PEMANFAATAN PERANGKAT LUNAK IP FIRE SEBAGAI PENDUKUNG SISTEM KEAMANAN JARINGAN STUDI KASUS : PT. XYZ

Arisantoso
Program Studi Teknik Informatika, Fakultas Teknik, Universitas Islam Attahiriyah
Jl. Kampung Melayu Kecil III No 15, Jakarta Selatan 12840
Email: arisantoso.kuliah@gmail.com

Abstrak

PT. XYZ bergerak di bidang jasa *design* dan digital printing terbesar di jakarta selatan, perusahaan tersebut memiliki karyawan berjumlah ± 30 orang terbagi 6 bagian seperti pimpinan, marketing, keuangan, admin, desain dan percetakan. Perusahaan ini sudah mempunyai jaringan dan akses internet dengan kecepatan *bandwidth* 3 *Mbps*. Sistem keamanan komputer saat ini terhadap ancaman dari pihak luar hanya mengandalkan antivirus gratis seperti smadav, dan Avira disetiap komputer. Dalam penggunaan akses *internet* semua karyawan masih dapat secara bebas mengakses *internet* baik situs yang positif dan situs yang negatif, pun demikian juga tidak ada pengaturan dan pengelolaan *bandwidth internet* sehingga apabila ada seorang karyawan yang sedang mengunduh data yang kapasitasnya besar tentu saja akan mempengaruhi *bandwidth internet* bagi karyawan lain yang hendak ber-internetan. Salah satu Faktor keamanan akses *internet* dapat dikelola berdasarkan hak akses dengan memanfaatkan perangkat lunak *IP Fire*, setiap karyawan dapat mengakses *internet* dengan *bandwidth* yang telah ditentukan. Metodologi yang digunakan adalah metode stress testing dikarenakan pengujian dilakukan secara bersamaan menggunakan beberapa komputer dengan cara mengakses beberapa alamat situs *website*. Hasil yang dicapai adalah menerapkan sistem keamanan jaringan *internet* pada PT. XYZ dengan memanfaatkan *IP Fire* untuk memfilter situs yang berbau pornografi dan sara dengan content filter URL dan management bandwith.

***Kata kunci**: IP Fire, Jaringan, Keamanan, Management Bandwidth, URL Filter.*

1. PENDAHULUAN

1.1. Latar Belakang

Pada umumnya, sebuah lembaga baik lembaga perusahaan, instansi, pendidikan memiliki jaringan komputer yang digunakan untuk menunjang aktifitas bisnis yang dijalankan oleh lembaga tersebut. Pemanfaatan teknologi jaringan komputer sebagai media komunikasi data digital saat ini semakin berkembang khususnya di bidang akses jaringan internet dikarenakan jaringan ini merupakan suatu jaringan kompleks dari suatu kesatuan yang terdiri dari sejumlah jaringan, khususnya memiliki bagian yang saling berhubungan dan saling tergantung. Dengan meningkatnya tingkat kebutuhan dan pemanfaatan teknologi jaringan menyebabkan para pengguna / user menginginkan akses jaringan internet yang maksimal baik dari segi efisiensi penggunaan sumber daya dengan hasil optimum serta tingkat keamanan yang baik.

Kebebasan penyediaan informasi yang ada di internet saat ini hampir tidak dibatasi, sehingga pengguna atau masyarakat luas dapat bersurfing secara bebas. Dampak dari masalah tersebut akan menyebabkan timbulnya masalah sosial, etika, moral, suku Agama dan Ras yang tidak bisa dihindari. Sebagai contoh pengguna dapat dengan mudah bersurfing untuk mengakses konten situs yang mengandung unsur porno baik berupa video, foto, gambar, artikel, cerita serta konten yang memuat hal-hal yang memojokkan, menjelek-jelekkan suatu Suku, Agama, dan Ras. Untuk membatasi penyebaran informasi pornografi dan Sara yang dapat menghancurkan moral bangsa Indonesia maka tanggal 25 Maret 2008 Dewan Perwakilan Rakyat (DPR) mengesahkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Sejak dikeluarkannya UU ITE ini, maka segala aktivitas didalamnya diatur dalam undang-undang tersebut. Salah satunya Undang-undang No. 11 dan Undang-undang No. 44 tahun 2008 tentang pornografi. Hal inilah yang menegaskan bahwa negara Republik Indonesia menentang segala macam yang berhubungan dengan pornografi dan kejahatan di dunia maya.

