

PERANCANGAN PROXY SERVER SEBAGAI MEDIA AUTENTIFIKASI MENGUNAKAN MIKROTIK DAN DEBIAN PADA JARINGAN ISTN

DESIGN PROXY SERVER AS AN AUTENTIFICATION MEDIA USING MICROTICS AND DEBIAN ON THE ISTN NETWORK

Adam Hamdan¹, Siti Madinah Ladjamuddin², Dudy Fadly S. Siregar³

Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi

Institut Sains dan Teknologi Nasional

Jl. Moh. Kahfi II, Bhumi Srengseng Indah, Jagakarsa, Jakarta Selatan 12640

Telp. (021) 7874647, Fax. (021) 7866955

¹hamdanadam@gmail.com, ²citymadinah07@istn.ac.id, ³dudyfadly@istn.ac.id,

ABSTRAKSI

Dalam pemakaian internet bersama-sama sering kali menimbulkan masalah, seperti tidak adanya filter akses jaringan internet untuk mencegah dari hal-hal yang negatif yang ada di internet, pemanfaatan internet yang tidak berdasarkan haknya. Untuk mengatasi permasalahan tersebut, maka dibuatlah suatu sistem optimalisasi dan filter pada jaringan internet ISTN, menggunakan server proxy. Karena sebuah instansi tentunya ingin memberikan yang terbaik dalam memberikan kualitas koneksi dan keamanan pada jaringan internet seperti masalah hak akses client, akses internet yang lambat, menangani adanya akses terhadap situs yang tidak sesuai dengan dunia pendidikan. Dengan menggunakan squid pada proxy server maka dapat di atur konfigurasi optimalisasi jaringan, manajemen, penggunaan IP serta alamat internet dan lainnya. Pada aplikasi ini digunakan sistem operasi linux debian 5 yang dirasakan sangat efektif dalam penggunaan pengaturan konfigurasi squid. Hasil yang didapat adalah proxy server yang dibuat sehingga mengatasi permasalahan-permasalahan yang ada pada jaringan internet ISTN.

Kata Kunci : *Proxy server, filtering, internet*

ABSTRACT

In the Internet usage together often cause problems, such as the absence of Internet access filters to prevent from the negative things that exist on the Internet, Internet utilization is not based on its rights. To solve these problems, a system of optimization and filtering is established on the Internet network ISTN, using a proxy server. Because an agency certainly wants to give the best in providing the quality of connection and security on the Internet network such as client permissions problems, slow Internet access, addressing the presence of access to sites that do not comply with the education World. By using Squid On a proxy server, it can be set to configure network optimization, management, IP usage and Internet address and others. In this application used Debian 5 Linux operating system that is felt very effective in the use of Squid configuration settings. The result is a proxy server that is created to overcome the problems that exist in the Internet network ISTN.

Keywords : *Proxy server, filtering, Internet*

1. PENDAHULUAN

Dalam dunia pendidikan dan dunia kerja saat ini sarana internet sangat diperlukan. Karena dengan internet dapat memudahkan mahasiswa maupun dosen dalam melaksanakan kegiatan belajar-mengajar. Namun untuk mendistribusikan internet dengan baik diperlukan infrastruktur dan sistem manajemen jaringan yang baik. Namun tanpa disadari tidak semua informasi yang ada di internet dapat dijadikan sebagai ilmu pengetahuan. Informasi-informasi tersebut tidak seluruhnya berdampak positif, bahkan tidak sedikit yang berdampak negatif. *Proxy Server* merupakan salah satu cara yang ampuh diterapkan dalam memblokir situs-situs negative atau yang tidak perlu di akses dalam

kegiatan belajar mengajar yang dapat diakses oleh mahasiswa

Andy Rachman dan M. Aminullah pada tahun 2013 dengan penelitiannya yang berjudul "*Rancang Bangun Proxy Server dan Analisis Pemakaian Internet Dengan Menggunakan SARG (Studi kasus di BMKG Juanda Surabaya)*" menjelaskan bahwa rancang bangun proxy server tersebut di buat dengan tujuan untuk mengatur penggunaan bandwidth internet pada BMKG Juanda dapat lebih dioptimalkan. Dalam melakukan analisis pemakaian internet dilakukan dengan memanfaatkan *Squid Analysis Report Generator* yang selanjutnya disebut SARG.^[1] M. Asmuddin Ahmad pada tahun 2012 dengan penelitian yang berjudul "*Analisis dan Implementasi Web Proxy ClearOs Sebagai*

Autentifikasi Jaringan Aminers Spot” Aminers Spot ini menerapkan teknologi jaringan dengan menyediakan layanan internet untuk mahasiswa dan pelajar yang tujuannya adalah supaya lebih mudah mendapatkan informasi melalui layanan yang luas tersebut. Untuk memperluas akses internet di lingkungan perumahan atau kos. Administrasi jaringan di spot tersebut menggunakan cara koneksi, yaitu dengan Lan dan via wireless.^[2]

Dari gambaran penelitian sebelumnya maka akan dilakukan penelitian tentang perancangan dan implementasi proxy server sebagai media autentifikasi menggunakan mikrotik dan debian pada jaringan ISTN. Karena sebuah instansi tentunya ingin memberikan yang terbaik dalam kualitas koneksi dan keamanan pada jaringan internet seperti masalah yang terdapat pada jaringan internet ISTN seperti hak akses client, menangani adanya akses terhadap situs situs ilegal, serta portal menuju akses internet itu sendiri.

Dengan penjabaran di atas yang akhirnya dibangun penelitian dengan judul “Perancangan Proxy Server Sebagai Media Autentifikasi Menggunakan Mikrotik dan Debian Pada Jaringan ISTN”.

Berdasarkan latar belakang di atas, maka rumusan masalah yang akan di bahas yaitu bagaimana memabangun sistem proxy server dan media autentifikasi yang dapat membatasi hak akses terhadap situs-situs yang tidak sesuai dengan dunia pendidikan.

