PEMFILTERAN *HYPERTEXT TRANSFER PROTOCOL SECURE* UNTUK PENGGUNAAN INTERNET YANG AMAN

Dian Novianto

Program Studi Teknik Informatika, STMIK ATMA LUHUR
Jl. Jenderal Sudirman Selindung, Pangkalpinang
diannovianto@atmaluhur.ac.id

ABSTRACT

The purpose of this study is to find out the best method to protect the computer network from virus attack that include in downloaded contents. Beside that, this research also aims to protect the connection to https. Data collection is done by observation and literature study. Method used in this research is experimental research, by trial and error to find the proper composition to do filtering. The result shows that squid proxy has no effect on https. In the other hand, if squid is collaborated by diladele web safety also does not affect the virus content. The collaboration of squid, diladele web safety and c-icap affects on filtering of https connection and virus content.

Key words: filtering, squid, diladele web safety, c-icap

ABSTRAK

Tujuan dari penelitian ini yaitu untuk mengamankan jaringan dari *virus* yang terkandung pada konten yang didownload. Selain itu juga dari penggunaan internet dengan koneksi melalui protokol *https* agar sesuai dengan ketentuan yang berlaku. Dalam penelitian ini pengumpulan data dilakukan dengan cara observasi dan studi pustaka, sedangkan metode penelitian yang digunakan adalah metode penelitian eksperimental, mencoba beberapa variabel untuk menemukan komposisi yang tepat dalam melakukan *filtering*. Dari hasil ujicoba yang dilakukan *squid proxy* tidak berpengaruh terhadap protokol *https*, sedangkan *squid* yang dikolaborasikan dengan *diladele web safety* tidak berpengaruh terhadap konten *virus*, kolaborasi antara *squid, diladele web safety* dan *c-icap* berpengaruh terhadap pemfilteran dari koneksi protokol *https* dan konten yang mengandung virus.

Kata Kunci: *filtering, squid, diladele web safety, c-icap*

1. PENDAHULUAN

Salah satu yang bisa diakses di internet adalah alamat *website*, Menurut *Coupey*, *website* adalah suatu jaringan dari dokumen-dokumen elektronik yang disebut halaman *web*, yang isinya dapat berupa teks, grafis, dan bahkan format suara dan format video [1]. *Web* ini menyediakan informasi bagi pemakai komputer yang terhubung ke internet dari sekedar informasi yang tidak berguna sama sekali sampai informasi yang serius, dari informasi yang gratisan sampai informasi yang komersial. Untuk

membatasi akses jaringan lokal yang akan mengakses suatu alamat website yang terdapat di internet, salah satu tekniknya dengan menjadikan *proxy server* sebagai filter dengan menggunakan aplikasi *squid proxy*, kita dapat melakukan pembatasan akses atau pemblokiran pada URL *web* tertentu. Fitur inilah yang saat ini banyak digunakan untuk memblokir beberapa URL *website* yang tidak dikehendaki untuk diakses. Namun pemblokiran pada *proxy* sering kali tidak efektif terlebih untuk koneksi dengan enkripsi pada HTTPS. Protokol HTTPS dirancang untuk menyediakan sarana komunikasi yang aman antara internet browser dan web server. Untuk mencapai tujuan ini protokol HTTPS mengenkripsi data melalui koneksi yang disediakan sehingga tidak dapat didekripsi dalam jumlah waktu yang wajar sehingga mencegah orang lain yang berniat mengambil data melalui koneksi ini.

Hal ini mungkin tidak selalu diinginkan oleh administrator jaringan. Isi yang biasanya diblokir tiba-tiba menjadi segera dapat diakses oleh siapa saja. Sebagai contoh sebuah jaringan sekolah di mana anak-anak dapat melihat konten yang dilarang karena hanya salah ketik istilah pencarian di *Google*. Apalagi hukum sering memaksa administrator untuk memblokir akses ke konten tersebut. Misalnya CIPA (*Children's Internet Protection Act* untuk lingkungan pendidikan di Amerika Serikat) sedangkan akses terenkripsi ke web membuat hampir tidak mungkin untuk memenuhi kewajiban tersebut. Saat ini banyak *website* yang telah menyediakan akses dengan HTTPS untuk meningkatkan privasi pengunjung mereka, hal itu juga menciptakan beberapa masalah untuk jaringan yang biasanya ditemukan di rumah atau kantor. Masalah utama di sini adalah inti dari protokol HTTPS sendiri tidak ada seorang pun kecuali browser dan web server mampu melihat dan mentransfer data.

