



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



**IMPLEMENTASI MITIGASI SERANGAN
DISTRIBUTED DENIAL OF SERVICE (DDOS)
PADA ROUTER MIKROTIK MENGGUNAKAN
METODE *FIREWALL RAW, RATE LIMIT, DAN
PORT HARDENING***

SKRIPSI

Alvito Revansyah Gunawan 2207421015

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN
JARINGAN**

**JURUSAN TEKNIK INFORMATIKA DAN
KOMPUTER**

POLITEKNIK NEGERI JAKARTA

2026



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



**IMPLEMENTASI MITIGASI SERANGAN
DISTRIBUTED DENIAL OF SERVICE (DDOS) PADA
ROUTER MIKROTIK MENGGUNAKAN METODE
*FIREWALL RAW, RATE LIMIT, DAN PORT
HARDENING***

SKRIPSI

**Dibuat untuk Melengkapi Syarat – Syarat yang Diperlukan untuk
Memperoleh Diploma Empat Politeknik**

Alvito Revansyah Gunawan

2207421015

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN
JARINGAN**

**JURUSAN TEKNIK INFORMATIKA DAN
KOMPUTER**

POLITEKNIK NEGERI JAKARTA

2026



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Alvito Revansyah Gunawan
NIM : 2207421015
Jurusan/Program Studi : Teknik Informatika dan Komputer/Teknik Multimedia dan Jaringan
Judul Skripsi : Implementasi Mitigasi Serangan Distributed Denial of Service (Ddos) Pada Router Mikrotik Menggunakan Metode Firewall Raw, Rate Limit, Dan Port Hardening.

Menyatakan dengan sebenarnya bahwa skripsi ini benar – benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri – ciri plagiat dan bentuk – bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 15 Juni 2026

Yang membuat pernyataan



Alvito Revansyah Gunawan

NIM. 2207421015



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama : Alvito Revansyah Gunawan
NIM : 2207421015
Program Studi : Teknik Multimedia dan Jaringan
Judul Skripsi : Implementasi Mitigasi Serangan Distributed Denial of Service (Ddos) Pada Router Mikrotik Menggunakan Metode Firewall Raw, Rate Limit, Dan Port Hardening

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari ~~...~~ Tanggal ~~...~~,
Bulan ~~...~~ Tahun 2026 dan dinyatakan **LULUS**.

Disahkan oleh:

Pembimbing I : Ariawan Andi Suhandana, S. Kom., M.T.I.
Penguji I : Defiana Arnaldy, S.Tp., M.Si.
Penguji II : Fachroni Arbi Murad, S. Kom., M. Kom.
Penguji III : Andika Riyadi Jasril, M.Pd.T.

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua



Dr. Anita Hidayati, S. Kom., M. Kom.

NIP. 197908032003122003



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Implementasi Mitigasi Serangan Distributed Denial of Service (DDoS) pada Router MikroTik Menggunakan Metode Port Hardening, Firewall RAW, dan Rate Limit”.

Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Diploma Empat pada Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta. Penelitian ini membahas penerapan *Firewall RAW*, *Rate Limiting*, *Port Hardening*, serta simulasi RTBH dalam mitigasi serangan DDoS pada router MikroTik.

Dalam penyusunan skripsi ini, penulis memperoleh bantuan, arahan, dan dukungan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Bapak Ariawan Andi Suhandana, S. Kom., M.T.I., selaku dosen pembimbing yang telah memberikan bimbingan, arahan, dan masukan selama proses penyusunan skripsi.
2. Seluruh dosen Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta, yang telah memberikan ilmu dan pengalaman selama masa perkuliahan.
3. Pihak PT XYZ yang telah memberikan informasi dan dukungan dalam proses pengumpulan data serta kebutuhan penelitian.
4. Bapak M. Ichwan Hardiansyah, selaku IP Network Engineer di PT XYZ, yang telah membantu memberikan informasi teknis, arahan, serta dukungan dalam proses implementasi dan pengujian pada penelitian ini.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

v

5. Orang tua dan keluarga yang selalu memberikan doa, dukungan, dan motivasi kepada penulis.
6. Teman-teman kelas TMJ 22 serta pihak yang telah memberikan dukungan, bantuan, dan semangat kepada penulis selama proses penyusunan skripsi ini.
7. Syifa Chandra Tiffani Sumardi, Muhammad Abdan Syakuron, Sahrul Apriandi, Jibril Khairy Akram, Raden Muhammad Fadil Azhar, Stephanie Meissya P dan Harsdyka Wibisono yang senantiasa memberikan dukungan, motivasi, serta menjadi tempat berbagi cerita dan pengalaman selama proses perkuliahan hingga penyelesaian skripsi ini.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun agar penelitian ini dapat menjadi lebih baik. Semoga skripsi ini dapat memberikan manfaat bagi pembaca, khususnya dalam bidang keamanan jaringan dan mitigasi serangan DDoS pada router MikroTik.

**POLITEKNIK
NEGERI
JAKARTA**

Depok, 2026

Penulis,

Alvito Revansyah Gunawan



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

**SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK
KEPENTINGAN AKADEMIS**

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini:

Nama : Alvito Revansyah Gunawan
NIM : 2207421015
Jurusan/Program Studi : Teknik Informatika dan Komputer/Teknik
Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

Implementasi Mitigasi Serangan *Distributed Denial Of Service (Ddos)* Pada Router Mikrotik Menggunakan Metode *Firewall Raw, Rate Limit, Dan Port Hardening*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 15 Juni 2026

Yang menyatakan



Alvito Revansyah Gunawan

NIM.2207421015



Implementasi Mitigasi Serangan *Distributed Denial of Service (Ddos)* Pada Router Mikrotik Menggunakan Metode *Firewall Raw, Rate Limit, Dan Port Hardening*

ABSTRAK

Serangan *Distributed Denial of Service (DDoS)* merupakan ancaman jaringan yang dapat menyebabkan layanan tidak tersedia akibat lonjakan trafik yang membebani router. Penelitian ini bertujuan menerapkan mitigasi serangan *DDoS* pada router MikroTik menggunakan metode *Firewall RAW, Rate Limiting, dan Port Hardening*, serta simulasi *Remotely Triggered Black Hole (RTBH)* sebagai langkah terakhir ketika trafik serangan perlu dibuang pada sisi upstream. Pengujian dilakukan pada jaringan uji terpisah dengan Kali Linux sebagai sumber serangan, MikroTik CHR sebagai router upstream, dan router MikroTik fisik sebagai objek pengujian akhir. Serangan yang diuji adalah *UDP Flood* dan *TCP SYN Flood* menggunakan *hping3*. Parameter pengamatan meliputi *CPU Load, Free Memory, traffic WAN*, dan jumlah paket yang diblokir. Hasil pengujian menunjukkan bahwa *Firewall RAW* mampu membuang trafik dari *IP attacker* pada tahap awal, sedangkan *Rate Limiting* membantu membatasi trafik berlebih yang masih diproses router. *Port Hardening* memperkuat akses manajemen melalui pembatasan layanan, penggantian *Telnet* dengan *SSH*, dan *port knocking*. Simulasi *RTBH* mampu menurunkan trafik ke router utama, tetapi seluruh trafik menuju *IP target* ikut terbang.

Kata kunci: *DDoS, Firewall RAW, MikroTik, Port Hardening, Rate Limiting, RTBH.*

POLITEKNIK
NEGERI
JAKARTA

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



DAFTAR ISI

SURAT PERNYATAAN BEBAS PLAGIARISME	ii
LEMBAR PENGESAHAN	iii
KATA PENGANTAR.....	iv
ABSTRAK	vii
DAFTAR ISI	viii
DAFTAR TABEL.....	x
DAFTAR GAMBAR	xi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	5
1.3 Batasan Masalah.....	6
1.4 Tujuan dan Manfaat	8
1.5 Sistematika Penulisan	9
BAB II TINJAUAN PUSTAKA	11
2.1 Penelitian Terkait.....	11
2.2 Konsep Dasar Keamanan Jaringan.....	13
2.3 Distributed Denial of Service (DDoS)	14
2.4 MikroTik RouterOS	14
2.5 Firewall Raw	15
2.6 Metode Port Hardening.....	15
2.7 Rate Limiting	16
2.8 Remotely Triggered Black Hole.....	17
BAB III METODE PENELITIAN.....	18
3.1 Rancangan Penelitian	18
3.1.1 Arsitektur Sistem.....	19
3.2 Tahapan Penelitian	27
3.3 Objek Penelitian	30
3.4 Teknik Analisis Data	31
BAB IV HASIL DAN PEMBAHASAN.....	33
4.1 Analisis Kebutuhan	33
4.1.1 Analisis Kebutuhan Firewall Raw	35

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.1.2	Analisis Kebutuhan Rate Limiting.....	36
4.1.3	Analisis Kebutuhan Port Hardening.....	37
4.1.4	Analisis Kebutuhan RTBH.....	38
4.2	Perancangan Sistem	39
4.2.1	Perancangan Topologi Sistem	39
4.2.2	Perancangan Alur Mitigasi.....	40
4.2.3	Perancangan Firewall RAW	41
4.2.4	Perancangan Rate Limiting	42
4.2.5	Perancangan Port Hardening.....	44
4.2.6	Perancangan Simulasi RTBH.....	46
4.3	Implementasi Sistem	47
4.3.1	Implementasi Topologi dan Konfigurasi Dasar	47
4.3.2	Implementasi Firewall RAW	51
4.3.3	Implementasi Rate Limiting.....	54
4.3.4	Implementasi Port Hardening	57
4.3.5	Implementasi Simulasi RTBH.....	60
4.3.6	Implementasi Monitoring Parameter Pengujian.....	63
4.4	Pengujian.....	68
4.4.1	Deskripsi Pengujian	68
4.4.2	Prosedur Pengujian	70
4.4.3	Data Hasil Pengujian.....	72
4.4.4	Analisis Data	115
BAB V	PENUTUP	123
5.1	Simpulan	123
5.2	Saran.....	125
DAFTAR PUSTAKA		126
DAFTAR RIWAYAT HIDUP PENULIS		128
LAMPIRAN		129



DAFTAR TABEL

Tabel 2.	1 Penelitian Terkait.....	11
Tabel 4.	1 Kebutuhan Perangkat	33
Tabel 4.	2 Status Existing Layanan Manajemen MikroTik.....	37
Tabel 4.	3 Rancangan Port Hardening.....	44
Tabel 4.	4 Konfigurasi IP Perangkat pada Topologi Pengujian	49
Tabel 4.	5 Alur Implementasi Firewall RAW.....	52
Tabel 4.	6 Implementasi Rate Limiting.....	56
Tabel 4.	7 Implementasi Port Hardening.....	59
Tabel 4.	8 Komponen Implementasi Simulasi RTBH.....	62
Tabel 4.	9 Parameter Monitoring Pengujian	67
Tabel 4.	10 Hasil Pengujian Fungsional Topologi dan Koneksi Dasar	73
Tabel 4.	11 Hasil Pengujian Fungsional Firewall RAW	76
Tabel 4.	12 Hasil Pengujian Fungsional Rate Limiting	79
Tabel 4.	13 Hasil Pengujian Fungsional Port Hardening	82
Tabel 4.	14 Hasil Pengujian Fungsional Simulasi RTBH	87
Tabel 4.	15 Hasil Pengujian UDP Flood Tanpa Mitigasi	91
Tabel 4.	16 Hasil Pengujian UDP Flood dengan Firewall RAW	94
Tabel 4.	17 Hasil Pengujian UDP Flood dengan Firewall RAW dan Rate Limiting.....	96
Tabel 4.	18 Hasil Pengujian UDP Flood dengan Simulasi RTBH	99
Tabel 4.	19 Hasil Pengujian TCP SYN Flood Tanpa Mitigasi.....	105
Tabel 4.	20 Hasil Pengujian TCP SYN Flood dengan Firewall RAW	107
Tabel 4.	21 Hasil Pengujian TCP SYN Flood dengan Firewall RAW dan Rate Limiting.....	110
Tabel 4.	22 Hasil Pengujian TCP SYN Flood dengan Simulasi RTBH....	112

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



DAFTAR GAMBAR

Gambar 1. 1 Data Monitoring Serangan pada Jaringan PT XYZ Sumber: IP Network Engineer PT XYZ	2
Gambar 3. 1 Topologi Existing Jaringan PT XYZ.....	21
Gambar 3. 2 Diagram Blok Sistem	22
Gambar 3. 3 Topologi Simulasi.....	24
Gambar 3. 4 Flowchart Proses Mitigasi Serangan DDoS	26
Gambar 3. 5 Tahapan Penelitian	27
Gambar 4. 1 Konfigurasi Penerusan Trafik pada Router Upstream.....	48
Gambar 4. 2 Konfigurasi IP Router Upstream dan MikroTik Utama.....	50
Gambar 4. 3 Konfigurasi Rule Deteksi Trafik UDP Flood dan TCP SYN Flood.....	53
Gambar 4. 4 Konfigurasi Rule Firewall RAW untuk Memblokir Attacker Terdeteksi.....	53
Gambar 4. 5 Konfigurasi Rule Rate Limiting pada MikroTik Utama	55
Gambar 4. 6 Konfigurasi Layanan Manajemen pada MikroTik Utama	58
Gambar 4. 7 Konfigurasi Blackhole Route pada Router Upstream	61
Gambar 4. 8 Aktivasi Blackhole Route pada Router Upstream.....	61
Gambar 4. 9 Penonaktifan Blackhole Route Setelah Skenario RTBH.....	62
Gambar 4. 10 Monitoring CPU Load dan Free Memory pada MikroTik Utama	64
Gambar 4. 11 Monitoring Traffic pada Interface WAN MikroTik Utama ...	65
Gambar 4. 12 Monitoring Counter Rule Firewall RAW	66
Gambar 4. 13 Monitoring Counter Rule Rate Limiting	66
Gambar 4. 14 Pengujian Konektivitas Kali Linux ke IP Publik Modem Simulasi	74
Gambar 4. 15 Pengujian Konektivitas Ubuntu Desktop ke Router MikroTik Utama	74
Gambar 4. 16 Trafik dari Sisi Attacker yang Diteruskan ke Interface WAN MikroTik Utama	75
Gambar 4. 17 Simulasi UDP Flood dari Kali Linux	77
Gambar 4. 18 Simulasi TCP SYN Flood dari Kali Linux.....	77
Gambar 4. 19 IP Attacker Masuk Address-List ddos-attackers	78
Gambar 4. 20 Counter Firewall RAW Meningkat Setelah Attacker Terdeteksi	78
Gambar 4. 21 Pengujian Rate Limiting terhadap UDP Flood.....	81
Gambar 4. 22 Pengujian Rate Limiting terhadap TCP SYN Flood	81
Gambar 4. 23 Status Layanan Manajemen Setelah Port Hardening	83
Gambar 4. 24 Pengujian Akses Telnet dari Sisi Luar Setelah Dinonaktifkan	84
Gambar 4. 25 Proses Port Knocking dari Jaringan Luar.....	84
Gambar 4. 26 Pengujian Akses SSH dari Jaringan Admin Internal	85
Gambar 4. 27 Pengujian Akses SSH dari Sisi Luar Sebelum Port Knocking	85
Gambar 4. 28 IP Sumber yang Berhasil Masuk Address-List secured-admin	86

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4. 29 Pengujian Akses SSH dari Sisi Luar Setelah Port Knocking	86
Gambar 4. 30 Trafik dari Kali Masih Diteruskan ke MikroTik Utama Sebelum RTBH.....	88
Gambar 4. 31 Aktivasi Blackhole Route pada Router Upstream.....	88
Gambar 4. 32 Pengujian Konektivitas Setelah RTBH Diaktifkan	89
Gambar 4. 33 Kondisi Interface WAN MikroTik Setelah RTBH Diaktifkan	89
Gambar 4. 34 Simulasi Serangan UDP Flood pada Tahap Pengujian.....	90
Gambar 4. 35 Snapshot UDP tanpa mitigasi.....	92
Gambar 4. 36 Monitoring Resource dan Traffic Saat UDP Flood Tanpa Mitigasi.....	93
Gambar 4. 37 Statistik Dropped Packets Firewall RAW pada Pengujian UDP Flood.....	93
Gambar 4. 38 Snapshot UDP Firewall Raw.....	95
Gambar 4. 39 Statistik Dropped Packets pada Pengujian UDP Flood dengan Firewall RAW dan Rate Limiting.....	97
Gambar 4. 40 Snapshot UDP Firewall Raw dan Rate Limiting.....	98
Gambar 4. 41 Aktivasi Blackhole Route pada Pengujian UDP Flood.....	99
Gambar 4. 42 Monitoring Resource dan Traffic Saat UDP Flood dengan RTBH Aktif	101
Gambar 4. 43 Snapshot UDP simulasi RTBH.....	102
Gambar 4. 44 Simulasi Serangan TCP SYN Flood pada Tahap Pengujian	103
Gambar 4. 45 Monitoring Resource dan Traffic Saat TCP SYN Flood Tanpa Mitigasi.....	104
Gambar 4. 46 Snapshot TCP SYN tanpa mitigasi.....	106
Gambar 4. 47 Statistik Dropped Packets Firewall RAW pada Pengujian TCP SYN Flood.....	107
Gambar 4. 48 Snapshot TCP SYN Firewall Raw	108
Gambar 4. 49 Statistik Dropped Packets pada Pengujian TCP SYN Flood dengan Firewall RAW dan Rate Limiting	109
Gambar 4. 50 Snapshot TCP SYN Raw dan Rate limit	111
Gambar 4. 51 Kondisi Interface WAN MikroTik Utama Setelah RTBH Diaktifkan.....	112
Gambar 4. 52 Monitoring Resource dan Traffic Saat TCP SYN Flood dengan RTBH Aktif	114



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB I PENDAHULUAN

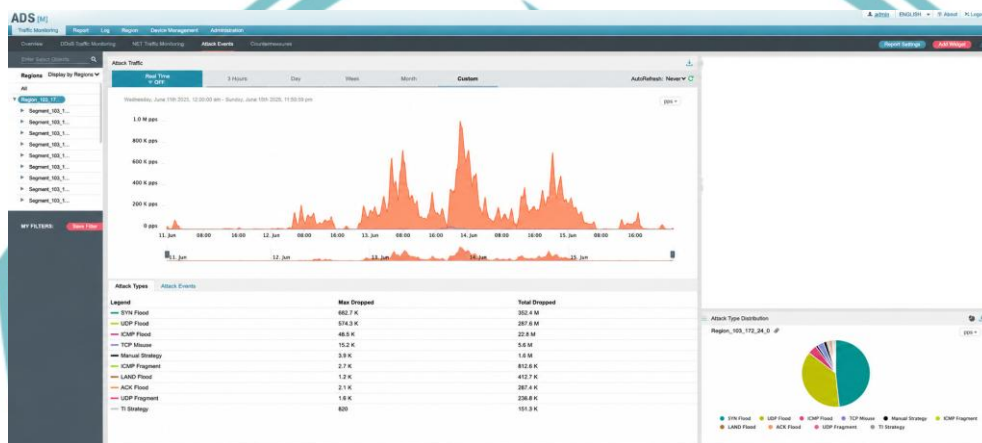
1.1 Latar Belakang

Perkembangan teknologi informasi yang semakin pesat menjadikan jaringan komputer sebagai komponen utama dalam mendukung operasional perusahaan, khususnya pada layanan berbasis internet. Tingginya ketergantungan terhadap jaringan menyebabkan aspek keamanan menjadi sangat penting, karena gangguan pada jaringan dapat berdampak langsung pada kualitas layanan dan aktivitas operasional. Salah satu ancaman yang sering terjadi pada infrastruktur jaringan adalah serangan siber yang menargetkan ketersediaan layanan, seperti serangan *Distributed Denial of Service* (DDoS), yang mampu melumpuhkan jaringan dalam waktu singkat dengan membanjiri lalu lintas data secara berlebihan (Mamuriyah et al., 2024; Susanto et al., 2023).

Router MikroTik berperan sebagai gerbang utama yang menghubungkan jaringan lokal dengan internet publik, sehingga menjadi salah satu target utama serangan DDoS. Ketika router tidak dilengkapi dengan konfigurasi keamanan yang memadai, serangan DDoS dapat menyebabkan lonjakan penggunaan sumber daya perangkat, seperti peningkatan beban CPU dan kepadatan lalu lintas jaringan. Kondisi ini berpotensi menyebabkan layanan jaringan menjadi tidak stabil atau bahkan tidak dapat diakses oleh pengguna yang sah (Riduan et al., 2025).

Berdasarkan informasi yang diperoleh melalui wawancara daring dengan pihak teknis PT XYZ, diketahui bahwa perusahaan mengalami permasalahan serius pada infrastruktur jaringan akibat serangan siber. Serangan tersebut menyebabkan gangguan layanan internet yang berdampak langsung pada operasional perusahaan. Pihak manajemen

menyampaikan bahwa gangguan jaringan yang terjadi menimbulkan kerugian materi yang diperkirakan mencapai kisaran 1 hingga 3 miliar rupiah, yang berasal dari hilangnya pendapatan layanan, biaya pemulihan sistem, serta penanganan gangguan jaringan. Selain itu, kondisi tersebut juga berdampak pada penurunan nilai perusahaan dan berkurangnya jumlah pelanggan akibat ketidakpuasan terhadap kualitas layanan yang diberikan.



Gambar 1. 1 Data Monitoring Serangan pada Jaringan PT XYZ

Sumber: IP Network Engineer PT XYZ

Berdasarkan data monitoring serangan dari PT XYZ, terlihat adanya lonjakan *attack traffic* dalam satuan *packet per second* (pps) pada periode 11 Juni 2025 sampai 15 Juni 2025. Pada grafik monitoring, trafik serangan mengalami beberapa lonjakan besar, dengan puncak tertinggi mendekati 1,0 juta pps sekitar tanggal 14 Juni 2025. Data *Attack Types* menunjukkan bahwa serangan yang dominan adalah *SYN Flood* dan *UDP Flood*, di mana *SYN Flood* memiliki nilai *Max Dropped* sebesar 682,7 K pps dengan *Total Dropped* sebesar 352,4 juta paket, sedangkan *UDP Flood* memiliki nilai *Max Dropped* sebesar 574,3 K pps dengan *Total Dropped* sebesar 287,6 juta paket. Besarnya jumlah paket yang diblokir menunjukkan bahwa jaringan menerima trafik *flooding* dalam volume tinggi dan berpotensi membebani perangkat router. Kondisi tersebut dapat menyebabkan peningkatan penggunaan



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

sumber daya perangkat, seperti *CPU Load* dan memori, serta mengganggu kestabilan layanan jaringan. Oleh karena itu, data monitoring ini digunakan sebagai dasar pemilihan skenario pengujian pada penelitian, yaitu *UDP Flood* dan *TCP SYN Flood* pada router MikroTik.

Dampak serangan tidak hanya dirasakan dari sisi finansial, tetapi juga memengaruhi kepercayaan publik terhadap PT XYZ. Banyaknya keluhan pelanggan serta sentimen negatif yang muncul di media sosial menunjukkan adanya penurunan reputasi layanan perusahaan. Dari sisi teknis, gangguan jaringan ditandai dengan lonjakan penggunaan *Central Processing Unit* (CPU) router hingga mencapai 100%, disertai dengan terkurasnya kapasitas *Random Access Memory* (RAM) dalam waktu singkat. Kondisi ini mengindikasikan bahwa serangan yang terjadi bersifat masif dan bertujuan untuk menghabiskan sumber daya perangkat jaringan, sehingga *router* tidak mampu memproses lalu lintas data secara normal dan layanan menjadi tidak tersedia bagi pengguna yang sah (Kushaeiri et al., 2024).

Serangan DDoS yang terjadi umumnya dilakukan dengan mengirimkan trafik dalam jumlah besar secara terus-menerus, sehingga memenuhi kapasitas bandwidth dan membebani proses pengolahan paket pada *router*. Akibatnya, lalu lintas data yang sah tidak dapat diproses dengan baik dan layanan jaringan menjadi tidak tersedia. Kondisi ini menunjukkan bahwa diperlukan mekanisme mitigasi yang mampu menyaring trafik berbahaya sejak tahap awal sebelum membebani sumber daya router (Siregar et al., 2025).

Pendekatan mitigasi serangan Denial of Service berbasis firewall telah dibahas dalam penelitian sebelumnya melalui analisis efektivitas penggunaan firewall iptables dalam menghadapi serangan Slowloris pada web server. Penelitian tersebut menunjukkan bahwa penerapan

firewall mampu membatasi serta memblokir lalu lintas serangan secara langsung, sehingga ketersediaan layanan tetap dapat dipertahankan meskipun sistem menerima trafik serangan. Hasil penelitian tersebut menegaskan bahwa mekanisme penyaringan trafik menggunakan firewall memiliki peran penting dalam menjaga stabilitas layanan jaringan dari serangan yang bertujuan mengganggu ketersediaan layanan (Oktivasari et al., 2022).

Untuk mengatasi permasalahan tersebut, penelitian ini menerapkan pendekatan keamanan berlapis dengan menggunakan metode *Firewall RAW*, *Rate Limiting*, dan *Port Hardening* pada router MikroTik. *Firewall RAW* digunakan untuk memblokir paket mencurigakan pada tahap awal pemrosesan, sehingga dapat mengurangi beban *CPU router*. *Rate Limiting* diterapkan untuk membatasi jumlah trafik atau koneksi dari satu sumber agar tidak melebihi batas yang ditentukan. Selain itu, *Port Hardening* digunakan untuk mengamankan akses manajemen *router* dengan membatasi *port* yang dapat diakses dari jaringan publik (Riduan et al., 2025; Hendry, 2024; Siregar et al., 2025).

Sebagai tambahan, penelitian ini juga mempertimbangkan penggunaan metode *Remotely Triggered Black Hole (RTBH)* sebagai salah satu cara untuk mengurangi dampak serangan DDoS pada jaringan. Metode ini bekerja dengan cara mengarahkan seluruh trafik yang menuju alamat IP target ke jalur khusus sehingga paket data tersebut dibuang sebelum mencapai jaringan utama. Dengan demikian, serangan dapat dihentikan dari sisi upstream dan tidak membebani router internal. Namun, penerapan RTBH secara langsung membutuhkan dukungan dari penyedia layanan internet (ISP) serta konfigurasi protokol routing seperti BGP, sehingga sulit diterapkan pada lingkungan penelitian atau jaringan internal yang memiliki keterbatasan akses. Oleh karena itu, pada penelitian ini RTBH hanya

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

disimulasikan secara sederhana menggunakan fitur blackhole route pada MikroTik untuk menggambarkan prinsip kerjanya, dan hasilnya digunakan sebagai skenario tambahan untuk menunjukkan kondisi ketika trafik harus dibuang pada sisi *upstream* (Khant Htal Myo, 2025).

Melalui penerapan ketiga metode tersebut, penelitian ini bertujuan untuk meningkatkan keamanan dan kestabilan jaringan PT XYZ dalam menghadapi serangan DDoS. Pendekatan ini difokuskan pada mitigasi di sisi gateway agar layanan tetap dapat berjalan tanpa harus memutus akses secara keseluruhan, seperti pada metode RTBH. Diharapkan sistem mitigasi yang diterapkan mampu mengurangi dampak serangan terhadap penggunaan CPU dan lalu lintas jaringan, sehingga layanan internet kepada pelanggan dapat tetap berjalan dengan baik dan gangguan operasional dapat diminimalkan.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, fokus penelitian ini adalah peningkatan keamanan infrastruktur jaringan melalui pendekatan preventif dan mitigasi teknis. Maka, rumusan masalah yang diajukan adalah:

1. Bagaimana kondisi kerentanan router MikroTik terhadap serangan *packet flooding* berupa *UDP Flood* dan *TCP SYN Flood* serta pengaruhnya terhadap CPU Load, Free Memory, dan trafik jaringan?
2. Bagaimana penerapan *Port Hardening* dapat mengurangi celah keamanan pada akses manajemen router MikroTik?
3. Bagaimana merancang dan mengimplementasikan *Firewall RAW* serta *Rate Limiting* untuk memitigasi serangan *UDP Flood* dan *TCP SYN Flood* pada router MikroTik?

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4. Sejauh mana efektivitas *Firewall RAW* dan *Rate Limiting* dalam mengurangi dampak serangan DDoS terhadap penggunaan sumber daya router?
5. Bagaimana penerapan simulasi metode Remotely Triggered Black Hole (RTBH) dalam menangani serangan DDoS pada router MikroTik?

1.3 Batasan Masalah

Berdasarkan latar belakang dan perumusan masalah yang telah diuraikan, ruang lingkup permasalahan pada penelitian ini perlu dibatasi agar pembahasan lebih terarah dan tidak meluas ke aspek keamanan jaringan lain yang berada di luar fokus penelitian. Oleh karena itu, batasan masalah dalam penelitian ini dirumuskan sebagai berikut:

1. Penelitian ini berfokus pada penanganan serangan Distributed Denial of Service (DDoS) pada lapisan Transport (Layer 4), khususnya UDP *Flood* dan TCP SYN *Flood*. Penelitian ini tidak membahas serangan pada lapisan aplikasi seperti HTTP *Flood*, Slowloris, maupun serangan lain seperti *phishing* dan SQL *injection*.
2. Pengukuran dampak serangan dibatasi pada kondisi sumber daya router dan lalu lintas jaringan, yaitu CPU Load, Free Memory, *traffic* WAN, serta jumlah paket yang diblokir oleh rule mitigasi. Penelitian ini tidak membahas dampak serangan terhadap server, aplikasi, atau layanan *backend* secara mendalam.
3. Objek penelitian tidak menggunakan jaringan operasional aktif PT XYZ. Implementasi awal dan validasi konfigurasi dilakukan pada lingkungan laboratorium menggunakan MikroTik CHR, sedangkan pengujian akhir dilakukan pada router MikroTik fisik

milik PT XYZ yang ditempatkan pada jaringan uji terpisah agar tidak mengganggu layanan pelanggan.

4. Metode mitigasi yang digunakan dibatasi pada fitur bawaan MikroTik, yaitu *Firewall RAW*, *Rate Limiting*, dan *Port Hardening*. Penelitian ini tidak membandingkan hasil mitigasi dengan perangkat Anti-DDoS pihak ketiga, *load balancing*, atau sistem keamanan eksternal lainnya.
5. Evaluasi efektivitas mitigasi dilakukan melalui skenario pengujian bertahap, yaitu tanpa mitigasi, *Firewall RAW*, kombinasi *Firewall RAW* dan *Rate Limiting*, serta simulasi RTBH. *Port Hardening* diuji secara terpisah melalui pengujian akses layanan manajemen router.
6. Simulasi RTBH pada penelitian ini hanya dilakukan menggunakan mekanisme *blackhole route* pada MikroTik. Penelitian ini tidak menerapkan RTBH nyata berbasis BGP dan tidak melibatkan kerja sama langsung dengan ISP atau pihak *upstream*.
7. Konfigurasi *Port Hardening* disesuaikan dengan informasi dari pihak teknis PT XYZ terkait layanan manajemen MikroTik yang digunakan. Layanan yang tidak digunakan seperti API, API-SSL, FTP, WWW, dan WWW-SSL dinonaktifkan, sedangkan layanan manajemen yang masih digunakan dibatasi sesuai kebutuhan pengujian.
8. Pengujian pada penelitian ini tidak menggunakan serangan DDoS nyata dari banyak sumber, melainkan merepresentasikan karakteristik trafik DDoS melalui simulasi *UDP Flood* dan *TCP SYN Flood* menggunakan satu perangkat Kali Linux pada jaringan uji terpisah.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.4 Tujuan dan Manfaat

Berdasarkan rumusan masalah yang telah disusun, penelitian ini memiliki tujuan yang ingin dicapai serta manfaat yang diharapkan bagi pengembangan ilmu maupun praktik keamanan jaringan komputer. Oleh karena itu, pada bagian ini diuraikan tujuan dan manfaat penelitian sebagai berikut.

Tujuan penelitian ini adalah:

1. Mengidentifikasi dan menganalisis dampak serangan *UDP Flood* dan *TCP SYN Flood* terhadap stabilitas sumber daya router MikroTik, khususnya CPU Load, Free Memory, dan *traffic* jaringan.
2. Menerapkan metode *Port Hardening* melalui pengaturan layanan dan pembatasan akses manajemen router untuk mengurangi celah keamanan pada perangkat MikroTik.
3. Merancang dan mengimplementasikan *Firewall RAW* serta *Rate Limiting* untuk memitigasi trafik serangan *UDP Flood* dan *TCP SYN Flood* pada router MikroTik.
4. Mengevaluasi efektivitas *Firewall RAW* dan *Rate Limiting* dalam menjaga efisiensi penggunaan sumber daya router, serta mengevaluasi *Port Hardening* dalam memperkuat keamanan akses manajemen router.
5. Untuk mengetahui penerapan dan hasil simulasi metode *Remotely Triggered Black Hole (RTBH)* dalam menangani serangan *DDoS* pada router MikroTik.

Secara umum, penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Menambah kajian ilmiah di bidang keamanan jaringan (*Network Security*), khususnya terkait mekanisme mitigasi serangan *Distributed Denial of Service (DDoS)* pada lapisan transport

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

menggunakan fitur bawaan RouterOS MikroTik tanpa bergantung pada perangkat keras tambahan.

2. Memberikan gambaran mengenai karakteristik serangan UDP *Flood* dan TCP SYN *Flood* terhadap penggunaan CPU Load, Free Memory, dan *traffic* jaringan pada router MikroTik.
3. Menjadi referensi teknis bagi administrator jaringan dalam menerapkan pertahanan berlapis melalui *Firewall RAW*, *Rate Limiting*, dan *Port Hardening* untuk meningkatkan keamanan router.
4. Memberikan masukan bagi PT XYZ dalam memahami penerapan mitigasi DDoS pada router MikroTik, terutama pada lingkungan uji yang disesuaikan dengan kondisi jaringan perusahaan tanpa mengganggu layanan operasional

Bagi pihak perusahaan PT XYZ dan administrator jaringan pada umumnya, hasil penelitian ini dapat menjadi referensi teknis dan rekomendasi *best practice* dalam mengamankan infrastruktur router dari serangan DDoS, serta meningkatkan keandalan layanan jaringan melalui konfigurasi *Firewall Raw*, *Rate Limiting*, dan *Port Hardening*.

1.5 Sistematika Penulisan

Sistematika penulisan dalam penelitian ini terdiri dari 5 bab, yaitu:

1. BAB I PENDAHULUAN

Bab I memuat latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat, serta sistematika penulisan terkait pada Implementasi Mitigasi Serangan *Distributed Denial of Service* (DDoS) pada Router MikroTik Menggunakan Metode *Port Hardening*, *Firewall Raw*, dan *Rate Limit*.

2. BAB II TINJAUAN PUSTAKA

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Bab II berisikan tinjauan pustaka dan landasan teori atau kajian ilmu secara garis besar mengenai topik permasalahan pada penelitian ini, serta beberapa penelitian-penelitian terdahulu berkaitan pada isu relevan.

3. BAB III METODOLOGI PENELITIAN

Bab III menjabarkan penjelasan mengenai perencanaan dan perancangan sistem keamanan jaringan yang akan dibangun berupa Rancangan Penelitian, Tahapan Penelitian, Objek Penelitian (Simulasi Virtual), Jadwal Penelitian, dan Rincian Biaya dalam melakukan penelitian ini.

4. BAB IV HASIL DAN PEMBAHASAN

Bab IV membahas hasil dari proses analisis kebutuhan, perancangan sistem, implementasi konfigurasi, serta pengujian sistem mitigasi serangan *DDoS* pada router MikroTik. Pada bab ini dijelaskan penerapan metode *Firewall RAW*, *Rate Limiting*, *Port Hardening*, serta simulasi *RTBH*, kemudian dilakukan pengujian terhadap serangan *UDP Flood* dan *TCP SYN Flood*. Hasil pengujian dianalisis berdasarkan parameter *CPU Load*, *Free Memory*, *traffic jaringan*, dan jumlah paket yang berhasil diblokir oleh rule mitigasi.

