

**IMPLEMENTASI *FIREWALL FILTER RULE* DAN *RAW*
SEBAGAI METODE PENGAMANAN JARINGAN PADA
PERPUSTAKAAN MTs NEGERI 1 BANTUL**

TUGAS AKHIR



diajukan oleh:

Makruf Ngabdur Rokhman (20.01.4563)

Eka Farliza Rizaldy (20.01.4451)

Nasywa Abdullah (20.01.4470)

**PROGRAM DIPLOMA
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

**IMPLEMENTASI *FIREWALL FILTER RULE* DAN *RAW*
SEBAGAI METODE PENGAMANAN JARINGAN PADA
PERPUSTAKAAN MTs NEGERI 1 BANTUL**

TUGAS AKHIR

Diajukan untuk memenuhi salah satu syarat mencapai gelar Ahli Madya
Komputer Program Diploma – Program Studi Teknik Informatika



diajukan oleh

Makruf Ngabdur Rokhman (20.01.4563)

Eka Fariza Rizaldy (20.01.4451)

Nasywa Abdullah (20.01.4470)

Kepada

**PROGRAM DIPLOMA
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2023

HALAMAN PERSETUJUAN

TUGAS AKHIR

IMPLEMENTASI *FIREWALL FILTER RULE* DAN *RAW* SEBAGAI METODE PENGAMANAN JARINGAN PADA PERPUSTAKAAN MTs NEGERI 1 BANTUL

yang dipersiapkan dan disusun oleh

Makruf Ngabdur Rokhman

20.01.4563

Telah disetujui oleh Dosen Pembimbing Tugas Akhir
pada tanggal 22 November 2023

Dosen Pembimbing,



Nila Feby Paspitasari, S.Kom, M.Cs

NIK. 190302161

HALAMAN PENGESAHAN

TUGAS AKHIR

**IMPLEMENTASI *FIREWALL FILTER RULE* DAN *RAW*
SEBAGAI METODE PENGAMANAN JARINGAN PADA
PERPUSTAKAAN MTs NEGERI 1 BANTUL**

yang disusun dan diajukan oleh

Makruf Ngabdur Rokhman

20.01.4563

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 November 2023

Susunan Dewan Penguji

Nama Penguji

**Ade Pujiyanto, M.Kom
NIK. 190302494**

**Barka Satya, M.Kom
NIK. 190302126**

Tanda Tangan



Tugas Akhir ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Ahli Madya komputer
Tanggal 22 November 2023

DEKAN FAKULTAS ILMU KOMPUTER



**Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096**

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan di bawah ini,

Nama mahasiswa : Makruf Ngabdur Rokhman

NIM : 20.01.4563

Menyatakan bahwa Tugas Akhir dengan judul berikut:

Implementasi *Firewall Filter Rule* dan *Raw* sebagai Metode Pengamanan Jaringan pada Perpustakaan MTs Negeri 1 Bantul

Dosen Pembimbing : Nila Feby Puspitasari, S.Kom, M.Cs

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 22 November 2023

Yang Menyatakan,



Makruf

HALAMAN PERSEMBAHAN

Segala puji dan syukur kepada Tuhan Yang Maha Esa, yang telah memberikan kesehatan, pertolongan dan hidayah-Nya sehingga kami dapat menulis dan menyelesaikan laporan tugas akhir yang telah kami susun. Oleh karena itu penulis ingin mengucapkan terimakasih kepada :

1. Tuhan Yang Maha Esa, atas berkah pertolongan dan kemudahan serta limpahan ilmu dan wawasan.
2. Orang Tua, terimakasih atas doa, semangat, nasehat dan kasih sayang dan doa restu yang tiada henti kepada anaknya.
3. Kampus kami Universitas Amikom Yogyakarta.
4. Dosen pembimbing kami Nila Feby Puspitasari, S.Kom. M.Cs
5. Kepala Sekolah MTs Negeri 1 Bantul yang telah memberi ijin penelitian tugas akhir di perpustakaan MTs Negeri 1 Bantul.
6. Pembimbing kami di MTs Negeri 1 Bantul Bapak Arief Rahman Hakim, S.Si yang memberikan arahan selama melakukan penelitian di MTs Negeri 1 Bantul.
7. Teman-teman di Universitas Amikom Yogyakarta.
8. Para pembaca tugas akhir ini semoga dapat memberi sedikit wawasan yang diharapkan berguna di kemudian hari.

