

**IMPLEMENTASI FIREWALL FILTER RULES SEBAGAI UPAYA
MENCIPTAKAN INTERNET SEHAT BERBASIS MIKROTIK**

SKRIPSI



Disusun Oleh

Danang Prastia

15.11.9371

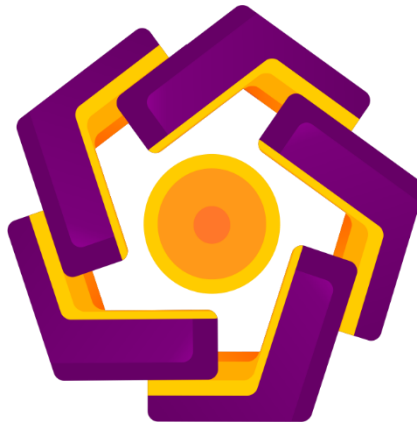
**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2019

**IMPLEMENTASI FIREWALL FILTER RULES SEBAGAI UPAYA
MENCIPTAKAN INTERNET SEHAT BERBASIS MIKROTIK**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana S1
pada Program Studi Informatika



Disusun Oleh

Danang Prastia

15.11.9371

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2019

PERSETUJUAN

SKRIPSI

**IMPLEMENTASI FIREWALL FILTER RULES SEBAGAI UPAYA
MENCIPTAKAN INTERNET SEHAT BERBASIS MIKROTIK**

yang dipersiapkan dan disusun oleh

Danang Prastia

15.11.9371

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 8 November 2019

Dosen Pembimbing,



Bayu Setiaji, M.Kom

NIK. 190302216

PENGESAHAN

SKRIPSI

**IMPLEMENTASI FIREWALL FILTER RULES SEBAGAI UPAYA
MENCIPTAKAN INTERNET SEHAT BERBASIS MIKROTIK**

yang dipersiapkan dan disusun oleh

Danang Prastia

15.11.9371

telah dipertahankan di depan Dewan Penguji
pada 18 November 2019

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Ichsan Wiratama, ST, M.Cs
NIK. 190302119



Eli Pujastuti, M.Kom
NIK. 190302227



Bayu Setiaji, M.Kom
NIK. 190302216



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 18 November 2019

DEKAN FAKULTAS ILMU KOMPUTER



Krisnawati, S.Si, M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 18 November 2019

