ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)

PENGEMBANGAN SISTEM PENGENDALIAN TRAFFIC DAN WEB FILTERING PADA JARINGAN INTERNET BERBASIS HOTSPOT

Riska Robianto
Fakultas Ilmu Komputer, Universitas Putra Indonesia "YPTK" Padang, Jalan Raya Lubuk Begalung
Telepon (0751) 776666 Faximili (0751) 71319, Padang Sumatera Barat, Indonesia
Email: riskarobianto@upiyptk.ac.id

Submitted: 18-03-2016, Rewiewed:17-05-2016, Accepted:24-05-2016
http://dx.doi.org/10.22216/jit.2016.v10i2.341

Abstrak

Pemanfaatan layanan Internet pada jaringan hotspot memunculkan permasalahan khususnya pada pengendalian traffic dan web filtering. Linux sebagai sistem operasi yang bersifat terbuka (open source), menawarkan berbagai sistem firewall internet untuk membantu proses pengelolaan traffic, bandwidth, dan web filtering salah satunya dengan menggunakan Smoothwall Express Linux yang dapat mengkonversi personal computer (PC) menjadi perangkat firewall internet yang handal dan stabil. Smoothwall memungkinkan untuk dintegrasikan dengan add-ons extends seperti AdvProxy dan URL Filter untuk meningkatkan kinerja dari Smoohtwall dan mempermudah konfigurasi terhadap pengendalian traffic dan web filtering. Penelitian ini dilakukan dengan mengumpulkan data dari berbagai sumber yang terkait, kemudian melakukan eksperimen dengan mengimplementasikan Smoohtwall dengan menambahkan add-ons extends untuk membantu administrator mengelola dan mengatur alokasi bandwidth tiap client, memblokir situs-situs (URL) yang tidak dinginkan. Berdasarkan hasil penelitian ini pengelolaan bandwidth dapat dibagi secara merata dan dapat memblokir situs-situs (URL) yang tidak dinginkan seperti situs porn, warez, bad word, dan updatesites sehingga kualitas koneksi jaringan lebih stabil.

Kata kunci: *hotspot, linux, pengelolaan bandwidth, penyaringan halaman web, smoothwall express.*

Abstract

Utilization of Internet services to the hotspot network raises particular problems in traffic control and web filtering. Linux as an operating system that is open (open source), offers a variety of internet firewall systems to assist in the management of traffic, bandwidth, web filtering and one using Smoothwall Express to Linux which can convert a personal computer (PC) to the Internet firewall reliable and stable. Smoothwall allows to integrated with the add-ons extends like AdvProxy and URL Filter to improve the performance of Smoohtwall and simplify configuration of the traffic control and web filtering. The research was conducted by collecting data from various sources related, then experiment with implementing Smoohtwall by adding add-ons extends to help administrators manage and regulate the bandwidth allocation of each client, block websites (URLs) that are not needed. Based on these results bandwidth management can be divided equally and can block websites (URLs) that are not needed like porn sites, warez, bad word, and also the quality of the network connection updatesites more stable.

Keywords : *hotspot, linux, bandwidth management , web page filtering, smoothwall express*

PENDAHULUAN

Pemanfaatan teknologi informasi di dunia pendidikan sangatlah berperan. Terutama untuk pemanfaatan teknologi komputer dan internet. Teknologi informasi tersebut digunakan untuk menunjang kelancaran proses akademis dan proses belajar mengajar, misalnya untuk sistem

penyebaran informasi dalam bentuk sistem informasi akademis, elearning, emading, perpustakaan digital, dan lain-lain.

Dengan kemajuan teknologi informasi tersebut memungkinkan suatu informasi diakses dimana saja, dan kapan saja, sehingga sangat membantu mobilitas. Apalagi dengan kemajuan teknologi *wireless* yang sangat menunjang mobilitas pengguna. Dengan *hotspot* pengguna jaringan bisa menikmati akses internet dimanapun berada selama di area *hotspot* tanpa harus menggunakan kabel. Di lingkungan sekolah sendiri dengan adanya layanan *hotspot* diharapkan akan mempercepat akses informasi bagi siswa, guru dan pegawai.

Akan tetapi ketersediaan fasilitas dan layanan saja belumlah ideal bila tidak diiringi dengan kebijakan teknologi informasi terutama untuk pemakaian internet. Jumlah pengguna *hotspot* yang banyak dengan intensitas pemakaian yang tinggi tidaklah sebanding dengan lebar jalur internet (*bandwidth*) yang tersedia sehingga menyebabkan *traffic overload.*

Menurut Badru Z (2008), padatnya lalu lintas data atau *traffic overload* membuat perangkat dalam jaringan seperti *switch*, *router* atau *access point* menjadi *crash* dan menyebabkan tidak beroperasinya keseluruhan jaringan.

Pengendalian suatu *bandwidth* yang tidak optimal dan tingginya *traffic* yang dihasilkan menyebabkan tidak lancar bahkan sering terputusnya koneksi internet. Hal yang sering menjadi penyebab tidak stabilnya *bandwidth* yang diterima oleh tiap pengguna (*user*) adalah permintaan untuk mengunduh file dan pengguna secara bebas dapat mengakses situs-situs (*URL*) apapun seperti situs porno.

Internet telah merevolusi cara orang menyebarkan informasi di seluruh dunia. Hal tersebut menawarkan akses instan ke hampir semua jenis sumber daya digital. Sayangnya, hal ini berlaku sama untuk konten legal maupun ilegal tanpa sensor Gossett dan Shorter (2011).

Seluruh masalah seperti yang dikemukan di atas terjadi karena sistem sekarang masih diterapkan secara konvensional tanpa penerapan sebuah *firewall* atau *router* sebagai sistem yang mengatur pengendalian *traffic* dan *web filtering* pada jaringan internet berbasis *hotspot*. Hal tersebut diketahui dengan pengujian terhadap konektivitas jaringan, *traffic* dan *bandwidth* dengan menggunakan utilitas *Packet Internet Groper* (*Ping*), *Web Browser* dan *Network Packet Analyzer* (*Wireshark*).

Untuk itu, diperlukan suatu upaya pengembangan sistem pengendalian *traffic* dan *web filtering* pada jaringan internet berbasis *hotspot* secara lebih baik terhadap manajemen *bandwidth* dan *URL filtering* menggunakan Smoothwall. Smoothwall adalah proyek open source yang didirikan pada tahun 2000 merupakan *firewall* internet gratis yang memiliki keamanan yang kuat GNU/sistem operasi Linux dan mudah untuk digunakan dengan antarmuka *web browser*.

METODE PENELITIAN

Pada dasarnya kegiatan yang dilakukan pada penelitian ini ada dua bagian, yaitu tahap identifikasi masalah sistem dan analisis sistem yang sedang berjalan secara garis besar untuk memperoleh pengertian dari permasalahan-permasalahan, efisiensi dan pertimbangan-pertimbangan yang mengarah ke pengembangan sistem.

Bertujuan untuk mengetahui kebutuhan dalam merancang suatu sistem dengan

ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)

mempertimbangkan beberapa faktor permasalahan yang ada. Permasalahan utama yang dihadapi adalah belum adanya sistem pengendalian *traffic* dan *web filtering* dalam jaringan yang dimiliki oleh SMA Negeri 10 Padang. Dalam hal ini upaya yang dapat dilakukan adalah dengan mencari informasi perangkat lunak dan metode yang tepat sehingga dapat menghasilkan solusi yang tepat sasaran serta mudah diimplementasikan.

Proses identifikasi masalah sistem dapat dilakukan berdasarkan pengamatan langsung pada sistem jaringan internet dan interview dengan beberapa pertanyaan yang diajukan pada pengguna (*user*). Contoh laporan kuisioner dan interview adalah seperti diperlihatkan pada Tabel 1.