Perusahaan (PT. XYZ) bergerak di bidang jasa design dan digital printing terbesar di jakarta selatan, saat ini perusahaan tersebut memiliki karyawan yang berjumlah ± 30 orang terbagi menjadi 6 bagian seperti bagian pimpinan, marketing, keuangan, admin, desain dan percetakan. Secara umum Perusahaan ini sudah mempunyai jaringan komputer dan juga telah berlangganan *internet* dengan kapasitas *bandwidth* sebesar 3 *Mbps*. Namun pada sistem keamanan komputer yang berjalan saat ini terhadap ancaman dari pihak luar yang dimiliki PT. XYZ masih mengandalkan antivirus free (gratis) seperti smadav, dan Avira disetiap komputer. Kemudian dalam penggunaan akses *internet* semua karyawan masih dapat secara bebas mengakses *internet* baik situs yang positif dan negatif, pun demikian juga tidak ada pengaturan bandwidth *internet* sehingga jika ada karyawan yang sedang mengunduh data yang kapasitasnya besar tentu saja akan mempengaruhi *bandwidth internet* bagi karyawan yang lain.

Untuk memudahkan dalam memanfaatkan akses *internet* oleh karyawan secara bersama-sama diperlukan suatu perangkat lunak yang dapat mendukung sistem keamanan jaringan dan pembagian bandwidth seperti IP Fire. Prinsip dasar IPFire menitikberatkan pada fleksibilitas dan kemudahan. IPFire bisa berjalan sebagai *firewall* pada platform berspesifikasi rendah, sebagai fileserver, gateway untuk karyawan, gateway kantor cabang perusahaan atau gateway pelanggan.

1.2. Rumusan Masalah

Berdasarkan analisis yang telah dilakukan maka rumusan masalah yang akan dibahas adalah:

1. Bagaimana merancang sistem keamanan jaringan internet pada PT.XYZ ?
2. Bagaimana mengelola bandwidth internet dan mengatur akses internet kepada para karyawan di PT. XYZ ?

2. METODOLOGI

Metodologi pada penelitian ini menggunakan metode *stress testing*. Pengujian ini bertujuan untuk melihat apakat perangkat lunak secara keseluruhan mampu menangani kebutuhan sumber daya yang tidak normal. Pengujian *stress testing* ini dilakukan secara bersamaan menggunakan beberapa komputer dengan cara mengakses beberapa alamat situs website yang telah di konfigurasi dengan *Uniform Resource Locator (URL) filter* dan *management bandwidth* pada perangkat lunak IP Fire.

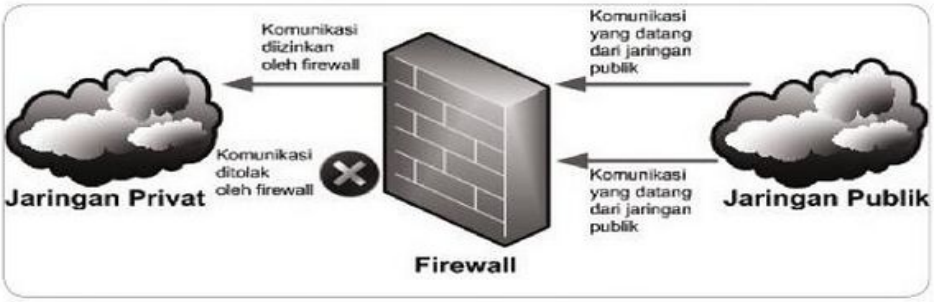
3. HASIL DAN PEMBAHASAN

3.1. Konsep Dasar Firewall

Menurut wahana (2010), *firewall* atau tembok api merupakan sistem atau perangkat yang menyaring lalu lintas jaringan yang dianggap aman untuk dilalui dan mencegah lalu lintas jaringan yang tidak aman. *Firewall* digunakan untuk mengontrol akses program atau aplikasi yang memiliki akses terhadap data keluar dan ke dalam dari komputer.

