KEAMANAN JARINGAN MENGGUNAKAN *UNIFIED THREAT MANAGEMENT* PADA *SERVER* BERBASISKAN LINUX

Bambang Heru[1]; Benny[2]; Defendy[3]; Wahyu Hento[4]

[1, 2, 3, 4]Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Bina Nusantara,
Jl. K.H. Syahdan No. 9, Kemanggisan/Palmerah, Jakarta Barat 11480
[1]bambang@inn.bppt.go.id

ABSTRACT

UTM is an application which integrated many security features become a single hardware platform. The reason behind this research is to build a system that protects the network in St. Bellarminus school. Research method that has been used in this research is spiral method, whereas the development of the application is continues and can be modified easily if there is new version of the security tools implemented in the application, or if there is a better security tools to be used. The outcome of the system is very good, because it can protects the network: cross-platform firewall, Intrusion Detection System, Proxy Server, email protection against virus and spam. In conclusion, the application can produce high effectiveness with low cost and this application is very useful in monitoring and configuring the network in St. Bellarminus school.

Keywords: *security network, unified threat management, anti virus, server, proxy, firewall*

ABSTRAK

UTM adalah suatu aplikasi yang mengintegrasikan berbagai fitur keamanan menjadi suatu platform hardware tunggal. Alasan pembangunan sistem ini adalah untuk memberikan proteksi menyeluruh pada jaringan di sekolah St. Bellarminus. Metode yang digunakan adalah metode spiral dimana pengembangan aplikasi ini akan bersifat berkelanjutan dan dapat dengan mudah diubah jika ada versi terbaru dari tools keamanan yang digunakan dalam aplikasi atau jika ada tools keamanan yang lebih baik. Hasil yang diberikan oleh aplikasi ini dapat dikatakan sangat baik karena memberikan proteksi jaringan, yaitu cross-platform firewall, Intrusion Detection System, Proxy Server, dan Proteksi terhadap -e-mail yang mengandung virus dan spam. Simpulan yang dapat ditarik dari aplikasi ini adalah aplikasi ini dapat menghasilkan efektivitas kerja yang lebih dengan biaya rendah dan aplikasi ini sangat berguna dalam memantau kondisi jaringan dan mengkonfigurasi jaringan di sekolah St. Bellarminus.

Kata kunci: *keamanan jaringan, unified threat management, anti virus, server, proxy, firewall*

PENDAHULUAN

Saat ini, media internet sudah digunakan secara luas dalam organisasi dan perusahaan. Akses dan transfer data pun dilakukan dengan mudah dan cepat. Akan tetapi dibalik itu, muncul isu keamanan jaringan yang dirasakan sangat berpengaruh terhadap perkembangan internet. Sistem jaringan yang terhubung ke internet memerlukan pengamanan yang lebih baik mengingat pemakaiannya yang juga cukup luas sehingga mengakibatkan tingkat ancaman yang juga tinggi. Beberapa ancaman muncul di internet, seperti virus, penyusupan jaringan, pencurian, perusakan, dan penyalahgunaan data. Pemanfaatan internet juga banyak disalahgunakan oleh pengguna sendiri. Dampak negatif seperti pornografi, kekerasan, perjudian, dan SARA juga menjadi permasalahan tersendiri.

Sistem pengamanan yang dapat menangani ancaman dari pihak luar melalui jaringan internet menjadi suatu hal yang mutlak dimiliki sebuah perusahaan atau organisasi. Dibalik itu, pengawasan atas pengguna koneksi internet dalam organisasi tersebut juga harus diperhatikan. Akses berlebih yang diberikan kepada pengguna akan mengakibatkan penyimpangan di luar kepentingan organisasi. Dalam hal ini, diperlukan pembatasan hak akses pengguna ke situs berisiko dan yang tidak diperkenankan oleh pihak organisasi.

Yayasan St. Bellarminus merupakan sebuah yayasan yang bergerak di bidang pendidikan dan menggunakan koneksi internet dalam kegiatan pembelajaran dan merupakan fasilitas untuk akses informasi bagi para guru dan siswa. Untuk itu, sistem pengamanan dan kontrol pengguna sangat diperlukan untuk mendukung kelancaran operasional dan kegiatan belajar mengajar. Saat tulisan ini dibuat,

Yayasan St. Bellarminus belum memiliki sistem keamanan jaringan, pemantauan jaringan, dan pembatasan hak akses pengguna ke internet.

Berdasarkan kondisi tersebut, dibutuhkan sebuah solusi sistem keamanan yang dapat melindungi data jaringan internal yayasan dari ancaman dan serangan dari luar. Sistem keamanan juga perlu dapat di-*monitor* dan di-*manage* oleh seorang *administrator* yang diberikan kewenangan terhadap sistem ini. Sistem diharapkan dapat bekerja dengan baik sehingga pengamanan jaringan dapat mendukung kegiatan operasional yayasan dan melindungi para siswa dari berbagai penyimpangan.

Ruang lingkup penelitian ini, meliputi analisis permasalahan yang dihadapi dalam hal keamanan jaringan yang terhubung ke internet meliputi keamanan dari sisi *firewall* dan *proxy*, proteksi e-mail, dan pemantauan jaringan. Perlindungan dilakukan untuk melindungi sistem jaringan internal dari ancaman pihak luar. Selain itu, akses pengguna terhadap situs akan dibatasi dari sisi *server*; Pengembangan aplikasi sistem keamanan jaringan yang mengintegrasikan beberapa *tools* keamanan jaringan yang telah ada sebagai solusi permasalahan keamanan jaringan; Aplikasi sistem keamanan jaringan ini akan diterapkan pada *platform* Linux Fedora 5 yang merupakan salah satu *distro* Linux berstatus *open source* dan banyak digunakan saat ini sebagai *network operating system*; *Tools* keamanan jaringan yang termasuk dalam sistem keamanan yang akan dikembangkan, meliputi *Antivirus*, *Firewall*, *Mail Filtering*, *Anti Spam*, *Web Proxy*, dan *Intrusion Detection System*; Sistem keamanan ini diterapkan pada Yayasan St. Bellarminus yang bergerak pada dunia pendidikan.

Tujuan penelitian adalah mengembangkan sebuah sistem keamanan jaringan menggunakan server berbasis linux pada Yayasan St. Bellarminus dengan mengintegrasikan beberapa fitur keamanan jaringan yang telah ada ke dalam suatu aplikasi berbasis web. Fitur keamanan jaringan yang diintegrasikan, antara lain *Firewall*, *Web Proxy*, *Intrusion Detection System*, Sistem *monitoring*, dan *Mail Filtering*.