5. BAB V PENUTUP

Bab V berisi kesimpulan dari hasil penelitian yang telah dilakukan serta saran untuk pengembangan penelitian selanjutnya. Kesimpulan disusun berdasarkan hasil implementasi dan pengujian sistem mitigasi yang telah diterapkan, sedangkan saran diberikan sebagai masukan untuk penyempurnaan sistem keamanan jaringan pada penelitian berikutnya.

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terkait

Penelitian terkait digunakan sebagai acuan untuk memahami pendekatan dan metode yang telah diterapkan pada penelitian-penelitian sebelumnya yang relevan dengan topik mitigasi serangan DDoS pada Router MikroTik. Penelitian-penelitian tersebut menjadi dasar dalam merumuskan kontribusi dan posisi penelitian ini terhadap literatur yang sudah ada. Ringkasan penelitian terkait yang dijadikan acuan dalam penelitian ini disajikan pada Tabel 2.1.

Tabel 2. 1 Penelitian Terkait

No	Judul Penelitian	Hasil Penelitian	Perbedaan
1	Analisa Dan Implementasi Keamanan Jaringan Berbasis Firewall Raw Terhadap Serangan DDoS Pada Router Mikrotik (Riduan et al., 2025)	Penelitian ini menguji efektivitas Firewall Raw dalam menangani tiga jenis serangan: TCP SYN Flood dan UDP Flood. Hasilnya menunjukkan bahwa penerapan Firewall Raw mampu memblokir paket serangan secara efektif dan menjaga stabilitas sumber daya router dibandingkan tanpa mitigasi.	Penelitian Riduan et al. berfokus pada penggunaan <i>Firewall RAW</i> untuk memblokir trafik serangan DDoS pada router MikroTik. Penelitian tersebut menjadi acuan utama dalam penerapan <i>Firewall RAW</i> karena menunjukkan bahwa pemblokiran paket pada tahap awal dapat membantu mengurangi beban pemrosesan router. Perbedaan penelitian ini terletak pada penambahan metode <i>Rate Limiting</i> , <i>Port Hardening</i> , serta simulasi RTBH sebagai pembanding. Selain itu, penelitian ini menggunakan mekanisme deteksi IP <i>attacker</i> secara dinamis sebelum trafik lanjutan dari sumber tersebut dibuang melalui

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

			Firewall RAW. Evaluasi pada penelitian ini juga difokuskan pada CPU Load, Free Memory, <i>traffic</i> WAN, dan jumlah paket yang diblokir oleh rule mitigasi.
2.	Membangun Sekuritas Jaringan Terhadap Penggunaan VPN, Serangan DDoS, Dan Akses Eksternal Ke Mikrotik Dengan Aplikasi Winbox (Hendry, 2024).	Penelitian ini berhasil mengamankan jaringan dari penggunaan VPN ilegal (<i>Browsec</i>) dan akses eksternal yang tidak sah. Hasilnya menunjukkan bahwa penerapan metode Port Knocking dan pembatasan akses pada aplikasi Winbox efektif menjaga integritas router dari upaya penyusupan dan serangan <i>Syn Flood</i> skala kecil.	Penelitian ini menitikberatkan pada keamanan akses administratif (<i>Management Plane</i>) menggunakan teknik Port Knocking dan blokir VPN. Berbeda dengan skripsi ini yang berfokus pada efisiensi sumber daya (<i>Resource Efficiency</i>) router menggunakan Firewall Raw dan Rate Limiting untuk memitigasi serangan volumetrik masif (<i>UDP Flood</i>), serta diuji melalui simulasi beban CPU. Penelitian Hendry menjadi acuan konsep Port Knocking dan pembatasan akses manajemen MikroTik. Pada penelitian tersebut, port knocking dilakukan melalui tahapan ICMP, Telnet, dan SSH
3.	Implementasi Keamanan Anti DdoS Menggunakan Router Mikrotik Pada Layanan Cloud Storage Basis Local (Siregar et al., 2024).	Penelitian ini berhasil mengamankan server <i>OwnCloud</i> di sekolah kejuruan dari serangan <i>SYN Flood</i> menggunakan fitur standar Filter Rules pada Mikrotik. Hasilnya, server tetap dapat	Penelitian tersebut berfokus pada perlindungan layanan spesifik (<i>Cloud Storage</i>) menggunakan <i>Filter Rules</i> standar (Layer 3). Sedangkan skripsi ini menggunakan metode Firewall Raw yang lebih ringan memproses beban CPU, dikombinasikan dengan Rate Limiting dan Port

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

		diakses saat serangan terjadi.	Hardening untuk melindungi Gateway utama perusahaan.
4.	Implementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking (Putra et al., 2023)	Penelitian ini menunjukkan bahwa firewall filtering dapat memblokir trafik berdasarkan aturan tertentu, sedangkan port knocking digunakan untuk mengamankan akses port agar tidak dapat diakses secara langsung dari luar jaringan.	Penelitian ini menerapkan 2 lapisan keamanan, yaitu firewall filtering dan port knocking. Sedangkan penelitian yang dilakukan menggunakan 3 lapisan keamanan (defense-in-depth), yaitu Firewall RAW sebagai penyaringan awal trafik, Rate Limiting untuk mengendalikan jumlah koneksi, dan Port Hardening untuk mengamankan akses manajemen router. Selain itu, penelitian ini tidak berfokus pada pengujian serangan DDoS secara terukur, sedangkan penelitian yang dilakukan menguji TCP SYN Flood dan UDP Flood serta mengevaluasi dampaknya terhadap penggunaan sumber daya router.

2.2 Konsep Dasar Keamanan Jaringan

Keamanan jaringan merupakan aspek fundamental dalam infrastruktur teknologi informasi yang bertujuan untuk melindungi sistem komputer dari akses ilegal, penyalahgunaan, maupun perusakan data. Dalam era digital saat ini, sistem yang terhubung ke internet sangat rentan terhadap infiltrasi oleh pihak yang tidak bertanggung jawab. Upaya pengamanan jaringan mutlak diperlukan menggunakan sistem yang mampu mencegah serangan pada lapisan jaringan (*network layer*) maupun aplikasi.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Perangkat router memegang peranan krusial sebagai pintu gerbang utama yang menghubungkan jaringan lokal (*Local Area Network*) dengan internet. Karena posisinya yang berada di garis terdepan, router sering menjadi target utama eksploitasi. Jika tidak dilindungi dengan mekanisme yang memadai, kerentanan pada router dapat menyebabkan kelumpuhan total pada layanan jaringan di belakangnya (Susanto et al, 2023).

2.3 Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) adalah jenis serangan siber yang bertujuan untuk membuat layanan jaringan, server, atau aplikasi menjadi tidak tersedia (*unavailable*) bagi pengguna yang sah. Serangan ini dilakukan dengan cara membanjiri target dengan lalu lintas data palsu secara masif. Tanpa perlindungan yang tepat, serangan DDoS dapat menyebabkan server tidak dapat diakses sama sekali, yang berdampak pada terhentinya operasional sistem (Siregar et al, 2024).

Berdasarkan karakteristiknya, serangan DDoS dapat dikategorikan menjadi beberapa jenis. Serangan ini menjadi serangan volumetrik seperti UDP Flood dan ICMP Flood, serta serangan protokol seperti TCP SYN Flood. Serangan SYN Flood bekerja dengan mengeksploitasi proses handshake protokol TCP yang menyebabkan memori router penuh, sedangkan serangan volumetrik bertujuan menghabiskan bandwidth yang tersedia (Riduan et al, 2025).

2.4 MikroTik RouterOS

MikroTik RouterOS adalah sistem operasi berbasis Linux yang mengubah perangkat keras komputer atau perangkat *routerboard* menjadi router jaringan yang handal. Sistem ini menyediakan berbagai fitur lengkap seperti *routing*, *firewall*, manajemen *bandwidth*, hingga hotspot. Bahwa fleksibilitas fitur firewall pada MikroTik memungkinkan administrator untuk merancang sistem keamanan yang

mampu mendeteksi dan memblokir ancaman seperti *Port Scanning* dan DoS (Wijaya et al, 2025).

Namun, kompleksitas konfigurasi pada MikroTik juga menjadi tantangan tersendiri. Konfigurasi manual pada router sering kali rentan terhadap kesalahan manusia (*human error*) dan inkonsistensi, yang dapat menjadi celah keamanan. Oleh karena itu, pemahaman mendalam mengenai fitur-fitur bawaan RouterOS sangat diperlukan untuk membangun pertahanan yang efektif (Lueis, 2025).

2.5 Firewall Raw

Fitur Firewall Raw pada MikroTik merupakan mekanisme penyaringan paket yang dirancang khusus untuk menangani lalu lintas data dengan volume tinggi. Berbeda dengan *firewall filter* biasa yang bekerja setelah proses pelacakan koneksi (*connection tracking*), *Firewall Raw* bekerja pada fase *Prerouting*. Keunggulan utama *Firewall Raw* adalah kemampuannya untuk membuang (*drop*) paket berbahaya sebelum paket tersebut membebani CPU router untuk pencatatan koneksi (Sitorus et al, 2025).

Efektivitas fitur ini dalam mitigasi DDoS telah terbukti secara empiris. Penerapan aturan drop pada tabel Raw berhasil memblokir serangan *TCP SYN Flood* dan *UDP Flood* secara signifikan. Lebih lanjut, Penggunaan *Raw Firewall* mampu menurunkan beban kerja CPU hingga 35% dibandingkan jika hanya menggunakan aturan firewall standar saat terjadi serangan (Riduan et al, 2025).

2.6 Metode Port Hardening

Port Hardening adalah langkah pencegahan yang dilakukan dengan cara menutup celah-celah keamanan yang terbuka pada perangkat jaringan. Prinsip utamanya adalah membatasi akses hanya pada layanan (*service*) dan port yang benar-benar dibutuhkan. Penerapan metode *Packet Filtering* yang ketat untuk menyeleksi lalu lintas berdasarkan

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

alamat IP dan nomor port, sehingga akses dari sumber yang tidak terotorisasi dapat ditolak (Susanto et al, 2023).

Selain menutup port yang tidak digunakan, pengamanan akses manajemen router juga termasuk dalam strategi ini. Pembatasan akses eksternal, seperti penggunaan VPN atau mekanisme *Port Knocking*, sangat efektif untuk melindungi router dari upaya peretasan akses (*brute force*) dan menjaga integritas konfigurasi perangkat dari pihak luar (Hendry, 2024).

2.7 Rate Limiting

Rate Limiting merupakan mekanisme pembatasan laju trafik atau koneksi yang masuk ke perangkat jaringan dalam satuan waktu tertentu. Dalam konteks mitigasi DDoS, metode ini digunakan untuk mencegah satu sumber IP mengirimkan paket atau membangun koneksi secara berlebihan, sehingga router tidak menerima beban pemrosesan yang terlalu besar.

Pada serangan TCP SYN Flood, *Rate Limiting* dapat diterapkan dengan membatasi jumlah koneksi baru TCP atau jumlah paket SYN dari satu sumber IP. Pembatasan ini bertujuan untuk mengurangi beban router dalam memproses permintaan awal koneksi TCP yang dikirim secara terus-menerus. Sementara itu, pada serangan UDP Flood, *Rate Limiting* digunakan untuk membatasi jumlah paket UDP yang masuk dari satu sumber IP agar trafik tidak memenuhi kapasitas jaringan dan tidak membebani pemrosesan router.

Dalam penelitian ini, *Rate Limiting* digunakan sebagai lapisan mitigasi setelah *Firewall RAW*. *Firewall RAW* berfungsi membuang trafik dari sumber yang sudah terdeteksi sebagai penyerang, sedangkan *Rate Limiting* berfungsi membatasi trafik atau koneksi berlebih yang masih diproses oleh router. Dengan demikian, *Rate Limiting* berperan sebagai pelengkap dalam menjaga penggunaan CPU, memori, dan trafik

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

jaringan tetap terkendali saat terjadi serangan *UDP Flood* maupun *TCP SYN Flood*.

2.8 Remotely Triggered Black Hole

Remotely Triggered Black Hole (RTBH) merupakan salah satu metode mitigasi serangan Distributed Denial of Service (DDoS) yang bekerja pada level routing dengan memanfaatkan protokol BGP. Metode ini dilakukan dengan cara mengumumkan prefix tertentu yang mengarah ke alamat IP target, kemudian menambahkan atribut khusus sehingga router akan mengarahkan seluruh trafik menuju alamat tersebut ke jalur blackhole (Null0). Akibatnya, paket data yang menuju target akan dibuang sebelum memasuki jaringan utama, sehingga dapat mengurangi beban pada router dan menjaga kestabilan jaringan secara keseluruhan. RTBH umumnya diterapkan pada jaringan berskala besar seperti penyedia layanan internet (ISP), karena memerlukan dukungan dari infrastruktur upstream dan konfigurasi BGP (Khant Htal Myo, 2025).

Meskipun efektif dalam menghentikan serangan, RTBH memiliki kelemahan yaitu seluruh trafik menuju alamat IP target akan ikut dibuang tanpa membedakan trafik normal dan trafik berbahaya. Hal ini menyebabkan layanan pada IP tersebut tidak dapat diakses selama mekanisme RTBH diterapkan. Oleh karena itu, metode ini biasanya digunakan sebagai langkah mitigasi ketika serangan sudah berdampak besar terhadap jaringan. Dalam penelitian ini, RTBH tidak diimplementasikan secara langsung pada jaringan nyata, melainkan hanya disimulasikan menggunakan fitur blackhole route pada MikroTik untuk memahami prinsip kerjanya dan sebagai perbandingan dengan metode mitigasi lainnya (Khant Htal Myo, 2025).

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB III

METODE PENELITIAN

3.1 Rancangan Penelitian

Penelitian ini menerapkan metode kuantitatif dengan pendekatan eksperimental yang bertujuan untuk menguji efektivitas sistem keamanan jaringan dalam menanggulangi serangan siber. Pendekatan ini dipilih untuk mereplikasi insiden yang terjadi di PT XYZ melalui simulasi laboratorium terkendali, di mana peneliti akan membandingkan kinerja perangkat *Router* pada kondisi tanpa perlindungan dan kondisi setelah penerapan strategi pertahanan berlapis (*Defense-in-Depth*). Desain penelitian ini berfokus pada hubungan sebab-akibat antara penerapan konfigurasi keamanan dengan stabilitas sumber daya perangkat saat menghadapi serangan.

Rancangan sistem keamanan ini bekerja dengan mekanisme penyaringan bertingkat untuk melindungi router dari kelelahan sumber daya (*resource exhaustion*). Pada lapisan pertahanan awal, sistem menerapkan *Port Hardening* yang berfungsi layaknya mengunci pintu akses manajemen, sehingga menutup celah bagi pihak luar yang mencoba menyusup ke sistem administrasi router. Selanjutnya, lalu lintas data akan diperiksa oleh *Firewall Rule* yang bertindak sebagai penjaga gerbang terdepan, fitur ini memilah dan membuang paket data berbahaya atau sampah secara dini sebelum paket tersebut sempat membebani *prosesor* (CPU). Sebagai lapisan terakhir, sistem menggunakan mekanisme *Rate Limiting* untuk mengatur lalu lintas jaringan dengan cara membatasi jumlah koneksi dari setiap pengguna, memastikan agar tidak ada satu pihak pun yang dapat memonopoli *bandwidth* atau memori router secara berlebihan.

Efektivitas dari rancangan sistem ini kemudian diukur berdasarkan data kuantitatif melalui perbandingan kinerja sistem sebelum dan sesudah mitigasi diterapkan. Indikator keberhasilan penelitian dilihat dari



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

kemampuan sistem dalam menurunkan atau mengendalikan CPU Load, menjaga ketersediaan Free Memory, mengurangi traffic WAN yang membebani router, serta meningkatkan jumlah paket serangan yang berhasil diblokir oleh rule mitigasi. Port Hardening dievaluasi secara terpisah berdasarkan keberhasilan pembatasan akses layanan manajemen router. Selain perbandingan kondisi sebelum dan sesudah mitigasi, penelitian ini juga melakukan pengujian bertahap untuk mengukur kontribusi Firewall RAW dan Rate Limiting terhadap efisiensi sumber daya router, sedangkan Port Hardening diuji secara terpisah untuk menilai keberhasilannya dalam mengamankan akses manajemen router. Sebagai tambahan, dilakukan simulasi sederhana metode Remotely Triggered Black Hole (RTBH) menggunakan mekanisme blackhole route pada MikroTik untuk menggambarkan prinsip pembuangan trafik pada level routing, tanpa implementasi langsung pada jaringan nyata.

3.1.1 Arsitektur Sistem

Berdasarkan informasi yang diperoleh dari pihak teknis PT XYZ, sistem keamanan jaringan pada kondisi awal telah menerapkan konfigurasi firewall dasar (*simple firewall*) pada router MikroTik. Konfigurasi ini memanfaatkan fitur keamanan bawaan MikroTik untuk melakukan penyaringan lalu lintas jaringan secara umum, seperti pembatasan akses dasar dan pemblokiran paket tertentu. Pada tahap awal, mekanisme ini dinilai cukup efektif dalam menahan serangan dalam skala kecil serta aktivitas lalu lintas yang tidak wajar.

Namun, seiring berjalannya waktu dan meningkatnya intensitas serta durasi serangan, mekanisme keamanan bawaan tersebut belum dirancang untuk menghadapi serangan DDoS yang bersifat masif dan berkelanjutan. Serangan yang berlangsung dalam waktu lama menyebabkan router harus memproses lalu lintas dalam jumlah besar

**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

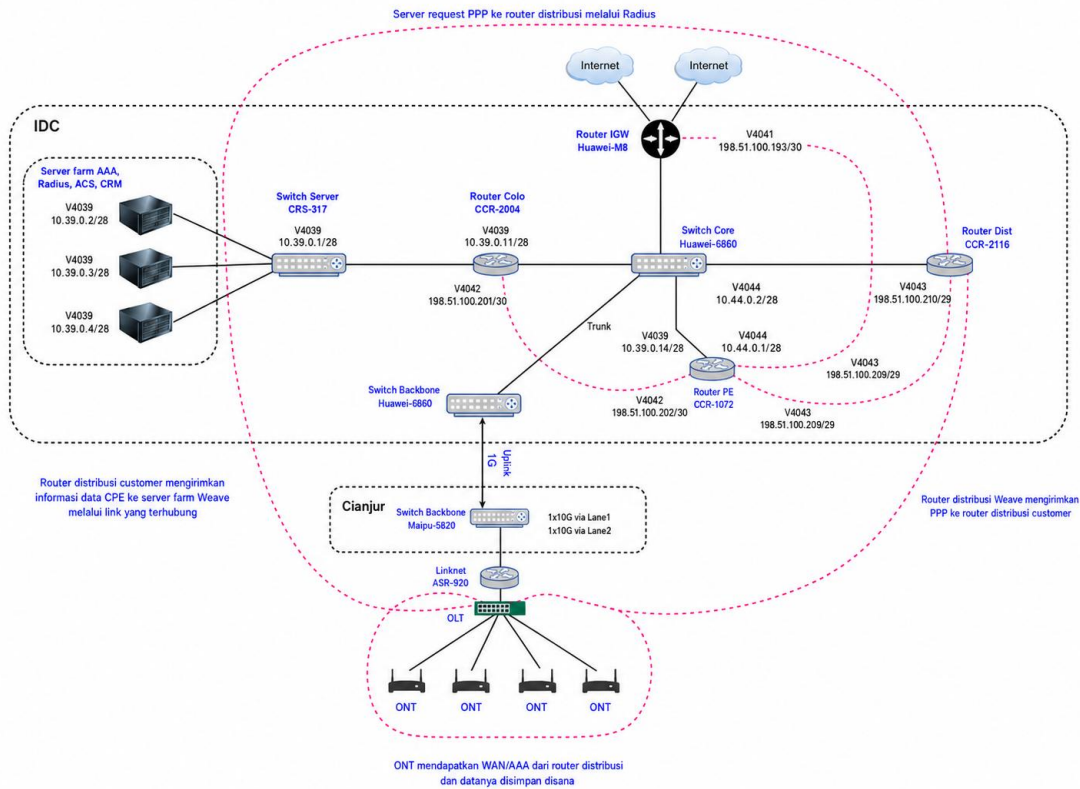
secara terus-menerus, sehingga beban kerja perangkat meningkat secara signifikan dan berdampak pada kestabilan layanan jaringan.

Selain itu, konfigurasi *firewall* dasar yang digunakan belum menerapkan mekanisme penyaringan paket pada tahap awal pemrosesan, sehingga sebagian besar trafik serangan tetap masuk ke proses *connection tracking*. Belum adanya pembatasan laju trafik (*rate limiting*) dari sumber tertentu menyebabkan router kesulitan membedakan antara lalu lintas normal dan lalu lintas serangan. Akibatnya, meskipun beberapa paket berhasil diblokir, peningkatan penggunaan CPU dan kepadatan bandwidth tetap terjadi, sehingga efektivitas sistem pertahanan menurun dan layanan jaringan kembali mengalami gangguan.

Berdasarkan informasi dari pihak teknis PT XYZ, topologi asli jaringan perusahaan terdiri dari beberapa perangkat utama seperti Router IGW, Switch Core, Router PE, Router Colo, Router Dist CCR-2116, Switch Backbone, OLT, ONT, serta server farm yang berisi layanan AAA, Radius, ACS, dan CRM. Pada topologi tersebut, Router Dist CCR-2116 berperan sebagai router distribusi yang terhubung dengan jalur backbone dan perangkat pelanggan melalui OLT dan ONT. Perangkat ini menjadi salah satu titik penting karena berperan dalam distribusi layanan menuju pelanggan.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 3. 1 Topologi Existing Jaringan PT XYZ

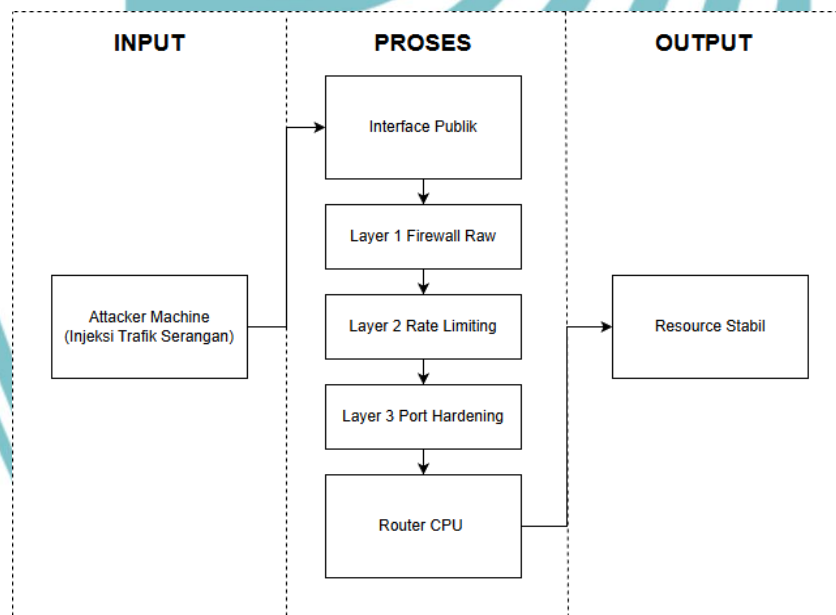
Berdasarkan Gambar 3.1, trafik pada jaringan PT XYZ tidak hanya berasal dari satu perangkat yang langsung terhubung ke router distribusi, tetapi dapat melewati beberapa perangkat perantara pada jalur jaringan. Pihak PT XYZ menjelaskan bahwa trafik yang tidak normal dapat masuk melalui sisi perangkat pelanggan, seperti ONT, kemudian melewati jalur jaringan hingga mencapai Router Dist CCR-2116. Oleh karena itu, penelitian ini menyederhanakan topologi asli tersebut ke dalam lingkungan uji yang lebih terkontrol. Pada topologi pengujian, jalur dari sisi luar direpresentasikan oleh Kali Linux, perangkat perantara direpresentasikan oleh MikroTik CHR upstream atau modem simulasi, sedangkan router distribusi direpresentasikan oleh MikroTik utama sebagai objek pengujian.

Penyederhanaan topologi ini dilakukan agar pola serangan yang terjadi pada jaringan PT XYZ tetap dapat direpresentasikan tanpa

mengganggu jaringan operasional perusahaan. Dengan demikian, pengujian dapat dilakukan secara aman pada jaringan uji terpisah, tetapi tetap mengacu pada alur trafik dari topologi asli PT XYZ.

Berdasarkan keterbatasan sistem keamanan pada kondisi awal, diperlukan rancangan sistem mitigasi yang lebih terstruktur untuk menghadapi serangan DDoS yang bersifat masif dan berkelanjutan. Oleh karena itu, penelitian ini mengusulkan arsitektur sistem keamanan yang dirancang dengan alur kerja yang terbagi ke dalam tiga tahapan utama, yaitu sisi input (sumber ancaman), proses (mekanisme pertahanan), dan output (hasil mitigasi) sebagaimana ditunjukkan pada diagram blok pada Gambar 3.2.

Pada bagian input, terdapat komponen Attacker Machine yang



Gambar 3. 2 Diagram Blok Sistem

merepresentasikan perangkat yang digunakan untuk mensimulasikan serangan. Dalam penelitian ini, perangkat tersebut menghasilkan trafik jaringan dalam jumlah besar yang diarahkan ke alamat IP publik pada router upstream atau modem simulasi, kemudian diteruskan menuju router MikroTik utama. Trafik tersebut mensimulasikan kondisi serangan DDoS seperti UDP Flood dan

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

TCP SYN Flood, yaitu ketika router menerima paket data secara terus-menerus dalam jumlah sangat banyak.

Trafik serangan tersebut masuk melalui interface publik router, yang merupakan jalur utama komunikasi antara jaringan internet dan jaringan internal. Semua paket yang masuk melalui interface ini akan diproses oleh router sebelum diteruskan ke jaringan lokal.

Pada bagian proses, router menerapkan mekanisme keamanan secara berlapis. Lapisan pertama adalah Firewall RAW, yang berfungsi sebagai penyaring awal untuk membuang paket yang terindikasi sebagai trafik serangan sebelum diproses lebih lanjut oleh sistem router. Dengan cara ini, beban kerja router dapat dikurangi karena paket berbahaya tidak perlu diproses lebih jauh.

Lapisan berikutnya adalah Rate Limiting, yang berfungsi membatasi jumlah koneksi atau paket yang dikirim oleh suatu alamat IP dalam waktu tertentu. Mekanisme ini mencegah satu sumber trafik mengirimkan paket secara berlebihan yang dapat menyebabkan kepadatan jaringan.

Selain itu, sistem juga menerapkan Port Hardening untuk mengamankan akses manajemen router. Pada tahap ini, port layanan administrasi seperti Winbox atau SSH dibatasi agar tidak dapat diakses secara bebas dari jaringan publik. Akses hanya diizinkan dari alamat IP tertentu yang telah dipercaya.

Pada bagian output, hasil yang diharapkan adalah kondisi sumber daya router tetap stabil meskipun menerima trafik serangan. Stabilitas ini dilihat dari penggunaan CPU dan memori yang tetap terkendali, serta trafik jaringan yang dapat difilter oleh sistem keamanan. Dengan demikian, router tetap dapat menjalankan fungsinya sebagai gateway jaringan tanpa mengalami gangguan yang signifikan.

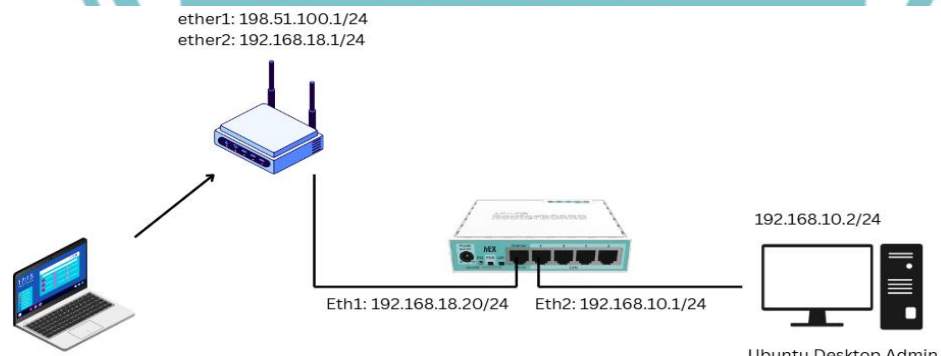


Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Rancangan topologi jaringan pada penelitian ini disusun melalui dua tahapan, yaitu tahap pengembangan (development) dan tahap implementasi. Pada tahap pengembangan, sistem keamanan jaringan terlebih dahulu diterapkan dan diuji pada lingkungan server virtual untuk memastikan konfigurasi dapat berjalan dengan baik tanpa mengganggu jaringan operasional. Setelah hasil pengujian menunjukkan sistem bekerja sesuai dengan tujuan penelitian, konfigurasi yang sama kemudian diimplementasikan pada perangkat jaringan yang digunakan oleh PT XYZ. Topologi jaringan yang digunakan pada tahap pengembangan dan implementasi memiliki struktur yang serupa agar hasil pengujian tetap relevan dengan kondisi jaringan sebenarnya.

Pada topologi Gambar 3.3, setiap perangkat memiliki peran dan fungsi yang berbeda sesuai dengan kebutuhan pengujian. Perangkat penyerang menggunakan laptop dengan sistem operasi Kali Linux. Kali Linux dipilih karena menyediakan berbagai tools pengujian keamanan jaringan yang digunakan untuk mensimulasikan serangan DDoS. Pada lingkungan simulasi, jalur dari sisi luar jaringan direpresentasikan melalui router upstream/modem virtual sebelum trafik diteruskan ke router MikroTik utama yang menjadi objek penelitian.



Gambar 3. 3 Topologi Simulasi

Tool utama yang digunakan pada perangkat penyerang adalah hping3, yang berfungsi untuk menghasilkan trafik serangan berupa



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

UDP *Flood* dan TCP *SYN Flood*. Tool ini memungkinkan pengiriman paket jaringan dalam jumlah besar secara terus-menerus dan terkontrol, sehingga dapat digunakan untuk mengamati respons router terhadap berbagai jenis serangan DDoS.

Router MikroTik pada topologi ini menggunakan sistem operasi MikroTik RouterOS dan berfungsi sebagai objek utama penelitian. Router ini menerima lalu lintas dari jaringan luar melalui interface Ether1 dan meneruskan atau memblokir paket berdasarkan konfigurasi keamanan yang diterapkan. Pada perangkat ini dilakukan penerapan metode mitigasi serangan DDoS, yaitu *Firewall RAW*, *Rate Limiting*, dan *Port Hardening*, yang bertujuan untuk menyaring trafik berbahaya sebelum membebani sumber daya router.

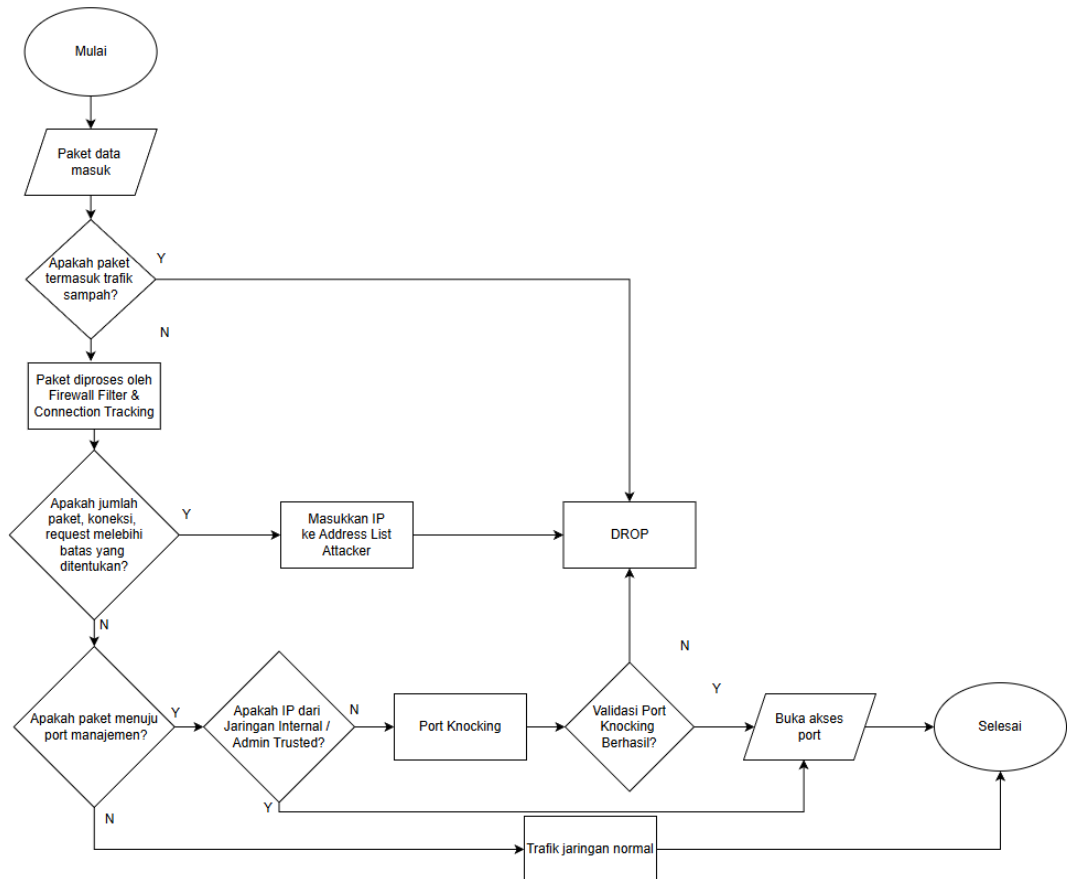
Di sisi jaringan lokal, komputer admin menggunakan sistem operasi Ubuntu Desktop dan terhubung ke router melalui interface Ether2. Komputer ini berfungsi sebagai perangkat pemantau selama proses pengujian berlangsung. Melalui komputer admin, dilakukan pemantauan kondisi router seperti penggunaan CPU, lalu lintas jaringan, serta memastikan bahwa koneksi jaringan lokal tetap berjalan normal saat router menerima serangan dari jaringan luar.

