JURNAL TEKNIK INFORMATIKA

Halaman Jurnal: <http://jurnal.stmik-dci.ac.id/index.php/jutekin/>

Halaman LPPM STMIK DCI : <http://lppm.stmik-dci.ac.id/>

IMPLEMENTASI FIREWALL DAN WEB FILTERING PADA MIKROTIK ROUTEROS UNTUK MENDUKUNG INTERNET SEHAT DAN AMAN (INSAN)

Deni Ahmad Jakaria¹, Aneu Yulianeu²

Prodi Teknik Informatika, STMIK DCI, Email : deni@stmik-dci.ac.id¹

Prodi Manajemen Informatika STMIK DCI, Email : aneu@stmik-dci.ac.id²

ABSTRAK

Internet telah menjadi bagian dari kebutuhan manusia yang tidak dapat dipisahkan dari kehidupan sehari-hari. Saat ini setiap orang dapat dengan mudah mengakses internet untuk mendapatkan informasi atau mencari hiburan. Sifat internet yang bebas menyebabkan banyaknya konten tidak pantas di Internet. Salah satu cara membatasi konten tersebut dengan menerapkan firewall di sisi router. Dengan menggunakan Layer 7 firewall diharapkan dapat menyaring konten yang tidak pantas. Layer 7 firewall melakukan penapisan konten web berdasarkan kata kunci. Implementasi firewall Layer 7 dapat diterapkan diantaranya menggunakan perangkat routerboard MikroTik.

Kata kunci : Mikrotik, Firewall, Web Filtering, Internet Sehat, Insan

I. PENDAHULUAN

Jumlah penduduk pengguna internet di Indonesia pada tahun 2018 mencapai 171,17 juta jiwa dari total populasi sebanyak 264,16 juta, penetrasi pengguna internet di Indonesia berada pada kisaran 64,8% meningkat dari tahun sebelumnya yaitu sebesar 54,68%. Informasi di internet tidak semua bersifat positif, terdapat konten tidak pantas yang dapat mempengaruhi di kehidupan nyata.

Untuk mengurangi dampak konten tidak pantas internet maka perlu dilakukan upaya untuk mengurangi atau

membatasi akses konten tidak pantas di internet. Salah satu upaya tersebut yaitu melalui program internet sehat dan aman (INSAN) yang dicanangkan oleh Kemkominfo dengan melibatkan seluruh komponen masyarakat.

Program INSAN diselenggarakan dalam bentuk roadshow, forum dengan menggunakan media antara lain tatap muka, internet, televisi, radio, media cetak, media luar ruang dan animasi. Kegiatan tersebut mensosialisasikan cyber ethics (berinternet secara sehat), selain itu juga memberikan panduan praktis perlindungan dari konten tidak

pantas dengan memanfaatkan sejumlah aplikasi untuk menyaring konten tidak pantas.

Proses untuk menyaring konten tidak pantas dari sisi pengguna dibutuhkan kesadaran dari penggunanya sendiri, namun terkadang konten tidak pantas masih bisa muncul tanpa diinginkan oleh pengguna internet. Maka perlu dilakukan penyaringan konten dari sisi penyedia (ISP) maupun dari perangkat home router yang menghubungkan pengguna ke jaringan internet.

Salah satu upaya tersebut dapat diterapkan dengan memanfaatkan teknik web filtering dan penapisan dari jalur home router yang merupakan pintu masuk pertama bagi pengguna internet di kantor, sekolah/kampus, warung internet, kafe/restoran yang menyediakan WiFi dan koneksi WiFi di ruang publik. MikroTik Router OS merupakan salah satu router yang banyak digunakan untuk membagi akses internet dikarenakan harga yang terjangkau namun cukup handal jika dibandingkan dengan produk lainnya. Router tersebut cukup mudah dikonfigurasi dan memiliki fitur yang memadai untuk melakukan penapisan konten tidak pantas menggunakan firewall dan teknik web filtering.

Berdasarkan survey yang dilakukan oleh APJII (APJII, 2018) pada tahun 2018 terdapat 171,17 juta jiwa penduduk Indonesia yang mengakses Internet dari total populasi sebanyak 264,16 juta orang. Dengan presentase penetrasi pengguna internet mencapai 64,8% pada tahun 2018, maka jumlah tersebut mengalami peningkatan sebesar 10,12% dibandingkan pada tahun 2017 dengan

jumlah penetrasi pengguna internet yang mencapai 54,68%.

