Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, Vol. 8, No. 2, Agustus 2022, Hal. 148-154
e-ISSN 2502-8995 p-ISSN 2460-8181

IMPLEMENTASI KEAMANAN HOTSPOT MENGGUNAKAN PROXY DAN FIREWALL DALAM MENGATASI RESIKO ANCAMAN SERANGAN

[1]Farhan Muhammad Naufal , [2]Muhammad Rizal Vahlevi , [3]Arif Widayana, [4]Muhammad Luthfi Zulfa, [5]Didi Juardi
[1,2,3,4,5]Teknik Informatika, Fakultas Ilmu Komputer, Universitas Singaperbangsa Karawang
Email: [1]farhan.naufal18193@student.unsika.ac.id, [2]muhammad.rizal18114@student.unsika.ac.id, [3]arif.widayana18195@student.unsika.ac.id, [4]luthfi.zulfa18086@student.unsika.ac.id, [5]didi.juardi@staff.unsika.ac.id

ABSTRAK

Dengan meningkatnya kejahatan di era digital, maka pelayanan dan keamanan jaringan wajib hukumnya untuk ditingkatkan. Pelayanan dan keamanan jaringan yang saat ini ada pada SMK ALLUTHFAH masih belum maksimal terutama di bagian pemfilteran ketika berselancar di internet dengan menggunakan jaringan internet yaitu hostpot sekolah. Penelitian ini memiliki tujuan untuk analisis sistem keamanan jaringan menggunakan proxy dan firewall dengan menggunakan router mikrotik sebagai proses implementasinya. Penelitian ini dilakukan di SMK AL-LUTHFAH yang terletak di Cikarang, dengan mempertimbangkan aspek siswa di sekolah tersebut, dimana pada proses belajar mengajar menggunakan internet sebagai sarana dalam menunjang kegiatan belajar mengajar yang dikhawatirkan rentan menerima ancaman serangan kejahatan digital atau siber. Penelitian ini menggunakan metode research and development, dimana alur penelitiannya yaitu membuat aturan proxy dan firewall selanjutnya mengkonfigurasi aturan tersebut pada gateway dan akan dilakukan uji tes terhadap setiap aturan yang telah dibuat. Konfigurasi yang diterapkan akan menjatuhkan semua paket data yang dianggap berbahaya pada sejumlah port. Memblok paket data menuju router gateway dari jaringan lokal maupun jaringan internet selain administrator. Memblok situs – situs yang dianggap berbahaya. Sehingga kesimpulannya, menerapkan aturan pada proxy dan firewall dapat mengamankan jaringan dari serangan awal cracker.

Kata kunci: *keamanan, hotspot, firewall, proxy, serangan jaringan*

Abstract

With the increase in crime in the digital era, it is obligatory to improve service and network security. The network services and security that currently exist at ALLUTHFAH Vocational School are still not optimal, especially in the filtering section when surfing the internet using the internet network, namely the school hotspot. This study aims to analyze network security systems using proxies and firewalls using a proxy router as the implementation process. This research was conducted at SMK AL-LUTHFAH located in Cikarang, taking into account the aspects of students at the school, where in the teaching and learning process using the internet as a means of supporting teaching and learning activities which are feared to be vulnerable to threats of digital or cyber crime attacks. This study uses research and development methods, where the research flow is to create proxy and firewall rules then configure these rules at the gateway and test tests will be carried out on each rule that has been made. The applied configuration will drop all data packets that are considered malicious on a number of ports. Blocking data packets to the gateway router from the local network or internet network other than the administrator. Block sites that are considered dangerous. So in conclusion, applying rules on proxies and firewalls can secure the network from cracker initial attacks.

