BAB 4
PENGUJIAN DAN ANALISA

Bab ini membahas pengujian proses *filtering* yang dilakukan pada alamat situs dan alamat IP yang akan difilter. Setelah melakukan pengujian, hasilnya akan ditampilkan menggunakan SARG (*Squid Analys Report Generator*).

1.1 Persiapan Pengujian

Sebelum melakukan pengujian, ada beberapa tahap yang harus diperiksa seperti, koneksi antara *proxy server* dengan klien, dan pengecekan *file* squid.conf. Langkah persiapan pengujian sebagai berikut:

1. Memeriksa koneksi antara *proxy server* dengan klien

   Pemeriksaan ini bertujuan untuk mengetahui koneksi antara *proxy server* yang memiliki alamat IP 192.168.1.2 dengan klien 1, yang memiliki alamat IP 192.168.2.2, dan klien 2 dengan alamat IP 192.168.2.3. Untuk melakukan pemeriksaan koneksi dengan perintah berikut:

   ```
   # ping -c3 192.168.2.2
   ```

   ```
   # ping -c3 192.168.2.3
   ```

2. Memeriksa squid.conf

   Pemeriksaan file squid.conf bertujuan untuk memeriksa squid.conf apa masih terdapat pesan kesalahan atau tidak. Jika masih terdapat pesan kesalahan *squid* tidak dapat dijalankan. Untuk memeriksa squid.conf dengan perintah berikut:

   ```
   # /usr/local/squid/sbin/squid -k parse
   ```

3. Menjalankan Squid

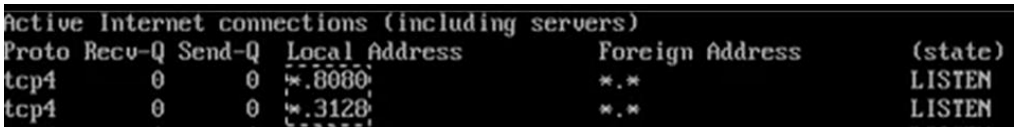
   Jika tidak terdapat pesan kesalahan pada Squid, langkah berikutnya adalah menjalankan *squid*. Untuk menjalankan Squid dengan perintah berikut:

   ```
   # /usr/local/squid/sbin/squid –DsY
   ```

Untuk melihat *port* dari Squid sudah terbuka atau belum dengan perintah berikut:

netstat –na|more

Hasil tampilan terlihat pada gambar di bawah ini.



Gambar **Error! No text of specified style in document.**.1 Tampilan Port Squid Yang Sudah Terbuka

Pada gambar 4.1 merupakan keterangan bahwa *port* dari Squid dalam kondisi sudah terbuka dengan tampilan pada *local address* 3128 dan 8080 merupakan *port* yang digunakan oleh Squid dengan *state* LISTEN, yang berarti proxy server sudah dapat akses.

1.2 Tahap-Tahap Pengujian

Tahap-tahap pengujian yang dilakukan adalah melakukan *filtering* berdasarkan alamat situs dan alamat IP. Tahap pengujian sebagai berikut:

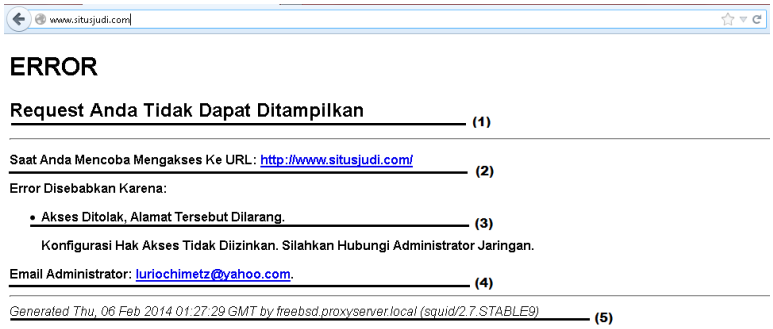
1.2.1 Filtering Berdasarkan Alamat Situs

Filtering berdasarkan alamat situs bertujuan untuk melakukan filter pada alamat situs yang akan difilter yang sudah didaftarkan pada ACL (*Access Control List*). Berikut contoh alamat situs sebelum difilter dapat dilihat pada gambar dibawah ini:



Gambar **Error! No text of specified style in document.**.2 Tampilan Alamat Situs Sebelum Difilter

Sebelum alamat situs www.situsjudi.com difilter, maka masih dapat diakses. Berikut tampilan hasil *filtering* alamat situs www.situsjudi.com yang sudah didaftarkan pada ACL seperti gambar dibawah ini:



Gambar **Error! No text of specified style in document.**.3 Tampilan Hasil Filtering Alamat Situs

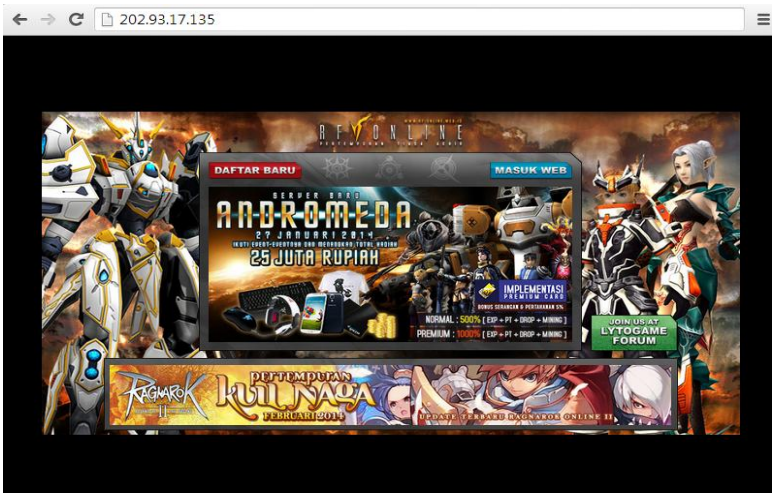
Berdasarkan hasil tampilan *filtering* pada alamat situs, bila komputer klien mengakses alamat situs yang difilter, maka akan dialihkan pada sebuah halaman yang berisi teks *error* yang diberikan *proxy server*.

Berikut keterangan lengkap tentang gambar 4.3:

1. Menunjukkan teks *error* yang menandakan *request* yang di akses tidak dapat ditampilkan.
2. Menunjukkan alamat situs yang difilter adalah www.situsjudi.com.
3. Menunjukkan penyebab alamat situs tidak dapat diakses yaitu akses ditolak, alamat tersebut dilarang.
4. Menunjukkan *email* dari administrator jaringan dengan nama luriochimetz@yahoo.com.
5. Menunjukkan waktu yang digunakan untuk mengakses alamat situs tersebut yaitu pada hari Thu/Kamis tanggal 6 Februari 2014 pada jam 01:27:29 yang dikirimkan *proxy server* dengan *hostname* freebsd.proxyserver.local menggunakan squid 2.7 STABLE9.

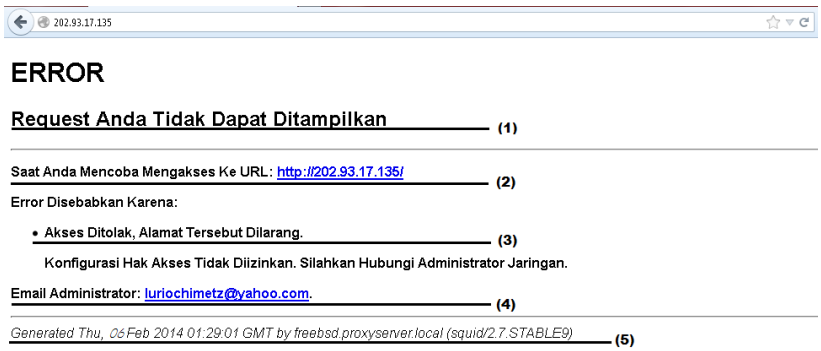
1.2.2 Filtering Berdasarkan Alamat IP

Filtering berdasarkan alamat IP bertujuan untuk melakukan filter pada alamat IP yang akan difilter yang sudah didaftarkan pada ACL (*Access Control List*). Berikut contoh alamat IP sebelum difilter dapat dilihat pada gambar dibawah ini:



Gambar **Error! No text of specified style in document.**.4 Alamat IP Sebelum Difilter