Manfaat penelitian adalah mengamankan sistem jaringan pada Yayasan St. Bellarminus yang saat ini tidak memiliki keamanan sama sekali dari ancaman yang ada pada jaringan komputer; Dengan mengintegrasikan beberapa fitur keamanan yang ada dan memberikan tampilan pengaturan sehingga mempermudah dalam hal *management* dan *monitoring* jaringan; Dan pengaksesan terhadap situs yang dianggap membahayakan dapat dikendalikan.

METODE PENELITIAN

Perangkat lunak sistem keamanan jaringan dibuat dengan kemampuan dapat memperbaharui fitur keamanan yang ada secara terus menerus sehingga diperlukan pengembangan menggunakan pendekatan metode *spiral* pada fase putaran yang pertama. Berikut ini adalah – tahap yang ada, yaitu *Costumer Communication, Planning, Risk analysis, Engineering, Construction and Release*, dan *Costumer Evaluation.*

TINJAUAN PUSTAKA

Menurut Stallings (2003:4), arti keamanan jaringan adalah melindungi jaringan tetapi melindungi dalam hal ini adalah masih mempunyai artian luas. Keamanan tidak hanya tentang menjaga orang di dalam jaringan dari dunia luar. Akan tetapi, juga menyediakan akses ke dalam jaringan dengan cara yang dikehendaki, mempersilakan orang di dalam jaringan itu untuk bekerja sama. Ada beberapa elemen tentang keamanan jaringan, yaitu *Integrity* (data yang diterima sama mestilah sama dengan yang diinginkan), *Realibilit*y (data dapat digunakan secara baik tanpa ada halangan), *Availability* (ketersediaan data jika diperlukan), *Security* (data yang dikirim maupun yang diterima dilindungi dari akses yang tidak diinginkan).

International Data Corporation (IDC) yang merupakan sebuah perusahaan analisis dan penelitian pasar yang mengkhususkan dalam Teknologi Informasi dan Telekomunikasi, mendefinisikan aplikasi keamanan *Unified Threat Management* sebagai suatu produk yang menggabungkan dan mengintegrasikan berbagai fitur keamanan menjadi suatu platform *hardware* tunggal. Kualifikasi dalam kategori ini meliputi kemampuan *firewall* jaringan, *network intrusion detection and prevention* (IDP), dan *anti-virus gateway*. Semua fitur keamanan ini tidak perlu berfungsi secara sempurna tetapi perlu ada dalam produk ini. Dalam kenyataan, perusahaan besar menawarkan layanan terhadap kontrol keamanan yang sangat bervariasi berdasarkan kebutuhan (http://en.wikipedia.org/wiki/Unified_threat_management.html).

PEMBAHASAN

Sistem yang Sedang Berjalan

Sistem yang sedang berjalan, yaitu jumlah komputer yang meningkat, baik digunakan untuk bagian administrasi, guru, maupun siswa; Banyaknya perangkat lunak yang digunakan untuk mendukung proses pembelajaran, seperti *Microsoft Office*, *Adobe*, dan *Macromedia*; Penambahan perangkat keras di kelas untuk mendukung proses pembelajaran; Perhatian kepada keaslian sistem operasi; Dan pemasangan akses internet dengan kecepatan tinggi untuk mendukung penggalian informasi di dunia maya.

Yayasan St.Bellarminus memiliki dua jaringan utama, yaitu VLAN 1 dan VLAN 2. Berikut penjelasan dari masing-masing jaringan. Pertama, VLAN 1. VLAN 1 merupakan *virtual* LAN untuk jaringan guru dan karyawan dengan alamat IP *private* dengan *segment network* 193.168.10.0 /24. Kedua, VLAN 2. VLAN 2 merupakan *virtual* LAN untuk jaringan siswa menggunakan alamat IP *private* dengan *segment network* 192.168.10.0 /24. Pada jaringan ini, *server* juga berfungsi sebagai PC router. Sistem operasi yang dipakai di *server* saat ini adalah Microsoft Windows Server 2000 sedangkan *software* yang digunakan agar dapat menjadi PC *router* adalah Kerio Winroute.

Analisis Permasalahan

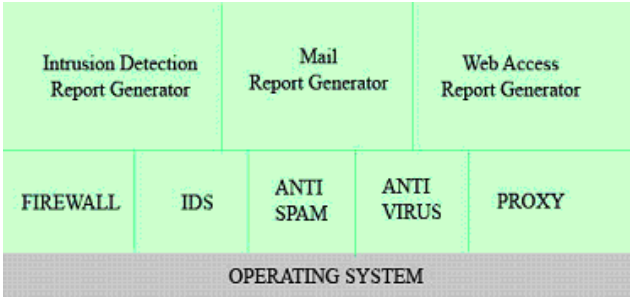
Penggunaan internet sebagai media informasi dan komunikasi yang utama bagi sekolah menimbulkan isu keamanan jaringan internal sekolah dari ancaman dan serangan di internet. Jaringan sekolah perlu mendapatkan proteksi keamanan yang baik agar terlindungi dari ancaman dan serangan di internet sehingga tidak mengganggu kegiatan pembelajaran yang sedang berjalan.

Sistem keamanan yang sekarang digunakan di yayasan St. Bellarminus kurang memberikan pengamanan yang baik dan menyeluruh. Berikut adalah beberapa kekurangan dan kendala yang masih dihadapi sistem keamanan yang sekarang digunakan: Tidak adanya fasilitas *network monitoring*; Tidak adanya sistem keamanan yang mengantisipasi *intrusion*; Tidak adanya *proxy server*; Sumber daya manusia yang tidak berspesialisasi di bidang jaringan; Kurangnya perhatian terhadap masalah keamanan jaringan; Biaya pemeliharaan yang tinggi.

Analisis Pemecahan Masalah

Peneliti memilih pemecahan masalah melalui pembuatan suatu sistem yang dapat memberikan keamanan yang menyeluruh yang disebut dengan *Unified Threat Management* (UTM). Kendala yang dihadapi oleh setiap pengguna sistem keamanan jaringan adalah *cost* dan *efficiency/usability*. Biasanya yang didapatkan dari sistem dengan *cost* yang rendah adalah *efficiency/usability* yang rendah pula. Akan tetapi, hal tersebut tidak menjadi mutlak dalam pengembangan sistem keamanan menggunakan aplikasi *open source*. Pengembangan ini juga dapat disesuaikan dengan spesifikasi dan kebutuhan sebuah jaringan.

Pada pemilihan fitur keamanan yang dibuat, diacu pada teknologi terbaru saat penelitian ini dibuat, yaitu *Network operating system* yang digunakan adalah Linux Fedora Core 5 dengan kernel 2.6.18.; *Firewall* menggunakan iptables versi kernel 2.6.18.; AntiSpam menggunakan SpamAssassin versi 3.1.7.; Database server menggunakan MySQL Server versi 5.0; Web IDE menggunakan PHP versi 5.1.6.; Web Server menggunakan Apache versi 2.0.; IDS menggunakan Snort versi 2.6.1.2.; Proxy Server menggunakan Squid 2.5; Antivirus menggunakan ClamAV 0.88.7.



