

CESS

(Journal of Computer Engineering, System and Science)

Available online: <https://jurnal.unimed.ac.id/2012/index.php/cess>

ISSN: 2502-714x (Print) | ISSN: 2502-7131 (Online)



Implementasi *Firewall* MikroTik Sebagai Upaya Meningkatkan Produktivitas Karyawan Melalui Pengendalian Akses Internet Non-Kerja Di PT XYZ

Implementation of MikroTik Firewall as an Effort to Increase Employee Productivity Through Control of Non-Work Internet Access at PT XYZ

Taufik Rahman^{1*}, Mochammad Dhanu Ramadhan², Bakhtiar Rifai³

^{1,2}Teknologi Informasi, Teknik Informatika, Universitas Bina Sarana Informatika, Indonesia

³Akutansi, Ekonomi dan Bisnis, Universitas Bina Sarana Informatika, Indonesia

^{1,2,3}Jl. Kramat Raya No.98, RT.2/RW.9, Kwitang, Kec. Senen, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10450

Email: ¹taufik@bsi.ac.id, ²mochdhanuramadhan@gmail.com, ³bakhtiar.bri@bsi.ac.id

*Corresponding Author

ABSTRAK

Penggunaan internet yang tidak terkontrol di lingkungan perusahaan dapat menimbulkan pemborosan bandwidth dan menurunkan produktivitas karyawan. Permasalahan tersebut juga terjadi di PT XYZ, di mana akses ke konten non-kerja selama jam operasional berdampak pada kualitas jaringan dan fokus kerja karyawan. Penelitian ini bertujuan untuk menganalisis dan mengimplementasikan *firewall* MikroTik sebagai solusi pengendalian akses internet non-kerja guna meningkatkan produktivitas karyawan. Metode penelitian yang digunakan adalah metode deskriptif dengan pendekatan observasi, wawancara, dan studi pustaka. Implementasi dilakukan menggunakan MikroTik RouterOS dengan konfigurasi Layer 7 Protocol, Address List, NAT, Time-Based Filtering, serta manajemen bandwidth dan monitoring jaringan. Hasil penelitian menunjukkan adanya penurunan signifikan trafik internet non-kerja hingga 70,8%, peningkatan stabilitas jaringan yang ditandai dengan penurunan *latency* dan *packet loss*, serta distribusi bandwidth yang lebih efisien. Selain itu, hasil kuesioner manajerial menunjukkan peningkatan fokus, disiplin, dan efektivitas kerja karyawan setelah penerapan *firewall*. Kesimpulan dari penelitian ini menunjukkan bahwa implementasi *firewall* MikroTik efektif dalam meningkatkan keamanan dan efisiensi jaringan serta berkontribusi positif terhadap peningkatan produktivitas karyawan di PT XYZ.

Kata Kunci: *Firewall MikroTik; Pengendalian Akses Internet; Produktivitas Karyawan; Content Filtering; Manajemen Bandwidth.*



ABSTRACT

Uncontrolled internet use in a company environment can lead to bandwidth waste and decrease employee productivity. This problem also occurs at PT XYZ, where access to non-work content during operating hours has an impact on network quality and employee focus on work. This study aims to analyze and implement the MikroTik firewall as a non-work internet access control solution to increase employee productivity. The research method used is a descriptive method with an observation, interview, and literature review approach. The implementation was carried out using MikroTik RouterOS with Layer 7 Protocol, Address List, NAT, Time-Based Filtering, as well as bandwidth management and network monitoring. The results showed a significant decrease in non-working internet traffic of up to 70.8%, an increase in network stability characterized by a decrease in latency and packet loss, and a more efficient distribution of bandwidth. In addition, the results of the managerial questionnaire showed an increase in employee focus, discipline, and work effectiveness after the implementation of the firewall. The conclusion of this study shows that the implementation of the MikroTik firewall is effective in improving network security and efficiency and contributes positively to increasing employee productivity at PT XYZ.

Keywords: MikroTik Firewall; Internet Access Control; Employee Productivity; Content Filtering; Bandwidth Management.

1. PENDAHULUAN

Perkembangan teknologi informasi menjadikan Internet sebagai komponen esensial dalam mendukung operasional perusahaan. Namun, akses yang tidak terkendali kerap dimanfaatkan karyawan untuk mengunjungi konten non-kerja seperti media sosial dan hiburan, yang berpotensi menurunkan produktivitas serta meningkatkan risiko keamanan jaringan. PT XYZ menghadapi permasalahan serupa dan membutuhkan mekanisme pengelolaan lalu lintas Internet yang selaras dengan kebijakan dan tujuan organisasi.

Jaringan Komputer merupakan salah satu ilmu di bidang Teknologi informasi yang mengalami perkembangan pesat[7]. Banyak sektor yang terdampak oleh kemajuan teknologi jaringan komputer terutama di sektor bisnis, pendidikan, serta aktivitas sehari-hari seperti media sosial dan transaksi perbankan. Namun, dengan kemajuan ini, ancaman siber juga semakin meningkat. Menurut laporan dari Kementerian Komunikasi dan Informatika, Indonesia berhasil memblokir lebih dari 23 juta serangan siber sepanjang tahun 2023. Ini menunjukkan pentingnya dalam melindungi jaringan terhadap serangan siber[8]. Dengan adanya *router* MikroTik, hal ini dapat menjadi solusi untuk membantu mengurangi kemungkinan karyawan mengakses jejaring sosial secara diam-diam[2].

