© 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

IMPLEMENTASI DAN ANALISIS *INDUSTRIAL DEMILITARIZED ZONE* (IDMZ) PADA INFRASTRUKTUR JARINGAN PT KALBIO GLOBAL MEDIKA

SKRIPSI

MUAMMAR ZAIN
2207421010

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

IMPLEMENTASI DAN ANALISIS *INDUSTRIAL DEMILITARIZED ZONE* (IDMZ) PADA INFRASTRUKTUR JARINGAN PT KALBIO GLOBAL MEDIKA

SKRIPSI

Dibuat untuk melengkapi syarat-syarat yang diperlukan untuk memperoleh diploma empat politeknik

MUAMMAR ZAIN

2207421010

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

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini:

Nama : Muammar Zain

NIM : 2207421010

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

Judul Skripsi : Implementasi dan Analisis *Industrial Demilitarized Zone* pada Infrastruktur Jaringan PT Kalbio Global Medika

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.

Cikarang 09 Februari 2026

Yang Membuat Pernyataan



Muammar Zain

NIM. 2207421010

© 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 : Muammar Zain

NIM : 2207421010

Program Studi : Teknik Multimedia dan Jaringan

Judul Skripsi : Implementasi & Analisis *Industrial Demilitarized Zone* pada Infrastruktur Jaringan PT Kalbio Global Medika

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu Tanggal 17 Bulan Juni Tahun 2026, dan dinyatakan **LULUS**.

Disahkan Oleh

Pembimbing I	Dr. Defiana Arnaldy, S.Tp., M.Si.	( )
Penguji I	Asep Kurniawan, S.T., M.Kom.	( )
Penguji II	Fachroni Arbi Murad, S.Kom., M.Kom.	( )
Penguji III	Iik Muhammad Malik Matin, S.T., M.T.	( )

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

Dr. Anita Hidayati, S.Kom., M.Kom.

NIP. 19790803200312200

© 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

KATA PENGANTAR

Puji syukur penulis ucapkan kepada Allah SWT atau segala berkat dan rahmat-Nya yang telah memudahkan penulis menyelesaikan skripsi ini, yang merupakan syarat untuk lulus di Politeknik Negeri Jakarta. Dalam proses penulisan skripsi ini, banyak pihak yang telah memberikan bantuan dan dukungan. Oleh karena itu, penulis ingin menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Kedua Orang tua yang selalu memberikan dukungan , mendoakan dan juga memfasilitasi segala macam kebutuhan selama kegiatan dari masa perkuliahan sampai proses skripsi ini berlangsung.
2. Bapak Dr. Defiana Arnaldy, S.Tp., M.Si. sebagai dosen pembimbing yang telah meluangkan banyak waktu, tenaga, dan pikirannya dalam membimbing selama kegiatan penelitian ini.
3. Bapak Steven Amadeus Selaku Manager PT Kalbio Global Medika yang memperbolehkan penyusunan skripsi dan pengambilan data observasi
4. Bapak Ade Kurnia Rahman dan Bapak Vincent Cunardy selaku Pembimbing di Industri yang selalu memberikan wawasan dan tempat bertukar pikiran selama kegiatan penelitian
5. PT Kalbio Global Medika yang bersedia memberikan kesempatan untuk melakukan penelitian
6. Seseorang dengan NIM. 2306321087 yang selalu membantu penulis dalam memberi semangat dan dukungan moral selama penyusunan skripsi.
7. Saudara Sandika Arga Pamungkas Selaku kakak tingkat yang selalu memberikan masukan dan ide selama penulis menyusun skripsi.

Akhir kata penulis memohon maaf atas kekeliruan dan kesalahan yang terdapat dalam Skripsi ini semoga dapat bermanfaat bagi pembacanya.

Cikarang 09 Februari 2026



Penulis

© 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 dibawah ini:

Nama : Muammar Zain

NIM : 2207421010

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:

Implementasi dan Analisis Industrial Demilitarized Zone (IDMZ) pada Infrastruktur Jaringan PT Kalbio Global Medika

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.

Cikarang 09 Februari 2026

Yang Membuat Pernyataan



Muammar Zain

NIM.2207421010

© 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

Implementasi dan Analisis *Industrial Demilitarized Zone* (IDMZ) pada Infrastruktur Jaringan PT Kalbio Global Medika

Abstrak

Perkembangan Industri 4.0 mendorong transformasi digital pada sektor biofarmasi di Indonesia, termasuk di PT Kalbio Global Medika. Kondisi eksisting menunjukkan jaringan OT pada zona produksi dapat diakses langsung dari jaringan internal perusahaan hanya dengan mengetahui IP dan port layanan aktif tanpa segmentasi jaringan maupun kontrol akses yang memadai. Hal ini menimbulkan risiko kebocoran data, penyalahgunaan akses, dan gangguan terhadap sistem kritikal. Penelitian ini bertujuan mengimplementasikan arsitektur Industrial Demilitarized Zone (IDMZ) berbasis firewall FortiGate mengacu pada model ISA-95/Purdue Level 3.5 menggunakan metode Network Development Life Cycle (NDLC). Evaluasi mencakup pengujian (QoS), efektivitas pemblokiran akses tidak sah, dan pencatatan log. Hasil pengujian menunjukkan throughput meningkat dari 35,313 Mbps menjadi 50,381 Mbps. Delay meningkat dari 7,346 ms menjadi 13,351 ms dan jitter dari 0,314 ms menjadi 0,823 ms, namun masih memenuhi kategori baik berdasarkan standar TIPHON. Packet loss tetap 0%. Firewall memblokir 100% akses langsung IT ke OT tanpa VPN, sementara log FortiGate merekam seluruh aktivitas trafik antar zona. Implementasi IDMZ terbukti meningkatkan keamanan jaringan dengan pemblokiran sebesar 100%, sementara performa tetap dalam kategori "Baik" berdasarkan standar TIPHON dengan peningkatan throughput 42,7% (dari 35,313 Mbps menjadi 50,381 Mbps), delay 13,351 ms, jitter 0,823 ms, dan packet loss 0%.

Kata Kunci: Industrial Demilitarized Zone ,Operational Technology, Segmentasi Jaringan ,Virtual Private Network.

© 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

DAFTAR ISI

BAB I..... 14
PENDAHULUAN..... 14
1.1 Latar Belakang..... 14
1.2 Rumusan Masalah..... 2
1.3 Batasan Masalah..... 3
1.4 Tujuan dan Manfaat..... 3
1.4.1 Tujuan..... 3
1.4.2 Manfaat..... 3
1.5 Sistematika Penulisan..... 4
BAB II..... 5
TINJAUAN PUSTAKA..... 5
2.1 Penelitian Terdahulu..... 5
2.2 Industrial Demilitarized Zone (IDMZ)..... 8
2.3 Firewall..... 9
2.4 Network Address Translation (NAT)..... 10
2.5 Virtual Local Area Network (VLAN)..... 10
2.6 PuTTY..... 11
2.7 Virtual Private Network (VPN)..... 12
2.8 Network Development Life Cycle (NDLC)..... 12
2.9 Quality of Service (QoS)..... 15
2.10 Windows Subsystem for Linux (WSL)..... 18
2.11 Linux Ubuntu..... 19
2.12 Raspberry Pi..... 19
2.13 Winbox..... 20
2.14 Flowchart..... 21
2.15 ISA 95/Purdue Model..... 22
BAB III..... 23
METODE PENELITIAN..... 23
3.1 Rancangan Penelitian..... 23
3.2 Tahapan Penelitian..... 24
3.3 Objek Penelitian..... 26
BAB IV..... 27
HASIL DAN PEMBAHASAN..... 27
4.1 Analisis Kebutuhan..... 27
4.1.1 Analisis Kebutuhan Perangkat Keras..... 27
4.1.2 Analisis Kebutuhan Tools..... 28
4.2 Perancangan Sistem..... 29
4.2.1 Topologi Jaringan Eksisting..... 29

POLITEKNIK NEGERI JAKARTA

© 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

4.2.2 Perancangan Topologi Jaringan Baru 30
4.2.3 Perencanaan IP Address 31
4.2.4 Policy Firewall List 32
4.2.5 Akses User Menuju Zona OT 34
4.3 Implementasi dan Konfigurasi 35
4.3.1 Setup Firewall 35
4.3.2 Konfigurasi Firewall 38
4.3.3 Konfigurasi VPN 43
4.3.4 Konfigurasi Switch Managable 48
4.3.5 Konfigurasi Mikrotik RB750G R3 50
4.3.6 Konfigurasi Raspberry PI 52
4.4 Pengujian Sistem 54
4.4.1 Prosedur Pengujian 55
4.4.1.1 Pengujian QoS Sebelum Implementasi 55
4.4.1.2 Pengujian QoS Sesudah Implementasi 57
4.4.1.3 Analisis Perbandingan QoS Sebelum & Sesudah 61
4.4.1.4 Pengujian Firewall 62
4.4.1.5 Pengujian Pencatatan Log 65
4.4.1.6 Pengujian Firewall dan Konektivitas 66
4.4.1.7 Analisis Efektivitas Firewall 67
BAB V 70
PENUTUP 70
5.1 Kesimpulan 70
5.2 Saran 71
DAFTAR PUSTAKA 72
DAFTAR RIWAYAT HIDUP 74
LAMPIRAN 75
Lampiran 1 - Surat Pengantar Pengambilan Data 75
Lampiran 2 - Surat Balasan dari Perusahaan 76
Lampiran 3 - Dokumentasi Wawancara 77
Lampiran 4 - Lembar Wawancara 78
Lampiran 5 - Dokumentasi Kegiatan 81

POLITEKNIK NEGERI JAKARTA

© 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

DAFTAR GAMBAR

Gambar 2.1 IDMZ....9
Gambar 2.2 Firewall....10
Gambar 2.3 NAT....10
Gambar 2.4 VLAN....11
Gambar 2.5 PuTTY....12
Gambar 2.6 VPN FortiClient....12
Gambar 2.7 NDLC....15
Gambar 2.8 WSL....19
Gambar 2.9 Linux Ubuntu....19
Gambar 2.10 Raspberry Pi....20
Gambar 2.11 Winbox....21
Gambar 2.12 ISA95/Purdue Model....22
Gambar 3.1 Tahapan Penelitian....24
Gambar 4.1 Topologi Jaringan Existing....30
Gambar 4.2 Rancangan Topologi Jaringan....31
Gambar 4.3 Flowchart User Akses OT....35
Gambar 4.4 PuTTY Remote....36
Gambar 4.5 PuTTY Admin....36
Gambar 4.6 PuTTY Interface....37
Gambar 4.7 Web Interface....37
Gambar 4.8 Menu Interface....38
Gambar 4.9 Create Interface....39
Gambar 4.10 DNS Database....40
Gambar 4.11 DNS Entries....40
Gambar 4.12 Login Page Sesudah DNS....41
Gambar 4.13 Konfigurasi OT_Core....42
Gambar 4.14 Konfigurasi IDMZ Port....43
Gambar 4.15 Firewall Policy....43
Gambar 4.16 Konfigurasi SSL VPN-Settings....44
Gambar 4.17 Konfigurasi SSL VPN Portals....45
Gambar 4.18 Konfigurasi User Groups....45
Gambar 4.19 Firewall Policy VPN to IDMZ....45
Gambar 4.20 Firewall Policy VPN to OT....46
Gambar 4.21 FortiClient VPN....46
Gambar 4.22 Login VPN....47
Gambar 4.23 Login Berhasil....47
Gambar 4.24 Ping Berhasil....48