Atas dasar efektifitas penggunaan *proxy server* sebagai filtering pada jaringan inilah saya tertarik untuk menjadi bahasan dalam penelitian ini. Dimana nantinya penulis akan melakukan uji coba dengan berbagai konfigurasi sehingga dapat memfilter koneksi https namun tetap menjaga privasi pengguna.

Sehubungan dengan masalah pada bagian pendahuluan, maka penulis merumuskan permasalahan dalam penelitian ini sebagai berikut:

"Bagaimana membuat sistem *filtering* menggunakan aplikasi *squid proxy* yang berfungsi dengan baik dalam melakukan *filtering* terhadap *website* untuk koneksi dengan protokol https"

Sesuai dengan permasalahan yang telah dirumuskan di atas, maka tujuan yang hendak dicapai dalam penelitian ini adalah untuk mengamankan jaringan terutama pada penggunaan internet dengan koneksi https agar sesuai dengan ketentuan yang berlaku.

Manfaat yang didapat dari penelitian ini adalah untuk melindungi privasi pengguna dan berkomunikasi dengan aman melalui media internet dengan menggunakan protokol *secure*, tetapi tidak melanggar peraturan yang ditetapkan oleh pemerintah maupun administrator jaringan.

Metode pengumpulan data yang dilakukan dalam penelitian ini adalah studi pustaka dan observasi. Studi pustaka merupakan teknik pengumpulan data dengan mengadakan studi penelaahan terhadap buku-buku, literatur-literatur, catatan-catatan, dan laporan-laporan yang ada hubungannya dengan masalah yang dipecahkan [2]. Disini penulis mengambil beberapa tulisan baik dari jurnal ataupun *website* yang berhubungan atau menunjang penelitian yang sedang penulis lakukan. Sedangkan observasi adalah pengujian dengan maksud atau tujuan tertentu mengenai sesuatu, khususnya dengan tujuan untuk mengumpulkan fakta, satu skor atau nilai, satu verbalisasi atau pengungkapan dengan kata–kata segala sesuatu yang telah diamati [3]. Penulis melakukan pengamatan pada jaringan internet pada saat berkomunikasi menggunakaan protokol http dan https untuk kemudian dicari teori – teori yang berkaitan dengan permasalahan tersebut.

2. METODE PENELITIAN

Pada penelitian ini penulis menggunakan metode penelitian eksperimental sebagai metode penelitian yang digunakan untuk mencari pengaruh perlakuan tertentu terhadap yang lain dalam kondisi yang terkendalikan [4]. Eksperimen merupakan modifikasi kondisi yang dilakukan secara sengaja dan terkontrol dalam menentukan peristiwa atau kejadian, serta pengamatan terhadap perubahan yang terjadi pada peristiwa itu sendiri.

Eksperimen pada intinya adalah pengamatan atau observasi terhadap hubungan kausal antara munculnya suatu akibat (variabel terikat) dan sebab (variabel bebas) tertentu, melalui suatu upaya sengaja yang dilakukan oleh peneliti [5].

2.1 DASAR TEORI

2.1.1 Proxy Server

Proxy server merupakan sebuah komputer atau kumpulan komputer yang diletakkan sebagai pelayanan pelanggan

(yang selanjutnya disebut klien) yang meminta pelayanan data baik dari pusat komputer (yang selanjutnya disebut dengan *Server*) ataupun dokumen web. Proxy server melayani komunikasi antara klien dan *server* yang dituju tanpa merubah permintaan ataupun balasan. Sebuah *proxy server* dapat melakukan penyaringan permintaan berdasarkan aturan-aturan yang telah dibuat dan memungkinkan komunikasi hanya jika permintaan diijinkan berdasarkan pada aturan-aturan yang telah dibuat dan disetujui dalam jaringan komputer. Aturan-aturan yang dibuat biasanya berdasarkan alamat berupa dns atau protokol internet (yang selanjutnya disebut IP Address) dari klien atau *server* tujuan[6].