Untuk memfokuskan bahasan maka diberikan batasan masalah dalam perancangan proxy server diantaranya adalah:

1. Perancangan proxy server ini hanya rancang bangun tidak untuk di implementasikan pada jaringan ISTN yang sesungguhnya.
2. Mengfilter akses internet clients dari situs yang mengandung konten porno, perjudian, kekerasan dan situs yang terdaftar atau yang tidak di butuhkan dalam situs blacklist.
3. *Utilitas* yang digunakan dalam membangun proxy server sebagai media autentifikasi yaitu linux debian, mikrotik, dan squid.

2. METODOLOGI PENELITIAN

Waktu dan Tempat Penelitian

Penelitian skripsi ini di lakukan pada bulan Februari 2018 sampai dengan Agustus 2018. Bertempat di Institut Sains dan Teknologi Nasional Jln. Moh Kahfi II, Srengseng Sawah, Jagakarsa, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12630.

Metode Pengumpulan Data

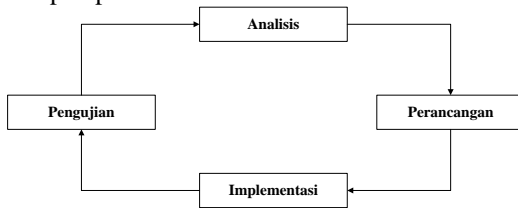
Metode pengumpulan data ini bertujuan untuk memperoleh data-data apa saja yang di butuhkan dalam membangun sebuah sistem. Dibawah ini adalah metode yang dilakukan dalam tahap pengumpulan data:

- a. Wawancara (*Interview*)
Wawancara telah dilaksanakan dengan melakukan tanya jawab secara langsung dengan staf NOC. Kesimpulan dari wawancara tersebut yaitu, ISTN membutuhkan pengembangan jaringan internet yang telah di bangun sebelumnya agar dapat di gunakan sebagaimana mestinya. Karena jaringan internet yang sudah ada saat ini tidak memiliki sistem seperti *proxy* server di dalamnya, hanya sebatas jaringan internet biasa. Hal itu menyebabkan penggunaan akses internet di ISTN masih sangat bebas dan tidak ada control pengamanan terhadap jaringan yang dapat disalah gunakan.
- b. Pengamatan (*Observation*)
Pengamatan telah di lakukan yaitu dengan cara melakukan pengamatan dan pengecekan mengenai kekurangan-kekurangan apa saja yang di butuhkan pada jaringan internet di ISTN. Setelah melakukan pengamatan terhadap jaringan internet yang telah tersedia sebelumnya, masih terdapat banyak kekurangan yaitu belum adanya server yang di rancang khusus untuk menangani jaringan internet, tidak memiliki sistem keamanan, akses internet sering melambat, tidak adanya pemfilteran client atau pemblokiran terhadap konten yang tidak harus di akses. Maka dari itu diperlukan adanya pengembangan agar jaringan internet tersebut dapat digunakan sebagai mana mestinya.
- c. Studi Kepustakaan (*Library Study*)
Metode pengumpulan data yang telah di lakukan yaitu, melalui buku, laporan laporan, E-journal, E-book, hasil penelitian ilmiah, internet dan sumber penulisan terpercaya lainnya yang berhubungan dengan proxy server sebagai bahan acuan dalam hal percangan proxy server di jaringan internet ISTN. Pengumpulan data yang di lakukan yaitu mengenai apa saja yang harus digunakan untuk merancang proxy server pada setiap jaringan internet di ISTN.

Teknik Pengembangan Sistem

Pengembangan sistem merupakan sebuah alternatif dalam berapresiasi dalam mendalami

suatu kajian ilmu. Metode pengembangan yang digunakan adalah NDLC (*Network Development Life Cycle*). Berikut gambar tahapan pada NDLC :



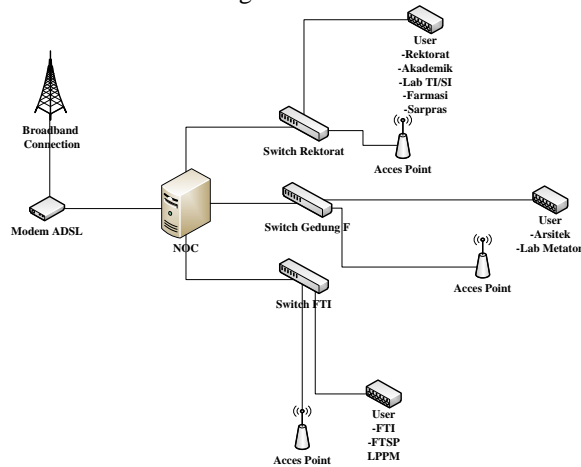
Gambar 1. Teknik Pengembangan Sistem

Analisis

Tahap awal ini dilakukan analisa kebutuhan analisa permasalahan yang muncul, analisa keinginan user dan analisa topologi / jaringan yang sudah ada saat ini.

Analisis Sistem Berjalan

Pada jaringan internet di ISTN Menggunakan jaringan kabel dan nirkabel untuk mendistribusikan internet. Konfigurasi yang digunakan menggunakan switch sebagai media pendistribusian kabel, dan acces point sebagai media pendistribusian nirkabel (WLAN). Alur kerja sistem yang berjalan pada jaringan internet di ISTN sebagai berikut :



Gambar 2. Analisis Sistem Berjalan

Identifikasi Masalah

Setelah melihat analisis sistem berjalan yang ada pada jaringan internet istn, dapat dilihat jika dalam topologi tersebut belum adanya sistem keamanan internet, belum adanya media Autentifikasi yang dapat mengatur hak akses client.

Solusi Penyelesaian Masalah

Berdasarkan hasil permasalahan yang ada, maka di usulkan pemecahan masalah dengan cara membangun sebuah proxy server sebagai media autentifikasi masuk ke gerbang internet,

sebab proxy dapat menangani hak akses client, dan pemblokiran akses secara bersamaan.

