

Volume.1, No.2, September 2023, pp. 41-52 JITAKU. Prodi Informatika, Fakultas Teknik Komputer, Universitas Cokroaminoto Palopo, Sulawesi Selatan, Indonesia. e-ISSN: (2986-7681).

Implementasi Keamanan Jaringan Menggunakan Web Proxy Pada Dinas Kebersihan Lingkungan Hidup Kota Palopo

Fhany Timang¹*, Vicky Bin Djusmin², Aswar Anas³ 1,2,3Universitas Cokroaminoto Palopo, Palopo

Email: ffhanytimang@gmail.com, vickydjusmin@gmail.com, aswaranasspd8@gmail.com

Info Artikel	ABSTRAK				
Dikirim: 3 Maret 2023	Penelitian ini bertujuan untuk melakukan implementasi terhadap				
Diterima: 14 April 2023	keamanan suatu jaringan internet, agar pengguna yang ada pada				
Diterbitkan: 30 September 2023	Dinas Lingkungan Hidup kota Palopo dapat terhindar dari ancaman-				
Kata kunci:	ancaman serangan dari pihak yang tidak bertanggung jawab, seperti				
Web Proxy;	mengambil data kemudian disalahgunakan. Penelitian ini				
Router mikrotik;	menggunakan metode observasi, pengumpulan data (wawancara),				
Jaringan;	dan studi pustaka. Hasil dari penelitian ini adalah keamanan jaringan				
	menjadi lebih optimal dengan adanya pembatasan akses internet pada				
	situs-situs tertentu yang yang dapat membahayakan penggunanya				
dengan diterapkannya web proxy. Metode penelitian yang dig					
adalah kualitatif. Penelitian kualitataif adalah penelitian yar					
	digunakan untuk melihat sistem yang ada pada objek penelitian yang				
	bersifat deskriptif. Dengan menggunakan metode kualitatif yang				
	bersifat deskripif menggunakan teknik pengumpulan data melalui				
	wawancara kepada infrorman yang dianggap berpotensi untuk				
	memberikan informasi tentang inplementasi keamanan jaringan				
	menggunakan web proxy pada dinas lingkungan hidup Kota Palopo.				
	Juga melalui observasi dan dokumentasi. Penelitian ini melihat				
	implementasi keamanan jaringan yang diyakini kurang aman karena				
	tidak menggunakan fitur firewall untuk menyaring (filter) paket data				
	yang masuk dan keluar dari jaringan internal lokal maupun dari				
	jaringan eksternal (internet), yang diidentifikasi melalui alamat IP.				
	Setelah dilakukan penelitian ini maka menghasilkan sebuah solusi				
	berupa router mikrotik, karena router mikrotik mempunyai fitur				
	sistem keamanan jaringan yang lengkap dan mudah digunakan.				

1. PENDAHULUAN

Web proxy adalah jenis proxy yang bekerja pada level aplikasi dan bertindak sebagai perantara antara browser web pengguna dan internet. Web proxy digunakan untuk menyembunyikan alamat IP pengguna dan memungkinkan pengguna untuk mengakses situs web yang diblokir. Sementara itu, server proxy adalah perangkat lunak atau perangkat keras yang bertindak sebagai perantara antara klien dan server tujuan.

Keduanya memiliki fungsi yang sama yaitu untuk menyembunyikan identitas asli pengguna, mempercepat akses internet, mengontrol penggunaan internet, dan membuka akses yang diblokir. Namun, web proxy hanya bekerja pada level aplikasi sedangkan server proxy dapat bekerja pada level jaringan yang lebih luas.

Dinas lingkungan hidup merupakan instansi pemerintahan yang berada di kota Palopo dan telah memiliki akses jaringan internet berupa wifi namun tidak memiliki sistem keamanan yang baik. Keamanan komputer yang tidak baik dapat terinfeksi malware. Penyebabnya adalah membuka situs-situs yang mengandung malware.

Contohnya membuka situs yang mempunyai konten judi online, scam, ataupun situs yang biasanya menyediakan keygen atau crack. Situs-situs tersebut masih dapat di akses, karena belum adanya sistem keamanan jaringan komputer yang dapat meminimalisir penyebaran malware.

Jika hal ini terus – terusan terjadi, maka komputer yang terinfeksi malware akan menyebabkan beberapa program, aplikasi, software, dan bahkan data yang ada di dalam komputer akan rusak dan hilang dengan sendirinya. Ini akan menjadi masalah besar ketika data atau program yang sangat penting tersebut rusak.

Untuk itu diperlukan sebuah analisis mengenai keamanan suatu jaringan internet, agar pengguna jaringan tersebut dapat terhindar dari ancaman-ancaman serangan dari pihak yang tidak bertanggung jawab, seperti mengambil data kemudian disalah gunakan. Penulis tertarik untuk mempelajari sistem web proxy dan solusi yang efisien untuk menyaring situs web berbahaya berdasarkan informasi latar belakang ini.

