



**ANALISIS KETAHANAN BGP DAN EIGRP
TERHADAP ROUTE INJECTION DENGAN
MITIGASI BASIC FILTERING MENGGUNAKAN
PREFIX-LIST
SKRIPSI**

Sahrul Apriandi 2207421012

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN
JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN
KOMPUTER
POLITEKNIK NEGERI JAKARTA
2026**



**ANALISIS KETAHANAN BGP DAN EIGRP
TERHADAP ROUTE INJECTION DENGAN
MITIGASI BASIC FILTERING MENGGUNAKAN
PREFIX-LIST**

SKRIPSI

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

Sahrul Apriandi

2207421012

**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 mengumunkan 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 : Sahrul Apriandi

NIM : 2207421012

Jurusan/Program Studi : Teknik Informatika dan Komputer/Teknik
Multimedia dan Jaringan

Judul Skripsi : Analisis Ketahanan BGP dan EIGRP terhadap
Route Injection dengan Mitigasi *Basic Filtering*
Menggunakan *Prefix-list*

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,

Yang membuat pernyataan



Sahrul Apriandi

NIM. 2207421012



© 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 : Sahrul Apriandi
NIM : 2207421012
Program Studi : Teknik Multimedia dan Jaringan
Judul Skripsi : Analisis Ketahanan BGP dan EIGRP terhadap
Route Injection dengan Mitigasi Basic Filtering
Menggunakan Prefix-list

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

Disahkan oleh:

Pembimbing I Defiana Arnaldy, S.Tp., M.Si.
Penguji I Asep Kurniawan, S.Pd., M.Kom.
Penguji II Fachroni Arbi Murad, S.Kom., M.Kom.
Penguji III Iik Muhamad Malik Matin, S.Kom., M.T.

(*[Signature]*)
(*[Signature]*)
(*[Signature]*)
(*[Signature]*)

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 mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas rahmat, karunia, dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis Ketahanan BGP dan EIGRP terhadap *Route Injection* dengan Mitigasi *Basic Filtering* Menggunakan *Prefix-list*”. 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.

Dalam penyusunan skripsi ini, penulis menyadari bahwa selesainya skripsi ini tidak terlepas dari doa, dukungan, arahan, dan bantuan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Allah SWT yang telah memberikan rahmat, kesehatan, kekuatan, dan kelancaran kepada penulis dalam menyelesaikan skripsi ini.
2. Bapak Defiana Arnaldy, S.Tp., M.Si., selaku dosen pembimbing yang telah memberikan arahan, bimbingan, masukan, serta waktu selama proses penyusunan skripsi ini.
3. Seluruh dosen dan staf Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta yang telah memberikan ilmu, bantuan, dan pelayanan akademik selama masa perkuliahan.
4. Almarhumah Ibu tercinta yang telah lebih dahulu tenang di sisi Allah SWT, atas kasih sayang, doa, dan pengorbanan yang menjadi kekuatan bagi penulis dalam menjalani proses pendidikan hingga tahap ini.
5. Ayah tercinta yang selalu berjuang, memberikan doa, dukungan, semangat, serta pengorbanan yang besar kepada penulis selama masa perkuliahan hingga penyusunan skripsi ini.
6. Saudara, om, dan tante yang telah memberikan doa, dukungan, motivasi, serta bantuan kepada penulis selama proses perkuliahan dan penyusunan skripsi.



© 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

7. Rekan-rekan Program Studi Teknik Multimedia dan Jaringan yang telah memberikan bantuan, dukungan, serta semangat selama masa perkuliahan hingga selesainya skripsi ini.
8. Syifa Chandra, Alvito, Jibrán, Salsabila, Indah Dwi, Shabrina, Wibi, Abdan, Rizki dan Audi yang telah memberikan dukungan, semangat, bantuan, serta menjadi tempat berbagi cerita selama proses perkuliahan hingga penyusunan skripsi ini.
9. Seluruh pihak yang tidak dapat disebutkan satu per satu, yang telah membantu dan memberikan dukungan kepada penulis dalam menyelesaikan skripsi ini.

Akhir kata, penulis berharap Allah SWT membalas segala kebaikan semua pihak yang telah membantu. Penulis menyadari bahwa skripsi ini masih memiliki keterbatasan, sehingga kritik dan saran yang membangun sangat diharapkan untuk perbaikan di masa mendatang. Semoga skripsi ini dapat memberikan manfaat bagi pembaca serta menjadi referensi dalam bidang keamanan *routing* dan jaringan komputer.

Depok, 9 Juni 2026

**POLITEKNIK
NEGERI
JAKARTA**

Sahrul Apriandi



© 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 di bawah ini:

Nama : Sahrul Apriandi
NIM : 2207421012
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:

Analisis Ketahanan BGP dan EIGRP terhadap *Route Injection* dengan Mitigasi *Basic Filtering* Menggunakan *Prefix-list*

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,

Yang menyatakan



Sahrul Apriandi

NIM. 2207421012



Analisis Ketahanan BGP dan EIGRP terhadap *Route Injection* dengan Mitigasi *Basic Filtering* Menggunakan *Prefix-list*

ABSTRAK

Keamanan routing merupakan aspek penting dalam menjaga stabilitas jaringan karena manipulasi informasi rute dapat menyebabkan perubahan jalur trafik dan gangguan konektivitas. Penelitian ini bertujuan menganalisis ketahanan Border Gateway Protocol (BGP) dan Enhanced Interior Gateway Routing Protocol (EIGRP) terhadap *route injection*, serta mengevaluasi efektivitas *basic filtering* menggunakan *prefix-list* sebagai mitigasi. Pengujian dilakukan pada simulasi Graphical Network Simulator 3 (GNS3) dengan tiga skenario, yaitu *baseline*, *route injection*, dan setelah mitigasi. Skenario *route injection* dilakukan oleh R4-ATTACKER dengan memasukkan rute tidak sah berupa *prefix host /32* menuju PC1, PC2, dan PC3, yaitu 192.168.16.2/32, 192.168.17.2/32, dan 192.168.18.2/32. Pada BGP, rute tidak sah masuk sebagai *prefix* yang diiklankan oleh R4-ATTACKER, sedangkan pada EIGRP rute tidak sah masuk sebagai rute eksternal dengan kode D EX. Evaluasi dilakukan berdasarkan *routing table*, *next-hop*, *ping*, *traceroute*, *Wireshark*, waktu pemulihan, *delay*, *throughput*, dan *packet loss*. Hasil pengujian menunjukkan bahwa saat *route injection*, nilai *packet loss* rata-rata meningkat menjadi 66,67% pada BGP dan EIGRP. Nilai *throughput* BGP menurun dari 1,440 Kbps pada kondisi *baseline* menjadi 0,957 Kbps saat *route injection*, sedangkan EIGRP menurun dari 1,498 Kbps menjadi 0,967 Kbps. Setelah mitigasi diterapkan, rute tidak sah berhasil ditolak, *packet loss* kembali menjadi 0%, dan *throughput* meningkat menjadi 1,477 Kbps pada BGP serta 1,468 Kbps pada EIGRP. Dengan demikian, *basic filtering* menggunakan *prefix-list* efektif dalam membatasi dampak *route injection* pada BGP dan EIGRP.

Kata kunci: *basic filtering*, BGP, EIGRP, *prefix-list*, Quality of Service, *route injection*.

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 mengumumkan 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
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS.....	vi
ABSTRAK	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	x
DAFTAR GAMBAR.....	xi
BAB I.....	1
PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	4
1.3 Batasan Masalah	5
1.4 Tujuan dan Manfaat.....	7
1.5 Sistematika Penulisan	8
BAB II.....	9
TINJAUAN PUSTAKA	9
2.1 Penelitian Terkait	9
2.2 Konsep <i>Routing</i> dan <i>Control Plane</i>	11
2.3 <i>Border Gateway Protocol</i> (BGP) dan <i>Autonomous System</i>	12
2.4 <i>Enhanced Interior Gateway Routing Protocol</i> (EIGRP).....	13
2.5 <i>Route Injection</i>	13
2.6 Mitigasi Basic Filtering Menggunakan Prefix-list.....	14
2.7 Parameter Evaluasi dan <i>Quality of Service</i> (QoS)	14
2.8 GNS3.....	17
2.9 Wireshark	17
BAB III.....	19
METODE PENELITIAN.....	19
3.1 Rancangan Penelitian	19
3.2 Tahapan Penelitian	21
3.3 Objek Penelitian.....	25
BAB IV	27



© 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

HASIL DAN PEMBAHASAN	27
4.1 Analisis Kebutuhan	27
4.2 Perancangan Sistem.....	29
4.2.1 Perancangan Topologi BGP.....	30
4.2.2 Perancangan Topologi EIGRP	32
4.2.3 Perancangan Pengalamatan IP	34
4.2.4 Perancangan Mekanisme Route Injection.....	36
4.2.5 Perancangan Mekanisme Mitigasi	37
4.2.6 Perancangan Skenario Pengujian.....	37
4.3 Implementasi Sistem	39
4.3.1 Implementasi <i>Routing</i> BGP.....	39
4.3.2 Implementasi <i>Routing</i> EIGRP	43
4.3.3 Verifikasi Konektivitas Jaringan	47
4.4 Pengujian	50
4.4.1 Deskripsi Pengujian	51
4.4.2 Prosedur Pengujian	52
4.4.3 Data Hasil Pengujian	54
4.4.4 Analisis Data / Evaluasi Pengujian	85
BAB V.....	107
PENUTUP	107
5.1 Simpulan.....	107
5.2 Saran	108
DAFTAR PUSTAKA	109
DAFTAR RIWAYAT HIDUP.....	112
LAMPIRAN	113