Analisis Kebutuhan

Analisa kebutuhan berupa hardware dan software apa saja yang diperlukan untuk membangun proxy server sebagai media autentifikasi pada jaringan ISTN.

Perangkat keras yang di gunakan (Hardware)

Berikut ini hardware yang di perlukan untuk membangun proxy server di antaranya :

PC Server

Dibawah ini merupakan spesifikasi PC server yang digunakan. Perangkat keras ini digunakan untuk membangun proxy server.

Mikrotik RB941-2nD-TC (hAP-Lite2)

Untuk membangun sebuah jaringan dibutuhkan sebuah router mikrotik yang digunakan sebagai pengatur lalu lintas data. Mikrotik yang digunakan adalah mikrotik dengan type RB941-2nD-TC

Tabel 1

No.	Perangkat	Penjelasan
1.	Processor	Kecepatan 2.6GHz
2.	Memory Fisik	2GB RAM
3.	Harddisk	320 GB

Router Switch D-Link N150

Router yang digunakan untuk menyebarkan data dari server menggunakan router switch dengan type D-Link N150.

Perangkat keras (hardware) lainnya, yaitu kabel UTP, RJ45.

Perangkat lunak yang digunakan (Software)

Penulis menggunakan beberapa perangkat lunak dalam penelitian ini. Perangkat lunak yang digunakan adalah sebagai berikut :

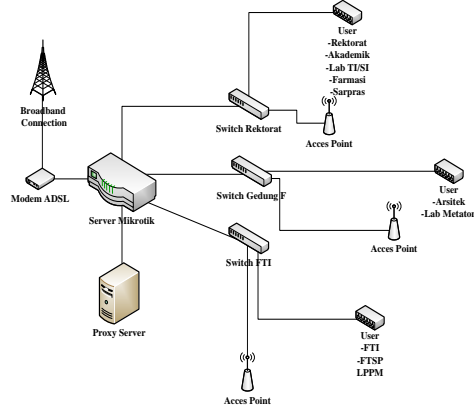
- System operasi Linux Debian 5
- Squid
- Winbox

Perancangan

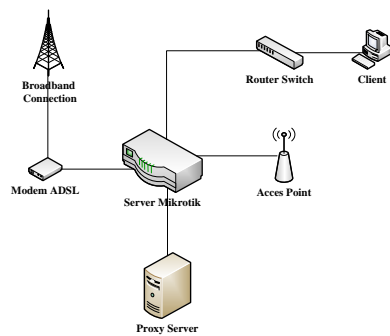
Dari data-data yang didapatkan sebelumnya, tahap design ini akan membuat gambar design topology jaringan interkoneksi yang akan dibangun, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Design bisa berupa design struktur topology, yang akan memberikan gambaran jelas tentang sistem yang akan dibangun.

Topologi Jaringan Usulan

Pada tahapan perancangan topologi jaringan ini menggunakan media kabel dan nirkabel. Berikut ini gambaran topologi jaringan internet usulan dan topologi jaringan real yang digunakan sebagai percobaan jaringan :



Gambar 3. Topologi Jaringan Usulan



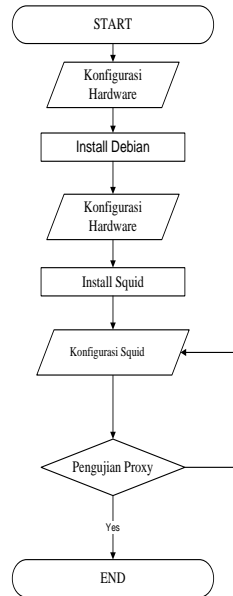
Gambar 4. Topologi Jaringan Real

Perancangan Sistem Usulan

Perancangan sistem usulan dideskripsikan dengan model analisis menggunakan beberapa flowchart. Untuk membantu perancangan dan melengkapi dokumentasi perancangan, flowchart yang di buat adalah flowchart perancangan proxy server, flowchart sistem usulan, dan flowchart filtering content.

Flowchart Perancangan Proxy Server

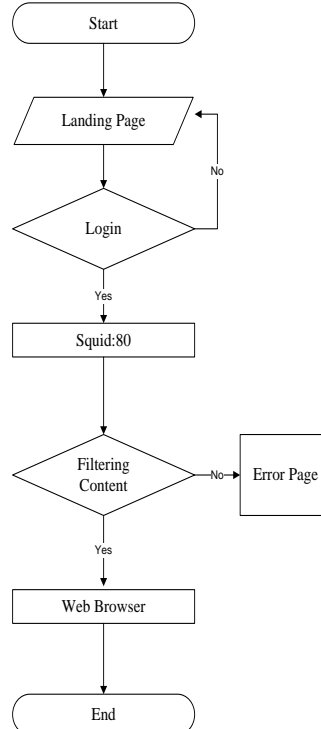
Adapun perancangan proxy server ini membutuhkan sebuah alur yang terstruktur dengan baik. Untuk mempermudah proses perancangan dan pengimplementasian menggunakan flowchart yang membantu dalam memahami proses perancangan yang akan dibuat.



Gambar 5. Flowchart Perancangan Proxy Server

Flowchart Sistem Usulan

Berikut ini merupakan flowchart proses sistem usulan yang dibangun:



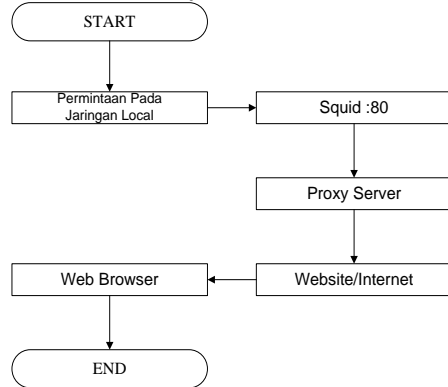
Gambar 6. Flowchart Proses Sistem Usulan

Dalam proses perancangan pembuatan proxy ini menggunakan suatu alur kerja sistem yaitu saat pertama kali dijalankan client di minta untuk login lalu melakukan permintaan dari web browser baik pencarian kata, gambar maupun alamat website/url secara default di teruskan melalui port 80. Squid memfilter

setiap sumber permintaan apakah dapat diteruskan atau tidak, apabila tidak dapat diteruskan akan di teruskan ke halaman penolakan akses atau error page.

