IMPLEMENTASI FIREWALL FILTER RULE DAN RAW SEBAGAI METODE PENGAMANAN JARINGAN PADA PERPUSTAKAAN XYZ

Makruf Ngabdur Rokhman[1]
[1]Prodi Teknik Informatika, Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta
makruf_rokhman@students.amikom.ac.id[1]

Eka Fariza Rizaldy [2]
[2]Prodi Teknik Informatika, Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta
ekafarizar@students.amikom.ac.id[2]

Nasywa Abdullah[3]
[3]Prodi Teknik Informatika, Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta
Nasywaabdullah113@students.amikom.ac.id[3]

Nila Feby Puspitasari[4]
[4]Prodi Teknik Informatika, Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta
nilafeby@amikom.ac.id[4]

ABSTRAK

Perpustakaan XYZ merupakan salah satu tempat belajar siswa yang ramai pengunjungnya, disana tersedia layanan jaringan internet yang dapat dimanfaatkan untuk kegiatan belajar. Jaringan internet yang tersedia pada perpustakaan belum menerapkan monitoring jaringan dan keamanan jaringan, sehingga jaringan internet masih rentan terhadap serangan siber salah satunya adalah Distributed Denial of Service syn attack (DDoS). Penelitian ini bertujuan untuk meningkatkan keamanan dan pengawasan akses internet di lingkungan perpustakaan XYZ dan menciptakan lingkungan belajar yang bebas dari konten yang tidak layak menggunakan firewall filter rule dan mengatasi serangan Distributed Denial of Service syn attack (DDoS) menggunakan firewall raw, serta monitoring jaringan dengan the dude. Untuk mencapai tujuan tersebut diperlukan manajemen jaringan dengan menggunakan perangkat mikrotik routerboard. Pada mikrotik sudah tersedia fitur Firewall (Filter rules, Raw, dan Address list). Dengan menggunakan router mikrotik, monitoring jaringan dapat dilakukan dengan memanfaatkan perangkat lunak The Dude. Hasil dari penelitian ini adalah dapat memberikan gambaran efektivitas monitoring jaringan, membatasi akses ke situs yang tidak layak (web filtering), dan keamanan perangkat jaringan dari serangan Distributed Denial of Service syn attack (DDoS). Di sisi lain, Perpustakaan XYZ akan memiliki akses internet yang melindungi penggunanya dari situs atau web yang berisi konten yang tidak layak. Perangkat router manajemen di perpustakaan XYZ terlindungi dari serangan Distributed Denial of Service syn attack (DDoS). Serta Perpustakaan XYZ akan memiliki perangkat yang digunakan untuk memantau lalu lintas data atau kondisi perangkat jaringan.

Kata kunci: Internet, Mikrotik, DDoS, Monitoring, Filter access

ABSTRACT

XYZ Library is one of the student learning places that is crowded with visitors, there are internet network services that can be utilized for learning activities. The internet network available in the library has not implemented network monitoring and network security, so that the internet network is still vulnerable to cyber attacks, one of which is Distributed Denial of Service syn attack (DDoS). This research aims to improve security and monitoring of internet access in the XYZ library environment and create a learning environment that is free from inappropriate content using firewall filter rules and overcoming Distributed Denial of Service syn attack (DDoS) attacks using raw firewalls, as well as network monitoring with the dude. To achieve these goals, network

management is needed using a Mikrotik routerboard device. Mikrotik already has Firewall features (Filter rules, Raw, and Address list). By using a proxy router, network monitoring can be done by utilizing The Dude software. The results of this research can provide an overview of the effectiveness of network monitoring, limiting access to inappropriate sites (web filtering), and the security of network devices from Distributed Denial of Service syn attacks (DDoS). On the other hand, XYZ Library will have internet access that protects its users from sites or webs that contain inappropriate content. The management router device in XYZ library is protected from Distributed Denial of Service syn attack (DDoS). And XYZ Library will have a device used to monitor data traffic or network device conditions.

***Keywords**: Internet, Mikrotik, DDoS, Monitoring, Filter access*

1. PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan merupakan aspek yang sangat penting dalam dunia teknologi informasi saat ini khususnya internet. Perangkat jaringan internet tidak luput dari berbagai jenis ancaman dan serangan. Salah satu cara yang umum digunakan untuk mengamankan adalah dengan menggunakan firewall. Firewall adalah sebuah perangkat atau perangkat lunak yang digunakan untuk mengontrol lalu lintas data yang masuk dan keluar dari jaringan. Oleh karena itu, jaringan internet akan lebih terkontrol dan aman.

Perpustakaan XYZ berfungsi sebagai tempat dimana siswa dan staf sekolah dapat mengakses berbagai jenis bahan bacaan dan sumber daya informasi, tidak terbatas pada buku cetak, tetapi juga mencakup media elektronik, seperti penggunaan internet, e-book, dan sumber daya digital lainnya.

Saat ini, Perpustakaan XYZ belum tersedia perangkat yang digunakan untuk mengatur arus lalu lintas data, sehingga keamanan jaringan dalam bentuk filter access ke situs yang yang berisi konten yang tidak layak belum bisa diterapkan, begitu juga keamanan dari serangan Distributed Denial of Service (DDoS), ataupun monitoring jaringan untuk memantau kondisi jaringan dan perangkat jaringan yang tersedia pada perpustakaan.

Berdasarkan pada paragraf sebelumnya, dapat dilakukan pemasangan router manajemen pada perpustakaan XYZ sehingga filter access ke situs yang yang berisi konten tidak layak dapat diterapkan. Mencegah dari serangan Distributed Denial of Service (DDoS) di sisi router juga dapat diterapkan, dan seluruh perangkat jaringan di perpustakaan yang terhubung ke router manajemen dapat dipantau kondisinya melalui sistem monitoring jaringan

Oleh karena itu, Peneliti tertarik untuk melakukan penelitian dengan judul "Implementasi Firewall Filter Rule dan Raw sebagai Metode Pengamanan Jaringan pada Perpustakaan XYZ dengan melakukan pemasangan router mikrotik sebagai router manajemen untuk mengontrol lalu lintas data di perpustakaan XYZ. Penggunaan router mikrotik dikarenakan firewall filter rule dan raw sudah tersedia pada perangkat tersebut. Dengan adanya router manajemen diharapkan dapat meningkatkan keamanan dan pengawasan akses internet di lingkungan perpustakaan, sehingga menciptakan lingkungan belajar yang baik dan bebas dari konten yang tidak layak.

1.2 Rumusan Masalah

Rumusan masalah pada penelitian ini adalah:

1. Metode apa yang digunakan untuk memfilter access ke situs yang bermuatan tidak layak?

2. Metode apa yang digunakan untuk mencegah serangan Distributed Denial of Service (DDoS) pada router?
3. Apa perangkat yang digunakan untuk monitoring jaringan di perpustakaan XYZ?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah:

1. Melakukan pembatasan akses ke situs atau web yang berisi konten tidak layak menggunakan firewall filter rule.
2. Melakukan pencegahan serangan Distributed Denial of Service (DDoS) syn attack pada router menggunakan firewall raw.
3. Monitoring jaringan menggunakan The Dude (Direct Unidentified Death Event).

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah:

1. Meningkatkan keamanan dan pengawasan akses internet di lingkungan perpustakaan XYZ.
2. Menciptakan lingkungan belajar yang bebas dari konten tidak layak.

1.5 Tinjauan Pustaka

Dalam penelitian ini peneliti memaparkan enam penelitian terdahulu yang relevan dengan permasalahan yang akan diteliti yaitu tentang "Implementasi Firewall Filter Rule dan Raw sebagai Metode Pengamanan Jaringan pada Perpustakaan XYZ".

Pada penelitian yang dilakukan oleh (Alfidzar & Parga Zen, 2022). Penelitian ini membahas tentang server yang mengalami serangan DoS yang menyebabkan kerusakan pada sistem operasi. Sehingga diperlukan suatu penanganan yang dapat menganalisis serangan terhadap beberapa ancaman. Penelitian ini menggunakan HoneyPy dengan Maltrail yang digunakan untuk metode pembuktian. Hasil penelitian ini yaitu HoneyPy dengan Maltrail mampu menjadi tolak ukur untuk digunakan sebagai peningkatan keamanan pada serangan di bagian server.

