ANALISA AKURASI *CONTENT FILTERING TOOLS* DALAM MENYARING SITUS-SITUS PORNO DI POLITEKNIK NEGERI SRIWIJAYA

R.A. Halimatussa'diyah[(1)], Yordan Hasan[(2)]
Staf Pengajar Jurusan Teknik Elektro Politeknik Negeri Sriwijaya
radenayu.winda@gmail.com
yordan_hasan@yahoo.com

ABSTAK

Sebagai media informasi dan komunikasi, internet memiliki manfaat dan kegunaan yang beragam. Beragam manfaat internet yang dewasa ini mulai memasuki segala sendi kehidupan manusia mulai bergeser ke arah yang oleh sebagian orang dikatakan negatif. Untuk mengatasi efek negatif internet tersebut, khususnya di kalangan pelajar dan mahasiswa, maka pemakaian internet perlu dibatasi dengan cara membatasi (filtering) kontent yang bisa diakses. Penelitian ini dimaksudkan untuk mengetahui tingkat keakuratan C*ontent Filtering Tools* yang pernah digunakan di Politeknik Sriwijaya dengan cara melakukan pengujian terhadap *tolls* tersebut, yaitu squid proxy, Nawala dan Dans Gardians dalam memblok situs-situs yang tidak diijinkan untuk diakses, khususnya yang memiliki konten pornography. Penelitian ini dilakukan dengan cara mengimplementasikan beberapa *content filtering tools* yaitu squid Proxy, Nawala dan DansGuardian, kemudian menguji *tools* tersebut dalam memblokir muatan-muatan pornography melalui beberapa tipe akses, yaitu melalui URL langsung, google web dan google *translate*. Data hasil pengujian tersebut kemudian dianalisa untuk mendapatkan kesimpulan *tool* yang mana yang memiliki kinerja terbaik dalam menyaring muatan-muatan pornography tersebut. Dari ketiga *content filtering tools* yang diuji keakuratannya didapatkan hasil DansGardian yang paling akurat dalam memblok situs-situs porno di Politeknik Negeri Sriwijaya. Namun demikian penggunaan DansGardian dalam menyaring konten pornography menyebabkan penurunan kinerja jaringan dari sisi waktu serta dibutuhkan resource yang besar, khususnya kapasitas server.

Kata Kunci : Keamanan Jaringan, Teknik-teknik Filtering, Content Filtering Tools.

ABSTRACT

As an information and communication media, the Internet has a variety of benefits and uses. Various benefits of the Internet today began entering all the human life aspects which is began to shift towards what some people say negative. To overcome the negative effects of the Internet, particularly among students, the use of the Internet needs to be restricted by limiting (filtering) content accessed. This reseach aimed to determine the level of accuracy of the Content Filtering Tools that has been used at the Polytechnic Sriwijaya by conducting tests on the tools : the Squid proxy, Nawala and Dans Gardians to block sites that are not permitted to be accessed, particularly those with pornography content. The research was conducted by implementing some content filtering tools Squid Proxy, Nawala and DansGuardian, then testing these tools in blocking pornography content over certain types of access, through direct URL, google web and google translate. The test results data are then analyzed to come to the conclusion which tool has the best performance in filtering the pornography content. Among the three tested content filtering tools obtained that DansGardian was the most accurate in blocking porn sites on the State Polytechnic of Sriwijaya. However the use of DansGardian in filtering pornography content will decrease network performance in terms of time and required a great resource, especially the capacity of the server.

Keywords : Network security, Filtering Techniques, Content Filtering Tools

I. PENDAHULUAN

1.1. Latar Belakang

Internet saat ini mulai menjadi sebuah kebutuhan bagi sebagian masyarakat Indonesia. Biaya yang relatif murah dan kebutuhan akan akses internet dan jaringan telekomunikasi yang luas, serta berbagai macam koneksi yang ditawarkan *provider* internet merupakan penyebab berkembangnya pengguna internet di indonesia.

Sebagai media informasi dan komunikasi, internet memiliki manfaat dan kegunaan yang beragam. Beragam manfaat internet yang dewasa ini mulai memasuki segala sendi kehidupan manusia mulai bergeser kearah yang oleh sebagian orang dikatakan negatif, antara lain dengan semakin banyaknya situs-situs porno yang beredar di internet yang menyebabkan efek negatif internet menjalar ke kalangan anak di bawah umur.

Untuk mengatasi efek negatif internet tersebut, khususnya di kalangan pelajar dan mahasiswa, maka pemakaian internet perlu dibatasi dengan cara membatasi *(filtering)* muatan-muatan yang bisa diakses.

