STRATEGI KEAMANAN JARINGAN DAN PENCEGAHAN SERANGAN DDOS DENGAN KONSEP FIREWALL FILTERING DAN RAW

Naufal Hafidh
Program Studi D3 Teknik Telekomunikasi
Universitas Telkom Kampus Jakarta
Jakarta, Indonesia
naufalh@student.telkomuniversity.ac.id

Nurwan Reza Fachrur Rozi, S.T., M.T.
Pembimbing 1 D3 Teknik Telekomunikasi
Universitas Telkom Kampus Jakarta
Jakarta, Indonesia
nurwan@telkomuniversity.ac.id

Ade Nurhayati, S.T., M.T.
Pembimbing 2 D3 Teknik Telekomunikasi
Universitas Telkom Kampus Jakarta
Jakarta, Indonesia
adenurhayati@telkomuniversity.ac.id

***Abstrak* — Strategi Keamanan Jaringan Dan Pencegahan Serangan DDoS Dengan Konsep Firewall Filtering Dan Raw ini bertujuan agar keamanan jaringan dalam perangkat Router di sebuah ruangan NOC & IT menjadi lebih aman dari ancaman serangan Distributed Denial of Service (DDoS) dan menjadikan lingkungan kerja NOC & IT terbebas dari akses beberapa situs web yang bersifat ilegal atau tidak layak. Pada ruangan NOC & IT ini memliki topologi jaringan berbentuk LAN & WLAN yang terdiri dari beberapa perangkat jaringan yang saling terkoneksi. Penelitian ini memanfaatkan konsep firewall filtering (filter rules) sebagai fitur pengelola masuk atau tidaknya suatu rute paket data yang melewati Router dari jaringan lokal ke internet serta konsep firewall raw sebagai fitur proteksi jaringan dari serangan DDoS. Untuk mengimplementasikan kedua konsep ini, dilaksanakan dengan perangkat manajemen jaringan RouterBoard MikroTik. Perancangan penelitian ini dimulai dari tahapan-tahapan yang meliputi tahap perencanaan penelitian, tahap pengumpulan data, tahap persiapan rancangan, serta tahap pengujian dan hasil. Untuk hasil dari penelitian ini adalah telah terlaksananya perancangan memblokir beberapa situs web ilegal dan mengamankan perangkat jaringan Router dari serangan DDoS, lalu dari sisi ruangan NOC & IT sudah terimplementasikan akses internet yang sehat dan terlindungi para karyawan dari beberapa situs web yang tidak layak serta pada perangkat Router yang terpasang di ruangan NOC & IT juga sudah terjaga dan aman dari serangan DDoS.**

***Kata kunci* — Jaringan Internet, Situs Web, DDoS, RouterBoard MikroTik, Firewall filtering, Firewall raw**

I. PENDAHULUAN

A. 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).

B. Rumusan Masalah

Pada rumusan masalah ini adalah :

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?

C. Batasan Masalah

Pada batasan masalah ini adalah :

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.

D. Tujuan Penelitian

Pada tujuan penelitian ini adalah :

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.

E. Manfaat Penelitian

Pada manfaat penelitan ini adalah :

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.

F. Metodologi Penelitian

Metode yang peneliti 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.

G. Tinjauan Pustaka

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 1 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 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 2 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.

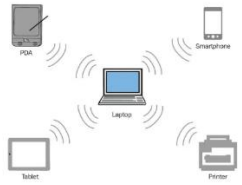
II. KAJIAN TEORI

A. Definisi Jaringan Internet

Jaringan internet merupakan sebuah jaringan komputer dengan sistem global yang saling terkoneksi satu sama lain di keseluruhan dunia dimana memakai model TCP/IP. Adanya internet sebagai sebuah jaringan dan infrastruktur dapat mengakomodasi efektifitas serta efisiensi operasional terutama di sebuah sarana komunikasi, publikasi hingga menghasilkan beberapa informasi yang diperlukan [4].

Terdapat beberapa jenis jaringan yang umum diterapkan berdasarkan cakupan wilayah atau geografis, antara lain :

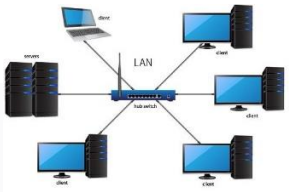
a. Personal Area Network (PAN)



Gambar 2.1 Desain Personal Area Network [6]

Merupakan jenis jaringan dengan cakupan wilayah yang lebih kecil dari LAN, digunakan sebagai koneksi pada perangkat pribadi seperti headset nirkabel yang terhubung ke komputer atau handphone melalui Bluetooth. PAN mempunyai kelebihan dalam segi mobilitas Dimana perangkat bisa berkomunikasi dalam jarak yang sangat dekat. Sehingga dalam jangakauan yang tergolong terbatas inilah menjadi kelemahan pada PAN, yakni tidak bisa dihubungkan perangkat pada lokasi yang lebih jauh.

b. Local Area Network (LAN)



Gambar 2.2 Desain Local Area Network [7]

Merupakan jenis jaringan dengan cakupan wilayah yang lebih besar dari PAN namun lebih kecil dari MAN dan WAN, digunakan untuk menghubungkan jaringan dalam jarak lingkup seperti kantor atau rumah. LAN memiliki fungsi utama yaitu memungkinkan perangkat di dalam jaraknya untuk saling berbagi sumber daya, misalnya file, printer dan koneksi internet. Pada LAN ini juga terdapat WLAN dan VLAN, WLAN merupakan jenis jaringan yang bersifat seperti LAN namun lebih fleksibel dikarenakan dalam koneksinya melalui media sinyal udara dan memakai teknologi frekuensi radio. Sedangkan VLAN merupakan jenis jaringan yang menerapkan koneksi logika dalam koneksi berbentuk fisik.

c. Metropolitan Area Network (MAN)

Gambar 2.3 Desain Metropolitan Area Network [7]

Merupakan jenis jaringan dengan cakupan wilayah yang lebih besar dari PAN dan LAN namun lebih kecil dari WAN, digunakan untuk menghubungkan jaringan dalam jarak lingkup seperti area perkotaan atau metropolitan. MAN bisa menggunakan berbagai teknologi yaitu serat optik ataupun kabel tembaga untuk mengkoneksikan ke berbagai lokasi dalam kota, sehingga sering digunakan oleh ISP dan bisnis besar yang perlu konektivitas antar lokasi di dalam kota.

d. Wide Area Network (WAN)

Gambar 2.4 Desain Wide Area Network [7]

Merupakan jenis jaringan internet yang paling umum digunakan dengan cakupan wilayah yang sangat luas bahkan melewati negara atau benua. WAN menghubungkan beberapa LAN dan pusat data di seluruh dunia yang memungkinkan untuk berkomunikasi dan akses data secara luas dan global.

Selain itu, terdapat 2 jenis jaringan internet berdasarkan jenis transmisi, antara lain:

a. Wired Network

Gambar 2.5 Kabel LAN UTP (Unshielded Twisted Pair) [8]

Adalah jenis transmisi yang menggunakan media kabel untuk mengirimkan transmisi data antar perangkat, contoh: kabel tembaga dan serat optik. Jaringan kabel ini memiliki kelebihan yakni dari segi keandalan dan kecepatan transfer data yang tinggi, sedangkan kekurangan dari jenis ini yakni mobilitas yang terbatas dikarenakan perangkat yang terkoneksi melalui kabel fisik.

b. Wireless Network

Gambar 2.1 Jaringan Sinyal Wireless [9]

Adalah jenis transmisi yang menggunakan sinyal nirkabel untuk mengirimkan transmisi data antar perangkat, contoh: Wi-Fi, Bluetooth dan seluler (4G/5G). Jaringan kabel ini memiliki kelebihan yakni dari segi kenyamanan mobilitas yang tinggi kepada user dan memungkinkan koneksi tanpa Batasan fisik, sedangkan kekurangan dari jenis ini yakni keandalan dan kecepatan transfer data yang sedikit lebih rendah serta sinyalnya yang rentan terhadap gangguan.

