

LAPORAN TUGAS AKHIR

IMPLEMENTASI *BORDER GATEWAY PROTOCOL (BGP)*
COMMUNITY UNTUK MITIGASI *DDOS FLOODING* DI
DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI JAWA TIMUR



DISUSUN OLEH:

ADI DWI CAHYONO
NIM 04323015

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS NAROTAMA
2025

LAPORAN TUGAS AKHIR

IMPLEMENTASI *BORDER GATEWAY PROTOCOL (BGP)* COMMUNITY UNTUK MITIGASI *DDOS FLOODING* DI DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR

Disusun Oleh :

ADI DWI CAHYONO
NIM: 04323015

Dipertahankan di depan Penguji Ujian Tugas Akhir
Program Studi Teknik Informatika
Fakultas Ilmu Komputer
Universitas Narotama Surabaya
Tanggal : 25 Juli 2025

Penguji

Ketua Program Studi

1. Lukman Junaedi, S.T., M.Kom.
NIDN : 0711018101

Moh. Noor Al Azam, S.Kom., M.MT.
NIDN : 0701097001

2. Dr. Aryo Nugroho, S.T., S.Kom., M.T.
NIDN : 0721077001

Fakultas Ilmu Komputer
Surabaya

3. Made Kamisutara, S.T., M.Kom
NIDN : 0706027501

Dr. Cahyo Darujati, S.T., M.T.
NIDN : 0710097402

LAPORAN TUGAS AKHIR

IMPLEMENTASI *BORDER GATEWAY PROTOCOL (BGP)* COMMUNITY UNTUK MITIGASI *DDOS FLOODING* DI DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR

Diajukan guna memenuhi persyaratan
Untuk memperoleh gelar **Sarjana Komputer (S.Kom)**
pada Program Studi Teknik Informatika
Fakultas Ilmu Komputer
Universitas Narotama Surabaya

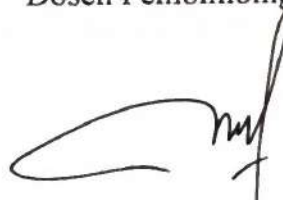
PRO PATRIA
Disusun Oleh:

ADI DWI CAHYONO
NIM: 04323015

Surabaya, 25 Juli 2025

Mengetahui/Menyetujui

Dosen Pembimbing,



Made Kamisutara, S.T., M.Kom

NIDN : 0706027501

SURAT PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Laporan Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan disuatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat Karya/Pendapat yang pernah ditulis oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam Daftar Acuan/Daftar Pustaka.

Apabila ditemukan suatu Jiplakan/Plagiat maka saya bersedia menerima akibat berupa sanksi Akademis dan sanksi lain yang diberikan oleh yang berwenang sesuai ketentuan peraturan dan perundang-undangan yang berlaku.

Surabaya, 25 Juli 2025



Adi Dwi Cahyono
NIM : 04323015

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah Subhanahu wa Ta'ala atas limpahan rahmat dan hidayah-Nya, sehingga laporan skripsi berjudul “Implementasi Border Gateway Protocol (BGP) Community untuk Mitigasi DDoS Flooding di Dinas Komunikasi dan Informatika Provinsi Jawa Timur” dapat diselesaikan dengan baik. Ucapan terima kasih penulis sampaikan kepada:

1. Bapak Made Kamisutara selaku Dosen Pembimbing atas bimbingan, arahan, dan motivasi yang diberikan.
2. Bapak Moh. Noor Al Azam selaku Ketua Program Studi Teknik Informatika beserta jajaran dosen dan staf administrasi atas dukungan akademik.
3. Pihak Dinas Komunikasi dan Informatika Provinsi Jawa Timur atas kesempatan, data, serta dukungan teknis.
4. Kedua orang tua dan keluarga atas doa, dukungan moral, dan material yang tiada henti.

Penulis menyadari masih adanya keterbatasan dalam penelitian ini, baik dari sisi ruang lingkup uji, variasi skenario serangan, maupun kedalaman analisis performa. Oleh karena itu kritik dan saran yang membangun sangat penulis harapkan demi penyempurnaan di masa mendatang.

