Penggunaan *Watchguard Firebox* Sebagai Penyaring Konten Pada Jaringan Internet Kantor BSITV

Supriyadi
STMIK NUSA MANDIRI JAKARTA
supriyadi.spy@bsi.ac.id

ABSTRACT - The use of content filtering system has been carried out in the Office BALI TV. Content filter used is Firebox which has the advantage of doing block the content of a website as a whole. Detection of viruses, worms or movements that lead to action in the form of hack can run optimally with the device. But blocking the entire content contained on a website raises problems, because not all content contained on the site a negative. This study uses a qualitative method to see the extent to which the use of content filtering is done at the Office BSITV. This usage is expected to be an input to determine the effective use of content filtering. It is advisable to create a device capable of detecting a content page by page, so that the selection process can be carried out relevant content.
Keywords: Firebox, detection, content filter

ABSTRAK - Pemakaian sistem penyaring konten telah dilakukan di Kantor BSITV. Penyaring konten yang dipakai adalah firebox yang memiliki keunggulan melakukan blok terhadap konten sebuah *website* secara menyeluruh. Pendeteksian virus, worm maupun gerakan yang mengarah pada tindakan berupa *hack* dapat berjalan secara maksimal melalui perangkat ini. Namun pemblokiran seluruh konten yang terdapat pada sebuah *website* memunculkan permasalahan, karena tidak semua konten yang terdapat pada sebuah situs tersebut negatif. Penelitian ini menggunakan metoda kualitatif untuk melihat sejauh mana penggunaan konten filtering dilakukan di Kantor BSITV. Penggunaan ini diharapkan menjadi masukan untuk menentukan penggunaan konten filtering yang efektif. Disarankan untuk menciptakan sebuah perangkat yang mampu mendeteksi sebuah konten *page* per *page*, sehingga proses penyeleksian konten dapat dilakukan secara relevan.

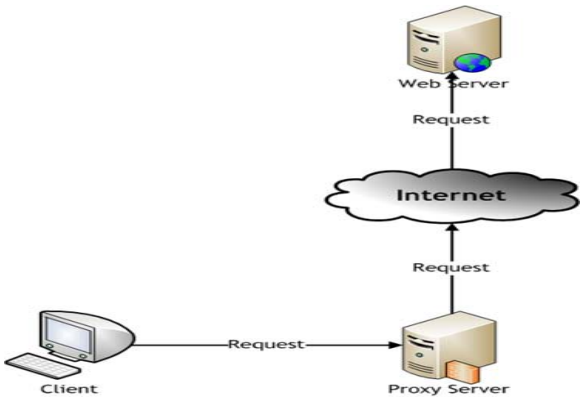
Kata Kunci : firebox, pendeteksian, penyaring konten

1.1. Pendahuluan

Ibarat dua sisi mata uang, perkembangan teknologi informasi melahirkan dua efek yakni efek negatif dan efek positif. Efek positifnya, teknologi informasi dan komunikasi memberikan berbagai kemudahan dalam menyelesaikan pekerjaan. Permasalahan geografis yang selama ini selalu menjadi kendala, sehingga membutuhkan ruang, waktu dan biaya yang besar dalam mengakses informasi telah diatasi dengan hadirnya fitur- fitur yang terdapat di dunia maya yang lebih efektif. Selain itu teknologi informasi menghadirkan pergeseran paradigma terhadap tingkat kepentingan informasi menjadi suatu hal yang paling berarti dan berharga. Lebih spesifik, teknologi informasi dan komunikasi, khususnya keberadaan dunia maya dewasa ini digunakan orang sebagai pusat rujukan informasi, bersosialisasi, melakukan transaksi dan aktivitas ekonomi, dan bahkan sebagai media dalam melakukan pembelajaran. Namun sisi lain kemajuan teknologi informasi dan komunikasi, khususnya fasilitas dunia maya menghasilkan konsekuensi negatif bagi penguna. Konsekuensi negatif yang kita anggap sebagai dampak negatif teknologi ini sama luasnya dengan manfaat positif teknologi ini. Sebagai sebuah perwujudan dari dunia yang maya, dunia maya memiliki hampir semua hal yang terdapat pada dunia nyata. Berbeda dalam dunia nyata, di dunia maya segala aktivitas dapat dilihat lebih visual dan nyata, serta amat mudah membuktikan setiap pelanggaran yang dilakukan seseorang. Secara garis besar internet memberi peluang terciptanya dampak negatif seperti pornografi, kecanduan hubungan maya, tayangan sadis dan lainnya. Dampak negatif tersebut semakin besar karena ketersediaan fitur dan mudahnya akses.