B. Situs Web Internet

Situs web (website) adalah sekumpulan informasi melalui internet yang terbagi menjadi halaman web yang saling terkoneksi yang disediakan dalam bentuk peorangan, kelompok bahkan organisasi/perusahaan. Pada situs web yang bersifat kebaikan maka dimunculkan isian yang menarik dan bermanfaat bagi kebutuhan pengguna. Begitupun sebaliknya, jika situs web yang bersifat kejahatan maka isian di dalamnya terdapat hal yang tidak layak dimanfaatkan oleh pengguna [10].

C. Keamanan Jaringan Internet

Keamanan jaringan internet merupakan sistem yang memiliki tugas untuk mengidentifikasi dan menangani akses yang ilegal pada suatu jaringan internet. Biasanya, dalam proses penggunaan komputer dari pengguna secara tenang dan tidak tau apa-apa ketika akses situs web tidak dikenal lalu mengunduh suatu file, folder ataupun terus menelusuri secara dalam dari situs web tersebut lalu tidak akan dipakai lagi setelah mengaksesnya. Hal seperti ini dapat berbahaya yang sembunyi pada keamanan jaringan komputer dimana setiap situs web yang tidak dikenal bisa saja mengandung virus atau yang bersifat negatif lainnya. Dikarenakan jika tidak dilakukan software maupun fitur sebagai filtering paket data jaringan, dapat berakibatkan kerusakan/infeksi dan kebocoran informasi terhadap komputer [11].

D. Cybercrime

Cybercrime adalah suatu tindak kejahatan yang dilakukan di dunia maya dimana pelaku menjalankan aksinya dengan menyadapkan data-data yang terhubung dengan perangkat jaringan. Dalam skala kecil, pengertian dari cybercrime adalah computer crime yang diarahkan terhadap sistem ataupun jaringan pada komputer. Sedangkan dalam skala besar, cybercrime adalah kejahatan yang telah mencakup luas pada komputer, jaringan komputer dan penggunanya dimana dilakukan dengan memakai alat bantu komputer (computer related crime) [12].

Oleh karena itu, Cybercrime sudah ditandakan sebagai melanggar hukum dikarenakan aksi ini melakukan masuk ke jaringan komputer pengguna lain tanda adanya izin. Kemampuan serbaguna yang ditunjukkan oleh kemajuan teknologi informasi dan komunikasi membedakannya dari tindak pidana serupa [13]. Terdapat macam-macam kejahatan pada cybercrime dari segi aktivitas, antara lain:

a. Akses Sistem Jaringan Secara Tidak Sah

Merupakan jenis kejahatan cybercrime pada saat penyusup masuk ke dalam sistem jaringan komputer pengguna lain secara diam-diam dan tanpa diketahui.

b. Konten Ilegal

Merupakan jenis kejahatan cybercrime yang dilakukan dengan memasukkan data atau informasi ke internet yang tidak benar atau tidak etis. Ini dapat dianggap sebagai pelanggaran hukum atau mengganggu, mulai dari menyebarkan perjudian, pornografi hingga berita palsu.

c. Penyebaran Virus

Merupakan jenis kejahatan cybercrime yang secara umum dilakukan menggunakan lewat email yang dimana membuat sistem email pengguna lain terserang virus tanpa disadari olehnya.

d. Cyber Spionase dan Sabotase

Cyber spionase merupakan jenis kejahatan cybercrime yang melakukan pengintaian ke sistem jaringan komputer pengguna lain. Sedangkan cyber sabotase 16 merupakan jenis kejahatan cybercrime yang melakukan mengganggu data, program maupun sistem komputer yang terhubung ke jaringan internet.

e. Carding

Merupakan jenis kejahatan cybercrime yang melakukan pencurian nomor kartu kredit pengguna lain yang kemudian dipergunakan transaksi perdagangan di internet, baik itu perdagangan legal maupun ilegal.

f. Cybersquatting dan Typosquatting

Cybersquatting merupakan jenis kejahatan cybercrime yang melakukan mendaftar nama domain perusahaan lain secara diam-diam yang kemudian menjual nama domain tersebut dengan harga yang tinggi. Typosquatting merupakan jenis kejahatan cybercrime yang membuat nama domain palsu dengan semirip nama domain yang asli.

g. Cyber Terrorism

Merupakan jenis kejahatan cybercrime ketika pengguna menjalankan aksi ancaman seperti cracking ke pemerintah atau warga negara.

h. Hacking dan Cracking

Hacking biasanya merujuk pada tindakan yang dilakukan oleh para ahli keamanan atau hacker dengan tujuan untuk menemukan kesalahan dalam sistem komputer dan jaringan untuk membantu meningkatkan pertahanan siber suatu organisasi. Sedangkan cracking lebih ke tindakan jahat yang bermaksud menghancurkan keamanan sistem jaringan komputer.

E. Distributed Denial of Service (DDoS)

DDoS merupakan jenis cybercrime yang dilakukan oleh pengguna tidak dikenal dengan menyerang sampai membanjiri pada arus lalu lintas jaringan sehingga mengakibatkan sumber daya dalam suatu komputer atau server menjadi habis [14].

Terdapat beberapa jenis serangan pada DDoS [15], sebagai berikut:

a. Neptune: Jenis serangan dari penyerang akan menjalankan serangan serta memeriksa kelemahan dalam proses three-way-handshake pada protokol TCP dimana secara terus-menerus mengirimkan paket SYN secara langsung yang berakibatkan sumber daya pada server jadi habis.

b. Smurf: Jenis serangan yang dilakukan dengan mengirimkan paket ICMP yang memiliki jumlah yang banyak sehingga suatu komputer pengguna lain akan mendapatkan kebanjiran terhadap beberapa pesan palsu.

F. Firewall

Firewall (tembok api) adalah sebuah fitur kemanan jaringan komputer terhadap pencegahan serangan dan penyusupan yang berakibat membahayakan kerahasiaan data sampai kerusakan pada infrastruktur jaringan [16].

Gambar 2.7 Skema Firewall dalam Jaringan [17]

Dalam metode atau mekanisme firewall yang digunakan yaitu pada hardware, software, atau sistem itu sendiri untuk melindungi, baik dengan menyaring, membatasi, atau bahkan menolak suatu atau semua hubungan dan kegiatan segmen tertentu pada jaringan pribadi dengan jaringan luar. Segmen ini dapat mencakup workstation, server, Router atau Local Area Network (LAN). Sebagian besar, firewall digunakan untuk melayani:

a. Komputer setiap orang yang terhubung langsung ke jaringan luar atau internet dan ingin melindungi semua yang ada di komputernya.

b. Jaringan komputer yang terdiri dari lebih dari satu komputer dan berbagai topologi jaringan yang digunakan oleh perusahaan, organisasi, dan lain-lain.

