e-ISSN: 2655-1438
p-ISSN: 2655-1632

Implementasi *Filtering Firewall* untuk Mengatasi Virus Worm Menggunakan Mikrotik Router OS v.6.7

Dinda Dewayani [1)], Ria Andriani [2)], Rahmat Dwi [3)], Leo Ramadi [4)]

[1,2,3)] Teknik Informatika Universitas AMIKOM Yogyakarta
email: dinda.09@students.amikom.ac.id[1)], ria@amikom.ac.id[2)], rahmat.prastanto@students.amikom.ac.i[3)], leo.candra@students.amikom.ac.id[4)]

Abstraksi

Seiring berkembang pesatnya teknologi saat ini, banyak orang dapat mengakses berbagai teknologi informasi dimana dan kapan saja serta sangat memudahkan semua pekerjaan dari jarak dekat maupun jauh. Untuk mengatasi ancaman sistem keamanan teknologi informasi, telah dilakukan uji coba menggunakan firewall pada jaringan. Sistem ini dapat mendeteksi dan memblokir virus secara otomatis. Jika sistem mendeteksi virus masuk, akan muncul notifikasi mengenai virus yang menyerang keamanan jaringan tersebut. Sistem melakukan pengecekan terhadap keluar masuknya paket dari jaringan dan mengizinkan ataupun menolaknya berdasarkan aturan yang telah tibuat oleh pengguna yaitu sistem filtering packet yang akan digunakan untuk mengaplikasikan filtering firewall untuk mengatasi virus worm menggunakan mikrotik.

***Kata Kunci* :** *Firewall,Malware,Worm*

Abstract

Along the growing development of technology in this time, many people can access various information technologies anywhere and anytime and are very useful for all jobs from near and far distances. To resolve the threat of information technology security systems, testing has been carried out using a firewall on the network. This system can detect and block viruses automatically. If the system detects an incoming virus, a notification will be show about the virus attacking the network's security. The system checks the entry and exit of packets from the network and allows or rejects them based on the rules that have been made by the user, namely the packet filtering system that will be used to apply firewall filtering to deal with worm viruses using a *mikrotik.*

***Keywords* :** *Firewall,Malware,Worm*

Pendahuluan

Saat ini kejahatan komputer semakin tedak terkendali bersamaan dengan berkembangnya Teknologi Informasi. Salah satu kejahatan komputer yang sering terjadi penyebaran virus Malware. Malware tersebut dapat mengganggu kinerja sistem komputer maupun jaringan bahkan dapat merusaknya.

Penyebaran virus malware dapat melalui jaringan internal dimana dalam jaringan tersebut ada komputer yang sedang terhubung ke internet. Pengguna dapat memberikan akses kepada virus walaupun dengan cara yang tidak mereka sadari melalui komputernya. Virus dapat masuk kedalam sebuah komputer kemudian menginfeksi sebuah file di dalamnya, lalu virus tersebut dapat menyebar ke file lainnya bahkan ke jaringan yang lebih besar.

Pencegahan dapat dilakukan dengan membuat sebuah mekanisme yang berfungsi menjaga keamanan jaringan. Mekanisme tersebut dapat mengecek keamanan dari lalu lintas jaringan yang diakses oleh pengguna melalui komputernya sehingga pengguna dapat menggunakan jaringan secara aman. Mekanisme tersebut bernama Firewall yang merupakan sistem keamanan yang mudah untuk diterapkan pada berbagai jenis jaringan, serta dapat dikonfigurasi secara manual.

Mekanisme keamanan ini mempunyai keunggulan dengan menggunakan Mikrotik Router OS v.6.7 yang merupakan alat yang paling mudah dalam penerapannya.

Tinjauan Pustaka

Dalam penelitian yang dilakukan oleh Imam Riadi (2011) tentang optimalisasi keamanan jaringan menggunakan pemfilteran aplikasi berbasis mikrotik. Hasil dari penelitian ini adalah dengan memanfaatkan fitur pada Mikrotik sebagai pengatur jalur lalu lintas dari data internet, serta sebagai pemberian ijin terhadap aplikasi yang dapat .[1]

Selanjutnya pada penelitian yang dilakukan oleh Glend Sondakh., Meicsy E. I. Najoan, ST., MT, Arie S. Lumenta, ST, MT.(2014) tentang Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat. Hasil penelitian ini adalah filtering menggunakkan metode positif list lebih aman dilakukan karna secara default semua port ditutup, sedangkan untuk metode Negatif list sangat mudah untuk di lakukan karena semua

port secara default kita buka, lalu kemudian kita tutup portnya satu-satu.[2]