Meski demikian semua informasi yang terdapat pada dunia maya yang di interpretasikan melalui laman *website y*ang ada saat ini memiliki manfaat selama digunakan secara bijaksana diartikan dengan menggunakan untuk tujuan yang bermanfaat

serta menyaring isi yang bersifat negatif. Untuk itu, dalam bentuk kampanye persuasif, penyaringan konten yang tersedia di dunia maya secara teknis sangat diperlukan. Ada beberapa cara penyaringan konten yang dapat dilakukan. Saat ini teknis penyaringan konten yang sering digunakan adalah dengan mengimplementasikan *proxy* yang terdapat pada jaringan. Pada teknik ini *proxy* akan memainkan peran untuk menyampaikan dan menerima permintaan dari user untuk mengakses konten dari server global.



Gambar 1. Konsep dan cara kerja proxy

Pada dasarnya proxy berfungsi sebagai *content checking*. Bila *proxy*diset untuk mem-filter konten yang mengandung kata "*sex*", maka semua paket yang mengandung kata "*sex*" akan ditolak. Meskipun pada setiap jaringan, khususnya jaringan l*ocal area network* selalu disertai sebuah *proxy*, karena fungsi vitalnya sebagai jembatan antara *client* dan *webserver* sekaligus sebagai otorisasi mengijinkan akses, namun kenyataanya efektifitas kinerja dalam melakukan penyaringan masih tidak cukup. Relevansi teknik penyaringan dengan kaidah kepantasan terhadap pengakses begitu erat kaitannya. Sisi lain dari alasan penyaringan sebuah konten juga dipengaruhi beberapa faktor yang bersifat non teknis. Dalam sebuah diskusi oleh ICTWATCH bersama dengan keberadaan UU ITE Nomor 8 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), khususnya pasal 27 ayat 1 harus dilakukan secara lebih nyata. Namun perlindungan terhadap masyarakat terkait akses ke negatif tidak dapat dipenuhi hanya undang undang tersebut. Kebijakan lebih teknis diperlukan untuk menciptakan akses ke dunia maya yang lebih sehat dan bermartabat.

Berdasarkan pemaparan diatas, penggunaan ini difokuskan pada sejauhmana perangkat penyaring konten yang digunakan pada jaringan kantor BSITV mampu melakukan *filtering* terhadap konten negatif, serta apa kelemahan dan kelebihan *tools* tersebut.

Penelitian ini diharapkan memberikan informasi teknis terkait dengan perangkat konten filtering sebagai media penyaringan informasi negatif, serta solusi pemilihan perangkat penyaring konten yang efektif.

2.1. Tinjauan Pustaka

Pada jaringan kantor BSITV, sistim jaringan komputer lokal mengadopsi topologi jaringan topologi *Mesh* atau biasa disebut topologi jala, dimana dalam topologi ini terbentuk suatu bentuk hubungan antar perangkat dimana setiap perangkat terhubung secara langsung ke perangkat lainnya yang ada di dalam jaringan

Gambar 2. Topologi Mesh yang digunakan dalam jaringan antar koneksi di kantor BSITV

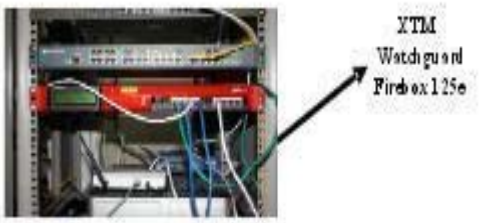
Pemilihan topologi ditujukan untuk keamanan data yang didistribusikan. Dengan menggunakan topologi ini data yang disampaikan antar satu komputer dengan komputer lain lebih aman karena menggunakan "*dedicated link*" komunikasi data secara langsung tanpa melalui komputer lain. Hal ini diperlukan karena data yang didistribusikan sangat penting seperti data statistik dan kependudukan.

