Manajemen Keamanan Internet Menggunakan Metode *Firewall Filtering* Untuk Penyaringan Konten Pada Router Mikrotik RB1100

Sidik[1*], David Saputra Hasiholan Panjaitan[2], Priatno[3], Esron Rikardo Nainggolan[4]

[1*,2,4]Program Studi Informatika, Fakultas Teknologi Informasi, Universitas Nusa Mandiri
JL. Damai No.8, Warung Jati Ragunan Pasar Minggu, Jakarta, Indonesia

[3]Program Studi: Teknologi Informasi, Fakuktas: Teknik dan Informatika, Universitas Bina Sarana Informatika
Jl. Kramat Raya No.98, Senen, Jakarta Pusat, Indonesia

e-mail: [1]sidik.sdk@nusamandiri.ac.id, [2]dhasiholanpanjaitan@gmail.com, [3]priatno.prn@bsi.ac.id, [4]esron.ekg@nusamandiri.ac.id

(*) Corresponding Author

Artikel Info : Diterima : 03-04-2023 | Direvisi : 12-05-2023 | Disetujui : 22-06-2023

Abstrak - Adanya ancaman keamanan dan penyalahgunaan internet seringkali menjadi masalah bagi perusahaan. Penggunaan VPN untuk akses ke halaman web yang mengandung konten negatif dan pornografi yang biasanya mengandung *malware, virus, trojan* dan lainnya. Hal ini tentu saja akan memberikan efek kerugian bagi perusahaan yang jaringan internetnya terkena serangan *malware, virus* maupun *trojan* akibat kebiasaan karyawan akses ke laman web yang mengandung konten negatif dan pornografi. Untuk mencegah adanya ancaman-ancaman tersebut dibutuhkan suatu metode pengaturan akses dan penggunaan jaringan internet sesuai dengan tujuannya. *Content filtering* digunakan untuk memfilter situs-situs atau alamat web yang tidak diperbolehkan oleh pihak perusahaan karena dianggap tidak ada keterkaitan langsung dengan bidang pekerjaannya. Metode *firewall filtering content* pada perangkat Mikrotik Routerboard RB1100 menggunakan aplikasi Winbox merupakan salah satu metode untuk mencapai tujuan yaitu memblok konten-konten negatif dan pornografi yang dapat di akses oleh karyawan pada jam kerja. Penelitian ini di implementasikan pada PT. Bebentara Perkasa Indonesia. Hasil dari penelitian ini, setelah *firewall filtering content* di terapkan, karyawan tidak dapat mengakses laman web yang mengandung kontent negatif dan pornografi dan tentu saja tidak berkaitan dengan pekerjaan sehingga berimplikasi pada pekerjaan menjadi lebih produktif, efisien dan optimal.

Kata Kunci : manajemen keamanan, akses internet, *firewall filtering, content filtering*

Abstracts *- The existence of security threats and internet abuse is often a problem for companies. Use of a VPN for access to web pages that contain negative and pornographic content which usually contain malware, viruses, trojans and others. This of course will have a detrimental effect on companies whose internet networks are exposed to attacks by malware, viruses or trojans due to employees' habit of accessing web pages that contain negative and pornographic content. To prevent these threats, a method of regulating access and use of the internet network is needed according to its purpose. Content filtering is used to filter sites or web addresses that are not allowed by the company because they are considered to have no direct connection with their field of work. The firewall filtering content method in the Winbox application is one of the methods to achieve the goal of blocking negative and pornographic content that can be accessed by employees during working hours. This research was implemented at PT. Indonesian Mighty Beasts. The results of this study, after the content filtering firewall is implemented, employees cannot access web pages that contain negative and pornographic content and of course are not work related so that the implications for work are more productive, efficient and optimal.*

Keywords : security management, internet access,firewall filtering, content filtering

PENDAHULUAN

Internet merupakan merupakan sebuah sistem komunikasi yang mampu menghubungkan jaringan-jaringan komputer diseluruh dunia. Internet dapat juga disebut sebagai interkoneksi antar jaringan komputer namun secara

umum internet harus dipandang sebagai sumber daya informasi (Walidaini & Muhammad Arifin, 2018). Kebutuhan akan akses internet sekarang ini sangatlah penting, mulai dari mengirim atau menerima e-mail, mencari informasi berita, *social media*, *internet banking*, melakukan pembelian barang atau jasa, *chatting*, aplikasi berbasis online dan masih banyak lainnya (Cholik, 2021). Selain manfaat positif yang didapat dari penggunaan internet, ternyata banyak juga dampak negatif dari penggunaan internet (Walidaini & Muhammad Arifin, 2018). Contohnya adalah akses ke laman-laman web yang mengandung konten sara, pornografi, penipuan, pencurian data dan sebagainya. Penggunaan media sosial yang tidak bijak, menyebar *hoax* atau berita bohong, penyebaran *virus, malware, trojan* merupakan sisi negatif dari penggunaan internet (Nursida, 2021). Oleh karena itu jika hal-hal itu terjadi pada sebuah perusahaan yang salah satu karyawannya akses laman web mengandung konten negatif maupun pornografi dan ternyata sudah di susupi dengan *virus*, *malware* maupun trojan akan berdampak pada jaringan internet di perusahaan tersebut dapat terganggu bahkan lumpuh (Nadhir et al., 2022).