2. METODE PENELITIAN

Penelitian ini menggunakan jenis penelitian kualitatif. Penelitian kualitatif adalah penelitian yang digunakan untuk melihat sistem yang ada pada objek penelitian yang bersifat deskriptif. Landasan teori dimanfaatkan sebagai pemandu agar fokus penelitian sesuai dengan fakta di lapangan. Selain itu, landasan teori juga bermanfaat memberikan gambaran umum tentang latar penelitian dan sebagai bahan pembahasan hasil penelitian.



Gambar 1. Tahapan Penelitian

2.1. Pengumpulan Data

Berikut adalah langkah-langkah yang dilakukan dalam tahapan penelitian, yaitu:

1. Observasi

Dalam tahap ini, peneliti melakukan observasi pada objek yang dituju, dimana pada penelitian ini penulis mengambil data-data penelitian dan gambaran objek secara umum untuk mengimplementasikan pengoptimalan jaringan.

2. Pengumpulan Data

Teknik pengumpulan data yang digunakan penulis dalam penelitian ini yaitu metode interview atau wawancara, dimana peneliti mengambil beberapa data dari pihak yang bertanggung jawab terhadap objek penelitian, dengan cara mengajukan pertanyaan. Kemudian teknik pengumpulan data lainnya adalah studi pustaka, dimana metode ini merupakan teknik untuk mengumpulkan data dengan cara mempelajari buku dan mencari referensi dari penelitian sebelumnya, baik berupa jurnal online maupun skripsi.

3. Studi Pustaka

Studi pustaka merupakan kegiatan untuk mencari referensi baik itu dari buku dan internet mengenai keamanan jaringan untuk menguatkan data yang akan dibuat.

2.2. Analisis Sistem

Analisis data merupakan upaya atau cara untuk mengelola data menjadi informasi sehingga karakteristik data tersebut mudah dipahami dan bermanfaat untuk solusi permasalahan, terutama masalah yang berkaitan dengan penelitian yang ada di Dinas Lingkungan Hidup Kota Palopo.

2.3. Sistem yang Berjalan



Gambar 2. Sistem yang Berjalan

Dari internet ke modem menyalurkan atau mengirim paket menuju access point untuk memancarkan jaringan. Jaringan yang dipancarkan melalui access point diterima oleh pengguna, kemudian pengguna dapat mengakses jaringan internet melalui komputer, laptop, atau handphone dari jarak jauh maupun dari jarak dekat. **2.4. Sistem yang Diusulkan**

Penambahan mikrotik untuk memblokir situs – situs yang mengandung konten terlarang menggunakan proxy (firewall) sehingga terciptanya sistem keamanan jaringan komputer untuk meminimalisir penyebaran malware di Dinas Lingkungan Hidup Kota Palopo. Dengan demikian akan menghasilkan keamanan jaringan yang lebih optimal.

2.5. Kebutuhan Fungsional

Kebutuhan fungsional dari sistem ini meliputi:

1. Sistem web proxy dapat memfilter situs-situs negatif sehingga terciptanya sistem keamanan jaringan komputer untuk meminimalisir penyebaran malware



Gambar 3.Sistem yang Diusulkan

2. Pengguna dapat mengakses jaringan wifi dengan baik dan optimal.

2.6. Kebutuhan Non-Fungsional

Pada penelitian ini alat dan bahan yang digunakan dalam merancang sistem ini terdiri dari dua yaitu:

- 1. Perangkat Lunak: Sistem operasi windows (64-bit), winbox.
- 2. Perangkat Keras: Laptop/pc, mikrotik RB95Iui-2ND, modem, access point, kabel UTP.

2.7. Implementasi

Tahapan selanjutnya yaitu implementasi pada tahapan ini akan dilakukan penerapan menggunakan web proxy pada mikrotik. Pada tahapan ini akan menjelaskan proses penerapan, langkah-langkah, serta pengujian

terhadap penerapan web proxy. Tahapan dalam penerapan ini yaitu melakukan konfigurasi pada mikrotik menggunakan aplikasi winbox yang berbasis Graphic User Interface (GUI) kemudian menghubungkan mikrotik ke ISP lalu melakukan pemblokiran pada situs – situs berbahaya.

2.8. Penarikan Kesimpulan

Tahap terakhir adalah penarikan kesimpulan. Penarikan kesimpulan dilakukan dari pengumpulan data dan uji coba pada sistem. Kesimpulan merujuk pada hasil akhir penelitian, sehingga dalam penarikan kesimpulan perlu memperhatikan segala aspek dan tahap yang dilakukan selama proses penelitian.

3. HASIL DAN PEMBAHASAN

Hasil penelitian merupakan tahap dimana peneliti melakukan implementasi sistem keamanan jaringan. Hasil dari implementasi sistem keamanan jaringan wifi ini dapat terlihat pada proses pertukaran data, baik pengiriman maupun penerimaan data.

