

Pembatasan Akses Jaringan Internet Pada Clearos Menggunakan Metode Access Control List

Indra Chaidir¹, Reski Rona Wirawan²

Manajemen Informatika
AMIK BSI Jakarta
Jl. RS. Fatmawati No. 20 Pondok Labu Jakarta Selatan
indra@bsi.ac.id

Teknik Informatika
STMIK Nusa Mandiri Jakarta
Jl. Kramat Raya No. 25 Jakarta Pusat 10450
rizkyrona15@gmail.com

Abstract – A demand for internet use is felt by workers. Therefore very much needed once an internet network in a company. The absence of restrictions in the use of internet connection may disrupt network security and network abuse, for it is designed internet access settings. One of the methods used is the Access Control List method applied to ClearOS Server. Access Control List method is one of the demand technique of data connection access and transmission of data packets from one computer to another. The results of research that the authors do prove that ClearOS with filtering method based on Access Control List can filter the identification of devices based on user accounts and the selection of data service requests based on the visited website address.

Key Word: Access Control, Filtering, ClearOS

I. PENDAHULUAN

Masalah yang sering muncul di PT. Selnat Optima ketika seseorang ingin mengakses sebuah alamat web menggunakan internet untuk kecepatan koneksi atau kecepatan akses tidak seperti yang diharapkan. Dikarenakan di PT. Selnat Optima mempunyai banyak user yang mengakses internet dan tidak adanya kontrol untuk penggunaannya. Adanya segala bentuk risiko, ancaman dan kerentanan yang dapat terjadi pada sistem keamanan jaringan (Akbar, 2015).

Masalah seperti ini sering muncul baik di kantor-kantor ataupun di sebuah warnet sekalipun, begitu pun juga yang terjadi di PT. Selnat Optima yang berlangganan menggunakan salah satu provider internet dengan paket dedicated yang besaran *bandwidth*-nya 13 Mbps. Dengan paket tersebut diharapkan dapat mencukupi kebutuhan koneksi internet untuk semua user, tetapi akan percuma jika tidak dibatasi aksesnya.

Akses berlebih yang diberikan kepada pengguna akan mengakibatkan penyimpangan di luar kepentingan organisasi (Heru, 2007). *Access Control List* (ACL) merupakan salah satu alternatif upaya untuk mengamankan jaringan komputer. (Simamora, Hendrarini, & Sitepu, 2011)

Maka untuk mengatasi permasalahan yang ada dibangunlah sebuah server ClearOS yang dimana didalamnya terdapat fitur Access Control List yang

berfungsi sebagai pembatas penggunaan koneksi internet untuk setiap divisi yang ada.

II. METODOLOGI PENELITIAN

Metode yang dilakukan dalam penelitian ini adalah Metode Rekayasa Sistem Jaringan. Tahap-tahapannya adalah sebagai berikut :

A. Requirements Gathering.

Tahapan ini adalah tahapan pengumpulan informasi yang dibutuhkan dan analisa kebutuhan. Kegiatan ini meliputi :

1) Studi Literatur.

Mengumpulkan informasi dari literature, studi pustaka atau jurnal tentang permasalahan dan pemecahannya menggunakan Access Control List.

2) Site Survey.

Kegiatan dalam Site Survey mencakup observasi dan wawancara secara langsung ke lokasi dimana kita akan melaksanakan perancangan jaringan komputer. Hal ini bertujuan untuk memperoleh data yang paling akurat tentang kondisi yang ada saat ini.

B. Selection Design.

Memilih dan memilih perangkat yang akan digunakan untuk setelah dilakukan analisa, pembuatan design jaringan, dan pembuatan server ClearOS tersebut adalah menginstal ClearOS guna mengaktifkan fitur *Access Control List* yang berada di ClearOS. Desain yang akan digunakan untuk membangun server ClearOS

yang akan diterapkan sebagai firewall dalam keamanan jaringan adalah distro linux yang ClearOS yang mengguakan metode Accesst Control List. Dan kemudian dilakukan pengujian *Accesst Control List* berdasarkan akun user ataupun alamat website yang di daftarkan server ClearOS.

