



**MANAJEMEN PROXY MENGGUNAKAN MIKROTIK DENGAN
METODE LAYER 7 PROTOCOL DAN MANGLE**



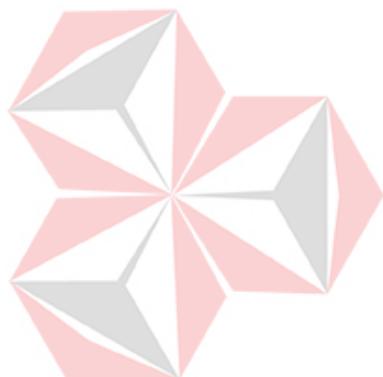
Oleh:
Adha Maulida Azmi
14410200056

FAKULTAS TEKNOLOGI DAN INFORMATIKA
UNIVERSITAS DINAMIKA
2022

**MANAJEMEN PROXY MENGGUNAKAN MIKROTIK DENGAN
METODE LAYER 7 PROTOCOL DAN MANGLE**

LAPORAN KERJA PRAKTIK

**Diajukan sebagai salah satu syarat untuk menyelesaikan
Program Sarjana Teknik**



**UNIVERSITAS
Dinamika**

Oleh:

**Nama : Adha Maulida Azmi
NIM : 14410200056
Program Studi : S1 Teknik Komputer**

**FAKULTAS TEKNOLOGI DAN INFORMATIKA
UNIVERSITAS DINAMIKA
2022**

LEMBAR PENGESAHAN

Manajemen Proxy Menggunakan Mikrotik Dengan Metode Layer 7 Protocol Dan Mangle

Laporan Kerja Praktik Oleh :

Adha Maulida Azmi

NIM : 14410200056

Telah diperiksa, diuji dan disetujui



Pembimbing,

Yosefine Triwidayastuti, M.T
NIDN. 0729038504

Disetujui :

Kediri, 2 Agustus 2022

Penyelia,

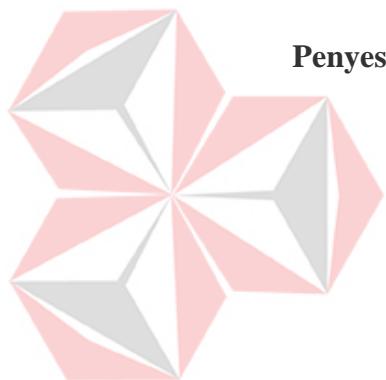


LULUK ZULAIKA, M.Pd.

Mengetahui,
Ketua Program S1 Teknik Komputer

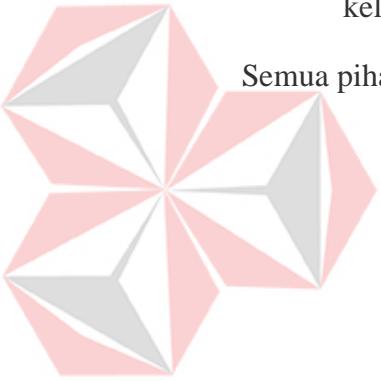


Pauladie Susanto., M.T.
NIDN. 0729047501



Penyesalan selalu datang terlambat, jangan sampai itu terjadi.

UNIVERSITAS
Dinamika



Kupersembahkan kepada
keluarga tercinta yang selalu memberi dukungan dan doa.

Semua pihak yang secara langsung dan tidak langsung membantu penulis
menyelesaikan Tugas Akhir ini.

UNIVERSITAS
Dinamika

PERNYATAAN
PERSETUJUAN PUBLIKASI DAN KEASLIAN KARYA ILMIAH

Sebagai mahasiswa **Universitas Dinamika**, Saya :

Nama : Adha Maulida Azmi
NIM : 14410200056
Program Studi : S1 Teknik Komputer
Fakultas : Fakultas Teknologi dan Informatika
Jenis Karya : Laporan Kerja Praktik
Judul Karya : **MANAJEMEN PROXY MENGGUNAKAN MIKROTIK DENGAN METODE LAYER 7 PROTOCOL DAN MANGLE**

Menyatakan dengan sesungguhnya bahwa :

1. Demi pengembangan Ilmu Pengetahuan, Teknologi dan Seni, Saya menyetujui memberikan kepada Universitas Dinamika Hak Bebas Royalti Non-Eksklusif (*Non-Exclusive Royalty Free Right*) atas seluruh isi/sebagian karya ilmiah Saya tersebut diatas untuk disimpan, dialihmediakan, dan dikelola dalam bentuk pangkalan data (*database*) untuk selanjutnya didistribusikan atau dipublikasikan demi kepentingan akademis dengan tetap mencantumkan nama Saya sebagai penulis atau pencipta dan sebagai pemilik Hak Cipta.
2. Karya tersebut diatas adalah hasil karya asli Saya, bukan plagiat baik sebagian maupun keseluruhan. Kutipan, karya, atau pendapat orang lain yang ada dalam karya ilmiah ini semata-mata hanya sebagai rujukan yang dicantumkan dalam Daftar Pustaka Saya.
3. Apabila dikemudian hari ditemukan dan terbukti terdapat tindakan plagiasi pada karya ilmiah ini, maka Saya bersedia untuk menerima pencabutan terhadap gelar kesarjanaan yang telah diberikan kepada Saya.

Demikian surat pernyataan ini Saya buat dengan benar-benarnya.

Kediri, 2 Agustus 2022



Adha Maulida Azmi
NIM : 14410200056

ABSTRAK

Internet merupakan hal yang tidak bisa dipisahkan dengan manusia dalam kehidupan sehari-hari, berkat perkembangan teknologi dan kebebasan berekspresi yang semakin bebas serta internet yang menyajikan banyak sekali fitur yang bisa dinikmati siapa saja. Dengan segala kelebihan dan kemudahannya tentu saja internet memiliki sisi negatifnya sendiri, banyak konten-konten negatif yang dapat diakses oleh siapa saja adalah salah satunya. Penulis tertarik untuk membuat sebuah *Proxy Server* yang bisa memblokir web-web negatif dengan menggunakan metode *7 layer protocol* dan *Mangle* berbasis mikrotik. Sistem yang penulis buat berhasil melakukan blokir pada web-web yang diinginkan dengan akurasi 100% dari ketikan web melalui *url* dan bukan dari *search engine*.

Kata Kunci: *Proxy, internet, mikrotik, Mangle, Layer 7 protocol.*



KATA PENGANTAR

Segala puji dan syukur kehadirat Tuhan Yang Maha Esa karena atas rahmat, karunia serta izin-Nya, penulis dapat menyelesaikan laporan kerja praktik yang berjudul **“Manajemen Proxy Menggunakan Mikrotik Dengan Metode Layer 7 Protocol dan Mangle”**. Laporan ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana Teknik pada Program studi S1 Teknik Komputer Universitas Dinamika.

Dalam penyusunan dan penyelesaian laporan kerja praktik ini, penulis mendapatkan bimbingan dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih sebesar-besarnya kepada:

1. Orang tua dan keluarga yang selalu memberikan semangat, fasilitas dan motivasi yang tak henti-hentinya sehingga penulis dapat menyelesaikan Tugas Akhir ini.
2. Yosefine Triwidayastuti, M.T. selaku Dosen Pembimbing kerja praktik yang memberikan penulis kesempatan kedua dan bantuan-bantuan untuk dapat menyelesaikan laporan kerja praktik ini.
3. Bapak Pauladie Susanto, S.Kom., M.T., selaku Ketua Program Studi S1 Teknik Komputer yang telah memberi penulis kesempatan untuk menyelesaikan laporan kerja praktik ini.
4. Semua Staf Dosen S1 Teknik Komputer yang telah memberikan ilmu yang sangat berharga yang telah membantu penulis sampai di titik ini dan dapat menyelesaikan laporan kerja praktik ini dengan kemampuan dan ilmu yang telah diterima.
5. Semua sedulur S1 Teknik Komputer yang menemani dan membantu saya selama proses belajar sehingga penulis tetap bisa melangkah maju menjadi pribadi yang lebih baik.
6. Serta semua pihak yang secara langsung dan tidak langsung membantu penulis dalam setiap kesempatan.