Untuk melakukan implementasi sistem keamanan jaringan digunakan sebuah alat berupa mikrotik. Proses dilakukan dalam melakukan implementasi keamanan jaringan sebagai berikut. 1. Login Winbox



Gambar 4. login winbox

2. Pilih menu interfaces kemudian rename ether I menjadi ISP dan ether II menjadi "admin". Rename bertujuan memberikan nama agar dapat dibedakan.

	ack Set										
⊥ CA	APSMAN										
inter inte	terfaces										
(1) (1)	Ireless										
Di Bri	idge										
🚉 PP	PP I	Interface Interface	List Ethernet Ed	IP Tunnel IP Tunn	el GRE Tunnel	VLAN VRRP	Bonding LTE				
🕎 Sw	vitch			tect Internet							
1. Me	esh			teet memor	and house in			100.0	Dealers to the	D. Destar (c. (c)	
The Ib	P	B & ADMIN	Ethemet	Actual N	1500 1598	11.21	sbos	2.0 kbps	Packet (p/s)	Pot Packet (p/s)	2
O MF	PLS P	R 🔶 ISP	Ethernet		1500 1598	0	bps	0 bps	(0	0
G R G R G R	Interface Lis	st									
D L	Interface	Interface Li	st Etherne	t EoIP Tur	nnel IP Tu	innel Gi	RE Tunnel	VLAN	VRRP	Bonding	
	+ -	*	- 7	Detect Int	emet						
In In	1.1.7										
⊕ W Br	Interface	<wlan1></wlan1>									
H Br H Br H PI S S	General	<wlan1> Wireless</wlan1>	HT HT M	ICS WDS	Nstreme	NV2	Status		Oł	× □ <	
H K H P S M P M B	General	<wlan1> Wireless Mode</wlan1>	HT HT M	ICS WDS	Nstreme	NV2 S	Status		Oł Can	<	C × FP Ti ▼
	General	<wlan1> Wireless Mode Band</wlan1>	HT HT M ap bridge	ICS WDS	Nstreme	NV2 S	Status Ŧ		Oł Cano App	< <tr> cel lly</tr>	
	General	<wlan1> Wireless Mode Band hannel Width</wlan1>	HT HT M ap bridge 2GHz-B/G 20/40MHz	ICS WDS 7/N z XX	Nstreme	NV2 S	Status		Oł Can App Disal	cel ly	
	General	<wlan1> Wireless Mode Band hannel Width Frequency</wlan1>	HT HT M ap bridge 2GHz-B/G 20/40MHz	ICS WDS	Nstreme	NV2 S	Status		Oł Can App Disa	cel ble	
H WU H BP H P N H P H P H P H P H P H P H P H P	General	<wli> Wireless Mode Band hannel Width Frequency SSID </wli>	HT HT M ap bridge 2GHz-B/G 20/40MHz auto	ICS WDS i/N z XX	Nstreme	NV2 S	Status 		Oł Cano App Disal	Cel oly oble onent	C/ FP Tì.▼

Gambar 6.wlan1 dan anable

3. Klik wlan1 dan enable ($\sqrt{}$) fungsinya untuk menghubungkan internet melalui wireless. Pastikan station diganti menjadi "ap bridge", kolom band diganti menjadi 2GHz-B/G/N, kolom channel width diganti menjadi 20/40MHz XX, kolom frequency diganti menjadi auto, dan SSID diganti menjadi "DLH-PLP".

4. Setelah itu masuk menu IP pilih DHCP client dan klik "+". Dhcp server berfungsi memberikan alamat IP otomatis yang valid ke DHCP client. Konfigurasi lainnya juga diberikan, seperti subnet mask, default gateway, DNS server, dan parameter jaringan lainnya yang diperlukan oleh perangkat untuk beroperasi dengan benar.

🖋 Quick Set		
CAPsMAN		
Interfaces		
Wireless		
Bridge		
🏣 PPP		
🙄 Switch		
T. Mesh		
꽃 IP	1	ARP
MPLS	1	Accounting
💢 Routing	1	Addresses
🖁 System	1	Cloud
👰 Queues		DHCP Client
Files		DHCP Relay
🗏 Log		DHCP Server
RADIUS		DNS
K Tools	1	Firewall
💷 New Termina		Hotspot
Make Supout	rif	IPsec
🚫 New WinBox		Kid Control

Gambar 7.menu ip

5. Pastikan interface ISP, user peer DNS dan NTP tercentang, serta add defalut route "yes". Jika semua sudah dilakukan klik apply dan ok.

DHCP Client DHCP	New DHCP Client			□×	
+ - / *	DHCP Advanc	ed Status		ОК	Find
Interface	Interfac	e: ISP	₹	Cancel	
		Use Peer DN	IS	Apply	
		Use Peer NT	TP	Disable	
	Add Default Rout	e: yes	₹	Comment	
				Сору	
				Remove	
				Release	
				Renew	
	enabled		Status: stopped		
0 items					

Gambar 8.interface isp

6. Kemudian masuk menu IP dan addresses. Addresses berfungsi membantu pengguna untuk mengatur dan mengelola alamat IP pada jaringan. Ini termasuk membuat jaringan yang berbeda, menetapkan alamat IP pada perangkat jaringan, dan memberikan izin akses terhadap jaringan untuk pengguna yang berbeda.