Beberapa penelitian menunjukkan bahwa beberapa aplikasi untuk *filtering content* saat ini sangat bervariasi (Houghton, 2008). Namun, filter-filter tersebut masih belum memiliki kemampuan untuk mengevaluasi dan menentukan secara tepat isi yang sebenarnya dari konteks halaman web, termasuk teks, gambar, video, dan banyak lagi. Akibatnya, kinerja filter sangat tergantung pada pengakuan *content* buatan program, campur tangan manusia secara administrasi, pengaturan yang dipilih, dan fitur.

Penelitian ini pun dimaksudkan untuk mengetahui tingkat keakuratan C*ontent Filtering Tools* yang pernah digunakan di Politeknik Negeri Sriwijaya dengan cara melakukan pengujian terhadap *tolls* tersebut, yaitu squid proxy, Nawala dan DansGuardian dalam memblok situs-situs porno.

1.2. Perumusan Masalah

Dari latar belakang di atas, penulis merumuskan masalah bagaimana tingkat keakuratan beberapa *tools filtering content* yang pernah dan sedang digunakan di Politeknik Sriwijaya yaitu squid proxy, Nawala dan DansGardians dalam menyaring muatan yang berbau pornography melalui beberapa tipe akses, yaitu akses URL, google web dan google *translate.*

1.3. Tujuan Penelitian

Penelitian ini bertujuan untuk menganalisa keakuratan beberapa *content filtering tools* di Politeknik Sriwijaya dalam memfilter muatan-muatan yang berbau pornography melalui beberapa tipe akses.

1.4. Manfaat Penelitian

Penulis berharap penelitian ini bisa menjadi acuan bagi pengelola jaringan di Politeknik Negeri Sriwijaya dalam menentukan aplikasi yang sebaiknya digunakan dalam memblok situs-situs porno.

1.5. Metode Pembahasan

Penelitian ini penelitian eksperimental untuk menguji keakuratan *content filtering tools* yang digunakan di Poiteknik Negeri Sriwijaya dalam memblok situs-situs porno. Penelitian ini dilakukan pada web server pusat Politeknik Negeri Sriwijaya.

Adapun populasi yang terlibat pada penelitian ini adalah situs-situs porno yang ada di internet dan sampel yang diambil sebanyak 205 situs berdasarkan informasi yang diterima dari berbagai sumber. Analisa yang disampaikan adalah analisa terhadap perbandingan keakuratan *content filtering tools* yaitu Nawala, proxy dan DansGuardians dalam memblok situs-situs porno tersebut, baik jika akses dilakukan melalui akses langsung ke URL, melalui google web ataupun melaui google terjemahan.

II. LANDASAN TEORI

2.1. Pengertian Jaringan Komputer

Jaringan komputer diartikan sebagai suatu himpunan interkoneksi sejumlah komputer yang dapat saling bertukar informasi (Raharjo, 2005). Bentuk koneksinya tidak harus malalui kabel saja melainkan dapat menggunakan serat optik, atau bahkan satelit komunikasi.

Dilihat dari ruang lingkup jangkauannya, jaringan komputer dibedakan menjadi: *Local Area Network (LAN), Metropolitan Area Network (MAN), dan Wide Area Network (WAN)* (Wijaya, 2003).

LAN merupakan suatu jaringan komunikasi yang saling menghubungkan berbagai jenis perangkat dan menyediakan pertukaran data diantara perangkat-perangkat tersebut. Biasanya *LAN* menggunakan pendekatan jaringan *broadcast* lebih dari pada pendeteksian *switching*. Dengan *broadcast communication network*, tidak ada *node-node* penengah. Pada masing-masing station terdapat sebuah *transmitter / receiver* yang menghubungkan media dengan *station* lain. Sebuah transmisi dari satu *station* disiarkan dan diterima oleh semua *station* lain. Data biasanya ditansmisikan dalam bentuk paket. Karena medianya dibagi, maka hanya ada satu *station* pada saat itu yang dapat mentransmisikan paket.

Wide Area Networks (WAN) dan *Metropolitan Area Network (MAN)* umumnya mencakup area yang luas sekali, melintasi jalan umum dan perlu juga menggunakan fasilitas umum. Biasanya suatu *WAN* terdiri dari sejumlah *node* penghubung. Suatu transmisi dari suatu perangkat diarahkan melalui *node-node* atau persimpangan -persimpangan internal menuju perangkat tujuan. *Node-node* ini tidak berkaitan dengan isi data, melainkan dimaksudkan untuk menyediakan fasilitas *switching* yang akan memindahkan data dari suatu *node* ke *node* yang lain sampai mencapai tujuan.