Tabel 1. Bentuk Laporan Pengamatan dan Interview

No	Nama Pengguna	Jenis Layanan Internet Yang Diakses					
		Down / Upload	Video Streaming	News Portal	Sosial Media	Chat	Games Online
1	Debby Amanda	√	√	×	√	×	×
2	Weni Avri Rahman	√	×	√	×	√	×
3	M.Hafizul Luthfi	√	×	×	√	√	×
4	Mona Indah Putriani	×	√	√	√	√	×
5	Agung Pernanda	√	×	√	√	√	√
6	M.Arief Saputra	√	√	√	×	√	√
7	Lukmanul Hakim	√	×	√	√	×	√
8	Ifdhal Suharmitan	√	√	×	√	×	×
9	Firmanul Qadri	√	×	√	×	√	√
10	Mardatillah	×	√	√	√	×	×
11	Gefri Dwi Putra	√	×	√	√	√	×
12	Mafira Yuwandari	√	√	√	×	×	×
13	Ulfa Inten Waluyani	×	√	√	×	√	×
14	Iqbal Kurnia	√	√	×	√	√	√
15	Erlan Farjun	√	×	√	√	√	√
Rata-rata (jumlah centang / jumlah data)		80%	53%	73%	67%	67%	40%

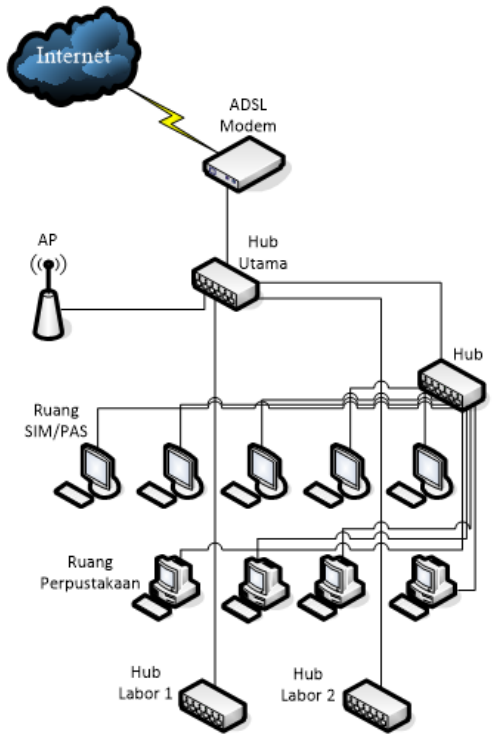
√ : ya mengakses
× : tidak mengakses

Dari laporan di atas didapatkan sebuah gambaran bahwa dari 15 orang responden sebagian besar akan menghabiskan alokasi *bandwidth* yang tersedia, hal ini karena digunakan untuk unduh/unggah sebesar 80% dan akses situs news dan situs lainnya (tanpa sensor) sebesar 73%. Untuk jenis layanan yang lain masih dengan presentase yang rendah, dan masing-masing layanan tidak bisa dilihat alamat (*address*) detailnya mengingat tidak ada laporan (*log*) dari sistem jaringan tersebut.

Pengguna dan responden dalam penelitian ini difokuskan kepada peserta didik dengan alasan jumlah pengguna terbanyak didominasi oleh peserta didik dibanding dengan guru atau karyawan.

ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)

Untuk menganalisa sistem yang sedang berjalan perlu diketahui bentuk atau topologi terutama pada jaringan internet berbasis *hotspot*, hal ini dimaksudkan untuk mempelajari dan memudahkan dalam pengembangan sistem yang direncanakan. Di SMA Negeri 10 Padang mengunakan topologi seperti dijelaskan pada Gambar 1.



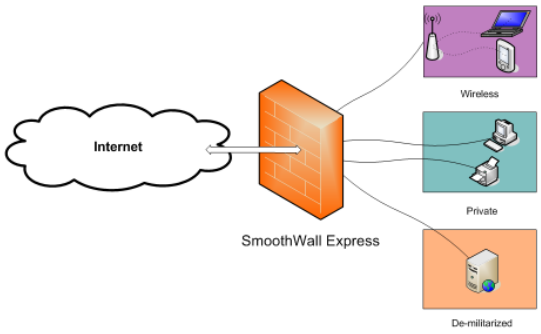
Gambar 1. Topologi Jaringan Lama

Dimana fungsi dan keterangan yang ada pada Gambar 1 di atas adalah (1) jaringan internet (*ISP)* menggunakan *provider* Telkom Speedy; (2) jaringan lokal di ruang SIM/PAS dengan jumlah *host* 5 unit *PC*; (3) jaringan lokal di ruang perpustakaan, dengan jumlah *host* 4 unit *PC* (4) jaringan lokal di labor 1 dengan jumlah *host* 32 unit *PC* (5) jaringan lokal di labor 2, dengan jumlah *host* 32 unit *PC;* (6) jaringan lokal dengan *access point* (hotspot).

Berikutnya merupakan tahapan dalam melakukan perancangan suatu sistem yang lebih baik dan dapat berjalan sesuai dengan tujuan pembuatan sistem berdasarkan berbagai aspek permasalahan dan kondisi yang telah dijelaskan sebelumnya. Untuk pengembangan sistem yang baru dapat diimplementasikan dengan Smoothwall.

Smoothwall sebagai salah satu solusi dari pemecahan masalah terutama pada sistem pengendalian *traffic* dan *web filtering* pada jaringan internet berbasis *hotspot*, maka perlu juga dipahami konsep penerapan (1) keamanan; (2) tipe konfigurasi jaringan dan pengendalian *traffic* jaringan serta; (3) integrasi dari *add-on extends* sebagai penunjang kinerjanya.

Keamanan (*security*), smoothwall atau disebut juga Smoothwall Express (*SE*) mendukung *De-Militarized Zone* (*DMZ*), sebuah jaringan yang biasanya digunakan untuk *server* yang perlu diakses dari internet, seperti *mail* dan *web server*. Secara default Smoothwall memblokir semua lalu lintas (*traffic*) ke *host* dan *server* di belakang Smoothwall yang berasal dari internet. Jika pengguna eksternal perlu menggunakan *server* di belakang Smoothwall maka akses ke *server* ini harus diblokir secara khusus. Konsep keamanan smoothwall dapat dilihat pada Gambar 2.



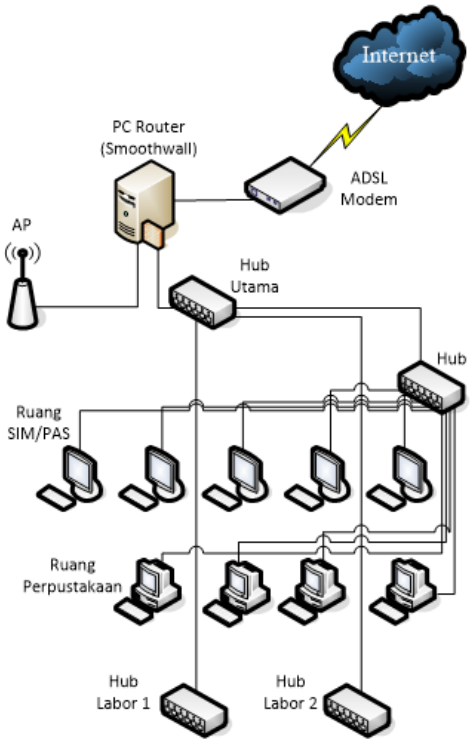
Gambar 2. Konsep Keamanan Smoothwall

ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)

Pada Smoothwall konfigurasi jaringan dibedakan menjadi beberapa kategori (1) jaringan lokal/internal (*green*); (2) jaringan luar/external (*red*); dan (3) D*e-Militarized Zone* (*orange*); serta (4) jaringan *wireless* (*purple*).

Mengendalikan *Traffic* jaringan (*Controlling Network Traffic*), smoothwall tidak saja sebagai firewall internet yang menghubungkan jaringan luar (external) dengan jaringan lokal (internal), akan tetapi juga berfungsi sebagai pengendali *traffic* jaringan, seperti mengelola lalu lintas masuk dan keluar, memblokir *IP* tertentu, dan manajemen *Quality of Service* (*QoS*).

Setelah melihat kelemahan dan kekurangan topologi jaringan pada sistem lama. Maka perlu dirancang sebuah sistem baru dengan mempertimbangkan beberapa aspek pengendalian *traffic* dan *web filtering* pada jaringan internet berbasis *hotspot* dengan menggunakan Smoothwall seperti dijelaskan pada Gambar 3.



Gambar 3. Topologi Sistem Baru

Dari topologi tersebut ditambahkan sebuah mesin Smoothwall yang berfungsi sebagai *firewall* internet sekaligus berfungsi sebagai sistem pengendalian *traffic* dan *web filtering* pada jaringan internet berbasis *hotspot*. Pada mesin Smoothwall inilah dilakukan konfigurasi untuk manajemen *bandwidth, traffic dan web filtering*.

Sebelum melangkah ke perancangan sistem jaringan internet berbasis *hotspot*, sebagai langkah awal adalah pengaturan pada *Modem ADSL*, dimana modem disini diset menjadi PPPoE sehingga konfigurasi jaringan external dari *ISP* nantinya tidak dilakukan pada mesin Smoothwall.

Berikutnya proses perancangan jaringan *hotspot* dapat dilakukan dengan instalasi sistem operasi *firewall* Smoothwall dan *web browser* pada sebuah *personal computer* (*PC*). Disinilah diterapkan konsep keamanan Smoothwall berdasarkan konfigurasi

jaringan Smoothwall seperti yang sudah diuraikan sebelumnya yaitu kategori *green-red-purple*.

