

**PERANCANGAN TOPOLOGI JARINGAN DAN KONFIGURASI
KEAMANAN WEB SERVER DAILY MANAGEMENT SYSTEM PADA PT
ZEUS KIMIATAMA INDONESIA**



LAPORAN MBKM MAGANG

**MUHAMMAD ZAIDAN FIQRI
00000060117**

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA
TANGERANG
2025**

**PERANCANGAN TOPOLOGI JARINGAN DAN KONFIGURASI
KEAMANAN WEB SERVER DAILY MANAGEMENT SYSTEM PADA PT
ZEUS KIMIATAMA INDONESIA**



UMN

**UNIVERSITAS
MULTIMEDIA
NUSANTARA**

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK DAN INFORMATIKA
UNIVERSITAS MULTIMEDIA NUSANTARA**

TANGERANG

2025

HALAMAN PERNYATAAN TIDAK PLAGIAT

Dengan ini saya,

Nama : Muhammad Zaidan Fiqri

NIM : 00000060117

Program Studi : Informatika

Menyatakan dengan sesungguhnya bahwa Tesis/Skripsi/Tugas Akhir/Laporan Magang/MBKM saya yang berjudul:

Perancangan Topologi Jaringan dan Konfigurasi Keamanan Web Server Daily Management System pada PT Zeus Kimiatama Indonesia

merupakan hasil karya saya sendiri, bukan merupakan hasil plagiat, dan tidak pula dituliskan oleh orang lain; Semua sumber, baik yang dikutip maupun dirujuk, telah saya cantumkan dan nyatakan dengan benar pada bagian Daftar Pustaka.

Jika di kemudian hari terbukti ditemukan kecurangan/penyimpangan, baik dalam pelaksanaan skripsi maupun dalam penulisan laporan karya ilmiah, saya bersedia menerima konsekuensi untuk dinyatakan TIDAK LULUS. Saya juga bersedia menanggung segala konsekuensi hukum yang berkaitan dengan tindak plagiarisme ini sebagai kesalahan saya pribadi dan bukan tanggung jawab Universitas Multimedia Nusantara.

Tangerang, 3 Januari 2025



(Muhammad Zaidan Fiqri)

UMMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

**HALAMAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK
KEPENTINGAN AKADEMIS**

Yang bertanda tangan di bawah ini:

Nama : Muhammad Zaidan Fiqri
NIM : 00000060117
Program Studi : Informatika
Jenjang : S1
Jenis Karya : Magang

Menyatakan dengan sesungguhnya bahwa:

- Saya bersedia memberikan izin sepenuhnya kepada Universitas Multimedia Nusantara untuk mempublikasikan hasil karya ilmiah saya di repositori Knowledge Center, sehingga dapat diakses oleh Civitas Akademika/Publik. Saya menyatakan bahwa karya ilmiah yang saya buat tidak mengandung data yang bersifat konfidensial dan saya juga tidak akan mencabut kembali izin yang telah saya berikan dengan alasan apapun.
- Saya tidak bersedia karena dalam proses pengajuan untuk diterbitkan ke jurnal/konferensi nasional/internasional (dibuktikan dengan *letter of acceptance*)**.

Tangerang, 3 Januari 2025

Yang menyatakan

UMN

Muhammad Zaidan Fiqri

UNIVERSITAS
MULTIMEDIA
NUSANTARA

** Jika tidak bisa membuktikan LoA jurnal/IJKI selama enam bulan ke depan, saya bersedia mengizinkan penuh karya ilmiah saya untuk diunggah ke KC UMN dan menjadi hak institusi UMN.

KATA PENGANTAR

Puji syukur dipanjatkan ke hadirat Tuhan Yang Maha Esa atas berkat dan rahmat-Nya sehingga laporan magang dengan judul “Perancangan Topologi Jaringan dan Konfigurasi Keamanan Web Server Daily Management System pada PT Zeus Kimiatama Indonesia” dapat diselesaikan. Laporan ini disusun sebagai salah satu syarat untuk menyelesaikan studi di Program Sarjana Teknik Informatika. Penyelesaian laporan ini tidak lepas dari dukungan dan bantuan berbagai pihak, oleh karena itu, rasa terima kasih yang sebesar-besarnya disampaikan kepada.