Gambar 1 Arsitektur UTM

Alasan penggunaan kesemua aplikasi tersebut adalah karena aplikasi tersebut mudah untuk di-*update* melalui *tool* Linux, *Yum Updater*, dan merupakan aplikasi *open source*.

Perancangan Sistem

Pengembangan sistem solusi yang akan dilakukan pada *platform* Linux Fedora 5 yang merupakan salah satu *distro* Linux berstatus *open source* dan banyak digunakan saat ini sebagai *network operating system*. Sistem solusi ini akan menggabungkan beberapa fitur keamanan jaringan yang telah ada ke dalam suatu aplikasi yang berbasiskan web. Bahasa pemrograman yang dipilih adalah PHP sedangkan *web server* yang digunakan

adalah Apache. Untuk *database server*, digunakan MySQL.

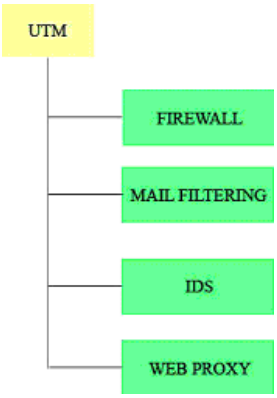
Untuk segi keamanan, digunakan beberapa cara: Memakai *store procedure* untuk mencegah *SQL injection;* Pengunaan *session* pada data; Tiap halaman dibuat validasi pengecekan session; Semua parameter yang diinput dilakukan validasi, data yang tidak sesuai akan ditolak; Semua validasi akan dijalankan di sisi server; Password pengguna akan dienkripsi dengan modul MD5.

Perancangan Fitur Sistem Solusi

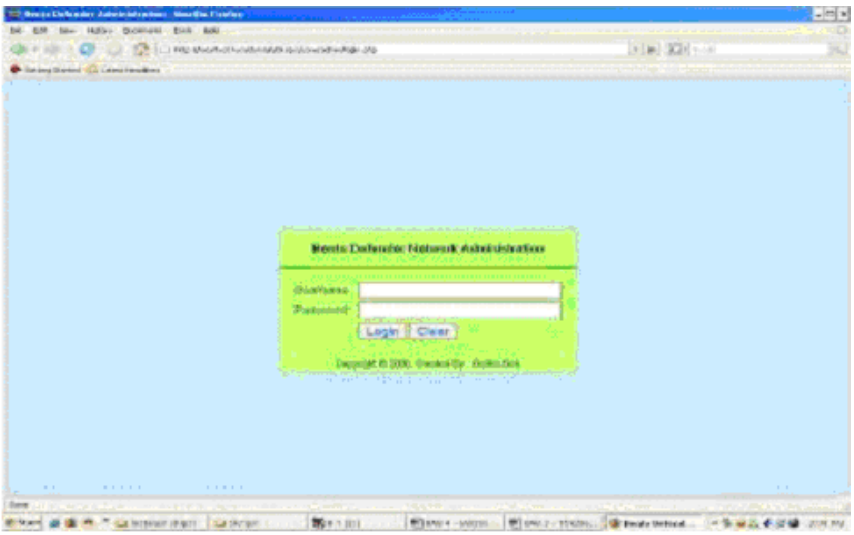
Sistem solusi yang baru akan memiliki beberapa fitur sebagai berikut. Pertama, *Firewall*. *Firewall* digunakan untuk mengontrol akses dari internet ke jaringan internal dan dari jaringan internal ke internet. Aplikasi yang digunakan adalah aplikasi iptables yang langsung terdapat pada Linux Fedora Core 5. Kedua, *Web Proxy*. *Web proxy* digunakan untuk *caching proxy server* dan pembatasan hak akses ke internet. Aplikasi yang digunakan adalah aplikasi squid sebagai *proxy controller* dan SARG (*Squid Analysis Report Generator*) sebagai *HTML-based proxy report generator*. Ketiga, *Intrusion Detection System*(IDS). *Intrusion Detection System* digunakan untuk menangkap *intruder* atau penyusup jaringan. Aplikasi yang digunakan adalah aplikasi snort sebagai IDS *controller* dan ACID (*Analysis Console for Intrusion Detection*) sebagai *HTML-based IDS report generator.* Keempat, *Mail Filtering*. *Mail Filtering* digunakan untuk *scan* dan *filter* setiap *e-mail* yang masuk atau keluar dari domain jaringan. Aplikasi yang digunakan adalah qmail *scanner* yang diintegrasikan dengan clamAV sebagai *antivirus* dan spamassassin sebagai *Anti Spam* sedangkan untuk *HTML-based mail report generator* digunakan isoqlog (Lihat Gambar 2).

Implementasi

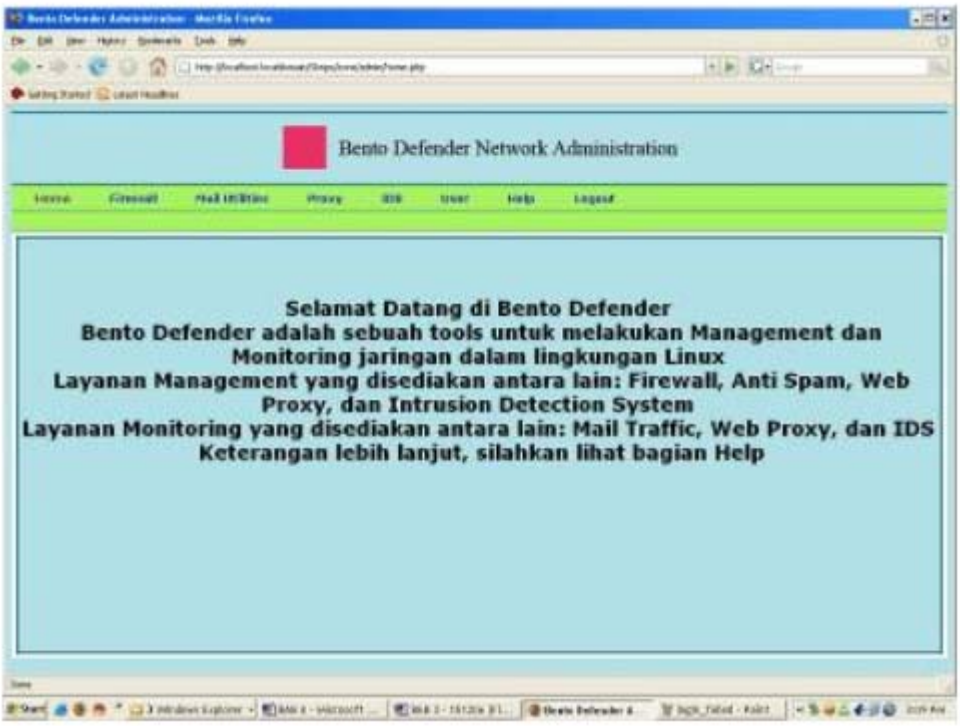
Jika nama *user* dan *password* benar maka administrator dapat mengakses sistem dengan tampilan awal di halaman *home* (Lihat Gambar 4).