Semoga Tuhan Yang Maha Esa senantiasa memberikan rahmat-Nya kepada seluruh pihak yang telah membantu penulis menyelesaikan laporan kerja praktik ini. Penulis menyadari bahwa laporan yang penulis susun masih jauh dari kata

sempurna sehingga penulis terbuka untuk kritikan dan saran yang bisa membantu penulis menyempurnakan laporan yang penulis susun.

Surabaya, 19 Juli 2022

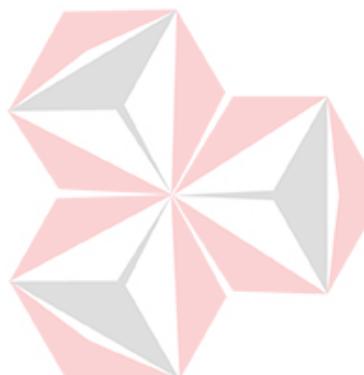
Penulis



DAFTAR ISI

	Halaman
ABSTRAK	vii
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR GAMBAR	xii
DAFTAR TABEL.....	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	1
1.3 Batasan Masalah.....	1
1.4 Tujuan.....	2
BAB II GAMBARAN UMUM PERUSAHAAN	3
2.1 Sejarah Singkat SMK Hidayatus Sholihin	3
2.2 Visi dan Misi SMK Hidayatus Sholihin.....	3
2.2.1 Visi	3
2.2.2 Misi.....	3
2.3 Lokasi SMK Hidayatus Sholihin.....	4
BAB III LANDASAN TEORI.....	6
3.1 <i>Firewall</i>	6
3.2 <i>Layer 7 Protocol</i>	6
3.3 <i>Mangle</i>	6
3.4 <i>Proxy Server</i>	6
3.5 Mikrotik <i>RouterOS</i>	7
3.6 Winbox.....	8
BAB IV DESKRIPSI KERJA PRAKTIK	16
4.1 Analisa Kebutuhan.....	9
4.1.1 Kebutuhan <i>Hardware</i>	9
4.1.2 Kebutuhan <i>Software</i>	9

4.2 <i>Flowchart</i> Cara Kerja.....	10
4.3 Perancangan	11
4.3.1 Topologi Jaringan	11
4.3.2 Instalasi Winbox	11
4.3.3 Konfigurasi Mikrotik	12
4.4 Pengujian	17
BAB V. PENUTUP.....	20
5.1 Kesimpulan.....	20
5.2 Saran.....	20
DAFTAR PUSTAKA	21
LAMPIRAN	22
BIODATA PENULIS	28



UNIVERSITAS
Dinamika

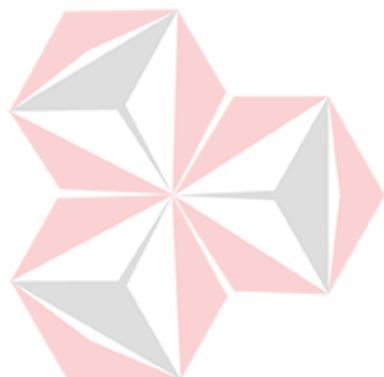
DAFTAR GAMBAR

	Halaman
Gambar 2.1 Lokasi SMK Hidayatus Sholihin	4
Gambar 2.2 Struktur organisasi SMK Hidayatus Sholihin	5
Gambar 3.1 Alur kerja proxy server	7
Gambar 3.2 Tampilan awal winbox	8
Gambar 4.2 <i>Flowchart</i> cara kerja.....	10
Gambar 4.3 Topologi jaringan	11
Gambar 4.4 Main menu winbox mikrotik.....	11
Gambar 4.5 Interface list.....	12
Gambar 4.6 DHCP client	13
Gambar 4.7 DHCP client terkoneksi.....	13
Gambar 4.8 Address list.....	14
Gambar 4.9 DHCP server	14
Gambar 4.10 NAT.....	15
Gambar 4.11 Hotspot	15
Gambar 4.12 <i>Firewall</i> 71 protocol.....	16
Gambar 4.13 <i>Filter rules</i> 71 protocol	16
Gambar 4.14 Mangle.....	16
Gambar 4.15 <i>Filter rules</i> mangle	17
Gambar 4.16 Uji coba facebook.com web	17
Gambar 4.17 Uji coba youtube.com web.....	18
Gambar 4.18 Uji coba facebook.com <i>search engine</i>	18
Gambar 4.19 Uji coba facebook.com <i>search engine</i>	19

DAFTAR TABEL

Halaman

Tabel 4.1..... 19



UNIVERSITAS
Dinamika

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dengan berkembangnya teknologi, internet menjadi kebutuhan yang penting dalam kegiatan sehari-hari mulai dari bersekolah, belanja, menonton berita dan lain sebagainya. Dengan internet kita dapat melakukan apapun yang kita mau dan berekspresi sesuka hati berkat banyaknya fitur yang disediakan oleh internet. Dengan segala kebebasanya tentu saja selain bermanfaat internet juga mempunyai dampak negatif, banyak konten-konten yang bersifat merusak dapat diakses oleh siapa saja.

Dengan adanya kebebasan dalam mengakses konten-konten negatif tersebut dibutuhkan *rule* untuk memblokir ataupun memfilter internet agar berkurang konten-konten negatif yang ada di internet. Walaupun tidak dapat dihilangkan sepenuhnya setidaknya internet dapat menjadi tempat yang lebih baik tanpa konten-konten negatif tersebut. Adapun upaya yang dapat dilakukan untuk mengurangi konten-konten negatif di internet yaitu dengan menggunakan *firewall*.

Perdasarkan permasalahan tersebut, penulis memiliki ide untuk membuat sebuah *proxy server* dengan menggunakan mikrotik dengan metode *layer 7 protocol* dan *mangle* pada jaringan internet SMK Hidayatus Sholihin. Dengan harapan murid-murid yang menggunakan jaringan SMK Hidayatus Sholihin dapat terhindar dari konten-konten negatif yang ada di internet.

1.2 Rumusan Masalah

Rumusan masalah dari permasalahan diatas adalah sebagai berikut:

Bagaimana cara merancang dan membangun *Proxy Server* pada jaringan SMK Hidayatus Sholihin dengan menggunakan mikrotik?

1.3 Batasan Masalah

Batasan masalah dalam Tugas Akhir ini adalah sebagai berikut:

1. Menggunakan router dengan sistem operasi mikrotik
2. Menggunakan 1 jalur internet milik SMK Hidayatus Shoolihin

1.4 Tujuan

Mengkonfigurasi Proxy Server pada mikrotik dengan menggunakan metode *layer 7 protocol* dan *mangle* pada jaringan di SMK Hidayatus Sholihin.



BAB II

GAMBARAN UMUM PERUSAHAAN

2.1 Sejarah Singkat SMK Hidayatus Sholihin

SMK Hidayatus Sholihin Turus kab. Kediri merupakan SMK swasta yang berdiri pada tahun 2008, merupakan Lembaga Pendidikan Kejuruan setara SMK berbasis pesantren dibawah yayasan Hidayatus Sholihin Kediri. SMK Hidayatus Sholihin beralamat di Jalan Raya No. 228, Turus, Gurah, Turus, Kediri. memakai kurikulum pendidikan nasional dan kurikulum pesantren.

Dengan 4 program keahlian unggulan yaitu : Teknik Kendaraan Ringan, Teknik Sepeda Motor, Teknik Komputer Jaringan dan Busana Butik. Lulusan SMK Hidayatus Sholihin selain diharapkan mempunyai skill dan keterampilan yang dapat berguna di masyarakat serta memiliki pemahaman agama yang mumpuni untuk berguna bagi nusa dan bangsa di dunia dan di akhirat.

