

PERANCANGAN WEB FILTERING DENGAN METODE FIREWALL FILTER RULES PADA JARINGAN KOMPUTER PT. INTI PAKET PRIMA BERBASIS MIKROTIK ROUTEROS

DESIGNING WEB FILTERING WITH THE FIREWALL FILTER RULES METHOD ON THE PT. CORE PRIMA PACKAGE BASED ON MIKROTIK ROUTEROS

Ari Mulyana¹, Andi Suprianto²

Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi
Institut Sains dan Teknologi Nasional
Jl. Moh Kahfi II, Bhumi Srengseng Indah, Jagakarsa, Jakarta Selatan 12640
Telp. (021) 7874647, Fax. (021) 7866955
¹arimulyana240@gmail.com,² andisuprianto@istn.ac.id

ABSTRAKSI

Jaringan komputer memiliki dua media transmisi data, yaitu menggunakan media kabel dan media nirkabel. Jaringan nirkabel lebih rentan terhadap ancaman serangan dibandingkan dengan jaringan kabel, karena komunikasi yang terjadi pada jaringan nirkabel bersifat terbuka. Diperlukan sistem keamanan jaringan yang baik untuk dapat menjaga keamanan data pengguna jaringan agar terhindar dari serangan yang dilakukan pihak-pihak yang tidak bertanggung jawab. Skripsi ini membahas tentang perancangan sistem keamanan jaringan dengan menggunakan teknologi Firewall filter rules pada jaringan nirkabel berbasis MikroTik RouterOS. Skripsi ini bertujuan untuk melindungi sistem pengguna dari ancaman atau pun serangan awal dan untuk membatasi serta memfilter hak akses pengguna terhadap konten atau situs yang berpotensi membahayakan sistem pengguna pada saat mengakses jaringan nirkabel.

Kata Kunci : *Keamanan Jaringan, Jaringan Nirkabel, Firewall, filter rules, MikroTik RouterOS*

ABSTRACT

Computer networks have two data transmission media, namely using wired media and wireless media. Wireless networks are more vulnerable to the threat of attack compared to wired networks, because the communication that occurs on wireless networks is open. A good network security system is needed to be able to maintain the security of network user data to avoid attacks made by irresponsible parties. This thesis discusses the design of a network security system using Firewall filter rules technology on a MikroTik RouterOS-based wireless network. This thesis aims to protect the user's system from threats or initial attacks and to restrict and filter user access rights to content or sites that have the potential to harm the user's system when accessing wireless networks.

Keywords : *Network Security, Wireless Network, Firewall, filter rules, MikroTik RouterOS*

1. PENDAHULUAN

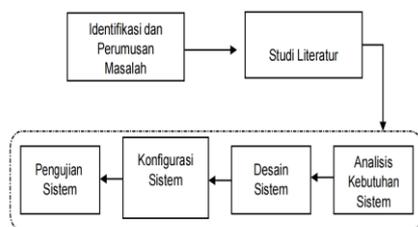
Pada zaman modern saat ini, perkembangan dalam bidang teknologi terjadi dengan sangat pesat. Perkembangan yang semakin pesat ini membawa perubahan yang tentunya memberikan banyak manfaat bagi kehidupan sehari-hari. Salah satu hal yang sangat berkembang dalam bidang teknologi ialah jaringan komputer. Jaringan komputer merupakan media dasar dalam menjalankan aktivitas dan produktivitas dengan memanfaatkan teknologi informasi. Berbicara mengenai jaringan komputer biasanya segala sesuatu itu harus berkaitan erat dengan layanan akses Internet dan juga loyalitas anggota. Penggunaan akses Internet ini tentunya sangat membantu dalam berbagai hal yang berkaitan dengan teknologi informasi seperti mencari sumber informasi, mengirimkan berbagai

informasi, berkomunikasi jarak jauh, dan sebagainya. Akan tetapi, tidak dapat dipungkiri bahwa layanan Internet ini terdapat situs web yang memiliki muatan negatif atau terlarang seperti situs pornografi, perjudian, penipuan, dan sebagainya. Salah satu solusi untuk mengatasi dan mencegah pengguna jaringan komputer dalam mengakses situs web bermuatan negatif ialah dengan menerapkan sistem web filtering terhadap jaringan komputer tersebut. Terdapat beberapa penelitian terdahulu yang sudah dilakukan dalam melakukan perancangan sistem web filtering terhadap jaringan komputer. Dalam penelitian yang dilakukan oleh Nurfauzi et al. (2018), perancangan sistem untuk mengatur filtering situs web dilakukan dengan memanfaatkan layanan Firewall pada sebuah jaringan komputer yang berbasis MikroTik di sebuah sekolah. Selain itu, terdapat juga

penelitian terkait implementasi sistem web filtering dengan memanfaatkan fitur WebProxy yang ada pada MikroTik seperti penelitian yang dilakukan oleh Haryanto et al. (2021). Kedua penelitian tersebut terbukti dapat menyaring, memblokir atau membatasi akses terhadap situs-situs web tertentu yang memiliki muatan negatif atau berpotensi membahayakan sistem pengguna saat mengakses jaringan Internet. Oleh karena itu penelitian ini dilakukan untuk mengembangkan penelitian tersebut, namun yang membedakan dari penelitian ini adalah perancangan sistem keamanan jaringan sebagai web filtering ini menggunakan metode Firewall Filter Rules, yang mana metode ini selain dapat digunakan untuk menyaring situs web bermuatan negatif, dapat juga digunakan untuk memblokir situs web bermuatan negatif tersebut ke situs lainnya yang lebih sehat dan aman.

