INTERNET POSTIF DENGAN METODE *WEB FILTERING* LAYER 7 PADA JARINGAN WIRELESS (STUDY CASE HOTSPOT RT4 CIPEUTEUY BARU SUMEDANG)

M. Agreindra Helmiawan
Dosen Jurusan Teknik Informatika STMIK Sumedang
Email :agreindra@stmik-sumedang.ac.id

ABSTRAK

Dampak dan pengaruh konten negatif telah banyak dimuat di berbagai media, pengaruh konten negatif tersebut berupa konten yang berbau pornografi, perjudian, penipuan dan sebagainya. Untuk menghindari dampak konten negatif tersebut, selalu ditekankan prinsip dasar yang harus diketahui dalam menggunakan internet.Salah satunya dengan menanamkan etika penggunaan internet secara sehat dan aman atau Cyber Ethics.Pengontrolan internet dapat dilakukan di mekanisme server di setiap jaringan internet daerah sampai ke unit server terkecil.Metode Web Filtering merupakan salah satu metode untuk mencapai tujuan internet sehat dan positif, kinerja dari metode Web Filtering yaitu proxy/caching digabungkan dengan Content Filtering System, sehingga web yang mengandung konten negatif dapat diblokir.Penelitian dan implementasi Web Filtering ini penulis lakukan di Hotspot RTRWnet RT4 Cipeuteuy Baru Sumedang.Hotspot ini digunakan untuk kepentingan masyarakat khususnya di Cipeuteuy baru RT4 RW 6 Cipeuteuy Baru Sumedang.

Kata kunci :Internet, Cyber Ethics, Web Filtering, Hotspot

PENDAHULUAN

a. Latar Belakang

Internet saat ini berkembang dan sangat dibutuhkan oleh masyarakat.Tidak sedikit internet juga telah mengubah pola hidup masyarakat dalam belajar, bekerja berkomunikasi dan aspek hidup lainnya.Masyarakat menggunakna internet dianggap lebih efektif dan efisien dalam berkomunikasi; contohnya email, dan jejaring social. Berdsarkan hasil survey yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia pada tahun 2013 mencapai ± 82 juta pengguna, meningkat 13 % dibanding 2012 yang mencapai 63 juta pengguna. APJII juga memperkirakan pengguna internet akan meningkat ±107 juta pengguna. Kementrian Komunikasi dan Informatika (Kemkominfo) juga membenarkan pernyataan tersebut dan menambahkan bahwa pengguna internet didominasi oleh pengguna muda yang berumur 15-30 tahun atau disebut dengan "Netizen". Pengguna muda juga melakukan pencarian data dan informasi pada internet, semakin banyak didapatkannya data dan informasi, semakin banyak pula konten negatif yang akan di dapatkan oleh pengguna muda.

Dampak dan pengaruh konten negatif telah banyak dimuat di berbagai media, pengaruh konten negatif tersebut berupa konten yang berbau pornografi, perjudian, penipuan dan sebagainya.Untuk menghindari dampak konten negatif tersebut, selalu ditekankan prinsip dasar yang harus diketahui dalam menggunakan internet.Salah satunya dengan menanamkan etika penggunaan internet secara sehat dan aman atau *Cyber Ethics*.Pihak Kemkominfo juga menyelenggarakan program INSAN (internet sehat dan aman) dan TRUST Positif sebagai aturan dan pemblokiran situs yang memilki konten negatif.Dengan adanya program tersebut, diharapkan dapat mengurangi dan menghilangkan konten negatif pada internet.Namun konten negatif masih dapat di akses oleh pengguna karena program tersebut masih di atur secara terpusat, sehingga pihak pusat tidak dapat mengontrol secara keseluruhan terhadap pengguna internet yang saat ini jumlahnya mencapai 100 juta pengguna.Pengontrolan internet dapat

dilakukan di mekanisme server di setiap jaringan internet daerah sampai ke unit server terkecil.

Metode *Web Filtering* merupakan salah satu metode untuk mencapai tujuan internet sehat dan positif, kinerja dari metode *Web Filtering* yaitu proxy/caching digabungkan dengan Content Filtering System, sehingga web yang mengandung konten negatif dapat diblokir.Penelitian dan implementasi *Web Filtering* ini penulis lakukan di Hotspot RTRWnet RT4 Cipeuteuy Baru Sumedang.Hotspot ini digunakan untuk kepentingan masyarakat khususnya di Cipeuteuy baru RT4 RW 6 Cipeuteuy Baru Sumedang.

b. Ruang Lingkup

Berdasarkan latar belakang yang telah dikemukakan maka lingkup permasalahan yang akan dibahas adalah sebagai berikut :

a) Membuat konsep aturan penggunaan internet melalui metode Web Filtering.
b) Membuat konfigurasi yang sesuai dalam mengikuti aturan Cyber Ethics untuk memisahkan konkonten internet negative dan positif dengan memanfaatkan Application Layer filtering.

c. Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut :

a) Internet yang aman dan sehat dengan perlindungan akses internet berdasarkan daftar informasi sehat dan terpercaya
b) Perlindungan pada masyarakat terhadap nilai etika, moral dan kaidah yang berlaku di Indonesia
c) Penghematan akses dan bandwidth internet.

d. Manfaat

Manfaat dari penelitian ini adalah :

a) Penggunaan internet yang sehat dan positif sehingga bermanfaat bagi warga Cipeteuy Baru RT4 Kelurahan Situ, Kecamatan Sumedang Utara
b) Adanya kinerja dari metode *Web Filtering* yaitu *proxy/caching* yang digabungkan dengan *Content Filtering System*, sehingga menghasilkan web yang mengandung konten negatif dapat diblokir.

e. Metode Penelitian

Pada penelitian ini penulis menggunakan beberapa metode untuk menyelesaikan masalah dengan berbagai cara, antara lain :

a) Studi Pustaka, pada tahap ini penulis melakukan studi pembelajaran yang terkait dengan metode *Web Filtering* dengan menggunakan media berupa Ebook, atau mencari bahan-bahan lainnya dari berbagai forum dan artikel online terkait dengan tata kelola dan perencanaan teknologi informasi.
b) Observasi, Survei dan Wawancara, Dimana penulis melakukan pengamatan langsung ke tempat atau organisasi.

PEMBAHASAN

Jaringan komputer adalah himpunan “interkoneksi” antara 2 komputer *autonomous* atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*). [1]

Komputer yang saling berhubungan dan dapat berkomunikasi dengan menggunakan protokol tertentu dan memakai alat misalnya *Network Internet Card (NIC),* modem, dll. [2]

Jaringan Komputer adalah sekelompok komputer otonom yang saling dihubungkan satu dengan lainnya menggunakan protokol komunikasi melalui media transmisi, sehingga dapat saling berbagi menggunakan sumber daya yang ada dan berkomunikasi. [1]

Jaringan komputer dapat dibedakan berdasarkan cakupan geografisnya. Ada empat kategori utama jaringan komputer yaitu :

a. LAN (*Local Area Network*)

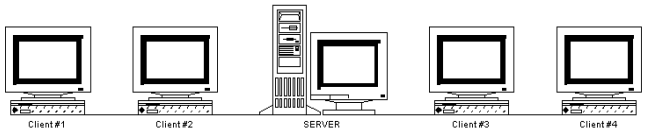
LAN (Local Area Network) adalahjaringan skala kecil, biasanya dalam 1 bangunan atau area. [2]