Penelitian oleh Muflih et al. (2025) berjudul “Implementasi Web Filtering Firewall Berbasis MikroTik RouterOS untuk Meningkatkan Keamanan Jaringan di Pondok Pesantren” mengimplementasikan web filtering firewall di pondok pesantren untuk membatasi konten negatif dan menciptakan lingkungan belajar yang aman [14].

Penelitian oleh (Imawan & Dwiasnati, 2025) berjudul “Efisiensi Penggunaan Jaringan melalui Firewall Layer 7 Protocol” meningkatkan efisiensi jaringan perusahaan dengan

memblokir akses non-kerja menggunakan *Firewall Layer 7 Protocol*, sehingga *bandwidth* meningkat dan produktivitas terjaga [15].

Firewall adalah perangkat keamanan jaringan yang sudah ada sejak tahun 1980-an sebagai sistem untuk mengawasi serta menyaring sumber jaringan yang masuk dan keluar berdasarkan aturan keamanan yang telah ditetapkan sebelumnya oleh administrator jaringan [9]. Fitur penyaringan konten digunakan untuk membatasi atau menolak akses ke situs maupun konten yang dianggap tidak relevan. Proses konfigurasi dilakukan melalui menu IP Firewall pada MikroTik RouterOS dengan menggunakan antarmuka aplikasi WinBox.[10][11].

Firewall filter rules menetapkan sejumlah parameter, termasuk address, protocol, port, time, dan interface, untuk mengatur lalu lintas jaringan. Aturan ini berfungsi mencegah aktivitas berbahaya dengan membatasi akses ke situs web tertentu, memblokir aplikasi seperti VPN, Torrent, port scanning, serta penggunaan recursive DNS yang tidak diinginkan. [11].

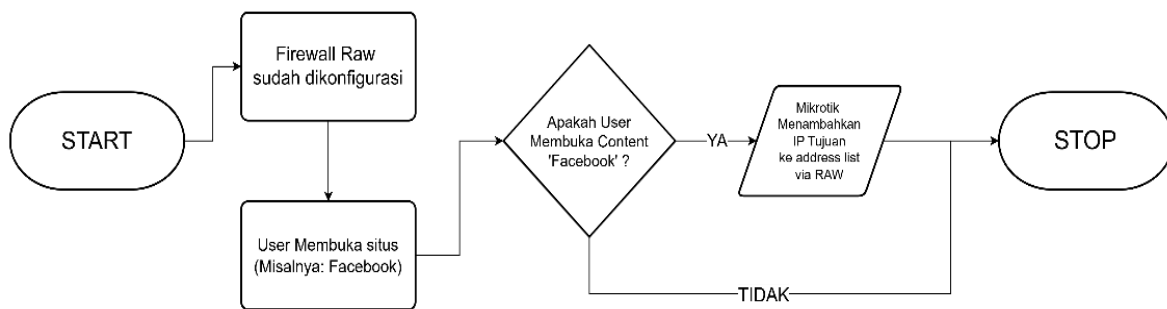
Firewall raw merupakan fitur yang juga berfungsi menangani *filter* paket dimana konsep pemblokiran sama seperti *firewall filter Rules*. Namun, *firewall raw* tidak membutuhkan sumber daya CPU sebanyak *firewall filter* karena pada raw memiliki kemampuan untuk *drop packet* sebelum proses *connection tracking* dimulai [12]. *Connection tracking* adalah kemampuan untuk melacak informasi seperti *source Address*, *destination Address*, *source and destination port*, tipe protokol, dan lain-lain pada koneksi yang sedang berlangsung. Dalam kata lain, raw menjadi lebih hemat sumber daya dikarenakan tidak menggunakan *connection tracking* dalam proses *filtering*. Sehingga dengan kemampuan ini dapat digunakan untuk *dropping* paket dalam jumlah besar dan cocok untuk mencegah serangan DDoS [13].

Firewall MikroTik dipandang sebagai solusi teknis yang efektif dalam membatasi akses ke situs dan aplikasi non-kerja melalui pengaturan berbasis kebijakan perusahaan. Implementasi teknologi ini diharapkan mampu meningkatkan produktivitas karyawan, menjaga keamanan data, dan memastikan pemanfaatan Internet hanya untuk kepentingan operasional[1]. Penelitian ini bertujuan untuk menganalisis pengaruh penerapan *firewall* MikroTik dalam pengendalian akses konten non-kerja terhadap peningkatan produktivitas karyawan di PT XYZ.