1. Bapak Dr. Ir. Andrey Andoko, M.Sc., selaku Rektor Universitas Multimedia Nusantara.
2. Bapak Dr. Eng. Niki Prastomo, S.T., M.Sc., selaku Dekan Fakultas Teknik dan Informatika Universitas Multimedia Nusantara.
3. Bapak Assoc. Prof. Arya Wicaksana, S.Kom., M.Eng.Sc. (OCA, CEH, CEI), selaku Ketua Program Studi Informatika Universitas Multimedia Nusantara.
4. Bapak Dennis Gunawan, S.Kom., M.Sc., sebagai Pembimbing yang telah banyak meluangkan waktu untuk memberikan bimbingan, arahan dan motivasi atas terselesainya laporan magang ini.
5. Bapak Vincentius Kurniawan, S.Kom., M.Eng., selaku penguji atas kesediaan waktunya untuk mengevaluasi, memberikan masukan, dan merevisi laporan magang ini, yang arahan serta perhatiannya sangat membantu dalam penyempurnaan laporan sehingga dapat diselesaikan dengan lebih baik dan sesuai harapan.
6. Bapak Sutrismiyanto selaku koordinator IT yang telah banyak memberikan kesempatan dan bimbingannya untuk belajar lebih dalam mengenai rancangan pembuatan alur jaringan keamanan di PT Zeus Kimiatama Indonesia.
7. Orang Tua dan keluarga saya yang telah memberikan bantuan dukungan material dan moral, sehingga penulis dapat menyelesaikan laporan magang ini.

8. Terima kasih kepada Dicky Hermawan selaku rekan kerja, atas dukungan dan arahnya di lapangan karena telah membagi ilmu dan pengalamannya sehingga pekerjaan ini dapat terlaksana dengan lebih efisien.

Semoga laporan magang ini dapat bermanfaat sebagai sumber informasi dan inspirasi bagi para pembaca

Tangerang, 3 Januari 2025



Muhammad Zaidan Fiqri



UMMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

**PERANCANGAN TOPOLOGI JARINGAN DAN KONFIGURASI
KEAMANAN WEB SERVER DAILY MANAGEMENT SYSTEM PADA PT
ZEUS KIMIATAMA INDONESIA**

Muhammad Zaidan Fiqri

ABSTRAK

Perkembangan pesat internet telah membawa kemudahan dalam berbagai aspek termasuk salah satu contohnya adalah digitalisasi sistem berbasis *website* di perusahaan seperti PT Zeus Kimatama Indonesia (ZEKINDO). Pada awalnya ZEKINDO mendigitalisasi sistem permintaan pembelian bahan mentah berbasis *website* dengan server lokal dikarenakan keterbatasan sumber daya yang dimiliki oleh *information technology* (IT) pada saat tersebut. Namun, dikarenakan meningkatnya ancaman siber seperti *brute force* dan *DDoS* yang belakangan ini hendak mengancam *web server* tim IT memutuskan untuk memanfaatkan perangkat jaringan dan keamanan yang diperoleh melalui akuisisi PT Croda Indonesia pada Januari 2024. Berbagai alat seperti *Firewall Cisco ASA 5512-X*, *MikroTik*, *Splunk*, *Switch Layer 2 Cisco Catalyst 2960*, *Ubuntu Server*, serta perangkat akses seperti *PuTTY*, kabel konsol, dan kabel LAN digunakan dalam proses ini. Hasilnya topologi jaringan ZEKINDO telah berhasil dirancang dan keamanan terhadap web server *daily management system* (DMS) telah dikonfigurasi sesuai kebutuhan departemen IT. Meskipun *load balancing* pada sisi server DMS telah diterapkan, implementasi pada bagian klien masih terkendala oleh kebutuhan IP publik. *Penetration testing* belum dilakukan karena keterbatasan waktu dan mobilitas yang tinggi. Langkah-langkah ini diambil sebagai upaya strategis dari departemen IT untuk menjaga kelancaran operasional perusahaan serta membantu menjaga keamanan sistem digital di tengah meningkatnya ancaman siber yang belakangan ini mengancam.

Kata kunci: Ancaman Siber, *Firewall Cisco ASA*, Keamanan Jaringan ZEKINDO, *Loadbalancing Server Lokal*, Topologi Jaringan ZEKINDO

UNIVERSITAS
MULTIMEDIA
NUSANTARA

***DESIGN OF NETWORK TOPOLOGY AND SECURITY CONFIGURATION
FOR THE WEB SERVER OF THE DAILY MANAGEMENT SYSTEM AT PT
ZEUS KIMIATAMA INDONESIA***

Muhammad Zaidan Fiqri

ABSTRACT

The rapid development of the internet has brought convenience, including the digitalization of systems in companies like PT Zeus Kimatama Indonesia (ZEKINDO). Initially, ZEKINDO digitalized its raw material purchase request system using a local server due to limited IT department resources. However, rising cyber threats such as brute force and DDoS attacks began targeting the web server. To address these issues, the IT team utilized networking and security devices acquired through PT Croda Indonesia in January 2024. Several tools were deployed, including the Cisco ASA 5512-X Firewall, MikroTik, Splunk, Cisco Catalyst 2960, Ubuntu Server, and access tools like PuTTY, console cables, and LAN cables. These efforts successfully established ZEKINDO's network topology and enhanced security for the Daily Management System (DMS) web server. While load balancing has been implemented on the server side, the client-side remains constrained by the need for public IP addresses. Penetration testing has not been conducted due to time limitations and high mobility demands. These strategic measures by the IT department aim to safeguard digital systems, ensuring smooth operations and maintaining system integrity amid increasing cyber threats.

Keywords: *Cyber Threats, Cisco ASA Firewall, Network Security, Load Balancing, ZEKINDO Topology.*



DAFTAR ISI

| | |
|---|------|
| HALAMAN JUDUL | i |
| PERNYATAAN TIDAK MELAKUKAN PLAGIAT | ii |
| HALAMAN PERSETUJUAN PUBLIKASI ILMIAH | iii |
| KATA PENGANTAR | iv |
| ABSTRAK | vi |
| ABSTRACT | vii |
| DAFTAR ISI | viii |
| DAFTAR GAMBAR | ix |
| DAFTAR TABEL | xi |
| DAFTAR LAMPIRAN | xii |
| BAB 1 PENDAHULUAN | 1 |
| 1.1 Latar Belakang Masalah | 1 |
| 1.2 Maksud dan Tujuan Kerja Magang | 2 |
| 1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang | 3 |
| BAB 2 GAMBARAN UMUM PERUSAHAAN | 4 |
| 2.1 Deskripsi Singkat Perusahaan | 4 |
| 2.2 Visi dan Misi Perusahaan | 4 |
| 2.2.1 Visi Perusahaan | 4 |
| 2.2.2 Misi Perusahaan | 5 |
| 2.3 Struktur Organisasi Perusahaan | 5 |
| BAB 3 PELAKSANAAN KERJA MAGANG | 8 |
| 3.1 Kedudukan dan Koordinasi | 8 |
| 3.2 Tugas yang Dilakukan | 8 |
| 3.3 Uraian Pelaksanaan Magang | 9 |
| 3.3.1 Requirement | 10 |
| 3.3.2 Implementasi | 11 |
| 3.4 Kendala dan Solusi yang Ditemukan | 46 |
| 3.4.1 Kendala | 46 |
| 3.4.2 Solusi | 47 |
| BAB 4 SIMPULAN DAN SARAN | 48 |
| 4.1 Simpulan | 48 |
| 4.2 Saran | 48 |
| DAFTAR PUSTAKA | 49 |

UNIVERSITAS
MULTIMEDIA
NUSANTARA

DAFTAR GAMBAR

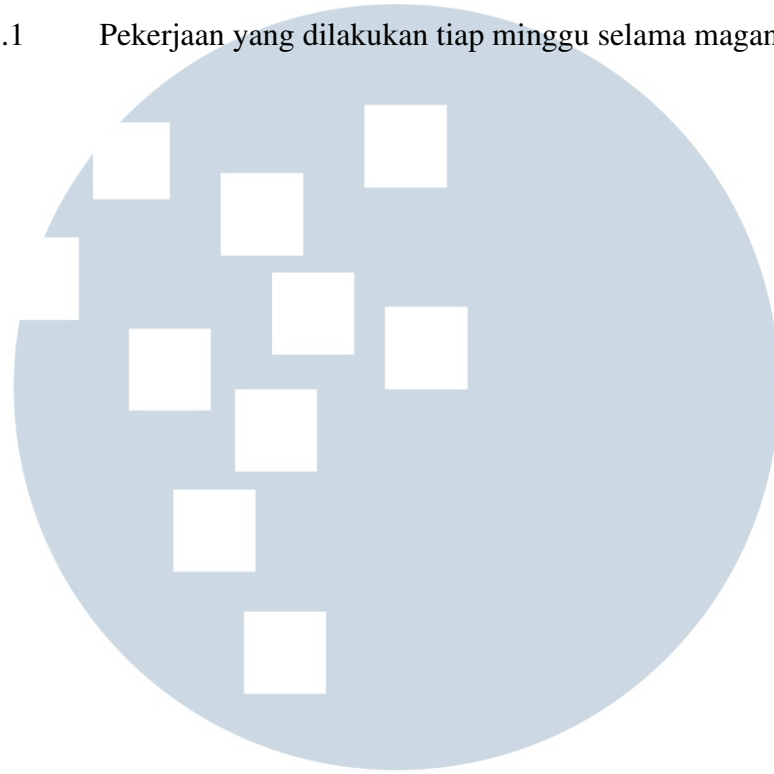
| | | |
|-------------|---|----|
| Gambar 2.1 | Struktur organisasi perusahaan PT Zeus Kimiatama Indonesia | 5 |
| Gambar 3.1 | <i>Topologi</i> perangkat jaringan dan keamanan | 11 |
| Gambar 3.2 | Pemberian peruntukan untuk antarmuka | 12 |
| Gambar 3.3 | Pembuatan <i>bridge</i> | 12 |
| Gambar 3.4 | Daftar antarmuka yang di jadikan <i>bridge</i> | 13 |
| Gambar 3.5 | Daftar dari alamat IP | 13 |
| Gambar 3.6 | Status <i>DHCP Client</i> | 14 |
| Gambar 3.7 | <i>DHCP Server</i> | 14 |
| Gambar 3.8 | Penerapan DNS pada <i>DHCP Server</i> | 15 |
| Gambar 3.9 | Penentuan <i>RangeIP Pool DHCP Server</i> | 15 |
| Gambar 3.10 | <i>Firewall NAT</i> | 15 |
| Gambar 3.11 | <i>Firewall Mangle</i> | 16 |
| Gambar 3.12 | <i>Service</i> yang dibuka dan ditutup | 17 |
| Gambar 3.13 | <i>Ping Test</i> ke jaringan <i>DMZ</i> dan <i>internal</i> | 18 |
| Gambar 3.14 | Mengubah <i>Hostname</i> dan set <i>password</i> | 19 |
| Gambar 3.15 | Menetapkan peruntukan <i>interface</i> sesuai dengan kebutuhan | 20 |
| Gambar 3.16 | Menetapkan peruntukan <i>interface</i> sesuai dengan kebutuhan | 21 |
| Gambar 3.17 | <i>Access Control List</i> yang diterapkan | 22 |
| Gambar 3.18 | <i>Config Logging</i> | 23 |
| Gambar 3.19 | Contoh <i>MTU, ICMP dan ARP Config</i> | 24 |
| Gambar 3.20 | <i>rules NAT</i> | 24 |
| Gambar 3.21 | Penerapan <i>access group</i> | 25 |
| Gambar 3.22 | <i>Timeout and Dynamic Access Policy</i> | 25 |
| Gambar 3.23 | Penerapan <i>Authentication, Authorization, and Accounting</i> | 25 |
| Gambar 3.24 | Konfigurasi <i>SNMP, Telnet, SSH and DHCP</i> | 26 |
| Gambar 3.25 | Konfigurasi <i>DHCP Address Range, Threat Detection and Class-Map</i> | 27 |
| Gambar 3.26 | Contoh penerapan <i>policy-map</i> | 29 |
| Gambar 3.27 | Set alamat IP statis pada <i>Ubuntu server</i> | 30 |
| Gambar 3.28 | <i>Ping test ke Cisco ASA</i> | 31 |
| Gambar 3.29 | <i>Status Netplan</i> | 31 |
| Gambar 3.30 | Hasil <i>Log Splunk</i> | 32 |
| Gambar 3.31 | Hasil <i>Log Splunk</i> . dengan <i>event</i> tertentu | 33 |
| Gambar 3.32 | Penamaan dan pengalokasian antarmuka | 34 |
| Gambar 3.33 | <i>DHCP Client</i> | 35 |
| Gambar 3.34 | <i>Nama Bridge</i> | 35 |
| Gambar 3.35 | <i>List Interface yang dimasukkan ke Bridge</i> | 35 |
| Gambar 3.36 | Penambahan IP untuk <i>Bridge</i> | 36 |
| Gambar 3.37 | Konfigurasi DHCP yang ditujukan ke interface <i>Bridge</i> | 36 |
| Gambar 3.38 | <i>Bridge</i> yang dibuat sudah berhasil menerima jaringan secara DHCP | 37 |
| Gambar 3.39 | <i>Device</i> yang terhubung melewati bridge sudah mendapat alamat IP dan MAC | 37 |
| Gambar 3.40 | Aturan <i>firewall</i> yang memungkinkan perangkat mengakses internet. | 37 |
| Gambar 3.41 | <i>IP Pool</i> setelah konfigurasi <i>DHCP Server</i> | 38 |

| | | |
|-------------|--|----|
| Gambar 3.42 | <i>Ping Test ke DNS Google, IP Gateway, dan DMZ</i> | 39 |
| Gambar 3.43 | Status <i>DHCP</i> pada <i>switch</i> | 39 |
| Gambar 3.44 | Status antarmuka ke 19 pada <i>switch</i> | 39 |
| Gambar 3.45 | Status antarmuka kedua pada <i>switch</i> | 40 |
| Gambar 3.46 | Status <i>VLAN</i> pada <i>switch</i> | 41 |
| Gambar 3.47 | <i>Ping Test</i> dari perangkat yang terhubung lewat <i>switch</i> | 42 |
| Gambar 3.48 | <i>Bruteforce login ssh web server</i> | 43 |
| Gambar 3.49 | <i>Routing dan DNS</i> yang dikonfigurasi | 43 |
| Gambar 3.50 | <i>Routing dan DNS</i> pada <i>file resolv</i> | 44 |
| Gambar 3.51 | Cek status pada konfigurasi yang sudah dilakukan | 44 |
| Gambar 3.52 | <i>Ping Test</i> ke <i>Bridge MikroTik</i> | 45 |
| Gambar 3.53 | <i>Ping Test</i> ke <i>Google dan DNS Google</i> | 46 |



DAFTAR TABEL

Tabel 3.1 Pekerjaan yang dilakukan tiap minggu selama magang . . . 9



UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

DAFTAR LAMPIRAN

| | | |
|------------|---|----|
| Lampiran 1 | MBKM-01 Cover Letter MBKM Internship Track 1 | 50 |
| Lampiran 2 | MBKM-02 MBKM Internship Track 1 Card | 51 |
| Lampiran 3 | MBKM-03 Daily Task - Internship Track 1 | 52 |
| Lampiran 4 | MBKM-04 Verification Form of Internship Report MBKM Internship Track 1 | 62 |
| Lampiran 5 | Form Bimbingan | 63 |
| Lampiran 6 | Hasil Turnitin | 64 |

