



**IMPLEMENTASI KEAMANAN INFRASTRUKTUR
NETWORK MENGGUNAKAN PERANGKAT FORTINET**

**FORTIGATE FIREWALL:
(STUDI KASUS DI PT X)**



LAPORAN SKRIPSI

**UNIVERSITAS
MERCU BUANA**

TIARA RAMAYANI

41521120046

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

2024



**IMPLEMENTASI KEAMANAN INFRASTRUKTUR
NETWORK MENGGUNAKAN PERANGKAT FORTINET
FORTIGATE FIREWALL:
(STUDI KASUS DI PT X)**

LAPORAN SKRIPSI

TIARA RAMAYANI

UNIVERSITAS 41521120046

MERCU BUANA

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2024**

HALAMAN PENYATAAN KARYA SENDIRI

Saya yang bertanda tangan di bawah ini:

Nama : Tiara Ramayani
NIM : 41521120046
Program Studi : Teknik Informatika
Judul Tugas Akhir : Implementasi Keamanan Infrastruktur *Network*
Menggunakan Perangkat Fortinet Fortigate *Firewall*: Studi Kasus di PT X

Menyatakan bahwa Laporan Skripsi ini adalah hasil karya saya sendiri dan bukan plagiat, serta semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar. Apabila ternyata ditemukan di dalam Laporan Skripsi saya terdapat unsur plagiat, maka saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.



Jakarta, 05 Februari 2024



UNIVERSITAS
MERCU BUANA
Tiara Ramayani

HALAMAN PENGESAHAN

Laporan Tugas Akhir ini diajukan oleh:

Nama : Tiara Ramayani
NIM : 41521120046
Program Studi : Teknik Informatika
Judul Tugas Akhir : Implementasi Keamanan Infrastruktur *Network*
Menggunakan Perangkat Fortinet Fortigate *Firewall*: Studi Kasus di PT X

Telah berhasil dipertahankan pada sidang di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Strata 1 pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Mercu Buana.

Disahkan oleh:

Pembimbing : Drs. Achmad Kodar, M.T., M.Kom
NIDN : 0323085801 ()
Ketua Penguji : Muhammad Rifqi, S.Kom, M.Kom
NIDN : 0301067101 ()
Penguji 1 : Prastika Indriyani, S.Kom., M.Cs
NIDN : 0312089401 ()
Penguji 2 : Raka Yusuf, ST, MTI
NIDN : 0315087101 ()

Jakarta, 05 Februari 2024

Mengetahui,

Dekan

Ketua Program Studi



Dr. Bambang Jokonowo, S.Si.,M.T.I



Dr. Hadi Santoso, S.Kom., M.Kom

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan Laporan Tugas Akhir ini. Penulisan Laporan Tugas Akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Komputer pada Fakultas Ilmu Komputer Universitas Mercu Buana. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan Tugas Akhir ini, sangatlah sulit bagi saya untuk menyelesaikan Laporan Tugas Akhir ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Ir. Andi Adriansyah, M.Eng selaku Rektor Universitas Mercu Buana.
2. Bapak Dr. Bambang Jokonowo, S.Si., M.T.I. selaku Dekan Fakultas Ilmu Komputer.
3. Dr. Hadi Santoso, S.Kom., M.Kom selaku Ketua Program Studi Teknik Informatika.
4. Bapak Drs. Achmad Kodar, M.T., M.Kom selaku Dosen Pembimbing Tugas Akhir yang telah membimbing dan memberikan saran untuk Tugas Akhir ini.
5. Raka Yusuf, ST, MTI selaku Dosen Pembimbing Akademik dan selaku penguji 2 untuk Tugas Akhir atas koreksi dan arahan serta masukannya.
6. Muhammad Rifqi, S.Kom., M.Kom selaku ketua penguji Tugas Akhir atas koreksi dan arahan serta masukannya.
7. Prastika Indriyanti, S.Kom., M.Cs selaku penguji 1 untuk Tugas Akhir atas koreksi dan arahan serta masukannya.
8. Orang tua dan keluarga yang telah memberikan dukungan dan do'a.
9. Seluruh rekan-rekan serta pihak yang terlibat dalam penyusunan Tugas Akhir ini yang tidak dapat disebutkan satu per satu.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga Laporan Tugas Akhir ini membawa manfaat bagi pengembangan ilmu.

Jakarta, 05 Februari 2024

Tiara Ramayani

**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR
UNTUK KEPENTINGAN AKADEMIS**

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

Nama : Tiara Ramayani
NIM : 41518120101
Program Studi : Teknik Informatika
Judul Tugas Akhir : Implementasi Keamanan Infrastruktur *Network*
Menggunakan Perangkat Fortinet Fortigate *Firewall*: Studi Kasus di PT X

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 Laporan Magang/ Tugas Akhir/ Tesis/ Disertasi 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, 05 Februari 2024

Yang menyatakan,



(Tiara Ramayani)

ABSTRAK

Nama : Tiara Ramayani
NIM : 41521120046
Program Studi : Teknik Informatika
Judul Tugas Akhir : Implementasi Keamanan Infrastruktur *Network*
Menggunakan Perangkat Fortinet Fortigate *Firewall*:
Studi Kasus di PT X
Pembimbing : Drs. Achmad Kodar, M.T., M.Kom

Dalam era perkembangan teknologi informasi yang pesat, jaringan komputer menjadi elemen kritis dalam mendukung operasional organisasi dan layanan publik. Keberlanjutan operasional dan keamanan infrastruktur jaringan menjadi aspek penting dalam melindungi data sensitif dan menjaga kontinuitas layanan. Dengan meningkatnya penggunaan internet, baik untuk tujuan positif maupun negatif, keamanan jaringan komputer menjadi fokus utama. Oleh karena itu, penting untuk menerapkan teknologi keamanan seperti *Firewall*, khususnya *Next Generation Firewall* (NGFW). Penelitian ini bertujuan untuk merancang keamanan infrastruktur jaringan menggunakan perangkat Fortigate *Firewall*. Melalui penerapan kebijakan dan aturan keamanan, penelitian ini bertujuan meningkatkan keamanan jaringan internal PT X. Penelitian ini menggunakan metode kualitatif dengan pendekatan *Network Development Life Cycle* (NDLC). Data dikumpulkan melalui analisis dokumen, wawancara dengan ahli keamanan jaringan, dan pengujian sistem menggunakan simulasi PNETLab. Pada tahap implementasi, Fortigate *Firewall* digunakan sebagai solusi keamanan. Fitur-fitur seperti antivirus, *web filtering*, *application control*, *network traffic policy*, dan *Intrusion Prevention System* diterapkan untuk meningkatkan keamanan jaringan. Hasil pengujian menunjukkan bahwa keamanan jaringan dapat ditingkatkan dengan efektif. Implementasi keamanan infrastruktur jaringan menggunakan Fortigate *Firewall* dapat memberikan keamanan yang signifikan. Dengan merancang kebijakan keamanan yang tepat dan memanfaatkan fitur-fitur keamanan, PT X dapat melindungi data sensitif dan menjaga kelangsungan operasional.

Kata Kunci: *Fortigate, NDLC, Firewall, PNETLab*

ABSTRACT

Name : Tiara Ramayani
NIM : 41521120046
Study Program : Informatics Engineering
Title Thesis : *Implementation of Network Infrastructure Security Using Fortinet Fortigate Firewall Device: Case Study at PT X*
Counsellor : Drs. Achmad Kodar, M.T., M.Kom

In the era of rapid development of information technology, computer networks have become a critical element in supporting organizational operations and public services. Operational sustainability and network infrastructure security are important aspects in protecting sensitive data and maintaining service continuity. With the increasing use of the internet, both for positive and negative purposes, computer network security has become a major focus. Therefore, it is important to implement security technologies such as Firewall, especially Next Generation Firewall (NGFW). This research aims to design network infrastructure security using Fortigate Firewall devices. Through the implementation of security policies and rules, this research aims to improve the security of PT X's internal network. This research uses a qualitative method with a Network Development Life Cycle (NDLC) approach. Data was collected through document analysis, interviews with network security experts, and system testing using PNETLab simulation. In the implementation stage, Fortigate Firewall is used as a security solution. Features such as antivirus, web filtering, application control, network traffic policy, and Intrusion Prevention System are implemented to improve network security. The test results show that network security can be improved effectively. Implementation of network infrastructure security using Fortigate Firewall can provide significant security. By designing appropriate security policies and utilizing security features, PT X can protect sensitive data and maintain operational continuity.

Keywords: *Fortigate, NDLC, Firewall, PNETLab*

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENYATAAN KARYA SENDIRI	ii
HALAMAN PENGESAHAN	iii
KATA PENGANTAR.....	iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS	v
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI.....	viii
DAFTAR TABEL	xi
DAFTAR GAMBAR.....	xiii
DAFTAR LAMPIRAN	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Tujuan Penelitian.....	4
1.4 Manfaat Penelitian.....	5
1.4.1 Manfaat Bagi Penulis	5
1.4.2 Manfaat Bagi <i>Network Engineer</i>	5
1.4.3 Manfaat Bagi Universitas Mercu Buana	5
1.5 Batasan Penelitian	5
BAB II TINJAUAN PUSTAKA.....	7
2.1 Penelitian Terdahulu	7
2.2 <i>Critical Review</i>	19
2.2.1 <i>Summarize</i>	22
2.2.2 <i>Synthesize</i>	23
2.2.3 <i>Comparison</i>	24
2.2.4 Kontribusi Penelitian.....	25
2.3 Teori Pendukung	26
2.3.1 <i>Firewall</i>	26
2.3.1 Perangkat Jaringan	28

2.3.2 Fortigate	30
2.3.3 <i>Rule</i> dan <i>Policy</i>	32
2.3.4 <i>Security Attack</i>	33
2.3.5 PNET-LAB (<i>Packet Network Emulator Tool Lab</i>).....	35
2.3.6 PuTTY	36
2.3.7 VMware <i>Workstation</i>	37
BAB III METODE PENELITIAN	38
3.1 Jenis Penelitian.....	38
3.2 Metode Pengumpulan Data	39
3.3 Tahapan Penelitian	41
3.3.1 Lokasi Penelitian	41
3.3.2 Lingkungan Penelitian.....	41
3.3.3 Akses Jaringan.....	41
3.3.4 Kolaborasi dan Konsultasi	41
3.4 Diagram Alir Penelitian	41
BAB IV HASIL DAN PEMBAHASAN	44
4.1 Spesifikasi Implementasi.....	44
4.2 Konfigurasi.....	44
4.2.1 Topologi	45
4.2.2 Konfigurasi VMware.....	47
4.2.3 Instalasi PNETLab Simulator Jaringan di VMWare.....	48
4.2.3.1 Persiapan Instalasi	48
4.2.3.2 Download Master PNETLab	48
4.2.3.3 Proses Instalasi	49
4.2.4 Penambahan <i>Node</i> pada PNETLab	53
4.3 Konfigurasi <i>Switch</i>	54
4.3.1 Konfigurasi <i>Switch Core</i>	54
4.3.2 Konfigurasi <i>Switch Access</i>	55
4.4 Konfigurasi Fortigate	55
4.4.1 Akses Fortigate Melalui Web Browser	56
4.4.2 Konfigurasi <i>Interface</i> Fortigate.....	57
4.4.3 Konfigurasi <i>Firewall Policy</i>	58

4.4.3.1 Antivirus.....	59
4.4.3.2 Web Filter.....	60
4.4.3.3 Application Control.....	60
4.4.3.4 Intrusion Prevention.....	61
4.5 Pengujian Sistem.....	62
4.5.1 <i>Default Policy</i>	62
4.5.2 <i>Blocking Policy</i>	64
4.5.2.1 <i>Blocking Youtube</i>	64
4.5.2.2 <i>Blocking Virus dan DDoS Attack</i>	66
4.6 Analisa Hasil.....	67
BAB V KESIMPULAN DAN SARAN.....	69
5.1 Kesimpulan.....	69
5.2 Saran.....	69
DAFTAR PUSTAKA.....	70
LAMPIRAN.....	73



UNIVERSITAS
MERCU BUANA

DAFTAR TABEL

Table 2.1 Review Jurnal “Pengamanan Sistem Jaringan Komputer dengan Teknologi Firewall”	7
Tabel 2.2 Review Jurnal “Analisis Next Generation Firewall Pada Perangkat Fortigate”	7
Tabel 2.3 Review Jurnal “Perancangan Filtering Firewall Menggunakan IPTables Di Jaringan Pusat Teknologi Informasi Unsrat”	8
Tabel 2.4 Review Jurnal “Design and implementation of an enhanced Firewall system for network and internet security”	9
Tabel 2.5 Review Jurnal “Design and Implementation of Enterprise Network Security System Based on Firewall”	10
Tabel 2.6 Review Jurnal “Penyusunan Panduan Pengelola Keamanan Informasi Untuk Firewall Configuration Berdasarkan Kerangka Kerja PCI DSS v.3.1 dan COBIT 5”	10
Tabel 2.7 Review Jurnal “High Availability’s Implementation on The Fortigate Firewall Using SD-WAN Zone and HA Cluster Active Passive”	11
Tabel 2.8 Review Jurnal “Penerapan Teknologi Fortigate Dalam Pembangunan Jaringan VPN-IP Berbasis IPSEC”	12
Tabel 2.9 Review Jurnal “Implementation of Load Balancing and Failover Network Using Fortinet SDWAN Technology at PT.Lintasarta”	13
Tabel 2.10 Review Jurnal “Analisis Penerapan Teknologi Traffic Steering SD-WAN Menggunakan Perangkat Fortigate”	13
Tabel 2.11 Review Jurnal “Analisa Keamanan Jaringan Dengan Mikrotik”	14
Tabel 2.12 Review Jurnal “Sistem Keamanan Jaringan Komputer Menggunakan Metode Watchguard Firebox Pada PT. Guna Karya Indonesia”	15
Tabel 2.13 Review Jurnal “Penerapan Network Development Life Cycle Untuk Pengembangan Teknologi Thin Client Pada Pendidikan KSM Pontianak”	16
Tabel 2.14 Review Jurnal “Penerapan Network Development Life Cycle Untuk Pengembangan Teknologi Thin Client Pada Pendidikan KSM Pontianak”	17
Tabel 2.15 Review Jurnal “Penerapan Network Development Life Cycle Untuk Pengembangan Teknologi Thin Client Pada Pendidikan KSM Pontianak”	18

Tabel 2.16 Jumlah Jurnal Penelitian	20
Tabel 4.1 Spesifikasi Sistem	44
Tabel 4.2 Daftar VLAN dan IP Adress	55
Tabel 4.3 Perbandingan <i>Default Policy</i> dan <i>Blocking Policy</i> pada Fortigate Firewall	68



DAFTAR GAMBAR

Gambar 1.1 Persentase Penduduk Usia 5 Tahun keatas yang Pernah Mengakses Internet dalam 3 Bulan Terakhir Menurut Klasifikasi Daerah, 2018-2022	1
Gambar 1.2 Topologi Simulasi Serangan Jaringan Lokal yang Melalui Fortigate . 3	
Gambar 2.1 Proses Critical Review	19
Gambar 2.2 Harzing Publish or Perish Penelitian Terdahulu	20
Gambar 2.3 Pengolahan VOS Viewer	21
Gambar 2.4 Pengolahan VOS Viewer	22
Gambar 2.5 GAP Penelitian Irisan antara Firewall dan Data	25
Gambar 2.6 Simulasi Firewall	26
Gambar 2.7 Kabel Unshielded Twisted Pair (UTP).....	28
Gambar 2.8 Kabel Fiber Optik.....	28
Gambar 2.9 Dashboard fortigate	30
Gambar 2.10 Topologi Jaringan Fortigate Jaringan Komputer	31
Gambar 2.11 <i>Model Security Attack</i>	33
Gambar 2.12 Dos dan DDoS <i>Attack</i>	34
Gambar 2.13 Menu Login PNETLab.....	35
Gambar 2.14 PuTTY	36
Gambar 2.15 VMware Workstation.....	37
Gambar 3.1 Siklus NDLC.....	38
Gambar 3.2 Tahap Penelitian Pengumpulan Data	40
Gambar 3.3 Prosedur Manajemen Insiden.....	40
Gambar 3.4 Diagram Alir Penelitian	42
Gambar 4.1 Topologi <i>Physical Existing</i> PT X.....	45
Gambar 4.2 Topologi Hasil Perancangan untuk PT X.....	46
Gambar 4.3 Langkah instalasi PNETLab.....	48
Gambar 4.4 Homepage PNETLab	48
Gambar 4.5 Pilihan Media Download PNETLab	49
Gambar 4.6 OVA PNETLab	49
Gambar 4.7 Penambahan File OVA PNETLab	50
Gambar 4.8 Import File OVA PNETLab.....	50

Gambar 4.9 Hasil PNETLab Setelah Ditambahkan.....	50
Gambar 4.10 Tampilan Awal PNETLab.....	51
Gambar 4.11 Halaman Utama PNETLAB di VMware	51
Gambar 4.12 Tampilan Awal PNETLab.....	52
Gambar 4.13 Halaman Login PNETLab.....	52
Gambar 4.14 Lembar Kerja PNETLab	52
Gambar 4.15 Topologi Infrstruktur Network di PNETLab	53
Gambar 4.16 <i>Flowchart</i> Tahapan Konfigurasi Fortigate.....	55
Gambar 4.17 Login Fortigate	56
Gambar 4.18 Dashboard Status Fortigate	56
Gambar 4.19 Konfigurasi Seluruh <i>Interface</i> Fortigate	57
Gambar 4.20 Konfigurasi Port 1 <i>Interface</i> Fortigate	57
Gambar 4.21 Konfigurasi DNS.....	58
Gambar 4.22 Konfigurasi <i>Policy</i>	58
Gambar 4.23 Konfigurasi Antivirus.....	59
Gambar 4.24 Konfigurasi <i>Web filter</i>	60
Gambar 4.25 Konfigurasi <i>Aplication Control</i>	60
Gambar 4.26 Konfigurasi <i>Intrusion Prevention</i>	61
Gambar 4.27 Hasil IPConfig di PC <i>Enduser</i>	62
Gambar 4.28 Hasil <i>Enduser</i> Ping ke Google	62
Gambar 4.29 Hasil <i>Enduser</i> Ping ke Youtube	62
Gambar 4.30 Hasil <i>Enduser</i> Akses ke detik.com.....	63
Gambar 4.31 Hasil <i>Traffic</i> yang Terdeteksi di Fortigate	63
Gambar 4.32 Hasil IPConfig di PC <i>Enduser</i>	64
Gambar 4.33 Hasil <i>Enduser</i> Ping ke Google	64
Gambar 4.34 Hasil <i>Enduser</i> Ping ke Youtube	64
Gambar 4.35 Hasil <i>Enduser</i> Akses ke detik.com.....	65
Gambar 4.36 Hasil <i>Enduser</i> Akses ke Youtube.....	65
Gambar 4.37 Hasil <i>Traffic</i> yang Terdeteksi di Fortigate	65
Gambar 4.38 Hasil Log Antivirus.....	66
Gambar 4.39 Hasil Log <i>Intrusion Prevention</i>	67

DAFTAR LAMPIRAN

Lampiran 1 Asistensi Bimbingan.....	73
Lampiran 2 Lampiran Halaman Pernyataan Luaran Tugas Akhir.....	74
Lampiran 3 Lampiran Naskah Artikel Jurnal.....	75
Lampiran 4 Curriculum Vitae	76
Lampiran 5 Surat Pernyataan HAKI.....	77
Lampiran 6 Surat Pengalihan Hak Cipta.....	78
Lampiran 7 Sertifikat BNSP	79
Lampiran 8 Form Revisi Dosen Penguji.....	80