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 TABEL

Tabel 2.1 Penelitian Terkait	9
Tabel 2. 2 Indeks Delay berdasarkan standar <i>TIPHON</i>	16
Tabel 2.3 Indeks <i>Packet loss</i> berdasarkan standar <i>TIPHON</i>	17
Tabel 4.1 Analisis Kebutuhan.....	27
Tabel 4.2 Kebutuhan Perangkat Penelitian.....	28
Tabel 4.3 Pembagian Autonomous System pada Topologi BGP.....	32
Tabel 4.4 Pembagian Router pada Topologi EIGRP	34
Tabel 4.5 Pengalamatan IP.....	35
Tabel 4.6 Skenario Pengujian.....	38
Tabel 4.7 Hasil Pengujian QoS Baseline pada Topologi BGP	57
Tabel 4.8 Hasil Pengujian QoS Baseline pada Topologi EIGRP	59
Tabel 4.9 Target Route Injection	60
Tabel 4.10 Hasil Pengujian QoS Saat Route Injection pada Topologi BGP	65
Tabel 4.11 Hasil Pengujian QoS Saat Route Injection pada Topologi EIGRP	70
Tabel 4.12 Hasil Pengujian QoS Setelah Mitigasi pada Topologi BGP.....	76
Tabel 4.13 Hasil Pengujian QoS Setelah Mitigasi pada Topologi EIGRP.....	80
Tabel 4.14 Hasil Pengujian QoS pada Topologi BGP	88
Tabel 4.15 Hasil Pengujian QoS Saat Route Injection pada Topologi BGP	88
Tabel 4.16 Hasil Pengujian QoS Setelah Mitigasi pada Topologi BGP.....	91
Tabel 4.17 Hasil Pengujian QoS Baseline pada Topologi EIGRP.....	93
Tabel 4.18 Hasil Pengujian QoS Saat <i>Route Injection</i> pada Topologi EIGRP.....	94
Tabel 4.19 Hasil Pengujian Waktu Konvergensi dan Pemulihan	96
Tabel 4.20 Rekapitulasi Perbandingan Rata-rata QoS BGP dan EIGRP	99
Tabel 4.21 Hasil Pengujian Waktu Serangan Masuk dan Pemulihan	103
Tabel 4.22 Perbandingan Hasil Pengamatan GNS3 dan Wireshark	105



DAFTAR GAMBAR

Gambar 3.1 Tahapan Penelitian.....	21
Gambar 4.1 Topologi BGP pada GNS3.....	31
Gambar 4.2 Topologi EIGRP pada GNS3	33
Gambar 4.3 Hasil Verifikasi Neighbor BGP pada R1-KOMINFO	42
Gambar 4.4 Verifikasi Neighbor EIGRP pada Router R1-KOMINFO.....	46
Gambar 4.5 Pengujian Konektivitas pada Kondisi Baseline	49
Gambar 4.6 Hasil Pengujian Ping Baseline pada Topologi BGP.....	56
Gambar 4.7 Capture ICMP Baseline pada Topologi BGP	56
Gambar 4.8 Hasil Pengujian Ping Baseline pada Topologi EIGRP	58
Gambar 4.9 Capture ICMP Baseline pada Topologi EIGRP.....	58
Gambar 4.10 Konfigurasi <i>Route Injection</i> pada R4-ATTACKER	61
Gambar 4.11 Hasil Verifikasi Route Injection BGP Target PC1	62
Gambar 4.12 Hasil Verifikasi Route Injection BGP Target PC2.....	62
Gambar 4.13 Hasil Verifikasi Route Injection BGP Target PC3	62
Gambar 4.14 Hasil Pengujian <i>Ping</i> Saat <i>Route Injection</i> pada Topologi BGP	63
Gambar 4.15 Capture ICMP Saat Route Injection pada Topologi BGP	64
Gambar 4.16 Konfigurasi <i>Route Injection</i> EIGRP pada R4-ATTACKER.....	67
Gambar 4.17 Hasil Verifikasi Route Injection EIGRP Target PC1	67
Gambar 4.18 Hasil Verifikasi <i>Route Injection</i> EIGRP Target PC2.....	68
Gambar 4.19 Hasil Verifikasi Route Injection EIGRP Target PC3	68
Gambar 4.20 Hasil Pengujian <i>Ping</i> Saat <i>Route Injection</i> pada Topologi EIGRP.	69
Gambar 4.21 <i>Capture</i> ICMP Saat <i>Route Injection</i> pada Topologi EIGRP.....	70
Gambar 4.22 Konfigurasi <i>Basic Filtering</i> BGP pada Router R1-KOMINFO	73
Gambar 4.23 Tabel BGP R1-KOMINFO Setelah Mitigasi BGP.....	73
Gambar 4.24 <i>Routing Table</i> R1-KOMINFO Setelah Mitigasi BGP	74
Gambar 4.25 Pemulihan Konektivitas Setelah Mitigasi BGP	75
Gambar 4.26 <i>Capture</i> ICMP Setelah Mitigasi BGP	75
Gambar 4.27 Konfigurasi <i>Basic Filtering</i> EIGRP pada Router R1-KOMINFO..	77
Gambar 4.28 <i>Routing Table</i> R1-KOMINFO Setelah Mitigasi EIGRP.....	78
Gambar 4.29 Pemulihan Konektivitas Setelah Mitigasi EIGRP	79
Gambar 4.30 <i>Capture</i> ICMP Setelah Mitigasi EIGRP	80
Gambar 4.31 Hasil <i>Traceroute</i> pada Topologi BGP.....	82
Gambar 4.32 Hasil <i>Traceroute</i> pada Topologi EIGRP	84
Gambar 4.33 Grafik Perbandingan Packet Loss BGP dan EIGRP.....	101
Gambar 4.34 Grafik Perbandingan Delay BGP dan EIGRP.....	102
Gambar 4.35 Grafik Perbandingan Throughput BGP dan EIGRP	102
Gambar 4.36 Grafik Perbandingan Waktu Serangan Masuk dan Pemulihan.....	104

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

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

BAB I PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah meningkatkan ketergantungan masyarakat terhadap jaringan komputer dan Internet dalam berbagai aktivitas. Jaringan komputer tidak hanya digunakan untuk pertukaran data, tetapi juga menjadi infrastruktur utama dalam mendukung layanan digital, komunikasi, dan operasional organisasi. (Kabir et al., 2021) menjelaskan bahwa komunikasi berbasis Internet telah menjadi bagian penting dalam kehidupan sehari-hari, sedangkan protokol *routing* berperan dalam menentukan jalur pengiriman data dari sumber menuju tujuan. Oleh karena itu, keandalan protokol *routing* menjadi faktor penting dalam menjaga ketersediaan dan kualitas layanan jaringan.

Dalam jaringan komputer, protokol *routing* digunakan untuk membangun dan memperbarui informasi rute agar paket data dapat dikirim melalui jalur yang sesuai. Protokol *routing* dinamis seperti *Border Gateway Protocol* (BGP) dan *Enhanced Interior Gateway Routing Protocol* (EIGRP) memungkinkan router bertukar informasi *routing* secara otomatis ketika terjadi perubahan kondisi jaringan. BGP banyak digunakan pada jaringan antar-*Autonomous System*, sedangkan EIGRP digunakan pada jaringan internal atau *enterprise*. Meskipun kedua protokol tersebut memiliki karakteristik berbeda, keduanya sama – sama bergantung pada validitas informasi *routing* yang diterima router dalam proses pemilihan jalur.

Keamanan *routing* menjadi penting karena kesalahan atau manipulasi informasi rute dapat menyebabkan router memilih jalur yang tidak semestinya. (OECD, 2022) menjelaskan bahwa sistem *routing* Internet masih menghadapi berbagai insiden seperti *route leak* dan *route hijacking* yang dapat mengganggu ketersediaan layanan serta mengalihkan trafik ke jalur yang tidak diinginkan. Pada BGP, salah satu serangan yang sering dibahas adalah *prefix hijacking*, yaitu kondisi ketika suatu *Autonomous System* mengiklankan prefix yang bukan miliknya. (Sermpezis et al., 2021)



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

menyatakan bahwa BGP prefix hijacking merupakan ancaman serius terhadap ketahanan dan keamanan komunikasi Internet karena dapat memengaruhi ketersediaan dan kerahasiaan komunikasi.

Insiden keamanan *routing* juga masih terjadi hingga saat ini. MANRS mencatat bahwa insiden *routing* seperti *route leak*, *route hijack*, dan IP *spoofing* dapat menyebabkan layanan Internet melambat, tidak dapat dijangkau, atau trafik dialihkan melalui jaringan yang tidak semestinya (Siddiqui, 2022). Selain itu (Labs, 2025) menjelaskan bahwa BGP *hijacking* masih menjadi ancaman karena BGP tidak memiliki mekanisme autentikasi bawaan yang kuat, sementara penerapan mekanisme keamanan seperti RPKI dan *Route Origin Validation* belum merata. Kondisi tersebut menunjukkan bahwa isu keamanan *routing* masih relevan untuk diteliti, khususnya pada skenario manipulasi informasi *routing*.