2.2 Visi dan Misi SMK Hidayatus Sholihin

2.2.1 Visi

Terciptanya sumber daya manusia yang beriman dan bertaqwa kepada ALLAH subhanahu wa ta'ala, berakhhlakul karimah dan menjadi insane yang berilmu, beramal serta memiliki keterampilan dan pengetahuan teknologi.

2.2.2 Misi

1. Memberikan pengetahuan dan pendidikan dasar-dasar agama islam ala ahlussunah wal jama'ah dan akhlak budi pekerti yang luhur.
2. Mengajarkan serta mengenalkan siswa untuk lebih mendekat pada nilai-nilai budaya agama islam dan kehidupan masyarakat.
3. Memberikan pelatihan dan keterampilan (*life skill*) yang disesuaikan dengan ilmu pengetahuan dan teknologi.
4. Memberikan bimbingan dan pengetahuan kerja di lingkungan sekolah maupun dunia industry serta melanjutkan studi ke jenjang yang lebih tinggi.

2.3 Lokasi SMK Hidayatus Sholihin

Lokasi SMK Hidayatus Sholihin yaitu di Jalan Raya No.228, Turus, Kec. Gurah, Kediri, Jawa Timur. Berikut adalah peta dari lokasi SMK Hidayatus Sholihin.

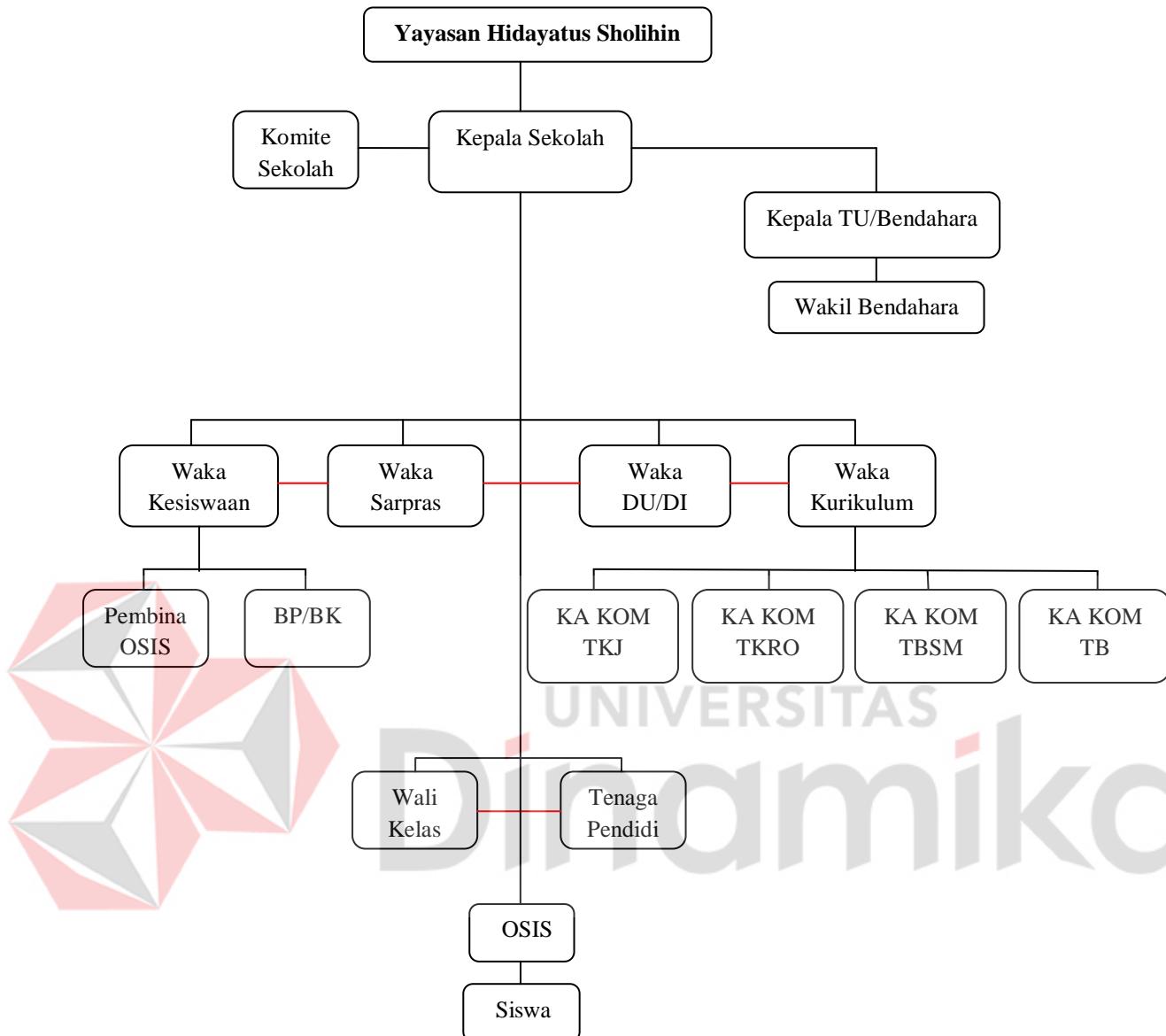


Gambar 2.1 Lokasi SMK Hidayatus Sholihin



UNIVERSITAS
Dinamika

2.4 Struktur Organisasi SMK Hidayatus Sholihin



Gambar 2.2 Stuktur organisasi SMK Hidayatus Sholihin

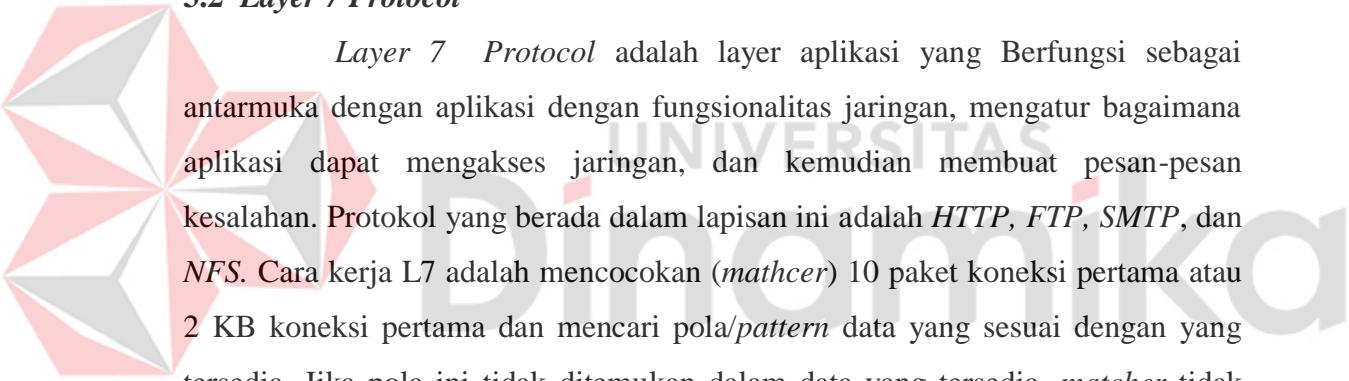
BAB III

LANDASAN TEORI

3.1 *Firewall*

Firewall adalah sistem keamanan pada jaringan komputer yang bertugas untuk melindungi komputer dari serangan *virus*, *malware*, dan jenis serangan lainnya yang dapat berpotensi membahayakan. Firewall sendiri memiliki tugas utama untuk memantau dan mengontrol seluruh akses yang masuk dan keluar lewat koneksi jaringan sesuai dengan aturan yang sudah ditetapkan. Selain itu, ia juga memiliki peranan untuk menjaga keamanan jaringan internet yang terhubung. Akan tetapi, banyak pengguna yang belum menyadari adanya sistem ini dan mengabaikannya.