Berdasarkan kabel yang digunakan ,ada dua cara membuat jaringan LAN, yaitu dengan kabel BNC dan kabel UTP

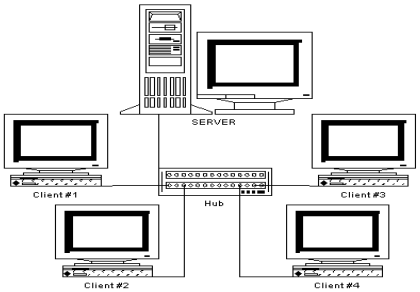
Keuntungan Jaringan LAN

1. Pertukaran file dapat dilakukan dengan mudah (File Sharing).
2. Pemakaian printer dapat dilakukan oleh semua client (Printer Sharing).
3. File-file data dapat disimpan pada server, sehingga data dapat diakses dari semua client menurut otorisasi sekuritas dari semua karyawan, yang dapat dibuat berdasarkan struktur organisasi perusahaan sehingga keamanan data terjamin.
4. File data yang keluar/masuk dari/ke server dapat di kontrol.
5. Proses backup data menjadi lebih mudah dan cepat.
6. Resiko kehilangan data oleh virus komputer menjadi sangat kecil sekali.
7. Komunikasi antar karyawan dapat dilakukan dengan menggunakan E-Mail & Chat.

Bila salah satu client/server terhubung dengan modem, maka semua atau sebagian komputer pada jaringan LAN dapat mengakses ke jaringan Internet atau mengirimkan fax melalui 1 modem.



Gambar 1 Jaringan Kabel LAN



Gambar 2 Jaringan LAN

b. WAN (*Wide Area Network*)

WAN (Wide Area Network) adalah jaringan skala besar, contohnya: antar kota atau antar negara. [2]

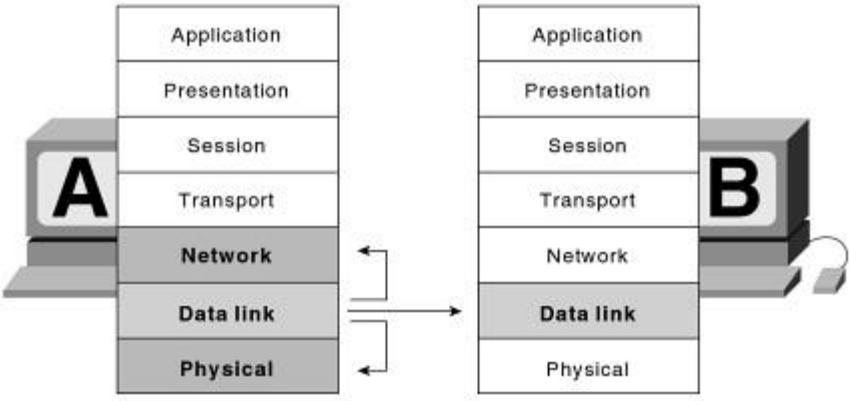
Dengan sistem jaringan ini, pertukaran data antar kantor dapat dilakukan dengan cepat serta dengan biaya yang relatif murah. Sistem jaringan ini dapat menggunakan jaringan Internet yang sudah ada, untuk menghubungkan antara kantor pusat dan kantor cabang atau dengan PC Stand Alone/Notebook yang berada di lain kota ataupun negara.

Keuntungan Jaringan WAN.

1. Server kantor pusat dapat berfungsi sebagai bank data dari kantor cabang.
2. Komunikasi antar kantor dapat menggunakan E-Mail & Chat.
3. Dokumen/File yang biasanya dikirimkan melalui fax ataupun paket pos, dapat dikirim melalui E-mail dan Transfer file dari/ke kantor pusat dan kantor cabang dengan biaya yang relatif murah dan dalam jangka waktu yang sangat cepat.

Pooling Data dan Updating Data antar kantor dapat dilakukan setiap hari pada waktu yang ditentukan.

OSI Layer



Gambar 3. OSI Layer
(Sumber :Internetworking Technologies Handbook - Cisco System Inc)

a. Layer 7
Layer 7 ini bernama *Application* Layer, yang berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan dan kemudian membuat pesan-pesan kesalahan. Protocol yang berada dalam lapisan ini adalah HTTP, FTP, SMTP dan NFS

b. Layer 6
Layer 6 ini bernama Presentation Layer, yang berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protocol yang berada dalam level ini adalah perangkat lunak redirector, seperti layanan Workstation dan juga Network shell (Virtual Network Computing) atau Remote Desktop Protocol.

c. Layer 5
Layer 5 ini bernama Session Layer, yang berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara atau dihancurkan, selain itu dilevel ini juga dilakukan resolusi nama.

d. Layer 4
Layer 4 ini bernama Transport Layer, berfungsi untuk memecah data ke dalam paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada level ini juga membuat sebuah tanda bahwa paket diterima dengan sukses dan mentransmisikan ulang terhadap paket-paket yang hilang ditengah jalan.

e. Layer 3
Layer 3 ini bernama Network Layer, yang berfungsi untuk mendefinisikan alamat-alamat IP, membuat header untuk paket-paket dan kemudian melakukan routing melalui internetworking dengan menggunakan router dan switch layer 3

f. Layer 2
Layer in bernama Datalink Layer, yang berfungsi menentukan bagaimana bit-bit data dikelempokkanmenjadi format yang disbut sebagai frame. Selain itu, pada level ini terjadi koreksi kesalahan, flow control, pengalamatan perangkat keras (seperti halnya MAC Address) dan menentukan bagaimana perangkat-perangkat jaringan seperti hub, bridge, repeater dan switch layer-2 beroperasi. Spesifikasi IEEE 802, membagi level ini menjadi 2 level yaitu Logical Link Control (LLC) dan lapisan Media Access Control (MAC).

g. Layer 1

Layer 1 ini bernama Physical Layer, yang berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan, topologi jaringan dan pengkabelan. Selain itu, level ini juga mendefinisikan bagaimana Network Interface Card (NIC) dapat berinteraksi dengan media kabel atau radio.

HTTP

HTTP (Hypertext Transfer Protocol) adalah sebuah protocol aplikasi yang mendistribusikan, kolaboratif dan sistem informasi hypermedia.HTTP adalah dasar dari komunikasi data untuk World Wide Web.Hypertext disini adalah text yang terstruktur yang digunakan sebagai tautan logis diantara node yang mengandung text.HTTP adalah protocol yang merubah atau mentransfer hypertext.

HTTP berfungsi sebagai respon permintaan melalui protocol pada komputer client. Sebagai contoh, client dan aplikasi browser yang berjalan pada komputer client, merequest HTTP ke server, server akan akan memberikan HTTP yang dituju dengan bentuk HTML (Hypertext Markup Language) sesuai dengan provide resources. Respon dari server tersebut mengandung informasi yang lengkap sesuai dengan request dari client.

Mikrotik RouterOS

Mikrotik RouterOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk IP network dan jaringan wireless [3]

MikroTik RouterOS™, merupakan sistem operasi Linux base yang diperuntukkan sebagai network router. Didesain untuk memberikan kemudahan bagi penggunanya.Administrasinya bisa dilakukan melalui Windows *Application* (WinBox).Selain itu instalasi dapat dilakukan pada Standard komputer PC (Personal Computer). PC yang akan dijadikan router mikrotik pun tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway. Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan resource PC yang memadai.