POLITEKNIK NEGERI JAKARTA

Gambar 4.25 Interface PuTTY.....49
Gambar 4.26 Pengaturan Password.....49
Gambar 4.27 Konfigurasi VLAN.....49
Gambar 4.28 Hasil VLAN.....50
Gambar 4.29 Hasil Ping.....50
Gambar 4.30 Login Winbox.....51
Gambar 4.31 Konfigurasi Address List.....51
Gambar 4.32 Route List.....51
Gambar 4.33 Firewall NAT.....52
Gambar 4.34 Ping Test.....52
Gambar 4.35 Konfigurasi IP Raspberry Pi.....54
Gambar 4.36 Cek IP Raspberry PI.....54
Gambar 4.37 Ping Menuju Zona IDMZ.....54
Gambar 4.38 Grafik Perbandingan Throughput.....59
Gambar 4.39 Grafik Perbandingan Delay.....60
Gambar 4.40 Grafik Perbandingan Jitter.....60
Gambar 4.41 Grafik Perbandingan Packet Loss.....61
Gambar 4.42 Hasil Pengujian 1.....63
Gambar 4.43 Hasil Pengujian 2.....63
Gambar 4.44 Pengujian 3.....64
Gambar 4.45 Pengujian 4.....65
Gambar 4.46 Log Tersimpan.....65
Gambar 4.47 Log VPN Tersimpan.....66
Gambar 4.48 Log Deny.....66

© 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

© 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

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu.....5
Tabel 2.2 Throughput..... 15
Tabel 2.3 Delay..... 16
Tabel 2.4 Jitter..... 17
Tabel 2.5 Packet loss..... 18
Tabel 2.6 Flowchart.....21
Tabel 3.1 List SSID & Gateway.....26
Tabel 4.1 Analisis Kebutuhan Perangkat Keras.....27
Tabel 4.2 Kebutuhan Tools.....28
Tabel 4.3 IP Address..... 32
Tabel 4.4 List Policy Firewall..... 33
Tabel 4.5 Hasil Pengujian QoS Sebelum Implementasi.....56
Tabel 4.6 Hasil Pengujian Sesudah Implementasi..... 58
Tabel 4.7 Analisis Perbandingan QoS.....61
Tabel 4.8 Skenario Pengujian.....66
Tabel 4.9 Analisis Efektivitas Firewall..... 67

© 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

DAFTAR LAMPIRAN

Lampiran 1 - Surat Pengantar Pengambilan Data..... 75
Lampiran 2 - Surat Balasan dari Perusahaan..... 76
Lampiran 3 - Dokumentasi Wawancara..... 77
Lampiran 4 - Lembar Wawancara..... 78
Lampiran 5 - Dokumentasi Kegiatan..... 81

© 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

BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan adalah aspek yang sangat penting dan krusial dalam menjaga keberlangsungan sistem informasi pada suatu perusahaan, terlebih lagi pada industri biofarmasi seperti PT Kalbio Global Medika yang sangat banyak bergantung pada jaringan internal, layanan server, serta komunikasi data untuk banyak menunjang aktivitas operasional sehari-hari. Ketika jaringan yang sifatnya kritikal dapat diakses oleh banyak pengguna, maka akan banyak bermunculan berbagai potensi keamanan, mulai dari akses yang tidak sah, penyalahgunaan akses hingga kebocoran data yang dapat mengganggu bahkan dapat menghentikan proses operasional perusahaan.

Berdasarkan keterangan Bapak Vincent Cunardy dan Bapak Ade Kurnia Rahman (2026) selaku pihak IT di PT Kalbio Global Medika, diketahui bahwa akses menuju ke *endpoint* produksi yang menyimpan banyak data sensitif dan data proses operasional masih tergolong cukup rawan. Hal ini dikarenakan selama perangkat terhubung ke jaringan WiFi internal perusahaan, pengguna akan langsung mengakses jaringan OT yang berada di area produksi hanya dengan mengetahui alamat IP dan port layanan yang berjalan, tanpa adanya pemisahan jaringan dan penyaringan hak akses, kondisi ini akan banyak menimbulkan potensi risiko keamanan yang serius. Selanjutnya dengan penerapan Industrial Demilitarized Zone (IDMZ) diharapkan dapat menciptakan lapisan pemisah keamanan walaupun perangkat sudah terhubung dengan jaringan internal perusahaan.

© 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

Pada lingkungan industri (OT) kebutuhan akan segmentasi jaringan menjadi semakin penting karena sistem OT bersifat kritikal dan akan berdampak langsung terhadap server dan juga mesin produksi. Model ISA-95/Purdue menempatkan Industrial Demilitarized Zone (IDMZ) pada level 3.5 sebagai batas antara jaringan IT dan OT, terutama pada kondisi konektivitas dan integrasi sistem OT dengan sistem enterprise maupun layanan berbasis cloud (Perducat et al., 2023). Penerapan IDMZ ini juga sejalan dengan kebutuhan PT Kalbio Global Medika dalam membangun lapisan keamanan guna memastikan bahwa setiap akses menuju zona produksi dapat dikendalikan secara ketat.

Berdasarkan permasalahan tersebut, penulis mengusulkan penelitian mengenai penerapan arsitektur keamanan jaringan berbasis *Industrial Demilitarized Zone* pada infrastruktur jaringan PT Kalbio Global Medika. Penelitian ini difokuskan pada perancangan segmentasi jaringan yang mewajibkan seluruh akses menuju server produksi melewati zona IDMZ, selanjutnya akan dicatat dalam mekanisme logging pada firewall, meliputi alamat IP pengguna dan waktu akses. Dengan pendekatan ini, diharapkan keamanan jaringan OT akan dapat ditingkatkan melalui kontrol akses yang terstruktur, terpantau, dan terdokumentasi dengan baik.

1.2 Rumusan Masalah

1) Bagaimana merancang arsitektur keamanan jaringan berbasis *Industrial Demilitarized Zone* (IDMZ) untuk membatasi akses langsung menuju endpoint produksi?
2) Bagaimana implementasi kontrol akses berbasis kebijakan menggunakan firewall dan VPN dalam mendukung keamanan jaringan OT?
3) Bagaimana dampak penerapan IDMZ terhadap performa jaringan, ditinjau dari parameter *latency,packet loss, jitter* dan *throughput* ?
4) Bagaimana penerapan mekanisme pencatatan log untuk memantau identitas dan waktu akses terhadap zona produksi?

© 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

1.3 Batasan Masalah

1) Pengujian keamanan dibatasi pada fungsionalitas, uji konektivitas, dan efektivitas pemblokiran akses yang tidak sah
2) Penelitian difokuskan pada perancangan dan analisis struktur keamanan jaringan berbasiskan IDMZ di lingkungan OT PT Kalbio Global Medika
3) Perangkat yang digunakan dalam penelitian ini dibatasi pada perangkat yang tersedia pada rancangan topologi penelitian
4) Pengujian keamanan tidak mencakup metode *Penetration Testing*, *Stress Test* dan *High Traffic Load Test*

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

1) Merancang arsitektur keamanan jaringan berbasis *Industrial Demilitarized Zone* (IDMZ) untuk membatasi akses langsung menuju *endpoint* produksi
2) Mengimplementasikan segmentasi jaringan dan kontrol akses berbasis kebijakan firewall dan VPN untuk meningkatkan keamanan jaringan OT di PT Kalbio Global Medika
3) Menganalisis dampak penerapan IDMZ terhadap performa jaringan berdasarkan parameter *throughput*, *delay*, *jitter* dan *packet loss* mengacu pada standar TIPHON
4) Menghasilkan mekanisme pencatatan log firewall untuk memantau identitas pengguna dan waktu akses terhadap zona produksi

1.4.2 Manfaat

Adapun manfaat yang akan dicapai dari penelitian ini

1) Data dari zona produksi akan semakin aman dikarenakan pemisahan segmentasi jaringan antara jaringan publik , internal dan kritikal
2) Mempermudah proses pemantauan akses jaringan dikarenakan aktivitas yang melewati zona OT akan tercatat melalui mekanisme log pada *firewall*

© 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

1.5 Sistematika Penulisan

Berikut ini adalah sistematika penulisan yang diterapkan dalam proses penyusunan laporan dari penelitian ini, adalah sebagai berikut:

1. BAB I PENDAHULUAN

Bab pertama pendahuluan, pada bagian ini berisikan penjelasan dari latar belakang penelitian. Bagian ini juga akan memuat rumusan, batasan masalah penelitian yang didapat dari latar belakang selanjutnya tujuan dan manfaat dari penelitian yang akan dilakukan

2. BAB II TINJAUAN PUSTAKA

Bab kedua tinjauan pustaka, berisikan beberapa penelitian yang relevan terkait penelitian terdahulu untuk dikaji dalam penelitian ini, serta menjadi landasan teori atau kajian ilmu yang relevan dengan penelitian ini.

3. BAB III METODE PENELITIAN

Bab ketiga metode penelitian, berisikan tentang rancangan penelitian yang akan dilakukan, yakni pemisahan segmentasi jaringan yang akan dilakukan meliputi tahapan penelitian dan objek penelitian

4. BAB IV HASIL DAN PEMBAHASAN

Bab keempat hasil dan pembahasan, membahas tentang evaluasi kebutuhan. Perancangan, implementasi, pengujian dan hasil evaluasi. Evaluasi kebutuhan mencakup identifikasi perangkat keras. Implementasi merupakan tahap penerapan rancangan ke dalam sistem yang telah dibangun. Selanjutnya akan dilakukan pengujian yang meliputi beberapa aspek keamanan hasil dari pengujian tersebut akan dianalisis untuk menilai keberhasilan penerapan sistem yang diusulkan

5. BAB V PENUTUP

Bab kelima penutup, berisikan tentang ringkasan hasil pengujian dari bab sebelumnya, serta menyajikan rekomendasi singkat untuk penelitian berikutnya berdasarkan hasil yang didapatkan.

© 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

BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Penelitian sebelumnya memiliki peran yang sangat penting bagi penulis dalam mewujudkan ide atau gagasan dalam proses penelitian, khususnya apabila penelitian tersebut relevan dengan topik yang akan diamati. Berikut ini merupakan beberapa referensi yang dijadikan penulis sebagai acuan untuk Implementasi & Analisis *Industrial Demilitarized Zone* (IDMZ) pada Infrastruktur Jaringan PT Kalbio Global Medika.

Tabel 2.1 Penelitian Terdahulu

Jurnal	Teknologi dan Cara Kerja	Hasil Penelitian	Catatan
Cybersecurity Threats, Vulnerabilities, Mitigation Measures in Industrial Control and Automation Systems: A Technical Review (Ocaka et al., 2021)	**Tujuan:** Menjabarkan ancaman, kerentanan , standar dan metode mitigasi keamanan siber pada ICAS (SCADA, DCS, PLC, SIS) yang termasuk dalam IT/OT **Teknologi:** *Industrial Demilitarized Zone , Network Segmentation, Filtering Traffic*	IDMZ sangat direkomendasikan sebagai lapisan pertahanan antara zona IT (*Enterprise)* dan OT (*Industrial)* berdasarkan Purdue Reference model level 0-5	**Gap:** Penelitian pada jurnal ini hanya bersifat review teoritis tanpa adanya implementasi *hardware* dan pengujian QoS.

