BAB I
PENDAHULUAN

1.1 Latar Belakang

Akses internet telah menjadi bagian penting dari kehidupan sehari-hari bagi jutaan orang di seluruh dunia di era digital yang semakin terhubung. Ini karena internet memungkinkan akses instan ke berbagai jenis informasi, layanan, dan hiburan sehingga memungkinkan komunikasi tanpa batas dan pertukaran pengetahuan yang luas di seluruh dunia [1].

Saat ini, keamanan jaringan sangat penting dalam dunia teknologi informasi, khususnya internet. Hal ini disebabkan karena perangkat jaringan internet rentan terhadap berbagai jenis bahaya dan serangan. Firewall merupakan salah satu metode yang paling umum untuk mengamankan sebuah jaringan. Firewall adalah perangkat lunak atau perangkat yang digunakan untuk mengontrol lalu lintas data yang masuk dan keluar dari jaringan. Oleh karena itu, jaringan internet akan lebih aman dan lebih terkontrol [2].

MikroTik adalah sistem dan perangkat lunak yang berfungsi sebagai Router jaringan yang kuat dengan banyak fitur untuk jaringan kabel dan nirkabel. MikroTik yang digunakan pada perangkat standar berbasis *hardware* pada komputer pribadi (PC) dikenal memiliki kestabilan, keunggulan dan elastisitas untuk mengelola berbagai paket data dan proses *routing*. Router adalah perangkat jaringan yang dapat menghubungkan jaringan ke jaringan lain, dimana bekerja dengan tabel *routing* yang disimpan dalam memori, yang memungkinkan Router untuk menentukan di mana dan bagaimana paket data harus dikirim [3].

Pada Router MikroTik dilengkapi dengan fitur *firewall* dan kemampuan *filtering* yang kuat, membuat sering digunakan oleh seorang *Administrator* jaringan untuk mengatur dan mengelola lalu lintas jaringan dalam suatu jaringan komputer. Maka dari itu, penulis memanfaatkan konsep *firewall filtering* dan *firewall raw*, yaitu mengamankan jaringan dalam pemblokiran beberapa situs ilegal dan tidak layak yang ada di internet serta pencegahan dari serangan seperti DDoS (*Distributed Denial of Service*).

Dari penelitian sebelumnya oleh Sutarti, Siswanto dan Sriansyah Bachtiar, “Analisis Web Phising Menggunakan Metode Network Forensic Dan Block Access Situs Dengan Router MikroTik” (2023). Penelitian ini membahas tentang 3 langkah yang dilakukan dalam

investigasi *network forensic*, yaitu : Akuisisi dan Pengintaian, Analisis, dan *Recovery*. Pada tahap akuisisi dan pengintaian dilakukan pencarian beberapa situs web yang diduga *phising*, tahap analisis pengecekan dilakukan pada salah satu situs web dan tahap *recovery* akan melakukan *blocking* pada *website* tersebut. Serta ditambahkan Router MikroTik di topologi jaringan agar user terjaga dari serangan *web phising* dengan rancangan menggunakan perangkat *hardware*, diantaranya : Processor, Memory, Harddisk, Modem dan Router, serta menggunakan perangkat software, diantaranya : Google Chrome, Wireshark dan Winbox.

Penelitian berikutnya oleh Tamsir Ariyadi dan Achmad Taufan Maulana, "Penerapan Web Proxy Dan Management Bandwidth Menggunakan MikroTik RouterBoard Pada Kantor Pos Palembang 30000" (2021). Penelitian ini membahas tentang penerapan *Web Proxy* sebagai pengontrol kinerja *internet* dimana bisa dilakukan blok *website* yang dapat mengganggu kinerja pegawai serta memanajemen *Bandwidth* menggunakan konsep *simple queue* agar memberikan jaringan *internet* yang optimal pada Kantor Pos Palembang 30000.

Penelitian berikutnya oleh Rully Mujiastuti dan Ibnu Prasetyo, "Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE" (2021). Penelitian ini membahas tentang implementasi keamaman jaringan dengan *Virtual Private Network* (VPN) sebagai akses ke *internet* lebih aman terhadap ancaman MITM (*Man In The Middle*) dan *Domain Name Services* (DNS) sebagai DNS *filtering* yang dapat memblokir iklan online saat pengguna mengakses *internet*.