Keywords: *security, hotspot, firewall, proxy, network attack*

A. PENDAHULUAN

Dengan seiring perkembangan teknologi jaringan komputer yang semakin pesat dan juga peningkatan kebutuhan masyarakat akan layanan yang menggunakan jaringan komputer yang cepat dan efisien dalam lingkungan kerja maupun rumah. Jaringan komputer yang ada saat ini merupakan suatu layanan yang sangat dibutuhkan dan mempunyai banyak manfaat yang lebih dibandingkan dengan komputer yang berdiri sendiri. Jaringan komputer memungkinkan pemakaian data, perangkat lunak dan perlatan secara bersama[1]. Sehingga kelompok kerja dapat berkomunikasi lebih efektif dan efisien. Meningkatnya kebutuhan layanan jaringan komputer

telah meningkatkan kerentanan sebuah sistem untuk dapat diserang dari berbagai macam ancaman yang ada. Kelemahan dalam suatu sistem pada program, desain, maupun implementasi dinamakan *Vulnerability*. Yang bisa mengakibatkan timbul suatu ancaman yang dinamakan *Threat*, dan berdasarkan ancaman yang ada, beasr kemungkinan terjadi serangan atau Attack yang akan mengancam sebuah sistem. Teknologi yang ada terkait proxy dan firewall terus menjadi bentuk yang paling umum dari perlindungan ancaman yang ada. SMK AL-LUTHFAH merupakan salah satu sekolah favorit yang ada di Ciantra, Cikarang Selatan, Bekasi. Pelayanan dan keamanan jaringan di SMK AL-LUTHFAH saat ini masih belum maksimal terutama pada bagian pemfilteran. Penelitian ini dilakukan untuk memaksimalkan dan menyelesaikan permasalahan pada SMK AL-LUTHFAH perihal pelayanan dan kemanan jaringannya.

Untuk itu diperlukan sebuah analisis mengenai keamanan suatu jaringan internet, agar pengguna yang menggunakan jaringan tersebut dapat terhindar dari ancaman-ancaman serangan dari pihak yang tidak bertanggung jawab, seperti mengambil data yang kemudian akan disalah gunakan. Serta penerapan jaringan skala kecil seperti rumah atau sekolahan, juga perlu diprioritaskan dalam sistem keamanannya pada jaringan internet yang dimiliki, karena penggunaan skala kecil di Indonesia saat ini sangat lah banyak dan kebanyakan dari pengguna adalah anak-anak usia sekolah yang rentan akan ancaman-ancaman dari kejahatan serangan digital atau siber.

.

B. LANDASAN TEORI

Mikrotik adalah sistem operasi independen berbasis Linux, khusus untuk komputer yang berfungsi sebagai router. Mikrotik sangat baik untuk keperluan administrasi jaringan komputer seperti merancang dan membangun sebuah sistem jaringan berskala kecil hingga yang kompleks[2]. (Menurut Irawan dkk, 2018.) Winbox adalah perangkat lunak yang dirancang khusus untuk mengkonfigurasi router Mikrotik dengan tampilan GUI (Graphic User Interface), perangkat lunak winbox bekerja pada port 8291[3].

Saat ini mikrotik memberi layanan kepada banyak ISP untuk layanan akses internet di seluruh dunia. Mikrotik pada hardware berbasis PC dikenal dengan kestabilan, kualitas kontrol, dan fleksibilitas untuk berbagai jenis paket data dan penanganan proses rute (routing)[4]. Fitur yang diberikan oleh mikrotik tidak hanya sekedar routing, tapi bisa juga melakukan manajemen akses pengguna, bandwidth, firewall, wireless access point, system hotspot, virtual private network server, dan lainnya[5].

Firewall adalah sebuah sistem atau kelompok sistem yang menerapkan sebuah access control policy terhadap lalu lintas jaringan yang melewati titik-titik akses dalam jaringan[6]. Tugas firewall untuk memastikan bahwa tidak ada tambahan diluar ruang lingkup yang diizinkan. Firewall untuk memastikan bahwa acces control policy diikuti oleh semua user di dalam jaringan [3].

