

PERANCANGAN PENGGUNAAN FIREWALL DAN PROXY SERVER UNTUK MEMBATASI HAK AKSES INTERNET

Nana Suryana¹, Dedi Dwi Saputra²

Teknik Informatika, Sekolah Tinggi Teknologi Indonesia
¹nanasuryanaparantina@gmail.com; ²putra.tkd@gmail.com

Abstract :The development of computer technology and information is very fast, especially on the provision of computer networks become very important for institutions especially Vocational High School, Institute and University. However, the impact of the development of information technology in line with the rising problems that can be arise such as : attacks on viruses, spam, spyware and others. In addressing the issue, the presence of pornographic sites and others can lower morale, especially for students, due to easy access of the internet. In this case it is also possible that the performance of lecturers and staff in using information systems and learning proses will be destroyed and can reduce the performance of the computer network. Firewall using iptables on proxy server and uses Squid Proxy with Ubuntu Linux Server that has been implemented in the Laboratory. Also can be used for various access to access computer network. With the fastest speed of internet access, then the access sites that are not useful for students and lectures will be block so the do not have access and make the security of the network more secure.

Key word : Network, Internet, Security

Abstrak : Perkembangan teknologi komputer dan informasi sangat cepat khususnya pada penyediaan jaringan komputer menjadi sangat penting sekali untuk institusi khususnya Sekolah Menengah Kejuruan, Institute dan Universitas. Namun, dampak dari perkembangan teknologi informasi sejalan dengan meningkatnya pula masalah yang dapat timbul seperti : penyerangan virus, spam, spyware dan lainnya. Dalam menyikapi masalah tersebut, kehadiran situs-situs pornografi dan lainnya dapat menurunkan moral, terutama untuk mahasiswa, dikarenakan mudahnya akses internet. Dalam kasus ini juga dimungkinkan unjuk kerja dari para dosen dan pegawai dalam menggunakan sistem informasi dan proses pembelajaran akan dihancurkan dan dapat menurunkan unjuk kerja dari jaringan komputer tersebut. Firewall menggunakan iptables pada proxy server dan menggunakan Proxy Squid dengan Server Linux Ubuntu yang telah di implementasikan di Laboratorium. Juga dapat digunakan berbagai akses untuk mengakses jaringan komputer. Dengan kecepatan akses internet yang sangat cepat, maka pada akses situs-situs yang tidak bermanfaat dan berguna bagi mahasiswa dan dosen akan di block sehingga mereka tidak mempunyai akses, sehingga menjadikan keamanan dari jaringan yang lebih aman.

Kata kunci: jaringan, internet, keamanan

I. PENDAHULUAN

Pesatnya perkembangan teknologi informasi (TI) dan komputerisasi saat ini, terutama berkaitan dengan jaringan komputer merupakan komponen yang sangat penting bagi instansi pendidikan. Saat ini para mahasiswa-mahasiswi dan dosen dapat memanfaatkan teknologi ini untuk pembelajaran TI dan tentunya

informasi selalu *up-to-date* tentang dunia pendidikan. Namun, dampak dari perkembangan teknologi informasi itu adalah semakin banyaknya permasalahan yang muncul antara lain: serangan *virus*, *spam*, *spyware*, dan lain sebagainya. Selain serangan-serangan tersebut, kehadiran situs-situs pornografi, dan lainnya akan dapat merusak moral khususnya bagi mahasiswa-mahasiswi

dikarenakan mudahnya akses internet tersebut. Dengan hal ini dimungkinkan pula kinerja dosen dalam pembelajaran maupun informasi yang tersampaikan akan terganggu dan kinerja jaringan dapat menurun. Sebuah jaringan komputer perlu memiliki “*tembok atau pagar*” layaknya sebuah bangunan rumah, yang dapat melindungi tempat vital dalam komunikasi data dan menyimpan komponen penting akan jaringan komputer tersebut. Dalam istilah komputer, “*tembok/pagar*” tersebut sering disebut dengan istilah *firewall*.

Pengerjaan penelitian tersebut akan memanfaatkan sebuah alat untuk menyaring situs-situs yang boleh diakses oleh pengguna jaringan internet serta menggeblok situs-situs yang “dilarang” untuk diakses oleh mahasiswa-mahasiswi dan dosen.