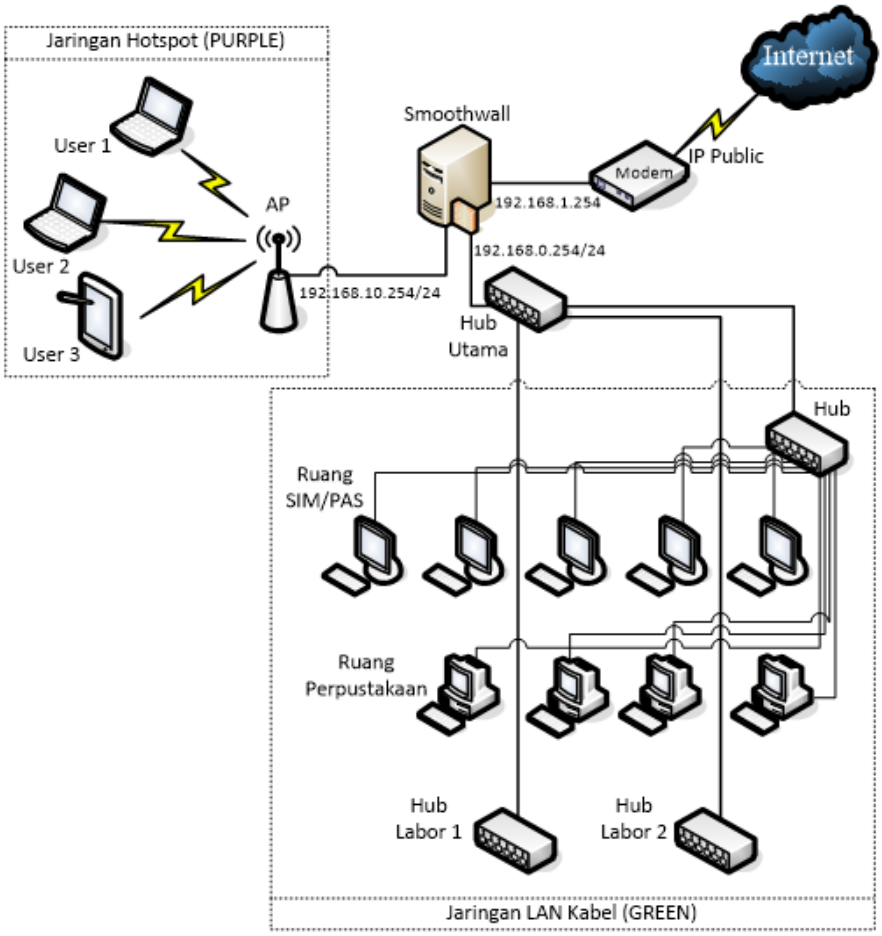
Untuk membangun sebuah *firewall* internet Smoothwall juga dapat diintegrasikan dengan *add-ons extends* untuk meningkatkan kinerja dari Smoothwall itu sendiri. *Add-ons extends* adalah perangkat lunak tambahan berupa modul maupun script di antaranya adalah *AdvProxy* dan *URL Filter*.

AdvProxy adalah modul tambahan untuk linux popular berbasis *firewall* seperti Smoothwall. Modul *AdvProxy* untuk memperluas fungsi *web proxy* dengan fitur seperti *transfer limits* dan *download throttling*. Sedangkan *URL Filter* sebagai *web filtering* untuk memblokir domain, file, dan situs-situs (*URL*) yang tidak dinginkan, termasuk situs (*URL*) *porn*, *warez* dan *updatesites*.

HASIL DAN PEMBAHASAN

Tahap setelah perancangan sistem adalah menyusun skenario pengujian sistem sebagai langkah strategis untuk menentukan tolak ukur keberhasilan atau ketercapaian sistem yang dirancang. Selain menentukan tolak ukur keberhasilan, kriteria pengujian untuk setiap skenario juga sangat diperlukan. Skenario ini digunakan untuk mempermudah melakukan pengujian pada lingkungan implementasinya dan untuk membuktikan bahwa sistem yang dirancang sudah berjalan dengan baik sesuai tujuan yang diharapkan. Sedangkan kriteria pengujian diperlukan sebagai acuan awal sebelum sistem tersebut diimplementasikan.
Skenario pengujian dilakukan pada sistem yang dirancang adalah sebagai berikut: (1) pengujian jaringan *hotspot* pada perancangan sistem menggunakan Smoothwall, seperti yang dijelaskan pada Gambar 4.

ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)



Gambar 4. Skenario Perancangan Smoothwall

Dalam skenario ini, beberapa perangkat seperti *personal computer* (*PC*), Laptop, *PDA atau Smartphone* sebagai pengguna diasumsikan mempunyai *IP DHCP* (*IP address default*) akan mengakses internet melalui jaringan *hotspot* (Purple) dengan *IP address* 192.168.10.254/24, sedangkan jaringan LAN kabel (Green) dengan *IP address* 192.168.0.254/24.

Melalui cara ini Smoothwall hanya akan menerima *traffic* data dari perangkat dalam jaringan Purple dan Green tersebut sesuai dengan *range* dan kelas *IP address* yang sudah ditentukan. Jika paket *request* berasal dari *IP address* yang diizinkan, maka *request* akan diproses dan direspon oleh Smoothwall untuk mengakses jaringan external (RED) dengan *IP* 180.241.221.50 (*IP Public*) melalui *IP* modem 192.168.1.254.

Kriteria pengujiannya adalah pendaftaran *IP address* pada Smoothwall. Indikator keberhasilanya adalah terhubung dengan *Domain Name Server* (*DNS*) atau *IP Public* dengan melakukan tes *Packet Internet Groper* (*Ping*). Dalam hal ini hanya *IP address* yang terdaftar saja yang dapat melakukan *request* layanan eksternal sedangkan *IP address* lain yang tidak terdaftar akan dilarang (*Banned*).

(2) Skenario kedua adalah menambahkan (konfigurasi) *Outgoing Rules*

dalam sistem Smoothwall. Setiap perangkat dalam jaringan *hotspot* akan diatur oleh *outgoing rules* yang mengelola lalu lintas jaringan keluar untuk layanan eksternal (internet). Prinsip *outgoing rules* adalah sebuah kebijakan membuka atau menutup *port-port* yang diperlukan.

Melalui cara ini Smoothwall hanya akan menerima *traffic* data dari perangkat dengan *IP address* dan *rules* yang diizinkan. Jika paket *request* merupakan *request* sesuai *rules* yang diizinkan, maka *request* akan diproses dan direspon oleh Smoothwall untuk mengakses jaringan external (*internet*).

Kriteria pengujiannya adalah konfigurasi *outgoing rules* pada Smoothwall. Indikator keberhasilannya adalah terhubung dengan *Domain Name Server* (*DNS*) dengan mengakses halaman *web* dengan *web browser* atau pesan penolakan dan peringatan terhadap pelanggaran *rules* yang telah ditetapkan.

(3) Skenario ketiga adalah (menambahkan) konfigurasi *Transfer Limits* dan *Download Throttling* yang berhubungan dengan pengendalian *traffic* salah satunya adalah kualitas pelayanan *bandwidth* (*Quality of Service*) dengan membatasi transfer data (unduh dan unggah) serta pembagian *bandwidth* secara merata untuk setiap pengguna (*user*) sesuai alokasi *bandwidth* yang tersedia.

Dengan cara ini, jaringan internet diyakini akan lebih stabil karena setiap *user* sudah mendapatkan jatah *bandwidth* yang sama dengan batasan *transfer* (unduh dan unggah) yang sama pula sehingga tidak ada penggunan (*user*) yang menggunakan *bandwidth* secara berlebihan atau mendominasi pemakaian.

Kriteria pengujiannya adalah *transfer limits* dan *download throttling*. Indikator keberhasilanya batas *transfer* maksimal (dalam satuan KB/s) sesuai nilai yang ditentukan (dalam satuan KB) atau pesan penolakan dan peringatan terhadap pelanggaran *rules* yang telah ditetapkan.

(4) Skenario keempat adalah (menambahkan) konfigurasi *Web Filtering* yang berhubungan dengan penyaringan situs dalam hal ini konfigurasi dilakukan pada *add-ons extends* yaitu *URL Filter* dengan memblokir (*block categories*) pengaksesan terhadap situs-situs yang dianggap berbahaya atau tidak diperlukan seperti: (a) situs *porn; (b) warez*; dan (c) *bad word* serta (d) *updatesites*.

Dengan cara ini, jaringan internet diyakini akan lebih aman karena pengaksesan situs *porn* dan *warez* dapat membawa *virus*, *trojan*, atau *spyware*. Kemudian dengan memblokir *updatesites* dapat menjaga koneksi internet tetap stabil karena *updatesites* akan menghabiskan banyak *resource* jaringan terutama *bandwidth*.