Dengan pembagian peran tersebut, topologi jaringan ini memungkinkan proses pengujian dilakukan secara terstruktur. Simulasi serangan dapat dilakukan dari sisi luar jaringan menggunakan *Kali Linux*, sementara efektivitas mekanisme mitigasi dapat diamati langsung pada router MikroTik melalui komputer admin. Pendekatan ini memastikan bahwa proses pengujian mencerminkan kondisi serangan yang realistis tanpa mengganggu jaringan operasional PT XYZ.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



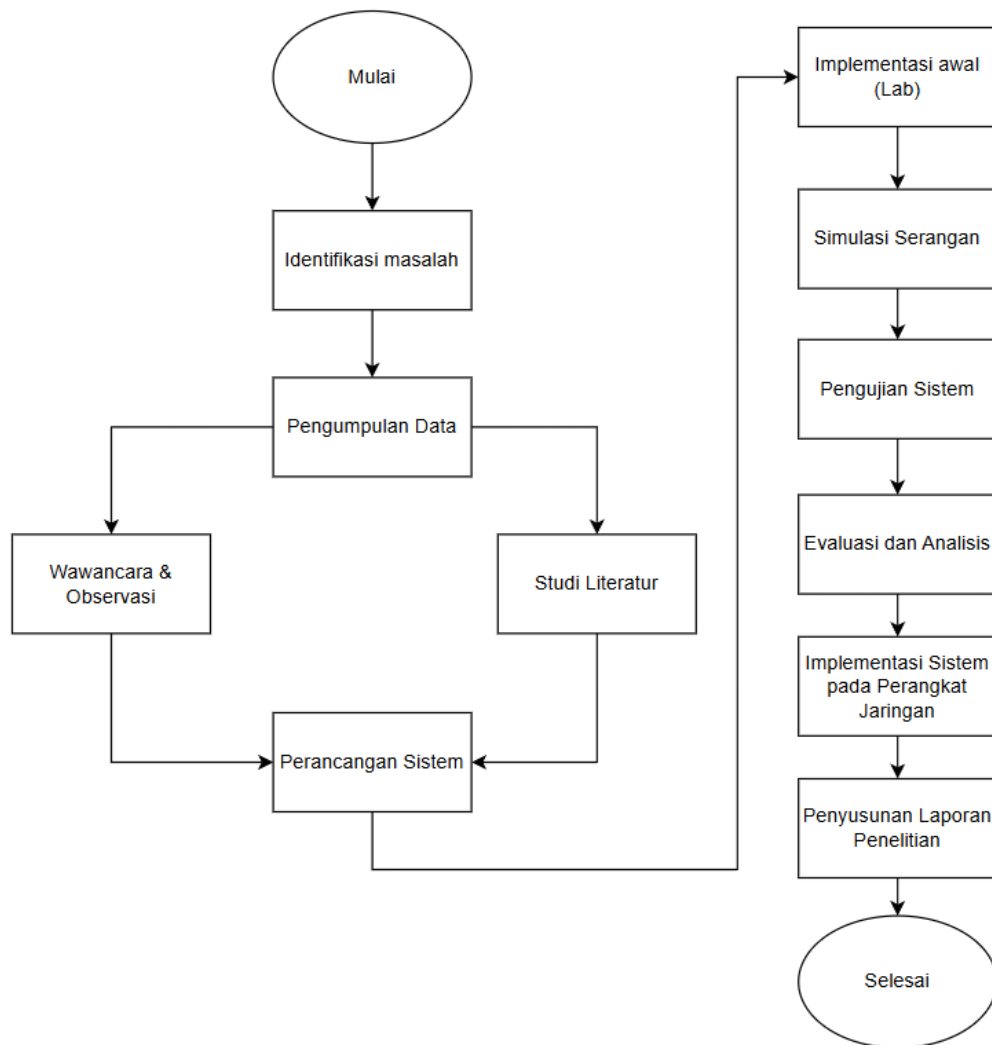
Gambar 3. 4 Flowchart Proses Mitigasi Serangan DDoS

Flowchart ini menunjukkan alur pemrosesan paket data pada router MikroTik untuk menjaga keamanan jaringan dari trafik tidak wajar. Paket yang masuk terlebih dahulu diperiksa untuk menentukan apakah termasuk trafik sampah atau melebihi batas koneksi yang ditetapkan. Paket yang terindikasi berbahaya akan langsung ditolak, sedangkan paket normal diproses lebih lanjut. Jika paket tidak mengarah ke port manajemen router, maka paket diteruskan sebagai trafik jaringan biasa.

Apabila paket mengarah ke port manajemen, sistem akan memeriksa apakah alamat IP berasal dari jaringan internal atau administrator terpercaya. Akses dari alamat IP tersebut akan langsung diizinkan. Namun, jika akses berasal dari jaringan luar, sistem menerapkan mekanisme *port knocking* sebagai proses validasi tambahan. *Port*

knocking dilakukan dengan mengakses port tertentu sesuai urutan yang telah ditentukan. Jika validasi berhasil, akses port manajemen dibuka sementara untuk alamat IP tersebut, sedangkan jika gagal, akses akan ditolak.

3.2 Tahapan Penelitian



Gambar 3. 5 Tahapan Penelitian

Tahapan penelitian ini menjelaskan langkah-langkah yang dilakukan dalam proses penelitian secara umum. Setiap tahapan disusun secara berurutan agar penelitian dapat berjalan dengan terstruktur dan menghasilkan hasil yang sesuai dengan tujuan penelitian. Penjelasan

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

tahapan penelitian berdasarkan flowchart pada Gambar 3.5 adalah sebagai berikut:

1. Identifikasi Masalah

Identifikasi masalah merupakan tahap awal dalam penelitian. Pada tahap ini dilakukan penentuan permasalahan yang akan diteliti berdasarkan kondisi yang ada dan kebutuhan yang ditemukan. Permasalahan yang telah ditentukan kemudian dirumuskan agar memiliki ruang lingkup yang jelas. Tujuan dari tahap ini adalah memastikan bahwa penelitian memiliki fokus yang terarah sebagai dasar dalam pelaksanaan tahapan selanjutnya.

2. Pengumpulan Data

Pengumpulan data merupakan langkah penting dalam memperoleh informasi yang dibutuhkan untuk mendukung penelitian. Data dikumpulkan melalui beberapa metode, antara lain wawancara, observasi, dan studi literatur. Wawancara digunakan untuk memperoleh informasi dan pemahaman dari narasumber yang berkaitan dengan objek penelitian. Observasi dilakukan untuk mengetahui kondisi secara langsung di lingkungan penelitian. Selain itu, studi literatur dilakukan dengan mempelajari sumber-sumber tertulis seperti buku, jurnal, dan penelitian sebelumnya yang relevan, sehingga dapat digunakan sebagai dasar dalam penyusunan penelitian.

3. Wawancara dan Observasi

Wawancara merupakan proses penggalan informasi yang dilakukan dengan narasumber untuk memperoleh data yang berkaitan dengan permasalahan penelitian. Sementara itu, observasi merupakan kegiatan pengamatan secara langsung terhadap kondisi yang ada di lokasi penelitian. Kedua metode ini digunakan untuk mendapatkan gambaran yang lebih jelas

mengenai objek penelitian serta mendukung proses analisis pada tahap selanjutnya.

4. Perancangan Sistem

Pada tahap perancangan sistem, disusun rancangan solusi berdasarkan hasil identifikasi masalah dan data yang telah dikumpulkan. Perancangan meliputi penentuan metode, alur kerja sistem, serta mekanisme yang akan diterapkan. Tahap ini bertujuan untuk menghasilkan desain sistem yang siap untuk diimplementasikan.

5. Implementasi Awal (Laboratorium)

Implementasi awal dilakukan pada lingkungan uji atau laboratorium. Pada tahap ini, rancangan sistem yang telah dibuat diterapkan pada perangkat atau simulasi jaringan untuk memastikan konfigurasi dapat berjalan dengan baik dan sesuai dengan perencanaan.

6. Simulasi Serangan

Simulasi serangan dilakukan untuk menguji sistem yang telah diimplementasikan. Tahap ini bertujuan untuk melihat respons sistem terhadap kondisi yang tidak normal, seperti serangan jaringan, serta memastikan mekanisme pengamanan dapat bekerja dengan baik.

7. Pengujian Sistem

Pengujian sistem dilakukan untuk mengetahui kinerja sistem secara keseluruhan. Pengujian dilakukan dengan mengamati kondisi sistem sebelum, saat, dan setelah simulasi dilakukan, guna memastikan sistem dapat berfungsi sesuai dengan tujuan penelitian.

8. Evaluasi dan Analisis

Pada tahap evaluasi dan analisis, dilakukan penilaian terhadap hasil pengujian sistem mitigasi serangan DDoS yang telah diterapkan. Analisis difokuskan pada kondisi kinerja perangkat

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

router MikroTik, khususnya pada penggunaan CPU dan lalu lintas jaringan (bandwidth/traffic).

9. Implementasi Sistem pada Perangkat Jaringan

Setelah sistem dinyatakan berjalan dengan baik pada tahap pengujian, sistem dapat diterapkan pada perangkat jaringan yang digunakan sebagai objek penelitian. Tahap ini bertujuan untuk memastikan sistem dapat digunakan pada lingkungan sebenarnya.

10. Penyusunan Laporan Penelitian

Tahap terakhir adalah penyusunan laporan penelitian. Laporan disusun berdasarkan seluruh proses dan hasil penelitian yang telah dilakukan, mulai dari perumusan masalah hingga kesimpulan dan saran.

3.3 Objek Penelitian

Penelitian ini berfokus pada penerapan sistem mitigasi serangan *Distributed Denial of Service* (DDoS) pada perangkat router MikroTik yang digunakan oleh PT XYZ dalam menyediakan layanan internet *WiFi* kepada pelanggan. Perangkat MikroTik tersebut ditempatkan di beberapa titik jaringan yang berada di wilayah kota dan daerah pelanggan, sehingga memiliki peran penting dalam menjaga kelancaran layanan jaringan.

Metode mitigasi yang diterapkan dalam penelitian ini meliputi penggunaan *Firewall RAW*, *Rate Limiting*, dan *Port Hardening*. *Firewall RAW* digunakan untuk menyaring dan menghentikan trafik yang tidak wajar sebelum diproses lebih lanjut oleh sistem router. *Rate Limiting* diterapkan untuk membatasi jumlah paket atau koneksi dari satu alamat IP agar tidak menyebabkan kelebihan beban pada perangkat. Selain itu, *Port Hardening* digunakan untuk mengamankan akses manajemen router dengan membatasi port yang dapat diakses, sehingga mengurangi risiko penyalahgunaan akses dari pihak yang tidak berwenang.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Tujuan dari penerapan metode tersebut adalah untuk meningkatkan keamanan dan kestabilan perangkat MikroTik, serta memastikan sistem mitigasi yang diterapkan mampu menangani serangan DDoS secara efektif. Dengan adanya sistem ini, diharapkan layanan jaringan PT XYZ tetap berjalan dengan baik meskipun terjadi serangan DDoS.

3.4 Teknik Analisis Data

Pada penelitian ini, analisis difokuskan pada kinerja router MikroTik saat menerima serangan DDoS serta setelah diterapkan mekanisme mitigasi secara bertahap. Parameter utama yang dianalisis meliputi penggunaan *CPU Load*, *Free Memory*, serta lalu lintas jaringan (total trafik masuk dan jumlah paket yang diblokir). Pemilihan parameter ini didasarkan pada karakteristik serangan *DDoS* yang secara langsung membebani sumber daya router dan menyebabkan kepadatan trafik pada interface jaringan.

Analisis dilakukan melalui pendekatan evaluasi per-layer resource efficiency, yaitu dengan menguji kinerja router dalam beberapa skenario bertahap: (1) tanpa mitigasi DDoS, (2) Firewall RAW aktif, (3) Firewall RAW dikombinasikan dengan Rate Limiting, serta (4) simulasi RTBH sebagai pembanding. Adapun Port Hardening diuji secara terpisah melalui pengujian akses layanan manajemen router, karena metode ini berfokus pada pengamanan management plane dan tidak secara langsung memengaruhi parameter *CPU Load*, *Free Memory*, maupun traffic jaringan pada pengujian flood.

Penggunaan *CPU* dan *Free Memory* diamati selama serangan *DDoS* jenis *TCP SYN Flood* dan *UDP Flood* berlangsung dalam setiap skenario pengujian. Data yang diperoleh dibandingkan untuk melihat penurunan beban CPU dan peningkatan ketersediaan memori setelah setiap lapisan keamanan diterapkan. Dengan demikian, dapat diketahui lapisan mana yang memberikan dampak paling signifikan terhadap stabilitas perangkat.

**Hak Cipta :**

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Selain itu, analisis lalu lintas jaringan dilakukan dengan memantau trafik pada interface router, termasuk peningkatan trafik masuk dan jumlah paket yang berhasil diblokir oleh sistem. Perbandingan antar skenario digunakan untuk menilai efektivitas mekanisme mitigasi dalam mengurangi lonjakan trafik akibat serangan DDoS.

Sebagai tambahan, dilakukan simulasi sederhana metode Remotely Triggered Black Hole (RTBH) dengan mengamati perubahan trafik yang dibuang melalui mekanisme blackhole route pada MikroTik. Pengamatan ini bertujuan untuk memahami dampak pembuangan trafik secara langsung terhadap beban jaringan tanpa melibatkan implementasi RTBH secara nyata pada level upstream.

Hasil analisis CPU, memori, dan trafik jaringan kemudian digunakan sebagai dasar untuk mengevaluasi efektivitas dan efisiensi masing-masing mekanisme mitigasi dalam menjaga kestabilan kinerja router MikroTik secara terukur dan sistematis.



**POLITEKNIK
NEGERI
JAKARTA**

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB IV

HASIL DAN PEMBAHASAN

4.1 Analisis Kebutuhan

Pada penelitian ini, analisis kebutuhan dilakukan untuk mengidentifikasi perangkat keras dan perangkat lunak yang digunakan dalam proses simulasi dan pengujian sistem. Seluruh kebutuhan disusun untuk mendukung implementasi jaringan berbasis virtual, sehingga pengujian dapat dilakukan secara terkontrol tanpa mengganggu jaringan nyata. Adapun rincian kebutuhan perangkat yang digunakan dalam penelitian ini disajikan pada tabel berikut.

Tabel 4. 1 Kebutuhan Perangkat

No	Nama Perangkat / Software	Spesifikasi	Keterangan
1	Laptop	RAM 8 GB, Processor i5, Storage 20 GB	Digunakan untuk menjalankan seluruh simulasi
2	VirtualBox	Version 7.0.24 r167081	Digunakan sebagai media virtualisasi
3	MikroTik CHR 1	Base Memory 2048 MB, Processor 4 CPU, Execution Cap 100%.	Digunakan sebagai router upstream/modem simulasi
4	MikroTik CHR 2	Base Memory 256 MB, Processor 1 CPU, Execution Cap 30%.	Digunakan sebagai router utama pada tahap implementasi awal/laboratorium

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Nama Perangkat / Software	Spesifikasi	Keterangan
5	Router MikroTik fisik	Perangkat MikroTik milik PT XYZ	Digunakan sebagai router utama pada tahap pengujian akhir
6	Kali Linux	Base Memory 4096 MB, Processor 5 CPU, Execution Cap 100%.	Digunakan sebagai mesin attacker
7	Ubuntu Desktop	Base Memory 6039 MB, Processor 6 CPU, Execution Cap 100%.	Digunakan sebagai perangkat client/admin untuk konfigurasi dan monitoring.
7	hping3	Tools bawaan Kali Linux	Digunakan untuk simulasi serangan DDoS
8	Winbox	Winbox 64bit v3.43	Digunakan untuk konfigurasi MikroTik
9	Jaringan Virtual	Internal Network / Host-only	Digunakan untuk menghubungkan antar VM

Berdasarkan Tabel 4.1, perangkat yang digunakan dalam penelitian dibagi menjadi dua kelompok utama, yaitu perangkat virtual untuk tahap implementasi awal dan perangkat fisik untuk pengujian akhir. Penggunaan MikroTik CHR dilakukan untuk memastikan konfigurasi dapat berjalan pada lingkungan laboratorium, sedangkan router MikroTik fisik digunakan pada tahap pengujian akhir agar hasil pengamatan lebih mendekati kondisi perangkat yang digunakan oleh pihak PT XYZ. Dengan susunan perangkat tersebut, proses

implementasi dan pengujian dapat dilakukan secara terkontrol tanpa mengganggu jaringan operasional perusahaan.

4.1.1 Analisis Kebutuhan Firewall Raw

Analisis kebutuhan *Firewall RAW* pada penelitian ini disusun berdasarkan informasi dari pihak teknis PT XYZ mengenai kebutuhan mitigasi trafik DDoS pada router MikroTik. Berdasarkan hasil wawancara, serangan DDoS yang pernah terjadi menyebabkan penggunaan CPU router meningkat hingga 100% dan memori cepat terkuras. Kondisi tersebut menunjukkan bahwa router mengalami *resource exhaustion* akibat memproses trafik dalam jumlah besar secara terus-menerus. Berdasarkan kondisi tersebut, *Firewall RAW* dibutuhkan sebagai mekanisme penyaringan awal terhadap trafik yang masuk ke router. *Firewall RAW* bekerja sebelum paket masuk ke proses *connection tracking*, sehingga trafik yang terindikasi sebagai serangan dapat dibuang lebih awal dan tidak membebani tahapan pemrosesan paket berikutnya. Kebutuhan *Firewall RAW* disesuaikan dengan batasan penelitian, yaitu serangan *UDP Flood* dan *TCP SYN Flood*. *UDP Flood* dipilih karena dapat menghasilkan trafik besar yang membebani *bandwidth* dan sumber daya router, sedangkan *TCP SYN Flood* membebani router melalui banyaknya permintaan koneksi baru pada proses awal komunikasi TCP.

Pada penelitian ini, *Firewall RAW* dikombinasikan dengan deteksi awal menggunakan *firewall filter*. Deteksi tersebut digunakan untuk mengenali trafik *UDP Flood* dan *TCP SYN Flood* yang melewati batas tertentu. IP sumber yang terindikasi sebagai *attacker* akan dimasukkan secara dinamis ke dalam *address-list* ddos-attackers, kemudian trafik lanjutan dari IP tersebut dibuang oleh *Firewall RAW* pada tahap awal pemrosesan paket.

Dengan demikian, kebutuhan utama *Firewall RAW* dalam penelitian ini adalah sebagai lapisan mitigasi awal untuk membuang trafik dari

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

sumber serangan yang telah teridentifikasi. Mekanisme ini diharapkan dapat membantu menjaga efisiensi penggunaan CPU dan memori router MikroTik selama pengujian serangan DDoS berlangsung.

4.1.2 Analisis Kebutuhan Rate Limiting

Pada penelitian ini, *Rate Limiting* dibutuhkan untuk membatasi trafik yang masuk ke router MikroTik agar tidak melebihi kemampuan pemrosesan perangkat. Kebutuhan ini didasarkan pada karakteristik serangan DDoS yang mengirimkan paket secara terus-menerus, sehingga dapat meningkatkan CPU Load, mengurangi Free Memory, dan menyebabkan kepadatan trafik jaringan.

Berdasarkan informasi dari pihak teknis PT XYZ, pembatasan trafik pada MikroTik perlu disesuaikan dengan kondisi trafik normal pelanggan agar tidak mengganggu pengguna yang sah. Oleh karena itu, nilai batas yang digunakan pada penelitian ini ditentukan untuk kebutuhan pengujian di lingkungan laboratorium dan tidak dijadikan standar tetap untuk jaringan operasional PT XYZ.

Rate Limiting pada penelitian ini digunakan sebagai lapisan mitigasi setelah *Firewall RAW*. *Firewall RAW* berfungsi membuang trafik dari sumber yang sudah terindikasi sebagai *attacker*, sedangkan *Rate Limiting* berfungsi membatasi trafik berlebih yang masih diproses oleh router. Dengan demikian, *Rate Limiting* tidak menggantikan peran *Firewall RAW*, tetapi menjadi mekanisme pelengkap agar trafik yang masih lolos tetap berada dalam batas wajar.

Kebutuhan *Rate Limiting* disesuaikan dengan fokus penelitian, yaitu serangan *UDP Flood* dan *TCP SYN Flood*. Pada *TCP SYN Flood*, pembatasan dilakukan untuk mengurangi paket SYN berlebih dari satu sumber IP. Sementara itu, pada *UDP Flood*, pembatasan digunakan untuk mengendalikan trafik UDP agar tidak memenuhi *bandwidth* dan membebani router. Selain itu, penerapan *Rate Limiting* setelah *Firewall*

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

RAW digunakan untuk mengontrol trafik yang masih lolos dari penyaringan awal tanpa langsung memutus seluruh layanan.

Dengan demikian, *Rate Limiting* berperan sebagai pembatas terhadap trafik yang masih diproses oleh router setelah tahap penyaringan awal. Pembatasan TCP SYN dan UDP digunakan agar router tidak menerima beban berlebih dari satu sumber IP. Nilai batas pada tahap pengujian tetap disesuaikan dengan kebutuhan laboratorium dan tidak merepresentasikan nilai final pada jaringan operasional PT XYZ.

4.1.3 Analisis Kebutuhan Port Hardening

Berdasarkan konfirmasi dengan pihak teknis PT XYZ, layanan manajemen pada MikroTik hanya menggunakan beberapa *service* tertentu. Pada kondisi awal, *Winbox* aktif pada port 7090 dan Telnet aktif pada port 2332, sedangkan SSH MikroTik pada port 2222 masih nonaktif. Layanan lain seperti API, API-SSL, FTP, WWW, dan WWW-SSL juga berada dalam kondisi nonaktif. Informasi ini digunakan sebagai dasar perancangan *Port Hardening* agar konfigurasi yang diterapkan tetap menyesuaikan kondisi layanan PT XYZ.

Status layanan manajemen MikroTik sebelum penerapan *Port Hardening* dirangkum pada Tabel 4.2.

Tabel 4. 2 Status Existing Layanan Manajemen MikroTik

Layanan	Port	Status Existing
API	8728	Nonaktif
API-SSL	8729	Nonaktif
FTP	21	Nonaktif
SSH MikroTik	2222	Nonaktif
Telnet	2332	Aktif
Winbox	7090	Aktif
WWW	80	Nonaktif
WWW-SSL	443	Nonaktif

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Berdasarkan Tabel 4.2, sebagian besar layanan yang tidak digunakan sudah nonaktif. Namun, Telnet masih aktif, sementara SSH belum digunakan. Kondisi ini menjadi dasar kebutuhan *Port Hardening*, yaitu menonaktifkan layanan yang tidak diperlukan, mengganti akses terminal Telnet dengan SSH, dan membatasi akses manajemen agar tidak terbuka bebas dari sisi luar jaringan.

Dengan demikian, kebutuhan utama *Port Hardening* adalah mengurangi permukaan serangan pada layanan manajemen MikroTik. Konfigurasi tetap menyesuaikan kebutuhan akses PT XYZ, tetapi dibuat lebih aman melalui pembatasan layanan dan validasi tambahan untuk akses dari luar jaringan.

4.1.4 Analisis Kebutuhan RTBH

Pada penelitian ini, *Remotely Triggered Black Hole* atau RTBH dibutuhkan sebagai skenario tambahan untuk memahami mekanisme mitigasi DDoS berbasis *routing*. Berbeda dengan *Firewall RAW* dan *Rate Limiting* yang bekerja dengan menyaring atau membatasi trafik, RTBH bekerja dengan mengarahkan trafik menuju IP target ke jalur *blackhole* agar trafik tersebut dibuang sebelum membebani jaringan utama.

Berdasarkan konfirmasi dengan pihak teknis PT XYZ, penerapan RTBH tidak dapat dilakukan langsung dari sisi internal perusahaan karena memerlukan izin, koordinasi, dan dukungan dari ISP atau pihak *upstream*, terutama jika menggunakan mekanisme *routing* seperti BGP. Selain itu, RTBH memiliki keterbatasan karena tidak membedakan trafik serangan dan trafik normal. Ketika *blackhole route* diterapkan, seluruh trafik menuju IP target akan ikut terbang, termasuk trafik dari pengguna yang sah.

Oleh karena itu, RTBH pada penelitian ini tidak dijadikan metode utama mitigasi. Metode utama tetap difokuskan pada *Firewall RAW*,

Rate Limiting, dan *Port Hardening* karena ketiga metode tersebut masih berupaya menjaga layanan bagi trafik normal. RTBH digunakan sebagai simulasi langkah terakhir apabila trafik serangan sudah sangat membebani jaringan dan mekanisme mitigasi utama tidak lagi mampu menahan dampak serangan secara optimal.

Dengan demikian, kebutuhan RTBH dalam penelitian ini adalah untuk menggambarkan mekanisme pembuangan trafik pada level *routing* menggunakan fitur *blackhole route* MikroTik. Simulasi ini tidak menggantikan metode mitigasi utama, tetapi menunjukkan skenario darurat ketika seluruh trafik menuju IP target perlu dihentikan dari sisi *upstream* untuk mencegah beban lebih lanjut pada router utama. Konsekuensinya, seluruh trafik menuju IP target, baik trafik normal maupun trafik serangan, akan ikut terbangun selama *blackhole route* aktif.

4.2 Perancangan Sistem

4.2.1 Perancangan Topologi Sistem

Topologi sistem pada penelitian ini disusun berdasarkan rancangan yang telah dijelaskan pada Bab III. Topologi dibangun dalam lingkungan simulasi dan terdiri dari empat komponen utama, yaitu perangkat *attacker*, router *upstream* atau modem simulasi, router MikroTik utama sebagai objek pengujian, serta komputer admin sebagai perangkat monitoring.

Perangkat *attacker* menggunakan Kali Linux untuk menghasilkan trafik serangan DDoS. Trafik dari Kali Linux diarahkan menuju IP publik pada router *upstream* atau modem simulasi, kemudian diteruskan ke router MikroTik utama. Keberadaan router *upstream* digunakan untuk merepresentasikan jalur trafik dari jaringan luar sebelum masuk ke router yang dilindungi.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pada tahap perancangan, MikroTik CHR utama digunakan sebagai perangkat validasi konfigurasi di lingkungan laboratorium. Setelah konfigurasi sesuai rancangan, peran router utama pada tahap pengujian akhir digantikan oleh perangkat MikroTik fisik milik PT XYZ. Router utama memiliki dua *interface*, yaitu ether1 sebagai jalur WAN yang terhubung ke router *upstream*, dan ether2 sebagai jalur LAN yang terhubung ke komputer admin.

Komputer admin berada pada jaringan lokal dan digunakan untuk konfigurasi serta monitoring selama pengujian berlangsung. Melalui perangkat ini, dilakukan pengamatan terhadap CPU, memori, trafik jaringan, dan rule mitigasi yang diterapkan pada router MikroTik utama.

Dengan rancangan tersebut, alur trafik pengujian dimulai dari Kali Linux sebagai sumber serangan, melewati router *upstream*, kemudian diteruskan ke *interface* WAN router MikroTik utama. Topologi ini digunakan agar proses pengujian dapat berjalan terstruktur dan tetap merepresentasikan alur serangan dari jaringan luar menuju router utama yang dilindungi.

4.2.2 Perancangan Alur Mitigasi

Perancangan alur mitigasi pada penelitian ini disusun menggunakan pendekatan *defense-in-depth*, yaitu penerapan beberapa lapisan keamanan yang bekerja secara bertahap dalam memproses trafik jaringan. Trafik dari perangkat *attacker* masuk melalui *interface* publik router, kemudian diperiksa oleh *Firewall RAW* sebagai penyaring awal. Mekanisme ini digunakan untuk membuang trafik yang terindikasi sebagai serangan sebelum masuk ke proses *connection tracking*, sehingga beban pemrosesan router dapat dikurangi sejak tahap awal.

Trafik yang masih lolos dari penyaringan awal akan diproses oleh *Rate Limiting* untuk membatasi paket atau koneksi dari sumber tertentu agar



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

tidak melebihi ambang batas yang ditentukan. Selain itu, *Port Hardening* diterapkan untuk mengamankan akses layanan manajemen router dengan membatasi port administrasi dan sumber akses yang diizinkan. Dengan alur tersebut, setiap metode memiliki peran yang saling melengkapi, yaitu *Firewall RAW* sebagai penyaring awal, *Rate Limiting* sebagai pembatas trafik berlebih, dan *Port Hardening* sebagai pengamanan akses manajemen router.

4.2.3 Perancangan Firewall RAW

Pada penelitian ini, *Firewall RAW* dirancang sebagai lapisan mitigasi awal untuk menangani trafik DDoS pada router MikroTik. Mekanisme ini dipilih karena bekerja pada fase *prerouting*, sehingga trafik dari sumber yang telah teridentifikasi sebagai *attacker* dapat dibuang sebelum masuk ke proses *connection tracking*. Dengan cara ini, paket serangan tidak perlu diproses lebih jauh oleh router.

Perancangan *Firewall RAW* difokuskan pada dua jenis serangan sesuai batasan penelitian, yaitu *UDP Flood* dan *TCP SYN Flood*. Kedua serangan tersebut berpotensi meningkatkan CPU Load, penggunaan memori, dan kepadatan trafik apabila tidak ditangani sejak tahap awal.

Dalam rancangan ini, sumber serangan tidak diasumsikan selalu diketahui sejak awal. Oleh karena itu, digunakan mekanisme deteksi awal melalui *firewall filter* untuk mengenali trafik UDP atau paket TCP SYN yang melebihi batas tertentu. IP sumber yang terindikasi sebagai penyerang akan dimasukkan secara otomatis ke dalam *address-list* *ddos-attackers*.

Setelah IP masuk ke dalam *address-list* *ddos-attackers*, *Firewall RAW* akan melakukan aksi *drop* terhadap trafik lanjutan dari IP tersebut pada *chain prerouting*. Dengan pembagian ini, *firewall filter* digunakan secara terbatas untuk deteksi awal, sedangkan proses pemblokiran



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

utama dilakukan oleh *Firewall RAW* agar trafik serangan dapat dibuang lebih cepat.

Penentuan ambang batas deteksi *Firewall RAW* disusun berdasarkan kebutuhan PT XYZ, acuan penelitian terdahulu, dan hasil penyesuaian pada lingkungan pengujian. Penelitian Riduan et al. (2025) menjadi acuan bahwa *Firewall RAW* efektif digunakan untuk menangani trafik DDoS seperti *TCP Flood* dan *UDP Flood*, tetapi penelitian tersebut tidak menetapkan nilai ambang batas yang berlaku untuk semua kondisi jaringan.

Berdasarkan hasil kalibrasi dengan mengamati CPU Load, Free Memory, *traffic WAN*, dan *counter firewall*, ambang deteksi pada penelitian ini ditetapkan sebesar 100 *packet/detik* untuk *TCP SYN Flood* dan 200 *packet/detik* untuk *UDP Flood*. Nilai tersebut digunakan untuk mengenali trafik berintensitas tinggi sebagai serangan, sehingga IP sumber dapat dimasukkan ke dalam *address-list ddos-attackers* dan trafik lanjutannya dibuang oleh *Firewall RAW*.

Dengan demikian, *Firewall RAW* berperan sebagai mekanisme pemblokiran awal terhadap trafik dari sumber serangan yang telah terdeteksi. Rancangan ini diharapkan dapat membantu menjaga efisiensi penggunaan sumber daya router saat menghadapi *UDP Flood* dan *TCP SYN Flood* pada lingkungan pengujian

4.2.4 Perancangan Rate Limiting

Rate Limiting pada penelitian ini dirancang sebagai lapisan mitigasi setelah *Firewall RAW*. Berdasarkan informasi dari pihak teknis PT XYZ, pembatasan trafik perlu disesuaikan dengan pola trafik normal pelanggan agar tidak mengganggu pengguna yang sah. Pada rancangan sistem, *Firewall RAW* digunakan untuk membuang trafik dari sumber yang telah terdeteksi sebagai *attacker*, sedangkan *Rate Limiting*



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

digunakan untuk membatasi trafik berlebih yang masih diproses oleh router.

Perancangan *Rate Limiting* difokuskan pada trafik TCP SYN dan UDP. Pembatasan TCP SYN digunakan untuk mengurangi permintaan koneksi awal TCP yang dikirim secara berlebihan dari satu sumber IP, sedangkan pembatasan UDP digunakan untuk mengurangi lonjakan paket UDP yang dapat memenuhi *bandwidth* dan membebani router. Dengan rancangan ini, trafik yang masih lolos dari penyaringan awal dapat dikendalikan tanpa langsung memutus seluruh layanan.

Rate Limiting tidak menggantikan peran *Firewall RAW*, tetapi menjadi mekanisme pelengkap. *Firewall RAW* menangani trafik dari sumber yang sudah terdeteksi sebagai *attacker*, sedangkan *Rate Limiting* menjaga agar trafik yang masih diproses router tetap berada dalam batas yang dapat ditangani. Dengan demikian, kedua metode ini bekerja secara berlapis dalam proses mitigasi serangan DDoS.

Nilai batas *Rate Limiting* ditentukan berdasarkan kebutuhan PT XYZ, acuan penelitian terdahulu, dan hasil penyesuaian pada lingkungan pengujian. Pada penelitian Hendry (2024), trafik SYN *Flood* dengan jumlah lebih dari 200 *packet*/detik digunakan sebagai indikator trafik yang perlu diblokir. Berdasarkan acuan tersebut dan hasil pengujian, batas *Rate Limiting* pada penelitian ini ditetapkan sebesar 40 *packet*/detik untuk TCP SYN dan 80 *packet*/detik untuk UDP.

Nilai *Rate Limiting* dibuat lebih rendah dibandingkan ambang deteksi *Firewall RAW* agar trafik yang mulai berlebih dapat dibatasi terlebih dahulu. Sementara itu, trafik dengan intensitas lebih tinggi akan dikategorikan sebagai serangan dan IP sumbernya dimasukkan ke dalam *address-list* ddos-attackers. Nilai tersebut digunakan untuk kebutuhan pengujian dan tidak dijadikan standar tetap untuk jaringan operasional PT XYZ.

4.2.5 Perancangan Port Hardening

Port Hardening pada penelitian ini dirancang untuk mengamankan akses manajemen router MikroTik. Berbeda dengan *Firewall RAW* dan *Rate Limiting* yang berfokus pada trafik DDoS, *Port Hardening* bertujuan mengurangi permukaan serangan dengan membatasi layanan, port, dan sumber akses yang dapat terhubung ke router.

Berdasarkan informasi dari pihak teknis PT XYZ, layanan manajemen yang aktif pada kondisi awal adalah *Winbox* pada port 7090 dan Telnet pada port 2332. Sementara itu, SSH MikroTik pada port 2222 masih nonaktif, sedangkan API, API-SSL, FTP, WWW, dan WWW-SSL juga tidak digunakan. Dari kondisi tersebut, rancangan *Port Hardening* dilakukan dengan menonaktifkan layanan yang tidak diperlukan, mempertahankan *Winbox* dengan pembatasan akses, serta mengganti Telnet dengan SSH karena SSH menyediakan komunikasi yang lebih aman.

Selain pembatasan layanan, penelitian ini menerapkan *port knocking* sebagai validasi tambahan untuk akses dari luar jaringan. Mekanisme ini mengharuskan sumber koneksi mengakses port tertentu secara berurutan. Jika urutan sesuai, IP sumber akan dimasukkan sementara ke dalam *address-list* secured-admin dan diberi akses ke layanan manajemen. Jika urutan tidak sesuai, akses tetap ditolak.

Rangkuman rancangan *Port Hardening* ditunjukkan pada Tabel 4.3.

Tabel 4. 3 Rancangan Port Hardening

No	Mekanisme	Kondisi Existing	Rancangan Port Hardening
1	Disable service tidak digunakan	API, API-SSL, FTP, WWW, WWW-SSL nonaktif	Tetap dinonaktifkan

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Mekanisme	Kondisi Existing	Rancangan Port Hardening
2	Winbox	Aktif pada port 7090	Tetap aktif, dibatasi hanya dari IP admin/internal
3	Telnet	Aktif pada port 2332	Direkomendasikan dinonaktifkan
4	SSH MikroTik	Nonaktif pada port 2222	Diaktifkan sebagai pengganti Telnet dan dibatasi IP admin
5	Port default	Sebagian port sudah diganti dari default	Tetap menggunakan port non-default sesuai kebutuhan
6	IP whitelist	Perlu disesuaikan dengan IP admin	Hanya IP admin/internal yang boleh akses manajemen
7	Port knocking	Digunakan sebagai validasi tambahan pada rancangan	IP yang berhasil knocking masuk address-list sementara
8	Drop akses tidak sah	Akses luar perlu dibatasi	Trafik ke port manajemen dari IP tidak dikenal ditolak

Berdasarkan Tabel 4.3, *Port Hardening* tidak hanya dilakukan dengan menutup layanan yang tidak digunakan, tetapi juga mengatur cara akses ke layanan manajemen. Telnet dinonaktifkan karena tidak terenkripsi, sedangkan SSH digunakan sebagai akses terminal yang lebih aman. Akses dari jaringan internal tetap diizinkan, sementara akses dari luar harus melalui *port knocking* terlebih dahulu.

Pola *port knocking* pada penelitian ini mengacu pada konsep validasi bertahap dari Hendry (2024), kemudian disesuaikan dengan kebutuhan



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

penelitian. Karena Telnet tidak digunakan dalam rancangan akhir, urutan validasi dibuat menggunakan port TCP 7001, 7002, dan 7003. Setelah IP sumber berhasil melewati urutan tersebut, IP akan masuk ke *address-list* secured-admin selama waktu tertentu dan diperbolehkan mengakses SSH serta *Winbox*. Jika IP belum melewati proses *knocking*, akses manajemen dari sisi luar akan ditolak.