II. KAJIAN LITERATUR

Sebuah lembaga tidak mungkin mengambil resiko kehancuran sistem komputerisasi yang telah ada. Untuk menghindari hal itu, maka diperlukan suatu sistem keamanan yang kuat. Dengan menggunakan *firewall* maka beberapa komputer yang terhubung ke *internet* akan dapat memproteksi jaringan internal terhadap serangan dari jaringan eksternal yang akan merusak sistem jaringan yang terhubung ke *internet*. Sistem keamanan jaringan dapat menghindari kehilangan data dari ancaman *hacker* atau serangan *virus*, *spam*

2.1 Intranet

Intranet adalah sebuah jaringan *private network* yang menggunakan protokol (*TCP/IP*) yang digunakan untuk berkomunikasi dan berbagi informasi dalam lingkup tertentu dengan area yang terbatas. Untuk membagi informasi rahasia perusahaan atau operasi dalam perusahaan tersebut kepada karyawan. Istilah *intranet* hanya merujuk kepada layanan yang terlihat yakni, situs web internal perusahaan. *Intranet* dapat juga disebut “jaringan *internet* pribadi” yang berskala lebih kecil dibandingkan *internet*. Hal-hal yang harus dimiliki ketika akan

membangun jaringan *intranet* yaitu beberapa komponen yang membangun *internet*, berupa protokol (*TCP/IP*, alamat IP, dan protokol lainnya), *client*, dan juga *server*.

Yang mengacu kepada kebutuhan informasi dalam bentuk web di dalam perusahaan. *Intranet* merupakan jaringan komputer dalam perusahaan yang menggunakan komunikasi data standar seperti dalam *internet*. *Intranet* digunakan untuk membantu alat dan aplikasi, misalnya kolaborasi dalam kerja sama (untuk memfasilitasi bekerja dalam kelompok dan telekonferensi) atau direktori perusahaan yang sudah canggih, penjualan dan alat manajemen hubungan dengan pelanggan, manajemen proyek, dan untuk memajukan produktivitas.

2.2 Internet

Internet (interconnection networking) adalah seluruh jaringan komputer yang saling terhubung menggunakan standar (*TCP/IP*) sebagai protokol pertukaran paket data untuk melayani milyaran pengguna diseluruh dunia. *Internet* banyak dimanfaatkan sebagai sumber informasi, tentang apa saja dalam jumlah yang tidak terbatas. Sebagai pengguna *internet* kita dapat memanfaatkan internet untuk mencari informasi apa saja yang dibutuhkan secara luas. *Internet* juga merupakan media komunikasi yang sangat handal dan murah. Dapat mengirimkan informasi keseluruhan dunia dalam hitungan detik dengan biaya yang sangat kecil dibanding dengan biaya menggunakan media komunikasi yang lain.

2.3 Switch



Gambar 1. Perangkat Switch

Switch adalah sebuah alat jaringan yang melakukan penjemputan tak tampak (penghubung atau penyekat (*segmentation*)) banyak jaringan dengan pengalihan berdasarkan alamat *MAC*. Daripada melewatkan paket ke semua *port*, *switch* meneruskannya ke *port* yang dialamatkan. Jadi, *switch* dapat secara drastis mengurangi *traffic network*. *Switch* memelihara daftar *MAC address* yang dihubungkan ke port-portnya yang digunakan untuk menentukan kemana harus mengirimi paketnya.

2.4 Modem ADSL

Modem ADSL (*Asynchronous Digital Subscriber Line*) adalah perangkat yang digunakan untuk menghubungkan komputer atau *router* ke saluran telepon, untuk menggunakan layanan ADSL. Layaknya jenis modem lainnya, modem ADSL merupakan *transceiver*. Disebut juga dengan DSL transceiver atau ATU-R. Singkatan NTBBA (*Network Termination Broad Band Acces*) juga sering kali ditemui di beberapa negara.

Beberapa modem ADSL juga mengelola dan membagi sambungan dari layanan DSL dengan beberapa komputer. Dalam hal ini, modem ADSL berfungsi sebagai DSL router atau *residential gateway*. Blok di dalam DSL *router* ada yang bertugas dalam proses *framing*, sementara yang umum dijumpai pada ADSL modem adalah *Ethernet* dan USB. Meskipun modem ADSL bekerja dalam modus bridge dan tidak membutuhkan *IP address public*, modem ADSL tetap disertai *IP address* untuk fungsi *management* seperti alamat *IP* 192.168.1.1

2.5 Proxy Server

Proxy Server adalah sebuah komputer *server* atau program komputer yang dapat bertindak sebagai komputer lainnya untuk melakukan *request* terhadap *content* dari *internet* atau *intranet*. *Proxy Server* bertindak sebagai *gateway* terhadap dunia *internet* untuk setiap komputer *client*. *Proxy Server* tidak terlihat oleh komputer *client*. Seorang pengguna yang berinteraksi dengan *internet* melalui sebuah *proxy server* tidak akan

mengetahui bahwa sebuah *proxy server* sedang menangani *request* yang dilakukannya. *Web server* menerima *request* dari *proxy server* akan menginterpretasikan *request-request* tersebut seolah-olah *request* itu datang secara langsung dari komputer *client*, bukan dari *proxy server*. *Proxy Server* juga dapat digunakan untuk mengamankan jaringan pribadi (*Intranet*) yang dihubungkan ke sebuah jaringan publik (*Internet*).