🚀 Quick Set						
CAPsMAN						
Interfaces						
Wireless						
👯 Bridge						
🛓 PPP		Adde	nan Lint			
🙄 Switch		Addi				
°∏° Mesh		+		Y		
₩ IP ト	ARP		Address /	Network	Interface	
MPLS N	Accounting		+ 192.168.1.25/24	192.168.1.0	ISP	
3 Routing	Addresses					
🐼 System 🗅	Cloud					
🙅 Queues	DHCP Client					
Files	DHCP Relay					
🛄 Log	DHCP Server					
and RADIUS	DNS					
🔀 Tools 🛛 🗅	Firewall					
Mew Terminal	Hotspot					

Gambar 9.menu ip

7. Kemudian atur address menjadi 172.22.22.1/24 dan interface menjadi admin, lalu pilih apply dan ok.

Address List	
	Find
Address / Network Interface	-
New Address	
Address: 172.22.22.1/24 OK	
Network: Cancel	
Interface: ISP The Apply	
Disable	
Comment	
Сору	
Remove	
enabled	
1 item	

Gambar 10.address

8. Setelah klik + dan atur address menjadi 10.10.20.1/24 serta interface diubah menjadi wlan1.

New Address	
Address: 10.10.20.1/24	ок
Network:	Cancel
Interface: ISP ADMIN	∓ Apply
ISP ether3	Disable
ether4 pwr-line 1	Comment
wan T	Сору
	Remove
enabled	



9. Pilih menu DNS lalu setting servers ke 8.8.8.8 dan 8.8.4.4. Setelah itu pastikan semuanya sesuai seperti max UDP, query timeout, max concument queries dan TCP sessions. DNS berfungsi menerjemahkan nama domain menjadi alamat IP. DNS server public 8.8.8.8 (milik Google) dan 1.1.1.1 (milik cloudflare).

	늘 PPP		DNS Settings		
	Thesh		Servers: 8.8.8.8	٠	OK
	🐺 IP 🗈 N	ARP	8.8.4.4		Cancel
		Accounting	Dynamic Servers: 192.168.1.1		Apply
	C Routing	Addresses	Use DoH Server:		0.0
	System N	Cloud	Verfy DoH Cettificate		Static
	🙅 Queues	DHCP Client			Cache
	Files	DHCP Relay	Allow Remote Requests		
	🗒 Log	DHCP Server	Max UDP Packet Size: 4096		
	RADIUS	DNS			
	🔀 Tools 🛛 🗅	Firewall	Query Server Timeout: 2.000 s	\square	
	🕅 New Terminal	Hotspot	Query Total Timeout: 10.000 s		
	Make Supout.rif	IPsec	Max. Concurrent Queries: 100		
	New WinBox	Kid Control			
×	🔣 Exit	Neighbors	Max. Concurrent TCP Sessions: 20	٠	

Gambar 12.menu dns

10. Kemudian pilih menu firewall. Firewall berfungsi sebagai pelindung jaringan, baik yang berasal dari WAN (Internet) maupun dari LAN (Local). Firewall menjaga keamanan jaringan dengan membatasi lalu lintas data dari network lain yang melewati router.

👯 Bridge			
🛓 PPP			
🙄 Switch		Frewall	
•] Mesh		Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols	
∰ IP ト	ARP	L Contern Find all	I
🕑 MPLS 🛛 🗅	Accounting		
🔀 Routing 🛛 🗅	Addresses	# Action Unain Src. Address Dst. Address Proto Src. Port Dst. Port in. Inter Uut. In	it l ▼
🔯 System 🗈	Cloud		
🗣 Queues	DHCP Client		
Files	DHCP Relay		
🗒 Log	DHCP Server		
RADIUS	DNS		
🗙 Tools 🛛 🗅	Firewall		
New Terminal	Hotspot		
Ы Make Supout rif	IPsec		
🔘 New WinBox	Kid Control		

Gambar 13.menu firewall

11. Klik menu NAT kemudian "+" dan akan muncul new NAT rule. Pilih fitur action, pilih masquerade dan ok. Masquerade berfungsi mengamankan jaringan lokal yang digunakan untuk mengubah alamat IP sumber perangkat yang ada dalam jaringan lokal menjadi alamat IP publik router, sehingga lalu lintas data yang keluar dari jaringan lokal terlihat berasal dari alamat IP router.