2. METODOLOGI PENELITIAN

Pada proses tahapan penelitian ini, metode penelitian yang digunakan penulis dalam tugas akhir ini adalah menggunakan metode sekuensial linear agar proses penelitian dapat dilakukan secara terarah, teratur dan sistematis sehingga menghasilkan sebuah output yang diproses secara spesifik. Dapat dilihat pada gambar dibawah ini.



Gambar Tahapan Penelitian

Identifikasi Masalah

Pada proses ini, penulis melakukan identifikasi permasalahan, setelah diidentifikasi, kemudian permasalahan tersebut dijadikan sebuah rumusan masalah, dapat dilihat pembahasan tersebut pada sub Bab 1 tentang Rumusan Masalah.

Studi Literatur

Pada proses ini, penulis melakukan pengumpulan data dengan mempelajari literatur yang berhubungan dengan teori yang bersangkutan dengan pembahasan tugas akhir ini seperti jaringan komputer, keamanan jaringan, jenis-jenis jaringan komputer, Web Filtering, MikroTik, winbox dan beberapa teori yang berkaitan dalam proses pembuatan tugas

akhir ini. Pengumpulan dari data studi literatur tersebut telah dijelaskan pada sub Bab 2 Tinjauan Pustaka.

Analisis Kebutuhan Sistem

Pada proses ini, penulis melakukan sebuah analisis kebutuhan perangkat dari sistem yang dibutuhkan dalam melakukan penelitian ini, yang dibutuhkan diantaranya perangkat keras (hardware) dan perangkat lunak (software).

Desain Sistem

Pada proses ini, penulis melakukan desain kebutuhan yang nantinya akan diimplementasikan. Adapun desain dari perancangan sistem meliputi, perancangan topologi jaringan berikut penjelasannya.

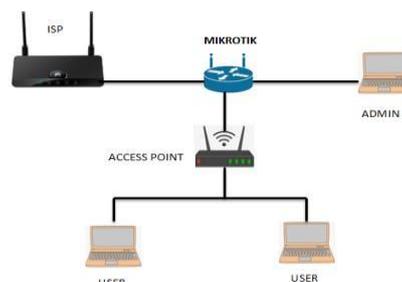
Perancangan topologi jaringan

Berikut merupakan tabel penetapan alamat IP address.

Tabel. Penetapan alamat IP

No	Nama Interface	Alamat IP Address
1.	Ether 1	192.168.1.12/24 (Menyesuaikan ISP)
2.	Ether 2	192.168.40.1/24
3.	Ether 3	192.168.50.1/24

Berdasarkan Tabel di atas merupakan penetapan alamat IP address terhadap komponen yang akan diterapkan pada topologi jaringan, setelah dilakukan penetapan alamat IP address, penulis melakukan sebuah perancangan topologi jaringan. penjelasan tersebut dapat dilihat pada gambar berikut.



Gambar Topologi Jaringan

Pada Gambar Topologi Jaringan di atas sebuah struktur jaringan yang berhubungan dengan peralatan yang digunakan dan pembentukan sebuah topologi jaringan. Perancangan ini dimaksudkan agar mempermudah dalam memahami struktur dan cara metode web filtering dengan menggunakan firewall filter rules. Perancangan topologi pada penerapan web filtering ini menggunakan topologi jaringan Star, dimana setiap perangkat yang di hubungkan ke pusat MikroTik Router.

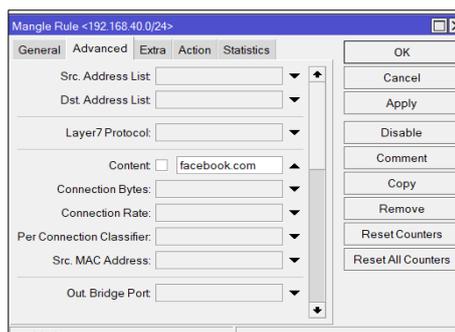
3. HASIL DAN PEMBAHASAN

Konfigurasi Sistem

Pada proses ini, penulis melakukan pengkonfigurasi sistem untuk melakukan kegiatan penelitian sesuai dengan desain penelitian yang sudah di tentukan sebelumnya meliputi, konfigurasi dasar jaringan dan konfigurasi penerapan web filtering dengan metode firewall filter rules pada jaringan komputer. Cara untuk melakukan penerapan implementasi tersebut dengan menggunakan aplikasi Winbox. Penjelasan tentang konfigurasi tersebut dapat dilihat seperti di bawah ini.

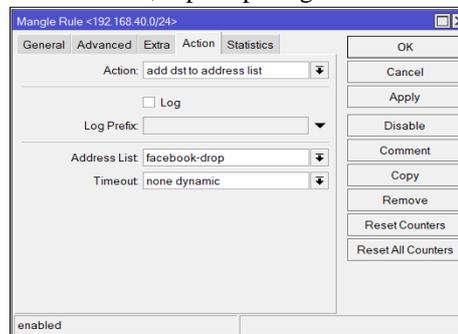
Konfigurasi Web Filtering

Penulis melakukan beberapa pembelokiran web filtering sosial media menggunakan firewall filter rules pada PT. Inti Paket Prima berbasis Mikrotik RouterOS. Dimana pengaturan web filtering tersebut akan sangat berfungsi mengamankan mikrotik dari user yang tidak bertanggung jawab atas hak akses dari mikrotik RouterOS. Adapun website yang di filtering antara lain: Facebook, Twitter, Tiktok, dan Shopee. Langkah-langkah penerapan konfigurasi web filtering menggunakan metode firewall filter rules. Yang pertama melakukan konfigurasi pembelokiran pada web facebook, dapat dilihat pada gambar berikut.