Internet memberikan keleluasaan bagi penggunanya untuk mengakses informasi tanpa batas, konten tersebut tidak semuanya bersifat positif. Pengaruh konten tidak pantas di internet berupa pornografi, perjudian, penipuan, pelecehan, pencemaran nama baik, cyberbullying, dan kejahatan dunia maya lain. Konten tidak pantas tersebut sebaiknya diblokir agar tidak merusak pengguna internet di kehidupan nyata.

Pemerintah Indonesia melalui Kementerian Komunikasi dan Informatika Indonesia (Kemkominfo) telah mencanangkan program internet sehat dan aman (INSAN) dengan tujuan untuk mensosialisasikan penggunaan Internet secara sehat dan aman, program ini dilakukan melalui pembelajaran etika berinternet dengan melibatkan seluruh komponen masyarakat.

Selain sosialisasi mengenai cyber ethics, beberapa penggiat telematika menerbitkan buku pedoman berinternet yang tidak hanya berisi pemahaman mengenai internet sehat tapi juga panduan praktis untuk menghindari anak terpapar konten tidak pantas dari internet.

Kominfo melalui Trust Positif (<https://trustpositif.kominfo.go.id>) menyediakan *list* yang berisi daftar web yang di-*blacklist* serta memberikan kesempatan kepada pengguna internet untuk melaporkan web yang mengandung konten tidak pantas. Upaya tersebut ditujukan untuk mengurangi dampak dari konten tidak pantas di Internet. Selain itu terdapat proyek DNS Nawala (<https://nawala.id>) yang dapat memblokir akses terhadap konten-konten yang dianggap tidak pantas yang

tidak sesuai dengan norma sosial, adat istiadat dan kesusilaan bangsa Indonesia.

Langkah untuk mengurangi akses konten tidak pantas dapat pula dilakukan dengan memanfaatkan fungsi firewall dan teknik web filtering yang terdapat pada MikroTik Router OS. Perangkat tersebut dipasang sebagai router yang menjadi penghubung antara pengguna internet menuju penyedia layanan internet atau Internet Service Provider (ISP). Mengingat masih banyak pengguna internet yang memanfaatkan akses internet dari kantor, sekolah/kampus, warung internet, kafe/restoran yang menyediakan WiFi dan koneksi WiFi di ruang publik maka perangkat tersebut cukup efektif untuk menyaring konten tidak pantas dari internet.

II. LANDASAN TEORI

2.1 MikroTik

MikroTik RouterOS merupakan sistem operasi dan perangkat lunak yang mengubah PC biasa atau perangkat keras MikroTik Routerboard menjadi router. MikroTik pertama kali dikembangkan di Latvia oleh John Trully dan Arnis Riekstins sekitar tahun 1996. Terdapat dua jenis MikroTik yaitu versi perangkat lunak yang dapat diinstal pada komputer personal dan versi perangkat keras yang built-in atau disebut RouterBoard (Azis & Herlambang, 2008).

Menurut Burgess (2011) MikroTik menjadi pilihan karena biaya lisensi relatif lebih murah dibandingkan perangkat lunak sejenis. Masih menurut Burgess (2011) kemampuan MikroTik dapat disejajarkan dengan router kelas enterprise dengan harga yang jauh lebih murah. Hal ini menjadi relevan bila dilihat sebgaiian besar pengguna MikroTik berasal dari negara berkembang (Azis &

Herlambang, 2008). Menurut Sofana (2017) MikroTik terdiri dari beberapa jenis diantaranya MikroTik RouterOS, MikroTik Lisensi dan MikroTik RouterBoard. Gambar 1 adalah contoh dari perangkat routerboard MikroTik.