4.2.6 Perancangan Simulasi RTBH

Perancangan simulasi *Remotely Triggered Black Hole* atau RTBH pada penelitian ini disusun untuk menggambarkan mekanisme pembuangan trafik pada level *routing*. Berdasarkan informasi dari pihak teknis PT XYZ, RTBH tidak dapat diterapkan langsung tanpa izin dan koordinasi dengan ISP atau pihak *upstream*, terutama jika menggunakan mekanisme *routing* seperti BGP. Oleh karena itu, RTBH pada penelitian ini tidak diterapkan secara nyata, tetapi disimulasikan menggunakan fitur *blackhole route* pada MikroTik.

Pada rancangan ini, trafik menuju IP target diarahkan ke jalur *blackhole* agar paket dibuang sebelum mencapai router utama. Mekanisme ini dapat mengurangi beban pada MikroTik utama karena trafik dihentikan lebih awal pada sisi *upstream*. Namun, RTBH memiliki keterbatasan karena tidak membedakan trafik normal dan trafik serangan. Seluruh trafik menuju IP target akan ikut terbuang, sehingga layanan pada alamat tersebut tidak dapat diakses selama *blackhole route* aktif.

Pada skenario pengujian, RTBH dilakukan setelah pengujian metode utama. Trafik serangan tetap diarahkan ke IP publik modem simulasi, kemudian router *upstream* dikonfigurasi agar trafik menuju WAN MikroTik utama diarahkan ke *blackhole route*. Parameter yang diamati meliputi CPU Load, Free Memory, trafik masuk, dan kondisi layanan setelah trafik dibuang pada sisi *upstream*.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Dengan demikian, perancangan RTBH pada penelitian ini berfungsi sebagai simulasi kondisi darurat ketika trafik serangan sudah sangat membebani jaringan dan metode mitigasi utama tidak lagi mampu menahan dampak serangan secara optimal. Simulasi ini tidak merepresentasikan implementasi RTBH nyata berbasis BGP pada jaringan operasional PT XYZ, tetapi digunakan untuk memahami prinsip pembuangan trafik menggunakan *blackhole route* pada MikroTik.

4.3 Implementasi Sistem

4.3.1 Implementasi Topologi dan Konfigurasi Dasar

Implementasi topologi pada penelitian ini dilakukan melalui dua tahap. Tahap pertama merupakan implementasi awal pada lingkungan virtual berbasis VirtualBox untuk memastikan konfigurasi dasar, Firewall RAW, Rate Limiting, Port Hardening, dan simulasi RTBH dapat berjalan sesuai rancangan. Pada tahap ini digunakan empat virtual machine, yaitu Kali Linux sebagai perangkat attacker, MikroTik CHR pertama sebagai router upstream atau modem simulasi, MikroTik CHR kedua sebagai router utama sementara, dan Ubuntu Desktop sebagai perangkat client/admin. Tahap kedua merupakan pengujian akhir dengan mengganti MikroTik CHR utama menggunakan perangkat MikroTik fisik milik PT XYZ, sedangkan Kali Linux dan router upstream tetap digunakan sebagai bagian dari lingkungan pengujian.

Router upstream atau modem simulasi berfungsi sebagai penghubung antara sisi attacker dan router MikroTik utama. Perangkat ini memiliki dua interface, yaitu ether1 yang terhubung dengan Kali Linux sebagai sisi jaringan luar dan ether2 yang terhubung dengan router MikroTik utama. Trafik yang masuk menuju IP publik modem simulasi kemudian diteruskan ke alamat IP WAN router MikroTik utama melalui

konfigurasi penerusan trafik. Konfigurasi penerusan trafik pada router upstream ditunjukkan pada Gambar 4.1.

Berdasarkan Gambar 4.1, router upstream dikonfigurasi agar trafik dari

```
[admin@ModemUpstream] > ip firewall nat print
Flags: X - disabled, I - invalid; D - dynamic
0      ::: teruskan trafik
       chain=dstnat action=dst-nat to-addresses=192.168.18.20
       dst-address=198.51.100.1 log=no log-prefix=""
[admin@ModemUpstream] >
```

Gambar 4. 1 Konfigurasi Penerusan Trafik pada Router Upstream

sisi luar jaringan yang menuju IP publik modem simulasi dapat diteruskan ke alamat WAN MikroTik utama. Dengan konfigurasi ini, router MikroTik utama tetap menjadi perangkat yang menerima trafik dari sisi luar, sehingga skenario pengujian dapat menyerupai kondisi ketika router menerima beban trafik dari jaringan publik.

Pada tahap implementasi awal, MikroTik CHR utama digunakan sebagai gateway sementara untuk validasi konfigurasi. Setelah konfigurasi dinyatakan berjalan sesuai rancangan, peran MikroTik CHR utama digantikan oleh router MikroTik fisik milik PT XYZ pada tahap pengujian akhir. Router utama memiliki dua interface, yaitu ether1 sebagai interface WAN yang terhubung ke router upstream, dan ether2 sebagai interface LAN yang terhubung ke Ubuntu Desktop. Pada router utama ini diterapkan Firewall RAW, Rate Limiting, dan Port Hardening, sedangkan simulasi RTBH diterapkan pada router upstream melalui mekanisme blackhole route.

Ubuntu Desktop ditempatkan pada sisi jaringan lokal dan digunakan sebagai perangkat client/admin. Perangkat ini digunakan untuk akses administrasi, konfigurasi, dan pemantauan kondisi router MikroTik utama selama proses implementasi dan pengujian. Dengan adanya perangkat admin di sisi LAN, proses pengelolaan router dapat dilakukan tanpa membuka akses manajemen secara bebas dari sisi luar jaringan.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pembagian alamat IP pada lingkungan implementasi ditunjukkan pada Tabel 4.4. Tabel ini digunakan untuk memperjelas posisi setiap perangkat dalam topologi serta hubungan antar-interface yang digunakan pada tahap implementasi awal dan pengujian akhir.

Tabel 4. 4 Konfigurasi IP Perangkat pada Topologi Pengujian

No	Perangkat	Interface	Alamat IP	Fungsi
1	Kali Linux	Adapter WAN	198.51.100.2/24	Perangkat attacker
2	MikroTik CHR Upstream / Modem Simulasi	ether1	198.51.100.1/24	IP publik simulasi yang menjadi tujuan serangan
3	MikroTik CHR Upstream / Modem Simulasi	ether2	192.168.18.1/24	Terhubung ke MikroTik utama
4	MikroTik CHR Utama	ether1 / WAN	192.168.18.20/24	Menerima trafik yang diteruskan dari modem simulasi
5	MikroTik CHR Utama	ether2 / LAN	192.168.10.1/24	Terhubung ke jaringan lokal/admin
6	Ubuntu Desktop	Adapter LAN	192.168.10.2/24	Perangkat client/admin

Berdasarkan Tabel 4.4, trafik dari Kali Linux diarahkan ke IP publik modem simulasi 198.51.100.1, kemudian diteruskan oleh router upstream menuju alamat WAN MikroTik utama 192.168.18.20. Sementara itu, Ubuntu Desktop berada pada jaringan LAN

192.168.10.0/24 untuk kebutuhan konfigurasi dan pemantauan. Pembagian alamat IP ini menjadi dasar agar setiap perangkat dapat berkomunikasi sesuai perannya dalam topologi penelitian.

Untuk memperlihatkan bahwa alamat IP telah diterapkan pada perangkat, konfigurasi IP router *upstream* dan MikroTik utama ditunjukkan pada Gambar 4.2.

```
[admin@ModemUpstream] > ip add pr
Columns: ADDRESS, NETWORK, INTERFACE
# ADDRESS      NETWORK      INTERFACE
;;; IP publik simulasi
0 198.51.100.1/24 198.51.100.0 ether1
;;; jalur ke mikrotik utama
1 192.168.18.1/24 192.168.18.0 ether2
[admin@ModemUpstream] >
[admin@MikroTik] > ip add pr
Columns: ADDRESS, NETWORK, INTERFACE, VRF
# ADDRESS      NETWORK      INTERFACE  VRF
;;; WAN dari modem simulasi
0 192.168.18.20/24 192.168.18.0 ether1    main
;;; LAN admin
1 192.168.10.1/24 192.168.10.0 ether2    main
[admin@MikroTik] >
```

Gambar 4. 2 Konfigurasi IP Router Upstream dan MikroTik Utama

Gambar 4.2 menunjukkan bahwa router upstream memiliki alamat IP pada sisi publik dan sisi penghubung ke router utama, sedangkan MikroTik utama memiliki alamat IP pada sisi WAN dan LAN. Konfigurasi ini menjadi dasar bagi penerapan rule Firewall RAW, Rate Limiting, Port Hardening, serta simulasi RTBH pada tahap berikutnya.

Dengan topologi tersebut, proses implementasi dapat dilakukan secara bertahap dan tetap terkontrol. Tahap awal menggunakan MikroTik CHR bertujuan untuk memvalidasi konfigurasi sebelum diterapkan pada perangkat fisik. Setelah konfigurasi dasar dan seluruh lapisan mitigasi siap, pengujian akhir dilakukan pada router MikroTik fisik milik PT XYZ agar data CPU, memori, dan trafik yang diperoleh lebih mendekati kondisi perangkat nyata. Hasil konektivitas dan bukti bahwa trafik benar-benar mencapai router utama tidak dibahas pada subbab ini, tetapi dipindahkan ke pengujian fungsional pada subbab 4.4.3.

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.3.2 Implementasi Firewall RAW

Implementasi Firewall RAW dilakukan pada MikroTik utama sebagai lapisan penyaringan awal terhadap trafik serangan. Pada tahap implementasi awal, konfigurasi diterapkan terlebih dahulu pada MikroTik CHR utama di lingkungan laboratorium. Setelah konfigurasi berjalan sesuai rancangan, konfigurasi yang sama dipindahkan ke router MikroTik fisik milik PT XYZ pada tahap pengujian akhir.

Mekanisme Firewall RAW pada penelitian ini tidak hanya menggunakan rule drop secara langsung, tetapi dikombinasikan dengan deteksi awal melalui firewall filter. Deteksi awal digunakan karena alamat IP sumber serangan tidak selalu diketahui sejak awal. Oleh karena itu, trafik dari sisi luar yang masuk melalui interface ether1 diperiksa berdasarkan jenis serangan yang menjadi fokus penelitian, yaitu UDP Flood dan TCP SYN Flood.

Apabila suatu alamat IP mengirimkan trafik melebihi ambang batas yang ditentukan, IP sumber tersebut akan dimasukkan secara otomatis ke dalam address-list ddos-attackers. Setelah IP masuk ke daftar tersebut, rule Firewall RAW akan membuang trafik berikutnya dari sumber yang sama pada chain prerouting. Dengan cara ini, paket dari sumber yang sudah terindikasi sebagai attacker dapat dihentikan lebih awal sebelum diproses lebih jauh oleh router.

Alur implementasi Firewall RAW pada penelitian ini dirangkum pada Tabel 4.5. Tabel ini menunjukkan urutan kerja mulai dari trafik masuk, proses deteksi, penambahan IP ke address-list, hingga pemblokiran trafik lanjutan melalui Firewall RAW.

Tabel 4. 5 Alur Implementasi Firewall RAW

No	Tahapan Implementasi	Penjelasan
1	Trafik serangan masuk ke MikroTik utama	Trafik berasal dari Kali Linux melalui modem simulasi
2	Firewall filter melakukan deteksi awal	Trafik UDP atau TCP SYN berlebih diperiksa
3	IP sumber dimasukkan ke address-list	IP yang melewati ambang batas masuk ke ddos-attackers
4	Firewall RAW melakukan drop	Trafik lanjutan dari IP attacker dibuang pada prerouting
5	Trafik serangan tidak diproses lebih jauh	Mengurangi beban pemrosesan router

Berdasarkan Tabel 4.5, *Firewall RAW* bekerja setelah sumber trafik terindikasi melalui proses deteksi awal. Tahapan ini dibuat agar pemblokiran tidak hanya bergantung pada IP tertentu yang sudah diketahui sebelumnya, tetapi dapat mengenali sumber serangan baru secara dinamis. Dengan demikian, konfigurasi ini lebih sesuai untuk skenario serangan yang alamat sumbernya dapat berubah.

Tahap pertama konfigurasi dilakukan pada *firewall filter* untuk mendeteksi trafik UDP *Flood* dan TCP SYN *Flood*. Rule ini berfungsi untuk mengenali sumber trafik yang melewati ambang batas dan memasukkannya ke dalam *address-list* ddos-attackers. Konfigurasi rule deteksi tersebut ditunjukkan pada Gambar 4.3.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
[admin@MikrotikUtama] > /ip firewall filter print
Flags: X - disabled, I - invalid; D - dynamic
0   ;;; Deteksi awal UDP Flood menuju router utama
    chain=input action=jump jump-target=detect-udp-flood protocol=udp
    dst-address=192.168.18.20 in-interface=ether1

1   ;;; UDP masih dalam batas normal
    chain=detect-udp-flood action=return dst-limit=200,200,src-address/10s

2   ;;; Masukkan sumber UDP Flood ke ddos-attackers
    chain=detect-udp-flood action=add-src-to-address-list
    address-list=ddos-attackers address-list-timeout=10m

3   ;;; Kembali ke chain input setelah deteksi UDP
    chain=detect-udp-flood action=return

4   ;;; Deteksi awal TCP SYN Flood menuju router utama
    chain=input action=jump jump-target=detect-syn-flood tcp-flags=syn
    protocol=tcp dst-address=192.168.18.20 in-interface=ether1

5   ;;; TCP SYN masih dalam batas normal
    chain=detect-syn-flood action=return dst-limit=100,100,src-address/10s

6   ;;; Masukkan sumber SYN Flood ke ddos-attackers
    chain=detect-syn-flood action=add-src-to-address-list
    address-list=ddos-attackers address-list-timeout=10m

7   ;;; Kembali ke chain input setelah deteksi SYN
    chain=detect-syn-flood action=return
```

Gambar 4. 3 Konfigurasi Rule Deteksi Trafik UDP Flood dan TCP SYN Flood

Gambar 4.3 menunjukkan rule deteksi awal yang digunakan untuk mengenali trafik UDP dan TCP SYN berlebih. Rule tersebut menjadi tahap awal sebelum Firewall RAW membuang trafik lanjutan dari sumber yang telah terdeteksi. Dengan adanya mekanisme ini, IP penyerang baru dapat dimasukkan ke daftar ddos-attackers secara otomatis.

Setelah rule deteksi dibuat, tahap berikutnya adalah menambahkan rule Firewall RAW pada chain prerouting. Rule ini digunakan untuk membuang trafik dari alamat IP yang sudah berada di dalam address-list ddos-attackers. Konfigurasi rule Firewall RAW ditunjukkan pada Gambar 4.4.

```
[admin@MikrotikUtama] > /ip firewall raw print
Flags: X - disabled, I - invalid; D - dynamic
0   ;;; RAW - Drop trafik dari attacker yang sudah terdeteksi
    chain=prerouting action=drop in-interface=ether1
    src-address-list=ddos-attackers
```

Gambar 4. 4 Konfigurasi Rule Firewall RAW untuk Memblokir Attacker Terdeteksi



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Berdasarkan Gambar 4.4, trafik dari sumber yang sudah masuk ke dalam address-list ddos-attackers akan langsung dibuang pada tahap prerouting. Posisi ini dipilih karena Firewall RAW bekerja sebelum proses pemrosesan paket yang lebih berat, sehingga dapat membantu mengurangi beban kerja router saat menerima trafik serangan.

Pada implementasi ini, deteksi difokuskan pada dua jenis trafik. Pertama, UDP Flood, yaitu pengiriman paket UDP dalam jumlah besar menuju router utama. Kedua, TCP SYN Flood, yaitu pengiriman paket TCP dengan flag SYN secara berulang untuk membanjiri proses awal koneksi. Kedua jenis trafik tersebut digunakan karena sesuai dengan batasan penelitian yang berfokus pada serangan DDoS Layer 4.

Konfigurasi ini menjadi dasar bagi pengujian fungsional Firewall RAW pada subbab 4.4.3. Pengujian tersebut digunakan untuk memastikan bahwa IP sumber serangan dapat masuk ke address-list ddos-attackers dan trafik lanjutan dari IP tersebut dapat dibuang melalui Firewall RAW.

4.3.3 Implementasi Rate Limiting

Implementasi Rate Limiting dilakukan pada MikroTik utama sebagai lapisan pengendalian trafik setelah mekanisme Firewall RAW. Pada tahap implementasi awal, konfigurasi diterapkan terlebih dahulu pada MikroTik CHR utama di lingkungan laboratorium. Setelah konfigurasi berjalan sesuai rancangan, konfigurasi yang sama digunakan pada router MikroTik fisik milik PT XYZ pada tahap pengujian akhir.

Rate Limiting digunakan untuk membatasi trafik atau koneksi berlebih yang masih diproses oleh router. Pada rancangan ini, trafik yang masuk melalui interface ether1 menuju alamat WAN MikroTik utama 192.168.18.20 diarahkan ke chain khusus bernama rate-limit-ddos. Penggunaan chain khusus bertujuan agar rule pembatasan trafik lebih mudah dikelola dan dipisahkan dari rule firewall lainnya.

Konfigurasi rule Rate Limiting pada MikroTik utama ditunjukkan pada Gambar 4.5. Gambar ini memperlihatkan rule yang digunakan untuk mengarahkan trafik masuk ke chain rate-limit-ddos, serta rule pembatasan untuk trafik TCP dan UDP.

```
8      ;;; Masuk ke chain Rate Limiting DDoS
      chain=input action=jump jump-target=rate-limit-ddos dst-address=192.168.18.20 in-interface=ether1

10     ;;; Rate Limit - TCP SYN masih dalam batas
      chain=rate-limit-ddos action=return tcp-flags=syn protocol=tcp dst-limit=40,40,src-address/10s

      chain=rate-limit-ddos action=drop tcp-flags=syn protocol=tcp

12     ;;; Rate Limit - UDP masih dalam batas
      chain=rate-limit-ddos action=return protocol=udp dst-limit=80,80,src-address/10s

13     ;;; Rate Limit - Drop UDP berlebih
      chain=rate-limit-ddos action=drop protocol=udp

14     ;;; Keluar dari chain Rate Limiting
      chain=rate-limit-ddos action=return

[admin@MikrotikUtama] /ip/firewall/raw>
```

Gambar 4. 5 Konfigurasi Rule Rate Limiting pada MikroTik Utama

Berdasarkan Gambar 4.5, rule Rate Limiting disusun untuk menangani trafik yang masuk dari sisi WAN. Trafik yang sesuai diarahkan terlebih dahulu ke chain rate-limit-ddos, kemudian diperiksa berdasarkan jenis trafiknya. Dengan pemisahan tersebut, pembatasan terhadap koneksi TCP baru, TCP SYN, dan UDP dapat dilakukan secara lebih terstruktur.

Pada implementasi ini, terdapat tiga mekanisme utama yang digunakan. Mekanisme pertama adalah pembatasan paket TCP SYN berlebih dari satu sumber IP. Rule ini digunakan untuk mengurangi dampak TCP SYN Flood, yaitu kondisi ketika sumber tertentu mengirimkan banyak paket SYN dalam waktu singkat. Trafik SYN yang masih berada dalam batas wajar tetap diproses, sedangkan paket SYN yang melebihi ambang batas akan dibuang. Mekanisme kedua adalah pembatasan paket TCP SYN berlebih untuk mengurangi dampak TCP SYN Flood. Mekanisme ketiga adalah pembatasan trafik UDP berlebih untuk mengendalikan paket UDP yang dikirim secara berlebihan menuju router.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Rangkuman implementasi Rate Limiting pada penelitian ini ditunjukkan pada Tabel 4.6. Tabel ini menjelaskan mekanisme yang diterapkan dan fungsi masing-masing rule dalam proses pembatasan trafik.

Tabel 4. 6 Implementasi Rate Limiting

No	Mekanisme Rate Limiting	Fungsi
1	Pembatasan paket TCP SYN berlebih	Mengurangi dampak TCP SYN Flood
2	Pembatasan trafik UDP berlebih	Mengurangi dampak UDP Flood
3	Chain khusus rate-limit-ddos	Memisahkan pengelolaan rule Rate Limiting agar lebih terstruktur

Berdasarkan Tabel 4.6, implementasi *Rate Limiting* difokuskan pada pembatasan paket TCP SYN dan trafik UDP. Pembagian ini dilakukan karena kedua jenis serangan memiliki karakteristik yang berbeda. TCP SYN *Flood* membebani router melalui banyaknya permintaan awal koneksi TCP, sedangkan UDP *Flood* membebani router melalui jumlah paket UDP yang dikirim secara terus-menerus.

Nilai batas pada masing-masing rule *Rate Limiting* ditentukan berdasarkan kebutuhan pengujian pada lingkungan laboratorium. Nilai tersebut tidak dijadikan sebagai standar tetap untuk jaringan operasional PT XYZ, karena penerapan pada kondisi nyata perlu menyesuaikan kapasitas router, pola trafik pelanggan, dan kebijakan jaringan yang berlaku. Konfigurasi ini menjadi dasar bagi pengujian fungsional *Rate Limiting* pada subbab 4.4.3, yaitu untuk memastikan rule pembatasan TCP SYN dan UDP dapat bekerja ketika trafik melebihi ambang batas yang telah ditentukan.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.3.4 Implementasi Port Hardening

Implementasi *Port Hardening* dilakukan pada MikroTik utama untuk memperkuat keamanan akses manajemen router. Pada tahap implementasi awal, konfigurasi diterapkan terlebih dahulu pada MikroTik CHR utama di lingkungan laboratorium. Setelah konfigurasi sesuai dengan rancangan, konfigurasi yang sama digunakan pada router MikroTik fisik milik PT XYZ pada tahap pengujian akhir.

Berbeda dengan *Firewall RAW* dan *Rate Limiting* yang berfokus pada pengendalian trafik serangan DDoS, *Port Hardening* diterapkan untuk mengurangi permukaan serangan pada layanan administrasi router. Implementasi ini disesuaikan dengan informasi dari pihak teknis PT XYZ mengenai kondisi layanan manajemen MikroTik. Pada kondisi awal, layanan *Winbox* aktif pada port 7090 dan Telnet aktif pada port 2332, sedangkan API, API-SSL, FTP, WWW, WWW-SSL, serta SSH MikroTik berada dalam kondisi nonaktif.

Berdasarkan kondisi tersebut, implementasi *Port Hardening* dilakukan dengan menonaktifkan layanan yang tidak digunakan, menutup layanan Telnet, mengaktifkan SSH sebagai pengganti akses terminal, serta membatasi akses layanan manajemen. SSH diaktifkan pada port 2222, sedangkan *Winbox* tetap digunakan pada port 7090 sesuai informasi port yang digunakan oleh pihak PT XYZ.

Konfigurasi layanan manajemen setelah proses *Port Hardening* ditunjukkan pada Gambar 4.6. Gambar ini memperlihatkan layanan yang dinonaktifkan dan layanan yang tetap digunakan untuk kebutuhan administrasi router.

```
[admin@MikrotikUtama] /ip/firewall/filter> /ip service print
Flags: D - DYNAMIC; X - DISABLED, I - INVALID
Columns: NAME, PORT, PROTO, CERTIFICATE, VRF, MAX-SESSIONS
#  NAME      PORT  PROTO  CERTIFICATE  VRF  MAX-SESSIONS
0  X ftp      21    tcp      main        20
1  X telnet   23    tcp      main        20
2  D dhcp     67    udp
3  D dhcpclient 68    udp
4  X www      80    tcp      main        20
5  X www-ssl  443   tcp      none        main    20
6  D btest    2000  tcp
7  ssh       2222  tcp      main        20
8  D discover 5678  udp
9  winbox    7090  tcp      main        20
10 X api      8728  tcp      main        20
11 X api-ssl  8729  tcp      none        main    20
[admin@MikrotikUtama] /ip/firewall/filter>
```

Gambar 4. 6 Konfigurasi Layanan Manajemen pada MikroTik Utama

Berdasarkan Gambar 4.6, layanan yang tidak digunakan seperti API, API-SSL, FTP, WWW, dan WWW-SSL berada dalam kondisi nonaktif. Telnet juga dinonaktifkan karena tidak digunakan dalam rancangan akhir. Sebagai gantinya, akses terminal diarahkan menggunakan SSH pada port 2222, sedangkan akses konfigurasi berbasis GUI tetap menggunakan *Winbox* pada port 7090.

Selain pengaturan layanan, implementasi *Port Hardening* juga dilakukan melalui pembatasan akses berdasarkan sumber koneksi. Perangkat Ubuntu Desktop pada jaringan lokal digunakan sebagai perangkat admin dan diizinkan mengakses layanan SSH serta *Winbox* melalui *interface* LAN. Pembatasan ini diterapkan agar administrasi dari jaringan internal tetap dapat dilakukan tanpa membuka akses manajemen secara bebas dari sisi luar jaringan.

Untuk akses dari sisi luar, diterapkan mekanisme *port knocking* sebagai validasi tambahan sebelum akses manajemen diizinkan. Urutan *port knocking* yang digunakan adalah port 7001, 7002, dan 7003. Apabila urutan tersebut dilakukan dengan benar, alamat IP sumber akan dimasukkan ke dalam *address-list* *secured-admin* selama periode waktu tertentu. Setelah masuk ke daftar tersebut, sumber dari luar diperbolehkan mengakses SSH pada port 2222 dan *Winbox* pada port

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

7090. Sebaliknya, akses menuju SSH dan *Winbox* dari luar akan ditolak apabila sumber belum melewati proses *port knocking*.

Rangkuman implementasi *Port Hardening* pada penelitian ini ditunjukkan pada Tabel 4.7. Tabel ini menjelaskan komponen yang diterapkan dan fungsi masing-masing konfigurasi dalam membatasi akses manajemen router.

Tabel 4. 7 Implementasi Port Hardening

No	Komponen Implementasi	Fungsi
1	Menonaktifkan API, API-SSL, FTP, WWW, dan WWW-SSL	Mengurangi layanan yang tidak digunakan
2	Menonaktifkan Telnet	Menghilangkan akses terminal yang tidak terenkripsi
3	Mengaktifkan SSH port 2222	Menyediakan akses terminal administrasi yang lebih aman
4	Mengaktifkan Winbox port 7090	Menyediakan akses GUI administrasi
5	Mengizinkan akses SSH/Winbox dari LAN admin	Memastikan admin lokal tetap dapat mengakses router
6	Port knocking 7001–7002–7003	Validasi tambahan untuk akses dari luar jaringan
7	Address-list secured-admin	Menyimpan IP luar yang telah lolos validasi sementara
8	Drop akses SSH/Winbox dari luar yang belum knocking	Menolak akses manajemen yang tidak tervalidasi

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Berdasarkan Tabel 4.7, implementasi *Port Hardening* tidak hanya dilakukan dengan menutup layanan yang tidak digunakan, tetapi juga mengatur ulang jalur akses administrasi. Akses dari jaringan lokal tetap diizinkan agar pengelolaan router dapat berjalan normal, sedangkan akses dari sisi luar harus melewati *port knocking* terlebih dahulu. Dengan mekanisme ini, layanan manajemen tidak terbuka bebas dari jaringan publik.

Konfigurasi ini menjadi dasar bagi pengujian fungsional *Port Hardening* pada subbab 4.4.3. Pengujian tersebut digunakan untuk memastikan layanan yang tidak diperlukan telah dinonaktifkan, akses dari jaringan lokal tetap dapat dilakukan, dan akses dari sisi luar hanya dapat dilakukan setelah proses *port knocking* berhasil.

4.3.5 Implementasi Simulasi RTBH

Implementasi simulasi *Remotely Triggered Black Hole* atau RTBH pada penelitian ini dilakukan sebagai skenario tambahan untuk menggambarkan mekanisme pembuangan trafik pada level *routing*. Simulasi ini tidak menggunakan RTBH berbasis BGP secara nyata, melainkan menggunakan fitur *blackhole route* pada router *upstream* atau modem simulasi. Pendekatan ini dipilih karena penerapan RTBH pada jaringan operasional memerlukan izin, koordinasi, serta dukungan dari pihak ISP atau *upstream*.

Pada topologi penelitian, Kali Linux berperan sebagai sumber trafik dari sisi luar jaringan. Trafik dari Kali Linux diarahkan menuju IP publik modem simulasi, yaitu 198.51.100.1. Pada kondisi normal, trafik yang menuju IP publik tersebut diteruskan oleh router *upstream* menuju alamat WAN MikroTik utama, yaitu 192.168.18.20. Dengan demikian, MikroTik utama tetap menjadi perangkat yang menerima trafik dari sisi luar melalui *interface* WAN.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Simulasi RTBH diterapkan pada router *upstream* dengan menambahkan *blackhole route* menuju alamat WAN MikroTik utama, yaitu 192.168.18.20/32. Route ini digunakan untuk membuang trafik menuju MikroTik utama sebelum trafik tersebut mencapai *interface* WAN router utama. Pada tahap implementasi, route dibuat dalam kondisi nonaktif terlebih dahulu agar skenario RTBH dapat diaktifkan hanya ketika pengujian RTBH dilakukan.

Konfigurasi awal *blackhole route* pada router *upstream* ditunjukkan pada Gambar 4.7. Gambar ini memperlihatkan route menuju alamat 192.168.18.20/32 dengan tipe *blackhole* yang disiapkan sebagai jalur pembuangan trafik menuju MikroTik utama.

```
[admin@ModemUpstream] > /ip route add dst-address=192.168.18.20/32 type=blackhole disabled=yes comment="Simulasi RTBH - Blackhole trafik menuju MikroTik utama"
```

Gambar 4. 7 Konfigurasi Blackhole Route pada Router Upstream

Berdasarkan Gambar 4.7, *blackhole route* diarahkan ke alamat 192.168.18.20/32, yaitu alamat WAN MikroTik utama. Route tersebut ditempatkan pada router upstream, bukan pada MikroTik utama, karena tujuan simulasi RTBH adalah menggambarkan pembuangan trafik sebelum mencapai router target. Pada kondisi awal, route dibuat nonaktif agar trafik tetap berjalan normal sampai skenario RTBH diaktifkan.

Setelah konfigurasi awal dibuat, route tersebut dapat diaktifkan ketika skenario RTBH akan dijalankan. Aktivasi *blackhole route* dilakukan pada router upstream agar seluruh trafik menuju alamat WAN MikroTik utama diarahkan ke jalur *blackhole*. Kondisi route setelah diaktifkan ditunjukkan pada Gambar 4.8.

```
[admin@ModemUpstream] > /ip route enable [find comment="Simulasi RTBH - Blackhole trafik menuju MikroTik utama"]  
[admin@ModemUpstream] >
```

Gambar 4. 8 Aktivasi Blackhole Route pada Router Upstream



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Berdasarkan Gambar 4.8, *blackhole route* berada dalam kondisi aktif. Pada kondisi ini, trafik menuju 192.168.18.20/32 tidak lagi diteruskan melalui jalur normal menuju MikroTik utama, tetapi diarahkan ke jalur *blackhole* pada router *upstream*. Konfigurasi ini digunakan saat skenario RTBH diuji sebagai pembandingan terhadap metode mitigasi utama.

Setelah skenario RTBH selesai digunakan, route tersebut perlu dinonaktifkan kembali agar trafik menuju MikroTik utama dapat berjalan melalui jalur normal. Proses penonaktifan ini penting karena RTBH membuang seluruh trafik menuju IP target, termasuk trafik normal. Kondisi *blackhole route* setelah dinonaktifkan kembali ditunjukkan pada Gambar 4.9.

```
[admin@ModemUpstream] > /ip route disable [find comment="Simulasi RTBH - Blackhole trafik menuju MikroTik utama"]
[admin@ModemUpstream] >
```

Gambar 4. 9 Penonaktifan Blackhole Route Setelah Skenario RTBH

Berdasarkan Gambar 4.9, *blackhole route* telah dikembalikan ke kondisi nonaktif. Dengan kondisi tersebut, trafik menuju alamat WAN MikroTik utama tidak lagi diarahkan ke jalur *blackhole*. Hal ini memungkinkan topologi kembali ke kondisi normal untuk skenario pengujian lainnya.

Komponen yang digunakan dalam implementasi simulasi RTBH dirangkum pada Tabel 4.8. Tabel ini menunjukkan perangkat dan alamat jaringan yang terlibat dalam proses pembuangan trafik pada sisi *upstream*.

Tabel 4. 8 Komponen Implementasi Simulasi RTBH

No	Komponen Implementasi	Fungsi
1	Kali Linux	Mengirimkan trafik menuju IP publik modem simulasi

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Komponen Implementasi	Fungsi
2	IP publik modem 198.51.100.1	Tujuan trafik dari sisi luar jaringan
3	MikroTik utama 192.168.18.20	Target trafik setelah diteruskan dari modem simulasi
4	Blackhole route 192.168.18.20/32	Membuang trafik menuju router utama
5	CHR Upstream / Modem Simulasi	Lokasi penerapan blackhole route
6	Torch pada interface WAN MikroTik utama	Memverifikasi apakah trafik masih mencapai router utama

Berdasarkan Tabel 4.8, simulasi RTBH diterapkan pada router *upstream*, bukan pada MikroTik utama. Hal ini sesuai dengan prinsip RTBH, yaitu menghentikan trafik sebelum masuk ke router target. Dengan demikian, RTBH berbeda dari *Firewall RAW* dan *Rate Limiting* yang bekerja pada router utama.

Implementasi simulasi RTBH ini menjadi dasar bagi pengujian fungsional pada subbab 4.4.3. Pengujian tersebut digunakan untuk memastikan bahwa ketika *blackhole route* diaktifkan pada router *upstream*, trafik menuju MikroTik utama dapat dibuang sebelum mencapai *interface* WAN router utama. Dalam penelitian ini, RTBH digunakan sebagai skenario pembandingan dan gambaran kondisi darurat, bukan sebagai solusi utama, karena mekanisme ini membuang seluruh trafik menuju IP target tanpa membedakan trafik serangan dan trafik normal.

4.3.6 Implementasi Monitoring Parameter Pengujian

Implementasi monitoring parameter pengujian dilakukan untuk menyiapkan proses pengambilan data pada tahap pengujian dan evaluasi sistem mitigasi. Parameter yang dipantau disesuaikan dengan kebutuhan penelitian dan informasi dari pihak teknis PT XYZ, yaitu



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

berfokus pada kondisi sumber daya router serta lalu lintas jaringan selama serangan DDoS berlangsung.

Pada tahap implementasi awal, monitoring disiapkan pada MikroTik CHR utama di lingkungan laboratorium. Setelah konfigurasi dinyatakan sesuai rancangan, proses monitoring yang sama digunakan pada router MikroTik fisik milik PT XYZ pada tahap pengujian akhir. Dengan demikian, parameter yang diamati tetap sama, sedangkan perangkat utama yang menjadi objek pengambilan data berubah dari CHR menjadi router fisik. Pola ini sudah sesuai dengan batasan penelitian yang menjelaskan bahwa implementasi awal dilakukan pada CHR dan pengujian akhir dilakukan pada router fisik milik PT XYZ.

Parameter pertama yang diamati adalah CPU Load dan Free Memory. CPU Load digunakan untuk mengetahui tingkat beban pemrosesan router ketika menerima trafik normal maupun trafik serangan. Sementara itu, Free Memory digunakan untuk mengetahui jumlah memori yang masih tersedia pada router selama pengujian berlangsung. Monitoring CPU Load dan Free Memory dilakukan menggunakan perintah `/system resource monitor`, seperti ditunjukkan pada Gambar 4.10.