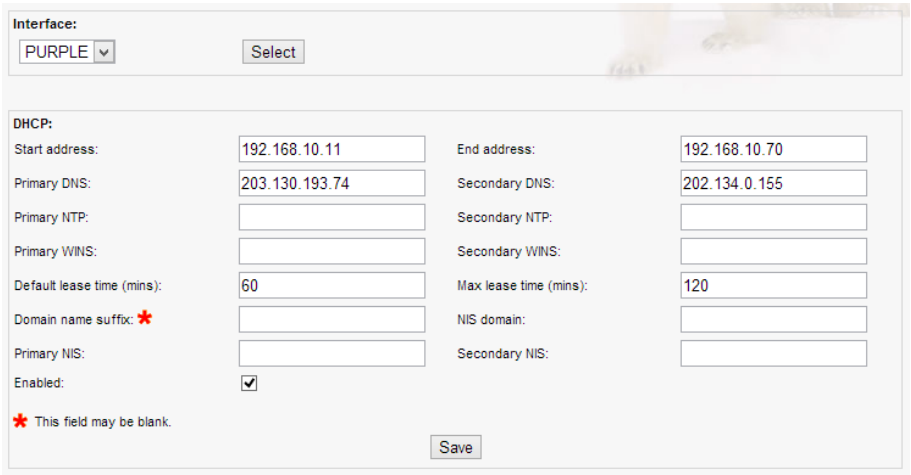
Kriteria pengujiannya adalah pemblokiran terhadap pengaksesan situs-situs yang dianggap berbahaya atau tidak diperlukan. Indikator keberhasilanya penolakan akses berupa pesan peringatan (*warning*) terhadap pelanggaran *rules* yang telah ditetapkan.

Untuk mempermudah pengujian pada lingkungan implementasinya, langkah berikut adalah mewujudkan implementasi skenario dengan kriteria tes dan indikator keberhasilan yang sudah ditetapkan sebelumnya untuk membuktikan bahwa sistem yang dirancang sudah berjalan dengan baik sesuai tujuan yang diharapkan.

(1) Implementasi dan pengujian jaringan *hotspot* pada perancangan sistem menggunakan Smoothwall. Adapun topologi sistem pengendalian *traffic* dan *web filtering*

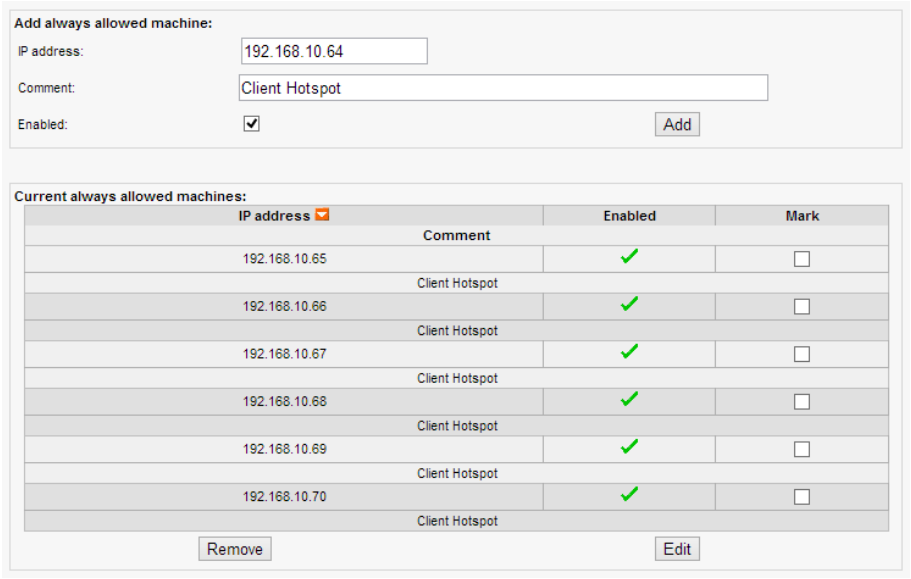
ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)

pada jaringan berbasis *hotspot* dapat dilihat pada Gambar 4 sebelumnya. Dari topologi tersebut, maka pada mesin Smoohtwall harus menggunakan beberapa *Card Ethernet* seperti telah dijelaskan sebelumnya (*Red-Green-Purple*). Untuk konfigurasi *IP* pengguna (*user*) disetting DHCP dapat diperhatikan pada Gambar 5.



Gambar 5. Konfigurasi Card Ethernet

Gambar 5 di atas menunjukan konfigurasi *range IP address* untuk *interface Purple* dimulai dari *address* 192.168.10.11 dan diakhiri *address* 192.168.10.70. Sedangkan konfigurasi *IP address* sebagai alamat pengguna (*user*) yang diizinkan dapat dilihat pada pada Gambar 6.

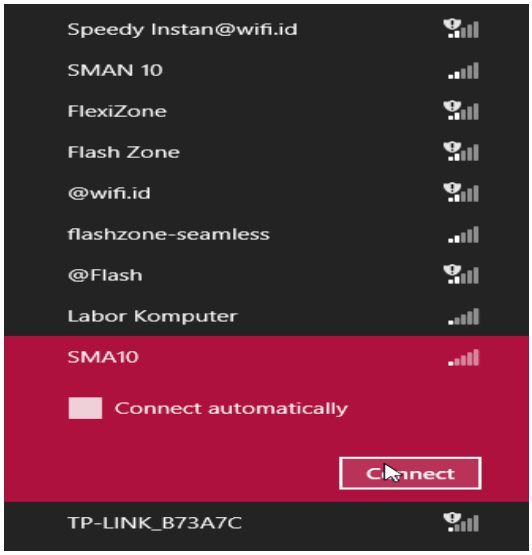


ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)

Gambar 6. Konfigurasi IP Address

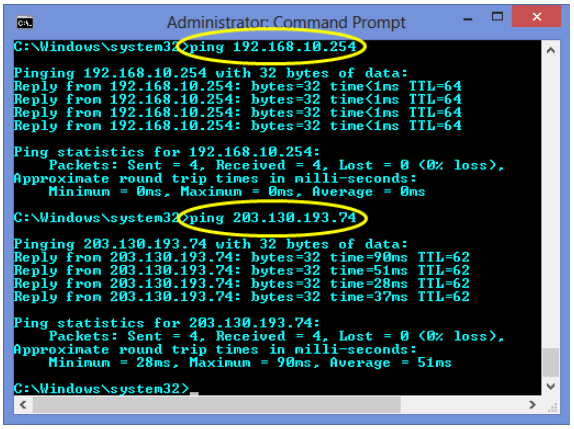
Gambar 6 adalah beberapa *IP address hotspot* yang akan digunakan dalam jaringan ini. Setiap *IP* harus didaftarkan terlebih dahulu sebanyak yang diperlukan karena secara *default* Smoothwall memblokir seluruh *IP* dalam jaringan lokal.

Selanjutnya adalah pengujian *wireless* LAN (*hotspot*). Langkah pengujian adalah pemeriksaan pada koneksi perangkat *wireless* LAN (*hotspot*). Hal tersebut untuk memastikan ketersediaan jaringan *hotspot*. Adapun langkah-langkah pengujiannya sebagai berikut: (a) koneksikan perangkat *Wireless* pengguna ke titik *hotspot* yang di tuju. Dalam penelitian ini area *hotspot* yang di tuju adalah SMA10. Perhatikan gambar 7.



Gambar 7. Koneksi Wireless (Hotspot)

(b) Setelah terkoneksi ke jaringan *hotspot*, buka *Command Prompt* dan lakukan tes *Ping* ke Smoothwall dan *DNS* dari *ISP* (Telkom Speedy) untuk memeriksa koneksi jaringan dan internet. Perhatikan gambar 8.

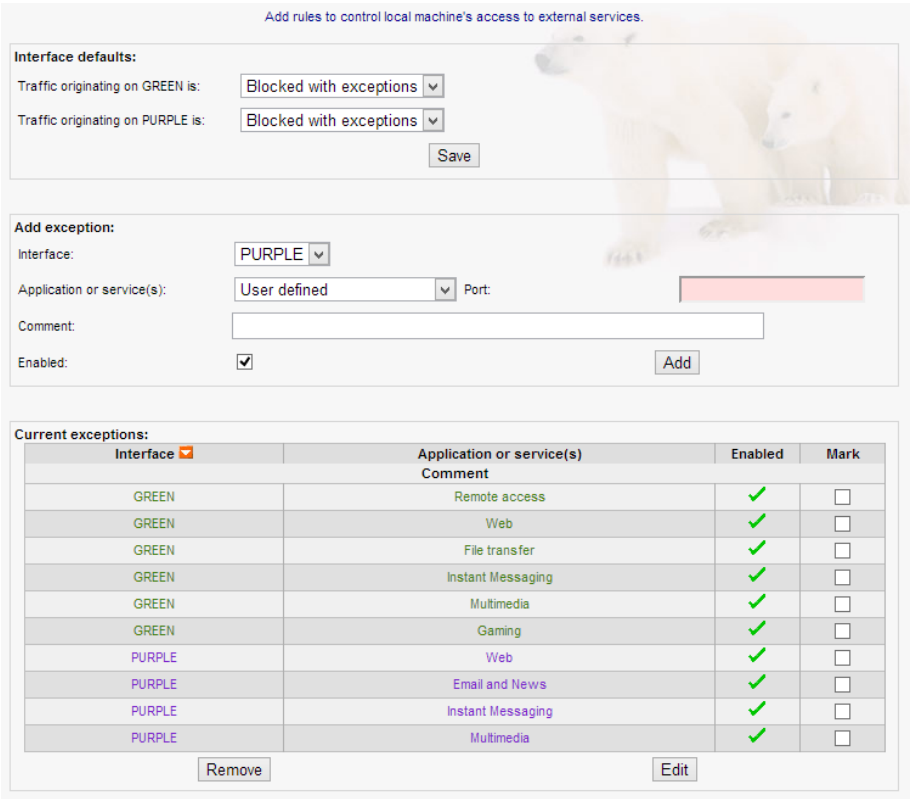


Gambar 8. Tampilan Test Ping

Pada Gambar 8 di atas, hasil tes *Ping* berhasil dilakukan ke Smoohtwall (192.168.10.254) pada jaringan *hotspot* (*Purple*) dan ke *Domain Name Server* (*DNS*) Telkom Speedy (203.130.193.74). Hasil tersebut memberikan informasi bahwa pengguna (*user*) tersambung dengan jaringan *hotspot* dan internet.