Gambar 2.1
Routerboard MikroTik

2.2 Firewall

Firewall merupakan perangkat keamanan jaringan yang memantau lalu lintas (traffic) jaringan yang masuk (incoming) maupun keluar (outgoing) dan memutuskan apakah paket data diijinkan atau diblok berdasarkan aturan khusus yang telah ditentukan. Firewall merupakan benteng pertahanan pertama pada jaringan komputer, firewall membangun pembatas antara jaringan internal yang aman dan terkendali dengan jaringan luar seperti internet. Firewall dapat berbentuk hardware, software atau keduanya (www.cisco.com, 2019).

2.3 Web Filtering

Cara kerja web filter yaitu memblokir akses web yang dianggap mengandung konten tidak pantas. MikroTik menyediakan fitur tersebut dengan beberapa cara/teknik (Takeuchi, 2017). Fitur atau *policy* untuk memblock web yang dapat diterapkan pada MikroTik diantaranya yaitu static DNS, web proxy, route policy, content filter, layer 7 firewall dan destination IP address/port block (Takeuchi, 2017).

Teknik yang akan implementasikan pada penelitian ini yaitu menggunakan content filter dan layer 7 firewall.

Content filter bekerja dengan cara menyaring packet dengan menggunakan teks yang terdapat pada packet tersebut. Packet yang berisi teks tertentu akan di-drop dan tidak akan diteruskan ke pengguna internet. Kelemahan teknik ini yaitu tidak dapat menyaring packet yang dienkripsi. Fitur tersebut dapat diakses pada menu IP Firewall di MikroTik RouterOS.

Fitur layer 7 firewall pada MikroTik bekerja dengan cara mencari sejumlah pola yang terdapat pada aliran data ICMP/TCP/UDP. Jika pola tidak ditemukan pada data yang dikumpulkan, maka fitur pencocokan akan berhenti untuk mencari. Proses ini membutuhkan sumber daya prosesor yang besar karena router harus mencari pola yang terdapat pada packets. Pencarian pola dapat menggunakan regular expressions sehingga lebih fleksibel namun perlu diingat bahwa teks pada regex bersifat case sensitive. Meskipun demikian menurut Greeff (2018) layer 7 firewall memiliki banyak kelebihan diantaranya lebih mudah diimplementasikan, sangat efektif serta dapat menapis berdasarkan kata kunci.

III. ANALISIS DAN DESAIN

3.1 Topologi Jaringan

Gambar 2 memperlihatkan desain topologi jaringan. Seperti tampak pada gambar terdapat dua router mikrotik. Router pertama menghubungkan jaringan LAN ke WAN. Router kedua berfungsi sebagai firewall, pada router ini akan diimplementasikan Layer 7 Firewall untuk menyaring konten. Akses

internet akan dibagikan kepada user melalui akses point.

Salah satu kelemahan dari Fitur Layer 7 Firewall yaitu *cpu load* yang tinggi (Greeff, 2019). Sehingga menggunakan dua router yang berbeda diharapkan dapat mengurangi *cpu load* pada router.

Pada router kedua aturan-aturan atau policy dari firewall layer 7 diimplementasikan, router kedua juga berfungsi sebagai DHCP server yang akan memberikan alamat IP dinamis ke pengguna Internet yang terhubung

Gambar 3.1

Desain Topologi Jaringan

melalui akses point.

IV. Pengalaman IP

Daftar pengalaman IP dapat dilihat di tabel 1. Setiap interface pada MikroTik akan diberikan alamat IP sesuai dengan tabel 1. Alokasi alamat IP untuk server DHCP dapat dilihat pada tabel 2. Seperti tampak di tabel 2, terdapat tiga dhcp server. Ujicoba implementasi Layer & dilakukan pada jaringan FreeWiFi.

Jumlah maksimum client yang dapat terhubung pada saat yang bersamaan sebanyak 60 client.