2.2. Prinsip Dasar Protokol

Model referensi jaringan terbuka *OSI* atau *Reference Model* untuk *open networking* adalah sebuah model arsitektural yang dikembangkan oleh badan International Organization for Standardization (ISO) di Eropa pada tahun 1974. Selain Model OSI, model jaringan yang lain adalah TCP/IP. (Purbo, Basamalah, Ismail, Thamrin, 1999)

2.2.1. Model OSI

Protokol model OSI terdiri dari 7 *layer* (lapisan) (George, 2006). *Physical Layer* berfungsi dalam pengiriman *raw bit* ke channel komunikasi. Masalah desain yang harus diperhatikan disini adalah memastikan bahwa bila satu sisi mengirim data 1 bit, data tersebut harus diterima oleh sisi lainnya sebagai 1 bit pula, dan bukan 0 bit. Selain itu, *layer* ini juga mendefinisikan bagaimana *Network Interface Card (NIC)* dapat berinteraksi dengan media kabel atau radio.

Data Link Layer menangani bingkai *(frame)* data antara jaringan dengan *Physical layer* . Pada

penerimaan akhir, *layer* ini mem -paket data mentah dari *Physical layer* kedalam bingkai data untuk pengiriman ke *Network layer*.

Network layer berfungsi untuk pengendalian operasi subnet, mendefinisikan alamat-alamat IP, membuat *header* untuk paket-paket, dan kemudian melakukan routing melalui internetworking dengan menggunakan router. Masalah desain yang penting adalah bagaimana caranya menentukan route pengiriman paket dari sumber ke tujuannya.

Fungsi dasar *Transport Layer* adalah menerima data dari *session layer*, memecah data menjadi bagian-bagian yang lebih kecil serta memberikan nomor urut ke paket-paket tersebut, meneruskan data ke *network layer*, dan menjamin bahwa semua potongan data tersebut bisa tiba di sisi lainnya dengan benar. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses *(acknowledgement*), dan mentransmisikan ulang terhadp paket-paket yang hilang di tengah jalan.

Session layer mengijinkan para pengguna untuk menetapkan *session* dengan pengguna lainnya. Sebuah session selain memungkinkan transport data biasa, seperti yang dilakukan oleh *transport layer*, juga menyediakan layanan yang istimewa untuk aplikasi-aplikasi tertentu

Presentation layer berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Layer ini bertanggung jawab bagaimana data dikonversi dan diformat untuk transfer data. Contoh konversi misalnya format text ASCII untuk dokumen, .gif dan JPG untuk gambar

Layer ke-7 / *application layer*, memberikan suatu antarmuka bagi *end-user* yang mengoperasikan peranti yang terhubung ke jaringan. Layer ini merupakan "apa yang *user* lihat", dalam konteks *loading* aplikasi (seperti web browser atau email); yang mana, *application layer* ini merupakan data yang *user* lihat selama menggunakan aplikasi dalam jaringan.

2.2.2. Model TCP/IP

TCP/IP terdiri atas sekumpulan protokol yang masing-masing bertanggung jawab atas bagian-bagian tertentu dari komunikasi data. Atas prinsip ini, tugas masing-masing protokol menjadi jelas dan lebih sederhana. Protokol yang satu tidak perlu mengetahui cara kerja protokol yang lain, sepanjang ia masih bisa saling mengirim dan menerima data. (Purbo at all, 1999, 21-23)

Karena penggunaan prinsip ini, TCP/IP menjadi protokol komunikasi data yang fleksibel. Protokol TCP/IP dapat diterapkan dengan mudah disetiap jenis komputer dan *interface* jaringan, karena sebagian besar isi protokol ini tidak spesifik terhadap satu komputer atau peralatan jaringan tertentu. Agar TCP/IP dapat berjalan di atas jaringan *interface* jaringan tertentu, hanya perlu dilakukan perubahan pada protokol yang berhubungan dengan *interface* jaringan saja. Sekumpulan protokol TCP/IP ini dimodelkan dengan empat layer TCP/IP

Application Layer (SMTP, FTP, HTTP, dll)
Transport Layer (TCP, UDP)
Internet Layer (IP, ICMP, ARP, dll)
Network Interface Layer (SMEthernet,X25,SLIP,PPP)

Gambar 2.1. Protokol TCP/IP

2.3. Teknik-teknik *Filtering* (Wolfgarten, 2006)

2.3.1. Network-Level Filtering

Network-level filtering adalah penyaringan atau *packet filtering* yang beroperasi pada lapisan 3 dan 4 model OSI. Setiap paket diperiksa secara *realtime* saat melewati perangkat penyaringan (misalnya router) dan berdasarkan isi dari header. Jenis penyaringan ini telah lama digunakan dan dilaksanakan dalam sebagian besar perangkat yang tersedia saat ini.

a. *Layer 3 filtering*

Network Layer (layer 3) dari model OSI terutama bertanggung jawab untuk pengalamatan logis dan routing data dan berisi informasi (misalnya alamat IP) sumber dan tujuan paket. Dengan menggunakan informasi, seseorang dapat mendefinisikan aturan untuk memblokir paket-paket tertentu berdasarkan alamat sumber dan / atau tujuan dan dengan demikian mencegah komunikasi apapun dari dan ke suatu host.

Misalnya aturan untuk menolak semua trafik TCP dan UDP dari atau ke alamat IP 212.158.224.81 yang berhubungan dengan website BBC :

deny ip host 212.58.224.81 any
deny ip any host 212.58.224.81

b. *Layer 4 filtering*

Layer 4 *(transport layer)* adalah terutama bertanggung jawab atas format dan penanganan transportasi data dengan cara transparan. Layer 4 menyediakan pengiriman data yang handal dan akurat ke lapisan berikutnya dan menggunakan protokol seperti TCP, UDP dan ICMP. Kedua protokol TCP dan UDP termasuk informasi (yaitu nomor port) dan jenis layanan (misalnya port 80 untuk HTTP). Contoh penyaringan pada layer 4 di Cisco-sintaks.

Deny tcp any host 213.133.109.150 eq 25

Dalam contoh ini, lalu lintas dari semua host dengan port sumber apapun ke port tujuan 25 (SMTP) pada 213.133.109.150 ditolak. Jika aturan tersebut

disebarkan, setiap host terpengaruh oleh penyaringan ini tidak mampu berkomunikasi dengan host 213.133.109.150 pada port 25 (yaitu mengirim email ke host itu). Meskipun penyaringan lapisan 4 menawarkan fleksibilitas yang lebih besar dan ketepatan dalam hal lingkup penyaringan, juga dapat memblokir akses ke sumber daya yang seharusnya tidak seharusnya diblok (overblocking). Misalnya suatu server HTTP dengan satu IP tunggal mungkin melayani beberapa (hingga ratusan atau ribuan) website, karenanya jika akses ke server web diblokir, maka akses ke semua website lain yang di-host pada server yang sama juga akan diblokir.

2.3.2. *Application-level Filtering*

Tidak seperti *network-level filtering, application-level filtering* diterapkan di layer 7 (layer aplikasi) dari model OSI. Oleh karena itu adalah mungkin untuk memeriksa dan menganalisis payload atau isi dari sebuah paket dan karenanya melakukan inspeksi yang sangat rinci pada data sebelum membuat keputusan filtering. Hal ini memungkinkan penyaringan yang akan diterapkan di protokol, bukan pada network level.

Selain itu seperti *network level filtering, application-level filtering* sering menyediakan cara untuk menginformasikan kepada *user* tentang proses *filtering*. Namun karena setiap paket harus diperiksa, dianalisa dan kemungkinan dieksekusi atau kadang-kadang bahkan kembali, *application-level filtering* tidak dapat dilakukan di *real-time* dan terutama di lingkungan dengan *bandwidth* yang tinggi membutuhkan sejumlah besar peralatan yang sangat mahal agar tetap praktis. Selanjutnya jika sebuah protokol terenkripsi secara tepat seperti *Secure Socket Layer* (SSL) atau *Secure Shell* (SSH) digunakan, *application-level filtering* kebanyakan menjadi mustahil karena muatan dari trafik jaringan ditransfer dalam bentuk yang sudah dienkripsi, dengan demikian tidak dapat diperiksa lagi.

1. Proxy

Aplikasi proxy firewall (sering hanya disebut sebagai "Proxy" atau "proxy server") beroperasi pada lapisan aplikasi model OSI dan bertindak sebagai perantara dalam menahan dan menanggapi permintaan antara hosts. 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.