```
[admin@MikroTik] > /system resource monitor
cpu-used: 1%
free-memory: 54360KiB
-- [Q quit|D dump|C-z pause]
```

Gambar 4. 10 Monitoring CPU Load dan Free Memory pada MikroTik Utama

Berdasarkan Gambar 4.10, perintah `/system resource monitor` digunakan untuk menampilkan kondisi sumber daya router secara langsung. Informasi CPU Load dan Free Memory dari tampilan tersebut menjadi dasar pencatatan data pada setiap skenario pengujian. Dengan parameter ini, perubahan beban router sebelum dan sesudah penerapan mitigasi dapat diamati secara terukur.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Parameter berikutnya adalah traffic jaringan pada interface WAN MikroTik utama, yaitu ether1. Interface ini dipilih karena menjadi jalur masuk trafik dari router upstream atau modem simulasi menuju router utama. Monitoring traffic pada interface WAN dilakukan menggunakan perintah `/interface monitor-traffic ether1`, seperti ditunjukkan pada Gambar 4.11.

```
[admin@MikrotikUtama] > /interface monitor-traffic ether1
name: ether1
rx-packets-per-second: 0
rx-bits-per-second: 0bps
fp-rx-packets-per-second: 0
fp-rx-bits-per-second: 0bps
rx-drops-per-second: 0
rx-errors-per-second: 0
tx-packets-per-second: 1
tx-bits-per-second: 2.7kbps
fp-tx-packets-per-second: 0
fp-tx-bits-per-second: 0bps
tx-drops-per-second: 0
tx-queue-drops-per-second: 0
tx-errors-per-second: 0
-- [Q quit|D dump|C-z pause]
```

Gambar 4. 11 Monitoring Traffic pada Interface WAN MikroTik Utama

Berdasarkan Gambar 4.11, perintah `/interface monitor-traffic ether1` digunakan untuk melihat kondisi *traffic* pada *interface* WAN MikroTik utama. Data yang diamati terutama adalah nilai *traffic* masuk seperti *rx-bits-per-second* dan *rx-packets-per-second*. Parameter tersebut digunakan untuk melihat perubahan volume trafik yang diterima router selama skenario serangan dan mitigasi berlangsung.

Selain sumber daya router dan *traffic* WAN, penelitian ini juga memantau jumlah paket yang diblokir oleh rule mitigasi. Pada *Firewall RAW*, monitoring dilakukan menggunakan perintah `/ip firewall raw print stats`. Perintah ini menampilkan *counter* rule RAW, termasuk jumlah paket yang dibuang dari sumber yang telah masuk ke dalam

address-list ddos-attackers. Tampilan monitoring *counter* rule *Firewall RAW* ditunjukkan pada Gambar 4.12.

```
[admin@MikrotikUtama] > /ip firewall raw print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN      ACTION  BYTES  PACKETS
;;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop      0      0
[admin@MikrotikUtama] >
```

Gambar 4. 12 Monitoring Counter Rule Firewall RAW

Berdasarkan Gambar 4.12, *counter* pada rule *Firewall RAW* digunakan untuk mengetahui jumlah paket yang dibuang pada tahap *prerouting*. Nilai pada kolom *PACKETS* dan *BYTES* menjadi indikator bahwa rule *RAW* menerima dan memblokir trafik dari sumber yang telah terdeteksi. Pada kondisi awal sebelum skenario dijalankan, nilai *counter* dapat berada pada angka nol karena belum ada trafik serangan yang diproses.

Monitoring berikutnya dilakukan pada rule *Rate Limiting* menggunakan perintah */ip firewall filter print stats*. Perintah ini digunakan untuk melihat *counter* pada rule pembatasan koneksi TCP baru, TCP SYN, dan UDP. Tampilan monitoring *counter* rule *Rate Limiting* ditunjukkan pada Gambar 4.13.

```
;;; Rate Limit - Drop total koneksi TCP baru berlebih per IP
9 rate-limit-ddos drop      0      0
;;; Rate Limit - TCP SYN masih dalam batas
10 rate-limit-ddos return    0      0
;;; Rate Limit - Drop TCP SYN berlebih
11 rate-limit-ddos drop      0      0
;;; Rate Limit - UDP masih dalam batas
12 rate-limit-ddos return    0      0
;;; Rate Limit - Drop UDP berlebih
13 rate-limit-ddos drop      0      0
```

Gambar 4. 13 Monitoring Counter Rule Rate Limiting

Berdasarkan Gambar 4.13, rule *Rate Limiting* dipantau melalui *counter* pada *firewall filter*. Nilai *counter* digunakan untuk mengetahui apakah trafik yang melebihi ambang batas telah diproses oleh rule pembatasan. Pada pengujian tertentu, *counter Rate Limiting* dapat bernilai kecil atau tidak meningkat besar ketika *Firewall RAW* aktif, karena trafik dari IP

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

yang sudah masuk ke ddos-attackers akan lebih dahulu dibuang oleh rule RAW.

Parameter monitoring yang digunakan dalam penelitian ini dirangkum pada Tabel 4.9. Tabel ini menunjukkan parameter yang diamati, lokasi pemantauan, serta tujuan pengambilan data pada setiap skenario pengujian.

Tabel 4. 9 Parameter Monitoring Pengujian

No	Parameter	Lokasi Monitoring	Tujuan
1	CPU Load	MikroTik CHR utama	Mengukur tingkat beban pemrosesan router
2	Free Memory	MikroTik CHR utama	Mengetahui ketersediaan memori router
3	Traffic jaringan	Interface ether1 MikroTik utama	Mengamati trafik masuk dari sisi upstream
4	Dropped packets Firewall RAW	Counter rule Firewall RAW	Mengetahui jumlah paket attacker yang dibuang pada tahap awal
5	Dropped packets Rate Limiting	Counter rule firewall filter	Mengetahui jumlah trafik berlebih yang berhasil dibatasi

Berdasarkan Tabel 4.9, parameter monitoring yang digunakan berfokus pada sumber daya router, kondisi *traffic* jaringan, dan jumlah paket yang diblokir. CPU Load dan Free Memory digunakan untuk melihat pengaruh serangan terhadap kemampuan perangkat, sedangkan *traffic* WAN dan *dropped packets* digunakan untuk melihat respons rule mitigasi terhadap trafik serangan.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Sebelum setiap skenario pengujian dijalankan, dilakukan pembersihan kondisi awal dengan mereset *counter firewall* dan menghapus *address-list ddos-attackers* apabila masih terdapat data dari pengujian sebelumnya. Langkah ini dilakukan agar setiap skenario dimulai dari kondisi yang sama, sehingga data hasil pengujian dapat dibandingkan secara lebih objektif.

Dengan adanya monitoring parameter ini, proses pengujian dapat dilakukan secara terstruktur. Data CPU Load, Free Memory, *traffic* WAN, dan *dropped packets* digunakan untuk membandingkan kondisi router pada setiap skenario mitigasi, yaitu tanpa mitigasi, *Firewall RAW*, *Firewall RAW* dengan *Rate Limiting*, serta simulasi RTBH. Sementara itu, *Port Hardening* dievaluasi secara terpisah melalui pengujian akses layanan manajemen router.

Setelah konfigurasi pada tahap laboratorium dinyatakan berjalan sesuai rancangan, konfigurasi yang sama dipindahkan ke perangkat MikroTik fisik milik PT XYZ untuk pengujian akhir. Pada tahap ini, MikroTik CHR utama tidak lagi digunakan sebagai objek pengambilan data utama, melainkan digantikan oleh router fisik. Perangkat virtual tetap digunakan untuk Kali Linux sebagai *attacker* dan MikroTik CHR *upstream* sebagai modem simulasi. Pergantian objek pengujian ini dilakukan agar data CPU Load, Free Memory, *traffic* WAN, dan *dropped packets* lebih merepresentasikan kondisi perangkat MikroTik yang digunakan pada lingkungan nyata, namun tetap berada dalam jaringan uji terpisah agar tidak mengganggu layanan operasional.

4.4 Pengujian

4.4.1 Deskripsi Pengujian

Pengujian pada penelitian ini dilakukan untuk mengetahui apakah sistem mitigasi serangan DDoS yang telah diimplementasikan dapat berjalan sesuai rancangan dan mampu mengurangi dampak serangan



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

terhadap router MikroTik. Sebelum pengujian akhir dilakukan, konfigurasi terlebih dahulu divalidasi pada MikroTik CHR di lingkungan laboratorium. Setelah konfigurasi dinyatakan sesuai, pengujian akhir dilakukan menggunakan router MikroTik fisik milik PT XYZ sebagai objek pengambilan data. Pada tahap ini, Kali Linux digunakan sebagai perangkat *attacker*, MikroTik CHR *upstream* digunakan sebagai modem simulasi, dan Ubuntu Desktop digunakan sebagai perangkat *client/admin*.

Jenis serangan yang digunakan adalah UDP *Flood* dan TCP SYN *Flood*. Kedua serangan tersebut dipilih karena termasuk serangan DDoS pada lapisan transport dan sesuai dengan ruang lingkup penelitian. UDP *Flood* merepresentasikan serangan volumetrik yang membanjiri trafik jaringan, sedangkan TCP SYN *Flood* merepresentasikan serangan protokol yang membebani proses awal pembentukan koneksi TCP. Trafik serangan dikirimkan dari Kali Linux menuju IP publik modem simulasi, kemudian diteruskan ke router MikroTik utama sebagai target pengujian.

Secara umum, pengujian dibagi menjadi dua bagian, yaitu pengujian fungsional dan pengujian performa. Pengujian fungsional dilakukan untuk memastikan konfigurasi topologi, *Firewall RAW*, *Rate Limiting*, *Port Hardening*, dan simulasi RTBH berjalan sesuai rancangan. Setelah itu, pengujian performa dilakukan untuk mengamati perubahan CPU Load, Free Memory, *traffic* WAN, dan jumlah paket yang diblokir selama serangan berlangsung.

Skenario pengujian performa disusun secara bertahap agar kontribusi masing-masing metode dapat terlihat. Skenario tersebut meliputi kondisi tanpa mitigasi, penggunaan *Firewall RAW*, kombinasi *Firewall RAW* dan *Rate Limiting*, serta simulasi RTBH. Kondisi tanpa mitigasi digunakan sebagai data dasar, sedangkan skenario mitigasi digunakan untuk melihat perubahan beban router setelah rule keamanan



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

diterapkan. RTBH digunakan sebagai simulasi langkah terakhir ketika trafik serangan perlu dibuang pada sisi *upstream* sebelum mencapai router utama.

Pengujian *Port Hardening* tidak dimasukkan ke dalam skenario performa CPU dan *traffic* karena metode ini tidak berfokus pada pemrosesan trafik UDP *Flood* atau TCP SYN *Flood*. *Port Hardening* dievaluasi secara fungsional melalui pengujian akses layanan manajemen, seperti status layanan router, akses SSH dari jaringan internal, penolakan akses dari sisi luar sebelum *port knocking*, serta keberhasilan akses sementara setelah proses *port knocking* dilakukan.

Dengan pembagian tersebut, efektivitas *Firewall RAW*, *Rate Limiting*, dan simulasi RTBH dianalisis dari sisi penggunaan sumber daya router dan trafik jaringan. Sementara itu, *Port Hardening* dianalisis dari sisi keamanan akses manajemen router.

4.4.2 Prosedur Pengujian

Prosedur pengujian dilakukan pada lingkungan uji terpisah dengan router MikroTik fisik sebagai objek utama pengambilan data. Kali Linux dan MikroTik CHR *upstream* tetap digunakan secara virtual untuk mensimulasikan sisi *attacker* dan modem/*upstream*. Trafik serangan dikirim dari Kali Linux menuju IP publik modem simulasi 198.51.100.1, kemudian diteruskan ke *interface* WAN router MikroTik fisik utama.

Sebelum pengujian dilakukan, kondisi awal sistem disiapkan agar setiap skenario memiliki titik awal yang setara. Persiapan meliputi pengecekan konektivitas antarperangkat, memastikan konfigurasi jaringan berjalan normal, menghapus isi *address-list* ddos-attackers, serta melakukan *reset counter* pada rule *firewall*. Langkah ini dilakukan agar data paket yang diblokir pada setiap skenario tidak tercampur dengan hasil pengujian sebelumnya.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pengujian dibagi menjadi dua tahap, yaitu pengujian fungsional dan pengujian performa. Pengujian fungsional dilakukan untuk memastikan konfigurasi topologi, *Firewall RAW*, *Rate Limiting*, *Port Hardening*, dan simulasi RTBH berjalan sesuai rancangan. Setelah itu, pengujian performa dilakukan untuk mencatat CPU Load, Free Memory, *traffic* pada *interface* WAN, serta jumlah paket yang diblokir oleh rule mitigasi.

Pada pengujian performa, serangan yang digunakan adalah *UDP Flood* dan *TCP SYN Flood*. Setiap serangan dijalankan dari Kali Linux menuju IP publik modem simulasi dengan periode pengamatan yang sama pada setiap skenario. Skenario yang diuji meliputi kondisi tanpa mitigasi, *Firewall RAW*, kombinasi *Firewall RAW* dan *Rate Limiting*, serta simulasi RTBH. Pada setiap skenario, rule mitigasi diaktifkan atau dinonaktifkan sesuai kebutuhan pengujian, kemudian dilakukan pencatatan CPU Load, Free Memory, *traffic* WAN, dan *dropped packets*.

Setelah pengujian *UDP Flood* selesai, serangan dihentikan dan kondisi awal dikembalikan dengan menghapus *address-list* serta melakukan *reset counter* kembali. Prosedur yang sama kemudian dilakukan pada pengujian *TCP SYN Flood*. Untuk skenario RTBH, *blackhole route* diaktifkan pada router *upstream* agar trafik menuju MikroTik utama dibuang sebelum mencapai *interface* WAN router utama.

Selain pengujian performa, *Port Hardening* diuji secara terpisah karena metode ini berfokus pada keamanan akses manajemen router, bukan pada pemrosesan trafik *UDP Flood* atau *TCP SYN Flood*. Pengujian dilakukan dengan memeriksa status layanan manajemen MikroTik, menguji akses Telnet dari sisi luar, menguji akses SSH dari jaringan admin internal, menguji akses SSH dari sisi luar sebelum *port knocking*, menjalankan proses *port knocking*, memverifikasi IP sumber pada



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

address-list secured-admin, serta menguji akses SSH dari sisi luar setelah proses *port knocking* berhasil.

Melalui prosedur tersebut, setiap skenario pengujian dapat dilakukan secara konsisten dan terukur. Data yang diperoleh kemudian disajikan pada subbab 4.4.3 sebagai dasar untuk menganalisis efektivitas masing-masing metode mitigasi terhadap kondisi sumber daya router, *traffic* jaringan, dan keamanan akses manajemen.

4.4.3 Data Hasil Pengujian

Data hasil pengujian pada penelitian ini dibagi menjadi dua jenis, yaitu pengujian fungsional dan pengujian performa. Pengujian fungsional dilakukan untuk memastikan bahwa setiap konfigurasi yang telah diimplementasikan dapat berjalan sesuai rancangan, meliputi koneksi dasar topologi, Firewall RAW, Rate Limiting, Port Hardening, dan simulasi RTBH. Sementara itu, pengujian performa dilakukan untuk mengukur pengaruh serangan UDP Flood dan TCP SYN Flood terhadap CPU Load, Free Memory, traffic WAN, serta jumlah paket yang diblokir pada setiap skenario mitigasi.

Pengujian fungsional dilakukan sebelum pengujian performa agar dapat dipastikan bahwa seluruh rule dan mekanisme mitigasi telah aktif dan bekerja sesuai perannya. Setelah pengujian fungsional selesai, pengujian performa dilakukan selama 10 menit dengan interval pencatatan setiap 1 menit pada masing-masing skenario.

A. Data Hasil Pengujian Fungsional

1. Pengujian Fungsional Topologi dan Koneksi Dasar

Pengujian fungsional topologi dilakukan untuk memastikan bahwa jalur komunikasi antara perangkat *attacker*, router *upstream* atau modem simulasi, router MikroTik utama, dan komputer admin telah berjalan sesuai rancangan. Pengujian ini menjadi tahap awal sebelum

pengujian performa dilakukan, karena seluruh skenario serangan membutuhkan jalur komunikasi yang sudah terhubung dengan benar. Pengujian dilakukan dengan memastikan Kali Linux dapat menjangkau IP publik modem simulasi, router *upstream* dapat terhubung ke alamat WAN MikroTik utama, serta Ubuntu Desktop dapat terhubung ke jaringan LAN MikroTik utama. Selain itu, pemantauan menggunakan fitur *Torch* dilakukan pada *interface* ether1 MikroTik utama untuk memastikan trafik dari sisi *attacker* benar-benar masuk melalui jalur WAN.

Ringkasan hasil pengujian fungsional topologi dan koneksi dasar ditunjukkan pada Tabel 4.10.

Tabel 4. 10 Hasil Pengujian Fungsional Topologi dan Koneksi Dasar

No	Pengujian	Hasil yang Diharapkan	Hasil
1	Ping Kali Linux ke IP publik modem simulasi	Kali dapat menjangkau 198.51.100.1	Berhasil
2	Ping router upstream ke WAN MikroTik utama	Router upstream dapat menjangkau 192.168.18.20	Berhasil
3	Ping Ubuntu Desktop ke LAN MikroTik utama	Ubuntu dapat menjangkau 192.168.10.1	Berhasil
4	Torch interface ether1 MikroTik utama	Trafik dari Kali terlihat masuk ke WAN MikroTik utama	Berhasil

Berdasarkan Tabel 4.10, seluruh jalur komunikasi dasar pada topologi pengujian telah berjalan sesuai rancangan. Kali Linux dapat menjangkau IP publik modem simulasi, router *upstream* dapat berkomunikasi dengan MikroTik utama, dan Ubuntu Desktop dapat

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

digunakan sebagai perangkat admin pada sisi LAN. Hasil ini menunjukkan bahwa topologi siap digunakan untuk pengujian fungsional lanjutan dan pengujian performa.

Bukti konektivitas dari Kali Linux menuju IP publik modem simulasi ditunjukkan pada Gambar 4.14. Pengujian ini dilakukan untuk memastikan bahwa perangkat *attacker* dapat menjangkau alamat tujuan awal sebelum trafik diteruskan ke MikroTik utama.

```
(kali㉿kali)-[~]
$ ping 198.51.100.1
PING 198.51.100.1 (198.51.100.1) 56(84) bytes of data.
64 bytes from 198.51.100.1: icmp_seq=1 ttl=63 time=2.38 ms
64 bytes from 198.51.100.1: icmp_seq=2 ttl=63 time=1.38 ms
64 bytes from 198.51.100.1: icmp_seq=3 ttl=63 time=2.59 ms
64 bytes from 198.51.100.1: icmp_seq=4 ttl=63 time=1.91 ms
64 bytes from 198.51.100.1: icmp_seq=5 ttl=63 time=2.33 ms
64 bytes from 198.51.100.1: icmp_seq=6 ttl=63 time=2.46 ms
64 bytes from 198.51.100.1: icmp_seq=7 ttl=63 time=1.31 ms
64 bytes from 198.51.100.1: icmp_seq=8 ttl=63 time=1.53 ms
```

Gambar 4. 14 Pengujian Konektivitas Kali Linux ke IP Publik Modem Simulasi

Berdasarkan Gambar 4.14, Kali Linux berhasil melakukan koneksi ke IP publik modem simulasi 198.51.100.1. Hal ini menunjukkan bahwa jalur dari sisi *attacker* menuju router *upstream* sudah berjalan dan dapat digunakan sebagai jalur awal pengiriman trafik serangan.

Selanjutnya, konektivitas dari Ubuntu Desktop menuju router MikroTik utama juga diuji. Pengujian ini dilakukan untuk memastikan bahwa perangkat admin pada sisi LAN dapat mengakses router utama untuk kebutuhan konfigurasi dan pemantauan selama pengujian.

```
alvito0731@alvito0731-VirtualBox:~$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=2.45 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=0.862 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=0.624 ms
^C
--- 192.168.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.624/1.312/2.450/0.810 ms
```

Gambar 4. 15 Pengujian Konektivitas Ubuntu Desktop ke Router MikroTik Utama

Berdasarkan Gambar 4.15, Ubuntu Desktop berhasil terhubung ke router MikroTik utama melalui jaringan LAN. Koneksi ini diperlukan agar proses administrasi, monitoring CPU, memori, *traffic*, serta pemeriksaan rule dapat dilakukan dari perangkat admin.

Setelah konektivitas dasar dipastikan, dilakukan pemantauan trafik menggunakan fitur *Torch* pada *interface* ether1 MikroTik utama. Pemantauan ini bertujuan untuk memastikan bahwa trafik dari sisi *attacker* yang melewati router *upstream* benar-benar diteruskan ke *interface* WAN MikroTik utama.

```
[admin@MikrotikUtama] > tool torch interface=ether1
Columns: MAC-PROTOCOL, IP-PROTOCOL, DSCP, SRC-ADDRESS, DST-ADDRESS, TX, RX,
TX-PACKETS, RX-PACKETS
MA IP-PROTOCOL DSCP SRC-ADDRESS DST-ADDRESS TX RX T R
ip icmp 0 198.51.100.2 192.168.18.20 784bps 784bps 1 1
[admin@MikrotikUtama] >
```

Gambar 4. 16 Trafik dari Sisi Attacker yang Diteruskan ke Interface WAN MikroTik Utama

Berdasarkan Gambar 4.16, trafik dari sisi *attacker* terlihat masuk ke *interface* WAN MikroTik utama. Hasil ini menunjukkan bahwa alur trafik dari Kali Linux menuju IP publik modem simulasi, kemudian diteruskan ke MikroTik utama, telah sesuai dengan rancangan topologi pengujian. Dengan demikian, pengujian fungsional pada layer berikutnya dapat dilanjutkan.

2. Pengujian Fungsional Firewall RAW

Pengujian fungsional *Firewall RAW* dilakukan untuk memastikan bahwa mekanisme deteksi sumber serangan dan pemblokiran trafik melalui *Firewall RAW* berjalan sesuai rancangan. Pengujian dilakukan dengan mengirimkan trafik UDP *Flood* dan TCP SYN *Flood* dari Kali Linux menuju IP publik modem simulasi. Trafik tersebut kemudian diteruskan ke *interface* WAN MikroTik utama.

Pada pengujian ini, apabila suatu sumber mengirimkan trafik melebihi ambang batas yang telah ditentukan, alamat IP sumber akan dimasukkan ke dalam *address-list* ddos-attackers. Setelah IP masuk ke

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

dalam *address-list* tersebut, trafik lanjutan dari sumber yang sama akan dibuang oleh *Firewall RAW* pada *chain prerouting*.

Ringkasan hasil pengujian fungsional *Firewall RAW* ditunjukkan pada Tabel 4.11. Tabel ini digunakan untuk memperlihatkan tahapan pengujian, hasil yang diharapkan, dan status keberhasilan dari setiap tahapan.

Tabel 4. 11 Hasil Pengujian Fungsional Firewall RAW

No	Pengujian	Hasil yang Diharapkan	Hasil
1	Mengirim trafik UDP/TCP SYN dari Kali	Trafik masuk ke interface WAN MikroTik utama	Berhasil
2	Deteksi sumber attacker	IP attacker masuk <i>address-list ddos-attackers</i>	Berhasil
3	RAW drop terhadap IP attacker	Counter rule RAW meningkat	Berhasil
4	Reset <i>address-list</i> dan counter	Kondisi awal kembali bersih sebelum skenario berikutnya	Berhasil

Berdasarkan Tabel 4.11, mekanisme *Firewall RAW* telah berjalan sesuai tahapan yang dirancang. Trafik serangan dapat dikirim dari Kali Linux, IP sumber dapat dikenali sebagai *attacker*, dan trafik lanjutan dari IP tersebut dapat dibuang melalui rule *Firewall RAW*. Proses reset juga dilakukan agar pengujian berikutnya dimulai dari kondisi awal yang bersih.

Pengujian pertama dilakukan dengan mengirimkan trafik UDP *Flood* dari Kali Linux menuju IP publik modem simulasi. Pengujian ini digunakan untuk melihat respons rule deteksi terhadap trafik UDP yang dikirim secara berlebihan. Hasil simulasi UDP *Flood* ditunjukkan pada Gambar 4.17.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
(kali@kali)-[~]
$ sudo hping3 --udp -p 53 -i u1000 198.51.100.1
HPING 198.51.100.1 (eth0 198.51.100.1): udp mode set, 28 headers + 0 data bytes
es
ICMP Port Unreachable from ip=198.51.100.1 name=UNKNOWN
status=0 port=2761 seq=0
ICMP Port Unreachable from ip=198.51.100.1 name=UNKNOWN
status=0 port=2762 seq=1
ICMP Port Unreachable from ip=198.51.100.1 name=UNKNOWN
status=0 port=2763 seq=2
ICMP Port Unreachable from ip=198.51.100.1 name=UNKNOWN
status=0 port=2764 seq=3
ICMP Port Unreachable from ip=198.51.100.1 name=UNKNOWN
status=0 port=2765 seq=4
ICMP Port Unreachable from ip=198.51.100.1 name=UNKNOWN
status=0 port=2766 seq=5
```

Gambar 4. 17 Simulasi UDP Flood dari Kali Linux

Berdasarkan Gambar 4.17, Kali Linux menjalankan pengiriman trafik UDP *Flood* menuju IP publik modem simulasi. Trafik ini digunakan sebagai pemicu awal untuk melihat apakah rule deteksi mampu mengenali sumber trafik yang melebihi batas dan memasukkannya ke dalam daftar *attacker*.

Selain UDP *Flood*, pengujian juga dilakukan menggunakan TCP SYN *Flood*. Pengujian ini bertujuan untuk memastikan rule deteksi dapat menangani trafik TCP SYN yang dikirim secara terus-menerus. Hasil simulasi TCP SYN *Flood* ditunjukkan pada Gambar 4.18.

```
(kali@kali)-[~]
$ sudo hping3 -S -p 80 -i u1000 198.51.100.1
HPING 198.51.100.1 (eth0 198.51.100.1): S set, 40 headers + 0 data bytes
len=46 ip=198.51.100.1 ttl=63 DF id=0 sport=80 flags=SA seq=0 win=64240 rtt=4
.2 ms
len=46 ip=198.51.100.1 ttl=63 DF id=0 sport=80 flags=SA seq=1 win=64240 rtt=2
.9 ms
len=46 ip=198.51.100.1 ttl=63 DF id=0 sport=80 flags=SA seq=2 win=64240 rtt=4
.8 ms
len=46 ip=198.51.100.1 ttl=63 DF id=0 sport=80 flags=SA seq=3 win=64240 rtt=2
.0 ms
len=46 ip=198.51.100.1 ttl=63 DF id=0 sport=80 flags=SA seq=4 win=64240 rtt=1
.3 ms
len=46 ip=198.51.100.1 ttl=63 DF id=0 sport=80 flags=SA seq=5 win=64240 rtt=3
.5 ms
```

Gambar 4. 18 Simulasi TCP SYN Flood dari Kali Linux

Berdasarkan Gambar 4.18, Kali Linux mengirimkan paket TCP dengan flag SYN secara berulang menuju IP publik modem simulasi. Trafik tersebut kemudian diteruskan ke router MikroTik utama dan digunakan untuk memicu mekanisme deteksi pada rule *firewall filter*.

Setelah trafik serangan dikirimkan, dilakukan pemeriksaan pada *address-list* *ddos-attackers*. Pemeriksaan ini bertujuan untuk memastikan bahwa alamat IP sumber yang melewati ambang batas berhasil tercatat sebagai sumber serangan. Hasil pemeriksaan *address-list* ditunjukkan pada Gambar 4.19.

```
[admin@MikrotikUtama] > /ip firewall address-list print where list=ddos-attackers
Flags: D - DYNAMIC
Columns: LIST, ADDRESS, CREATION-TIME, TIMEOUT
# LIST ADDRESS CREATION-TIME TIMEOUT
2 D ddos-attackers 198.51.100.2 2026-05-13 07:24:21 9m54s
[admin@MikrotikUtama] >
```

Gambar 4. 19 IP Attacker Masuk Address-List *ddos-attackers*

Berdasarkan Gambar 4.19, alamat IP sumber serangan telah masuk ke dalam *address-list* *ddos-attackers*. Hal ini menunjukkan bahwa mekanisme deteksi awal berhasil mengenali sumber trafik yang melebihi batas. Daftar ini kemudian digunakan oleh *Firewall RAW* sebagai acuan untuk membuang trafik lanjutan dari sumber yang sama.

Tahap berikutnya adalah memeriksa *counter* pada rule *Firewall RAW*. Pemeriksaan ini dilakukan untuk melihat apakah trafik dari IP yang telah terdaftar sebagai *attacker* benar-benar dibuang pada *chain prerouting*. Hasil peningkatan *counter* rule *Firewall RAW* ditunjukkan pada Gambar 4.20.

```
[admin@MikrotikUtama] > /ip firewall raw print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN ACTION BYTES PACKETS
;;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop 13 520 338
[admin@MikrotikUtama] > /ip firewall raw print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN ACTION BYTES PACKETS
;;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop 39 112 1 252
[admin@MikrotikUtama] >
```

Gambar 4. 20 Counter Firewall RAW Meningkat Setelah Attacker Terdeteksi

Berdasarkan Gambar 4.20, nilai *counter* pada rule *Firewall RAW* mengalami peningkatan setelah IP sumber masuk ke dalam *address-list* *ddos-attackers*. Kondisi ini menunjukkan bahwa trafik lanjutan dari IP *attacker* berhasil dibuang oleh *Firewall RAW* sebelum diproses lebih

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

jauh oleh router. Dengan demikian, pengujian fungsional *Firewall RAW* menunjukkan bahwa mekanisme deteksi dan pemblokiran telah berjalan sesuai rancangan.

3. Pengujian Fungsional Rate Limiting

Pengujian fungsional *Rate Limiting* dilakukan untuk memastikan bahwa rule pembatasan trafik berlebih dapat bekerja sesuai rancangan. Pengujian dilakukan terhadap trafik TCP SYN dan UDP yang dikirim dari Kali Linux menuju IP publik modem simulasi. Pada pengujian ini, parameter yang diamati adalah *counter* rule *Rate Limiting* untuk mengetahui apakah trafik yang melebihi ambang batas dapat dikenali dan dibatasi oleh router.

Pengujian ini juga memperhatikan hubungan antara *Rate Limiting* dan *Firewall RAW*. Pada skenario gabungan, trafik dari IP yang sudah masuk ke *address-list* *ddos-attackers* dapat lebih dahulu dibuang oleh *Firewall RAW*. Oleh karena itu, *counter Rate Limiting* tidak selalu meningkat besar ketika *Firewall RAW* aktif, karena sebagian trafik sudah ditangani lebih awal oleh rule RAW.

Ringkasan hasil pengujian fungsional *Rate Limiting* ditunjukkan pada Tabel 4.12. Tabel ini digunakan untuk memperlihatkan tahapan pengujian, hasil yang diharapkan, dan status keberhasilan dari rule pembatasan trafik.

Tabel 4. 12 Hasil Pengujian Fungsional Rate Limiting

No	Pengujian	Hasil yang Diharapkan	Hasil
1	Trafik UDP melebihi batas Rate Limiting	Counter Rate Limit - Drop UDP berlebih meningkat	Berhasil
2	Trafik TCP SYN melebihi batas Rate Limiting	Counter Rate Limit - Drop TCP SYN berlebih meningkat saat	Berhasil

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Pengujian	Hasil yang Diharapkan	Hasil
		RAW tidak mengambil alih lebih dulu	
3	RAW dan Rate Limiting aktif bersamaan	RAW dapat lebih dominan setelah IP masuk ddos-attackers	Berhasil
4	Reset counter filter	Counter kembali bersih sebelum skenario berikutnya	Berhasil

Berdasarkan Tabel 4.12, rule *Rate Limiting* dapat bekerja untuk membatasi trafik UDP dan TCP SYN yang melewati ambang batas. Hasil pengujian juga menunjukkan bahwa pada kondisi tertentu, *Firewall RAW* dapat lebih dominan karena trafik dari IP yang telah terdeteksi sebagai *attacker* dibuang lebih awal melalui *chain prerouting*. Dengan demikian, kecilnya *counter Rate Limiting* pada skenario gabungan tidak menunjukkan kegagalan rule, melainkan menunjukkan bahwa trafik sudah lebih dahulu ditangani oleh *Firewall RAW*.

Pengujian pertama dilakukan terhadap trafik UDP *Flood*. Pada pengujian ini, Kali Linux mengirimkan paket UDP secara berlebihan menuju IP publik modem simulasi. Rule *Rate Limiting* kemudian diamati untuk melihat apakah trafik UDP yang melebihi batas dapat dikenali dan dibatasi. Hasil pengujian *Rate Limiting* terhadap UDP *Flood* ditunjukkan pada Gambar 4.21.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
(kali@kali)-[~]
$ sudo hping3 --udp -p 53 -i u1000 198.51.100.1
[sudo] password for kali:
HPING 198.51.100.1 (eth0 198.51.100.1): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=198.51.100.1 name=UNKNOWN
status=0 port=2080 seq=0
ICMP Port Unreachable from ip=198.51.100.1 name=UNKNOWN
status=0 port=2081 seq=1
ICMP Port Unreachable from ip=198.51.100.1 name=UNKNOWN
status=0 port=2082 seq=2
ICMP Port Unreachable from ip=198.51.100.1 name=UNKNOWN
status=0 port=2083 seq=3
ICMP Port Unreachable from ip=198.51.100.1 name=UNKNOWN
status=0 port=2084 seq=4
;;; Rate Limit - Drop UDP berlebih
13 rate-limit-ddos drop 19 012 679
```

Gambar 4. 21 Pengujian Rate Limiting terhadap UDP Flood

Berdasarkan Gambar 4.21, rule *Rate Limiting* terhadap trafik UDP menunjukkan adanya aktivitas pada *counter*. Hal ini menandakan bahwa trafik UDP yang melebihi batas dapat dikenali oleh rule pembatasan dan diproses sesuai rancangan. Pengujian ini membuktikan bahwa mekanisme pembatasan UDP dapat digunakan untuk mengurangi dampak *UDP Flood*.

Pengujian berikutnya dilakukan terhadap trafik *TCP SYN Flood*. Trafik ini digunakan untuk melihat apakah rule pembatasan TCP SYN dapat bekerja ketika terdapat banyak permintaan koneksi awal dari satu sumber. Hasil pengujian *Rate Limiting* terhadap *TCP SYN Flood* ditunjukkan pada Gambar 4.22.