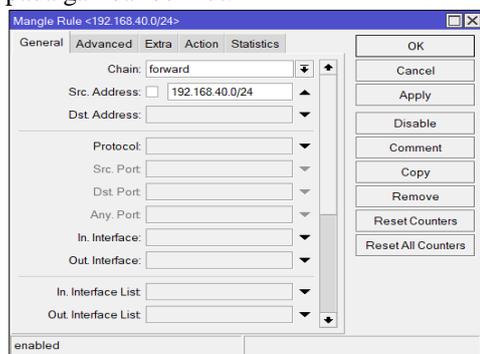
Gambar firewall mangle pada web Facebook Tab Advanced

Pada gambar diatas beralih ke tab advanced isikan nama web yang akan di filter, disini penulis melakukan blokir pada web facebook, yang harus diisi pada "content : facebook.com, seperti pada gambar di atas.



Gambar firewall mangle pada web Facebook Tab Action

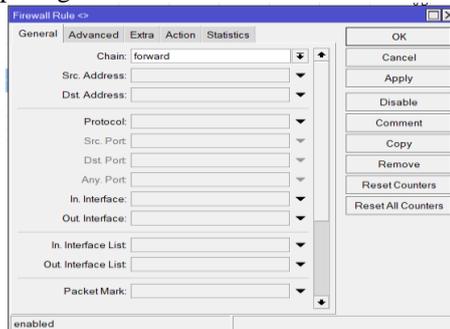
Pada gambar diatas pada tab action, isi " add dst to address list" lalu address list isi dengan nama "facebook-drop" dan masukkan timeout none dynamic, lalu pilih apply kemudian ok. Langkah selanjutnya melakukan konfigurasi firewall pada tab filter rules. Firewall filter rules merupakan salah satu firewall pada mikrotik yang digunakan untuk menentukan apakah suatu paket data dapat masuk atau tidak kedalam sistem router mikrotik paket data yang akan ditangani fitur filter ini adalah paket data yang ditunjukan pada salah satu interface router. Dapat dilihat pada gambar berikut.



Gambar firewall mangle pada web Facebook Tab General

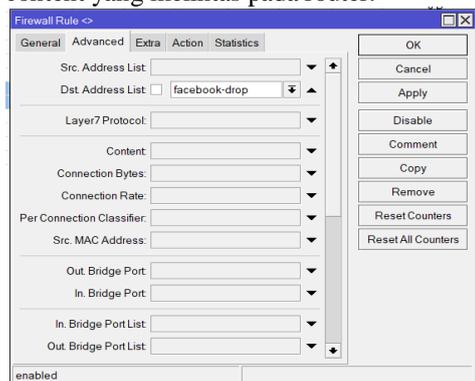
Pada gambar firewall mangle pada web Facebook Tab General di atas merupakan fitur firewall

mangle yang berfungsi untuk memberikan tanda marking atau penandaan pada suite paket data tertentu, dimana paket data yang telah di tandai ini nanti nya dapat digunakan oleh beberapa fitur yang ada pada router Mikrotik. Dapat dilihat pada tab General isikan "chain:forward" lalu masukan "scr.address: 192.168.40.0/24" yang diproteksi oleh Winbox, seperti terlihat pada gambar di atas.



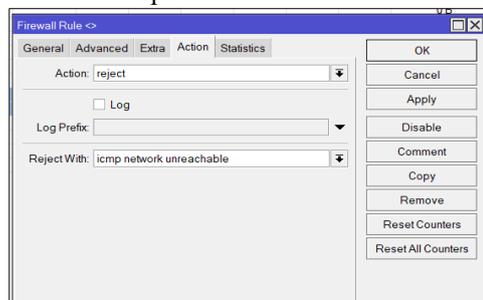
Gambar firewall filter rules pada web Facebook Tab General

Pada gambar di atas merupakan tampilan pada menu firewall filter rules pada tab general, isikan “Chain:Forward”, fungsinya untuk menangani paket data yang akan melintas pada router. sepintas fungsi chain forward hampir sama dengan NAT namun chain forward tidak melakukan perubahan IP Address ketika data melintas pada router, chain forward biasanya digunakan untuk melakukan akses blocking pada data atau content yang melintas pada router.



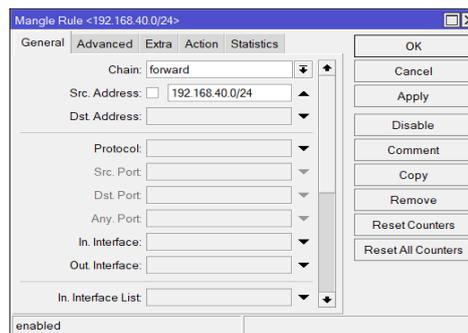
Gambar firewall filter rules pada web Facebook Tab Advanced

Pada gambar di atas merupakan tampilan pada menu firewall filter rules tab advanced pilih address list yang sudah di buat sebelumnya isikan dengan nama “facebookdrop”.



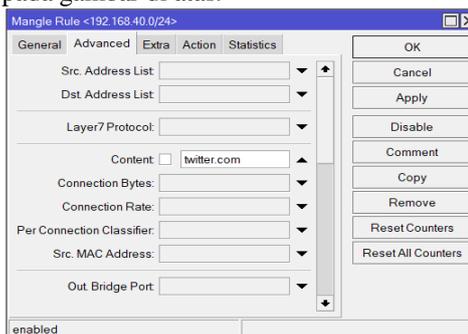
Gambar firewall filter rules pada web Facebook Tab Action

Pada gambar di atas merupakan tampilan pada menu firewall filter rules tab action. Pilih pada “action: reject” berfungsi menolak paket tetap mengirimkan pesan penolakan ICMP Sumber, lalu pilih apply kemudian ok, setelah melakukan konfigurasi web facebook yang telah di filtering ini, maka akan otomatis web facebook sudah tidak dapat di akses oleh pengguna lain. Langkah selanjutnya melakukan konfigurasi pemblokiran pada web Twitter, dapat dilihat pada gambar berikut.



