



PERANCANGAN SISTEM *WEB FILTERING* DENGAN METODE *DNS FORWARDING* PADA JARINGAN KOMPUTER BERBASIS MIKROTIK ROUTEROS

Randy Ikhsan Ramadhan^a, Siti Madinah Ladjamuddin^b

^a Teknik Informatika, randyikhsanramadhan@gmail.com, Institut Sains dan Teknologi Nasional

^b Teknik Informatika, citymadinah07@istn.ac.id, Institut Sains dan Teknologi Nasional

ABSTRACT

Internet services in the age of technology like today are certainly helpful in our daily lives. There are so many benefits that can be obtained from this Internet services, such as finding sources of information, sending various information, online communicating, etc. However, it is undeniable that Internet services has negative websites. One of solution to prevent network users from accessing these negative websites is by implementing web filtering system. Therefore, the purpose of this research is to design a network security system that is used as web filtering to minimize access to negative websites on the Internet. To achieve this, the author used DNS Forwarding method to design the prevention system on a computer network. DNS Forwarding is a useful method for filtering out websites that have negative content and also useful for forwarding those websites to other websites that healthier and safer. The design of this network security system is applied to a computer network based on MikroTik RouterOS that utilizes the MikroTik RB941-2nD-TC hAP-Lite as the main device. The results of the web filtering system design with the DNS Forwarding method are proven to be able to minimize the access to negative websites on the user's network system when accessing the Internet.

Keywords: *Web Filtering, DNS Forwarding, MikroTik Router*

ABSTRAK

Penggunaan layanan Internet pada zaman teknologi seperti sekarang ini tentunya sangat membantu dalam kehidupan sehari-hari. Banyak sekali manfaat yang bisa didapatkan dari layanan Internet ini, seperti mencari sumber informasi, mengirim berbagai informasi, berkomunikasi jarak jauh, dan lain sebagainya. Namun tidak dapat dipungkiri bahwa layanan Internet juga memiliki situs web yang bermuatan negatif. Salah satu solusi untuk mencegah pengguna jaringan Internet dalam mengakses situs web bermuatan negatif tersebut dapat dilakukan dengan cara menerapkan sistem *web filtering*. Oleh karena itu, tujuan dalam penelitian ini adalah untuk merancang suatu sistem keamanan jaringan yang digunakan sebagai *web filtering* guna meminimalisir pengaksesan situs web bermuatan negatif yang terdapat di Internet. Dalam mewujudkan hal tersebut, penulis menggunakan metode *DNS Forwarding* untuk merancang sistem tersebut pada sebuah jaringan komputer. *DNS Forwarding* merupakan sebuah metode yang berguna untuk menyaring situs web yang memiliki muatan negatif dan juga berguna untuk mengalihkan situs web tersebut ke situs web lainnya yang lebih sehat dan aman. Perancangan sistem keamanan jaringan ini diterapkan pada jaringan komputer berbasis MikroTik RouterOS yang memanfaatkan MikroTik RB941-2nD-TC hAP-Lite sebagai perangkat utamanya. Hasil dari perancangan sistem *web filtering* dengan metode *DNS Forwarding* ini terbukti dapat meminimalisir pengaksesan situs web bermuatan negatif pada sistem pengguna saat mengakses jaringan Internet.

Kata kunci: *Penyaringan Situs Web, DNS Forwarding, MikroTik Router*

1. PENDAHULUAN

Pada zaman modern saat ini, perkembangan dalam bidang teknologi terjadi dengan sangat pesat. Perkembangan yang semakin pesat ini membawa perubahan yang tentunya memberikan banyak manfaat bagi kehidupan sehari-hari. Salah satu hal yang sangat berkembang dalam bidang teknologi ialah jaringan komputer. Jaringan komputer merupakan media dasar dalam menjalankan aktivitas dan produktivitas dengan memanfaatkan teknologi informasi.

Berbicara mengenai jaringan komputer biasanya berkaitan erat dengan layanan akses Internet. Penggunaan akses Internet ini tentunya sangat membantu dalam berbagai hal yang berkaitan dengan

Received Mei 17, 2022; Revised Juni 5, 2022; Accepted Juli 25, 2022

teknologi informasi seperti mencari sumber informasi, mengirimkan berbagai informasi, berkomunikasi jarak jauh, dan sebagainya. Akan tetapi, tidak dapat dipungkiri bahwa layanan Internet ini terdapat situs web yang memiliki muatan negatif atau terlarang seperti situs pornografi, perjudian, penipuan, dan sebagainya.

Salah satu solusi untuk mengatasi dan mencegah pengguna jaringan komputer dalam mengakses situs web bermuatan negatif ialah dengan menerapkan sistem *web filtering* terhadap jaringan komputer tersebut. Terdapat beberapa penelitian terdahulu yang sudah dilakukan dalam melakukan perancangan sistem *web filtering* terhadap jaringan komputer.

Dalam penelitian yang dilakukan oleh Nurfauzi et al. (2018), perancangan sistem untuk mengatur *filtering* situs web dilakukan dengan memanfaatkan layanan Firewall pada sebuah jaringan komputer yang berbasis MikroTik di sebuah sekolah. Selain itu, terdapat juga penelitian terkait implementasi sistem *web filtering* dengan memanfaatkan fitur *Web Proxy* yang ada pada MikroTik seperti penelitian yang dilakukan oleh Haryanto et al. (2021). Kedua penelitian tersebut terbukti dapat menyaring, memblokir atau membatasi akses terhadap situs-situs web tertentu yang memiliki muatan negatif atau berpotensi membahayakan sistem pengguna saat mengakses jaringan Internet.

