Filtering *Domain Name Server* (DNS) untuk Membangun Internet Sehat Menggunakan Routerboard Mikrotik *(Development of Safety Internet with Filtering Domain Names Server (DNS) on Mikrotik Routerbroad)*

Firmansyah[1], Rachmat Adi Purnama[2]

[1]*Sistem Informasi, Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri Jakarta (STMIK Nusa Mandiri Jakarta)*
Jl. Damai No. 8, Warung Jati Barat (Margasatwa), Pasar Minggu, Jakarta Selatan

[2]*Sistem Informasi, Universitas Bina Sarana Informatika*
JL. Kamal Raya No. 18, Cengkareng Barat, Cengkareng, Jakarta Barat

[1]firmansyah.fmy@nusamandiri.ac.id
[2]rachmat.rap@bsi.ac.id

Abstrak - Maraknya penggunaan akses internet belakangan ini khususya pada remaja, membuat kekhawatiran tersendiri bagi orang tua. Dengan menggunakan jasa internet, pengguna layanan internet dengan sangat mudahnya melakukan pencarian dan mengakses kedalam website berkonten negatif dan pornografi. Dari data yang didapatkan akses terhadap website dengan konten negatif masih sangat tinggi dengan peringkat 17 dari Top Website Rangking. Hal ini merupakan sebuah alasan mengapa penulis melakukan penelitian menggunakan DNS filtering dengan tujuan untuk membatasi akses terhadap situs berkonten negatif dan barbau pornografi. Sesuai dengan peraturan pemerintah yang menginginkan Indonesia menjadi pengguna dan penyedia Internet Sehat bagi semua kalangan. Untuk mewujudkan penerapan Internet Sehat, penulis mencoba melakukan penelitian menggunakan RouterBoard Mikrotik untuk melakukan implementasi DNS Filtering untuk membangun Internet sehat menggunakan router mikrotik. Jika nantinya terdapat pengguna layanan internet yang mencoba melakukan akses kedalam jaringan internet dengan cara melakukan perubahan DNS secara manual dan menggunakan Open DNS maka akses internetnya akan terputus ataupun terblokir. Semua pengguna layanan internet pada jaringan ditekankan untuk menggunakan layanan DNS yang telah ditentukan.

Kata Kunci: Pornografi, Internet Sehat, DNS Filtering

Abstract - Increasing use of the internet access has recently khususya in teenagers, makes its own worries for parents. By using the internet services, internet service users with very easy it is to do a search and access into the website of negative and sites related to pornography. From the data obtained access to websites with negative content is still very high with 17 ratings from Top Website Rankings. This is a reason why writers doing research using DNS filtering to limit access to sites related to negative sites and pornography barbau. In accordance with government regulation who want Indonesia being the users and providers of the Internet healthy for all circles. To realize a healthy Internet application, the author tried to do research using the Mikrotik RouterBoard DNS implementations to perform Filtering for building healthy Internet use mikrotik router. If later there is internet service users who tried to access into the internet network by means of DNS changes manually and use Open DNS then Internet access will be terminated or blocked. All users of the internet services on the network to use DNS service emphasised its predetermined.

Keywords: Pornography, Internet Filtering, DNS Healthy

I. PENDAHULUAN

Pada era modern ini, nilai informasi sangatlah penting dan dibutuhkan oleh berbagai kalangan, baik itu dari kalangan pemakai maupun pembuat informasi maka kehadiran teknologi informasi sangatlah mutlak diperlukan.

[1] Pemanfaatan internet telah mengubah pola hidup dan budaya manusia dalam belajar, bekerja, berkomunikasi, berbelanja dan aspek lainnya. Hadirnya jaringan komputer merupakan solusi yang terbaik untuk masalah kecepatan dan keakuratan informasi. Banyak sekali keuntungan apabila menggunakan jaringan komputer. Pengguna atau *user* diberikan kebebasan dalam berselancar diinternet tanpa batasan, serta pengguna atau *user* dapat membuka situs yang berbau dewasa dengan merubah DNS *(Domain Name Server)* secara manual. [9] DNS atau yang sering disingkat dengan DNS adalah sebuah perangkat yang bertugas menerjemahkan sebuah alamat website di internet menjadi sebuah alamat IP, hal ini perlu dilakukan karena komputer sebernarnya tidak dapat mengenali karakter-karakter yang terangkai membentuk sebuah nama alamat website selayaknya manusia, komputer hanya mengenal nomor. [2] Remaja merupakan kalangan yang paling rentan dalam penyalahgunaan kemajuan teknologi internet, maka perlu upaya serius untuk memberikan pengetahuan dan keterampilan yang benar dalam memanfaatkan kemajuan tersebut.

