PEMFILTERAN HYPERTEXT TRANSFER PROTOCOL SECURE UNTUK PENGGUNAAN INTERNET YANG AMAN

Dian Novianto, PH. Saksono, Syahril Rizal

Magister Teknik Informatika
Universitas Bina Darma
Jl. A. Yani No. 12, Palembang 30624, Indonesia

Abstrak

Tujuan dari penelitian ini yaitu untuk mengamankan jaringan dari virus yang terkandung pada konten yang didownload serta pada 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: *Arsitektur teknologi informasi, cloud computing, perguruan tinggi*

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. Website atau situs dapat diartikan sebagai kumpulan halaman-halaman yang digunakan untuk menampilkan informasi teks, gambar diam atau gerak, animasi, suara, dan atau gabungan dari semuanya itu baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait dimana masing-masing dihubungkan dengan jaringan-jaringan halaman (hyperlink).

Untuk membatasi akses jaringan lokal yang akan mengakses suatu alamat website yang terdapat di internet, salah satu tekniknya dengan menjadikan proxy server sebagai filter-aplikasi squid proxy, kita dapat melakukan pembatasan akses atau pemblokiran pada URL situs tertentu. Fitur inilah yang saat ini banyak digunakan untuk memblokir beberapa URL

situs-situs 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. 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. 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 dalam lembaga pendidikan untuk memblokir akses ke konten tersebut misalnya CIPA (Children's Internet Protection Act untuk lingkungan pendidikan di Amerika Serikat) sedangkan akses terenkripsi ke situs web membuat hampir tidak mungkin untuk memenuhi kewajiban tersebut.

1.1 Identifikasi Masalah

Dari uraian pendahuluan diatas, diperlukan sistem proxy yang dapat berfungsi dengan baik untuk semua internet protokol yang ada terlebih untuk koneksi internet yang di enkripsi melalui protokol https.

1.2 Tujuan Penelitian

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.

1.3 Manfaat Penelitian

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.

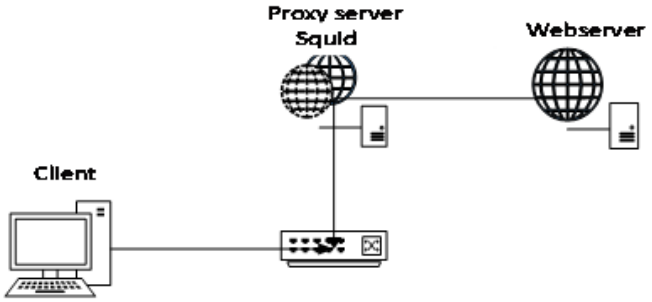
2 METODE PENELITIAN

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 [2]. 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 [3].

2.1 Metode Pengumpulan Data

penulis melakukan Studi pustaka dan observasi. Studi pustaka adalah pengumpulan data dengan cara membaca dan mengutip teori-teori yang berasal dari buku dan tulisan-tulisan lain yang relevan dengan penelitian ini. Disini penulis mengambil beberapa tulisan baik dari buku, jurnal ataupun website yang berhubungan atau menunjang penelitian yang sedang penulis lakukan. Sedangkan observasi adalah pengamatan dan pencatatan dengan sistematis atas fenomena-fenomena yang diteliti. Penulis melakukan pengamatan pada jaringan internet pada saat berkomunikasi menggunakaan protokol http dan https untuk kemudian dicari teori teori yang berkaitan dengan permasalahan tersebut.



Gambar 1: Skema Pengujian 1

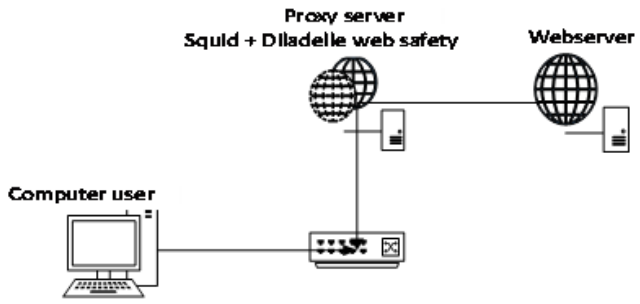
2.2 Skema Penelitian

penulis melakukan beberapa simulasi berdasarkan data hasil observasi dan studi pustaka, dimana ada tiga komputer yang bertindak sebagai client, proxy server, dan webserver.