Manajemen keamanan internet yang penulis rancang menggunakan metode *firewall filtering* berbasis *content* (penyaringan berbasis konten) yang berfokus pada alamat-alamat web (situs) media sosial, web mengandung konten negatif dan pornografi yang tidak ada kaitan atau relevansi dengan pekerjaan (Sidik et al., 2021). Terdapat banyak jenis metode *firewall filtering* pada aplikasi Winbox diantaranya: *port and protocol parameter*, *interface, P2P protocol, mangle, connection state, Address list, layer 7 protocol, content filtering, Mac adress* (Wirawan, 2022). Metode *firewall filtering content* diterapkan pada perangkat Mikrotik Routerboard RB1100 menggunakan aplikasi Winbox. Router Mikrotik merupakan perangkat yang mendukung sistem keamanan jaringan yang didalamnya mendukung metode keamanan *firewall* (Alfred & Chandra, 2018). Perangkat ini dapat digunakan untuk pemblokiran konten yang berbau negatif, pornografi dan memaksa pengguna agar menghentikan pengguna mengakses konten tertentu (Langobelen et al., 2019). Berdasarkan jenis-jenis *firewall filtering* yang sudah disebutkan, penulis memilih menggunakan konsep *firewall filtering* berbasis *content* dengan alasan konfigurasi yang sederhana tetapi dengan hasil yang maksimal yaitu memblok alamat-alamat web yang di inginkan dengan langsung menuliskan kata-kata yang ingin di saring (*filter*) sehingga hasilnya lebih efektif.

PT. Bebentara Perkasa Indonesia merupakan sebuah perusahaan yang sangat membutuhkan jaringan internet, karena untuk menunjang kinerja karyawan dalam mengerjakan proyek yang akan diberikan kepada customer apabila sewaktu–sewaktu terjadi masalah (Meryawan et al., 2022). Tanpa adanya *firewall filtering content*, maka banyak karyawan yang menggunakan internet untuk membuka situs atau laman web yang tidak berhubungan dengan pekerjaan (Dewi & Islami, 2021). Dalam menyikapi permasalahan tersebut maka penulis tertarik untuk melakukan pengelolaan keamanan internet berbasis *content filtering* pada jaringan di PT.Bebentara Perkasa Indonesia, agar setiap karyawan tidak dapat membuka atau mengakses situs atau laman web yang tidak ada kaitannya dengan pekerjaan, dan setelah di blokirnya situs tersebut dipastikan karyawan dapat bekerja dengan fokus dan tepat waktu (Muzakir & Ulfa, 2019). *Firewall filtering* dapat berfungsi sebagai *firewall packing* (Perdana et al., 2023). *Firewall filtering* yang digunakan untuk melindungi jaringan lokal dari serangan atau gangguan yang berasal dari jaringan internet dengan cara melakukan *fitering* atas *packet* yang lewat dari dan ke jaringan- jaringan yang dihubungkan dan dapat dikonfigurasi untuk menolak akses ke website tertentu pada waktu - waktu tertentu (Stefanus Eko Prasetyo, 2021). *Firewall filtering content* merupakan metode pembuatan konfigurasi *firewall* untuk memblokir situs-situs tertentu dari sedang diakses (Bayu Santosa & Ali Akbar Rismayadi, 2022).

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini yaitu metode eksperimen. Metode eksperimen merupakan salah satu jenis penelitian kuantitatif yang mempunyai arti mencoba, mencari tahu dan melakukan konfirmasi (Alamsyah & Nugroho, 2022). Pada metode eksperimen terdapat beberapa tahapan yaitu, studi literatur, analisa, perancangan, implementasi, pengujian sistem, evaluasi dan dokumentasi (Hadi & Desmulyati, 2021)

A. Studi Literatur

Studi literatur atau disebut juga studi pustaka merupakan tahapan mencari bahan-bahan kepustakaan yang berasal dari artikel ilmiah berupa jurnal, prosiding, buku-buku referensi dan artikel internet yang relevan dengan objek penelitian dan memenuhi kaidah kekinian (*novelty*).