Saat merancang firewall, status koneksi dari sebuah paket data harus diperhatikan. Ada 4 status koneksi yang dapat dimiliki sebuah paket data, yaitu:

1. New, paket dengan status ini menunjukan bahwa paket tersebut merupakan paket pertama dari sebuah koneksi.
2. Established, paket dengan status ini menunjukan bahwa paket tersebut merupakan kelanjutan dari paket new.
3. Related, paket ini merupakan paket baru tetapi sebenarnya merupakan kelanjutan dari koneksi yang telah ada sebelumnya.
4. Invalid, paket data ini adalah paket yang tidak memiliki hubungan dengan paket lain maupun koneksi lain[3].

Proxy adalah suatu sistem yang memungkinkan untuk bisa mengakses jaringan internet menggunakan IP yang berbeda dengan yang diterima oleh perangkat. Sistem ini menggunakan proxy server untuk dapat bekerja. Sedangkan proxy server itu sendiri merupakan perangkat atau komputer yang digunakan untuk menyediakan layanan proxy[7].

Beberapa server proxy bisa berupa sekelompok aplikasi atau server yang memblokir layanan internet umum. Misalnya, proxy HTTP memotong akses web sedangkan proxy SMTP memotong akses terhadap email[8]. Server proxy menggunakan skema pengalamatan jaringan untuk menyajikan satu alamat IP milik organisasi ke internet. Setelah itu, semua request pengguna diantar ke internet lalu responnya dikembalikan ke pengguna tersebut.

Gateway adalah suatu perangkat yang menghubungkan jaringan komputer yang satu atau lebih jaringan komputer dengan media komunikasi yang berbeda sehinga informasi pada saat jaringan komputer di alihkan akan berbeda dengan media jaringan yang berbeda[9]. Gateway juga dapat di artikan sebagai komputer yang dapat menghubungkan 2 buah jaringan atau lebih karena memiliki minimal 2 buah network interface. Untuk dapat menghubungkan 2 buah jaringan yang berbeda protokolnya, gateway harus mengkonversi setiap protokol yang berbeda pada setiap jaringan komputer sehingga dapat di hubungkan satu sama lain[10]. Gateway yang berbeda protokol tidak bisa di sambungkan karena protokolnya yang berbeda, maka secara otomatis pada saat mengirim informasi dari komputer satu dengan komputer lainnya tidak dapat di akses, maka dari itu

protokol nya harus di konversikan agar dapat lancar mengakses suatu informasi dengan mudah[10].

Gateway dapat menjadi jalan atau rute untuk menunjukan tujuan dari suatu alamat pada internet dan gateway dapat berfungsi layak nya router, gateway juga dapat menghubungkan satu jaringan dengan jaringan lainnya meskipun setiap jaringan tersebut memiliki arsitektur dan pola topologi yang berbeda[11]. Selain itu gateway dapat menghubungkan suatu jaringan komputer yang besar dengan jaringan yang besar lainnya, tidak hanya itu gateway juga bisa menghubungkan jaringan komputer yang besar dengan jaringan komputer yang lebih kecil.

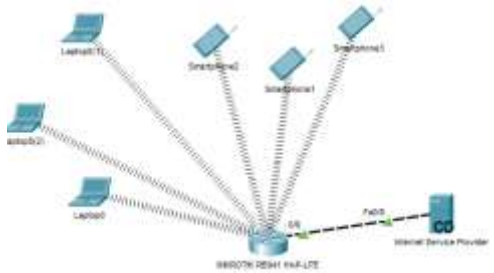
C. METODE PENELITIAN

Pada penelitian ini metode yang digunakan adalah Research and Development dimana metode ini digunakan untuk menghasilkan serta melakukan uji coba pada hasil atau produk yang telah dibuat[12]. Dimana hasil yang diharapkan pada penelitian ini adalah untuk dapat merancang sistem jaringan dan menerapkannya dalam upaya mengatasi ancaman yang terjadi. Berikut tahapan dari penelitian ini, yaitu:

1. Studi Literatur dan Pengumpulan Data Pada tahap ini diperlukan untuk dapat mempelajari serta memahami literatur yang ada pada artikel, buku, maupun jurnal dan melakukan pengumpulan informasi yang berhubungan dengan penelitian yang dilakukan[13].
2. Perancangan Sistem Jaringan Selanjutnya melakukan persiapan untuk merancang jaringan atau sering disebut rancang bangun jaringan yang menggambarkan bagaimana jaringan dibentuk, dapat berupa penggambaran, perencanaan, dan pembuatan sketsa atau pengaturan beberapa elemen terpisah ke dalam satu kesatuan yang utuh, termasuk mengkonfigurasikan komponen software dan hardware suatu jaringan.
3. Implementasi Jaringan Langkah terakhir adalah penerapan pada rancang bangun jaringan yang sudah dibuat kemudian melakukan instalasi hardware dan software yang dibutuhkan untuk membentuk sistem jaringan. Selanjutnya dilakukan konfigurasi mikrotik untuk membuat gateway jaringan.

D. HASIL DAN PEMBAHASAN

Bagian ini menjelaskan bagaimana proses penelitian dilakukan dengan memperhatikan pada penelitian-penelitian yang serupa. Berikut skema topologi yang diusulkan dalam penelitian ini pada gambar 1 di bawah ini.



Gambar 1. Rancangan topologi yang diajukan

Dari gambar topologi diatas, mikrotik dengan tipe RB941 Hap-lite memiliki fungsi penting, yaitu sebagai pengatur dari lalu lintas jaringan internet pada sebuah jaringan hotspot. Dari penelitian yang kami ajukan, kami akan melakukan pengaturan jaringan hotspot menggunakan mikrotik untuk membuat sistem keamanan sederhana dengan memanfaatkan proxy dan firewall yang tersedia pada router mikrotik untuk mencegah virus dan serangan siber lainnya ketika user berselancar di internet. Berikut ini hasil dari penelitian yang telah dilakukan yaitu;

D.1. Alat dan Bahan

1. Mikrotik RB941 Hap-lite Mikrotik merupakan se buah router yang berasal dari negara eropa yaitu Latvia. Masuk ke Indonesia pada tahun 2001, memiliki slogan “Routing the World”. Penggunaan mikrotik saat ini sangat beragam, baik dari perusahaan skala kecil hingga skala besar-pun masih menggunakan mikrotik, karena konfigurasi cukup mudah dan harga cukup tercangkau ketimbang merek lainnya[14]. Pada penelitian ini kami menggunakan tipe RB941 Hap-lite. Arti dari penamaan Mikrotik ini adalah sebagai berikut : Kode RB = Singkatan dari “RouterBoard”. Kode 9 = Merupakan jenis tipe dari mikrotik tersebut. Kode 4 = Merupakan jumlah port yang tersedia. Kode 1 = Interfaces wireless yang tersedia.
2. Sebuah personal Computer / Laptop PC atau lapt op pada penelitian ini digunakan untuk melakukan konfigurasi proxy dan firewall pada router mikrotik, serta digunakan sekaligus untuk melakukan pengujian pada tahap akhir.
3. Aplikasi Winbox Winbox merupakan aplikasi portabel yang diperuntukan untuk melakukan konfigurasi router mikrotik[15].
4. Sebuah smartphone Smartphone digunakan untuk melakukan pengujian pada tahap akhir.
5. Dua (2) Kabel LAN Kabel digunakan untuk menghubungkan antara mikrotik dengan jaringan internet dan menghubungkan mikrotik dengan PC atau laptop untuk melakukan konfigurasi.
6. Koneksi internet, disini merupakan ISP yang digunakan pada studi kasus kami pada penelitian kali

ini yaitu SMK Al-Luthfah. ISP yang digunakan adalah SKINET dengan kecepatan +-30/Mbps.