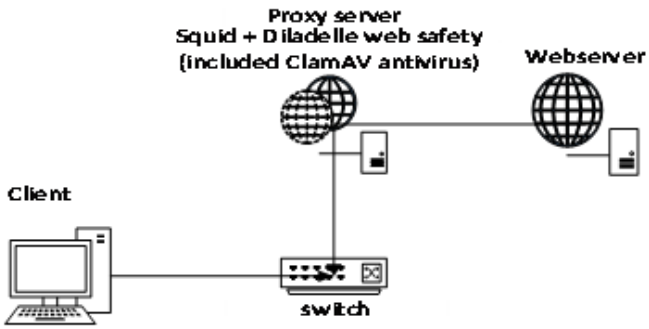
Pada awalnya proxy server hanya di install aplikasi squid yang merupakan variabel terikat sebagai basis untuk melakukan filtering, untuk membuktikan bahwa squid tidak mampu untuk melakukan filtering pada koneksi https.Pada pengujian awal penulis akan mencoba mengkonfigurasi squid proxy agar mampu melakukan pemblokiran terhadap alamat website perjudian bwin.com, dengan cara memasukkan DNS bwin.com kedalam ACL squid proxy. Selanjutnya penulis akan mencoba mengakses website tersebut dari komputer client dengan protocol http, apabila proxy berhasil melakukan tugas nya dalam memfilter website bwin.com tersebut, penulis akan langsung mencoba dengan mengakses alamat website tersebut dengan menggunakan protokol https, karena bwin.com menyediakan sambungan dengan sertifikat keamanan yang diakses menggunakan protocol https. Apabila website bwin.com tersebut dapat dibuka, artinya squid proxy tidak berfungsi dengan baik. Penulis akan menambahkan dilladele web safety ke dalam proxy server yang akan di kolaborasikan dengan aplikasi squid proxy. Seperti gambar di bawah ini

Pada pengujian kedua penulis akan mengkonfigurasi diladelle web safety agar mampu memfilter sambungan https dari website bwin.com. selah dikonfigurasi penulis akan melakukan uji coba kedua dari komputer client, apabila sambungan aman dari protocol https website bwin.com mampu di filter, maka komputer client akan mendapat pemberitahuan bahwa website yang diakses mengandung konten yang dilarang. Selanjutnya penulis akan melakukan uji coba ketiga dengan mendownload sample virus dari website http://www.eicar.org/download/eicarcom2.zi

disinilah akan dilihat apakah squid yang dikolaborasikan dengan diladelle web safety mampu memblok download yang dilakukan atau tidak. Apabila squid dan diladelle web safety mampu melakukan pemblokiran maka skema 3 tidak diperlukan lagi, dan ujicoba cukup sampai disini, tapi apabila diladelle web safety tidak mampu melakukan pemblokiran langkah selanjutnya adalah melakukan pengembangan pada proxy server, yaitu mengintegrasikan diladelle web safety sebagai ICAP rewriter dengan database dari ClamAV antivirus. Seperti pada gambar di bawah ini :



Gambar 2: Skema Pengujian 2



Gambar 3: Skema Pengujian 3

3 HASIL DAN PEMBAHASAN

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 alamat website bukan melalui ip address, sedangkan web server dibutuhkan untuk menampung halaman web yang sudah disiapkan.

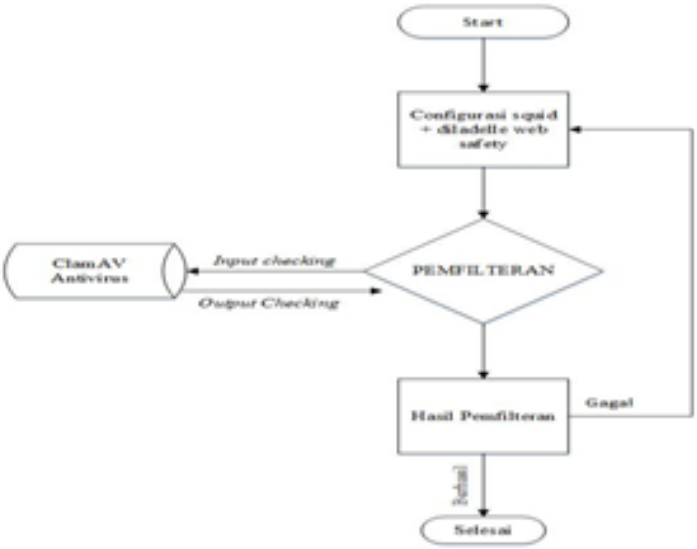
Ketika ujicoba pertama dilakukan, klien mengirimkan permintaan melalui web browser ke alamat website www.bwin.com kepada web server, kemudian web server memberikan balasan dengan mengirimkan konten yang diminta oleh klien seperti gambar 4 dibawah ini.