KATA PENGANTAR

Dengan mengucapkan syukur kepada Tuhan Yang Maha Esa atas rahmat, nikmat, serta karunia nya, Tugas Akhir yang berjudul “Implementasi Firewall Filter Rule dan Raw sebagai Metode Pengamanan Jaringan pada Perpustakaan MTs Negeri 1 Bantul” ini dapat selesai.

Tugas Akhir ini merupakan salah satu syarat yang harus dipenuhi untuk memperoleh gelar Ahli Madya Komputer pada prodi Diploma 3 Teknik Informatika Fakultas Ilmu Komputer Universitas Amikom Yogyakarta. Dalam penulisan Tugas Akhir ini, penulis mendapatkan bimbingan, nasehat, serta semangat dari banyak pihak. Maka dari itu, penulis ingin mengucapkan terimakasih kepada:

1. Bapak Prof. Dr. M. Suyanto, M.M selaku Rektor Universitas Amikom Yogyakarta.
2. Bapak Hanif Al-Fatta, M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
3. Bapak Barka Satya, M.Kom selaku ketua Prodi Diploma 3 Teknik Informatika Universitas Amikom Yogyakarta.
4. Ibu Nila Feby Puspitasari, S.Kom, M.Cs selaku Dosen pembimbing Tugas Akhir.
5. Kepada seluruh Staf Dosen dan Karyawan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
6. Kepada Bapak Muhammad Arief Rahman Hakim, S.Si selaku Guru pembimbing penelitian di MTs Negeri 1 Bantul.
7. Kepada seluruh Staf Guru dan Karyawan MTs Negeri 1 Bantul.

Kekurangan, kesalahan, dan kekhilafan dikarenakan keterbatasan kemampuan penulis. Maka dari itu penulis memohon maaf yang sebesar-besarnya. Penulis juga menerima kritik dan saran dari semua pihak demi perbaikan yang dapat mengembangkan Tugas Akhir ini