D.2. Konfigurasi

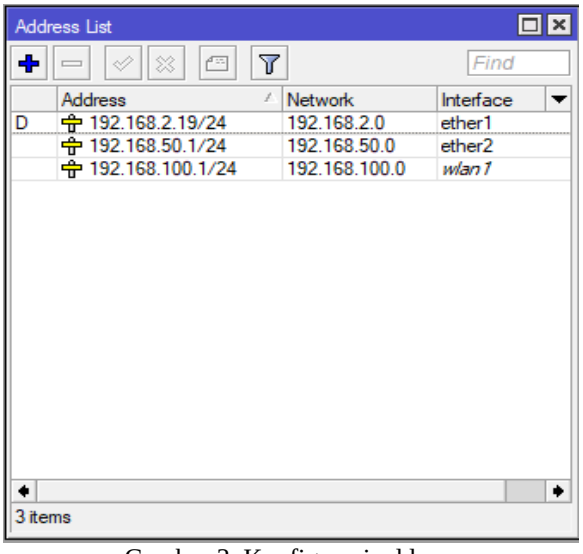
Untuk tahapan konfigurasi terbagi menjadi 3 bagian yaitu konfigurasi pada hotspot wireless, web proxy dan firewall, kami jabarkan berikut ini.

1. Hotspot

Pada tahapan ini, sebagai tahap awal dalam penelitian kami. Konfigurasi hotspot yang dilakukan merupakan konfigurasi sederhana, dimana memanfaatkan fitur yang ada pada router yaitu menggunakan interfaces wireless sebagai *access point*. Berikut hasil dari konfigurasi hotspot yang kami lakukan.

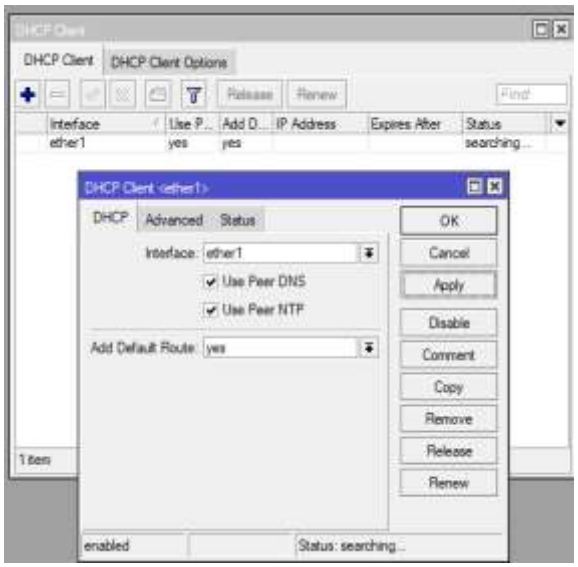
Gambar 2. Konfigurasi wireless

Pada konfigurasi wireless, mode yang kami gunakan adalan ap-bridge, dikarenakan kami ingin membuat sebuah access point. Kemudian untuk SSID kami beri nama Wireless_Testing dengan password yaitu 12345678.



Gambar 3. Konfigurasi address

Selanjutnya yaitu konfigurasi alamat IP. Disini kami menambahkan untuk 3 interfaces yaitu ether 1, ether 2 dan wlan 1. Dimana ether 1 didapat dari hasil dhcp client, kemudian ether 2 merupakan ip yang digunakan untuk mengecek hasil konfigurasi secara wired dengan ip yaitu 192.168.50.1/24 dimana /24 adalah prefix dari netmask 255.255.255.0 dengan jumlah user yang dapat ditampung sebanyak 253 dan wlan 1 sebagai ip untuk hotspot kami yaitu 192.168.100.1/24.



Gambar 4. Memanggil DHCP client

Kemudian kami menggunakan fitur dhcp client pada ether 1, agar router mendapatkan koneksi internet dari ISP.