Dari gambar diatas 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.

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 5 dibawah ini.

Dari gambar diatas squid proxy telah bekerja dengan baik sesuai dengan konfigurasi yang penulis lakukan sebelumnya, hal ini dibuktikan dengan tidak bisa diaksesnya website www.bwin.com yang sebelumnya dapat diakses, ini dikarenakan cara kerja squid proxy yang memfilter sesuai dengan access control list yang telah ditetapkan bahwa website www.bwin.com tidak boleh diakses oleh klien, pada saat klien mengirimkan permintaan pada proxy untuk mengakses web server dari website www.bwin.com, pada saat browser klien mengirimkan header permintaan, http request dikirimkan ke server proxy. Header tersebut diterima squid dan dibaca, dari hasil pembacaan tersebut squid akan memparsing url dan dicocokan dengan database proxy, apabila dalam pemeriksaan tersebut ternyata url yang di request masuk dalam kategori blacklist dalam acl squid proxy, maka squid akan mengirimkan pemberitahuan kepada klien bahwa akses menuju website yang dituju tidak dapat diteruskan. Dan hal ini telah terjadi pada pengujian kedua yang penulis lakukan.



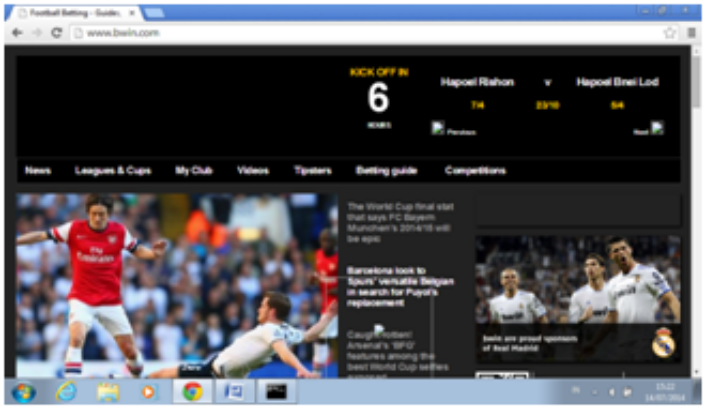
Gambar 4: Flowchart Pengujian

3.3 Analisis Pemfilteran Https

Pada pengujian yang ketiga penulis telah memasang ssl pada web server www.bwin.com yang digunakan untuk enkripsi sambungan antara klien dan web server. Penulis menggunakan OpenSSL untuk membuat agar dapat menggunakan protokol secure dari ssl, dimana openssl sendiri menggunakan enkripsi rsa (Rivest, Shamir dan Adleman), rsa merupakan algoritma yang menerapkan kunci public dan kunci private untuk mengenkripsi sambungan data, cara kerja dari algoritma rsa dalam mengenkripsi dan mendekripsi data dapat dilihat pada gambar 6 di bawah ini

Selanjutnya setelah penulis berhasil menambahkan openssl kedalam web server, penulis selanjutnya melakukan ujicoba ketiga, yaitu pengaksesan alamat website www.bwin.com melalui protocol 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 dibawah ini.

Hal tersebut dapat terjadi karena cara kerja proxy yang hanya memeriksa header permintaan dari klien, kemudian disesuaikan dengan database yang ada pada proxy server itu sendiri termasuk dalam hal ini access control list. Sedangkan pada koneksi https sesuai dengan konsep pertukaran kunci tadi, komunikasi antara klien dan web server telah di enkripsi sehingga proxy tidak dapat bekerja dengan baik dalam memfilter koneksi tersebut.