2.1.2 Squid Proxy

Squid adalah *proxy caching* untuk Web yang mendukung koneksi HTTP, HTTPS, FTP, dan banyak lagi. Hal ini dapat mempercepat waktu respon sebuah website karena memiliki *caching* pada *proxy server* dan menggunakan kembali halaman web yang sering diminta oleh klien yang tersimpan didalam *cache proxy* [7]. Squid memiliki kontrol akses yang luas, salah satunya adalah melakukan filtering terhadap url atau konten sebuah website karena squid mempunyai pengaturan dalam bentuk ACL (*access Control List*).

2.1.3 Diladele Web Safety

Diladele Web Safety bertindak sebagai *server* ICAP yang dipasangkan dengan *Squid*. Skema penyebaran ini memungkinkan untuk penyaringan dan pemeriksaan mendalam pada SSL lalu lintas web yang terenkripsi melalui HTTPS ke situs yang difilter dan konten yang dilarang akan diblokir seperti pada HTTP normal [8].

2.1.4 C-ICAP

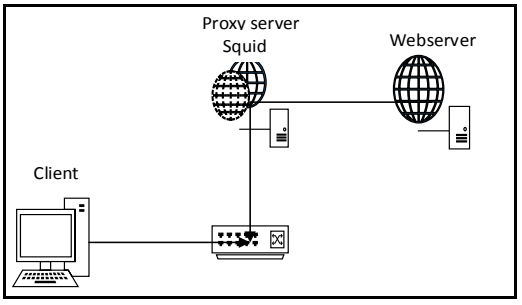
C-ICAP merupakan implementasi dari *server* ICAP dan dapat digunakan dengan proxy yang mendukung protokol ICAP untuk melaksanakan layanan adaptasi dan penyaringan konten [9].
Sebagian besar proxy komersial maupun gratis telah mendukung protokol ICAP. salah satunya Squid Server 3.x *opensource proxy* yang telah mendukungnya.

2.2 PERANCANGAN

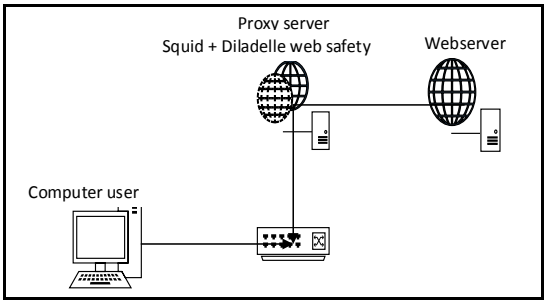
2.2.1 Skema Simulasi

Sebelum Melakukan ujicoba penulis mendesain beberapa skema simulasi berdasarkan data hasil observasi dan studi pustaka, agar sesuai dengan tujuan dari penelitian ini. Dimana akan ada tiga komputer yang bertindak sebagai *client,*

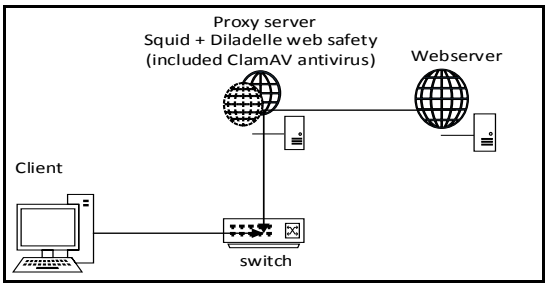
proxy server, dan *webserver*. Adapun skema pengujian dapat dilihat pada Gambar 1, Gambar 2., Gambar 3, dan Gambar 4.