Proxy Server yang berfungsi sebagai sebuah "agen keamanan" untuk sebuah jaringan pribadi (*Intranet*). Umumnya dikenal sebagai (*Firewall*). *Proxy* dapat dipahami sebagai pihak ketiga yang berdiri ditengah-tengah antara kedua pihak yang saling berhubungan dan berfungsi sebagai perantara, sedemikian sehingga pihak pertama dan pihak kedua tidak secara langsung berhubungan, akan tetapi masing-masing berhubungan dengan perantara, yaitu *Proxy*.

Adapun fungsi dari suatu *proxy* dalam komunikasi jaringan komputer dan internet. *Proxy server* mempunyai 3 fungsi utama, yaitu : *Connection Sharing*, *Filtering* dan *Caching*. *Proxy* dalam pengertiannya sebagai perantara, bekerja dalam berbagai jenis protokol komunikasi jaringan dan dapat berada pada level-level yang berbeda pada hirarki layer protokol komunikasi jaringan. Suatu perantara dapat saja bekerja pada layer *Data-Link*, layer *Network* dan layer *Transport*, maupun layer aplikasi dalam hirarki layer komunikasi jaringan menurut OSI.

Jaringan lokal yang terhubung ke jaringan lain atau *internet*, pengguna tidak langsung berhubungan dengan jaringan luar atau *internet*, tetapi harus melewati suatu *gateway*, yang bertindak sebagai batas antara jaringan lokal dan jaringan luar. *Gateway* ini sangat penting, karena jaringan lokal harus dapat dilindungi dengan baik dari bahaya yang mungkin berasal dari *internet*, dan hal tersebut akan sulit dilakukan bila tidak ada garis batas yang jelas jaringan lokal dan *internet*.

2.6 Linux

Linux adalah nama yang diberikan kepada sistem operasi komputer bertipe *unix*. *Linux* merupakan salah satu contoh hasil pengembangan perangkat lunak bebas dan sumber terbuka utama (*open source*). Adapun manfaat dari sistem operasi *linux*, adalah sebagai berikut :

1. *Linux* merupakan sistem operasi bebas dan terbuka (*open source*).
2. *Linux* mudah digunakan karena distro *linux* sudah mendukung GUI (*Graphic User Interface*) dan juga *user friendly*.
3. Hampir semua aplikasi yang terdapat pada *windows*, telah terdapat alternatifnya di *linux* karena banyak komunitas-komunitas pengembangnya, semisal *source-forget.net*, atau bila terpaksa kita bisa menjalankan *software* untuk *windows* di *linux* dengan bantuan *emulator* seperti *wine* sehingga file ekstension (*.*exe*) dan (*.*msi*) dapat dijalankan.
4. Keamanan lebih tangguh, karena proteksi *password* yang kuat
5. *Linux* *relative* stabil, *linux* dapat di install di spesifikasi *hardware* yang rendah. Perangkat keras yang lama dapat dijalankan dengan baik di *linux*.
6. *Linux* mempunyai kompatibilitas ke belakang yang lebih baik (*better-backward-compatibility*).
7. Perangkat keras yang telah berusia lama, masih sangat berguna dan dapat dijalankan dengan baik di atas *linux*. Selain itu, tidak pernah ditemui dokumen-dokumen yang lebih baru tidak dapat dibaca pada *linux* versi yang lebih lama.
8. Dukungan komunitas yang beragam dan menyebar diseluruh dunia.
9. *Linux* selain gratis untuk digunakan, gratis pula untuk dimodifikasi dan didistribusikan ulang.
10. *Linux* membutuhkan *resource* yang lebih kecil dari *windows*, sehingga cocok untuk komputer dengan spesifikasi minimal. Selain itu hampir semua distro populer menyediakan versi 32 bit maupun 64 bit.
11. Lebih dari 80% dari atas 500 superkomputer di dunia menjalankan *Linux*.

12. *Linux* sangat kuat bahasa scripting yang memberikan kekuatan besar untuk sistem administrator.