Gambar 5. Konfigurasi DHCP server

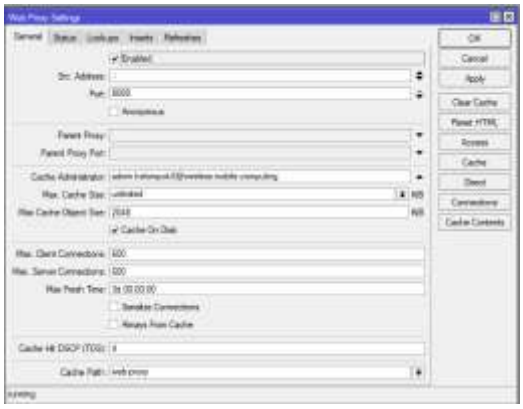
Selanjutnya kami mengkonfigurasi DHCP Server, agar client yang terkoneksi dengan Hotspot yang kami buat dapat langsung mendapatkan IP secara otomatis.

Gambar 6. Konfigurasi jalur NAT

Tahap terakhir adalah membuat jalur NAT (*Network Address Translation*). Jalur ini berfungsi untuk menjadi penghubung antara Jalur internet dengan port-port yang ada pada router, sehingga nantinya port router lainnya akan mendapatkan koneksi internet dari ether 1 yang di ambil dari DHCP Client sebelumnya. Pada tahapan ini chain yang digunakan adalah Source-Nat atau srcnat dan action yang digunakan adalah masquerade.

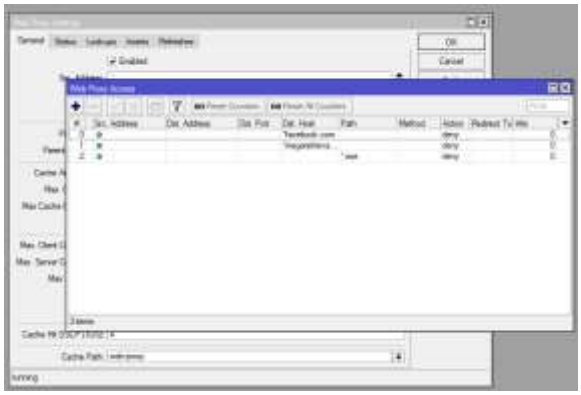
2. Web Proxy

Seperti yang sudah dijelaskan pada pendahuluan, web proxy pada penelitian kali ini kami gunakan untuk membatasi akses internet kepada pengguna sehingga diharapkan pengguna dapat terhindar dari bahaya kejahatan siber seperti malware dan virus lainnya. Untuk konfigurasi pada mikrotik berada pada bagian sub menu ip kemudian tab web proxy, berikut tampilan konfigurasinya.



Gambar 7. Konfigurasi proxy

Kami menggunakan port 8080 karena merupakan port http dan mengaktifkan mode cache untuk dapat melakukan pembatasan. Selanjutnya adalah melakukan penambahan website yang akan dibatasi pada menu access yang terdapat pada web proxy, berikut hasilnya.

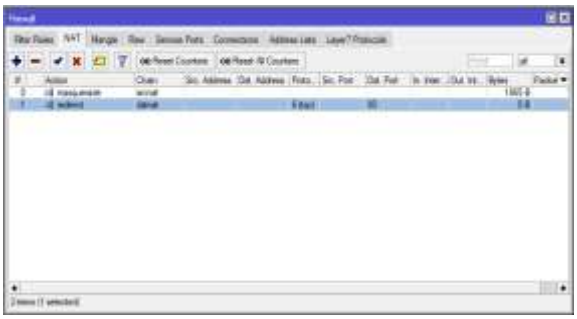


Gambar 8. Mendaftarkan situs yang akan diblokir

Dua situs yang akan kami blokir dan satu file download berbasis .exe yang akan kami batasi.