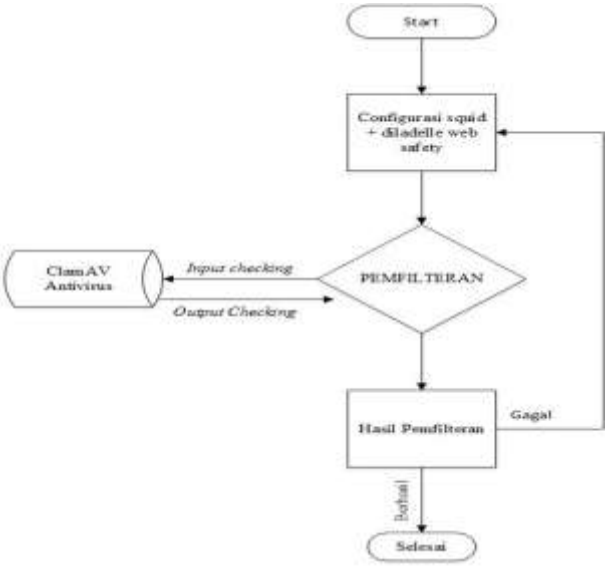
Gambar 1. Skema Pengujian 1



Gambar 2. Skema Pengujian 2



Gambar 3. Skema Pengujian 3



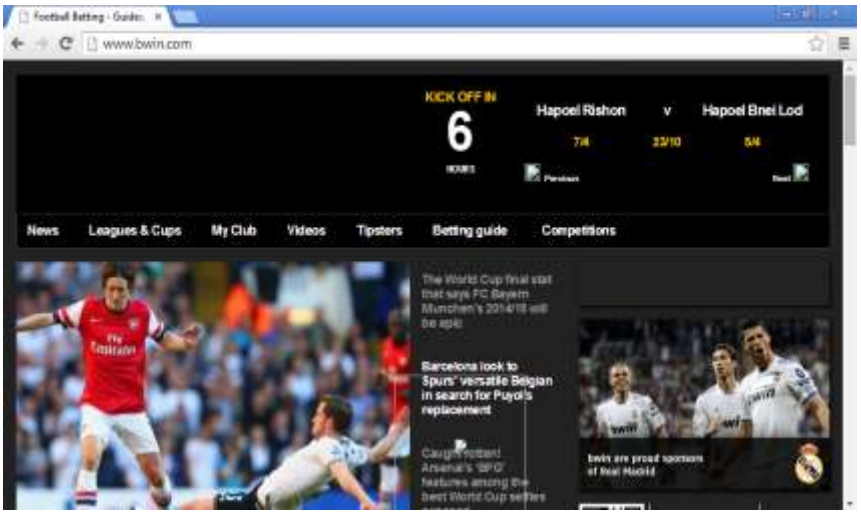
Gambar 4. Flowchart Pengujian

3. HASIL DAN PEMBAHASAN

Dari skema simulasi yang telah dirancang sebelumnya, untuk pembuktian dilakukanlah ujicoba seperti dibawah ini :

3.1 Pengujian Domain Dan Web Server

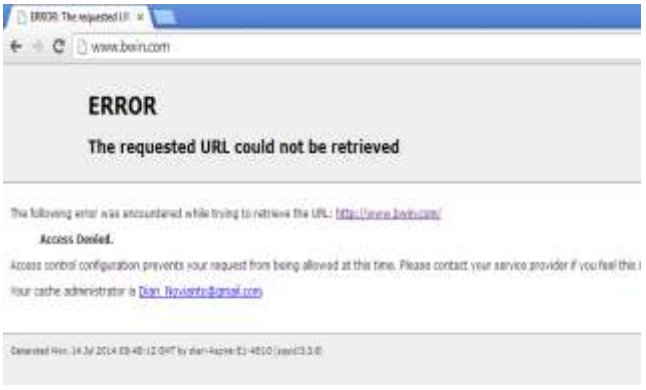
Pertama kali adalah konfigurasi *dns server* dan *web server*, ini dilakukan untuk mengetahui apakah klien bisa mengakses *website* yang telah disiapkan, dns disiapkan agar klien dapat mengakses melalui nama alamat *website* bukan melalui *ip address*, sedangkan *web server* dibutuhkan untuk menampung halaman web yang sudah disiapkan. Ketika ujicoba pertama dilakukan, klien mengirimkan permintaan melalui *web browser* ke alamat *website www.bwin.com* kepada *web server*, kemudian *web server* memberikan balasan dengan mengirimkan konten yang diminta oleh klien. Apabila klien dapat mengakses *website www.bwin.com* dengan lancar, artinya konfigurasi dari *dns server* dan *web server* sudah benar dan keduanya sudah bekerja dengan baik. Uji coba akses web dapat dilihat pada Gambar 5.