Gambar 2 Perancangan Fitur Sistem Solusi

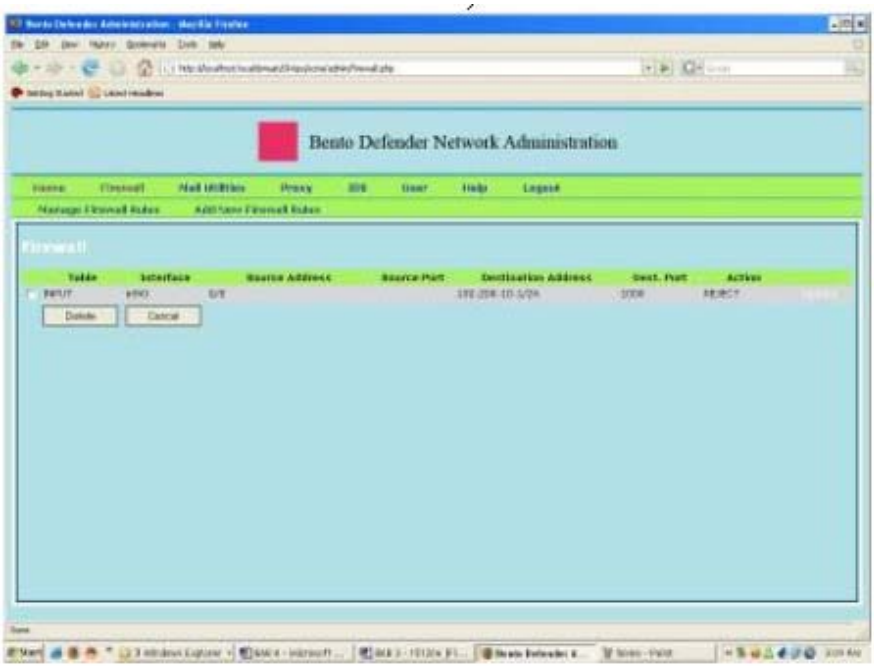


Gambar 3 Halaman *Login*



Gambar 4 Halaman *Home*

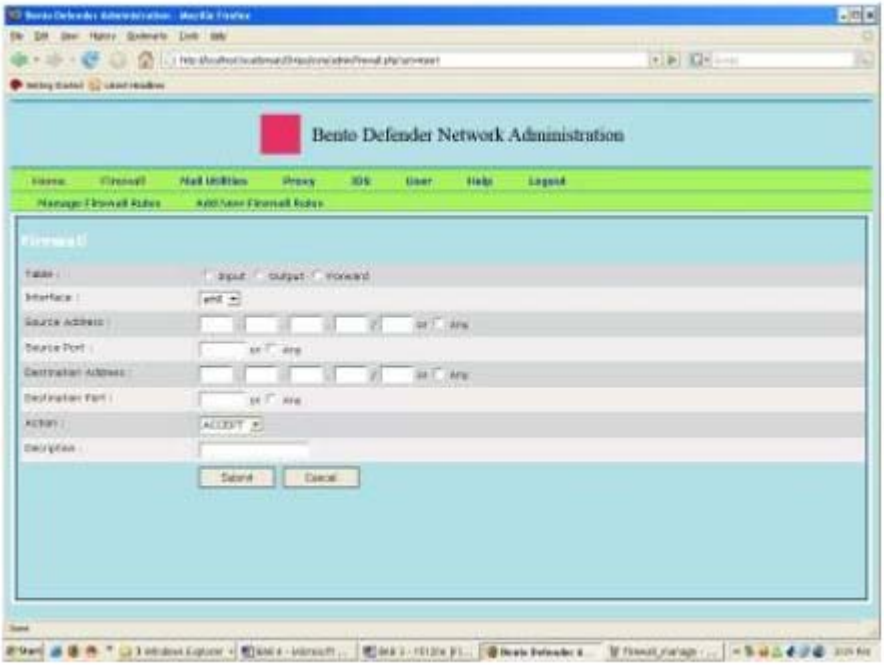
Administrator dapat mulai menggunakan sistem dari pilihan menu yang tersedia: *Firewall*, *Mail Utilities*, *Proxy*, *IDS*, *User*, *Help*, dan *Logout*. Jika membuka menu *Firewall*, administrator dapat melihat *rule-rule firewall* yang telah ditambahkan (*rule* ini tidak termasuk *rule* yang sudah ada dalam sistem ketika Linux di-*install*) (Lihat Gambar 5).



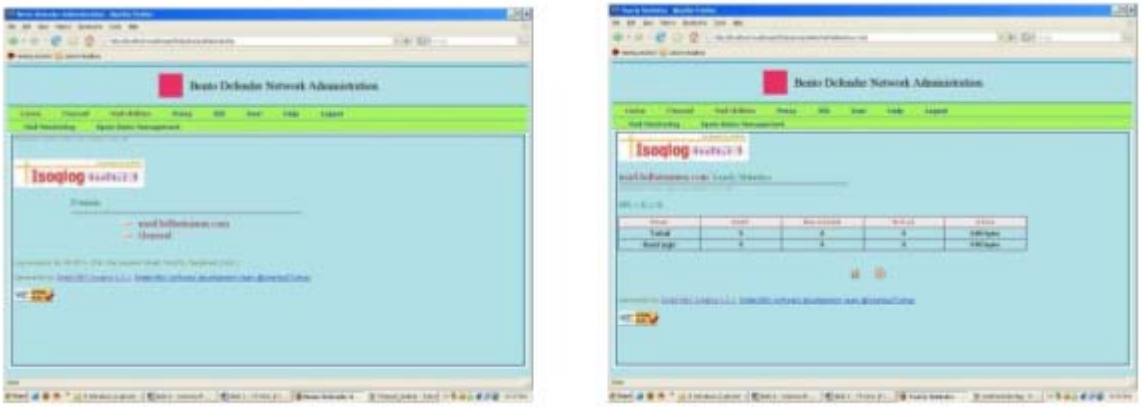
Halaman 5 *Firewall*

Submenu yang ditampilkan adalah *Manage Firewall Rules* dan *Add New Firewall Rules*. Jika ingin menambahkan *rule* dalam *firewall*, administrator dapat memasukkannya di halaman *Add New Firewall Rules* atau jika ingin mengubah *rule* dalam *firewall*, administrator dapat melakukannya di halaman *Add NewFirewall Rules* dengan parameter yang sudah terisi (Lihat Gambar 6).