Kejahatan komputer atau lebih lazim disebut dengan *cyber crime* pada dunia maya seringkali dilakukan oleh sekelompok orang yang ingin menembus suatu keamanan sistem. [3] Terlihat pada Tabel I, berdasarkan data mengenai Top Website *Rangking* pengguna akses internet di Indonesia menunjukan data pengaksesan terhadap situs *Adult*/konten dewasa sangat tinggi, yaitu menduduki posisi peringkat ke-26. [4]Sedangkan Top Website *Rangking* di Dunia, akses terhadap website berkonten dewasa mendukuki peringkat ke-8 sedikit dibawah dari website jejaring sosial.

TABEL I
TOP WEBSITE RANGKING INDONESIA

No	Domain (10.000)	Traffic Share	Rank World
1	Google.com	16.68%	#1
2	Facebook.com	6.28%	#3
3	Youtube.com	5.15%	#2
4	Tribunnews.com	2.49%	#106
5	Google.co.id	1.89%	#135
6	Detik.com	1.42%	#217
7	Instagram.com	0.96%	#5
8	Whatsapp.com	0.96%	#30
9	Bukalapak.com	0.95%	#315
10	Wikipedia.org	0.92%	#10
11	Brainly.co.id	0.86%	#346
12	Tokopedia.com	0.85%	#339
13	Yahoo.com	0.84%	#7
14	Twitter.com	0.82%	#6
...			
26	Xnxx.com	0.37%	#12
27	Olx.co.id	0.35%	#482
28	Appsflyer.com	0.35%	#883

Dengan menerapkan keamanan DNS *Filtering* diharapkan mampu membatasi akses terhadap pengguna untuk melakukan akses kedalam website berkonten negatif, hal ini bertujuan untuk membangun sistem internet sehat bagi pengguna layanan internet saat ini. [7] Meskipun Kementrian Kominfo telah melancarkan program operasi blokir terhadap konten porno dan sosialisasi internet sehat yang bekerjasama dengan operator. Namun nyatanya masih banyak anak-anak yang mampu mengakses konten porno dengan menelusuri kata-kata yang sangat sederhana. [6] Dalam mengupayai peperangan terhadap situs bermuatan negatif akhirnya Menkominfo mengeluarkan program DNS Nasional yang mengaharuskan semua penyedia layanan internet melakukan sinkronisasi DNS mereka dengan DNS *Trust*+Positif.

[5] Internet sehat adalah penggunaan internet sesuai dengan batas-batasnya, beretika dan tidak membuat seseorang menjadi antisosial. Dalam penelitian ini penulis akan menggunakan DNS Nawala dan *Filtering Open* DNS menggunakan *firewall* mikrotik. *Firewall* adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Saat ini lebih banyak situs web berbahaya dibandungkan dengan web ataupun situs yang sah. Hal ini akan menjadi sebuah tanda tanya yang sangat besar tentang bagaimana Anda bisa tetap aman saat menggunakan internet?.

Salah satu solusi yang digunakan bagi penyedia jasa internet (ISP) adalah melakukan penyaringan website berkonten negatif. Penelitian ini bertujuan untuk melihat kinerja dari sebuah *filtering* DNS jika terdapat pengguna yang mencoba melakukan perubahan DNS secara manual dari DNS yang telah disediakan didalam jaringan. Serta melihat dampak yang terjadi jika pengguna tersebut mencoba merubah DNS secara manual. [10] Internet sehat adalah penggunaan internet sesuai dengan batas-batasanya, beretika dan tidak membuat seseorang menjadi anti sosial. [8] Pada penelitian sebelumnya telah dilakukan pemblokiran situs porno dengan menggunakan DNS nawala dan squid. DNS Nawala digunakan sebagai *name server* dari proxy. Sehingga ketika komputer client tersebut mengakses situs porno akan diblokir oleh DNS nawala. Squid digunakan untuk memblokir situs yang mengandung kata-kata yang ditentukan oleh admin. Ketika dalam sebuah website mengandung kata-kata yang telah ditentukan tersebut, maka situs tersebut akan diblokir.