Dengan firewall, sistem jaringan komputer dapat melindungi data sensitif dan mengatur lalu lintas pengaksesan baik dari dalam maupun dari luar sistem. Sehingga memiliki empat fungsi umum pada firewall yang diantaranya:

a. Mengawasi dan mengatur lalu lintas.

b. Melakukan autentikasi terhadap akses.

c. Melindungi sumber daya dalam jaringan private.

d. menyimpan catatan setiap peristiwa lalu melaporkannya kepada Administrator.

G. MikroTik

Gambar 2.8 Logo MikroTik [18]

Situs MikroTik suatu perangkat jaringan pada komputer meliputi hardware dan software yang difungsikan mulai dari sebagai Router, alat filtering dan lain sebagainya. Untuk hardware di MikroTik dapat berupa Router PC yang sudah terdapat installer pada PC dan perangkat RouterBoard yang sudah dibuat atau dirancang langsung dari perusahaan MikroTik. Sedangkan untuk software di MikroTik terdapat beberapa nama RouterOS beserta versi-versi yang dimilikinya [19].

H. RouterBoard MikroTik

Gambar 2.9 RouterBoard MikroTik [20]

RouterBoard MikroTik adalah perangkat Router jaringan buatan MikroTik yang terdiri dari prosesor, RAM dan ROM. Pada perangkat ini dilengkapi dengan RouterOS, sehingga pengguna dapat langsung menggunakannya tanpa harus menginstal program. Lalu pada fungsi-fungsi dari RouterBoard dengan perlengkapan RouterOS diantaranya sebagai Router jaringan, memanajemen bandwidth hingga juga bisa sebagai hotspot server [21].

I. Firewall Filter Rule

Firewall filter rules adalah salah satu fitur firewall MikroTik yang dapat dimanfaatkan sebagai pemblokir aktivitas jaringan yang memiliki potensi berbahaya, misalkan memblokir situs web ilegal atau tidak dikenal serta penggunaan aplikasi seperti Torrent, VPN, port scanning dan recursive DNS [22].

Pada filter rules terdapat tiga chain, antara lain:

- Forward: Berfungsi untuk menangani trafik paket data yang hanya melewati Router.
- Input: Berfungsi untuk menangani trafik paket data yang masuk ke Router melalui interface Router. Paket tidak dapat melewati Router jika bertentangan dengan aturan atau rules chain input.
- Output: Merupakan kebalikan dari input, dimana berfungsi untuk memproses trafik paket data yang keluar dari Router dan melalui salah satu interface.

J. Firewall Raw

Firewall raw merupakan fitur yang juga berfungsi menangani filter paket dimana konsep pemblokiran sama seperti firewall filter rules. Namun, firewall raw tidak membutuhkan sumber daya CPU sebanyak firewall filter karena pada raw memiliki kemampuan untuk drop packet sebelum proses connection tracking dimulai. Connection tracking adalah kemampuan untuk melacak informasi seperti source address, destination address, source and destination port, tipe protokol, dan lain-lain pada koneksi yang sedang berlangsung. Dalam kata lain, raw menjadi lebih hemat sumber daya dikarenakan tidak menggunakan connection tracking dalam proses filtering. Sehingga dengan kemampuan ini dapat digunakan untuk dropping paket dalam jumlah besar dan cocok untuk mencegah serangan DDoS [23].

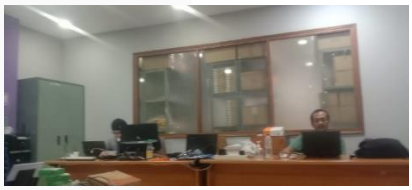
III. METODE

A. Gambaran Umum Penelitian

PT. Cendikia Global Solusi (CGS) adalah sebuah perusahaan yang bergerak di bidang jaringan fiber optic dan telekomunikasi yang berlokasi di Kompleks Ruko Majapahit Permai, Jl. Majapahit No. 18-22 Blok A No.3-4, Jakarta 10160. Dalam kantor CGS, terdapat ruangan divisi NOC & IT dimana dalam ruangan kerjanya sudah terdapat arsitektur jaringan LAN dan WLAN serta terdapat koneksi internet, namun memiliki kekurangan pada fitur firewall sebagai keamanan dan penjagaan jaringan pada perangkat RouterBoard server NOC & IT.

Gambar 3.1 Meja Kerja PC Staff NOC West, Central dan East

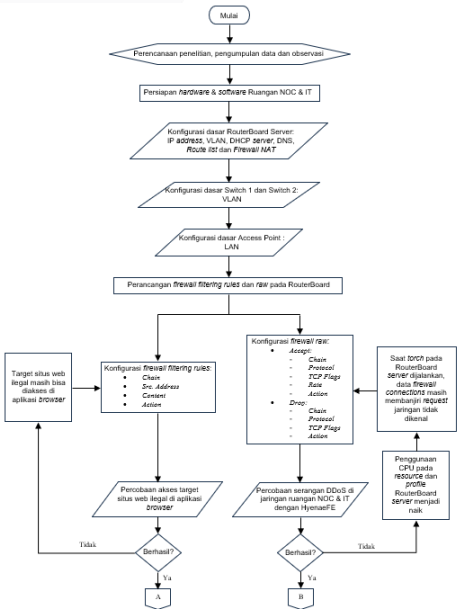
Gambar 3.2 Meja Kerja PC Admin dan Supervisor NOC



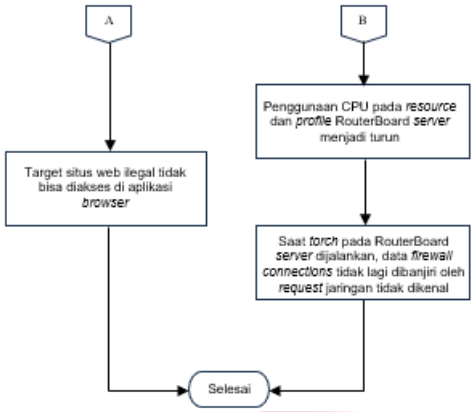
Gambar 3.3 Meja Kerja Laptop Staff IT

B. Diagram Alir Penelitian

Pada bagian diagram alir penelitian berisikan langkah-langkah dalam mengerjakan fitur keamanan jaringan sampai selesai.



Gambar 3.4 Diagram Alir Implementasi Firewall Filtering Rules dan Firewall Raw



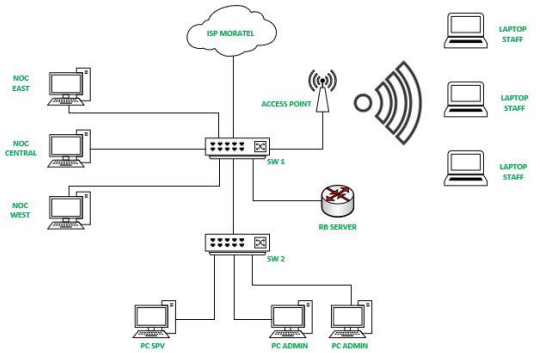
Gambar 3.5 Diagram Alir Implementasi Firewall Filtering Rules dan Firewall Raw Setelah Berhasil Dilakukan

a. Perencanaan Penelitian

Tahapan ini merupakan tahap pertama yang dilakukan dalam kegiatan mengidentifikasi masalah di PT. Cendikia Global Solusi pada ruangan NOC & IT. Untuk hasil dari tahapan perencanaan penelitian ini didapatkan bahwa perangkat Router MikroTik di ruangan NOC & IT PT. Cendikia Global Solusi hanya memiliki fitur dan konfigurasi firewall NAT untuk berinternet, sehingga diperlukan fitur keamanan jaringan dari firewall secara maksimal.