2.7 Firewall

Firewall adalah suatu mekanisme untuk melindungi keamanan jaringan komputer dengan menyaring paket-paket data yang keluar dan masuk di jaringan. Paket data yang "baik" diperbolehkan untuk melewati jaringan dan paket data yang dianggap "jahat" tidak diperbolehkan untuk melewati jaringan. *Firewall* dapat berupa perangkat lunak atau perangkat keras yang ditanam didalam perangkat lunak yang dapat memfilter paket data.

Firewall juga berfungsi untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Keamanan jaringan komputer tetap akan terjaga dengan disaringnya paket data yang keluar dan masuk.

Fungsi *Firewall*, Antara lain :

1. Mengontrol dan mengawasi paket data yang mengalir
Firewall harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan *private* yang dilindungi oleh *firewall*. *Firewall* harus dapat melakukan pemeriksaan terhadap paket data yang akan melewati jaringan *private*.
Beberapa kriteri yang akan dilakukan *firewall* apakah memperbolehkan paket data lewat atau tidak, antara lain : Alamat IP dari komputer sumber, Port TCP/UDP sumber dari sumber, Alamat IP dari komputer tujuan dan Port TCP/UDP tujuan data pada komputer tujuan.
2. Melakukan autentikasi terhadap akses
Firewall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntut *firewall* untuk mampu mendeteksi protocol aplikasi tertentu atau spesifikasi.
3. Mencatat semua kejadian di jaringan
Memungkinkan membantu sebagai pendeteksian dini akan kemungkinan pengebolan didalam jaringan.

2.8 Topologi Jaringan

Topologi Jaringan adalah suatu konsep untuk menghubungkan beberapa atau banyak komputer sekaligus menjadi suatu jaringan yang saling terkoneksi. Setiap macam topologi akan berbeda dari segi kecepatan pengiriman data, biaya pembuatan, serta kemudahan dalam proses maintainencenya. Juga setiap jenis topologi jaringan komputer memiliki kelebihan serta kekurangannya masing-masing. Jenis-jenis topologi antara lain topologi ring, topologi star, topologi bus, topologi *mesh* dan topologi *tree*.

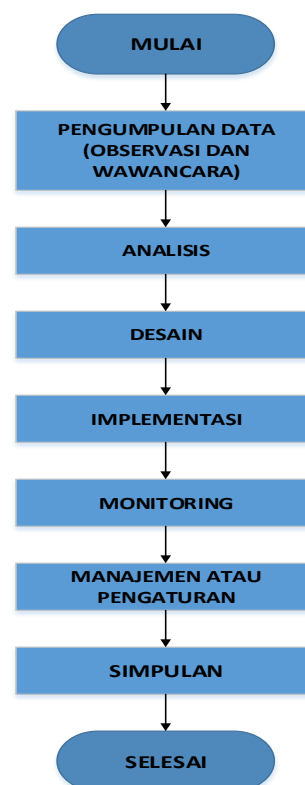
III. METODOLOGI PENELITIAN

3.1 Metode Penelitian

Metode penelitian yang digunakan penulis adalah metode *Network Development Life Cycle* (NDLC). Dengan metode ini bertujuan mempunyai fase, tahapan, langkah atau mekanisme proses merancang jaringan komputer dengan baik dan benar. Dengan mengacu pada model penelitian ini penulis melakukan pendekatan dalam kegiatan penelitian sebagai berikut :

1. Analisis merupakan tahap awal peneliti melakukan, analisa permasalahan yang muncul, analisa topologi jaringan yang sudah ada saat ini.
2. Desain data yang didapatkan sebelumnya, pada tahap desain ini akan membuat gambar desain topologi jaringan interkoneksi yang akan dibangun, diharapkan dari gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada.

3. Implementasi menggunakan spesifikasi rancangan sebagai masukan prosesnya untuk menghasilkan keluaran yang telah dihasilkan. Pada tahap sebelumnya dimana berupa instruksi penerapan sistem secara nyata yang terbagi menjadi dua bagian, yaitu "konfigurasi dan analisis". Yang meliputi proses instalasi dan konfigurasi terhadap rancangan topologi jaringan dan komponen pada ruang.
4. Monitoring atau Pengawasan terhadap efektivitas kinerja dari sistem yang sudah dibangun atau diterapkan, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari *user* pada tahap awal analisis maka perlu melakukan kegiatan pemantauan atau pengawasan terhadap sistem yang telah dibuat.
5. Manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah *policy*. Kebijakan perlu dibuat untuk membuat atau mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan terjaga.