3.2 *Layer 7 Protocol*



Layer 7 Protocol adalah layer aplikasi yang Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam lapisan ini adalah *HTTP*, *FTP*, *SMTP*, dan *NFS*. Cara kerja L7 adalah mencocokan (*mathcer*) 10 paket koneksi pertama atau 2 KB koneksi pertama dan mencari pola/*pattern* data yang sesuai dengan yang tersedia. Jika pola ini tidak ditemukan dalam data yang tersedia, *matcher* tidak memeriksa lebih lanjut. Dan akan dianggap *unknown connections*. Anda harus mempertimbangkan bahwa banyak koneksi secara signifikan akan meningkatkan penggunaan memori pada RB maupun PC *Router* anda. Untuk menghindari itu tambahkan regular *firewall matchers* (*pattern*) untuk mengurangi jumlah data yang dikirimkan ke layer-7 filter.

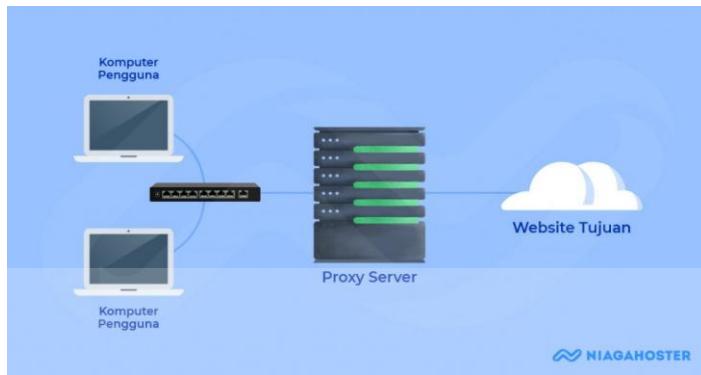
3.3 *Mangle*

Mangle pada *Firewall* mikrotik dapat digunakan untuk manandai packet data. Tanda (marking) tersebut bisa digunakan pada fitur lain seperti Filter, Routing, NAT, ataupun Queue. Pada implementasi di lapangan mangle bisa digunakan untuk melakukan managemen proxy, Router yang melakukan

managemen proxy biasanya merupakan router Utama yang juga digunakan untuk melakukan *management bandwidth*.

3.4 *Proxy Server*

Proxy server adalah perangkat komputer atau *software* yang bekerja sebagai *proxy*, yaitu menjadi perantara bagi Anda dan server tujuan. Jadi, ketika mengakses internet, Anda tidak langsung terhubung ke website tujuan karena akan melalui server terlebih dahulu. Misalnya, ketika mengakses sebuah website.



Gambar 3.1 Alur kerja *proxy server*

(Sumber : <https://www.niagahoster.co.id/blog/proxy-server/>)

Dengan adanya *proxy*, Anda juga bisa melakukan aktivitas internet yang lebih aman. Alasannya, informasi asli Anda bisa disamarkan dengan bantuan proxy tersebut. Jadi, tidak mudah dicuri oleh hacker. Tak hanya itu, *proxy server* juga cukup efektif digunakan sebagai sebuah gateway. Nantinya, semua koneksi yang dilakukan akan sesuai dengan setting gateway yang ditetapkan. Dengan begitu, tidak mudah disusupi serangan dari luar yang tidak diinginkan.

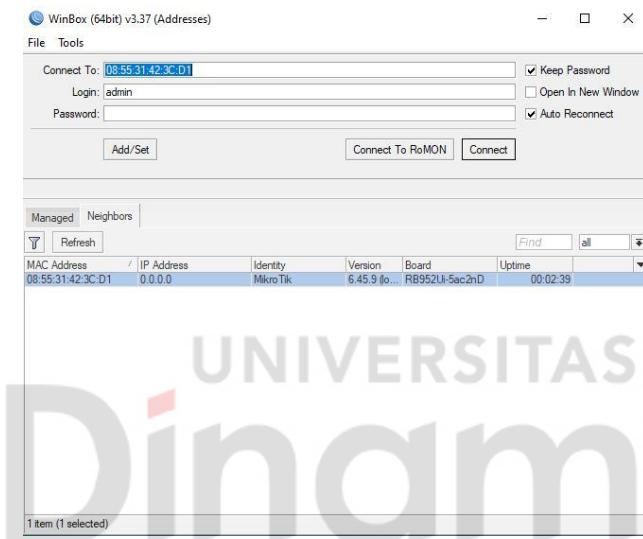
3.5 *Mikrotik RouterOS*

Mikrotik adalah sistem operasi yang berbasis perangkat lunak (*software*) yang dipergunakan untuk menjadikan komputer sebagai router sebuah jaringan. Mikrotik juga menggunakan sistem operasi berbasis Linux dan menjadi dasar network router. Sistem operasi (*OS*) ini sangat cocok untuk membangun administrasi jaringan komputer yang berskala kecil hingga besar.

Router OS yang biasa ada pada Mikrotik merupakan sebuah Sistem Operasi yang memiliki basis Unix atau Linux yang mampu membuat suatu komputer dapat berfungsi layaknya seperti Router, Firewall, Bridge, HotSpot, proxy Server, dan Bandwidth Management.

3.6 Winbox

Winbox adalah *utility* mikrotik berbasis *GUI (Graphical User Interface)* berbasis windows untuk mengakses dan mengatur konfigurasi Mikrotik *RouterOS*.



Gambar 3.2 Tampilan awal winbox

BAB IV

DESKRIPSI KERJA PRAKTIK

4.1 Analisa Kebutuhan

Analisa kebutuhan ini dilakukan untuk mengetahui perangkat apa saja yang dibutuhkan untuk bisa merancang *proxy sever*.

4.1.1 Kebutuhan *Hardware*

Adapun kebutuhan perangkat keras (*hardware*) dalam penggerjaan *project* ini sebagai berikut :

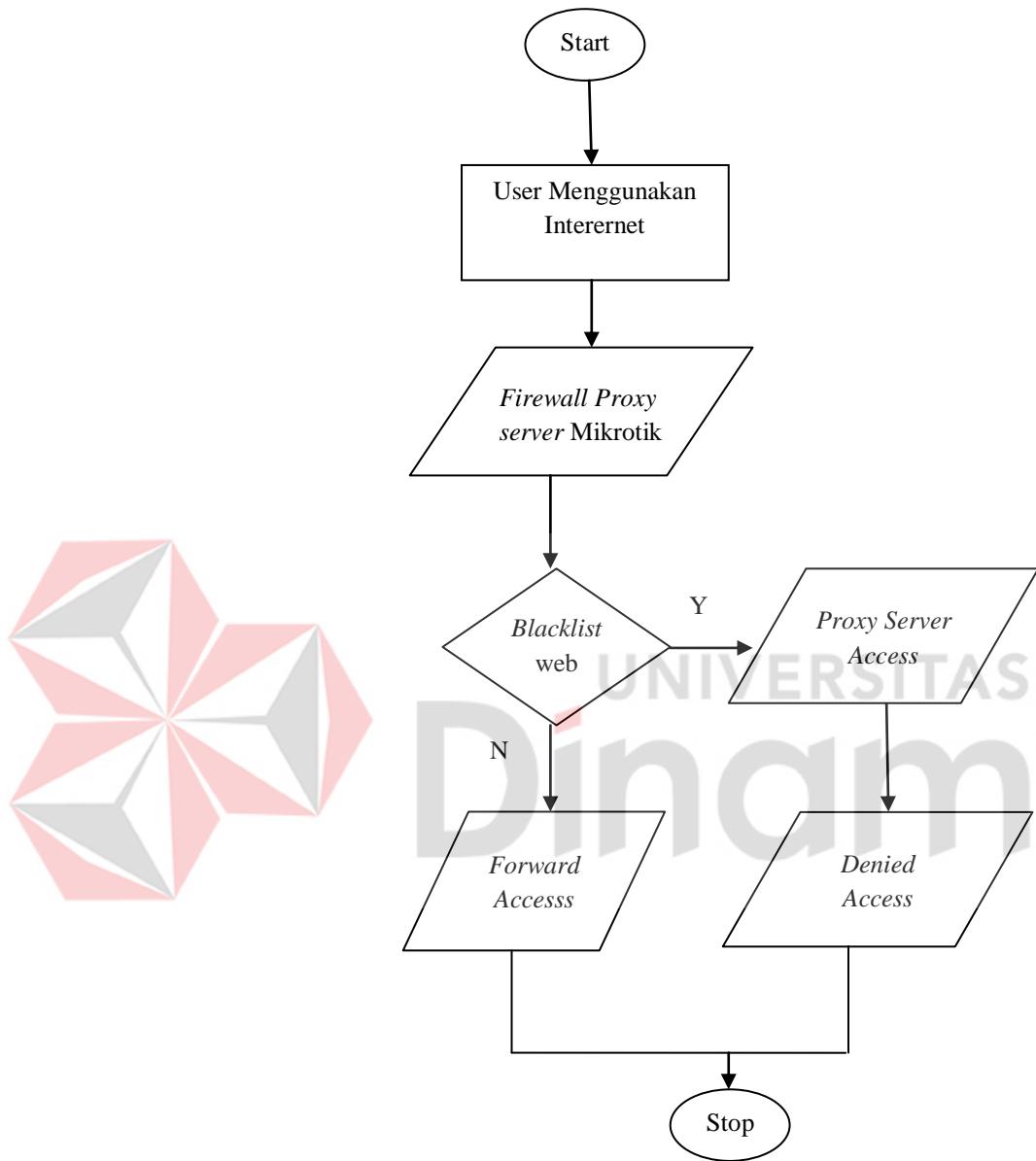
1. Laptop / PC
2. Mikrotik
3. Kabel UTP
4. *Access Point*