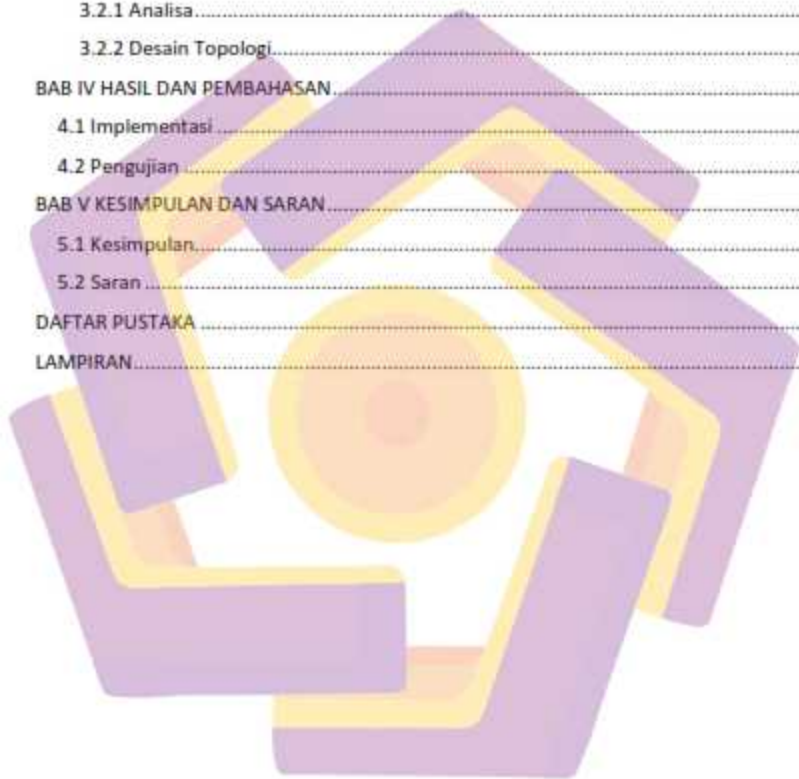
Yogyakarta, 31 Oktober 2023

Penulis

DAFTAR ISI

HALAMAN JUDUL.....	1
HALAMAN PERSETUJUAN	2
HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR.....	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	ix
DAFTAR TABEL	xi
DAFTAR LAMPIRAN.....	xii
INTISARI	xiii
Abstract.....	xiv
BAB I PENDAHULUAN	15
1.1 Latar Belakang Masalah.....	15
1.2 Perumusan masalah.....	16
1.3 Tujuan Penelitian	16
1.4 Batasan Masalah.....	17
1.5 Manfaat Penelitian	17
1.6 Sistematika Penulisan	18
BAB II TINJAUAN PUSTAKA	19
2.1 Literature Review.....	19
2.2 Landasan Teori.....	24
2.2.1 Pengertian Jaringan Internet	24
2.2.2 Topologi Jaringan.....	24
2.2.3 Mikrotik Routerboard.....	27
2.2.4 Pengertian Jaringan <i>Wireless</i>	27
2.2.5 <i>Monitoring</i> Jaringan.....	27
2.2.6 <i>The Dude</i>	28
2.2.7 Keamanan Jaringan.....	28
2.2.8 Ancaman Keamanan Jaringan.....	29
2.2.9 <i>Firewall Filter Rule</i>	30
2.2.10 Pengertian <i>Firewall</i>	31
2.2.11 <i>Firewall Raw</i>	31

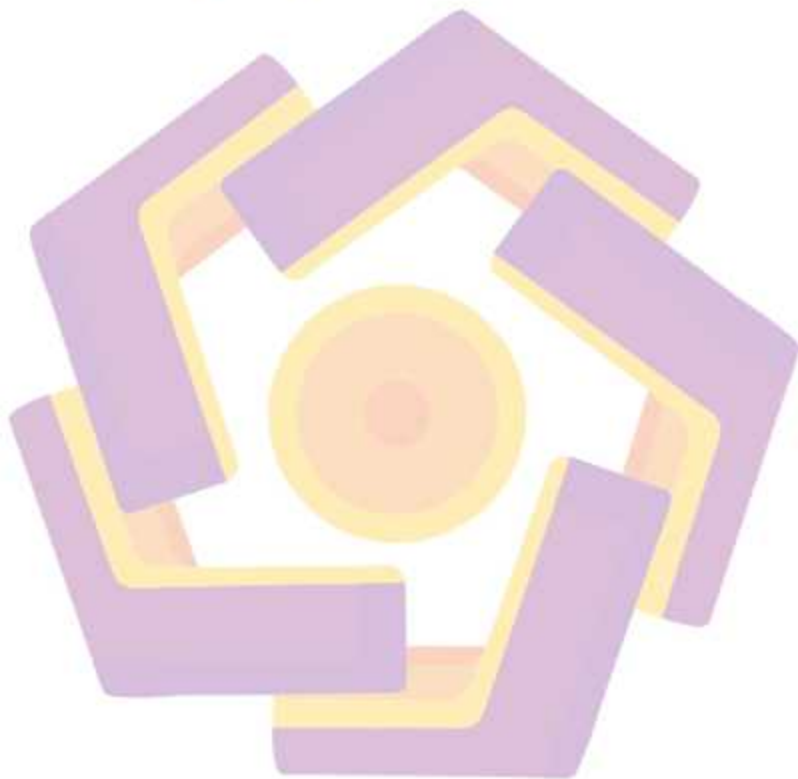
2.2.12 Network Development Life Cycle (NDLC)	31
BAB III METODOLOGI PENELITIAN	33
3.1 Proses Alur Penelitian	33
3.1.1 Tahap Perencanaan Penelitian	33
3.1.2 Pengumpulan Data	34
3.1.3 Analisa dan Perancangan	37
3.2 Alur Network Development Life Cycle (NDLC)	37
3.2.1 Analisa	38
3.2.2 Desain Topologi	40
BAB IV HASIL DAN PEMBAHASAN	42
4.1 Implementasi	42
4.2 Pengujian	55
BAB V KESIMPULAN DAN SARAN	66
5.1 Kesimpulan	66
5.2 Saran	66
DAFTAR PUSTAKA	67
LAMPIRAN	69