2.2. Sistim Penyaring Konten Kantor BSITV

Pada jaringan kantor BSITV efektivitas penggunaan *proxy* dan *firewall* untuk melakukan pengontrolan atas akses yang dilakukan user. *Proxy* yang digunakan pada server jaringan ini sudah lengkap. Saat ini konfigurasi pada *MS Proxy Server* dan *WinGate* yang bekerja pada layer aplikasi mampu melakukan pengontrolan terhadap seluruh aplikasi yang digunakan pada jaringan. Hasil penelitian menunjukan tipe *MS Proxy Server* dan *Win Gate* mampu menyortir seluruh lalulintas paket yang masuk.

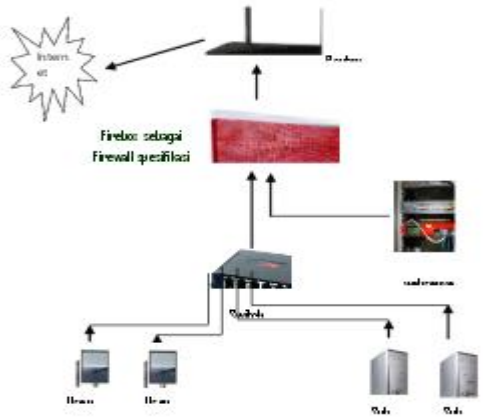
Kondisi ini tentu tidak mencukupi untuk melindungi dan memantau jaringan bebas dari akses yang tidak terdeteksi. Perkembangan berbagai tipe proxy yang sebagian besar dapat diperoleh secara gratis menimbulkan fenomena baru. Sebagus apapun tipe *proxy* yang digunakan saat ini dapat dipastikan tidak akan mampu melakukan pengontrolan seluruh aktivitas. Sebagai contoh sebuah *web proxy* dapat diperoleh secara gratis mampu melakukan browsing tanpa harus khawatir oleh adanya pemblokiran situs karena semua request akan dilewatkan di *web proxy* tersebut.

Jaringan pada kantor BSITV juga dilengkapi dengan *firewall* yang bekerja saling mendukung dengan *proxy. Firewall* yang digunakan adalah *WebBlocker* yang merupakan produk sebuah vendor berbasis di Amerika Serikat. Sistim langganan keamanan terintegrasi *XTM WatchGuard* dan *Firebox X e-Series* peralatan dengan nomor seri X1250e.



Gambar 3. Bentuk fisik *webblocker* sebagai penyaring konten

Secara umum fungsi *webblocker* ini untuk melakukan pengamatan terhadap segala aktivitas yang dilakukan oleh user dalam lingkup jaringan, dengan mengenali konten yang disajikan oleh sebuah website. Pada weblocker ini terdapat fitur tambahan berupa perangkat proteksi antivirus, spyware dan anti spam. Ini diperlukan karena banyaknya data siaran yang harus dilindungi ketika terjadisebuah distribusi data. Keberadaan firewall yang komprehensif ini tentunya untuk memberikan perlindungan secara total terhadap setiap akses yang tidak dikehendaki. *Firewall watchguard* ini bekerja dengan memfokuskan semua paket yang masuk melalui proses identifikasi. Watchguard firebox 125e akan mengidentifikasi sebuah paket yang diakses user melalui pengecekan alamat IP baik komputer sumber maupun komputer tujuan untuk membandingkan apakah IP dimaksud merupakan IP yang memiliki indikasi merusak, kemudian mengecek *port* yang digunakan dan membandingkan dengan database yang dimiliki serta melakukan pengecekan terhadap protokol IP yang digunakan. Indikator firewall ini menolak atau melewatkan paket tersebut berdasarkan daftar *database* yang sudah ada sebelumnya.



Gambar 4. Cara kerja dan fungsi *firebox* sebagai *firewall*

2.3. Keunggulan Watchguard Firebox 125e

Dari sisi fitur, *firebox 125e* memiliki beberapa keunggulan diantaranya memiliki kemampuan melakukan penyaringan IP adress.

Selain itu fleksibilitas pengkonfigurasian dapat dilakukan melalui port yang digunakan.

Artinya untuk dapat memblok sebuah situs berbagai tipe dapat dilakukan dengan menutup port tertentu, sehingga seluruh web yang berbasis pada port tersebut tidak akan dapat diakses user. Selain itu *firebox 125e* juga merupakan sebuah paket watchguard yang terdiri dari perangkat lunak firewall sekaligus terintegrasi dengan perangkat keras.