4.1.2 Kebutuhan *Software*

Adapun kebutuhan perangkat lunak (*Software*) dalam penggerjaan *project* ini sebagai berikut :

1. Sistem operasi Windows
2. Winbox

4.2 Flowchart Cara Kerja

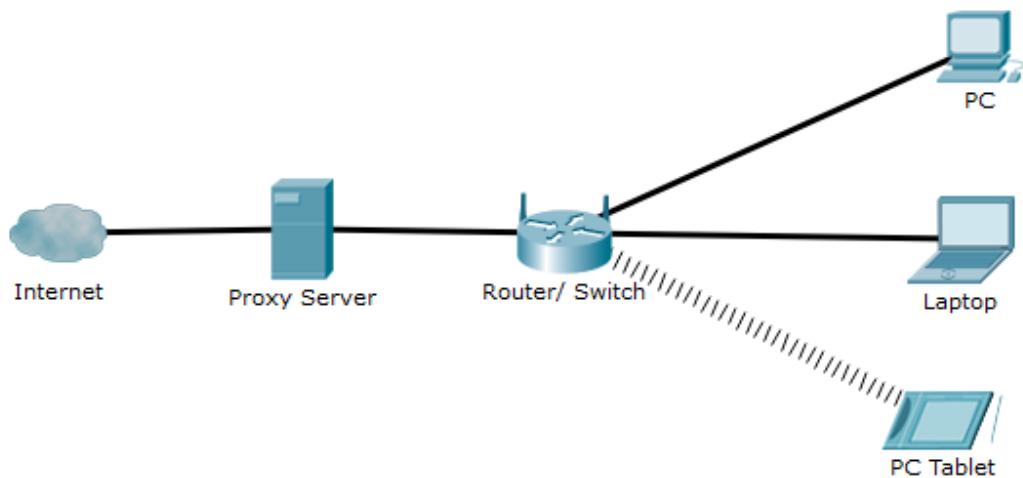


Gambar 4.2 *Flowchart* cara kerja

Dapat dilihat pada Gambar 4.2 ketika *user* menggunakan internet, *firewall proxy server* akan melakukan pengecekan. Apakah *user* mengakses web yang ada dalam *list blacklist*, jika tidak maka *request user* akan *deforward* ke web yang dituju dan jika *user* mengakses web yang ada dalam *list blacklist* maka akses ditolak dan internet akan diputus.

4.3 Perancangan

4.3.1 Topologi Jaringan



Gambar 4.3 Topologi jaringan

Dapat dilihat pada Gambar 4.3 dimana semua perangkat yang terhubung dalam jaringan akan melewati *proxy server* terlebih dahulu. Karena *client* atau *user* mendapatkan ip dari server maka semua akses *user* akan dapat dipantau dan diatur oleh *server* dengan harapan untuk meminimalisir akses konten-konten negatif.

4.3.2 Instalasi winbox

Instalasi winbox adalah langkah awal sebelum melakukan konfigurasi *proxy server*.



Gambar 4.4 *Main menu* winbox mikrotik

4.3.3 Konfigurasi Mikrotik

Berikut adalah langkah-langkah konfigurasi mikrotik untuk menjadi *proxy server*.

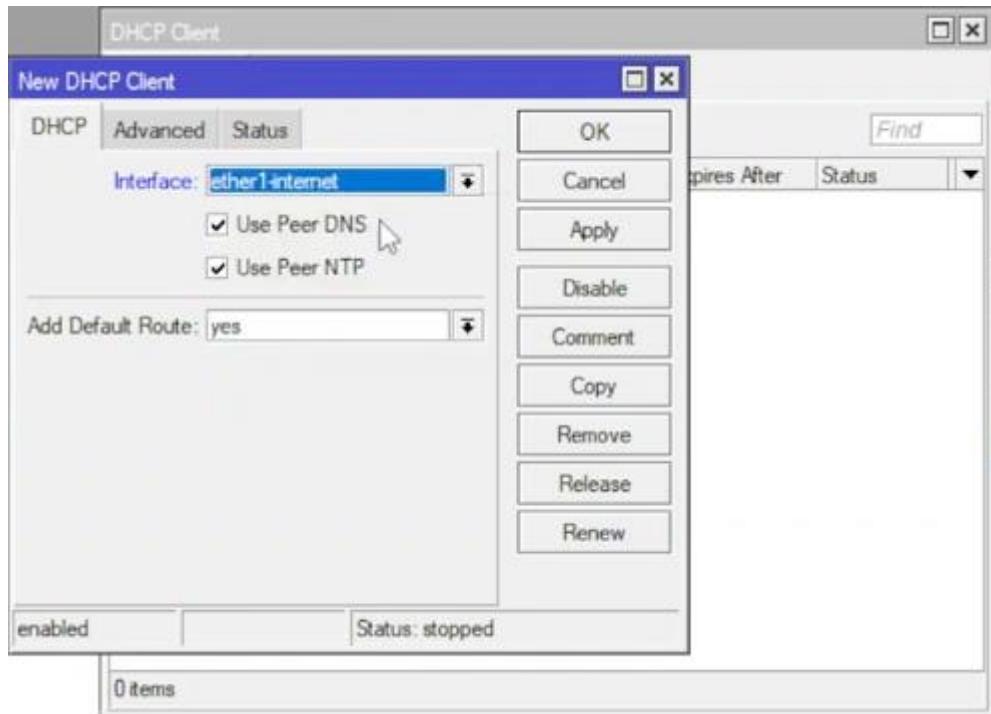


UNIVERSITAS
Dinamika

Interface List						
Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN
					Detect Internet	
Name	Type	Actual MTU	L2 MTU	Tx	Rx	
R ether1-internet	Ethernet	1500	1598	0 bps	0	
R ether2-PC	Ethernet	1500	1598	67.7 kbps	4.5 k	
R ether3	Ethernet	1500	1598	0 bps	0	
R ether4	Ethernet	1500	1598	0 bps	0	
R pwr-line1	PWR	1500	1598	0 bps	0	
wlan1-WiFi	Wireless (Atheros AR9)	1500	1600	0 bps	0	

Gambar 4.5 Interface list

Pada Gambar 4.5 terlihat *ethernet* yang di gunakan hanya 2 port, yaitu *ethernet* 1 yang disambungkan ke internet yang diberi nama ether1-internet dan *ethernet* 2 yang terhubung ke pc yang diberi nama ether2-PC dan pengaktifan Wlan1 yang diberi nama wlan1-Wifi.