Beberapa fungsi *firewall* adalah :

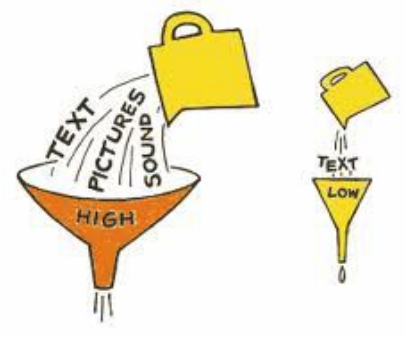
1. Melakukan pengaturan dan kontrol lalu lintas jaringan
2. Melakukan otentikasi terhadap akses
3. Melindungi sumber daya dalam jaringan privat
4. Mencatat semua kejadian, dan melaporkan kepada administrator



Gambar 1. Ilustrasi Firewall

3.2. Definisi Bandwidth

Menurut iwan (2012) pengertian *bandwidth* adalah cakupan luas atau lebar frekuensi yang digunakan oleh sinyal pada media transmisi. Dengan kata lain, *bandwidth* adalah perbedaan pada komponen sinyal frekuensi yang tinggi dan yang rendah. Proses menentukan jatah *bandwidth* kepada pemakai dan aplikasi dalam suatu jaringan dinamakan alokasi data transfer. Di dalamnya ada juga pengaturan dalam menentukan prioritas aliran data berdasarkan kepentingan dan sensitifitas data tersebut. Perusahaan yang mampu membeli kecepatan data transfer yang tinggi dari ISP akan mendapatkan *bandwidth* yang tinggi pula, namun semakin tinggi harga yang harus dibayar. Jika sebuah teknologi jaringan baru dikembangkan dan infrastruktur jaringan yang ada diperbaharui, maka aplikasi yang digunakan akan mengalami peningkatan dalam hal konsumsi jalur transmisi.



Gambar 2. Ilustrasi Bandwidth

3.3. Definisi URL Filter

Menurut ipfire.org (2014) URL-Filter dibuat untuk melakukan penyaringan akses web. Disini anda dapat melakukan pemblokiran akses internet, misalnya memblokir konten yang tidak sesuai untuk anak dibawah umur. Anda dapat memblokir domain, URL atau frase tertentu dengan mudah.

3.4. IP Fire

Menurut ipfire.org (2014) IP FIRE merupakan perangkat lunak sistem operasi yang digunakan sebagai *firewall, router, proxy server*, dan lain-lain yang berguna untuk mengamankan sistem jaringan komputer. IPFIRE di distribusikan dibawah lisensi *General Public License* (GPL) / sering kita menyebutnya linux sehingga dapat kita peroleh secara gratis dengan mengunduhnya di situs resminya yaitu http://www.ipfire.org/en/index. IP FIRE sendiri merupakan pengembangan dari IPCOP dan *Smoothwall* yang kemudian dikembangkan sendiri secara mandiri oleh team pengembang IP FIRE. Dalam mengembangkan proyek ini team pengembang IP FIRE menitik beratkan pada kemudahan instalasi, kemudahan konfigurasi karena IP FIRE dapat dikonfigurasi melalui *browser interface* dan tingkat level keamanan yang tinggi, selain itu team pengembang IP FIRE juga benar-benar memperhatikan masalah keamanan jaringan komputer secara dinamis dan berkala agar tetap aman.