Gambar 2 Flow Chart NDLC

3.2 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Observasi

Observasi merupakan metode yang dilakukan dengan cara mengamati langsung objek yang berhubungan langsung dengan judul penulis. Dalam hal ini penulis melakukan pengamatan secara langsung ke lokasi. Hal ini bertujuan untuk memperoleh data yang akurat tentang kondisi yang ada pada saat ini. Dalam proses observasi, dilakukan pendokumentasian hal-hal penting yang berkaitan dengan proses analisis jaringan, seperti : jumlah pengguna, aplikasi yang dibutuhkan nantinya, penggunaan dan peralatan yang dipakai, tingkat keamanan jaringan serta seberapa penting jaringan yang dibutuhkan

2. Wawancara

Wawancara merupakan metode yang dilakukan untuk mendapatkan data yang akurat, dengan melakukan wawancara untuk mengetahui tata cara dalam mengolah jaringan komputer yang selama ini digunakan. Untuk mendukung hal tersebut dalam hal ini melakukan wawancara langsung kepada asisten laboratorium. Hasil dari wawancara tersebut mendokumentasikan tentang topologi jaringan yang sudah ada di tempat yang menjadi objek penelitian, baik topologi fisik maupun logis.

a. Informasi yang dicatat dalam pendokumentasian topologi logis dari hasil wawancara adalah sebagai berikut : kema untuk IP (*internet protocol*) *addressing*, konfigurasi *sharing* dan *bandwidth* modem Speedy Telkom.

b. Informasi yang dicatat dalam pendokumentasian topologi fisik dari hasil wawancara adalah sebagai berikut : Lokasi fisik dari peralatan seperti *modem speedy*, *switch*, dan *host*, bagaimana peralatan tersebut saling terkoneksi serta jalur dan panjang kabel atau media transmisi lainnya.

IV HASIL DAN PEMBAHASAN

4.1 Analisa Permasalahan

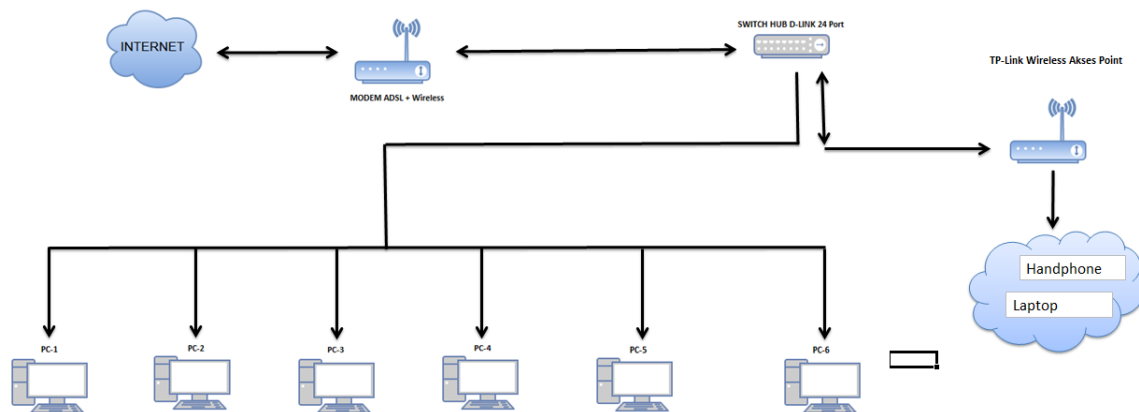
Berdasarkan hasil wawancara dan observasi pada saat pengumpulan data penelitian, ditemukan permasalahan yang terjadi pada laboratorium yaitu :

1. Dengan mudahnya mengakses *internet* di ruang laboratorium, hal tersebut dapat mengganggu kegiatan belajar dan mengajar yang berjalan pada saat di ruang laboratorium.
2. Selain dapat mengganggu kegiatan belajar dan mengajar, ancaman lain ialah serangan *virus*, *spam*, dan *spyware* melalui media *internet* yang dapat merusak sistem komputer *client*. Belum lagi ditambah dengan kehadiran situs-situs pornografi yang dapat merusak moral mahasiswa/i yang sedang belajar, karena minimnya keamanan jaringan yang diterapkan di ruangan tersebut. Dengan hal ini dimungkinkan pula kinerja dosen yang mengajar pada saat di ruang laboratorium akan terganggu dan kinerja jaringan dapat menurun.
3. Pada saat *client-A* mengirimkan data ke *client-B* proses pengiriman data tersebut menggunakan *bandwidth*, dan hal ini dapat berdampak kepada *client* lainnya yang sedang mengakses *internet*. Karena tidak ada pemisah antara jaringan *internet* dan *intranet*.

Untuk mendapatkan apa yang dibutuhkan pada saat penelitian, melakukan analisa pada ruang laboratorium dengan pengamatan langsung.