II. METODE PENELITIAN

A. Model Analisis

Dalam melakukan penelitian implementasi DNS *filtering* untuk membangun internet sehat penulis menggunakan bantuan perangkat RouterBoard Mikrotik 951-2HnD yang digunakan untuk melakukan *filtering* terhadap Open DNS dengan menggunakan metode *firewall filter action drop*. Serta dengan bantuan satu (1) buah perangkat switch dan empat (4) buah *Personal Computer* yang digunakan untuk melakukan pengujian jaringan.

B. Perancangan Sistem

1) Winbox. Dengan menggunakan *software* winbox v3.18 penulis melakukan remote terhadap perangkat mikrotik dikarenakan lebih praktis dan lebih mudah dalam melakukan konfigurasi pada perangkat RouterBoard Mikrotik.

2) Sistem Operasi. Sistem operasi yang digunakan untuk melakukan penelitian ini menggunakan sistem operasi Windows XP, sistem operasi inidipilih dikarenakan lebih ringan dibandingkan sistem operasi lainnya.

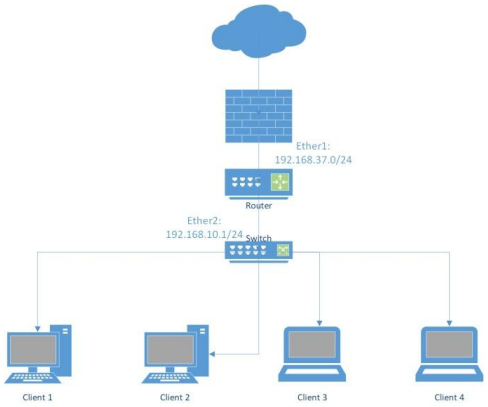
III. HASIL DAN PEMBAHASAN

A. Konfigurasi IP Address, DNS dan DHCP

Untuk melakukan konfigurasi terhadap routerboard mikrotik agar dapat melakukan akses kedalam jaringan internet. Langkah pertama yang penulis lakukan adalah melakukan konfigurasi IP address terhadap interface ether1yang terhubung langsung dengan ISP. Interface ether1 ini nantinya akan menggunakan cara kerja dari NAT (Network Address Translation) yang digunakan untuk menghubungkan antara jaringan lokal dengan jaringan publik.

TABEL II
SPESIFIKASI IP ADDRESS

Device	Interface	IP Address
Routerboard	Ether1	192.168.137.254/24
	Ether2	192.168.10.1/24
Client 1 Client 2 Client 3 Client 4	LAN Card	DHCP Client



Gambar 1. Topologi Jaringan

Jika melihat terhadap Tabel II dan Gambar 1, ISP atau akses internet terhubung langsung dengan interface ether1. ISP mengalokasikan IP Address 192.168.137.1/24 terhadap jaringan yang tersedia pada Gambar 3 dan secar langsung terhubung dengan interfac ether1. IP Address yang digunakan oleh Routerboard interface ether1 adalah 192.168.137.254 dengan menggunakan Subnetmask 255.255.255.0 dkarenakan antara ISP dengan interface ether1 haruslah menggunakan network yang sama. Konfigurasi yang pertama dilakukan adalah memberikan IP Address terhadap Routerboard interface ether1 dengan cara:

[admin@mikrotik]> ip address add address=192.168.137.254/24 interface=ether1

Konfigurasi ini digunakan untuk memberikan IP Address terhadap interface ether1 yang terhubung langsung dengan akses internet. Setelah memberikan IP Address terhadap ether1, langkah selanjutnya adalah memberikan alamat gateway, DNS serta firewall NAT terhadap interface ether1 dengan menggunakan perintah:

[admin@mikrotik]> ip route add gateway=192.168.137.1

Perintah "ip router" digunakan untuk mengaktifkan tabel routing gateway dengan alokasi IP Address 192.168.137.1.