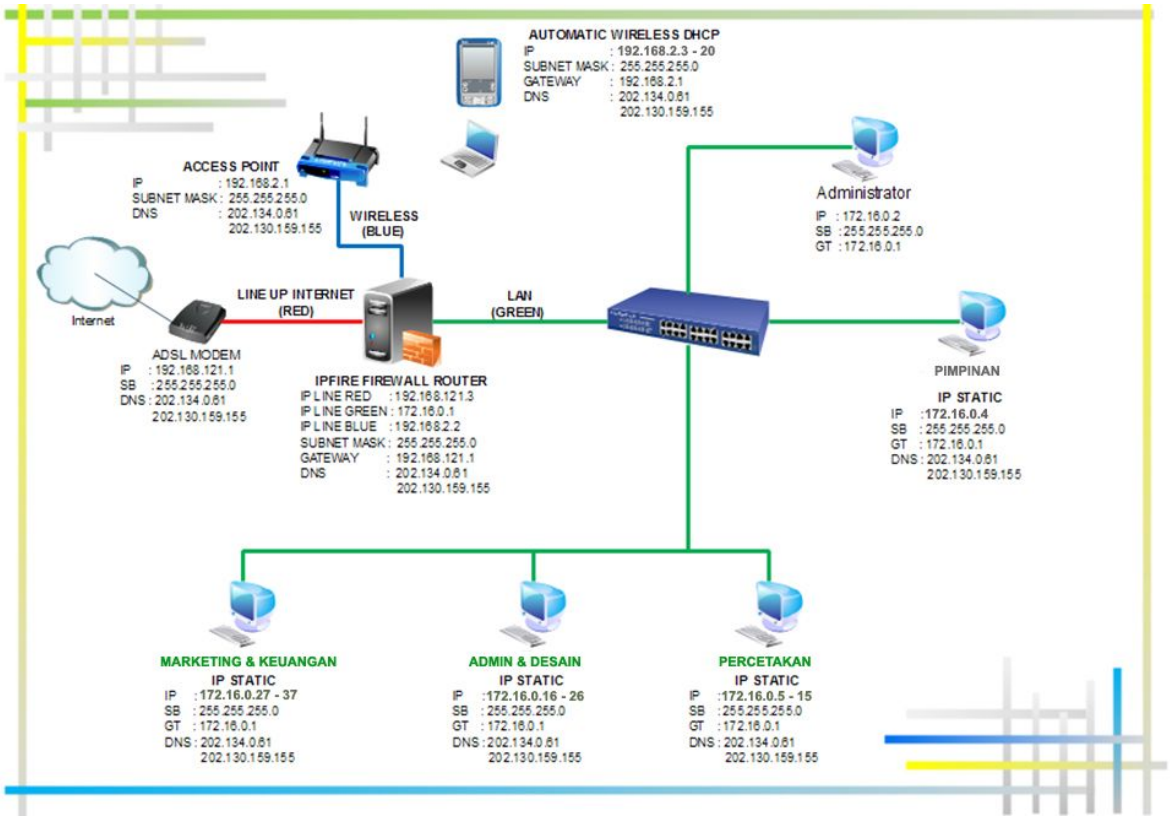
Gambar 3. Logo IP Fire

3.5. Rancangan Sistem Keamanan Jaringan

Pada tahap ini akan dilakukan perancangan sistem keamanan jaringan seperti : usulan topologi jaringan, pengkonfigurasian IP Fire sebagai URL Filter, *management bandwidth* dan alat pemantauan kondisi trafik lalu lintas data.

3.5.1. Desain Topologi

Desain topologi yang digunakan adalah desain topologi star. Pada gambar 4 terlihat ada 3 lalu lintas jaringan seperti *Line Up Internet* (RED), *LAN* (GREEN), *WIRELESS* (BLUE). Pada desain topologi ini IP FIRE *Firewall Router* difungsikan sebagai *gateway* / sebuah mekanisme yang menyediakan akses ke sebuah sistem lain yang terhubung ke dalam sebuah *network* dan sekaligus juga sebagai *traffic Filtering* (Firewall). Semua akses lalulintas data baik yang masuk dan keluar yang melewati IP Fire akan disaring terlebih dahulu untuk diperiksa, dan selanjutnya akan di kirim ketujuannya.



Gambar 4. Desain Topologi Jaringan yang diusulkan

3.5.2. Segmentasi Internet Protocol (IP)

Agar setiap komputer karwayan dapat saling berkomunikasi satu sama lainnya, komputer tersebut harus diberikan alamat komputer, alamat komputer tersebut adalah *Internet Protocol* (IP). Dalam sebuah jaringan terdapat terdapat yang disebut sebagai segmen, Segmen adalah pembagian IP pada sebuah jaringan yang telah ditentukan sedemikian rupa oleh administrator jaringan tersebut, disini akan dijelaskan tentang pembagian IP atau sering disebut sebagai segmentasi IP.