B. Analisa

Pada tahapan ini, penulis melakukan analisis terhadap jaringan komputer berjalan (yang sudah di implementasikan) pada tempat penelitian. Analisis yang dilakukan diantaranya, konfigurasi alamat IP, topologi jaringan, rancangan skema jaringan, manajemen jaringan sampai dengan keamanan jaringan yang terpasang.

C. Perancangan Implementasi

Pada fase ini, ditentukan perangkat lunak dan perangkat keras yang digunakan dan diusulkan untuk mengatasi permasalahan yang ada pada tahapan sebelumnya. Perangkat lunak (*software*) yang digunakan untuk sistem

operasi terdapat Windows yang sudah terpasang mesin virtual VMWare, aplikasi Winbox yang dijadikan sebagai *console* untuk konfigurasi pada router MikroTik dan di implementasikan pada Routerboard RB1100

D. Pengujian Sistem

Tahapan pengujian sistem dibagi menjadi dua yaitu tahapan pengujian awal dan tahapan pengujian akhir. Pengujian awal merupakan tahapan sebelum adanya penambahan perangkat Routerboard RB1100 dan belum adanya konfigurasi keamanan akses internet menggunakan metode *string*. Pada tahapan pengujian akhir menggunakan aplikasi Winbox yang ada pada MikroTik Routerboard.

E. Evaluasi

Tahapan ini merupakan tahapan setelah proses pengujian sistem sudah dilakukan. Hasil dari tahapan evaluasi dijadikan dasar apakah manajemen keamanan internet berbasis penyaringan konten (*content filtering*) dinyatakan berhasil dan efektif atau tidak.

HASIL DAN PEMBAHASAN

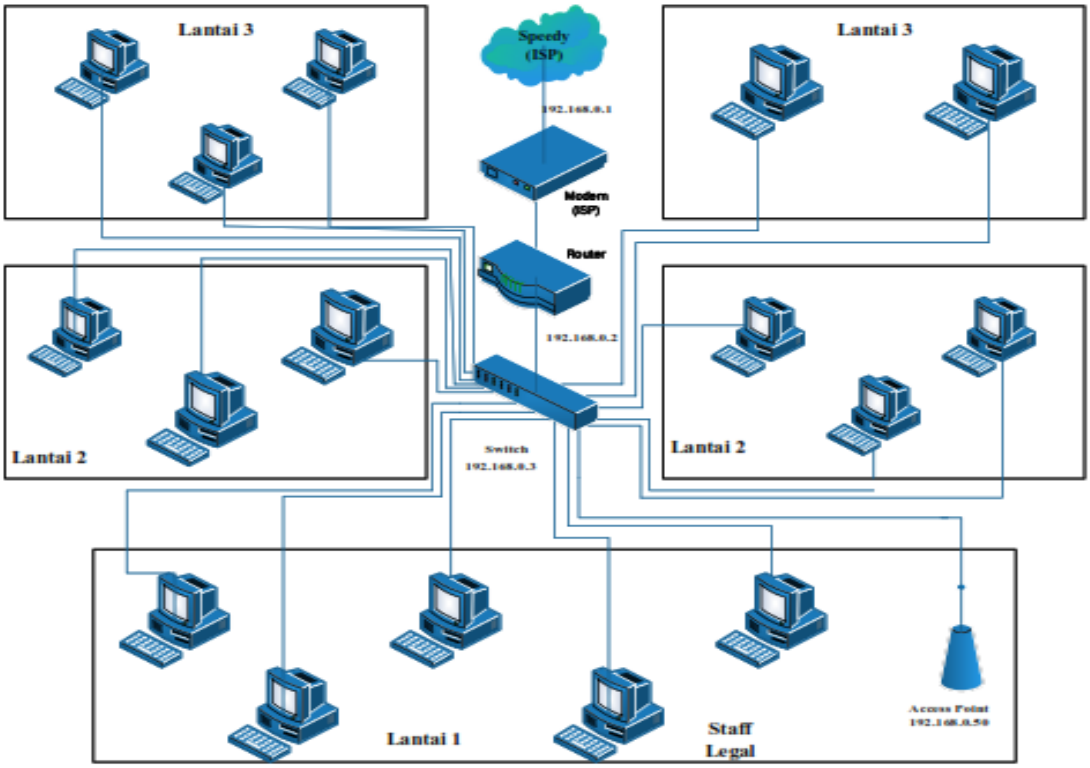
1. Skema Jaringan

Skema jaringan pada gambar 1 merupakan skema jaringan yang penulis usulkan. Pada skema jaringan ini pada dasarnya tidak ada perubahan pada topologi jaringannya, hanya ada penambahan perangkat baru yaitu berupa Router MikroTik Rb1100 yang nantinya akan ada konfigurasi pada apliaksi Winbox terkait manajemen keamanan internet berbasis *content filtering*. Pada skema jaringan usulan ini penulis menggunakan IP Publik (*ether1*) yang digunakan untuk menghubungkan ke ISP Speedy dari Telkom. Sedangkan untuk perangkat diantaranya Routerboard RB1100 dan Switch TP-LinkTL- SG1048 diberikan IP adress masing-masing. Pada tabel.1 merupakan pembagian alamat IP (*IP adress*) pada skema jaringan usulan.