3. Firewall

Selain menggunakan proxy dalam pembatasan, pada penelitian kali ini firewall berfungsi sebagai jembatan pengantur lalu lintas dari jaringan internet untuk itu penggunaannya sangat diperlukan pada penelitian kali ini. Untuk konfigurasi berada sub menu IP kemudian tab firewall, berikut hasil dari konfigurasi.

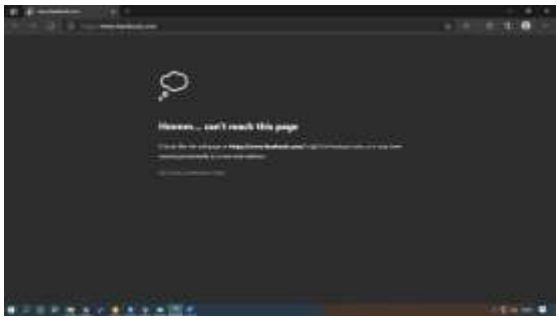


Gambar 9. Konfigurasi firewall

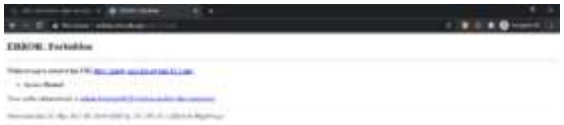
Terdapat dua konfigurasi, dimana konfigurasi pertama merupakan konfigurasi untuk memberikan akses internet kepada pengguna. Sedangkan konfigurasi kedua sebagai pembatas akses internet dimana action diberikan adalah redirect yang berfungsi untuk mengalihkan pengguna untuk secara default masuk ke sistem proxy jika pengguna membuka website atau file yang blokir sebelumnya

D.3. Pengujian

Setelah melakukan konfigurasi, kemudian kami melakukan pengujian dengan mengakses situs dan mendownload file yang sudah diblokir apakah berhasil atau tidak berikut hasilnya.



Gambar 10. Pengujian 1 (blokir media sosial)



Gambar 11. Pengujian 2 (blokir situs ilegal)

Gambar 12. Pengujian 3 (blokir file)

Pada pengujian dikatakan berhasil karena situs tidak dapat diakses, untuk situs judi dan download file berhasil dialihkan kedalam proxy sedangkan facebook tidak karena situs facebook menggunakan port https (443) bukan port http (80) sehingga tidak dialihkan ke dalam proxy yang menyebabkan tampilannya berbeda

E. Kesimpulan

Berdasarkan analisa dari bab – bab sebelumnya dan teori yang ada, maka ditarik kesimpulan bahwa:

1. Port yang digunakan adalah 8080 karena merupakan port http dan mengaktifkan mode cache untuk dapat melakukan pembatasan.
2. Terdapat dua konfigurasi, yaitu konfigurasi untuk memberikan akses internet kepada pengguna dan konfigurasi pembatasan akses internet dimana action yang diberikan adalah redirect yang berfungsi untuk mengalihkan pengguna untuk secara default masuk ke sistem proxy jika pengguna membuka website atau file yang blokir sebelumnya
3. Hasil pengujian dapat dikatakan berhasil karena situs judi dan download file berhasil dialihkan kedalam proxy, Sedangkan facebook tidak karena situs facebook menggunakan port https (443) bukan port http (80) sehingga tidak dialihkan ke dalam proxy yang menyebabkan tampilannya sedikit berbeda.

REFERENSI

[1] A. M. L. - AMIK BSI Purwokerto and Y. B. - AMIK BSI Purwokerto, “Analisis Sistem Pengelolaan, Pemeliharaan dan Keamanan Jaringan Internet Pada IT Telkom Purwokerto,” *Evolusi J. Sains dan Manaj.*, vol. 6, no. 2, pp. 49–56, 2018, doi: 10.31294/evolusi.v6i2.4427.