4.2 Analisa Topologi Jaringan

Pada gambar 3 menjelaskan topologi jaringan komputer pada ruangan laboratorium. Media yang digunakan perangkat sistem informasi pada jaringan komputer menggunakan jaringan *local area network* (LAN) dengan menggunakan kabel UTP, modem ADSL Telkom TD-W8951ND, *switch D-Link DGS-1024 D 24 Port*, *TP-Link Wireless access point* dan dengan *bandwidth up to 3Mbps*, yang berguna untuk fasilitas layanan *internet*.



Gambar 3 Kondisi Topologi Awal (Lama)

4.3. Analisa Perangkat Keras

Penggunaan sistem komputer sebagai alat bantu dalam menyelesaikan pekerjaan sudah bukan menjadi hal yang aneh, tapi merupakan suatu keharusan karena banyak kemudahan-kemudahan yang bisa diperoleh. Komputer terdiri perangkat keras dan perangkat lunak. Perangkat keras yang digunakan dalam penelitian ini penulis menggunakan perangkat keras, antara lain :

1. Personal komputer *environment server*, spesifikasi : *Processor Intel® Core™2 Duo*, *VGA On Board*, *LAN On Board*, *RAM 2 GB DDR3*, *Hard Disk 160 GB* dan *External Ethernet Card TP-Link 1000Mbps*
2. Personal komputer *client side*, spesifikasi : *Processor Intel® Core™2 Duo*, *VGA On Board*, *LAN On Board*, *RAM 2 GB DDR3* dan *Hard Disk 160 GB*

4.4 Analisa Perangkat Lunak

Perangkat keras berfungsi jika diberikan instruksi-instruksi kepadanya. Instruksi-instruksi inilah disebut dengan perangkat lunak. Dalam penelitian ini penyusun menggunakan beberapa perangkat lunak, antar lain:

1. Sistem operasi *Linux Ubuntu* versi 16.10 (*Xenial Xerus*) 64 bit digunakan dalam pengembangan sistem ini, sebagai *environment server* dimana rule-rule pada *firewall* dan *proxy server* akan diimplementasikan.
2. Sistem operasi *Microsoft Windows 7 Profesional 32 bit* digunakan sebagai *client*
3. *Squid* versi 3.5 Stable, digunakan sebagai *proxy server* yang akan diimplementasikan pada *environment server*.
4. *Netdata Monitoring*, digunakan untuk memantau *performance server*.
5. *Squid Analyzer*, digunakan untuk menganalisa trafik data yang masuk ke *proxy server*.
6. *OpenSSH*, digunakan untuk mendukung komunikasi terenkripsi pada jaringan komputer, menggunakan protocol *ssh*
7. *Xshell*, digunakan untuk *ssh* ke *environment server* untuk kebutuhan checking, dsb.

4.5 Analisa Sistem

Implementasi jaringan yang akan dibangun harus memenuhi beberapa persyaratan dibawah ini :

1. Implementasi ini terdiri dari jaringan *client-server*, yang dimana pada jaringan *client-server* memiliki akses lebih tinggi karena penyedia fasilitas jaringan dan pengelolannya dilakukan oleh satu komputer khusus