```
(kali@kali)-[~]
$ sudo hping3 -S -p 80 -i u1000 198.51.100.1
HPING 198.51.100.1 (eth0 198.51.100.1): S set, 40 headers + 0 data bytes
len=46 ip=198.51.100.1 ttl=63 DF id=0 sport=80 flags=SA seq=0 win=64240 rtt=3.0 ms
len=46 ip=198.51.100.1 ttl=63 DF id=0 sport=80 flags=SA seq=1 win=64240 rtt=1.7 ms
len=46 ip=198.51.100.1 ttl=63 DF id=0 sport=80 flags=SA seq=2 win=64240 rtt=2.7 ms
len=46 ip=198.51.100.1 ttl=63 DF id=0 sport=80 flags=SA seq=3 win=64240 rtt=2.1 ms
len=46 ip=198.51.100.1 ttl=63 DF id=0 sport=80 flags=SA seq=4 win=64240 rtt=5.1 ms
;;; Rate Limit - Drop TCP SYN berlebih
11 rate-limit-ddos drop 2 680 67
```

Gambar 4. 22 Pengujian Rate Limiting terhadap TCP SYN Flood

Berdasarkan Gambar 4.22, rule *Rate Limiting* terhadap TCP SYN dapat digunakan untuk membatasi paket SYN yang melebihi ambang batas. Apabila pada skenario gabungan nilai *counter* tidak meningkat besar,

kondisi tersebut masih sesuai dengan rancangan karena trafik dari IP yang sudah masuk ke ddos-attackers lebih dahulu dibuang oleh Firewall RAW. Dengan demikian, pengujian fungsional Rate Limiting menunjukkan bahwa rule pembatasan trafik UDP dan TCP SYN telah berjalan sesuai perannya.

4. Pengujian Fungsional Port Hardening

Pengujian fungsional *Port Hardening* dilakukan untuk memastikan bahwa akses layanan manajemen router telah dibatasi sesuai rancangan. Pengujian ini tidak menggunakan parameter CPU Load atau *traffic flood*, karena *Port Hardening* berfokus pada pengamanan akses administrasi router, bukan pada penurunan beban trafik serangan DDoS.

Pengujian dilakukan dengan memeriksa status layanan manajemen MikroTik, menguji akses Telnet dari sisi luar, menguji akses SSH dari jaringan LAN admin, menguji akses SSH dari sisi luar sebelum *port knocking*, menjalankan urutan *port knocking*, memeriksa IP sumber pada *address-list* *secured-admin*, serta menguji akses SSH dari sisi luar setelah proses *port knocking* berhasil.

Ringkasan hasil pengujian fungsional *Port Hardening* ditunjukkan pada Tabel 4.13. Tabel ini digunakan untuk memperlihatkan tahapan pengujian, hasil yang diharapkan, dan status keberhasilan pembatasan akses manajemen router.

Tabel 4. 13 Hasil Pengujian Fungsional Port Hardening

No	Pengujian	Hasil yang Diharapkan	Hasil
1	Cek service MikroTik	API, API-SSL, FTP, WWW, WWW-SSL, dan Telnet nonaktif	Berhasil
2	Akses Telnet dari sisi luar	Koneksi ditolak/gagal	Berhasil

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Pengujian	Hasil yang Diharapkan	Hasil
3	Akses SSH dari Ubuntu Desktop/LAN	SSH ke MikroTik utama berhasil	Berhasil
4	Akses SSH dari Kali sebelum knocking	SSH dari luar gagal	Berhasil
5	Port knocking 7001–7002–7003	IP Kali masuk secured-admin	Berhasil
6	Akses SSH dari Kali setelah knocking	SSH dari luar berhasil sementara	Berhasil

Berdasarkan Tabel 4.13, pengujian *Port Hardening* menunjukkan bahwa layanan manajemen router telah dibatasi sesuai rancangan. Layanan yang tidak digunakan berada dalam kondisi nonaktif, akses dari jaringan lokal tetap dapat dilakukan, sedangkan akses dari sisi luar hanya dapat dilakukan setelah sumber berhasil melewati proses *port knocking*.

Status layanan manajemen MikroTik setelah proses *Port Hardening* ditunjukkan pada Gambar 4.23. Pengujian ini dilakukan untuk memastikan bahwa layanan yang tidak diperlukan telah dinonaktifkan dan layanan administrasi yang digunakan telah disesuaikan.

```
[admin@MikrotikUtama] > /ip service print
Flags: D - DYNAMIC; X - DISABLED, I - INVALID
Columns: NAME, PORT, PROTO, CERTIFICATE, VRF, MAX-SESSIONS
#  NAME      PORT  PROTO  CERTIFICATE  VRF  MAX-SESSIONS
0  X ftp       21    tcp       none        main  20
1  I dhcp      67    udp       none        main  20
2  I dhcpclient 68    udp       none        main  20
3  X www      80    tcp       none        main  20
4  X www-ssl  443   tcp       none        main  20
5  I btest    2000  tcp       none        main  20
6  X ssh      2222  tcp       none        main  20
7  X telnet   2332  tcp       none        main  20
8  I discover 5678  udp       none        main  20
9  I winbox   7090  tcp       none        main  20
10 X api      8728  tcp       none        main  20
11 X api-ssl  8729  tcp       none        main  20
[admin@MikrotikUtama] >
```

Gambar 4. 23 Status Layanan Manajemen Setelah Port Hardening

Berdasarkan Gambar 4.23, layanan seperti API, API-SSL, FTP, WWW, WWW-SSL, dan Telnet berada dalam kondisi nonaktif. SSH digunakan sebagai akses terminal administrasi, sedangkan *Winbox* tetap digunakan

sebagai akses konfigurasi berbasis GUI. Kondisi ini menunjukkan bahwa permukaan akses manajemen router telah dikurangi.

Pengujian berikutnya dilakukan untuk memastikan bahwa Telnet tidak dapat digunakan dari sisi luar jaringan setelah layanan tersebut dinonaktifkan. Hasil pengujian akses Telnet ditunjukkan pada Gambar 4.24.

```
(kali@kali)-[~]
$ telnet 198.51.100.1 2332
Trying 198.51.100.1 ...
telnet: Unable to connect to remote host: Connection timed out
```

Gambar 4. 24 Pengujian Akses Telnet dari Sisi Luar Setelah Dinonaktifkan

Berdasarkan Gambar 4.24, akses Telnet dari sisi luar tidak berhasil dilakukan. Hasil ini sesuai dengan rancangan *Port Hardening* karena Telnet tidak digunakan dalam konfigurasi akhir dan dinonaktifkan untuk mengurangi risiko akses terminal yang tidak aman.

Selanjutnya, dilakukan pengujian akses SSH dari jaringan admin internal menggunakan Ubuntu Desktop. Pengujian ini bertujuan untuk memastikan bahwa administrator pada sisi LAN tetap dapat mengakses router untuk kebutuhan konfigurasi dan pemantauan.

```
(kali@kali)-[~]
$ nc -zv 198.51.100.1 7001
198.51.100.1: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [198.51.100.1] 7001 (?): Connection refused

(kali@kali)-[~]
$ nc -zv 198.51.100.1 7002
198.51.100.1: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [198.51.100.1] 7002 (?): Connection refused

(kali@kali)-[~]
$ nc -zv 198.51.100.1 7003
198.51.100.1: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [198.51.100.1] 7003 (?): Connection refused

(kali@kali)-[~]
$ ssh admin@198.51.100.1 -p 2222
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
admin@198.51.100.1's password: 
```

Gambar 4. 25 Proses Port Knocking dari Jaringan Luar

Berdasarkan Gambar 4.25, akses SSH dari Ubuntu Desktop pada jaringan LAN berhasil dilakukan menuju MikroTik utama. Hal ini menunjukkan bahwa pembatasan akses tidak mengganggu kebutuhan administrasi dari jaringan internal yang telah diizinkan.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Setelah akses internal dipastikan berjalan, pengujian dilakukan dari sisi luar jaringan menggunakan Kali Linux sebelum proses *port knocking*. Pengujian ini bertujuan untuk memastikan bahwa akses SSH dari luar tidak dapat dilakukan secara langsung.

```
[admin@MikrotikUtama] > client_loop: send disconnect: Broken pipe
alvito0731@alvito0731-VirtualBox: $ ssh admin@192.168.10.1 -p 2222
admin@192.168.10.1's password:

MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTT      KKK
MMM MMMM MMM III KKK KKK RRRRRR 000000 TTT III KKK KKK
MMM MM MMM III KKKKK RRR RRR 000 000 TTT III KKKKK
MMM MMM III KKK KKK RRRRRR 000 000 TTT III KKK KKK
MMM MMM III KKK KKK RRR RRR 000000 TTT III KKK KKK

MikroTik RouterOS 7.21.4 (c) 1999-2026 https://www.mikrotik.com/

Press F1 for help

[admin@MikrotikUtama] >
```

Gambar 4. 26 Pengujian Akses SSH dari Jaringan Admin Internal

Berdasarkan Gambar 4.26, akses SSH dari Kali Linux sebelum melakukan *port knocking* tidak berhasil. Kondisi ini menunjukkan bahwa layanan manajemen dari sisi luar tidak terbuka bebas dan hanya dapat diakses setelah melalui validasi tambahan.

Tahap berikutnya adalah menjalankan proses *port knocking* dari sisi luar jaringan. Urutan port yang digunakan pada penelitian ini adalah 7001, 7002, dan 7003. Hasil proses *port knocking* ditunjukkan pada Gambar 4.27.

```
(kali@kali)-[~]
$ ssh admin@198.51.100.1 -p 2222
ssh: connect to host 198.51.100.1 port 2222: Connection timed out
(kali@kali)-[~]
```

Gambar 4. 27 Pengujian Akses SSH dari Sisi Luar Sebelum Port Knocking

Berdasarkan Gambar 4.27, Kali Linux melakukan akses ke port 7001, 7002, dan 7003 secara berurutan. Urutan ini digunakan sebagai validasi agar IP sumber dapat dikenali sebagai alamat yang berhak memperoleh akses sementara ke layanan manajemen.

Setelah proses *port knocking* dilakukan, dilakukan pemeriksaan pada *address-list* *secured-admin*. Pemeriksaan ini bertujuan untuk

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

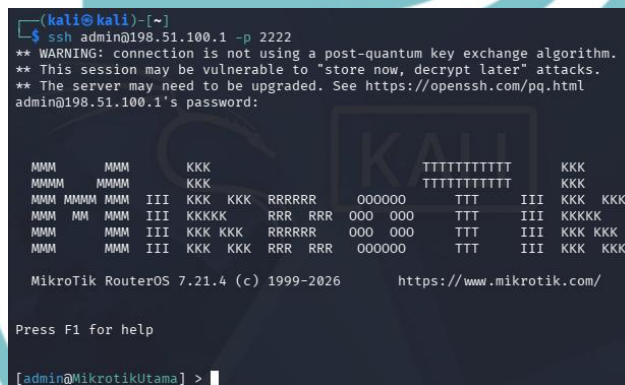
memastikan bahwa IP sumber dari Kali Linux telah masuk ke daftar alamat yang diizinkan sementara.

```
[admin@MikrotikUtama] > /ip firewall address-list print where list=secured-admin
Flags: D - DYNAMIC
Columns: LIST, ADDRESS, CREATION-TIME, TIMEOUT
# LIST ADDRESS CREATION-TIME TIMEOUT
0 D secured-admin 198.51.100.2 2026-05-17 10:26:13 9m17s
[admin@MikrotikUtama] >
```

Gambar 4. 28 IP Sumber yang Berhasil Masuk Address-List secured-admin

Berdasarkan Gambar 4.28, IP sumber dari jaringan luar telah masuk ke dalam *address-list* secured-admin. Hal ini menunjukkan bahwa proses *port knocking* berhasil dilakukan dan router memberikan izin akses sementara kepada sumber tersebut.

Pengujian terakhir dilakukan dengan mengakses SSH dari Kali Linux setelah IP sumber masuk ke *address-list* secured-admin. Hasil pengujian akses SSH setelah proses *port knocking* ditunjukkan pada Gambar 4.29.



```
(kali@kali) ~$ ssh admin@198.51.100.1 -p 2222
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
admin@198.51.100.1's password:

MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMM     MMMM     KKK
MMM  MMMM  MMM  III  KKK  KKK  RRRRRR  000000  TTT  III  KKK  KKK
MMM  MM  MMM  III  KKKKK  RRR  RRR  000 000  TTT  III  KKKKK
MMM  MMM  III  KKK  KKK  RRRRRR  000 000  TTT  III  KKK  KKK
MMM      MMM  III  KKK  KKK  RRR  RRR  000000  TTT  III  KKK  KKK

MikroTik RouterOS 7.21.4 (c) 1999-2026      https://www.mikrotik.com/
Press F1 for help

[admin@MikrotikUtama] >
```

Gambar 4. 29 Pengujian Akses SSH dari Sisi Luar Setelah Port Knocking

Berdasarkan Gambar 4.29, akses SSH dari sisi luar berhasil dilakukan setelah proses *port knocking* selesai dan IP sumber masuk ke secured-admin. Hasil ini menunjukkan bahwa *Port Hardening* bekerja sesuai rancangan, yaitu menolak akses langsung dari luar tetapi tetap menyediakan akses sementara bagi sumber yang telah tervalidasi.

5. Pengujian Fungsional Simulasi RTBH

Pengujian fungsional simulasi RTBH dilakukan untuk memastikan bahwa *blackhole route* pada router *upstream* dapat membuang trafik

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

menuju router MikroTik utama. Pengujian dilakukan dengan membandingkan kondisi sebelum dan sesudah *blackhole route* diaktifkan. Pada kondisi normal, trafik dari Kali Linux menuju IP publik modem simulasi masih diteruskan ke alamat WAN MikroTik utama. Setelah *blackhole route* menuju 192.168.18.20/32 diaktifkan pada router *upstream*, trafik menuju MikroTik utama tidak lagi diteruskan melalui jalur normal, tetapi dibuang pada sisi *upstream*.

Ringkasan hasil pengujian fungsional simulasi RTBH ditunjukkan pada Tabel 4.14. Tabel ini digunakan untuk memperlihatkan kondisi sebelum RTBH aktif, proses aktivasi *blackhole route*, serta perubahan kondisi trafik setelah RTBH diterapkan.

Tabel 4. 14 Hasil Pengujian Fungsional Simulasi RTBH

No	Pengujian	Hasil yang Diharapkan	Hasil
1	Kondisi sebelum RTBH	Trafik dari Kali masih terlihat di WAN MikroTik utama	Berhasil
2	Aktivasi <i>blackhole route</i> di <i>upstream</i>	Route <i>blackhole</i> menuju 192.168.18.20/32 aktif	Berhasil
3	Kondisi setelah RTBH aktif	Trafik tidak lagi diteruskan ke MikroTik utama	Berhasil
4	Monitoring WAN MikroTik utama	Traffic WAN turun atau mendekati nol	Berhasil

Berdasarkan Tabel 4.14, simulasi RTBH menunjukkan perubahan alur trafik setelah *blackhole route* diaktifkan pada router *upstream*. Sebelum RTBH aktif, trafik masih diteruskan menuju MikroTik utama. Setelah RTBH aktif, trafik menuju alamat WAN MikroTik utama tidak lagi diteruskan, sehingga beban trafik pada router utama dapat dikurangi.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Kondisi sebelum RTBH diaktifkan ditunjukkan pada Gambar 4.30. Pada tahap ini, trafik dari Kali Linux masih dikirim menuju IP publik modem simulasi dan diteruskan oleh router *upstream* ke *interface* WAN MikroTik utama.

```
[admin@MikrotikUtama] > /tool torch interface=ether1
Columns: MAC-PROTOCOL, IP-PROTOCOL, DSCP, SRC-ADDRESS, DST-ADDRESS, TX, RX, TX-PACKETS, RX-PACKETS
MAC-PROTOCOL IP-PROTOCOL DSCP SRC-ADDRESS DST-ADDRESS TX RX TX-PACKETS RX-PACKETS
ip icmp 0 198.51.100.2 192.168.18.20 784bps 784bps 1 1
```

Gambar 4. 30 Trafik dari Kali Masih Diteruskan ke MikroTik Utama Sebelum RTBH

Berdasarkan Gambar 4.30, trafik dari Kali Linux masih terlihat masuk pada *interface* WAN MikroTik utama. Kondisi ini menunjukkan bahwa sebelum *blackhole route* diaktifkan, router *upstream* masih meneruskan trafik menuju alamat WAN MikroTik utama secara normal.

Tahap berikutnya adalah mengaktifkan *blackhole route* pada router *upstream*. Aktivasi ini dilakukan agar trafik menuju alamat 192.168.18.20/32 tidak lagi diteruskan ke MikroTik utama, melainkan dibuang pada sisi *upstream*. Kondisi *blackhole route* yang telah aktif ditunjukkan pada Gambar 4.31.

```
[admin@ModemUpstream] > /ip route enable [find comment="Simulasi RTBH - Blackhole trafik menuju MikroTik utama"]
[admin@ModemUpstream] > /ip route print
Flags: D - DYNAMIC; A - ACTIVE; c - CONNECT, s - STATIC
Columns: DST-ADDRESS, GATEWAY, ROUTING-TABLE, DISTANCE
# DST-ADDRESS GATEWAY ROUTING-TABLE DISTANCE
Dac 192.168.18.0/24 ether2 main 0
;; Simulasi RTBH - Blackhole trafik menuju MikroTik utama
0 As 192.168.18.20/32 main 1
Dac 198.51.100.0/24 ether1 main 0
[admin@ModemUpstream] >
```

Gambar 4. 31 Aktivasi Blackhole Route pada Router Upstream

Berdasarkan Gambar 4.31, *blackhole route* menuju 192.168.18.20/32 telah aktif pada router *upstream*. Route ini menjadi jalur pembuangan trafik menuju alamat WAN MikroTik utama, sehingga trafik dari sisi luar tidak lagi diteruskan melalui jalur normal.

Setelah *blackhole route* aktif, dilakukan pengujian konektivitas dari Kali Linux menuju IP publik modem simulasi. Pengujian ini bertujuan untuk melihat perubahan akses setelah trafik menuju MikroTik utama

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

dibuang pada sisi *upstream*. Hasil pengujian konektivitas setelah RTBH diaktifkan ditunjukkan pada Gambar 4.32.

```
(kali@kali)-[~]
$ ping 198.51.100.1
PING 198.51.100.1 (198.51.100.1) 56(84) bytes of data.
```

Gambar 4. 32 Pengujian Konektivitas Setelah RTBH Diaktifkan

Berdasarkan Gambar 4.32, konektivitas menuju target mengalami gangguan setelah RTBH diaktifkan. Kondisi ini sesuai dengan karakteristik RTBH, karena seluruh trafik menuju IP target dibuang tanpa membedakan trafik normal dan trafik serangan. Dengan demikian, RTBH dapat mengurangi trafik ke router utama, tetapi berdampak pada ketersediaan akses ke alamat target.

Pemantauan terakhir dilakukan pada *interface* WAN MikroTik utama setelah RTBH aktif. Pemantauan ini bertujuan untuk memastikan bahwa trafik yang sebelumnya masuk ke router utama tidak lagi terlihat atau berada pada nilai sangat rendah. Hasil monitoring *interface* WAN setelah RTBH diaktifkan ditunjukkan pada Gambar 4.33.

```
[admin@MikrotikUtama] > /tool torch interface=ether1
```

Gambar 4. 33 Kondisi Interface WAN MikroTik Setelah RTBH Diaktifkan

Berdasarkan Gambar 4.33, *traffic* pada *interface* WAN MikroTik utama mengalami penurunan atau mendekati nol setelah *blackhole route* aktif. Hal ini menunjukkan bahwa trafik menuju MikroTik utama telah dibuang pada router *upstream* sebelum mencapai router utama. Dengan demikian, pengujian fungsional simulasi RTBH menunjukkan bahwa mekanisme pembuangan trafik pada sisi *upstream* telah berjalan sesuai rancangan.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

B. Data Hasil Pengujian UDP Flood

Pengujian *UDP Flood* dilakukan untuk mengetahui kondisi router MikroTik utama ketika menerima trafik UDP dalam jumlah besar secara terus-menerus. Serangan dijalankan dari Kali Linux menggunakan *hping3* dengan mode *flood* menuju IP publik modem simulasi. Trafik tersebut kemudian diteruskan oleh router *upstream* menuju *interface* WAN MikroTik utama.

Pengujian ini dilakukan pada beberapa skenario, yaitu tanpa mitigasi, *Firewall RAW*, *Firewall RAW* dan *Rate Limiting*, serta simulasi RTBH. Parameter yang diamati meliputi CPU Load, Free Memory, *traffic* WAN pada *interface* ether1, dan jumlah paket yang diblokir oleh rule mitigasi apabila rule tersebut aktif.

Simulasi serangan *UDP Flood* yang dijalankan dari Kali Linux ditunjukkan pada Gambar 4.34. Gambar ini digunakan sebagai bukti bahwa trafik *UDP Flood* dikirim menuju IP publik modem simulasi pada tahap pengujian.

```
(kali@kali)-[~]
$ sudo hping3 --udp -p 53 --flood 198.51.100.1
[sudo] password for kali:
HPING 198.51.100.1 (eth0 198.51.100.1): udp mode set, 28 headers + 0 data bytes
es
hping in flood mode, no replies will be shown
```

Gambar 4. 34 Simulasi Serangan UDP Flood pada Tahap Pengujian

Berdasarkan Gambar 4.34, Kali Linux menjalankan serangan *UDP Flood* menuju IP publik modem simulasi. Trafik tersebut digunakan sebagai beban uji untuk melihat perubahan kondisi router pada setiap skenario mitigasi. Setelah serangan dijalankan, data CPU Load, Free Memory, dan *traffic* WAN dicatat secara berkala selama periode pengamatan.

1. Hasil Pengujian UDP Flood Tanpa Mitigasi

Pada skenario ini, rule *Firewall RAW* dan *Rate Limiting* dinonaktifkan sehingga router MikroTik utama menerima trafik *UDP Flood* tanpa perlindungan mitigasi DDoS. Kondisi ini digunakan sebagai data dasar atau *baseline* untuk membandingkan perubahan performa router pada skenario mitigasi berikutnya.

Data hasil pengujian *UDP Flood* tanpa mitigasi disajikan pada Tabel 4.15. Tabel ini menunjukkan perubahan CPU Load, Free Memory, dan *traffic* WAN pada *interface* ether1 selama 10 menit pengamatan.

Tabel 4. 15 Hasil Pengujian UDP Flood Tanpa Mitigasi

Menit	CPU Load	Free Memory	Traffic WAN ether1
1	62%	30328KiB	2.2Mbps
2	79%	29820KiB	2.4Mbps
3	63%	29156KiB	2.0Mbps
4	74%	29080KiB	1972.8kbps
5	64%	28344KiB	1924.0kbps
6	72%	28576KiB	1691.0kbps
7	84%	28492KiB	2.0Mbps
8	49%	28356KiB	1737.7kbps
9	80%	28180KiB	1838.2kbps
10	56%	28084KiB	1754.9kbps

Berdasarkan Tabel 4.15, data menunjukkan kondisi router saat menerima *UDP Flood* tanpa mitigasi. Nilai CPU Load, Free Memory, dan *traffic* WAN pada tabel ini digunakan sebagai data pembanding terhadap skenario mitigasi berikutnya. Pembahasan lebih lanjut mengenai perubahan nilai pada setiap skenario dijelaskan pada subbab 4.4.4.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
[admin@MikroTik] > /system resource monitor once
cpu-used: 62%
free-memory: 30328KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 79%
free-memory: 29820KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 63%
free-memory: 29156KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 74%
free-memory: 29080KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 64%
free-memory: 28344KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 72%
free-memory: 28576KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 84%
free-memory: 28492KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 49%
free-memory: 28356KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 80%
free-memory: 28180KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 56%
free-memory: 28084KiB
[admin@MikroTik] >
```

Gambar 4. 35 Snapshot UDP tanpa mitigasi

Berdasarkan Gambar 4.35, nilai *CPU Load* dan *Free Memory* saat pengujian *UDP Flood* tanpa mitigasi dicatat langsung menggunakan perintah `/system resource monitor once`. Data ini menjadi bukti pendukung kondisi sumber daya router pada Tabel 4.15.

2. Hasil Pengujian UDP Flood dengan Firewall RAW

Pada skenario ini, mekanisme deteksi *attacker* dan rule *drop Firewall RAW* diaktifkan. Ketika sumber serangan terdeteksi, IP *attacker* akan dimasukkan ke dalam *address-list* *ddos-attackers*. Setelah itu, trafik lanjutan dari IP tersebut dibuang pada tahap *prerouting* oleh *Firewall RAW*.

Monitoring resource dan *traffic* dilakukan saat serangan *UDP Flood* berlangsung untuk mencatat kondisi *CPU Load*, *Free Memory*, dan *traffic* WAN pada *interface* *ether1*. Hasil monitoring tersebut ditunjukkan pada Gambar 4.36.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
[admin@MikroTik] > /interface monitor-traffic ether1
name: ether1
rx-packets-per-second: 4 349
rx-bits-per-second: 2.0Mbps
fp-rx-packets-per-second: 0
fp-rx-bits-per-second: 0bps
rx-drops-per-second: 0
rx-errors-per-second: 0
tx-packets-per-second: 103
tx-bits-per-second: 57.6kbps
fp-tx-packets-per-second: 0
fp-tx-bits-per-second: 0bps
tx-drops-per-second: 0
tx-queue-drops-per-second: 0
tx-errors-per-second: 0
-- [Q quit|D dump|C-z pause]

[admin@MikroTik] > /system resource monitor
cpu-used: 63%
free-memory: 29156KiB
-- [Q quit|D dump|C-z pause]
```

Gambar 4. 36 Monitoring Resource dan Traffic Saat UDP Flood Tanpa Mitigasi

Berdasarkan Gambar 4.36, proses monitoring dilakukan pada router MikroTik utama ketika UDP Flood berjalan dengan Firewall RAW aktif. Data dari tampilan resource dan traffic tersebut digunakan sebagai dasar pencatatan nilai pada tabel hasil pengujian.

Selain resource dan traffic, pengujian ini juga mencatat jumlah paket yang dibuang oleh rule Firewall RAW. Statistik dropped packets pada rule RAW ditunjukkan pada Gambar 4.37.

```
[admin@MikroTik] > /interface monitor-traffic ether1
name: ether1
rx-packets-per-second: 4 580
rx-bits-per-second: 2.1Mbps
fp-rx-packets-per-second: 0
fp-rx-bits-per-second: 0bps
rx-drops-per-second: 0
rx-errors-per-second: 0
tx-packets-per-second: 0
tx-bits-per-second: 0bps
fp-tx-packets-per-second: 0
fp-tx-bits-per-second: 0bps
tx-drops-per-second: 0
tx-queue-drops-per-second: 0
tx-errors-per-second: 0
-- [Q quit|D dump|C-z pause]

[admin@MikroTik] > /system resource monitor
cpu-used: 49%
free-memory: 54656KiB
-- [Q quit|D dump|C-z pause]
```

```
;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop 8 104 572 289 449
[admin@MikroTik] > /ip firewall raw print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN ACTION BYTES PACKETS
;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop 15 984 780 570 885
[admin@MikroTik] > /ip firewall raw print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN ACTION BYTES PACKETS
;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop 22 308 972 796 749
[admin@MikroTik] >
```

Gambar 4. 37 Statistik Dropped Packets Firewall RAW pada Pengujian UDP Flood

Berdasarkan Gambar 4.37, rule Firewall RAW menunjukkan adanya paket yang dibuang selama pengujian UDP Flood. Nilai counter

tersebut digunakan untuk mengetahui jumlah paket dari sumber *attacker* yang berhasil diblokir pada tahap *prerouting*.

Data hasil pengujian UDP *Flood* dengan *Firewall RAW* disajikan pada Tabel 4.16. Tabel ini memuat data CPU Load, Free Memory, *traffic* WAN, dan jumlah *dropped packets* selama 10 menit pengamatan.

Tabel 4. 16 Hasil Pengujian UDP Flood dengan Firewall RAW

Menit	CPU Load	Free Memory	Traffic WAN ether1	Dropped Packets
1	58%	56884KiB	1304.3kbps	289 449
2	70%	55612KiB	1395.7kbps	570 885
3	49%	54656KiB	2.1Mbps	796 749
4	73%	55592KiB	1532.7kbps	1 029 556
5	69%	56444KiB	1237.1kbps	1 256 322
6	56%	55560KiB	1654.1kbps	1 491 309
7	50%	55560KiB	1244.3kbps	1 736 816
8	52%	55560KiB	1326.2kbps	1 983 362
9	73%	55560KiB	1378.8kbps	2 236 889
10	56%	55560KiB	1872.0kbps	2 480 400

Berdasarkan Tabel 4.16, data menunjukkan kondisi router saat UDP *Flood* diuji dengan *Firewall RAW* aktif. Selain CPU Load, Free Memory, dan *traffic* WAN, tabel ini juga mencatat peningkatan jumlah paket yang dibuang oleh rule RAW. Data tersebut digunakan sebagai pembandingan terhadap kondisi tanpa mitigasi dan skenario mitigasi lainnya pada subbab analisis

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
[admin@MikroTik] > /system resource monitor once
cpu-used: 58%
free-memory: 56884KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 70%
free-memory: 55612KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 49%
free-memory: 54656KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 73%
free-memory: 55592KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 69%
free-memory: 56444KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 56%
free-memory: 55560KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 50%
free-memory: 55560KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 52%
free-memory: 55560KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 73%
free-memory: 55560KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 56%
free-memory: 55560KiB
```

Gambar 4. 38 Snapshot UDP Firewall Raw

Berdasarkan Gambar 4.38, nilai *CPU Load* dan *Free Memory* saat pengujian *UDP Flood* dengan *Firewall RAW* diperoleh langsung dari monitoring router MikroTik. Gambar ini mendukung data pada Tabel 4.16 bahwa kondisi sumber daya router dicatat selama RAW aktif.

3. Hasil Pengujian UDP Flood dengan Firewall RAW dan Rate Limiting

Pada skenario ini, *Firewall RAW* dan *Rate Limiting* diaktifkan secara bersamaan. *Firewall RAW* berfungsi untuk memblokir sumber serangan yang telah terdeteksi, sedangkan *Rate Limiting* digunakan untuk membatasi trafik UDP berlebih yang masih sempat diproses sebelum pemblokiran RAW mengambil alih.

Data hasil pengujian *UDP Flood* dengan kombinasi *Firewall RAW* dan *Rate Limiting* disajikan pada Tabel 4.17. Tabel ini memuat CPU Load, Free Memory, *traffic* WAN, jumlah *dropped packets* pada *Firewall RAW*, serta jumlah paket UDP yang dibatasi oleh *Rate Limiting* selama 10 menit pengamatan.

Tabel 4. 17 Hasil Pengujian UDP Flood dengan Firewall RAW dan Rate Limiting

Menit	CPU Load	Free Memory	Traffic WAN ether1	Dropped Packets	Dropped Packets Rate Limiting UDP
1	66%	55496KiB	1330.0kbps	443 267	132
2	69%	55496KiB	2.5Mbps	815 263	132
3	62%	55560KiB	2.4Mbps	1 192 462	132
4	67%	55400KiB	2.6Mbps	1 561 843	132
5	77%	55368KiB	2.0Mbps	1 937 513	132
6	72%	55356KiB	1760.5kbps	2 303 122	132
7	65%	55356KiB	1667.0kbps	2 667 219	132
8	58%	55356KiB	1799.5kbps	3 023 151	132
9	62%	55292KiB	2.0Mbps	3 256 396	132
10	70%	55292KiB	1905.5kbps	3 617 384	132

Berdasarkan Tabel 4.17, data menunjukkan kondisi router saat UDP Flood diuji dengan kombinasi *Firewall RAW* dan *Rate Limiting*. Tabel ini juga memperlihatkan bahwa paket yang diblokir oleh RAW dan paket yang diproses oleh *Rate Limiting* dicatat secara terpisah. Data tersebut digunakan sebagai pembandingan terhadap skenario tanpa mitigasi dan skenario *Firewall RAW* saja.

Statistik paket yang diblokir pada skenario UDP Flood dengan *Firewall RAW* dan *Rate Limiting* ditunjukkan pada Gambar 4.39. Gambar ini digunakan untuk memperlihatkan *counter rule* mitigasi yang aktif selama pengujian berlangsung.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```

Terminal <6>
# CHAIN ACTION BYTES PACKETS
;;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop 53 999 624 1 928 558
[admin@MikroTik] > /ip firewall raw reset-counters
numbers: 0
[admin@MikroTik] > /ip firewall raw print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN ACTION BYTES PACKETS
;;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop 0 0
[admin@MikroTik] > /ip firewall raw print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN ACTION BYTES PACKETS
;;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop 12 411 476 443 267
[admin@MikroTik] > /ip firewall raw print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN ACTION BYTES PACKETS
;;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop 22 827 364 815 263
[admin@MikroTik] > /ip firewall raw print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN ACTION BYTES PACKETS
;;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop 33 388 936 1 192 462
[admin@MikroTik] > /ip firewall raw print stats

[admin@MikroTik] > /interface monitor-traffic ether1
name: ether1
rx-packets-per-second: 5 147
rx-bits-per-second: 2.4Mbps
fp-rx-packets-per-second: 0
fp-rx-bits-per-second: 0bps
rx-drops-per-second: 0
rx-errors-per-second: 0
tx-packets-per-second: 1
tx-bits-per-second: 3.0kbps
fp-tx-packets-per-second: 0
fp-tx-bits-per-second: 0bps
tx-drops-per-second: 0
tx-queue-drops-per-second: 0
tx-errors-per-second: 0
[Q quit|D dump|C-z pause]

[admin@MikroTik] > /system resource monitor
cpu-used: 62%
free-memory: 55560KiB
[Q quit|D dump|C-z pause]

Terminal <7>
0 input jump 6 076 217
;;; UDP masih dalam batas normal
1 detect-udp-flood return 5 908 211
;;; Masukkan sumber UDP Flood ke ddos-attackers
2 detect-udp-flood add-src-to-address-list 168 6
;;; Kembali ke chain input setelah deteksi UDP
3 detect-udp-flood return 168 6
;;; Deteksi awal TCP SYN Flood menuju router utama
4 input jump 0 0
;;; TCP SYN masih dalam batas normal
5 detect-syn-flood return 0 0
;;; Masukkan sumber SYN Flood ke ddos-attackers
6 detect-syn-flood add-src-to-address-list 0 0
;;; Kembali ke chain input setelah deteksi SYN
7 detect-syn-flood return 0 0
;;; Masuk ke chain Rate Limiting DDoS
8 input jump 6 076 217
;;; Rate Limit - Drop total koneksi TCP baru berlebih per IP
9 rate-limit-ddos drop 0 0
;;; Rate Limit - TCP SYN masih dalam batas
10 rate-limit-ddos return 0 0
;;; Rate Limit - Drop TCP SYN berlebih
11 rate-limit-ddos drop 0 0
;;; Rate Limit - UDP masih dalam batas
12 rate-limit-ddos return 2 380 85
;;; Rate Limit - Drop UDP berlebih
13 rate-limit-ddos drop 3 696 132
;;; Keluar dari chain Rate Limiting
14 rate-limit-ddos return 0 0
;;; Port Hardening - Izinkan SSH dan Winbox dari LAN admin
15 input accept 0 0
;;; Port Knocking - Tahap 1
16 input add-src-to-address-list 0 0
;;; Port Knocking - Tahap 2
17 input add-src-to-address-list 0 0
;;; Port Knocking - Tahap 3 berhasil, masukkan secured-admin
18 input add-src-to-address-list 0 0
19 input accept 0 0
;;; Port Hardening - Drop akses SSH dan Winbox dari luar yang belum knocking
20 input drop 0 0
[admin@MikroTik] > /ip firewall filter print stats
  
```

Gambar 4. 39 Statistik Dropped Packets pada Pengujian UDP Flood dengan Firewall RAW dan Rate Limiting

Berdasarkan Gambar 4.39, *counter* rule mitigasi menunjukkan adanya paket yang diblokir selama pengujian UDP *Flood*. Nilai tersebut menjadi data pendukung untuk tabel hasil pengujian dan akan dianalisis lebih lanjut pada subbab 4.4.4.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
[admin@MikroTik] > /system resource monitor once
cpu-used: 66%
free-memory: 55496KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 69%
free-memory: 55496KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 62%
free-memory: 55560KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 67%
free-memory: 55400KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 77%
free-memory: 55368KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 72%
free-memory: 55356KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 65%
free-memory: 55356KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 58%
free-memory: 55356KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 62%
free-memory: 55292KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 70%
free-memory: 55292KiB
[admin@MikroTik] >
```

Gambar 4. 40 Snapshot UDP Firewall Raw dan Rate Limiting

Berdasarkan Gambar 4.40, nilai *CPU Load* dan *Free Memory* saat pengujian *UDP Flood* dengan kombinasi *Firewall RAW* dan *Rate Limiting* dicatat langsung dari router. Data ini menjadi bukti pendukung kondisi sumber daya router pada Tabel 4.17.

4. Hasil Pengujian UDP Flood dengan Simulasi RTBH
Pada skenario RTBH, blackhole route diaktifkan pada router upstream atau modem simulasi. Mekanisme ini membuat trafik menuju MikroTik utama dibuang pada sisi upstream sebelum mencapai interface WAN router utama. Oleh karena itu, parameter yang tetap diamati adalah CPU Load, Free Memory, dan traffic WAN pada MikroTik utama untuk melihat kondisi router setelah trafik dibuang lebih awal.