C. Implementation.

Server ClearOS ini akan diimplementasikan di PT. Selnnet Optima yang dimana server ClearOS ini sebagai firewall yang berfungsi sebagai filter dalam penggunaan internet yang digunakan oleh user setiap hari dan server ClearOS ini akan memfilter alamat website ataupun akun user yang di daftarkan di dalam server ClearOS.

D. Operation.

Tahapan dimana jaringan computer telah direkayasa seperti telah diimplementasikan Access Control List pada jaringan lingkungan kerja setempat.

E. Review and Evaluation.

Tahapan dimana dilakukan proses peninjauan dan evaluasi setelah jaringan komputer dioperasikan. Dalam tahap ini dilakukan perbandingan antara kinerja jaringan sebelum dan sesudah dilakukan rekayasa. Bandingkan apakah tujuan yang diinginkan perusahaan sudah sesuai dengan hasil.

Bahan yang digunakan dalam penelitian ini sebagai berikut :

- a. Perangkat Keras
 - 1) 1 (satu) Server sebagai proxy.
 - 2) Komputer, dua atau lebih sebagai client.
 - 3) Monitor, mouse dan keyboard.
 - 4) Switch Cisco Catalyst 2950 24 port
 - 5) Kabel UTP Category 5 Straight-Link
 - 6) Router type cyberram CR100i
- b. Perangkat Lunak
 - 1) ClearOS untuk Server
 - 2) Windowa XP dan Windows 7
 - 3) Putty
 - 4) Mozilla Firefox dan Internet Explorer

Koneksi Internet menggunakan Provider Neuviz , total bandwidth 13 Mbps.

III. HASIL DAN PEMBAHASAN

Dalam manajemen jaringan menggunakan server ClearOS dibutuhkan beberapa perangkat keras maupun perangkat lunak, adapun beberapa hal yang berkaitan dengan manajemen jaringan dalam proses penelitian ini yaitu:

1. Server ClearOS

ClearOS adalah linux yang di kostumasi khusus untuk keperluan server. Dengan berbagai fitur yang powerfull dan setting yang simple,

ClearOS menjadi alternative pilihan, baik untuk pemula yang tidak mengerti linux sama sekali maupun untuk profesional yang memerlukan kemampuan terbaik dari OS linux server. Berbasis Linux Red Hat Enterprise 5, Menjadikan ClearOS memiliki source base yang kuat dan stabil untuk dijalankan sebagai server di warnet, game online, perkantoran, dan perusahaan.

2. Metode Access List

Access list adalah pengelompokan paket berdasarkan kategori. Access list bisa sangat membantu ketika membutuhkan pengontrolan dalam lalu lintas network. access list menjadi tool pilihan untuk pengambilan keputusan pada situasi ini.

Penggunaan access list yang paling umum dan paling mudah untuk dimengerti adalah penyaringan paket yang tidak diinginkan ketika mengimplementasikan kebijakan keamanan. Sebagai contoh kita dapat mengatur access list untuk membuat keputusan yang sangat spesifik tentang peraturan pola lalu lintas sehingga access list hanya memperbolehkan host tertentu mengakses sumber daya WWW sementara yang lainnya ditolak. Dengan kombinasi access list yang benar, network manager mempunyai kekuasaan untuk memaksa hampir semua kebijakan keamanan yang bisa mereka ciptakan.

Access list juga bisa digunakan pada situasi lain yang tidak harus meliputi penolakan paket. Sebagai contoh access list digunakan untuk mengontrol network mana yang akan atau tidak dinyatakan oleh protocol dynamic routing. Konfigurasikan access list dengan cara yang sama. Perbedaannya di sini hanyalah bagaimana menerapkannya ke protocol routing dan bukan ke interface.

3. Perancangan Simulasi.

Untuk simulasi pengujian penelitian ini menggunakan virtualisasi. Virtualisasi memungkinkan beberapa sistem operasi untuk berjalan secara bersamaan di dalam beberapa komputer atau mesin virtual pada satu komputer fisik (Rasian & Mursanto, 2009).