b. Pengumpuan Data

Tahapan ini merupakan tahap yang masih berkaitan dengan tahap perencanaan penelitian dimana dilakukan dari kegiatan observasi. Kegiatan ini dilaksanakan dan diimplementasikan langsung di PT. Cendikia Global Solusi dalam ruangan kerja NOC & IT dengan menggunakan topologi atau arsitektur jaringan yang diusulkan sebagai berikut:



Gambar 3.6 Usulan Topologi Jaringan Penelitian

c. Persiapan Penelitian

Tahapan ini dilakukan pada saat malam hari dimana pekerjaan para karyawan di hari tersebut tidak terlalu padat sehingga dapat memulai pengerjaan strategi keamanan jaringan dalam blok situs web dan pencegahan serangan DDoS yaitu membuat konfigurasi firewall filtering dan firewall raw, dimana digunakan beberapa perangkat hardware dan software yang sudah terdapat di topologi jaringan ruangan NOC & IT.

C. Implementasi Penelitian

Tahapan ini adalah tahap pelaksanaan konfigurasi keamanan jaringan yaitu pemblokiran situs web ilegal dan pencegahan serangan DDoS pada RouterBoard server melalui remote jaringan yang sama dan telah diberikan hak akses di salah satu PC Admin.

1. Konfigurasi Dasar RouterBoard Server MikroTik

Dalam RouterBoard server di ruangan NOC & IT terdapat konfigurasi dasar yang ini terdiri dari address list, VLAN, DHCP server, DNS, route list dan firewall NAT. Dengan adanya konfigurasi ini, setiap perangkat kerja (PC dan Laptop) para karyawan NOC & IT saling terkoneksi dan terhubung ke jaringan internet.

2. Konfigurasi Dasar Switch

Pelaksanaan ini dilakukan sebagai memberikan banyak koneksivitas dan segmen ke beberapa user dan perangkat jaringan lainnya, dimana hanya terdapat konfigurasi VLAN didalamnya.

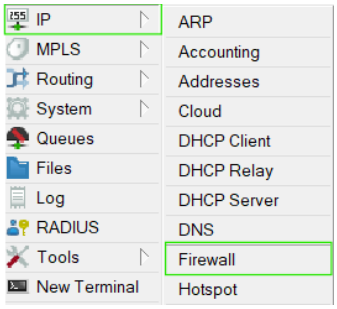
3. Konfigurasi Dasar Access Point

Pelaksanaan ini dilakukan sebagai memberikan koneksi wireless dan menghasilkan sinyal Wi-Fi kepada perangkat perangkat-perangkat kerja karyawan NOC & IT. Untuk konfigurasinya adalah pada bagian LAN yang telah diterapkan di alamat IP VLAN 10 pada RouterBoard server.

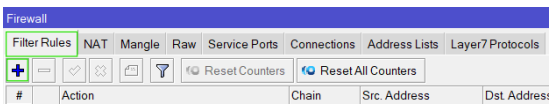
4. Konfigurasi Firewall Filter Rules

Pada konfigurasi ini adalah membuat pemblokiran beberapa situs web ilegal dan tidak layak bertipe nama domain website yang diisikan di bagian content dengan menggunakan metode drop, yaitu menolak atau membatasi trafik paket data situs web tersebut yang keluar masuk melalui RouterBoard server. Untuk konfigurasinya yang perlu dilakukan adalah sebagai berikut:

- Masuk ke Winbox RouterBoard server, lalu pilih menu IP > Firewall > Filter Rules. Langkah ini bertujuan memunculkan tampilan awal firewall perangkat RouterBoard server. Kemudian, untuk menambahkan sebuah konfigurasi pilih simbol tambah (+) di bagian bawah tulisan filter rules pada gambar berikut:

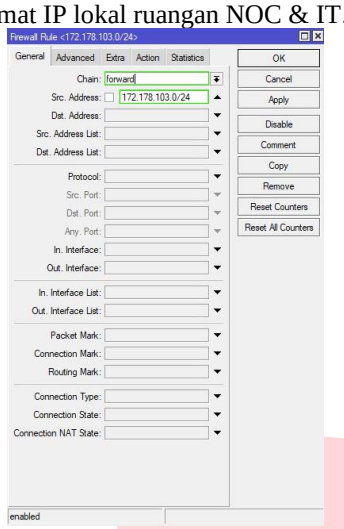


Gambar 3.7 Tahapan Filter Rules: IP > Firewall



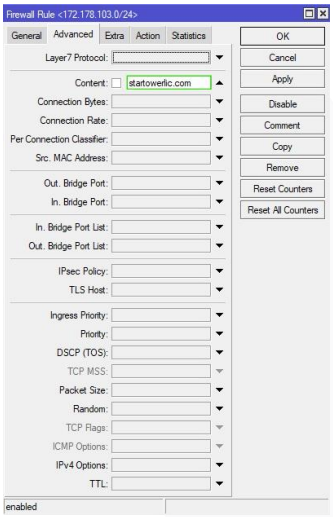
Gambar 3.8 Tahapan Filter Rules: Memilih +

- Pada General, pilih Chain: forward dan Src. Address adalah alamat IP lokal ruangan NOC & IT.



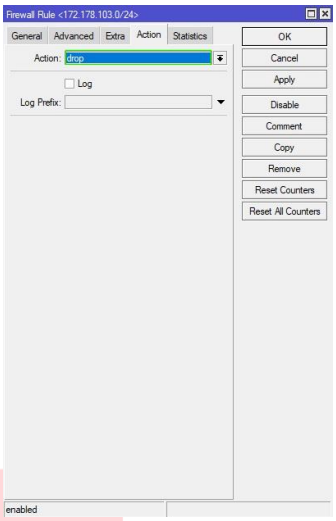
Gambar 3.9 Tahapan Filter Rules: Input Chain dan Src. Address

- Di Advanced bagian Content, isikan target situs web yang bersifat tidak layak dan berbahaya sehingga pada pengisaian ini akan diarahkan untuk pemblokiran.

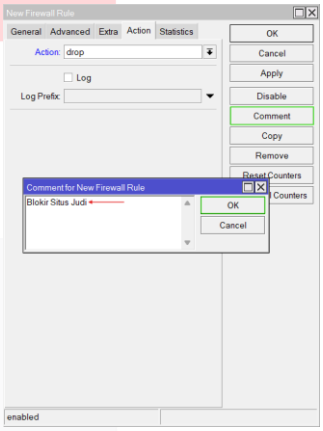


Gambar 3.10 Tahapan Filter Rules: Input Content

- Lalu di Action, pilih drop untuk menolak atau membatasi paket data dari situs web yang tidak layak dan berbahaya tersebut keluar masuk pada RouterBoard server ke arah jaringan lokal ruangan NOC & IT. Serta, berikan Comment untuk membuat label nama konfigurasi dari blok situs tersebut.