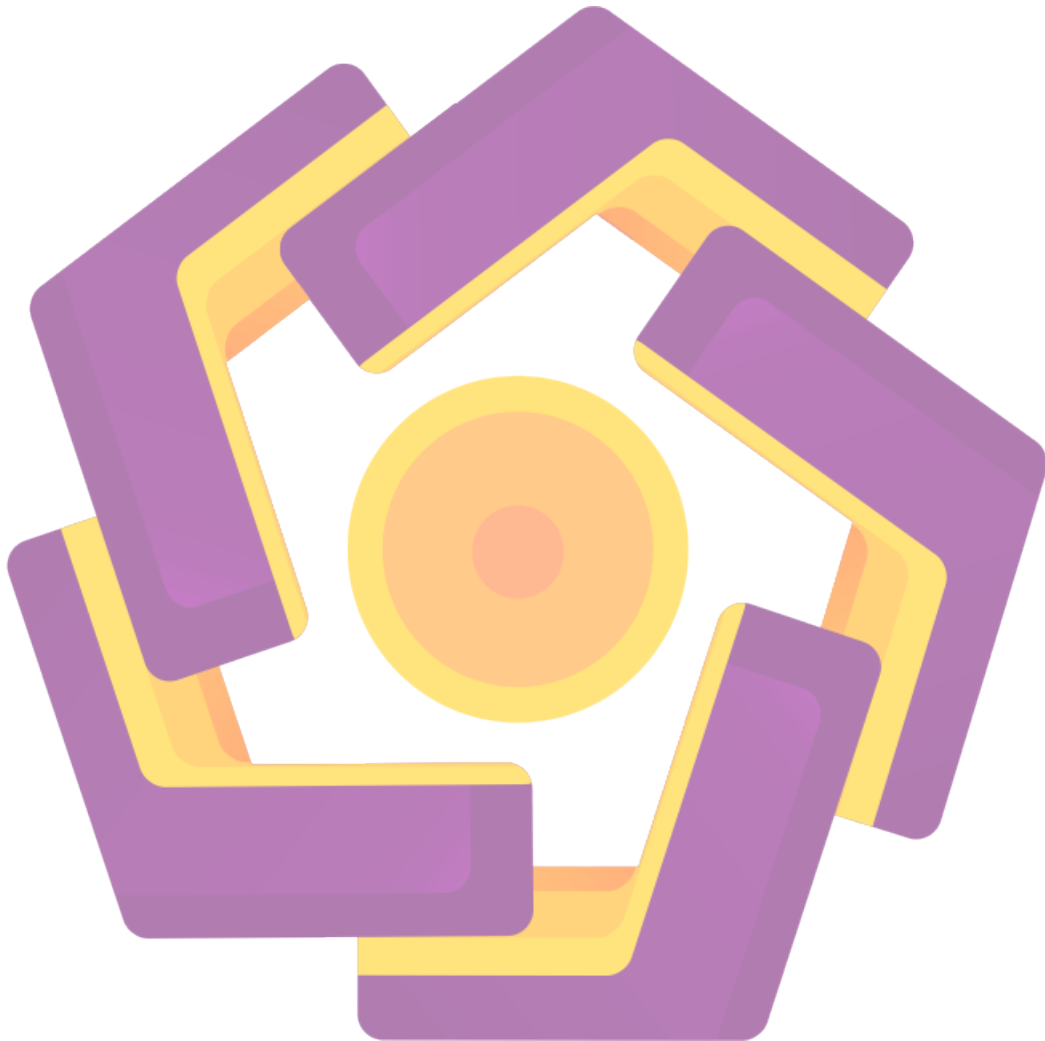


Danang Prastia
NIM. 15.11.9371

MOTTO

“Jutaan orang bahkan tidak menyadari bahwa sebenarnya pekerjaan seberat apapun dapat diselesaikan jika ada niatan, kemauan dan Do'a yang kuat”

~ Danang Prastia



PERSEMBAHAN

Skripsi ini bukanlah sesuatu yang terbaik, namun penulis mempersembahkan skripsi ini kepada :

1. Kedua orang tua, Bapak Heru Asmoro dan Ibu Betty Handayani, beserta segenap keluarga yang telah memberikan dukungan dan doa untuk kelancaran dalam menempuh kuliah serta dalam penyelesaian skripsi ini.
2. Bapak Bayu Setiaji, M.Kom., selaku dosen pembimbing, yang telah memberikan pengarahan serta saran dalam menyelesaikan tugas akhir skripsi ini.
3. Teman – teman dari kelas 15-S1 IF-13, yang telah menjadi teman sekaligus keluarga selama perkuliahan di UNIVERSITAS AMIKOM YOGYAKARTA.
4. Teman – teman yang telah menemani dan membantu dalam masa penyusunan tugas akhir atau skripsi ini.

KATA PENGANTAR