Firewall	New NAT Rule	
Filter Rules NAT Mangle Raw Service	General Advanced Extra Action Statistics	ОК
	Action: masquerade	Cancel
# Action Chain Src. Address	Log	Apply
	Log Prefix:	Disable
	To Ports:	Comment
		Сору
		Remove
		Reset Counters
		Reset All Counters
•		-
0 items		
	enabled	

Gambar 14.menu nat

12. Setelah itu reboot winbox terlebih dahulu dan yes. Reboot membantu membantu mengoptimalkan kinerja sistem, melakukan pembaruan otomatis, mengosongkan RAM, dan mengatasi kesalahan dengan cara memulai ulang perangkat.

10.48			
	PPP		
	Switch		
° 1°	Mesh	Auto Upgrade	
255	IP D	Certificates	Reboot
0	MPLS N	Clock	NEDO01
3\$	Routing D	Console	
302	System 1	History	Do you want to reboot the router?
-	Queues	Identity	,
	Files	LEDs	
臝	Log	License	Yes No
4 ?	RADIUS	Logging	
\sim	Tools N	Note	
<u> </u>	New Terminal	Packages	
	Make Supout.nf	Password	
0	New WinBox	Ports	
< 🖾	Exit	Reboot	
2		Reset Configuration	

Gambar 15.reboot weinbox

13. Pilih menu hotspot kemudian hotspot setup. Hotspot adalah fungsi yang memungkinkan otentikasi pengguna yang akan menggunakan jaringan internet nirkabel (Wi-Fi). Dengan hotspot, Anda dapat menyediakan akses internet kepada pelanggan melalui menu login.

°T <mark>°</mark> Mesh		ARP						
IP	\triangleright	Accounting	Hotspot					
MPLS		Addresses	Servers	Server Profiles	Users	User Profiles	Active	Host
Carting Routing		Cloud					7101110	11000
💭 System		DHCP Client	+ -		Rese		tspot Setu	p
👰 Queues		DHCP Relay	Nam	e	Interfa	ice	Address F	ool
Files		DHCP Server						
🚊 Log		DNS						
RADIUS		Firewall						
🔀 Tools	\uparrow	Hotspot						
New Terminal		IPsec						
Make Supout.	if	Kid Control						

Gambar 16.menu hotspot

14. Pastikan hotspot interface "wlan1", local address "10.10.20.1/24", angka terakhir diganti menjadi 100, certificate "none", ip address "0.0.0.0", DNS server ditambah "192.168.1.1", rename DNS menjadi "dlh-plp.net", password for user "admin", dan setup successfully.

Hotspot Setup	Hotspot Setup
Select interface to run HotSpot on	Set HotSpot address for interface
HotSpot Interface: wlan1	Local Address of Network: 10.10.20.1/24
	Masquerade N
Back Next	Back Next
Hotspot Setup	
Set pool for HotSpot addresses	Hotspot Setup
Address Pool of Network: 10.10.20.2-10.10.20.100	Select hotspot SSL certificate
	Select Certificate: none
Back Next Cano	Back Next
Hotspot Setup	Hotspot Setup
Hotspot Setup Select SMTP server	Hotspot Setup Setup DNS configuration
Hotspot Setup Select SMTP server IP Address of SMTP Server: 0.0.0.0	Hotspot Setup Setup DNS configuration DNS Servers: 18.8.8.8
Hotspot Setup Select SMTP server IP Address of SMTP Server: 0.0.0.0	Hotspot Setup Setup DNS configuration DNS Servers: 6.8.8.8 8.8.4.4
Hotspot Setup Select SMTP server IP Address of SMTP Server: 0.000 Back Next	Hotspot Setup Setup DNS configuration DNS Servers: 8.8.8.6 8.8.4.4 192.168.1.1
Hotspot Setup Select SMTP server IP Address of SMTP Server: 0.0.0.0 Back Next Hotspot Setup	Hotspot Setup Setup DNS configuration DNS Servers: 8.8.8.8 8.8.4.4 192.168.1.1 Back Next
Hotspot Setup Select SMTP server IP Address of SMTP Server: 0.0.0.0 Back Next Hotspot Setup DNS name of local hotspot server	Hotspot Setup Setup DNS configuration DNS Servers: 8.8.8.6 8.8.4.4 192.168.1.1 Back Next Hotspot Setup
Hotspot Setup Select SMTP server: 0.0.0.0 IP Address of SMTP Server: 0.0.0.0 Back Next Hotspot Setup DNS name of local hotspot server DNS Name: dih.pip.net	Hotspot Setup Setup DNS configuration DNS Servers: 88.8.6 8.8.4.4 192.168.1.1 Back Next Hotspot Setup Create local HotSpot user
Hotspot Setup Select SMTP server IP Address of SMTP Server: 00.0.0.0 Back Next DNS name of local hotspot server DNS name: @h.pip.net	Hotspot Setup Setup DNS configuration DNS Servers: 88.8.9 8.8.4.4 192.168.1.1 Back Next Hotspot Setup Create local HotSpot user Name of Local HotSpot User, admin
Hotspot Setup Select SMTP server IP Address of SMTP Server. 0.0.0.0 Back Next Hotspot Setup DNS name of local hotspot server DNS Name: [dh-pip.net]	Hotspot Setup Setup DNS configuration DNS Servers: [8.8.8.8] 8.8.4.4 192.168.1.1 Back Next Hotspot Setup Create local HotSpot user Name of Local HotSpot user Password for the User; admin

Gambar 17.hotspot interface

15. Di menu user profiles klik "+" dan ganti nama uprof1 menjadi "R.KADIS", shared users ketikan "2", dan rate limit "5M/5M". User profiles berfungsi menjadi login administrator, pengaturan hak akses, dan monitoring lalu lintas jarigan.