Tabel 1. Pembagian alamat IP (*IP adress*)

Perangkat	Interface	IP adress	Gateway
Modem Zisa OP156-AC	ISP (ether1)	192.168.0.1	192.168.0.250
Router MikroTik RB1100	(ether2)	192.168.0.2	192.168.0.251
Switch TP-Link TL-SG1048	Vlan1	192.168.0.3	192.168.0.254

Sumber: hasil penelitian (2023)



Sumber: Hasil penelitian (2023)

Gambar 1. Skema jaringan usulan

Keamanan Jaringan

Untuk sistem keamanan jaringan pada PT. Bebentara Perkasa Indonesia Jakarta yang penulis usulkan, diantaranya:

1. Memberikan proteksi password pada Acces Point menggunakan keamanan WPA(*Wi-Fi Protected Access*).
2. Memberikan password pada semua PC yang ada.
3. Menggunakan sistem keamanan Intrusion Detection and Prevention System (IDPS) salah satunya adalah SNORT IDS yangan sangat efektif untuk mendeteksi atau memblokir penyusupan atau serangan, berfokus pada identifikasi serangan diam-diam, multi-tahap, dan rumit seperti serangan buffer overflow

Rancangan Aplikasi

Dalam rancangan aplikasi, ada beberapa aplikasi yang digunakan untuk meningkatkan kinerja jaringan dan untuk konfigurasi menajemen akses internet yang penulis lakukan dalam bentuk simulasi yaitu:

1. VMWare
2. MikroTik RouterOS
3. Winbox

Cara kerja dari manajemen keamanan internet berbasis *content filtering* menggunakan aplikasi Winbox yang penulis lakukan yaitu: menentukan alamat-alamat website yang akan di blok terlebih dahulu berdasarkan *string* (teks) yang tidak ada kaitannya dengan pekerjaan dari karyawan. Alamat-alamat *website* itu seperti media sosial, situs porno, media online, audio dan video streaming, *search engine.* Kemudian masukan list alamat *website* tersebut ke dalam aplikasi Winbox, lakukan pengujian dengan menggunakan *browser*. Pastikan semua alamat *website* yang ada dalam list tersebut tidak dapat dibuka atau di akses oleh karyawan agar tidak mengganggu jam kerja dan kinerja karyawan akan semakin meningkat. Pada tabel 2 terdapat contoh list alamat website yang penulis terapkan *content filtering.*

Tabel 2. Alamat *Website* yang di Blok

URL (http/ https)	***Pemblokiran* URL**	
	Tanpa *Conten Fitering*	Dengan *content filtering*
facebook.com	*Allow*	*Drop/ Deny*
twitter.com	*Allow*	*Drop/ Deny*
redtube.com	*Allow*	*Drop/ Deny*
playboy.com	*Allow*	*Drop/ Deny*
detik.com	*Allow*	*Drop/ Deny*
youtube.com	*Allow*	*Drop/ Deny*
movie.com	*Allow*	*Drop/ Deny*

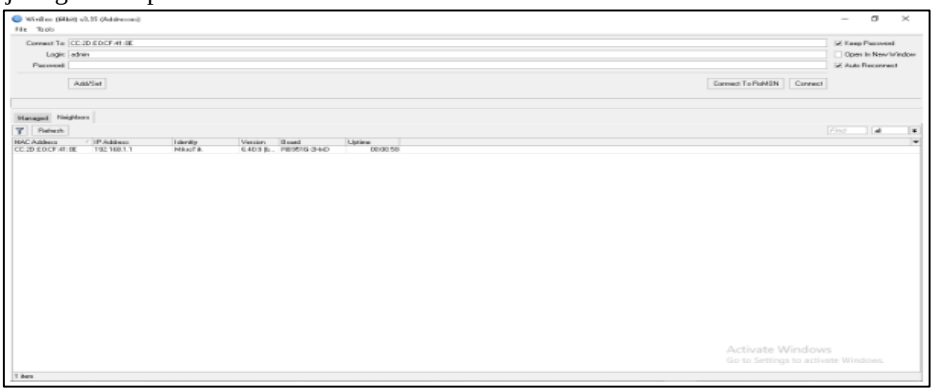
Sumber: Hasil penelitian (2023)

Perancangan *Firewall Filtering Content*

Berikut tahapan-tahapan dalam proses manajemen keamanan internet berbasis *firewall filtering content* pada perangkat MikroTik RouterOS menggunakan aplikasi Winbox.

1. Konfigurasi *Firewall*

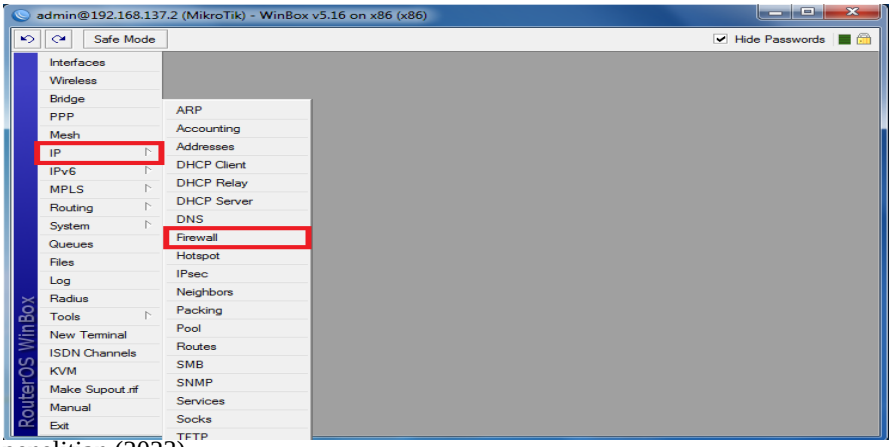
Firewall dapat berupa perangkat lunak (program komputer atau aplikasi) atau perangkat keras (peralatan khusus untuk menjalankan program *firewall*) perangkat yang menyaring lalu lintas jaringan antara jaringan. Perangkat ini penting dan sangat diperlukan karena bertindak sebagai gerbang keamanan antara jaring komputer internal dan jaringan komputer eksternal.



Sumber: Hasil penelitian (2023)

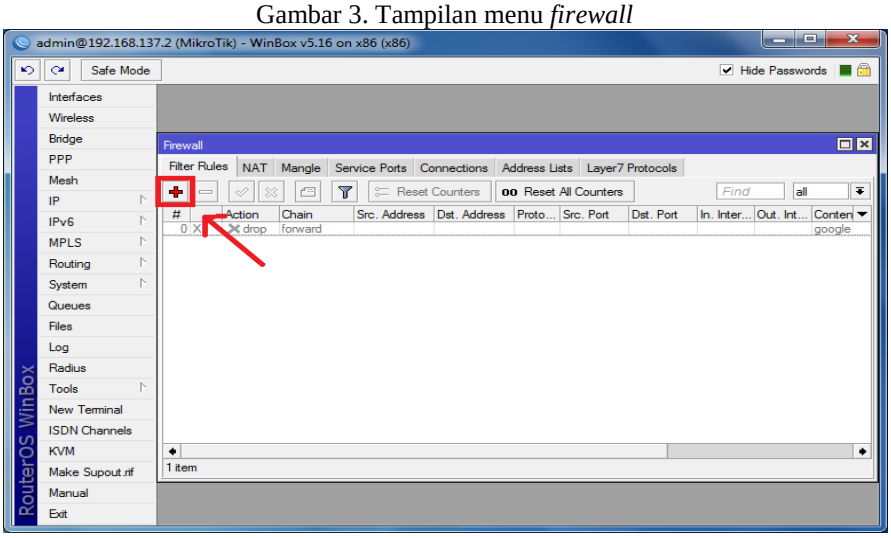
Gambar 2. Tampilan awal aplikasi Winbox

Pada tahapan konfigurasi *firewall* menggunakan aplikasi Winbox, pastikan aplikasi sudah terbuka kemudian jaringan komputer sudah terhubung (terkoneksi) dengan komputer yang di indikasikan pada lampu MikroTik yang menyala. Pilih login dengan MAC Address saat login pertama kali menggunakan aplikasi Winbox. Kemudian tekan tombol Connect, kemudian pada menu IP pilih menu *firewall*, kemudian klik ikon plus (+) untuk menambahkan konfigurasi untuk memblok situs.



Sumber: Hasil penelitian (2023)

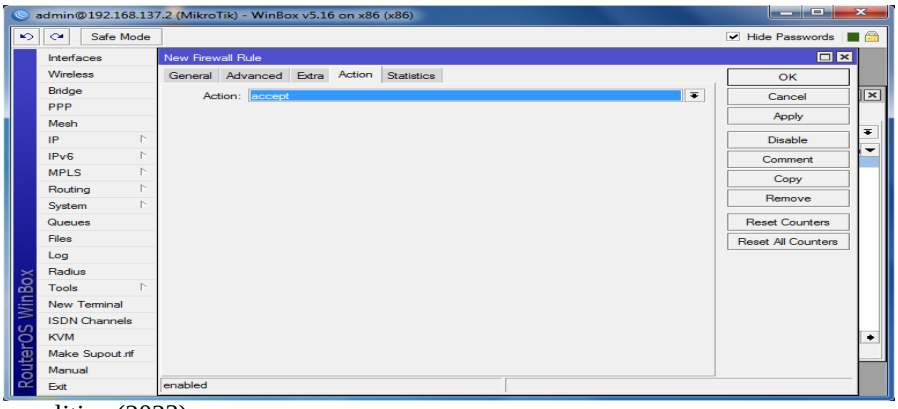
Gambar 3. Tampilan menu *firewall*



Sumber: Hasil penelitian (2023)

Gambar 4. Tampilan menu *firewall* penambahan konfigurasi situs

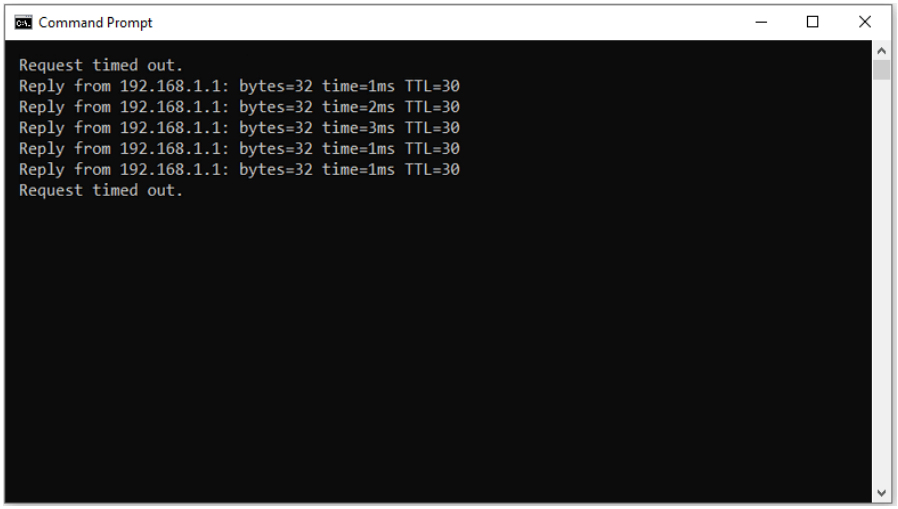
Pada menu *Firewall* ini nanti terdapat beberapa menu lain yang digunakan untuk konfigurasi *content filtering* nya yang terdiri dari tab *General, Advanced dan Action*. Untuk mengkonfigurasi isikan kolom *content* dalam bentuk string pada kolom *content* yang ada pada tab *Advanced*, isikan teks atau *string* dari situs yang akan diblok. Sebagai contoh penulis akan memblok situs youtube. Kemudian pada tab *Action*, konfigurasi action diubah menjadi *drop*. Action = *Drop* Data yang berasal dari klien akan dibuang (*drop*) oleh router.



Sumber: Hasil penelitian (2023)

Gambar 5. Tampilan menu firewall konfigurasi *action*

Tahapan ini dilakukan secara diam-diam, dengan tidak mengirimkan pesan penolakan ICMP (*Internet Control Message Protocol*). Untuk membuktikan apakah alamat web sudah benar di blok dapat di cek dengan menuliskan perintah CMD pada menu RUN, maka akan di munculkan hasilnya berupa RTO (*requesr time out*).



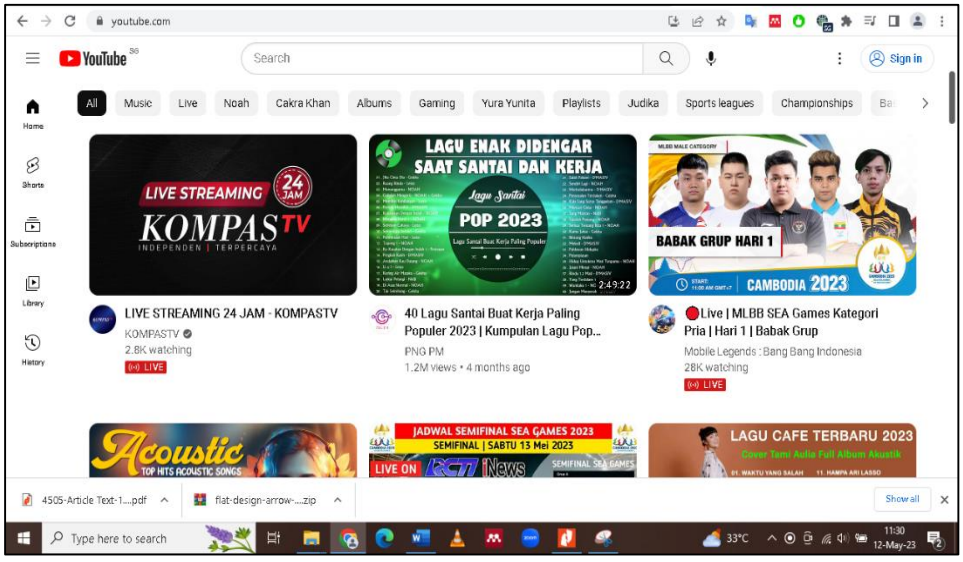
Sumber: Hasil penelitian (2023)