Filter ialah melakukan filtering content apakah konten tersebut mengandung unsure pornografi atau suatu halaman yang tidak boleh diakses.

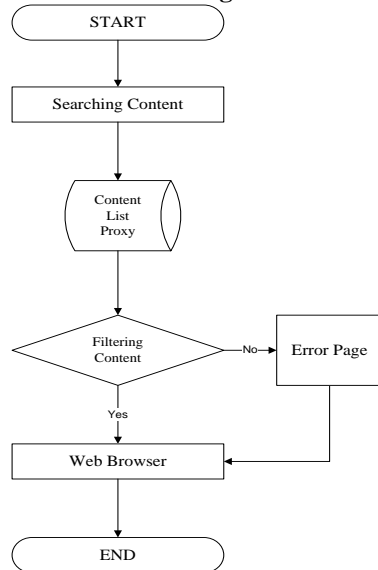
Flowchart Proxy Server



Gambar 7. Flowchart Proses Proxy Server

Dalam Proses proxy server menggambarkan alur setiap permintaan client pada jaringan local secara default diteruskan melalui port 80. Dan teruskan ke web server yang ada di jaringan public. Jadi setiap permintaan client ditangani oleh proxy server sebelum menuju web server.

Flowchart Filtering Content



Gambar 8. Flowchart Filtering Content

Mempunyai alur yaitu client melakukan permintaan pada web browser melalui jaringan internet proxy, dan proxy

akan melakukan validasi apakah content yang diminta tersebut terdapat pada content list terlarang atau tidak, jika terdapat pada list maka akan dilakukan blocking dengan menampilkan error page pada web browser.

Implementasi

Tahapan ini memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi menerapkan semua yang telah di rencanakan dan dirancang sebelumnya. Tahap implementasi merupakan tahapan yang sangat menentukan dari berhasil atau tidaknya project yang dibangun.

Pengujian

Pada tahap ini dilakukan pengujian terhadap system yang telah di implementasikan pada jaringan sesungguhnya. Proses pengujian di lakukan untuk memastikan bahwa semua pernyataan telah di uji untuk menemukan kesalahan kesalahan yang ada. Memastikan bahwa sistem berjalan sesuai dengan kebutuhan dan desain yang telah di buat.

3. HASIL DAN PEMBAHASAN

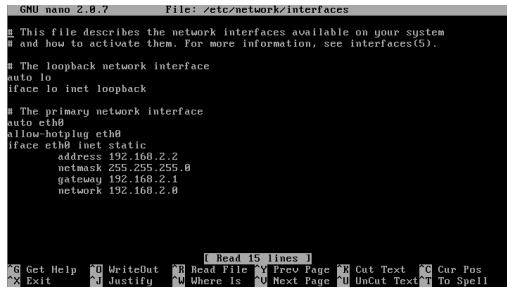
Instalasi Linux Debian

Dalam melakukan instalasi linux debian untuk dijadikan OS server proxy tahapan instalasinya masih sama. Debian dapat dijalankan dengan GUI ataupun CLI, namun pada sistem yang di bangun menggunakan sistem standar alias CLI, karena memiliki beberapa keuntungan, salah satunya tidak memakan banyak memory karena hanya berbasis teks.

Konfigurasi IP Address

Pemberian alamat IP address pada komputer server dilakukan secara manual (statically). Berikut ini adalah tahap-tahapnya :

1. Ketik script nano /etc/network/interfaces pada linux dengan root user.
2. Pada file interfaces yang ada tambahkan script konfigurasi Ethernet card dengan meng-input IP address, netmask, network, gateway pada eth0. Seperti pada gambar dibawah ini :



Gambar 9 Setting Ip Address

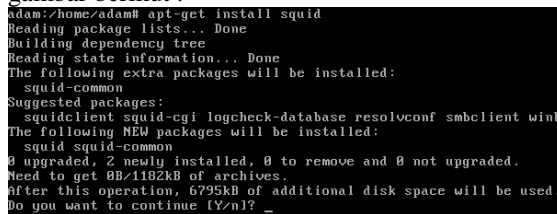
Masukkan IP berdasarkan table berikut :

Tabel 2. Konfigurasi IP Address

Keterangan	IP Address
IP address	192.168.2.2
Netmask	255.255.255.0
Gateway	192.168.2.1
Network	192.168.2.0

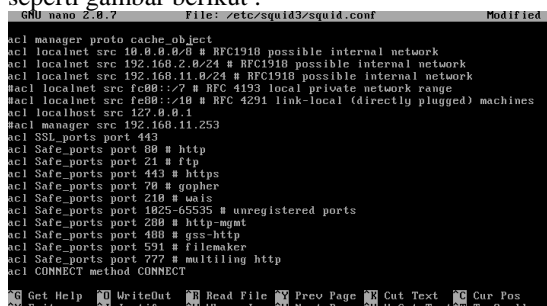
Konfigurasi Proxy Server

Langkah pertama untuk melakukan konfigurasi proxy server setelah setting ip address adalah melakukan install paket squid yang tersedia pada linux dengan script : apt-get install squid lalu tekan enter seperti pada gambar berikut :



Gambar 10 Install Squid

Setelah instalasi squid berhasil tanpa ada kesalahan lanjut pada tahap selanjutnya yaitu edit file squid.conf dengan menggunakan perintah script : nano /etc/squid/squid.conf seperti gambar berikut :



Gambar 11 Tampilan squid.conf

Tampilan diatas merupakan potongan bagian paling atas dari file konfigurasi squid (squid.conf). kemudian pada halaman selanjutnya beri listing yang terdiri dari TAG-TAG konfigurasi. Tag-tag konfigurasi yang nantinya akan diinput script sehingga akan tercapai tujuan dalam pembuatan proxy server . Hanya listing yang tidak diawali tanda pagar

(#) saja yang akan aktif. Jadi apabila ada tag yang diawali dengan tanda pagar (#) maka tag tersebut tidak aktif.