Analogi di atas menjelaskan konsep dan fungsi dasar dari suatu proxy dalam komunikasi jaringan komputer dan internet. Proxy server mempunyai 3 fungsi utama yaitu *Connection Sharing*, *Filtering* dan *Caching.*

a. Connection Sharing

Karena proxy bekerja pada layer aplikasi, proxy server dapat berjalan pada banyak aplikasi antara lain HTTP Proxy atau Web Proxy untuk protokol HTTP atau Web, FTP Proxy, SMTP/POP Proxy untuk email, NNTP proxy untuk Newsgroup, Real Audio / Real Video Proxy untuk *multimedia streaming*, IRC proxy untuk *Internet Relay Chat (IRC)*, dan lain-lain. Masing-masing hanya akan menerima, meneruskan atau melakukan filter atas paket yang dihasilkan oleh layanan yang bersesuaian.

b. Filtering

Dalam suatu 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 antara jaringan lokal dan internet. Gateway juga bertindak sebagai titik dimana sejumlah koneksi dari pengguna lokal akan terhubung kepadanya, dan suatu koneksi ke jaringan luar juga terhubung kepadanya. Dalam hal ini, gateway adalah juga sebagai proxy server, karena menyediakan layanan sebagai perantara antara jaringan lokal dan jaringan luar atau internet.

Karena firewall melakukan *filtering* berdasarkan suatu daftar aturan dan pengaturan akses tertentu, maka lebih mudah mengatur dan mengendalikan trafik dari sumber-sumber yang tidak dipercaya. Firewall juga melakukan *filtering* berdasarkan jenis protokol yang digunakan (TCP,UDP,ICMP) dan port TCP atau UDP yang digunakan oleh suatu layanan (semisal telnet atau FTP). Sehingga firewall melakukan kendali dengan metode boleh lewat atau tidak boleh lewat, sesuai dengan daftar aturan dan pengaturan akses yang dibuat.

c. Caching

Fungsi dasar yang ketiga dan sangat penting dari suatu proxy server adalah *caching.* Proxy server memiliki mekanisme penyimpanan obyek-obyek yang sudah pernah diminta dari server-server di internet, biasa disebut *caching.* Karena itu, proxy server yang juga melakukan proses *caching* juga biasa disebut *cache server*.

Mekanisme *caching* akan menyimpan obyek-obyek yang merupakan hasil permintaan dari para pengguna, yang didapat dari internet. Karena proxy server bertindak sebagai perantara, maka proxy server mendapatkan obyek-obyek tersebut lebih dahulu dari sumbernya untuk kemudian diteruskan kepada peminta yang sesungguhnya. Dalam proses tersebut, proxy server juga sekaligus menyimpan obyek-obyek tersebut untuk dirinya sendiri dalam ruang disk yang disediakan (cache).

2. *Deep Packet Inspection*

Teknik lain untuk membentuk *filtering content* pada level aplikasi adalah menggunakan '*deep packet inspction'* yang berhubungan dengan kemampuan suatu firewall atau IDS dalam memeriksa suatu paket atau

traffic stream dan membuat keputusan yang signifikan pada data tersebut berdasarkan isi dari data tersebux1.

3. *DNS Filtering*

Domain Name System (DNS) adalah *distribute database system* yang digunakan untuk pencarian nama komputer (*name resolution*) di jaringan yang mengunakan TCP/IP (*Transmission Control Protocol/ Internet Protocol).* DNS biasa digunakan pada aplikasi yang terhubung ke Internet seperti web browser atau e-mail, dimana DNS membantu memetakan *host name* (misalnya www.dcu.ie) ke IP address yang sesuai (misalnya 136.206.1.2) . Meskipun tidak pernah dimaksudkan untuk digunakan sebagai mekanisme penyaringan, tetapi saat ini menjadi salah satu pilihan cara memblokir suatu akses karena kesederhanaan dan efektivitas dalam hal manipulasi yang dapat dilakukan.

Dornseif adalah orang pertama pertama yang mempelajari teknik ini pada tahun 2003 dan mengidentifikasi enam teknik untuk melakukan *DNS filtering*, yaitu