[*admin*@mikrotik]> ip dns set server=180.131.144.144,180.131.145.145 allow-remote-request=yes

DNS server yang digunakan merupakan DNS Nawala yang sudah menerapkan filtering terhadap konten-konten negatif diinternet. Hal ini bertujuan untuk membatasi akses internet ke dalam website-website berkonten negatif dan berbau pornografi.

[admin@mikrotik]> ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade

Firewall NAT digunakan untuk melakukan *Network Address Translation* dengan tujuan agar jaringan lokal dapat terkoneksi kedalam jaringan publik. Ataupun agar *client* dapat berkomunikasi kedalam jaringan internet. Langkah selanjutnya, penulis akan memberikan IP Address terhadap *interface* ether2 yang nantinya akan digunakan oleh *client* untuk berkomunikasi kedalam jaringan.

[admin@mikrotik]> ip address add address=192.168.10.1/24 interface=ether2

Setelah memberikan IP *Address* terhadap interface ether2. Penulis akan mengaktifkan fitur DHCP *Server* terhadap *interface* ether2, dengan tujuan untuk memudahkan dalam melakukan instalasi pada jaringan dan memberikan IP *Address* secara otomatis terhadap *user* yang akan terkoneksi.

```
[admin@MikroTik] > ip dhcp-server setup
Select interface to run DHCP server on

dhcp server interface: ether2
Select network for DHCP addresses
```

Gambar 2. DHCP Server

Terlihat pada gambar 2, adalah konfigurasi yang dilakukan untuk mengaktifkan interface DHCP Server pada interface ether2.

```
dhcp address space: 192.168.10.0/24
Select gateway for given network

gateway for dhcp network: 192.168.10.1
Select pool of ip addresses given out by DHCP server
```

Gambar 3. Network dan Gateway

Network yang digunakan adalah 192.168.10.0/24 dikarenakan IP address yang digunakan pada ether2 192.168.10.1/24. Dan IP Address yang digunakan terhadap interface ether2 nantinya akan digunakan sebagai alamat gateway dari client terlihat pada Gambar 3.

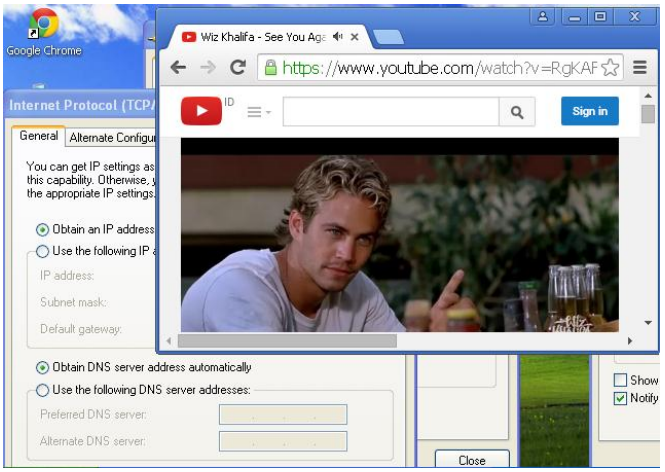
```
addresses to give out: 192.168.10.2-192.168.10.254
Select DNS servers

dns servers: 180.131.144.144,180.131.145.145
Select lease time

lease time: 3d_
```

Gambar 4. Range IP, DNS Server dan Lease Time

Dijelaskan pada gambar 4, adalah proses pembuatan dari alokasi IP Address yang nantinya akan digunakan sebagai DHCP Server, serta mendaftarkan DNS Server Nawala. Setiap client yang terkoneksi kedalam jaringan dapat menggunakan akses jaringan selama 3 hari sesuai dengan Lease time yang telah diberikan oleh administrator jaringan.