Rule dapat dihapus dari halaman *Manage Firewall Rules* melalui tombol '*Delete*'. Dari pilihan menu utama, administrator dapat melihat data pengiriman *e-mail* di menu *Mail Utilities* (Lihat Gambar 7).



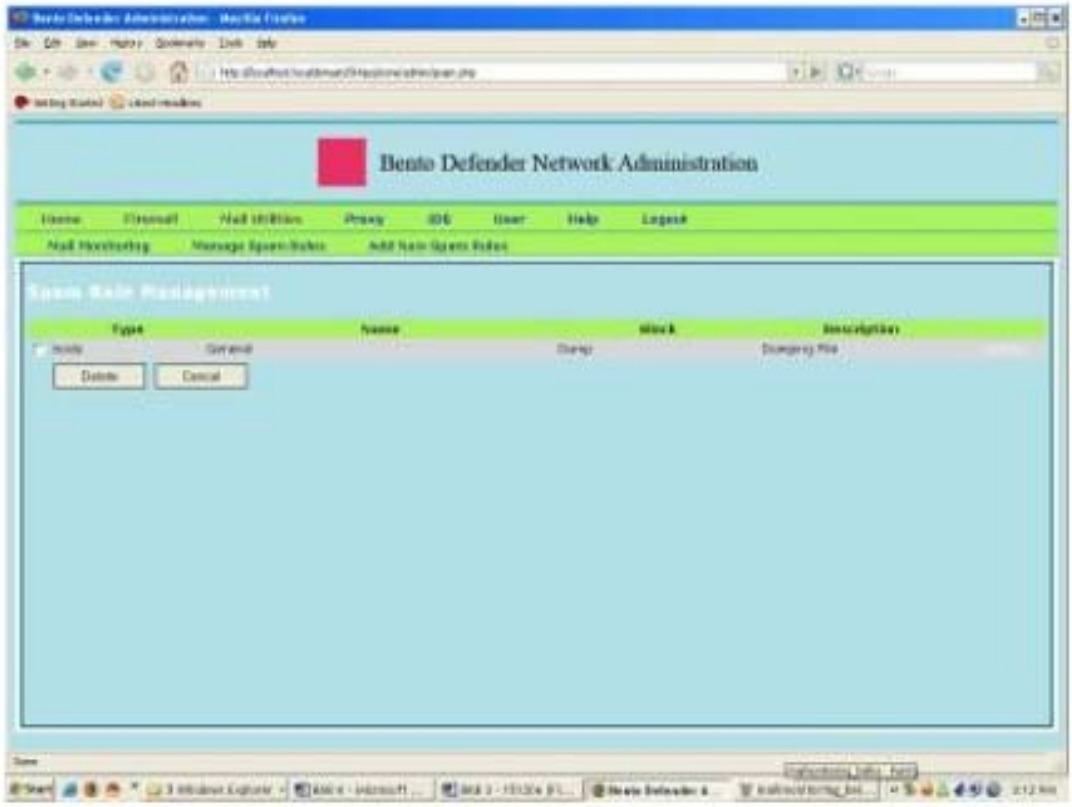
Gambar 6 Halaman Menambah dan Mengubah *Rule Firewall*



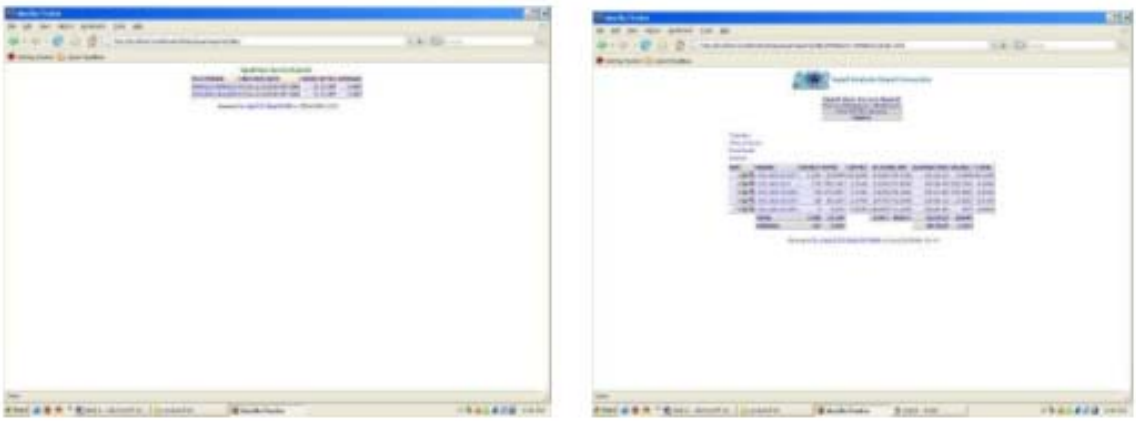
Gambar 7 Halaman *isoqlog*

Jika administrator memilih *Spam Rules Management* maka administrator dapat mengatur *rule* untuk kriteria *spam* (Lihat Gambar 8).

Submenu yang ditampilkan sama seperti halaman *Firewall* dan fiturnya sama seperti *Firewall*. Jika administrator memilih *Proxy* maka administrator dapat melihat data para pengguna jaringan dalam lingkup harian, mingguan, dan bulanan (Lihat Gambar 9).