Tabel 3 Script Transparent Proxy

```
....
#TAG: http_port
http_port 3128 transparent
....
#TAG: cache_mgr
Cache_mgr adam.hamdan16@gmail.com
....
#TAG: V=visible_hostname
Visible_hostname adam.hamdan.com
```

Pada listing konfigurasi di atas, selain menambahkan kata transparent juga menambahkan perintah cache_mgr dan visible_hostname, sebagai identitas dan contact administrator yang bisa dihubungi jika ada pesan error yang tampil dikarenakan pembatasan hak akses.

Salah satu cara untuk mengelola hak akses internet secara optimal adalah dengan membatasi akses internet tertentu.konfigurasi untuk menangani penutupan akses alamat yang diblokir adalah sebagai berikut :

Tabel 4 Script Filtering Alamat Website

```
#TAG: acl
....
acl local src 192.168.11.0/24
acl blockir dstdomain
"/etc/squid/blockdomain"
....
#TAG: http_access
http_access deny blockir
http_access allow local
....
```

Pada konfigurasi ini diharuskan membuat file blockdomain yang disimpan di direktori /etc/squid/ dengan menggunakan text editor nano. File ini berisi alamat-alamat yang tidak dapat diakses karena alasan-alasan tertentu.

Berikut ini contoh isi file blockdomain:

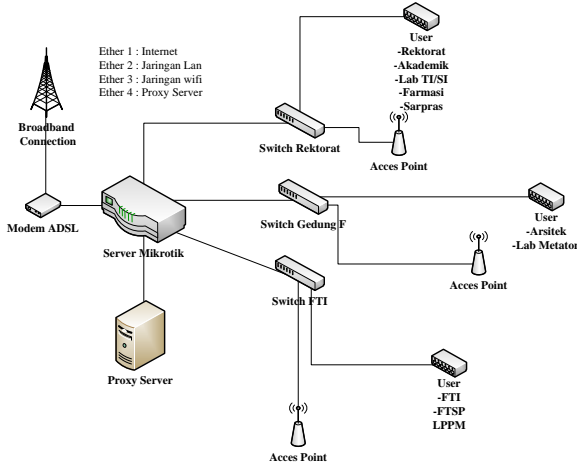
Tabel 5 Isi File Blockdomain

```
.youtube.com
.facebook.com
.twitter.com
```

Semakin banyak alamat internet yang dimasukkan, semakin banyak pula pengurangan kuota pemakaian untuk alamat-alamat yang tidak perlu. Jika ada permintaan menuju alamat tertentu yang termasuk dalam domainblock maka web browser akan menampilkan pesan penolakan.

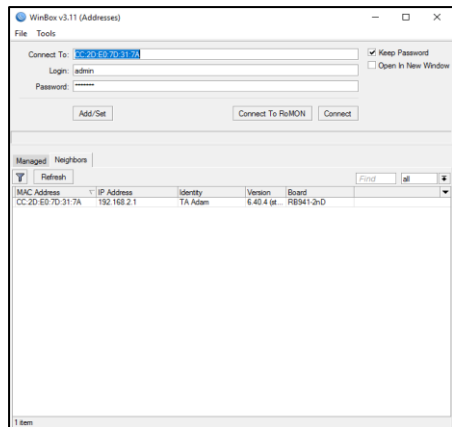
Konfigurasi Router Mikrotik

Pada tahap konfigurasi ini adalah salah satu tahap penerapan dari sistem yang telah di rancang. Untuk Konfigurasi menggunakan RouterOS Mikrotik versi 3.11 dengan *topology* jaringan sebagai berikut :



Gambar 12 Topology Jaringan

Login Menggunakan *MacAddress* yang terdeteksi dari mikrotik seperti gambar di bawah ini:



Gambar 13 Login Mikrotik

Setelah login berhasil masuk ke menu utama winbox dan masuk ke menu *interfaces* yang pertama di lakukan adalah atur *port ethernet* sesuai dengan apa yang sudah kita rancang di *topology* seperti gambar di bawah ini :

Interface	Type	Actual MTU	L2 MTU	Tx
R ether1-Modem	Ethernet	1500	1598	0 bps
S ether2-Jaringan	Ethernet	1500	1598	67.8 kbps
S ether3-Wifi	Ethernet	1500	1598	0 bps
S ether4-Proxy	Ethernet	1500	1598	0 bps
X wlan1	Wireless (Atheros AR9...	1500	1600	0 bps

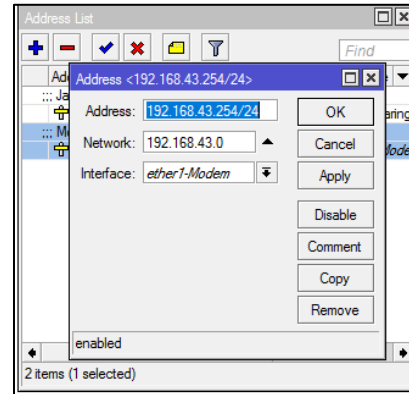
Gambar 14 Interfaces List

Berikut adalah konfigurasi *port ethernet* yang akan di gunakan :

Tabel 6 Konfigurasi Ethernet port Mikrotik

Ethernet	IP address
Ethernet 1 = Modem	
Ethernet 2 = Proxy Server	192.168.2.2
Ethernet 3 = Jaringan Lokal(LAN)	192.168.11.0/24
Ethernet 4 = Jaringan Hotspot	192.168.11.0/24