Puji syukur kita panjatkan kepada Allah SWT karena Rahmat dan Karunia-Nya sehingga penulis dapat menyelesaikan laporan skripsi ini dengan judul “Implementasi Firewall Filter Rules Sebagai upaya Menciptakan Internet Sehat Berbasis Mikrotik“. Keberhasilan dalam menyelesaikan pembuatan laporan skripsi ini adalah berkat bantuan dan dukungan dari berbagai pihak. Maka dari itu pada kesempatan kali ini penulis mengucapkan terimakasih sebesar-besarnya kepada:

1. Prof. Dr. M. Suyanto, M.M selaku Rektor Universitas Amikom Yogyakarta.
2. Ibu Krisnawati, S. Si, M.T., selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Bapak Sudarmawan, M.T., selaku Kaprodi Universitas AMIKOM Yogyakarta
4. Bapak Bayu Setiaji, M.Kom., selaku dosen pembimbing.
5. Bapak Tristanto Ari Aji, M.Kom., selaku dosen wali
6. Bapak / Ibu Dosen khususnya Jurusan Teknik Informatika di Universitas Amikom Yogyakarta yang telah membekali penulis dengan beberapa disiplin ilmu yang berguna.
7. Kedua orang tua penulis yang telah membesarkan, mendidik, dan selalu memberikan dukungan serta doa untuk menunjang perjalanan hidup
8. Keluarga, sahabat, teman, dan semua pihak yang telah membantu dan mendukung sehingga terselesainya skripsi ini.