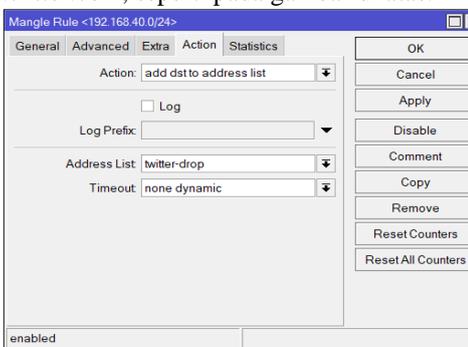
Gambar firewall mangle pada web Twitter Tab General

Pada gambar di atas merupakan tampilan fitur firewall mangle yang berfungsi untuk memberikan tanda marking atau penandaan pada suatu paket data tertentu, dimana paket data yang telah di tandai ini nantinya dapat digunakan oleh beberapa fitur yang ada pada router Mikrotik. Dapat dilihat pada tab General isikan “chain:forward” lalu masukan “src.address: 192.168.40.0/24” yang diproteksi oleh Winbox, seperti terlihat pada gambar di atas.



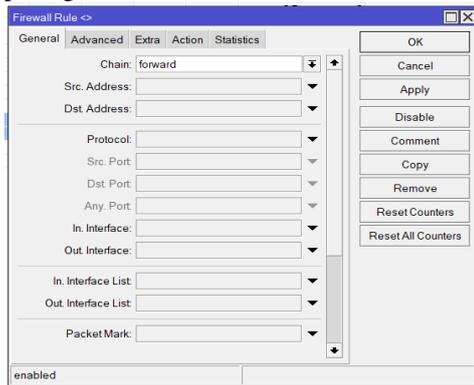
Gambar firewall mangle pada web Twitter Tab Advanced

Pada gambar diatas beralih ke tab advanced isikan nama web yang akan di filter, disini penulis melakukan blokir pada web twitter, yang harus diisi pada “content :tritter.com, seperti pada gambar di atas.



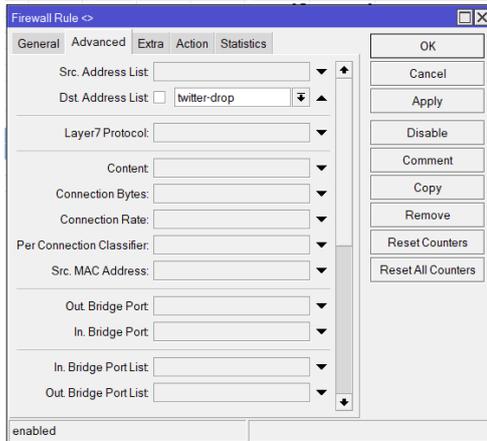
Gambar firewall mangle pada web Twitter Tab Action

Pada gambar diatas pada tab action, isi " add dst to address list" lalu address list isi dengan nama "twitter-drop" dan masukkan "timeout none dynamic", lalu pilih apply kemudian ok. Langkah selanjutnya melakukan konfigurasi firewall pada tab filter rules. Firewall filter rules merupakan salah satu firewall pada mikrotik yang digunakan untuk menentukan apakah suatu paket data dapat masuk atau tidak kedalam sistem router mikrotik paket data yang akan ditangani fitur filter ini adalah paket data yang ditunjukan pada salah satu interface router. Dapat dilihat pada gambar berikut.



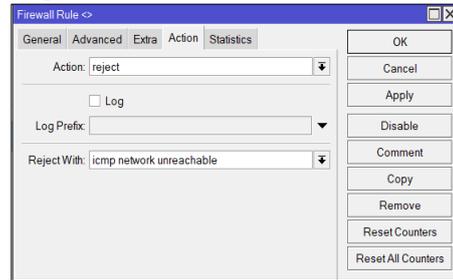
Gambar firewall filter rules pada web Twitter Tab General

Pada gambar di atas merupakan tampilan pada menu firewall filter rules pada tab general, isikan "Chain:Forward", fungsinya untuk menangani paket data yang akan melintas pada router. seperti fungsi chain forward hampir sama dengan NAT namun chain forward tidak melakukan perubahan IP Address ketika data melintas pada router, chain forward biasanya digunakan untuk melakukan akses blocking pada data atau content yang melintas pada router.



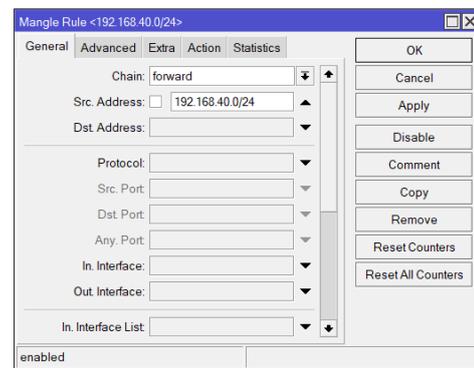
Gambar firewall filter rules pada web Twitter Tab Advanced

Pada gambar di atas merupakan tampilan pada menu firewall filter rules tab advanced pilih address list yang sudah di buat sebelumnya isikan dengan nama "twitter-drop".