Selain BGP, jaringan internal yang menggunakan EIGRP juga perlu diperhatikan dari sisi ketahanan *routing*. EIGRP dikenal sebagai protokol *routing* dinamis yang mampu menentukan jalur terbaik dan beradaptasi terhadap perubahan topologi jaringan. (Kabir et al., 2021) menggunakan EIGRP sebagai salah satu protokol yang dianalisis berdasarkan *latency*, *throughput*, dan *convergence time* pada jaringan *enterprise* (Antoni Musril et al., 2021) juga menunjukkan bahwa EIGRP dapat diterapkan pada jaringan kampus dengan pengukuran *Quality of Service* (QoS) seperti *throughput*, *packet loss*, *latency*, dan *jitter*. Namun, kemampuan EIGRP dalam memilih rute dan melakukan konvergensi tidak berarti protokol tersebut bebas dari risiko manipulasi informasi *routing*, terutama apabila terdapat *route injection* atau informasi rute yang tidak sah masuk ke domain *routing* internal.

Dampak dari manipulasi informasi *routing* tidak hanya terlihat pada perubahan jalur, tetapi juga dapat memengaruhi kualitas layanan jaringan. Ketika router memilih rute yang salah atau tidak valid, paket data dapat mengalami gangguan berupa peningkatan *delay*, penurunan *throughput*,



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

atau *packet loss*. (Antoni Musril et al., 2021) menjelaskan bahwa QoS digunakan untuk mengukur kemampuan jaringan dalam memberikan layanan. (Nisa et al., 2024) juga menjelaskan bahwa pengujian QoS dapat dilakukan menggunakan parameter *throughput*, *delay*, *jitter*, dan *packet loss* untuk mengetahui kualitas kinerja jaringan. Dengan demikian, QoS dapat digunakan sebagai indikator untuk menilai dampak serangan *routing* dan efektivitas mitigasi yang diterapkan.

Berbagai mekanisme keamanan telah dikembangkan untuk mengurangi risiko manipulasi informasi *routing*, seperti *Internet Routing Registry* (IRR), *Resource Public Key Infrastructure* (RPKI), *Route Origin Validation* (ROV), dan BGPsec. Namun, (OECD, 2022) menjelaskan bahwa belum ada satu mekanisme yang dapat menyelesaikan seluruh permasalahan keamanan *routing* secara menyeluruh. Selain itu, beberapa mekanisme keamanan membutuhkan penerapan yang lebih kompleks dan belum selalu mudah diterapkan secara merata pada jaringan operasional. Oleh karena itu, mekanisme yang lebih sederhana dan mudah dikonfigurasi seperti *basic filtering* masih relevan untuk diuji sebagai langkah mitigasi.

Basic filtering dapat diterapkan dengan mengendalikan informasi *routing* yang masuk maupun keluar dari router. (McDaniel et al., 2021) menunjukkan bahwa mekanisme filtering dapat membatasi propagasi *route leak* secara signifikan pada BGP. Sementara itu, *distribute-list* dan *prefix-list* dapat digunakan untuk mengontrol *routing* update pada protokol *routing* dinamis agar informasi rute yang diterima atau diiklankan menjadi lebih terkontrol (Global, 2023). Dengan demikian, *basic filtering* menjadi mekanisme mitigasi yang praktis karena dapat diterapkan melalui konfigurasi router tanpa membutuhkan infrastruktur keamanan tambahan yang kompleks.

Berdasarkan penelitian sebelumnya, (Eko Kurniawanto, 2021) telah membahas implementasi BGP pada jaringan MAN dan melakukan pengujian kualitas layanan menggunakan parameter QoS. Namun,



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

penelitian tersebut belum membahas aspek keamanan *routing*, skenario serangan, mitigasi, maupun perbandingan dengan protokol EIGRP. Di sisi lain, penelitian terkait EIGRP seperti (Kabir et al., 2021) dan (Antoni Musril et al., 2021) lebih banyak berfokus pada performa *routing* dan QoS, bukan pada pengujian ketahanan terhadap manipulasi informasi *routing*. Oleh karena itu, masih diperlukan penelitian yang menguji dan membandingkan ketahanan BGP dan EIGRP terhadap manipulasi informasi *routing* serta mengevaluasi efektivitas *basic filtering* sebagai mekanisme mitigasi.

Berdasarkan uraian tersebut, penelitian ini dilakukan untuk menganalisis perbandingan ketahanan protokol BGP dan EIGRP terhadap manipulasi informasi *routing*, dengan skenario *route injection* pada BGP dan EIGRP. Penelitian ini juga mengevaluasi efektivitas *basic filtering* dalam memitigasi serangan berdasarkan parameter QoS berupa *throughput*, *delay*, dan *packet loss*. Hasil penelitian diharapkan dapat memberikan bukti empiris mengenai dampak manipulasi *routing* terhadap kualitas layanan jaringan serta menjadi referensi bagi administrator jaringan dalam menerapkan mekanisme keamanan *routing* yang sederhana dan mudah diimplementasikan.

1.2 Perumusan Masalah

Berdasarkan latar belakang, masih terdapat sejumlah persoalan terkait kerentanan pertukaran informasi *routing* terhadap manipulasi *route advertisement*, khususnya melalui *route injection* pada BGP dan EIGRP. Selain itu, diperlukan evaluasi terhadap mekanisme mitigasi yang lebih ringan dan realistis seperti *basic filtering* pada protokol BGP dan EIGRP di lingkungan simulasi GNS3. Oleh karena itu, permasalahan dalam penelitian ini dirumuskan sebagai berikut:

1. Bagaimana karakteristik *routing* dan *Quality of Service* (QoS) pada protokol BGP dan EIGRP dalam kondisi *baseline* sebelum terjadi manipulasi informasi *routing*?



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

2. Bagaimana dampak *route injection* terhadap *routing table*, pemilihan jalur komunikasi, waktu konvergensi atau pemulihan, *delay*, *throughput*, dan *packet loss* pada protokol BGP dan EIGRP?
3. Bagaimana penerapan *basic filtering* berbasis *prefix-list* dalam menolak rute tidak sah yang berasal dari *router attacker* pada protokol BGP dan EIGRP?
4. Bagaimana efektivitas *basic filtering* dalam memitigasi manipulasi informasi *routing* pada BGP dan EIGRP berdasarkan perubahan *routing table*, konektivitas, dan parameter QoS?

1.3 Batasan Masalah

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

1. Penelitian ini dilakukan menggunakan simulasi jaringan pada GNS3, sehingga hasil pengujian merepresentasikan kondisi pada lingkungan simulasi dan tidak dimaksudkan sebagai representasi langsung jaringan produksi.
2. Protokol *routing* yang dianalisis dibatasi pada *Border Gateway Protocol* (BGP) dan *Enhanced Interior Gateway Routing Protocol* (EIGRP) dengan satu topologi fisik yang sama. Topologi penelitian terdiri dari PC-ATTACKER sebagai representasi sumber serangan dari Internet, R1-KOMINFO sebagai router utama dan *gateway* menuju Internet, R2-CAPIL, R3-SANGIR, R4-ATTACKER sebagai *compromised router*, *switch backbone*, serta tiga client pengujian yaitu PC1, PC2, dan PC3.
3. Skenario serangan dibatasi pada *route injection*, yaitu penyisipan route atau prefix tidak sah ke dalam proses *routing*. Pada BGP, *route injection* dilakukan melalui pengiklanan prefix tidak sah dari *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 mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

attacker, sedangkan pada EIGRP dilakukan melalui *static route* palsu yang di-*redistribute* ke proses EIGRP.

4. Penelitian ini tidak membahas proses eksploitasi, teknik peretasan, pencurian kredensial, maupun proses *attacker* memperoleh akses administratif ke router. Dalam penelitian ini, PC-ATTACKER ditempatkan pada sisi Internet sebagai representasi sumber serangan eksternal dan diasumsikan telah berhasil memperoleh akses kendali terhadap R4-ATTACKER. Router R4-ATTACKER kemudian berperan sebagai *compromised router* yang digunakan untuk melakukan *route injection*.
5. Mitigasi yang digunakan dibatasi pada *basic filtering* berbasis *prefix-list* untuk menolak *prefix* atau route tidak sah yang berasal dari *router attacker*. Pada BGP, *filtering* diterapkan pada router penerima *update* dari *neighbor attacker*, sedangkan pada EIGRP *filtering* diterapkan pada *router legitimate* yang menerima *update route* dari *attacker* dalam domain EIGRP.
6. Parameter pengujian dibatasi pada perubahan *routing table*, *next-hop* atau jalur terpilih, waktu konvergensi atau pemulihan, serta parameter *Quality of Service* (QoS) yang meliputi *delay*, *throughput*, dan *packet loss*. *Traffic* pengujian menggunakan ICMP ping dan dianalisis melalui hasil terminal serta capture Wireshark. Pengujian dilakukan terhadap tiga host tujuan, yaitu PC1 dengan alamat 192.168.16.2, PC2 dengan alamat 192.168.17.2, dan PC3 dengan alamat 192.168.18.2 pada kondisi *baseline*, *route injection*, dan setelah mitigasi.
7. Penelitian ini tidak membahas serangan data plane seperti ARP *spoofing*, *sniffing*, *Man-in-the-Middle*, *firewall bypass*, maupun enkripsi aplikasi, serta tidak membahas mekanisme keamanan *routing* lain seperti RPKI, BGPsec, autentikasi *routing*, *firewall-based access control*, atau *intrusion detection system* karena fokus mitigasi dibatasi pada *basic filtering*.



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, khususnya pada aspek keamanan *routing* atau control plane. Oleh karena itu, pada bagian ini diuraikan tujuan dan manfaat penelitian sebagai berikut.