© 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

Demilitarized Network to Secure the Data stored in Industrial Network (Nuñez Alvarez et al., 2021)	**Tujuan:** Mendesain & Mensimulasikan jaringan DMZ dengan 3 *multi-legged firewalls* **Teknologi:** firewall, screened-subnet firewall, *multi-legged firewalls*, *packet filtering*, dan iptables	Konfigurasi DMZ dengan 3 multi-legged firewall berhasil untuk memblokir akses langsung dari jaringan bisnis ke jaringan industri selama proses uji coba selama 6 bulan.	**Gap:** Penelitian ini menggunakan simulasi (Cisco Packet Tracer) dan *Firewall Open-Source* (iptables). Bukan perangkat komersial langsung selain itu tidak ada juga pengujian QoS.
Industrial Network Segmentation Model with Sub-zone and Sub-conduit (Ganesan et al., 2024)	**Tujuan:** Membuat model segmentasi jaringan industri yang mengacu pada ISA/IEC-62443 yang akan membatasi aliran data yang tidak perlu melalui konsep zones & conduits, serta akan menambah detail dengan sub-zone dan	Model sub-zone dan sub-conduit yang dihasilkan memungkinkan untuk membuat kebijakan keamanan hierarki, sub-conduit hanya akan mengizinkan trafik yang telah diizinkan oleh parent conduit	**Gap:** Penelitian ini murni berupa model formal tanpa adanya implementasi dari *hardware* maupun *software* dan tanpa pengujian

© 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

	sub-conduit **Teknologi:** ISA/IEC-62443 zone & conduit, sub-zone, sub-conduit, hierarchical security policy		
Evolution and trends of cloud on industrial OT network (Perducat, M., et al.,2023)	**Tujuan:** Menunjang koneksi antar cloud ke OT dengan mengurangi attack surface,lalu DMZ dipakai menjadi zona penyangga sehingga server yang perlu komunikasi tidak terkekspos ke jaringan luar **Teknologi:** Industrial DMZ (Level 3.5) + Port Knocking	ISA-95 dengan model IDMZ yang konvensional ditemukan mulai tidak memadai untuk ekosistem hybrid cloud. IDMZ level 3.5 tetap relevan sebagai garis demarkasi antara IT dan OT namun perlu adanya kombinasi dengan pendekatan *zero-trust*	**Gap:** Penelitian ini bersifat tinjauan strategis atau futuristik tanpa adanya implementasi teknis dan tanpa pengujian kuantitatif
An archetype for mitigating the security threats in	**Tujuan:** Untuk mengurangi ancaman	Topologi NGFW *multi-cloud* lebih konsisten untuk	**Gap:** Penelitian ini berfokus pada lingkungan pada

© 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

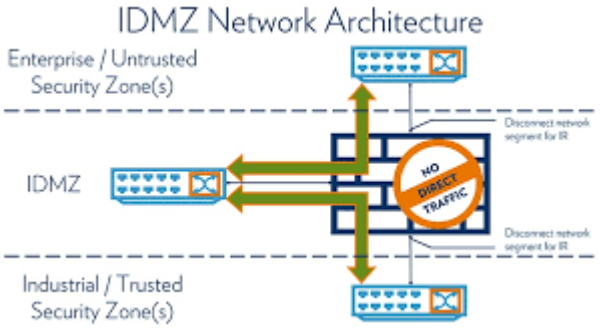
multi-cloud environment by implementing tree-based next-generation firewalls (Hussain et al., 2021)	keamanan dilingkungan multi-cloud dengan pengamanan yang berlapis lapis memakai Next-Generation Firewall (NGFW) dan konsep DMZ **Teknologi:** Tree-based NGFW + DMZ sebagai zona pemisah	menjaga *Throughput* (71.09% pada 4096 rules) dibandingkan dengan implementasi (51.35% Hyper-V , 35.15% ESXi) NGFW dapat mengatasi kelemahan single firewall pada skala yang besar	multi-cloud menggunakan virtual firewall tanpa hardware fisik dan juga tidak mengukur parameter keamanan akses antar zona

2.2 Industrial Demilitarized Zone (IDMZ)

Industrial Demilitarized Zone (IDMZ) adalah sebuah zona / segmentasi jaringan perantara yang berfungsi sebagai *barrier* antara jaringan OT "*trusted*" dan jaringan IT "*untrusted*", sehingga akses langsung dari jaringan luar tidak dapat langsung dilakukan menuju aset OT yang sifatnya kritikal. IDMZ umumnya diterapkan melalui mekanisme seperti *firewall* dan segmentasi jaringan agar memastikan hanya koneksi yang diperlukan dan terverifikasi yang bisa melintas, dan tujuannya jelas untuk mengurangi risiko ancaman , serta mencegah segala bentuk akses yang tidak sah terhadap aset kritikal (Perducat et al., 2023)

© 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



Gambar 2.1 IDMZ

2.3 Firewall

Firewall adalah perangkat keamanan jaringan yang fungsinya untuk memfilter atau menyaring lalu lintas dan juga mengendalikan akses berdasarkan aturan yang ada, sehingga hanya trafik yang diizinkan atau yang sesuai dengan aturan saja yang dapat melintas antar segmentasi jaringan. Dalam lingkungan jaringan yang dinamis (contoh *multi-cloud*), firewall tradisional dinilai kurang memadai untuk dapat menangani kompleksitas dan trafik yang tinggi, sehingga dibutuhkan *Next Generation Firewall* (NGFW) yang mampu melakukan kontrol secara lebih transparan , mengintegrasikan *intrusion prevention system* (IPS) , menerapkan *filtering device* dan juga application awareness untuk meningkatkan sistem keamanan (Hussain et al., 2021). Dalam implementasi keamanan jaringan di lingkungan kehidupan sehari hari, penggunaan *firewall* berbasis perangkat keras seperti FortiGate terbukti efektif dalam upaya mengatur lalu lintas jaringan melalui mekanisme *security profiles* , *web filtering* , dan juga *application control* yang memungkinkan administrator menetapkan kebijakan secara granular (Arbie dan Raharjo, 2024). Lebih lanjut lagi menurut (Arslan dan Firdaus, 2026) menunjukkan bahwa implementasi *Firewall hardware* Fortinet pada infrastruktur jaringan institusi mampu mengendalikan lalu lintas data secara real-time dan selain itu juga meminimalisir potensi ancaman siber melalui pemantauan trafik yang berkelanjutan.

© Hak Cipta milik Politeknik Negeri Jakarta

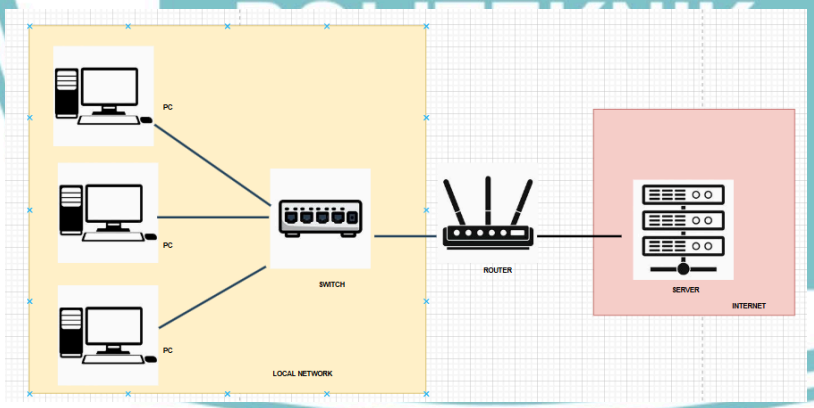
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 2.2 Firewall

2.4 Network Address Translation (NAT)

Network Address Translation (NAT) adalah proses memetakan alamat IP privat ke IP Public ataupun sebaliknya. NAT memiliki peran yang sangat penting dalam implementasi IDMZ karena bisa berfungsi sebagai penghubung antara jaringan internal , IDMZ dan jaringan publik. Selain itu NAT bisa digabungkan atau dikombinasikan dengan pembatasan akses port/protokol sehingga hanya layanan yang diizinkan yang bisa mengakses ke zona IDMZ, sementara akses langsung ke server yang sifatnya kritikal di jaringan internal harus tetap dicegah karena setiap permintaan / request harus melewati proses translasi oleh aturan yang telah ditentukan (Anggraeni dan Jasa, 2022).



Gambar 2.3 NAT

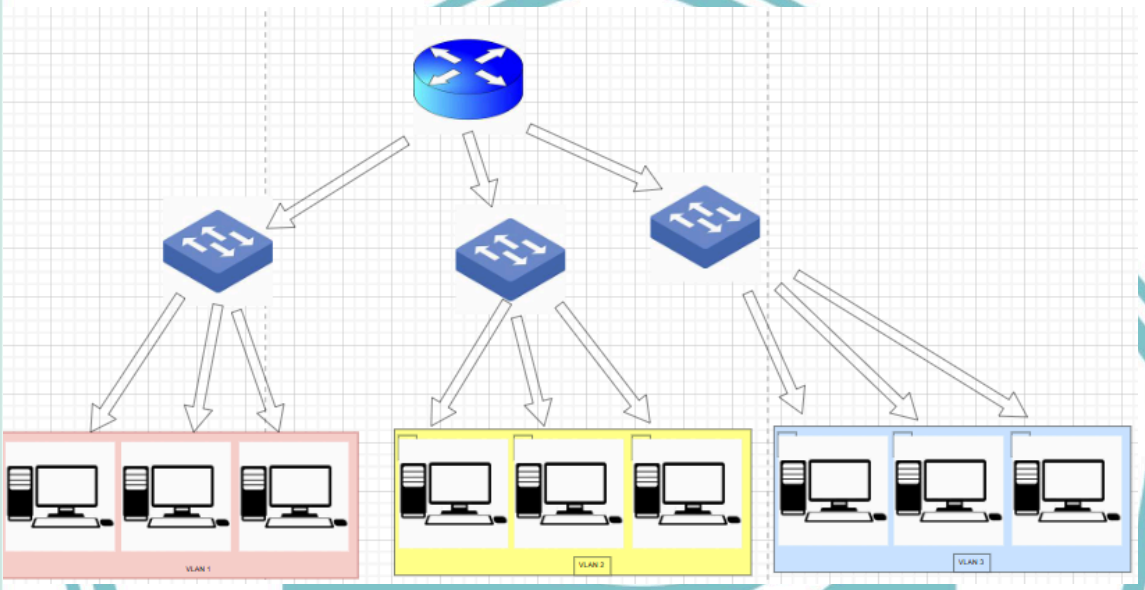
2.5 *Virtual Local Area Network* (VLAN)

Virtual Local Area Network (VLAN) merupakan suatu teknik pemisahan jaringan secara logis yang digunakan untuk mengelompokkan perangkat ke dalam segmen jaringan yang berbeda walaupun masih pada infrastruktur fisik yang sama. Dalam

© 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

kasus IDMZ VLAN umumnya digunakan untuk membentuk segmentasi antar zona antara IT,IDMZ,OT dan juga menetapkan jalur akses yang terkontrol menjadikan hanya trafik yang diizinkan yang bisa melintas untuk menuju ke layanan tertentu. Pendekatan segmentasi ini juga sejalan dengan peran IDMZ yang menjadikan *barrier* antara jaringan OT yang dikenal "*trusted*" dan jaringan "IT" yang kita kenal "*untrusted*" (Perducat et al., 2023)



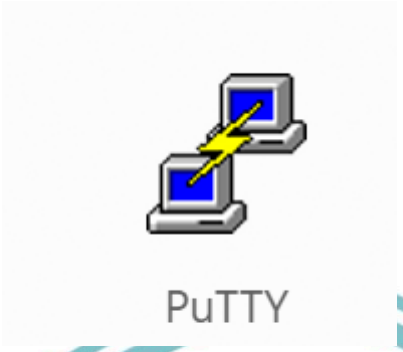
Gambar 2.4 VLAN

2.6 PuTTY

PuTTY merupakan aplikasi terminal untuk remote login yang fungsinya untuk mengakses dan konfigurasi perangkat atau server dari jarak jauh, utamanya melalui protokol SSH atau bisa juga dari Telnet/Serial. Dalam penelitian DMZ dan Port Knocking, PuTTY berfungsi untuk pengujian koneksi via remote dari client windows ke router / server setelah rule akses yang sudah diterapkan (Saputro et al., 2020)

© 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



Gambar 2.5 PuTTY

2.7 Virtual Private Network (VPN)

Virtual Private Network (VPN) adalah teknologi yang digunakan untuk komunikasi yang aman, pengguna jarak jauh tetap dapat mengakses ke layanan internal dengan perlindungan enkripsi dan kontrol akses. Pada lingkungan multi cloud VPN menjadi bagian dari "*secure fabric*" yang berfungsi untuk menjaga keamanan konektivitas jaringan, berdampingan dengan network security dan access control.(Hussain et al., 2021). Pada implementasi keamanan jaringan berbasiskan *FortiGate*, VPN dapat langsung diintegrasikan dengan kebijakan *firewall* melalui mekanisme SSL-VPN yang memungkinkan pengguna dari luar zona atau jaringan dapat mengakses ke suatu zona tertentu secara lebih aman berdasarkan aturan akses yang telah ditetapkan oleh administrator (Arbie dan Raharjo, 2024).