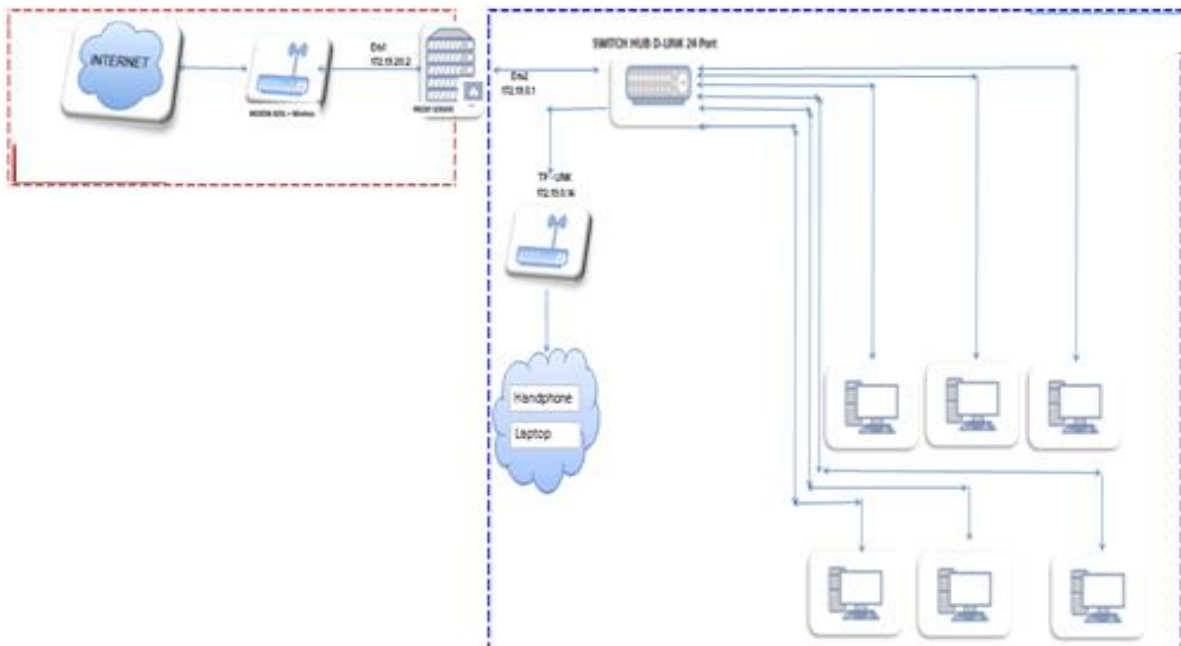
- yang tidak terbebani dengan tugas-tugas yang lain.
- 2. Komputer *server* sebagai media untuk pemisah antara jaringan internet dan jaringan intranet.
- 3. Komputer *server* sebagai *connection sharing*, yang dimana dapat memberikan layanan pada komputer *client* berupa *internet*.
- 4. Komputer *server* yang akan diimplementasi perlu diterapkan sebuah aturan untuk menentukan hak akses *internet* pada komputer *client*.
- 5. Komputer *server* memerlukan penyimpanan data sebagai *cache* yang harus disimpan di dalam komputer *server*.

- 6. Pada komputer *server* juga berfungsi sebagai sistem keamanan jaringan, hal ini memberikan rasa aman kepada *client* pada saat mengakses *internet*.

4.6 Perancangan Jaringan

Perancangan pada laboratorium terdapat 16 *client*, Akses *internet* menggunakan *speedy*, yang telah dibangun oleh *system administrator network*.

4.7 Perancangan Jaringan Baru



Gambar 3 Perancangan Jaringan Baru

Pada gambar 3 menjelaskan perancangan jaringan sesudah diimplementasi proxy server pada ruangan laboratorium. Media yang digunakan untuk membedakan koneksi *internet* dan *intranet* adalah sebuah komputer, yang dimana kabel UTP yang ditarik dari modem *speedy* di masukan kedalam port LAN on board *eth1* lalu di keluarkan melalui *eth2* kearah *switch D-Link DGS-1024 D 24 Port*. Setelah itu disebarakan ke *TP-Link wireless* dan personal komputer sebagai *client*.

4.8 Pembagian Jaringan Baru

Pada tahap ini melakukan pembagian jaringan yang telah dibangun. Adapun pembagian jaringan sebagai berikut :

Table 1. Pembagian Jaringan Proxy Server

Perangkat	IP Address	Keterangan
<i>Modem Speedy</i>	xxx.xx.xx.x	Gateway
<i>Proxy Server Ether-1</i>	xxx.xx.xx.x	<i>Interface-1 (internet)</i>
<i>Proxy Server Ether-2</i>	xxx.xx.xx.x	<i>Interface-2 (intranet)</i>

Table 2. Pembagian Jaringan Client

Perangkat	IP Address	Keterangan
Personal Komputer-1	xxx.xx.x.x	Client-1
Personal Komputer-2	xxx.xx.x.x	Client-2
Personal Komputer-3	xxx.xx.x.x	Client-3
Personal Komputer-4	xxx.xx.x.x	Client-4
Personal Komputer-5	xxx.xx.x.x	Client-5
Personal Komputer-6	xxx.xx.x.x	Client-6
Personal Komputer-7	xxx.xx.x.x	Client-7
Personal Komputer-8	xxx.xx.x.x	Client-8
Personal Komputer-9	xxx.xx.x.x	Client-9
Personal Komputer-10	xxx.xx.x.x	Client-10
Personal Komputer-11	xxx.xx.x.x	Client-11
Personal Komputer-12	xxx.xx.x.x	Client-12
Wifi Laboratorium	xxx.xx.x.x	Client-13

4.8 Instalasi dan Konfigurasi

Hal-hal yang dilakukan selanjutnya adalah :