Tabel 4.1
Alamat IP

Perangkat	Interface	Alamat IP	Prefix	Subnet Mask
Mikrotik	ether1-WAN	192.168.5.253	/30	255.255.255.0
	ether2-pustaka	192.168.7.62	/26	255.255.255.224
	ether3-FreeWiFi	192.168.7.126	/26	255.255.255.224
	ether4-reserved1	192.168.7.190	/26	255.255.255.224
	ether5-reserved2	192.168.7.254	/26	255.255.255.224

Tabel 4.2
Alokasi Alamat IP untuk DHCP Server

DHCP	Interface	Range IP	Gateway	DNS Server
dhcp1-pustaka	ether2-pustaka	192.168.7.1 - 192.168.7.60	192.168.7.62	1.1.1.1
dhcp2-freewifi	ether3-FreeWiFi	192.168.7.65 - 192.168.7.124	192.168.7.126	1.1.1.1
dhcp3	ether4-reserved1	192.168.7.129 - 172.168.7.188	192.168.7.190	1.1.1.1

4.1 Cara Kerja Layer 7 Firewall

Menurut (Takeuchi, 2017) Layer 7 Firewall bekerja dengan cara mencari pola yang terdapat di packet streams ICMP/TCP/UDP pada 10 packet pertama dan 2KB packets. Jika pola tidak ditemukan pada kumpulan data, maka proses pencocokan akan dihentikan. Proses ini akan membebani cpu (*high cpu load*) disebabkan router harus mencari pola pada setiap packets yang masuk ke router.

jendela pada winbox untuk menambahkan New Firewall L7 Protocol.

Gambar 5.1
Firewall L7 Protocol

V. IMPLEMENTASI DAN PENGUJIAN

5.1 Konfigurasi Layer 7 Firewall

Proses setting konfigurasi Layer 7 Firewall dilakukan dengan menggunakan Winbox. Fitur Layer 7 Firewall dapat diakses dari menu IP -> Firewall. Sebelum membuat policy, tambahkan kata kunci yang akan digunakan sebagai rules untuk memblokir web. Fitur ini terdapat di tab Layer 7 Protocols di menu Firewall. Klik icon '+' (add), kemudian beri nama, dilanjutkan dengan memasukan kata kunci pada kotak Regexp (regular expression). Gambar 5.1, menampilkan

Tambahkan Rule Firewall Baru, klik pada tab Filter Rules, klik icon '+'. Pada kotak pilihan Chain pilih Forward. Protocol yang dipilih tcp (6), dengan port 80 (port http) dan port 443 (port https) diisikan pada kotak Dst. Port. In Interface merupakan interface dimana packet akan diteruskan (ditujukan ke jaringan LAN) sedangkan Out Interface ditujukan ke jaringan luar (WAN atau Internet). Gambar 5.2 memperlihatkan setting untuk policy baru firewall (New Firewall Rule). Pada kolom src. Address, In.

Interface dan Out. Interface dapat disesuaikan dengan konfigurasi jaringan yang digunakan.

Gambar 5.2
New Firewall Rule

Langkah selanjutnya pada tab Advanced kolom Layer7 Protocol, pilih kata kunci yang akan dicari pada packet streams. Item ini akan muncul otomatis sesuai dengan jumlah kata kunci yang telah diinput pada menu sebelumnya. Gambar 5.3 memperlihatkan setting pilihan Layer7 Protocol.

Gambar 5.3
Layer7 Protocol

Selanjutnya tentukan aksi yang akan dilakukan pada packet jika ditemukan kecocokan sesuai dengan rules. Packet

akan di-drop, tidak akan diteruskan ke client (lihat gambar 5.4).

Gambar 5.4
Action Drop

Cara lain untuk membuat rules baru firewall L7 yaitu menggunakan CLI (command line interface). Pada winbox dapat diakses dari menu New Terminal. Berikut ini contoh menambahkan rules baru menggunakan perintah command line.

(http://onnocenter.or.id/wiki/index.php/Mikrotik:_Layer_7_Protocol_L7P)

```
/ip firewall layer7-
protocol add
regexp=^.*togel.*
name=togel
/ip firewall layer7-
protocol add
regexp=^.*porn.* name=porn
/ip firewall layer7-
protocol print

/ip firewall filter add
chain=forward layer7-
protocol=porn action=drop
/ip firewall filter add
chain=forward layer7-
protocol=togel action=drop
```

Tahap selanjutnya perlu dilakukan ujicoba untuk memastikan bahwa Layer 7 Firewall dapat bekerja efektif untuk

memblokir konten sesuai dengan pola yang telah diinputkan.

Hasil ujicoba dapat dilihat pada tangkapan layar di gambar 5.5. Browser yang digunakan yaitu Google Chrome, mengakses laman web bioskop.red. Browser akan menampilkan pesan bahwa halaman yang dituju tidak dapat ditampilkan.

kolom Bytes dan Packets menampilkan informasi banyaknya packets yang berhasil di-drop oleh Layer7 Firewall.