Oleh karena itu, penelitian ini dilakukan untuk mengembangkan penelitian tersebut, namun yang membedakan dari penelitian ini adalah perancangan sistem keamanan jaringan sebagai *web filtering* ini menggunakan metode *DNS Forwarding*, yang mana metode ini selain dapat digunakan untuk menyaring situs web bermuatan negatif, dapat juga digunakan untuk mengalihkan (*forwarding*) situs web bermuatan negatif tersebut ke situs lainnya yang lebih sehat dan aman.

2. TINJAUAN PUSTAKA

2.1. Jaringan Komputer

Menurut Lestari dan Permana (2019), jaringan komputer merupakan sebuah sistem yang terdiri dari sekelompok komputer otonom yang saling terkoneksi satu dengan yang lainnya menggunakan protokol komunikasi melalui media komunikasi untuk dapat saling berbagi informasi, program-program atau pun penggunaan perangkat. Lestari dan Permana (2019) juga menjelaskan bahwa suatu jaringan komputer terdiri dari komputer, *software* dan perangkat jaringan yang bekerja sama dalam suatu ruang lingkup untuk mencapai suatu tujuan. Untuk mencapai tujuan tersebut, setiap bagian dari jaringan komputer meminta dan memberikan layanan. Pihak yang meminta atau menerima layanan disebut dengan *client* dan yang memberikan atau mengirim disebut *server*. Arsitektur jaringan ini disebut dengan sistem *client-server* yang mana telah digunakan pada hampir seluruh aplikasi jaringan komputer di dunia.

2.2. Internet

Menurut Vinka dan Michele (2021), *Interconnected Network* atau yang biasa dikenal dengan Internet adalah sebuah sistem teknologi informasi yang menghubungkan perangkat di seluruh dunia dan membentuk suatu jaringan yang sangat luas. Jaringan Internet ini berisi berbagai informasi dalam bentuk teks, gambar, audio, video, dan lain-lain yang diakses melalui jaringan *world wide web* (WWW). Publik dapat mengakses Internet dengan mengirimkan data menggunakan standar Protokol Internet atau yang dikenal sebagai IP. Internet dapat dikatakan sebagai media yang digunakan untuk mengefisienkan proses komunikasi dalam skala global menggunakan aplikasi seperti *website*, *email*, VoIP, dan lain-lain.

Menurut Yusup et al. (2019), karakteristik komputer dan Internet, perorangan ataupun secara kelompok dapat bekerja tanpa dibatasi oleh tempat dan waktu. Kapan saja dan di mana saja orang bisa menjalankan pekerjaannya dengan komputer dan Internet.

2.3. Sistem Keamanan Jaringan

Dilansir dari *www.kompas.com* (2021b), sistem merupakan sekumpulan elemen atau komponen yang saling berkaitan dan saling mempengaruhi dalam melakukan kegiatan bersama untuk mencapai suatu tujuan tertentu. Sedangkan berdasarkan penjelasan yang dikutip dari *www.cisco.com* (2021), keamanan jaringan adalah aktivitas apa pun yang dirancang untuk melindungi kegunaan dan integritas jaringan komputer. Sehingga dapat dikatakan bahwa keamanan jaringan merupakan sekumpulan elemen atau komponen dari prosedur-prosedur yang saling berhubungan untuk melindungi kegunaan dan integritas data dan jaringan komputer.

2.4. Web Filtering

Web filtering merupakan sebuah proses untuk membatasi, menyaring atau memblokir hak akses sistem pengguna terhadap suatu situs web tertentu. Muhamad Zeni (2018) menjelaskan bahwa

cara kerja *web filter* yaitu memblokir akses terhadap web yang dianggap mengandung konten tidak pantas. MikroTik menyediakan fitur tersebut dengan beberapa cara atau teknik. Sistem kendali *web filtering* ini nantinya akan menentukan situs apa saja yang tidak boleh diakses dan mana yang tersedia.

2.5. Web Browser

Menurut Firmansyah dan Pitriani (2017), *Web Browser* atau *Browser* merupakan sebuah aplikasi perangkat lunak yang digunakan untuk mengambil dan menyajikan sumber informasi dalam mengakses laman *web* atau program-program *web*.

2.6. DNS Forwarding

Menurut Ayunindya (2021), *Domain Name System (DNS)* merupakan sebuah sistem yang membantu manusia dan komputer untuk saling berkomunikasi saat mengakses situs web melalui Internet. Manusia menggunakan nama (URL), komputer menggunakan angka (alamat IP), dan DNS berada di antaranya untuk “menerjemahkan” URL menjadi angka yang bisa dipahami oleh komputer.

Menurut Nuha (2017), *DNS Forwarding* merupakan suatu metode yang dilakukan oleh DNS server untuk mengubah arah pencarian dari permintaan *name query*. Dengan kata lain, metode pada sistem ini “memaksa” sistem pengguna untuk melakukan *resolve* DNS yang ingin dituju oleh pengguna ke *DNS Forwarder* terlebih dahulu. Sehingga situs web yang ingin dituju oleh pengguna akan dialihkan (*forward*) ke alamat yang ditentukan oleh DNS Server.

2.7. Network Address Translation (NAT)

Berdasarkan penjelasan yang disebutkan oleh Riyadi (2019), *Network Address Translation (NAT)* adalah sebuah sistem untuk menggabungkan lebih dari satu komputer untuk dihubungkan ke dalam jaringan Internet hanya dengan menggunakan sebuah alamat IP. Sehingga setiap komputer di dalam NAT ketika mengakses Internet akan terlihat memiliki alamat IP yang sama jika dilacak. Dengan kata lain, sebuah alamat IP pada jaringan lokal akan terlebih dahulu ditranslasikan oleh NAT untuk dapat mengakses IP publik di jaringan komputer.