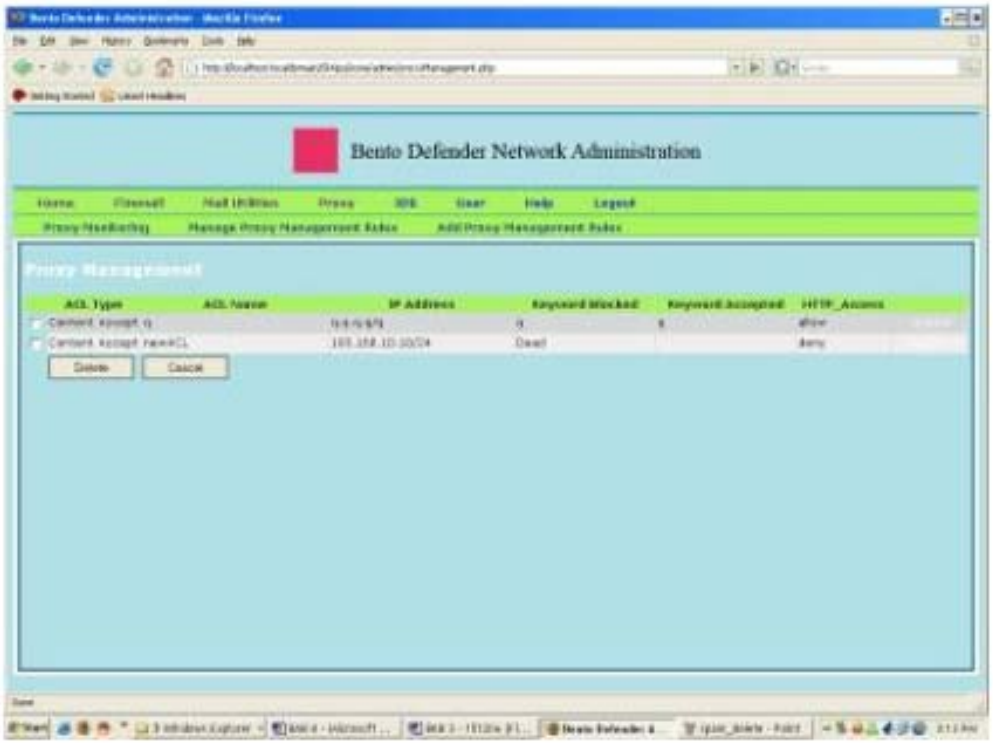
Gambar 8 Halaman *Spam*



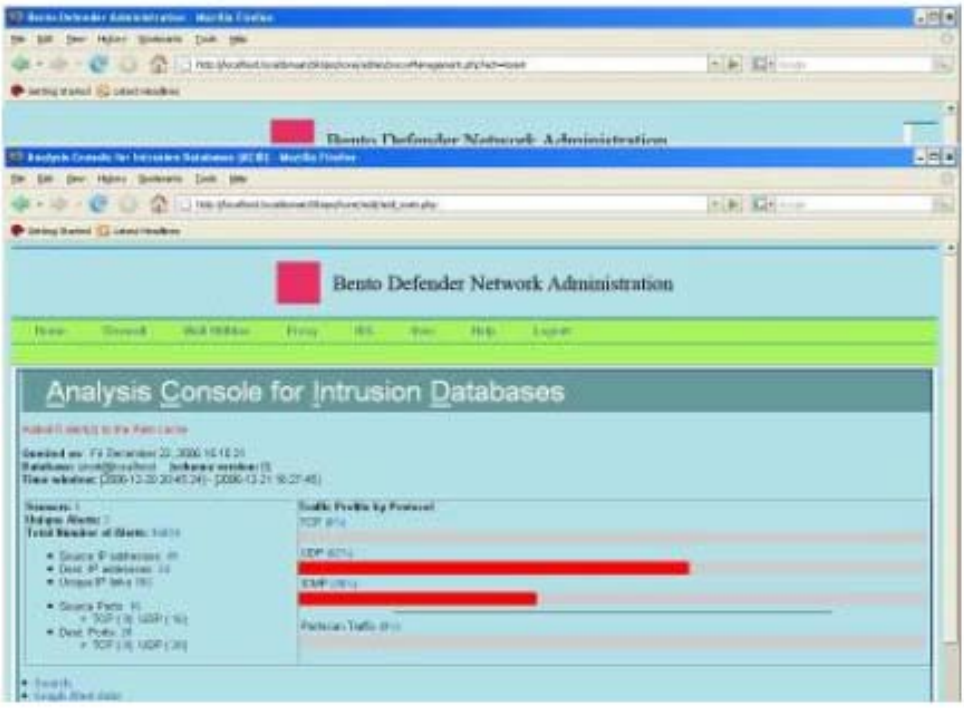
Gambar 9 Halaman *sarg*

Jika administrator memilih *Proxy Rules Management* maka administrator dapat mengatur *rule* untuk membatasi situs dan akses pengguna jaringan (Lihat Gambar 10).

Submenu yang ditampilkan sama seperti halaman *Firewall* dan fiturnya sama seperti *Firewall.* Jika administrator memilih *IDS* maka administrator dapat melihat data *intrusion* yang tercatat dalam sistem (Lihat Gambar 11).