Sejarah MikroTik RouterOS

MikroTik adalah sebuah perusahaan kecil berkantor pusat di Latvia, bersebelahan dengan Rusia.Pembentukannya diprakarsai oleh John Trully dan Arnis Riekstins.John Trully adalah seorang berkewarganegaraan Amerika yang berimigrasi ke Latvia. Di Latvia ia bejumpa dengan Arnis, Seorang darjana Fisika dan Mekanik sekitar tahun 1995. John dan Arnis mulai me-routing dunia pada tahun 1996 (misi MikroTik adalah merouting seluruh dunia). Mulai dengan sistem Linux dan MS-DOS yang dikombinasikan dengan teknologi Wireless-LAN (WLAN) Aeronet berkecepatan 2 Mbps di Moldova, negara tetangg Latvia, baru kemudian melayani lima pelanggannya di Latvia.

Prinsip dasar mereka bukan membuat Wireless ISP (W-ISP), tetapi membuat program router yang handal dan dapat dijalankan diseluruh dunia.Latvia hanya merupakan tempat eksperimen John dan Arnis, karena saat ini mereka sudah membantu negara-negara lain termasuk Srilanka yang melayani sekitar 400 pengguna.

Linux yang pertama kali digunakan adalah Kernel 2.2 yang dikembangkan secara bersama-sama denag bantuan 5-15 orang staff Research and Development (R&D) MikroTik yang sekarang menguasai dunia routing di negara-negara berkembang. Menurut Arnis, selain staf di lingkungan MikroTik, mereka juga merekrut tenega-tenaga lepas dan pihak ketiga yang dengan intensif mengembangkan MikroTik secara marathon.

MikrotikOS ini digunakan pada jaringan wireless RT4 Cipeuteuy Baru Sumedang yang berfungsi sebagai mengatur lalu-lintas data dan manajemen jaringan.MikrotikOS ini tertanam pada perangkat Routerboard 951H 2Hnd.

Fitur-Fitur Mikrotik

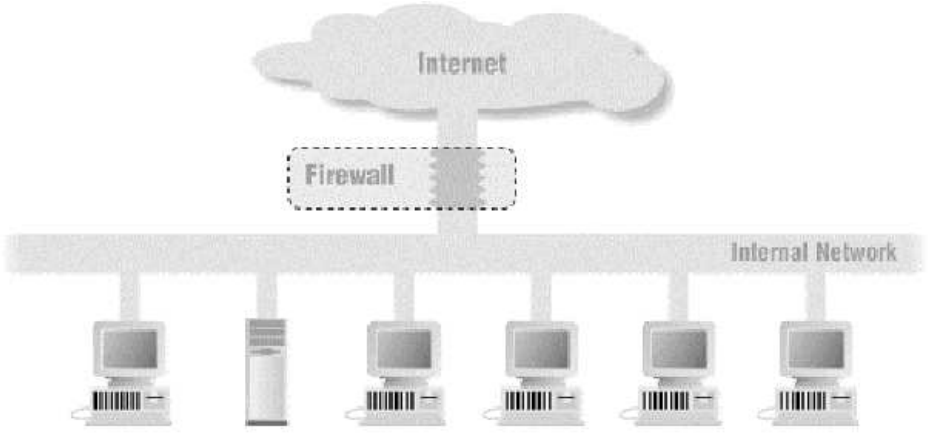
1. **Address List** : Pengelompokan IP Address berdasarkan nama
2. **Asynchronous** : Mendukung serial PPP dial-in / dial-out, dengan otentikasi CHAP, PAP, MSCHAPv1 dan MSCHAPv2, Radius, dial on demand, modem pool hingga 128 ports.
3. **Bonding** : Mendukung dalam pengkombinasian beberapa antarmuka ethernet ke dalam 1 pipa pada koneksi cepat.
4. **Bridge** : Mendukung fungsi bridge spinning tree, multiple bridge interface, bridging *firewall*ing.
5. **Data Rate Management** : QoS berbasis HTB dengan penggunaan burst, PCQ, RED, SFQ, FIFO queue, CIR, MIR, limit antar peer to peer
6. **DHCP** : Mendukung DHCP tiap antarmuka; DHCP Relay; DHCP Client, multiple network DHCP; static and dynamic DHCP leases.
7. ***Firewall* dan NAT** : Mendukung pemfilteran koneksi peer to peer, source NAT dan destination NAT. Mampu memfilter berdasarkan MAC, IP address, range port, protokol IP, pemilihan opsi protokol seperti ICMP, TCP Flags dan MSS.
8. **Hotspot** : Hotspot gateway dengan otentikasi RADIUS. Mendukung limit data rate, SSL ,HTTPS.
9. **IPSec :** Protokol AH dan ESP untuk IPSec; MODP Diffie-Hellmann groups 1, 2, 5; MD5 dan algoritma SHA1 hashing; algoritma enkirpsi menggunakan DES, 3DES, AES-128, AES-192, AES-256; Perfect Forwarding Secresy (PFS) MODP groups 1, 2,5 ISDN : mendukung ISDN dial-in/dial-out. Dengan otentikasi PAP, CHAP, MSCHAPv1 dan MSCHAPv2, Radius. Mendukung 128K bundle, Cisco HDLC, x751, x75ui, x75bui line protokol.
10. **M3P** : MikroTik Protokol Paket Packer untuk wireless links dan ethernet.
11. **MNDP** : MikroTik Discovery Neighbour Protokol, juga mendukung Cisco Discovery Protokol (CDP).
12. **Monitoring / Accounting** : Laporan Traffic IP, log, statistik graph yang dapat diakses melalui HTTP.
13. **NTP** : Network Time Protokol untuk server dan clients; sinkronisasi menggunakan system GPS.
14. **Poin to Point Tunneling Protocol** : PPTP, PPPoE dan L2TP Access Consentrator; protokol otentikasi menggunakan PAP, CHAP, MSCHAPv1, MSCHAPv2; otentikasi dan laporan Radius; enkripsi MPPE; kompresi untuk PPoE; limit data rate.
15. **Proxy** : Cache untuk FTP dan HTTP proxy server, HTTPS proxy; transparent proxy untuk DNS dan HTTP; mendukung protokol SOCKS; mendukung parent proxy; static DNS.
16. **Routing** : Routing statik dan dinamik; RIP v1/v2, OSPF v2, BGP v4.
17. **SDSL** : Mendukung Single Line DSL; mode pemutusan jalur koneksi dan jaringan.
18. **Simple Tunnel** : Tunnel IPIP dan EoIP (Ethernet over IP).
19. **SNMP** : Simple Network Monitoring Protocol mode akses read-only.
20. **Synchronous** : V.35, V.24, E1/T1, X21, DS3 (T3) media ttypes; sync-PPP, Cisco HDLC; Frame Relay line protokol; ANSI-617d (ANDI atau annex D) dan Q933a (CCITT atau annex A); Frame Relay jenis LMI.
21. **Tool** : Ping, Traceroute; bandwidth test; ping flood; telnet; SSH; packet sniffer; Dinamik DNS update.