Gambar 3.11 Tahapan Filter Rules: Input Action (Drop)



Gambar 3.12 Tahapan Filter Rules: Input Comment

Dari tahapan di atas merupakan konfigurasi pada RouterBoard server secara grafis atau disebut sebagai GUI (Graphical User Interface). Berikut terdapat juga cara konfigurasi pada RouterBoard server secara sistem perintah atau disebut dengan CLI (Command Line Interface):

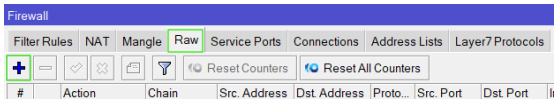
```
[Admin@Router-Noc-Lt-1] > ip firewall filter add chain=forward src-address=172.178.103.0/24 content=startowerlic.com action=drop
```

5. Konfigurasi Firewall Raw untuk Pencegahan Serangan DDoS

Di konfigurasi ini dilakukan menjadi 2 pembuatan firewall raw, pertama adalah konfigurasi firewall sebagai pembatasan trafik paket data yang diizinkan untuk masuk, lalu kedua adalah konfigurasi firewall untuk untuk menghentikan trafik paket data yang sudah dideteksi sebagai serangan DDoS bertipe TCP syn attack.

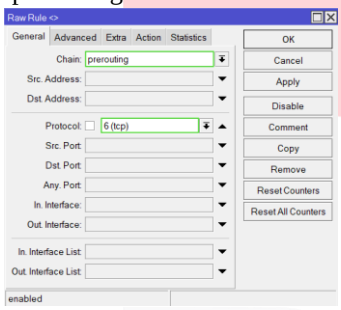
a. Konfigurasi Firewall Raw Pertama

- Dimulai dari Winbox di tampilan firewall filter rules sebelumnya, menuju ke pilihan Raw dan untuk menambahkan sebuah konfigurasi pilih simbol tambah (+) di bagian bawah tulisan filter rules pada gambar berikut:



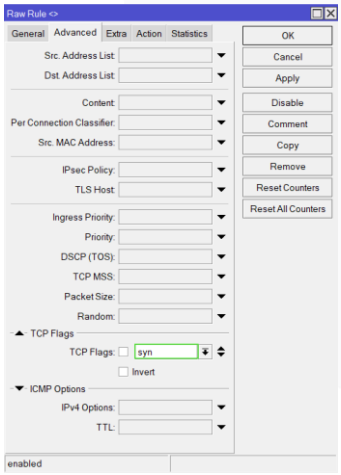
Gambar 3.13 Tahapan Firewall Raw: Penambahan Konfigurasi Raw Pertama

- Pada General, pilih Chain: prerouting dan Protocol: 6 (tcp). Artinya saat trafik TCP yang melewati dan masuk ke dalam RouterBoard server bisa ditangkap oleh chain prerouting.



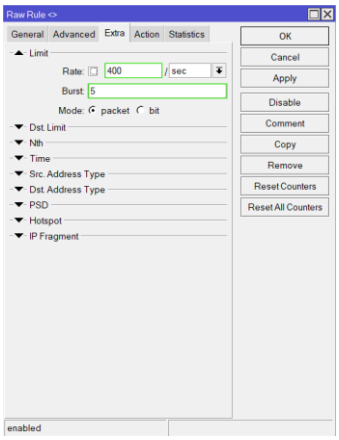
Gambar 3.14 Tahapan Firewall Raw: Input Chain dan Protocol

- Berikutnya di Advanced, pilih TCP Flags: syn sehingga pengelolaan koneksi dan arus lalu lintas digunakan untuk menyinkronkan koneksi TCP.



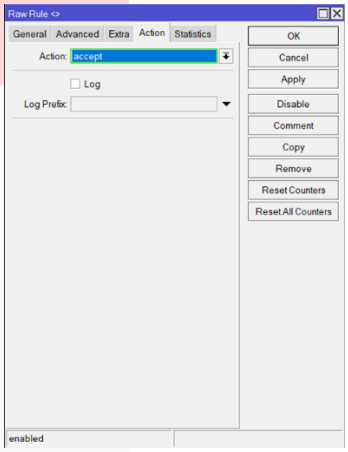
Gambar 3.15 Tahapan Firewall Raw: Input TCP Flags

- Lalu di Extra, isikan Rate 400/sec dengan Burst 5 (default), artinya paket data yang masuk sudah diatur hanya sampai 400 dengan ditambahkan 5 sebagai range yang diterima atau ditampung dari 400 paket data tersebut.



Gambar 3.16 Tahapan Firewall Raw: Input Rate dan Burst

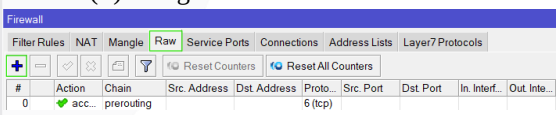
- Terakhir di Action, pilih accept agar perbatasan paket datanya dapat diizinkan masuk.



Gambar 3.17 Tahapan Firewall Raw: Input Action (Accept)

b. Konfigurasi Pencegahan Serangan DDoS

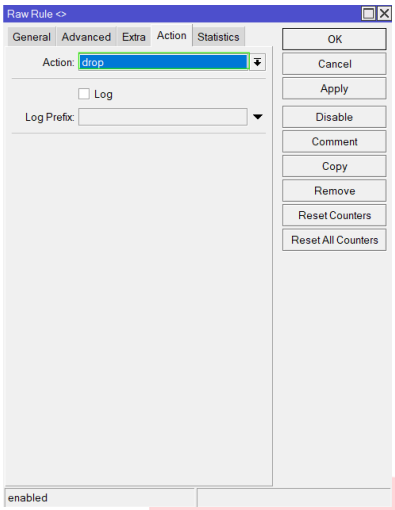
- Pada Raw di tampilan Firewall, lanjut untuk menambahkan konfigurasi baru dengan klik simbol tambah (+) dari gambar berikut:



Gambar 3.18 Tahapan Firewall Raw: Penambahan Konfigurasi Raw Kedua

- Sama seperti tahapan konfigurasi pertama yaitu pembatasan paket data. Di bagian General, pilih Chain: prerouting dan Protocol: 6 (tcp). Serta di Advanced, pilih TCP Flags: syn.

- Terakhir di bagian Action, pilih drop dimana saat paket data yang masuk sudah melebihi sebanyak 400 dan range 5 akan ditahan atau ditolak, dikarenakan paket data yang melebihi tersebut sudah dideteksi menjadi serangan DDoS.



Gambar 3.19 Tahapan Firewall Raw: Input Action (Drop)

Dari tahapan di atas merupakan konfigurasi pada RouterBoard server secara grafis atau disebut sebagai GUI (Graphical User Interface). Berikut terdapat juga cara konfigurasi pada RouterBoard server secara sistem perintah atau disebut dengan CLI (Command Line Interface):

```
[Admin@Router-Noc-Lt-1] > ip firewall raw add chain=prerouting protocol=tcp tcp-flags=syn limit=400.5:packet action=accept

[Admin@Router-Noc-Lt-1] > ip firewall raw add chain=prerouting protocol=tcp tcp-flags=syn action=drop
```

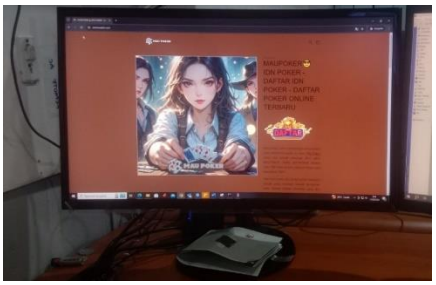
IV. HASIL DAN PEMBAHASAN

A. Percobaan Firewall Filter Rules untuk Blokir Situs

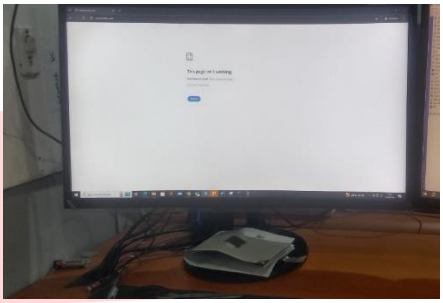
Keberhasilan konfgurasi keamanan jaringan firewall filtering (filter rules) dapat dilihat dari trafik Bytes yang mulai bertambah. Untuk trafik tersebut berasal dari target situs web yang telah dimasukkan konfigurasi firewall filter rules. Nilai trafik situs web yang bertambah menandakan bahwa terdapat pengguna yang akses situs web yang sudah ditargetkan sebagai website ilegal dan tidak layak, sehingga situs web tersebut sudah diatur untuk pemblokiran yang dapat dilihat status action yaitu drop pada gambar di bawah ini:

Gambar 4.1 Tampilan Konfigurasi Firewall Filter Rules

Percobaan hasil keamanan jaringan dalam salah satu blokir situs web ini dilaksanakan mulai dari salah satu perangkat PC NOC menggunakan aplikasi browser. Sebagai berikut perbandingan kondisi sebelum dan setelah diaktifkan fitur firewall filtering (filter rules) pada gambar di bawah ini:

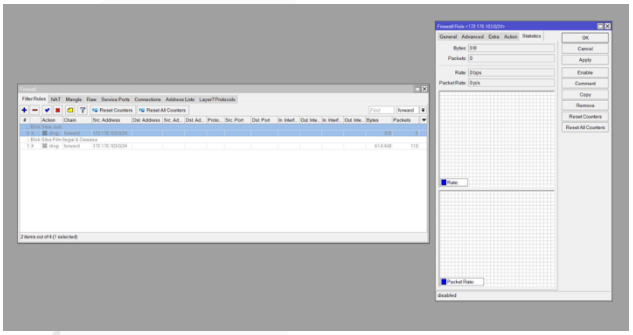


Gambar 4.2 Percobaan Akses Situs Web 1 di PC Admin NOC Sebelum Fitur Firewall Filter Rules Diaktifkan

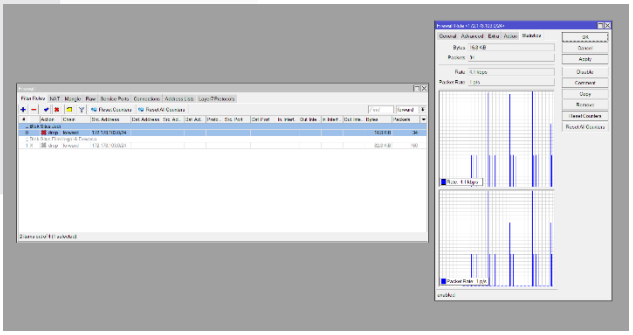


Gambar 4.3 Percobaan Akses Situs Web 1 di PC Admin NOC Setelah Fitur Firewall Filter Rules Diaktifkan

Dari hasil percobaan di atas, didapatkan data pengukuran keberhasilan dari pemblokiran situs web yang dilakukan menggunakan statistics firewall rules MikroTik, sebagai berikut :



Gambar 4.4 Parameter Pengukuran Firewall Filter Rule (Off) Blokir Situs Web



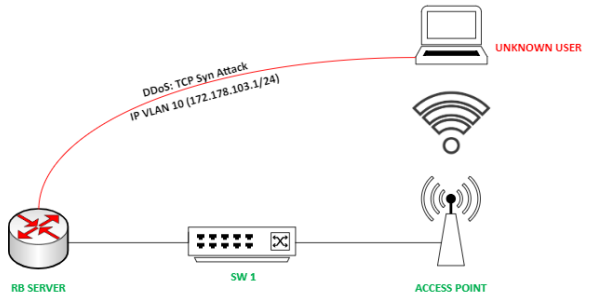
Gambar 4.5 Parameter Pengukuran Firewall Filter Rule (On) Blokir Situs Web

Tabel 4.1 Hasil Pengukuran Lalu Lintas Jaringan Terhadap Pemblokiran Situs Web

No	Status Firewall Filtering (Filter Rules)	Waktu (second/s)	Bytes	Packets	Rate (bps)	Packet Rate (p/s)
1	Mati	0s - 30s	0B	0	0 bps	0 p/s
2	Hidup	5s	5.9 KiB	12	4.0 kbps	1 p/s
		15s	9.9 KiB	20	4.1 kbps	1 p/s
		30s	16.8 KiB	34	4.1 kbps	1 p/s

B. Percobaan Firewall Raw untuk Pencegahan Serangan DDoS

Agar bisa melihat keberhasilan hasil konfigurasi keamanan jaringan dalam pencegahan serangan DDoS, dilakukan simulasi penyerangan dengan aplikasi HyenaeFE dengan cara pada sebuah perangkat Laptop tidak dikenal masuk ke jaringan lokal (172.178.103.1) perangkat RouterBoard server NOC & IT. Sebagai berikut untuk ilustrasi penyerangan DDoS pada gambar di bawah ini:



Gambar 4.6 Skenario Penyerangan DDoS (TCP Syn Attack)

Simulasi ini diawali dari pengecekan kondisi pertama CPU terlebih dahulu pada perangkat RouterBoard server NOC & IT dimana terdapat 4 CPU dimiliki oleh RouterBoard tersebut, untuk melihat pengecekan CPU sendiri bisa melalui Resources dan Profile di Winbox. Lalu jalankan arus lalu lintas paket data jaringan lokal (VLAN 10) menggunakan Torch supaya selain memunculkan proses arus lalu lintas juga dapat memunculkan kinerja CPU.

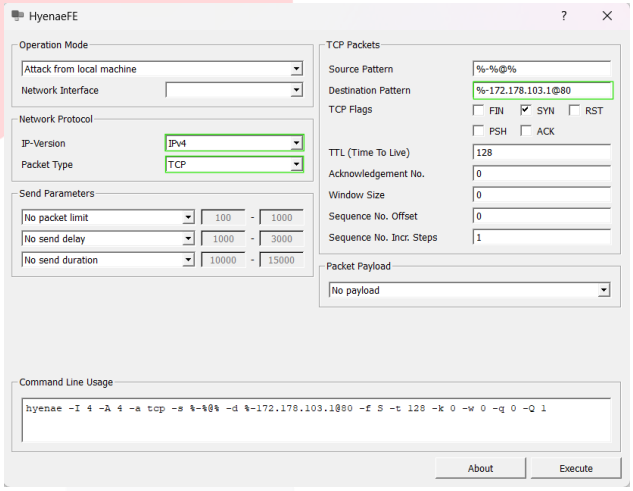
Gambar 4.7 Tampilan Winbox: Kondisi Normal CPU RouterBoard MikroTik

Sebagai berikut data hasil pengukuran kondisi normal Router MikroTik yang dilakukan selama 1 menit pada table 4.2 di bawah ini :

Tabel 4.2 Hasil Pengukuran CPU & Resource Kondisi Normal RouterBoard NOC & IT

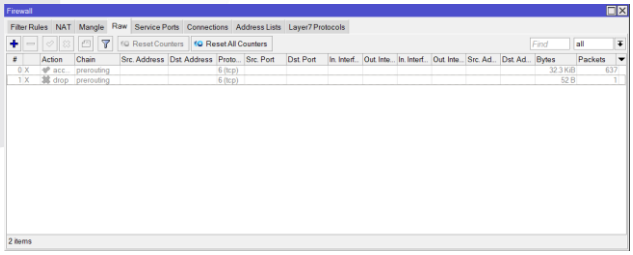
No	Waktu (second/s)	Persentase CPU (%)	Usage CPU0	Usage CPU1	Usage CPU2	Usage CPU3	Resources Firewall Connection (Items)
1	3s	0%	0.5	0.5	1.0	0.5	13 items
2	5s	0%	1.0	1.0	0.0	0.5	14 items
3	10s	1%	0.5	1.0	0.0	1.0	16 items
4	15s	0%	1.0	0.5	1.0	1.0	14 items
5	30s	1%	0.5	0.5	0.5	4.0	14 items
6	60s	0%	1.0	0.5	0.0	0.5	13 items

Kemudian, penyerang memasukkan alamat IP lokal RouterBoard server NOC & IT yaitu 172.178.103.1 ke aplikasi HyenaeFE untuk melakukan serangan DDoS jenis TCP syn attack. Dilakukan pengisian pada bagian packet type adalah TCP dan destination pattern adalah %-172.178.103.1@80, setelah itu pilih Execute untuk memulai serangan DDoS menuju perangkat RouterBoard server NOC & IT.

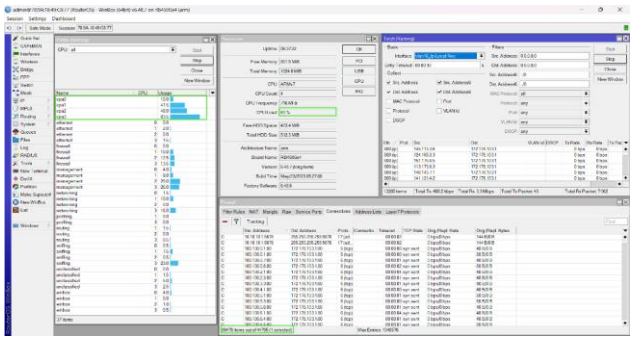


Gambar 4.8 Penyerangan Menggunakan Software HyenaeFE

Agar hasil simulasi penyerangan DDoS berhasil dilakukan, dimatikan fitur keamanan jaringan firewall raw terlebih dahulu sehingga terlihat perubahan pada persentase kinerja dan penggunaan CPU serta arus lalu lintas paket data jaringan di firewall connection.



Gambar 4.9 Konfigurasi Firewall Raw Saat Dimatikan



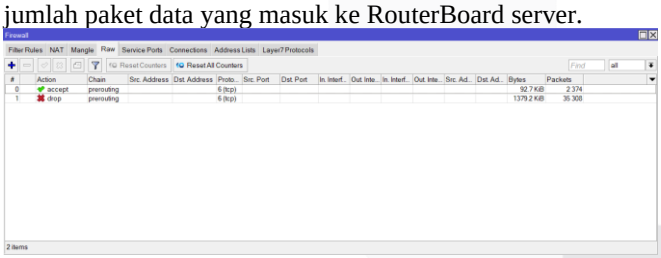
Gambar 4.10 Tampilan Winbox: Kondisi CPU RouterBoard MikroTik Terkena Serangan DDoS

Berikut hasil pengukuran kondisi Router MikroTik saat mematikan firewall raw dan menjalankan serangan DDoS pada tabel 4.2 di bawah ini :

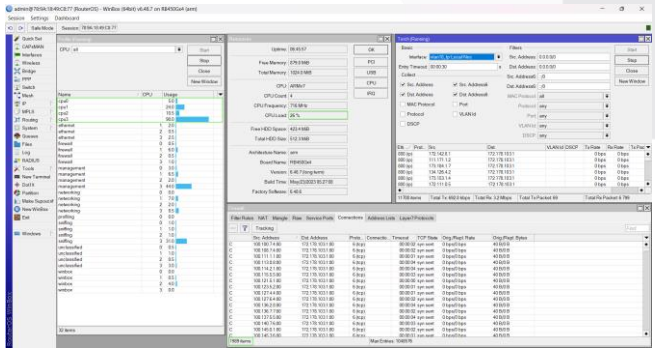
Tabel 4.3 Hasil Pengukuran CPU & Resource RouterBoard NOC & IT Terserang DDoS

No	Waktu (second/s)	Persentase CPU (%)	Usage CPU0	Usage CPU1	Usage CPU2	Usage CPU3	Resource Firewall Connection (Items)
1	3s	34%	17.5	11.5	14.5	19.5	1041 items
2	5s	55%	16.0	32.5	76.0	34.0	2578 items
3	10s	46%	22.0	58.0	82.5	40.0	11654 items
4	15s	58%	27.0	66.5	21.5	76.0	19527 items
5	30s	61%	18.5	81.0	94.0	31.0	39707 items
6	60s	61%	10.0	41.5	48.0	83.5	89478 items

Sehingga dilakukan pencegahan dari serangan DDoS tipe syn attack dengan mengaktifkan Kembali fitur fitur keamanan jaringan firewall raw dan dapat dilihat perubahan kembali pada persentase kinerja CPU di resource, penggunaan keempat CPU di profile yang mulai menurun, serta pada firewall connection telah diatur dan disaring jumlah paket data yang masuk ke RouterBoard server.



Gambar 4.11 Konfigurasi Firewall Raw Saat Diaktifkan



Gambar 4.12 Tampilan Winbox Kondisi CPU RouterBoard MikroTik Setelah Konfigurasi Firewall diaktifkan

Berikut hasil pengukuran kondisi Router MikroTik saat mengaktifkan firewall raw dalam rentang hitungan detik pada tabel di bawah ini :

Tabel 4.4 Hasil Pengukuran CPU & Resource RouterBoard NOC & IT Menggunakan Firewall Raw

No	Waktu (second/s)	Persentase CPU (%)	Usage CPU0	Usage CPU1	Usage CPU2	Usage CPU3	Resource Firewall Connection (Items)
1	3s	28%	13.0	91.5	4.0	15.5	2426 items
2	5s	29%	12.5	19.5	15.0	91.0	2414 items
3	10s	28%	2.5	16.0	13.5	90.5	2000 items
4	15s	28%	3.0	91.0	4.5	26.0	2042 items
5	30s	29%	23.5	13.5	15.0	91.5	2422 items
6	60s	26%	5.0	24.0	10.5	90.0	1989 items

V. KESIMPULAN

Berdasarkan hasil penelitan dari strategi keamanan jaringan dan pencegahan serangan DDoS dapat disimpulkan bahwa keamanan jaringan untuk pemblokiran situs illegal dan tidak layak menggunakan fitur firewall filtering (filter rules) berhasil diterapkan dan bekerja dengan baik, antara kondisi firewall filter rule dimatikan dan dihidupkan. Ketika fitur firewall filter rule dimatikan, tidak ada data-data yang dikirim atau diterima, yaitu 0 bytes, 0 packets, 0 bps dan 0 p/s, sedangkan setelah fitur firewall filter rule dihidupkan terdapat data-data yang keluar secara meningkat. Sehingga, antara hasil pengukuran pemblokiran situs web pertama dan kedua memiliki keluaran data yang berbeda dimana hasil pengukuran data yang ditransfer, jumlah paket, laju transmisi data dan laju paket pada blokir situs web kedua lebih tinggi daripada situs web pertama. Dapat dianalisa pengukuran situs web pertama sampai 30 detik dihasilkan data yang ditransfer 16.8 KiB, jumlah paket 34, laju transmisi data 4.1 kbps dan laju paket 1 p/s. Sementara, pengukuran situs web kedua sampai 30 detik dihasilkan data yang ditransfer 78.3 KiB, jumlah paket 151, laju transmisi data 4.1 kbps dan laju paket 1 p/s.