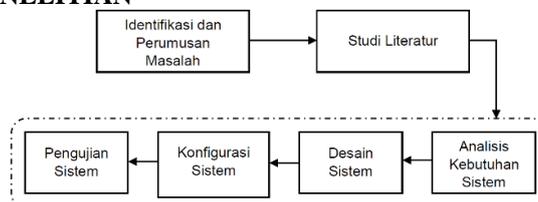
Riyadi (2019) juga menjelaskan bahwa NAT merupakan salah satu fasilitas yang terdapat pada MikroTik Router. NAT memungkinkan pengguna yang memiliki alamat tidak terdaftar (*private address*) untuk bisa mengakses Internet karena alamat yang tidak terdaftar tidak memungkinkan untuk terkoneksi dengan jaringan Internet apabila tidak melalui metode NAT. Jadi Internet menganggap *request* data bersumber dari MikroTik yang mana memiliki IP publik, sedangkan MikroTik akan meneruskan (*forward*) ke sistem pengguna (*client*) yang melakukan *request*.

2.8. MikroTik

Menurut Irawan et al. (2018), MikroTik merupakan nama perusahaan yang berasal dari negara Latvia yang didirikan pada tahun 1996. MikroTik adalah perusahaan yang mengembangkan Router dan sistem ISP nirkabel. MikroTik terbagi menjadi 2 macam tipe, yaitu *hardware* (RouterBOARD) dan *software* (RouterOS). MikroTik juga memiliki perangkat lunak khusus untuk melakukan konfigurasi terhadap MikroTik Router, yaitu WinBox.

Kurniawan (2020) menjelaskan bahwa Router adalah perangkat keras yang dipakai untuk menghubungkan beberapa jaringan, baik itu jaringan yang sama atau juga jaringan yang berbeda. *Routing* adalah proses pengiriman paket data dengan melalui jaringan dari satu perangkat ke perangkat lainnya.

3. METODOLOGI PENELITIAN



Gambar 1. Tahapan Penelitian

Agar lebih langkah-langkah yang dilakukan oleh penulis dalam penelitian ini dapat lebih mudah dipahami, berikut ini disertakan penjelasan terperinci mengenai metodologi penelitian yang digunakan dalam penelitian ini.

a. Tahapan Penelitian

Dalam penelitian ini, tahapan penelitian atau model proses yang digunakan oleh penulis adalah sekuensial linier.

1. Identifikasi dan Perumusan Masalah

Sebuah penelitian tentunya berawal dari adanya suatu permasalahan, setelah masalah diidentifikasi dan dibatasi kemudian permasalahan tersebut dirumuskan.

2. Studi Literatur

Metode pengumpulan data yang dilakukan penulis dalam penelitian ini adalah dengan mempelajari literatur yang berkaitan dengan teori jaringan komputer, keamanan jaringan, pembahasan mengenai *web filtering*, dan pengumpulan informasi beberapa contoh metode dalam perancangan sistem *web filtering* khususnya pada perangkat MikroTik.

3. Tahap Analisis Kebutuhan Sistem

Pada tahap ini dilakukan analisis kebutuhan perangkat yang dibutuhkan dalam penelitian ini, baik perangkat keras (*hardware*) atau pun perangkat lunak (*software*). Selain melakukan analisis dan mempersiapkan perangkat yang dibutuhkan, pada tahap ini juga dilakukan pendefinisian peran terhadap masing-masing perangkat yang dibutuhkan tersebut.

4. Tahap Desain Sistem

Tahap desain sistem ini merupakan tahap untuk menerjemahkan kebutuhan-kebutuhan yang akan dicapai pada tahap analisis ke dalam sebuah bentuk desain atau perancangan sebelum melakukan konfigurasi sistem. Hal-hal tersebut meliputi perancangan topologi jaringan dan identifikasi tugas-tugas pada setiap *node* dalam topologi jaringan terhadap sistem keamanan jaringan.

5. Tahap Konfigurasi Sistem

Tahap konfigurasi sistem ini adalah tahap untuk membuat dan melakukan aktivitas penelitian sesuai dengan desain penelitian yang telah ditentukan. Konfigurasi ini diantaranya adalah konfigurasi *wireless interface*, konfigurasi alamat IP, konfigurasi DHCP Server, konfigurasi DNS Server, membuat daftar situs target yang ingin dibatasi dengan fitur *DNS Static* dan membuat *filtering access rule* dengan fitur NAT terhadap situs target agar dapat dibatasi dan dialihkan ke situs web lainnya.

6. Tahap Pengujian Sistem

Tahap pengujian sistem ini merupakan proses untuk memastikan bahwa perancangan sistem keamanan jaringan ini telah berhasil, tujuannya agar penelitian ini dapat terbukti memberikan hasil aktual sesuai dengan yang dibutuhkan dan diharapkan. Hasil yang dimaksud pada tahap pengujian ini ialah apakah situs web bermuatan negatif yang berusaha diakses oleh pengguna jaringan ini dapat berhasil disaring dan dialihkan atau tidak.

b. Instrumen Penelitian

Berikut merupakan instrumen-instrumen yang secara langsung atau pun tidak langsung dimanfaatkan dalam melaksanakan penelitian ini, diantaranya:

1. Perangkat Keras (*Hardware*)

- MikroTik RB941-2nD-TC hAP-Lite
Perangkat ini digunakan sebagai router *gateway* dan dikonfigurasi sebagai sistem *web filtering* pada jaringan komputer.
- Laptop Acer Aspire E1-470
Perangkat ini digunakan untuk melakukan konfigurasi terhadap MikroTik Router dengan bantuan perangkat lunak WinBox. Perangkat ini juga digunakan sebagai *client-1* untuk melakukan pengujian terhadap sistem *web filtering* pada jaringan komputer.
- Laptop ASUS X450CC
Perangkat ini digunakan sebagai *client-2* untuk melakukan pengujian terhadap sistem *web filtering* pada jaringan komputer.

