

**IMPLEMENTASI *CONTENT FILTERING*
DENGAN MENGGUNAKAN *SOFTWARE* DANSGUARDIAN
(Studi Kasus : Teknik Informatika Universitas Pasundan Bandung)**

TUGAS AKHIR

Disusun sebagai salah satu syarat untuk kelulusan
Program Strata 1, Program Studi Teknik Informatika,
Universitas Pasundan Bandung

oleh :

Yudi Muhamad Takiyudin
NRP : 10.304.0064



**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG
MEI 2015**

LEMBAR PENGESAHAN
LAPORAN TUGAS AKHIR

Telah disetujui dan disahkan Laporan Tugas Akhir, dari :

Nama : Yudi Muhamad Takiyudin
Nrp : 10.304.0064

Dengan judul :

“IMPLEMENTASI *CONTENT FILTERING*
DENGAN MENGGUNAKAN *SOFTWARE* DANSGUARDIAN”
(Studi Kasus : Teknik Informatika Universitas Pasundan Bandung)

Bandung, Mei 2015

Menyetujui,

Pembimbing Utama,

Pembimbing Pendamping,

(Doddy Ferdiansyah, S.T, M.T)

(Iwan Kurniawan, S.T)

ABSTRAK

Sebagai media informasi dan komunikasi, internet memiliki manfaat dan kegunaan yang sangat beragam. Beragam manfaat internet yang dewasa ini mulai memasuki segala sendi kehidupan manusia mulai bergeser ke arah yang oleh sebagian orang dikatakan negatif. Untuk mengatasi efek negatif dari internet tersebut, khususnya dikalangan pelajar dan mahasiswa, maka pemakaian internet perlu dibatasi dengan cara menyaring (*filtering*) konten-konten yang diakses.

Tugas akhir ini dimaksudkan untuk menerapkan kebijakan terhadap *content filtering* pada jaringan Teknik Informatika UNPAS untuk membatasi akses situs-situs yang terdapat konten bermuatan negatif dengan cara membuat rancangan kebijakan *content filtering* jaringan dan mengimplementasikan kebijakan tersebut kedalam konfigurasi jaringan Teknik Informatika UNPAS. Implementasi *content filtering* dilakukan dengan menggunakan *software* dansguardian untuk melakukan penyaringan konten. Selanjutnya hasil dari implementasi tersebut dilakukan pengujian terhadap konten bermuatan negatif dengan cara mengakses situs-situs yang terdapat konten bermuatan negatif.

Hasil dari penelitian tugas akhir ini adalah server jaringan komputer yang di dalamnya telah terkonfigurasi *software content filtering* sehingga akses yang melalui jaringan Teknik Informatika akan dilakukan penyaringan berdasarkan konten.

Kata Kunci : Jaringan komputer, dansguardian, internet, *content filtering*, kebijakan, konten negatif.

ABSTRACT

As information and communications media, internet has very diverse benefits and uses. Various benefits of internet nowadays have begun to enter all aspects of human life, and it starts to shift towards what some people called negative. To overcome the negative effects of internet, especially among students, the use of internet should be limited by filtering accessed content.

This final assignment is intended to apply policies on content filtering in the network of Informatics Engineering UNPAS in order to restrict access to sites that contain negative content by making design of network content filtering policy and implement those policies into the network configuration of Informatics Engineering UNPAS. Implementation of content filtering is performed using dansguardian software in order to perform content filtering. Furthermore, as the result of the implementation, a test against sites that contain negative content would be performed by accessing sites that contain negative content.

The result of this research is a computer network server in which the content filtering software has been configured in the computer network server, so that access through Informatics Engineering network will be filtered based on the sites' content.

Keywords: Computer networks, dansguardian, internet, content filtering, policy, negatively content.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Puji dan syukur penulis panjatkan kepada Allah SWT. yang telah melimpahkan rahmat, taufik serta hidayah-Nya sehingga penulis dapat membuat laporan tugas akhir dengan judul “Implementasi *Content Filtering* Dengan Menggunakan *Software* Dansguardian” (Studi Kasus Teknik Informatika Universitas Pasundan Bandung)

Adapun penulisan laporan ini bertujuan untuk memenuhi salah satu syarat kelulusan Program Strata 1, di Program Studi Teknik Informatika Universitas Pasundan.

Penulis menyadari laporan ini dapat terwujud berkat bantuan dan dorongan dari berbagai pihak yang telah memberikan banyak masukan, nasehat, saran, kritik dan dukungan moril maupun dukungan materil kepada penulis. Oleh sebab itu penulis mengucapkan banyak terimakasih kepada:

1. Kedua pembimbing, Bapak Iwan Kurniawan, S.T. dan Bapak Doddy Ferdiansyah, S.T, M.T.
2. Orang tua dan keluarga yang selalu mendoakan, mendukung dan memberikan motivasi dalam pembuatan laporan tugas akhir ini.
3. Seluruh civitas akademika Teknik Informatika Pasundan di Universitas Pasundan Bandung yang telah memberikan bekal ilmu selama penulis menimba ilmu.
4. Teman-teman dan rekan-rekan tercinta yang telah memberikan semangat dan dukungan dalam menjalani proses kehidupan.
5. Semua pihak yang tidak dapat penulis sebutkan satu-persatu yang telah membantu dalam penyusunan tugas akhir.