Gambar 6. Tampilan RTO pada laman web yang di blok

2. Pengujian Jaringan

A. Pengujian Jaringan Awal

Berikut ini adalah tampilan jaringan awal dalam hal situs yang dapat diakses sebelum dikonfigurasi *firewall* pada menggunakan metode *content filtering.*



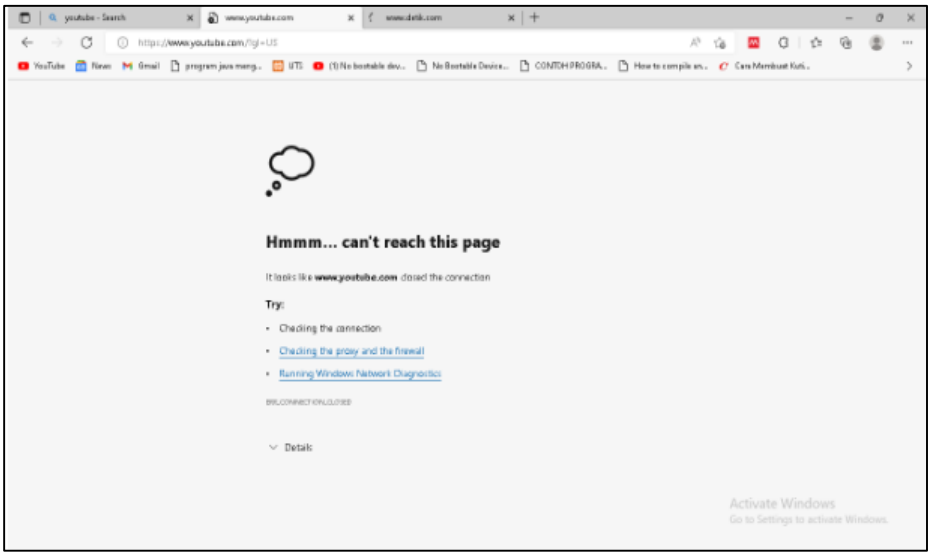
Sumber: Hasil penelitian (2023)

Gambar 7. Situs alamat youtube sebelum dilakukan *content filtering*

Pada jaringan awal sebelum diterapkan manajemen keamanan internet menggunakan *content filtering* dengan metode *string*, alamat situs Youtube (http://youtube.com) masih dapat di akses.

B. Pengujian Jaringan Akhir

Setelah dikonfigurasi dengan menambahkan *content filtering* menggunakan metode *Action = Drop*, maka alamat-alamat *website* yang tadi sudah di masukan ke dalam konfigurasi *firewall content filtering*, tidak dapat di akses. Pada gambar.8 merupakan contoh dari alamat website Youtube yang sudah di berikan *firewall filtering content.* Penggunaan metode *firewall filtering content* terbukti sangat efektif untuk memblok alamat web yang di isikan pada aplikasi Winbox.



Sumber: Hasil penelitian (2023)

Gambar.8 Hasil pengujian alamat website yang di blok

KESIMPULAN

Berdasarkan hasil dari penelitian dan simulasi pada jaringan yang telah dilakukan, penulis merangkum kesimpulan diantaranya: adanya penambahan perangkat berupa MikroTik Routerboard RB1100 ke dalam jaringan yang ada membuat jaringan internet menjadi lebih efektif dan terkontrol. Penggunaan aplikasi Winbox pada perangkat MikroTik Routerboard RB1100 mudah di konfigurasi dan di implementasikan. Penerapan manajemen keamanan internet menggunakan *firewall filtering* dengan metode *content filtering* pada aplikasi Winbox, terbukti sangat efektif untuk mencegah karyawan mengakses laman web (situs) yang tidak ada kaitan atau hubungan dengan pekerjaan. Sehingga dengan kebijakan ini, diharapkan kinerja karyawan makin meningkat.

