Sistem Keamanan Jaringan Menggunakan *Firewall* Dengan Metode *Port Blocking* Dan *Firewall Filtering*

Dwiki Wicaksono *[1], Indrastanti R. Widiasari[2]
[1,2]Universitas Kristen Satya Wacana; Jl. Diponegoro No.52-60, Salatiga, Kec.Sidorejo, Kota Salatiga, Jawa Tengah, 50711, (0289)321212
[3]Jurusan Teknik Informatika, FTI UKSW, Salatiga
e-mail: *[1]672017111@student.uksw.edu, [2]indrastanti@uksw.edu

Abstrak

Firewall merupakan bagian penting dalam suatu keamanan jaringan dimana akses lalu lintas internet banyak digunakan dalam dunia pendidikan maupun pekerjaan. Dalam hal ini firewall sangat diperlukan untuk mengatur akses lalu lintas internet agar melindungi sistem dari ancaman dan serangan. Penelitian ini membahas tentang sistem keamanan jaringan menggunakan firewall dengan metode port blocking dan firewall filtering. Penelitian ini menggunakan router Mikrotik dan aplikasi Winbox untuk meremote router untuk membuat rule firewall yang berisi blocking port komunikasi dan pembatasan akses internet menggunakan web proxy dengan memblock situs http dan https dalam suatu jaringan. Hasil penelitian ini diuji menggunakan aplikasi Nmap Zenmap untuk melihat sisa port komunikasi yang terbuka dan menggunakan browser untuk mengakses web situs yang dialihkan dan di block. Dengan memaksimalkan dan mengoptimalkan kinerja firewall sebuah jaringan internet akan lebih aman dan meminimalisir ancaman serangan dari luar.

***Kata Kunci**:* Firewall, Keamanan Jaringan, *port blocking*, *web proxy*, MikroTik

Abstract

Firewall is an important part in a network security where internet traffic access is widely used in education and work. In this case a firewall is needed to regulate internet traffic access in order to protect the system from threats and attacks. This study discusses the network security system using a firewall with port blocking and firewall filtering methods. This study uses a Mikrotik router and Winbox application to remotely router to create a firewall rule that contains blocking communication ports and restricting internet access using a web proxy by blocking http and https sites in a network. The results of this study were tested using the Nmap application to see the remaining open communication ports and using a browser to access web sites that were redirected and blocked. By maximizing and optimizing the performance of a firewall, an internet network will be safer and minimize the threat of external attacks.

Keywords: *Firewall, Network Security, port blocking, web proxy, MikroTik*

1. PENDAHULUAN

Keamanan jaringan merupakan bagian penting dalam sebuah jaringan komputer. Kini jaringan komputer sangat penting dan banyak digunakan dalam pendidikan maupun dalam dunia pekerjaan. Dalam jaringan komputer itu sendiri ada hal yang sangat penting yaitu keamanan jaringan. Hal tersebut sangat vital dikarenakan kelemahan – kelemahan yang ada

didalam jaringan komputer dapat dicuri jika keamanan jaringan tersebut lemah. Banyak organisasi maupun kelompok mengabaikan pentingannya kemanan dalam jaringan dan lebih mengutamakan tampilan. Tanpa disadari sistem dalam jaringan komputer mengalami masalah, sehingga keamanan jaringan memang penting untuk melindungi suatu jaringan dari *malware* maupun *virus*.

Berdasarkan penelitian yang menjelaskan tentang sistem keamanan jaringan yang dirancang menggunakan firewall *security port*. Dimana seringnya terjadi pencurian data yang memanfaatkan perangkat lain untuk bisa mengambil alih hak akses jaringan sehingga membutuhkan suatu sistem keamanan jaringan seperti penerapan *firewall security port.*[1]

Penelitian yang menjelaskan tentang sistem yang menggunakan implementsi *traffic filtering* yang mengijinkan akses atau menutup akses *traffic* data yang masuk. Sering terjadi pengambilan data secara illegal dan perusakan jaringan sehingga dibuat suatu sistem yang dapat melindungi data yang penting maka digunakanlah *firewall* dan *traffic filtering.* Dengan adanya implementasi dan perancangan *firewall* dan *traffic filtering* suatu jaringan pada perusahaan akan menjadi lebih aman dengan memanfaatkan fungsi dari *Cisco Router* 1721 *series*. [2]

Penelitian tentang permasalahan suatu jaringan pada kampus yang disebabkan oleh penyebaran malware yang membuat jaringan menjadi lambat. Pengelolaan router dengan lebih spesifik sesuai dengan kebutuhan suatu jaringan dan pengoptimalan bandwidth yang ada. Dengan membuat aturan maupun perintah yang mengatur kinerja firewall agar dapat melakukan *filtering* sehingga mikrotik router lebih maksimal. [3]

Pada penelitian dengan cara menggunakan kinerja firewall secara optimal maka akan menjadi pondasi suatu jaringan. Hasil daripada penelitian yang dilakukan menggunakan metode DMZ pada suatu jaringan yang dapat melakukan *fillter DoS attack* dengan maksimal, dan penelitian dapat melakukan *block* pada serangan sehingga jaringan menjadi lebih aman. [4]

Keamanan jaringan merupakan suatu sistem yang berfungsi untuk pengamanan dalam suatu jaringan supaya terhindar dari berbagai macam ancaman dari luar yang dapat merusak jaringan dan tindakan pencurian data yang ada pada suatu perusahaan.[5]