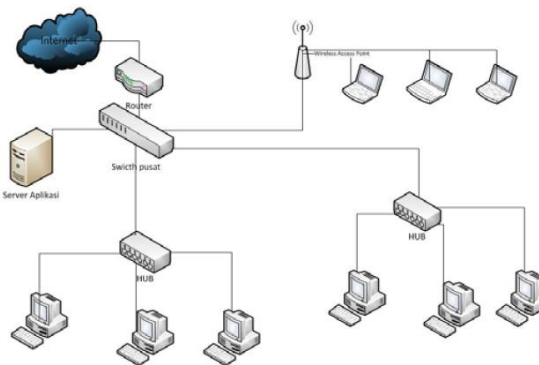
Perangkat lunak yang digunakan adalah VirtualBox. Virtual Box adalah sebuah aplikasi yang dapat mensimulasikan operating sistem baru didalam sistem operasi. Perangkat keras yang terdapat dalam mesin virtual sama seperti perangkat keras yang dipakai pc ataupun laptop, misalnya CPU, RAM, harddisk, keyboard, mouse, dan soundcard dengan kata lain pc di dalam pc.

Sistem operasi yang diinstal melalui virtual box disebut *guest operating system* (sistem operasi

tamu). Sistem operasi tersebut dapat dijalankan berdampingan dengan sistem operasi utama atau *host operating system* yaitu di mana vmware diinstall, sistem virtual box dapat dibangun di atas Windows dan Linux.

4. Skema Jaringan.

Setelah melakukan penelitian di PT. Selnet Optima, dapat digambarkan skema jaringan komputer yaitu terdapat pada gambar sebagai berikut :



Sumber: Wirawan (2017)

Gambar 1. Skema Jaringan Komputer PT. Selnet Optima

5. Pengaturan Akses.

Untuk mengimplementasikan Access Control List pada ClearOS, terlebih dahulu kita lakukan beberapa hal-hal berikut:

a. Konfigurasi ClearOS.

Untuk konfigurasi ClearOS, penulis menggunakan web browser. Setelah mendaftarkan ip yang digunakan server clearos yang telah di install. Dengan alamat [https://\(ip\):81](https://(ip):81).



Sumber: Wirawan (2017)

Gambar 2. Tampilan ClearOS Web base

b. Pengaturan Proxy dan Filtering

Pada *clearos* ini penulis membagi access control lists kedalam 4 bagaian, Sesuai divisi di PT Selnet optima secara garis besarnya yaitu:

- a) fullakses untuk manager, direktur dan supervisor
- b) Finance untuk staff keuangan
- c) Deny untuk divisi enggeiner yang hanya membutuhkan local jaringan
- d) Collection untuk divisi yang hanya mengakses satu web aplikasi client



Sumber: Wirawan (2017)

Gambar 3. Pengaturan Access Control List

c. Pengaturan User Defined Groups

user defined groups pada ClearOS bertujuan untuk menentukan user dari jaringan lokal ke jaringan yang terkoneksi *internet*. Dengan cara klik system – group – add menambahkan *group* seperti gambar:



Sumber: Wirawan (2017).

Gambar 4. Pengaturan *group access control*

d. Pengaturan Add/Time Periods

Pengaturan Add/time Periodes bertujuan untuk menentukan jadwal atau masa berlaku dari access control, dengan cara klik menu

Gateway – Access Control – add/time periods.

Pengaturan Add/time Perodes bertujuan untuk menentukan jadwal atau masa berlaku dari access control, dengan cara klik menu Gateway – Access Control – add/time periods.

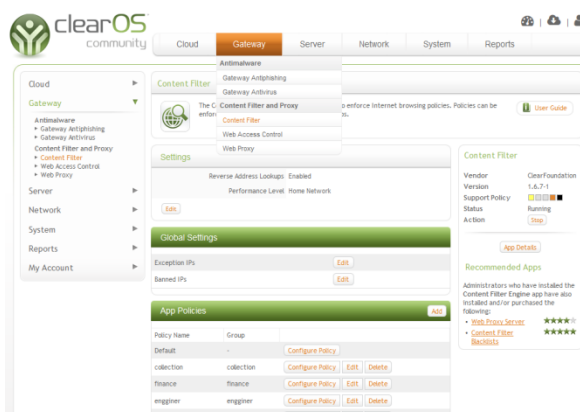


Sumber: Wirawan (2017).