B. Uji Konektifitas 1

Uji konektifitas yang pertama kali adalah melakukan pengecekan terhadap client yang terhubung kedalam jaringan komputer. Hal ini bertujuan untuk mengetahui client tersebut mendapatkan alokasi IP Address secara otomatis atau tidak.



Gambar 5. Uji Konektifitas

TABEL III
SPESIFIKASI IP ADRESS

Device	IP Address	Gateway	DNS Server
Client 1	192.168.10.254	192.168.10.1	180.131.144.144 180.131.145.145
Client 2	192.168.10.253		
Client 3	192.168.10.252		
Client 4	192.168.10.251		

Jika dilihat pada gambar 5 dan tabel III, client yang terhubung kedalam jaringan komputer sudah mendapatkan alokasi IP Address, Subnetmask, Gateway dan DNS secara DHCP dan dapat melakukan akses terhadap jaringan internet.

C. Konfigurasi DNS Filtering

DNS Filtering digunakan untuk melakukan pemblokiran terhadap client yang mencoba melakukan perubahan DNS Server secara manual. Hal ini sering dilakukan oleh beberapa pengguna jaringan internet yang mencoba mengakses kedalam website dengan konten negatif. Untuk melakukan pemblokiran terhadap pengguna jasa internet yang mencoba melakukan perubahan DNS secara manual, penulis menggunakan konfigurasi sebagai berikut:

[admin@mikrotik]>ip firewall filter add chain=forward dst-address=!180.131.144.144 protocol=tcp dst-port=53 action=drop

[admin@mikrotik]>ip firewall filter add chain=forward dst-address=!180.131.144.144 protocol=udp dst-port=53 action=drop

Konfigurasi terasebut digunakan untuk melakukan drop terhadap protokol TCP dan UDP jika client mencoba menggunakan DNS server selain 180.131.144.144.

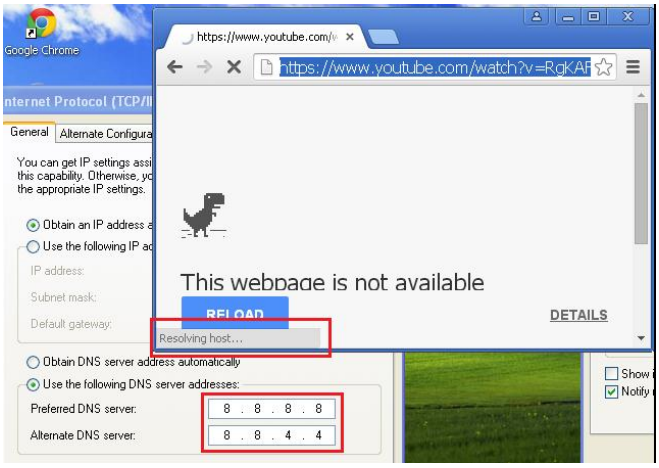
[admin@mikrotik]>ip firewall filter add chain=forward dst-address=!180.131.145.145 protocol=tcp dst-port=53 action=drop

[admin@mikrotik]>ip firewall filter add chain=forward dst-address=!180.131.145.145 protocol=udp dst-port=53 action=drop

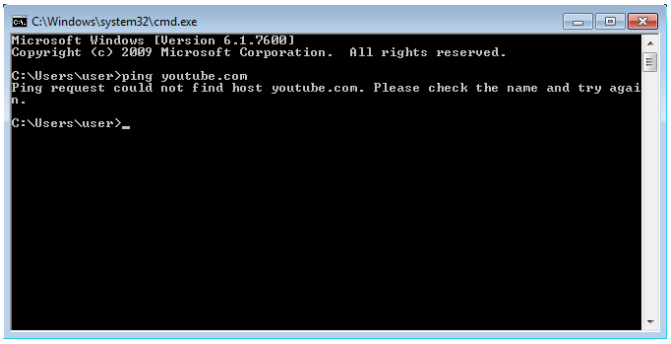
Adapun konfigurasi diatas digunakan untuk melakukan drop terhadap protokol TCP dan UDP jika client mencoba menggunakan DNS server selain 180.131.145.145. Jadi semua client akan dipaksakan untuk menggunakan DNS yang telah disediakan oleh sever. Jika terdapat client yang mencoba melakukan perubahan DNS Server secara manual maka client tersebut tidak dapat terhubung kedalam jaringan internet.