2. Perangkat Lunak (*Software*)

- MikroTik RouterOS SMIPS-BE versi 6.45.9
Perangkat lunak ini merupakan sistem operasi yang terdapat pada MikroTik Router. Sistem operasi ini dikonfigurasi sebagai sistem *web filtering* dengan metode *DNS Forwarding*.

- Sistem Operasi Windows 10 Pro 64-bit
Perangkat lunak ini merupakan sistem operasi yang terdapat pada komputer *client-1*, yang mana sistem operasi ini dimanfaatkan dalam proses uji konektivitas terhadap jaringan komputer dan proses pengujian terhadap sistem *web filtering*.
- Sistem Operasi Windows 10 Education 64-bit
Perangkat lunak ini merupakan sistem operasi yang terdapat pada komputer *client-2*, yang mana sistem operasi ini dimanfaatkan dalam proses uji konektivitas terhadap jaringan komputer dan proses pengujian terhadap sistem *web filtering*.
- WinBox versi 3.27 64-bit
Perangkat lunak WinBox ini merupakan aplikasi yang digunakan untuk melakukan konfigurasi terhadap MikroTik Router dengan tampilan *Graphical User Interface* (GUI).
- *Command Prompt*
Perangkat lunak ini dimanfaatkan untuk memeriksa informasi jaringan *wireless interface* yang terdapat pada komputer *client* untuk memastikan bahwa *client* telah mendapatkan alamat IP secara otomatis, dan juga digunakan untuk menguji bahwa sistem *web filtering* telah berhasil dan bekerja dengan baik, yaitu dengan melakukan *name server lookup* (*nslookup*).
- Microsoft Edge versi 98.0.1108.56 64-bit
Perangkat lunak ini merupakan aplikasi *web browser* yang digunakan untuk melakukan simulasi pengujian sistem *web filtering* dari komputer *client-1*.
- Mozilla Firefox versi 97.0.1 64-bit
Perangkat lunak ini merupakan aplikasi *web browser* yang digunakan untuk melakukan simulasi pengujian sistem *web filtering* dari komputer *client-2*.

c. Desain Penelitian



Gambar 2. Desain Penelitian

Perancangan sistem keamanan jaringan sebagai *web filtering* ini utamanya memanfaatkan teknologi DNS Server, namun untuk menerapkan metode *DNS Forwarding* ini juga memanfaatkan fitur *Network Address Translation* (NAT) yang terdapat pada MikroTik. Fitur NAT sendiri digunakan untuk membuat *filtering access rule* agar situs target dapat diblokir atau disaring dan dialihkan ke situs web lainnya. Sedangkan untuk membuat daftar situs target itu sendiri, penulis menggunakan fitur *DNS Static*. Desain penelitian terkait perancangan sistem keamanan jaringan ini dapat dilihat pada gambar berikut ini.

1. Persiapan dan Perencanaan Sistem

Proses ini bertujuan untuk mempersiapkan segala kebutuhan perangkat yang digunakan dalam penelitian ini. Perangkat tersebut terdiri dari perangkat keras (*hardware*) dan perangkat lunak (*software*). Kemudian dilakukan juga perencanaan terkait penggunaan perangkat-perangkat tersebut untuk didefinisikan dalam proses perancangan sistem keamanan jaringan sebagai *web filtering*.

2. Perancangan Topologi Jaringan

Perancangan topologi jaringan ini merupakan proses untuk menjelaskan struktur dan cara berkomunikasi terhadap perangkat-perangkat atau komponen-komponen yang digunakan dalam penelitian ini. Topologi jaringan ini dirancang guna mempermudah dalam melakukan konfigurasi sistem.

3. Konfigurasi Dasar Jaringan

Konfigurasi dasar jaringan yang dilakukan dalam penelitian ini meliputi konfigurasi *wireless interface* (WLAN), konfigurasi alamat IP, konfigurasi translasi alamat IP privat ke alamat IP publik, konfigurasi DHCP Server dan konfigurasi DNS Server.

4. Membuat Daftar Situs Target

Proses ini merupakan proses untuk melakukan *entry* alamat situs web yang ingin disaring (*filtering*) dan kemudian dialihkan (*forwarding*) ke alamat situs web lainnya. Proses pembuatan daftar alamat situs target ini menggunakan fitur *DNS Static* yang terdapat pada MikroTik.

5. Membuat *Filtering Access Rule*

Proses selanjutnya adalah proses untuk membuat aturan atau *rule* agar alamat situs web yang telah dibuat pada daftar *DNS Static* dapat berhasil disaring (*filtering*) dan dialihkan (*forwarding*) ke alamat situs tujuan. Pembuatan *filtering access rule* ini memanfaatkan fitur *Network Address Translation* (NAT) yang terdapat pada MikroTik.

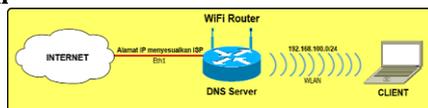
6. Uji Konektivitas dan Pengujian Sistem

Proses terakhir ini adalah proses untuk melakukan pengujian konektivitas terhadap *client* yang terhubung dengan jaringan WLAN pada MikroTik Router dan melakukan pengujian terhadap rancangan sistem *web filtering* pada jaringan komputer berbasis MikroTik RouterOS. Kedua proses pengujian tersebut dilakukan pada lebih dari satu komputer *client*, hal tersebut bertujuan untuk memastikan bahwa rancangan sistem *web filtering* ini dapat diterapkan pada semua *client* yang terkoneksi dengan jaringan komputer berbasis MikroTik RouterOS ini.