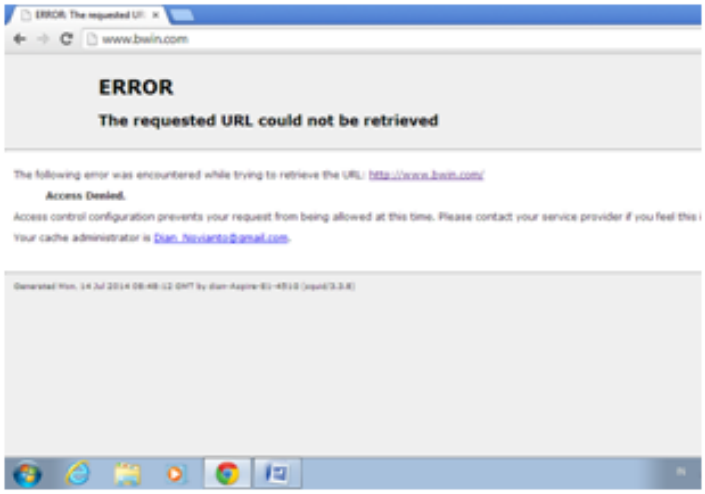


Gambar 5: Pengujian Squid

3.4 Analisis Pemfilteran Diladele Web Safety

Karena pada pengujian ketiga squid proxy tidak dapat bekerja dengan baik, dilakukanlah konfigurasi selanjutnya yaitu kolaborasi antara squid proxy dan diladele web safety untuk melakukan filtering terhadap koneksi dari https.

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 mampu melakukan pemeriksaan mendalam dari enkripsi ssl lalu lintas web dan menyesuaikan dengan pengaturan yang terdapat didalamnya, antara lain berdasarkan kategori seperti dating, nudity, gambling, explicit adult content, gaming dan lainnya. Dari



Gambar 6: Cara Kerja RSA

konfigurasi tersebut penulis melakukan ujicoba terhadap koneksi dari https www.bwin.com, hasilnya dapat terlihat seperti gambar 8 dibawah ini.

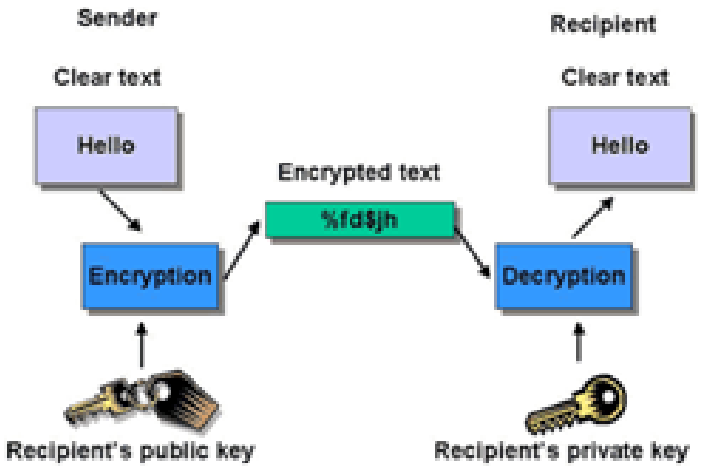
Dari pengujian diatas terbukti mampu memfilter koneksi https dari website www.bwin.com, untuk lebih meningkatkan keamanan sebagai server icap diladele yang dikonfigurasi dengan squid kemudian diuji coba untuk memfilter content yang mengandung virus yang diambil sampelnya dari website eicar.org, ternyata dari ujicoba tersebut kolaborasi antara squid proxy dan diladele web safety belum dapat memfilter file yang di download yang mengandung virus didalamnya dikarenakan tidak terintegrasi dengan database antivirus seperti database ClamAv.

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 yaitu srv_clamav, kemudia srv_clamav akan memberikan hasil scanning kepada proxy server atau dikenal dengan respond mode untuk di teruskan ke klien. 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 dibawah ini.

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



Gambar 7: Uji Coba SSL

Gambar 8: Pengujian Diladele

Gambar 9: Pengujian C-ICAP

4 KESIMPULAN

Dari hasil pembahasan pada bab sebelumnya di dapatkan beberapa kesimpulan yang dapat ditarikadalah untuk mencapai hasil yang di inginkan dalam penelitian ini yaitu pem-

Gambar 10: Flowchart Pengujian

filteran https dan pemfilteran virus internet, tidak bisa hanya menggunakan salah satu perangkat lunak pada variabel bebas, selain itu Kolaborasi antara squid, diladelle web safety dan C-Icap mampu memfilter https dan virus sesuai dengan tujuan dari penelitian ini.

5 Referensi

1. Coupey, Eloise. (2001). Marketing and the Internet, Conceptual Foundation. Prentice-Hall.

2. Sugiyono dalam Tjutju Soendari. Penelitian Eksperimental. Universitas Pendidikan Indonesia

3. Tjutju Soendari. Penelitian Eksperimental. Universitas Pendidikan Indonesia.