Akhir kata, semoga Allah Subhanahu wa Ta'ala membalas semua kebaikan pihak yang telah membantu dan semoga laporan ini bermanfaat bagi pembaca.

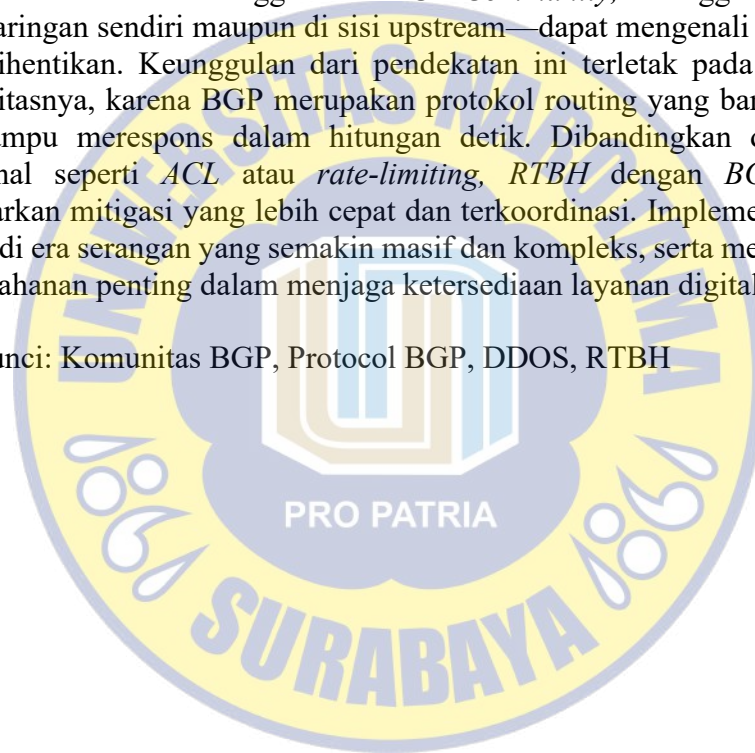
Surabaya, 25 Juli 2025

Adi Dwi Cahyono

ABSTRAK

Serangan *DDoS* (*Distributed Denial-of-Service*) merupakan salah satu ancaman paling serius dalam jaringan, terutama ketika sejumlah besar lalu lintas secara sengaja diarahkan untuk melumpuhkan layanan. Dalam kondisi seperti ini, kemampuan jaringan untuk merespons dengan cepat menjadi sangat krusial. Salah satu pendekatan yang telah terbukti efektif adalah penggunaan *Remote Triggered Black Hole (RTBH)* melalui *protokol BGP (Border Gateway Protocol)*. Dengan teknik ini, lalu lintas berbahaya yang menuju ke IP atau prefix tertentu dapat diblokir secara otomatis sebelum mencapai jaringan inti. Proses ini dilakukan dengan menandai rute menggunakan *BGP Community*, sehingga router—baik di dalam jaringan sendiri maupun di sisi upstream—dapat mengenali rute mana yang harus dihentikan. Keunggulan dari pendekatan ini terletak pada kecepatan dan skalabilitasnya, karena BGP merupakan protokol routing yang banyak digunakan dan mampu merespons dalam hitungan detik. Dibandingkan dengan metode tradisional seperti *ACL* atau *rate-limiting*, *RTBH* dengan *BGP Community* menawarkan mitigasi yang lebih cepat dan terkoordinasi. Implementasi ini sangat relevan di era serangan yang semakin masif dan kompleks, serta menjadi salah satu lini pertahanan penting dalam menjaga ketersediaan layanan digital.