4. HASIL DAN PEMBAHASAN

Dalam penelitian ini, penulis melakukan perancangan dan konfigurasi terhadap sistem keamanan jaringan sebagai *web filtering*. Hal tersebut meliputi perancangan topologi jaringan, konfigurasi dasar jaringan, membuat daftar situs target dan membuat *filtering access rule* sehingga metode *DNS Forwarding* yang digunakan sebagai sistem *web filtering* ini dapat berhasil.

a. Rancangan Topologi Jaringan



Gambar 3. Rancangan Topologi Jaringan

Penelitian ini menggunakan jenis topologi jaringan *Star* pada rancangan sistem *web filtering* ini, dimana setiap perangkat *client* dihubungkan ke *node* pusat (WiFi Router).

Berdasarkan Gambar 3 terkait topologi jaringan di atas dapat diketahui bahwa fitur utama pada sistem ini, yakni DNS Server akan diinstalasikan pada perangkat WiFi Router. WiFi Router ini juga memanfaatkan fitur layanan DHCP Server agar *client* yang terkoneksi pada jaringan tersebut akan mendapatkan alamat IP secara otomatis. Berikut merupakan alokasi alamat IP pada jaringan komputer berbasis MikroTik Router ini.

Tabel 1. Pengalokasian Alamat IP

Perangkat	Interface	Alamat IP
WiFi Router	Eth1	(Menyesuaikan dari ISP)
	WLAN (Gateway)	192.168.100.1/24
Client	WLAN	192.168.100.xxx/24

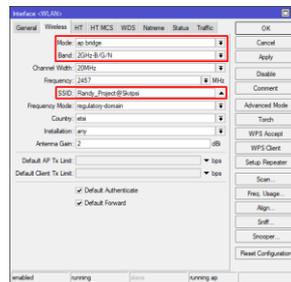
Dalam penelitian ini, penulis menggunakan alamat DNS Server milik Nawala, yang mana layanan DNS Server Nawala ini berkembang untuk menyaring situs-situs yang berbahaya dan melanggar peraturan perundang-undangan seperti situs penipuan, *malware*, dan *phising*. Umumnya DNS Server membutuhkan dua jenis alamat IP, yakni alamat *primary* dan *secondary*.

Tabel 2. Alamat DNS Server Nawala

DNS Service	DNS Address
Primary address	180.131.144.144
Secondary address	180.131.145.145

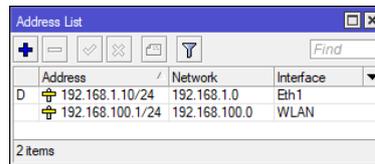
b. Konfigurasi Sistem

Dalam perancangan sistem *web filtering* menggunakan metode *DNS Forwarding* ini, tahap pertama yang diperlukan ialah melakukan konfigurasi dasar jaringan seperti konfigurasi *wireless interface*, konfigurasi pengalokasian alamat IP, konfigurasi DHCP Server dan konfigurasi DNS Server. Konfigurasi *wireless interface* pada perangkat MikroTik Router dapat dilihat pada gambar berikut.

Gambar 4. Konfigurasi *Wireless Interface* (WLAN)

Berdasarkan Gambar 4, dapat dilihat bahwa pada *interface* WLAN terdapat beberapa konfigurasi yang harus dilakukan, tujuannya agar perangkat MikroTik Router dapat memancarkan sinyal sehingga *client* dapat terkoneksi pada jaringan WLAN tersebut.

Berikut merupakan konfigurasi terkait pengalokasian alamat IP terhadap *interface* atau perangkat MikroTik Router. Konfigurasi alamat IP tersebut dapat dilihat pada gambar berikut.



Gambar 5. Konfigurasi Alamat IP

Berdasarkan Gambar 5, dapat dilihat bahwa alamat IP pada *interface* Eth1 adalah 192.168.1.10/24, yang mana alamat tersebut merupakan alamat IP *Dynamic* yang menyesuaikan dari ISP. Sedangkan alamat IP pada *interface* WLAN adalah 192.168.100.1/24, yang mana alamat tersebut merupakan *Gateway* terhadap *client* yang terkoneksi pada jaringan WLAN ini.

Tahap berikutnya adalah melakukan konfigurasi untuk memastikan bahwa MikroTik Router terkoneksi ke jaringan publik. Konfigurasi tersebut dilakukan dengan menambahkan *script rule* melalui *terminal* MikroTik Router sebagai berikut.

Script Rule 1. Rule untuk Translasi Private Address ke Public Address

```
/ip firewall nat add chain=srcnat out-interface=Eth1 action=masquerade
```

Script rule di atas bertujuan untuk mentranslasi alamat IP Privat menjadi alamat IP Publik, sehingga MikroTik Router dapat terkoneksi ke jaringan publik melalui *interface* Eth1.