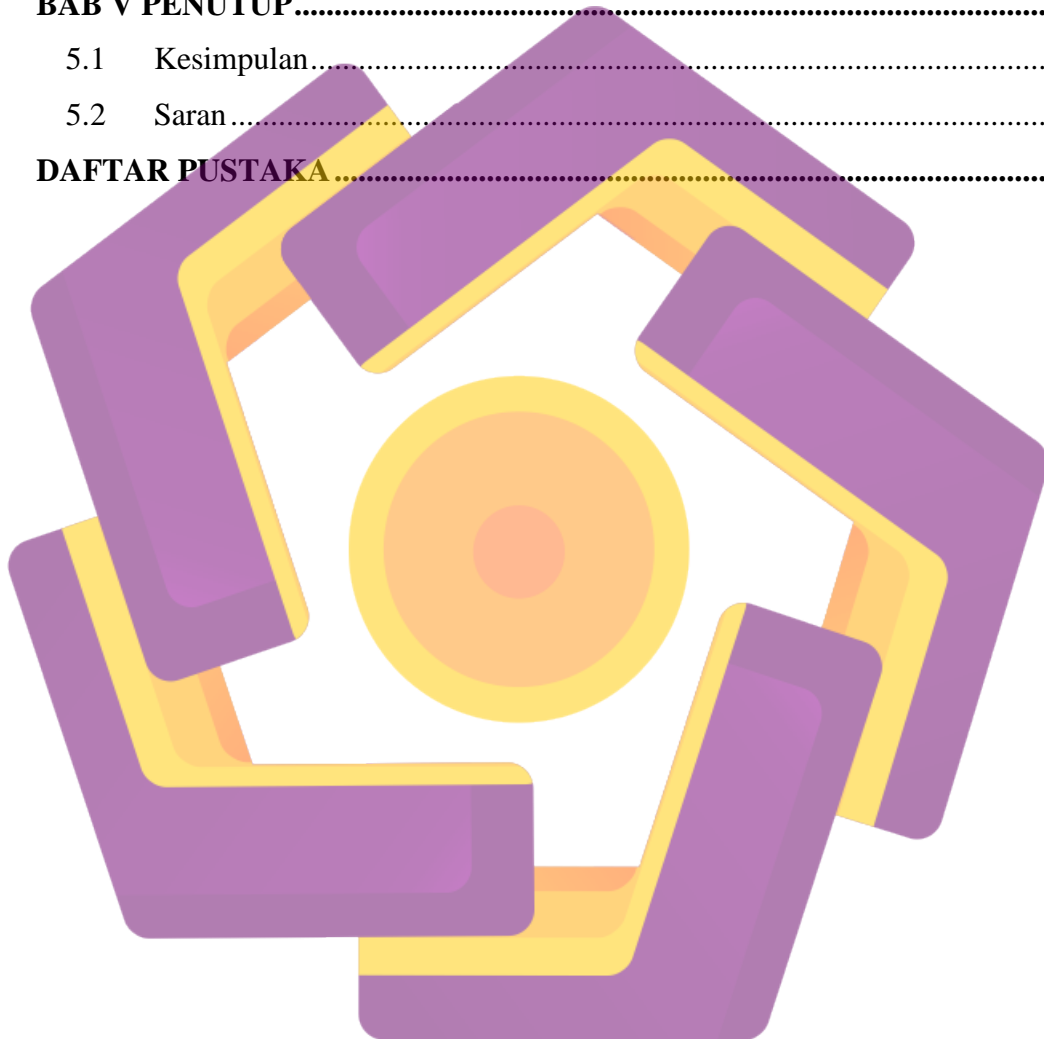
Semoga segala bentuk dukungan dan bantuan dari pihak yang telah penulis sebutkan dapat menjadi amalan dan berkah dan mendapat balasan dari Tuhan Y.M.E. Penulis menyadari, laporan skripsi ini masih banyak kelemahan dan kekurangan nya. Karena itu kritik dan saran yang membangun akan diterima dengan senang hati, mudah – mudahan keberadaan Tugas Akhir ini dapat bermanfaat dan menambah wawasan kita.