Tujuan penelitian ini adalah:

1. Menganalisis karakteristik kualitas layanan jaringan pada protokol BGP dan EIGRP pada kondisi normal berdasarkan parameter *throughput*, *delay*, dan *packet loss*.
2. Menganalisis pengaruh *route injection* terhadap *routing* table, jalur komunikasi, dan kualitas layanan jaringan pada protokol BGP dan EIGRP berdasarkan parameter *throughput*, *delay*, dan *packet loss*.
3. Membandingkan tingkat ketahanan protokol BGP dan EIGRP terhadap *route injection* berdasarkan perubahan *routing* table, waktu konvergensi atau pemulihan, *throughput*, *delay*, dan *packet loss* dari kondisi normal ke kondisi saat serangan.
4. Menganalisis efektivitas penerapan *basic filtering* berbasis *prefix-list* dalam memitigasi *route injection* pada protokol BGP dan EIGRP berdasarkan perubahan *routing* table, waktu pemulihan, *throughput*, *delay*, dan *packet loss*.

Secara umum, penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Memberikan informasi mengenai karakteristik kualitas layanan jaringan pada protokol BGP dan EIGRP pada kondisi normal maupun saat terjadi *route injection* berdasarkan parameter *throughput*, *delay*, dan *packet loss*.
2. Menjadi referensi dalam memahami perbedaan tingkat ketahanan protokol BGP dan EIGRP terhadap *route injection*.



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

3. Memberikan gambaran mengenai efektivitas penerapan *basic filtering* berbasis *prefix-list* sebagai mekanisme mitigasi terhadap *route injection*.
4. Menjadi referensi bagi administrator jaringan dalam menerapkan mekanisme keamanan dasar untuk membatasi masuknya route atau prefix tidak sah ke dalam *routing table*.
5. Menambah referensi penelitian mengenai keamanan *routing*, khususnya terkait perbandingan ketahanan protokol BGP dan EIGRP terhadap *route injection* serta efektivitas *basic filtering* berdasarkan parameter *Quality of Service* (QoS).

1.5 Sistematika Penulisan

Berikut adalah sistematika penulisan yang digunakan dalam penelitian ini, yaitu sebagai berikut:

1. Bab I Pendahuluan
Bab ini membahas latar belakang penelitian, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan.
2. Bab II Tinjauan Pustaka
Bab ini membahas teori yang mendukung penelitian, meliputi *routing*, *control plane*, BGP, EIGRP, *route injection*, *basic filtering*, *Quality of Service* (QoS), serta penelitian terdahulu yang relevan.
3. Bab III Metode Penelitian
Bab ini menjelaskan rancangan penelitian, tahapan penelitian, objek penelitian, diagram alir sistem, skenario pengujian, serta metode pengambilan dan analisis data yang digunakan dalam penelitian.
4. Bab IV Hasil dan Pembahasan
Bab ini menyajikan hasil implementasi, pengujian, dan analisis sistem, meliputi mekanisme *routing*, *route injection*, *basic filtering*, perubahan rute, waktu konvergensi, serta pengukuran *Quality of Service* (QoS).
5. Bab V Penutup
Bab ini berisi kesimpulan penelitian berdasarkan hasil pengujian yang diperoleh serta saran untuk pengembangan penelitian selanjutnya.

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

BAB V PENUTUP

5.1 Simpulan

Berdasarkan hasil perancangan, implementasi, pengujian, dan analisis yang telah dilakukan, diperoleh beberapa simpulan sebagai berikut:

1. Pada kondisi *baseline*, simulasi jaringan pada GNS3 berhasil merepresentasikan pengujian keamanan *routing* pada dua protokol, yaitu BGP sebagai protokol *routing* antar-*Autonomous System* dan EIGRP sebagai protokol *routing* internal. Kondisi *baseline* menunjukkan bahwa hubungan *neighbor* berhasil terbentuk, *routing table* menggunakan rute valid, konektivitas antar-*client* berjalan normal, dan nilai *packet loss* pada topologi BGP maupun EIGRP sebesar 0%. Hal ini menunjukkan bahwa sebelum *route injection* diterapkan, kedua topologi berada dalam kondisi stabil.
2. Skenario *route injection* berhasil memengaruhi proses pemilihan jalur pada BGP dan EIGRP. Pada BGP, R4-ATTACKER mengiklankan *prefix host /32* tidak sah menuju PC1, PC2, dan PC3 melalui sesi *neighbor* BGP. Pada EIGRP, R4-ATTACKER memasukkan rute statis menuju Null0, kemudian rute tersebut di-*redistribute* ke dalam EIGRP sehingga muncul sebagai rute eksternal dengan kode D EX. Karena *prefix /32* lebih spesifik dibandingkan rute valid */24*, *router* memilih rute tidak sah tersebut berdasarkan prinsip *longest prefix match*. Kondisi ini menyebabkan perubahan *next-hop* menuju R4-ATTACKER dan mengganggu jalur komunikasi yang menuju atau melibatkan target serangan.
3. Dampak *route injection* terlihat pada perubahan kualitas layanan jaringan. Pada kondisi serangan, nilai *packet loss* rata-rata meningkat menjadi 66,67% pada BGP dan EIGRP. Nilai *throughput* BGP menurun dari 1,440 Kbps pada kondisi *baseline* menjadi 0,957 Kbps saat *route injection*, sedangkan EIGRP menurun dari 1,498 Kbps menjadi 0,967 Kbps. Hasil ini menunjukkan bahwa *route*



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

injection tidak hanya memengaruhi informasi *routing* pada *control plane*, tetapi juga berdampak terhadap komunikasi pada *data plane*, terutama pada alur yang menuju atau melibatkan target serangan.

4. Penerapan mitigasi *basic filtering* menggunakan *prefix-list* berhasil menolak rute tidak sah dari R4-ATTACKER pada BGP dan EIGRP. Pada BGP, *prefix-list* diterapkan secara *inbound* pada *neighbor* R4-ATTACKER. Pada EIGRP, *prefix-list* diterapkan melalui *distribute-list* pada antarmuka jaringan transit. Setelah mitigasi diterapkan, rute tidak sah tidak lagi digunakan, konektivitas antar-*client* kembali normal, nilai *packet loss* kembali menjadi 0%, dan *throughput* meningkat menjadi 1,477 Kbps pada BGP serta 1,468 Kbps pada EIGRP. Dengan demikian, *basic filtering* menggunakan *prefix-list* terbukti efektif dalam membatasi dampak *route injection* pada *control plane routing* BGP maupun EIGRP.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran untuk pengembangan penelitian selanjutnya, yaitu sebagai berikut:

1. Penelitian selanjutnya dapat menguji variasi serangan *routing* lain, seperti *route leak*, manipulasi AS path, atau serangan terhadap pembentukan *neighbor*.
2. Mitigasi dapat dikembangkan dengan membandingkan *prefix-list* dengan metode lain, seperti RPKI/ROV, BGPsec, autentikasi EIGRP, atau kebijakan *filtering* tambahan.
3. Pengujian selanjutnya dapat menggunakan topologi yang lebih kompleks, jumlah router dan *client* yang lebih banyak, serta trafik selain ICMP, seperti TCP atau UDP.
4. Pada jaringan nyata, administrator disarankan menerapkan kebijakan *filtering* dan validasi *prefix* agar rute tidak sah tidak mudah masuk ke proses *routing*.



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

DAFTAR PUSTAKA

- Antoni Musril, H., Sri Artika, F., Derta, S., Darmawati, G., & Okra, R. (2021). Quality of Service EIGRP *Routing* Protocol on Campus Area Network. *Journal of Physics: Conference Series*, 1779(1). <https://doi.org/10.1088/1742-6596/1779/1/012005>
- Auliya, K. X., & Dian W. Chandra. (2025). Analisis hubungan antara kualitas layanan jaringan dan pengalaman pengguna pada layanan video streaming youtube. *IT-Explore: Jurnal Penerapan Teknologi Informasi Dan Komunikasi*, 4(3), 272–281. <https://doi.org/10.24246/itexplore.v4i3.2025.pp272-281>
- Eko Kurniawanto, S. P. (2021). Implementasi *Routing* Protokol Border Gateway Protocol (Bgp) Pada Router Mikrotik Rb 2011 Di Kominfo Kabupaten Solok Selatan. *Jurnal Teknoif Teknik Informatika Institut Teknologi Padang*, 9(2), 97–103. <https://doi.org/10.21063/jtif.2021.v9.2.97-103>
- Global, P. (2023). *Everything You Need to Know About Distribute and Prefix Lists*. https://info.pivitglobal.com/resources/distribute-and-prefix-lists?utm_source
- Kabir, M. H., Kabir, M. A., Islam, M. S., Mortuza, M. G., & Mohiuddin, M. (2021). Performance Analysis of Mesh Based Enterprise Network Using RIP, EIGRP and OSPF *Routing* Protocols. *Engineering Proceedings*, 10(1). <https://doi.org/10.3390/ecsa-8-11285>
- Labs, Q. (2025). *Understanding BGP hijacking: risks, real-world examples, and how to protect your network in 2025*. <https://qrator.net/blog/details/why-bgp-hijacking-still-threatens-global-networks/>
- McDaniel, T., Smith, J. M., & Schuchard, M. (2021). Flexsealing BGP Against Route Leaks: Peerlock Active Measurement and Analysis. *28th Annual Network and Distributed System Security Symposium, NDSS 2021*, 1–16. <https://doi.org/10.14722/ndss.2021.23080>
- Nisa, I. S. N., Rahmat Miyarno Saputro, Tegar Fatwa Nugroho, & Alfirna Rizqi Lahitani. (2024). Analisis Quality of Service (QoS) Menggunakan Standar



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

Parameter Tiphon pada Jaringan Internet Berbasis Wi-Fi Kampus 1 Unjaya. *Teknomatika: Jurnal Informatika Dan Komputer*, 17(1), 1–9. <https://doi.org/10.30989/teknomatika.v17i1.1307>

Nugroho, H. A. S. A., Sonhaji, & Prasetyo, A. C. (2024). Evaluasi Kinerja Jaringan WiFi Mahasiswa: Analisis Throughput, Delay, Jitter, dan Packet loss. *Jurnal BATIRSI*, 8(1), 23–27.