DAFTAR GAMBAR

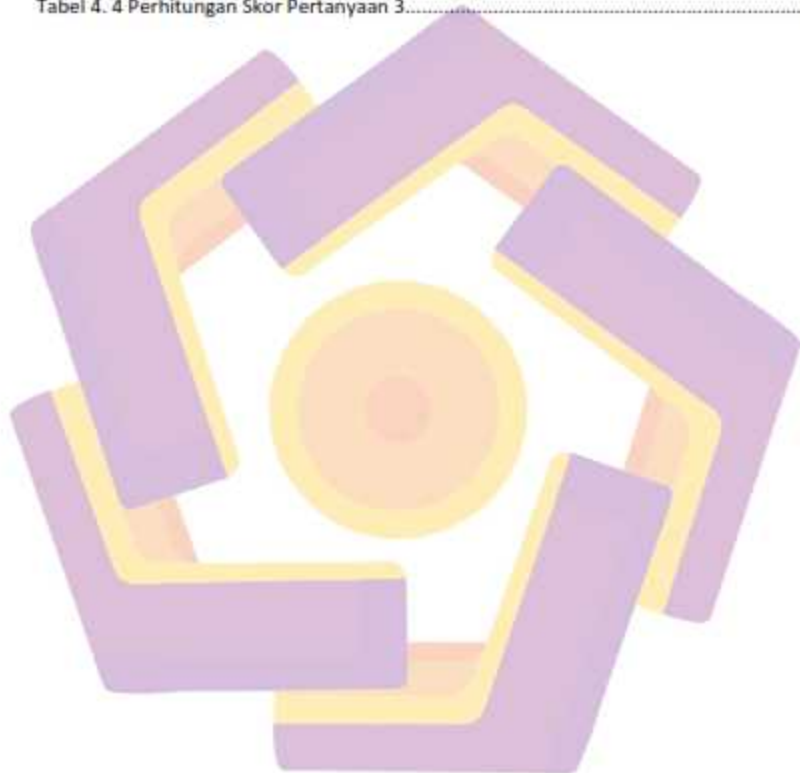
Gambar 2. 1 Gambar Topologi <i>Bus</i>	24
Gambar 2. 2 Gambar Topologi <i>Star</i>	25
Gambar 2. 3 Gambar Topologi <i>Ring</i>	25
Gambar 2. 4 Gambar Topologi <i>Tree</i>	26
Gambar 2. 5 Gambar Topologi <i>Mesh</i>	26
Gambar 2.6 Logo Mikrotik	27
Gambar 2.7 <i>The Dude</i>	28
Gambar 2.8 <i>Firewall</i>	31
Gambar 3. 1 <i>Flowchart</i> Alur Penelitian.....	33
Gambar 3.2 Topologi Jaringan Perpustakaan.....	34
Gambar 3. 3 Alur <i>Network Development Life Cycle</i>	37
Gambar 3. 4 Topologi Jaringan Perpustakaan.....	38
Gambar 3. 5 Topologi Jaringan Baru.....	40
Gambar 4. 1 <i>Interface bridge</i>	42
Gambar 4. 2 <i>Interface</i> yang di bridge.....	42
Gambar 4. 3 <i>Ip Address</i>	43
Gambar 4. 4 <i>Firewall NAT</i>	43
Gambar 4. 5 <i>DHCP Client</i>	43
Gambar 4. 6 Konfigurasi <i>Domain Name Server</i>	44
Gambar 4. 7 <i>DHCP Server</i>	44
Gambar 4. 8 Konfigurasi <i>DHCP Server</i>	44
Gambar 4. 9 <i>Flowchart Web Filtering</i>	45
Gambar 4. 10 <i>Filter rule web filtering</i> bagian 1.....	46
Gambar 4. 11 <i>Filter rule web filtering</i> bagian 2.....	46
Gambar 4. 12 <i>Filter rule web filtering</i> bagian 3.....	47
Gambar 4. 13 <i>Filter rule web filtering</i> bagian 4.....	47
Gambar 4. 14 <i>Filter rule web filtering</i> bagian 5.....	48
Gambar 4. 15 <i>Filter rule web filtering</i> bagian 6.....	48
Gambar 4. 16 <i>Preview Filter rule</i> yang sudah dibuat.....	49
Gambar 4. 17 <i>Flowchart Firewall Raw</i>	49
Gambar 4. 18 Konfigurasi <i>Firewall RAW</i> bagian 1.....	50
Gambar 4. 19 Konfigurasi <i>Firewall RAW</i> bagian 2.....	51
Gambar 4. 20 Konfigurasi <i>Firewall RAW</i> bagian 3.....	51
Gambar 4. 21 Konfigurasi <i>Firewall RAW</i> bagian 4.....	52
Gambar 4. 22 Konfigurasi <i>Firewall RAW</i> bagian 5.....	52
Gambar 4. 23 Konfigurasi <i>Firewall RAW</i> bagian 6.....	53
Gambar 4. 24 Konfigurasi <i>Firewall RAW</i> bagian 6.....	53
Gambar 4. 25 Konfigurasi <i>Firewall RAW</i> bagian 7.....	53
Gambar 4. 26 Mengaktifkan <i>The Dude Server</i>	54
Gambar 4. 27 Mengubah <i>data directory</i>	54
Gambar 4. 28 Mengaktifkan <i>SNMP</i>	55
Gambar 4. 29 Pengujian <i>web filtering</i> pada laptop.....	56
Gambar 4. 30 Pengujian <i>web filtering</i> melalui laptop.....	56
Gambar 4. 31 Pengujian <i>web filtering</i> melalui handphone.....	57
Gambar 4. 32 Skenario Penyerangan.....	57