DAFTAR ISI

JUDUL	i
PERSETUJUAN	ii
PENGESAHAN	iii
PERNYATAAN	iv
MOTTO	v
PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR TABEL	xi
DAFTAR GAMBAR	xii
INTISARI	xiv
ABSTRACT	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian	4
1.6 Metode Penelitian.....	5
1.6.1 Metode Pengumpulan Data.....	5
1.6.2 Metode Pengembangan	5
1.7 Metode Penulisan	7
BAB II LANADASAN TEORI	8
2.1 Tinjauan Pustaka	8
2.2 Internet.....	9
2.2.1 Definisi Internet	9
2.2.2 Sejarah Internet	10
2.3 Internet Sehat.....	10
2.4 IP Address	11

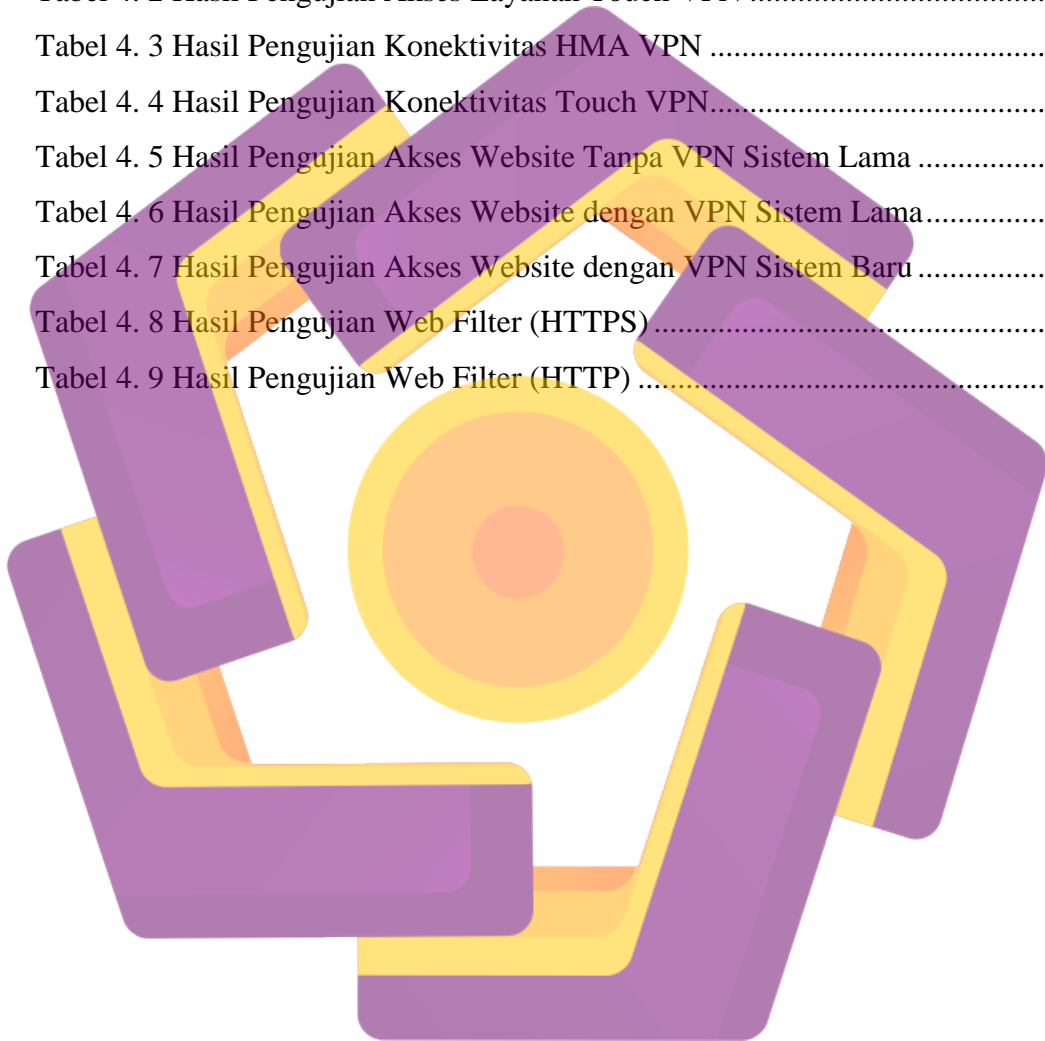
2.4.1	IP Address Versi 4	11
2.5	DNS (Domain Name System)	12
2.5.1	Definisi DNS (Domain Name System)	12
2.5.2	Struktur DNS.....	13
2.6	Virtual Private Network (VPN).....	14
2.7	Mikrotik.....	15
2.8	Firewall.....	15
2.8.1	Definisi Firewall.....	15
2.8.2	Lokasi Firewall Pada Jaringan Komputer.....	15
2.8.3	Cara kerja Firewall.....	16
2.9	NDLC	16
2.10	Aplikasi Pendukung	19
2.10.1	Winbox.....	19
2.10.2	Hide My Ass (HMA) VPN	20
2.10.3	Touch VPN.....	20
BAB III	METODE PENELITIAN	21
3.1	Metode Pengumpulan Data	21
3.1.1	Studi Pustaka.....	21
3.1.2	Observasi.....	21
3.2	Metode Pengembangan	22
3.2.1	Analisis.....	22
3.2.2	Perancangan	26
3.2.3	Implementasi.....	28
3.2.4	Monitoring (Pengawasan)	28
3.2.5	Management (Pemeliharaan)	28
3.3	Skenario Pengujian.....	29
3.3.1	Pengujian Firewall Filter Rules untuk Memblokir VPN	29
3.3.2	Pengujian Firewall Filter Rules untuk Web Filtering	30
BAB IV	IMPLEMENTASI DAN PEMBAHASAN	31
4.1	Implementasi	31
4.1.1	Implementasi Topologi Jaringan.....	31