Segmentasi IP yang akan digunakan dalam implementasi yang mengacu pada gambar topologi jaringan yang diusulkan diantaranya :

1. Jalur Merah (RED) adalah segmentasi IP Fire *Router* dengan koneksi *internet* dari ADSL Router, IP Address yang digunakan adalah 192.168.121.1
2. Jalur Hijau (GREEN) adalah segmentasi IP Fire Router dengan koneksi *Local Area Network* (LAN) yang menuju *Switch Hub* ke jaringan lokal, *IP Address* yang digunakan adalah 172.16.0.1 yang nantinya IP ini menjadi *Gateway* pada komputer client untuk akses *internet*.

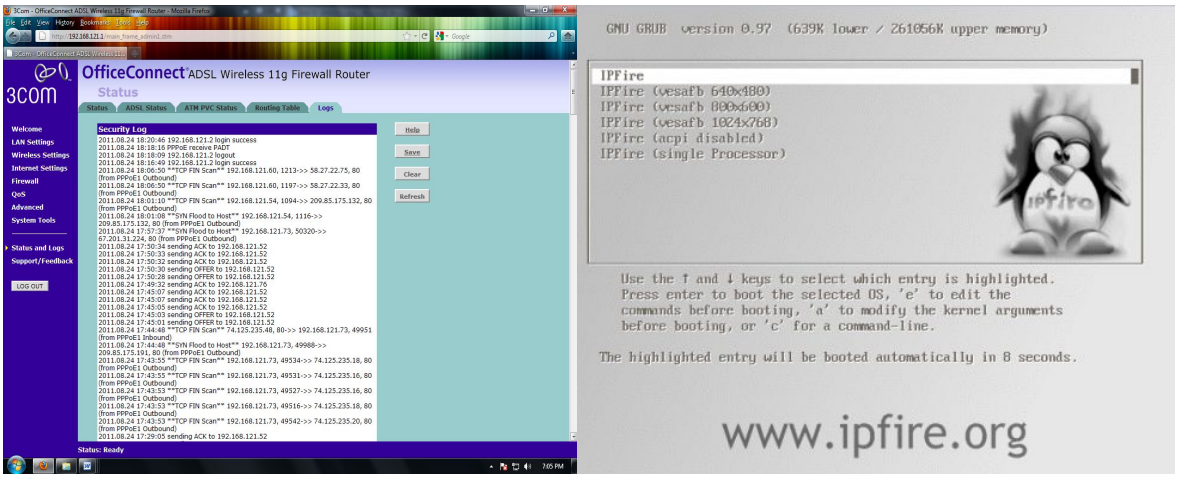
3. Jalur Biru (BLUE) adalah segmentasi *IP Fire Router* untuk koneksi internet pelanggan yang mempunyai labtop, *gadget, handphone* dan lain sebagainya dengan *Wireless*, maka perlu Access Point untuk memancarkan signalnya. IP yang digunakan adalah 192.168.2.1. IP ini akan menjadi *Gateway* untuk komputer pelanggan.

Tabel 1. Tabel Pengaturan Akses Antar Segmen *IP Fire Router*

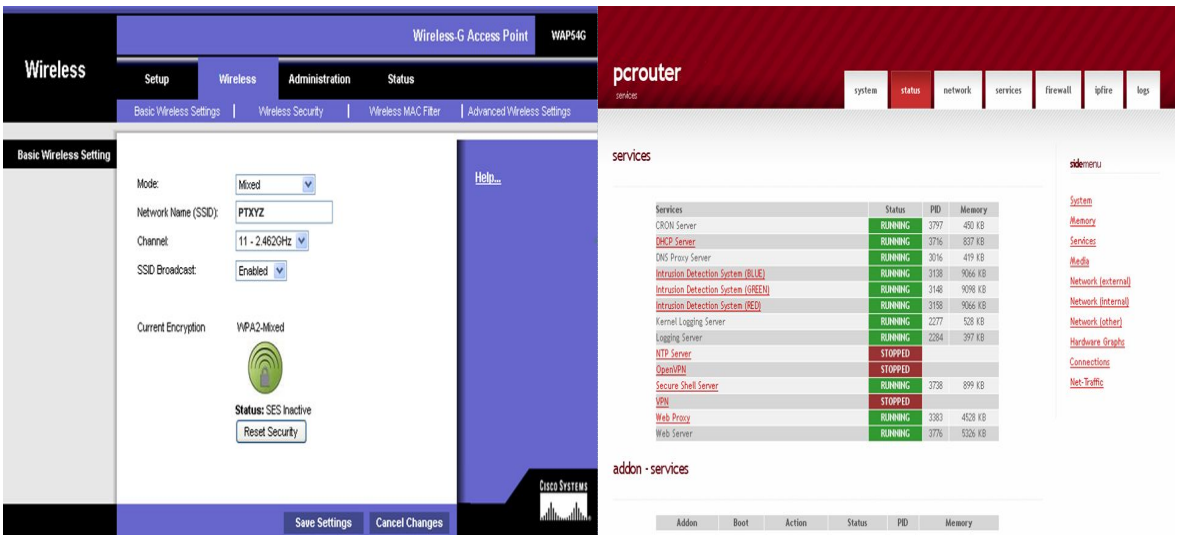
Network	IP	Status
INTERNET	192.168.121.3	Connected - (0d 0h 2m 46s)
Gateway:	192.168.121.1	
DNS-Server:	180.131.144.144	180.131.145.145
LAN	172.16.0.1	Proxy on (transparent)
Wireless	192.168.2.2	Proxy on (transparent)

