

AKSELERATOR

Vol. 4 No. 2 pp.87-97

pISSN. 2541-1268

eISSN. 2721-7779

## IMPLEMENTASI MONITORING JARINGAN FIREWALL FILTERING BERBASIS WEB SERVICE DI PT SARI WANGI MENTARI

Yansen<sup>1</sup>, Rino<sup>2</sup>

Fakultas Sains dan Teknologi, Universitas Buddhi Dharma  
Jalan Imam Bonjol No. 41, Tangerang, Indonesia

Email: [1yansenlim9@gmail.com](mailto:1yansenlim9@gmail.com), [2mr.rino85@gmail.com](mailto:2mr.rino85@gmail.com)

### Abstrak

Monitoring merupakan bagian penting dalam suatu keamanan jaringan dimana akses lalu lintas internet banyak digunakan dalam dunia pendidikan maupun pekerjaan. Dalam hal ini Monitoring sangat diperlukan untuk memantau aktivitas pada perangkat jaringan. Penelitian ini membahas tentang sistem Monitoring jaringan menggunakan Web service dan melakukan keamanan dengan metode port blocking dan firewall filtering. Penelitian ini menggunakan router Mikrotik dan aplikasi Winbox meremote router untuk membuat rule firewall dan menggunakan Xampp untuk mendukung web service. Rule firewall berisi blocking port komunikasi yang rawan terhadap serangan virus dan malware, dan pembatasan akses lalu lintas internet menggunakan web proxy dengan memblock situs http dan https dalam suatu jaringan. Hasil penelitian ini diuji menggunakan aplikasi Nmap 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, Web Service*

### Latar Belakang

Pada saat ini kemajuan teknologi berkembang dengan sangat cepat, terlebih dengan kemajuan teknologi komputer, pada kehidupan sekarang ini penggunaan teknologi komputer dan web sangat dibutuhkan dalam kehidupan manusia, begitu pula dengan keberadaan teknologi komputer dan web yang telah di terakhir menjadi kebutuhan hidup manusia yang tidak dapat dipisahkan dengan dorongan ini individu dapat lebih efektif memeriksa jenis informasi yang berbeda. Sistem komputer tidak begitu berkembang di dalam perusahaan, hampir di setiap perusahaan terdapat jaringan komputer yang dapat menghubungkan satu komputer dengan komputer lainnya sehingga dapat berkomunikasi dan bertukar data untuk mempersingkat dan mempercepat pekerjaan di dalam perusahaan.

Namun dalam perkembangan teknologi, banyak orang yang menyalahgunakannya, orang-orang yang tidak memiliki hak untuk mencoba masuk ke dalam sistem komputer untuk merusak atau mengubah data dan berusaha untuk merusaknya, menghentikan sistem komputer sehingga mereka tidak dapat melakukan kewajiban mereka.

Dalam sebuah sistem komputer, sangat penting memiliki keamanan sistem komputer untuk mengawasi aktivitas jaringan sehingga orang-orang yang tidak memiliki hak dapat berharap untuk memasuki sistem tersebut, sependapat dengan Rendra Towidjojo dalam buku Mikrotik Kung Fu Kitab 2 (2013). : 115), kapasitas *firewall* untuk memperkuat keamanan organisasi dengan memilih kumpulan informasi apa yang dapat masuk atau keluar dari organisasi..

## Metode Penelitian

Penelitian yang digunakan pada metode *Network Development Life Cycle (NDLC)*, yaitu suatu pendekatan proses dalam komunikasi data yang menggunakan siklus yang tiada awal dan akhirnya dalam membangun sebuah jaringan provider, mencakup sejumlah tahap yaitu analisis, desain, simulasi *prototype*, implementasi, *monitoring* dan manajemen

Tahapan-tahapan pada NDLC:

1. *Analysis*, Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa topologi / jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya adalah wawancara, *survey*, langsung ke lapangan.
2. *Design*, Dari data-data yang didapatkan sebelumnya, tahap *Design* ini akan membuat gambar design topologi jaringan interkoneksi yang akan dibangun, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. *Design* bisa berupa *design* struktur topologi yang akan memberikan gambaran jelas tentang project yang akan dibangun.
3. *Simulation Prototype*, beberapa *networker's* akan membuat dalam bentuk simulasi dengan bantuan *Tools* khusus di bidang *network* dan sebagainya, hal ini dimaksudkan untuk melihat kinerja awal dari *network* yang akan dibangun dan sebagai bahan presentasi dan sharing dengan team *work* lainnya. Namun karena keterbatasan perangkat lunak simulasi ini, banyak para *networker's* yang hanya menggunakan alat Bantu tools untuk membangun *topology* yang akan didesain.
4. *Implementation*, di tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi *networker's* akan menerapkan semua yang telah direncanakan dan di design sebelumnya. *Implementasi* merupakan tahapan yang sangat menentukan dari berhasil / gagalnya project yang akan dibangun dan di tahap inilah *Team Work* akan diuji di lapangan untuk menyelesaikan masalah teknis dan non teknis
5. *Management*, di manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah *Policy*, kebijakan perlu dibuat untuk membuat / mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *Reliability* terjaga. *Policy* akan sangat tergantung dengan kebijakan level management dan strategi bisnis perusahaan tersebut.

## Tinjauan Pustaka

Table 1

No	Data Jurnal	Keterangan
1	Judul	ANALISIS DAN OPTIMASI DARI SIMULASI KEAMANAN JARINGAN MENGGUNAKAN FIREWALL MIKROTIK STUDI KASUS DI TAMAN PINTAR YOGYAKARTA
2	Jurnal	Jurnal JARKOM
3	Volume dan Halaman	Vol. 7 No. 2 Desember 2019
4	Tanggal & Tahun	2019
5	Penulis	Ebrahim Sinyo Rio Ola Balen Langobelen, Rr. Yuliana Rachmawati, Catur Iswahyudi
6	Penerbit	AKPRIND Yogyakarta
7	Tujuan Penelitian	Tujuan penelitian yang hendak dicapai dari penelitian ini adalah melakukan analisis dari simulasi kamanan jaringan yang disesuaikan dengan topologi jaringan di Taman Pintar Yogyakarta dengan memanfaatkan berbagai fitur yang ada pada Mikrotik seperti firewall dan fitur pendukung keamanan

		jaringan lainnya di Taman Pintar Yogyakarta
8	Lokasi dan Subjek	TAMAN PINTAR YOGYAKARTA
9	Perancangan Sistem	Secara umum penelitian ini menghasilkan konfigurasi untuk sistem keamanan jaringan komputer Taman Pintar Yogyakarta menggunakan firewall router Mikrotik yang meliputi konfigurasi untuk firewall, pengelolaan service port serta konfigurasi filter untuk Bridge.
10	Hasil Penelitian	Penelitian ini menerapkan empat konfigurasi firewall yang difungsikan untuk memblokir aktivitas pengguna atau serangan dari luar yang dapat membahayakan sistem keamanan jaringan. Konfigurasi tersebut yaitu blokir penggunaan aplikasi gratis VPN, blokir penggunaan aplikasi torrent, blokir seragan DDOS serta melakukan penyamaran untuk scanning port menggunakan NMAP.
11	Kekuatan Penelitian	Menerapkan VPN untuk memblokir serang DDOS dan penggunaan Torent
12	Kelemahan Penelitian	VPN yang digunakan gratis sehingga masih diragukan dalam keamanan privasinya
13	Kesimpulan	Analisis dan Optimalisasi sistem keamanan jaringan pada Taman Pintar Yogyakarta dapat dilaksanakan dengan baik. Menerapkan metodologi PPDI0 penelitian ini melakukan beberapa konfigurasi kemanan jaringan yang meliputi konfigurasi untuk firewall, pengelolaan service port serta konfigurasi filter untuk Bridge. Hal tersebut dipaparkan secara jelas dalam hasil dan pembahasan penelitian ini yang dilengkapi dengan ujicoba kasus dari masing-masing pembahasan

Table 2

No	Data Jurnal	Keterangan
1	Judul	PENGGUNAAN METODE IDS DALAM IMPLEMENTASI FIREWALL PADA JARINGAN UNTUK DETEKSI SERANGAN Distributed Denial Of Service (DDoS)
2	Jurnal	Jurnal Sistem Komputer Musirawas
3	Volume dan Halaman	Vol. 6, No. 2,
4	Tanggal & Tahun	Desember 2021
5	Penulis	Rizki Aulianita , Nu'man Musyaffa , Rini Martiwi
6	Penerbit	Universitas Bina Sarana Informatika
7	Tujuan Penelitian	Dalam pencegahan terjadinya serangan DDoS maka dilakukan pengamanan yang baik pada router mikrotik, salah satu penerapan metode dalam pengamanan jaringan yaitu dengan menggunakan metode IDS (Instrusion Detection System)
8	Lokasi dan Subjek	Universitas Bina Sarana Informatika
9	Perancangan Sistem	penerapan filter firewall, penulis menggunakan fitur lain yang ada pada router mikrotik yang penulis gunakan yaitu fitur torch dimana fitur ini sebagai tools yang dapat melihat pemakaian bandwith serta IP address mana yang sedang melakukan permintaan paket data pada jaringan internet sehingga IP address yang tidak dikenal akan terlihat pemakaian bandwith jaringan internetnya.
10	Hasil Penelitian	Penelitian ini, penulis menggunakan topologi jaringan

		Small Office Home Office (SOHO) topologi ini hanya 1 router mikrotik dan juga Access Point dan sedikit perangkat lainnya yang berguna untuk menyebarkan sinyal wireless jika klien tidak membutuhkan kabel untuk koneksinya
11	Kekuatan Penelitian	Menerapkan filter firewall menggunakan fitur yang ada pada mikrotik
12	Kelemahan Penelitian	-
13	Kesimpulan	Berdasarkan hasil testing penyerangan menggunakan aplikasi UDP unicorn untuk melihat bagaimana DDoS membuat suatu router berjalan lambat serta membuat badwith yang ada tanpa firewall dan yang telah dikonfigurasi menggunakan firewall fitur rules, maka perubahan keamanan yang signifikan terhadap router mikrotik sebagai perangkat yang sangat vital dalam jaringan internet baik untuk bertukar informasi maupun dalam hal lain yang berguna untuk user

### Tipe Alat yang di gunakan

#### 1. Kabel UTP

Cara kerja kabel UTP adalah dapat dimanfaatkan sebagai kabel untuk sistem Nearby Zone Organize (LAN) pada jaringan komputer/kerangka jaringan,.



Gambar 1. Kabel UTP

#### 2. Router Mikrotik

Switch Mikrotik disini akan digunakan sebagai alat untuk pengaturan tambahan untuk organisasi organisasi yang telah dibuat. Misalnya untuk hambatan kapasitas *transmisi, firewall, pembuatan VLAN,*



Gambar 2. Mikrotik RB941

Sumber <https://id.manuals.plus/mikrotik/rb941-2nd-tc-hap-lite-tc-routers-and-wireless-manual>

### 3. Modem

Modem merupakan gadget komunikasi yang berfungsi sebagai alat komunikasi dua arah sehingga pengaturan *web* dapat jauh lebih baik didapat oleh perangkat komputer / seluler. Dalam hal ini modulator adalah bagian dari modem yang berfungsi untuk mengubah flag informasi menjadi flag carrier yang siap dikirim. Sedangkan demodulator adalah bagian dari modem yang berfungsi untuk mempartisi flag data dari flag pembawa sehingga dapat diperoleh secara sah.



Gambar 3. Modem Wifi Bolt Ultra LTE

#### Kebutuhan sistem

Tabel 3 Tabel Kebutuhan Sistem

No.	Keperluan Pengguna	Keterangan
1.	Dapat terhubung ke internet	✓
2.	Dapat menambahkan pengguna jaringan lewat web service	✓
3.	Dapat memantau aktivitas pengguna.	✓
4.	Melakukan pemblokiran terhadap pengguna nakal yang ingin melemahkan jaringan atau ingin masuk kedalam jaringan secara tidak sah.	✓
5.	Web service dapat di gunakan dengan mudah	✓

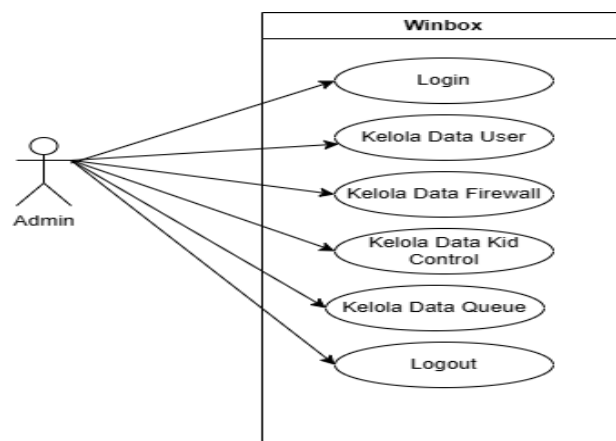
Tabel 4 Tabel Analisa Kebutuhan Alat

No.	Alat yang digunakan	Keterangan
1.	<i>Mikrotik RB941</i>	Sebagai alat untuk melakukan penyettingan jaringan
2.	<i>Modem wifi 4G Bolt</i>	Sebagai peyalur sumber internet
3.	Kabel <i>UTP</i>	Penghubung antara semua alat yang akan dihubungkan

4.	<i>laptop</i>	Sebagai admin untuk melakukan monitoring jaringan melalui web service dan melakukan penyettingan firewall rules di winbox
----	---------------	---

### Use Case Diagram

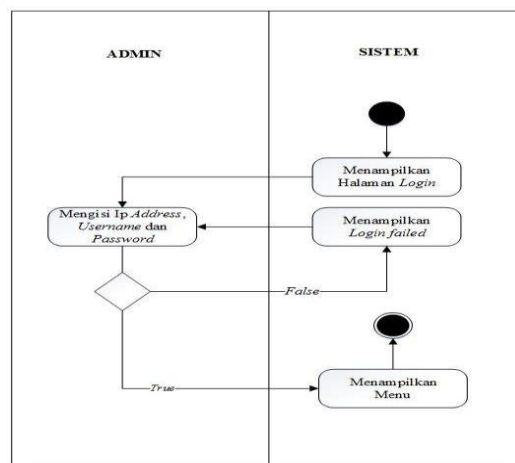
Memfaatkan grafik kasus menggambarkan kegunaan yang diantisipasi dari suatu kerangka kerja. Kasus penggunaan berbicara tentang interaksi antara artis pertunjukan dan kerangka kerja. Untuk mengetahui pergerakan framework dalam framework pengaturan di PT Sari Wangi Mentari.



Gambar 4. Use Case Diagram

### Activity Diagram

Bagan Gerakan adalah bagian dari pertunjukan energik yang digunakan untuk menggambarkan alur kerja atau formulir kerangka kerja. Bagan ini menunjukkan bagaimana suatu proses dimulai,



Gambar 5. Activity Diagram

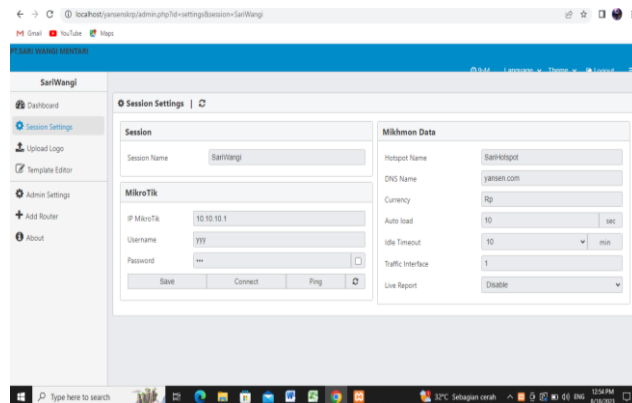
Tabel 5 Kriteria penilaian pada *kuesioner*

No	Pertanyaan	Jumlah Nilai Responden						
		1	2	3	4	5	6	7
1	Apakah web ini service mudah di gunakan?	5	5	5	5	4	4	4
2	Apakah web service ini membantu perusahaan dalam memonitoring jaringan ?	5	5	4	5	5	5	5
3	Apakah dengan penyettingan firewall rules membatu meningkatkan kemanan jaringan di PT.Sari Wangi mentari ?	5	5	5	5	5	5	5
4	bagaimana menurut anda dengan web service untuk memonitoring jaringan?	5	5	5	5	4	5	4
5	bagaimana kinerja dari web service monitoring	4	3	5	5	4	5	4

## Hasil Pembahasan

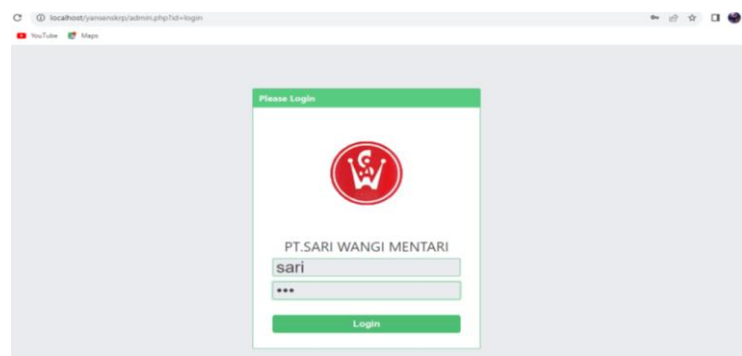
### Tampilan Program

Menghubungkan mikrotik dengan web service



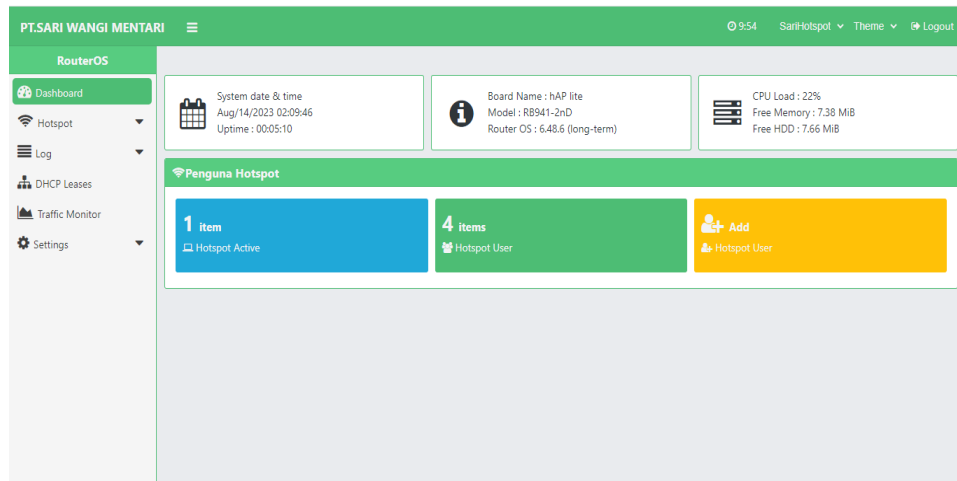
Gambar 6. Menghubungkan web service

Tampilan halaman login web monitoring



Gambar 7. Tampilan Login

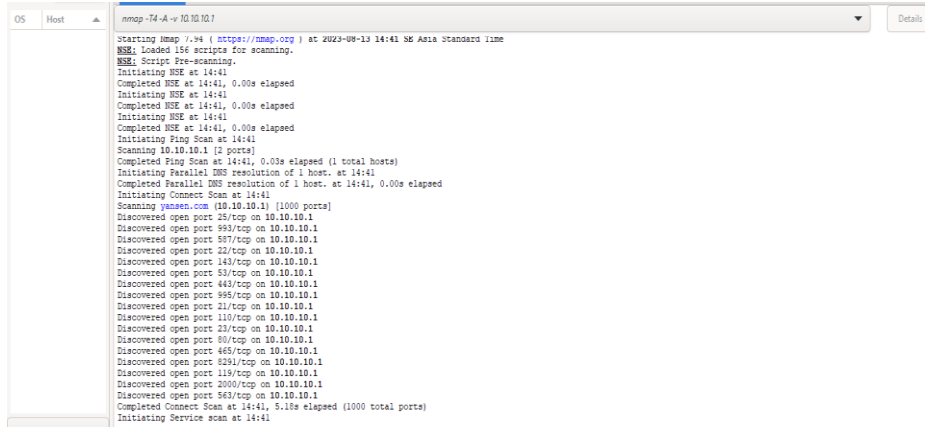
## Dashboard web monitoring



Gambar 8. Tampilan dashboard

## Pengujian firewall

### Pengujian scanning port



Gambar 9. Scanning port

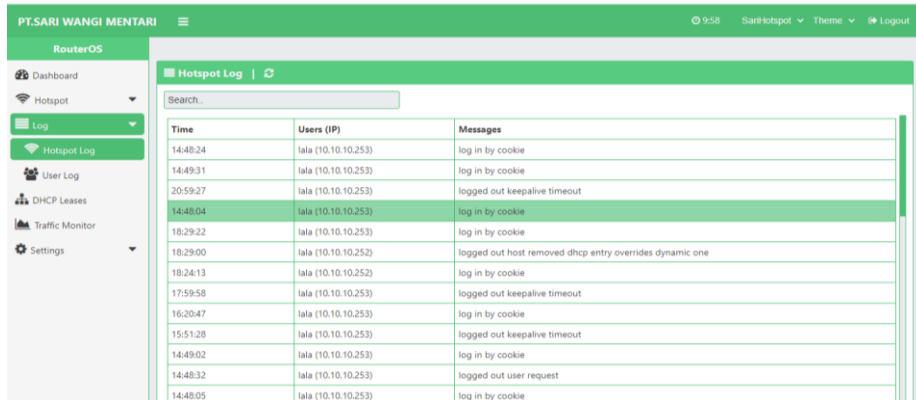
## Traffing monitoring



Gambar 10. Traffic monitoring



## Memonitoring aktivitas user

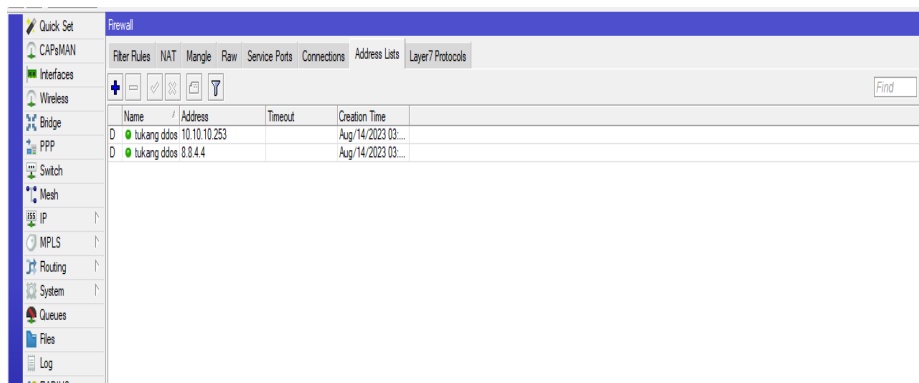


The screenshot shows the RouterOS Hotspot Log interface. The left sidebar contains navigation options: Dashboard, Hotspot, Log, Hotspot Log (selected), User Log, DHCP Leases, Traffic Monitor, and Settings. The main area displays a table of log entries with columns for Time, Users (IP), and Messages.

Time	Users (IP)	Messages
14:48:24	lala (10.10.10.253)	log in by cookie
14:49:31	lala (10.10.10.253)	log in by cookie
20:59:27	lala (10.10.10.253)	logged out keepalive timeout
14:48:04	lala (10.10.10.253)	log in by cookie
18:29:22	lala (10.10.10.253)	log in by cookie
18:29:00	lala (10.10.10.252)	logged out host removed dhcp entry overrides dynamic one
18:24:13	lala (10.10.10.252)	log in by cookie
17:59:58	lala (10.10.10.253)	logged out keepalive timeout
16:20:47	lala (10.10.10.253)	log in by cookie
15:51:28	lala (10.10.10.253)	logged out keepalive timeout
14:49:02	lala (10.10.10.253)	log in by cookie
14:48:32	lala (10.10.10.253)	logged out user request
14:48:05	lala (10.10.10.253)	log in by cookie

Gambar 11. Monitoring aktivitas user

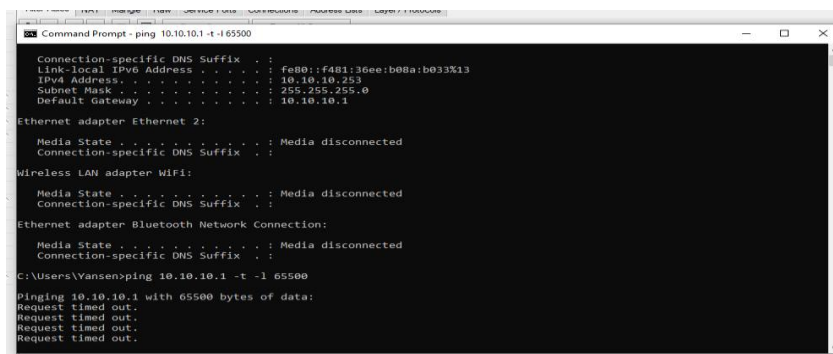
## Pemblokiran ip penyerang



The screenshot shows the Mikrotik WinBox Firewall Filter configuration window. The 'Filter Rules' tab is active, showing a list of rules. Two rules are visible, both named 'lakang ddose'.

Name	Address	Timeout	Creation Time
D lakang ddose	10.10.10.253		Aug/14/2023 03:...
D lakang ddose	8.8.4.4		Aug/14/2023 03:...