Gambar 5. Ujicoba akses web

3.2 Analisis Pemfilteran Http

Pada pengujian kedua *Squid proxy* di install dan dikonfigurasi untuk memfilter koneksi http antara klien dan server, untuk menguji bahwa konfigurasi yang dibuat telah berjalan dengan baik pada protokol http, dilakukan ujicoba kedua dari *web browser* klien yang mengirimkan permintaan kepada *proxy* untuk diteruskan ke *web server* dari alamat *website www.bwin.com*, dari ujicoba yang dilakukan *proxy* telah berjalan dengan baik seperti Gambar 6.



Gambar 6. Pengujian Squid

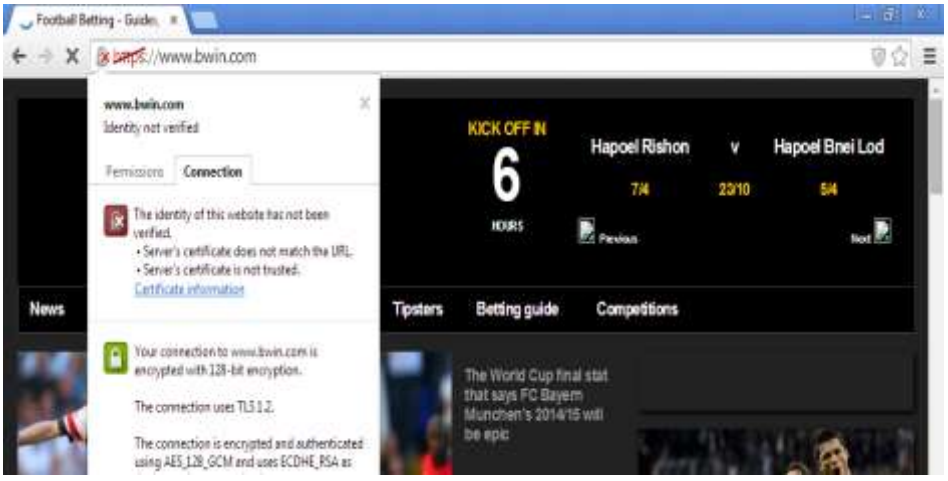
Berdasarkan Gambar 6. aplikasi *squid proxy* pada *proxy server* telah bekerja dengan baik sesuai dengan konfigurasi yang penulis lakukan sebelumnya, pada saat klien mengirimkan permintaan pada *proxy server* untuk mengakses *web server* dari *website www.bwin.com*, klien mengirimkan *header* permintaan, *http request* dikirimkan ke *proxy server*. *Header*

tersebut diterima aplikasi *squid proxy* dan dibaca, dari hasil pembacaan tersebut *squid proxy* akan memparsing url dan dicocokan dengan pengaturan *proxy server*.

3.3 Analisis Pemfilteran Https

Pada pengujian yang ketiga penulis telah memasang ssl (*secure socket layer)* pada *web server www.bwin.com* yang digunakan untuk enkripsi sambungan antara klien dan *web server*. Penulis menggunakan *OpenSSL* untuk membuat protokol secure, dimana *openssl* sendiri menggunakan enkripsi rsa (*Rivest, Shamir* dan *Adleman*).

Selanjutnya pengaksesan alamat *website www.bwin.com* melalui protokol https, yang terjadi selanjutnya adalah website yang tadinya bisa di filter oleh *squid proxy*, saat ini sudah bisa diakses oleh klien kembali, hal ini bisa dilihat pada Gambar 7.



Gambar 7. Uji Coba SSL

Hal tersebut dapat terjadi karena cara kerja *squid proxy* yang hanya memeriksa header permintaan dari klien, kemudian disesuaikan dengan pengaturan yang ada pada *proxy server* itu sendiri termasuk dalam hal ini *access control list*.