Gambar 4. 33 Serangan DDoS menggunakan LOIC.....	57
Gambar 4. 34 Pengujian DDoS bagian 1	58
Gambar 4. 35 Pengujian DDoS bagian 2	58
Gambar 4. 36 Login ke The Dude Client	59
Gambar 4. 37 Mendeteksi perangkat pada The Dude client	59
Gambar 4. 38 Tampilan monitoring pada The Dude client	60
Gambar 4. 39 Parameter Chart.....	60
Gambar 4. 40 Chart Internet.....	61
Gambar 4. 41 Chart Resource Mikrotik.....	62



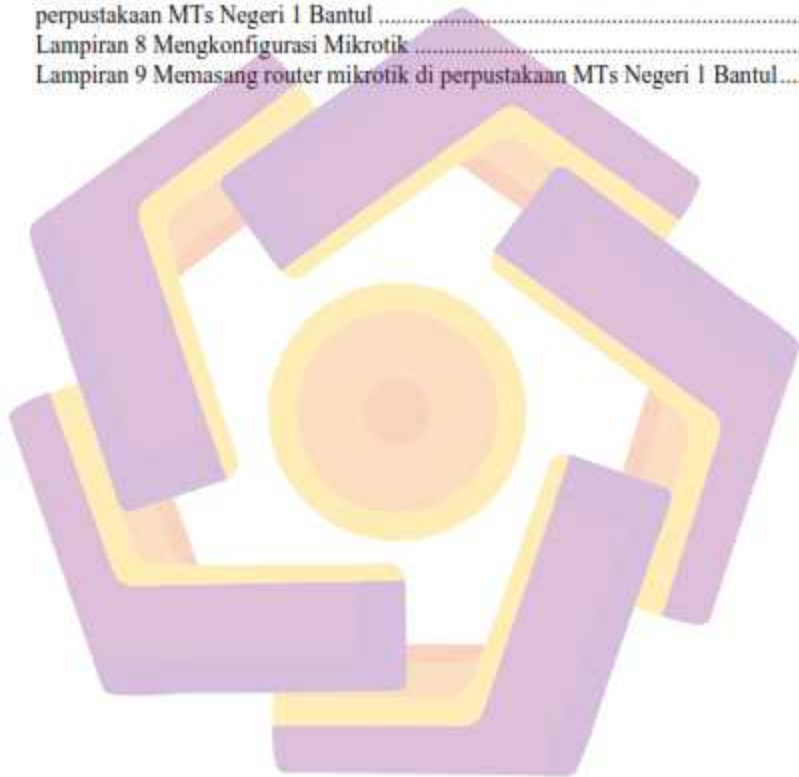
DAFTAR TABEL

Tabel 2. 1 Tabel Perbandingan	21
Tabel 3.1 Wawancara	35
Tabel 3.2 Solusi Permasalahan	36
Tabel 3.3 Tabel Kebutuhan <i>Hardware</i>	39
Tabel 3.4 Tabel Kebutuhan <i>Software</i>	40
Tabel 4. 1 Kuesioner	63
Tabel 4. 2 Perhitungan Skor Pertanyaan 1	64
Tabel 4. 3 Perhitungan Skor Pertanyaan 2	64
Tabel 4. 4 Perhitungan Skor Pertanyaan 3	65