Semoga Allah SWT. memberikan balasan yang lebih baik kepada semua pihak yang telah memberikan bantuan, bimbingan, nasehat, doa dan dukungan dalam proses tugas akhir ini.

Penulis menyadari bahwa penyusunan laporan tugas akhir yang disusun masih banyak kekurangan, sehingga kritik dan saran dari semua pihak sangatlah diharapkan agar kedepannya dapat lebih baik lagi.

Akhir kata semoga penulisan laporan tugas akhir ini dapat diterima dan bermanfaat bagi semua pihak.

Wassalamu'alaikum Wr. Wb.

Bandung, Mei 2015

Penulis

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	iv
DAFTAR ISTILAH	vi
DAFTAR GAMBAR	vii
DAFTAR TABEL	ix
DAFTAR SIMBOL	x
BAB 1 PENDAHULUAN	1-1
1.1 Latar Belakang	1-1
1.2 Identifikasi Masalah	1-2
1.3 Tujuan Tugas Akhir	1-2
1.4 Lingkup Tugas Akhir	1-2
1.5 Metodologi Tugas Akhir	1-2
1.6 Skenario Pembentukan BAB	1-3
1.7 Sistematika Penulisan	1-4
BAB 2 LANDASAN TEORI	2-1
2.1 Jaringan Komputer	2-1
2.1.1 Berdasarkan jangkauan geografis	2-1
2.1.2 Berdasarkan distribusi sumber informasi/data	2-3
2.1.3 Berdasarkan Media Transmisi Data	2-3
2.1.4 Berdasarkan Peranan Komputer Dalam Proses Data	2-4
2.2 <i>Content Filtering</i> (Penyaringan Konten)	2-5
2.2.1 Pengertian <i>Content Filtering</i> (Penyaringan Konten)	2-5
2.2.2 Pemasangan <i>Content Filtering</i>	2-6
2.2.3 Tipe/Jenis <i>Filtering</i>	2-6
2.2.4 <i>Layer Filtering</i>	2-6
2.3 Pengertian Kebijakan	2-7
2.4 Dansguardian	2-9
2.5 <i>Proxy</i>	2-9
2.6 Peraturan KOMINFO Tentang Pengendalian Situs Internet Bermuatan Negatif	2-9
2.7 Prinsip CIA Dalam Keamanan Jaringan	2-11
BAB 3 ANALISIS DAN PERANCANGAN	3-1
3.1 Kerangka Tugas Akhir	3-1
3.2 Skema Tugas Akhir	3-3

3.3	Analisis	3-3
3.3.1	Analisis Prodi Teknik Informatika Universitas Pasundan	3-3
3.3.2	Analisis Keadaan Jaringan Yang Sedang Berjalan	3-4
3.3.3	Analisis Teknik Untuk Melakukan <i>Content Filtering</i>	3-13
3.3.4	Analisis Software Dansguardian	3-13
3.3.5	Analisis Pemetaan Kebutuhan Rancangan Kebijakan	3-14
3.4	Perancangan	3-15
3.4.1	Perancangan Topologi Jaringan Teknik Informatika UNPAS	3-15
3.4.2	Perancangan Alokasi <i>IP Address</i>	3-16
3.5	Skenario Pengujian	3-16
BAB 4	IMPLEMENTASI DAN PENGUJIAN	4-1
4.1	Rancangan Kebijakan Jaringan Teknik Informatika UNPAS	4-1
4.2	Spesifikasi Kebutuhan	4-2
4.2.1	Kebutuhan Perangkat Keras (<i>Hardware</i>)	4-2
4.2.2	Kebutuhan Perangkat Lunak (<i>Software</i>)	4-2
4.3	Implementasi	4-3
4.3.1	Konfigurasi <i>IP Address</i> Pada Server	4-4
4.3.2	Instalasi Dansguardian	4-5
4.3.3	Konfigurasi Dansguardian	4-5
4.4	Pengujian	4-10
4.4.1	Pengujian Koneksi Melalui <i>Ping</i>	4-10
4.4.2	Pengujian Akses Konten Bermuatan Negatif	4-10
BAB 5	KESIMPULAN DAN SARAN	5-1
5.1	Kesimpulan	5-1
5.2	Saran	5-1

DAFTAR ISTILAH

No.	Istilah	Keterangan
1.	<i>Content</i>	Konten atau isi
2.	<i>Filtering</i>	Penyaringan
3.	<i>Rule</i>	Alur
4.	<i>Blacklist</i>	Daftar hitam atau daftar yang diblokir
5.	<i>Client</i>	Klayen
6.	<i>Existing</i>	Sistem yang berjalan
7.	<i>Gateway</i>	Gerbang jaringan
8.	<i>Cache</i>	Mekanisme penyimpanan data sekunder digunakan untuk menyimpan data/intruksi yang sering diakses
9.	<i>Troubleshooting</i>	Penyelesaian suatu masalah pada komputer
10.	<i>Firewall</i>	Software yang menjadi sistem keamanan jaringan
11.	<i>Traffic</i>	Alur data dan informasi
12.	<i>Torrent</i>	Media alternatif untuk <i>upload</i> dan <i>download</i> file pada internet
13.	<i>Phrase</i>	Kata
14.	<i>Ethernet</i>	perangkat fisik teknologi dan data link layer untuk jaringan area lokal (LAN)
15.	<i>Interface</i>	Antar muka