2. METODE PENELITIAN

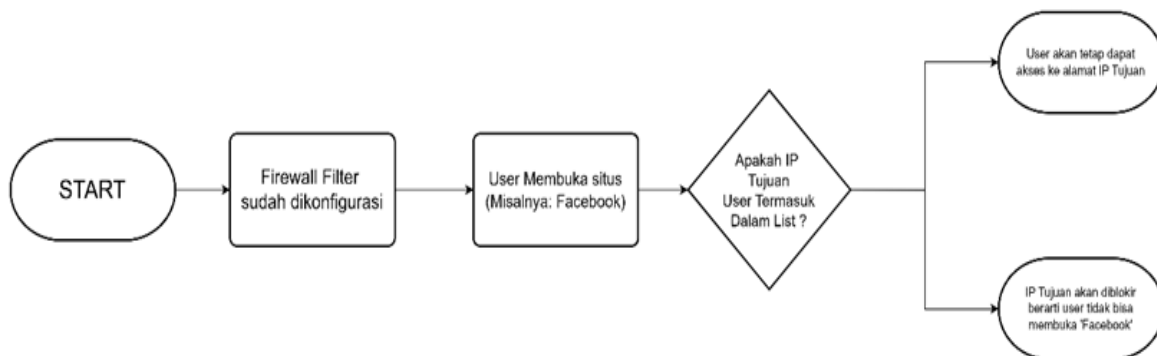
Metode penelitian yang digunakan adalah metode deskriptif, yang berfungsi untuk memaparkan secara terstruktur dan objektif bagaimana penerapan firewall MikroTik dilakukan dalam membatasi akses terhadap konten non-kerja serta pengaruhnya terhadap tingkat produktivitas karyawan.

Dan adanya proses filter atau penyaringan dibagi menjadi dua tahap, yang masing-masing dijelaskan dalam *Flowchart* berikut:



Gambar 1. Flowchart Firewall RAW

Menunjukkan langkah pertama yang diambil MikroTik saat mendeteksi koneksi keluar dan mencatat IP tujuan pengguna. Teknik RAW kemudian secara otomatis menambahkan IP ke daftar alamat.



Gambar 2. Flowchart Firewall Filter

Proses selanjutnya berlanjut ke tahap penyaringan. IP tujuan pengguna akan diperiksa oleh filter firewall untuk melihat apakah alamat tersebut termasuk dalam daftar alamat yang dibuat. Firewall akan segera memutuskan koneksi jika alamat IP ditemukan dalam daftar blokir. Di sisi lain, koneksi dapat diarahkan ke internet jika alamat IP tidak ditemukan.

Kedua fase ini memungkinkan sistem firewall MikroTik secara efisien dan otomatis membatasi akses pengguna ke materi tertentu tanpa memerlukan administrator jaringan untuk campur tangan secara manual.

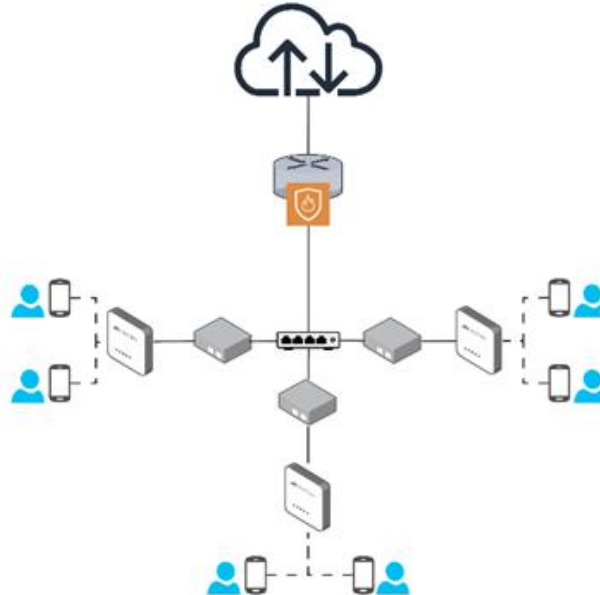
3. HASIL DAN PEMBAHASAN

Jaringan usulan dirancang untuk mengatasi permasalahan akses Internet di PT XYZ, khususnya terkait pengendalian trafik, efisiensi bandwidth, dan peningkatan produktivitas karyawan. Perubahan utama meliputi penempatan MikroTik Router sebagai gerbang utama (*main gateway*) untuk mengatur dan menyaring seluruh trafik data, penerapan fitur firewall, *web filtering*, Layer 7 Protocol, manajemen bandwidth, serta monitoring trafik secara berkala.

Selain itu, diterapkan kebijakan penggunaan Internet berbasis jadwal (*schedule*), penerapan *whitelist/blacklist* situs, dan logging aktivitas pengguna untuk kebutuhan audit dan evaluasi efisiensi kerja. Implementasi ini memungkinkan kontrol trafik yang lebih optimal, peningkatan fokus karyawan pada aktivitas kerja, serta memperkuat keamanan jaringan dari akses tidak sah dan potensi ancaman siber.

3.1. Topologi Jaringan

Topologi jaringan yang diusulkan menggunakan Topologi Bintang terpusat dengan Router MikroTik sebagai core router sekaligus firewall utama. Seluruh perangkat pengguna terhubung melalui *Access Point* yang terkoneksi ke *Switch unmanaged*, kemudian diteruskan ke *Fiber Optic Converter* sebelum menuju Router MikroTik untuk dilakukan proses *filtering* sebelum akses Internet diberikan.