1. Instalasi Linux Ubuntu 16.04 (*Xenial Xerus*)
2. Konfigurasi IP
3. Konfigurasi *Routing*
4. Konfigurasi *Firewall*
5. Instalasi dan Konfigurasi *Squid*
6. Instalasi dan Konfigurasi *Monitoring Tools*, yakni :
 - a. Instalasi dan Konfigurasi *Netdata Monitoring*
 - b. Instalasi dan Konfigurasi *Squid analyzer*
7. Tips dan Trik
Untuk menghindari adanya pencurian akses internet secara *illegal*, pada laboratorium dengan metode *deep penetration testing (intruder)*. Maka, cara mengatasinya sebagai berikut :
 - a. Non aktifkan *service ip forwarding* pada file *"/etc/sysctl.conf"*, seperti gambar dibawah ini :
 - b. Kemudian lakukan *restart server* dengan perintah *"init 6"*

8. Pengujian Sistem

- a. Uji Coba Struktural
Uji coba struktural dilakukan dengan menjalankan jaringan untuk mengetahui kesesuaian struktur jaringan yang telah dibuat dalam perancangan, dalam hal ini menjalankan hasil akses internet berdasarkan alur yang ada dalam perancangan jaringan yang berjalan dengan baik dan sesuai dengan rancangan desain
- b. Uji Coba Fungsional
Setelah uji coba struktural berhasil maka dilanjutkan dengan uji coba fungsional dimana dilakukan pengujian fungsi-fungsi yang telah dimasukkan pada saat pendeteksian dan jaringan sebelumnya apakah berjalan atau tidak. Diantaranya dilakukan test koneksi dari *server proxy* ke *internet*, dari *client* ke *server proxy*, dan dari *client* ke *internet* (dalam 1 gateway). Dengan fungsi *ping* sehingga dapat mengetahui koneksi dapat berjalan dengan baik.
- c. Uji Coba Validasi
Uji coba validasi dilakukan untuk melihat hasil dari kesesuaian implementasi yang telah di terapkan adalah dengan cara akses dari *client* ke *internet* (akses url-url yang *block*).

5. KESIMPULAN

Perancangan komputer *proxy server* dengan menggunakan *squid stable version 3.5* untuk membatasi hak akses internet pada laboratorium. Berdasarkan hasil penelitian tersebut, dapat disimpulkan sebagai berikut :

1. Implementasi *proxy server* dapat dibuat dengan menggunakan *personal computer (PC)*, dengan sistem operasi linux Ubuntu 16.04 (*xenial xerus*).
2. *Firewall* yang diimplementasikan selain untuk keamanan pada *proxy server*, juga dikonfigurasi sebagai *routing* dan *connection sharing* untuk *client* agar mendapatkan koneksi *internet*.

3. *Proxy server* bertujuan untuk membuat koneksi *intranet*, memisahkan antara koneksi *internet* dan *intranet* pada laboratorium, melakukan ACL (*Access Control List*) *ip address* mana saja yang boleh melakukan akses interne serta memblokir situs-situs tertentu agar tidak dapat diakses oleh *client*.

DAFTAR PUSTAKA

- Haas, J. 2003, Squid-Proxy Server, http://www.linux.about.com/od/ubusrv_doc/a/ubusg26t01.html, diakses tanggal 05 Agustus 2016.
- Sully, B. 2010. IP Tables Firewall Script and Configuration File For Linux, http://www.linux.about.com/od/ubusrv_doc/a/ubusg26t01.html, diakses tanggal 05 Agustus 2016.
- Supriyanto, 2005. Step By Step Konfigurasi Squid Proxy Server dengan Berbagai Studi Kasus, http://www.linux.about.com/od/ubusrv_doc/a/ubusg26t01.html, diakses tanggal 05 Agustus 2016.
- Suyama,T. 2009. Proxy Server ,<http://www.belajarit.um.ac.id/index.php/jaringan/18-pengenalan-jaringan-komputer/43-proxy-server.html>, diakses tanggal 05 Agustus 2016.
- Veloso, Bryan. 2011. Squid, <http://stresslinuxs.wordpress.com/networking/squid-proxy/> diakses pada tanggal 05 Agustus 2016.
- Ubuntu Official Documentation, <https://help.ubuntu.com/community/Iptables> diakses pada tanggal 30 September 2016.
- Techmint, 2016. Real-Time Performance Monitoring Tool for Linux Systems, <http://www.tecmint.com/netdata-real-time-linux-performance-network-monitoring-tool/> diakses pada tanggal 01 November 2016.
- Rizal Rahman, 2014. Memonitoring kinerja squid proxy dengan squid analyzer di Ubuntu 12.04 server, <http://www.linuxku.com/2014/02/Memonitor-Kinerja-Squid-Proxy-dengan-Squid-Analyzer-di-Ubuntu-12-04-Server.html> diakses pada tanggal 01 November 2016.