Gene	al Queue So	ripts		OK	
terost	Name:	R.KADIS		Cancel	
Isers User Profiles	Address Pool:	none		Apply	Cookie
	Session Timeout:		•	Сору	
Name / S	Idle Timeout:	none	• • j	Remove	
😝 default Ki	epalive Timeout:	00:02:00	▲ '		
S	atus Autorefresh:	00:01:00			
	Shared Users:	2			
	Rate Limit (rx/tx):	5M/5M	•		
		 Add MAC Cookie 			
MAC	Cookie Timeout:	3d 00:00:00			
	Address List:		\$		
	Incoming Filter:		•		
	Outgoing Filter:		•		
Incom	ing Packet Mark:		•		
0utgo	ing Packet Mark:		•		
0	pen Status Page:	always	Ŧ		
		Transparent Proxy			



16. Tambahkan lagi user profiles, rename menjadi "KABID", shared user "3", rate limit "5M/5M", kemudian tambah lagi rename menjadi "SEKERTARIS", shared user "4", rate limit "5M/5M", dan tambah lagi rename menjadi "PELAYANAN", shared user "8", rate limit "10M/10M", pilih apply dan ok.

lotspot User Profile <kabid></kabid>			lotspot User Profile <	SEKERTARIS>		
General Queue Scripts		ОК	General Queue	Scripts		Oł
Name: KABID		Canc	Nan	ne: SEKERTARIS		Can
Address Pool: none		∓ Appl	Address Po	ool: none	₹	Арр
Session Timeout:		Cop	Session Timeo	ut:	•	Cor
Idle Timeout: none	•	A Remo	Idle Timeo	ut: none	₹ ▲	Remo
Keepalive Timeout: 00:02:00]▲	Keepalive Timeo	ut: 00:02:00	▲	
Status Autorefresh: 00:01:00			Status Autorefree	sh: 00:01:00		
Shared Users: 3			Shared Use	ers: 4		
Rate Limit (rx/tx): 5M/5M		▲	Rate Limit (nx/t	tx): 5M/5M	▲	
Add MA	C Cookie			Add MAC Co	okie	
MAC Cookie Timeout: 3d 00:00:0	0		MAC Cookie Timeo	ut: 3d 00:00:00		
	Hotspot User Profile <p< th=""><th>ELAYANAN></th><th></th><th></th><th></th><th></th></p<>	ELAYANAN>				
	General Queue S	cripts		OK		
	Name	PELAYANAN		Cancel		
	Address Pool	: none	₹	Apply		
	Session Timeout	:		Сору		
	Idle Timeout	: none	₹ ▲	Remove		
	Keepalive Timeout	: 00:02:00	▲			
	Status Autorefresh	: 00:01:00				
	Shared Users	: 8	▲			
	Rate Limit (rx/tx)	: 10M/10M	▲			
		Add MAC Cooki	e			
	MAC Cookie Timeout	: 3d 00:00:00				

Gambar 19.user profiles

17. Setelah itu pilih menu users dan tambahkan hotspot user baru. Ubah server menjadi hotspot1, rename "kadis", password "kadis", dan pilih profile "R.KADIS".

Hotspot							
Servers	Server Profile	s Users	User Profiles	Active	Hosts	IP Bindings	Serv
+ -	lew Hotspot Us	er					×
S	General Limit	s Statisti	ics			ОК	
	Server:	hotspot1		•	5 [Cancel	
	Name:	kadis				Apply	
	Password:	•••••				Disable	
	Address:					Comment	
	MAC Address:					Сору	
	Routes:	n.KADIS				Remove	
	Email:				,	Reset Counte	rs
					F	Reset All Count	ers

Gambar 20.menu user

18. Tambahkan lagi user baru. Ubah server menjadi "hotspot1", rename "kabid", password "kabid", profile "kabid". Kemudian tambahkan lagi user baru ubah server menjadi "hotspot1", rename "sekertaris", password "1234", profile "sekertaris". Terakhir tambahkan lagi user baru ubah server menjadi "hotspot1", rename "user", password "user", profile "pelayanan", pilih apply an ok.