3.5.3. Implementasi IP Fire

Implementasi sistem keamanan jaringan menggunakan perangkat lunak IP Fire dimulai dengan mengkonfigurasi *modem*. Setelah konfigurasi selesai selanjutnya ke tahap berikutnya melakukan instalasi dan konfigurasi pada komputer *server* dengan sistem operasi IP Fire. Selanjutnya konfigurasi *access point* dan langkah terakhir konfigurasi IP *Address* di setiap komputer *client*.



Gambar 5. Konfigurasi Modem ADSL dan Instalasi IP Fire



Gambar 6. Konfigurasi Akses Point dan Tampilan Awal IP Fire

3.5.4. Pengujian Perangkat Lunak IP Fire

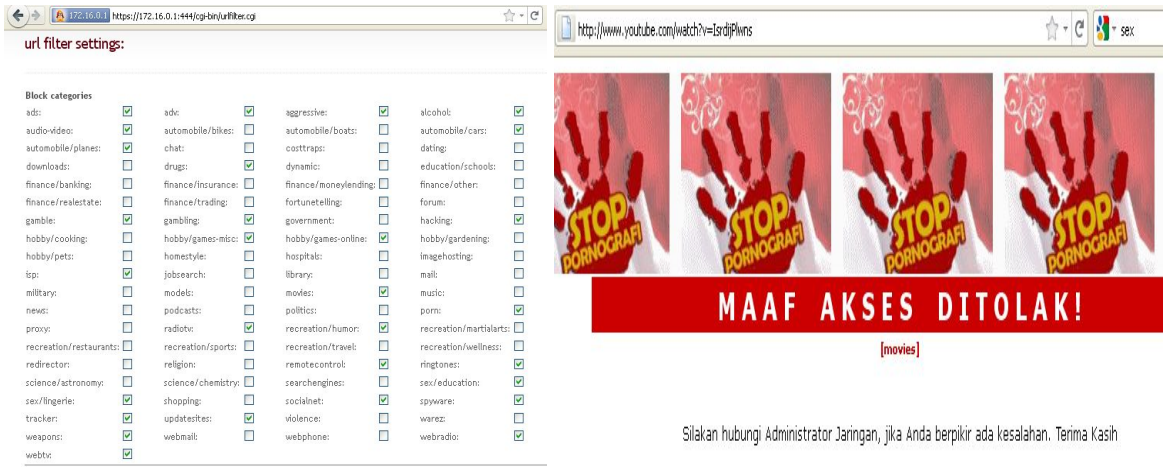
Pada proses pengujian perangkat lunak IP Fire dilakukan dengan menggunakan metode *stress test*. Proses pengujian ini dilakukan untuk mengetahui kesiapan sumber daya yang dirancang apakah sudah sesuai dengan kebutuhan yang ditetapkan sehingga pada saat implementasi dapat berjalan sesuai pada rancangan yang diusulkan. Adapun skenario pengujian perangkat lunak IP Fire pada Tabel 2 dibawah ini :