OECD. (2022). *Routing security: BGP incidents, mitigation techniques and policy actions*. (330). [https://www.oecd-ilibrary.org/science-and-technology/routing-security_40be69c8-en%0Afiles/11282/OECD - 2022 - Routing security BGP incidents, mitigation techni.pdf](https://www.oecd-ilibrary.org/science-and-technology/routing-security_40be69c8-en%0Afiles/11282/OECD-2022-Routing-security-BGP-incidents-mitigation-techni.pdf)

Pranaya, V. B., & Wellem, T. (2021). Implementasi BGP dan Resource Public Key Infrastructure menggunakan BIRD untuk Keamanan Routing. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, 5(6), 1161–1170. <https://doi.org/10.29207/resti.v5i6.3631>

Saad, M., Anwar, A., Ahmad, A., Alasmarty, H., Yuksel, M., & Mohaisen, D. (2022). RouteChain: Towards Blockchain-based secure and efficient BGP routing. *Computer Networks*, 217(September). <https://doi.org/10.1016/j.comnet.2022.109362>

Sahal Nurhidayah, M., Pranindito, D., & Dyah Wahyuningrum, R. (2022). Analisis dan Simulasi Routing Border Gateway Protocol (BGP) Antar Autonomous System menggunakan Free Range Routing (FRR). *Jurnal Litek : Jurnal Listrik Telekomunikasi Elektronika*, 19(2), 48–56. <https://doi.org/10.30811/litek.v19i2.11>

Scott, B. A., Johnstone, M. N., & Szewczyk, P. (2024). A Survey of Advanced Border Gateway Protocol Attack Detection Techniques. *Sensors*, 24(19), 6414. <https://doi.org/10.3390/s24196414>

Sermpezis, P., Kotronis, V., Arakadakis, K., & Vakali, A. (2021). Estimating the Impact of BGP Prefix Hijacking. *2021 IFIP Networking Conference, IFIP Networking* 2021. <https://doi.org/10.23919/IFIPNetworking52078.2021.9472813>



© 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

- Shapira, T., & Shavitt, Y. (2022). AP2Vec: An Unsupervised Approach for BGP Hijacking Detection. *IEEE Transactions on Network and Service Management*, 19(3), 2255–2268. <https://doi.org/10.1109/TNSM.2022.3166450>
- Siddiqui, A. (2022). *BGP Security in 2021 - MANRS*. https://manrs.org/2022/02/bgp-security-in-2021/?utm_source
- Vidananda Agastya, I. B., Wiharta, D. M., & Putra Sastra, N. (2021). Perancangan Jaringan Dengan Protokol Eigrp Di Universitas Udayana. *Jurnal SPEKTRUM*, 8(2), 61. <https://doi.org/10.24843/spektrum.2021.v08.i02.p8>



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

DAFTAR RIWAYAT HIDUP



Sahrul Apriandi lahir di Banyumas pada tanggal 27 April 2004. Penulis menyelesaikan pendidikan dasar di SDN Sepanjang Jaya 1 Kota Bekasi pada tahun 2016. Setelah itu, penulis melanjutkan pendidikan ke SMPN 16 Kota Bekasi dan lulus pada tahun 2019.

Pada tahun 2022, penulis menyelesaikan pendidikan menengah kejuruan di SMKN 3 Kota Bekasi. Setelah menyelesaikan pendidikan menengah kejuruan, penulis melanjutkan pendidikan tinggi di Politeknik Negeri Jakarta, Jurusan Teknik Informatika dan Komputer, Program Studi Teknik Multimedia dan Jaringan.

**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

LAMPIRAN

Bukti Konfigurasi Route Injection melalui Redistribusi Static Route pada EIGRP

```
R4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#ip route 192.168.17.2 255.255.255.255 Null0
R4(config)#
R4(config)#router eigrp 100
R4(config-router)# redistribute static metric 10000 100 255 1 1500
R4(config-router)#end
R4#
```

Konfigurasi Route Injection melalui Pengiklanan Prefix BGP pada R4-
ATTACKER

```
R4-ATTACKER#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4-ATTACKER(config)#ip route 192.168.17.2 255.255.255.255 Null0
R4-ATTACKER(config)#
R4-ATTACKER(config)#router bgp 6440
R4-ATTACKER(config-router)# network 192.168.17.2 mask 255.255.255.255
R4-ATTACKER(config-router)#
R4-ATTACKER(config-router)#end
R4-ATTACKER#clear ip bgp * soft
```

Hasil Verifikasi Rute Tidak Sah EIGRP Saat *Route Injection*

```
R1-KOMINFO#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

    192.168.17.0/24 is variably subnetted, 2 subnets, 2 masks
D       192.168.17.0/24 [90/30720] via 172.16.1.20, 00:26:07, FastEthernet0/0
D EX    192.168.17.2/32
        [170/284160] via 172.16.1.40, 00:00:56, FastEthernet0/0
D       192.168.18.0/24 [90/30720] via 172.16.1.30, 00:26:07, FastEthernet0/0
```

Hasil Verifikasi *Routing EIGRP Setelah Mitigasi Basic Filtering*



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

```
R1-KOMINFO#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

D    192.168.17.0/24 [90/30720] via 172.16.1.20, 00:29:16, FastEthernet0/0
D    192.168.18.0/24 [90/30720] via 172.16.1.30, 00:29:16, FastEthernet0/0
```

Rute Tidak Sah 192.168.17.2/32 pada *Routing Table* R1-KOMINFO

```
R1-KOMINFO#show ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

    192.168.17.0/24 is variably subnetted, 2 subnets, 2 masks
B       192.168.17.0/24 [20/0] via 172.16.1.20, 00:03:40
B       192.168.17.2/32 [20/0] via 172.16.1.40, 00:00:31
B       192.168.18.0/24 [20/0] via 172.16.1.30, 00:03:40
```

Status Neighbor BGP dan Penerimaan Prefix dari R4-ATTACKER saat Route

Injection

```
R1-KOMINFO#show ip bgp summary
BGP router identifier 192.168.16.1, local AS number 6410
BGP table version is 5, main routing table version 5
4 network entries using 576 bytes of memory
4 path entries using 320 bytes of memory
4/4 BGP path/bestpath attribute entries using 544 bytes of memory
3 BGP AS-PATH entries using 72 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1512 total bytes of memory
BGP activity 4/0 prefixes, 4/0 paths, scan interval 60 secs

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
172.16.1.20    4      6420     10     11      5    0    0 00:05:34      1
172.16.1.30    4      6430     10     11      5    0    0 00:05:33      1
172.16.1.40    4      6440     13     18      5    0    0 00:05:35      1
R1-KOMINFO#
```

Verifikasi Prefix-list dan Tabel BGP Setelah Mitigasi pada R1-KOMINFO



© 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

```
R1-KOMINFO#show ip prefix-list FILTER-INVALID-BGP
ip prefix-list FILTER-INVALID-BGP: 2 entries
  seq 5 deny 192.168.17.2/32
  seq 100 permit 0.0.0.0/0 le 32
R1-KOMINFO#show ip bgp
BGP table version is 6, local router ID is 192.168.16.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop        Metric LocPrf Weight Path
*> 192.168.16.0      0.0.0.0          0         32768 i
*> 192.168.17.0      172.16.1.20      0           0 6420 i
*> 192.168.18.0      172.16.1.30      0           0 6430 i
```

Capture ICMP Saat *Route Injection* pada BGP

No.	Time	Source	Destination	Protocol	Length	Info
3	3.333528	192.168.16.2	192.168.17.2	ICMP	98	Echo (ping) request id=0xef4b, seq=1/256, ttl=63 (no response found!)
4	3.348729	172.16.1.30	192.168.16.2	ICMP	70	Destination unreachable (Host unreachable)
5	4.399099	192.168.16.2	192.168.17.2	ICMP	98	Echo (ping) request id=0xf04b, seq=2/512, ttl=63 (no response found!)
6	4.414310	172.16.1.30	192.168.16.2	ICMP	70	Destination unreachable (Host unreachable)
7	5.466356	192.168.16.2	192.168.17.2	ICMP	98	Echo (ping) request id=0xf14b, seq=3/768, ttl=63 (no response found!)
8	5.481888	172.16.1.30	192.168.16.2	ICMP	70	Destination unreachable (Host unreachable)
11	6.536318	192.168.16.2	192.168.17.2	ICMP	98	Echo (ping) request id=0xf24b, seq=4/1024, ttl=63 (no response found!)
12	6.552054	172.16.1.30	192.168.16.2	ICMP	70	Destination unreachable (Host unreachable)
13	7.613546	192.168.16.2	192.168.17.2	ICMP	98	Echo (ping) request id=0xf34b, seq=5/1280, ttl=63 (no response found!)
14	7.629228	172.16.1.30	192.168.16.2	ICMP	70	Destination unreachable (Host unreachable)