Penelitian berikutnya oleh Kartini Harahap, "Penerapan Algoritma Exact String Matching Dalam Pembuatan Program Blokir Situs Porno" (2019). Penelitian ini membahas tentang memblokir situs porno menggunakan metode *Exact String Matching*, fitur *Porn Situs Monitoring* dan *Visual Basic.Net* 2010, yaitu fitur-fitur dimana setiap kata yang memiliki unsur kesamaan pada saat diinput ke *website* maka konten yang diinput tersebut akan ditutup.

Penelitian berikutnya oleh Muhammad Husaini, Wire Bagye dan Maulana Ashari, "Implementasi Fitur Layer 7 Protocols MikroTik RB750 Di SMKN 1 Narmada" (2019). Penelitian ini membahas tentang pemblokiran beberapa situs yang tidak diinginkan dirancang menggunakan protokol *https Proxy Server* dengan fitur *Layer 7 Protocol* MikroTik RB750 di jaringan SMKN 1 Narmada.

Penelitian berikutnya oleh Asyiq Maulana, Nugroho Suharto dan Aad Hariyadi, "*Implementation of MikroTik Firewall for Website Access Restriction and Prevention of DoS (Denial of Service) Attacks on Internet Networks of Al-Mahrusiyah Vocational School*

Lirboyo" (2023). Penelitian ini membahas tentang pengujian firewall pada Router MikroTik menggunakan kombinasi filter dan Raw untuk memblokir akses website media sosial dan situs streaming film. Sehingga *client* tidak dapat mengakses dan browser pada *client* menampilkan pemuatan terus menerus.

Penelitian berikutnya oleh Karel Hynek, Dmitrii Vekshin, Jan Luxemburk, Tomas Cejka dan Armin Wasicek, "*Summary of DNS Over HTTPS Abuse*" (2022). Penelitian ini membahas tentang implementasi *protocol DNS over HTTPS* (DoH) sebagai cara mengatasi masalah privasi *Domain Name System* (DNS), salah satu dilakukan penelitain dalam kemanan jaringan terkait DoH yaitu: *DoH Blocking/Filtering*, yaitu memungkinkan pencegahan koneksi ke penyedia DoH yang tidak diizinkan dan tidak dapat dipercaya lalu memblokirnya secara tepat waktu.

Penelitian berikutnya oleh Norma Guti´errez, "*Malicious Websites Blocking System using Deep Learning algorithms*" (2021). Penelitian ini membahas tentang implemetasi *Malicious URL detection* yang merupakan deteksi Dimana memastikan pengguna melakukan penjelejahan dengan aman dan memblokir konten dan situs yang tidak diinginkan. Berikutnya peneliti memformat ulang *Visualisation of Malicious & Benign Web-pages Dataset* (VoMBWeb) dan mengekstrak fitur dasar situs web yang ada (berbahaya dan tidak berbahaya) untuk melakukan penelitian. Selain itu, peneliti menerapkan *Feed Forward Neural Network* (FFNN) untuk menghitung klasifikasi label. Setelah mempelajari berbagai variasi FFNN dan melakukan beberapa percobaan, peneliti menyimpulkan bahwa jaringannya dapat membedakan situs web berbahaya dari situs web jinak secara efisien dan efektif.

Penelitian berikutnya oleh Ibnu Muakhori, Sunardi dan Abdul Fadlil, "*Security Of Dynamic Domain Name System Servers Against DDOS Attacks Using IPTABLE And FAIL2BA*" (2020). Penelitian ini membahas tentang pencegahan serangan bertipe *Bruteforce* dengan menerapkan IPTable dan Fail2ban untuk memblokir Alamat IP penyerang. Fail2ban adalah paket program sebagai pendeteksi upaya login yang gagal lalu memblokir alamat IP *host* asli dimana bekerja dengan mengubah *rules* konfigurasi *firewall* (IPTable) dengan konfigurasi yang terdapat pada Fail2ban itu sendiri, sehingga ketika Fail2ban dijalakan maka akan mengambil melalui fungsi *firewall* yang ada di *server*.

Penelitian berikutnya oleh Ni'matul Ulfaha, Ninon Oktaviani Irawana, Piska Dwi Nurfadilaa, Putri Yuni Ristantia dan Jehad A.H Hammad, "*Blocking Pornography Sites on the Internet Private and University Access*" (2019). Penelitian ini membahas tentang

pengkajian teknik yang dilakukan oleh ISP dalam melakukan pemblokiran situs pornografi, sehingga didapatkan lima teknik yang digunakan oleh ISP yaitu *DNS Filtering*, *DNS Poisoning and spoofing*, *Border Gateway Protocol* (*BGP*), *Positive Trust* dan *Application Control & URL filtering*.