22. **UPnP** : Mendukung antarmuka Universal Plug and Play.
23. **VLAN** : Mendukung Virtual LAN IEEE 802.1q untuk jaringan ethernet dan wireless; multiple VLAN; VLAN bridging.
24. **VoIP** : Mendukung aplikasi voice over IP.
25. **VRRP** : Mendukung Virtual Router Redudant Protocol.
26. **WinBox** : Aplikasi mode GUI untuk meremote dan mengkonfigurasi MikroTik RouterOS.

Firewall

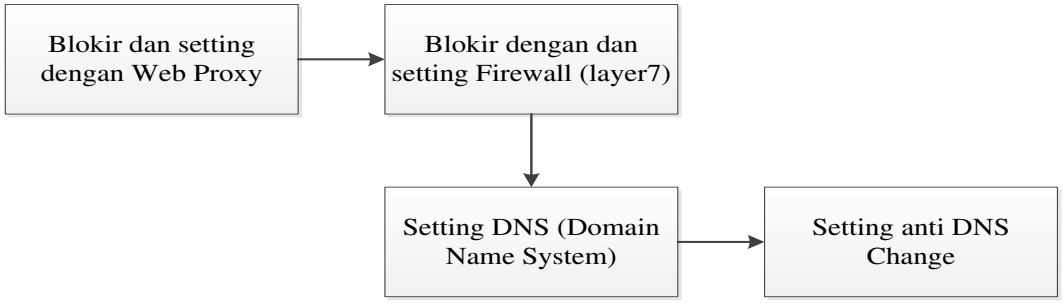
"A firewall is a way to restrict access between the Internet and your internal network. You typically install a firewall at the point of maximum leverage, the point where your network connects to the Internet. The existence of a firewall at your site can greatly reduce the odds that outside attackers will penetrate your internal systems and networks. The firewall can also keep your own users from compromising your systems by sending dangerous information - unencrypted passwords and sensitive data – to the outside world" [4]

Dapat di ambil kesimpulan bahwa firewall merupakan system atau perangkat yang mengizinkan lalulintas data dari jaringan luar yang masuk ke system local pada computer, firewall juga mengamankan akses masuk dengan menggunakan prosedur atau aturan dalam memfilter lalu lintas data tersebut.Letak firewall dapat di gambarkan seperti pada gambar 4, sebagai berikut :



Gambar 4. *Firewall*
(Sumber :Building Internet Firewall, 2000)

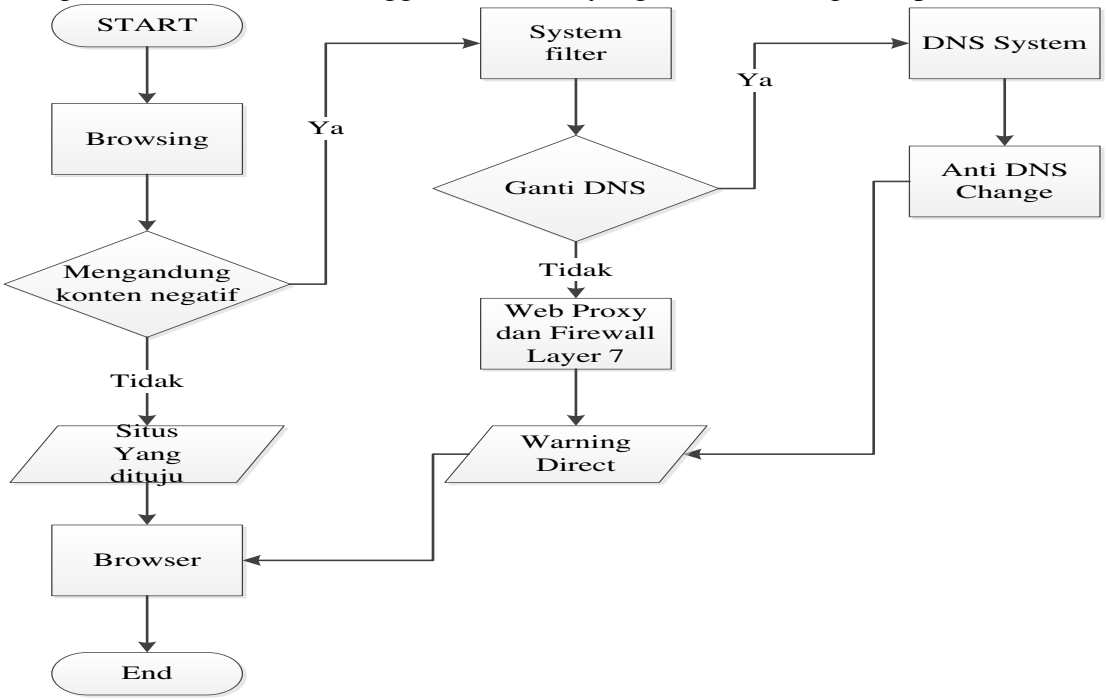
A. Implementasi Internet Sehat Dengan Metode *Web Filtering* Layer 7 Pada Jaringan Wireless (Study Case Hotspot RT4 Cipeuteuy Baru)



Gambar 5. Schema System Method

Skema sistem pada gambar diatas, merupakan skema yang digunakan oleh penulis sebagai dasar aturan dan tujuan untuk internet sehat. Berikut penjelasan gambar :

1. Blokir dan setting *Web Proxy*, blok ini melakukan konfigurasi, aturan dan membuat list untuk situs yang mengandung konten negatif.
2. Blokir dan setting *firewall* (layer7), blok ini mirip dengan blok pertama, tambahannya adalah blok ini berfungsi disaat user menggunakan external proxy, maka blok ini ini akan memfilter dan melakukan pengecekan ulang terhadap situs yang mengandung konten negatif yang nantinya akan diblokir.
3. Setting DNS, blok ini melakukan konfigurasi DNS untuk Client secara universal terhadap client yang terkoneksi dengan jaringan. DNS yang digunakan adalah DNS Nawala (Nawala ini adalah DNS yang diatur oleh pihak Kemkominfo dengan tujuan untuk memblokir situs yang mengandung konten negatif).
4. Setting anti DNS Change, blok ini adalah konfigurasi untuk mengantisipasi user merubah DNS secara manual pada komputernya masing-masing. Dengan arti bahwa anti DNS Change ini memaksa user menggunakan DNS yang telah di konfigurasi pada mikrotik.



Gambar 6. Flowchart *Web Filtering*

Penjelasan Gambar :

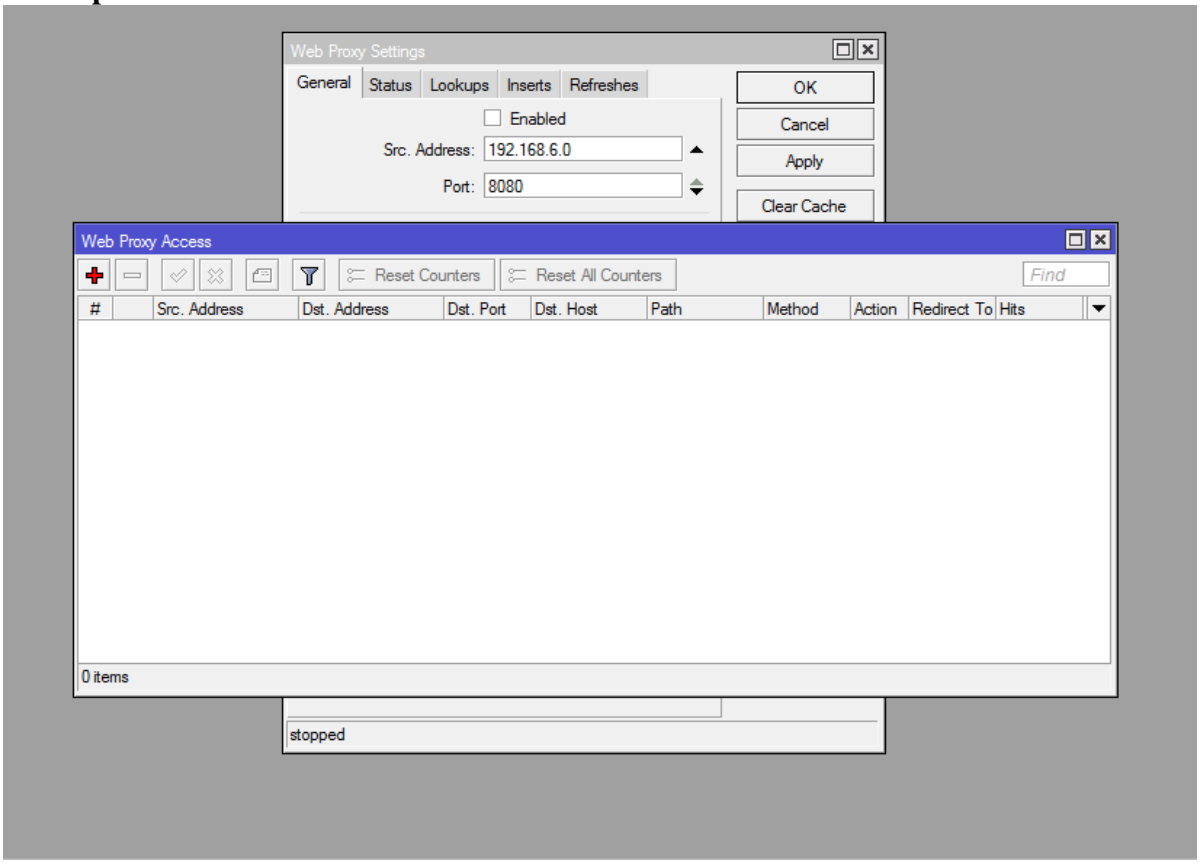
1. Saat user browsing, sistem akan menganalisa situs yang dituju, jika situs yang dituju tidak mengandung konten negatif, maka akan diteruskan ke browser user.
2. Jika user melakukan browsing dan didapati mengandung konten negatif, system filter akan di direct ke sistem *Web Proxy*.
3. Sebelum *Web Proxy* melakukan blokir situs, sistem filter akan mengecek terlebih dahulu DNS yang digunakan, jika DNS tidak diubah maka user akan di direct ke interface blokir yang ditampilkan ke browser user.
4. Jika sistem filter mendapatkan user mengganti DNS, maka Anti DNS change akan memaksa user untuk menggunakan DNS yang telah dikonfigurasi di mikrotik, dan diteruskan ke interface blokir dan ditampilkan ke browser user.

Dari pemaparan schema sytem method dan flowchart system, maka penulis mengambil sampel daftar situs yang mengandung konten negatif yang nanti dijadikan dafta konfigurasi pada mikrotik.

Tabel 2. Daftar Situs yang diblokir

Situs Web yang mengandung konten Negatif	**Blokir Situs + Proxy**
www.bangros.com	**Drop/Deny**
www.redtube.com	**Drop/Deny**
www.xxx.com	**Drop/Deny**
www.sukatoro.com	**Drop/Deny**
www.sex.com	**Drop/Deny**
www.wo-jac.jp	**Drop/Deny**

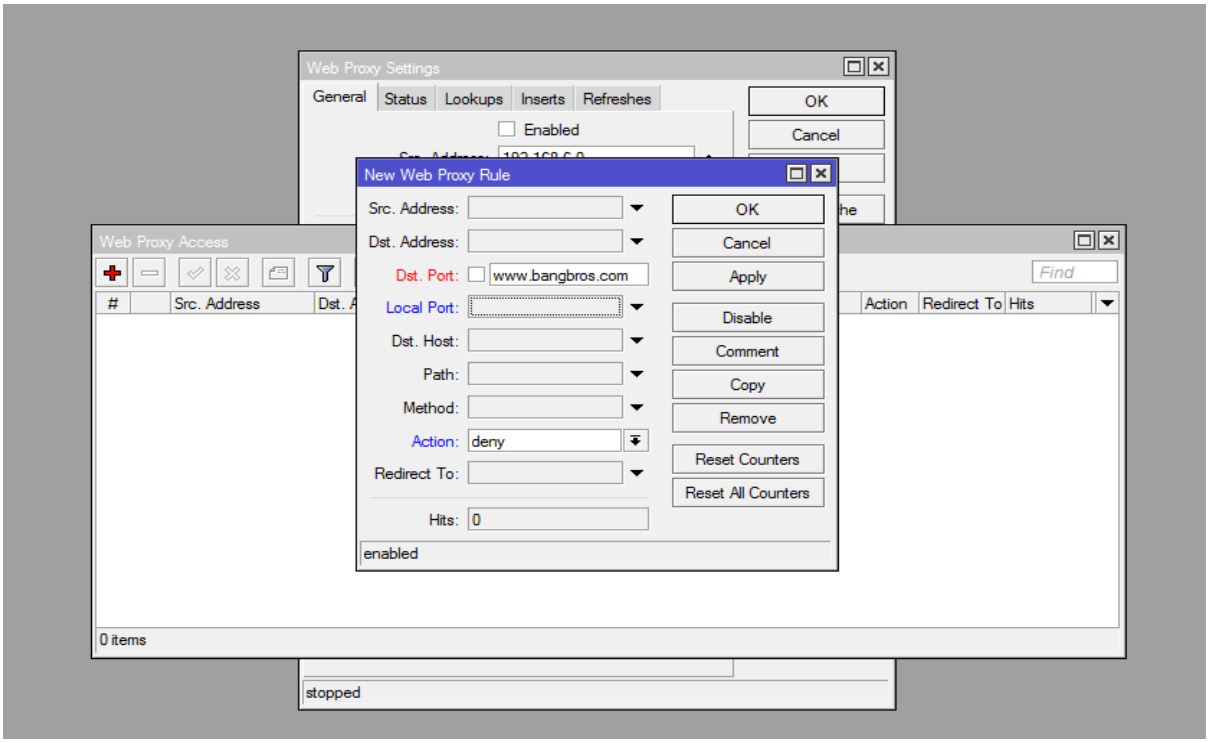
A. Implementasi



Gambar 7. Setting Access *Web Proxy*

Penjelasan gambar :