Capture ICMP Setelah Mitigasi pada EIGRP

No.	Time	Source	Destination	Protocol	Length	Info
6	16.850927	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request id=0x1c40, seq=1/256, ttl=63 (reply in 8)
7	18.862717	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request id=0x1e40, seq=2/512, ttl=63 (reply in 9)
8	19.902807	192.168.18.2	192.168.17.2	ICMP	98	Echo (ping) reply id=0x1c40, seq=1/256, ttl=63 (request in 6)
9	19.902807	192.168.18.2	192.168.17.2	ICMP	98	Echo (ping) reply id=0x1e40, seq=2/512, ttl=63 (request in 7)
11	20.876392	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request id=0x2040, seq=3/768, ttl=63 (reply in 12)
12	20.906334	192.168.18.2	192.168.17.2	ICMP	98	Echo (ping) reply id=0x2040, seq=3/768, ttl=63 (request in 11)
13	21.960099	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request id=0x2140, seq=4/1024, ttl=63 (reply in 14)
14	21.989872	192.168.18.2	192.168.17.2	ICMP	98	Echo (ping) reply id=0x2140, seq=4/1024, ttl=63 (request in 13)
15	23.040136	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request id=0x2340, seq=5/1280, ttl=63 (reply in 16)
16	23.069696	192.168.18.2	192.168.17.2	ICMP	98	Echo (ping) reply id=0x2340, seq=5/1280, ttl=63 (request in 15)
17	24.126601	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request id=0x2440, seq=6/1536, ttl=63 (reply in 18)
18	24.157347	192.168.18.2	192.168.17.2	ICMP	98	Echo (ping) reply id=0x2440, seq=6/1536, ttl=63 (request in 17)
20	25.207331	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request id=0x2540, seq=7/1792, ttl=63 (reply in 21)
21	25.238368	192.168.18.2	192.168.17.2	ICMP	98	Echo (ping) reply id=0x2540, seq=7/1792, ttl=63 (request in 20)
23	26.272704	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request id=0x2640, seq=8/2048, ttl=63 (reply in 24)
24	26.302591	192.168.18.2	192.168.17.2	ICMP	98	Echo (ping) reply id=0x2640, seq=8/2048, ttl=63 (request in 23)
25	27.356620	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request id=0x2740, seq=9/2304, ttl=63 (reply in 26)



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

Hasil Pengujian Ping 30 Paket dari PC1 menuju PC3

```
PC1> ping 192.168.18.2 -c 30
84 bytes from 192.168.18.2 icmp_seq=1 ttl=62 time=75.734 ms
84 bytes from 192.168.18.2 icmp_seq=2 ttl=62 time=60.855 ms
84 bytes from 192.168.18.2 icmp_seq=3 ttl=62 time=60.173 ms
84 bytes from 192.168.18.2 icmp_seq=4 ttl=62 time=62.182 ms
84 bytes from 192.168.18.2 icmp_seq=5 ttl=62 time=62.237 ms
84 bytes from 192.168.18.2 icmp_seq=6 ttl=62 time=60.599 ms
84 bytes from 192.168.18.2 icmp_seq=7 ttl=62 time=61.792 ms
84 bytes from 192.168.18.2 icmp_seq=8 ttl=62 time=60.989 ms
84 bytes from 192.168.18.2 icmp_seq=9 ttl=62 time=60.292 ms
84 bytes from 192.168.18.2 icmp_seq=10 ttl=62 time=60.700 ms
84 bytes from 192.168.18.2 icmp_seq=11 ttl=62 time=60.866 ms
84 bytes from 192.168.18.2 icmp_seq=12 ttl=62 time=60.560 ms
84 bytes from 192.168.18.2 icmp_seq=13 ttl=62 time=62.326 ms
84 bytes from 192.168.18.2 icmp_seq=14 ttl=62 time=61.338 ms
84 bytes from 192.168.18.2 icmp_seq=15 ttl=62 time=60.603 ms
84 bytes from 192.168.18.2 icmp_seq=16 ttl=62 time=60.539 ms
84 bytes from 192.168.18.2 icmp_seq=17 ttl=62 time=61.965 ms
84 bytes from 192.168.18.2 icmp_seq=18 ttl=62 time=62.191 ms
84 bytes from 192.168.18.2 icmp_seq=19 ttl=62 time=61.950 ms
84 bytes from 192.168.18.2 icmp_seq=20 ttl=62 time=60.574 ms
84 bytes from 192.168.18.2 icmp_seq=21 ttl=62 time=59.555 ms
84 bytes from 192.168.18.2 icmp_seq=22 ttl=62 time=63.033 ms
84 bytes from 192.168.18.2 icmp_seq=23 ttl=62 time=62.534 ms
84 bytes from 192.168.18.2 icmp_seq=24 ttl=62 time=61.174 ms
84 bytes from 192.168.18.2 icmp_seq=25 ttl=62 time=60.295 ms
84 bytes from 192.168.18.2 icmp_seq=26 ttl=62 time=61.760 ms
84 bytes from 192.168.18.2 icmp_seq=27 ttl=62 time=59.746 ms
84 bytes from 192.168.18.2 icmp_seq=28 ttl=62 time=61.232 ms
84 bytes from 192.168.18.2 icmp_seq=29 ttl=62 time=61.792 ms
84 bytes from 192.168.18.2 icmp_seq=30 ttl=62 time=62.192 ms
```

Hasil Pengujian Ping 30 Paket dari PC2 menuju PC3

```
PC2> ping 192.168.18.2 -c 30
192.168.18.2 icmp_seq=1 timeout
192.168.18.2 icmp_seq=2 timeout
84 bytes from 192.168.18.2 icmp_seq=3 ttl=62 time=61.373 ms
84 bytes from 192.168.18.2 icmp_seq=4 ttl=62 time=60.352 ms
84 bytes from 192.168.18.2 icmp_seq=5 ttl=62 time=60.278 ms
84 bytes from 192.168.18.2 icmp_seq=6 ttl=62 time=61.195 ms
84 bytes from 192.168.18.2 icmp_seq=7 ttl=62 time=62.133 ms
84 bytes from 192.168.18.2 icmp_seq=8 ttl=62 time=60.521 ms
84 bytes from 192.168.18.2 icmp_seq=9 ttl=62 time=60.307 ms
84 bytes from 192.168.18.2 icmp_seq=10 ttl=62 time=62.680 ms
84 bytes from 192.168.18.2 icmp_seq=11 ttl=62 time=60.829 ms
84 bytes from 192.168.18.2 icmp_seq=12 ttl=62 time=63.102 ms
84 bytes from 192.168.18.2 icmp_seq=13 ttl=62 time=60.958 ms
84 bytes from 192.168.18.2 icmp_seq=14 ttl=62 time=57.655 ms
84 bytes from 192.168.18.2 icmp_seq=15 ttl=62 time=62.169 ms
84 bytes from 192.168.18.2 icmp_seq=16 ttl=62 time=61.014 ms
84 bytes from 192.168.18.2 icmp_seq=17 ttl=62 time=59.982 ms
84 bytes from 192.168.18.2 icmp_seq=18 ttl=62 time=61.288 ms
84 bytes from 192.168.18.2 icmp_seq=19 ttl=62 time=61.382 ms
84 bytes from 192.168.18.2 icmp_seq=20 ttl=62 time=59.996 ms
84 bytes from 192.168.18.2 icmp_seq=21 ttl=62 time=61.597 ms
84 bytes from 192.168.18.2 icmp_seq=22 ttl=62 time=61.396 ms
84 bytes from 192.168.18.2 icmp_seq=23 ttl=62 time=62.370 ms
84 bytes from 192.168.18.2 icmp_seq=24 ttl=62 time=62.043 ms
84 bytes from 192.168.18.2 icmp_seq=25 ttl=62 time=60.039 ms
84 bytes from 192.168.18.2 icmp_seq=26 ttl=62 time=61.665 ms
84 bytes from 192.168.18.2 icmp_seq=27 ttl=62 time=61.929 ms
84 bytes from 192.168.18.2 icmp_seq=28 ttl=62 time=60.937 ms
84 bytes from 192.168.18.2 icmp_seq=29 ttl=62 time=61.808 ms
84 bytes from 192.168.18.2 icmp_seq=30 ttl=62 time=61.800 ms
```



Hasil Verifikasi Rute BGP pada Router R1-KOMINFO

```
R1-KOMINFO#show ip route 192.168.18.2
Routing entry for 192.168.18.0/24
  Known via "bgp 6410", distance 20, metric 0
  Tag 6430, type external
  Last update from 172.16.1.30 02:06:39 ago
  Routing Descriptor Blocks:
    * 172.16.1.30, from 172.16.1.30, 02:06:39 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 6430
      MPLS label: none
```