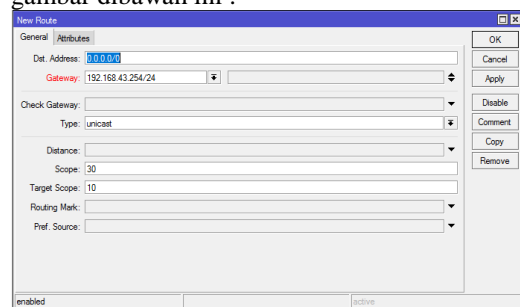
Setelah memberikan setiap label pada port Ethernet yang harus di lakukan setelah itu berikan ip pada setiap port sesuai dengan kebutuhannya seperti gambar di bawah ini:



Gambar 15 Ip Address

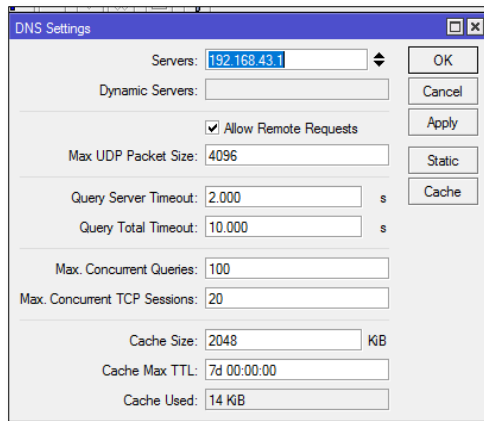
Pada gambar di atas sudah di berikan ip address kepada port Ethernet 1 yang berfungsi sebagai sumber internet, lakukan pemberian ip address kepada setiap port Ethernet sesuai dengan kebutuhannya masing-masing.

Pada tahap selanjutnya yaitu membuat mikrotik dapat terhubung ke internet dengan cara masuk ke menu IP ->Routes dan di menu Route List kita klik tombol + lalu masukkan gateway sesuai dengan IP modem seperti pada gambar dibawah ini :



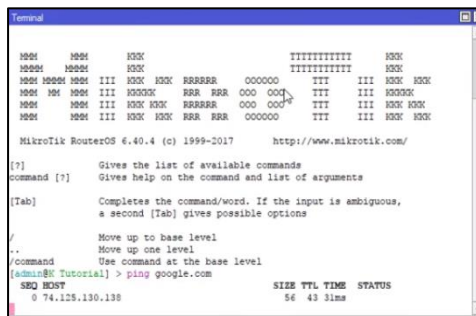
Gambar 16 IP Routes

Setelah menambahkan gateway di ip routes yaitu menambahkan dns seperti gambar di bawah ini :



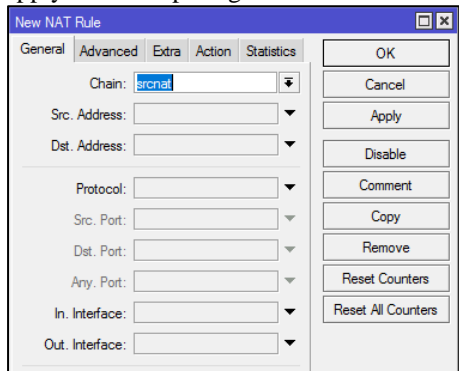
Gambar 17 DNS Setting

Setelah menambahkan ip routes dan dns pada mikrotik, cek koneksi pada mikrotik apakah mikrotik sudah terhubung dengan internet dengan cara buka terminal lalu ping google.com, jika sudah terkoneksi maka jawaban ping akan seperti gambar dibawah ini :

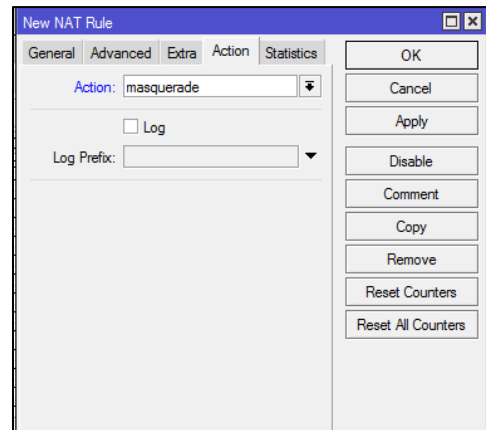


Gambar 18 Ping Google.com

Langkah selanjutnya adalah mengkonfigurasi firewall, digunakan agar client yang terhubung pada Ethernet 2 dan Ethernet 3 baik jaringan local (LAN) ataupun jaringan Hotspot dapat tersambung juga ke internet. Masuk ke menu ip lalu firewall, setelah masuk ke menu firewall cari tab NAT klik dan klik tombol +, setelah itu di tab menu General isi pada menu chain dengan 'srcnat', setelah itu pergi ke menu tab Action isi menu action dengan 'masquerade' lalu klik tombol apply lalu ok seperti gambar di bawah ini :

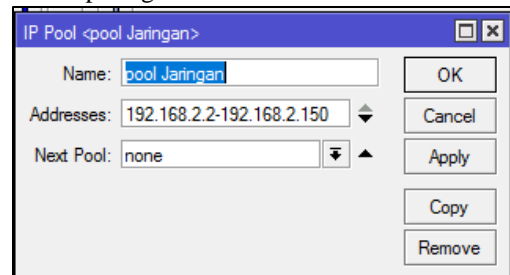


Gambar 19 NAT



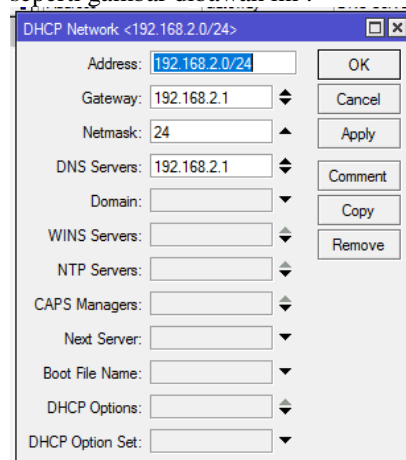
Gambar 20 NAT Rule

Setelah berhasil konfigurasi firewall yang harus di lakukan adalah membuat IP Pool, ip pool ini berfungsi untuk membagikan ip kepada semua client yang terhubung pada ethernet 2 dan ethernet 3. Disini diberikan ip pool 192.168.2.2 – 192.168.2.150 yang artinya client akan mendapatkan ip dari rentan .2 - .150 seperti gambar dibawah ini :