2.4. Kelemahan Watchguard Firebox 125e

Selain keunggulan yang dimiliki *Watchguard Firebox 125e* juga memiliki beberapa kelemahan. Beberapa kelemahan yang dapat diidetifikasi dalam penelitian ini adalah *Watchguard Firebox 125e* yang digunakan sebagai *firewall* untuk melindungi jaringan berjalan secara sporadis, dimana metode penyaringan konten yang masuk langsung menutup semua akses berdasarkan port, sehingga keseluruhan informasi yang ada dalam website tersebut secara otomatis tidak akan bisa diakses.

Hal ini sebenarnya sangat bertentangan dengan kebebasan dalam memperoleh informasi. Upaya pemblokiran seharusnya dilakukan dengan bijaksana. Artinya pembatasan atau pemblokiran bukan berarti membatasi hak manusia untuk memperoleh informasi. Esensi pembatasan dan pemblokiran bertujuan untuk menyelamatkan bangsa ini dari kerusakan.

Pembatasan sebagian konten negatif di jaringan situs website juga sebagai upaya untuk meningkatkan harkat dan martabat bangsa ini di panggung dunia. Artinya sebagai sebuah bangsa besar yang sejajar dengan bangsa bangsa lain di dunia ini bangsa Indonesia juga memiliki etika dalam melakukan akses informasi melalui dunia maya. Selain itu, besarnya biaya yang dibutuhkan dalam melakukan identifikasi dan pembentukan database yang akan terkonfigurasi juga akan menjadi masalah ketika penganggarannya tidak dilakukan secara tepat. Proses update perangkat yang harus dilakukan kepada vendor pemilik lisensi watchguard *firebox 125e* juga membutuhkan biaya yang tidak sedikit, padahal bila perangkat tidak terupdate secara berkala sangat mempengaruhi kemampuan pembentukan database sesuai pertumbuhan website yang pesat.

3.1. Metode Penelitian

Penelitian ini dilaksanakan di Kantor BSITV Jalan Kayu Jati V No.2, dengan fokus pengamatan terhadap kinerja jaringan yang berada di Lantai II. Objek pengambilan data terdiri dari data aktivitas lalu lintas jaringan dari menu Manajemen Admin, dokumen awal pembangunan jaringan dan wawancara mendalam terhadap seluruh elemen yang terkait dengan manajemen pengelolaan jaringan.

Penelitian ini memakai pendekatan kualitatif dengan analisis deskriptif, yaitu mencatat dan menggambarkan secara teliti seluruh fenomena yang ditemukan di lapangan. Peneliti secara langsung mengamati objek penelitian untuk melakukan interpretasi data lapangan, sekaligus memilih informan sebagai sumber data serta melakukan penilaian kualitas data, menafsirkan serta membuat kesimpulan atas temuan di lapangan. Alasan pemilihan metode ini didasarkan pada fenomena perkembangan teknologi informasi, khususnya konten dunia maya yang sangat dinamis, dan selalu pendekatan secara persuasif dan penjabaran naratif diharapkan mampu menggali semua fenomena dan kencenderungan yang berkembang.

Sedangkan analisa data dilakukan dalam beberapa tahapan dari tahapan *trustworthines, credibility,* hingga *authenticity*. Tahapan ini dilakukan untuk melihat realita yang diungkapkan informan dengan melihat pengalaman informan terkait topik, menguji kredibilitas informan dari jawaban serta memfasilitasi pengungkapan konstruksi personal informan. Validasi data dilakukan dengan menggunakan teknik triangulasi yaitu melakukan pengecekan dari sumber data yaitu pengelola dan manajemen admin jaringan, pejabat yang memiliki otoritas terhadap keberlangsungan jaringan, data lalu lintas jaringan serta para pengunjung atau user yang menggunakan jaringan.

Keberagaman data yang diperoleh akan di deskripsikan, dikategorikan, untuk melihat pendapat yang sama dan melakukan *member chek* terhadap data yang berbeda untuk dibuatkan kesepakatan diantara sumber data.

3.2. Hasil dan Pembahasan

Secara teknis, seluruh otoritas yang ada yang

memiliki wewenang terkait dengan keberadaan infrastruktur teknologi informasi dan komunikasi dan unsur-unsur pendukungnya sudah memiliki konsep pemanfaatan yang sangat jelas. Penyediaan perangkat baik dari sisi *hardrware, software* maupun *tools* lainnya sudah sangat mencukupi. Dari sisi keamanan data, khususnya perlindungan terhadap user yang mengakses melalui jaringan terhadap konten yang akan diakses cukup kuat, dimana manajemen administrator jaringan memilih untuk memperkuat sistim pengamanan jaringan dengan melakukan duplikasi pengamanan.