Pada penelitian yang dilakukan oleh Yanuar Dwi Jatmiko Wismoaji & Imam Riadi (2015) mengenai analisis perancangan firewall paket filtering dan proxy server untuk optimasi bandwidth (studi kasus di lab riset UAD kampus 3). Hasil dari penelitian ini adalah Firewall pada paket filtering yang dikembangkan dengan memblokir situs menggunakan metode drop IPTables dan pencocokan string algoritma KMP. Manajemen bandwidth yang dibangun dengan membatasi kecepatan akses untuk mengunduh file pada ekstensi tertentu dan download maupun browsing pada jam tertentu. Pengujian sistem menggunakan uji kelayakan yang hasilnya didapatkan bahwa sangat setuju = 20 %, setuju = 78 %, dan kurang setuju = 2 %. Berdasarkan pengujian tersebut dapat disimpulkan bahwa sistem layak dan direkomendasikan untuk diterapkan di laboratorium riset UAD. Sistem mampu menangani permasalahan mengenai situs pornografi yang dapat terakses dan penggunaan bandwidth yang belum optimal untuk praktikum. [3]
Selanjutnya pada penelitian yang dilakukan oleh Siti Nur Khasanah (2016) tentang Keamanan Jaringan Dengan Packet Filtering Firewall (Studi Kasus: PT. Sukses Berkat Mandiri Jakarta). Hasil penelitian ini adalah pembatasan resource yang digunakan dalam sebuah perusahaan dapat menggunakan packet filtering firewall, hal ini dapat memberikan dampak kearah yang lebih baik untuk perusahaan tersebut dalam segi penggunaan jaringan internet. Sedangkan untuk mengatur keamanan jaringan LAN ataupun WAN dapat mengunakan Untanggle karena memiliki fitur yang lengkap. [4]

Kemudian pada penelitian yang dilakukan oleh Eko Agus Darmadi & Kurnia (2018) mengenai perancangan pengamanan firewall pada jaringan LAN menggunakan metode packet filtering. Hasil dari penelitian ini adalah dengan menggunakan metode packet filtering sistem dapat memblokir situs yang dirasa perusahaan tidak berhubungan dengan pekerjaan karyawannya. Sehingga dengan begitu kinerja karyawan tidak akan bertambah turun karena penyalah gunaan fasilitas yang telah disediakan oleh perusahaan.[5]

Selanjutnya pada penelitian yang dilakukan oleh Muhamad Ryansyah, Muhammad Sony Maulana (2018) tentang Malware Security Menggunakan Filtering Firewall Dengan Metode Port Blocking Pada Mikrotik RB 1100AHx2. Hasil penelitian ini adalah dengan mengetahui jika penyebab suatu jaringan internet menjadi lambat bukan hanya dari segi bandwidth saja namun masih banyak kemungkinan penyebab yang mempengaruhi kecepatan suatu jaringan. Salah satunya karena penyebaran malware ke dalam jaringan tersebut, dengan adanya metode port blocking pada mikrotik dapat meminimalisir kemungkinan terjadi kelambatan pada jaringan sebuah perusahaan yang besar .[6]

Metode Penelitian

Dalam penelitian ini adapun alur yang akan digunakan, dapat dilihat pada gambar 1 berikut:

1.Mengidentifikasi masalah yang sedang terjadi pada masyarakat pada tahapan ini penulis lebih mengacu pada tema permasalahan Keamanan Jaringan yg sering terjadi pada era ini. Mencari jurnal-jurnal sejenis untuk membantu menyelesaiakan tema pemasalahan. Karena penyebaran virus melalui internet sedang marak terjadi dan sangat merugikan masyarakat luas. Studi literatur berguna untuk mengumpulkan berbagai macam informasi. Data yang terkumpul akan sangat berguna untuk menganalisa masalah penyebaran virus pada sebuah jaringan. Metode kualitatif adalah metode yang digunakan dalam penelitian ini. Dimana pengumpulan data dapat diperoleh dari makalah, jurnal ilmiah dan sumber-sumber lainnya. Rumusan masalah dapat diperoleh dari hasil analisis data yang telah terkumpul. Hal ini bertujuan agar penelitian ini tidak melenceng terlalu jauh dari tujuan utama yang telah di tentukan. Dalam merumuskan masalah ini dapat difokuskan pada permasalahan tentang penyebaran malware dalam suatu jaringan yg sering merugikan masyarakat terutama pengguna teknologi informasi.