Implementasi dan pengujian *Outgoing Rules* pada perancangan sistem menggunakan Smoothwall. Untuk konfigurasi *outgoing rules* dapat dilakukan di Smoothwall, perhatikan pada Gambar 8.

ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)

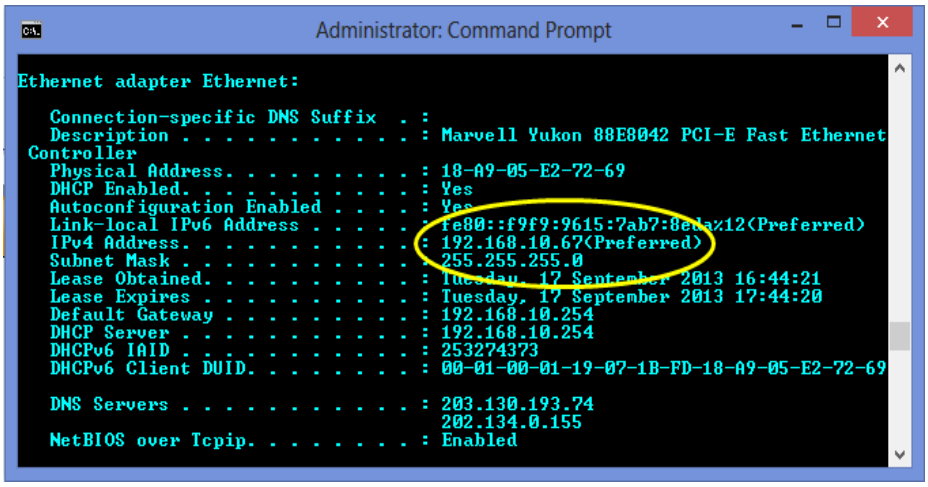


Gambar 8. Konfigurasi Outgoing Rules

Pada Gambar 8 di atas terlihat *rule-rule* yang mengontrol akses jaringan lokal ke jaringan luar (*external*). Secara default *firewall* Smoothwall membuka beberapa *port* jaringan lokal yang menuju akses luar (*external*) untuk itu perlu ditambahkan *rule* pengecualian (*exceptions*) yang mengizinkan beberapa *port* untuk bisa dilalui atau ditutup pada jaringan lokal baik jaringan LAN kabel maupun jaringan LAN nirkabel (*hotspot*).

Setelah perangkat pengguna (*user*) terkoneksi dengan jaringan *hotspot* dan internet, langkah selanjutnya tahap pengujian *outgoing rules* dengan mengakses halaman *website* menggunakan *web browser*. Adapun langkah-langkah pengujiannya sebagai berikut: (a) buka *Command Prompt* dengan mengetikkan "*ipconfig/all*" untuk melihat *IP address* yang didapatkan. Perhatikan gambar 9.

ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)



Gambar 9. Tampilan IP *Address*

Pada Gambar 9 di atas terlihat bahwa pengguna (*user*) mendapatkan *IP address* 192.168.10.67 sesuai dengan *range* dan *IP* yang sudah ditentukan pada Smoothwall untuk jaringan *hotspot*. Hasil ini menunjukkan bahwa langkah konfigurasi *IP DHCP* pada Gambar 5 berjalan dengan baik.

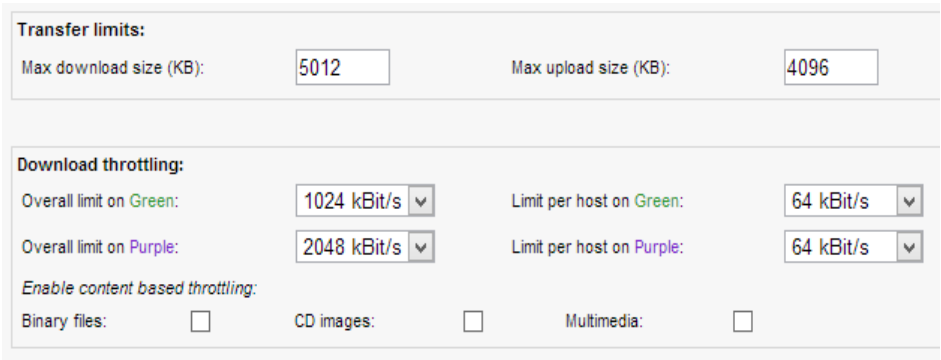
(b) Buka *web browser*. Akses halaman *website* untuk pengujian *outgoing rules* dengan ketentuan, akses *website http* (*port* 80) atau *website https* (*port* 443).

Gambar 10. Tampilan Pengujian Website http (*port* 80)

Apabila *web browser* berhasil menampilkan halaman situs (*URL*) yang diakses seperti pada Gambar 10 di atas, berarti *outgoing rules* yang ditetapkan pada Smoohtwall bekerja dengan baik dalam mengizinkan *http* atau *https*.

(3) Implementasi dan pengujian konfigurasi *Transfer Limits* dan *Download Throttling*. Untuk konfigurasinya dapat dilakukan di Smoothwall, perhatikan pada Gambar 11.

JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V10.i2 (120-140)
ISSN: 1979-9292
E-ISSN: 2460-5611

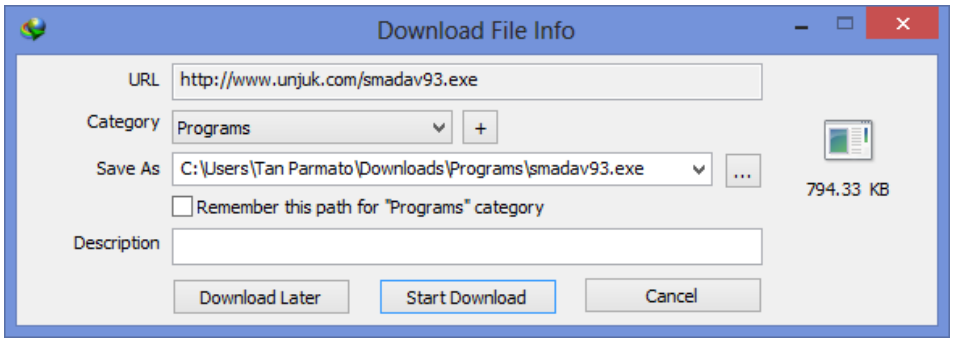


Gambar 11. Konfigurasi Transfer Limits dan Download Throttling

Setelah konfigurasi dilakukan langkah selanjutnya tahap pengujian dengan mengakses halaman *website* menggunakan *web browser*. Adapun langkah-langkah pengujiannya sebagai berikut: (a) akses *website* untuk menguji *Transfer Limits*, misal: http://www.clamav.net/lang/en/, lakukan pengunduhan dengan klik *file main.dvd*.

Gambar 12. Tampilan Akses Ditolak

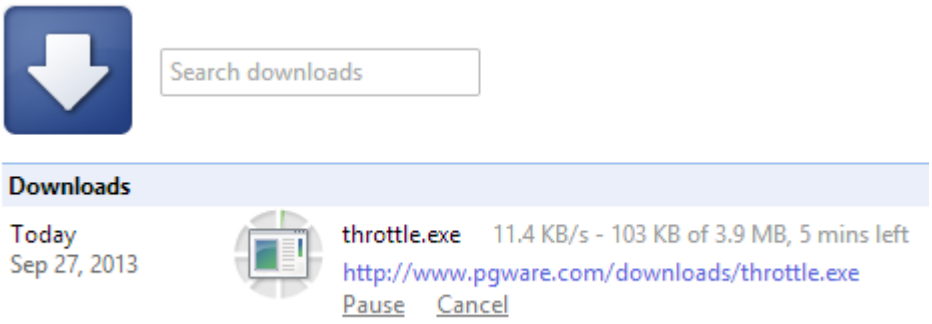
Apabila *web browser* berhasil menampilkan pesan seperti pada Gambar 12 di atas, berarti konfigurasi *transfer limits* bekerja dengan baik karena pengguna (*user*) melakukan pengunduhan dengan ukuran *file* 61 MB (62464 KB), sedangkan ukuran unduhan yang diizinkan maksimal 5 MB (5012 KB). (b) akses website http://www.smadav.net/, lakukan *unduh* dengan klik teks *Download Rev. 9.3*.