Gambar 4.6 *DHCP client*

Langkah selanjutnya adalah mensetting *DHCP Client* yang ada pada menu IP > DHCP Client > Add > set *Interface* ke port Ethernet yang terhubung ke internet, yaitu ethernet 1 seperti pada Gambar 4.6 > Apply > Ok. Jika langkah sudah benar maka mikrotik sudah terhubung ke internet dan sudah mendapat *IP* secara otomatis dari *ISP* seperti pada gambar 4.7.



Gambar 4.7 *DHCP client terkoneksi*

Selanjutnya adalah memberikan *IP* untuk *ether2* yang terhubung ke *pc* dan *wlan1* yang untuk *wifi* seperti gambar 4.8 dengan melalui menu *IP > Addresses > Add* > lalu isikan *IP* yang diinginkan dan ubah *Interface* ke *port ethernet* yang diinginkan, beri ip masing-masing untuk setiap port.



Address List			
	Address	Network	Interface
1	172.16.1.1/24	172.16.1.0	wlan1-WiFi
D	192.168.0.119...	192.168.0.0	ether1-internet
	192.168.10.1/...	192.168.10.0	ether2-PC

Gambar 4.8 *Address list*

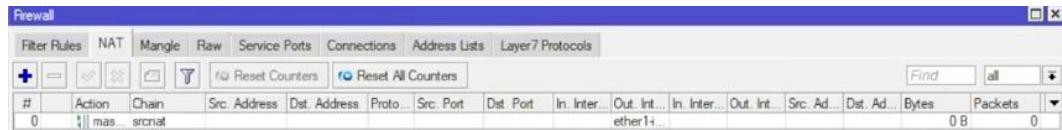
Langkah selanjutnya adalah *menset-up DHCP Server* dengan tujuan agar user/client yang terhubung ke *ether2* ataupun *wifi* akan mendapat *ip* secara otomatis melalui menu *IP > DHCP Server > DHCP Setup >* lakukan masing-masing untuk *interface ether2* dan *wlan1* seperti pada Gambar 4.9.



DHCP Server						
DHCP		Networks		Leases		Options
+ - ✓ ✖		DHCP Config		DHCP Setup		Option Sets
	Name	Interface	Relay	Lease Time	Address Pool	Add AR...
	dhcp1	ether2-PC		00:10:00	dhcp_pool0	no
	dhcp2	wlan1-WiFi		00:10:00	dhcp_pool1	no

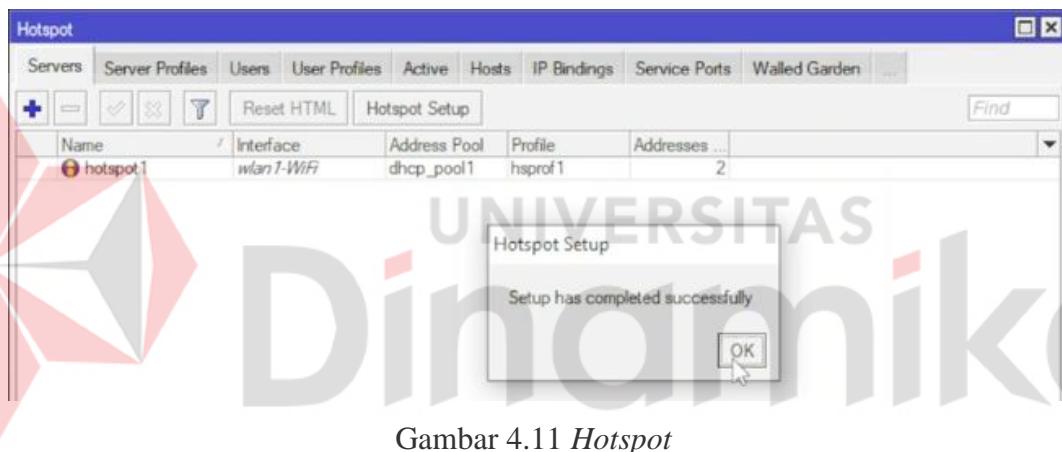
Gambar 4.9 *DHCP server*

Sampai langkah ini *client* sudah otomatis mendapatkan *ip* dari *server* tapi belum bisa terkoneksi ke *internet*, untuk bisa terkoneksi ke *internet* maka perlu ditambahi setting *NAT* pada menu *IP > Firewall > NAT > Add >* pada tab *general chain = srcnat, Out. Interface* adalah *port ethernet* yang mengarah ke *internet* yaitu *port ether1*, pada tab *action* pilih *masquerade > Apply > Ok*. Seperti pada Gambar 4.10.



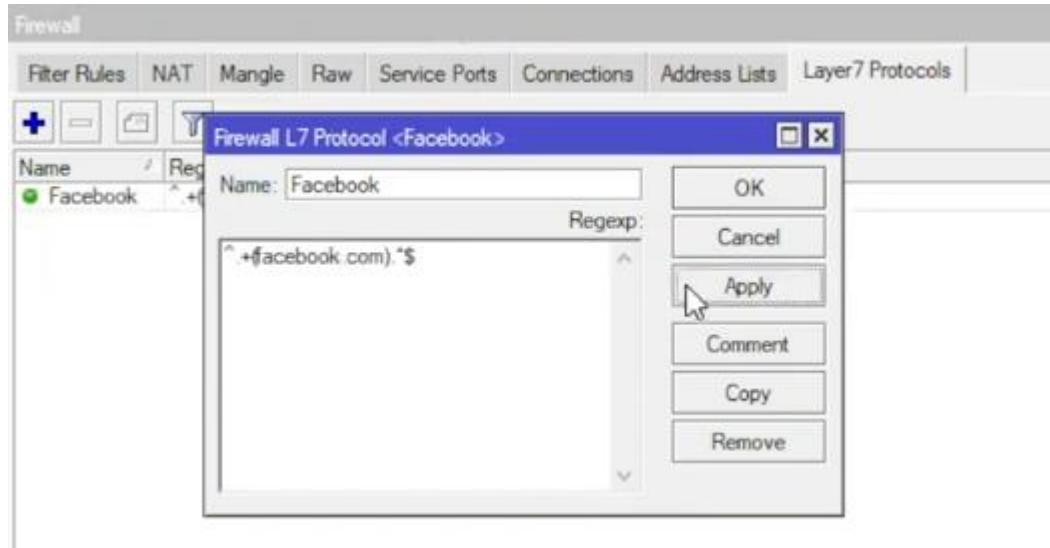
Gambar 4.10 NAT

Selanjunya membuat *hotspot* untuk nanti *user/client* terhubung, *IP > Hotspot > Server > Hotspot setup* > lalu pilih *interface* yang ingin digunakan untuk *hotspot* yaitu *wlan1*, *next* > hilangkan tanda centang pada *masquerade netwok*, *next* > pada menu *DNS name* mengisi nama yang digunakan untuk nanti *login* > untuk *admin* bisa diberi *password* juga bisa dikosongkan, *next*. Jika setting bena maka akan seperti pada Gambar 4.11.