Gambar 2.6 VPN FortiClient

2.8 Network Development Life Cycle (NDLC)

Network Development Life Cycle (NDLC) adalah pendekatan dari pengembangan jaringan yang dilakukan secara bertahap dan berurutan untuk memastikan jaringan

© 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

yang akan dibangun bisa sesuai dengan kebutuhan, dan diimplementasikan dengan benar. NDLC ini menekankan pada pelaksanaan rangkaian proses pembangunan jaringan secara sistematis dan sekuensial, mulai dari tahap pengumpulan data hingga tahap pengelolaan jangka panjang. Penggunaan metode NDLC akan menjamin seluruh rangkaian penelitian dan pengembangan dilaksanakan secara terstruktur , sistematis dan terarah. Menurut Murad, Kurniawan dan Rasyidin (2025) implementasi NDLC terdiri dari 6 tahap utama yang saling berkesinambungan, yaitu:

1. Analisis

   Tahap ini bertujuan untuk menganalisis kebutuhan sistem, permasalahan yang dihadapi, harapan pengguna, dan pemilihan topologi jaringan yang paling sesuai. Data yang diperoleh dijadikan dasar untuk merumuskan masalah utama yang harus dipecahkan, khususnya terkait keamanan jaringan. Proses analisis juga melibatkan identifikasi sistem jaringan yang sedang digunakan, sehingga dapat memberikan gambaran awal mengenai pengembangan sistem yang akan diterapkan di masa depan. Hasil identifikasi ini mempermudah perencanaan sistem yang sesuai dengan kebutuhan.

2. Desain

   Pada tahap desain, dilakukan perancangan topologi jaringan keamanan berdasarkan kondisi jaringan saat ini. Proses desain melibatkan pembuatan diagram dan rancangan teknis yang akan menjadi acuan untuk implementasi berikutnya. Langkah ini bertujuan memastikan sistem dirancang secara efektif untuk memenuhi standar keamanan yang dibutuhkan.

3. Simulasi

   Setelah desain selesai, dilakukan simulasi untuk memvisualisasikan cara kerja sistem yang telah dirancang. . Tujuan simulasi adalah untuk menguji performa awal sistem serta menilai sejauh mana sistem yang dirancang dapat memenuhi kebutuhan dan menghadapi skenario penggunaan yang telah diprediksi.

4. Implementasi

© 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

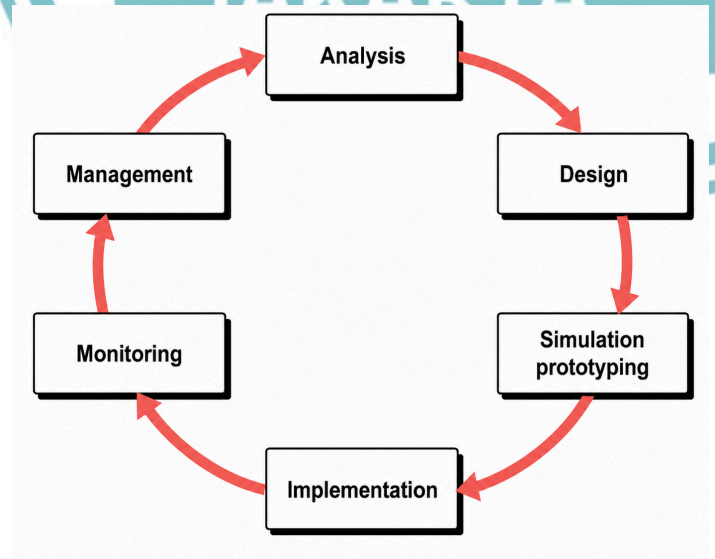
Tahap implementasi melibatkan penerapan sistem yang telah dirancang ke dalam jaringan yang sedang berjalan. Proses ini membutuhkan waktu yang relatif lama karena mencakup instalasi, konfigurasi, dan integrasi dengan sistem yang ada. Melalui tahap ini, akan terlihat bagaimana sistem yang baru berfungsi dalam lingkungan nyata, serta potensi perbaikan yang diperlukan untuk menyempurnakan kinerjanya.

5. Monitoring

   Setelah sistem diterapkan, dilakukan pemantauan secara berkala untuk mengevaluasi performa dan stabilitasnya. Tahap ini penting untuk memastikan sistem mampu menghadapi berbagai ancaman keamanan. Administrator jaringan bertugas mengawasi lalu lintas data, memeriksa kelancaran sistem, dan memastikan semua transaksi data berjalan dengan aman. Pemantauan ini juga bertujuan mendeteksi potensi kelemahan yang mungkin muncul.

6. Manajemen

   Pada tahap akhir, dilakukan pengelolaan dan pemeliharaan sistem untuk menjamin keberlangsungan operasionalnya. Sistem yang telah diterapkan perlu dirawat dengan baik agar tetap stabil dan mampu berfungsi dalam jangka panjang. Jika ditemukan kerentanan atau masalah keamanan, perbaikan dilakukan secara optimal, dan jika diperlukan, implementasi ulang dapat dilakukan. Tahap ini memastikan sistem tetap relevan dan aman dari potensi ancaman di masa mendatang.



© 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

Gambar 2.7 NDLC

2.9 Quality of Service (QoS)

Penelitian QoS dalam penelitian ini mengacu pada standar Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) yang membagi kualitas jaringan menjadi empat parameter utama yaitu *Throughput,Delay,Jitter,* dan *packet loss* (Aryandi et al., 2023). *Quality of Service* adalah cara penilaian seberapa baik suatu komunikasi pada jaringan komputer sebagai usaha untuk mengukur karakteristik dari suatu layanan. *Qos* digunakan untuk menilai kumpulan *field* kinerja yang sudah ditentukan pada suatu layanan, mengacu dari kapabilitas jaringan dalam melayani di dalam suatu trafik.(I. B. A. E. M. Putra et al., 2021). Berikut adalah pengertian dari parameter *QoS* dalam persentase penilaian *QoS* berdasarkan Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON).

1) *Throughput*

   Throughput merupakan *bandwidth* yang diukur dalam satuan waktu tertentu dalam proses mentransmisikan sebuah *file*. *Throughput* menggambarkan total dari kedatangan paket yang sukses pada interval waktu tertentu dan dibagi dengan durasi interval waktu tersebut.

Tabel 2.2 Throughput

Kategori *Throughput*	Throughput	Indeks
Sangat Baik	>2.1 Mbps	4
Baik	1200 kbps - 2.1 Mbps	3
Cukup	700 - 1200 kbps	2
Kurang Baik	338 - 700 kbps	1
Buruk	0-338 kbps	0

Berdasarkan Tabel 2.2, nilai *throughput* bisa dikategorikan sangat baik apabila lebih dari 2.1 Mbps, baik dalam rentang 1200 Kbps - 2.1 Mbps, cukup 700 - 1200 Kbps, dan kurang baik 338 - 700 Kbps, dan buruk apabila dibawah 0-338 Kbp.

© 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

Standar ini menetapkan kategori sangat baik tanpa batas atas sehingga nilai yang melebihi 2.1 Mbps tetap masuk dalam kategori sangat baik (Aryandi et al., 2023).Berikut ini merupakan rumus untuk menghitung Throughput:

$$\text{Throughput} = \frac{Jumlah\ data\ yang\ dikirim\ (kb)}{Waktu\ pengiriman\ data\ (s)}$$

2) *Delay*

Delay merupakan sebuah parameter yang menunjukkan total waktu yang dibutuhkan bagi paket dalam menempuh jarak dari *source* ke *destination.* Ada beberapa hal yang bisa mempengaruhi delay, yaitu perangkat keras, jarak dan *congestion*

Tabel 2.3 Delay

Kategori Delay	Delay	Indeks
Sangat Baik	<150 ms	4
Baik	150 ms - 300 ms	3
Sedang	300 ms - 450 ms	2
Tidak Baik	>450 ms	1

Berdasarkan Tabel 2.3, nilai delay dikategorikan sangat baik apabila berada di bawah 150 ms, baik apabila berada pada rentang 150 ms hingga 300 ms, cukup apabila berada pada rentang 300 ms hingga 450 ms, kurang baik apabila berada pada rentang 450 ms hingga 600 ms, dan buruk apabila melebihi 600 ms. Semakin kecil nilai delay yang diperoleh, semakin cepat paket data sampai ke tujuan, yang mengindikasikan semakin baik responsivitas jaringan tersebut (Aryandi et al., 2023).Berikut adalah rumus yang digunakan untuk menghitung rata-rata delay:

$$\text{Rata-rata Delay} = \frac{Jumlah\ Delay}{Jumlah\ Paket\ Diterima}$$

3) *Jitter*

© 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

Jitter merupakan hal yang sangat berhubungan dengan latency, yang menjelaskan banyaknya variasi delay dalam proses transmisi data di dalam suatu jaringan. *Delay* antrian dalam *router* atau *switch* yang akan menghasilkan *jitter*. Hal ini bisa terjadi karena ragam variasi waktu dalam mengolah suatu data, panjang antrian beserta waktu perhimpunan ulang terhadap paket pada akhir transmisi *jitter*

Tabel 2.4 *Jitter*

Kategori *Jitter*	*Jitter*	Indeks
Sangat Baik	0 ms	4
Baik	0 ms - 75 ms	3
Sedang	75 ms - 125 ms	2
Tidak Baik	125 ms - 225 ms	1

Berdasarkan Tabel 2.4, nilai *jitter* dikategorikan sangat baik apabila bernilai 0 ms, baik apabila berada pada rentang 0 ms hingga 75 ms, cukup apabila berada pada rentang 75 ms hingga 125 ms, kurang baik apabila berada pada rentang 125 ms hingga 225 ms, dan buruk apabila melebihi 225 ms. Nilai *jitter* yang mendekati 0 ms menunjukkan bahwa waktu tempuh antar paket sangat konsisten, yang mencerminkan kestabilan jaringan dalam mengirimkan data secara berurutan. Sebaliknya, nilai *jitter* yang tinggi dapat menyebabkan gangguan pada layanan yang sensitif terhadap keterlambatan seperti komunikasi *real-time* dan monitoring sistem produksi (Aryandi et al., 2023). Rumus Pengukuran Jitter sebagai berikut :

$$\text{Jitter} = \frac{Jumlah\ Variasi\ Delay}{Jumlah\ Paket\ Diterima}$$

4) *Packet loss*

Packet loss merupakan sebuah parameter yang menggambarkan suatu keadaan total paket yang hilang, hal ini bisa terjadi karena disebabkan

© 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

collision serta *congestion* di dalam suatu jaringan. Hal ini juga bisa berpengaruh pada seluruh sistem sebab akan mengurangi efisiensi pada jaringan dengan keseluruhan.