Berikut adalah tabel referensi perbandingan jurnal nasional dan internasional pada Tabel 1.1 dan 1.2 di bawah ini:

Tabel 1.1 Daftar Referensi Jurnal Nasional

No	Jurnal	Persamaan	Perbedaan
1	Sutarti, Siswanto dan Sriansyah Bachtiar, *Analisis Web Phising Menggunakan Metode Network Forensic Dan Block Access Situs Dengan Router MikroTik*. Vol. 10, No. 1, Maret 2023 https://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/view/7048	- Keamanan jaringan - Blokir Situs Web - Berbasis Router MikroTik	- Pengecekan *Web Phising* dengan konsep *Network Forensik*
2	Tamsir Ariyadi, A. Taufan Maulana, *Penerapan Web Proxy Dan Management Bandwidth Menggunakan MikroTik RouterBoard Pada Kantor Pos Palembang 30000*. Vol. 9, No. 2, 10 September 2021 http://ejournal.upbatam.ac.id/index.php/jif/article/view/4444	- Keamanan jaringan - Blokir Situs Web - Berbasis Router MikroTik	- *Management Bandwidth* menggunakan metode *simple queue*
3	Rully Mujiastuti, Ibnu Prasetyo, *Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE*. 17 November 2021	- Kemanan jaringan - Blokir Situs Web	- Konsep VPN Server - DNS *filtering*

	https://jurnal.umj.ac.id/index.php/semnastek/article/view/11484		
4	Kartini Harahap, *Penerapan Algoritma Exact String Matching Dalam Pembuatan Program Blokir Situs Porno*. Vol. 8, No. 1, Juli 2019 http://ejurnal.stmik-budidarma.ac.id/index.php/pelita/article/view/1525	- Kemanan jaringan - Blokir Situs Web	- Metode *Exact String Matching*, fitur *Porn Situs Monitoring* dan *Visual Basic.Net* 2010
5	Muhammad Husnaini, Wire Bagye, Maulana Ashari, *Implementasi Fitur Layer 7 Protocols MikroTik RB750 di SMKN 1 Narmada*. Vol. 2, No. 1, April 2019 https://www.e-journal.stmiklombok.ac.id/index.php/jire/article/view/94	- Keamanan jaringan - Blokir Situs Web - Berbasis Router MikroTik - Topologi jaringan LAN/WLAN	- Konsep *Proxy Server* (*https*) dengan fitur *Layer 7 Protocol*

Tabel 1.2 Daftar Referensi Jurnal Internasional

No	Jurnal	Persamaan	Perbedaan
1	Asyiq Maulana, Nugroho Suharto dan Aad Hariyadi, *Implementation of MikroTik Firewall for Website Access Restriction and Prevention of DoS (Denial of Service) Attacks on Internet Networks of Al-Mahrusiyah Vocational School Lirboyo*. Vol. 13, No. 1, 31 March 2023	- Keamanan jaringan - Blokir situs web - Pencegahan serangan DoS/DDoS - Berbasis Router MikroTik	- Terget pemblokiran situs yaitu website media sosial dan *streaming*

	http://jartel.polinema.ac.id/index.php/jartel/article/view/547		
2	Karel Hynek, Dmitrii Vekshin, Jan Luxemburk, Tomas Cejka dan Armin Wasicek, *Summary of DNS Over HTTPS Abuse*. Vol. 10, May 2022 https://ieeexplore.ieee.org/abstract/document/9775718/	- Keamanan jaringan - Blokir Situs web	- Mengimplem ntasi *protocol DNS over HTTPS* (DoH) dengan konsep *DoH Blocking/Filtering*
3	Norma Guti´errez, *Malicious Websites Blocking System using Deep Learning algorithms*. July 2021 https://upcommons.upc.edu/handle/2117/357059	- Keamanan jaringan - Blokir situs web	- Konsep *Malicious URL detection* - *Feed Forward Neural Network* (FFNN)
4	Ibnu Muakhori, Sunardi dan Abdul Fadlil, *Security Of Dynamic Domain Name System Servers Against DDOS Attacks Using IPTABLE And FAIL2BA*. Vol. 4, No.1, 1 May 2020 https://iocscience.org/ejournal/index.php/mantik/index	- Keamanan jaringan - Blokir situs web	- Penerapan teknik IPTable dan Fail2ban