Tabel 2. Skenario pengujian perangkat lunak IP Fire

No	Fitur Perangkat Lunak IP Fire	Pengujian
1	Fitur URL Filter	Dalam pengujian ini mencoba untuk mengakses situs pornografi baik yang belum maupun yang sudah dimasukkan dalam daftar situs yang di *blacklist* sesuai dengan alamat website.
2	Fitur *Management Bandwidth*	Mencoba melakukan akses *streaming* di salah satu situs *streaming* video untuk melihat satuan kecepatan data *streaming*
3	Fitur *Intrusion Detection System* (IDS)	Melakukan serangan *icmp ping sweep* pada jaringan

3.5.4.1. Pengujian URL Filter

Fitur URL Filter ini dapat berguna untuk mengklasifikasikan *whitelist* dan *blacklist* terhadap nama domain, konten isi yang di *browsing*, dan mengklasifikasikan alamat-alamat *website* kedalam beberapa jenis kategori, seperti *Ads, Social Networking, Shopping* dan lainnya. Berikut hasil pengujian URL Filter :



Gambar 7. URL Filter dan Hasil

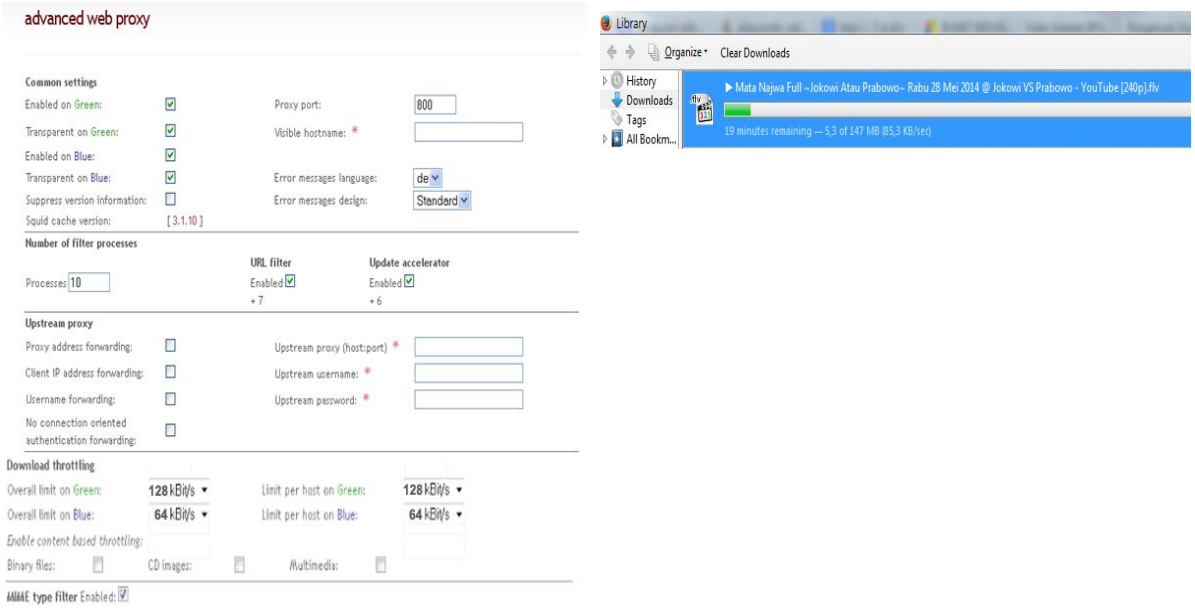
Gambar 8. Hasil URL Filter

3.5.4.2. Pengujian Management Bandwidth

Pada konfigurasi *bandwidth* ini akan diterapkan pembagian *bandwidth* berdasarkan 2 jalur lalu lintas jaringan seperti berikut :