D. Uji Konektifitas 2

Setelah selesai melakukan konfigurasi DNS filtering, penulis mencoba melakukan uji konektifitas terhadap client yang berusaha untuk melakukan akses kedalam jaringan internet dengan melakukan perubahan terhadap DNS Server yang telah diberikan. Pada gambar 6, dapat dilihat sebuah pengguna yang melakukan perubahan DNS secara manual tidak dapat melakukan akses kedalam jaringan internet. Hal ini disebabkan, administrator jaringan telah menentukan DNS mana saja yang berhak melakukan akses kedalam jaringan internet.



Gambar 6. User melakukan perubahan DNS



Gambar 7. Uji Konektifitas

Dari gambar 7, dapat disimpulkan semua client yang terkoneksi kedalam jaringan internet hanya dapat melakukan akses kedalam jaringan internet jika menggunakan DNS yang telah ditentukan. Hal ini bertujuan untuk membatasi dan meminimalisir penggunaan Open DNS untuk melakukan akses terhadap situs negatif yang tersedia pada jaringan internet

IV. KESIMPULAN

A. Masih mudahnya pengguna jasa internet untuk melakukan akses kedalam website-website berkonten negatif.

B. Membatasi akses internet menggunakan DNS Sehat untuk meminimalisir pencarian konten negatif didalam jaringan internet.

C. Menutup akses terhadap internet jika menggunakan Open DNS

DAFTAR PUSTAKA

[1] Kominfo, "Internet Sehat dan Aman (INSAN)l," *kominfo.com*, 2019. [Online]. Available: https://kominfo.go.id/index.php/content/detail/3303/Internet-Sehat-dan-Aman--INSAN-/0/internet_sehat. [Accessed: 10-Jan-2019].

[2] W. Parimita, H. Eryanto, and R. Faslah, "Pengembangan Perilaku Berinternet Sehat Melalui Pembuatan Blog Ilmiah Siswa," *J. Pemberdaya Masy. Madani*, vol. 1, no. 1, pp. 33–45, 2017.

[3] SimilarWeb, "Top Websites Ranking," *similarweb*, 2019. [Online]. Available: https://pro.similarweb.com/#/industry/topsites/All/360/1m?webSource=Total. [Accessed: 18-Feb-2019].

[4] SimilarWeb, "Top Websites Ranking In Industry," *similarweb*, 2019. [Online]. Available: https://pro.similarweb.com/#/industry/topsites/All/360/1m?webSource=Total. [Accessed: 18-Feb-2019].

[5] Amarudin and A. Yuliansyah, "Analisis Penerapan Mikrotik Router Sebagai User Manager Untuk Menciptakan Internet Sehat Menggunakan Simulasi Virtual Machine," *J. TAM (Technology Accept. Model. Vol.*, vol. 9, no. 1, pp. 62–66, 2018.

[6] Kominfo, "Kominfo Finalisasi DNS Nasional Kategori," *kominfo*, 2019. [Online]. Available: https://www.kominfo.go.id/content/detail/4991/kominfo-finalisasi-dns-nasional/0/sorotan_media. [Accessed: 10-Jan-2019].

[7] R. Panuju, "Perilaku Mengakses Internet Di Warung Kopi Behavior Access Internet In Coffee Shop," *J. Sosioteknologi*, vol. 16, no. 3, pp. 259–273, 2016.

[8] I. Sofana, *Cisco CCNA dan Jaringan Komputer Edisi Revisi*, 2nd ed. Bandung: Informatika, 2014.

[9] Athailah, *Panduan Singkat Menguasai Router Mikrotik Untuk Pemula*. Jakarta: Media Kita, 2013.

[10] S. Wijayanta and Muslihudin, "Pembangunan Web Proxy Dengan Mikrotik Untuk Mendukung Internet Sehat Di Smk Muhammadiyah 1 Patuk Gunungkidul," *J. Sarj. Tek. Inform.*, vol. 1, no. 1, pp. 259–267, 2013.