Sebelum data pengujian dicatat, blackhole route pada router upstream diaktifkan terlebih dahulu. Aktivasi route ini dilakukan agar trafik menuju alamat WAN MikroTik utama 192.168.18.20/32 tidak lagi

diteruskan ke router utama. Kondisi aktivasi blackhole route ditunjukkan pada Gambar 4.41.

```
[admin@ModemUpstream] > /ip firewall nat print
Flags: X - disabled, I - invalid; D - dynamic
0    ::: teruskan trafik
     chain=dstnat action=dst-nat to-addresses=192.168.18.20 dst-address=198.51.100.1 log=no
     log-prefix=""
[admin@ModemUpstream] > /ip route print
Flags: D - DiNAmic; A - ACTIVE; c - CONNECT, s - STATIC
Columns: DST-ADDRESS, GATEWAY, ROUTING-TABLE, DISTANCE
#    DST-ADDRESS    GATEWAY  ROUTING-TABLE  DISTANCE
DAdc 192.168.18.0/24 ether2    main           0
::: Simulasi RTBH - Blackhole trafik menuju MikroTik utama
0    As 192.168.18.20/32      main           1
DAdc 198.51.100.0/24 ether1    main           0
[admin@ModemUpstream] >
```

Gambar 4. 41 Aktivasi Blackhole Route pada Pengujian UDP Flood

Berdasarkan Gambar 4.41, *blackhole route* menuju alamat 192.168.18.20/32 telah aktif pada router *upstream*. Dengan kondisi tersebut, trafik *UDP Flood* yang diarahkan ke IP publik modem simulasi akan dibuang pada sisi *upstream* sebelum mencapai MikroTik utama.

Data hasil pengujian *UDP Flood* dengan simulasi RTBH disajikan pada Tabel 4.18. Tabel ini menunjukkan CPU Load, Free Memory, *traffic* WAN pada *interface* ether1, serta keterangan kondisi trafik selama 10 menit pengamatan.

Tabel 4. 18 Hasil Pengujian UDP Flood dengan Simulasi RTBH

Menit	CPU Load	Free Memory	Traffic WAN ether1	Keterangan
1	1%	54044KiB	0bps	Trafik dibuang di upstream
2	5%	53696KiB	0bps	Trafik dibuang di upstream
3	5%	53440KiB	0bps	Trafik dibuang di upstream
4	5%	53376KiB	0bps	Trafik dibuang di upstream

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Menit	CPU Load	Free Memory	Traffic WAN ether1	Keterangan
5	3%	53184KiB	0bps	Trafik dibuang di upstream
6	4%	53152KiB	0bps	Trafik dibuang di upstream
7	6%	53120KiB	0bps	Trafik dibuang di upstream
8	4%	53088KiB	0bps	Trafik dibuang di upstream
9	4%	52928KiB	5.9kbps	Trafik dibuang di upstream
10	6%	52928KiB	600bps	Trafik dibuang di upstream

Berdasarkan Tabel 4.18, data menunjukkan kondisi router MikroTik utama saat simulasi RTBH diterapkan pada pengujian *UDP Flood*. Nilai CPU Load, Free Memory, dan *traffic* WAN pada tabel ini digunakan sebagai pembanding terhadap skenario tanpa mitigasi, *Firewall RAW*, serta kombinasi *Firewall RAW* dan *Rate Limiting*. Pembahasan lebih lanjut mengenai perbandingan data disajikan pada subbab 4.4.4.

Monitoring resource dan *traffic* saat *UDP Flood* dengan RTBH aktif ditunjukkan pada Gambar 4.42. Gambar ini digunakan untuk memperlihatkan kondisi CPU, memori, dan *traffic* WAN pada MikroTik utama setelah trafik dibuang pada sisi *upstream*.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
[admin@MikroTik] > /system resource monitor once
cpu-used: 3%
free-memory: 53184KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 4%
free-memory: 53152KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 6%
free-memory: 53152KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 6%
free-memory: 53120KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 5%
free-memory: 53088KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 4%
free-memory: 53088KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 6%
free-memory: 52928KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 4%
free-memory: 52928KiB
[admin@MikroTik] >

Terminal <5>
tx-drops-per-second: 0
tx-queue-drops-per-second: 0
tx-errors-per-second: 0
[admin@MikroTik] > /interface monitor-traffic ether1 once
name: ether1
rx-packets-per-second: 4
rx-bits-per-second: 5.9kbps
fp-rx-packets-per-second: 0
fp-rx-bits-per-second: 0bps
rx-drops-per-second: 0
rx-errors-per-second: 0
tx-packets-per-second: 0
tx-bits-per-second: 0bps
fp-tx-packets-per-second: 0
fp-tx-bits-per-second: 0bps
tx-drops-per-second: 0
tx-queue-drops-per-second: 0
tx-errors-per-second: 0
[admin@MikroTik] > /interface monitor-traffic ether1 once
name: ether1
rx-packets-per-second: 0
rx-bits-per-second: 0bps
```

Gambar 4. 42 Monitoring Resource dan Traffic Saat UDP Flood dengan RTBH Aktif

Berdasarkan Gambar 4.42, monitoring menunjukkan kondisi router MikroTik utama ketika RTBH aktif. Tampilan tersebut menjadi pendukung data pada Tabel 4.18, khususnya untuk menunjukkan bahwa *traffic* menuju *interface* WAN router utama berada pada kondisi sangat rendah selama skenario RTBH berlangsung.



Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
[admin@MikroTik] > /system resource monitor once
cpu-used: 1%
free-memory: 54044KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 5%
free-memory: 53696KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 5%
free-memory: 53440KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 5%
free-memory: 53376KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 3%
free-memory: 53184KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 4%
free-memory: 53152KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 6%
free-memory: 53120KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 4%
free-memory: 53088KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 4%
free-memory: 52928KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 6%
free-memory: 52928KiB
[admin@MikroTik] >
```

Gambar 4. 43 Snapshot UDP simulasi RTBH

Berdasarkan Gambar 4.43, nilai *CPU Load* dan *Free Memory* saat pengujian *UDP Flood* dengan RTBH dicatat menggunakan `/system resource monitor once`. Data ini mendukung Tabel 4.18 bahwa beban router lebih rendah saat trafik dibuang melalui *blackhole route*.

C. Data Hasil Pengujian TCP SYN Flood

Pengujian berikutnya dilakukan menggunakan serangan *TCP SYN Flood*. Serangan dijalankan dari Kali Linux menuju IP publik modem simulasi menggunakan `hping3` dengan flag SYN. Trafik tersebut kemudian diteruskan oleh router *upstream* menuju *interface* WAN MikroTik utama.

Pengujian *TCP SYN Flood* dilakukan dengan pola skenario yang sama seperti *UDP Flood*, yaitu tanpa mitigasi, *Firewall RAW*, *Firewall RAW* dan *Rate Limiting*, serta simulasi RTBH. Pengujian ini bertujuan untuk memperoleh data pembandingan mengenai kondisi router saat menerima serangan berbasis protokol TCP.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Simulasi serangan TCP SYN *Flood* pada tahap pengujian ditunjukkan pada Gambar 4.44. Gambar ini digunakan sebagai bukti bahwa trafik TCP SYN *Flood* dikirim dari Kali Linux menuju IP publik modem simulasi.

```
(kali@kali)-[~]
$ sudo hping3 -S -p 80 --flood 198.51.100.1
HPING 198.51.100.1 (eth0 198.51.100.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Gambar 4. 44 Simulasi Serangan TCP SYN Flood pada Tahap Pengujian

Berdasarkan Gambar 4.44, Kali Linux menjalankan serangan TCP SYN *Flood* menggunakan *hping3*. Trafik tersebut digunakan sebagai beban uji untuk melihat kondisi router pada setiap skenario mitigasi. Data hasil pengamatan kemudian dicatat berdasarkan interval waktu yang telah ditentukan.

1. Hasil Pengujian TCP SYN Flood Tanpa Mitigasi

Pada skenario ini, seluruh mekanisme mitigasi DDoS dinonaktifkan. Router MikroTik utama menerima trafik TCP SYN *Flood* secara langsung tanpa penyaringan awal melalui *Firewall RAW* maupun pembatasan trafik menggunakan *Rate Limiting*. Kondisi ini digunakan sebagai data dasar atau *baseline* untuk dibandingkan dengan skenario mitigasi berikutnya.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Monitoring resource dan *traffic* saat TCP SYN Flood tanpa mitigasi ditunjukkan pada Gambar 4.45. Gambar ini memperlihatkan kondisi CPU Load, Free Memory, dan *traffic* WAN ketika router menerima trafik serangan tanpa perlindungan mitigasi.

```
[admin@MikroTik] > /interface monitor-traffic ether1
name: ether1
rx-packets-per-second: 2 743
rx-bits-per-second: 1316.5kbps
fp-rx-packets-per-second: 0
fp-rx-bits-per-second: 0bps
rx-drops-per-second: 0
rx-errors-per-second: 0
tx-packets-per-second: 2 743
tx-bits-per-second: 1316.5kbps
fp-tx-packets-per-second: 0
fp-tx-bits-per-second: 0bps
tx-drops-per-second: 0
tx-queue-drops-per-second: 0
tx-errors-per-second: 0
-- [Q quit|D dump|C-z pause]

Press F1 for help

[admin@MikroTik] > /system resource monitor
cpu-used: 100%
free-memory: 54032KiB
-- [Q quit|D dump|C-z pause]
```

Gambar 4. 45 Monitoring Resource dan Traffic Saat TCP SYN Flood Tanpa Mitigasi

Berdasarkan Gambar 4.45, monitoring dilakukan pada MikroTik utama ketika serangan TCP SYN Flood berjalan tanpa mitigasi. Data dari tampilan tersebut digunakan sebagai dasar pencatatan nilai CPU Load, Free Memory, dan *traffic* WAN pada tabel hasil pengujian.

Data hasil pengujian TCP SYN Flood tanpa mitigasi disajikan pada Tabel 4.19. Tabel ini menunjukkan kondisi CPU Load, Free Memory, dan *traffic* WAN pada *interface* ether1 selama 10 menit pengamatan.

Tabel 4. 19 Hasil Pengujian TCP SYN Flood Tanpa Mitigasi

Menit	CPU Load	Free Memory	Traffic WAN ether1
1	100%	55420KiB	1270.1kbps
2	100%	54032KiB	1316.5kbps
3	100%	53852KiB	1455.1kbps
4	100%	53820KiB	921.6kbps
5	100%	53756KiB	1090.0kbps
6	100%	53664KiB	1433.6kbps
7	100%	53692KiB	1064.5kbps
8	91%	53628KiB	1064.5kbps
9	100%	53640KiB	1329.2kbps
10	100%	53628KiB	1099.4kbps

Berdasarkan Tabel 4.19, data menunjukkan kondisi router saat menerima TCP SYN Flood tanpa mitigasi. Nilai CPU Load, Free Memory, dan traffic WAN pada tabel ini digunakan sebagai data pembandingan terhadap skenario Firewall RAW, kombinasi Firewall RAW dan Rate Limiting, serta simulasi RTBH. Pembahasan lebih lanjut mengenai perubahan nilai pada setiap skenario dijelaskan pada subbab 4.4.4.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
[admin@MikroTik] > /system resource monitor once
cpu-used: 100%
free-memory: 55420KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 100%
free-memory: 54032KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 100%
free-memory: 53852KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 100%
free-memory: 53820KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 100%
free-memory: 53756KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 100%
free-memory: 53664KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 100%
free-memory: 53692KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 91%
free-memory: 53628KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 100%
free-memory: 53640KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 100%
free-memory: 53628KiB
```

Gambar 4. 46 Snapshot TCP SYN tanpa mitigasi

Berdasarkan Gambar 4.46, nilai *CPU Load* dan *Free Memory* saat pengujian *TCP SYN Flood* tanpa mitigasi dicatat langsung dari router MikroTik. Data ini menjadi bukti pendukung bahwa router mengalami beban sumber daya selama serangan berlangsung, sesuai Tabel 4.19.

2. Hasil Pengujian TCP SYN Flood dengan Firewall RAW

Pada skenario ini, rule deteksi *attacker* dan *Firewall RAW* diaktifkan untuk menangani trafik *TCP SYN Flood*. Ketika IP sumber terindikasi mengirimkan trafik melebihi ambang batas, IP tersebut dimasukkan ke dalam *address-list* *ddos-attackers*. Setelah itu, trafik lanjutan dari IP yang sama dibuang oleh *Firewall RAW* pada tahap *prerouting*.

Statistik paket yang dibuang oleh *Firewall RAW* selama pengujian *TCP SYN Flood* ditunjukkan pada Gambar 4.47. Gambar ini digunakan untuk memperlihatkan bahwa rule RAW aktif dan mencatat paket yang berhasil diblokir selama proses pengujian berlangsung.

```
[admin@MikroTik] > /interface monitor-traffic
name: ether1
rx-packets-per-second: 3 371
rx-bits-per-second: 1618.0kbps
fp-rx-packets-per-second: 0
fp-rx-bits-per-second: 0bps
rx-drops-per-second: 0
rx-errors-per-second: 0
tx-packets-per-second: 0
tx-bits-per-second: 0bps
fp-tx-packets-per-second: 0
fp-tx-bits-per-second: 0bps
tx-drops-per-second: 0
tx-queue-drops-per-second: 0
tx-errors-per-second: 0
[Q quit|D dump|C-z pause]

[admin@MikroTik] > /ip firewall raw print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN ACTION BYTES PACKETS
;;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop 0 0
[admin@MikroTik] > /ip firewall raw print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN ACTION BYTES PACKETS
;;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop 8 719 600 217 990
[admin@MikroTik] >

[admin@MikroTik] > /system resource monitor
cpu-used: 49%
free-memory: 53584KiB
[Q quit|D dump|C-z pause]
```

Gambar 4. 47 Statistik Dropped Packets Firewall RAW pada Pengujian TCP SYN Flood

Berdasarkan Gambar 4.47, *counter* pada rule *Firewall RAW* menunjukkan adanya paket yang dibuang selama pengujian TCP SYN Flood. Nilai tersebut menjadi data pendukung untuk melihat jumlah paket yang berhasil diblokir oleh rule RAW pada tabel hasil pengujian. Data hasil pengujian TCP SYN Flood dengan *Firewall RAW* disajikan pada Tabel 4.20. Tabel ini memuat CPU Load, Free Memory, *traffic* WAN pada *interface* ether1, dan jumlah *dropped packets* selama 10 menit pengamatan.

Tabel 4. 20 Hasil Pengujian TCP SYN Flood dengan Firewall RAW

Menit	CPU Load	Free Memory	Traffic WAN ether1	Dropped Packets
1	49%	53584KiB	1618.0kbps	217 990
2	54%	53812KiB	1875.8kbps	517 657
3	49%	53748KiB	1766.7kbps	776 709
4	56%	53716KiB	2.5Mbps	1 023 323
5	55%	53556KiB	2.4Mbps	1 254 609
6	62%	53524KiB	2.3Mbps	1 499 102
7	59%	53524KiB	2.4Mbps	1 642 096
8	61%	53428KiB	1934.2kbps	1 784 319
9	48%	53364KiB	1033.2kbps	1 929 799

Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Menit	CPU Load	Free Memory	Traffic WAN ether1	Dropped Packets
10	58%	53076KiB	1747.7kbps	2 074 074

Berdasarkan Tabel 4.20, data menunjukkan kondisi router saat TCP SYN Flood diuji dengan *Firewall RAW* aktif. Tabel ini juga mencatat jumlah paket yang dibuang oleh rule RAW selama pengujian berlangsung. Data tersebut digunakan sebagai pembandingan terhadap kondisi tanpa mitigasi dan skenario mitigasi lainnya pada subbab analisis.

```

[admin@MikroTik] > /system resource monitor once
cpu-used: 49%
free-memory: 53584KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 54%
free-memory: 53812KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 49%
free-memory: 53748KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 56%
free-memory: 53716KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 55%
free-memory: 53556KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 62%
free-memory: 53524KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 59%
free-memory: 53524KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 61%
free-memory: 53428KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 48%
free-memory: 53364KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 58%
free-memory: 53076KiB
  
```

Gambar 4. 48 Snapshot TCP SYN Firewall Raw

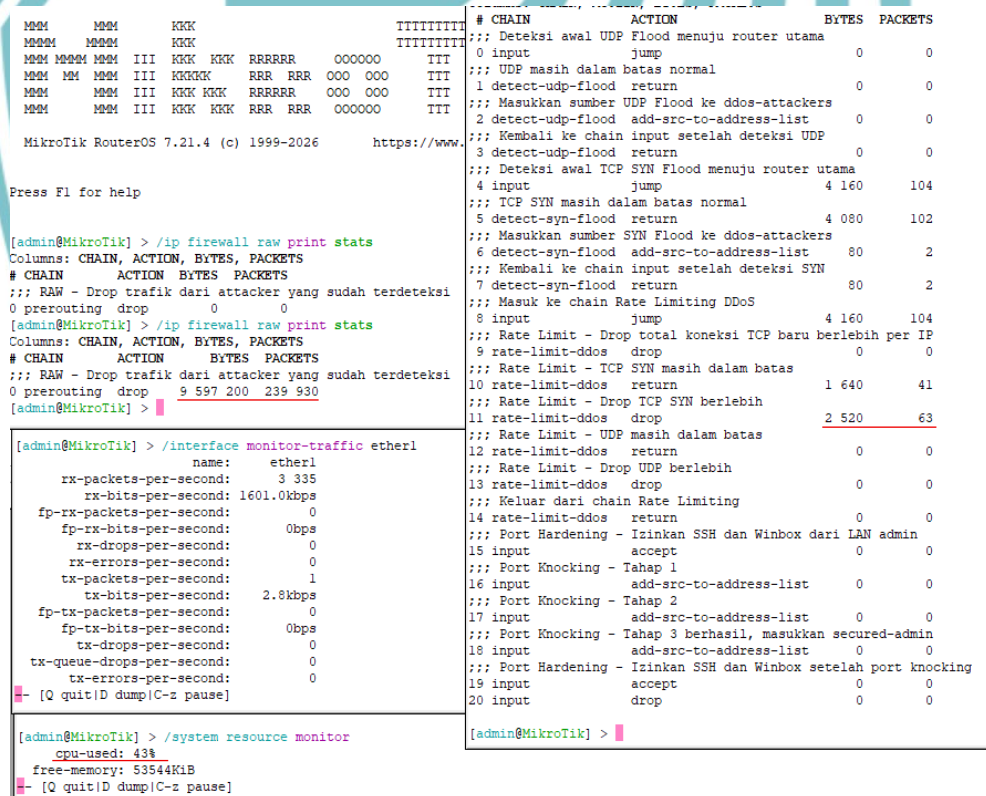
Berdasarkan Gambar 4.48, nilai *CPU Load* dan *Free Memory* saat pengujian *TCP SYN Flood* dengan *Firewall RAW* diperoleh dari monitoring langsung router. Gambar ini mendukung data pada Tabel 4.20 bahwa sumber daya router dicatat selama RAW aktif.

3. Hasil Pengujian TCP SYN Flood dengan Firewall RAW dan Rate Limiting

Pada skenario ini, *Firewall RAW* dan *Rate Limiting* diaktifkan secara bersamaan. *Firewall RAW* digunakan untuk membuang trafik dari IP

yang telah terdeteksi sebagai *attacker*, sedangkan *Rate Limiting* digunakan untuk membatasi paket TCP SYN berlebih dari satu sumber IP. Pada skenario gabungan ini, sebagian besar trafik dari IP penyerang dapat lebih dahulu dibuang oleh *Firewall RAW* setelah IP tersebut masuk ke dalam *address-list* ddos-attackers. Oleh karena itu, nilai *dropped packets Rate Limiting* SYN dapat terlihat kecil karena RAW lebih dominan dalam menangani trafik lanjutan.

Statistik paket yang diblokir pada pengujian TCP SYN Flood dengan *Firewall RAW* dan *Rate Limiting* ditunjukkan pada Gambar 4.49. Gambar ini digunakan untuk memperlihatkan *counter* rule mitigasi yang aktif selama pengujian berlangsung.



```

MikroTik RouterOS 7.21.4 (c) 1999-2026 https://www.mikrotik.com
Press F1 for help

[admin@MikroTik] > /ip firewall raw print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN ACTION BYTES PACKETS
;;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop 0 0
[admin@MikroTik] > /ip firewall rule print stats
Columns: CHAIN, ACTION, BYTES, PACKETS
# CHAIN ACTION BYTES PACKETS
;;; RAW - Drop trafik dari attacker yang sudah terdeteksi
0 prerouting drop 9 597 200 239 930
[admin@MikroTik] >

[admin@MikroTik] > /interface monitor-traffic ether1
name: ether1
rx-packets-per-second: 3 335
rx-bits-per-second: 1601.0kbps
fp-rx-packets-per-second: 0
fp-rx-bits-per-second: 0bps
rx-drops-per-second: 0
rx-errors-per-second: 0
tx-packets-per-second: 1
tx-bits-per-second: 2.8kbps
fp-tx-packets-per-second: 0
fp-tx-bits-per-second: 0bps
tx-drops-per-second: 0
tx-queue-drops-per-second: 0
tx-errors-per-second: 0
[admin@MikroTik] >

[admin@MikroTik] > /system resource monitor
cpu-used: 43%
free-memory: 53544KiB
[admin@MikroTik] >

# CHAIN ACTION ACTION BYTES PACKETS
;;; Deteksi awal UDP Flood menuju router utama
0 input jump 0 0
;;; UDP masih dalam batas normal
1 detect-udp-flood return 0 0
;;; Masukkan sumber UDP Flood ke ddos-attackers
2 detect-udp-flood add-src-to-address-list 0 0
;;; Kembali ke chain input setelah deteksi UDP
3 detect-udp-flood return 0 0
;;; Deteksi awal TCP SYN Flood menuju router utama
4 input jump 4 160 104
;;; TCP SYN masih dalam batas normal
5 detect-syn-flood return 4 080 102
;;; Masukkan sumber SYN Flood ke ddos-attackers
6 detect-syn-flood add-src-to-address-list 80 2
;;; Kembali ke chain input setelah deteksi SYN
7 detect-syn-flood return 80 2
;;; Masuk ke chain Rate Limiting DDoS
8 input jump 4 160 104
;;; Rate Limit - Drop total koneksi TCP baru berlebih per IP
9 rate-limit-ddos drop 0 0
;;; Rate Limit - TCP SYN masih dalam batas
10 rate-limit-ddos return 1 640 41
;;; Rate Limit - Drop TCP SYN berlebih
11 rate-limit-ddos drop 2 520 63
;;; Rate Limit - UDP masih dalam batas
12 rate-limit-ddos return 0 0
;;; Rate Limit - Drop UDP berlebih
13 rate-limit-ddos drop 0 0
;;; Keluar dari chain Rate Limiting
14 rate-limit-ddos return 0 0
;;; Port Hardening - Izinkan SSH dan Winbox dari LAN admin
15 input accept 0 0
;;; Port Knocking - Tahap 1
16 input add-src-to-address-list 0 0
;;; Port Knocking - Tahap 2
17 input add-src-to-address-list 0 0
;;; Port Knocking - Tahap 3 berhasil, masukkan secured-admin
18 input add-src-to-address-list 0 0
;;; Port Hardening - Izinkan SSH dan Winbox setelah port knocking
19 input accept 0 0
20 input drop 0 0
  
```

Gambar 4. 49 Statistik Dropped Packets pada Pengujian TCP SYN Flood dengan Firewall RAW dan Rate Limiting

Berdasarkan Gambar 4.49, *counter rule* mitigasi menunjukkan adanya paket yang diblokir selama pengujian TCP SYN Flood. Data pada *counter* tersebut digunakan sebagai pendukung pencatatan jumlah *dropped packets* pada tabel hasil pengujian.

Data hasil pengujian TCP SYN Flood dengan *Firewall RAW* dan *Rate Limiting* disajikan pada Tabel 4.21. Tabel ini memuat CPU Load, Free Memory, *traffic* WAN, jumlah paket yang dibuang oleh *Firewall RAW*, serta jumlah paket SYN yang dibatasi oleh *Rate Limiting* selama 10 menit pengamatan.

Tabel 4. 21 Hasil Pengujian TCP SYN Flood dengan Firewall RAW dan Rate Limiting

Menit	CPU Load	Free Memory	Traffic WAN ether1	Dropped Packets	Dropped Packets Rate Limiting SYN
1	43%	53544KiB	1601.0kbps	239 930	63
2	78%	53844KiB	2.2Mbps	431 996	63
3	65%	53812KiB	1703.5kbps	622 267	63
4	62%	53812KiB	2.4Mbps	823 019	63
5	61%	53716KiB	1001.8kbps	1 017 598	63
6	29%	53684KiB	1192.8kbps	1 229 760	63
7	41%	53684KiB	2.3Mbps	1 393 743	63
8	69%	53684KiB	1437.5kbps	1 663 397	63
9	30%	53556KiB	1139.8kbps	1 838 260	63
10	49%	53556KiB	1165.9kbps	1 974 194	63

Berdasarkan Tabel 4.21, data menunjukkan kondisi router saat TCP SYN Flood diuji dengan kombinasi *Firewall RAW* dan *Rate Limiting*. Nilai *dropped packets* RAW dan *dropped packets Rate Limiting* SYN dicatat secara terpisah agar peran masing-masing rule dapat terlihat.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pembahasan lebih lanjut mengenai hubungan antara *Firewall RAW* dan *Rate Limiting* dijelaskan pada subbab 4.4.4.

```
[admin@MikroTik] > /system resource monitor once
cpu-used: 43%
free-memory: 53544KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 78%
free-memory: 53844KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 65%
free-memory: 53812KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 62%
free-memory: 53812KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 61%
free-memory: 53716KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 29%
free-memory: 53684KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 41%
free-memory: 53684KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 69%
free-memory: 53684KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 30%
free-memory: 53556KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 49%
free-memory: 53556KiB
```

Gambar 4. 50 Snapshot TCP SYN Raw dan Rate limit

Berdasarkan Gambar 4.50, nilai *CPU Load* dan *Free Memory* saat pengujian *TCP SYN Flood* dengan kombinasi *Firewall RAW* dan *Rate Limiting* dicatat langsung menggunakan `/system resource monitor once`. Data ini menjadi bukti pendukung kondisi sumber daya router pada Tabel 4.21.

4. Hasil Pengujian TCP SYN Flood dengan Simulasi RTBH

Pada skenario RTBH, *blackhole route* diaktifkan pada router *upstream* untuk membuang trafik yang seharusnya diteruskan ke MikroTik utama. Dengan mekanisme ini, trafik *TCP SYN Flood* dihentikan pada sisi *upstream* sebelum mencapai *interface* WAN router utama. Parameter yang tetap diamati adalah CPU Load, Free Memory, dan *traffic* WAN untuk melihat kondisi router utama ketika trafik serangan tidak lagi diteruskan ke target.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Kondisi *interface* WAN MikroTik utama setelah RTBH diaktifkan ditunjukkan pada Gambar 4.51. Gambar ini digunakan untuk memperlihatkan bahwa trafik TCP SYN *Flood* yang seharusnya menuju router utama telah dibuang terlebih dahulu pada sisi *upstream*.

```
[admin@MikroTik] > /tool torch interface=ether1
Columns: MAC-PROTOCOL, IP-PROTOCOL, DSCP, SRC-ADDRESS, SRC-PORT, DST-ADDRESS
MAC-PROTOCOL  IP-  DSCP  SRC-ADDRESS          SRC-PORT      DST-ADDRESS  >
ip             udp   0     192.168.18.1         5678 (discovery) 255.255.255.2 >
ip             udp   0     255.255.255.255      67 (bootps)     0.0.0.0       >
ipv6           udp   0     fe80::a00:27ff:fe2b:721f 5678 (discovery) ff02::1       >
-- [Q quit|D dump|C-z pause]
```

Gambar 4. 51 Kondisi Interface WAN MikroTik Utama Setelah RTBH Diaktifkan

Berdasarkan Gambar 4.44, *traffic* pada *interface* WAN MikroTik utama berada pada kondisi rendah setelah *blackhole route* diaktifkan. Kondisi ini menunjukkan bahwa trafik dari sisi luar tidak lagi diteruskan secara normal ke MikroTik utama.

Data hasil pengujian TCP SYN *Flood* dengan simulasi RTBH disajikan pada Tabel 4.22. Tabel ini memuat CPU Load, Free Memory, *traffic* WAN pada *interface* ether1, serta keterangan kondisi trafik selama 10 menit pengamatan.

Tabel 4. 22 Hasil Pengujian TCP SYN Flood dengan Simulasi RTBH

Menit	CPU Load	Free Memory	Traffic WAN ether1	Keterangan
1	5	49836KiB	6.0kbps	Trafik dibuang di upstream
2	3	49932KiB	0bps	Trafik dibuang di upstream
3	5	49900KiB	0bps	Trafik dibuang di upstream
4	4	49932KiB	0bps	Trafik dibuang di upstream
5	4	49868KiB	0bps	Trafik dibuang di upstream

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Menit	CPU Load	Free Memory	Traffic WAN ether1	Keterangan
6	4	49900KiB	0bps	Trafik dibuang di upstream
7	5	49836KiB	0bps	Trafik dibuang di upstream
8	4	49728KiB	0bps	Trafik dibuang di upstream
9	2	49696KiB	0bps	Trafik dibuang di upstream
10	3	49760KiB	0bps	Trafik dibuang di upstream

Berdasarkan Tabel 4.22, data menunjukkan kondisi router MikroTik utama saat simulasi RTBH diterapkan pada pengujian TCP SYN *Flood*. Nilai CPU Load, Free Memory, dan *traffic* WAN pada tabel ini digunakan sebagai pembandingan terhadap skenario tanpa mitigasi, *Firewall RAW*, serta kombinasi *Firewall RAW* dan *Rate Limiting*. Pembahasan lebih lanjut mengenai perbandingan data disajikan pada subbab 4.4.4.

Monitoring resource dan *traffic* saat TCP SYN *Flood* dengan RTBH aktif ditunjukkan pada Gambar 4.52. Gambar ini digunakan sebagai pendukung data pada tabel, khususnya untuk memperlihatkan kondisi CPU, memori, dan *traffic* WAN ketika trafik dibuang pada sisi *upstream*.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
[admin@MikroTik] > /system resource monitor once
cpu-used: 5%
free-memory: 49836KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 3%
free-memory: 49932KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 5%
free-memory: 49900KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 4%
free-memory: 49932KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 4%
free-memory: 49868KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 4%
free-memory: 49900KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 5%
free-memory: 49836KiB
[admin@MikroTik] > /system resource monitor once
cpu-used: 4%
free-memory: 49728KiB