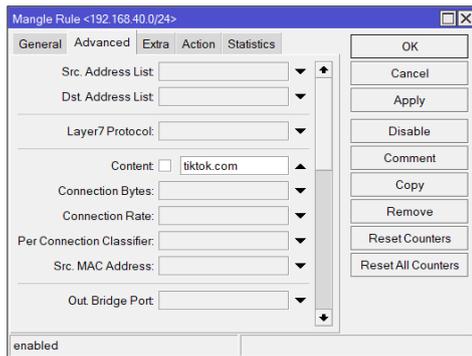
Gambar firewall filter rules pada web Twitter Tab Action

Pada gambar di atas merupakan tampilan pada menu firewall filter rules tab action. Pilih pada "action: reject" berfungsi menolak paket tetap mengirimkan pesan penolakan ICMP Sumber, lalu pilih apply kemudian ok, setelah melakukan konfigurasi web Twitter yang telah difiltering ini, maka akan otomatis web Twitter sudah tidak dapat di akses oleh pengguna lain. Langkah selanjutnya melakukan konfigurasi pemblokiran pada web Tiktok, dapat dilihat pada gambar berikut.



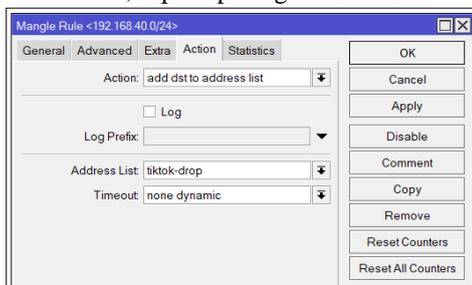
Gambar firewall mangle pada web Tiktok Tab General

Pada gambar di atas merupakan tampilan fitur firewall mangle yang berfungsi untuk memberikan tanda marking atau penandaan pada suatu paket data tertentu, dimana paket data yang telah di tandai ini nantinya dapat digunakan oleh beberapa fitur yang ada pada router Mikrotik. Dapat dilihat pada tab General isikan "chain:forward" lalu masukan "scr.address: 192.168.40.0/24" yang diproteksi oleh Winbox, seperti terlihat pada gambar di atas.



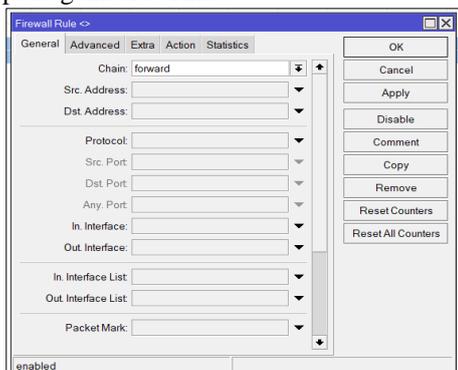
Gambar firewall mangle pada web Tiktok Tab Advanced

Pada gambar diatas beralih ke tab advanced isikan nama web yang akan di filter, disini penulis melakukan blokir pada web tiktok, yang harus diisi pada "content :tiktok.com, seperti pada gambar di atas.



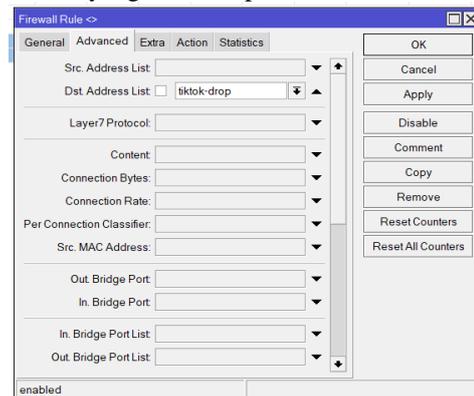
Gambar firewall mangle pada web Tiktok Tab Action

Pada gambar diatas pada tab action, isi " add dst to address list" lalu address list isi dengan nama "tiktok-drop" dan masukkan "timeout none dynamic", lalu pilih applykemudian ok. Langkah selanjutnya melakukan konfigurasi firewall pada tab filter rules. Firewall filter rules merupakan salah satu firewall pada mikrotik yang digunakan untuk menentukan apakah suatu paket data dapat masuk atau tidak kedalam sistem router mikrotik paket data yang akan ditangani fitur filter ini adalah paket data yang ditunjukkan pada salah satu interface router. Dapat dilihat pada gambar berikut.



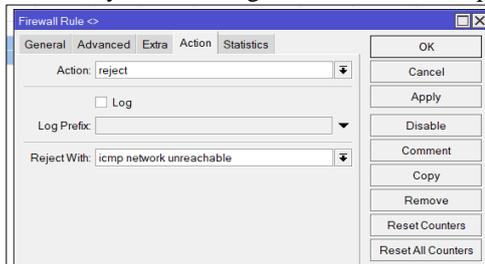
Gambar firewall filter rules pada web Tiktok Tab General

Pada gambar di atas merupakan tampilan pada menu firewall filter rules pada tab general, isikan "Chain:Forward", fungsinya untuk menangani paket data yang akan melintas pada router. sepintas fungsi chain forward hampir sama dengan NAT namun chain forward tidak melakukan perubahan IP Address ketika data melintas pada router, chain forward biasanya digunakan untuk melakukan akses blocking pada data atau content yang melintas pada router.