Hasil Pengujian Ping 30 Paket dari PC2 Menuju Jaringan 192.168.16.2

```
PC2> ping 192.168.16.2 -c 30
84 bytes from 192.168.16.2 icmp_seq=1 ttl=62 time=61.207 ms
84 bytes from 192.168.16.2 icmp_seq=2 ttl=62 time=62.888 ms
84 bytes from 192.168.16.2 icmp_seq=3 ttl=62 time=61.519 ms
84 bytes from 192.168.16.2 icmp_seq=4 ttl=62 time=60.462 ms
84 bytes from 192.168.16.2 icmp_seq=5 ttl=62 time=61.166 ms
84 bytes from 192.168.16.2 icmp_seq=6 ttl=62 time=60.823 ms
84 bytes from 192.168.16.2 icmp_seq=7 ttl=62 time=60.224 ms
84 bytes from 192.168.16.2 icmp_seq=8 ttl=62 time=67.869 ms
84 bytes from 192.168.16.2 icmp_seq=9 ttl=62 time=61.070 ms
84 bytes from 192.168.16.2 icmp_seq=10 ttl=62 time=61.156 ms
84 bytes from 192.168.16.2 icmp_seq=11 ttl=62 time=62.458 ms
84 bytes from 192.168.16.2 icmp_seq=12 ttl=62 time=72.276 ms
84 bytes from 192.168.16.2 icmp_seq=13 ttl=62 time=62.381 ms
84 bytes from 192.168.16.2 icmp_seq=14 ttl=62 time=61.355 ms
84 bytes from 192.168.16.2 icmp_seq=15 ttl=62 time=62.558 ms
84 bytes from 192.168.16.2 icmp_seq=16 ttl=62 time=61.420 ms
84 bytes from 192.168.16.2 icmp_seq=17 ttl=62 time=62.121 ms
84 bytes from 192.168.16.2 icmp_seq=18 ttl=62 time=62.589 ms
84 bytes from 192.168.16.2 icmp_seq=19 ttl=62 time=61.370 ms
84 bytes from 192.168.16.2 icmp_seq=20 ttl=62 time=60.964 ms
84 bytes from 192.168.16.2 icmp_seq=21 ttl=62 time=60.417 ms
84 bytes from 192.168.16.2 icmp_seq=22 ttl=62 time=61.394 ms
84 bytes from 192.168.16.2 icmp_seq=23 ttl=62 time=61.289 ms
84 bytes from 192.168.16.2 icmp_seq=24 ttl=62 time=63.642 ms
84 bytes from 192.168.16.2 icmp_seq=25 ttl=62 time=62.905 ms
84 bytes from 192.168.16.2 icmp_seq=26 ttl=62 time=74.522 ms
84 bytes from 192.168.16.2 icmp_seq=27 ttl=62 time=48.258 ms
84 bytes from 192.168.16.2 icmp_seq=28 ttl=62 time=56.000 ms
84 bytes from 192.168.16.2 icmp_seq=29 ttl=62 time=59.326 ms
84 bytes from 192.168.16.2 icmp_seq=30 ttl=62 time=61.835 ms
```

Capture Paket ICMP Selama Pengujian Konektivitas

No.	Time	Source	Destination	Protocol	Length	Info
23.738306	192.168.16.2	192.168.18.2	ICMP	98	Echo (ping) request	id=0xc321, seq=1/256, ttl=63 (reply in 3)
33.769362	192.168.18.2	192.168.16.2	ICMP	98	Echo (ping) reply	id=0xc321, seq=1/256, ttl=63 (request in 2)
44.827182	192.168.16.2	192.168.18.2	ICMP	98	Echo (ping) request	id=0xc521, seq=2/512, ttl=63 (request in 5)
54.856946	192.168.18.2	192.168.16.2	ICMP	98	Echo (ping) reply	id=0xc521, seq=2/512, ttl=63 (request in 4)
65.912484	192.168.16.2	192.168.18.2	ICMP	98	Echo (ping) request	id=0xc621, seq=3/768, ttl=63 (reply in 7)
75.942565	192.168.18.2	192.168.16.2	ICMP	98	Echo (ping) reply	id=0xc621, seq=3/768, ttl=63 (request in 6)
86.990648	192.168.16.2	192.168.18.2	ICMP	98	Echo (ping) request	id=0xc721, seq=4/1024, ttl=63 (reply in 9)
97.021202	192.168.18.2	192.168.16.2	ICMP	98	Echo (ping) reply	id=0xc721, seq=4/1024, ttl=63 (request in 8)
108.077892	192.168.16.2	192.168.18.2	ICMP	98	Echo (ping) request	id=0xc821, seq=5/1280, ttl=63 (reply in 11)
118.109430	192.168.18.2	192.168.16.2	ICMP	98	Echo (ping) reply	id=0xc821, seq=5/1280, ttl=63 (request in 10)
129.160396	192.168.16.2	192.168.18.2	ICMP	98	Echo (ping) request	id=0xc921, seq=6/1536, ttl=63 (reply in 13)



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

Hasil Verifikasi Rute BGP pada Router R1-KOMINFO

```
R1-KOMINFO#show ip bgp 192.168.18.2
BGP routing table entry for 192.168.18.2/32, version 17
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
    1
  Refresh Epoch 14
  6440
    172.16.1.40 from 172.16.1.40 (4.4.4.4)
      Origin IGP, metric 0, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
R1-KOMINFO#show ip route 192.168.18.2
Routing entry for 192.168.18.2/32
  Known via "bgp 6410", distance 20, metric 0
  Tag 6440, type external
  Last update from 172.16.1.40 00:42:49 ago
  Routing Descriptor Blocks:
    * 172.16.1.40, from 172.16.1.40, 00:42:49 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 6440
      MPLS label: none
```

Hasil Konfigurasi *Route Injection* pada Router Attacker

```
R4-ATTACKER#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4-ATTACKER(config)#ip route 192.168.18.2 255.255.255.255 Null0
R4-ATTACKER(config)#
R4-ATTACKER(config)#router bgp 6440
R4-ATTACKER(config-router)# network 192.168.18.2 mask 255.255.255.255
R4-ATTACKER(config-router)#end
```

Hasil Konfigurasi *Basic Filtering* pada Router R1-KOMINFO

```
R1-KOMINFO#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1-KOMINFO(config)#$ist FILTER-INVALID-BGP seq 5 deny 192.168.18.2/32
%Insertion failed - seq # exists with different policy: 5
R1-KOMINFO(config)#$ist FILTER-INVALID-BGP seq 10 permit 0.0.0.0/0 le 32
R1-KOMINFO(config)#
R1-KOMINFO(config)#router bgp 6410
R1-KOMINFO(config-router)#$72.16.1.40 prefix-list FILTER-INVALID-BGP in
R1-KOMINFO(config-router)#end
```

Hasil Pengujian *Traceroute* Menuju Jaringan 192.168.18.2

```
PC1> trace 192.168.18.2
Trace to 192.168.18.2, 8 hops max, press Ctrl+C to stop
 1  192.168.16.1    15.658 ms  14.193 ms  15.079 ms
 2  172.16.1.40    45.362 ms  45.876 ms  45.781 ms
 3  *172.16.1.40    45.859 ms  (ICMP type:3, code:1, Destination host unreachable)
```

Capture Paket ICMP Setelah Mitigasi pada EIGRP

No.	Time	Source	Destination	Protocol	Length	Info
83	31.458956	192.168.18.2	192.168.17.2	ICMP	98	Echo (ping) reply id=0x29ee, seq=25/6400, ttl=63 (request in 8)
84	32.512750	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request id=0x2aee, seq=26/6656, ttl=63 (reply in 85)
85	32.542511	192.168.18.2	192.168.17.2	ICMP	98	Echo (ping) reply id=0x2aee, seq=26/6656, ttl=63 (request in 8)
88	33.594640	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request id=0x2bee, seq=27/6912, ttl=63 (reply in 89)
89	33.625418	192.168.18.2	192.168.17.2	ICMP	98	Echo (ping) reply id=0x2bee, seq=27/6912, ttl=63 (request in 8)
93	34.677765	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request id=0x2cee, seq=28/7168, ttl=63 (reply in 94)
94	34.707670	192.168.18.2	192.168.17.2	ICMP	98	Echo (ping) reply id=0x2cee, seq=28/7168, ttl=63 (request in 9)
95	35.760221	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request id=0x2dee, seq=29/7424, ttl=63 (reply in 96)
96	35.791025	192.168.18.2	192.168.17.2	ICMP	98	Echo (ping) reply id=0x2dee, seq=29/7424, ttl=63 (request in 9)
97	36.849156	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request id=0x2eee, seq=30/7680, ttl=63 (reply in 98)
98	36.880175	192.168.18.2	192.168.17.2	ICMP	98	Echo (ping) reply id=0x2eee, seq=30/7680, ttl=63 (request in 9)



Hasil Verifikasi Tabel *Routing* EIGRP Setelah Mitigasi

```
R1-KOMINFO#show ip route eigrp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

D    192.168.17.0/24 [90/30720] via 172.16.1.20, 03:26:02, FastEthernet0/0
    192.168.18.0/24 is variably subnetted, 2 subnets, 2 masks
D    192.168.18.0/24 [90/30720] via 172.16.1.30, 03:26:02, FastEthernet0/0
D EX 192.168.18.2/32
    [170/284160] via 172.16.1.40, 00:00:02, FastEthernet0/0
```