Kata Kunci: Komunitas BGP, Protocol BGP, DDOS, RTBH



ABSTRACT

Distributed Denial-of-Service (DDoS) attacks represent one of the most serious threats to networks, especially when a large volume of traffic is deliberately directed to disrupt services. In such situations, the network's ability to respond swiftly becomes crucial. One approach that has proven effective is the use of Remote Triggered Black Hole (RTBH) via the Border Gateway Protocol (BGP). With this technique, malicious traffic destined for specific IPs or prefixes can be automatically blocked before reaching the core network. This process is carried out by tagging routes using BGP Community, enabling routers—both within the local network and at the upstream level—to identify which routes should be dropped. The main advantage of this approach lies in its speed and scalability, as BGP is a widely used routing protocol capable of responding within seconds. Compared to traditional methods such as ACLs or rate-limiting, RTBH with BGP Community offers faster and more coordinated mitigation. This implementation is highly relevant in an era of increasingly massive and complex attacks, and serves as a crucial line of defense in maintaining the availability of digital services.

Keywords: BGP Community, BGP Protocol, DDoS, RTBH



DAFTAR ISI

HALAMAN SAMPUL	i
HALAMAN JUDUL.....	ii
HALAMAN PERSETUJUAN PEMBIMBING	iii
HALAMAN PENGESAHAN LAPORAN AKHIR.....	iv
SURAT PERNYATAAN	v
MOTTO DAN PERSEMBAHAN.....	vi
KATA PENGANTAR.....	vii
ABSTRAK.....	viii
DAFTAR ISI.....	x
DAFTAR GAMBAR.....	xii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	4
1.2 Rumusan Masalah.....	4
1.3 Tujuan Penilitan.....	4
1.4 Manfaat Penelitian.....	3
BAB II TINJAUAN PUSTAKA.....	6
2.1 Penelitian Sebelumnya.....	6
2.2 Kajian Teoritis.....	8
BAB III METODOLOGI PENEILITIAN	38
3.1 Metode Pengupulan Data.....	38
3.2 Metode Pengembangan Sistem.....	39
BAB IV HASIL DAN PEMBAHASAN.....	44
4.1 Analisis	44
4.2 Desain	46
4.3 Simulasi	50
4.4 Implementasi.....	53
4.5 Monitoring	65
4.6 Manajemen	70

BAB V PENUTUP.....	72
5.1 Kesimpulan	72
5.2 Saran	73
DAFTAR PUSTAKA.....	74
LAMPIRAN	77



DAFTAR GAMBAR

Gambar 2.1 Jenis Routing Dinamis	9
Gambar 2.2 Jenis topologi iBGP	17
Gambar 2.3 Jenis Topologi eBGP	18
Gambar 2.4 Topologi iBGP dan eBGP	19
Gambar 2.5 Jenis BGP Atribut	20
Gambar 2.6 Skema Route Reflector	25
Gambar 2.7 Ilustrasi serangan ddos.....	28
Gambar 2.8 Kantor Dinas Kominfo Jatim.....	34
Gambar 3.1 Metodologi NDLC	40
Gambar 4.1 Topologi Existingg	45
Gambar 4.2 Rancangan Desain Topologi.....	47
Gambar 4.3 Topologi pada GNS	51
Gambar 4.4 Setting add filter RTBH pada core 1	58
Gambar 4.5 Setting add filter RTBH pada core 2	59
Gambar 4.6 Setting add filter RTBH pada core 3	59
Gambar 4.7 Setting add out-filter BGP peer core-to-border_A ...	60
Gambar 4.8 Setting add out-filter BGP peer core-to-border_B....	60
Gambar 4.9 Tabel Routing Penerimaan Prefix A.....	61
Gambar 4.10 Tabel Routing Penerimaan Prefix B.....	61
Gambar 4.11 Setting add filter in-from-border	62
Gambar 4.12 Setting add filter in-from-border	62
Gambar 4.13 Setting add filter in-from-border	63
Gambar 4.14 Penambahan IP Bogon.....	63
Gambar 4.15 Tabel Routing Penerimaan Tag	64
Gambar 4.16 Tes ping ke IP Target DDOS.....	64
Gambar 4.17 Skenario Serangan	66
Gambar 4.18 Tes Ping ke Legitimate site.....	67
Gambar 4.19 Penggunaan TFgen	67
Gambar 4.20 Monitoring Traffic DDOS	68

Gambar 4.21 Tes Ping dari user 268

Gambar 4.22 Menganktignan filter RTBH.....69