Sebelum alamat situs 202.93.17.135 difilter, maka masih dapat di akses. Berikut tampilan hasil *filtering* alamat situs 202.93.17.135 yang sudah didaftarkan pada ACL seperti gambar dibawah ini:



Gambar **Error! No text of specified style in document.**.5 Tampilan Alamat IP Sesudah Difilter

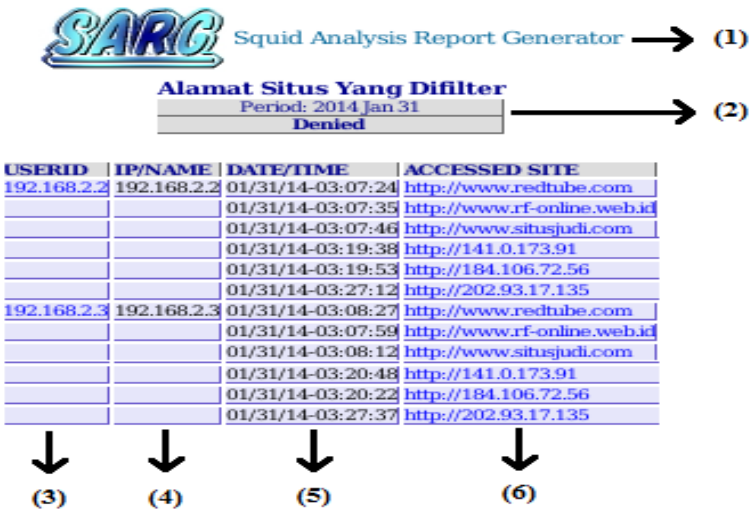
Berdasarkan hasil tampilan *filtering* pada alamat IP, bila komputer klien mengakses alamat IP yang difilter, maka akan dialihkan pada sebuah halaman yang berisi teks *error* yang diberikan *proxy server*.

Berikut keterangan lengkap tentang gambar 4.5:

1. Menunjukkan teks *error* yang menandakan *request* yang di akses tidak dapat ditampilkan.
2. Menunjukkan alamat situs yang difilter adalah 202.93.17.135.
3. Menunjukkan penyebab dari alamat situs tidak dapat diakses yaitu akses ditolak, alamat tersebut dilarang.
4. Menunjukkan *email* dari administrator jaringan dengan nama luriochimetz@yahoo.com.
5. Menunjukkan waktu yang digunakan untuk mengakses alamat situs tersebut yaitu pada hari Fri/Jumat tanggal 06 Februari 2014 pada jam 01:29:01 yang dikirimkan *proxy server* dengan *hostname* freebsd.proxyserver.local menggunakan versi squid 2.7 STABLE9.

1.3 Menampilkan Report Menggunakan SARG

Setelah melakukan pengujian *filtering* pada alamat situs dan alamat IP, selanjutnya ditampilkan pada sebuah halaman *report* yang berisi alamat IP klien, keterangan waktu kapan digunakan untuk mengakses alamat situs, dan alamat situs dan alamat IP yang difilter, sehingga administrator dapat mengetahui informasi dalam mengakses alamat situs dan alamat IP.



Gambar **Error! No text of specified style in document.**.6 Tampilan SARG Untuk Alamat Situs dan Alamat IP Yang Difilter

Berikut keterangan lengkap dari gambar 4.4:

1. Menunjukkan nama program yang digunakan untuk menampilkan *report* yaitu SARG (*Squid Analys Report Generator*).
2. Menunjukkan judul dari *report* tersebut adalah Alamat Situs Yang Difilter dan waktu pengambilan *report* pada tanggal 31 Januari 2014.
3. Menunjukkan penamaan komputer klien berdasarkan USERID yang berisi alamat IP klien.
4. IP/NAME: menampilkan alamat IP klien yang mengakses alamat situs yang difilter.
5. DATE/TIME: menunjukkan keterangan waktu kapan digunakan untuk mengakses alamat situs yang difilter.
6. ACCESSED SITE: menampilkan alamat situs dan alamat IP yang diakses oleh klien. Dimana alamat situs dan alamat IP tersebut sudah terdaftar pada ACL, sedangkan untuk alamat situs yang belum didaftarkan tidak akan difilter dan ditampilkan pada *report*.