DAFTAR LAMPIRAN

Lampiran 1 Wawancara kepada pembimbing di MTs Negeri 1 Bantul	69
Lampiran 2 Tampilan pintu gerbang MTs negeri 1 Bantul	69
Lampiran 3 Tampilan halaman depan MTs negeri 1 Bantul	69
Lampiran 4 Tampilan tempat penerimaan tamu di perpustakaan MTs Negeri 1 Bantul.....	70
Lampiran 5 Tampilan suasana perpustakaan MTs Negeri 1 Bantul	70
Lampiran 6 Pemasangan router	70
Lampiran 7 Router Mikrotik yang digunakan untuk konfigurasi jaringan di perpustakaan MTs Negeri 1 Bantul	71
Lampiran 8 Mengkonfigurasi Mikrotik	71
Lampiran 9 Memasang router mikrotik di perpustakaan MTs Negeri 1 Bantul.....	72



INTISARI

Perpustakaan MTs Negeri 1 Bantul merupakan salah satu tempat belajar siswa yang ramai pengunjungnya, disana tersedia layanan jaringan internet yang dapat dimanfaatkan untuk kegiatan belajar. Jaringan internet yang tersedia pada perpustakaan belum menerapkan monitoring jaringan dan keamanan jaringan, sehingga jaringan internet masih rentan terhadap serangan siber salah satunya adalah *Distributed Denial of Service syn attack (DDoS)*. Penelitian ini bertujuan untuk meningkatkan keamanan dan pengawasan akses internet di lingkungan perpustakaan madrasah dan menciptakan lingkungan belajar yang bebas dari konten yang tidak layak menggunakan *firewall filter rule* dan mengatasi serangan *Distributed Denial of Service syn attack (DDoS)* menggunakan *firewall raw*, serta monitoring jaringan dengan *The Dude*. Untuk mencapai tujuan tersebut diperlukan manajemen jaringan dengan menggunakan perangkat mikrotik routerboard. Pada mikrotik sudah tersedia fitur Firewall (*Filter rules, Raw, dan Address list*). Dengan menggunakan router mikrotik, *monitoring* jaringan dapat dilakukan dengan memanfaatkan perangkat lunak *The Dude*. Hasil dari penelitian ini adalah dapat memberikan gambaran efektivitas *monitoring* jaringan, membatasi akses ke situs yang tidak layak (*web filtering*), dan keamanan perangkat jaringan dari serangan *Distributed Denial of Service syn attack (DDoS)*. Di sisi lain, Perpustakaan MTs Negeri 1 Bantul akan memiliki akses internet yang melindungi penggunaannya dari situs atau web yang berisi konten yang tidak layak. Perangkat router manajemen di perpustakaan MTs Negeri 1 Bantul terlindungi dari serangan *Distributed Denial of Service syn attack (DDoS)*. Serta Perpustakaan MTs Negeri 1 Bantul akan memiliki perangkat yang digunakan untuk memantau lalu lintas data atau kondisi perangkat jaringan.

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

Abstract

The library of MTs Negeri 1 Bantul is one of the places of learning for students who are busy visitors, there are internet network services that can be utilized for learning activities. The internet network available in the library has not implemented network monitoring and network security, so that the internet network is still vulnerable to cyber attacks, one of which is Distributed Denial of Service syn attack (DDoS). This research aims to improve security and monitoring of internet access in the madrasah library environment and create a learning environment that is free from inappropriate content using firewall filter rules and overcoming Distributed Denial of Service syn attacks (DDoS) attacks using raw firewalls, as well as network monitoring with the dude. To achieve these goals, network management is needed using a Mikrotik routerboard device. Mikrotik already has Firewall features (Filter rules, Raw, and Address list). By using a proxy router, network monitoring can be done by utilizing The Dude software. The results of this research can provide an overview of the effectiveness of network monitoring, limiting access to inappropriate sites (web filtering), and the security of network devices from Distributed Denial of Service syn attacks (DDoS). On the other hand, the MTs Negeri 1 Bantul Library will have internet access that protects its users from sites or websites that contain inappropriate content. The management router device in the library of MTs Negeri 1 Bantul is protected from Distributed Denial of Service syn attack (DDoS). And the MTs Negeri 1 Bantul Library will have a device used to monitor data traffic or network device conditions.

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