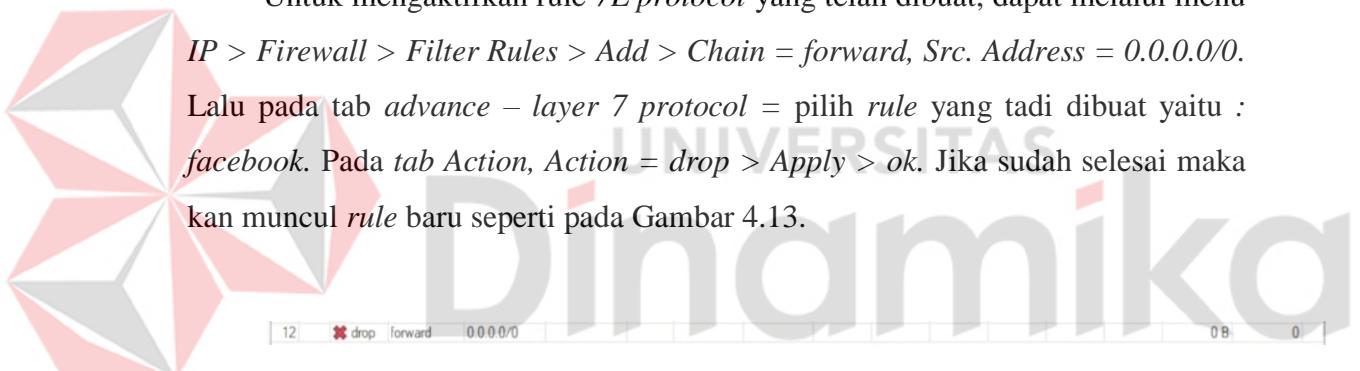
Gambar 4.11 Hotspot

Langkah selanjutnya adalah melakukan blokir situs dengan menggunakan *layer 7 protocol*, *IP > Firewall > Layer 7 protocol > Add* > pada kolom *name*, dapat diisi dengan web yang ingin diblokir, seperti : *facebook.com*, pada kolom *Regexp* dapat diisi dengan nama web tadi dengan formula : *^.+(nama web).*\$*. Karena ingin memblok *facebook* maka diisikan *^.+(facebook.com).*\$* > *Apply* > *Ok*. Seperti pada Gambar 4.12.



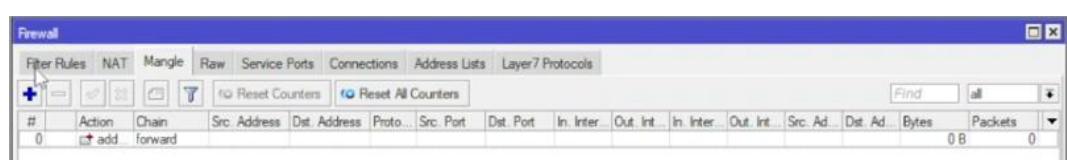
Gambar 4.12 Firewall 7l protocol

Untuk mengaktifkan rule 7L protocol yang telah dibuat, dapat melalui menu *IP > Firewall > Filter Rules > Add > Chain = forward, Src. Address = 0.0.0.0/0*. Lalu pada tab *advance – layer 7 protocol* = pilih *rule* yang tadi dibuat yaitu : *facebook*. Pada tab *Action*, *Action = drop > Apply > ok*. Jika sudah selesai maka akan muncul *rule* baru seperti pada Gambar 4.13.



Gambar 4.13 Filter rules 7l protocol

Selanjutnya adalah memblokir situs menggunakan *Mangle*, pada menu *IP > Firewall > Mangle > Add >* pada *tab general, chain = forward*. Pada *tab advance, content =* isikan situs yang ingin di blokir, *youtube.com*. Pada *tab action, action = add dst to address list, address list =* isikan nama web yang ingin di blokir, *youtube > Apply > Ok*. Jika sudah maka tampilanya akan seperti pada Gambar 4.14.



Gambar 4.14 *Mangle*

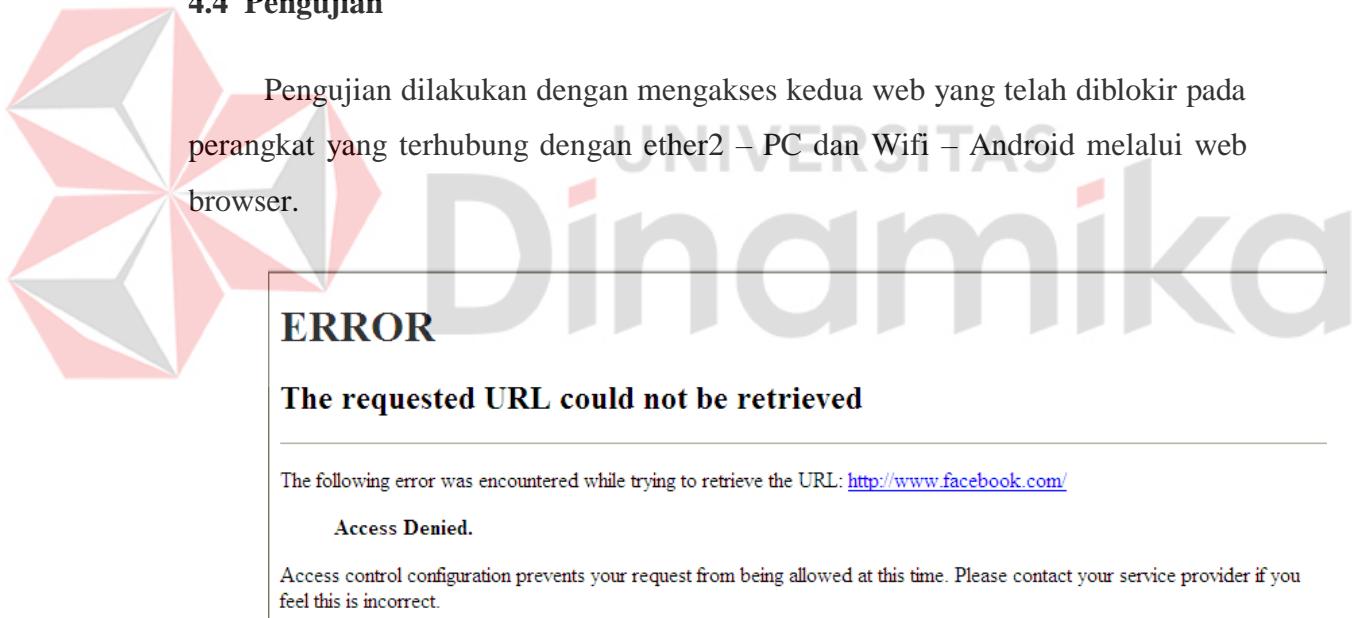
Sama seperti *7 layer protocol*, perlu ditambahkan *filter rule* agar setting yang telah dibuat bisa berfungsi, *IP > Firewall > Filter rules > Add > General, Chain = forward, Src. Address = 0.0.0.0/0*. Pada *tab Advanced, Dst. Address List*, pilih nama web yang tadi dibuat yaitu : youtube. Pada *tab Action, Action = reject/drop > Apply > Ok*. Jika sudah selesai maka akan muncul *rule* baru seperti pada Gambar 4.15.