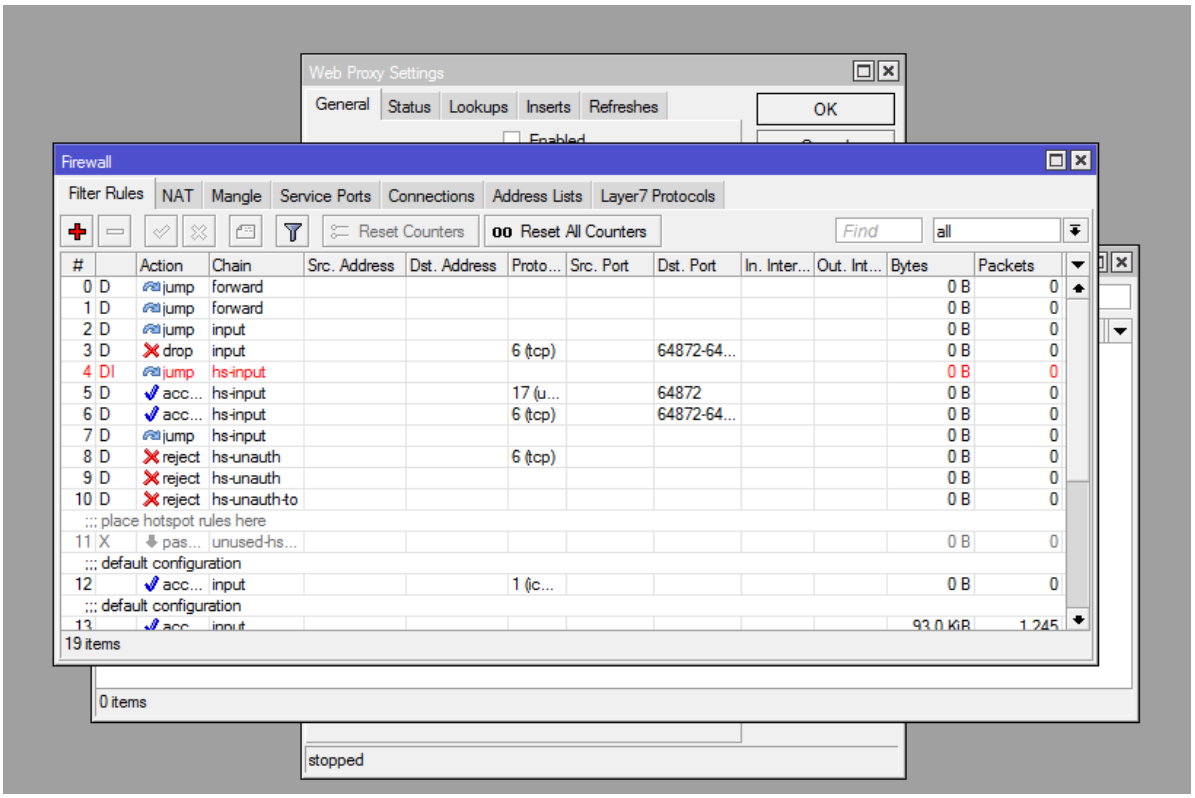
1. Setting *Web Proxy* access
2. Menginput daftar alamat situs yang memiliki konten negatif.



Gambar 8. Setting Daftar Situs Negatif

Penjelasan gambar:

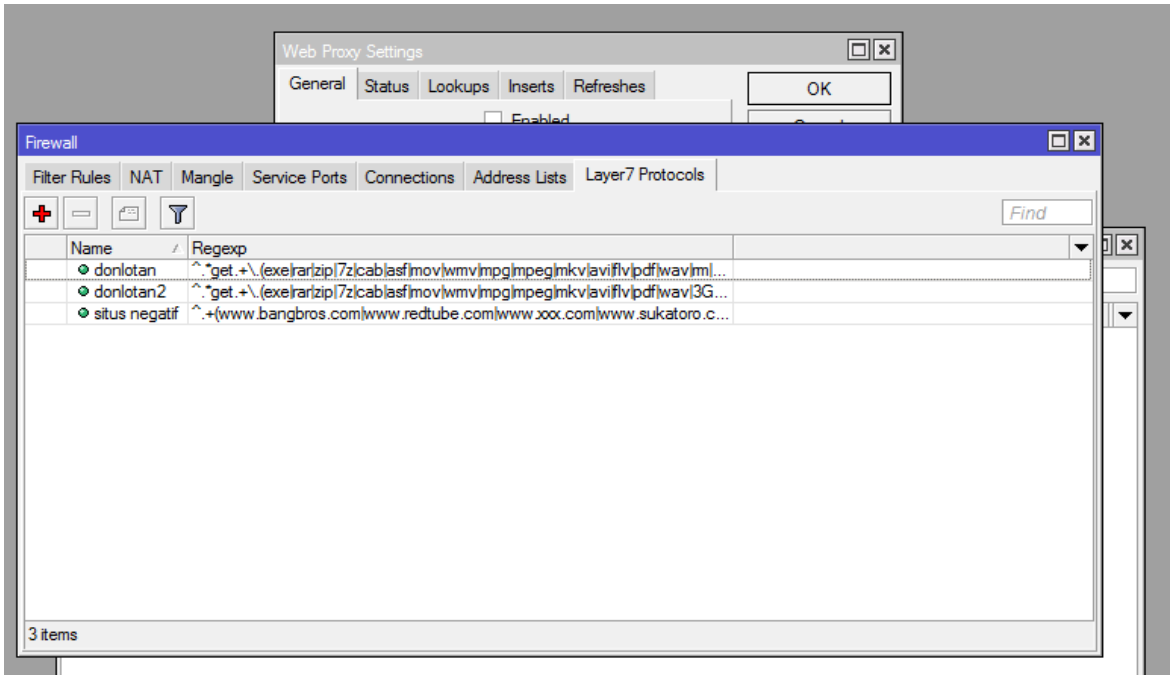
1. Mengkonfigurasi dan membuat aturan alamat situs yang nantinya akan diblokir
2. Konfigurasi access situs tersebut di tolak



Gambar 9. Aturan *Firewall*

Penjelasan gambar :

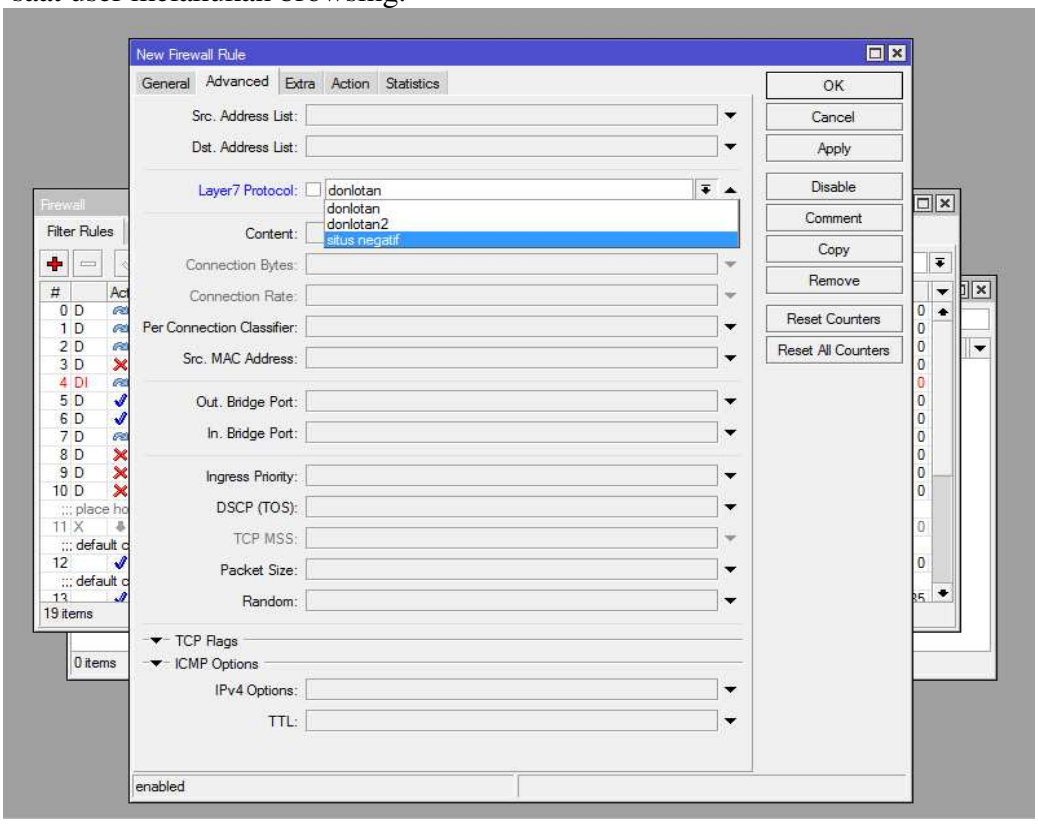
1. Konfigurasi aturan filter pada *firewall*
2. Aturan filter ini sebagai dasar untuk konfigurasi protocol layer 7