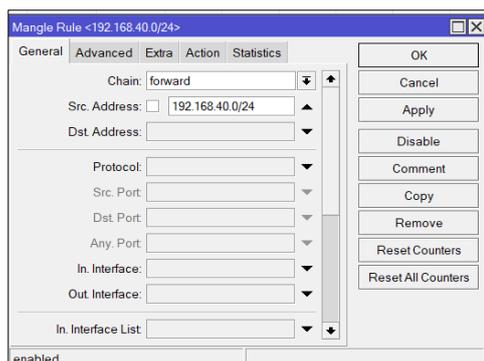
Gambar firewall filter rules pada web Tiktok Tab Advanced

Pada gambar di atas merupakan tampilan pada menu firewall filter rules tab advanced pilih address list yang sudah di buat sebelumnya isikan dengan nama "tiktok-drop".



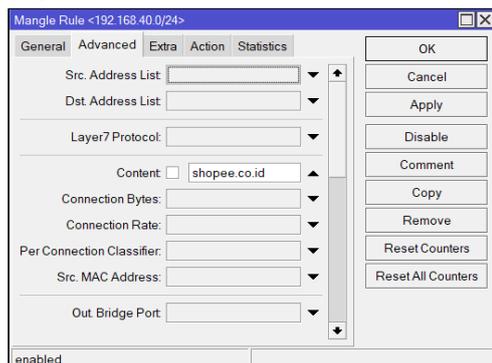
Gambar firewall filter rules pada web Tiktok Tab Action

Pada gambar di atas merupakan tampilan pada menu firewall filter rules tab action. Pilih pada "action: reject" berfungsi menolak paket tetap mengirimkan pesan penolakan ICMP Sumber, lalu pilih apply kemudian ok,setelah melakukan konfigurasi web Tiktok yang telah di filtering ini, maka akan otomatis web Tiktok sudah tidak dapat di akses oleh pengguna lain. Langkah selanjutnya melakukan konfigurasi pemblokiran pada web Shopee, dapat dilihat pada gambar berikut.



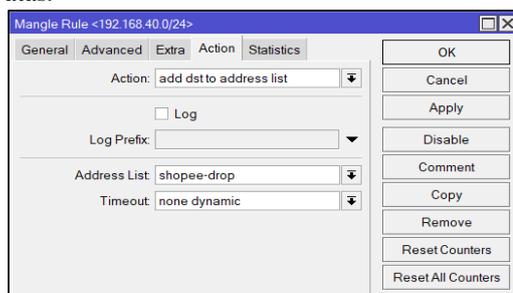
Gambar firewall mangle pada web Shopee Tab General

Pada gambar di atas merupakan tampilan fitur firewall mangle yang berfungsi untuk memberikan tanda marking atau penandaan pada suatu paket data tertentu, dimana paket data yang telah di tandai ini nantinya dapat digunakan oleh beberapa fitur yang ada pada router Mikrotik. Dapat dilihat pada tab General isikan “chain:forward” lalu masukan “scr.address: 192.168.40.0/24” yang diproteksi oleh Winbox, seperti terlihat pada gambar di atas.



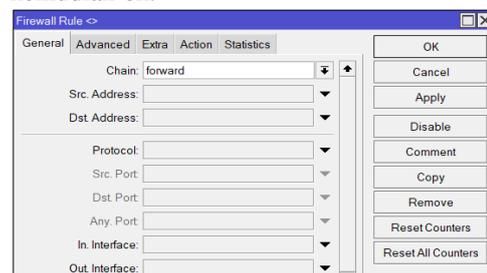
Gambar firewall mangle pada web Shopee Tab Advanced

Pada gambar diatas beralih ke tab advanced isikan nama web yang akan di filter, disini penulis melakukan blokir pada web shopee, yang harus diisi pada “content:shopee.co.id”, seperti pada gambar di atas.



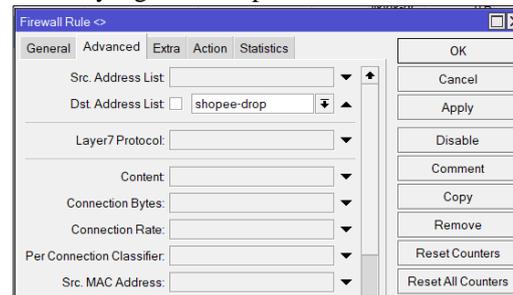
Gambar firewall mangle pada web Shopee Tab Action

Pada gambar diatas pada tab action, isi " add dst to address list" lalu address list isi dengan nama “shopee-drop” dan masukkan “timeout none dynamic”, lalu pilih apply kemudian ok.



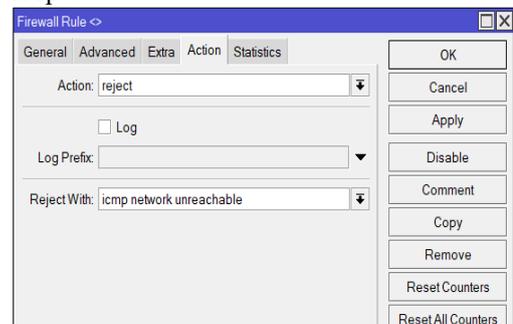
Gambar firewall filter rules pada web Shopee Tab General

Pada gambar di atas merupakan tampilan pada menu firewall filter rules pada tab general, isikan “Chain:Forward”, fungsinya untuk menangani paket data yang akan melintas pada router. sepintas fungsi chain forward hampir sama dengan NAT namun chain forward tidak melakukan perubahan IP Address ketika data melintas pada router, chain forward biasanya digunakan untuk melakukan akses blocking pada data atau content yang melintas pada router.



Gambar firewall filter rules pada web Shopee Tab Advanced

Pada gambar di atas merupakan tampilan pada menu firewall filter rules tab advanced pilih address list yang sudah di buat sebelumnya isikan dengan nama “shopee-drop”.