Gambar 12. Pemblokiran ip penyerang



```
Command Prompt - ping 10.10.10.1 -t -l 65500

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::f481:36ee:b08a:b033%13
IPv4 Address. . . . . : 10.10.10.253
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.10.1

Ethernet adapter Ethernet 2:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix . : 

Wireless LAN adapter WiFi:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix . : 

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix . : 

C:\Users\Vansen>ping 10.10.10.1 -t -l 65500

Pinging 10.10.10.1 with 65500 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

Gambar 13. Pemblokiran ip penyerang

## Kesimpulan

Dari hasil penelitian yang penulis mendapatkan beberapa kesimpulan sebagai berikut:

1. Dari hasil pengujian yang di lakukan setelah melakukan analisa jaringan di PT.SARI WANGI MENTARI penulis melakukan keamanan jaringan dengan menerapkan pengaturan *firewall* dan *memblokir port-port* yang sering di gunakan untuk melakukan remote atau peretasan .

2. bisa *memonitoring* dan *controlling aktifitas* pengguna jaringan melalui mikrotik atau *web service*.
3. Bisa membatasi akses pengguna yang menggunakan internet secara berlebihan dengan melakukan pembagian *bandwith* dan menggunakan *fitur kid control*.

### Ucapan Terima Kasih

Terima kasih kepada staff PT. Sari wangi mentari dan dosen pembimbing saya bapak Rino serta Fakultas Sains Teknologi Universitas Buddhi Dharma.

### Referensi :

- [1] Al Ghifari, A. a. (2020). Perencanaan Jaringan Local Area Network Di Gedung Dakwah Muhammadiyah Kabupaten Sragen Dengan Cisco Packet Tracer.
- [2] Amarudin, A. (2018). Analisis Dan Implementasi Keamanan Jaringan Pada Mikrotik. *Prosiding Semnastek*.
- [3] Azis, H. &. (2018). Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids. *Jurnal Manajemen, Vol. 8*.
- [4] Efrahim Sinyo Rio Ola Balen Langobelen, R. Y. (AKPRIND Yogyakarta). ANALISIS DAN OPTIMASI DARI SIMULASI KEAMANAN JARINGAN MENGGUNAKAN FIREWALL MIKROTIK STUDI KASUS DI TAMAN PINTAR YOGYAKARTA. Vol. 7 No. 2 Desember 2019.
- [5] Fajar, R. (2 Agustus 2019). Mengenal Diagram UML (Unified Modeling Language).
- [6] Haris, A. I. (2022). Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. *Jurnal Sistem, Vol. 11, No 67-76*.
- [7] Hariyudo, R. R. (2017). "Pemetaan Dan Perancangan Jaringan Komputer Di Gedung Rektorat Baru Di lain.
- [8] Herlambang, M. L. (2008). Panduan Lengkap Menguasai Router Masa Depan Menggunakan Mikrotik RouterOS. *ANDI*.
- [9] Krismadinata, M. A. ( Oct. 2018). "Suatu Kajian Literatur Masalah-Masalah yang Dihadapi dalam Mata Kuliah Jaringan Komputer. *INVOTEK J. Inov. Vokasional Dan Teknol, vol. 18, no. 2, pp. 1–8*.
- [10] Mhd.Fakhmi, L. M. (Oktober 2021). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw. *Seminar Nasional Industri dan Teknologi (SNIT), Vol. 2021 SNIT 2021*.

- [11] Mulyanto, Y. H. (n.d.). Analisis Keamanan Wireless Local Area Network (WLAN) Terhadap Serangan Brute Force Dengan Metode Penetration Testing. *Jurnal Informatika Teknologi dan Sains*, Vol. 4, No. 26-35.
- [12] Purbo, O. W. (2019). Keamanan Jaringan Internet.
- [13] Santoso, J. D. (n.d.). Keamanan Jaringan Nirkabel Menggunakan Wireless IntrusionDetection System. *INFOS Journal-Information System Journal,,* Vol. 1, No 44-50.
- [14] Rizki Aulianita, N. M. (Desember 2021). PENGGUNAAN METODE IDS DALAM IMPLEMENTASI FIREWALL PADA JARINGAN UNTUK DETEKSI SERANGAN Distributed Denial Of Service (DDoS). *Jurnal Sistem Komputer Musirawas*, Vol. 6, No. 2,.