Gambar 5. Pengaturan Add/time periods

e. Pengaturan Content Filter

Content filter ini berfungsi untuk situs atau web mana saja yang tidak boleh diakses masuk ke fitur gateway dan memilih Access Control.



Sumber: Wirawan (2017).

Gambar 6. Pengaturan Content Filter.

6. Pengujian Awal Jaringan.

Untuk pengujian awal, semua user dapat mengakses semua alamat website. Untuk itu perlu diaktifkan fitur agar user diberi pembatas dalam mengakses internet atau alamat website.

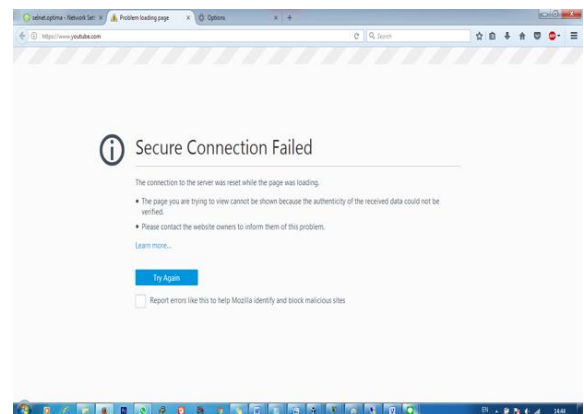
- Mendaftarkan App Group Policies di Access Control

- Pendaftaran User berdasarkan group.

- Memasukan user kedalam group untuk Access Control List

7. Pengujian Akhir Jaringan.

Setelah melakukan konfigurasi dan mengaktifkan fitur Access Control List. Pada waktu yang telah ditentukan, user tidak dapat mengakses website yang didaftarkan. Seperti gambar 7 meruakan



hasil pengujian hak akses.

Sumber: Wirawan (2017).

Gambar 7. Hasil Pengujian Akhir

IV. KESIMPULAN

Dari hasil implementasi yang dilakukan di dalam didapat beberapa kesimpulan pengujian yaitu:

- Dengan dibangunnya server ClearOS sebagai proxy server pengguna internet dapat mengelola pemakaian internet yang ada sesuai dengan kebutuhan.
- Dengan diterapkannya sistem filtering menggunakan server ClearOS sebagai proxy server, maka penggunaan internet lebih terkontrol karena user tidak dapat mengakses situs-situs atau konten-konten tertentu.
- Metode Access Control List yang terdapat didalam fitur ClearOS dapat menyediakan dan memberikan hak akses kepada pengguna jaringan berdasarkan akun per user, dengan demikian dapat membantu seorang Network Administrator jaringan mengamankan akses jaringan.

REFERENSI

- Aditya, A. N. (2013). *30 Menit Mahir Membuat Jaringan Komputer*. Jakarta: Dunia Komputer.
- Akbar, Y. H. (2015). Evaluasi Keamanan Jaringan Wireless Hotspot Menggunakan Metode Square (Studi Kasus Warnet Medianet Sumedang). *Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK Sumedang*, 9, 2.

- Heru, B., Benny, Defendy, & Hento, W. (2007). Keamanan Jaringan Menggunakan Unified Threat Management Pada Server Berbasis Linux. *Journal* , 1, 1.
- Rasian, R., & Mursanto, P. (2009). Perbandingan Kinerja Pendekatan Virtualisasi. *Jurnal Sistem Informasi* , 5, 2.
- Simamora, S., Hendrarini, N., & Sitepu, E. L. (2011). Metode Access Control List sebagai Solusi Alternatif Seleksi Permintaan Layanan Data pada Koneksi Internet. *Jurnal Teknologi Informasi Politeknik Telkom* , 1, 1.