Gambar 21 IP Pool

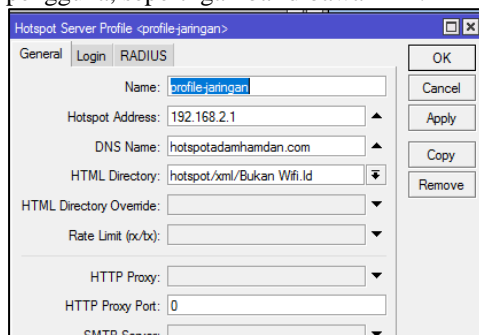
Setelah itu konfigurasi Dhcp Server yang berfungsi untuk membagikan ip kepada seluruh client agar mendapat ip secara otomatis. Pada menu dhcp server klik tab Network lalu klik tombol + lalu isikan kolom address, gateway, netmask, dan dns server seperti gambar dibawah ini :



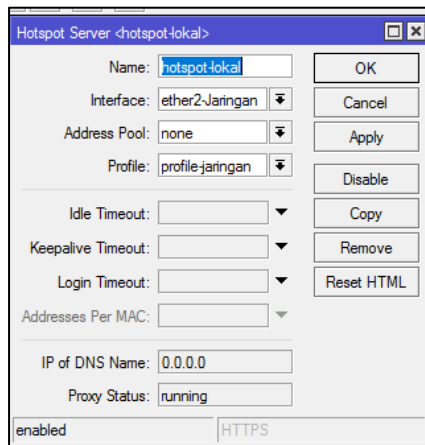
Gambar 22 DHCP Network

Setelah berhasil membangun jaringan lan, berhasil memberikan ip kepada setiap client serta client dapat terhubung ke internet langkah selanjutnya adalah membangun hotspot server.

Langkah pertama adalah masuk ke menu ip, pilih *hotspot*, setelah masuk ke menu *hotspot* yang harus di lakukan adalah membuat *hotspot profile* terlebih dahulu, dimana *hotspot profile* berfungsi untuk menentukan hak akses pada setiap user yang akan kita buat nantinya, setelah berhasil membuat *hotspot profile* yang harus dilakukan adalah membuat user, buat user sesuai dengan kebutuhan masing masing pengguna, seperti gambar dibawah ini :

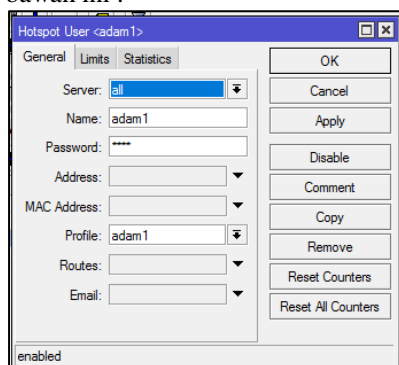


Gambar 23 Hotspot Server Profile



Gambar 24 Hotspot Server

Setelah melakukan konfigurasi hotspot profile dan hotspot server maka selanjutnya kita akan membuat user seperti gambar di bawah ini :



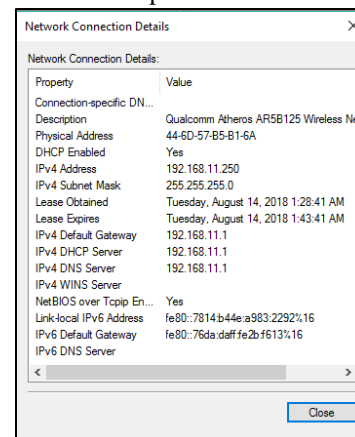
Gambar 25 Hotspot User

Pengujian dan Hasil

Sebelum dilakukannya pengujian, ada tahap yang harus dilakukan terlebih dahulu, yaitu memastikan koneksi harus berjalan dengan baik dari segi koneksi jaringan maupun koneksi internet. Pengujian ini dilakukan pada komputer client.

Pengujian Jaringan Server – Client

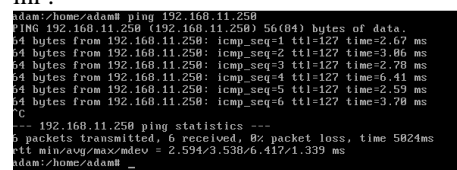
Pengujian di lakukan dengan memastikan koneksi antara komputer *server* ke *client* dan *client* ke *server* dapat terhubung dengan baik yang dapat dilakukan koneksi dari komputer *server* maupun *client*. Tahap awal dengan memastikan pemasangan kabel sudah benar, jika sudah terpasang dengan baik maka pada LAN *card* biasanya terdapat lampu indicator yang akan menyala, beigtu juga pada *access point* ataupun *router switch*. Setelah pemasangan kabel dilakukan dengan baik, selanjutnya setting ip *address client* dengan menggunakan DHCP, yang artinya semua client akan mendapatkan ip *address* otomatis dari *server* mikrotik yang sudah kita konfigurasi. Maka semua *client* akan mendapatkan ip 192.168.11.2 – 192.168.11.250, seperti gambar dibawah ini *client* mendapatkan IP 192.168.11.250



Gambar 26 IP address client

Pengujian *ping* dari komputer *server* ke komputer *client* yang memiliki IP 192.168.11.250 dengan perintah *script : ping 192.168.11.250*