a. Ditolak: Cara termudah untuk menghentikan pengguna dari menghubungkan ke host tertentu adalah hanya menolak terhadap akses ke suatu *domain*. Oleh karena itu DNS standar mendefinisikan jawabannya "DITOLAK" yang berarti bahwa "nama server menolak untuk melakukan operasi tertentu. Dalam hal ini, pesan kesalahan yang disampaikan dapat berupa "host tidak ditemukan" atau "koneksi ditolak" ..
b. Nxdomain: suatu manipulasi di mana keberadaan dari sebuah domain tertentu ditolak ("NXDOMAIN, *non-existing domain* ") oleh *rekursif DNS server provider*. pesan kesalahan "host tidak ditemukan" akan mencegah pengguna dari terhubung ke host target.
c. Pembajakan Nama (Name hijacking) : Mengacu pada modifikasi yang disengaja di mana permintaan pengguna untuk menuju domain tertentu dijawab dengan data palsu. Hal ini biasanya akan mengakibatkan pengguna yang sengaja diarahkan ("Dibajak") ke situs lain.
d. Pembatalan Nama (*Name Invalidation*) : Teknik yang mirip dengan "pembajakan nama"di mana domain yang dituju dinyatakan tidak valid. Hal ini akan menampikan pesan kesalahan "Tidak bisa menghubungkan". Dornseif mengacu metode ini sebagai " *name astrayment* ".
e. Diam : Cara lain untuk menolak akses ke domain tertentu adalah diam, tidak menanggapi permintaan tersebut sama sekali. Hal ini akan mengakibatkan keterlambatan atau kehabisan batas waktu dan akhirnya akan penampilkan pesan kesalahan “host tidak ditemukan”.
f. *Provoked server failer* : Jenis gangguan ini akan menyebabkan pesan kegagalan server akan dikirim ke klien yang mencoba untuk menuju suatu domain tertentu. Maka pengguna akan menerima pesan kesalahan (misalnya "tidak bisa terhubung") dan tidak akan dapat terhubung ke domain yang dituju.

2.4. Penelitian Sebelumnya

Beberapa penelitian telah dilakukan terhadap aplikasi-aplikasi ataupun teknik-teknik dalam proses *filtering content* dipandang dari sudut teknis. Sebastian Wolfgarten dalam tulisannya ‘Investigating large-scale Internet content filtering’, memaparkan hasil analisanya terhadap proses *filtering content* internet dalam skala luas dan mengadakan investigasi langsung terhadap kondisi internet di RRC. Ia memaparkan bahwa teknik *filtering* dapat dilakukan berdasarkan tingkatan yang berbeda yaitu network level filtering dan application level filtering. *Network level filtering* yaitu filtering yang dilakukan pada layer 3 dan 4 model OSI, sedangkan *application level filtering* dilakukan pada layer 7 model OSI dengan menggunakan proxy server, *deep packet inspection*, dan DNS manipulations.

Mayur Lodha dalam tulisannya ‘Web Content Filtering” membandingkan teknik-teknik *filtering content* antara teknik *web filtering content* dan teknik *email filtering content*. Teknik *filtering* web dapat dilakukan dengan menggunakan firewall, filtering berdasarkan URL, dan *keyword scanning*. Sedangkan teknik *filtering* email umumnya dilakukan secara manual dengan mendeteksi email yang merupakan spam.

III. METODOLOGI

Penelitian ini merupakan penelitian eksperimental yang dilakukan untuk mengetahui keakuratan 3 *content filtering tools* yang digunakan untuk memblok situs-situs porno di politeknik Negeri sriwijaya.

3.1. Pengukuran dan cara pengamatan variabel

Pengkuran dilakukan berdasarkan tingkat keberhasilan *content filtering tools* tersebut dalam memblok situs-situs porno, baik jika akses dilakukan melalui akses langsung ke URL, melalui google web ataupun melaui google terjemahan.

3.2. Teknik dan analisa data

Analisa data pada tesis ini dilakukan berdasarkan persentse keberhasilan beberapa *content filtering tools* yaitu Nawala, Proxy dan, DansGuardian dalam memblok situs-situs porno di Politeknik Negeri Sriwijaya melalui beberapa cara pengaksesan .

IV. HASIL DAN PEMBAHASAN

4.1. Data Hasil Pengujian

Data hasil pengujian terhadap 205 situs porno yang coba diblok oleh 3 content filtering tools dapat dilihat pada tabel 4.1. berikut .

Tabel 4.1. Jumlah Situs Porno yang Bisa diakses .

Akses	Nawala	Proxy	Dans Gardians
URL	23	163	2
Google web	1	0	0
Google translate	52	2	1
jumlah	76	165	3

Pengujian terlebih dahulu dilakukan melalui akses langsung ke URL, bila tidak berhasil maka dicoba melalui google web dan jika tidak berhasil juga, maka dilakukan akses melalui google *translate.*

Dari Tabel 4.1. terlihat bahwa untuk jaringan yang hanya menggunakan Nawala sebagai *content filtering tool*, akses terhadap situs porno sebagian besar masih bisa dilakukan, di mana dari 205 situs porno yang dicoba, 23 situs berhasil diakses langsung melalui URL nya, 1 akses berhasil dilakukan melalui google web, sedangkan 52 berhasil diakses melalui google *translate* setelah sebelumnya dicoba melalui akses langsung dan google web. Sehingga jumlah semua situs yang bisa diakses saat Nawala terpasang adalah 76 situs porno.