DAFTAR GAMBAR





Gambar 1.1 Metologi Tugas Akhir	1-2
Gambar 2.1 Jaringan Local Area Network (LAN).....	2-1
Gambar 2.2 Jaringan Wide Area Network (WAN).....	2-2
Gambar 2.3 Jaringan Metropolitan Area Network (MAN)	2-3
Gambar 2.4 Jaringan Berkabel (Wired Network).	2-4
Gambar 2.5 Jaringan Nirkabel (Wireless Network).....	2-4
Gambar 2.6 Content Filtering.....	2-5
Gambar 2.7 Confidentiality, Integrity, Availability	2-11
Gambar 3.1 Kerangka Tugas Akhir Tahap 1	3-1
Gambar 3.2 Kerangka Tugas Akhir Tahap 2-5	3-2
Gambar 3.3 Topologi jaringan komputer di Teknik Informatika Universitas Pasundan	3-5
Gambar 3.4 <i>Rule filtering</i> pada jaringan Informatika UNPAS (bagian 1).....	3-7
Gambar 3.5 <i>Rule filtering</i> pada jaringan Informatika UNPAS (bagian 2).....	3-8
Gambar 3.6 <i>Rule filtering</i> pada jaringan Informatika UNPAS (bagian 3).....	3-8
Gambar 3.7 Blok Akses WHM Via Wifii	3-9
Gambar 3.8 <i>Rule filtering</i> pada jaringan Informatika UNPAS (bagian 4).....	3-9
Gambar 3.9 konfigurasi pada proxy server (bagian 1).....	3-10
Gambar 3.10 Konfigurasi pada proxy server (bagian 2).....	3-10
Gambar 3.11 Konfigurasi pada proxy server (bagian 3).....	3-11
Gambar 3.12 Konfigurasi pada proxy server (bagian 4).....	3-11
Gambar 3.13 Konfigurasi pada proxy server (bagian 5).....	3-12
Gambar 3.14 Konfigurasi pada proxy server (bagian 6).....	3-12
Gambar 3.15 Pemetaan kebijakan content filtering	3-14
Gambar 3.16 Topologi Jaringan Informatika yang akan dibangun.....	3-15
Gambar 4.1 Login Menggunakan PuTTY.....	4-3
Gambar 4.2 Login ke ubuntu server.....	4-4
Gambar 4.3 Konfigurasi alamat IP pada server	4-4
Gambar 4.4 Proses instalasi dansguardian	4-5
Gambar 4.5 Download Blacklist dari shalla.....	4-6
Gambar 4.6 Kategori blacklist dari shalla.....	4-6
Gambar 4.7 Konfigurasi kategori blacklist	4-7
Gambar 4.8 Konfigurasi kategori blacklist (lanjutan gambar 4.7).....	4-7
Gambar 4.9 Pemblokiran berdasarkan nama domain.....	4-8
Gambar 4.10 Pemblokiran berdasarkan URL	4-8
Gambar 4.11 Konfigurasi pemblokiran berdasarkan kata yang dicari.....	4-9

Gambar 4.12 Fitur bannedregexpurllist.....	4-9
Gambar 4.13 Pemblokiran berdasarkan IP address	4-10
Gambar 4.14 Tes ping dari komputer klien ke server	4-10
Gambar 4.15 Pencarian berdasarkan kata pada search engine	4-11
Gambar 4.16 Tampilan layar ketika situs/website diblokir	4-11
Gambar 4.18 Tampilan halaman URL yang diblokir	4-12
Gambar 4.19 Tampilan pemblokiran website yang menggunakan IP address	4-13

DAFTAR TABEL

Tabel 3.1 Pengamatan Akses Konten Bermuatan Negatif	3-6
Tabel 3.2 Tabel Perancangan Alokasi IP Address	3-16
Tabel 4.1 Kategori content filtering pada jaringan teknik informatika UNPAS	4-1
Tabel 4.2 Spesifikasi kebutuhan perangkat keras	4-2
Tabel 4.3 Spesifikasi Perangkat Lunak	4-2
Tabel 4.4 Hasil Pengujian Akses Terhadap Website Bermuatan Negatif	4-13

DAFTAR SIMBOL

No.	Simbol	Nama Simbol	Keterangan
1.		<i>Start process</i>	Simbol yang digunakan untuk awal proses dimulai
2.		<i>Process</i>	Simbol yang digunakan untuk menunjukkan pengolahan yang dilakukan komputer atau menyatakan suatu posisi
3.		<i>Arus / flow</i>	Simbol yang menyatakan alur / langkah dari suatu proses
4.		<i>End process</i>	Simbol yang digunakan untuk menandai akhir proses