Gambar 3. Topologi Jaringan

Perangkat pendukung meliputi, switch unmanaged untuk distribusi jaringan ke berbagai area, media converter untuk konversi sinyal fiber optik ke Ethernet, serta *Access Point* sebagai penyedia koneksi nirkabel. Sistem keamanan diperkuat dengan konfigurasi Filter Rules, RAW, dan Address List pada Router MikroTik untuk membatasi akses non-produktif, menyaring trafik tidak diinginkan, serta mengelompokkan alamat IP atau domain yang diblokir maupun diizinkan.

Tabel 1. Konfigurasi *Firewall Filter* pada MikroTik

No	Action	Chain	Src. Address	Protocol	Dst. Port	Dst Address List	Layer7-Protocols	Keterangan Tujuan / Aplikasi
1	Allow	forward	10.200.66.0/23	any	any	WhatsApp	-	Mengizinkan akses WhatsApp
2	Allow	forward	10.200.66.0/23	any	any	Google Mail	-	Mengizinkan akses Gmail
3	Allow	forward	10.200.66.0/23	any	any	Microsoft	-	Mengizinkan akses Microsoft
4	Allow	forward	10.200.66.0/23	any	any	Zoom	-	Mengizinkan akses Zoom

5	Drop	forward	10.200.66.0/23	17 (udp)	500	-	-	Blokir VPN IPsec
6	Drop	forward	10.200.66.0/23	17 (udp)	4500	-	-	Blokir VPN IPsec
7	Drop	forward	10.200.66.0/23	17 (udp)	1701	-	-	Blokir VPN I2tp Blokir
8	Drop	forward	10.200.66.0/23	6 (tcp)	443	Thunder- VPN	-	Thunder VPN Blokir
9	Drop	forward	10.200.66.0/23	17 (udp)	443	Thunder- VPN	-	Thunder VPN Blokir
10	Drop	forward	10.200.66.0/23	any	any	Facebook	-	Facebook Blokir
11	Drop	forward	10.200.66.0/23	any	any	Instagram	-	Instagram Blokir
12	Drop	forward	10.200.66.0/23	any	any	Tiktok	-	Tiktok Blokir
13	Drop	forward	10.200.66.0/23	17 (udp)	443		-	QUIC Blokir
14	Drop	forward	10.200.66.0/23	any	any	Youtube	-	Youtube Blokir
15	Drop	forward	10.200.66.0/23	17 (udp)	443		-	QUIC Blokir
16	Drop	forward	10.200.66.0/23	any	any	Netflix	-	Netflix Blokir
17	Drop	forward	10.200.66.0/23	any	any	Twitter	-	Twitter Blokir
18	Drop	forward	10.200.66.0/23	any	any	Shopee	-	Shopee Blokir
19	Drop	forward	10.200.66.0/23	6 (tcp)	any 5521,5222,5	-	block_pes	Blokir PES
20	Drop	forward	10.200.66.0/23	17 (udp)	730- 5740,30000, 50000	-	-	Blokir PES
21	Drop	forward	10.200.66.0/23	any	any 8013,8080,8	pes_servers	-	Blokir PES
22	Drop	forward	10.200.66.0/23	6 (tcp)	085,8086,80 88,15692,17 500,20371	-	-	Blokir PUBG
23	Drop	forward	10.200.66.0/23	17 (udp)	8030,8700	-	-	Blokir PUBG
24	Drop	forward	10.200.66.0/23	17 (udp)	30000- 31000,10003	-	-	Blokir Mobile Legend
25	Drop	forward	10.200.66.0/23	6 (tcp)	30000- 31000,10003	-	-	Blokir Mobile Legend
26	Drop	forward	10.200.66.0/23	any	any	MobileLeg ends	-	Blokir Mobile Legend

27	Drop	forward	10.200.66.0/23	6 (tcp)	13054,1370 1,17101	-	-	Blokir Magic Chess
28	Drop	forward	10.200.66.0/23	6 (tcp)	5010,5692,8 011,8500,80 85,8099,880 1,10017,200 00,25000,30 000,31003	-	-	Blokir Magic Chess
29	Drop	forward	10.200.66.0/23	17 (udp)	5010,5692,8 011,8801,25 000,30000,3 1003	-	-	Blokir Magic Chess