Hasil Pengujian *Ping* 30 Paket dari PC1 Menuju Jaringan 192.168.18.2

```
PC1> ping 192.168.18.2 -c 30
84 bytes from 192.168.18.2 icmp_seq=1 ttl=62 time=61.191 ms
84 bytes from 192.168.18.2 icmp_seq=2 ttl=62 time=60.042 ms
84 bytes from 192.168.18.2 icmp_seq=3 ttl=62 time=61.830 ms
84 bytes from 192.168.18.2 icmp_seq=4 ttl=62 time=60.109 ms
84 bytes from 192.168.18.2 icmp_seq=5 ttl=62 time=62.294 ms
84 bytes from 192.168.18.2 icmp_seq=6 ttl=62 time=61.270 ms
84 bytes from 192.168.18.2 icmp_seq=7 ttl=62 time=61.368 ms
84 bytes from 192.168.18.2 icmp_seq=8 ttl=62 time=61.380 ms
84 bytes from 192.168.18.2 icmp_seq=9 ttl=62 time=61.125 ms
84 bytes from 192.168.18.2 icmp_seq=10 ttl=62 time=62.149 ms
84 bytes from 192.168.18.2 icmp_seq=11 ttl=62 time=61.125 ms
84 bytes from 192.168.18.2 icmp_seq=12 ttl=62 time=60.874 ms
84 bytes from 192.168.18.2 icmp_seq=13 ttl=62 time=61.476 ms
84 bytes from 192.168.18.2 icmp_seq=14 ttl=62 time=61.751 ms
84 bytes from 192.168.18.2 icmp_seq=15 ttl=62 time=61.592 ms
84 bytes from 192.168.18.2 icmp_seq=16 ttl=62 time=62.227 ms
84 bytes from 192.168.18.2 icmp_seq=17 ttl=62 time=61.176 ms
84 bytes from 192.168.18.2 icmp_seq=18 ttl=62 time=61.692 ms
84 bytes from 192.168.18.2 icmp_seq=19 ttl=62 time=60.526 ms
84 bytes from 192.168.18.2 icmp_seq=20 ttl=62 time=62.179 ms
84 bytes from 192.168.18.2 icmp_seq=21 ttl=62 time=61.552 ms
84 bytes from 192.168.18.2 icmp_seq=22 ttl=62 time=61.679 ms
84 bytes from 192.168.18.2 icmp_seq=23 ttl=62 time=60.613 ms
84 bytes from 192.168.18.2 icmp_seq=24 ttl=62 time=63.482 ms
84 bytes from 192.168.18.2 icmp_seq=25 ttl=62 time=54.771 ms
84 bytes from 192.168.18.2 icmp_seq=26 ttl=62 time=64.642 ms
84 bytes from 192.168.18.2 icmp_seq=27 ttl=62 time=60.830 ms
84 bytes from 192.168.18.2 icmp_seq=28 ttl=62 time=60.187 ms
84 bytes from 192.168.18.2 icmp_seq=29 ttl=62 time=62.232 ms
84 bytes from 192.168.18.2 icmp_seq=30 ttl=62 time=61.278 ms
```

Capture Paket ICMP Sebelum Mitigasi pada EIGRP

No.	Time	Source	Destination	Protocol	Length	Info
75.013734	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request	id=0x59e9, seq=1/256, ttl=63 (no response fo
85.028658	192.16.1.40	192.168.17.2	ICMP	70	Destination unreachable (Host unreachable)	
96.030224	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request	id=0x5a0, seq=2/512, ttl=63 (no response fo
106.094733	192.16.1.40	192.168.17.2	ICMP	70	Destination unreachable (Host unreachable)	
137.148027	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request	id=0x5be9, seq=3/768, ttl=63 (no response fo
147.164584	192.16.1.40	192.168.17.2	ICMP	70	Destination unreachable (Host unreachable)	
168.218579	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request	id=0x5ce9, seq=4/1024, ttl=63 (no response f
178.233705	192.16.1.40	192.168.17.2	ICMP	70	Destination unreachable (Host unreachable)	
219.201616	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request	id=0x5de9, seq=5/1280, ttl=63 (no response f
229.296896	192.16.1.40	192.168.17.2	ICMP	70	Destination unreachable (Host unreachable)	
2410.350070	192.168.17.2	192.168.18.2	ICMP	98	Echo (ping) request	id=0x5ee9, seq=6/1536, ttl=63 (no response f



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

Hasil Pengujian *Ping* 30 Paket dari PC2 Menuju Jaringan 192.168.18.2 Setelah Mitigasi

```
PC2> ping 192.168.18.2 -c 30
84 bytes from 192.168.18.2 icmp_seq=1 ttl=62 time=62.769 ms
84 bytes from 192.168.18.2 icmp_seq=2 ttl=62 time=61.696 ms
84 bytes from 192.168.18.2 icmp_seq=3 ttl=62 time=62.380 ms
84 bytes from 192.168.18.2 icmp_seq=4 ttl=62 time=60.840 ms
84 bytes from 192.168.18.2 icmp_seq=5 ttl=62 time=60.712 ms
84 bytes from 192.168.18.2 icmp_seq=6 ttl=62 time=61.440 ms
84 bytes from 192.168.18.2 icmp_seq=7 ttl=62 time=59.281 ms
84 bytes from 192.168.18.2 icmp_seq=8 ttl=62 time=62.255 ms
84 bytes from 192.168.18.2 icmp_seq=9 ttl=62 time=61.093 ms
84 bytes from 192.168.18.2 icmp_seq=10 ttl=62 time=60.194 ms
84 bytes from 192.168.18.2 icmp_seq=11 ttl=62 time=61.952 ms
84 bytes from 192.168.18.2 icmp_seq=12 ttl=62 time=60.662 ms
84 bytes from 192.168.18.2 icmp_seq=13 ttl=62 time=61.273 ms
84 bytes from 192.168.18.2 icmp_seq=14 ttl=62 time=61.718 ms
84 bytes from 192.168.18.2 icmp_seq=15 ttl=62 time=61.324 ms
84 bytes from 192.168.18.2 icmp_seq=16 ttl=62 time=60.438 ms
84 bytes from 192.168.18.2 icmp_seq=17 ttl=62 time=60.729 ms
84 bytes from 192.168.18.2 icmp_seq=18 ttl=62 time=61.439 ms
84 bytes from 192.168.18.2 icmp_seq=19 ttl=62 time=62.117 ms
84 bytes from 192.168.18.2 icmp_seq=20 ttl=62 time=60.503 ms
84 bytes from 192.168.18.2 icmp_seq=21 ttl=62 time=61.276 ms
84 bytes from 192.168.18.2 icmp_seq=22 ttl=62 time=61.577 ms
84 bytes from 192.168.18.2 icmp_seq=23 ttl=62 time=61.830 ms
84 bytes from 192.168.18.2 icmp_seq=24 ttl=62 time=62.132 ms
84 bytes from 192.168.18.2 icmp_seq=25 ttl=62 time=61.606 ms
84 bytes from 192.168.18.2 icmp_seq=26 ttl=62 time=61.349 ms
84 bytes from 192.168.18.2 icmp_seq=27 ttl=62 time=61.330 ms
84 bytes from 192.168.18.2 icmp_seq=28 ttl=62 time=62.201 ms
84 bytes from 192.168.18.2 icmp_seq=29 ttl=62 time=61.469 ms
84 bytes from 192.168.18.2 icmp_seq=30 ttl=62 time=61.895 ms
```

Hasil Pengujian *Ping* 30 Paket dari PC1 Menuju Jaringan 192.168.18.2 Setelah Mitigasi

```
PC1> ping 192.168.18.2 -c 30
84 bytes from 192.168.18.2 icmp_seq=1 ttl=62 time=60.562 ms
84 bytes from 192.168.18.2 icmp_seq=2 ttl=62 time=60.404 ms
84 bytes from 192.168.18.2 icmp_seq=3 ttl=62 time=61.276 ms
84 bytes from 192.168.18.2 icmp_seq=4 ttl=62 time=61.205 ms
84 bytes from 192.168.18.2 icmp_seq=5 ttl=62 time=60.996 ms
84 bytes from 192.168.18.2 icmp_seq=6 ttl=62 time=60.356 ms
84 bytes from 192.168.18.2 icmp_seq=7 ttl=62 time=61.003 ms
84 bytes from 192.168.18.2 icmp_seq=8 ttl=62 time=61.225 ms
84 bytes from 192.168.18.2 icmp_seq=9 ttl=62 time=61.628 ms
84 bytes from 192.168.18.2 icmp_seq=10 ttl=62 time=61.978 ms
84 bytes from 192.168.18.2 icmp_seq=11 ttl=62 time=59.926 ms
84 bytes from 192.168.18.2 icmp_seq=12 ttl=62 time=62.356 ms
84 bytes from 192.168.18.2 icmp_seq=13 ttl=62 time=61.809 ms
84 bytes from 192.168.18.2 icmp_seq=14 ttl=62 time=60.542 ms
84 bytes from 192.168.18.2 icmp_seq=15 ttl=62 time=60.810 ms
84 bytes from 192.168.18.2 icmp_seq=16 ttl=62 time=60.273 ms
84 bytes from 192.168.18.2 icmp_seq=17 ttl=62 time=61.519 ms
84 bytes from 192.168.18.2 icmp_seq=18 ttl=62 time=61.302 ms
84 bytes from 192.168.18.2 icmp_seq=19 ttl=62 time=61.065 ms
84 bytes from 192.168.18.2 icmp_seq=20 ttl=62 time=60.864 ms
84 bytes from 192.168.18.2 icmp_seq=21 ttl=62 time=60.516 ms
84 bytes from 192.168.18.2 icmp_seq=22 ttl=62 time=60.658 ms
84 bytes from 192.168.18.2 icmp_seq=23 ttl=62 time=60.018 ms
84 bytes from 192.168.18.2 icmp_seq=24 ttl=62 time=60.474 ms
84 bytes from 192.168.18.2 icmp_seq=25 ttl=62 time=63.599 ms
84 bytes from 192.168.18.2 icmp_seq=26 ttl=62 time=61.614 ms
84 bytes from 192.168.18.2 icmp_seq=27 ttl=62 time=61.257 ms
84 bytes from 192.168.18.2 icmp_seq=28 ttl=62 time=61.947 ms
84 bytes from 192.168.18.2 icmp_seq=29 ttl=62 time=60.982 ms
84 bytes from 192.168.18.2 icmp_seq=30 ttl=62 time=61.074 ms
```