0/24 comment="Dari
jaringan lokal"
 13. add chain=input src-address=10.0.0.0/8 comment="Dari luar
jaringan lokal"
 14. # akhir yang bisa dirubah #
 15. add chain=input action=log log-prefix="DROP INPUT"
comment="Log everything else"
 16. add chain=input action=drop comment="Drop everything else"
-

LAMPIRAN

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Jurusan D3 Listrik</title>
<link type="text/css" href="menu.css" rel="stylesheet" />
<script type="text/javascript" src="jquery.js"></script>
<script type="text/javascript" src="menu.js"></script>
<script language="JavaScript" type="text/JavaScript">
    <link type="text/css" href="menus.css" rel="stylesheet" />
    <script type="text/javascript" src="jquery.js"></script>
<script type="text/javascript" src="menus.js"></script>
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth;                document.MM_pgH=innerHeight;
onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();
}
MM_reloadPage(true);
-->
<style type="text/css">
<!--
#Layer7 {
    position: absolute;
    left: 7px;
    top: 496px;
    width: 241px;
    height: 536px;
    z-index: 107;
}
#Layer8 {
    position: absolute;
    left: 11px;
    top: 363px;
    width: 234px;
    height: 55px;
    z-index: 107;
    background-color: #0033CC;
}
#Layer9 {
    position: absolute;
    left: 10px;
    top: 418px;
    width: 242px;
    height: 59px;
    z-index: 108;
}
#Layer10 {
    position: absolute;
    left: 10px;
    top: 473px;
    width: 244px;
    height: 59px;
    z-index: 109;
    background-color: #0000FF;
}
}

```