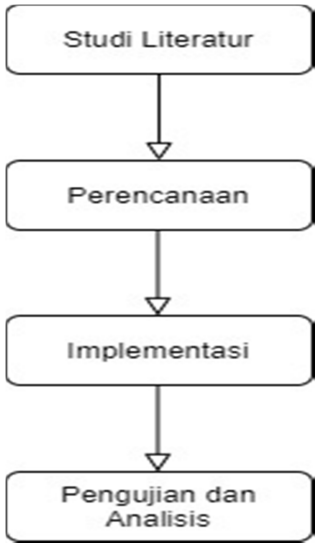
Port adalah suatu tempat yang menjadi lalu lintas informasi untuk keluar masuk dari suatu komputer.[6] *Port blocking* digunakan untuk mencegah lalulintas data yang berlangsung pada *port-port* yang ditentukan rawan terhadap serangan *virus* atau *malware.* [7]

Firewall merupakan suatu jenis teknologi keamanan jaringan yang berguna untuk mengatur paket data yang masuk ke dalam jaringan dan paket data yang di blokir. Firewall juga digunakan untuk melindungi, membatasi maupun menolak jaringan pribadi dengan jaringan luar yang berbahaya.[8] Firewall filter, adalah suatu metode untuk memilah data mana yang diijinkan dan yang tidak diijinkan.[9] Parameter utama dalam membuat *rule* Firewall diatur dalam parameter *chain* yang digunakan untuk menentukan jenis lalu lintas data yang akan diatur dalam *Firewall.* Proxy adalah suatu sistem yang memungkinkan kita untuk bisa mengakses suatu jaringan internet menggunakan *IP* yang berbeda dan dapat diterima oleh perangkat.[10]

Berdasarkan penelitian – penelitian yang pernah dilaksanakan terkait keamanan jaringan, maka akan dilakukan penelitian yang membahas tentang Analisa Sistem Keamanan Jaringan Menggunakan Firewall Dengan Metode *Port Blocking* dan *Firewall Filtering*. Dengan cara memaksimalkan kinerja *firewall* untuk memblock *port* komunikasi yang terbuka yang rawan terhadap serangan *malware* dan *virus* serta mengoptimalkan pembatasan akses jaringan internet dengan memblok situs http dan https dalam sebuah jaringan lokal.

2. METODE PENELITIAN

Metode yang yang digunakan pada penelitian yaitu studi literatur dengan memperhatikan kinerja sistem *firewall* dengan filterisasi *port blocking* dan *firewall filtering* sebagai pedoman dalam pelaksanaan penelitian. Penelitian ini dilakukan pada jaringan komputer lokal. Adapun flowchart tahapan yang digunakan untuk penelitian ini.



Gambar 1. Flowchart Penelitian

a. Studi Literatur

Tahap ini merupakan pengumpulan kajian dengan memperhatikan jurnal, bacaan-bacaan dan literatur yang berkaitan dengan sistem keamanan jaringan pada jaringan lokal. Dengan implementasi metode *port blocking* dan *firewall filtering* pada jaringan lokal.

b. Perencanaan

Dalam tahap perencanaan dilakukan penentuan *software* dan *hardware* yang digunakan. Rancangan *port* yang diblokir dan *rule access list* yang mengizinkan atau memblok tipe data tertentu. *Software* dan *Hardware* yang dibutuhkan dalam proses pelaksanaan penelitian ini adalah sebagai berikut:

- Winbox
- Nmap Zenmap GUI
- Browser

Hardware dan kebutuhan lain yang dibutuhkan:

- Router Mikrotik RB450GX4
- Modem
- Laptop
- Akses internet

Rule firewall yang digunakan untuk mendrop paket lalulintas data masuk ke dalam *port* yang rawan dari serangan *Worm, Trojan, Portmapper,* dan *Virus*. Dengan cara meminimalisir TCP *Port* dan UDP *Port* yang terbuka. Berikut rancangan *port* yang akan di blokir pada penelitian ini disajikan Gambar Tabel 1

Tabel 1. Rancangan *Port*

No	Nomor Port TCP	Jenis Port	Nomor Port UDP	Jenis Port
1	69	TCP	69	UDP
2	111	TCP	111	UDP
3	135-139	TCP	135-139	UDP
4	445	TCP	445	UDP
5	593	TCP	4444	UDP
6	1024-1030	TCP	9204	UDP
7	1080	TCP		
8	1214	TCP		
9	1363	TCP		
10	1364	TCP		
11	1368	TCP		
12	1373	TCP		
13	1377	TCP		
14	1433-1434	TCP		
15	2049	TCP		
16	2745	TCP		
17	3127-3128	TCP		
18	3410	TCP		
19	4444	TCP		
20	5554	TCP		
21	8866	TCP		
22	9898	TCP		
23	10000	TCP		
24	10080	TCP		
25	12345-12346	TCP		
26	17300	TCP		
27	20034	TCP		

c. *Implementation*

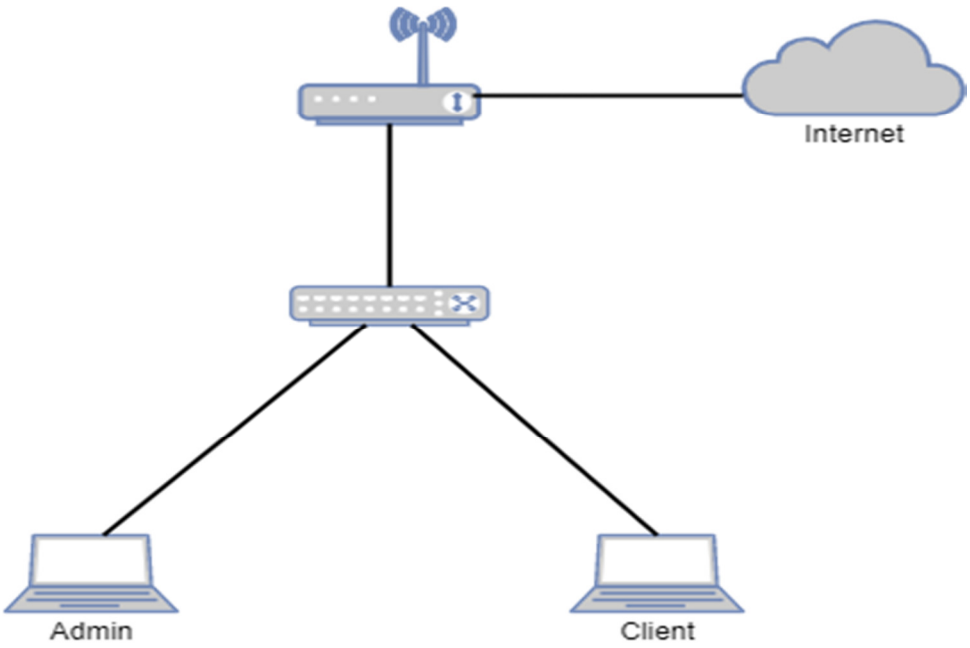
Implementasi merupakan tahap yang melakukan konfigurasi *rule firewall*, yang berfungsi menutup *port* komunikasi yang tidak digunakan dan pembatasan akses penggunaan jaringan internet.

d. *Pengujian dan Analisis*

Dalam tahap proses yang dilakukan adalah pengujian untuk mengetahui hasil penelitian setelah dilakukan implementasi metode *port blocking* dan *firewall filtering* pada jaringan lokal.

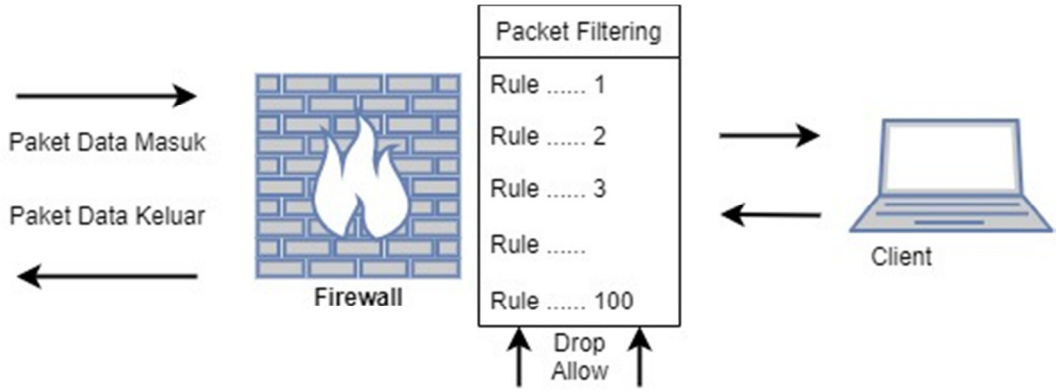
3. HASIL DAN PEMBAHASAN

Dalam penelitian ini perancangan, implementasi serta pembahasannya. Penulis telah mempersiapkan rancangan topologi jaringan untuk implementasi yang berisi komputer *client,* admin, Mikrotik Router, dan *access point* yang terhubung dengan internet. Desain jaringan lokal pada penelitian ini seperti pada Gambar 2



Gambar 2**.** Topologi Jaringan pada Penelitian

Dalam tahap implementasi akan dirancang metode *firewall* yang akan digunakan untuk pemfilteran satu layer yaitu dengan menggunakan *Firewall Packet Filtering*, yang digunakan untuk mengatur akses dan izin keluar masuk paket yang dimana telah di beri rule untuk paket yang di blokir dan di beri akses. Ilustrasi aliran data firewall seperti pada Gambar 3



Gambar 3. Ilustrasi Aliran Data *Firewall*

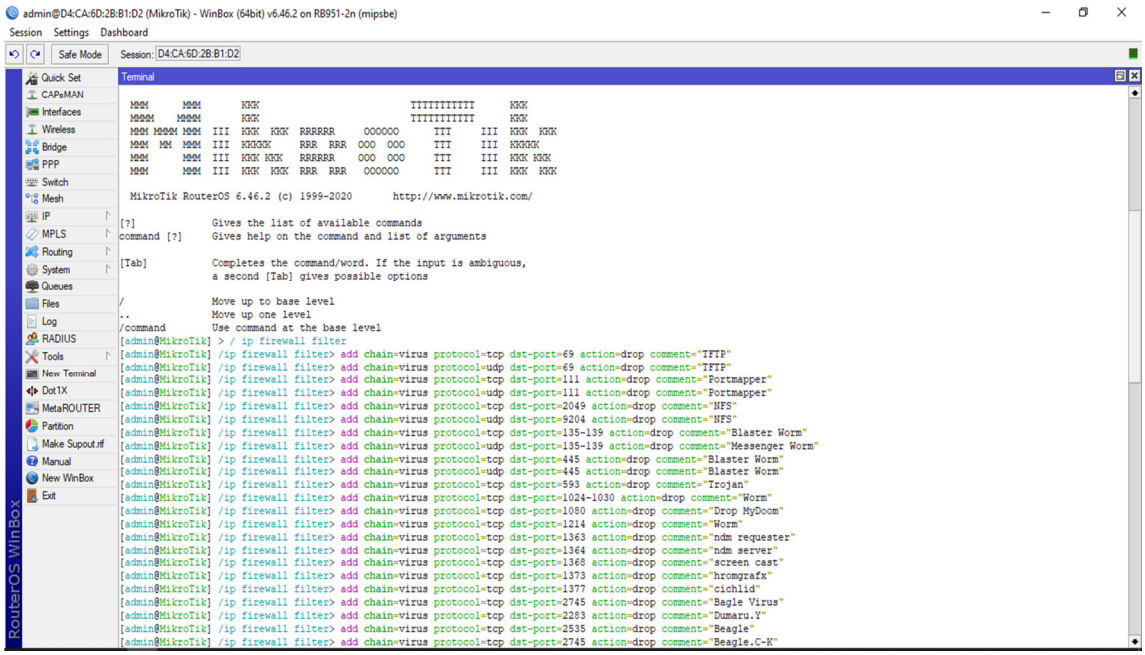
a. Proses Input Rule Firewall

Dalam langkah ini proses *input rule firewall* dilakukan dengan menutup *port* yang rentan diserang menggunakan perintah pada *command* di terminal MikroTik pada aplikasi Winbox.

Tabel 2. Kode Program *Rule Firewall*

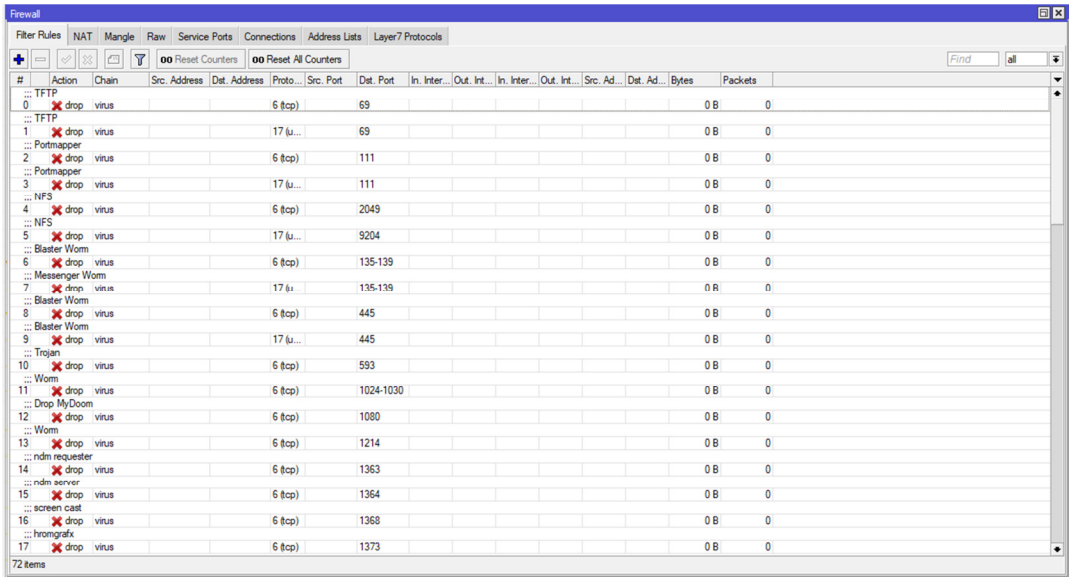
```
/ip firewall filter
Add chain=block protocol=tcp dst-port=69 action=drop
Add chain=block protocol=udp dst-port=69 action=drop
Add chain=block protocol=tcp dst-port=111 action=drop
Add chain=block protocol=udp dst-port=111 action=drop
Add chain=block protocol=tcp dst-port=135-139 action=drop
Add chain=block protocol=udp dst-port=135-139 action=drop
Add chain=block protocol=tcp dst-port=445 action=drop
Add chain=block protocol=udp dst-port=445 action=drop
Add chain=block protocol=udp dst-port=4444 action=drop
Add chain=block protocol=udp dst-port=9204 action=drop
Add chain=block protocol=tcp dst-port=593 action=drop
Add chain=block protocol=tcp dst-port=1024-1030 action=drop
Add chain=block protocol=tcp dst-port=1080 action=drop
Add chain=block protocol=tcp dst-port=1214 action=drop
Add chain=block protocol=tcp dst-port=1363 action=drop
Add chain=block protocol=tcp dst-port=1364 action=drop
Add chain=block protocol=tcp dst-port=1368 action=drop
Add chain=block protocol=tcp dst-port=1373 action=drop
Add chain=block protocol=tcp dst-port=1377 action=drop
Add chain=block protocol=tcp dst-port=1433-1434 action=drop
Add chain=block protocol=tcp dst-port=2049 action=drop
Add chain=block protocol=tcp dst-port=2745 action=drop
Add chain=block protocol=tcp dst-port=3127-3128 action=drop
Add chain=block protocol=tcp dst-port=3410 action=drop
Add chain=block protocol=tcp dst-port=4444 action=drop
Add chain=block protocol=tcp dst-port=5554 action=drop
Add chain=block protocol=tcp dst-port=8866 action=drop
Add chain=block protocol=tcp dst-port=9898 action=drop
Add chain=block protocol=tcp dst-port=10000 action=drop
Add chain=block protocol=tcp dst-port=10080 action=drop
Add chain=block protocol=tcp dst-port=12345-12346 action=drop
Add chain=block protocol=tcp dst-port=17300 action drop
Add chain=block protocol=tcp dst-port=20034 action drop
```

Berdasarkan Kode Program 1 perintah yang digunakan adalah */ip firewall filter* kemudian parameter *chain* diisi dengan jenis *traffic* yang akan di *manage* menggunakan firewall. Dalam proses penelitian *traffic* yang digunakan adalah *block* untuk *blocking port*. Protocol TCP dan UDP berdasarkan dst port yang akan di *block*, kemudian *action* diisi dengan *drop* dikarenakan akan menutup akses port.



Gambar 4. Tampilan *Input Rule Firewall* pada Terminal

Pada Gambar 4 tampilan hasil *input rule firewall* pada terminal setelah selesai mengisi parameter-parameter maka akan muncul pada *list firewall filter.* Ketika ada trafik paket data yang akan melewati router maka akan dilakukan pengecekan oleh *rule firewall filter*. Jika terdapat paket yang melalui *port* yang didefinisikan maka paket data akan di *drop.*

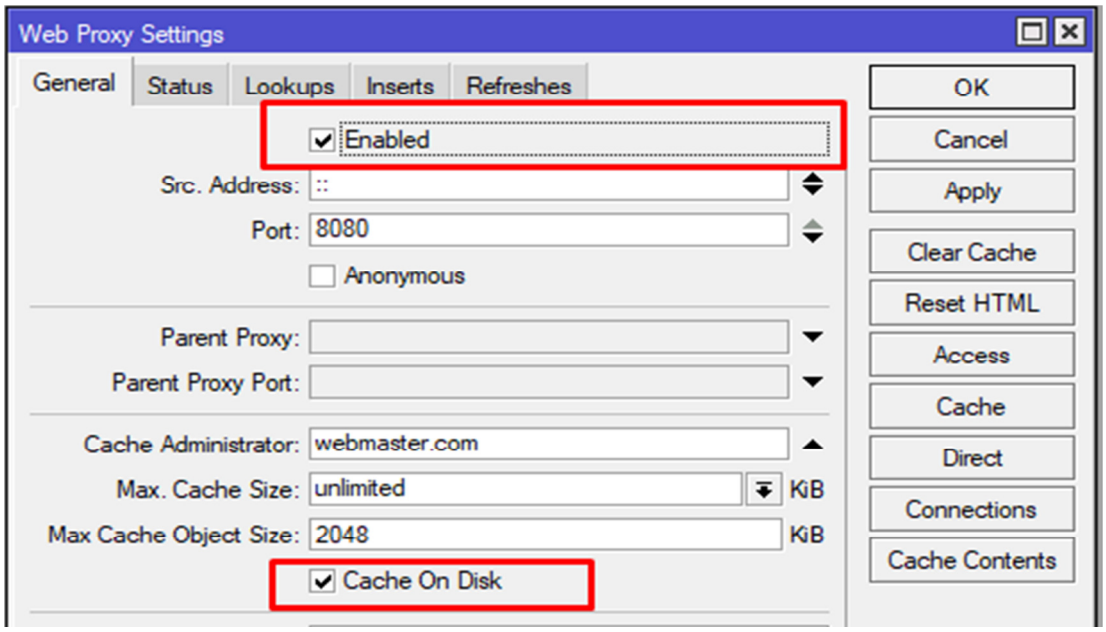


Gambar 5**.** Tampilan Hasil *Rule Firewall*

Pada Gambar 5 dapat dilihat parameter chain *block* sudah memblok port yang dirancang. Dalam daftar *port* yang diberi akses salah satunya port 8291 yang berguna untuk meremote router menggunakan winbox dan *port* yang digunakan untuk melakukan ping. Setelah itu akan dilakukan pengujian menggunakan aplikasi Zenmap Nmap GUI untuk mengetahui *port* jaringan yang masih terbuka.

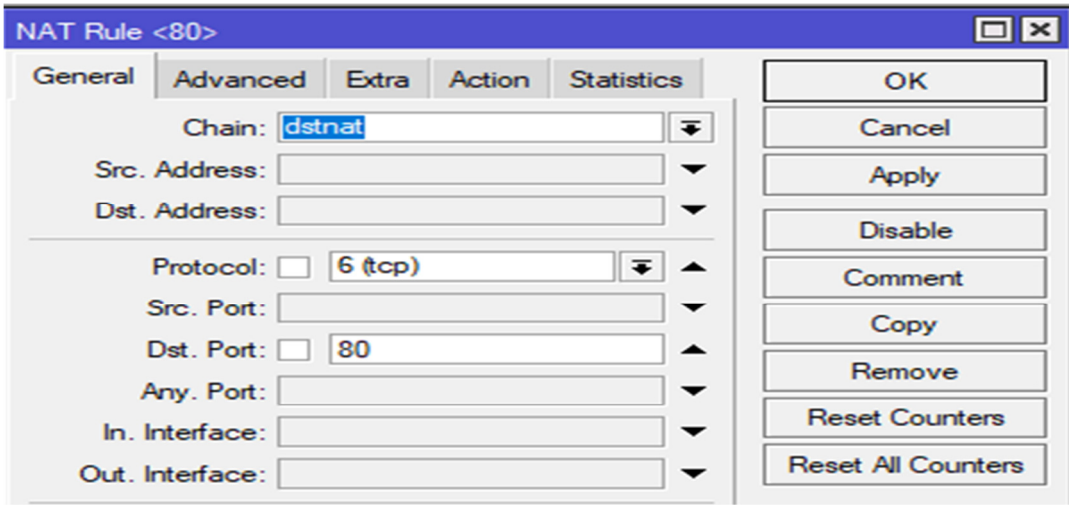
b. Proses Block Situs

Pada proses ini *client* saat mengakses sebuah situs akan dilakukan pemfilteran jika situs yang diakses tidak di *block* oleh admin maka situs tersebut akan dapat di akses dan jika situs yang diakses di *block* maka *client* tidak dapat mengakses situs tersebut atau akan dialihkan ke domain lain. Dalam proses ini akan menggunakan *web proxy* dimana *firewall* akan me *redirect* port 80 ke 8080 (*web proxy*). Pada aplikasi Winbox tampilan awal pilih menu *IP* kemudian pilih *Web Proxy*.



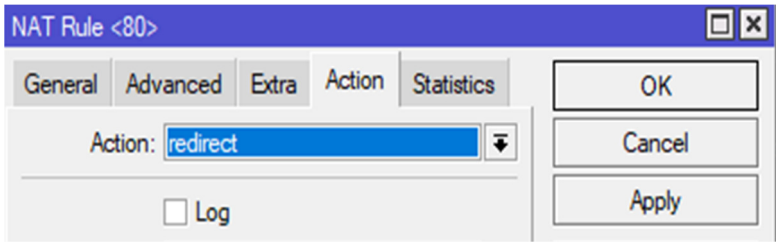
Gambar 6. Tampilan *Setting Web Proxy*

Gambar 6 adalah tampilan *setting* pada *Web Proxy* kemudian centang pada bagian *Enabled* dan *Cache On Disk* lalu klik *Apply*.



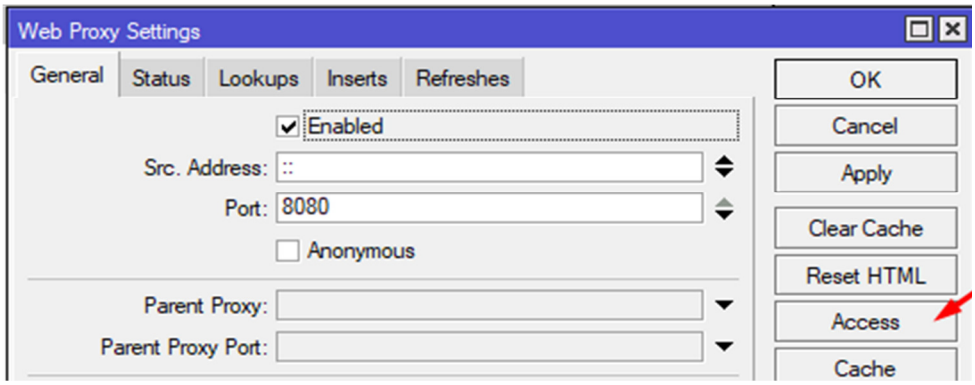
Gambar 7. Tampilan *Setting NAT Rule*

Pada Gambar 7 Tampilan NAT *Rule* isi *Chain* dengan dstnat kemudian Protocol 6 tcp, dan Dst.Port 80 lalu klik *Apply*.



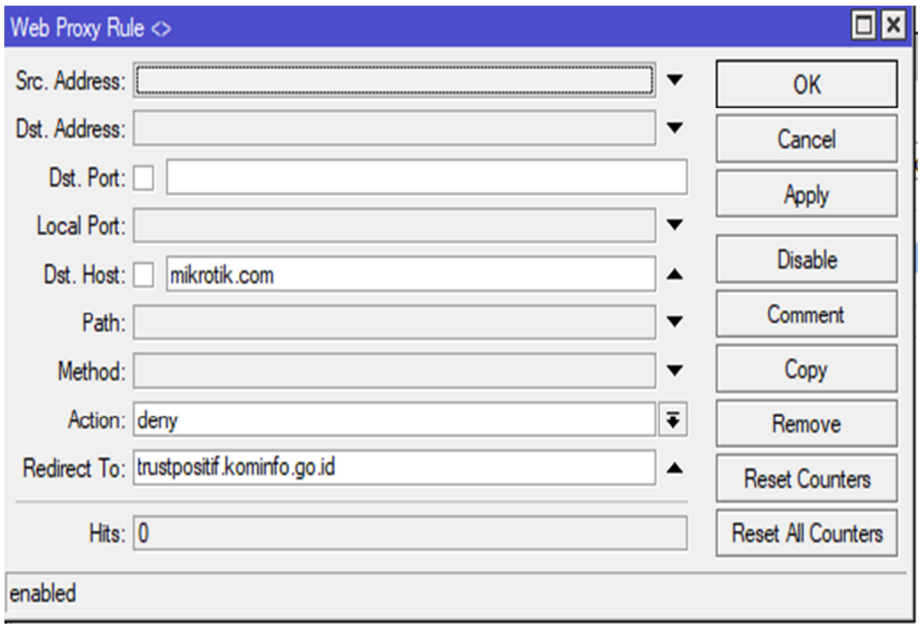
Gambar 8. Tampilan *Tab Action NAT Rule*

Gambar 8 pada tab *Action* isi dengan *redirect* kemudian pada tab *To Ports* 8080 yang merupakan *port* dari *Web Proxy* klik *Apply* lalu *OK*.



Gambar 9. Tampilan *Web Proxy Setting*

Pada Gambar 9 tampilan web proxy *setting* klik *Acces.*

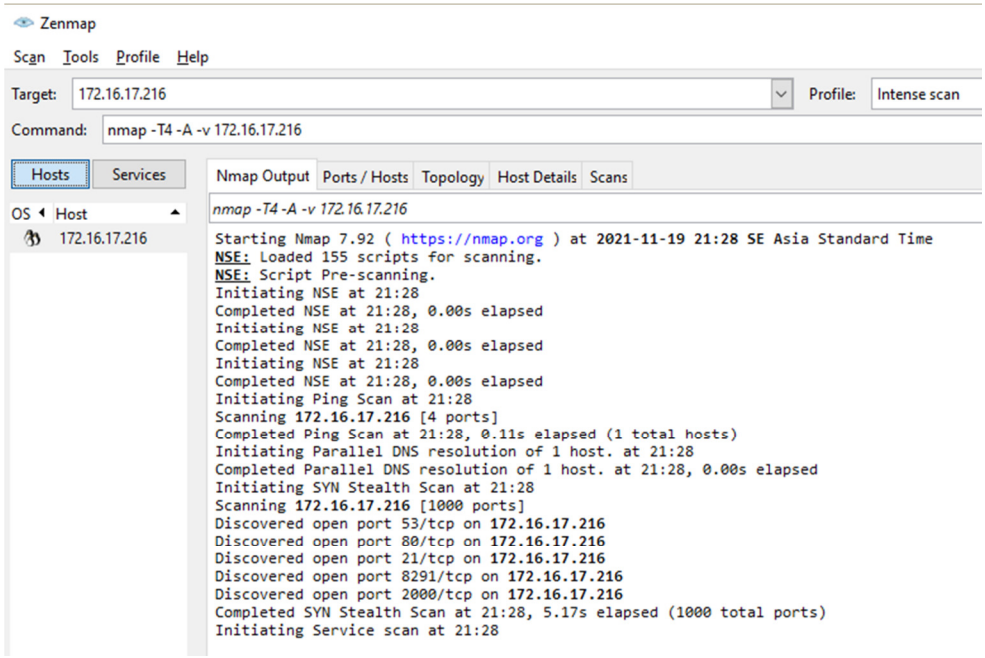


Gambar 10. Tampilan *Web Proxy Rule*

Gambar 10 merupakan tampilan *web proxy rule* pada Dst. Host isi dengan domain situs mikrotik.com kemudian pada bagian *Action* pilih *deny*. Pada opsi *Redirect To* di isi dengan trustpositif.kominfo.go.id dimana situs akan dialihkan ke domain tersebut.

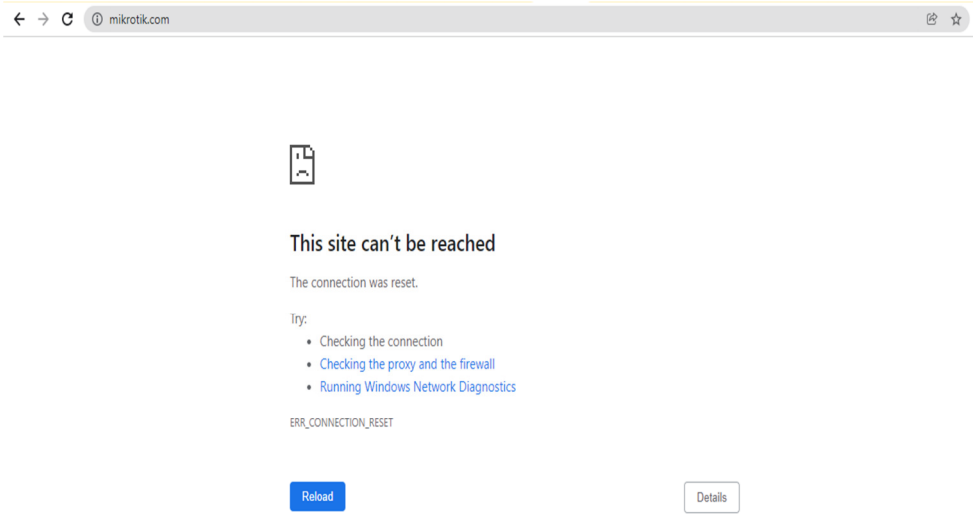
c. Pengujian dan Analisis

Pengujian dilakukan menggunakan cara *scan port* berdasarkan ip 172.16.17.216 dari *gateway* pada *ether 2* menggunakan aplikasi Nmap pada metode *port blocking* pada penelitian ini. Hasil pengujian menggunakan Nmap sebagai berikut:



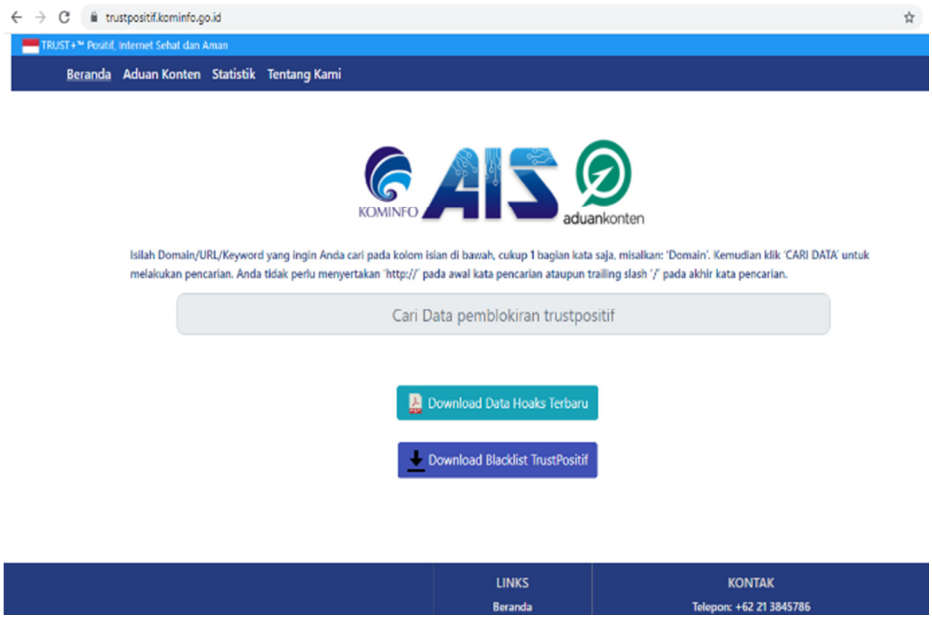
Gambar 11. Hasil *Scan Nmap*

Pada Gambar 11 merupakan proses *scanning* menggunakan *ip address* 172.16.17.216 yang merupakan *ip gateway* untuk melihat sisa *port* yang terbuka. Sehingga proses input *rule firewall* pada sistem keamanan jaringan menggunakan metode *port blocking* sudah berhasil memblokir akses *port* yang bisa di masuki oleh peretas, dan hanya menyisakan *port* komunikasi yang aman digunakan. Seperti *port* 8291 untuk meremote router menggunakan winbox, *port* 53 DNS, *port* 80 default koneksi http, *port* 21 FTP, dan *port* 2000 Cisco-sccp. Pengujian pada situs yang telah telah diblok menggunakan *web proxy* diuji dengan menggunakan *browser*.



Gambar 12. Tampilan Situs yang Diblok

Saat mengakses domain mikrotik.com akan menghasilkan tampilan seperti pada Gambar 12 karena aksesnya diblok sehingga halaman *web* tidak akan muncul. Pada akses domain http maka situs akan otomatis dialihkan ke alamat domain trustpositif.kominfo.go.id. seperti pada Gambar 13



Gambar 13. Tampilan *Output* Pengalihan Situs

Gambar 13 menunjukkan alamat domain pengalihan situs yang sudah di setting pada tab *Web Proxy Rule*. Situs dapat dialihkan karena domain yang di masukan adalah http.

4. KESIMPULAN

Berdasarkan penelitian yang dilakukan berjudul Sistem Keamanan Jaringan Menggunakan *Firewall* dengan Metode *Port Blocking* dan *Firewall Filtering* dapat diambil kesimpulan bahwa penerapan metode *port blocking* ini dapat meminimalisir risiko masuknya *virus* dan *malware* yang dapat memicu serangan pada suatu jaringan. Sistem yang dirancang untuk mengamankan lalu lintas paket data melalui router dengan proses pemfilteran sesuai dengan kententuan yang dirancang. Sistem yang diterapkan pada proses *block* situs yang dihasilkan adalah jika situs yang diblok https maka halaman tidak akan muncul tetapi jika situs yang di block http maka dapat dialihkan ke alamat domain lainnya sesuai dengan *rule* pada MikroTik yang sudah ditentukan.

5. SARAN

Untuk penelitian lebih lanjut perlu dikembangkan penambahan *port* yang akan diblok dan mengkaji lebih dalam lagi mengenai keamanan jaringan menggunakan *firewall* sehingga dapat diketahui efektifitas penerapan dari sistem keamanan jaringan.

UCAPAN TERIMAKASIH

Penulis mengucapkan terimakasih kepada Tuhan Yang Maha Esa, kedua orang tua, dan saudara serta kepada pembimbing ibu Dr. Indrastanti R. Widiasari, M.T. atas bimbingan dan dukungan dalam melakukan penulisan jurnal sehingga bisa berjalan dengan baik.

DAFTAR PUSTAKA

[1] M. U. S. Saleh Opim Salim; Sinaga, Hendra H, *"Implementasi dan Perbandingan Firewall Security Menggunakan Mikrotik dan M0n0wall pada Local Area Network," Alkhawarizmi*, No. Vol 1, No 1 (2012): Jurnal Alkhawarizimi, pp. 1–8, 2012.

[2] A. Hikmaturokhman, A. Purwanto, and R. Munadi, *"Analisis Perancangan dan Implementasi Firewall dan Traffic Filtering Menggunakan Cisco Router," Semin. Nas. Inform.*, Vol. 1, No. 3, pp. 1–8, 2015.

[3] I. G. K. O. Mardiyana, *"Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik pada Laboratorium Komputer STIKOM Bali," STMIK Stikom*, No. 86, pp. 804–807, 2015.

[4] I. Anugrah and R. H. Rahmanto, *"Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone," PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, Vol. 5, No. 2, pp. 91–106, 2018, doi: 10.33558/piksel.v5i2.271.

[5] S. Hidayatulloh, *"Analisis dan Optimalisasi Keamanan Jaringan Menggunakan Protokol Ipsec," J. Inform.*, Vol. 1, No. 2, pp. 93–104, 2014, doi: 10.31311/ji.v1i2.47.

[6] A. Tedyyana and S. Supria, *"Perancangan Sistem Pendeteksi dan Pencegahan Penyebaran Malware Melalui SMS Gateway," INOVTEK Polbeng - Seri Inform.*, Vol. 3, No. 1, p. 34, 2018, doi: 10.35314/isi.v3i1.340.

[7] M. G. Kaur and N. Kaur, *"Penetration Testing – Reconnaissance with NMAP Tool," Int. J. Adv. Res. Comput. Sci.*, Vol. 8, No. 3, pp. 844–846, 2017.

[8] M. Anif, S. Hws, and M. D. Huri, *"Penerapan Intrusion Detection System (IDS) Dengan Metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang," J. TELE, Vol. 13 Nomor 1*, Vol. 13, No. 1, pp. 25–30, 2015, doi: 10.1155/2017/3680758.

[9] M. S. Maulana and M. Ryansyah, *"Malware Security Menggunakan Filtering Firewall Dengan Metode Port Blocking pada Mikrotik RB 1100AHx2," J. Sist. dan Teknol. Inf.*, Vol. 6, No. 3, p. 112, 2018, doi: 10.26418/justin.v6i3.26716.

[10] W. Wahyudi, *"Membangun Proxy Server Cv Global Max Menggunakan Sistem Operasi Linux Blankon 6.0 Ombilin Sebagai Manajemen Akses Jaringan," Edik Inform.*, Vol. 1, No. 1, pp. 63–71, 2017, doi: 10.22202/ei.2014.v1i1.1441.