Tabel 2.5 *Packet loss*

Kategori *Packet loss*	*Packet loss*	Indeks
Sangat Baik	0%	4
Baik	3%	3
Sedang	15%	2
Tidak Baik	25%	1

Berdasarkan Tabel 2.5, nilai *packet loss* dikategorikan sangat baik apabila bernilai 0%, baik apabila berada pada 3%, cukup apabila berada 15%, kurang baik apabila pada 25%, dan buruk apabila melebihi 25%. Nilai *packet loss* 0% menunjukkan bahwa seluruh paket yang dikirimkan berhasil diterima oleh tujuan tanpa ada yang hilang selama proses transmisi. Kondisi ini sangat kritis dalam lingkungan jaringan OT karena kehilangan paket data yang membawa informasi proses produksi dapat berdampak langsung pada keandalan sistem kendali dan monitoring instrumen di area produksi (Aryandi et al., 2023). Penghitungan Rumus Pengukuran seperti dibawah ini.

$$\text{Packet Loss} = \frac{Paket\ Data\ Dikirim - Paket\ Data\ Diterima}{Paket\ Data\ Dikirim} \text{ x } 100\%$$

2.10 Windows Subsystem for Linux (WSL)

Windows Subsystem for Linux atau yang biasa dikenal dengan WSL adalah sebuah fitur pada sistem operasi windows yang akan memungkinkan penggunanya menjalankan lingkungan linux diatas windows. Pada WSL 2, sistem menggunakan arsitektur berbasis virtual machine dengan kernel linux penuh, dengan demikian kompatibilitas dan dari segi performanya akan lebih baik dibandingkan dengan versi WSL sebelumnya. Hal ini yang membuat WSL

© 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

digunakan dalam kebutuhan administrasi sistem yang membutuhkan tool linux di lingkungan windows



Gambar 2.8 WSL

2.11 Linux Ubuntu

Ubuntu merupakan salah satu distro linux yang banyak digunakan sebagai sistem operasi pada suatu lingkungan komputasi/server karena sifatnya *open source* dan *fleksibel* (Nasrullah et al,. 2025). Linux ini sangat relevan untuk digunakan sebagai sistem operasi dalam proses pengujian jaringan contohnya pada penelitian (Kurnadi,2024) yang menggunakan ubuntu 22.04 pada WSL 2 sebagai objek penelitian.



Gambar 2.9 Linux Ubuntu

2.12 Raspberry Pi

Raspberry Pi adalah sebuah komputer yang berukuran mini yang banyak digunakan untuk berbagai kebutuhan komputasi dan proyek elektronik (Fernando,

© 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

Jasa dan Hartati 2022). Pada penelitian ini Raspberry Pi digunakan sebagai endpoint produksi yang terhubung langsung dengan instrumen instrumen yang ada di produksi dan lab, sehingga berperan sebagai bagian dari segmentasi jaringan produksi yang aksesnya akan dibatasi melalui implementasi *Industrial Demilitarized Zone* (IDMZ).



Gambar 2.10 Raspberry Pi

2.13 Winbox

Winbox adalah sebuah aplikasi yang berbasis *Graphical User Interface* (GUI) yang digunakan untuk melakukan konfigurasi perangkat jaringan Mikrotik secara langsung melalui interface ethernet maupun IP, sehingga bisa memudahkan administrator untuk melakukan setting firewall , NAT ,VLAN serta membangun segmentasi jaringan IDMZ. Winbox merupakan layanan manajemen yang umumnya menggunakan TCP 8291, aksesnya perlu dikontrol dengan ketat agar tidak menjadi celah keamanan , salah satu cara pendekatannya adalah dengan cara menutup (blocking) port winbox dari akses umum dan hanya mengizinkan akses yang terkontrol, contohnya adalah metode port knocking yang skema nya adalah membuka akses setelah ada “tanda” tertentu sehingga port manajemen tidak mudah terdeteksi apabila ada pemindaian (port scanning) (Saputro et al., 2020)

© 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



Gambar 2.11 Winbox

2.14 *Flowchart*

Flowchart atau yang kita kenal dengan Bagan alir merupakan teknik analitis gambar yang digunakan untuk mempresentasikan alur atau langkah dalam sebuah proses secara visual, yang bertujuan untuk memberikan informasi secara jelas dan ringkas. Dengan demikian *flowchart* akan sangat berguna untuk memahami, menganalisis dan menyederhanakan proses atau sistem. (Tuasamu et al., 2023).

Tabel 2.6 Flowchart

No	Simbol	Nama	Fungsi
1		Arus/*Flow*	Untuk menyatakan jalannya suatu proses.
2		*Connector*	Menyatakan sambungan dalam satu proses ke proses lainnya pada halaman yang sama
3		Proses	Fungsi pemerosesan yang dilakukan pada sistem, untuk menghasilkan perubahan data atau informasi

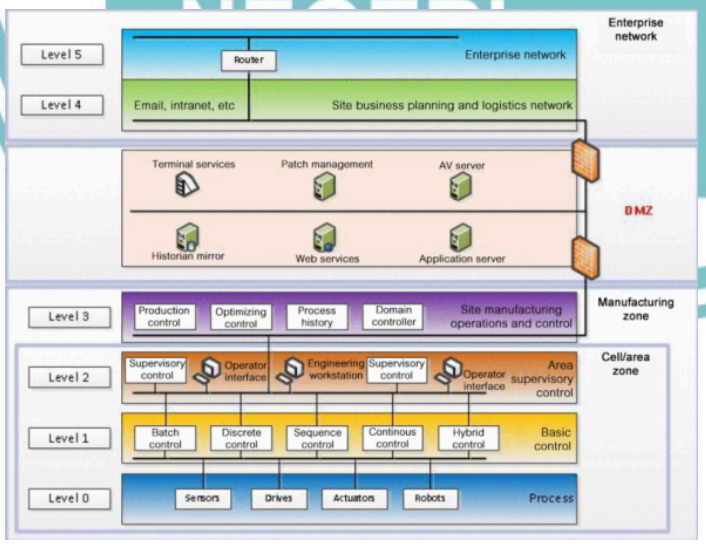
© Hak Cipta milik Politeknik Negeri Jakarta

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

4		*Decision/Kondisi*	Menunjukkan dua kondisi tertentu dengan dua kemungkinan, yaitu ya atau tidak.
5		Terminal	Menyatakan mulai dan berakhirnya suatu program.
6		*Input / Output*	Menyatakan proses input dan output

2.15 ISA 95/Purdue Model

Dalam lingkungan Operational Technology (OT), arsitektur jaringan sering direferensikan terhadap model hierarkis ISA-95 / Purdue Model. (Perducat et al., 2023). Tujuannya adalah menstandarkan komunikasi antar subsistem dalam lingkungan manufaktur sehingga perancang sistem dapat mengandalkan aturan dan praktik terbaik yang dapat diprediksi dan *scalable*. Model ISA-95 membagi jaringan industri menjadi enam level yang disusun secara hierarkis, seperti ditunjukkan pada Gambar 2.12. Setiap level memiliki fungsi dan tingkat kepercayaan keamanan yang berbeda.



Gambar 2.12 ISA95/Purdue Model

© 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

BAB III

METODE PENELITIAN

3.1 Rancangan Penelitian

Penelitian dilakukan berfokus pada implementasi dan analisis *Industrial Demilitarized Zone* (IDMZ) pada infrastruktur jaringan PT Kalbio Global Medika hal ini dimaksudkan sebagai upaya meningkatkan keamanan akses terhadap zona produksi. Kondisi awal jaringan masih memungkinakan untuk mengakses langsung menuju layanan zona produksi ketika terhubung ke dalam jaringan WiFi internal, sehingga tidak ada pembatasan ataupun pemisahan zona keamanan antara pengguna internal/IT , tamu , magang , dan juga sistem produksi. Oleh karena itu , penelitian ini merancang struktur jaringan baru dengan memanfaatkan segmentasi IDMZ, firewall, NAT, dan VLAN agar akses menuju zona produksi bisa melalui proses verifikasi dan validasi terlebih dahulu.

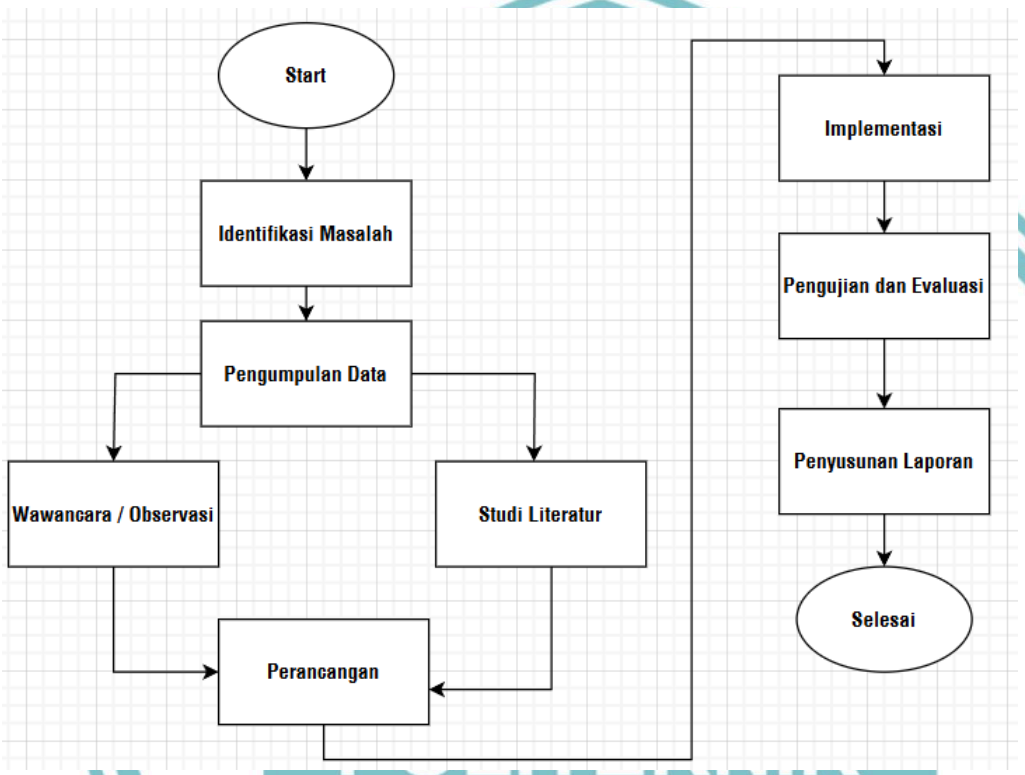
Rancangan diawali dengan pemetaan kebutuhan jaringan kemudian dilanjutkan dengan pembagian *interface* pada firewall menjadi tiga segmen utama. Pada tahap implementasi konfigurasi dilakukan dengan menggunakan FortiGate GUI Interface untuk pengaturan *policy*, pembuatan vlan , konfigurasi NAT dan juga port forwarding. Evaluasi dilakukan melalui tiga aspek pengujian. Pertama, pengujian untuk melihat seberapa besar persentase firewall mampu untuk memblokir akses yang tidak sah. Kedua, dilakukan pengujian performa jaringan sebelum dan sesudah implementasi IDMZ seperti throughput, latency, jitter dan packet loss. Ketiga, dilakukan pengujian pencatatan log firewall untuk memastikan setiap trafik yang melewati firewall bisa menjadi bukti audit. Penelitian ini menggunakan pendekatan kuantitatif, hal ini disebabkan karena evaluasi keberhasilan diukur dari parameter terukur berdasarkan standar TIPHON, serta persentase efektivitas pemblokiran firewall yang dihitung secara numerik.