Untuk penggunaan *filtering tool* yang hanya menggunakan Proxy, 163 situs porno dapat diakses secara langsung melalui URL dan 2 situs dapat dilakukan melalui google *translate* Sehingga semua situs yang dapat diakses saat proxy terpasang sebanyak 165 situs..

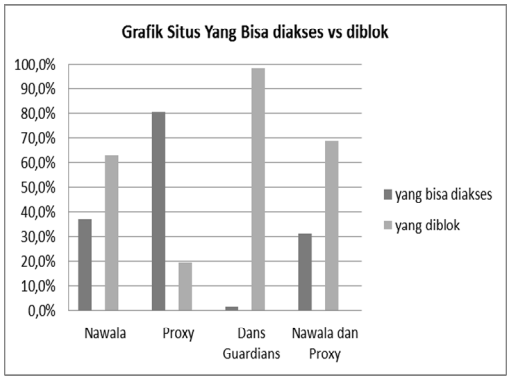
Untuk pengujian keakuratan *content filtering tool* DansGuardian, hanya 3 situs yang dapat diakses dari 205 situs porno yaitu 2 situs melalui akses URL langsung dan 1 situs melalui google *translate.*

V. ANALISIS DAN PEMBAHASAN

Tabel 5.1. berikut menunjukkan perbandingan (persentase) antara jumlah situs porno yang berhasil diakses (gagal diblok) oleh masing-masing *tools* dengan jumlah situs porno yang berhasil diblok oleh *tools* tersebut.

Tabel 5.1. Perbandingan Jumlah Situs yang bisa diakses vs yang diblok

	Yang bisa diakses		Yang diblok	
Nawala	76	37,1%	129	62,9%
Proxy	165	80,5%	40	19,5%
Dans Guardians	3	1,5%	202	98,5%
Nawala + Proxy	64	31,2%	141	68,8%



Gambar 5.1. Grafik Perbandingan Keberhasilan Proses Blocking Situs Porno

5.1. Analisis Kinerja Proxy

Dari hasil pengujian terhadap 3 *content filtering tools* yang pernah digunakan di Poiteknik Negeri Sriwijaya yaitu Proxy, Nawala dan Dans Gardian terlihat bahwa penggunaan Proxy untuk memblok situs-situs porno sangat rendah. Hal ini dikarenakan Proxy hanya memblok berdasarkan keyword dan URL yang kita daftarkan pada list, sehingga dengan berkembang dan bertambahnya situs-situs pornografi maka sebagian besar situs-situs porno tersebut bisa diakses (Vlachos, Karakoidas, 2010). Untuk pemakaian Proxy sebagai *content filtering tool*, dibutuhkan admin yang aktif, sehingga update list terhadap keyword dan URL yang berisi *content* porno dapat terus dilakukan. Sedangkan pengamatan dari sisi waktu, proses loading ataupun blocking lebih cepat waktunya dibandingkan jika kita menggunakan Nawala dan DansGardian.

5.2. Analisis Kinerja Nawala

Untuk penggunaan Nawala sebagai *content filtering tool* terlihat lebih baik dari proxy, tetapi hasil yang didapatkan juga belum maksimal, karena 37,1% dari situs porno yang diuji, masih dapat diakses. Hal ini dikarenakan Nawala tidak hanya memblok berdasarkan URL yang ada di *list* tetapi juga semua yang mengarah ke domain (URL) yang dinilai mengganggu termasuk spam, situs-situs yang menyediakan '*open proxy*' juga dapat di blok (http://www.nawala.org/) .

5.3. Analisis Kinerja DansGuardian

Untuk penggunaan DansGuardian sebagai *content filtering tool* hasilnya lebih akurat dalam memblok situs-situs porno dibandingkan Proxy dan Nawala. Dimana dari hasil pengujian 98,5 % berhasil diblok. Hal ini dikarenakan selain DansGuardian memiliki white list dan black list, DansGuardian pun melakukan update terhadap *whilte list* dan *black list* dengan sendirinya (Houghton, 2010). Hanya saja pemakaian DansGuardian membutuhkan sumber daya yang besar mengingat prinsip kerja DansGuardian dalam menyaring paket data sangat kompleks dan

membutuhkan memori yang besar, apalagi untuk trafik yang padat.

Dari pengamatan selama proses pengujian, proses loading suatu situs saat DansGuardian terpasang lebih lama dibanding menggunakan Proxy dan Nawala. Selain mempunyai kemampuan dalam hal *content filtering*, DansGuardian juga mempunyai *feature* untuk *picture filtering (*Houghton, 2010). Hal ini juga menyebabkan lamanya loading suatu situs saat DansGuardian terpasang sehingga hal ini akan mempengaruhi kinerja jaringan yang menjadi lambat saat *loading* ataupun *browsing* suatu situs.

VI. KESIMPULAN DAN SARAN

6.1. Kesimpulan

Dari ketiga *content filtering tools* yang diuji keakuratannya didapatkan hasil DansGardian yang paling akurat dalam memblok situs-situs porno di Politeknik Negeri Sriwijaya. Tetapi pemasangan DansGuardian menyebabkan penurunan kinerja jaringan dari sisi waktu. Karena dari hasil pengamatan selama proses pengujian terlihat proses loading ataupun browsing suatu situs akan membutuhkan waktu yang lama. tidak seperti pada saat Proxy atau Nawala ataupun Proxy + Nawala terpasang bersama-sama.

Pemakaian Proxy sebagai content filtering tool membutuhkan admin yang aktif sehingga dapat mengupdate content list yang akan diblok. Sedangkan dari sisi waktu, pemakaian proxy lebih efisien karena selama proses pengujian, loading ataupun browsing terhadap suatu situs tidak membutuhkan waktu yang lama seperti saat DansGuardian terpasang.

6.2. Saran

Perlu ditinjau ulang pemakaian *content filtering tool* linux firewall squid Proxy dan Nawala untuk pemblokiran terhadap situs-situs porno di Politeknik Negeri Sriwijaya, mengingat dengan menggunakan *tools* tersebut masih banyak situs-situs porno yang berhasil diakses.

Untuk mendapatkan hasil yang lebih akurat, perlu juga dilakukan pengujian terhadap situs-situs porno berupa situs lokal & internasional melalui *keyword* dalam 2 bahasa yaitu Indonesia dan Inggeris.

Dari hasil pengujian penulis menyarankan untuk menggunakan DansGuardian sebagai *content filtering tool* untuk memblok situs-situs porno di Politeknik Negeri Sriwijaya. Tetapi dikarenakan jumlah *user* yang ada dan trafik jaringan yang begitu padat, maka penggunaan DansGuardian ini membutuhkan *resource* yang besar terutama server, sehingga perlu juga dikembangkan perancaan IT untuk mendukung infrastruktur yang dibutuhkan.

DAFTAR PUSTAKA

Duraiswamy K., G Palanivel, '*Intrusion Detection System in UDP Protocol'*, IJCSNS International Journal of Computer Science and Network Security, vol.10 No.3. March 2010.

Gheorghe Lucian, 2006, *Designing and Implementing Linux Firewalls and QoS using netfilter, iproute2, NAT, and L7-filter*, Birmingham – Mumbai.

Jan Sarah Houghton, *Internet Filtering software Test*, Digital Futures Senior Librarian, Original Report Submitted February 4, 2008, Revised report submitted April 2, 2008. www.sjlibrary.org/about/sjpl/commision/agen0208_report.pdf di akses tanggal 25 oktober 2010.

Loda, Mayur 'Web Content Filtering', mdl2130@columbia.edu diakses 29 Oktober 2010.

Purbo Onno W., Bassalamah Adnan, Fahmi Ismail, Thamrin Achmad Husni, 1999, *TCP/IP Standar, Desain dan Implementasi*, cetakan kedua, Elex Media Komputindo, Jakarta.

Rahardjo Budi, 2005, *Keamanan Sistem Informasi Berbasis Internet*, Versi 5.4,P. Insan Infonesia-Bandung.

Soelistijanto DS. Bambang, '*Analisis Status Port TCP Dalam Implementasi Sistem Keamanan Jaringan*', SIGMA, Vol.6.No 1, Januari 2003:51-61, ISSN : 1410-5888.

Vlachos Vasileios, Karakoidas Vassilos, '*Chapperone : a content filtering web proxy based on public health policies'*, diakses 29 Oktober 2010

Wijaya Hendra, 2003, *Cisco Router*, Elex Media Komputindo, Jakarta.

Wolfgarten Sebastian, 2006, '*Investigating large-scale Internet content filtering, sbastian@wolfgorton.com*. Diakses 29 Oktober 2010.

Anonim, http://www.nawala.org/ , diakses 29 Oktober 2010.