3.4 Analisis Pemfilteran Diladele Web Safety

Karena pada pengujian ketiga aplikasi *squid proxy* tidak dapat bekerja dengan baik, dilakukanlah konfigurasi selanjutnya yaitu kolaborasi antara *squid proxy* dan *diladele web safety*. *Diladele web safety* merupakan perangkat lunak yang mengadopsi konsep *internet content adaptation protocol* dan *Url rewriter* yang dapat dikolaborasikan dengan *squid proxy* 3.x, dimana *diladele web safety* mampu melakukan pemeriksaan mendalam dari enkripsi ssl lalu lintas web dan

menyesuaikan dengan pengaturan yang terdapat didalamnya. Dari konfigurasi tersebut penulis melakukan ujicoba terhadap koneksi dari *https www.bwin.com*, hasilnya dapat terlihat seperti Gambar 8.

Gambar 8. Pengujian Diladele

Berdasarkan pengujian diatas terbukti mampu memfilter koneksi https dari *website www.bwin.com*, untuk lebih meningkatkan keamanan sebagai *server icap diladele* yang dikonfigurasi dengan *squid proxy* kemudian diuji coba untuk memfilter konten yang mengandung virus yang diambil sampelnya dari website eicar.org.

3.5 Analisis Pemfilteran C-Icap

Pada Konfigurasi sebelumnya kolaborasi antara *squid proxy* dan *diladele web safety* belum mampu memfilter virus, maka untuk lebih meningkatkan keamanan dari jaringan lokal, dilakukan penambahan C-ICAP sebagai ICAP server yang berfungsi untuk memfilter konten yang mengandung virus. Cara kerja dari c-icap yaitu seluruh permintaan dari klien yang dikirimkan kepada *proxy server* akan diteruskan oleh *proxy server* kepada *c-icap server* untuk diproses oleh *service* yang tersedia, yaitu *service scanning virus* yang disediakan oleh modul c-icap. Setelah konfigurasi penulis lakukan, selanjutnya adalah ujicoba untuk mengetahui apakah c-icap bekerja dengan baik dan mampu memfilter konten yang mengandung virus, ujicoba dilakukan dengan mendownload sample virus dari *website eicar.org* seperti Gambar 9.

Gambar 9. Pengujian C-ICAP

Hasil dari pengujian tersebut dapat diketahui bahwa C-ICAP *server* yang mempunyai database info virus dari *ClamAv* mampu memfilter konten yang didownload yang diketahui mengandung virus.

4. SIMPULAN

Berdasarkan hasil pembahasan pada bagian sebelumnya di dapatkan beberapa kesimpulan yang dapat ditarik adalah untuk mencapai hasil yang di inginkan dalam penelitian ini yaitu pemfilteran https dan pemfilteran virus internet, tidak bisa hanya menggunakan salah satu perangkat lunak yang telah ditentukan, selain itu Kolaborasi antara *squid, diladelle web safety* dan C-Icap mampu memfilter https dan virus sesuai dengan tujuan dari penelitian ini.

DAFTAR PUSTAKA

[1] Coupey, Eloise. 2001. *Marketing and the Internet, Conceptual Foundation*. Prentice Hall.

[2] M. nazir, 2003. *Metode Penelitian*, Jakarta, Ghalia Indonesia, cet.ke-5.

[3] Chaplin, JP., *Kamus Lengkap Psikologi*, Terj. Dr. Kartini Kartono, Jakarta:

[4] Rajawali Pers, 2009.

[5] Sugiyono dalam Tjutju Soendari. *Penelitian Eksperimental*. Universitas Pendidikan Indonesia

[6] Tjutju Soendari. *Penelitian Eksperimental*. Universitas Pendidikan Indonesia.

[7] Thanki Kunal U and Patel Chirag R, 2012, Improve squid proxy's performance using new cache replacement architecture, International journal of management IT and Engineering, Vol.2 Issue 7.

[8] http://www.squid-cache.org/

[9] http://quintolabs.com/solution.php

[10] http://c-icap.sourceforge.net/