© 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

3.2 Tahapan Penelitian

Pada penelitian ini, Penulis menyusun alur pelaksanaan penelitian secara sistematis agar tahapan penelitian yang akan dilakukan bisa berjalan sesuai dengan tujuan penelitian. Adapun alur tahapan penelitian dapat dilihat pada gambar 3.1



Gambar 3.1 Tahapan Penelitian

Tahapan penelitian menjelaskan tahapan yang dilakukan oleh penulis dalam penelitian, berikut ini adalah penjelasan dari flowchart pada gambar 3.1

1. Identifikasi Masalah

   Identifikasi masalah adalah langkah pertama dari proses sebuah penelitian, Dimana penulis menentukan masalah dan topik yang akan diteliti, dan akan memberikan solusi sebagai solusi dari tanggapan masalah tersebut. Pada langkah ini juga penulis melakukan pengamatan situasi untuk menemukan masalah yang signifikan. Tujuannya agar dari identifikasi masalah tersebut penulis bisa memastikan bahwa kegiatan penelitian berfokus yang jelas dan juga spesifik, selanjutnya bisa dijadikan sebagai acuan atau pondasi dari seluruh proses penelitian yang akan dikerjakan.

2. Pengumpulan Data

   Pengumpulan data adalah langkah selanjutnya sekaligus langkah yang penting dalam memperoleh seluruh informasi yang dibutuhkan untuk menjawab penelitian. Data bisa dikumpulkan melalui berbagai mekanisme seperti wawancara, observasi dan juga studi literatur. Wawancara memungkinkan penulis dapat pemahaman baru dari seorang narasumber, observasi memberikan kesempatan untuk mengamati kondisi secara nyata pada tempat penelitian sedangkan studi literatur untuk mencari referensi dan membangun proses penelitian yang berkaitan dengan topik terdahulu.

3. Wawancara dan Observasi

   Wawancara adalah proses penulis untuk menggali informasi yang bersangkutan dengan object yang akan diteliti, sedangkan observasi adalah pengamatan secara langsung terkait dengan kondisi yang ada di tempat penelitian.

4. Perancangan

   Tahapan ini dilakukan perancangan dan realisasi berdasarkan hasil wawancara , observasi dan studi literatur. Sehingga bisa tercapainya tujuan dan manfaat pada saat proses realisasi

5. Implementasi

   Pada tahap ini akan membuat sistem sesuai dengan rancangan yang sudah dibangun sebelumnya.

6. Pengujian dan Evaluasi

   Pada tahap ini sistem yang sudah dibuat akan diuji sesuai dengan kriteria dan akan diuji sesuai dengan fungsionalitas. Selain itu juga hasilnya akan dianalisis dan dievaluasi yang bertujuan untuk mengetahui kekurangan yang akan dijadikan pada penelitian selanjutnya.

7. Penyusunan Laporan Penelitian

   Ini adalah tahap terakhir dari sebuah penelitian dan akan disertai dengan adanya dokumentasi.

© 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

© 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

3.3 Objek Penelitian

Objek pada penelitian ini adalah infrastruktur jaringan PT Kalbio Global Medika, khususnya jalur akses dari jaringan internal/IT menuju endpoint/zona produksi. Berdasarkan hasil wawancara dan observasi, kondisi saat ini belum memiliki pemisahan jaringan / zona keamanan yang jelas. Seluruh pengguna yang terhubung ke jaringan WiFi internal baik Office, Tamu, Intern, berada dalam satu jaringan dengan sistem zona produksi sehingga akses langsung menuju endpoint produksi masih sangat mudah dilakukan tanpa melalui mekanisme verifikasi apapun. Hasil observasi terhadap jaringan WiFi yang berada pada jaringan PT Kalbio Global Medika berada pada tabel 3.1 berikut

Tabel 3.1 List SSID & Gateway

Nama SSID	Gateway
ONEKalbe.net	10.125.4.xxx
Kalbio	10.125.4.xxx
Kalbio_intern	192.168.126.xxx
Kalbe_guest	192.168.200.xxx

Kondisi tersebut menimbulkan risiko keamanan yang cukup serius mulai dari potensi kebocoran data, penyalahgunaan akses, hingga penyerangan terhadap device pada sistem OT yang sifatnya kritikal. Oleh karena itu, objek yang menjadi fokus implementasi pada penelitian ini mencakup konfigurasi perangkat jaringan, segmentasi jaringan serta hasil evaluasinya dilihat dari perbandingan performa jaringan dengan parameter QoS sebelum dan sesudah implementasi IDMZ, efektivitas pemblokiran akses yang tidak sah dan pencatatan pada log firewall.

© 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

BAB IV
HASIL DAN PEMBAHASAN

4.1 Analisis Kebutuhan

Pada tahap ini dilakukan seluruh identifikasi terhadap kebutuhan untuk mendukung implementasi penelitian, kebutuhan tersebut meliputi spesifikasi perangkat keras yang akan digunakan sebagai komponen utama serta *tools* pendukung yang diperlukan mulai dari proses konfigurasi dan pengujian. Analisis ini bertujuan agar implementasi IDMZ dapat berjalan sesuai dengan rancangan dan memenuhi target yang diharapkan. Berdasarkan hasil wawancara dan observasi di PT Kalbio Global Medika, implementasi IDMZ memerlukan 5 perangkat keras utama. Firewall FortiGate yang fungsinya untuk melakukan segmentasi zona dan mengatur lalu lintas jaringan. Switch manageable untuk distribusi trafik sekaligus memisahkan segmen antar jaringan. Selain itu, Raspberry Pi 3B+ juga berperan sebagai representasi dari endpoint produksi yang terhubung ke Mikrotik RB750Gr3. Mikrotik disini berfungsi sebagai NAT router yang menghubungkan zona OT dengan subnet *endpoint*.

4.1.1 Analisis Kebutuhan Perangkat Keras

Berikut ini adalah perangkat keras yang digunakan dalam penelitian implementasi dan analisis IDMZ pada infrastruktur jaringan PT Kalbio Global Medika.

Tabel 4.1 Analisis Kebutuhan Perangkat Keras

Perangkat Keras	Fungsi	Spesifikasi
Firewall Fortinet (FortiGate)	Sebagai pusat konfigurasi keamanan jaringan, *firewall policy* dan segmentasi antar zona	18x GE RJ45 , 8x GE SFP , 4x 10GE SFP+
Switch Managable	Menghubungkan perangkat jaringan dan mendukung pemisahan zona jaringan	6x modular slots (vl modules) , Up to 144x 1G RJ45 / SFP ports or 24x 10G uplinks (modular dependent) , 1x

© 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

		fan tray (redundant cooling)
Raspberry PI 3 B+	Menjadi endpoint pada jaringan OT yang harus dipisahkan dari jaringan internal	Broadcom BCM2837B0, quad-core 64-bit ARM Cortex-A53 @ 1.4GHz , 1GB LPDDR2 SDRAM. , dual-band 2.4GHz & 5GHz 802.11 b/g/n/ac, Bluetooth 4.2 + BLE.
Laptop Lenovo Ideapad Gaming 3	Melakukan konfigurasi	AMD Ryzen 7 5800H , Nvidia Geforce RTX 3050 , 16GB
Mikrotik RB750Gr 3	Menjadi perangkat NATR	5× Gigabit Ethernet (10/100/1000) , MediaTek MT7621A, 2 core / 4 thread, 880 MHz , 2 input (DC jack + PoE-in), 8–30 V, passive PoE-in; max power 10 W

4.1.2 Analisis Kebutuhan Tools

Selain perangkat keras, penelitian ini juga menggunakan beberapa *tools* pendukung dalam proses konfigurasi, implementasi dan pengujian.

Tabel 4.2 Kebutuhan Tools

Tools	Fungsi
FortiGate GUI	Digunakan untuk melakukan konfigurasi Firewall Policy , VLAN Settings , Routing, SSL-VPN, DNS
WSL2 Ubuntu	Digunakan untuk lingkungan pengujian parameter QoS jaringan
Iperf3	Mengukur kualitas bandwidth / throughput pada jaringan
Ping	Mengukur konektivitas dari segi delay / latency
Command Prompt (CMD)	Menjalankan perintah pengujian pada

© 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

	jaringan
PuTTY	Mengakses perangkat jaringan melalui terminal
Winbox	Melakukan konfigurasi NAT untuk perangkat controller pada zona level 0-2

4.2 Perancangan Sistem

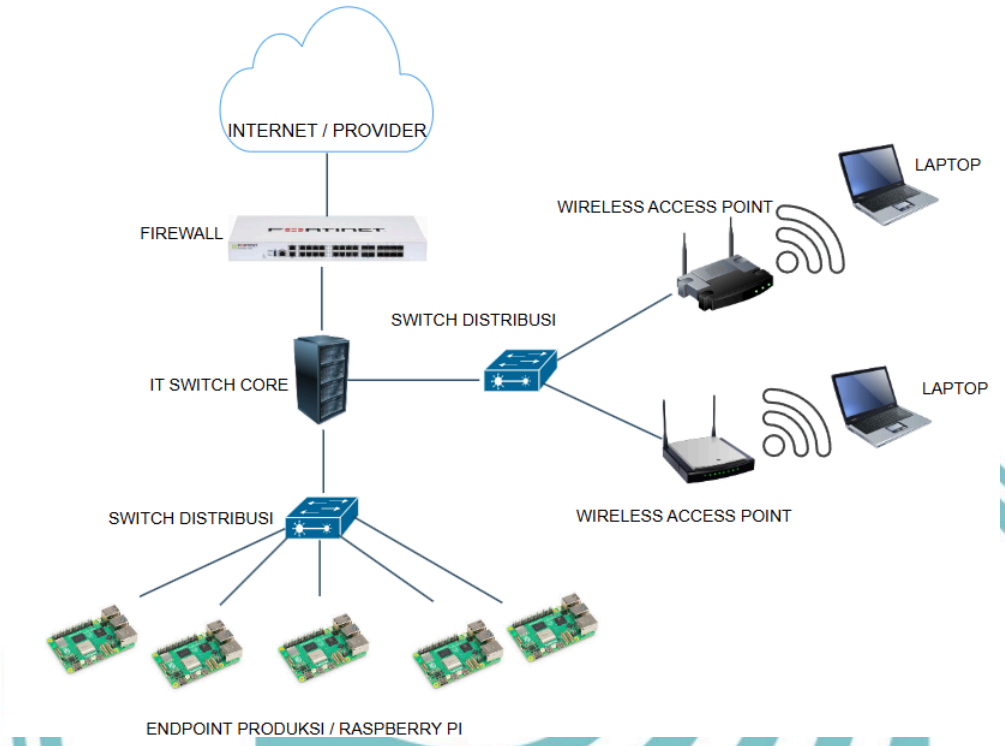
Perancangan sistem fungsinya untuk menyusun arsitektur jaringan baru yang menerapkan konsep Industrial Demilitarized Zone (IDMZ) sebagai zona perantara antara jaringan Internal/IT dengan jaringan *Operational Technology* (OT). Perancangan mencakup pemetaan topologi eksisting,rancangan topologi baru, perencanaan alamat IP, Penyusunan daftar kebijakan *firewall* , serta flowchart akses pengguna menuju zona OT.