Gambar 13. Tampilan Unduh File

Apabila muncul tampilan seperti pada Gambar 13 di atas, berarti konfigurasi *transfer limits* juga bekerja dengan baik karena pengguna (*user*) hanya melakukan pengunduhan dengan ukuran *file* kurang dari 1 MB (794.33 KB), artinya kurang dari batas maksimal yang ditentukan 5 MB (5012 KB).

(c) Unduh sebuah file untuk menguji *download throttling* (batas kecepatan *download* untuk setiap *user*). Dalam hal ini dilakukan uji coba unduh sebuah *file exe* (*throttle.exe*) dengan ukuran 3.9 MB, perhatikan Gambar 14.

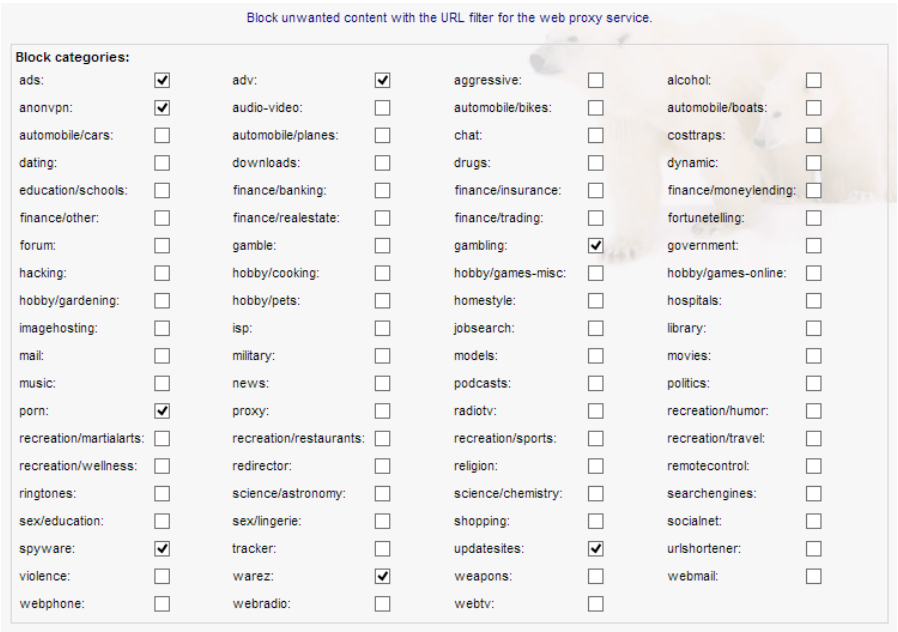


Gambar 14. Tampilan Hasil Unduhan

Gambar 14 di atas menunjukkan bahwa kecepatan unduh berhasil ditekan dengan kisaran 11.4 KB/s - 103 KB/s. 11 KB/s untuk setiap *user* dengan kondisi *traffic* tinggi dan 103 KB/s untuk kondisi *traffic* normal. Itu berarti konfigurasi *download throttling* sudah berjalan dengan baik.

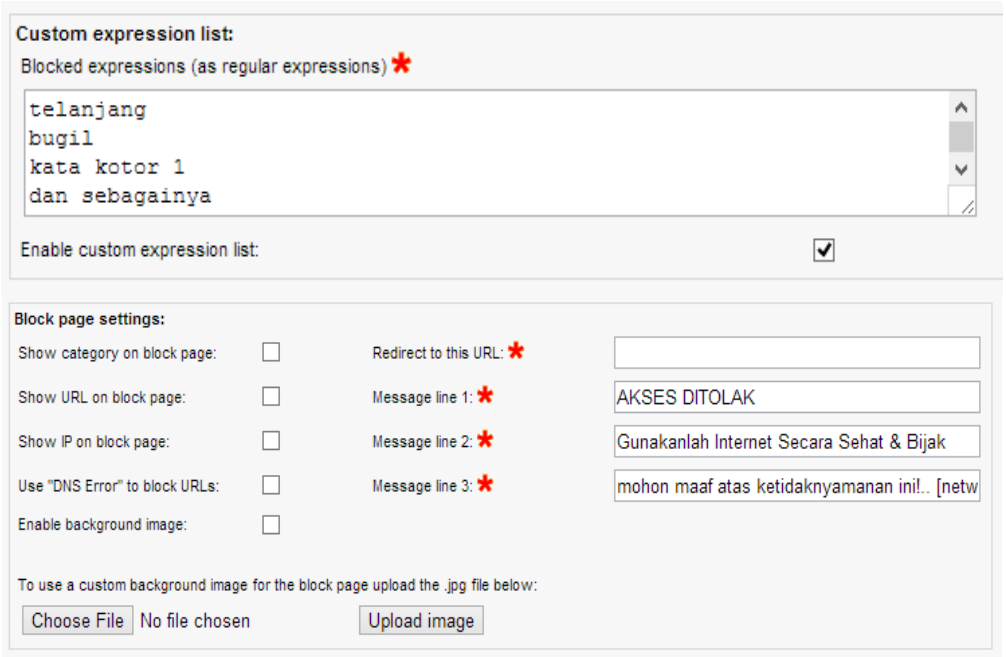
(4) Implementasi dan pengujian konfigurasi *Web Filtering*. Untuk konfigurasinya dapat dilakukan di Smoothwall. Perhatikan Gambar 15.

JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V10.i2 (120-140)
ISSN: 1979-9292
E-ISSN: 2460-5611



Gambar 15. Konfigurasi Block Categories

Pada Gambar 15 di atas, ada beberapa kategori *website* yang diblok seperti *porn*, *warez*, dan *updatesites*. Sedangkan untuk penggunaan *keyword* dengan kata-kata kotor (*bad word*) dalam pencarian dapat diblokir dengan cara seperti dicontohkan pada Gambar 16.



Gambar 16. Konfigurasi Bad Word

ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)

Pada konfigurasi di atas, setiap pengguna (*user*) yang mencoba menggunakan *keyword* dengan kata-kata kotor termasuk mengakses situs-situs (*URL*) dengan *block categories rules*, maka sistem akan memberikan pesan peringatan "AKSES DITOLAK".

Setelah konfigurasi dilakukan langkah selanjutnya tahap pengujian dengan mengakses halaman *website* menggunakan *web browser*. Adapun langkah-langkah pengujiannya sebagai berikut: (a) akses *website* untuk menguji *web filtering* dengan *block categories*, misal: http://www.youporn.com, dan http://keygen.us/.

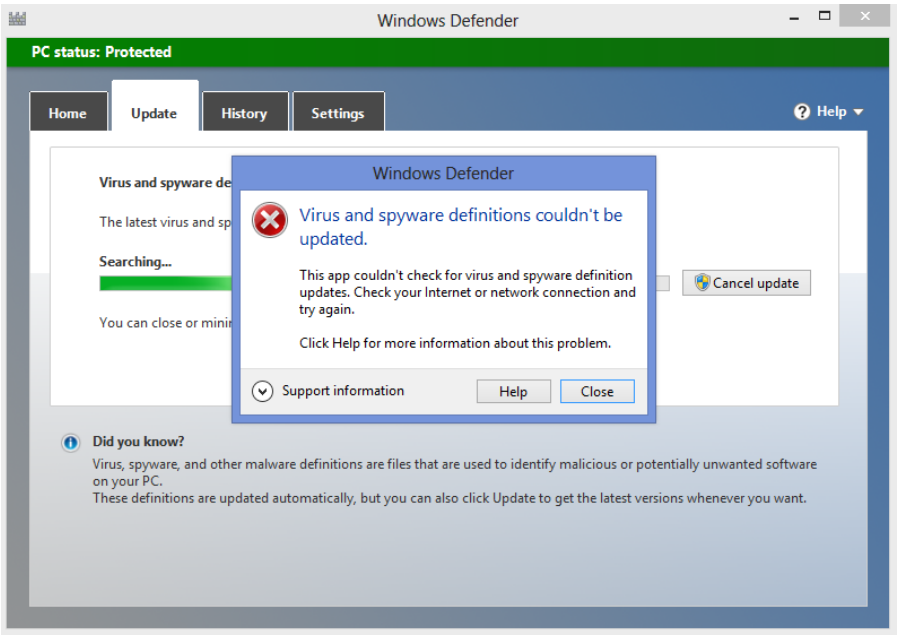
(b) Akses *website* untuk menguji *web filtering* dengan penggunaan *keyword* kata-kata kotor, misal: bugil, telanjang, dan lain sebagainya.

Gambar 17. Tampilan Akses Ditolak

Apabila *web browser* berhasil menampilkan halaman seperti pada Gambar 17 berarti *web filtering* pada Smoohtwall bekerja dengan baik dalam memblokir situs (*URL*) yang tidak diinginkan dan dapat memberikan respon penolakan dengan pesan peringatan.