REFERENSI

Alamsyah, I. R., & Nugroho, R. A. (2022). Pengaruh Latihan Shooting Dengan Metode Beef Terhadap Akurasi Free Throw Siswi Ekstrakurikuler Basket Smk Neger 4 Bandar Lampung. *Journal Of Physical Education*, *3*(2), 1–5. https://doi.org/10.33365/joupe.v3i2.1890

Alfred, & Chandra, J. C. (2018). Pemanfaatan Firewall pada Jaringan Komputer SMK Fadilah. *Journal I D E A L I S*, *1*(5), 422–428. http://jom.fti.budiluhur.ac.id/index.php/IDEALIS/article/download/1037/263

Bayu Santosa, & Ali Akbar Rismayadi. (2022). Implementasi Keamanan Jaringan Lan Menggunakan Mikrotik Dengan Metode Firewall Filtering. *E-PROSIDING TEKNIK INFORMATIKA Vol. 3, No. 1, Juni 2022*, *3*(1), 1–12.

Cholik, C. A. (2021). *PERKEMBANGAN TEKNOLOGI INFORMASI KOMUNIKASI / ICT DALAM BERBAGAI BIDANG*. *2*(March), 1–19.

Dewi, S., & Islami, A. I. (2021). Implementasi Web Filtering Menggunakan Router Fortigate FG300D. *INSANtek*, *2*(1), 22–27. https://doi.org/10.31294/instk.v2i1.424

Hadi, R. A., & Desmulyati, D. (2021). Implementasi Load Balancing Dengan Metode Peer Connection Classifier Pada Cabang PT. Astra Credit Companies. *Computer Science (CO-SCIENCE)*, *1*(2), 91–96. https://doi.org/10.31294/coscience.v1i2.415

Langobelen, E. S. R. O. B., Rachmawati, Y., & Iswahyudi, C. (2019). Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus Di Taman Pintar Yogyakarta. *Jurnal JARKOM*, *7*(2), 95–102.

Meryawan, I. W., Suryawan, T. G. A. W. K., & Handayani, M. M. (2022). Perceived Value pada Customer Loyalty Peran Mediasi Customer Engagement. *Jurnal Pendidikan Ekonomi Undiksha*, *14*(2), 339–349. https://doi.org/10.23887/jjpe.v14i2.52119

Muzakir, A., & Ulfa, M. (2019). ANALISIS KINERJA PACKET FILTERING BERBASIS MIKROTIK ROUTERBOARD PADA SISTEM KEAMANAN JARINGAN. *Jurnal Teknik Industri, Mesin, Elektro Dan Ilmu Komputer*, *10*(1), 15–20.

Nadhir, M., Radiyah, U., & Qomarudin, M. (2022). Optimalisasi Keamanan Wide Area Network (WAN) Menggunakan Raw Firewall Berbasis Mikrotik pada PT. Permata Graha Nusantara. *INTI Nusa Mandiri*, *17*(1), 16–23. https://doi.org/10.33480/inti.v17i1.3401

Nursida, I. (2021). Membangun Minat Belajar Agama Masyarakat Melalui Pemanfaatan Internet Secara Sehat. *Al-*

Ibanah, *06*(01), 105–125. http://ojs.jurnalalibanah.id/index.php/alibanah/article/view/24

Perdana, M. R., Testiana, G., & Informasi, S. (2023). *FIREWALL DAN WEB FILTERING DENGAN MIKROTIK PADA*. 52–59.

Sidik, S., Rahadjeng, I. R., & Fajrin, A. I. (2021). Implementasi Manajemen Bandwidth Menggunakan Simple Queue Dan Filtering Content Pada Pusat Pelatihan Kerja Pengembangan Industri jakarta Timur. *Reputasi: JurnalRekayasaPerangkatLunak*, *1*(1). http://eprints.bsi.ac.id/index.php/reputasi/article/view/134/234

Stefanus Eko Prasetyo, H. (2021). *Analısıs Dan Perancangan Monıtorıng Dan Notıfikası System Web Applıcatıon Fırewall Menggunakan Zabbıx*. *1*(1), 851–859.

Walidaini, B., & Muhammad Arifin, A. M. (2018). Pemanfaatan Internet Untuk Belajar Pada Mahasiswa. *Jurnal Penelitian Bimbingan Dan Konseling*, *3*(1). https://doi.org/10.30870/jpbk.v3i1.3200

Wirawan, H. S. (2022). Perancangan Keamanan Akses Internet Berbasis Text Filtering Pada Universitas Atma Jaya Makassar. *TEMATIKA: Jurnal Penelitian Teknik Informatika Dan Sistem Informasi*, *9*(2), 71–82. https://doi.org/10.56963/tematika.v9i2.131