4.2.1 Topologi Jaringan Eksisting

Topologi jaringan eksisting di PT Kalbio Global Medika adalah kondisi awal sebelum diterapkannya IDMZ. Berdasarkan hasil observasi, koneksi dari zona internal perusahaan terhubung langsung ke switch distribusi utama, yang selanjutnya akan terhubung ke mesin instrumen / *endpoint* di area produksi. Berikut ini adalah gambaran topologi jaringan eksisting.

© 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



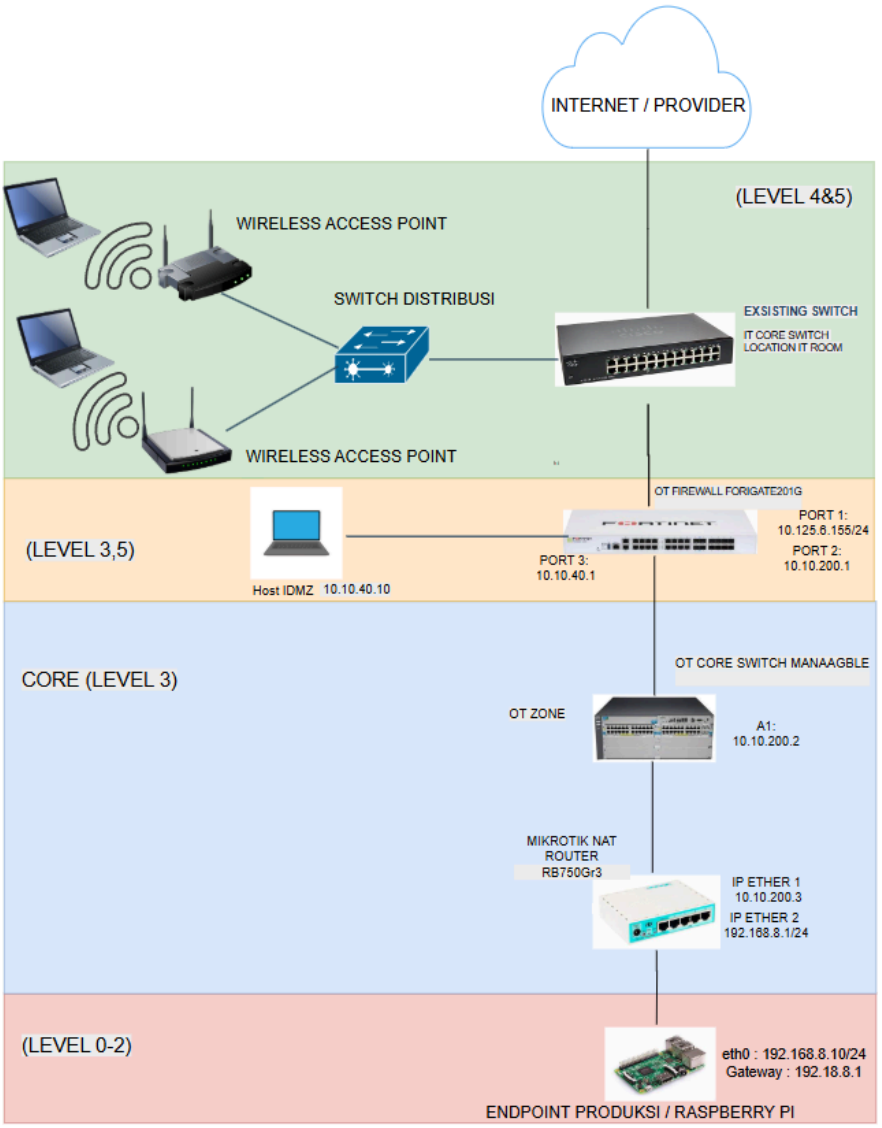
Gambar 4.1 Topologi Jaringan *Existing*

4.2.2 Perancangan Topologi Jaringan Baru

Berdasarkan permasalahan yang ada pada topologi eksisting, penulis merancang arsitektur baru dengan menempatkan *firewall* FortiGate sebagai pusat segmentasi. Zona jaringan dibagi menjadi 4 zona utama: Zona Internal/IT (Level 4-5), Zona IDMZ (Level 3,5), dan Zona OT Core (Level 3) dan Zona *Endpoint* OT (Level 0-2). Seluruh trafik komunikasi data dari IT menuju OT harus melewati zona IDMZ terlebih dahulu dan tunduk pada kebijakan *firewall* yang sudah ditetapkan. Rancangan topologi jaringan dapat dilihat pada gambar berikut.

© 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



Gambar 4.2 Rancangan Topologi Jaringan

4.2.3 Perencanaan IP *Address*

Perencanaan IP *Address* merupakan bagian yang penting dalam perancangan arsitektur *Industrial Demilitarized Zone*, karena setiap zona jaringan harus memiliki alamat dan gateway yang jelas agar proses segmentasi jaringan dapat berjalan dengan baik sesuai dengan yang sudah direncanakan. Pembagian IP Address dilakukan berdasarkan fungsi pada masing-masing zona yang terdiri dari zona internal/IT, zona IDMZ, zona OT, endpoint produksi dan juga VPN pool. Pembagian ini digunakan untuk memastikan bahwa setiap komunikasi antar zona tidak berjalan secara langsung dan dapat dikendalikan oleh firewall.

© 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

Tabel 4.3 IP Address

No	Zona	Interface	IP Address	Gateway	Keterangan
1	Internal/IT	Client internal	10.125.4.xx	10.125.4.xx	Perangkat client(karyawan) yang terhubung ke jaringan internal perusahaan
2	Internal/IT	FortiGate Internal Access	10.125.6.xx	10.125.6.xx	IP FortiGate untuk akses web interface firewall
3	SSL VPN	Remote Gateway FortiClient	10.125.6.xx	-	Alamat tujuan FortiClient VPN saat melakukan koneksi VPN
4	SSL VPN	VPN Pool	10.10.50.x/24	10.10.50.x/24	Pool IP yang diberikan kepada client VPN
5	IDMZ	FortiGate Interface IDMZ	10.10.40.1	-	Gateway Zona IDMZ
6	IDMZ	PC/Host IDMZ	10.10.40.10	10.10.40.1	Host IDMZ
7	OT	FortiGate Interface OT_Core	10.10.200.1	-	Gateway Zona OT
8	OT	Switch Managable	10.10.200.2	10.10.200.1	Perangkat Distribusi jaringan OT
9	OT	Mikrotik Ether1	10.10.200.3	10.10.200.1	Interface Mikrotik Zona OT
10	Endpoint Raspberry PI	Mikrotik Ether2	192.168.8.1	-	Gateway Raspberry PI
11	Endpoint Raspberry PI	Raspberry PI	192.168.8.10	192.168.8.1	Endpoint Raspberry PI

4.2.4 *Policy Firewall List*

Policy Firewall List adalah daftar aturan akses yang digunakan untuk mengatur komunikasi antar zona jaringan pada Industrial Demilitarized Zone. Daftar ini dibuat sebagai acuan konfigurasi firewall pada FortiGate agar setiap trafik yang

© 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

melewati zona Internal/IT, IDMZ, OT, VPN dan Endpoint Raspberry PI dapat dikendalikan dan dapat tercatat. Pada rancangan ini akses langsung dari jaringan luar maupun jaringan internal/IT menuju zona OT dan endpoint raspberry pi tidak bisa dilakukan. Akses menuju OT hanya dapat dilakukan melalui zona IDMZ atau koneksi VPN yang telah melalui proses autentikasi.

Tabel 4.4 *List Policy Firewall*

NO	Nama Policy	Source	Destination	Service	Action	Keterangan
	ALLOW_IT_TO_IDMZ	Internal / IT	IDMZ	HTTP , HTTPS, PING, SSH	Allow	Mengizinkan perangkat pada jaringan internal/IT untuk mengakses zona IDMZ
2	ALLOW_IDMZ_TO_OT	IDMZ	OT_Core	HTTPS, PING, SSH	Allow	Mengizinkan host pada zona IDMZ untuk melakukan komunikasi terbatas menuju zona OT
3	ALLOW_IDMZ_TO_RASPI	IDMZ	OT_Core	PING	Allow	Mengizinkan pengujian konektivitas dari zona IDMZ menuju *endpoint* raspberry pi
4	ALLOW_VPN_TO_IDMZ	SSL VPN	IDMZ	ALL	Allow	Mengizinkan pengguna yang telah tersambung SSL VPN mengakses jaringan IDMZ
5	ALLOW_VPN_TO_OT	SSL	OT_CORE	ALL	Allow	Mengizinkan pengguna VPN mengakses jaringan OT setelah melewati proses autentikasi

© Hak Cipta milik Politeknik Negeri Jakarta

		VPN				dan pemeriksaan *policy firewall*
7	DENY_IT_TO_OT	Internal / IT	OT_CORE	ALL	Deny	Memblokir seluruh akses langsung dari jaringan internal menuju *endpoint* Raspberry PI
8	DENY_IT_TO_RASPI	Internal / IT	*Endpoint* Raspberry PI	ALL	Deny	Memblokir seluruh jaringan akses langsung dari jaringan internal/IT menuju *endpoint* raspberry pi
8	DENY_OT_TO_IT	OT	Internal/IT	ALL	Deny	Memblokir komunikasi dari jaringan OT menuju internal

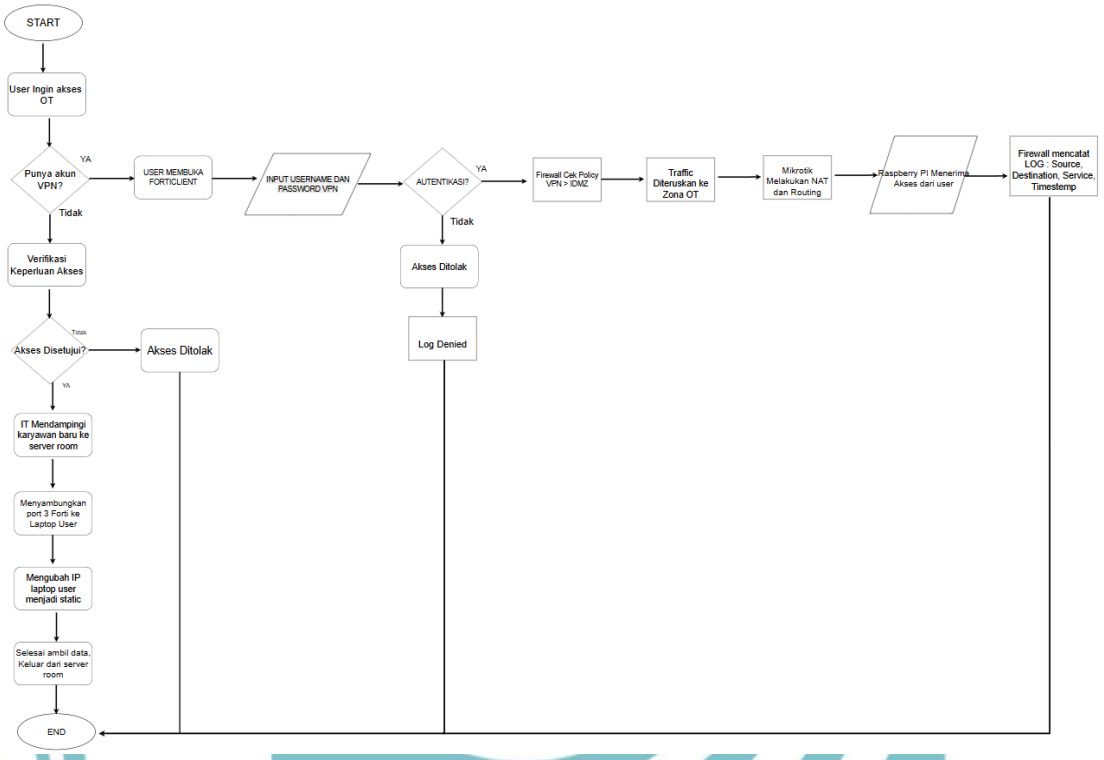
4.2.5 Akses User Menuju Zona OT

Akses user menuju zona Operational Technology (OT) pada penelitian ini dilakukan melalui dua cara: pertama dengan perangkat laptop client yang telah terhubung ke SSL VPN menggunakan aplikasi FortiClient, dan kedua dengan laptop client yang terhubung langsung dengan kabel LAN pada port 3 FortiGate. Flowchart akses user menuju zona OT dapat dilihat pada Gambar 3.4.