Jika koneksi memang terhubung dengan baik, maka perintah tersebut akan menampilkan pesan seperti gambar dibawah ini :



Gambar 27 Hasil Perintah Ping Dari Server ke Client

Pengujian dari sisi *client* yang menggunakan sistem operasi windows ke komputer *server* yang memiliki IP 192.168.2.2 dan test dilakukan pada aplikasi DOS dengan perintah *script: ping 192.168.2.2*.

```
C:\Users\Adam Hamdan>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=2ms TTL=63
Reply from 192.168.2.2: bytes=32 time=2ms TTL=63
Reply from 192.168.2.2: bytes=32 time=2ms TTL=63
Reply from 192.168.2.2: bytes=32 time=2ms TTL=63
Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms
C:\Users\Adam Hamdan>
```

Gambar 28 Hasil ping dari server ke client

Maksud dari isi pesan yang di peroleh dapat disimpulkan adanya koneksi antara komputer *client* ke komputer *server*, begitu juga sebaliknya.

Pengujian Media Autentifikasi

Pengujian dilakukan dengan melakukan koneksi ke jaringan internet yang sudah dibangun, baik dari jaringan lokal (LAN) maupun hotspot. Berikut ini tampilan jika *client* sudah terkoneksi pada jaringan dan ingin melakukan koneksi ke internet, maka secara otomatis browser akan langsung mengarahkan ke halaman autentifikasi seperti gambar di bawah ini :



Gambar 29 Landing Page

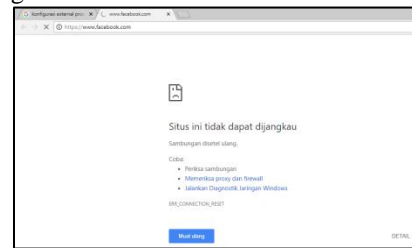
Setelah kita login dengan username dan password maka akan keluar tabel yang memberi tahu hak access dalam pemakaian internet tersebut seperti gambar di bawah ini :

Selamat Datang... adam1!	
Session Waktu:	Unlimited
Session Used:	Unlimited
Bytes up/down:	548 B / 0 B
Status Bandwidth:	Unlimited
Lama Uptime:	0s
status refresh:	1m
Logout	

Gambar 30 Tabel Login Sukses

Pengujian Proxy Server

Setelah melakukan sharing koneksi jaringan, koneksi internet dan melewati media autentifikasi, selanjutnya melakukan pengujian proxy server. Pengujian dilakukan dengan mengakses alamat domain yang sudah ditentukan pada saat konfigurasi, jika tidak dapat diakses maka pemblokiran berhasil. Berikut ini tampilan yang tampak ketika proxy tidak mengizinkan untuk mengakses konten yang dilarang dengan melakukan percobaan mengakses salah satu situs yang sudah di block yaitu <https://www.facebook.com/>. Seperti pada gambar :



Gambar 31 Error page Filtering Alamat Domain

Ketika client mencoba mengakses domain yang diblock oleh proxy maka akan timbul *loading* yang lama dan muncul halaman error seperti gambar diatas, seakan-akan browser kehilangan koneksi internet, dan yang sebenarnya terjadi adalah proxy telah melakukan block terhadap domain tersebut yang tidak diketahui oleh *client*.

4. SIMPULAN

Berdasarkan hasil dari analisis, perancangan, dan pengujian, maka dapat disimpulkan bahwa dengan cara membangun sebuah proxy server sebagai media autentifikasi dapat menangani hak akses client sebelum masuk ke gerbang internet, dan proxy server dapat melakukan pemblokiran akses secara bersamaan.

5. DAFTAR PUSTAKA

- [1] Agitya, Lingga. 2014. Eksplorasi Metodologi SDLC. Sistem Informasi UNIKOM
- [2] Aswan M.Si. 2015. Kumpulan Program Kreatif Dengan VB. Bandung: Penerbit, Informatika
- [3] Basri., H. 2014. Modul Pelatihan Quantum GIS. Indonesia Urban Water, Sanitation and Hygiene (IUWASH) .Surakarta
- [4] Imran., M., A. 2014. Definisi Perangkat Lunak. Gavamedia. Kristanto, Jogjakarta

- [5] Khairana.,R.U. 2016. Kerentanan Banjir di Bekasi. Universitas Indonesia, Fakultas MIPA, Departemen Geografi. Depok
- [6] Muludi. K., Hijriani. A., Zhia. K., 2014. Perancangan Aplikasi Desktop Sistem Informasi Geografis (SIG) Penyebaran Wisata Kuliner di Kota Bandar Lampung. Universitas Negri Lampung, Fakultas MIPA, Jurusan Ilmu Komputer. Lampung
- [7] Prahasta, E. 2016, Sistem Manajemen Basis Data, Informatika, Bandung.
- [8] Putra,W.A., 2015. Pengamanan Data. Universitas PGRI Yogyakarta
- [9] Rangkuti. A.C., Nugraha. A.L., Hani'ah., 2014. Aplikasi SIG Berbasis *Desktop* Untuk Sebaran Lokasi Usaha Pertambangan di Kabupaten Wonogiri. Universitas Diponegoro, Fakultas Teknik, Program Studi Teknik Geodesi. Semarang
- [10] Rastuti, Abdillah, L.A., Agustini, E.P., 2015. Sistem Informasi Geografis Potensi Wilayah Kabupaten Banyuasin Berbasis Web. Universitas Bina Darma, Fakultas Ilmu Komputer, Program Studi Sistem Informasi. Palembang
- [11] Riyanto.,Putra,E.,P., dan Indelarko., A.2015. Pengembangan Aplikasi Sistem Informasi Geografis Berbasis Desktop dan web. Gava Media. YogyakartaTriyono, J. Wahyudi, K. 2016. Tingkat Pencemaran Industri Di Kabupaten Gresik. Yogyakarta