Setelah MikroTik Router dapat terkoneksi dengan jaringan publik, hal yang perlu dilakukan adalah membuat *client* yang terkoneksi dengan MikroTik Router bisa mendapatkan alamat IP secara otomatis. Dengan demikian, penulis menggunakan fitur DHCP Server terhadap *interface* WLAN agar *client* tersebut

tidak perlu melakukan konfigurasi alamat IP secara manual saat terkoneksi dengan jaringan WLAN. Konfigurasi DHCP Server tersebut dapat dilihat pada gambar berikut.

```

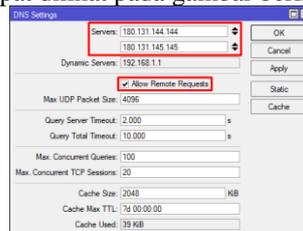
Terminal
[admin@Randy_MikroTik] > /ip dhcp-server setup
Select interface to run DHCP server on
dhcp server interface: WLAN
Select network for DHCP addresses
dhcp address space: 192.168.100.0/24
Select gateway for given network
gateway for dhcp network: 192.168.100.1
Select pool of ip addresses given out by DHCP server
addresses to give out: 192.168.100.2-192.168.100.254
Select DNS servers
dns servers: 180.131.144.144,180.131.145.145
Select lease time
lease time: 10m
[admin@Randy_MikroTik] >

```

Gambar 6. Konfigurasi DHCP Server

Berdasarkan Gambar 6, dapat dilihat bahwa pada *interface* WLAN, penulis menggunakan alamat 192.168.100.0/24 sebagai *network address* sesuai dengan alokasi alamat IP yang dikonfigurasi sebelumnya. Alamat *gateway* yang digunakan agar *client* dapat terhubung ke Internet adalah 192.168.100.1, sedangkan *range* alamat IP yang diberikan terhadap *client* adalah 192.168.100.2 sampai 192.168.100.254. Untuk DNS Server, penulis menggunakan alamat DNS Nawala yaitu 180.131.144.144 sebagai *primary address* dan 180.131.145.145 sebagai *secondary address*. Sementara *lease time* yang diberikan untuk *client* tersebut adalah 10 menit.

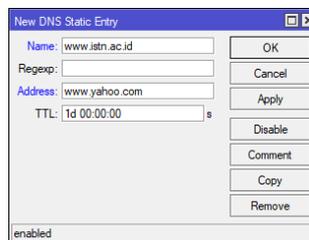
Berikut merupakan konfigurasi utama dalam menerapkan metode *DNS Forwarding*, yaitu konfigurasi DNS Server. Pada tahap ini, hal yang perlu dilakukan adalah menambahkan alamat DNS pada MikroTik Router. Konfigurasi DNS Server ini dapat dilihat pada gambar berikut.



Gambar 7. Konfigurasi DNS Server

Berdasarkan Gambar 7 di atas dapat dilihat bahwa alamat DNS yang ditambahkan ialah alamat DNS Nawala, yaitu 180.131.144.144 sebagai *primary address* dan 180.131.145.145 sebagai *secondary address*. Selain menambahkan alamat DNS Server, hal yang perlu dilakukan adalah memastikan bahwa opsi *Allow Remote Requests* dicentang. Hal ini dilakukan supaya alamat IP yang terdapat pada *interface* MikroTik Router dapat dijadikan sebagai alamat DNS Server bagi *client*.

Tahap selanjutnya adalah membuat daftar situs target, yaitu dengan menggunakan fitur *DNS Static*. Konfigurasi ini hanya perlu menentukan alamat situs web yang ingin dialihkan dan juga mengisi alamat situs web yang ingin dituju. Konfigurasi tersebut dapat dilihat pada gambar berikut.



Gambar 8. DNS Static Entry

Berdasarkan Gambar 8, penulis mengambil contoh situs milik kampus Institut Sains dan Teknologi Nasional yaitu www.istn.ac.id dimana situs tersebut akan dialihkan ke situs www.yahoo.com. Pada parameter *Address* ini dapat diisi dengan alamat IP atau pun diisi dengan nama domain situs web yang

ingin dituju. Penambahan daftar situs target ini tentunya dapat dilakukan terhadap lebih dari satu situs web sekaligus, seperti yang terlihat pada gambar berikut.

#	Name	Regexp	Address	TTL (s)
0	www.istn.ac.id		202.165.107.48	1d 00:00:00
1	www.vidio.com		172.217.194.99	1d 00:00:00
2	www.kaskus.co.id		103.102.166.224	1d 00:00:00

Gambar 9. Daftar Situs Target pada *DNS Static*

Berdasarkan Gambar 9, penulis menambahkan dua contoh situs lainnya. Situs tersebut diantaranya adalah www.vidio.com yang mana akan dialihkan ke situs www.google.com, dan juga situs www.kaskus.co.id yang mana akan dialihkan ke situs www.wikipedia.org.

Agar metode *DNS Forwarding* ini dapat berjalan, maka diperlukan *rule* untuk melakukan *filtering access* dengan menggunakan fitur *Network Address Translation (NAT)*. Konfigurasi *filtering access rule* dengan fitur NAT ini dilakukan dengan cara memasukkan *script rule* melalui *terminal* MikroTik Router. Ada pun *script rule* tersebut adalah sebagai berikut.

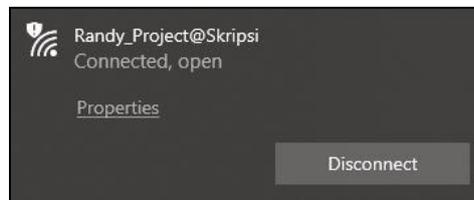
Script Rule 2. Filtering Access Rule dengan Fitur NAT

```
/ip firewall nat add chain=dstnat protocol=udp dst-port=53 in-interface-list=WLAN action=redirect to-ports=53
/ip firewall nat add chain=dstnat protocol=tcp dst-port=53 in-interface-list=WLAN action=redirect to-ports=53
```

Script rule di atas bertujuan agar semua trafik resolve DNS (port 53) terhadap protokol UDP dan TCP di jaringan *interface* WLAN dialihkan ke DNS Server lokal yang telah dikonfigurasi sebelumnya.

c. Uji Konektivitas

Dalam penelitian ini, penulis melakukan uji konektivitas terhadap *client* yang terhubung dengan jaringan komputer yang telah dikonfigurasi sebelumnya. Pengujian ini bertujuan untuk mengetahui apakah *client* mendapatkan alokasi alamat IP secara otomatis atau tidak. Hal pertama yang perlu dilakukan tentunya adalah memastikan *client* terhubung dengan jaringan komputer, seperti yang dapat dilihat pada gambar berikut.