Hotspot User <	use	r>						Hotspot Us	er ⊲k	abid:	>			
General Lim	nits	Statistics				ОК		General	Limi	its :	Statistics		Γ	ОК
Server:	h	otspot1		Ŧ		Cancel		Ser	ver:	hots	pot1	₹		Cancel
Name:	us	ser				Apply		Na	me:	kabi	d			Apply
Password:	-	••				Disable		Passw	ord:	•••••				Disable
Address:	Ļ			•		Comment	-	Addr	ess:			•		Comment
MAC Address:						Сору	_	MAC Add	ess:					Conv
Routes:	Ē			•		Remove	_	Pr	otile:	KAB	ID	-		Bemove
Email:	F			-	F	Reset Counte	ers	Rol	nail:					Reset Counters
					Re	eset All Courr	ters		nuii.					Reset All Countern
			Hotspor Genera Par A MAC A	Serv Nar sswo ddre Prof Rout	Limits ver: h me: s ord: * ess: file: S tes: nail:	Statistics otspot1 ekertaris EKERTARIS	6		₹ ▼ ₹ ₹		OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters			

Gambar 21.ubah server

19. Masuk menu firewall kemudian pilih filter rules klik advanced, ketik facebook.com di kolom content. Setelah itu, pilih extra dan time, serta pilih action dan pilih drop. Action = drop berfungsi mengamankan jaringan dengan menghindari lalu lintas yang mencurigakan atau berbahaya secara diam-diam.

Interfaces			Frewall						
Wireless			Filter F	Rules NA	T Mangle	Raw	Service Ports	Connections	Address List
Bridge					2 @ 5	7 (o	Reset Counters	C Report A	Countere
🟣 PPP				- [* [*					Counters
TSwitch			#	New Firewa	all Rule				
*T <mark>\$</mark> Mesh			1 1	General	Advanced	Extra	Action Stat	ietice	
ESS IP	1	ARP		Cicitoria		LAura	Action Stat	lauca	
MPLS	\sim	Accounting		S	rc. Address L	ist:			•
3 Routing	1	Addresses		D	st. Address l	list :			•
🔯 System		Cloud							
💂 Queues		DHCP Client		۱۱	ayer / Proto	COI:			•
Files		DHCP Relay			Conte	ent: 📃	facebook.com		
🚊 Log		DHCP Server		с.	nnection Bv	tes:			•
RADIUS		DNS			onnection B:	ata ·			
🔀 Tools	1	Firewall							
Dew Termin	al	Hotspot		Per Conne	ection Classif	her:			
D. H.L. O		IPass		Src	MAC Addre	ess:			— —
Firewall Rule	\diamond								ШŇ
General	Advan	iced Extra	Action	Statistics				Ok	(
Actio	n: dro	p					Ŧ	Cano	cel
		Log						Арр	ly
Log Prefi	x:						•	Disat	ble
								-	

Gambar 22.menu firewall

20. Lakukan hal yang sama dengan drop "tiktok.com", "Instagram.com", "poker88.com", "luxury138dd.com", "qq-domino.com", "omiqq.com", "pornhub.com", "xhamster", "redtube.com", "sex.com", "canibalcafe.com".

New Firewall Rule	
General Advanced Extra Action Statistics	ОК
Src. Address List:	Cancel
Dst. Address List:	Apply
Layer7 Protocol:	Disable
Content: tiktok.com	Comment

Gambar 23.drop

21. Hasil Pemblokiran

D 🗟 14144	on x f, antigation x f factorizon	X . New tab	× 🗟 porma	100m		× +			ø
- C O I	https://bkbok.com		.A ^b	\$	8	0 0	٢	-	
	Hmmm can't reach this page								
	The connection was reset.								
	Try:								
	Banning network diagnostics with Get Halp								
	Checking the connection								
	Checking the proxy and the fermal								
	HIA, COMMETTON, MORT								
C Microsof	It Edge								
				_					

Gambar 24.hasil pemblokiran

Sistem web proxy mampu memblokir kurang lebih 1500 URL, contoh nama-nama URL yang dapat diblokir oleh web proxy mikrotik yang terdapat pada mikrotik.

No	Kategori	Alamat Web
1.	Social Media	www.facebook.com
2.		www.tiktok.com
3.		www.instagram.com
4.	Perjudian	www.poker88.com
5.		www.luxury138dd.com
6.		www.qq-domino.com
7.		www.omiqq.com
8.	Pornografi	www.p*rnh*b.com
9.		www.xhamster.com
10.		www.r*dtube.com
11.		www.s*x.com
12.	Kekerasan	www.cannib*lcafe.ca

Tabel 1 Daftar Website yang Diblokir

Sistem web proxy mampu memblokir kurang lebih 150 keyword, diantaranya 50 keyword porno berbahasa indonesia, 50 keyword berbahasa asing, dan 50 keyword lain (kekerasan, perjudian, dan kejahatan). Contoh nama-nama keyword yang dapat diblokir di mikrotik

label	2 Daftar Keyword yang Diblokir	
	Pemblokiran Keyword	
Keyword	Tanpa Proxy	Dengan Proxy Filter
P*rn	Allow	Denied
S*x	Allow	Denied
B*k*p	Allow	Denied
Inovatif	Allow	Allow
Artikel	Allow	Allow

Implementasi sistem keamanan jaringan yang sesuai pada Dinas Lingkungan Hidup Kota Palopo adalah menggunakan mikrotik dengan bantuan firewall. Perbedaan sistem keamanan jaringan wifi yang lama dengan sistem keamanan dan pembuatan sistem keamanan jaringan wifi yang baru adalah menggunakan sistem keamanan dengan bantuan firewall, sedangkan sistem keamanan yang lama tidak menggunakan firewall sehingga pengguna dapat mengakses internet dengan lebih baik lagi.