Gambar 10. Setting Protokol *Firewall*

Penjelasan gambar :

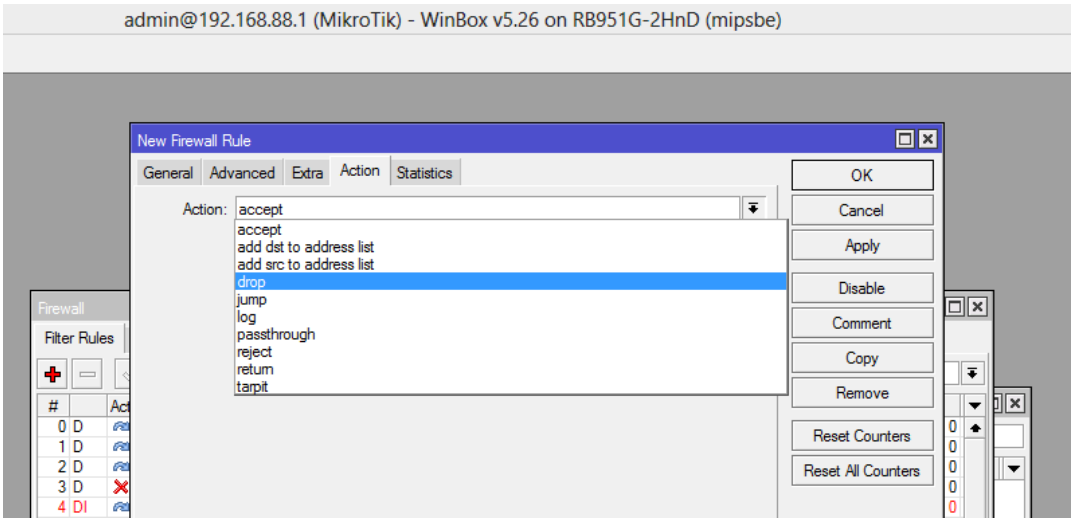
1. Membuat daftar situs blacklist pada protocol layer 7
2. Pada pembuatan daftar situs di protocol ini, situs akan langsung dikenali oleh sistem saat user melakukan browsing.



Gambar 11. Setting Access Layer 7 Protocol

Penjelasan gambar :

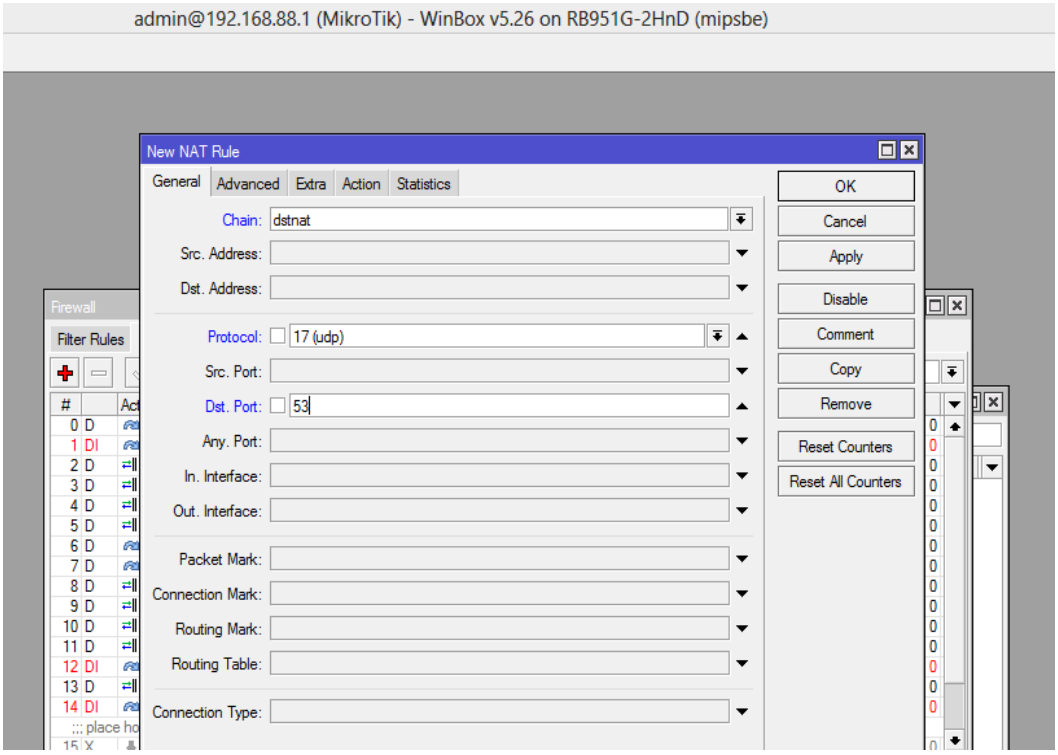
1. Membuat aturan access *firewall* dengan aturan blacklist daftar situs yang mengandung konten negatif.



Gambar 12. Setting Action *Firewall*

Penjelasan gambar :