2.Melakukan percobaan terhadap masalah penyebaran malware pada suatu jaringan yg sering merugikan masyarakat sehingga penulis dapat memberikan solusi yg dapat diterapkan pada masyarakat luas, jika penelitian yang dilakukan gagal maka akan melakukan uji coba lagi, jika penelitian berhasil maka hasil dari uji coba yg telah dilakukan dapat diterapkan.

Dengan menggunakan sebuah Virtual Machine sebagai Router dengan spesifikasi Mikrotik Router OS v.6.7, RAM 512 MB, HDD 500 MB, Ethernet virtual Host, Ethernet NAT. Dan sebagai client dengan spesifikasi Windows XP 32-bit, HDD 30 GB, RAM 1 GB, Ethernet virtual Host.

3. Menerapkan sistem Filltering Firewall pada Mikrotik Router OS v.6.7saat percobaan.

Hasil dan Pembahasan

Untuk mengetahui secara lebih lengkap infomasi default port malware dapat ditemukan dari beberapa atikel di internet. Berikut ini adalah beberapa contoh default port dan protokol malware pada Tabel 1.

e-ISSN: 2655-1438
p-ISSN: 2655-1632

Port	Protocol	Keyword	Description
20	tcp	ftp-data	File Transfer \[Default Data\]
20	udp	ftp-data	File Transfer \[Default Data\]
20	tcp	SennaSpyFTPserver	\[trojan\] Senna Spy FTP server
21	tcp	ftp	File Transfer \[Control\]
21	udp	ftp	File Transfer \[Control\]
21	tcp	BackConstruction	\[trojan\] Back Construction
21	tcp	DarkFTP	\[trojan\] Dark FTP
21	tcp	DolyTrojan	\[trojan\] Doly Trojan
21	tcp	InvisibleFTP	\[trojan\] Invisible FTP
21	tcp	Juggernaut42	\[trojan\] Juggernaut 42
21	tcp	Larva	\[trojan\] Larva
21	tcp	NetAdministrator	\[trojan\] Net Administrator
21	tcp	Ramen	\[trojan\] Ramen
21	tcp	RTB666	\[trojan\] RTB 666
21	tcp	SennaSpyFTPserver	\[trojan\] Senna Spy FTP server
21	tcp	Traitor21	\[trojan\] Traitor 21
21	tcp	\[trojan\]TheFlu	\[trojan\] The Flu
21	tcp	WebEx	\[trojan\] WebEx
21	tcp	WinCrash	\[trojan\] WinCrash
21	tcp	AudioGalaxy	AudioGalaxy file sharing app
22	tcp	Adoresshd	\[trojan\] Adore sshd
22	tcp	Shaft	\[trojan\] Shaft

Tabel 1. Default Port Dan Protocol Malware

A. Perancangan Sistem

Untuk mengetahui bagaimana suatu malware tersebar dalam suatu jaingan, penulis mengunakan mesin virtual sebagai media Router dan Client untuk melihat cara kerja penyebaran malware tersebut. Pada RouterOS mikrotik tersebut kita dapat menganalisis hasil dari lalu lintas jaringan tersebut.

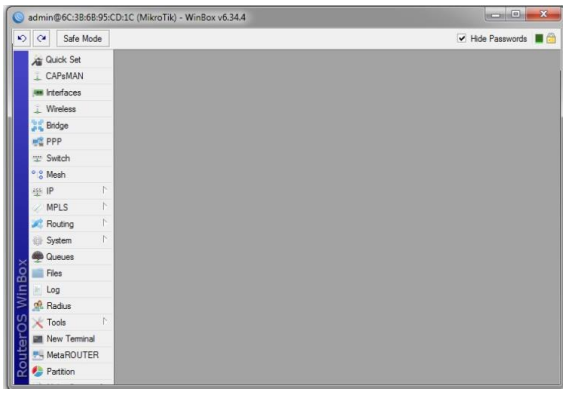
B. Implementasi Sistem

Untuk menambahkan konfigurasi pada RouterOS Mikrotik, kita dapat menggunakan winbox untuk membuat firewall dengan cara sebagai berikut:

1. Akses router yang terpasang pada sebuah jaringan agar dapat diatur sesuai dengan kebutuhan. Gunakan Winbox agar lebih mudah dalam mengatur router karena winbox dapat menampilkan semua fitur dan pengaturan yang tersedia dalam mikrotik dalam bentuk GUI. Pada gambar 2 merupakan tampilan untuk mengakses mikrotik.

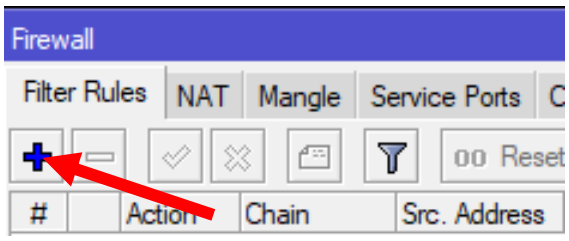
Gambar 2. Tampilan Login Winbox

2. Jika berhasil login dan mendapat akses ke router mikrotik menggunakan winbox. Maka akan muncuk seperti tampilan pada gambar 3 yang didalamnya terdapat berbagai fitur pengaturan yang telah disediakan oleh mikrotik.



Gambar 3. Tampilan Menu Utama Winbox

3. Buka menu IP > Firewall > Tab Filter Rule > + (untuk menambahkan firewall). Sedangkan firewall sendiri berfungsi untuk melindungi jaringan privat dengan cara mengawasi arus data yang melewati router yang telah dipasangi firewall tersebut. Penambahan Rule berada pada gambar 4.

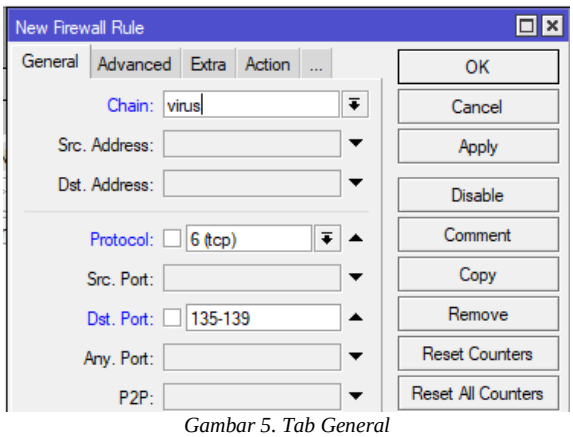


Gambar 4. Menambah Konfigurasi Filter Rules

4. Pada tab General dapat diisi seperti berikut ini:

   Chain : Virus
   Protocol : tcp
   Dst-port : 135-139

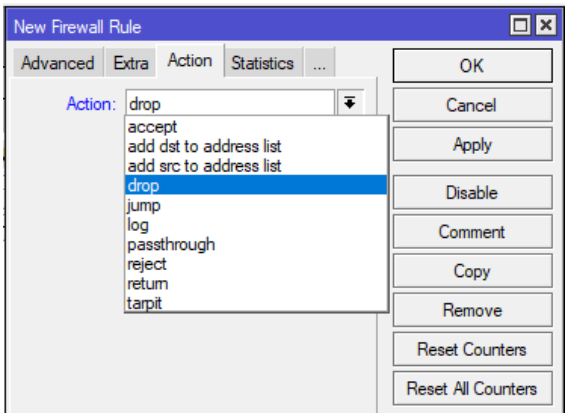
   Chain disini berfungsi sebagai definisi terhadap aturan yang sedang dibuat(ditambahkan). Untuk protokol sendiri berfungsi sebagai penentukan bagaimana cara sebuah paket data ditransmisikan. Sedangkan dst-port berfungsi sebagai port mana yang akan di eksekusi ataupun di pantau. Cara konfigurasi ada pada Gambar 5.



Gambar 5. Tab General

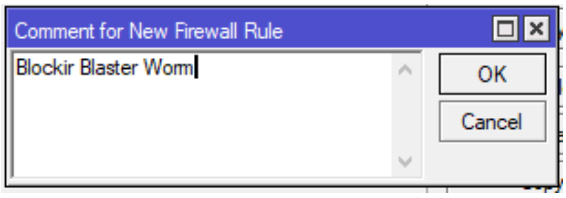
5. Di tab Action isi kolom dengan *drop*. Drop berfungsi sebagai perintah untuk menolak paket secara "diam-diam". Maksud dari "diam-diam"

disini adalah tidak mengirimkan pesan penolakan ke ICMP, langkah seperti Gambar 6.



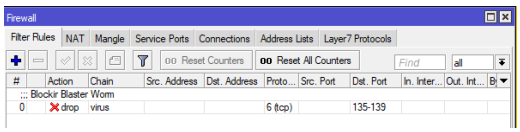
Gambar 6. Tab Action

6. Karena banyak port yang akan diblok, maka penulis tambahkan nama konfigurasi pada kolom komentar yang bertujuan agar mudah untuk mengetahui tujuan dari konfigurasi tersebut pada Gambar 7.



Gambar 7. Memberi nama untuk konfigurasi

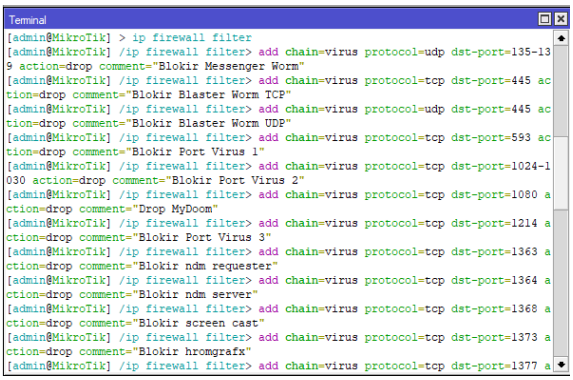
7. Ketika langkah – langkah diatas telah dilakukan maka akan menghasilkan sebuah keluaran berupa firewall untuk memblokir virus jenis worm seperti Gambar 8.



Gambar 8. Firewall yang telah dibuat

8. Winbox adalah salah satu software GUI yang dapat mempermudah dalam melakukan seting konfigurasi pada mikrotik. Salah satu fitur yang sering digunakan pada mikrotik adalah filtering firewall. Fitur ini sendiri sering kali digunakan untuk membuat filter Rule , Forwarding (NAT) dan bisa juga sebagai penanda untuk koneksi ataupun paket dari trafik data router (Mangle). Kesesuaian rule yang dibuat dapat mempengaruhi kinerja dari firewall yang diinginkan. Fitur firewall memiliki sebuah parameter utama yang bernama Chain. Parameter ini berfungsi untuk menentukan jenis trafik akan diatur pada fitur dan fungsi firewall (**Filter Rule, NAT, Mangle**).

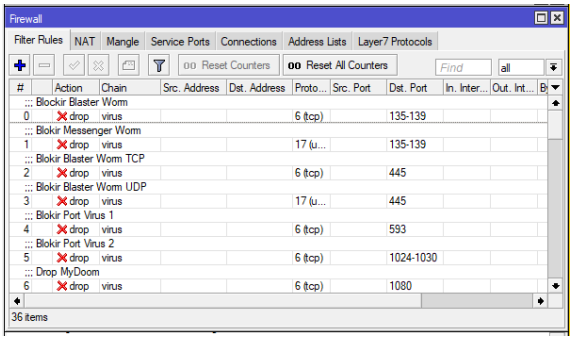
   selain menggunakan cara diatas, menambahkan firewall juga dapat dilakukan menggunakan terminal. Hal ini dilakukan untuk lebih menyingkat waktu apabila firewall yang akan ditambahkan berjumlah banyak. Yaitu dengan masuk ke menu New Terminal kemudian masukan perintah berikut:
   >> ip firewall filter
   >> add chain=virus protocol=tcp dst-port=135-139 action=drop comment=”Drop Messenger Worm”
   Untuk lebih lengkapnya dapat dilakukan seperti Gambar 9.



Gambar 9. Membuat Firewall dengan terminal

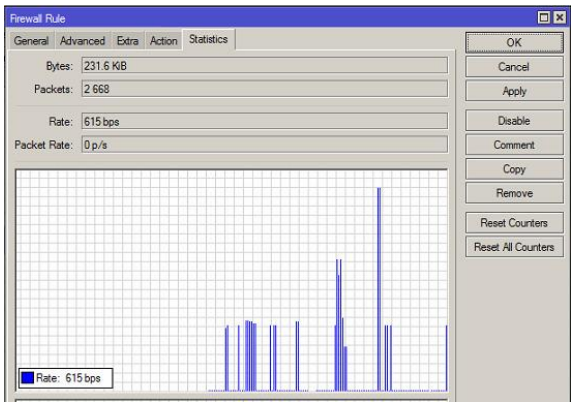
9. Dengan menggunakan terminal, penambahan Filter Firewall menjadi lebih mudah dan juga dapat memasukkan lebih banyak Firewall untuk memblokir virus worm yang memungkinkan menyerang pengguna. Dengan menggunakan terminal ini juga dapat menghemat dan mempercepat dalam konfigurasi Filter Firewall dibandingkan menggunakan GUI di atas serta konfigurasi lebih aman karena perintah tersebut dijelaskan secara detail dan lengkap.

   Dibawah ini adalah hasil dari penambahan Filtering Firewall menggunakan terminal. Beberapa konfigurasi yang telah dimasukkan akan muncul pada menu Firewall, seperti chain, port, protokol dan action untuk memblokir virus worm yang masuk. Dengan begitu keamanan jaringan mampu menjaga akses internet dan sistem dari virus dan juga berguna untuk pengeceken apabila terjadi masalah pada konfigurasi atau kekurangan pada konfigurasi saat mengatasi virus. Hasil konfigurasi seperti Gambar 10.



Gambar 10. Firewall yang telah di buat

10. Berikut adalah hasil statistik dari firewall yang telah dibuat menggunakan fitur filtering firewall pada mikrotik. Terlihat pada gambar 11, paket data yang melintas pada protokol tcp dst-port 135-139 digambarkan dalam diagram statik dibawah ini.



Gambar 11. Firewall yang telah di buat

Kesimpulan

Setelah hasil uji coba yang kami lakukan, dalam mengaplikasikan filtering firewall menggunakan mikrotik terbukti mampu memblokir virus worm pada suatu jaringan. Dengan mengkonfigurasi melalui winbox, virus worm dapat diblokir menggunakan action drop untuk mengatasi port virus worm dan proses konfigurasi yang mudah di implementasikan sehingga membuat keamanan jaringan menjadi lebih aman.

Saran

Karena pengaplikasian filtering firewall tersebut menggunakan Virtual Machine, konfigurasi pada winbox kemungkinan ada yang berbeda dengan perangkat asli, sehingga penerapan dalam filtering firewall tersebut akan kurang maksimal jika ada konfigurasi yang kurang lengkap.

Daftar Pustaka

[1] Riadi, Imam. 2011 "Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik.", Vol:1, No.1, junalwebsite. [online]. Available: https://is.uad.ac.id/jusi/wp-content/uploads/08-JUSI-Vol-1-No-1-_Optimalisasi-Keamanan-Jaringan-Menggunakan-Pemfilteran-Aplikasi-Berbasis-Mikrotik

[2] Sondakh, Glend, Meicsy E. I. Najoan, ST., MT, Arie S. Lumenta, ST, MT. 2014. "Perancangan Filtering Firewall Menggunakan Ip tables Di Jaringan Pusat Teknologi Informasi Unsrat." jurnal website. [online]. Available: https://ejournal.unsrat.ac.id/index.php/

[3] Jatmiko, Yanuar Dwi, Wismoaji, Imam Riadi. 2015. "Analisis Perancangan Firewall Paket Filtering Dan Proxy Server Untuk Optimasi Bandwidth (Studi Kasus Di Lab Riset Universitas Ahmad Dahlan Kampus 3)" .Vol:3, No:1. Jurnal website. [online]. Available: http://journal.uad.ac.id/index.php/JSTIF/.

[4] Khasanah ,Siti Nur. 2016. "Keamanan Jaringan Dengan Packet Filtering Firewall (Studi Kasus: PT. SuksesBerkatMandiriJakarta)". Vol:4, No:2, jurnal website. [online]. Available: https://ejournal.bsi.ac.id/ejurnal/index.php/khatulistiwa/article/view/1270/

[5] Darmadi, Eko Agus, Kurnia. 2018. "Perancangan Pengamanan Firewall Pada Jaringan Lan Menggunakan Metode Packet Filtering". Vol:17, No:2, jurnal website. [online]. Available: https://www.academia.edu/38328354/Jurnal_UNIBI_PERANCANGAN_PENGAMANAN_FIREWALL_PADA_JARINGAN_LAN_MENGGUNAKAN_METODE_PACKET_FILTERING

[6] Ryansyah, Muhamad and Maulana, Muhammad Sony. 2018. "Malware Security Menggunakan Filtering Firewall Dengan Metode Port Blocking Pada Mikrotik RB 1100AHx2". Vol:6, No:3, jurnal website. [online]. Available: http://jurnal.untan.ac.id/index.php/justin/article/download/26716/75676577541