Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 4 No. 1 Juli 2022 Hal. 427-431
DOI : https://doi.org/10.47233/jteksis.v4i2.561
ISSN :**2655-8238**

SISTEM KEAMANAN JARINGAN KOMPUTER BRIDGE FIREWALL MENGGUNAKAN ROUTER BOARD MIKROTIK RB750

Ahmad Robbahul Barra[1)], Arif Rahman Sujatmika[2)], Izzatul Umami[3)].
[123]Fakultas Teknik, Universitas Darul Ulum Jombang, Jl. Gus Dur No.29A, Mojongapitindah, Mojongapit, Kec. Jombang, Kabupaten Jombang, Jawa Timur 61419
email: b412ra@gmail.com, arifsujatmika@gmail.com, izzatulumami@gmail.com

Abstract

Currently to get a strong firewall is still constrained by expensive costs. Only large companies or agencies can obtain these devices, while small and medium-sized companies are still unable to obtain reliable firewall devices. Therefore, it is necessary to need inexpensive security devices or firewalls for medium and small companies and agencies to protect computer networks from outside interference. Mikrotik RB 750 is a router that can be used to make a network security system that is reliable, inexpensive and easy to configure. In this study, the author tries to provide a network security system solution using Packet Filter Firewall with the router in bridge mode and compares network security systems in other research journals. From the results of the comparison, several series of network security protections are produced, namely changing the proxy to bridge mode, IP address protection, content protection with mangle, Mikrotik device protection, traceroute protection, port scanner protection, Bogon IP protection, and Bruteforce FTP protection. After conducting a series of tests from the results of the network protection setup using the Mikrotik RB 750 in bridge mode, the authors conclude that not all packets that pass through the bridge firewall device can be filtered. One of them is ICMP flooding packets. Mikrotik devices with Firewall bridge mode cannot calculate the number of ICMP packets that pass, so the author blocks ICMP packets with the 8:0 option (echo request) that goes to the local network.

Keywords: *Network Security, Firewall, RB750, Mikrotik, Packet Filtering*

Abstrak

Saat ini untuk mendapatkan firewall yang tangguh masih terkendala oleh biaya mahal. Hanya perusahaan atau instansi besar saja yang dapat memperoleh perangkat terebut, semantara perusahaan kecil dan menengah masih belum bisa untuk mendapatkan perangkat firewall yang handal. Oleh karena itu perlu dibutuhkan perangkat keamanan atau firewall yang murah untuk perusahaan dan instansi menengah dan kecil untuk melindungi jaringan komputer dari gamgguan luar. Mikrotik RB 750 adalah sebuah router yang dapat digunakan untuk menjadikan sistem keamanan jaringan yang handal, murah dan mudah dalam mengkonfigurasi. Pada penelitian ini penulis mencoba memberikan solusi sistem keamanan jaringan menggunakan Packet Filter Firewall dengan router berada pada mode bridge serta membandingkan sistem keamanan jaringan pada jurnal penelitian yang lain. Dari hasil perbandingan tersebut menghasilkan beberapa rangkaian proteksi keamanan jaringan yaitu merubah mikrotik menjadi mode bridge, proteksi IP address, proteksi konten dengan mangle, proteksi perangkat mikrotik, proteksi traceroute, proteksi port scanner, proteksi Bogon IP, dan proteksi FTP Bruteforce. Setelah melakukan serangkaian tes dari hasil setup proteksi jaringan menggunakan mikrotik RB 750 pada mode bridge ini, penulis menyimpulkan tidak semua paket yang lewat pada perangkat bridge firewall dapat disaring. Salah satunya adalah paket ICMP flooding. Perangkat Mikrotik dengan mode bridge Firewall tidak dapat melakukan perhitungan jumlah paket ICMP yang lewat, sehingga penulis melakukan pemblokiran paket ICMP dengan opsi 8:0 (echo request) yang menuju ke jaringan lokal.

Kata kunci: *Keamanan Jaringan, Firewall, RB750, Mikrotik, Packet Filtering*

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 4 No. 1 Juli 2022 Hal. 427-431
DOI : https://doi.org/10.47233/jteksis.v4i2.561
ISSN :**2655-8238**

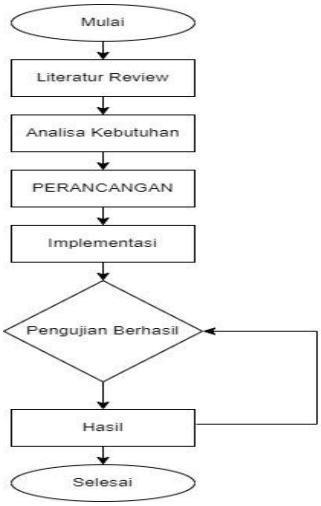
PENDAHULUAN

Internet merupakan sebuah jaringan komputer terbuka di dunia, konsekuensi yang harus di tanggung adalah tidak ada jaminan kemanan bagi jaringan yang terhubung di internet. Artinya jika operator jaringan tidak hati-hati dalam mengatur sistemnya, maka kemungkinan besar jaringan yang terhubung ke internet akan dengan mudah dimasuki orang yang tidak diundang dari luar. Dengan memanfaatkan celah-celah dan port-port yang terbuka pada jaringan, para peretas dapat dengan mudah masuk kejaringan dan mengganggunya.maka dari itu, untuk menanggulangi hal tersebut perlu dibutuhkan sistem keamanan jaringan atau firewall. [1]

Saat ini untuk mendapatkan firewall yang tangguh masih terkendala oleh biaya mahal. Hanya perusahaan atau instansi besar saja yang dapat memperoleh perangkat terebut, semantara perusahaan kecil dan menengah masih belum bisa untuk mendapatkan perangkat firewall yang mumpuni itu. Oleh karena itu perlu dibutuhkan perangkat keamanan atau firewall yang murah untuk perusahaan dan instansi menengah dan kecil untuk melindungi jaringan komputer dari gamgguan luar. Mikrotik adalah sebuah sistem operasi yang dapat digunakan untuk menjadikan komputer menjadi router network yang handal, murah dan mudah dalam mengkonfigurasi. [2].

METODE PENELITIAN

Literature review ini menganalisis artikel yang relevan dan berfokus pada metode keamanan jaringan menggunakan mikrotik yang menghasilkan sistem keamanan jaringan yang handal. Adapun artikel yang digunakan pada literature review ini adalah artikel yang didapatkan dengan menggunakan Google Scholar dengan memasukkan kata kunci "Keamanan Jaringan", "Mikrotik" "Sistem jaringan", dan "RB750". Artikel yang digunakan adalah 3 artikel yang diterbitkan enam tahun terakhir.

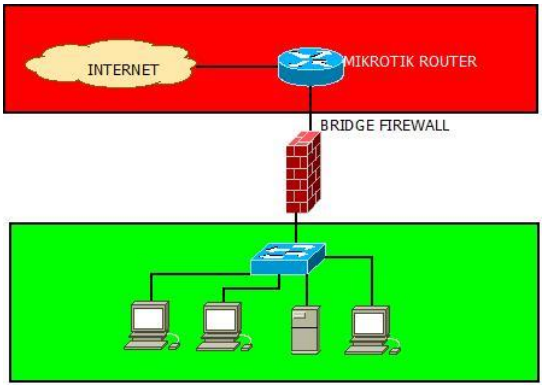


Metode yang digunakan kali ini yaitu penyaringan paket atau packet filtering. Packet filtering adalah salah satu jenis teknologi keamanan yang digunakan untuk mengatur paket-paket apa saja yang diizinkan masuk kedalam sistem atau jaringan dan paket paket apa saja yang diblokir. Packet filtering umumnya digunakan untuk memblokir lalu lintas mencurigakan yang datang dari alamat IP yag dicurigai, Nomor port TCP yang mencurigakan, jenis protocol aplikasi yang mencurigakan, dan kriteria lainnya. Akhir-akhir ini, fitur packet filtering telah dimasukkan ke dalam banyak sistem operasi (IPTables dalam GNU/Linux, dan IP Filter dalam windows)..

Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 4 No. 1 Juli 2022 Hal. 427-431
DOI : https://doi.org/10.47233/jteksis.v4i2.561 ISSN :**2655-8238**

HASIL DAN PEMBAHASAN

Dalam tugas akhir ini perangkat bridge diletakkan diantara modem dan jaringan privat, lalu firewall diisikan pada perangkat bridge tersebut tanpa mengubah IP address yang masuk maupun keluar dari perangkat bridge.




```
[admin@MikroTik] > /interface bridge print
Flags: X - disabled, R - running
 0  R name="bridge1" mtu=auto actual-mtu=1500 l2mtu=1598 arp=enabled
      mac-address=E4:8D:8C:C5:30:ED protocol-mode=rstp priority=0x8000
      auto-mac=yes admin-mac=00:00:00:00:00:00 max-message-age=20s
      forward-delay=15s transmit-hold-count=6 ageing-time=5m
[admin@MikroTik] >
```

Pada tampilan diatas menunjukkan bahwa huruf " R " yang berada dibawah tulisan *Flags*, menandakan bahwa *bridge* dalam kondisi aktif.

Pengujian Proteksi Tracerout

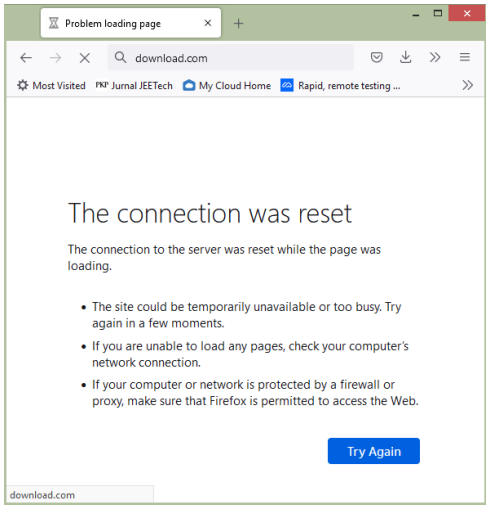
Untuk pengujian penulis menjalankan perintah tracert ke www.google.com, seperti tampilan di bawah ini.

```
C:\Users\admin>tracert www.google.com

Tracing route to forcesafesearch.google.com [216.239.38.120]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12    70 ms    63 ms    74 ms  216.239.38.120

Trace complete.
```

hasil fungsi *traceroute* tidak dapat menampilkan *IP router* yang dilalui, dan hanya dapat menampilkan *IP* tujuan (www.google.com) saja.

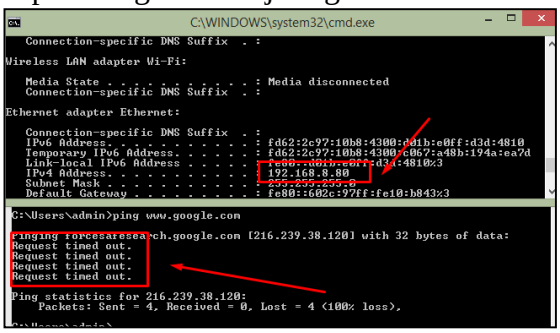
Pengujian Proteksi Konten

Untuk pengujian, penulis memberikan perintah ping dan mengakses dari web browser ke konten download. Hasilnya adalah akses ke web ke alamat www.download.com tidak dapat dijalankan.



Pengujian Proteksi IP Address

Pada pengujian proteksi *IP address*. Hanya *IP Address* yang dijinkan saja yang dapat mengakses ke jaringan.

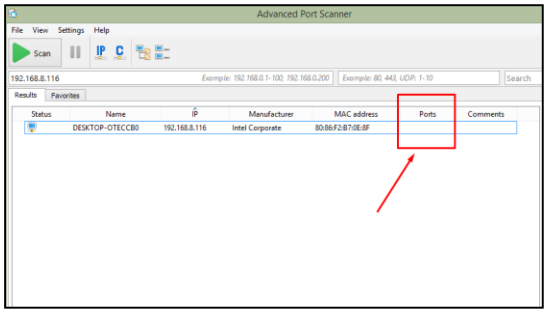


Karena IP address sumber tidak sama dengan IP address yang tertulis pada list "ournetwork", maka tidak diijinkan untuk akses pada jaringan.

Pengujian Port Scanner

Untuk pengujian, penulis menggunakan aplikasi Advanced Port Scanner. Berikut adalah hasilnya

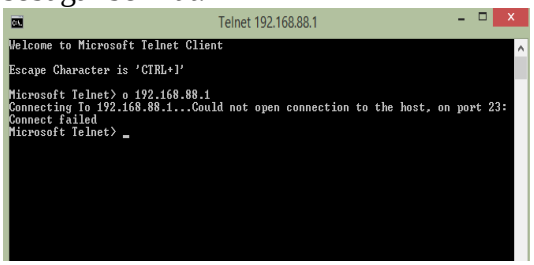
Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 4 No. 1 Juli 2022 Hal. 427-431
DOI : https://doi.org/10.47233/jteksis.v4i2.561
ISSN :**2655-8238**



Pada pengujian tersebut, dilakukan scanning port ke alamat 192.168.8.116 yang terhubung pada port 1 (ether 1 gateway) menggunakan aplikasi Advanced Port Scanner, tetapi tidak dapat menampilkan port yang terbuka.

Pengujian Proteksi Perangkat Mikrotik.

Pengujian proteksi perangkat perangkat menggunakan telnet. Hasilnya sebagai berikut.



Karena host menggunakan IP address 192.168.88.120 yang tidak terdaftar pada list remote, maka host tersebut tidak dapat melakukan remote pada perangkat Mikrotik.

Hasil Proteksi Bogon IP

Tampilan berikut merupakan hasil script untuk list Bogon IP.

```
[admin@MikroTik] > /ip firewall address-list print
Flags: X - disabled, D - dynamic
 #    LIST                ADDRESS
 0    ournetwork          192.168.137.1
 1    list-bogon          0.0.0.0/8
 2    list-bogon          127.0.0.0/8
 3    list-bogon          224.0.0.0/8
 4    list-bogon          224.0.0.0/4
 5    list-bogon          10.0.0.0/8
 6    list-bogon          172.16.0.0/12
 7    list-bogon          192.168.0.0/16
 8    list-bogon          192.0.0.0/24
 9    list-bogon          169.254.0.0/16
10    list-bogon          192.0.2.0/24
11    list-bogon          198.18.0.0/15
12    list-bogon          198.51.100.0/24
13    list-bogon          203.0.113.0/24
```

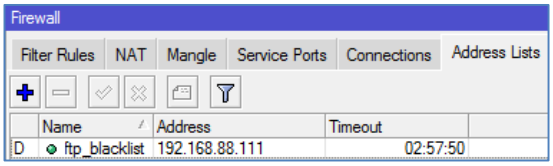
IP address yang tertulis dalam list bogon adalah IP bogon atau IP yang tidak dialokasikan. Untuk hasil proteksinya adalah sebagai berikut.

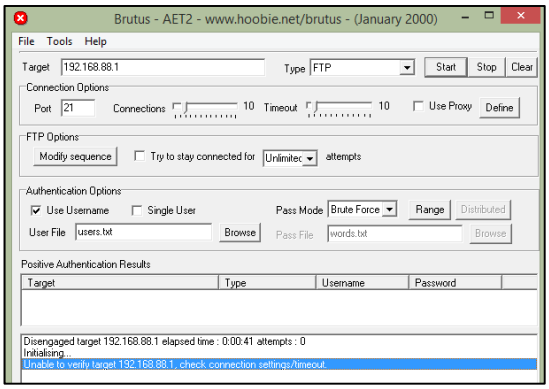
```
chain=input action=drop src-address-list=list-bogon
in-interface=ether1-gateway log=no log-prefix=""
```

Pengujian Proteksi FTP Bruteforce

Untuk melakukan pengujian, penulis terlebih dahulu melakukan penggantian user dan password default Mikrotik dengan user = admin dan password = aa.

Selanjutnya untuk pengujian proteksi Brute Force penulis menggunakan aplikasi Brutus.





Maksud dari tampilan tersebut adalah ketika aplikasi Brutus melakukan login dengan user = admin, percobaan *bruteforce login* dihentikan oleh perangkat dengan tanda tulisan timeout dan throttle berwarna merah.

SIMPULAN

Berdasarkan uraian pada bab-bab sebelumnya, maka penulis menarik kesimpulan bahwa Metode yang digunakan pada tugas akhir ini adalah packet filtering, tetapi tidak semua paket yang lewat pada perangkat bridge firewall dapat disaring. Salah satunya adalah paket

 ISSN :**2655-8238**

ICMP flooding. Perangkat Mikrotik dengan mode bridge Firewall tidak dapat melakukan perhitungan jumlah paket ICMP yang lewat, sehingga penulis melakukan pemblokiran paket ICMP dengan opsi 8:0 (echo request) yang menuju ke jaringan lokal.

UCAPAN TERIMAKASIH

Dalam penelitian ini tidak lepas dari dukungan berbagai pihak dan pada kesempatan ini penulis ingin mengucapkan terima kasih kepada pihak-pihak yang terlah membantu, terutama kepada :

1. Ketua Yayasan Universitas Darul Ulum Jombang.
2. Dekan Fakultas Teknik Universitas Darul Ulum Jombang

DAFTAR PUSTAKA

Sujito, Fatkhur Roji, "Sistem Keamanan Internat Dengan Menggunakan IP Tables Sebagai Firewall," *Sistem Informasi STMIK Pradnya Paramita. Jurnal Ilmiah DINAMIKA DOTCOM Vol. 1 No.1 Januari 2010,* [Online]. Available: website: https://adoc.pub/sistem-keamanan-internet-dengan-menggunakaniptables-sebagai.html.

Haerudin, "Analisa dan Implementasi Sistem Keamanan Router Mikrotik dari Serangan *Winbox Exploitation*, *Brute-Force*, DoS" Universitas Internasional Batam. *Jurnal Media Informatika Budidarma Volume 5, Nomor 3, Juli 2021, Page 848-855,* [Online]. Available Online at https://ejurnal.stmikbudidarma.ac.id/index.php/mib.

Ino Anugrah, R.Hengki Rahmanto, "Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone" Universitas Islam 45. *Jurnal Penelitian Ilmu Komputer, Sistem Embedded & Logic 5(2) : 91-106 (2017).*

Fadlil, A., Riadi, I., & Aji, S. (2017). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. *Jurnal Ilmu Teknik Elektro Komputer dan Informatika (JITEKI) , 3* (1), 1119

Amarudin, A., & Ulum, F. (2018). Desain Keamanan Jaringan Pada Mikrotik *Router* Os Menggunakan Metode Port Knocking. *JURNAL TEKNOINFO, 12* (2), 72-75.

Muzakir, A., & Ulfa, M. (2019). Analisis Kinerja *Packet* Filtering Berbasis Mikrotik *Router*board Pada Sistem Keamanan Jaringan. *Simetris : Jurnal Teknik Mesin, Elektro dan Ilmu Komputer, 10* (1), 15-20

Juardi, D. (2017). Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus. *SYNTAX: Jurnal Informatika , 6* (1), 11-19.