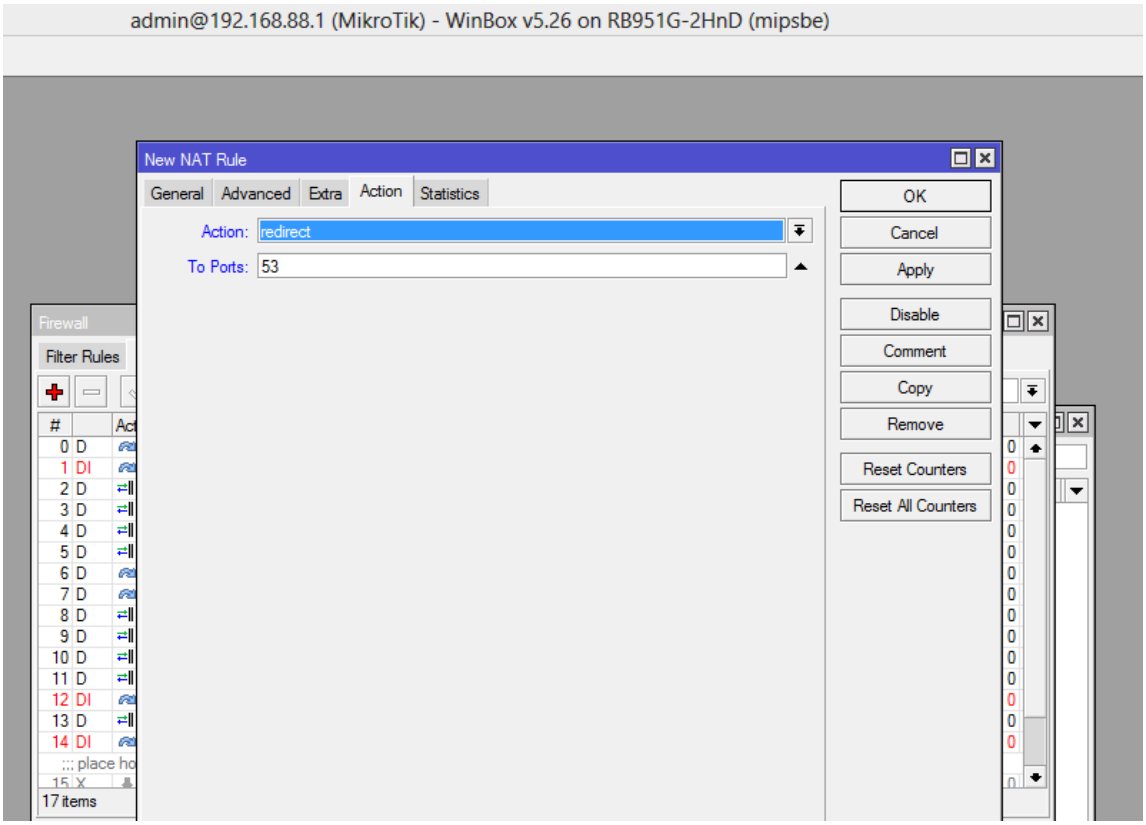
1. Action *firewall* ini berfungsi sebagai memutuskan koneksi saat mendeteksi protocol yang telah diatur dengan rule konten negatif.



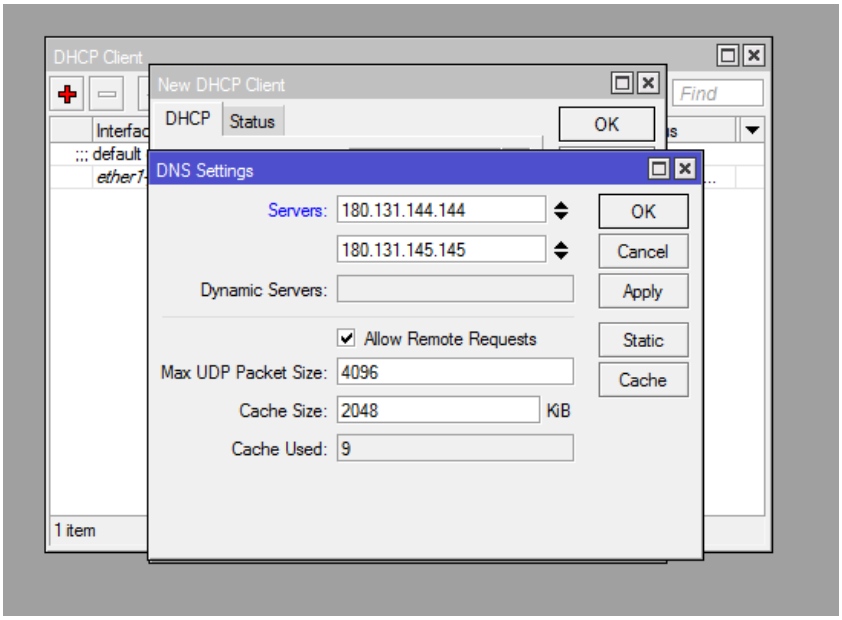
Gambar 13. Setting Port Direct Filter

Penjelasan gambar 13 dan 14 :

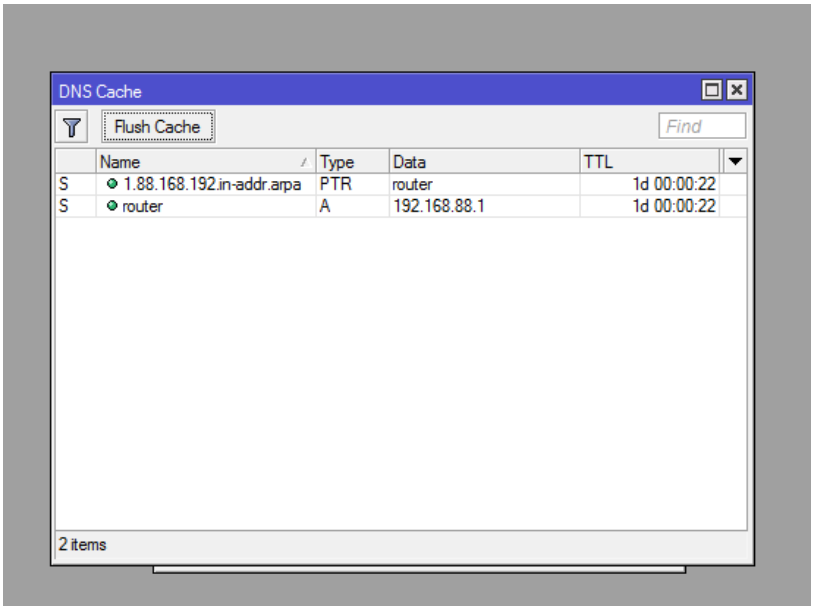
1. Konfigurasi pada port direct filter ini berfungsi untuk mendirect halaman web ke halaman blokir apabila terdeteksi konten negatif.



Gambar 14.Setting Access Port Direct



Gambar 15. Setting General DHCP DNS



Gambar 16. Setting Anti DNS Change

Penjelasan gambar 15 &16 :

Penulis menggunakan konfigurasi general DNS untuk memaksakan pemasangan DNS pada komputer client, hal ini ditujukan untuk menghindari penggantian DNS secara manual oleh pengguna, serta penulis menggunakan Flush Cache untuk mengunci DNS pada sisi komputer client.

PENUTUP

a. Kesimpulan

1. Internet Sehat merupakan perlindungan dari dampak negatif yang banyak tersebar di internet khususnya di situs-situs tertentu.
2. Dengan metode *Web Filtering* ini dapat mewujudkan internet sehat di server local/kecil, khususnya pada jaringan wireless RT 4 Cipeuteuy Baru. Dengan adanya *Web Filtering* ini juga dapat mengurangi bandwidth. Pengaruh pengurangan bandwidth tersebut hasil daftar blokir yang dikonfigurasi pada sistem *Web Filtering*.

b. Saran

1. Internet Sehat tidak cukup hanya dikonfigurasi pada server atau ISP, CyberEthic pun harus ditanamkan pada masyarakat supaya penggunaan internet dapat dipergunakan dengan bijak.
2. Metode Web Filtering ini dapat dikembangkan untuk mencegah dan menutup celah yang mungkin masih dapat ditembus oleh pengguna internet.

DAFTAR PUSTAKA

[1] Melwin Syafrizal, 2005, “Pengantar Jaringan Komputer”, Andi, Yogyakarta
[2] Cisco System Inc, 2012, “Introducing to Networking”& “Internetworking Technologies Handbook”, CCNA
[3] http://mikrotik.co.id/artikel-detail.php?kategori=2
[4] Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman, 2000, “Building Internet Firewall”, ISBN: 1-56592-871-7