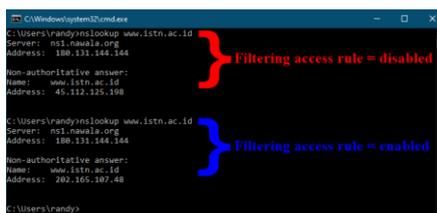


Gambar 10. *Client* Terhubung dengan Jaringan WLAN

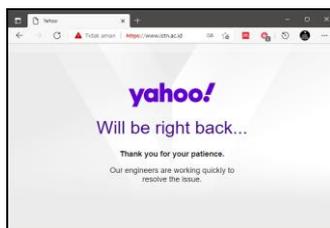
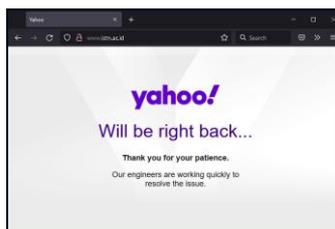
Setelah *client* terhubung dengan jaringan komputer, penulis memeriksa informasi jaringan terkait *network interface* di komputer *client*, khususnya pada *wireless interface*. Penulis memanfaatkan aplikasi *command prompt* yang terdapat pada sistem operasi Windows 10 untuk memeriksa informasi terkait *network interface* tersebut. Untuk menampilkan informasi jaringan tersebut dapat dilakukan dengan menuliskan perintah *ipconfig /all* pada aplikasi *command prompt*. Berikut merupakan informasi jaringan *wireless LAN* pada komputer *client*.

```
C:\WINDOWS\system32\cmd.exe
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . . . :
Description . . . . . : Qualcomm Atheros AR956x Wireless Network Adapter
Physical Address. . . . . : 40-10-2F-FA-08-32
Dhcp Enabled. . . . . : Yes
Autocconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80:5832:a8c9:39c4:ad5e%7(Preferred)
IPv4 Address. . . . . : 192.168.100.254(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Kamis, 24 Februari 2022 16:20:46
Lease Expires . . . . . : Kamis, 24 Februari 2022 16:30:45
Default Gateway . . . . . : 192.168.100.1
Dhcp Server . . . . . : 192.168.100.1
Dhcpv6 IAID . . . . . : 8814871
Dhcpv6 Client DUID. . . . . : 08-01-00-01-1F-C6-E1-09-38-65-EC-32-25-C4
DNS Servers . . . . . : 192.168.100.1
NetBIOS over Tcpip. . . . . : Enabled
```

Gambar 11. Informasi Jaringan WLAN pada *Client-1*

Gambar 16. Perintah *nslookup* terhadap Situs Target pada *Client-2*

Penulis mencoba melakukan akses terhadap situs www.istn.ac.id untuk memastikan apakah sistem *web filtering* dengan metode *DNS Forwarding* ini berhasil mengalihkan situs www.istn.ac.id tersebut ke situs www.yahoo.com atau tidak. Hasil dari percobaan akses situs web tersebut dapat dilihat pada gambar berikut.

Gambar 17. Percobaan Akses terhadap Situs Target pada *Client-1*Gambar 18. Percobaan Akses terhadap Situs Target pada *Client-2*

Gambar 17 dan Gambar 18 di atas menunjukkan bahwa situs www.istn.ac.id berhasil diblokir atau disaring, kemudian berhasil dialihkan ke situs www.yahoo.com, sehingga tampilan yang muncul bukanlah tampilan situs www.istn.ac.id melainkan tampilan dari situs www.yahoo.com.

Dengan berhasilnya pengujian terkait proses penyaringan (*filtering*) dan pengalihan (*forwarding*) pada situs target ini, dapat disimpulkan bahwa sistem keamanan jaringan komputer sebagai *web filtering* menggunakan metode *DNS Forwarding* pada jaringan komputer berbasis MikroTik RouterOS ini telah berhasil dan bekerja dengan baik.

5. KESIMPULAN

Berdasarkan hasil dari pengujian dan analisis yang dilakukan dalam penelitian ini, maka penulis dapat menyimpulkan bahwa:

1. Penyaringan (*filtering*) terhadap situs web bermuatan negatif pada sistem pengguna saat mengakses jaringan Internet ini dapat diterapkan dengan membuat *filtering access rule* yang memanfaatkan fitur *Network Address Translation* (NAT) pada MikroTik.
2. Pengalihan (*forwarding*) situs web bermuatan negatif ke situs web lainnya yang lebih sehat dan aman dapat diterapkan dengan membuat daftar situs web tersebut yang memanfaatkan fitur *DNS Static* pada MikroTik.
3. Hasil simulasi pengujian sistem *web filtering* dengan metode *DNS Forwarding* yang diterapkan pada jaringan komputer berbasis MikroTik RouterOS ini menunjukkan bahwa sistem keamanan jaringan tersebut dapat meminimalisir pengaksesan situs web bermuatan negatif bagi sistem pengguna saat mengakses jaringan publik atau Internet.