4.1.2	Implementasi Firewall Filter Rules.....	37
4.2	Monitoring.....	42
4.2.1	Pengujian.....	42
4.2.2	Hasil Pengujian	52
4.3	Management	56
BAB V	PENUTUP.....	57
5.1	Kesimpulan.....	57
5.2	Saran.....	58
DAFTAR PUSTAKA	59



DAFTAR TABEL

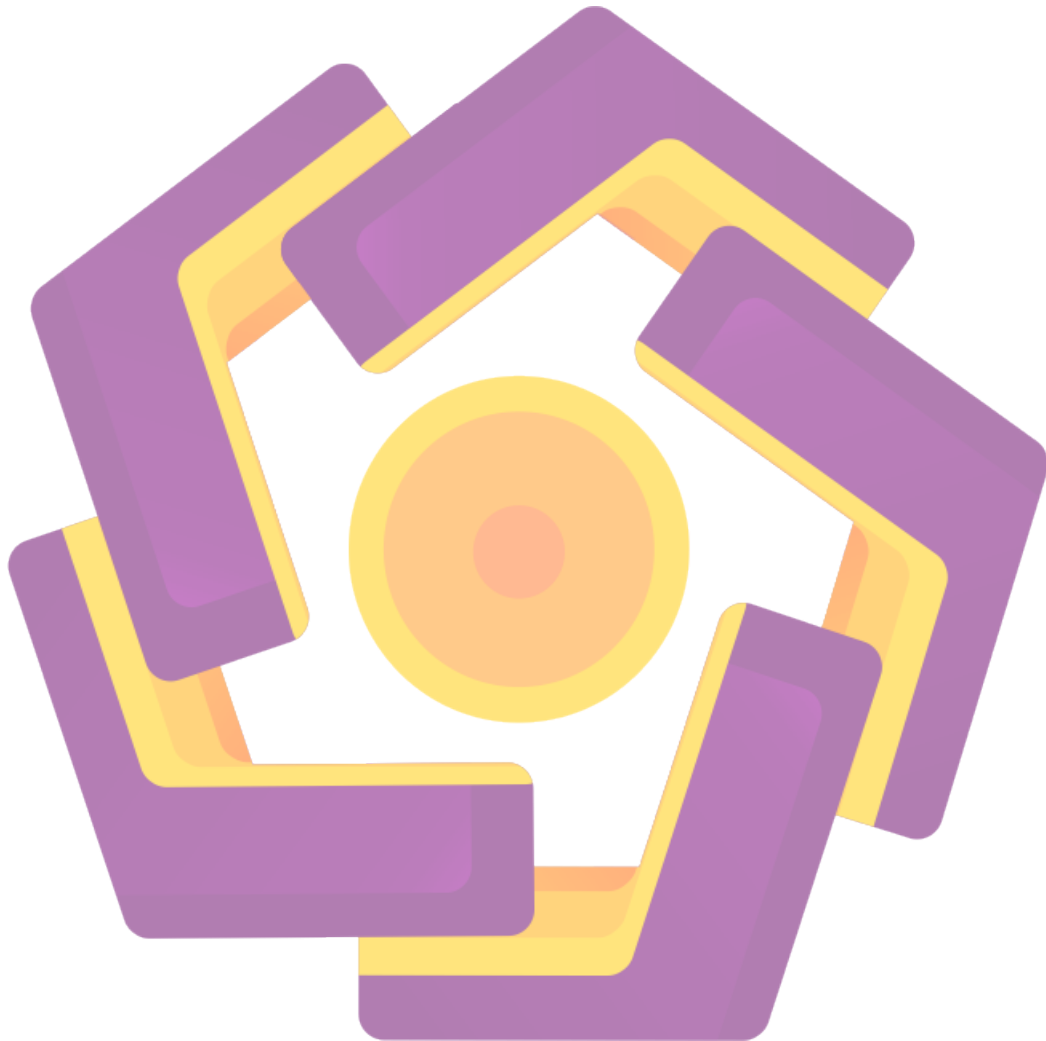
Tabel 3. 1 Kebutuhan Hardware	24
Tabel 3. 2 Kebutuhan Software.....	25
Tabel 4. 1 Hasil Pengujian Akese Layanan HMA VPN	52
Tabel 4. 2 Hasil Pengujian Akses Layanan Touch VPN	52
Tabel 4. 3 Hasil Pengujian Konektivitas HMA VPN	53
Tabel 4. 4 Hasil Pengujian Konektivitas Touch VPN.....	53
Tabel 4. 5 Hasil Pengujian Akses Website Tanpa VPN Sistem Lama	54
Tabel 4. 6 Hasil Pengujian Akses Website dengan VPN Sistem Lama.....	54
Tabel 4. 7 Hasil Pengujian Akses Website dengan VPN Sistem Baru	54
Tabel 4. 8 Hasil Pengujian Web Filter (HTTPS)	55
Tabel 4. 9 Hasil Pengujian Web Filter (HTTP)	55