Tabel 3. Konfigurasi Management Bandwidth

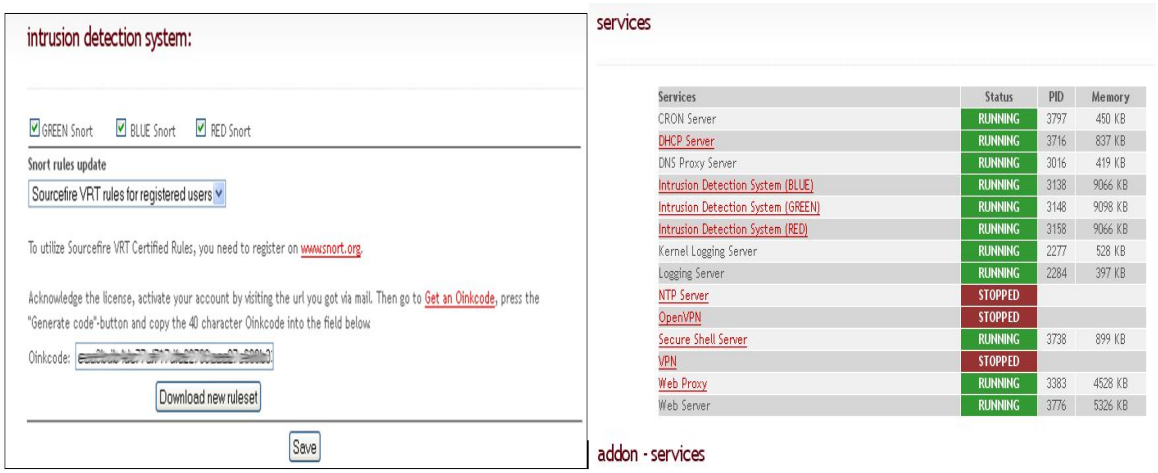
No	Jaringan	Kecepatan Bandwidth
1	GREEN	128 kBit/s
2	BLUE	64 kBit/s



Gambar 9. Pengujian *Management Bandwidth*

3.5.4.3. Pengujian *Intrusion Detection System* (IDS)

Intrusion Detection System (IDS) meruakan suatu sistem mendeteksi dan melakukan pencegahan terhadap penyusupan dan penyerangan dari jaringan eksternal maupun internal. Aplikasi IDS yang terpasang pada IP Fire adalah aplikasi *Snort* dalam situsnya www.snort.org, ini secara *default* akan terinstal dengan baik di IP Fire. Berikut pengujian *Intrusion Detection System* (IDS) pada IP Fire seperti berikut :



Gambar 10. Pengujian *Intrusion Detection System* (IDS)

4. KESIMPULAN

Atas dasar analisis dan pembahasan diatas maka dapat ditarik beberapa kesimpulan sebagai berikut :

1. Penerapan sistem keamanan jaringan *internet* pada PT. XYZ dapat dilakukan dengan memanfaatkan perangkat lunak IP Fire dikarenakan perangkat linux ini mudah diaplikasikan, tidak memerlukan lisensi *software (open source),* dan handal fungsi-fungsinya sebagai *firewall* router.
2. Pengelolaan *bandwidth management* dapat dilakukan pada menu *advanced web proxy* dengan mengatur *download throttling* baik di jaringan LAN (GREEN) maupun *Wirelless* (BLUE). Kemudian setiap karyawan dibatasi akses internetnya dengan memanfaatkan *content filter URL* di komputer *server* untuk memblokir situs-situs yang berbau pornografi dan sara.

DAFTAR PUSTAKA

Hizbullah, A. 2012. Optimalisasi Bandwidth dan Keamanan Jaringan dengan Filterisasi pada Warung Internet menggunakan Mikrotik *Routerboard.* Jurnal Komputasi Universitas Lampung, Vol 1, No. 1.

Id-Sirti. Undang Undang Informasi dan Transaksi Elektronik, www. folder.idsirtii.or.id. Diakses 17 Nopember 2014, jam 20.59.

Ipfire.org. URL-Filter. www.ipfire.org. Diakses 17 Nopember 2014, jam 20.15.

Iwan. Pengertian Bandwidth itu apa? biar tahu simak di sini. www.ridwanaz.com. Diakses : 16 Nopember 2014, jam 20.15.

Riza, T.A, Eryzebuan, Y.A., Ahmad, U.A. 2010. *Implementasi Manajemen Trafik dan Bandwidth Internet dengan IPCop.* Jurnal Inkom STMIK Bandung, Vol. IV No. 1.

Setiawan, Deris. 2005. Sistem Keamanan Jaringan. Elexmedia : jakarta 2015.

Wahana, K. 2010. Cara Mudah Membangun Jaringan Komputer & Internet. Media Kita: Jakarta.