Pada penelitian yang dilakukan oleh (Faisal Qomarudin & Amrullah, 2022). Penelitian ini membahas mengenai sistem monitoring jaringan untuk melakukan pengecekan pada jaringan di suatu perusahaan agar administrator dapat mengetahui kondisi jaringan dengan menggunakan protokol Internet Control Message Protocol. Hasil dari penelitian ini adalah sebuah sistem monitoring jaringan yang menampilkan status jaringan dan memantau jaringan dengan notifikasi telegram, log jaringan untuk mempermudah troubleshooting, manajemen Internet Protocol dan pengaturan sistem backdoor dengan nama SIMONIT.

Pada penelitian yang dilakukan oleh (Rahman, 2023). Penelitian ini membahas mengenai keamanan jaringan dengan menerapkan Pi-Hole DNS Server untuk memfilter website negatif dan iklan yang tidak diinginkan sesuai dengan program yang dicanangkan oleh Pemerintah (Kemkominfo) yaitu penggunaan internet yang sehat dan aman. Hasil penelitian ini adalah penerapan Pi-Hole DNS Server terhadap topologi jaringan RT/RW Net terbukti dapat memfilter atau menyaring website yang mengandung situs-situs negatif dan dapat memblokir iklan yang tidak diinginkan, keberhasilan dalam memfilter tersebut dikategorikan 100% efektif, serta kualitas jaringan setelah penerapan Pi-Hole DNS Server dikategorikan baik dalam metode pengujian QoS.

Pada penelitian yang dilakukan oleh (Syaripudin & Nugraha, 2023). Pada penelitian ini membahas bahwa Garage Freshmart membutuhkan pembatasan akses ke sosial media untuk memaksimalkan kinerja karyawan pada jam kerja, sehingga karyawan tidak dapat mengakses social media saat bekerja. Hasil dari penelitian ini adalah blok website menggunakan layer 7 protocol pada

mikrotik dapat menjadikan salah satu alternatif sebagai alat manajemen sistem jaringan yang mampu khususnya memblokir website sosial media. Sehingga pemilik toko dapat memaksimalkan kinerja karyawan dalam bekerja dan dapat meminimalisir kemungkinan karyawan dapat membuka akses sosial media melalui komputer yang tersedia.

Pada penelitian yang dilakukan oleh (Rasyiidin, 2021). Membahas mengenai monitoring berbasis SNMP dengan menggunakan Cacti. SNMP merupakan protokol jaringan yang digunakan untuk monitoring perangkat jaringan terutama server, yang membuat pengirim dan penerima saling bertukaran informasi. Hasil penelitian ini yaitu dengan adanya Cacti seorang administrator jaringan dapat menganalisa penggunaan setiap perangkat dan melihat pengguna siapa saja yang sedang mengakses kedalam perangkat. Administrator jaringan juga mendapatkan hasil analisa yang menyebabkan kondisi server bermasalah, misalnya memori penuh atau server dalam keadaan mati.

Pada penelitian yang dilakukan oleh (Jagad et al., 2020). Penelitian ini membahas tentang keamanan jaringan dengan memanfaatkan mikrotik routerboard dari UDP flood di Dinas Pendidikan Bengkalis. UDP flood merupakan jenis serangan DoS yang dapat berakibat pada lumpuhnya suatu perangkat jaringan. Hasil dari penelitian ini yaitu bahwa mikrotik routerboard bisa mengamankan jaringan dari serangan udp flood menggunakan firewall dengan baik.

2. LANDASAN TEORI

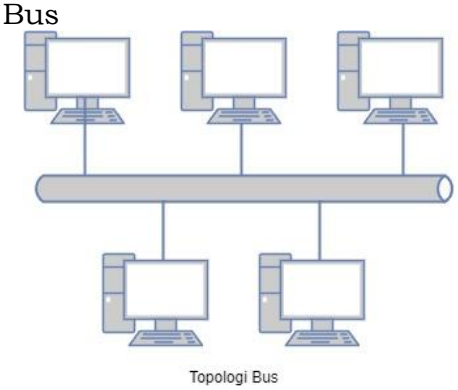
2.1 Pengertian Jaringan Internet. Internet (Inter-Network) merupakan sekumpulan jaringan komputer menghubungkan website/situs akademik, pemerintahan, bisnis, organisasi, dan individu. Internet menyediakan akses ke pelayanan telekomunikasi serta sumber informasi bagi jutaan user di seluruh dunia(Rusito).

Internet adalah interkoneksi jaringan komputer skala besar, yang dihubungkan menggunakan protokol khusus. Jadi sebenarnya internet merupakan bagian dari WAN. Cakupan internet adalah satu dunia bahkan tidak menutup kemungkinan antarplanet. Koneksi antarjaringan komputer dapat dilakukan berkat dukungan dari protokol TCP/IP (Transmission Control Protocol/Internet Protocol) (Sofana, 2015).

2.2 Topologi Jaringan

Topologi jaringan diartikan sebagai layout atau arsitektur jaringan komputer. Topologi berkaitan dengan cara komponen-komponen jaringan (seperti: server, router, switch) saling berkomunikasi melalui media transmisi data. Topologi jaringan terbagi menjadi 5 diantaranya:

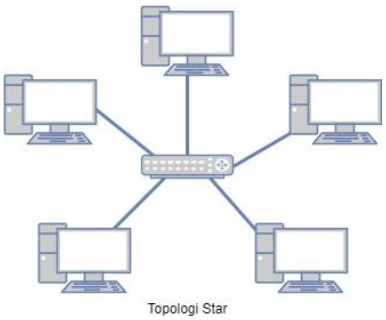
1. Bus



Gambar 2.1 Gambar Topologi Bus
(Sumber: Penulis, 2023)

Topologi bus sering juga disebut daisy chain atau ethernet bus topologies. Jaringan yang menggunakan topologi bus dapat dikenali dari penggunaan sebuah kabel backbone (kabel utama) yang menghubungkan semua peralatan jaringan. Karena kabel backbone menjadi satu-satunya jalan lalu lintas data maka apabila kabel terputus akan menyebabkan jaringan terputus total.

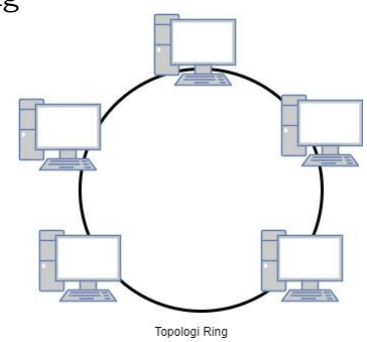
2. Star



Gambar 2.2 Gambar Topologi Star
(Sumber: Penulis, 2023)

Topologi star dikenali dengan keberadaan sebuah sentral berupa hub yang menghubungkan semua node. Setiap node menggunakan sebuah kabel UTP (Unshielded Twisted Pair) atau STP (Shield Twisted Pair) yang dihubungkan dari ethernet ke hub. Karena setiap node terhubung dengan hub, apabila ada kabel atau segmen yang putus tidak akan menyebabkan jaringan lumpuh.

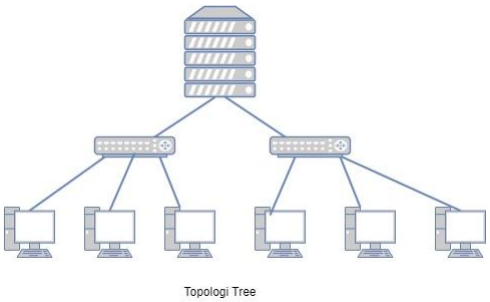
3. Ring



Gambar 2.3 Gambar Topologi Ring
(Sumber: Penulis, 2023)

Topologi ring dapat dikenali dari setiap kabel backbone yang membentuk cincin. Setelah sampai pada komputer terakhir maka ujung kabel akan kembali dihubungkan dengan komputer pertama. Pada topologi ini data mengalir satu arah bisa searah jarum jam atau sebaliknya.

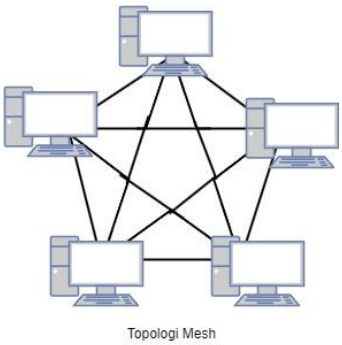
4. Tree



Gambar 2.4 Gambar Topologi Tree
(Sumber: Penulis, 2023)

Topologi tree merupakan gabungan topologi star yang dihubungkan dengan topologi bus. Topologi tree digunakan untuk menghubungkan beberapa LAN dengan LAN lain. Hubungan antar-LAN dilakukan via hub. Setiap hub dapat dianggap sebagai akar (root) dari masing-masing pohon (tree). Topologi tree dapat mengatasi kekurangan topologi bus yang disebabkan persoalan broadcast traffic, dan kekurangan topologi star yang disebabkan oleh keterbatasan port.

5. Mesh



Gambar 2.5 Gambar Topologi Mesh
(Sumber: Penulis, 2023)

Topologi mesh dapat dikenali dengan hubungan point to point ke setiap komputer. Topologi mesh sangat jarang digunakan. Selain rumit juga sangat boros kabel. Apabila jumlah komputer semakin banyak maka instalasi kabel jaringan juga akan semakin rumit (Sofana, 2015).

2.3 Mikrotik Routerboard

Gambar 2.6 Logo Mikrotik
(Sumber: mikrotik.com, 2023)

Routerboard merupakan perangkat keras (hardware) yang dikembangkan oleh perusahaan Mikrotik. Routerboard berukuran sangat kecil dan lebih praktis, kemudian anda juga dapat melakukan proses instalasi RouterOS pada Routerboard yang telah terkonfigurasi dengan baik. Routerboard terdiri dari sebuah processor, ROM, RAM, dan flash memory (Deni Bahtiar,2021).

2.4 Pengertian Jaringan Wireless

Jaringan tanpa kabel (wireless) atau jaringan nirkabel merupakan suatu jalan keluar terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Pada saat ini jaringan nirkabel atau wireless sudah banyak digunakan dengan memanfaatkan jasa satelit dan bahkan mampu memberi kecepatan akses yang lebih cepat bila dibandingkan dengan jaringan yang menggunakan kabel (Yudi mulyanto).

2.5 Monitoring Jaringan

Monitoring jaringan adalah salah satu fungsi dari management yang berguna menganalisa apakah jaringan masih cukup layak untuk digunakan atau perlu tambahan kapasitas. Hasil monitoring juga dapat membantu jika admin ingin mendesain ulang jaringan yang telah ada. Banyak hal dalam jaringan yang bisa dimonitoring, salah satu diantaranya load traffic jaringan yang lewat pada sebuah router atau interface komputer. Monitoring dapat dilakukan dengan standar SNMP, selain load traffic jaringan, kondisi jaringan harus dimonitoring. Misalnya status up dan down dari sebuah perangkat jaringan (Fauzy, 2015).

2.6 The Dude

Gambar 2.7 The Dude
(Sumber:www.drwindows.de/news/wp-content/uploads/2020/06/the-dude_pgb.jpg, 2023)

The Dude adalah aplikasi freeware (perangkat lunak gratis) dari MikroTik yang dapat meningkatkan pengelolaan lingkungan jaringan. Melalui The Dude bisa memantau apakah layanan Web, Telnet atau layanan yang lainnya hidup atau mati. Kemudian juga aplikasi The Dude bisa untuk menyimpan grafik seperti MRTG yang terakumulasi dari waktu ke waktu. Jadi administrator bisa melihat kapan perangkat ini mati atau juga bisa melihat tidak hanya perangkatnya tetapi juga jaringannya. Apabila mememeriksa. administrator tidak perlu membuka satu persatu routernya, tapi di satu halaman yang digunakan untuk memonitor, bisa terlihat berbagai informasi mengenai jaringan. Misalnya bisa melihat CPU Load routernya berapa. Kemudian bisa melihat penyimpanan yang tersisa berapa (Rahayu, 2022).

2.7 Keamanan Jaringan. Keamanan infrastruktur jaringan komputer dan internet merupakan salah satu bagian dari sistem informasi yang cukup berperan penting dalam menjaga integritas dan validitas data, juga dapat menjamin ketersediaan layanan bagi setiap penggunanya (user). Sistem terutama infrastruktur yang sudah dibangun, haruslah dapat dilindungi dari bermacam jenis serangan dari pihak yang tidak bertanggung jawab.

Jaringan dirancang atau didesain sebagai komunikasi data jalan raya (highway) dengan tujuan untuk meningkatkan akses ke dalam sistem komputer, sementara security (keamanan) dirancang atau didesain untuk mengontrol akses ke dalam suatu jaringan. Perlu pemahaman yang cukup kuat mengenai infrastruktur fisik dan logika dari suatu jaringan, serta harus dapat memastikan bahwa jaringan yang ada saat ini (existing) efisien dan sehat (Farizy & Sita Eriana, 2022).

2.8 Denial of Service (DoS)

DoS adalah jenis serangan yang diluncurkan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber resource yang dimiliki oleh komputer (misalnya menggunakan semua sumber CPU, Memori) sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga layanan ini tidak dapat digunakan dan akhirnya akan crash (Lelisa Army, 2022).

2.9 Distributed Denial of Service (DDoS)

DDoS (Distributed Denial of Service) adalah salah satu jenis serangan Denial of Service Attack yang menggunakan banyak host penyerang baik itu menggunakan komputer yang didedikasikan untuk melakukan penyerangan atau komputer yang dipaksa menjadi zombie untuk menyerang satu buah host target dalam sebuah jaringan.

Cara kerja DDoS biasanya mematikan semua layanan yang sedang aktif atau membanjiri jaringan dengan sejumlah pesan yang besar. Sederhananya, DDoS mengeksploitasi lubang keamanan di protokol TCP/IP yang disebut SynFlood, yaitu sistem target yang dituju akan dibanjiri oleh permintaan yang sangat banyak jumlahnya (flooding), sehingga akses menjadi sangat sibuk (Lelisa Army, 2022).

2.10 Firewall Filter Rule

Fitur Filter pada firewall digunakan untuk menentukan apakah suatu paket data dapat masuk atau tidak ke dalam sistem router itu sendiri. Paket data yang akan ditangani fitur Filter ini adalah paket data yang ditunjukkan pada salah satu interface router. Fitur Filter ini juga dapat menangani paket data yang melintasi router dari jaringan local ke internet, sehingga fitur filter lainnya dapat dikolaborasikan dengan NAT. Fitur filter pada Router Mikrotik memiliki 3 chain, yaitu input, output, dan forward (Towidjojo, 2013).

2.11 Pengertian Firewall

Gambar 2.8 Firewall
(Sumber : stock.adobe.com/images/vector-illustration-of-firewall-icon-network-security-symbol-protection-logo-cyber-security-and-protection/286498799, 2023)

Firewall merupakan perangkat yang berfungsi untuk memeriksa dan menentukan paket data yang dapat keluar atau masuk dari sebuah jaringan. Dengan kemampuan menentukan apakah sebuah paket data bisa masuk dan keluar dari suatu jaringan maka firewall berperan untuk melindungi jaringan dari serangan yang berasal dari jaringan luar (outside network). Misalnya difungsikan untuk melindungi jaringan lokal (LAN) dari kemungkinan serangan yang berasal dari internet. Selain ditujukan untuk melindungi jaringan, firewall juga dapat difungsikan untuk melindungi sebuah komputer user tau host (single host), firewall jenis ini disebut host firewall (Towidjojo, 2013).

2.12 Firewall Raw

Firewall Raw merupakan salah satu fitur pada mikrotik yang bisa digunakan untuk bypass atau drop paket sebelum connection tracking. Karena tidak melewati connection tracking, maka penggunaan firewall raw ini akan lebih efektif dan menghemat CPU dibandingkan menggunakan firewall filter. Secara konsep, Raw bisa melakukan filtering seperti layaknya firewall filter. Dan biasanya digunakan untuk memproteksi jaringan dari DDOS Mitigation. Firewall Raw bisa juga digunakan untuk bypass koneksi tertentu agar tidak membebani CPU.

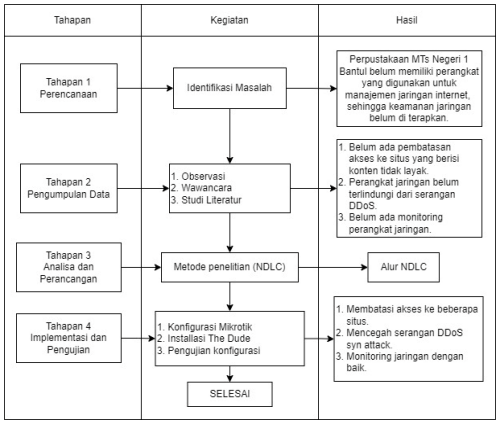
2.13 Network Development Life Cycle (NDLC)

NDLC mendefinisikan siklus proses perancangan atau pengembangan suatu sistem jaringan komputer. NDLC mempunyai elemen yang mendefinisikan fase, tahapan, langkah atau mekanisme proses spesifik. Kata cycle merupakan kunci deskriptif dari siklus hidup pengembangan sistem jaringan yang menggambarkan secara keseluruhan proses dan tahapan pengembangan sistem jaringan yang berkesinambungan (Kurniawan, 2016).

3. METODE PENELITIAN

3.1 Proses Alur Penelitian

Proses alur penelitian menggambarkan langkah-langkah dalam menyelesaikan penelitian ini, terdapat 4 tahapan yaitu Perencanaan, Pengumpulan Data, Analisa dan Perancangan, serta Implementasi dan Pengujian. Gambar 3.1 adalah flowchart alur penelitian.



Gambar 3.1 Flowchart Alur Penelitian
(Sumber: Penulis, 2023)

3.1.1 Tahap Perencanaan Penelitian

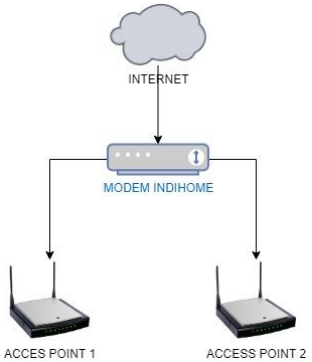
Tahap ini adalah tahapan paling awal dimana proses identifikasi permasalahan yang akan diteliti dilakukan. Melalui identifikasi masalah tersebut akan digunakan sebagai acuan dalam menentukan batasan masalah dan tujuan penelitian. Penjelasan identifikasi masalah berdasarkan pada flowchart alur penelitian adalah sebagai berikut:

1. Identifikasi Masalah
Perpustakaan XYZ belum memiliki perangkat yang digunakan untuk manajemen jaringan. Dengan tidak adanya perangkat tersebut kontrol dan keamanan jaringan internet di perpustakaan tidak dapat dilakukan secara maksimal.

3.1.2 Pengumpulan Data

Pada tahap ini pengumpulan data yang terkait dengan proses identifikasi masalah dilakukan melalui 3 metode yaitu observasi, wawancara, dan studi literatur. Berikut adalah penjelasanya:

1. Observasi.
Pada tahap ini, pengumpulan data dilakukan secara langsung di objek penelitian. Dari observasi yang telah peneliti lakukan, didapatkan hasil arsitektur jaringan internet perpustakaan XYZ dalam bentuk topologi pada Gambar 3.2.



Gambar 3.2 Topologi Jaringan Perpustakaan
(Sumber: Penulis, 2023)

Berdasarkan gambar di atas, diketahui akses internet dari penyedia layanan internet (Internet Service Provider) Indihome didistribusikan secara langsung dari modem ke *access point*.

2. Wawancara.
   Pada tahap ini merupakan sesi tanya jawab dengan penanggung jawab infrastruktur IT perpustakaan XYZ. Hasil wawancara akan dibahas pada Tabel 3.1

Tabel 3.1 Wawancara

No	Pertanyaan	Narasumber	Jawaban
1	Berapa bandwidth internet yang digunakan sekarang?	Guru	Bandwidth yang digunakan sekarang 100mbps paket gaming dari indihome
2	Apakah sudah tersedia perangkat yang digunakan untuk manajemen jaringan internet di perpustakaan?	Guru	Belum ada, untuk saat ini jaringan internetnya langsung terhubung ke modem indihome.
3	Apakah sudah menerapkan metode keamanan jaringan terkait dengan serangan DDoS?	Guru	Untuk keamanan jaringan belum ada
4	Apakah ada pembatasan akses internet, seperti blokir situs atau web?	Guru	Belum ada.
5	Bagaimana untuk pemantauan jaringan internetnya?	Guru	Kalau itu juga belum ada. Jika ada masalah pada jaringan nya itu nanti biasanya ada yang melapor.

(Sumber: Penulis, 2023)

Berdasarkan pada tabel diatas, dapat diidentifikasi permasalahan yang terdapat pada objek penelitian. Pada perpustakaan XYZ belum tersedia perangkat untuk manajemen jaringan yang berdampak pada keamanan jaringan berupa web filtering dan keamanan dari serangan DDoS belum dapat diterapkan. Monitoring jaringan masih belum diterapkan pada perpustakaan sehingga lalu lintas data belum bisa dipantau. Solusi yang diusulkan oleh peneliti ditunjukan pada tabel di bawah.

Tabel 3.2 Solusi Permasalahan

No	Masalah	Solusi
1	Belum ada manajemen jaringan internet.	Melakukan pemasangan router mikrotik.
2	Belum ada pembatasan akses blokir website atau situs.	Melakukan pembatasan akses menggunakan firewall filter rule pada mikrotik.
3	Belum ada keamanan untuk mengatasi serangan DDoS.	Mengatasi serangan DDoS menggunakan firewall raw pada mikrotik.
4	Belum ada monitoring jaringan.	Melakukan instalasi The Dude untuk monitoring jaringan internet.

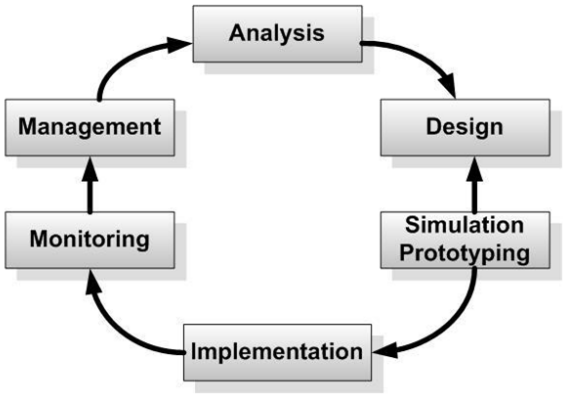
(Sumber: Penulis, 2023)

3. Studi Literatur.
   Pada tahap ini adalah mengumpulkan data dari berbagai referensi jurnal dan buku yang digunakan sebagai acuan pada literature review dan landasan teori berdasarkan hasil dari observasi dan wawancara.

3.1.3 Analisa dan Perancangan

Pada tahapan ini peneliti menggunakan metode penelitian Network Development Life Cycle (NDLC) terdiri dari analisa, desain, simulasi prototype, implementasi, monitoring, dan management. Adapun penjelasanya akan dibahas pada pembahasan selanjutnya.

3.2 Alur Network Development Life Cycle (NDLC)



Gambar 3.2 Alur NDLC
(Sumber: Penulis, 2023)

Penjelasan dari alur Network Development Life Cycle (NDLC) sebagai berikut:

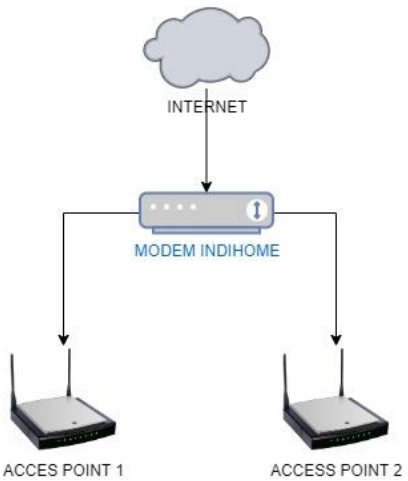
a. Analisa
   Tahapan awal yang dilakukan adalah analisa permasalahan dan analisa kebutuhan,

b. Desain
Dari data-data yang didapatkan sebelumnya akan dibuat sebuah topologi baru yang akan diterapkan.
c. Simulasi Prototype
Pada tahap ini proses simulasi prototype tidak dilakukan oleh peneliti.
d. Implementasi
Pada proses ini akan dilakukan pemasangan router manajemen pada perpustakaan XYZ.
e. Monitoring
Tahapan monitoring merupakan tahapan penting agar jaringan internet pada perpustakaan XYZ dapat berjalan sesuai dengan tujuan penelitian.
f.Management
Pada tahap ini, dilakukan dokumentasi konfigurasi yang telah dilakukan untuk memudahkan jika akan melakukan perubahan atau pengembangan jaringan di perpustakaan XYZ.

3.2.1Analisa

3.2.1.1 Analisa Permasalahan

Analisa permasalahan dilakukan guna mengidentifikasi permasalahan pada topologi jaringan internet di perpustakaan XYZ.



Gambar 3.3 Topologi Jaringan Perpustakaan
(Sumber: Penulis, 2023)

Pada Gambar 3.4 diatas, topologi jaringan internet belum menerapkan router untuk manajemen jaringan. Belum tersedianya perangkat manajemen jaringan menyebabkan pengamanan jaringan internet belum bisa dilakukan.

3.2.1.2 Analisa Kebutuhan Fungsional

Analisa kebutuhan fungsional dilakukan dengan tujuan untuk mendalami terkait metode pengamanan jaringan yang diusulkan oleh peneliti:

a. Manajemen Jaringan
Menyediakan perangkat untuk mengelola jaringan internet di perpustakaan.
b. Keamanan Jaringan
   a. Melakukan filtering terhadap situs yang berisi konten tidak layak menggunakan firewall filter rule, guna menciptakan lingkungan belajar yang bebas dari konten yang tidak layak.
   b. Melakukan pencegahan serangan DDoS syn attack terhadap router menggunakan firewall raw.
c. Monitoring Jaringan
Menyediakan monitoring jaringan menggunakan The Dude, guna memantau perangkat jaringan dan lalu lintas data.

3.2.1.3 Analisa Kebutuhan Non Fungsional

Analisa kebutuhan non fungsional dilaksanakan dengan maksud untuk mengidentifikasi perangkat keras (hardware) dan perangkat lunak (software) yang dibutuhkan dalam penelitian.

a. Kebutuhan Perangkat Keras (Hardware).
Kebutuhan perangkat keras akan dipaparkan pada Tabel 3.3.

Tabel 3.3 Kebutuhan Perangkat Keras

No	Nama Perangkat	Spesifikasi	Fungsi
1	Mikrotik RB750GR3	a. CPU MT7621A 2 Core 4 threads 880Mhz. b. 16MB *Memory*.	Sebagai router manajemen.
2	Laptop		Untuk konfigurasi mikrotik dan sebagai The Dude client.
3	Kabel UTP	Cat 5E	Sebagai penghubung antara mikrotik dan *access point*.
4	TP Link WR941	a. Data rates up to 450Mbps. b. Frequency 2.4Ghz (single band).	Sebagai pemancar internet secara wireless (tanpa kabel).
5	Handphone		Menguji koneksi dan konfigurasi.
6	Flashdisk	16GB	Sebagai penyimpanan tambahan mikrotik.

(Sumber: Penulis, 2023)

b. Kebutuhan Perangkat Lunak (Software).
Kebutuhan perangkat lunak akan dipaparkan pada Tabel 3.4.

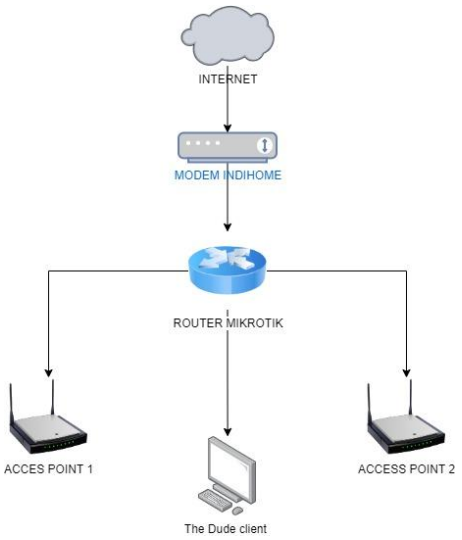
Tabel 3.4 Kebutuhan Perangkat Lunak

No	Nama	Fungsi
1	Windows 10	Sistem operasi laptop.
2	Winbox	Untuk konfigurasi mikrotik.
3	The Dude Server & Client	Software monitoring jaringan.
4	LOIC (Low Orbit Ion Cannon)	Untuk melakukan serangan DDoS.
5	Browser	Untuk mengetes fungsi pembatasan akses ke situs yang berisi konten tidak pantas.

(Sumber: Penulis, 2023)

3.2.2 Desain Topologi

Dari topologi jaringan yang digunakan pada perpustakaan saat ini tidak memungkinkan untuk dilakukannya pengamanan jaringan maka peneliti mengusulkan topologi jaringan yang didasarkan pada desain topologi tree untuk diterapkan di perpustakaan. Gambar topologi jaringan ditunjukan pada Gambar 3.5



Gambar 3.4 Topologi Jaringan Baru
(Sumber: Penulis, 2023)

Berdasarkan Gambar 3.5, topologi jaringan yang diterapkan di perpustakaan XYZ terdapat beberapa perangkat. Berikut daftar perangkat beserta fungsinya:

a. Modem
Modem merupakan perangkat yang digunakan sebagai jalur masuknya internet dari ISP (Internet Service Provider) ke perpustakaan XYZ. ISP yang digunakan oleh perpustakaan XYZ adalah Indihome.

b. Router Mikrotik
Router Mikrotik merupakan perangkat yang digunakan untuk melakukan konfigurasi dan manajemen yang diterapkan pada perpustakaan perpustakaan XYZ.

c. The Dude Client
The Dude client merupakan perangkat yang digunakan untuk monitoring jaringan di perpustakaan perpustakaan XYZ.

d. Access Point
Access Point merupakan perangkat yang digunakan untuk menyebarkan internet di perpustakaan perpustakaan XYZ.

4. HASIL DAN PEMBAHASAN

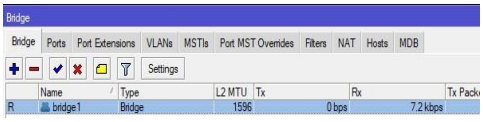
4.1 Implementasi

4.1.1 Konfigurasi Dasar Mikrotik

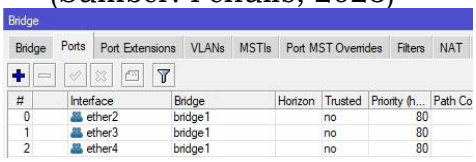
Konfigurasi dilakukan agar router dapat memiliki dan memberikan akses internet kepada perangkat yang terhubung pada router.Konfigurasi pada router meliputi:

a. Konfigurasi Bridge

Interface bridge digunakan untuk menggabungkan beberapa interface ethernet menjadi satu interface yaitu bridge1. Port ethernet yang dibridge adalah ether2, 3, dan 4 yang digunakan oleh access point dan the dude client dengan network IP 192.168.20.0/24. Gambar 4.1 merupkan interface bridge yang telah dibuat.



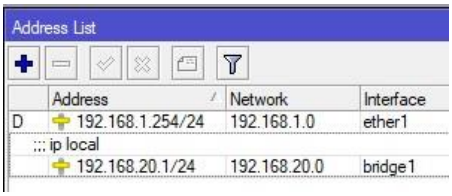
Gambar 4.1 Interface Bridge
(Sumber: Penulis, 2023)



Gambar 4.2 Ethernet Yang Dibridge
(Sumber: Penulis, 2023)

b. Address List

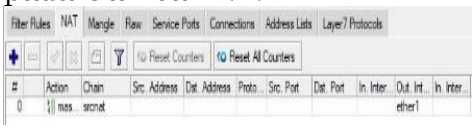
Menambahkan alamat ip yang digunakan pada interface bridge1 yaitu 192.168.20.1/24. Konfigurasi ditunjukan pada Gambar 4.3.



Gambar 4.3 IP Address
(Sumber: Penulis, 2023)

c. NAT

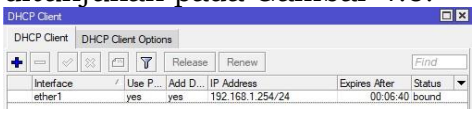
Konfigurasi NAT digunakan untuk mentranslasikan ip address lokal menjadi ip address public agar perangkat yang terhubung ke mikrotik dapat memiliki akses ke internet. Konfigurasi NAT ditunjukan pada Gambar 4.4.



Gambar 4.4 Konfigurasi NAT
(Sumber: Penulis, 2023)

d. DHCP Client

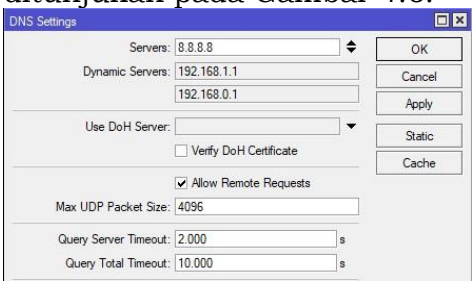
DHCP client perlu dikonfigurasi agar router mendapatkan ip address secara otomatis dari ISP (Internet Service Provider). Konfigurasi DHCP Client ditunjukan pada Gambar 4.5.



Gambar 4.5 DHCP Client
(Sumber: Penulis, 2023)

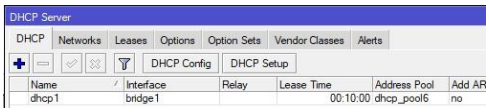
e. DNS Server

Konfigurasi DNS Server pada mikrotik dilakukan dengan menambahkan DNS Google 8.8.8.8. Konfigurasi DNS Server ditunjukan pada Gambar 4.6.



Gambar 4.6 DNS Server
(Sumber: Penulis, 2023)

f. DHCP Server
konfigurasi DHCP Server pada interface bridge1 agar interface bridge1 dapat memberikan ip address secara otomatis kepada perangkat yang terhubung pada interface bridge 1. Konfigurasi DHCP Server ditunjukan pada Gambar 4.7.



Gambar 4.7 DHCP Server
(Sumber: Penulis, 2023)

4.1.2 Konfigurasi Web Filtering

Konfigurasi filter rules pada penelitian ini dibagi menjadi 2 rule. Filter rules yang pertama digunakan untuk menangkap paket data dan data akan disimpan pada address list. Filter rules yang kedua digunakan untuk melakukan blokir terhadap situs berdasarkan data pada address list. Berikut adalah perintah CLI untuk web filtering dengan filter rule:

a. Menangkap Data
*ip firewall filter add chain=forward src-address=192.168.20.0 content=**(namasitus.xyz)** action=add-dst-to-address-list address-list=**(Sesuaikan dengan content)***

b. Blokir
*ip firewall filter add chain=forward src-address=192.168.20.0 dst-address-list= **Sesuaikan dengan address list)** action=drop*

4.1.3 Melindungi Router Dari DDoS Syn Attack

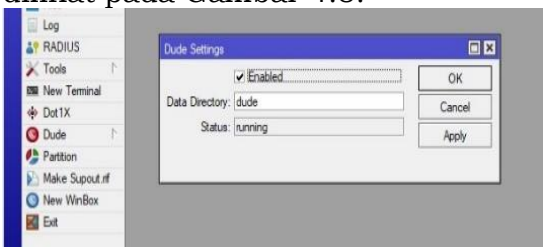
Terdapat 2 firewall raw yang peneliti gunakan, raw yang pertama digunakan untuk mengatur batas paket data yang diperbolehkan masuk dan raw kedua digunakan untuk mengatasi serangan DDoS syn attack. Apabila terdapat paket data masuk melebihi batas yang telah diatur, maka paket data tersebut akan dikenali sebagai serangan DDoS syn attack dan akan diteruskan ke firewall raw kedua untuk dilakukan penanganan. Berikut adalah perintah konfigurasi CLI untuk raw:

a. Mengatur Batasan Data
ip firewall raw add chain=prerouting src-address=192.168.20.0 protocol=tcp tcp-flags=syn limit=400,5 action=accept

b. Blokir
ip firewall raw add chain=prerouting src-address=192.168.20.0 protocol=tcp tcp-flags=syn action=drop

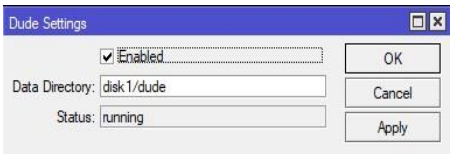
4.1.4 Monitoring Dengan The Dude

Agar dapat melakukan monitoring jaringan menggunakan The Dude, layanan The Dude server pada router harus dijalankan terlebih dahulu. Untuk mengaktifkan The Dude dapat dilihat pada Gambar 4.8.



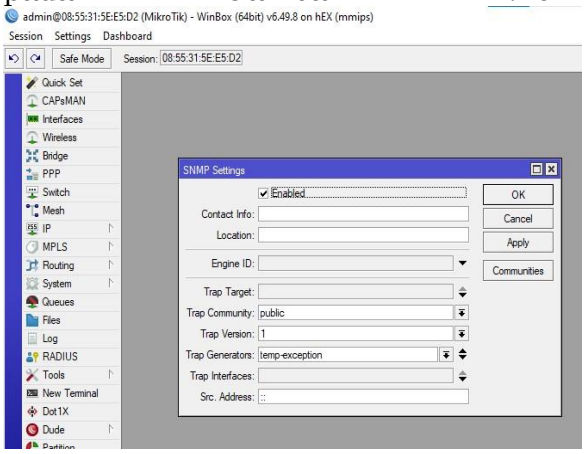
Gambar 4.8 Mengaktifkan The Dude
(Sumber: Penulis, 2023)

Karena pada mikrotik RB750GR3 membutuhkan memori tambahan untuk menyimpan data monitoring The Dude, maka pada bagian data directory perlu diubah agar data monitoring dapat tersimpan pada flashdisk. Gambar 4.9 adalah proses mengubah data directory.



Gambar 4.9 Mengubah Data Directory
(Sumber: Penulis, 2023)

Konfigurasi selanjutnya adalah menjalankan layanan SNMP di Mikrotik. Fungsi SNMP agar perangkat jaringan selain dari Mikrotik dapat terdeteksi oleh The Dude. Konfigurasi SNMP ditunjukan pada Gambar 4.10

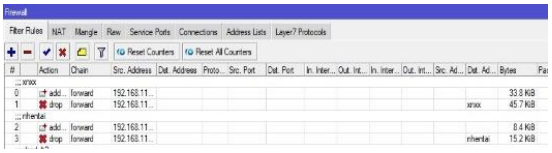


Gambar 4.10 Mengaktifkan SNMP
(Sumber: Penulis, 2023)

4.2 Pengujian

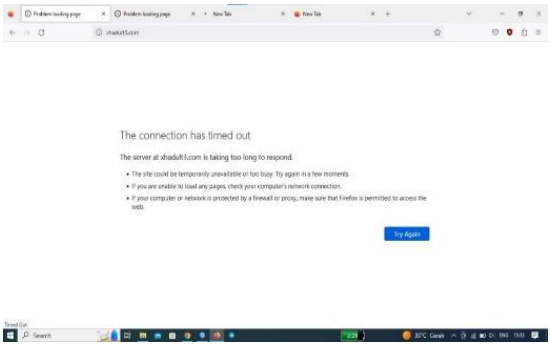
4.2.1 Pengujian Web Filtering

Trafik bytes yang terdapat pada firewall filter rules akan bertambah apabila terdapat user yang mengakses situs yang sudah di filter pada filter rules. Trafik bytes dapat dilihat pada Gambar 4.11.



Gambar 4.11 Trafik bytes
(Sumber: Penulis, 2023)

Pengujian web filtering dilakukan dengan mengakses situs yang telah difilter menggunakan laptop dan handphone, pengujian web filtering dilakukan sebanyak 3 kali. Hasil yang peneliti dapatkan adalah situs atau website yang sudah difilter tidak dapat diakses. Hasil pengujian ditunjukan pada Gambar 4.12.



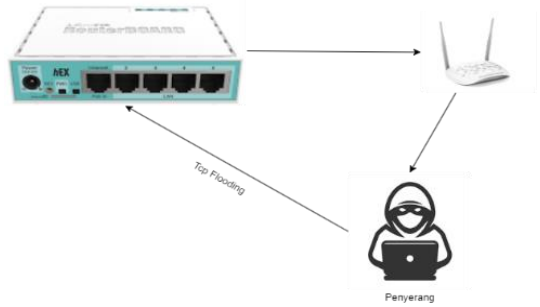
Gambar 4.12 Pengujian Melalui Laptop
(Sumber: Penulis, 2023)

Pengujian web filtering melalui handphone ditunjukan pada Gambar 4.13.

Gambar 4.13 Pengujian Pada Handphone
(Sumber: Penulis, 2023)

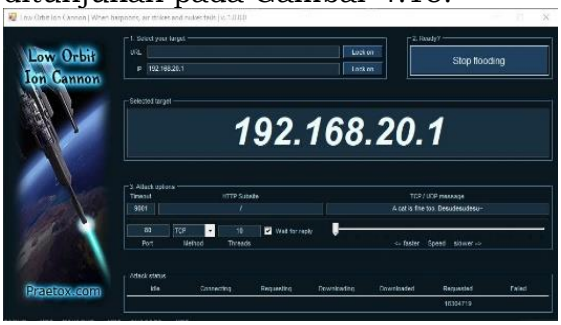
4.2.2 Pengujian DDoS Syn Attack

Skenario penyerangan DDoS dapat dilihat pada Gambar 4.14.



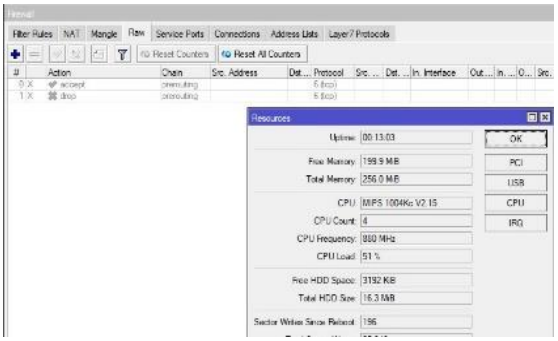
Gambar 4.14 Skenario Pengujian
(Sumber: Penulis, 2023)

Dalam pengujian ini peneliti menggunakan aplikasi LOIC untuk melakukan serangan DDoS ke IP Address Mikrotik yaitu 192.168.20.1 proses penyerangan ditunjukan pada Gambar 4.15.



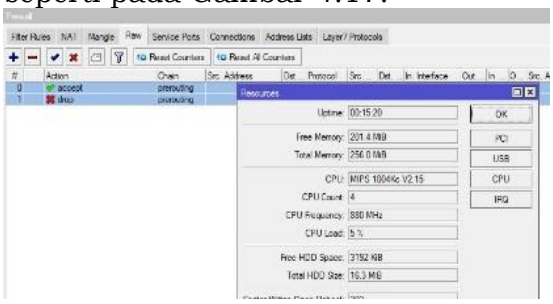
Gambar 4.15 Penyerangan Dengan LOIC
(Sumber: Penulis, 2023)

Hasil dari serangan DDoS syn attack jika firewall raw tidak diaktifkan adalah penggunaan CPU pada mikrotik naik menjadi 50% seperti yang ditunjukan pada Gambar 4.16.



Gambar 4.16 Pengujian DDoS 1
(Sumber: Penulis, 2023)

Hasil pengujian serangan DDoS syn attack jika firewall raw dalam keadaan aktif adalah pemakaian CPU Load turun dengan signifikan seperti pada Gambar 4.17.



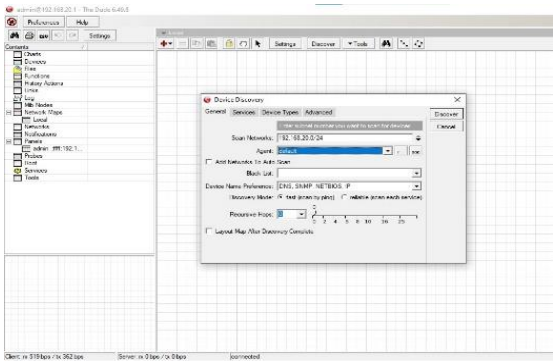
Gambar 4.17 Pengujian DDoS 2
(Sumber: Penulis, 2023)

4.2.3 Pengujian The Dude

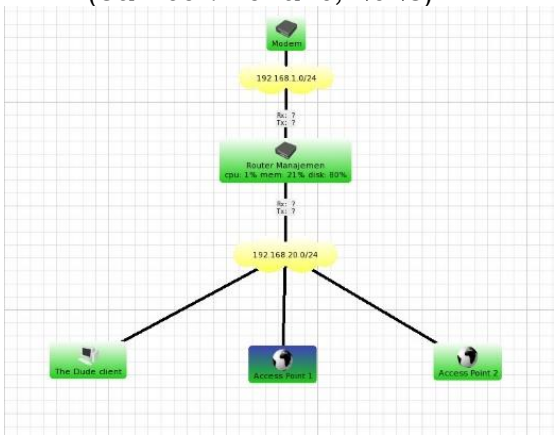
Monitoring jaringan pada The Dude memerlukan proses login ke The Dude Client menggunakan ip address router, username, dan password dari mikrotik. Username yang digunakan adalah username yang mempunyai akses full (read dan write) pada mikrotik. Proses login ditunjukan pada Gambar 4.18.

Gambar 4.18 Login The Dude
(Sumber: Penulis, 2023)

Setelah berhasil login, diperlukan proses memindai perangkat yang terhubung ke mikrotik. Pemindaian dilakukan secara otomatis menggunakan menu discover. Jika proses discover telah selesai, maka akan menampilkan seluruh perangkat jaringan yang tersambung ke mikrotik. Proses discover ditunjukan pada Gambar 4.19.

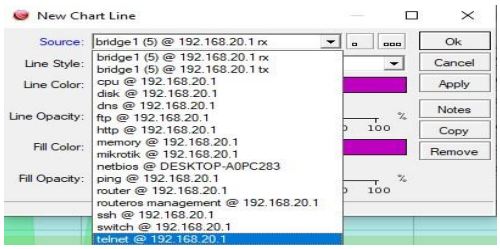


Gambar 4.19 Proses Discover
(Sumber: Penulis, 2023)



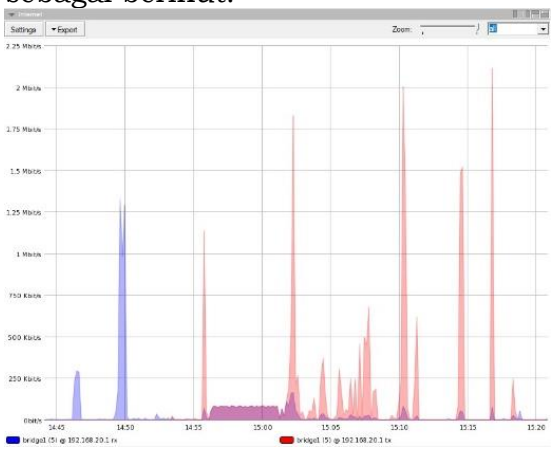
Gambar 4.20 Hasil Discover
(Sumber: Penulis, 2023)

Melalui Gambar 4.20, dapat diketahui perangkat yang mengalami kendala. Terdapat indikator warna untuk mengetahui kondisi jaringan atau perangkat yang terhubung ke mikrotik. warna hijau (menandakan bahwa perangkat sedang aktif dan sambungan bagus), warna orange (menandakan bahwa perangkat sedang aktif namun ada beberapa layanan yang sedang tidak aktif), dan warna merah (menandakan bahwa perangkat sedang tidak aktif). Pemantauan penggunaan sumber daya internet maupun router dapat dipantau dengan lebih detail menggunakan chart. Terdapat parameter monitoring yang dapat digunakan dalam membuat chart, parameter tersebut ditunjukan pada Gambar 4.21.



Gambar 4.21 Parameter Chart
(Sumber: Penulis, 2023)

Chart monitoring internet adalah sebagai berikut:

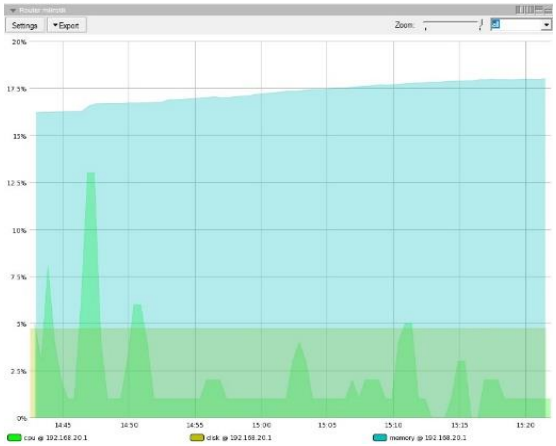


Gambar 4.22 Chart Monitoring Internet
(Sumber: Penulis, 2023)

Pada chart diatas dapat diketahui trafik lalu lintas data pada interface bridge1. Parameter yang digunakan dalam memantau trafik lalu lintas data adalah parameter TX (Transmit) dan RX (Receive). The Dude

memungkinkan administrator jaringan untuk mengintegrasikan parameter monitoring TX dan RX dalam grafik atau chart yang jelas dan mudah dimengerti. Dengan demikian, administrator dapat secara visual melihat aliran data yang masuk (RX) dan keluar (TX) dari perangkat jaringan. Data ini membantu dalam mengidentifikasi masalah jaringan dan analisis lalu lintas data.

Chart monitoring resource mikrotik ditunjukan pada Gambar 4.23.



Gambar 4.23 Chart Resource Mikrotik
(Sumber: Penulis, 2023)

Monitoring resource atau sumber daya pada router mikrotik pada penelitian ini adalah mengukur parameter-parameter kinerja perangkat keras, seperti penggunaan CPU, kapasitas penyimpanan (disk), dan penggunaan memori (memory). The Dude menyediakan fitur untuk mengintegrasikan parameter-parameter ini dalam bentuk chart atau grafik yang memberikan visualisasi data yang jelas dan terstruktur. Melalui chart, administrator jaringan dapat memantau dan menganalisis sejauh mana perangkat keras berfungsi, serta mengidentifikasi potensi masalah. Pemantauan CPU, disk, dan memory dengan The Dude dapat memberi informasi tentang kesehatan perangkat keras, memungkinkan dalam menjaga kinerja dan stabilitas jaringan, serta membantu dalam perencanaan dan pengelolaan sumber daya dengan lebih efektif.

5. PENUTUP

Penerapan pembatasan akses ke situs yang berisi konten tidak layak atau web filtering dapat berjalan dengan baik, user yang terhubung ke jaringan perpustakaan XYZ tidak dapat mengakses website atau situs yang telah difilter oleh router.

a. Pengamanan dari serangan DDoS syn attack menggunakan Raw pada mikrotik terbukti mampu untuk mengatasi serangan tersebut.
b. Monitoring jaringan menggunakan The Dude dapat membantu untuk memantau perangkat-perangkat jaringan yang terhubung ke router manajemen.

DAFTAR PUSTAKA

Alfidzar, H., & Parga Zen, B. (2022). *Implementasi HoneyPy Dengan Malicious Traffic Detection System (Maltrail) Guna Mendeteksi Serangan DOS Pada Server*. *4*(2), 32–045. https://doi.org/10.20895/INISTA.V4I2

Deni Bahtiar1, W. J. F. A. M. S. S. W. D. R. P. T. R. J. R. Z. R. D. (n.d.). PENGENALAN DASAR INSTALASI JARINGAN KOMPUTER MENGGUNAKAN MIKROTIK. *Jurnal Kreativitas Mahasiswa Informatika Volume 2 Nomor 3 Tahun 2021 Page 507 - 518 p-ISSN: 2797-6327 e-ISSN: -*. Retrieved August 9, 2023, from https://core.ac.uk/download/pdf/524980292.pdf

Faisal Qomarudin, M., & Amrullah, A. (2022). SISTEM MONITORING JARINGAN REALTIME BERBASIS INTERNET CONTROL MESSAGE PROTOCOL. *JINTECH: Journal of Information Technology*, *3*(2). https://journal.ar-raniry.ac.id/index.php/jintech

Farizy, S., & Sita Eriana, E. (2022). *KEAMANAN SISTEM INFORMASI*. www.unpam.ac.id

Fauzy, I. (2015). *APLIKASI BERBASIS ANDROID UNTUK MEMANTAU JARINGAN WIFI DAN SERVER UNIVERSITAS DARMA PERSADA*.

Jagad, B., Putra, G., Musri, T., Kom, M., & Gultom, L. M. (2020).

PEMANFAATAN MIKROTIK ROUTERBOARD SEBAGAI KEAMANAN JARINGAN DARI UDP FLOOD DENGAN MENGGUNAKAN FIREWALL DI DINAS PENDIDIKAN BENGKALIS. In *Seminar Nasional Industri dan Teknologi (SNIT)*. https://snit-polbeng.org/eprosiding/index.php/snit/article/view/136/138

Kurniawan STMIK Mura Lubuklinggau Jl Jend Besar Soeharto Km, R. H., & Lubuk Kupang Kec Lubuk Linggau selatan, kel. (2016). ANALISIS DAN IMPLEMENTASI DESAIN JARINGAN HOTSPOT BERBASIS MIKROTIK MENGGUNAKAN METODE NDLC (NETWORK DEVELOPMENT LIFE CYCLE) PADA BPU BAGAS RAYA LUBUKLINGGAU. In *Jurnal Ilmiah Betrik* (Vol. 07, Issue 01).

Lelisa Army, W., Barovih, G., Bayu Seta, H., Aji Sri Margiutomo, S., Arifianto, T., Pujianto, D., & Irfan Fajri, T. (2022). *TEKNOLOGI JARINGAN KOMPUTER*. www.penerbitwidina.com

Rahayu, S. P., Gusti, I., Putra, L., & Prismana, E. (2022). Implementasi Monitoring Manajemen Jaringan Dengan Software The Dude Berbasis Telegram Messenger. *Journal of Informatics and Computer Science*, *04*. https://ejournal.unesa.ac.id/index.php/jinacs/article/view/48101/40862

Rahman, M. (2023). Implementasi Web Content Filtering Pada Jaringan RT/RW Net Menggunakan Pi-Hole DNS Server. In *Generation Journal* (Vol. 7, Issue 1).

Rasyiidin, M. Y. B., Murad, F. A., & Murad. (2021). Monitoring Server Berbasis SNMP Menggunakan Cacti pada Server Lokal. *Jurnal Ilmiah FIFO*, *13*(1), 14. https://doi.org/10.22441/fifo.2021.v13i1.002

Rusito, S., Kom, M., & Kom. (n.d.). *Dasar Internet Teknologi IoT (Internet of Thing) dan Bahasa HTML*.

Sofana, I. (2015). *MEMBANGUN JARINGAN KOMPUTER*. Informatika Bandung.

Syaripudin, A., & Nugraha, A. (2023). Analisa Dan Implementasi Blocking Website Dengan Metode 7 Layer Pada Perangkat Mikrotik Di Garage Freshmart. In *Jurnal Informatika MULTI* (Vol. 1, Issue 4). https://jurnal.publikasitecno.id/index.php/jim447

Towidjojo, R. (2013). *Mikrotik kung fu : kitab 1*. Jasakom.

Yudi mulyanto, herfandi, randi candra kirana. (n.d.). *ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK(WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING*. Retrieved August 9, 2023, from http://jurnal.uts.ac.id/index.php/JINTEKS/article/view/1528/885