Gambar firewall filter rules pada web Shopee Tab Action

Pada gambar di atas merupakan tampilan pada menu firewall filter rules tab action. Pilih pada "action: reject" berfungsi menolak paket tetap mengirimkan pesan penolakan ICMP Sumber, lalu pilih apply kemudian ok, setelah melakukan konfigurasi web Shopee yang telah di filtering ini, maka akan otomatis web Shopee sudah tidak dapat di akses oleh pengguna lain. Setelah dilakukan penerapan proses pemblokiran web yang sudah di filtering berbasis firewall filter rules, maka web tersebut diatas tidak bisa lagi di akses oleh pengguna lain, bisa dibuktikan pada peroses pengujian system.

Pengujian Sistem

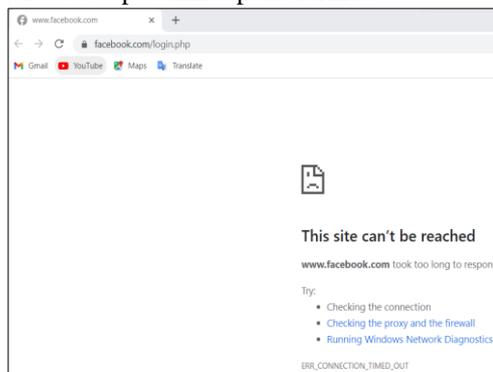
Pada proses ini, penulis melakukan pengujian sistem keamanan jaringan telah dibuat sebelumnya untuk memastikan kembali bahwa sistem yang telah di buat telah berhasil atau tidaknya, tujuannya bahawa penelitian ini telah berhasil sesuai yang dibutuhkan dan diharapkan. Penjelasan mengenai uji coba sistem telah dijelaskan pada sub point 4.

Uji Coba Sistem

Setelah instalasi dan konfigurasi sistem keamanan jaringan menggunakan firewall filter rules berbasis MikroTik RouterOS telah selesai, penulis akan menampilkan hasil pengujian sistem web target yang sudah di tentukan sebelumnya yaitu web Facebook, Twitter, Tiktok, Shopee menggunakan Microsoft Edge atau Google Crome, berikut pengujian sistemnya.

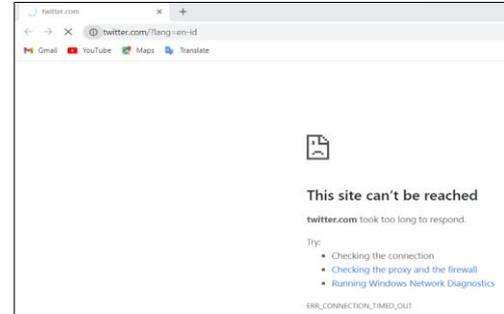
Pengujian Konektivitas Sesudah Web Di Filtering

Penulis mencoba melakukan akses terhadap situs web target antara lain web Facebook, Twitter, Tiktok, dan Shopee untuk memastikan apakah sistem web filtering dengan metode firewall filter rules ini telah berhasil atau tidak, dan hasil dari percobaan akses situs web tersebut dapat dilihat pada berikut.



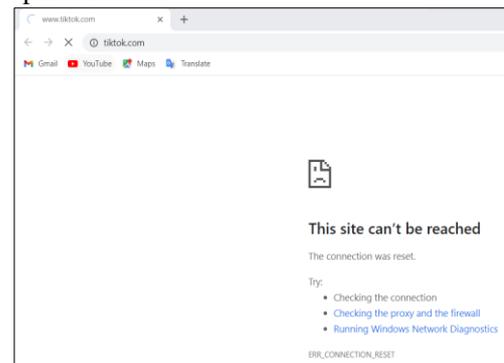
Gambar Situs Web Facebook Berhasil Terblokir

Pada gambar diatas merupakan tampilan dari situs web facebook.com dimana gambar tersebut menampilkan gagal mengakses atau telah terblokir serta tidak dapat diakses oleh user atau client. Artinya konfigurasi web filtering pada firewall rules telah berhasil diaplikasikan.



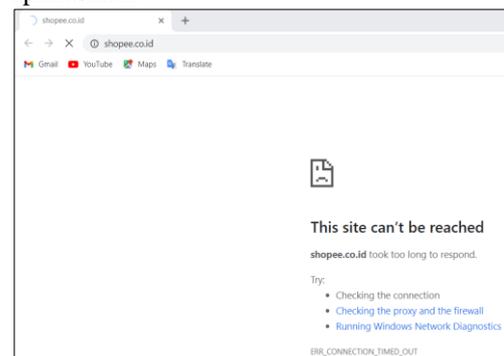
Gambar Situs Web Twitter Berhasil Terblokir

Pada gambar diatas merupakan tampilan dari situs web twitter.com dimana gambar tersebut menampilkan gagal mengakses atau telah terblokir serta tidak dapat diakses oleh user atau client. Artinya konfigurasi web filtering pada firewall rules telah berhasil di aplikasikan.



Gambar Situs Web Tiktok Berhasil Terblokir

Pada gambar diatas merupakan tampilan dari situs web tiktok.com dimana gambar tersebut menampilkan gagal mengakses atau telah terblokir serta tidak dapat diakses oleh user atau client. Artinya konfigurasi web filtering pada firewall rules telah berhasil di aplikasikan.



Gambar Situs Web Shopee Berhasil Terblokir

Pada gambar 30 diatas merupakan tampilan dari situs web Shopee.com dimana gambar tersebut menampilkan gagal mengakses atau telah terblokir serta tidak dapat diakses oleh user atau client. Artinya konfigurasi web filtering pada firewall rules telah berhasil di aplikasikan.

