



**ANALISIS KOMPARATIF NGFW FORTIGATE DAN PALO  
ALTO TERHADAP SERANGAN DOS DAN FITUR  
APPLICATION CONTROL-SSL INSPECTION**

**TUGAS AKHIR  
SKRIPSI**



**UNIVERSITAS  
MERCU BUANA**

**RIDWAN  
41522110079**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS MERCU BUANA  
JAKARTA  
2026**



**ANALISIS KOMPARATIF NGFW FORTIGATE DAN PALO  
ALTO TERHADAP SERANGAN DOS DAN FITUR  
APPLICATION CONTROL–SSL INSPECTION**

**TUGAS AKHIR  
SKRIPSI**

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana**

**UNIVERSITAS  
MERCU BUANA**  
**RIDWAN**  
**41522110079**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS MERCU BUANA  
JAKARTA  
2026**

## HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama : Ridwan  
NIM : 41522110079  
Program Studi : Fakultas Ilmu Komputer/ Teknik Informatika

Menyatakan bahwa laporan Tugas Akhir ini adalah hasil karya saya sendiri, tidak mengandung unsur plagiarisme, pelanggaran hak cipta, atau konten ilegal dalam bentuk apapun dan tidak melanggar hukum atau hak pihak manapun.

Apabila di kemudian hari ditemukan pelanggaran terhadap pernyataan ini, saya bersedia menanggung seluruh konsekuensi hukum dan membebaskan Universitas Mercu Buana dari segala bentuk tuntutan hukum dan saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

Demikian pernyataan ini saya buat dengan sebenar-benarnya untuk digunakan sebagaimana mestinya.

Jakarta, 10 Agustus 2026



Ridwan

**PERNYATAAN SIMILARITY CHECK**  
**/SIMILARITY CHECK STATEMENT**

Saya yang bertanda tangan dibawah ini menyatakan, bahwa karya ilmiah yang ditulis oleh  
*/The undersigned, hereby declare that the scientific work written by*

|                              |                      |
|------------------------------|----------------------|
| Nama /Name                   | : Ridwan             |
| NIM /Student ID Number       | : 41522110079        |
| Program Studi /Study Program | : Teknik Informatika |

Dengan Judul Tugas Akhir

*/The title:*

**“ANALISIS KOMPARATIF NGFW FORTIGATE DAN PALO ALTO TERHADAP SERANGAN DOS DAN FITUR APPLICATION CONTROL–SSL INSPECTION”**

telah dilakukan pengecekan *similarity* dengan sistem Turnitin pada tanggal:

*/Similarity checks have been carried out with the Turnitin system on the date:*

31 Juli 2026

dengan nilai persentase sebesar :

*/with a percentage value of:*

18%

dinyatakan memenuhi standar sesuai dengan ketentuan berlaku di **Fakultas Ilmu Komputer** Universitas Mercu Buana. */declared to meet standards in accordance with applicable regulations at the Faculty of Computer Science, Universitas Mercu Buana.*

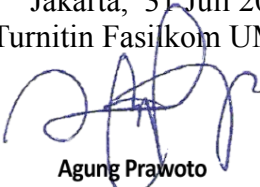
File hasil cek similarity turnitin:

*/Turnitin similarity report file*

[https://drive.google.com/file/d/1yv9tQqym0XrrCZpGuDFc9O3O-VtHt7iP/view?usp=drive\\_link](https://drive.google.com/file/d/1yv9tQqym0XrrCZpGuDFc9O3O-VtHt7iP/view?usp=drive_link)



Jakarta, 31 Juli 2026  
Admin Turnitin Fasikom UMB



Agung Prawoto

**Agung Prawoto, S.Kom., B.Sc**  
NIK : 322970503

## HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama : Ridwan  
NIM : 41522110079  
Fakultas/Program Studi : Fakultas Ilmu Komputer / Teknik Informatika  
Judul Tugas Akhir : Analisis Komparatif NGFW Fortigate dan Palo Alto terhadap Serangan DoS dan Fitur Application Control-SSL Inspection

Telah berhasil dipertahankan pada sidang tanggal 10 Agustus 2026 dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Mercu Buana.

Disahkan oleh:

Pembimbing

Rushendra, Ir., S.Kom, MT  
NIDN/NUPTK: 0408067402

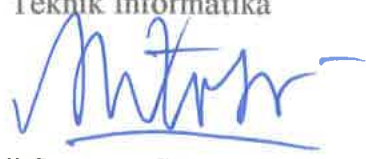
Jakarta, 10 Agustus 2026

Mengetahui,

Dekan Fakultas Ilmu Komputer

Ketua Program Studi  
Teknik Informatika

  
Dr. Bambang Jekonowo, S.Si., MTI  
NIDN/NUPTK: 0320037002

  
Dr. Hadi Santoso, S.Kom., M.Kom  
NIDN/NUPTK: 0225067701

## KATA PENGANTAR

Puji syukur kehadiran Tuhan yang Maha Esa, atas segala rahmat dan ridha-Nya sehingga penulis dapat menyelesaikan proposal penelitian yang merupakan salah satu persyaratan kelulusan Program Studi Strata Satu (S1) pada jurusan Teknik Informatika, Universitas Mercu Buana. Penulis menyadari bahwa proposal penelitian ini masih jauh dari sempurna, karena kesempurnaan sejatinya hanya milik Tuhan yang Maha Esa. Dengan demikian, saran dan masukan yang membangun senantiasa penulis terima dengan senang hati. Serta berkat dukungan, motivasi, bantuan, bimbingan, dan doa dari banyak pihak, penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Andi Adriansyah, M.Eng. selaku Rektor Universitas Mercu Buana.
2. Bapak Dr. Bambang Jokonowo, S.Si., MTI selaku Dekan Fakultas Ilmu Komputer.
3. Bapak Dr. Hadi Santoso, S.Kom., M.Kom. selaku Ketua Program Studi Teknik Informatika Universitas Mercubuana.
4. Bapak Rushendra, Ir., S.Kom, MT. selaku dosen pembimbing Tugas Akhir yang telah memberikan pengarahan, motivasi, menyediakan waktu, tenaga, pikiran, dan kesabaran yang tidak terbatas sehingga proses pembuatan proposal ini berjalan dengan lancar.
5. Kedua Orang Tua saya yang selalu mensupport dan mendukung saya selama menjalani masa studi sebagai mahasiswa Universitas Mercubuana..
6. Semua teman kuliah yang selalu berbagi informasi dan memberikan dukungan dalam bentuk yang berbeda-beda.

Akhir kata, penulis berharap semoga Tuhan yang Maha Esa membalas kebaikan dan selalu mencurahkan rahmat, hidayah, serta panjang umur kepada kita semua, aamiin. Terima Kasih.

Jakarta, 10 Agustus 2026

Ridwan

**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS  
AKHIR DI REPOSITORI UMB**

Sebagai sivitas akademik Universitas Mercubuana, saya yang bertanda tangan di bawah ini:

Nama : Ridwan  
NIM : 41522110079  
Program Studi : Fakultas Ilmu Komputer/ Teknik Informatika  
Analisis Komparatif NGFW Fortigate dan Palo  
Judul Laporan Skripsi : Alto terhadap Serangan DoS dan Fitur  
Application Control-SSL Inspection

Demi pengembangan ilmu pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non-Eksklusif (Non-exclusive Royalty-Free Right)** atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan)

Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

UNIVERSITAS  
MERCU BUANA

Jakarta, 10 Agustus 2026  
Yang Menyatakan



Ridwan

# COMPARATIVE ANALYSIS OF FORTIGATE AND PALO ALTO NGFW AGAINST DOS ATTACKS AND APPLICATION CONTROL–SSL INSPECTION FEATURES

RIDWAN

## ABSTRACT

*Denial of Service (DoS) attacks remain a primary threat to network service availability, while conventional firewalls are limited to filtering at the network and transport layers. This study compares the performance of two Next-Generation Firewalls (NGFW), FortiGate VM and Palo Alto VM, against TCP Flood and UDP Flood attacks, and verifies the functionality of Application Control and SSL/TLS Inspection. A quantitative approach with a comparative experimental design was applied in a closed virtual laboratory built on PNETLab, with identical vCPU and RAM allocations for both devices. Attacks were generated from Kali Linux using hping3 for 300 seconds per session, while data were captured automatically by a Python script at 10-second intervals across three scenarios: normal traffic, TCP Flood, and UDP Flood. The measured parameters were latency, throughput, active sessions, CPU usage, and memory usage. The results show that FortiGate maintained an average latency of 8.22 ms under TCP Flood and 5.15 ms under UDP Flood, whereas Palo Alto reached 168.39 ms and 73.61 ms. FortiGate's latency degradation against the baseline was 217.4% under TCP Flood, far lower than Palo Alto at 2,380.0%. Conversely, FortiGate's active sessions surged by 7,938.1% to 1,545.73 sessions during UDP Flood, while Palo Alto rose only 216.8% to 9.60 sessions. FortiGate's CPU load increased to 21.40% under UDP Flood, whereas Palo Alto's memory usage remained high, ranging from 87.67% to 91.25% from the baseline onward. Under the TIPHON standard, FortiGate consistently scored index 4 across all scenarios, whereas Palo Alto dropped from index 4 to 3 under TCP Flood. Functional testing confirmed that both devices successfully blocked encrypted threats and applications according to the applied policies. It is concluded that FortiGate excels in latency, while Palo Alto enforces stricter session control, so NGFW selection should be aligned with organizational priorities.*

**Keywords:** Application Control, Denial of Service, Next-Generation Firewall, SSL Inspection, TIPHON.

## DAFTAR ISI

|                                                    |      |
|----------------------------------------------------|------|
| HALAMAN SAMPUL .....                               | 0    |
| HALAMAN JUDUL .....                                | i    |
| HALAMAN PERNYATAAN KARYA SENDIRI .....             | ii   |
| HALAMAN SURAT KETERANGAN HASIL UJI TURNITIN .....  | iii  |
| HALAMAN PENGESAHAN .....                           | iv   |
| KATA PENGANTAR .....                               | v    |
| HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUG ..... | vi   |
| ABSTRAK.....                                       | vi   |
| ABSTRACT.....                                      | vii  |
| DAFTAR ISI.....                                    | viii |
| DAFTAR TABEL.....                                  | xi   |
| DAFTAR GAMBAR .....                                | xii  |
| DAFTAR LAMPIRAN.....                               | xiv  |
| BAB I PENDAHULUAN.....                             | 1    |
| 1.2 Latar Belakang .....                           | 1    |
| 1.3 Rumusan Masalah.....                           | 5    |
| 1.4 Tujuan Penelitian .....                        | 5    |
| 1.5 Batasan Masalah .....                          | 6    |
| 1.6 Manfaat Penelitian .....                       | 6    |
| BAB II TINJAUAN PUSTAKA .....                      | 8    |
| 2.1 Landasan Teori Utama .....                     | 8    |
| 2.1.1 Keamanan Jaringan .....                      | 8    |
| 2.1.2 Firewall.....                                | 11   |
| 2.1.3 Next Generation Firewall (NGFW).....         | 14   |
| 2.1.4 Distributed Denial of Service (DDoS) .....   | 17   |
| 2.1.5 Serangan TCP Flood .....                     | 20   |
| 2.1.6 Serangan UDP Flood.....                      | 22   |
| 2.1.7 Application Control .....                    | 24   |
| 2.1.8 Inspeksi SSL/TLS.....                        | 27   |
| 2.1.9 Parameter Performa Jaringan .....            | 29   |
| 2.2 Penelitian Terdahulu .....                     | 33   |
| 2.3 Celah Penelitian (Research Gap) .....          | 40   |

|                                   |                                                                        |    |
|-----------------------------------|------------------------------------------------------------------------|----|
| 2.4                               | Posisi Penelitian .....                                                | 44 |
| BAB III METODE PENELITIAN .....   |                                                                        | 47 |
| 3.1                               | Pendekatan Penelitian dan Jenis Penelitian .....                       | 47 |
| 3.1.1                             | Variabel Penelitian .....                                              | 47 |
| 3.2                               | Desain Penelitian .....                                                | 49 |
| 3.3                               | Alur Konfigurasi dan Pemrosesan Data .....                             | 51 |
| 3.4                               | Alat dan Bahan Penelitian .....                                        | 52 |
| 3.4.1                             | Perangkat Lunak Pendukung .....                                        | 53 |
| 3.5                               | Topologi dan Arsitektur Jaringan Pengujian .....                       | 54 |
| 3.6                               | Skenario dan Simulasi Serangan .....                                   | 55 |
| 3.7                               | Instrumen Monitoring dan Pengambilan Data .....                        | 57 |
| 3.8                               | Teknik Pengumpulan Data dan Parameter Pengukuran .....                 | 59 |
| 3.9                               | Metode Analisis Data .....                                             | 60 |
| 3.9.1                             | Statistik Deskriptif .....                                             | 61 |
| 3.9.2                             | Perhitungan Throughput, Latency, dan Packet Loss .....                 | 61 |
| 3.9.3                             | Perhitungan Dampak Serangan dan Overhead Fitur .....                   | 62 |
| 3.9.4                             | Kategorisasi Kualitas Layanan (Standar TIPHON) .....                   | 62 |
| 3.10                              | Prosedur Penelitian .....                                              | 63 |
| 3.11                              | Evaluasi Hasil Penelitian .....                                        | 65 |
| BAB IV HASIL DAN PEMBAHASAN ..... |                                                                        | 67 |
| 4.1                               | Pelaksanaan Eksperimen Skenario S1 sampai S6 .....                     | 67 |
| 4.2                               | Sinkronisasi Metodologi dengan Pelaksanaan .....                       | 68 |
| 4.2.1                             | Realisasi Interval Pengambilan Sampel .....                            | 68 |
| 4.2.2                             | Penyesuaian Cakupan Parameter yang Dilaporkan .....                    | 69 |
| 4.2.3                             | Diferensiasi Throughput dan Efektivitas Mitigasi .....                 | 70 |
| 4.3                               | Hasil Pengukuran Kuantitatif Agregat .....                             | 72 |
| 4.4                               | Analisis Degradasi Performa Akibat Serangan DoS .....                  | 74 |
| 4.4.1                             | Degradasi Akibat TCP SYN Flood (S2 versus S1) .....                    | 75 |
| 4.4.2                             | Degradasi Akibat UDP Flood (S3 versus S1) .....                        | 76 |
| 4.5                               | Analisis Overhead Fitur Keamanan Secara Berpasangan .....              | 77 |
| 4.5.1                             | Direct Feature Overhead pada Trafik Normal (S4 versus S1) .....        | 78 |
| 4.5.2                             | Combined Load pada Serangan TCP SYN Flood (S5 versus S2) .....         | 79 |
| 4.5.3                             | Combined Load pada Serangan UDP Flood (S6 versus S3) .....             | 80 |
| 4.5.4                             | Rekapitulasi Degradasi dan Overhead .....                              | 81 |
| 4.6                               | Analisis Kritis terhadap Data Monitoring .....                         | 83 |
| 4.6.1                             | Anomali Utilisasi CPU Palo Alto VM pada Skenario S2 dan S3 .....       | 83 |
| 4.6.2                             | Perilaku Session Table pada Serangan TCP dan UDP .....                 | 84 |
| 4.6.3                             | Arah Perubahan Ingress Throughput yang Berlawanan antar Platform ..... | 85 |
| 4.6.4                             | Komparabilitas Metrik Utilisasi Memori antar Platform .....            | 86 |
| 4.7                               | Kategorisasi Kualitas Layanan Menurut Standar TIPHON .....             | 86 |
| 4.8                               | Kriteria Penilaian Komparatif dan Sintesis Hasil .....                 | 88 |

|                                         |    |
|-----------------------------------------|----|
| BAB V PENUTUP .....                     | 90 |
| 5.1 Kesimpulan .....                    | 90 |
| 5.2 Rekomendasi Pemilihan Platform..... | 91 |
| 5.3 Keterbatasan Penelitian.....        | 93 |
| 5.4 Saran .....                         | 94 |
| DAFTAR PUSTAKA .....                    | 95 |
| LAMPIRAN.....                           | 97 |



## DAFTAR TABEL

|                                                                                             |    |
|---------------------------------------------------------------------------------------------|----|
| Tabel 2.1 Penelitian Terdahulu yang Relevan .....                                           | 37 |
| Tabel 2.2 Peta Penelitian (Posisi Penelitian terhadap Penelitian Terdahulu) .....           | 42 |
| Tabel 3.1 Identifikasi Variabel Penelitian .....                                            | 48 |
| Tabel 3.2 Definisi Enam Skenario Pengujian .....                                            | 50 |
| Tabel 3.3 Rekapitulasi Jumlah Simulasi dan Data yang Dihasilkan .....                       | 50 |
| Tabel 3.4 Spesifikasi Perangkat dan Lingkungan Pengujian .....                              | 53 |
| Tabel 3.5 Parameter Simulasi Serangan (hping3) .....                                        | 56 |
| Tabel 3.6 Atribut Data dan Parameter Pengukuran .....                                       | 59 |
| Tabel 3.7 Kategori Latency (Delay) Menurut Standar TIPHON .....                             | 63 |
| Tabel 3.8 Kategori Throughput Menurut Standar TIPHON .....                                  | 63 |
| Tabel 3.9 Tahapan Pelaksanaan Penelitian dan Luaran Tiap Tahap .....                        | 65 |
| Tabel 4.1 Matriks Rancangan dan Status Pelaksanaan Skenario Pengujian .....                 | 68 |
| Tabel 4.2 Interval Sampling Nominal dan Realisasi Terukur .....                             | 69 |
| Tabel 4.3 Definisi Operasional Metrik Throughput dan Efektivitas Mitigasi .....             | 71 |
| Tabel 4.4 Rekapitulasi Rerata Parameter Performa Skenario S1 sampai S .....                 | 72 |
| Tabel 4.5 Degradasi Performa Akibat Serangan TCP SYN Flood (S2 versus S1) .....             | 75 |
| Tabel 4.6 Degradasi Performa Akibat Serangan UDP Flood (S3 versus S1) .....                 | 76 |
| Tabel 4.7 Overhead Aktivasi Fitur Keamanan pada Trafik Normal (S4 versus S1) .....          | 78 |
| Tabel 4.8 Overhead Aktivasi Fitur Keamanan pada Serangan TCP SYN Flood (S5 versus S2) ..... | 79 |
| Tabel 4.9 Overhead Aktivasi Fitur Keamanan pada Serangan UDP Flood (S6 versus S3) .....     | 80 |
| Tabel 4.10 Rekapitulasi Selisih Nilai pada Seluruh Pasangan Skenario .....                  | 81 |
| Tabel 4.11 Kategorisasi Latensi Menurut Standar TIPHON pada Seluruh Skenario .....          | 86 |
| Tabel 4.12 Penerapan Kriteria Penilaian Komparatif FortiGate VM dan Palo Alto VM .....      | 88 |
| Tabel 5.1 Matriks Rekomendasi Pemilihan Platform NGFW Berdasarkan Konteks Kebutuhan .....   | 92 |

## DAFTAR GAMBAR

|                                                                                                 |    |
|-------------------------------------------------------------------------------------------------|----|
| Gambar 2.1 Keamanan Jaringan .....                                                              | 9  |
| Gambar 2.2 Pemetaan CIA Triad terhadap Ruang Lingkup Penelitian Ini .....                       | 10 |
| Gambar 2.3 Arsitektur Kerja Firewall Tradisional .....                                          | 12 |
| Gambar 2.4 Perbandingan Cakupan Inspeksi Firewall Tradisional dan NGFW ..                       | 13 |
| Gambar 2.5 Arsitektur Next-Generation Firewall (NGFW).....                                      | 15 |
| Gambar 2.6 Perbandingan Arsitektur Pemrosesan Paket FortiGate dan Palo Alto .....               | 16 |
| Gambar 2.7 Skema Serangan Distributed Denial of Service (DDoS) .....                            | 18 |
| Gambar 2.8 Posisi Serangan pada Penelitian Ini terhadap Konsep DDoS .....                       | 19 |
| Gambar 2.9 Mekanisme Serangan TCP Flood .....                                                   | 20 |
| Gambar 2.10 Rantai Dampak Serangan TCP Flood terhadap Parameter Uji .....                       | 21 |
| Gambar 2.11 Mekanisme Serangan UDP Flood.....                                                   | 22 |
| Gambar 2.12 Perbandingan Karakteristik Serangan TCP Flood dan UDP Flood                         | 24 |
| Gambar 2.13 Mekanisme Application Control .....                                                 | 25 |
| Gambar 2.14 Perbandingan Penerapan Application Control pada FortiGate dan Palo Alto .....       | 26 |
| Gambar 2.15 Mekanisme Inspeksi SSL/TLS pada NGFW .....                                          | 28 |
| Gambar 2.16 Perbandingan Mekanisme SSL/TLS Inspection pada FortiGate dan Palo Alto .....        | 29 |
| Gambar 2.17 Parameter Evaluasi Performa Jaringan .....                                          | 30 |
| Gambar 2.18 Pemetaan Parameter Pengukuran terhadap Rumusan Masalah dan Skenario Pengujian ..... | 32 |
| Gambar 2.19 Roadmap Penelitian .....                                                            | 45 |
| Gambar 2.20 Peta Posisi Penelitian terhadap Penelitian Terdahulu .....                          | 45 |
| Gambar 3.1 Ringkasan Metodologi Penelitian .....                                                | 49 |
| Gambar 3.2 Matriks Skenario Pengujian Faktorial $3 \times$ .....                                | 49 |
| Gambar 3.3 Diagram Alir Konfigurasi Perangkat dan Pemrosesan Data.....                          | 52 |
| Gambar 3.4 Skema Segmentasi Jaringan dan Rencana Pengalamanan IP .....                          | 54 |
| Gambar 3.5 Topologi Pengujian FortiGate VM .....                                                | 55 |
| Gambar 3.6 Topologi Pengujian Palo Alto VM .....                                                | 55 |
| Gambar 3.7 Diagram Alir Eksekusi Skenario Pengujian.....                                        | 57 |
| Gambar 3.8 Arsitektur Sistem Akuisisi Data Berbasis Python.....                                 | 58 |
| Gambar 3.9 Diagram Alir Logika Script Monitoring (monitor.py).....                              | 58 |
| Gambar 3.10 Skema Titik Pengukuran Parameter Performa.....                                      | 60 |
| Gambar 3.11 Tahapan Pipeline Analisis Data .....                                                | 61 |
| Gambar 3.12 Diagram Alir Prosedur Penelitian Secara Keseluruhan .....                           | 64 |
| Gambar 4.1 Perbandingan Latensi Rerata Kedua Platform pada Skenario S1 sampai S .....           | 73 |
| Gambar 4.2 Perbandingan Utilisasi CPU dan Memori pada Skenario S1 sampai S .....                | 73 |
| Gambar 4.3 Perbandingan Jumlah Sesi Aktif pada Skenario S1 sampai S6 (Skala Logaritmik) .....   | 74 |
| Gambar 4.4 Degradasi Seluruh Parameter terhadap Baseline S1 pada Skenario Serangan.....         | 77 |

|                                                                                         |    |
|-----------------------------------------------------------------------------------------|----|
| Gambar 4.5 Overhead Relatif Aktivasi Fitur Keamanan pada Ketiga Pasangan Skenario ..... | 82 |
| Gambar 4.6 Tambahan Latensi Absolut Akibat Aktivasi Fitur Keamanan .....                | 83 |
| Gambar 4.7 Perbandingan Indeks Kualitas Layanan TIPHON pada Skenario S1 sampai S .....  | 87 |



## DAFTAR LAMPIRAN

|                                                    |     |
|----------------------------------------------------|-----|
| Lampiran 1 Kartu Asistensi .....                   | 97  |
| Lampiran 2 Curriculum Vitae .....                  | 98  |
| Lampiran 3 Surat Pernyataan & Pengalihan HAKI..... | 99  |
| Lampiran 4 Sertifikasi BNSP.....                   | 101 |