DAFTAR PUSTAKA

- [1] Nurfauzi, A., Nainggolan, E. R., Khasanah, S. N., & Setiadi, A. (2018). Implementasi Firewall Filtering Web Dan Manajemen Bandwith Menggunakan Mikrotik. *Snit 2018*, 1(1), 162–167.
- [2] Haryanto, Rahmah, R. D., & Sari, A. P. (2021). Implementasi Web Proxy Menggunakan Router Mikrotik Pada Kantor Suku Dinas Walikota Administrasi Jakarta Barat. *JIKA (Journal Informatika) Universitas Muhammadiyah Tangerang*, 5(3), 298–306.
- [3] Lestari, I., & Permana, R. (2019). Analisis Sistem Jaringan Komputer di Sekolah Menengah Kejuruan Al-Madani Pontianak. *International Journal of Natural Science and Engineering*, 2(3), 99.
- [4] Kompas.com. (2021). *Jaringan Komputer: Pengertian dan Manfaatnya*. Diakses pada 14 Oktober 2021, dari <https://www.kompas.com/skola/read/2021/04/01/144401569/jaringan-komputer-pengertian-dan-manfaatnya>.
- [5] Dewaweb.com. (2021). *Jaringan Komputer: Pengertian, Topologi, dan Jenisnya*. Diakses pada 14 Oktober 2021, dari <https://www.dewaweb.com/blog/jaringan-komputer-pengertian-jenis/>.
- [6] Astuti, Novia Fuji. (2020). *8 Jenis Jaringan Komputer dan Fungsinya yang Wajib Diketahui / merdeka.com*. Diakses pada 17 Februari 2022, dari <https://www.merdeka.com/jabar/8-jenis-jaringan-komputer-dan-fungsinya-yang-wajib-diketahui-klm.html>.
- [7] Setiawan, Heri. (2019). *5 Jenis-Jenis Jaringan Komputer, Lengkap dengan Pengertiannya - Tekno Liputan6.com*. Diakses pada 14 Oktober 2021, dari <https://www.liputan6.com/teknoread/3908662/5-jenis-jenis-jaringan-komputer-lengkap-dengan-pengertiannya>.
- [8] Vinka, A. M., & Michele, N. (2021). Pengaruh Teknologi Internet Terhadap Pengetahuan Masyarakat Jakarta Seputar Informasi Vaksinasi Covid-19. *Jurnal Teknologi Informasi Dan Komunikasi*, 8(1), 1–13.
- [9] Yusup, P. M., Komariah, N., Prahatmaja, N., & CMS, S. (2019). Pemanfaatan Internet Untuk Penghidupan Di Kalangan Pemuda Pedesaan. *Baca: Jurnal Dokumentasi Dan Informasi*, 40(2), 217.
- [10] Kompas.com. (2021). *Sistem: Pengertian Para Ahli, Karakteristik, Elemen, dan Jenisnya*. Diakses pada 17 Februari 2022, dari <https://www.kompas.com/skola/read/2021/08/02/131754769/sistem-pengertian-para-ahli-karakteristik-elemen-dan-jenisnya>.
- [11] Cisco. (2021). *What Is Network Security? - Cisco*. Diakses pada 07 Mei 2021, dari <https://www.cisco.com/c/en/us/products/security/what-is-network-security.html>.
- [12] Zeni, Muhamad. (2018). Implementasi Firewall dan Web Filtering Pada MikroTik RouterOS Untuk Mendukung Internet Sehat dan Aman (INSAN). *Jurnal Teknik Informatika Atmaluhur*, 6(1), 76–83.
- [13] Yoki, Firmansyah & Pitriani. (2017). Penerapan Metode SDLC Waterfall Dalam Pembuatan Aplikasi Pelayanan Anggota Pada CU Duta Usaha Bersama Pontianak. *Jurnal Bianglala Informatika*, 5(2), 53–61.
- [14] Ayunindya, Faradilla. (2021). *Apa Itu DNS dan Cara Kerja DNS: Pembahasan Lengkap*. Diakses pada 14 Oktober 2021, dari <https://www.hostinger.co.id/tutorial/apa-itu-dns>.
- [15] Nuha, Ulun. (2017). *DNS FORWARDING*. Diakses pada 17 Februari 2022, dari <https://www.ulun.web.id/2017/02/dns-forwarding.html>.
- [16] Riyadi, Hermawan. (2019). *Pengertian NAT Adalah : Fungsi & Cara Kerja NAT dalam Jaringan*. Diakses pada 14 Oktober 2021, dari <https://www.nesabamedia.com/pengertian-fungsi-dan-cara-kerja-nat/>.
- [17] Irawan, G. T., Djaohar, M., & M. Ficky Duskarnaen. (2018). Perancangan Dan Implementasi Sistem Keamanan Jaringan Menggunakan Firewall dan Web Proxy Berbasis Mikrotik di SMA Negeri 1 Kota Sukabumi. *PINTER : Jurnal Pendidikan Teknik Informatika Dan Komputer*, 2(1), 27–32.
- [18] . Kurniawan, Andre. (2020). *3 Fungsi Router, Pahami Cara Kerja dan Perbedaannya dengan Modem / merdeka.com*. Diakses pada 07 Mei 2021, dari <https://www.merdeka.com/jabar/3-fungsi-router-pahami-cara-kerja-dan-perbedaannya-dengan-modem-klm.html>.
- [19] Utopicomputers.com. (2019). *Apa Itu Mikrotik Routerboard? Berikut Pengertian dan Fungsinya*. Diakses pada 17 Februari 2022, dari <https://www.utopicomputers.com/apa-itu-mikrotik-routerboard-berikut-pengertian-dan-fungsinya/>.
- [20] Saputri, Yunisda Dwi. (2019). *6 Fungsi Mikrotik Lengkap dengan Penjelasan dan Jenisnya - Tekno Liputan6.com*. Diakses pada 07 Mei 2021, dari <https://www.liputan6.com/teknoread/3922672/6-fungsi-mikrotik-lengkap-dengan-penjelasan-dan-jenisnya>.