5	Ni'matul Ulfaha, Ninon Oktaviani Irawana, Piska Dwi Nurfadilaa, Putri Yuni Ristantia dan Jehad A.H Hammad, *Blocking Pornography Sites on the Internet Private and University Access*. Vol. 3, No. 1, March 2019 http://pubs.ascee.org/index.php/businta/article/view/161	- Keamanan jaringan - Blokir situs web	- Penerapan 4 teknik, yaitu *DNS Filtering*, *DNS Poisoning and spoofing*, *Border Gateway Protocol* (*BGP*), *Positive Trust* dan *Application Control & URL filtering*.

Berdasarkan penelitian sebelumnya, penulis ingin membuat sistem keamanan jaringan untuk pemblokiran situs ilegal dan tidak layak serta pencegahan dari serangan *Distributed Denial of Service* (DDoS) dengan menerapkan Router MikroTik sebagai Router manajemen dan pengatur lalu lintas data di sebuah jaringan LAN & WLAN ruangan NOC & IT PT. Cendikia Global Solusi, sehingga dari penulis memperkenalkan fitur *firewall filtering* (*filter rules*) dan *firewall raw* pada Router MikroTik kepada para karyawan NOC & IT. Maka dari itu, judul yang diangkat untuk melakukan penelitian ini adalah "Strategi Keamanan Jaringan Dan Pencegahan Serangan DDoS Dengan Konsep Firewall Filtering Dan Raw".

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian proyek akhir ini yaitu:

1. Menggunakan konsep keamanan jaringan apa untuk memblokir akses situs yang ilegal atau tidak layak?
2. Dengan menggunakan metode keamanan jaringan apa agar tercegah dari serangan DDoS (*Distributed Denial of Service*) pada Router?
3. Perangkat apa saja yang digunakan untuk mengimplementasi strategi keamanan jaringan berbasis MikroTik dengan konsep *firewall filtering* dan *firewall raw*?

1.3 Batasan Masalah

Batasan masalah dalam penelitian proyek akhir ini yaitu:

1. Memblokir akses ke situs web ilegal atau tidak layak dengan menggunakan *firewall filtering* (*filter rules*) MikroTik dengan melihat parameter

keberhasilannya berada di jumlah data yang ditransfer (*bytes*) dan jumlah paket data yang berjalan di jaringan melalui RouterBoard MikroTik (*packets*) .

2. Mencegah serangan DDoS (*Distributed Denial of Service*) pada Router dengan menggunakan *firewall raw* MikroTik dengan melihat parameter keberhasilannya berada di perubahan *persentase* dan penggunaan CPU serta di *resources* pada *firewall connections*.
3. Jenis keamanan jaringan dan serangan DDoS yang akan diuji cobakan adalah tipe *content* berupa nama *domain website* pada *firewall filtering* (*filter rule*) dan tipe TCP *syn attack* pada *firewall raw*.
4. Mengimplementasi blok situs web ilegal dan pencegahan serangan DDoS dengan berbasis MikroTik serta berfokus pada perangkat Router RB450Gx4, Switch TP-Link SG3424, Access Point BDCOM GP1704-4F-E dan beberapa perangkat *host client* (PC dan Laptop)
5. Menggunakan desain jaringan LAN & WLAN ruangan NOC & IT PT. Cendikia Global Solusi.

1.4 Tujuan Penelitian

Tujuan dalam penelitian proyek akhir ini yaitu:

1. Mengantisipasi keamanan jaringan dalam mengakses situs ilegal atau tidak layak dengan mengusulkan konsep *firewall filtering* (*filter rules*) berbasis MikroTik dengan hasil pengukuran parameternnya adalah pada monitoring *statistics firewall filter rules* MikroTik.
2. Menggunakan *firewall raw* berbasis MikroTik sebagai cara menghindari serangan DDoS (*Distributed Denial of Service*) terhadap arus lalu lintas dan trafik paket data jaringan dalam Router dengan hasil pengukuran perameternya adalah pada *persentase* CPU dan jumlah paket *resources* di *firewall connections* perangkat RouterBoard MikroTik.