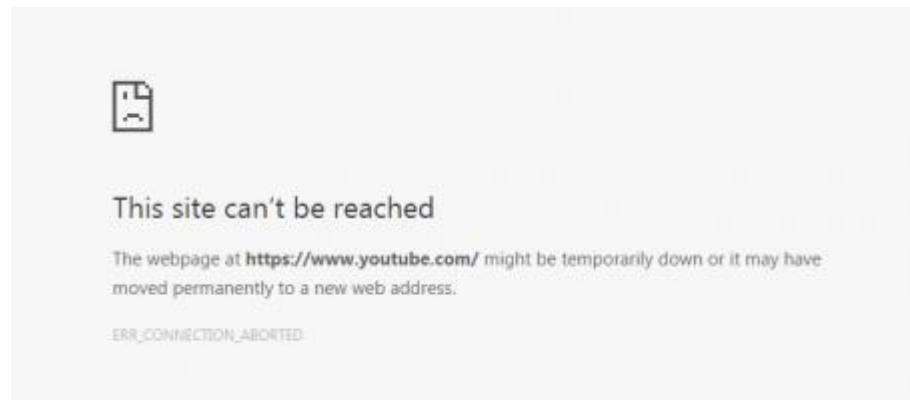
Gambar 4.15 *Filter rules mangle*

4.4 Pengujian

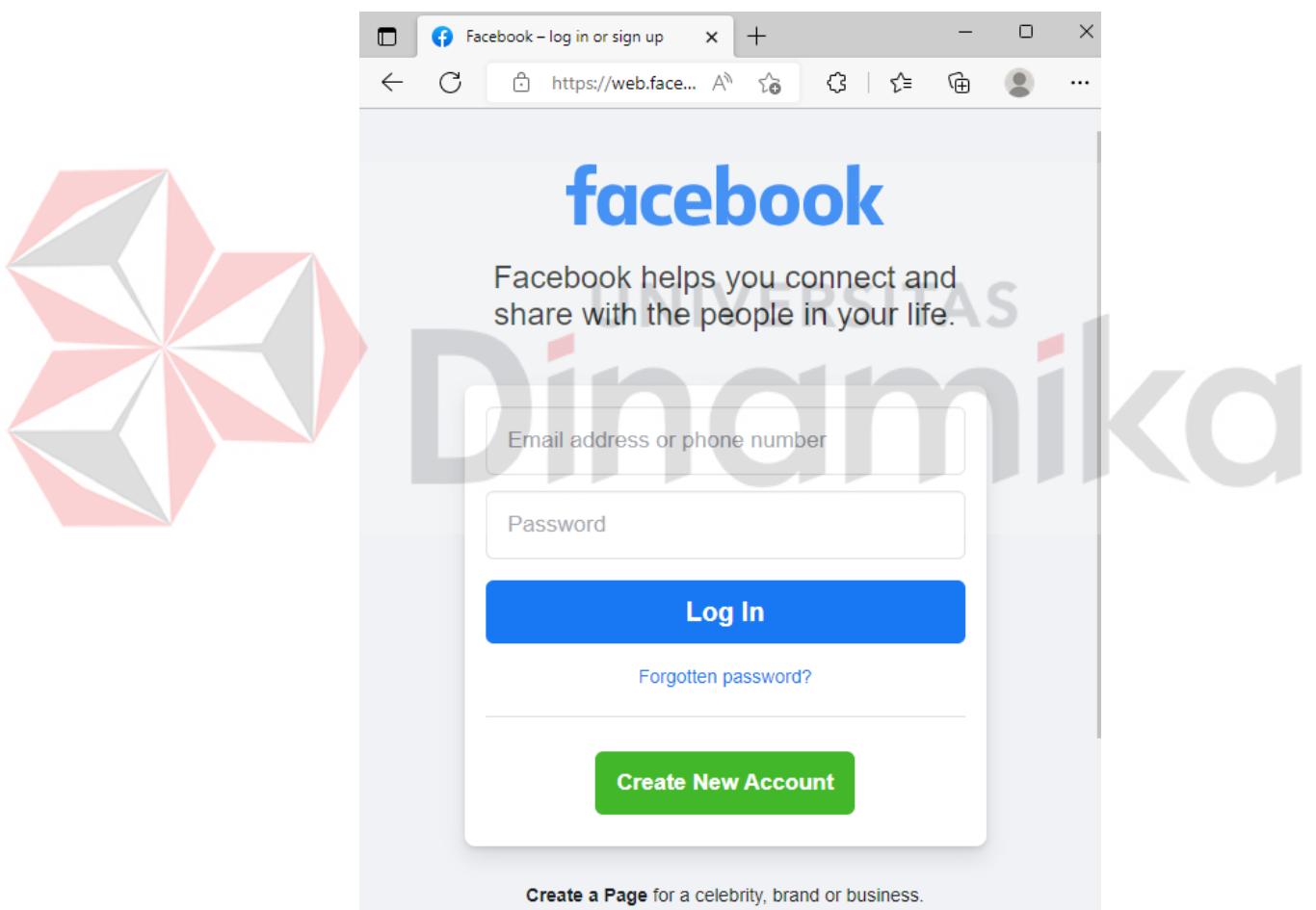
Pengujian dilakukan dengan mengakses kedua web yang telah diblokir pada perangkat yang terhubung dengan ether2 – PC dan Wifi – Android melalui web browser.



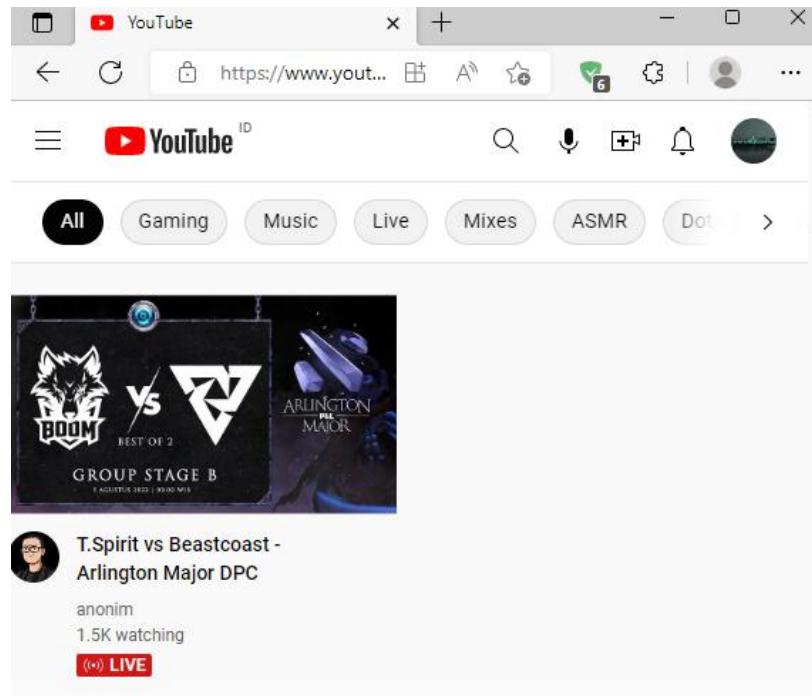
Gambar 4.16 Uji coba facebook.com web



Gambar 4.17 Uji coba youtube.com web



Gambar 4.18 Uji coba facebook search engine



Gambar 4.19 Uji coba youtube *search engine*

Tabel 4.1. Hasil uji coba *proxy server*

Website\Device	Browser PC	Browser Android	Search Engine PC	Search Engine Android
Facebook.com	Denied	Denied	Forward	Forward
Youtube.com	Denied	Denied	Forward	Forward

Dapat dilihat pada Tabel 4.1 bahwa jika user mengakses web yang di blokir melalui *url* maka 100% web akan terblokir, sebaliknya jika menggunakan *search engine* maka semua web yang di blokir masih tetap bisa diakses walau sudah berada dalam *list blacklist*.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil dari pengujian yang dilakukan pada penelitian ini didapatkan beberapa poin kesimpulan sebagai berikut:

1. Pemblokiran web yang diinginkan telah berhasil seperti terlihat pada Gambar 4.16 dan 4.17.
2. Web hanya bisa terblokir jika user mencari web langsung di kolom *search web browser* dan tidak melalui *search engine*.
3. Hanya dapat memblokir alamat web yang sama persis seperti yang diinputkan di *rules*.

5.2 Saran

Bisa ditambahkan rule tambahan atau hardware tambahan agar hasil blokir situs lebih maksimal dan tidak terpaku pada satu alamat web yang diinputkan atau bersifat *flexible*.

DAFTAR PUSTAKA

Ayokonfig.com. (2016). *Pengertian Mikrotik RouterOS*. Retreived from ayoconfig : <https://www.ayokonfig.com/2016/11/pengertian-mikrotik-routeros.html>

Decoding.com. (2021). *Apa itu firewall*. Retrieved from decoding : <https://www.dicoding.com/blog/apa-itu-firewall/>

Kurniawan, Andre Arta. (2019). *Membangun Proxy Server Pada Jaringan PT. CROSS NETWORK INDONESIA Dengan Menggunakan Mikrotik*.Universitas Dinamika, Surabaya.

Mikrotikacademy. (2021). *Tutorial Cara Menggunakan Winbox*. Retreived from mikrotikacademy : <https://mikrotikacademy.https://www.idn.id/tutorial-cara-menggunakan-winbox/>

Niagahoster.co.id. (2021). *Proxy Server*. Retrieved from niagahoster : <https://www.niagahoster.co.id/blog/proxy-server/>