Dari hasil ujicoba membuktikan bahwa Layer7 Firewall efektif untuk memblokir konten Internet yang kurang pantas. Namun demikian perlu diperhatikan jumlah rules pada Firewall, disebabkan tingginya beban cpu untuk memproses Layer7 Firewall. Hal ini akan

Gambar 5.5
Browser tidak dapat mengakses laman web yang diblokir

Firewall									
Filter Rules									
NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols									
<input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="✓"/> <input type="button" value="✗"/> <input type="button" value="📁"/> <input type="button" value="🔍"/> <input type="button" value="🔄"/> <input type="button" value="🔄"/> <input type="button" value="🔄"/> <input type="button" value="🔄"/>									
<input type="button" value="Reset Counters"/> <input type="button" value="Reset All Counters"/> <input type="text" value="Find"/> <input type="text" value="all"/> <input type="button" value="⌵"/>									
#	Action	Chain	Src. Address	Proto...	Src. Port	Dst. Port	In. Interface	Bytes	Packets
0	✗ drop	forward	192.168.7.64/26	6 (tcp)		80,443	ether3-FreeWIFI	339.1 KiB	1 420
1	✗ drop	forward	192.168.7.64/26	6 (tcp)		80,443	ether3-FreeWIFI	122.1 KiB	502
2	✗ drop	forward	192.168.7.64/26	6 (tcp)		80,443	ether3-FreeWIFI	12.7 KiB	39
3 items									

Gambar 5.6
Firewall Filter Rules

Gambar 5.5 memperlihatkan hasil tangkapan layar dari aplikasi Winbox. Pada jendela firewall dapat dilihat pada

memberatkan kerja router terutama jika menggunakan routerboard MikroTik yang memiliki sumber daya terbatas.

VI. SIMPULAN DAN SARAN

Berikut kesimpulan dari hasil penelitian yang telah dilakukan:

1. Layer7 Firewall terbukti efektif untuk memblokir web berdasarkan kata kunci dengan menggunakan regexp.
2. Layer7 Firewall menyebabkan load cpu yang tinggi pada router.

Adapun saran yang dapat disampaikan adalah:

1. Beban cpu yang tinggi pada router dimungkinkan dapat diatasi dengan menggunakan spesifikasi routerboard yang lebih baik.
2. Alternatif penggunaan teknik blocking selain menggunakan Layer7 Firewall perlu dipertimbangkan jika ternyata sangat membebani kinerja router.

DAFTAR PUSTAKA

APJII (2018). Survey APJII. Tersedia di <https://apjii.or.id/survei2018s/>. Diakses tanggal: 8 Agustus 2019

Herlambang, M.L. dan Azis, C.L. (2008). Panduan Lengkap Menguasai Router Masa Depan Menggunakan MikroTik RouterOS. Yogyakarta: Andi Publisher.

Burgess, D. (2011). Learn RouterOS (2nd edition). Link Technologies, Inc.

Purbo, O.W. (2006). Internet Wireless dan Hotspot. Jakarta: Elex Media Komputindo.

Greeff, Paul. (2019). Web Content Filtering and Log Data Analysis with MikroTik Routers. Tersedia di https://mum.mikrotik.com/presentations/TR18/presentation_6167_

1539848033.pdf. Diakses tanggal: 18 Agustus 2019.

Takeuchi, Michael. (2017). Website Blocking PolicyWith MikroTik RouterOS. Tersedia di https://mum.mikrotik.com/presentations/VN17/presentation_4493_1494480323.pdf. Diakses tanggal: 18 Agustus 2019.

<https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>. Diakses tanggal: 18 Agustus 2019.

Towidjojo, Rendra (2015). MikroTik Kung Fu Kitab 1. Jakarta: Jasakom.

Towidjojo, Rendra (2013). Konsep & Implementasi Routing Dengan Router MikroTik. Jakarta: Jasakom.

Wahana (2014). Mudah Belajar MikroTik Menggunakan Metode Virtualisasi. Yogyakarta: Andi Publisher.