DAFTAR GAMBAR

Gambar 2. 1 Virtual Private Network	14
Gambar 2. 2 lokasi Firewall Pada Jaringan Komputer	16
Gambar 2. 3 NDLC (Network Development Life Cycle).....	17
Gambar 3. 1 Topologi Jaringan yang Berjalan	23
Gambar 3. 2 Topologi Jaringan yang Akan digunakan.....	27
Gambar 4. 1 Inisialisasi Interface.....	32
Gambar 4. 2 Pengalamatan IP	32
Gambar 4. 3 Konfigurasi DNS.....	33
Gambar 4. 4 Konfigurasi Routing Table.....	33
Gambar 4. 5 Konfigurasi DHCP Server.....	34
Gambar 4. 6 Konfigurasi Chain NAT Rule	34
Gambar 4. 7 Konfigurasi Action NAT Rule	35
Gambar 4. 8 Konfigurasi Hotspot	35
Gambar 4. 9 Konfigurasi WAN	36
Gambar 4. 10 Konfigurasi LAN Host.....	36
Gambar 4. 11 Konfigurasi WLAN.....	37
Gambar 4. 12 DNS HMA VPN.....	38
Gambar 4. 13 DNS Touch VPN.....	38
Gambar 4. 14 Script grab DNS Cache	39
Gambar 4. 15 Konfigurasi Scheduler.....	40
Gambar 4. 16 Konfigurasi Firewall Filter untuk Block VPN	41
Gambar 4. 17 Konfigurasi Firewall Filter untuk Web Filter	42
Gambar 4. 18 Mengaktifkan HMA VPN	43
Gambar 4. 19 IP HMA yang Tercatat di Address Lists	44
Gambar 4. 20 Touch VPN berstatus Aktif	45
Gambar 4. 21 Pengujian HMA VPN pada Smartphone.....	46
Gambar 4. 22 Gambar 4.22 Uji Konektivitas HMA VPN	47
Gambar 4. 23 Uji Konektivitas Touch VPN pada Browser	47
Gambar 4. 24 Uji Konektivitas HMA VPN di Smartphone.....	48

Gambar 4. 25 Akses Playboy.com Tanpa VPN	49
Gambar 4. 26 Akses Playboy.com dengan VPN di Sistem Lama	49
Gambar 4. 27 Akses Playboy.com Dengan VPN di Sistem Baru	50
Gambar 4. 28 Pengujian Protokol HTTPS	51
Gambar 4. 29 Pengujian Protokol HTTP	51



INTISARI

Internet memiliki peranan penting dalam penyebaran teknologi dan informasi, internet mempermudah dalam memberi informasi kepada masyarakat luas dan juga banyak digunakan dalam bidang industri, penelitian, kesehatan, dan lain sebagainya. Informasi yang beredar di internet tidak dibatasi, informasi yang beredar bersifat positif dan negative, informasi yang bersifat negative seperti pornografi, perjudian, obat-obatan, dan penipuan banyak beredar di internet.

Pengguna internet jika dilihat dari usia sangatlah kompleks mulai dari kalangan anak-anak hingga orang dewasa. *Filter* terhadap konten yang beredar di internet merupakan salah satu upaya menciptakan internet sehat untuk masyarakat, agar informasi yang diterima merupakan informasi yang bersifat positif.

Pemerintah telah menerapkan *filter* terhadap konten negative, namun masih banyak orang yang masih bisa mengakses konten tersebut dengan menggunakan aplikasi VPN dan Web Proxy. Penelitian ini dilakukan untuk membantu upaya pemerintah dalam menyaring konten negative, *firewall filter rules* digunakan untuk memfilter *website* yang mengandung unsur negative dan juga untuk membatasi layanan VPN dengan menggunakan Mikrotik, penulis mengimplementasikan system ini pada jaringan lokal.

Kata Kunci : VPN, Filter Rule, Internet

ABSTRACT

The internet has an important role in the dissemination of technology and information, the internet makes it easy to provide information to the wider community and is also widely used in industry, research, health and so forth. Information circulating on the internet is not restricted, information that is positive and negative, information that is negative is such as pornography, gambling, drugs and fraud is circulating on the internet.

Internet users when viewed from age are very complex ranging from children to adults. Filtering the content circulating on the internet is one of the efforts to create a healthy internet for the community, so that the information received is positive information.

The government has applied filter to negative content, but there are still many people who can still access the content using VPN and Web Proxy. This research was conducted to assist government effort in filtering negative content, firewall filter rules are used to filter that contain negative element and also to limit VPN service using Mikrotik, the authors implement this system on the local network.

Keyword : VPN, Filter Rule, Internet