Untuk *Updatesites* uji dengan melakukan *update* terhadap aplikasi yang ada seperti antivirus *Windows Defender*. Apabila sistem berhasil menampilkan halaman seperti pada Gambar 18, berarti *web filtering* pada Smoohtwall bekerja dengan baik dalam menolak *updatesites* karena secara umum untuk *meng-update* sebuah sistem operasi maupun aplikasi akan menghabiskan banyak *bandwidth* dengan tingkat *traffic* yang tinggi.

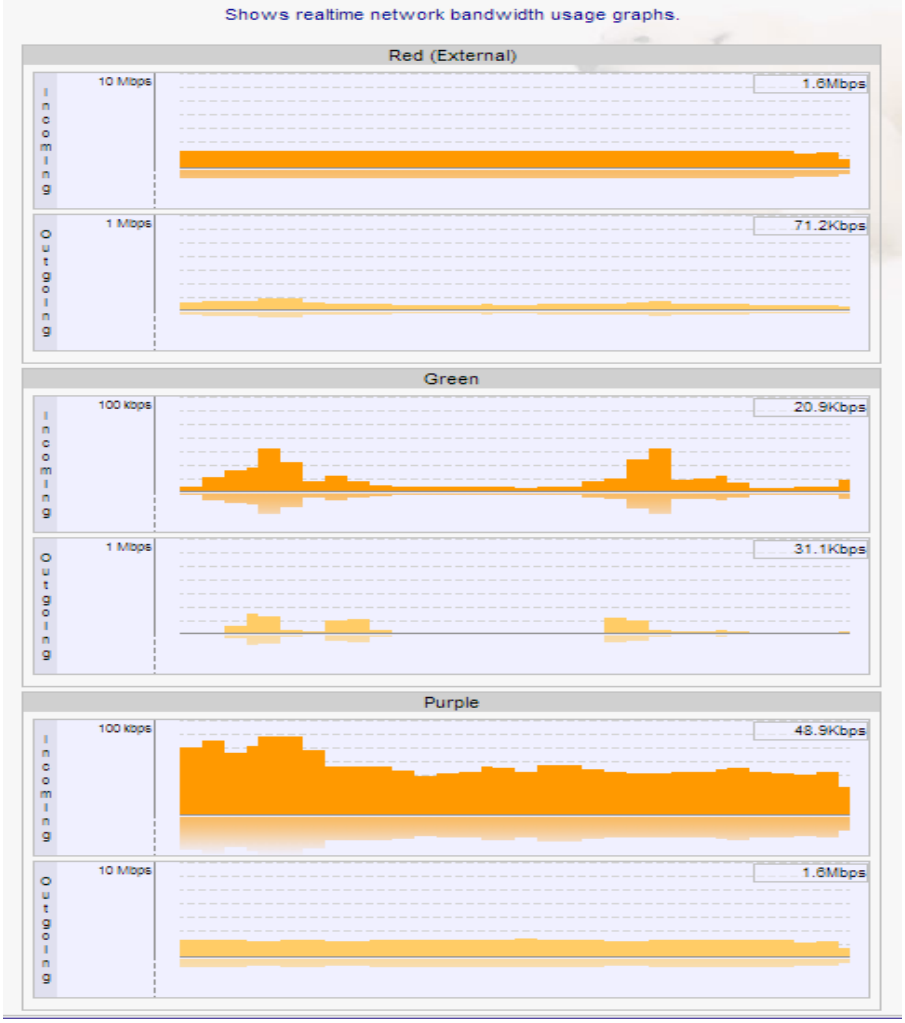
ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)



Gambar 18. Tampilan Penolakan Updatesites

Selain hasil yang didapatkan dari implementasi pengujian pada setiap kriteria tes yang diberikan dari skenario pengujian, hasil lain dari pengembangan sistem pengendalian *traffic* dan *web filtering* pada jaringan internet berbasis *hotspot* juga berupa analisa mengenai perbandingan data yang diperoleh dari monitoring menggunakan Smoothwall dan tanpa menggunakan Smoothwall (sistem manual secara konvensional). Perbandingan hasil pengujiannya dapat dilihat dari gambar-gambar berikut.

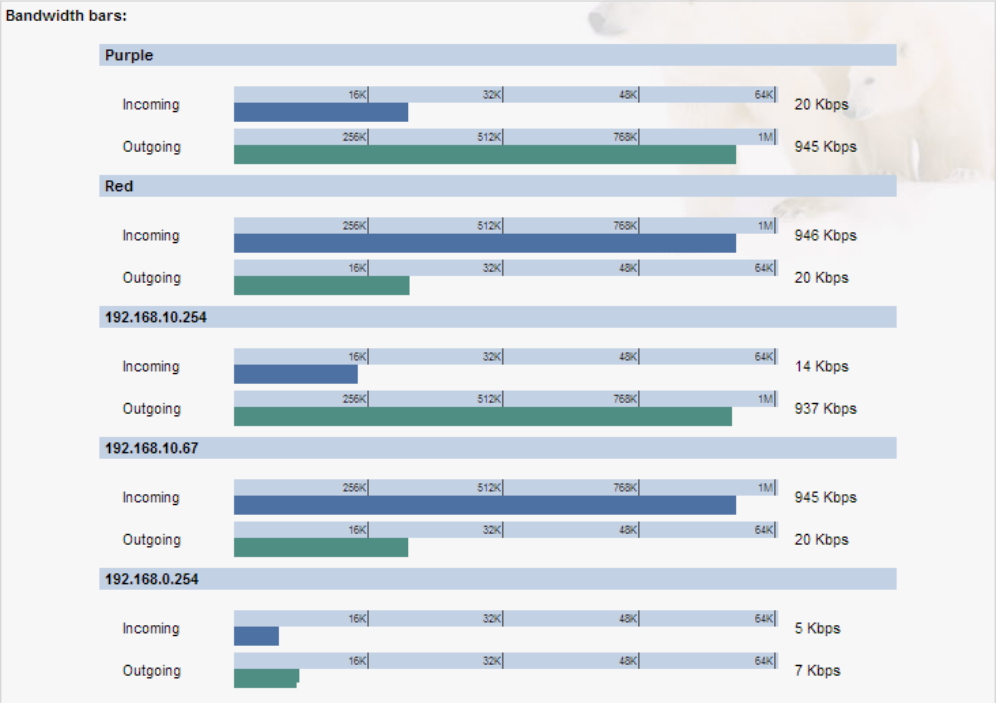
ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)



Gambar 19. Monitoring Traffic Pada Smoohtwall

Pada Gambar 19 merupakan hasil monitoring *traffic* pada Smoohtwall secara *realtime*. Monitoring berupa grafik baik pada *interface* LAN lokal, *hotspot* dan internet. Hasil monitoring *traffic* di atas menyimpulkan bahwa, dengan pemakaian *outgoing rules* pada Smoohtwall, *traffic* jaringan dapat selalu dipantau dan diketahui baik jaringan ke dalam (*incoming*) maupun jaringan keluar (*outgoing*).

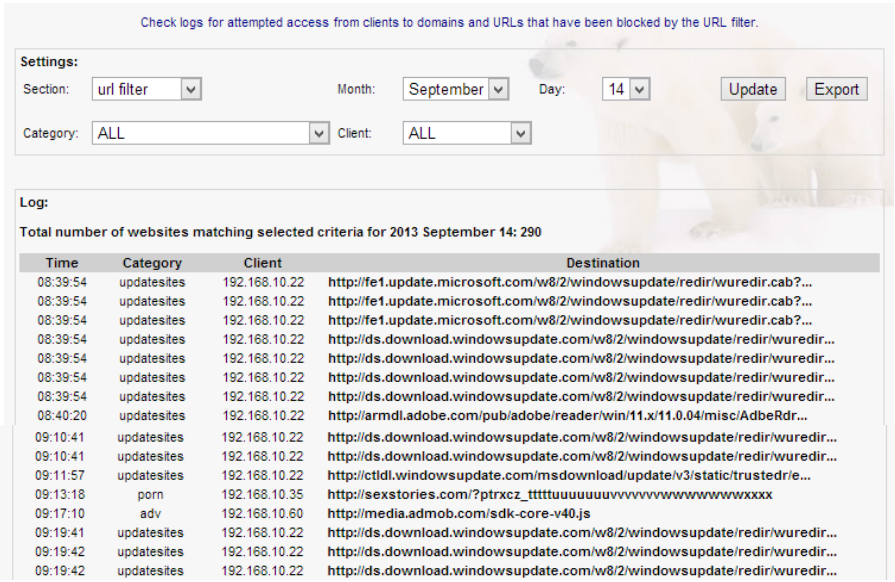
ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)



Gambar 20. Monitoring Bandwidth Pada Smoohtwall

Pada Gambar 20 merupakan hasil monitoring *bandwidth* pada Smoohtwall *secara reltime* dengan memakai metode *transfer limits* dan *download throttling*. Monitoring tersebut memberikan informasi jumlah pemakaian *bandwidth* pada jaringan internet baik pemakaian ke dalam (*incoming*) maupun pemakain keluar (*outgoing*).

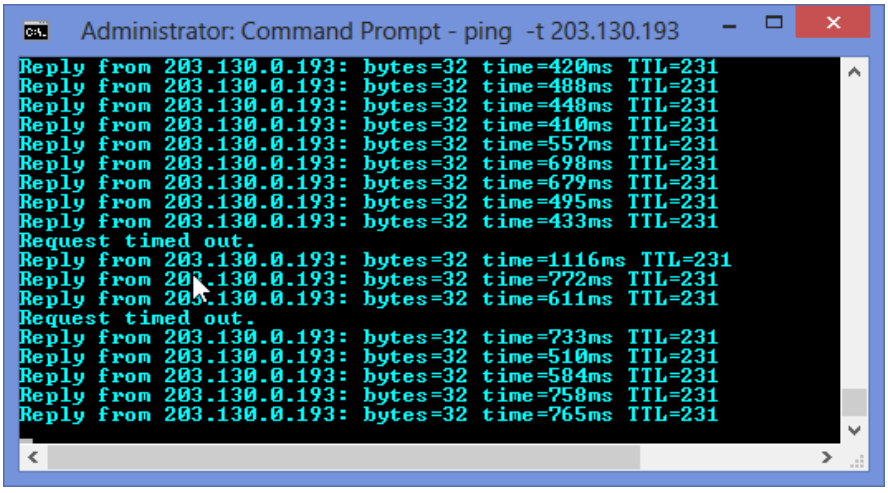
ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)



Gambar 21. Log URL Filter Pada Smoohtwall

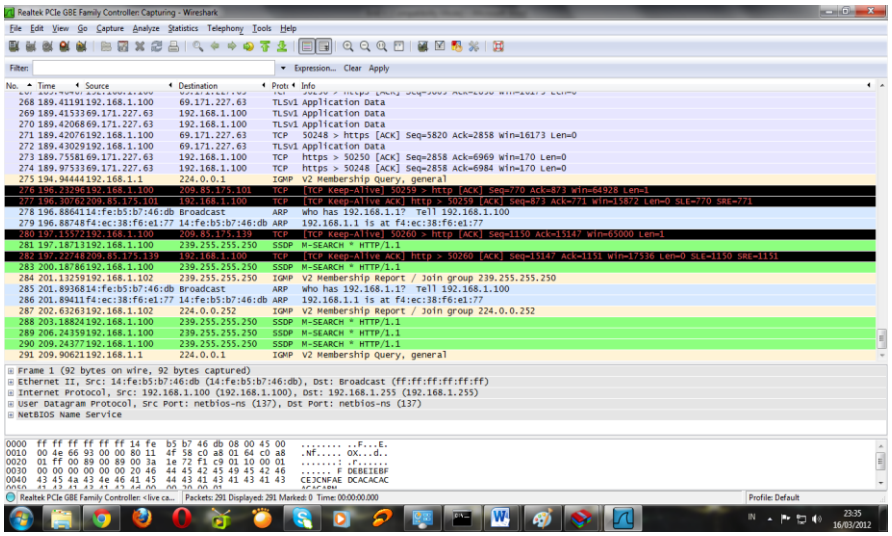
Pada Gambar 21 merupakan hasil laporan (*log*) dari penerapan *URL Filter* pada Smoohtwall. *Log* tersebut dapat dilihat berdasarkan hasil konfigurasi dari *block categories* (pada Gambar 15), serta dapat dilihat per hari dan per *IP Address*.

Sedangkan pada sistem lama (tanpa Smoothwall) tidak didapatkan data monitoring berupa grafik mengenai pemakaian *bandwidth*, maupun laporan pemakaian layanan internet karena tidak ada sistem yang mengelola hal tersebut. Hanya saja tingginya *traffic* dan bebasnya pengaksesan situs (*URL*) tanpa sensor dapat diketahui dengan melakukan tes *Packet Internet Groper* (*Ping*) dan *Network Packet Analyzer* (*Wireshark*).



Gambar 22. Tes Ping Tanpa Smoothwall

ISSN: 1979-9292
JURNAL IPTEKS TERAPAN E-ISSN: 2460-5611
Research of Applied Science and Education V10.i2 (120-140)



Gambar 23. Monitoring Traffic dan Bandwidth Tanpa Smoohtwall

Dari hasil pengujian dan monitoring data di atas dapat dijelaskan bahwa, setiap pengguna (*user*) secara bebas dapat mengakses layanan aplikasi internet tanpa adanya *filtering* dan manajemen *bandwidth* sehingga *traffic* dalam jaringan tinggi akibatnya koneksi internet sering *down* (terputus).

Dengan demikian pengembangan sistem pengendalian *traffic* dan *web filtering* pada jaringan internet berbasis *hotspot* menggunakan Smoohtwall, terbukti dapat mengendalikan *traffic* dan penyaringan halaman *website* (*web filtering*) sehingga dapat menjaga alokasi *bandwidth* yang tersedia agar kualitas koneksi jaringan lebih stabil.

SIMPULAN

Berdasarkan hasil dari pengujian yang dilakukan dalam pengembangan sistem pengendalian *traffic* dan *web filtering* pada jaringan inernet berbasis hotspot dengan menggunakan Smoothwall, maka didapatkan bahwa Smoohtwall dapat digunakan sebagai *firewall* internet untuk mengendalikan *traffic* dan penyaringan halaman *website* pada jaringan internet berbasis *hotspot* sehingga menekan konsumsi bandwidth berlebihan. Selain itu, penggabungan *add-ons extends AdvProxy* dan *URL Filter* pada Smoothwall dapat memudahkan konfigurasi *transfer limits* dan *download throttling* sehingga *traffic* pada jaringan internet terutama *hotspot* dapat dipantau dan dikelola dengan baik serta dapat memblokir pengaksesan situs (*URL*) yang tidak diinginkan dengan memberikan laporan (log) per hari dari setiap pengguna (*user*).

UCAPAN TERIMAKASIH

Penelitian ini dapat juga tidak terlepas dari bantuan dan dukungan dari berbagai pihak, untuk itu penulis ingin mengucapkan terimakasih diantaranya kepada: (1) keluarga besar SMA Negeri 10 Padang, atas izin tempat dan fasilitas untuk melakukan penelitian; (2) pembimbing akademik Dr. Rusdiyanto Roestam dan Dr. Ir. Gunadi Widi Nurcahyo, MSc. (3) rektor Universitas Putra Indonesia “YPTK” Padang Prof. DR. Sarjon Devit, S.Kom, M.Sc (4) keluarga besar dan civitas akademika Universitas

Putra Indonesia YPTK Padang dan (5) seluruh pihak yang tidak dapat dituliskan satu per satu.

DAFTAR PUSTAKA

Abdullah, Lolly Amalia. 2007. *Panduan Topologi dan Keamanan*. Direktorat Sistem Informasi Perangkat Lunak dan Konten Jakarta.

Agus. F, dkk. 2010. *Optimasi Manajemen Bandwidth Pada Jaringan Intranet Universitas Mulawarman*. Jurnal Informatika Mulawarman Volume 5 Nomor 1 Februari 2010.

Balaji, 2013. *Design of IMAR Using Proxy Server in Wireless Network*. International Journal of Advanced research in Computer Science and Software Engineering Volume 3 Issue 2, Februari 2013.

Chau M, Chen H. 2007. *A Machine Learning Approach to Web Page Filtering Using Content and Structure Analysis*. The University of Arizona. Tucson.

Gosset, Sorter 2011. *Effectivenes of Internet Content Filtering*. Journal of Information Technologies Impact Vol. 11 No. 2. 2011.

Kadam S, Kulkarni, 2012. *Improving the Performance of Squid Proxy Server by using SCSI HDD and Blocking the Media Sreaming*. International Journal of Computer Application Volume 47 No. 25. Juni 2012.

Maulana, dkk. 2010. *Implementasi Manajemen Bandwidth Intervlan Dengan VYATTA*. Politkenik Telkom, Bandung.

Novaria Kunang Y, Zuhri Yadi Ilham. 2013. *Pengembangan Sistem Autentikasi Hotspot Akademis Terpusat Berbasis Teknologi Web Service*. Seminar Nasional Aplikasi Teknologi Informasi, Yogyakarta.

Promila, Chhillar, 2012. *Wi-Fi Security by Using Proxy Server*. International Journal of Computational Engineering Research Vol. 2 Issue 5. 2012.

Rachman, dkk. 2008. *TCP/IP Dalam Dunia Informatika dan Telekomunikasi*. Informatika, Bandung.

Roy Sangita, dkk, 2012. *A Novel Approach to Prevent SQL Injection Attack Using URL Filter*. International Journal of Innovation, Management and Technology, Vol. 3 No. 5. 2012.

Sekhar S, Jain Aruna. 2013. *Hybrid Cache Replacement Policy for Proxy Server*, International Journal of Advanced Research in Communication Engineering Volume 2 Issue 3, March 2013.

Van Basten, M. 2009. *Optimasi Firewall Pada Jaringan Skala Luas*. Universitas Brawijaya.