Terminal <5>
[admin@MikroTik] > /interface monitor-traffic ether1 once
name: ether1
rx-packets-per-second: 4
rx-bits-per-second: 6.0kbps
fp-rx-packets-per-second: 0
fp-rx-bits-per-second: 0bps
rx-drops-per-second: 0
rx-errors-per-second: 0
tx-packets-per-second: 0
tx-bits-per-second: 0bps
fp-tx-packets-per-second: 0
fp-tx-bits-per-second: 0bps
tx-drops-per-second: 0
tx-queue-drops-per-second: 0
tx-errors-per-second: 0
[admin@MikroTik] > /interface monitor-traffic ether1 once
name: ether1
rx-packets-per-second: 0
rx-bits-per-second: 0bps
fp-rx-packets-per-second: 0
fp-rx-bits-per-second: 0bps
```

Gambar 4. 52 Monitoring Resource dan Traffic Saat TCP SYN Flood dengan RTBH Aktif

Berdasarkan Gambar 4.52, monitoring menunjukkan kondisi router MikroTik utama ketika RTBH aktif. Tampilan tersebut menjadi pendukung data pada Tabel 4.22 dan memperlihatkan bahwa *traffic* menuju *interface* WAN router utama berada pada kondisi rendah selama skenario RTBH berlangsung.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.4.4 Analisis Data

Analisis data dilakukan berdasarkan hasil pengujian pada subbab 4.4.3. Pengujian dilakukan terhadap dua jenis serangan yang sesuai dengan kondisi kasus pada PT XYZ, yaitu UDP Flood dan TCP SYN Flood. Serangan dikirimkan dari Kali Linux menuju IP publik modem simulasi, kemudian diteruskan ke router MikroTik fisik utama sebagai objek pengujian.

Parameter yang dianalisis meliputi CPU Load, Free Memory, traffic WAN pada interface ether1, serta jumlah paket yang berhasil diblokir oleh rule mitigasi. Analisis dilakukan dengan membandingkan kondisi tanpa mitigasi, Firewall RAW, Firewall RAW dengan Rate Limiting, serta simulasi RTBH. Sementara itu, Port Hardening dianalisis secara terpisah karena berfokus pada pengamanan akses manajemen router, bukan pada penurunan beban trafik flood.

1. Analisis Hasil Tanpa Mitigasi

Pada skenario tanpa mitigasi, rule Firewall RAW dan Rate Limiting dinonaktifkan sehingga router MikroTik fisik utama menerima trafik serangan secara langsung dari sisi WAN. Kondisi ini digunakan sebagai baseline untuk melihat dampak serangan sebelum sistem mitigasi diterapkan.

Pada pengujian UDP Flood tanpa mitigasi, CPU Load berada pada rentang 49% hingga 84%, dengan rata-rata sekitar 68,3%. Free Memory mengalami penurunan dari 30328 KiB pada menit pertama menjadi 28084 KiB pada menit ke-10. Traffic WAN pada interface ether1 berada pada kisaran sekitar 1691,0 kbps hingga 2,4 Mbps. Data ini menunjukkan bahwa serangan UDP Flood memberikan beban yang cukup signifikan terhadap router, meskipun CPU belum mencapai 100%.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pada pengujian TCP SYN Flood tanpa mitigasi, dampak serangan terlihat lebih berat. CPU Load berada pada nilai 100% hampir sepanjang pengujian, hanya turun menjadi 91% pada menit ke-8. Rata-rata CPU Load pada skenario ini mencapai sekitar 99,1%. Free Memory juga mengalami penurunan dari 55420 KiB menjadi sekitar 53628 KiB, sedangkan traffic WAN tetap masuk melalui ether1 selama serangan berlangsung. Kondisi ini menunjukkan bahwa TCP SYN Flood lebih membebani router dibandingkan UDP Flood pada pengujian ini.

Berdasarkan kedua hasil tersebut, dapat disimpulkan bahwa kondisi tanpa mitigasi menyebabkan router harus memproses trafik serangan secara langsung. Hal ini berdampak pada peningkatan CPU Load dan penurunan Free Memory. Pada kasus TCP SYN Flood, beban CPU bahkan mencapai kondisi maksimum, sehingga menunjukkan bahwa jenis serangan ini memiliki pengaruh besar terhadap kemampuan pemrosesan router.

2. Analisis Hasil Firewall RAW

Pada skenario Firewall RAW, sistem menggunakan mekanisme deteksi awal untuk memasukkan IP sumber serangan ke dalam address-list ddos-attackers. Setelah IP tersebut terdeteksi, trafik berikutnya dari sumber yang sama dibuang oleh Firewall RAW pada tahap prerouting. Mekanisme ini bertujuan agar paket serangan tidak diproses lebih jauh oleh router.

Pada pengujian UDP Flood dengan Firewall RAW, CPU Load berada pada rentang 49% hingga 73%, dengan rata-rata sekitar 60,6%. Nilai ini lebih rendah dibandingkan skenario UDP Flood tanpa mitigasi yang memiliki rata-rata sekitar 68,3%. Selain itu, Free Memory pada skenario Firewall RAW berada pada kisaran yang lebih tinggi, yaitu sekitar 54656 KiB hingga 56884 KiB, dibandingkan tanpa mitigasi yang berada pada kisaran sekitar 28084 KiB hingga 30328 KiB.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Counter dropped packets pada Firewall RAW terus meningkat hingga mencapai 2.480.400 paket pada menit ke-10.

Hasil tersebut menunjukkan bahwa Firewall RAW berhasil membuang trafik dari sumber yang telah terdeteksi sebagai attacker. Peningkatan dropped packets membuktikan bahwa rule RAW bekerja selama serangan berlangsung. Penurunan rata-rata CPU Load juga menunjukkan bahwa paket yang sudah masuk daftar attacker tidak lagi diproses lebih jauh oleh router.

Pada pengujian TCP SYN Flood dengan Firewall RAW, CPU Load berada pada rentang 48% hingga 62% selama 10 menit pengamatan. Nilai tersebut lebih rendah dibandingkan kondisi TCP SYN Flood tanpa mitigasi yang mencapai rata-rata sekitar 99,1%. Selain itu, *counter dropped packets* pada Firewall RAW terus meningkat dari 217.990 paket pada menit pertama menjadi 2.074.074 paket pada menit ke-10. Peningkatan tersebut menunjukkan bahwa rule Firewall RAW bekerja secara aktif dalam membuang paket TCP SYN dari sumber yang telah terdeteksi sebagai *attacker*.

Hasil ini sejalan dengan penelitian Riduan et al. yang menunjukkan bahwa Firewall RAW mampu memblokir sebagian besar paket serangan dan menurunkan penggunaan CPU router saat menghadapi DDoS. Pada penelitian tersebut, Firewall RAW mampu memblokir paket serangan TCP dan UDP dalam jumlah besar serta menurunkan CPU Load pada beberapa skenario pengujian.

Dengan demikian, pada pengujian TCP SYN Flood, Firewall RAW terbukti membantu menurunkan beban CPU dibandingkan kondisi tanpa mitigasi. Selain itu, peningkatan jumlah *dropped packets* menunjukkan bahwa trafik lanjutan dari IP *attacker* berhasil dibuang pada tahap *prerouting*, sehingga tidak diproses lebih jauh oleh router.

3. Analisis Hasil Firewall RAW dan Rate Limiting

Pada skenario kombinasi *Firewall RAW* dan *Rate Limiting*, kedua metode diaktifkan secara bersamaan. *Firewall RAW* berfungsi untuk membuang trafik dari *IP attacker* yang telah terdeteksi, sedangkan *Rate Limiting* berfungsi untuk membatasi trafik berlebih yang masih sempat diproses oleh router sebelum pemblokiran RAW mengambil alih.

Pada pengujian *UDP Flood* dengan *Firewall RAW* dan *Rate Limiting*, CPU Load berada pada rentang 58% hingga 77%, dengan rata-rata sekitar 66,8%. Nilai ini sedikit lebih tinggi dibandingkan skenario *Firewall RAW* saja yang memiliki rata-rata sekitar 60,6%, tetapi masih berada di bawah kondisi tanpa mitigasi pada beberapa menit pengujian. Free Memory berada pada kisaran 55292 KiB hingga 55560 KiB, yang menunjukkan kondisi memori relatif stabil selama pengujian berlangsung.

Jumlah *dropped packets* pada *Firewall RAW* terus meningkat hingga mencapai 3.617.384 paket pada menit ke-10. Sementara itu, *counter dropped packets Rate Limiting UDP* tercatat 132 paket dan tidak mengalami peningkatan besar selama pengujian. Kondisi ini menunjukkan bahwa pada skenario gabungan, *Firewall RAW* lebih dominan setelah *IP attacker* masuk ke dalam *address-list ddos-attackers*. Trafik berikutnya langsung dibuang pada tahap RAW, sehingga hanya sebagian kecil trafik yang masih sempat ditangani oleh *Rate Limiting*.

Pada pengujian *TCP SYN Flood* dengan *Firewall RAW* dan *Rate Limiting*, CPU Load berada pada rentang 29% hingga 78%, dengan rata-rata sekitar 52,7%. Nilai ini jauh lebih rendah dibandingkan skenario *TCP SYN Flood* tanpa mitigasi yang memiliki rata-rata sekitar 99,1%. Jumlah *dropped packets* pada *Firewall RAW* meningkat hingga

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.974.194 paket pada menit ke-10, sedangkan *dropped packets Rate Limiting* SYN tercatat 63 paket.

Nilai *dropped packets Rate Limiting* SYN yang kecil bukan berarti konfigurasi *Rate Limiting* gagal. Kondisi tersebut terjadi karena *Firewall RAW* bekerja lebih awal setelah IP *attacker* terdeteksi. Ketika IP sumber serangan sudah masuk ke dalam *address-list* ddos-attackers, paket berikutnya langsung dibuang oleh RAW sehingga tidak banyak lagi trafik yang mencapai rule *Rate Limiting*. Dengan demikian, pada skenario gabungan, *Firewall RAW* menjadi mekanisme yang lebih dominan, sedangkan *Rate Limiting* tetap berperan sebagai pembatas trafik berlebih yang masih sempat diproses router.

Berdasarkan hasil tersebut, kombinasi *Firewall RAW* dan *Rate Limiting* tetap relevan sebagai sistem mitigasi berlapis. *Firewall RAW* berfungsi sebagai pemblokiran awal yang efisien, sedangkan *Rate Limiting* menjadi pengendali tambahan terhadap trafik UDP dan TCP SYN yang masih lolos dari penyaringan awal. Pada pengujian TCP SYN *Flood*, kombinasi ini menunjukkan penurunan CPU Load yang paling terlihat dibandingkan kondisi tanpa mitigasi.

4. Analisis Hasil RTBH

Simulasi RTBH dilakukan dengan mengaktifkan blackhole route pada router upstream atau modem simulasi. Mekanisme ini membuat trafik menuju router MikroTik fisik utama dibuang di sisi upstream sebelum mencapai interface WAN router utama.

Pada pengujian UDP Flood dengan simulasi RTBH, CPU Load MikroTik utama berada pada rentang 1% hingga 6%, dengan traffic WAN mayoritas 0 bps. Hal ini menunjukkan bahwa trafik serangan tidak lagi mencapai MikroTik utama karena sudah dibuang oleh router upstream. Free Memory juga berada pada kondisi relatif stabil, yaitu sekitar 52928 KiB hingga 54044 KiB.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pada pengujian TCP SYN Flood dengan simulasi RTBH, hasil yang diperoleh juga menunjukkan pola serupa. CPU Load berada pada nilai rendah, yaitu sekitar 3% hingga 5% pada data yang terlihat, dan traffic WAN berada pada nilai 0 bps hingga 6,0 kbps. Kondisi ini menunjukkan bahwa router utama hampir tidak menerima trafik serangan karena paket sudah dihentikan sebelum mencapai target.

Berdasarkan hasil tersebut, RTBH menjadi metode yang sangat efektif untuk menurunkan beban router utama karena trafik serangan dibuang di sisi upstream. Namun, metode ini memiliki kelemahan penting, yaitu seluruh trafik menuju IP target ikut dibuang tanpa membedakan trafik normal dan trafik serangan. Oleh karena itu, RTBH lebih tepat diposisikan sebagai metode pembanding atau mekanisme darurat ketika serangan sudah sangat besar, bukan sebagai solusi utama yang tetap menjaga ketersediaan layanan.

Dengan demikian, RTBH mampu menurunkan CPU Load dan traffic WAN secara drastis, tetapi konsekuensinya adalah layanan pada IP target tidak dapat diakses selama blackhole route aktif. Hal ini berbeda dengan Firewall RAW dan Rate Limiting yang masih berusaha memproses atau menyaring trafik secara selektif.

5. Analisis Hasil Port Hardening

Pengujian Port Hardening dilakukan secara terpisah dari pengujian CPU, Free Memory, dan traffic flood. Hal ini karena Port Hardening berfokus pada pengamanan akses manajemen router, bukan pada pemrosesan langsung trafik UDP Flood atau TCP SYN Flood.

Hasil implementasi menunjukkan bahwa layanan yang tidak digunakan seperti API, API-SSL, FTP, WWW, dan WWW-SSL dinonaktifkan. Layanan Telnet juga dinonaktifkan karena tidak menggunakan komunikasi terenkripsi. Sebagai pengganti akses terminal, SSH diaktifkan pada port 2222, sedangkan Winbox tetap digunakan pada



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

port 7090. Selain itu, akses SSH dan Winbox dari jaringan LAN admin diizinkan secara langsung, sedangkan akses dari sisi luar harus melalui port knocking terlebih dahulu.

Pada pengujian akses, SSH dari Ubuntu Desktop di sisi LAN dapat dilakukan secara langsung. Sebaliknya, akses SSH dari Kali Linux melalui sisi luar tidak dapat dilakukan sebelum proses port knocking dijalankan. Setelah Kali Linux melakukan urutan port knocking yang sesuai, IP sumber masuk ke address-list secured-admin, kemudian akses SSH dari sisi luar dapat dilakukan sementara.

Hasil ini menunjukkan bahwa Port Hardening berhasil membatasi akses layanan manajemen router. Metode ini tidak memberikan pengaruh langsung terhadap penurunan CPU Load pada serangan flood, tetapi berperan penting dalam mengurangi permukaan serangan pada layanan administrasi router. Dengan demikian, Port Hardening menjadi lapisan keamanan yang melindungi management plane, sedangkan Firewall RAW dan Rate Limiting berfokus pada pengendalian trafik serangan.

6. Kesimpulan Analisis Data

Berdasarkan hasil pengujian, serangan UDP Flood dan TCP SYN Flood terbukti memberikan dampak terhadap router MikroTik fisik utama. Pada kondisi tanpa mitigasi, UDP Flood menghasilkan CPU Load rata-rata sekitar 68,3%, sedangkan TCP SYN Flood menghasilkan CPU Load yang jauh lebih tinggi, yaitu sekitar 99,1%. Hal ini menunjukkan bahwa TCP SYN Flood menjadi jenis serangan yang paling membebani router pada pengujian ini.

Firewall RAW terbukti mampu menurunkan beban router dengan membuang trafik dari IP attacker pada tahap awal. Pada UDP Flood, rata-rata CPU Load turun dari sekitar 68,3% menjadi 60,6%, dan dropped packets RAW meningkat hingga 2.480.400 paket. Pada TCP SYN Flood, counter dropped packets juga meningkat secara signifikan,



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

yang menunjukkan bahwa rule RAW bekerja dalam membuang paket serangan.

Kombinasi Firewall RAW dan Rate Limiting memberikan hasil yang cukup baik, terutama pada TCP SYN Flood. Rata-rata CPU Load turun dari sekitar 99,1% pada kondisi tanpa mitigasi menjadi sekitar 52,7% pada skenario gabungan. Walaupun counter Rate Limiting tidak meningkat besar, hal tersebut dapat dijelaskan karena Firewall RAW bekerja lebih dominan setelah IP attacker masuk ke address-list.

Simulasi RTBH memberikan penurunan beban paling besar karena trafik serangan dibuang di router upstream sebelum mencapai MikroTik utama. CPU Load MikroTik utama berada pada kisaran rendah dan traffic WAN mendekati nol. Namun, metode ini memiliki konsekuensi karena seluruh trafik menuju IP target ikut dibuang, sehingga layanan pada IP tersebut tidak tersedia selama RTBH aktif.

Port Hardening berhasil memperkuat keamanan akses manajemen router melalui penonaktifan service yang tidak digunakan, penggantian Telnet dengan SSH, pembatasan akses dari jaringan luar, dan penerapan port knocking. Hasil ini menunjukkan bahwa Port Hardening berperan sebagai lapisan perlindungan akses administrasi, bukan sebagai metode utama untuk menurunkan CPU Load pada serangan flood.

Secara keseluruhan, metode mitigasi yang diterapkan berhasil menunjukkan fungsi masing-masing. Firewall RAW menjadi lapisan utama untuk membuang trafik attacker secara awal, Rate Limiting menjadi pelengkap untuk membatasi trafik berlebih, Port Hardening mengamankan akses manajemen router, sedangkan RTBH menjadi pembanding untuk kondisi darurat ketika seluruh trafik menuju target perlu dibuang di sisi upstream.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB V PENUTUP

Bab ini berisi simpulan dan saran berdasarkan hasil implementasi dan pengujian sistem mitigasi serangan DDoS pada router MikroTik. Simpulan disusun berdasarkan hasil pengujian terhadap serangan *UDP Flood* dan *TCP SYN Flood*, sedangkan saran diberikan sebagai masukan untuk pengembangan penelitian dan penerapan sistem keamanan jaringan selanjutnya.

5.1 Simpulan

Berdasarkan hasil pengujian, serangan *UDP Flood* dan *TCP SYN Flood* terbukti memberikan dampak terhadap stabilitas sumber daya router MikroTik. Pada kondisi tanpa mitigasi, serangan *UDP Flood* menyebabkan peningkatan *CPU Load*, penurunan *Free Memory*, serta kenaikan *traffic* pada *interface* WAN. Sementara itu, serangan *TCP SYN Flood* memberikan dampak yang lebih besar terhadap beban CPU karena router harus memproses banyak permintaan koneksi TCP secara terus-menerus. Hal ini menunjukkan bahwa router MikroTik tetap memiliki kerentanan terhadap serangan *packet flooding* apabila belum dilengkapi dengan konfigurasi mitigasi yang sesuai.

Penerapan *Port Hardening* berhasil dilakukan dengan menonaktifkan layanan manajemen yang tidak digunakan, seperti API, API-SSL, FTP, WWW, WWW-SSL, dan Telnet. Akses manajemen kemudian diperkuat dengan penggunaan SSH, pembatasan akses dari jaringan luar, serta penerapan *port knocking*. Hasil pengujian menunjukkan bahwa akses Telnet dari sisi luar tidak dapat dilakukan, akses SSH dari jaringan luar ditolak sebelum proses *port knocking*, dan akses hanya dapat dilakukan setelah alamat IP sumber berhasil masuk ke daftar *secured-admin*. Dengan demikian, *Port Hardening* dapat mengurangi celah keamanan pada akses manajemen router MikroTik.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Perancangan dan implementasi *Firewall RAW* serta *Rate Limiting* berhasil diterapkan untuk memitigasi trafik serangan *UDP Flood* dan *TCP SYN Flood*. *Firewall RAW* digunakan untuk membuang trafik dari IP *attacker* yang telah terdeteksi pada tahap awal melalui *chain prerouting*, sehingga paket serangan tidak diproses lebih jauh oleh router. Sementara itu, *Rate Limiting* digunakan untuk membatasi paket *UDP* dan *TCP SYN* berlebih yang masih sempat diproses oleh router. Implementasi ini menunjukkan bahwa kedua metode dapat bekerja sebagai mekanisme mitigasi berlapis pada router MikroTik.

Hasil evaluasi menunjukkan bahwa *Firewall RAW* dan *Rate Limiting* mampu membantu menjaga efisiensi penggunaan sumber daya router saat terjadi serangan. Pada skenario *TCP SYN Flood*, kondisi tanpa mitigasi menyebabkan *CPU Load* sangat tinggi, sedangkan setelah *Firewall RAW* diterapkan, beban CPU menjadi lebih terkendali dan jumlah paket yang diblokir terus meningkat. Pada skenario kombinasi *Firewall RAW* dan *Rate Limiting*, *Firewall RAW* terlihat lebih dominan karena trafik dari IP *attacker* langsung dibuang setelah terdeteksi, sedangkan *Rate Limiting* berperan sebagai lapisan tambahan untuk membatasi trafik berlebih. Selain itu, *Port Hardening* terbukti memperkuat keamanan akses manajemen router, meskipun pengujiannya dilakukan secara fungsional dan bukan berdasarkan parameter CPU atau memori.

Simulasi *Remotely Triggered Black Hole* atau RTBH berhasil diterapkan menggunakan mekanisme *blackhole route* pada router *upstream*. Hasil pengujian menunjukkan bahwa ketika RTBH diaktifkan, trafik serangan tidak lagi diteruskan ke MikroTik utama sehingga *traffic* pada *interface* WAN menurun secara signifikan dan beban CPU router utama menjadi rendah. Namun, RTBH juga membuang seluruh trafik menuju IP target, termasuk trafik normal. Oleh karena itu, RTBH tidak digunakan sebagai metode utama,



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

melainkan sebagai langkah terakhir ketika mitigasi utama seperti *Firewall RAW*, *Rate Limiting*, dan *Port Hardening* tidak mampu menahan dampak serangan yang lebih besar.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat digunakan untuk pengembangan penelitian selanjutnya maupun penerapan pada lingkungan jaringan yang lebih luas.

Pertama, nilai ambang batas pada *Firewall RAW* dan *Rate Limiting* perlu disesuaikan kembali apabila diterapkan pada jaringan operasional. Nilai batas yang digunakan pada penelitian ini disusun berdasarkan kebutuhan pengujian dan kondisi perangkat yang digunakan, sehingga pada penerapan nyata perlu dilakukan penyesuaian terhadap pola trafik normal pelanggan agar tidak menyebabkan *false positive*.

Kedua, penelitian selanjutnya dapat menambahkan parameter pengujian lain seperti latency, packet loss, atau throughput. Parameter tersebut dapat digunakan untuk melihat dampak mitigasi tidak hanya dari sisi CPU Load, Free Memory, dan *traffic* jaringan, tetapi juga dari sisi kualitas layanan yang dirasakan oleh pengguna.

Ketiga, simulasi RTBH dapat dikembangkan lebih lanjut dengan rancangan yang lebih mendekati kondisi jaringan skala besar. Pada penelitian ini, RTBH masih disimulasikan menggunakan *blackhole route* pada MikroTik, sehingga penelitian selanjutnya dapat mengkaji skenario RTBH yang melibatkan mekanisme *routing* yang lebih lengkap pada lingkungan uji yang aman dan terkontrol.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR PUSTAKA

- Fikri, A. H., Rahmi, A. A., & Rahman, R. (2025). *Analisis keamanan protokol Telnet vs SSH menggunakan Wireshark dalam jaringan terbuka*. Journal of System & Technology, 1(1), 26–29.
- Haniyah, W., Hidayat, M. C., Putra, Z. F. I., Pertama, V. A., & Setiawan, A. (2024). *Simulasi serangan Denial of Service (DoS) menggunakan Hping3 melalui Kali Linux*. Journal of Internet and Software Engineering, 1–8.
- Hardono, H. (2024). *Manajemen bandwidth router MikroTik menggunakan metode Simple Queue di laboratorium komputer SMA Swasta Kemala Bhayangkari Kotabumi*. Jurnal Sienna, 5(1).
- Hendry, S. (2024). *Membangun sekuritas jaringan terhadap penggunaan VPN, serangan DDoS, dan akses eksternal ke MikroTik*. Samarinda: STMIK Widya Cipta Dharma.
- Khant Htal Myo. (2025). *BGP Routing Security Using Remotely Triggered Blackholing*.
- Kushaeiri, F. A., Muhyidin, Y., & Singasatia, D. (2024). *Implementasi pencegahan serangan DDoS pada router MikroTik menggunakan metode ethical hacking*. Jurnal Ilmiah Sain dan Teknologi, 2(11), 229–244.
- Lueis, P. dan Kanigoro, B. (2025). *Multithreaded Automation for Mass Configuration of MikroTik Routers in Campus Networks*. Proceedings of the International Conference on Cyber and IT Service Management (CITSM).
- Mamuriyah, N., Prasetyo, S. E., & Sijabat, A. O. (2024). *Rancangan sistem keamanan jaringan dari serangan DDoS menggunakan*

metode pengujian penetrasi. Jurnal Teknologi dan Sistem Informasi Bisnis, 6(1), 162–167.

Oktivasari, P., Zain, A.R., Agustin, M., Kurniawan, A., Murad, F.A. and Anshor, M.F. (2022) *Analysis of Effectiveness of Iptables on Web Server from Slowloris Attack*. Proceedings of the 5th International Conference of Computer and Informatics Engineering (IC2IE). IEEE, pp. 215–219. doi:10.1109/IC2IE56416.2022.9970143.

Riduan, M. A. O., Riska, & Alamsyah, H. (2025). *Analisa dan implementasi keamanan jaringan berbasis firewall raw terhadap serangan DDoS pada router MikroTik*. Jurnal Media Infotama, 21(1).

Siregar, M. I., Lubis, I., & Liza, R. (2025). *Implementasi keamanan anti DDoS menggunakan router MikroTik pada layanan cloud storage berbasis lokal*. Jurnal Networking System and Security System, 2(1).

Sitorus, M. A., Nasution, D. dan Iqbal, M. (2025). *Analisis Efektivitas RAW Firewall MikroTik dalam Mitigasi Serangan DDoS pada Infrastruktur Jaringan*. Journal of Science and Social Research, 8(2), 3354–3358.

Susanto, Daru, A. F. dan Christanto, F. W. (2023). *Packet Filtering Gateway and Application Layer Gateway on MikroTik Router Based Firewalls for Server and Internet Access Restrictions*. Proceedings of the IEEE International Conference on Technology, Engineering, and Computing Applications.

Wijaya, F. I., Innuddin, M., & Latif, K. A. (2025). *Analisa penerapan fitur firewall pada MikroTik untuk mengamankan dari serangan Denial of Service (DoS)*. Panthera: Jurnal Ilmiah Pendidikan Sains dan Terapan, 5(3), 570–592.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR RIWAYAT HIDUP PENULIS



Penulis bernama Alvito Revansyah Gunawan, lahir di Jakarta pada tanggal 31 Januari 2003. Penulis menyelesaikan pendidikan dasar di SDN 01 Kebon Kosong pada tahun 2015, kemudian melanjutkan pendidikan di SMPN 59 Jakarta dan lulus pada tahun 2018. Selanjutnya, penulis menempuh pendidikan menengah kejuruan di SMKN 1 Jakarta dan lulus pada tahun 2022.

Setelah menyelesaikan pendidikan menengah kejuruan, penulis melanjutkan pendidikan ke jenjang perguruan tinggi di Politeknik Negeri Jakarta, Jurusan Teknik Informatika dan Komputer, Program Studi Teknik Multimedia dan Jaringan. Selama menjalani perkuliahan, penulis mempelajari berbagai bidang terkait jaringan komputer, keamanan jaringan, sistem komputer, serta teknologi multimedia.

**POLITEKNIK
NEGERI
JAKARTA**

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LAMPIRAN

Lampiran 1 – Dokumentasi Wawancara

Tempat : Daring (Online)

Tanggal : 17 Januari 2026

Narasumber : Pihak PT XYZ (M. Ichwan Hardiansyah - IP Network Engineer)

Wawancara dilakukan untuk memvalidasi permasalahan terkait kerentanan infrastruktur jaringan PT XYZ pasca-insiden serangan siber tahun 2025. Data yang diperoleh meliputi detail teknis mengenai kelelahan sumber daya (resource exhaustion) dan dampak kerugian finansial perusahaan. Hasil diskusi ini selanjutnya dijadikan dasar penentuan kebutuhan sistem, khususnya dalam perancangan konfigurasi Firewall Raw dan manajemen trafik sebagai solusi mitigasi utama.

Pertanyaan	Jawaban
Bisa diceritakan mengenai insiden keamanan yang pernah terjadi di PT XYZ?	Pada tahun 2025, kami mengalami satu insiden berupa serangan DDoS. Meskipun hanya sekali, dampaknya sangat fatal karena menyebabkan traffic full dan pelanggan normal yang lain tidak mendapatkan traffic, akhirnya jaringan menjadi lemot.
Secara teknis, apa yang terjadi pada perangkat Router saat insiden itu berlangsung?	Saat kejadian, Resource CPU Router melonjak hingga 100% dan RAM terkuras habis.
Apa dampak kerugian yang dialami perusahaan akibat insiden tersebut?	Estimasi kerugian materi saat itu mencapai 1-3 Milyar Rupiah. Selain itu, reputasi kami sempat turun drastis, kehilangan subscribers, karena banyaknya keluhan

(lanjutan)

	pelanggan di media sosial dan juga omongan tetangga.
Sebenarnya apa sih pemicu utama serangan DDoS ini bisa terjadi, Mas? Apakah tim IT punya gambaran siapa yang melancarkan serangan?	penyebabnya ada dua sisi. Pertama dari penyerang, kebanyakan sih motifnya uang atau pemerasan, kayak Ransom DDoS. Tapi ada juga yang cuma iseng uji coba botnet atau malah persaingan bisnis (kompetitor). Kedua sisi korban, Firewall masih settingan standar, server langsung terekspos ke internet, dan kita nggak pasang rate-limit. Jadi pas diserang, trafik langsung lolos semua bikin router hang
Berdasarkan kejadian tersebut, bagian apa saja yang harus saya analisis dalam penelitian ini?	Mungkin dari kita ingin melihat analisis dari CPU dan Bandwidth/Traffic. Untuk metode nya saya sarankan menggunakan Firewall Filtering atau ACL, Rate Limit, dan konfigurasi di bagian port.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

(lanjutan)

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Apakah penerapan sistem mitigasi serangan DDoS ini dilakukan langsung pada perangkat fisik di kantor PT XYZ, atau ada tahapan pengujian terlebih dahulu sebelum diimplementasikan?	Implementasi tidak langsung dilakukan di jaringan kantor. Pengujian dan simulasi dilakukan terlebih dahulu pada lingkungan virtual atau laboratorium. Setelah sistem dianggap sudah berjalan dengan baik dan stabil, barulah diterapkan pada jaringan operasional PT XYZ.
Apakah topologi asli jaringan PT XYZ dapat dijadikan dasar penyusunan topologi pengujian pada penelitian ini?	Ya. Topologi asli PT XYZ terdiri dari perangkat seperti Router IGW, Switch Core, Router PE, Router Colo, Router Dist CCR-2116, Switch Backbone, OLT, ONT, dan server pendukung. Dalam penelitian ini, alur tersebut dapat disederhanakan menjadi Kali Linux sebagai sumber trafik, MikroTik CHR upstream sebagai perantara/modem simulasi, MikroTik utama sebagai router target, dan Ubuntu Desktop sebagai perangkat admin.
Apakah di PT XYZ ada aturan khusus terkait penggunaan Firewall RAW pada MikroTik?	Tidak ada aturan yang terlalu kompleks. Firewall RAW dapat digunakan untuk drop awal trafik serangan seperti UDP Flood dan TCP SYN Flood dari interface publik, serta trafik dari IP attacker yang sudah diketahui. Namun, untuk akses port manajemen seperti Winbox/SSH, sebaiknya tidak langsung dibuang, tetapi divalidasi terlebih dahulu melalui port knocking. Rule RAW disarankan tetap sederhana agar tidak menambah beban

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

	CPU dan tidak mengganggu trafik normal pelanggan.
Apakah ada aturan atau arahan terkait penerapan Rate Limiting pada MikroTik untuk mitigasi DDoS?	Untuk Rate Limiting, pembatasan bisa dilakukan pada trafik atau koneksi berlebih dari satu sumber IP. Fokusnya bisa pada koneksi baru TCP, trafik UDP berlebih, dan total koneksi dari satu IP. Namun, nilai batasnya tidak bisa dibuat sembarangan karena harus menyesuaikan trafik normal pelanggan agar tidak mengganggu layanan.
Apakah terdapat aturan khusus terkait Port Hardening pada MikroTik, seperti port/service yang dibuka, ditutup, atau dibatasi aksesnya?	Untuk MikroTik, layanan yang aktif adalah Winbox pada port 7090 dan Telnet pada port 2332. Layanan lain seperti API, API-SSL, FTP, SSH MikroTik, WWW, dan WWW-SSL tidak aktif. Untuk perangkat selain MikroTik, akses administrasi yang dibuka hanya SSH.
Apakah ada aturan khusus jika ingin menggunakan RTBH sebagai mitigasi DDoS di jaringan PT XYZ?	Ada. RTBH tidak bisa langsung diterapkan dari sisi internal saja karena perlu izin dan koordinasi dengan ISP/upstream, terutama jika menggunakan routing seperti BGP. Secara sederhana, RTBH bekerja dengan mengarahkan seluruh trafik yang menuju IP target ke jalur blackhole, sehingga trafik tersebut dibuang sebelum masuk ke jaringan utama. Namun, metode ini tidak membedakan trafik serangan dan trafik normal, sehingga semua trafik ke IP target



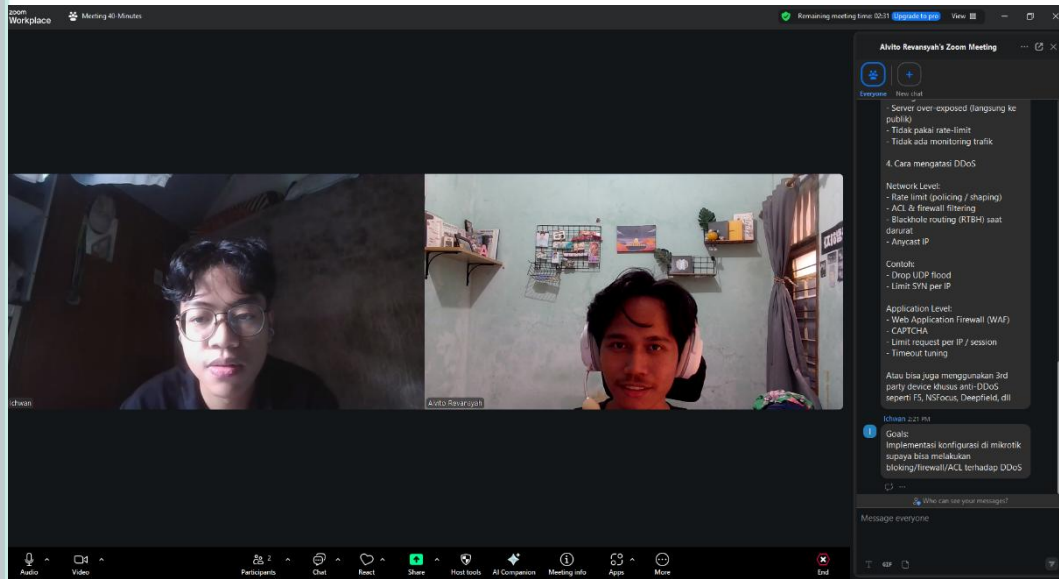
© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

	ikut terbang. Karena dampaknya cukup besar terhadap ketersediaan layanan, penerapan RTBH biasanya hanya dilakukan pada kondisi tertentu ketika serangan sudah sangat mengganggu jaringan.
Dari sisi mana trafik tidak normal dapat masuk pada topologi asli PT XYZ?	Trafik tidak normal dapat masuk melalui sisi perangkat pelanggan seperti ONT, kemudian melewati jalur jaringan sampai mencapai Router Dist CCR-2116. Oleh karena itu, Router Dist CCR-2116 menjadi perangkat yang menerima dampak utama dari peningkatan trafik.
Apakah pengujian akhir boleh dilakukan pada jaringan operasional aktif PT XYZ?	Tidak. Pengujian tidak dilakukan pada jaringan operasional aktif agar tidak mengganggu layanan pelanggan. Konfigurasi divalidasi terlebih dahulu di lingkungan laboratorium, kemudian pengujian akhir dilakukan pada perangkat Mikrotik fisik milik PT XYZ di jaringan uji terpisah.

Lampiran 2 – Dokumentasi Wawancara



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

POLITEKNIK
NEGERI
JAKARTA

Lampiran 3 – Implementasi Sistem di Lingkungan Perusahaan



© Hak Cipta milik Politeknik Negeri Jakarta

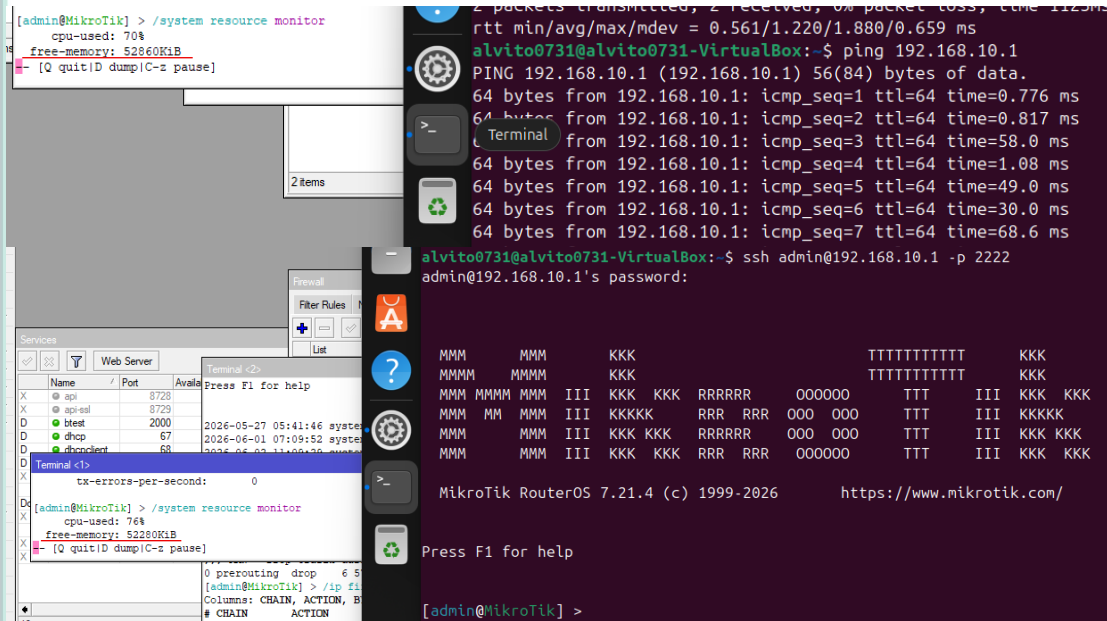
Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lampiran 4 – Pengujian akses Admin pada saat serangan berjalan

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



```
[admin@MikroTik] > /system resource monitor
cpu-used: 70%
free-memory: 52860KiB
[Q quit][D dump][C-s pause]
```

```
Services
Name / Port Available
X @ api 8728
X @ apical 8729
D @ btest 2000
D @ dhcp 67
D @ dhcpv6 68
Terminal 1
tk-errors-per-second: 0
[admin@MikroTik] > /system resource monitor
cpu-used: 76%
free-memory: 52280KiB
[Q quit][D dump][C-s pause]
```

```
Terminal 2
Press F1 for help
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.776 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=0.817 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=58.0 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=1.08 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=64 time=49.0 ms
64 bytes from 192.168.10.1: icmp_seq=6 ttl=64 time=30.0 ms
64 bytes from 192.168.10.1: icmp_seq=7 ttl=64 time=68.6 ms
alvito0731@alvito0731-VirtualBox: ~$ ssh admin@192.168.10.1 -p 2222
admin@192.168.10.1's password:
```

```
MMM MMM KKK TTTTTTTTTT KKK
MMMM MMM KKK
MMM MMM III KKK KKK RRRRRR 000000 TTT III KKK KKK
MMM MM III KKKKKK RRR RRR 000 000 TTT III KKKKK
MMM MMM III KKK KKK RRRRRR 000 000 TTT III KKK KKK
MMM MM III KKK KKK RRR RRR 000000 TTT III KKK KKK

MikroTik RouterOS 7.21.4 (c) 1999-2026 https://www.mikrotik.com/

Press F1 for help

[admin@MikroTik] >
```

Lampiran 5 – Counter Rate Limiting bertambah

```

;;; Rate Limit - TCP SYN masih dalam batas
10 rate-limit-ddos return 6 280 157
;;; Rate Limit - Drop TCP SYN berlebih
11 rate-limit-ddos drop 1 128 200 28 205
;;; Rate Limit - UDP masih dalam batas
12 rate-limit-ddos return 37 044 1 323
;;; Rate Limit - Drop UDP berlebih
13 rate-limit-ddos drop 1 727 964 61 713
;;; Rate Limit - TCP SYN masih dalam batas
10 rate-limit-ddos return 26 280 657
;;; Rate Limit - Drop TCP SYN berlebih
11 rate-limit-ddos drop 5 416 920 135 423
;;; Rate Limit - UDP masih dalam batas
12 rate-limit-ddos return 52 864 1 888
;;; Rate Limit - Drop UDP berlebih
13 rate-limit-ddos drop 2 381 372 85 049

```



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta