

# SISTEM KEAMANAN JARINGAN KOMPUTER BRIDGE FIREWALL

*by Izzatul Umami*

---

**Submission date:** 31-Aug-2022 11:04PM (UTC-0400)

**Submission ID:** 1890413730

**File name:** SISTEM\_KEAMANAN\_JARINGAN\_KOMPUTER\_BRIDGE\_FIREWALL.docx (169.99K)

**Word count:** 1490

**Character count:** 9476

## **SISTEM KEAMANAN JARINGAN KOMPUTER BRIDGE FIREWALL MENGUNAKAN ROUTER BOARD MIKROTIK RB750**

**Ahmad Fabbahul Barra<sup>1)</sup>, Arif Rahman Sujatmika<sup>2)</sup>, Izzatul Umami<sup>3)</sup>.**

<sup>123</sup>Fakultas Teknik, Universitas Darul Ulum Jombang, Jl. Gus Dur No.29A, Mojongapitindah, Mojongapit,  
Kec. Jombang, Kabupaten Jombang, Jawa Timur 61419  
email: [b412ra@gmail.com](mailto:b412ra@gmail.com), [arifsujatmika@gmail.com](mailto:arifsujatmika@gmail.com), [izzatulumami@gmail.com](mailto: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 tersebut, sementara 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 gangguan 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

7  
This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license



## 2 PENDAHULUAN

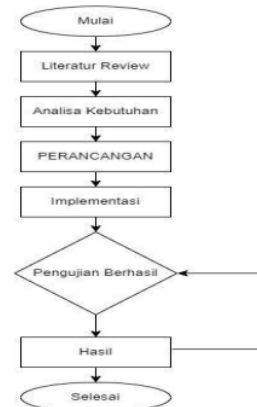
Internet merupakan sebuah jaringan komputer terbuka di dunia, konsekuensi yang harus di tanggung adalah tidak ada jaminan kewanaman bagi jaringan yang terhubung di internet. Artinya jika operator jaringan tidak hati-hati dalam mengatur sistemnya, maka kemungkinan besar jaringan yang terhubung ke internet 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 ke jaringan dan menggangukannya. 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 tersebut, sementara 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 gangguan luar. Mikrotik adalah sebuah sistem operasi yang dapat digunakan untuk menjadikan komputer menjadi router network yang handal, murah dan mudah dalam mengkonfigurasi. [2].

## 3 METODE PENELITIAN

Literature review ini menganalisis artikel yang relevan dan berfokus pada metode keamanan jaringan menggunakan mikrotik yang menghasilkan sistem

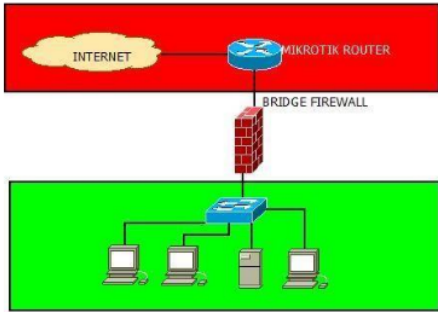
5  
keamanan jaringan yang handal. Adapun artikel yang digunakan pada literature review ini adalah artikel yang didapatkan dengan menggunakan Google Scholar dengan memasukkan kata kunci “Keamanan Jaringan”, “Mikrotik” “Sistem jaringan”, dan “RB750”. Artikel yang digunakan adalah 3 artikel yang diterbitkan 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 yang dicurigai, Nomor port TCP yang mencurigakan, jenis protocol aplikasi yang mencurigakan, dan kriteria lainnya. Akhirnya ini, fitur packet filtering telah dimasukkan ke dalam banyak sistem operasi (IPTables dalam GNU/Linux, dan IP Filter dalam windows)..

### 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=C4:8D:8C:C5:30:ED protocol-mode=rsmp 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

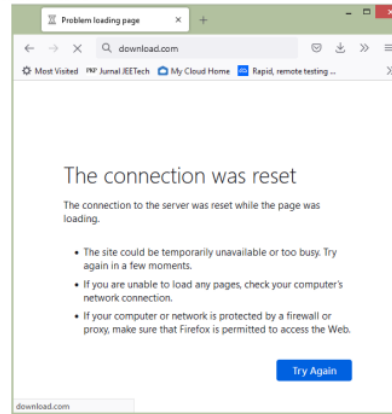
Untuk pengujian penulis menjalankan perintah *tracert* ke [www.google.com](http://www.google.com), seperti tampilan di bawah ini.

```
C:\Users\admin>tracert www.google.com
Tracing route to forncasafesearch.google.com [216.239.38.120]
over a maximum of 30 hops:
 0  * * * * Request timed out.
 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](http://www.google.com)) saja.

### Pengujian Proteksi Konten

Untuk pengujian, penulis memberikan perintah *ping* dan mengakses dari web browser ke konten *download.com*. Hasilnya adalah akses ke web ke alamat [www.download.com](http://www.download.com) tidak dapat dijalankan.



### Pengujian Proteksi IP Address

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

```
C:\WINDOWS\system32\cmd.exe
Connection-specific DNS Suffix  : 
Wireless LAN adapter Wi-Fi: 
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  : 
Ethernet adapter Ethernet: 
Connection-specific DNS Suffix  : 
IP Address . . . . . : f86212c9710b8c300c04b1a0ff1d3d4810
Temporary IP Address . . . . . : f86212c9710b8c300c04b1a0ff1d3d4810
Link-local IPv6 Address . . . . . : fe80::c04b1a0ff1d3d4810::
IPv4 Address . . . . . : 172.168.4.80
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::c04b1a0ff1d3d4810::

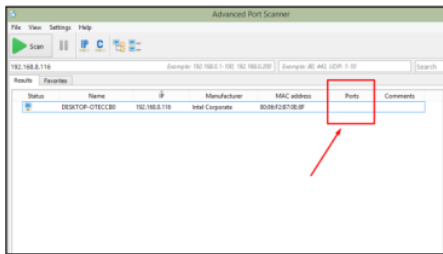
C:\Users\admin>ping www.google.com
Pinging forncasafesearch.google.com [216.239.38.120] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 216.239.38.120:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    (Minimum = 0ms, Maximum = 0ms, Average = 0ms)
```

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

### Pengujian Port Scanner

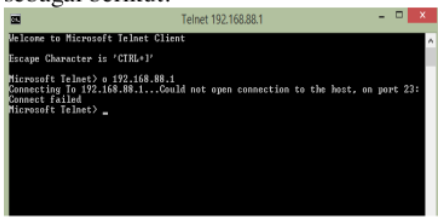
Untuk pengujian, penulis menggunakan aplikasi *Advanced Port Scanner*. Berikut adalah hasilnya



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.*

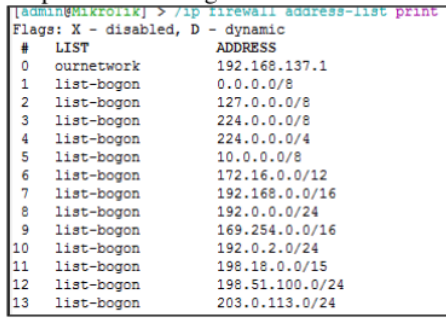
Pengujian proteksi perangkat menggunakan telnet. Hasilnya sebagai berikut.



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.



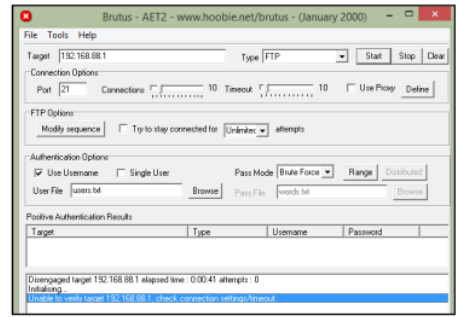
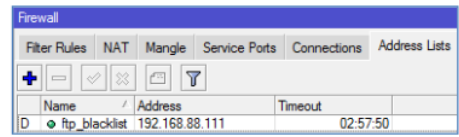
IP address yang tertulis dalam list bogon adalah IP bogon atau IP yang tidak dialokasikan. Untuk hasil proteksinya adalah sebagai berikut.

```
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 brute force login dihentikan oleh perangkat dengan tanda tulisan timeout dan throttle berwarna merah.

8  
**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



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 TERIMA KASIH

6  
Dalam penelitian ini tidak lepas dari dukungan berbagai pihak dan pada kesempatan ini penulis ingin mengucapkan terima kasih kepada pihak-pihak yang telah membantu, terutama kepada :

- 10  
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: <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://ejournal.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 Routerboard 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.

# SISTEM KEAMANAN JARINGAN KOMPUTER BRIDGE FIREWALL

## ORIGINALITY REPORT

17%

SIMILARITY INDEX

12%

INTERNET SOURCES

9%

PUBLICATIONS

6%

STUDENT PAPERS

## PRIMARY SOURCES

1	Mochzen Gito Resmi, Teguh Iman Hermanto, Miftah Al Ghozali. "Product Recommendation System Application Using Web-Based Equivalence Class Transformation (Eclat) algorithm", SinkrOn, 2022 Publication	6%
2	<a href="http://www.unsri.ac.id">www.unsri.ac.id</a> Internet Source	3%
3	<a href="http://core.ac.uk">core.ac.uk</a> Internet Source	1%
4	<a href="http://repository.undar.ac.id">repository.undar.ac.id</a> Internet Source	1%
5	<a href="http://jurnal.staimuhblora.ac.id">jurnal.staimuhblora.ac.id</a> Internet Source	1%
6	<a href="http://www.coursehero.com">www.coursehero.com</a> Internet Source	1%
7	<a href="http://123dok.com">123dok.com</a> Internet Source	1%
8	<a href="http://accountance.wordpress.com">accountance.wordpress.com</a> Internet Source	

1 %

9

journal.um-surabaya.ac.id

Internet Source

1 %

10

media.neliti.com

Internet Source

1 %

Exclude quotes On

Exclude matches Off

Exclude bibliography On



# SISTEM KEAMANAN JARINGAN KOMPUTER BRIDGE FIREWALL

GRADEMARK REPORT

FINAL GRADE

**/0**

GENERAL COMMENTS

**Instructor**

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5