1.5 Manfaat Penelitian

Setelah dengan permasalahan dan tujuan penelitian yang telah disebutkan di atas, maka manfaat penelitian dapat dirumuskan sebagai berikut:

1. Memperkenalkan dan memberikan fitur-fitur keamanan jaringan, yaitu *firewall filtering* dan *firewall raw*, kepada para karyawan lalu menerapkannya di lingkungan kerja NOC & IT PT. Cendikia Global Solusi.

2. Menciptakan jaringan di lingkungan kerja NOC & IT PT. Cendikia Global Solusi, baik dari perangkat kerja NOC & IT maupun para karyawan NOC & IT, menjadi bebas dan terlindungi dari situs web ilegal dan tidak layak digunakan.
3. Meningkatkan keamanan dan kinerja pada perangkat RouterBoard MikroTik dalam koneksi dan trafik paket data di jaringan LAN & WLAN ruangan NOC & IT PT. Cendikia Global Solusi.

1.6 Metodologi Penelitian

Metode yang penulis lakukan dalam mencari data yang diperlukan adalah dengan menggunakan metode :

1. Perencanaan penelitian

   Tahap ini adalah tahapan dimana proses identifikasi permasalahan yang akan diteliti.
2. Pengumpulan data

   Pada tahap ini mengenai tentang proses identifikasi masalah yang dikumpulkan melalui observasi penelitian.
3. Implementasi

   Tahap implementasi dilaksanakan untuk memulai konfigurasi *firewall filtering* dan *firewall raw* sebagai keamanan jaringan dalam pemblokiran situs web ilegal dan tidak layak digunakan serta pencegahan dari serangan DDoS.
4. Pengujian dan hasil

   Tahap ini adalah tahapan dibuatkan skenario dari konsep *firewall filtering* dan *firewall raw* yang sudah dikonfigurasi untuk pengujian apakah dari kedua fitur keamanan jaringan RouterBoard MikroTik ini dapat berfungsi dengan baik.

1.7 Sistematika Penulisan

Secara umum, sistematika penulisan proyek akhir ini terdiri dari beberapa bab dengan metode penyampaian sebagai berikut :

BAB I PENDAHULUAN

Berisi latar belakang, tujuan penelitian, rumusan masalah, batasan masalah, metodologi penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Berisi beberapa teori dan data-data pendukung pada proyek akhir yang kemudian

mengacu ke pengerjaan proyek akhir.

BAB III PERANCANGAN DESAIN DAN KONFIGURASI KEAMANAN JARINGAN

Berisi gambaran umum lokasi penelitian, diagram alir yang terbagi penjelasan di dalamnya yaitu perencanaan penelitian, pengumpulan data dan persiapan penelitian, hingga implementasi penelitian mulai dari konfigurasi dasar perangkat Router, Switch, Access Point hingga konfigurasi keamanan jaringan *fiewall filtering* (*filter rules*) dan *firewall raw*.

BAB IV HASIL DAN ANALISA

Berisi hasil percobaan dan menganalisa keamanan jaringan pada konfigurasi *firewall filtering* (*filter rules*) untuk pemblokiran situs web ilegal atau tidak layak dan konfigurasi *firewall raw* untuk pencegahan serangan DDoS.

BAB V PENUTUP

Berisi kesimpulan dari bab iv serta saran atau pertimbangan dari penulis.

1.8 Jadwal Pengerjaan Proyek Akhir

Merupakan jadwal penyelesaian kegiatan proyek akhir yang telah penulis buat pada tabel 1.3 di bawah ini:

Tabel 1.3 Jadwal Penyusunan Proyek Akhir

NO	Kegiatan	Waktu							
		Jan	Feb	Mar	Apr	Mei	Jun	Jul	Aug
1	Tahapan Persiapan Penelitian								
	a. Pengajuan Judul								
	b. Pengajuan Proyek Akhir								
	c. Perizinan Penelitian								
2	Tahap Pelaksanaan Penelitian								
	a. Pengumpulan Data Proyek Akhir								
	b. Implementasi dan Menerapkan Fitur								

	Keamanan Jaringan *firewall filtering* (*filter rules*) dan *firewall raw* dari perangkat RouterBoard MikroTik								
	c. Percobaan Hasil dari Implemetasi Keamanan Jaringan *firewall filtering* (*filter rules*) dan *firewall raw* dari perangkat RouterBoard MikroTik								
3	Tahap Penyusunan Proyek Akhir								