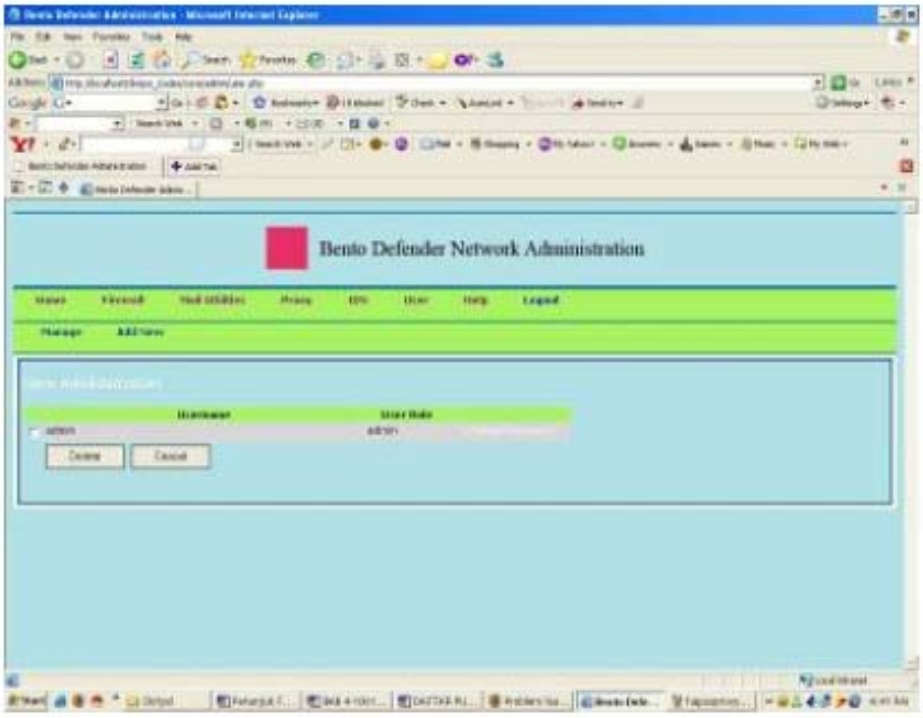
Gambar 10 Halaman *Proxy Management*



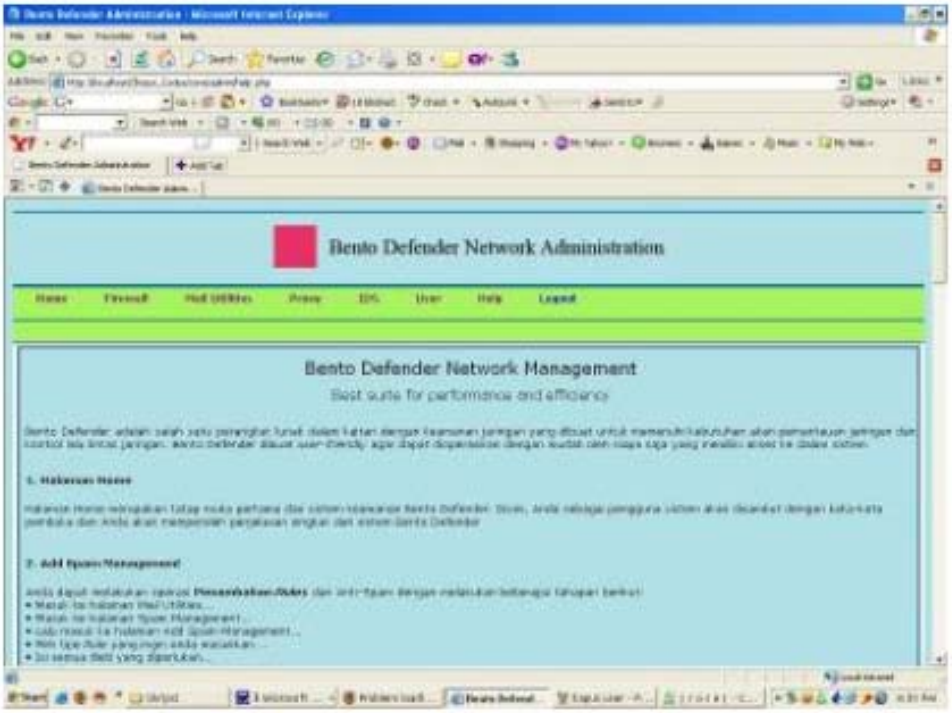
Gambar 11 Halaman *ACID*

Jika administrator memilih *User* maka administrator dapat melakukan penambahan, penghapusan, dan pengubahan pengguna sistem (Lihat Gambar 12).

Submenu yang ditampilkan adalah *Manage, Delete,* dan *Add New*. Jika ingin menambahkan *user* yang dapat mengakses sistem, administrator dapat memasukkannya di halaman *Add New*. Jika administrator memilih *Help* maka administrator dapat melihat petunjuk penggunaan sistem Bento Defender (Lihat Gambar 13).



Gambar 12 Halaman *User*



Gambar 13 Halaman *Help*

Jika administrator ingin mengakhiri administrasi sistem, administrator harus memilih *Logout* dengan menjawab **Yes** (Lihat Gambar 14).

Evaluasi Kemampuan Fitur Sistem

Untuk mengukur kinerja sistem, diadakan beberapa pengujian terhadap *tools* yang digunakan. Pengujian yang dilakukan, antara lain sebagai berikut. Pertama, pengujian dengan mengirimkan *email Spam* (Lihat Tabel 1).

Dari data di atas, didapatkan rata-rata ketepatan penyaringan *Spam* senilai:

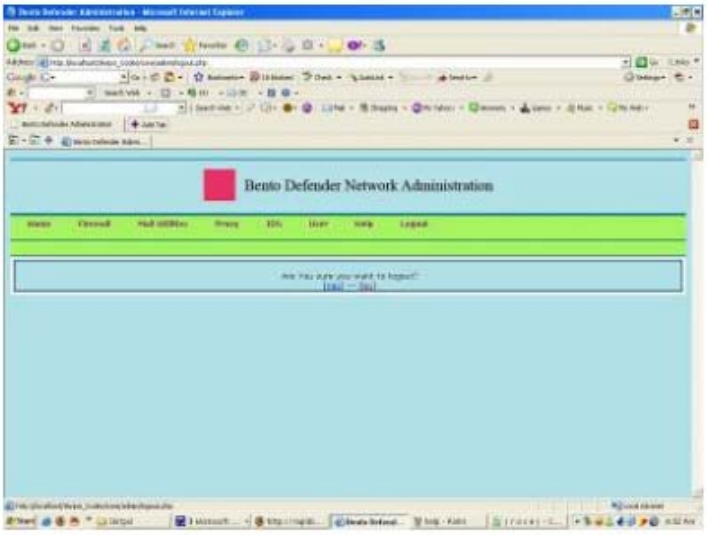
= (90 + 100 + 90 + 95 + 85) : 5
= 92.50 %

Jadi, rata-rata persentase ketepatan penyaringan *email* yang mengandung *Spam* adalah 92.50% sedangkan sebesar 7.50% ketidaktepatan pemfilteran disebabkan oleh padatnya lalu lintas jaringan dan banyaknya *email* yang masuk dalam satu satuan waktu. Kedua, pengujian dengan mengirimkan *email* dengan *attachment Virus* (Lihat Tabel 2).

Dari data di atas, didapatkan rata-rata ketepatan pendeteksian *email* bervirus senilai:

= (100 + 100 + 98.33 + 96.67 + 96) : 5
= 98.20 %

Jadi, rata-rata persentase ketepatan pendeteksian *email* bervirus adalah 98.20% sedangkan sebesar 1.80% ketidaktepatan pendeteksian disebabkan oleh banyaknya *client* yang dikirimi virus. Dari hasil ini, dapat ditarik simpulan bahwa Anti Virus ClamAV menunjukkan kinerja yang menurun dalam intensitas *email* y ang tinggi tetapi masih dalam batas yang dapat ditolerir.



Gambar 14 Halaman *Logout*

Tabel 1 Hasil Pengujian Penyaringan *Spam*

No.	Kata-Kata	Email ditolak	Email terkirim	Persentase
1	SPAM	18	2	90
2	PORN	20	0	100
3	SEX	18	2	90
4	XXX	19	1	95
5	DRUGS	17	3	85

Tabel 2 Hasil Pengujian Pengiriman *Email* Bervirus

No.	Jumlah email	Email ditolak	Email terkirim	Persentase
1	20	20	0	100
2	45	45	0	100
3	60	59	1	98.33
4	120	116	4	96.67
5	150	144	6	96

Ketiga, pengujian *rule firewall* dan *proxy*. Pengujian ketepatan *rule firewall* dan *proxy* dilakukan dengan menambah *rule* baru di *port* yang biasa digunakan seperti port 80 (HTTP) dan 25 (TELNET). Dan dilakukan penutupan semua port dan alamat tujuan. Setelah itu, dilakukan akses dari komputer *client* ke situs sembarang dan menghasilkan laporan berikut.

Tampilan pembatasan akses situs

Evaluasi dari Sisi Teknis dan Kelebihan

Pada Tabel berikut, disajikan informasi mengenai perbandingan sistem keamanan jaringan dari beberapa vendor dengan sistem keamanan Bento Defender (Lihat tabel 3).