Duplikasi pengamanan dimaksud terdiri dari penggunaan *proxy* sequid untuk seluruh aktivitas internel jaringan dan menggunakan *firewall* berbasis *watchguard firebox* seri 125e untuk setiap akses masuk. Cara kerja *firewall* dengan langsung menutup seluruh port yang diidentifikasi atau berpeluang memiliki konten yang tidak baik sesungguhnya bukan tindakan yang bijak. Sebagian isi situs tersebut pasti akan memiliki manfaat sepanjang dilakukan model pengaksesan yang sehat. Pemilahan terhadap sebuah situs tertentu untuk melihat serta menciptakan cara pandang penilaian yang lebih parsial sangat diperlukan untuk menciptakan pola akses informasi yang relevan. Sebuah perangkat yang mampu mendeteksi konten secara *page by page* diharapkan mampu mengatasi permasalahan filtering ini, khususnya di negara yang belum dapat menentukan secara spesifik memberikan kategori konten negatif atau positif.

Teknik penyaringan konten pada jaringan kantor BSITV sebaiknya dilakukan secara parsial dan terpisah dengan fungsi *firewall*, untuk menghindari pemblokan sebuah situs secara keseluruhan, karena sebagian isi situs yang diblok melalui fungsi firewall dipastikan memiliki konten positif yang dibutuhkan *user*. Selain itu dalam mengkonfigurasikan *database* untuk menyeleksi situs yang dianggap memiliki potensi negatif dan berbahaya
sebaiknya dilakukan secara lebih bijak dengan memperhatikan seluruh aspek konten yang terdapat pada situs dimaksud. Peluang untuk melakukan kerjasama dengan Kementerian Komunikasi dan Informatika terkait pengembangan dan penggunaan software penyaring konten dapat dilakukan. Sebagai acuan saat ini Kementerian Komunikasi dan informatika edang melakukan uji coba penggunaan *trush+* sebagai sebuah perangkat penyaring konten pintar untuk melakukan pendeteksian setiap konten secara detil dan *page by page*.

4.1. **Kesimpulan**

Sistem penyaring konten telah diterapkan di Kantor BSITV. Penyaring konten yang dipakai adalah *firebox* yang memiliki keunggulan melakukan blok terhadap konten sebuah *website* secara menyeluruh. Pendeteksian *virus*, *worm* maupun gerakan yang mengarah pada tindakan berupa *hack* dapat berjalan secara maksimal melalui perangkat ini. Namun pemblokiran seluruh konten yang terdapat pada sebuah *website* memunculkan permasalahan, karena tidak semua konten yang terdapat pada sebuah situs tersebut negatif. Penelitian ini menggunakan metoda kualitatif untuk melihat sejauh mana penggunaan konten *filtering* dilakukan di Kantor BSITV. Penggunaan ini diharapkan menjadi masukan untuk menentukan penggunaan konten *filtering* yang efektif. Disarankan untuk menciptakan sebuah perangkat yang mampu mendeteksi sebuah konten *page* per *page*, sehingga proses penyeleksian konten dapat dilakukan secara relevan.

DAFTAR PUSTAKA

[1] Mulyana, Dedy, 2002. Metodologi Penelitian Kualitatif. Paradigma Baru Ilmu Komunikasi dan Ilmu Sosial Lainnya. Remaja Rosda Karya. Bandung.

[2] Pardosi, Mico, 2007. Pengantar Instalasi Jaringan, Penerbit Informatika. Bandung

[3] Salahuddin. M. 2010. Penyaringan Konten Negatif di Internet. Indonesia

Security Incident Response Team On Internet Infrastructure (ID-SIRTII). Jakarta

[4] Sugiono, 2008. Metode Penelitian Kuantitatif, Kualitatif dan R&D. Alfabeta. Bandung

[5] Sopandi, Dede. 2006. Instalasi dan Konfigurasi Jaringan Komputer. Penerbit Informatika. Bandung.

[6] Sembiring, Tifatul, 2012, Laporan Konfrensi Pers Terkait Aturan Pengawasan Konten Negatif Bagi Provider Penyedia Konten, (27 Oktober 2010) http://www.kominfo.go.id

[7] Tim Perumus. 2011. Focus Group Discussion : Draf dan Acuan Etika On-Line.