Filter Rules NAT Mangling Row						Service Ports	Connections	Address Lists	Layer/Protocols				
Filter Rules NAT Mangling Row						Service Ports	Connections	Address Lists	Layer/Protocols				
#	Action	Chain	Content	Bytes	Packets								
-- add IP's Whatsapp													
0	add dst to address list	preouting	cdn.whatsapp.net	396.0 KB	586								
1	add dst to address list	preouting	fb.whatsapp.net	660.4 KB	956								
2	add dst to address list	preouting	whatsapp.net	1397.7 KB	2136								
3	add dst to address list	preouting	whatsapp.com	144.6 KB	206								
-- add IP's Facebook													
4	add dst to address list	preouting	facebook.com	0.0	0								
5	add dst to address list	preouting	fbcdn.net	0.0	0								
6	add dst to address list	preouting	facebook.net	0.0	0								
7	add dst to address list	preouting	fbcdn.com	0.0	0								
8	add dst to address list	preouting	fb.com	0.0	0								
9	add dst to address list	preouting	fb.gd	0.0	0								
10	add dst to address list	preouting	fbstatic.ch	0.0	0								
11	add dst to address list	preouting	messenger.com	0.0	0								
12	add dst to address list	preouting	m.me	1440.0	1								
-- add IP's Instagram													
13	add dst to address list	preouting	instagram.com	0.0	0								
14	add dst to address list	preouting	cdninstagram.com	0.0	0								
15	add dst to address list	preouting	threads.net	0.0	0								
-- add IP's TikTok													
16	add dst to address list	preouting	tiktok.com	0.0	0								
17	add dst to address list	preouting	tiktokpdx.com	0.0	0								
18	add dst to address list	preouting	tiktokch.com	0.0	0								
19	add dst to address list	preouting	tiktokch.eu.com	0.0	0								
20	add dst to address list	preouting	dykeweb.com	0.0	0								
21	add dst to address list	preouting	appsflyerlink.com	0.0	0								
22	add dst to address list	preouting	micropay.com	0.0	0								
23	add dst to address list	preouting	tiktokch.eu.com	0.0	0								
-- add IP's Gmail													
24	add dst to address list	preouting	googleusercontent.com	7.0 KB	5								
25	add dst to address list	preouting	googleapis.com	52.6 KB	67								
26	add dst to address list	preouting	google.com	90.2 KB	104								
27	add dst to address list	preouting	google.com	90.2 KB	104								
-- add IP's Outlook													
28	add dst to address list	preouting	o365.com	11.3 KB	23								
29	add dst to address list	preouting	office365.com	40.3 KB	30								
30	add dst to address list	preouting	akype.com	303.3 KB	243								
31	add dst to address list	preouting	adms.com	0.0	0								
32	add dst to address list	preouting	crkrc.com	0.0	0								
33	add dst to address list	preouting	data.microsoft.com	2449.3 KB	3104								
34	add dst to address list	preouting	office.net	331.5 KB	830								
-- add IP's Zoom													
35	add dst to address list	preouting	zoom.us	316.5 KB	410								

36 items

Gambar 4. Pengelompokan IP Address Tujuan menggunakan metode RAW

Fennel						
Filter Rules NAT Mangle Rule Service Ports Connections Address List Layer/Protocol						
	Address	Timeout	Creation Time			
D	Traffic	43.132.168.234		Jun-27-2025	16:40:56	1
D	Traffic	23.221.52.115		Jun-27-2025	16:40:56	1
D	Traffic	163.161.169.200		Jun-27-2025	16:40:51	1
D	Traffic	71.18.171.162		Jun-27-2025	16:40:47	1
D	Traffic	163.161.158.186		Jun-27-2025	16:40:27	1
D	Google Mail	74.125.68.162		Jun-27-2025	16:40:27	1
D	Traffic	71.18.1225		Jun-27-2025	16:40:07	1
D	Traffic	154.94.116.18		Jun-27-2025	16:40:05	1
D	Traffic	164.96.116.21		Jun-27-2025	16:40:05	1
D	Traffic	154.172.62.65		Jun-27-2025	16:39:27	1
D	Traffic	23.62.212.170		Jun-27-2025	16:39:19	1
D	Traffic	23.45.136.162		Jun-27-2025	16:39:19	1
D	Traffic	154.94.116.4		Jun-27-2025	16:39:07	1
D	Traffic	163.215.67.4		Jun-27-2025	16:39:05	1
D	Microsoft	62.162.143.209		Jun-27-2025	16:38:49	1
D	Google Mail	142.250.4.132		Jun-27-2025	16:38:35	1
D	Traffic	154.172.62.66		Jun-27-2025	16:38:26	1
D	Traffic	23.216.168.169		Jun-27-2025	16:38:26	1
D	Traffic	154.167.183.145		Jun-27-2025	16:38:24	1
D	Traffic	23.62.212.143		Jun-27-2025	16:38:07	1
D	Traffic	23.214.108.69		Jun-27-2025	16:37:47	1
D	Google Mail	74.125.130.180		Jun-27-2025	16:37:46	1
D	Google Mail	172.203.118.132		Jun-27-2025	16:37:26	1
D	Traffic	23.214.168.16		Jun-27-2025	16:37:26	1
D	Google Mail	74.125.208.132		Jun-27-2025	16:37:12	1
D	Traffic	23.62.212.168		Jun-27-2025	16:37:06	1
D	Whatsapp	114.125.240.228	48231642	Jun-27-2025	16:37:04	1
D	Traffic	154.94.116.6		Jun-27-2025	16:37:04	1
D	Traffic	66.7.228.91		Jun-27-2025	16:36:40	1
D	Google Mail	74.125.68.18		Jun-27-2025	16:36:15	1
D	Traffic	154.172.62.75		Jun-27-2025	16:36:14	1
D	Traffic	168.95.927.149		Jun-27-2025	16:36:14	1
D	Traffic	71.18.251.7		Jun-27-2025	16:36:09	1
D	Traffic	23.214.165.137		Jun-27-2025	16:36:06	1
D	Facebook	3.22.168.24	48231630	Jun-27-2025	16:36:06	1
D	Traffic	154.94.121.168		Jun-27-2025	16:36:02	1
D	Traffic	43.132.166.242		Jun-27-2025	16:36:01	1
D	Facebook	13.35.31.70	48231643	Jun-27-2025	16:36:00	1
D	Facebook	13.35.31.20	48231643	Jun-27-2025	16:35:58	1
D	Traffic	23.228.46.26		Jun-27-2025	16:35:46	1
D	Traffic	23.228.46.26		Jun-27-2025	16:35:40	1
D	Google Mail	74.125.68.136		Jun-27-2025	16:35:36	1
D	Facebook	3.143.61.93	48231645	Jun-27-2025	16:35:32	1
D	Traffic	71.18.1.229		Jun-27-2025	16:35:31	1

Gambar 5. Hasil Pengelompokan IP ditandai pada *Address List* MikroTik

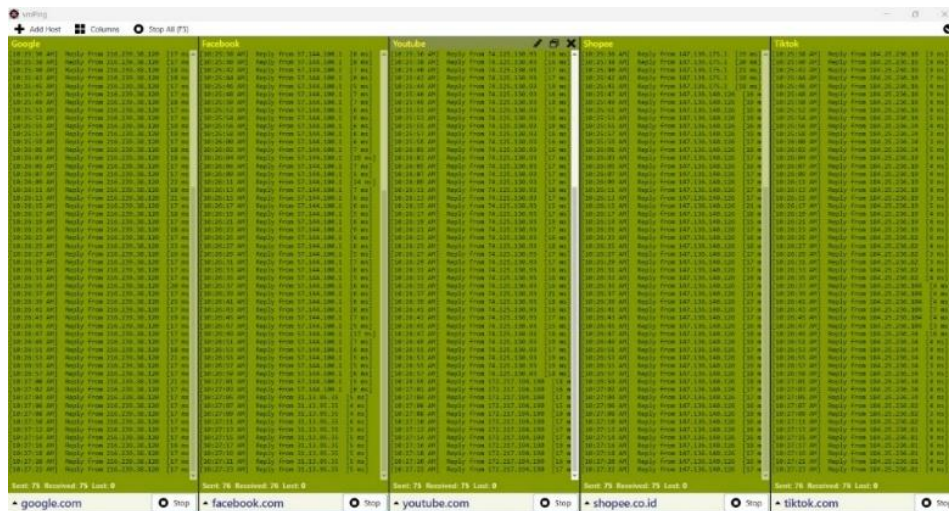
3.2. Pengujian Jaringan

Pengujian jaringan dilakukan untuk mengevaluasi performa dan efisiensi sistem jaringan sebelum dan sesudah implementasi firewall MikroTik. Pengujian ini bertujuan untuk mengetahui sejauh mana peningkatan performa jaringan dan dampaknya terhadap produktivitas karyawan, terutama dalam hal kestabilan koneksi, efisiensi penggunaan bandwidth, dan keamanan akses.

Pengujian dilakukan dengan metode komparatif, yaitu membandingkan kondisi jaringan sebelum dan sesudah implementasi firewall, baik dari segi perangkat keras (*hardware*) maupun perangkat lunak (*software*) dan konfigurasi jaringan.

3.2.1. Pengujian Jaringan Awal

Sebelum dilakukan konfigurasi *firewall*, pengujian dilakukan terhadap beberapa situs populer untuk mengetahui sejauh mana akses *Internet* terbuka bagi pengguna. Pengujian dilakukan menggunakan tools vmPing untuk memantau respon koneksi menggunakan protokol ICMP.



Gambar 6. Monitoring vmPing sebelum penerapan *Firewall*

Dapat disimpulkan bahwa sebelum dilakukan konfigurasi, seluruh situs populer yang diuji masih dapat diakses secara penuh oleh pengguna jaringan. Tidak terdapat sistem penyaringan konten, sehingga pengguna dapat bebas mengakses situs hiburan, media sosial, maupun *e-commerce* selama jam kerja.

Selain situs web, pengujian juga dilakukan terhadap beberapa aplikasi *game online* populer yang umum digunakan oleh pengguna perangkat mobile.

3.2.2. Pengujian Jaringan Akhir

Setelah konfigurasi *firewall* diterapkan pada perangkat MikroTik, dilakukan pengujian ulang terhadap beberapa situs populer dan aplikasi *game* untuk mengevaluasi efektivitas sistem dalam membatasi akses non-produktif. Pengujian dilakukan menggunakan aplikasi vmPing untuk memantau konektivitas menggunakan protokol ICMP, serta melalui browser dan aplikasi mobile secara langsung.



Gambar 7. Monitoring vmPing sesudah penerapan *Firewall*

Selain situs, pengujian juga dilakukan terhadap beberapa aplikasi *game online*. Tujuannya adalah untuk memastikan bahwa trafik hiburan yang berpotensi mengganggu produktivitas juga dibatasi secara efektif oleh sistem.

3.3. Data Kuesioner Manajerial (Atasan / Supervisor)

Kuesioner diberikan kepada atasan langsung (Supervisor/Manajer) untuk menilai fokus kerja karyawan sebelum dan sesudah implementasi firewall MikroTik.

1. Instrumen Penilaian

Skala Likert 1–5 (1 = Sangat Rendah, 5 = Sangat Tinggi)

Tabel 2. Hasil Kuesioner Manajemen

Indikator Penilaian Fokus Kerja	Sebelum Implementasi	Sesudah Implementasi
Tingkat fokus karyawan saat jam kerja	2,6	4,1
Kepatuhan terhadap jam kerja produktif	2,8	4,3
Frekuensi distraksi internet non-kerja	4,2	2,1
Efektivitas penyelesaian tugas	2,9	4,0
Disiplin penggunaan internet kantor	2,5	4,2

Hasil kuesioner menunjukkan peningkatan signifikan pada fokus dan disiplin kerja karyawan setelah pembatasan akses internet non-kerja diterapkan, yang dinilai langsung oleh pihak manajemen.

2. Data Statistik Penggunaan Bandwidth Internet

Data diperoleh dari monitoring trafik MikroTik (*Torch / Graph / Interface Traffic*) selama jam kerja.

Tabel 3. Perbandingan Penggunaan Bandwidth (MB/GB)

Jenis Trafik	Sebelum Firewall Sesudah Firewall Perubahan		
Trafik Non-Kerja (Media Sosial, Streaming, Game)	120 GB/bulan	35 GB/bulan	↓ 70,8%
Trafik Kerja (Email, Sistem Internal, Cloud Kerja)	80 GB/bulan	85 GB/bulan	↑ 6,25%
Total Penggunaan Bandwidth	200 GB/bulan	120 GB/bulan	↓ 40%

Analisis Teknis, Trafik non-kerja mengalami penurunan drastis setelah penerapan firewall MikroTik, Trafik kerja relatif stabil bahkan meningkat, menunjukkan bandwidth lebih optimal untuk kebutuhan operasional, Pengendalian akses internet berdampak langsung pada efisiensi jaringan dan produktivitas kerja

4. KESIMPULAN

Berdasarkan hasil penelitian dengan judul “Implementasi Firewall MikroTik sebagai Upaya Meningkatkan Produktivitas Karyawan Melalui Pengendalian Akses Internet Non-Kerja di PT XYZ”, dapat disimpulkan bahwa permasalahan utama jaringan di PT XYZ sebelum penelitian dilakukan adalah tidak terkendalinya akses internet karyawan terhadap konten non-kerja. Kondisi tersebut menyebabkan pemborosan bandwidth, penurunan kualitas layanan jaringan, serta berdampak pada menurunnya fokus dan produktivitas karyawan selama jam kerja. Implementasi firewall MikroTik RouterOS dengan konfigurasi Layer 7 Protocol, Address List, NAT, dan Time-Based Filtering terbukti efektif dalam membatasi akses internet non-produktif dan memprioritaskan layanan yang berkaitan langsung dengan aktivitas kerja. Hasil pengujian jaringan menunjukkan adanya peningkatan kinerja yang signifikan, ditandai dengan penurunan nilai *latency* dan *packet loss*, koneksi jaringan yang lebih stabil, serta distribusi bandwidth yang lebih efisien antar pengguna. Dari sisi pemanfaatan jaringan, data statistik penggunaan bandwidth memperlihatkan penurunan konsumsi trafik non-kerja dari 120 GB/bulan menjadi 35 GB/bulan atau sebesar 70,8%, sementara trafik kerja mengalami peningkatan dari 80 GB/bulan menjadi 85 GB/bulan. Hal ini menunjukkan bahwa penerapan firewall MikroTik mampu mengoptimalkan penggunaan bandwidth sesuai dengan kebutuhan operasional perusahaan. Selain itu, berdasarkan hasil kuesioner manajerial, terjadi peningkatan signifikan pada aspek produktivitas karyawan, di mana tingkat fokus kerja meningkat dari 2,6 menjadi 4,1, kepatuhan terhadap jam kerja produktif meningkat dari 2,8 menjadi 4,3, serta efektivitas penyelesaian tugas meningkat dari 2,9 menjadi 4,0. Penurunan frekuensi distraksi akibat akses internet non-kerja juga terlihat jelas, dari 4,2 menjadi 2,1, berdasarkan penilaian atasan langsung. Lebih lanjut, penerapan fitur monitoring, logging, dan manajemen bandwidth (*Queue*) pada MikroTik memberikan kontrol yang optimal bagi tim IT dalam menjaga keamanan, efisiensi, dan stabilitas jaringan. Secara keseluruhan, penelitian ini membuktikan bahwa implementasi firewall MikroTik memberikan dampak positif yang signifikan terhadap kinerja jaringan dan produktivitas karyawan di PT XYZ, karena akses internet menjadi lebih terarah pada kebutuhan pekerjaan dan distraksi digital dapat dikurangi secara nyata.

DAFTAR PUSTAKA

- [1] P. Limit, A. Browsing, I. Pada, S. Jam, K. Di, and P. T. Xyz, "Jurnal Teknologi Terpadu PENERAPAN LIMIT AKSES BROWSING INTERNET PADA SAAT JAM," vol. 7, no. 1, pp. 31–38, 2021.
- [2] C. N. Syahputri, C. Anggraini, H. F. Anugerah, I. Zufria, and M. I. Nahwi, "Penerapan Kinerja Filter Rule dengan Metode Raw dan Layer 7 Protocol di Router MikroTik," *J. Kridatama Sains Dan Teknol.*, vol. 5, no. 02, pp. 433–447, 2023, doi: 10.53863/kst.v5i02.969.
- [3] I. Saputra, T. U. Kalsum, and H. Alamsyah, "The Implementation Of Network Management And Security Using MikroTik And Proxy Server At SMK N 3 Seluma," *J. Media Comput. Sci.*, vol. 3, no. 1, pp. 17–32, 2024, doi: 10.37676/jmcs.v3i1.5422.
- [4] Haryanto, R. D. Rahmah, and A. P. Sari, "Implementasi Web Proxy Menggunakan Router MikroTik Pada Kantor Suku Dinas Walikota Administrasi Jakarta Barat," *JIKA (Journal Inform. Univ. Muhammadiyah Tangerang)*, vol. 5(3), pp. 298–306, 2021, [Online]. Available: <http://jurnal.umt.ac.id/index.php/jika/article/view/4543>
- [5] I. P. Sari, I. H. Batubara, M. Basri, and A. H. Hazidar, "Implementasi Internet of Things Berbasis Website dalam Pemesanan Jasa Rumah Service Teknisi Komputer dan Jaringan Komputer," *Blend Sains J. Tek.*, vol. 1, no. 2, pp. 157–163, 2022, doi: 10.56211/blendsains.v1i2.136.
- [6] H. Septanto, A. K. Wardani, and A. Hidayatullah, "Pelatihan Crimping Kabel UTP Tipe Straight dan Cross Over Jaringan Komputer LAN untuk Para Pemuda Kelurahan Pulo Gebang, Kecamatan Cakung, Jakarta Timur," *J. Karya untuk Masy.*, vol. 5, no. 1, pp. 45–58, 2024, doi: 10.36914/jkum.v5i1.1081.
- [7] F. Timang, V. Bin Djusmin, and A. Anas, "Implementasi Keamanan Jaringan Menggunakan Web Proxy Pada Dinas Kebersihan Lingkungan Hidup Kota Palopo," no. 2, pp. 41–52, 2023.
- [8] H. P. Fitrian, B. F. Noorjamil, F. Rahmawati, and S. A. Rachman, "Analisis Efektivitas Firewall dalam Memfilter dan Melindungi Lalu Lintas Jaringan," vol. 8, no. 1, pp. 95–102, 2025.
- [9] T. Rahman and H. Nurdin, "Abdul Hamid No.77, RT.8/RW.4, Cawang, Kramat Jati, Jakarta Timur 13630 1 Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri," *Jl. Raya Jatiwaringin*, vol. 5, no. 1, p. 23, 2020.
- [10] O. Jaringan, W. D. I. Kantor, and D. Bumi, "Optimasi jaringan wi-fi di kantor desa bumi jaya melalui pembatasan akses game online," vol. 5, no. 1, pp. 184–191, 2025.
- [11] C. K. Wilujeng and A. Voutama, "Implementasi Firewall Filter Rules Sebagai Filtering Content Pada Jaringan Komputer Menggunakan MikroTik," *JATI (Jurnal Mhs. Tek. Inform.)*, vol. 8, no. 3, pp. 2680–2685, 2024, doi: 10.36040/jati.v8i3.9530.
- [12] R. J. Tampubolon, P. Poningsih, S. Solikhun, I. Gunawan, and Z. M. Nasution, "Implementasi Filtering Firewall Dan Hardening Web Server Untuk Mencegah Serangan Http Dos Pada Dinas Lingkungan Hidup Pematangsiantar," *Device*, vol. 11, no. 2, pp. 21–29, 2021, doi: 10.32699/device.v11i2.2091.
- [13] F. N. A. Baskara Kadi, M. Rendy, "Implementasi Firewall MikroTik Sebagai Marking Route

Untuk,” vol. 2, no. 2, pp. 132–139, 2023.

- [14] G. Z. Muflih, F. Teknik, T. Informatika, K. Jaringan, M. Routeros, and P. Pesantren, “Implementasi Web Filtering Firewall untuk Keamanan pada Jaringan Internet di Pondok Pesantren Al Hidayah Kebumen,” vol. 8, pp. 46–59, 2025.
- [15] S. A. Imawan and S. Dwiasnati, “Implementasi Pemblokiran Situs Dengan Firewall Layer 7 Protokol Menggunakan Metode NDLC Pada Router MikroTik,” vol. 11, no. 1, 2025.