Berdasarkan hasil wawancara dengan staf IT yang menggunakan aplikasi ini, didapat hasil evaluasi secara menyeluruh sebagai berikut: Dengan adanya aplikasi Bento Defender, akses kepada situs yang tidak layak dapat dibatasi; Staf IT dapat melakukan pemantauan terhadap aktivitas jaringan, baik yang bersih atau mengandung ancaman; Pembaharuan versi *tools* Bento Defender dapat dilakukan dengan mudah melalui *Yum Updater*; Pengaturan terhadap *tools* keamanan yang ada dapat dilakukan lebih mudah karena *tools* tersebut diintegrasikan dan ditampilkan dalam tatap muka yang bersifat *user-friendly*; Jika diukur dari satuan Kinerja/Harga, kemampuan Bento Defender termasuk bernilai 80 dari 100; Staf masih mengalami kesulitan dalam melakukan pembaharuan *antivirus database definition* karena masih harus menggunakan sintaks konsol *fresclam*; Kurang terbiasanya staf dalam lingkungan Linux serta tampilan antarmuka yang standar (*web interface*) menjadikan staf jenuh; Dan secara keseluruhan, aplikasi ini sangat membantu Yayasan St. Bellarminus dalam hal kontrol dan konfigurasi jaringan.

Tampilan *Proxy Monitoring > Denied Reports*

PENUTUP

Dari hasil penelitian yang telah dilakukan, dapat ditarik beberapa simpulan sebagai berikut. Pertama, suatu sistem komputer yang terhubung jaringan dengan memiliki kepentingan khusus, harus lebih memperhatikan keamanan datanya, terlebih untuk yayasan St. Bellarminus yang menggunakan fasilitas internet untuk mendukung kegiatan belajar mengajar. Kedua, aplikasi keamanan jaringan yang ada saat ini sangat beragam, mulai dari *firewall*, *antivirus*, *proxy*, *mail scanner*, dan sebagainya. Hal itu dapat merumitkan dalam hal pengaturan aplikasi dan dibutuhkan staf yang ahli pada bidang jaringan. Ketiga, dengan adanya *Unified Threat Management* (UTM), kerumitan dalam hal pengaturan aplikasi akan berkurang disebabkan

Tabel 3 Evaluasi Perbandingan Sistem

Feature	*Equiinet UTM Total Protection*	*Watchguard Firebox X Core X1250e UTM Solution*	*Bento Defender*
Hardware Based	-	√	√
Software Based	√	-	-
Web Based	√	-	√
Anti-Spam	√	√	√
Anti-Virus	√	√	√
Upgrade	√ (dengan biaya)	√	√ (per *tools*)
IDS	-	√	√
Gigabit LAN	-	√	√
License	1 tahun	1 tahun	1 tahun
Price	$1,494.00	$7,297.50	free (for the first)

pengaturan sebagian besar dari aplikasi digabung menjadi satu kesatuan (dalam *web*).

Keempat, UTM dapat diatur melalui program administrasi berbasiskan *web* sehingga dapat dilakukan oleh komputer lain melalui *web browser*. Kelima, UTM yang dibuat oleh peneliti memiliki tingkat biaya yang lebih rendah dibandingkan dengan UTM yang telah ada serta tidak memerlukan biaya untuk sistem operasi *server* karena UTM yang dibuat peneliti berjalan di sistem operasi *open source*, yaitu Linux Fedora Core 5. Selain itu, keuntungan yang didapatkan dari aplikasi UTM yang dibuat adalah kemampuan untuk melakukan pembaharuan versi yang mudah dan tidak terpaku dengan hanya satu sistem operasi (*multi-platform*). Keenam, aplikasi Bento Defender sebagai UTM yang dibuat peneliti sangat membantu yayasan St. Bellarminus dalam hal kontrol dan proteksi jaringan. *Proxy* membatasi akses pengguna dalam *web*. *Firewall* membantu membatasi akses pengguna terhadap alamat IP dan *port* yang diperuntukkan bagi pengguna khusus. IDS memberikan laporan penyusupan yang terjadi dalam sistem sehingga keputusan dapat diambil secepatnya serta *mail management* memberikan proteksi terhadap *email* bervirus dan yang mengandung *spam.*

Saran yang dapat diberikan untuk pengembangan sistem serupa agar menjadi lebih baik lagi di masa mendatang, antara lain *Tools* keamanan jaringan yang digunakan sebaiknya di-*update* secara berkala; Penggunaan *distro* Linux sangat diajurkan mengingat efisiensi yang dihasilkan oleh *distro* ini sangat tinggi; Selalu mencari informasi perkembangan teknologi yang ada pada *tools* yang digunakan dan melakukan *upgrade* pada *tools* tersebut. Aplikasi ini masih dapat digunakan atau diperbaharui untuk versi *upgrade* terbaru; Diperlukan sistematika *backup* agar sistem yang dipakai tetap dapat berjalan bila terjadi suatu masalah; Peningkatan kualitas perangkat keras yang digunakan sangat disarankan mengingat semakin tinggi spesifikasi perangkat keras siste, maka kinerja, performa, kapasitas pengguna (komputer), dan daya tahan sistem akan semakin meningkat; Fitur keamanan jaringan masih dapat ditambahkan, seperti *secure dns* dan lain sebagainya; Berdasarkan hasil pengamatan bahwa masih adanya kelemahan dalam proses pendeteksian *virus* oleh sistem ini maka disarankan agar setiap pengguna (komputer) tetap memiliki *anti virus* internal; Diperlukan suatu laporan yang terintegrasi untuk memantau semua kegiatan jaringan. Laporan tersebut diperuntukkan bagi petinggi yayasan yang ingin melihat laporan dengan format yang menyeluruh dan mudah dimengerti.

DAFTAR PUSTAKA

Anonymous. 2006. http://id.wikipedia.org/wiki/Linux

_____.2006. http://qmail-scanner.sourceforge.net/

Bragg, Roberta.2004. *The Complete Reference Network Security.* New York: McGraw-Hill.

Connolly, Thomas and Carolyn Begg. 2005. *Database Systems: A Practical Approach to Design, Implementation, and Management.* New York: McGraw-Hill.

Ramakrishnan, Raghu and Johannes Gehrke. 2003. *Database Management Systems*. New York: McGraw-Hill.

Comer, Douglas E. 1999. *Computer Networks and Internets 2nd Edition*. New Jersey: Prentice-Hall.

Kurose, James F. 2003. *Computer Networking, A Top-Down Approach Featuring the Internet 2nd Edition.* Boston: Addison Wesley.

Norton, Peter. 1999. *Complete Guide to Networking.* Indiana: SAMs Publishing.

Stallings, William. 2003. *Cryptography and Network Security: Principles and Practice.* New Jersey: Prentice-Hall.

Syukri, Muhammad. 2002. *PC Router dengan GNU/Linux*. Jakarta: Elex Media Komputindo.

Tanenbaum, Andrew S. 2003. *Computer Networks 4th Edition.* New Jersey: Prentice-Hall.