Sosial media dilakukan pemblokiran untuk membatasi penggunaannya saat bekerja, karena bukan menjadi bagian dari pekerjaan. Pegawai dapat mengakses sosial media jika diizinkan oleh admin. Banyak dampak positif dalam penggunaan sosial media, akan tetapi terdapat juga dampak negative didalam sosial media. Maka dari itu penggunaanya harus dibatasi.

Pemfilteran web proxy dengan mikrotik saat membuka website memberikan efek waktu akses lebih cepat, akan tetapi dalam penelitian ini pemfilteran web proxy dengan mikrotik tidak mampu menangkap seluruh konten tidak sehat pada penggunaan internet. Disamping karena terlalu banyaknya situs tidak sehat juga disebabkan

beberapa definisi dari keyword memiliki kesamaan makna, yaitu kata "cerdas" yang dalam bahasa indonesia memiliki arti pandai dan "cerdas" dalam bahasa spanyol berarti memiliki arti bulu, pada situs www.cerdas.com yang seharusnya terdapat konten yang positif didalamnya ternyata didalamnya terdapat konten pornografi. Web proxy mikrotik juga tidak bisa memblokir konten email, isi file gambar, video, iklan yang menggunakan javascript dan flash.

4. KESIMPULAN

Dari hasil penelitian yang dilakukan dan konfigurasi usulan, maka dapat ditarik kesimpulan bahwa dengan penerapan web proxy, maka keamanan jaringan menjadi lebih optimal dengan adanya pembatasan akses internet pada situs-situs tertentu yang dapat membahayakan penggunanya.

Penggunaan bandwidth internet untuk koneksi langsung menjadi lebih berkurang dan juga kemampuan untuk membatasi akses/memfilter sebuah permintaan data dari suatu server akan memfilter situs maupun aplikasi yang boleh dan tidak boleh diakses oleh client.

DAFTAR PUSTAKA

- M. Novriansyah, "Pemanfaatan Web Proxy Sebagai Pengoptimal Keamanan Jaringan Wireless LAN,". JURNAL KHATULISTIWA INFORMATIKA, Vol. 8(1), 34-39, 2020.
- [2] N. Pendang, "Analisis Sistem Keamanan Jaringan Wifi Menggunakan Mikrotik Pada Smp Negeri 7 Palopo," 2020.
- [3] I. Afifuddin, "Analisis Kinerja Web Proxy Dan Management Bandwith Dengan Metode PCQ (Studi Kasus: Smpn 8 Bandar Lampung)," Teknologipintar.Org, Vol. 2(10), 1-13, 2022.
- [4] M.R. Maulana, "Analisa Penerapan Filtering Proxy Server Pada Keamanan Jaringan Komputer Untuk Meminimalisr Penyebaran Malware (Studi Kasus Cakrabuana Cruiseship & School Cirebon)," Jurnal UMJ, Vol. 12, 64-73, 2021.
- [5] F. M. Naufal," Implementasi Keamanan Hotspot Menggunakan Proxy Dan Firewall Dalam Mengatasi Resiko Ancaman Serangan," Jurnal Ilmiah Rekayasa Dan Manajemen Sistem Informasi, Vol. 8(2), 148-154, 2022.
- [6] A. S. Wantoro, "Sistem Monitoring Perawatan Dan Perbaikan Fasilitas PT PLN (Studi Kasus : Kota Metro Lampung)," Jurnal TEKNO KOMPAK, Vol. 15(1), 116-130, 2021.
- [7] R. Ocanitra, "Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port Pada Vitaa Multi Oxygen," Jurnal Sistem Dan Teknologi Informasi, Vol. 7(1), 52-59, 2019.
- [8] A. Mikola, "Analisis Load Balancing Berbasis Mikrotik Dalam Meningkatkan Kemampuan Server Di Institut Shanti Bhuana," Journal Of Information Technology, Vol. 2(2), 17-20, 2022.
- [9] M. Effendy, "Analisa Keamanan Jaringan Local Area Network (LAN) Pada PT. Banaran Sukses Mandiri Depok," 14-31, 2019.
- [10] U. S. Dartono, "Penerapan Metode Per Connection Classifier (Pcc) Pada Perancangan Load Balancing Dengan Router Mikrotik," Jurnal Elektro Dan Informatika Swadharma (JEIS), Vol. 1(1), 2021.