[2] M. Muhammad and I. Hasan, “ANALISA DAN PENGEMBANGAN JARINGAN WIRELESS BERBASIS MIKROTIK ROUTER OS V . 5 . 20 DI SEKOLAH DASAR NEGERI 24 PALU,” vol. 2, no. 1, 2016.

[3] V. O. L. N. O. Juni, “PERANCANGAN DAN IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN FIREWALL DAN WEB PROXY BERBASIS MIKROTIK DI SMA NEGERI 1 KOTA SUKABUMI Avalaiable at : Avalaiable at :,” vol. 2, no. 1, pp. 27–32.

[4] L. D. Samsumar and S. Hadi, “PENGEMBANGAN JARINGAN KOMPUTER NIRKABEL (WiFi) MENGGUNAKAN MIKROTIK ROUTER (STUDI KASUS PADA SMA PGRI AIKMEL),” vol. 4, no. 1, pp. 1–9, 2018.

[5] M. Ali and F. Latifah, “IMPLEMENASI BLOCK ACCESS PENGGUNA LAYANAN INTERNET DENGAN METODE FILTER RULE dan LAYER 7 PROTOCOL,” *J. Inf. Syst. Applied, Manag. Account. Res.*, vol. 5, no. 2, p. 340, 2021, doi: 10.52362/jisamar.v5i2.422.

[6] A. Ainurridho *et al.*, “SIMULASI JARINGAN WIRELESS DAN MANAGEMENT BANDWDITH DENGAN METODE FIREWALL MANGLE DAN QUEUE TREE UNTUK PRIORITY TRAFFIC,” vol. 11, no. 1, 2022.

[7] J. K. Informatika, “PEMANFAATAN WEB PROXY SEBAGAI PENGOPTIMAL KEAMANAN,” vol. VIII, no. 1, pp. 34–39, 2020.

[8] E. Putra and Arifin, “Web Proxy Server Linux Debian 8 Jessie untuk Blokir Situs pada SMK Al-Washliyah Pasar Senen Kota Medan Provinsi Sumatera Utara,” *J. Ilm. Core IT*, no.

x, pp. 1–12, 2019.

[9] T. Afif, A. Bhawiyuga, and R. A. Siregar, "Implementasi Perangkat Gateway Untuk Pengiriman Data Sensor Dari Lapangan Ke Pusat Data Pada Jaringan Wireless Sensor Network Berbasis Perangkat nRF24L01," vol. 3, no. 4, pp. 3695–3701, 2019, [Online]. Available: http://j-ptiik.ub.ac.id.

[10] T. Gunawan, P. Studi, M. Informatika, P. Studi, M. Informatika, and I. K. Pesawaran, "KONFIGURASI GATEWAY SERVER," vol. 02, no. 01, pp. 1–7, 2021.

[11] H. Wijoyo, "Sistem Informasi Pemesanan Makanan Dan Minuman Di Rumah Makan Putri Minang Jaya," *JS (Jurnal Sekolah) Univ. Negeri Medan*, vol. 3, no. 3, pp. 214–224, 2019, doi: http://dx.doi.org/10.24114/js.v3i3.14761.

[12] M. Sidik, "Perancangan dan Pengembangan E-commerce dengan Metode Research and Development," vol. 04, 2019.

[13] A. Aisyah, P. Studi, P. Matematika, S. Pascasarjana, and U. P. Indonesia, "Studi literatur : Pendekatan induktif untuk meningkatkan kemampuan generalisasi dan self confident siswa SMK," vol. 2, no. 1, pp. 1–12, 2016.

[14] N. Sarip and A. Setyanto, "Packet Filtering Based On Differentiated Services Code Point For DHCP Starvation Attacks Prevention," *J. Pekommas*, vol. 4, no. 2, p. 137, 2019, doi: 10.30818/jpkm.2019.2040204.

[15] B. Lampung, "No Title," vol. 12, no. 1, 2016.