Serta keamanan jaringan untuk pencegahan serangan DDoS menggunakan fitur firewall raw berhasil diterapkan dan bekerja dengan baik, dalam mengurangi beban dan kinerja CPU RouterBoard server NOC & IT dan mengontrol jumlah trafik paket data selama serangan DDoS. Berdasarkan angka-angka empiris menunjukan penurunan persentase CPU dari 34% hingga 61% saat diserang DDoS menjadi 26% hingga 29% setelah digunakan firewall raw, serta jumlah pembanjiran request alamat IP tidak dikenal yang hampir 90000 koneksi saat diserang DDoS berhasil diatur menjadi kisaran 1989-2426 koneksi dalam trafik lalu lintas yang berjalan di RouterBoard server NOC & IT.

REFERENSI

[1] I. Istikomah and I. Khoiril Mala, “Dampak Internet terhadap Pola Interaksi Masyarakat di Desa Tawangharjo,” Bisnis dan Digital (JIMaKeBiDi), vol. 1, no. 2, 2024, [Online]. Available: http://www.ut.ac.id

[2] M. Ngabdur Rokhman, E. Fariza Rizaldy, N. Abdullah, and N. Feby Puspitasari, “IMPLEMENTASI FIREWALL FILTER RULE DAN RAW SEBAGAI METODE PENGAMANAN JARINGAN PADA PERPUSTAKAAN XYZ,” vol. 11, pp. 58–75, 2023.

[3] E. Purwanto, “IMPLEMENTASI JARINGAN HOTSPOT DENGAN MENGGUNAKAN ROUTER MIKROTIK SEBAGAI PENUNJANG PEMBELAJARAN,” vol. 1, pp. 20–27, 2015.

[4] R. Dewantara, P. A. Cakranegara, A. J. Wahidin, A. Muditomo, I. Gede, and I. Sudipa, “Implementasi Metode Preference Selection Index Dalam Penentuan Jaringan Dan Pemanfaatan Internet Pada Provinsi Indonesia,” 2022.
[5] S. Wongkar, A. Sinsuw, and X. Najoan, “Analisa Implementasi Jaringan Internet Dengan Menggabungkan Jaringan LAN Dan WLAN Di Desa Kawangkoan Bawah Wilayah Amurang II,” vol. 4, pp. 62–68, 2015.
[6] Jagad ID, “Personal Area Network : Pengertian, Karakteristik, Manfaat, Contoh, Kelebihan dan Kekurangan.” Accessed: Jul. 24, 2024. [Online]. Available: https://jagad.id/wp-content/uploads/2020/04/Definisi-Personal-Area-Network-Adalah-Arti-Pengertian-Karakteristik-Manfaat-Contoh-Kelebihan-dan-Kekurangan-1024x785.png.webp
[7] Putra, “Pengertian Lengkap LAN, MAN, WAN dan Contohnya,” 2020. Accessed: Jul. 24, 2024. [Online]. Available: https://salamadian.com/pengertian-lan-man-wan/
[8] Niko, “5 Hal Dasar dari Jaringan Komputer (Networking) yang Penting Untuk Diketahui,” 2014. Accessed: Jul. 24, 2024. [Online]. Available: https://pintarkomputer.com/wp-content/uploads/2014/06/5-Hal-Dasar-dari-Jaringan-Komputer-Networking-yang-Penting-Untuk-Diketahui-1-1024x683.jpg
[9] content diengcyber, “JARINGAN NIRKABEL : Pengertian, Jenis, Fungsi, dan manfaatnya,” 2022. Accessed: Jul. 24, 2024. [Online]. Available: https://i0.wp.com/diengcyber.com/wp-content/uploads/2022/04/1649388451221.jpg?w=784&ssl=1
[10] I. Rochmawati, “ANALISIS USER INTERFACE SITUS WEB IWEARUP.COM,” 2019. [Online]. Available: www.iwearup.com
[11] Z. Munawar, M. Kom, and N. I. Putri, “KEAMANAN JARINGAN KOMPUTER PADA ERA BIG DATA,” 2020.
[12] A. Suhaemin and M. U. Prodi Hukum Pidana Islam Bunga Bangsa Cirebon Dosen Prodi Hukum Pidana Islam UI Bunga Bangsa Cirebon, “KARAKTERISTIK CYBERCRIME DI INDONESIA,” 2023.
[13] Y. M. Saragih, A. Putera, and U. Siahaan, “Cyber Crime Prevention Strategy in Indonesia,” 2016. [Online]. Available: www.internationaljournalssrg.org
[14] N. Mamuriyah, S. E. Prasetyo, and A. O. Sijabat, “Rancangan Sistem Keamanan Jaringan dari serangan DDoS Menggunakan Metode Pengujian Penetrasi,” Jurnal Teknologi Dan Sistem Informasi Bisnis, vol. 6, no. 1, pp. 162–167, Jan. 2024, doi: 10.47233/jteksis.v6i1.1124.
[15] D. B. Satmoko, P. Sukarno, and E. M. Jadied, “Peningkatan Akurasi Pendeteksian Serangan DDoS Menggunakan Multiclassifier Ensemble Learning dan Chi-Square,” 2018.
[16] J. T. Akhir and Z. A. Pribadi, “Analisis dan Implementasi Firewall dengan Metode Stateful Multilayer Inspection Pada Mikrotik Router OS.”
[17] Admin Aptika, “Keamanan Jaringan Internet dan Firewall,” 2017. Accessed: Jul. 24, 2024. [Online]. Available: https://aptika.kominfo.go.id/wp-content/uploads/2018/10/Firewall-1.png
[18] “MikroTik Logo, symbol, meaning, history, PNG, brand,” 2023. Accessed: Jul. 24, 2024. [Online]. Available: https://logos-world.net/wp-content/uploads/2023/02/MikroTik-Logo-500x281.png
[19] F. Ulum, “DESAIN KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS MENGGUNAKAN METODE PORT KNOCKING,” 2018.
[20] “Mikrotik RouterBoard RB450G RouterOS LV5, 1 Serial Port, Switch Gigabit 5 port.” Accessed: Jul. 24, 2024. [Online]. Available: https://sysnetcenter.com/1264-large_default/MikroTik-RouterBoard-450g-680mhz-serial-port-switch-gigabit-case-power-supply.jpg
[21] Gi. Mardiana, “Sistem Pemesanan Menu Berbasis Web memanfaatkan Mikrotik API,” p. 19, 2015.
[22] A. I. Haris, B. Riyanto, F. Surachman, and A. A. Ramadhan, “Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi,” Komputika : Jurnal Sistem Komputer, vol. 11, no. 1, pp. 67–76, Jan. 2022, doi: 10.34010/komputika.v11i1.5227.
[23] L. Mashur Gultom, T. Informatika Politeknik Negeri Bengkalis JLBathin Alam, and S. Alam Bengkalis-Riau, “Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw,” 2021.