Dengan berhasilnya pengujian terkait proses pemblokiran web filtering pada situs target ini, dapat disimpulkan bahwa sistem keamanan jaringan komputer sebagai web filtering menggunakan metode Firewall Filter Rules pada jaringan komputer berbasis MikroTik RouterOS ini telah berhasil dan bekerja dengan baik.

4. SIMPULAN

Berdasarkan pengujian yang dilakukan dalam penelitian ini maka dapat disimpulkan bahwa :

1. Penggunaan perangkat LAN Internet yang didukung oleh Mikrotik memberikan kontribusi bagi upaya mengontrol situs akses dari user atau client. Dengan adanya mikrotik lebih teratur dalam pengelolaan penggunaan internet.
2. Dengan penggunaan perangkat LAN yang didukung oleh Mikrotik, dapat mengawasi pengguna dalam mengakses situs menjadi lebih terkontrol sehingga penggunaan akses menjadi tepat guna.

Saran

Dengan mempertimbangkan keterbatasan waktu dan pengetahuan yang dimiliki oleh peneliti maka sangat diperlukan pengembangan selanjutnya di masa mendatang. Adapun saran pengembangan tersebut antara lain sebagai berikut:

1. Konfigurasi ini hanya memblokir akses internet seperti Facebook, Twitter, Tiktok, Shopee, serta melakukan Scheduler untuk akses internet.
2. Dapat dikembangkan dengan metode lain maupun software yang lain.

5. DAFTAR PUSTAKA

[1] Admin. (2020). PENGERTIAN, JENIS-JENIS, SEJARAH DAN PERINTAH DASAR MIKROTIK. SMKAN 1 Panjalu.

[2] Ariffudin, M. (2022). Web Browser Adalah: Pengertian, Fungsi, Cara Kerja, dan Jenisnya. Niagahoster.

[3] Brades, T., & Irwansyah, I. (2022). Pemanfaatan Metode Port Knocking dan Blocking Untuk Kamanan Jaringan BPKAD Provinsi Sumsel. Prosiding Semhavok, 3(2), 99–107.

[4] Elearning, H. (2019). Jenis-jenis Jaringan Komputer Berdasarkan Area (LAN, MAN, WAN). Humbel.

[5] Hidayat, A., & Prakoso, D. S. P. (2021). RANCANGAN TOPOLOGI DAN IMPLEMENTASI JARINGAN INTERNET PADA PERUSAHAAN PT KRESNA GRAHA INVESTAMA Tbk. Akik. Jurnal Teknik Informatika, 3(1), 82.

[6] Jakaria, D. A. (2020). Implementasi Firewall Dan Web Filtering Pada Mikrotik Routeros Untuk Mendukung Internet Sehat Dan Aman (Insan). JUTEKIN (Jurnal Teknik Informatika), 8(2).
<https://doi.org/10.51530/jutekin.v8i2.480>

[7] RI Ramadhan, Siti Madinah Ladjamuddin; Perancangan Sistem Web Filtering Dengan Metode DNS Forwarding pada Jaringan Komputer Berbasis Mikrotik Routeros; Vol. 2 No. 2 (2022): Juli : Jurnal Informatika dan Teknologi Komputer ;
<https://journal.amikveteran.ac.id/index.php/jitek/article/view/231>, 146–157.

[8] Khafif, F. (2021). Peningkatan Pelayanan Internet Menggunakan Mikrotik Dan Software Winbox Di Ptipd Uin Walisongo Semarang. 3rd National Seminar on Maritime and Interdisciplinary Studies, 3(1), 3–6.

[9] Kurniawan, A. (2023). Aplikasi para seniman untuk menggambar dan melukis. Gurupendidikan.Com.
[https://www.gurupendidikan.co.id/jaringankomputer/#:~:text=Tujuan dari jaringan komputer ialah agar bisa mencapai,melakukan pengiriman yang memerikan layanan disebut dengan peladen server.](https://www.gurupendidikan.co.id/jaringankomputer/#:~:text=Tujuan%20dari%20jaringan%20komputer%20ialah%20agar%20bisa%20mencapai,melakukan%20pengiriman%20yang%20memerikan%20layanan%20disebut%20dengan%20peladen%20server%20.)

[10] Kurniawan, D. (2021a). Jenis-Jenis Jaringan Berdasarkan Distribusi Sumber Informasi atau Data. Omah Sejuta Tutorial.

[11] Kurniawan, D. (2021b). Tujuan dan Manfaat Jaringan Komputer. Omah Sejuta Tutorial. Mustofa, T. A., Sutanta, E., & Triyono, J. (2019). Perancangan Dan Implementasi Sistem Monitoring Jaringan Wi-Fi Menggunakan Mikromon

- Online Di Wisma Muslim. Jurnal JARKOM, 7(2), 65– 76.
- [12] Nugraha, J. (2021). Manfaat Jaringan Komputer, Lengkap Beserta Pengertian dan Jenisnya. Merdeka.Com.
- [13] Ridwanti, A. E. (2023). 10 Fungsi dan Manfaat Jaringan Komputer. Dianisa.Com.
- [14] FRI Ramadhan, Siti Madinah Ladjamuddin; Perancangan Sistem Web Filtering Dengan Metode DNS Forwarding pada Jaringan Komputer Berbasis Mikrotik Routeros; Vol. 2 No. 2 (2022): Juli : Jurnal Informatika dan Teknologi Komputer ; <https://journal.amikveteran.ac.id/index.php/jitek/article/view/231>
- [15] Yohanness, F. (2020). Analisa Dan Perancangan Keamanan Jaringan Lokal Menggunakan Security Onion Dan Mikrotik. Journal of Information System and Technology, 01(02), 37–61.