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 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



Gambar 4.3 Flowchart User Akses OT

4.3 Implementasi dan Konfigurasi

Tahap implementasi dan konfigurasi adalah tahapan dari penerapan rancangan arsitektur yang sudah dibuat dari proses sebelumnya. Pada tahapan ini seluruh desain segmentasi jaringan dan aturan kontrol direalisasikan ke dalam perangkat jaringan yang digunakan, sehingga kondisi *Existing* yang dimana akses langsung menuju kontroler Endpoint Raspberry PI bisa digunakan dapat berubah menjadi akses yang lebih aman dan terkontrol melalui zona *Industrial Demilitarized Zone* (IDMZ). Berikut ini adalah langkah langkah konfigurasi yang dilakukan pada penelitian ini.

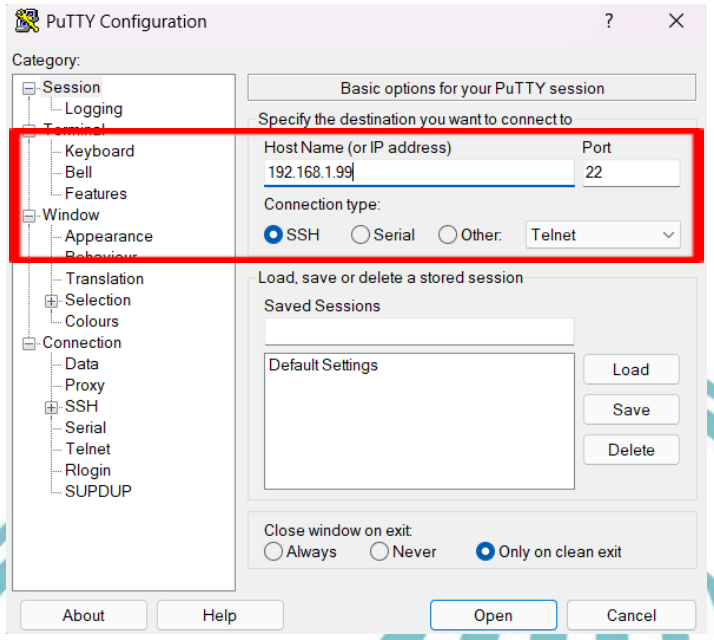
4.3.1 Setup Firewall

Pada bagian awal implementasi ini firewall harus ada beberapa konfigurasi yang dilakukan mulai dari konfigurasi dari laptop ke port MGMT pada firewall dan disetting melalui aplikasi PuTTY.

© Hak Cipta milik Politeknik Negeri Jakarta

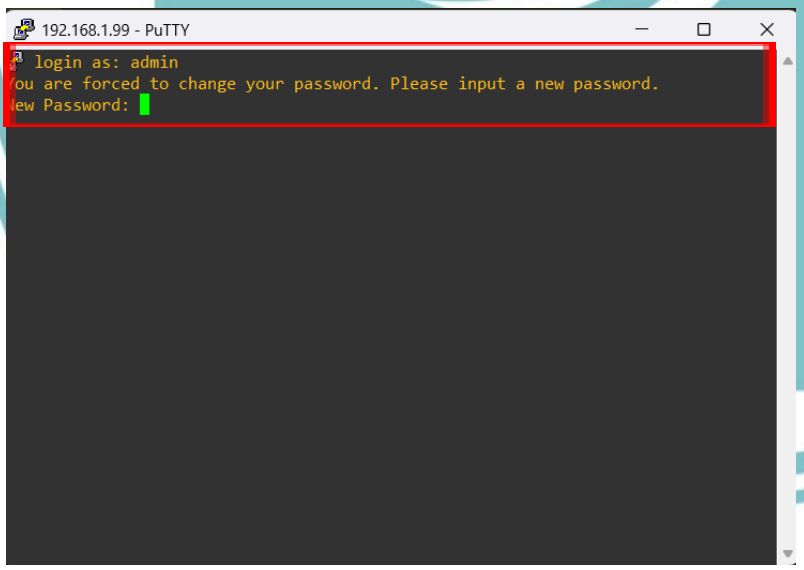
Hak Cipta :

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



Gambar 4.4 PuTTY Remote

Selanjutnya masuk sebagai “admin” dan masukkan password dan konfirmasikan password baru yang akan digunakan



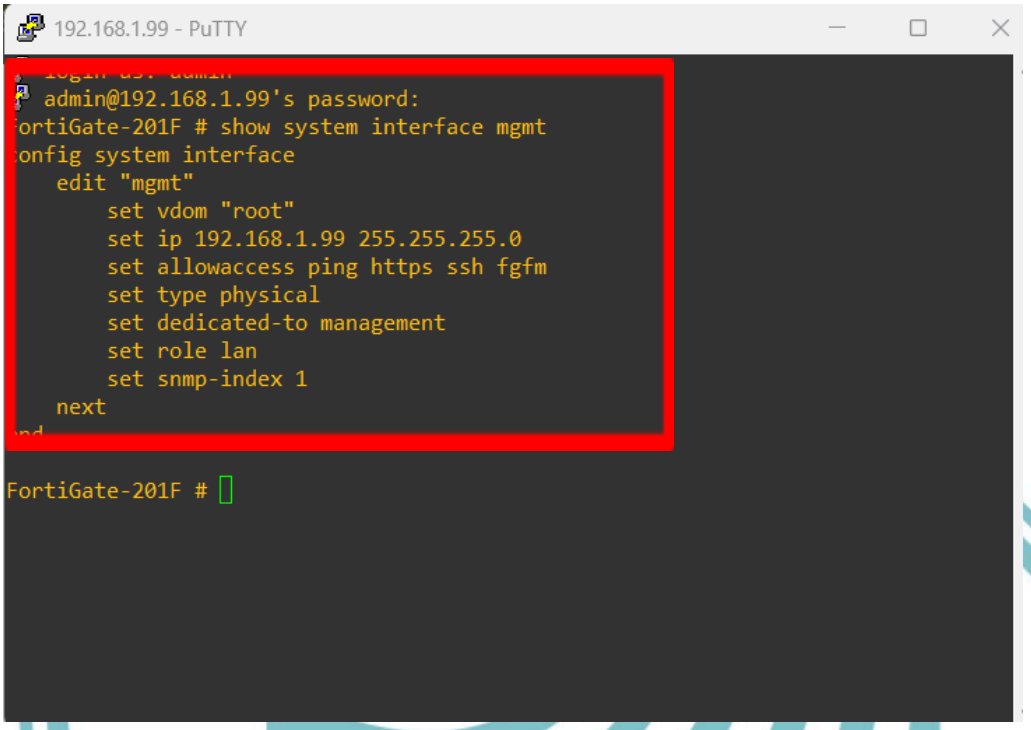
Gambar 4.5 PuTTY Admin

Setelah proses masuk berhasil dilakukan, selanjutnya tahap pengecekan terhadap interface yang terdaftar dan apabila diperlukan penambahan protokol lain juga dapat dilakukan pada menu yang sama.

© Hak Cipta milik Politeknik Negeri Jakarta

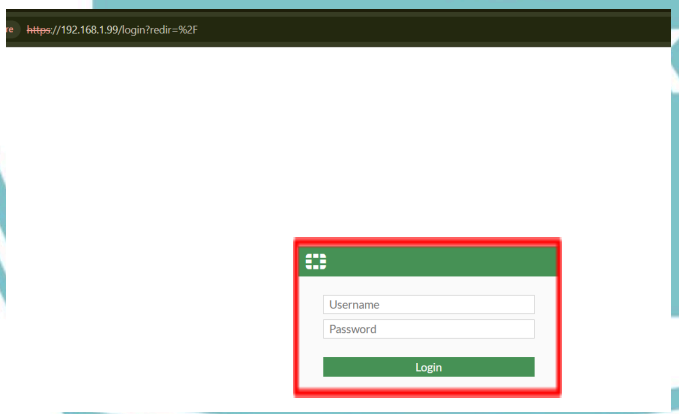
Hak Cipta :

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



Gambar 4.6 PuTTY Interface

Selanjutnya masukkan username dan password yang tadi sudah dibuat dan lanjut menuju proses login



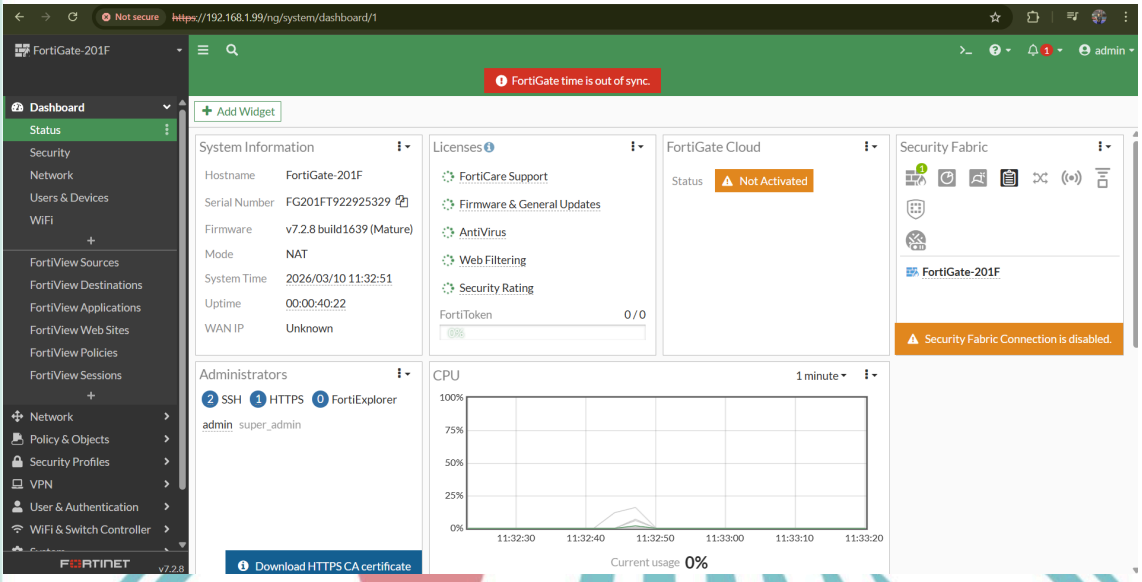
Gambar 4.7 Web Interface

Terakhir ini adalah menu ketika sudah berhasil untuk login ke interface website Firewall Fortigate

© 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



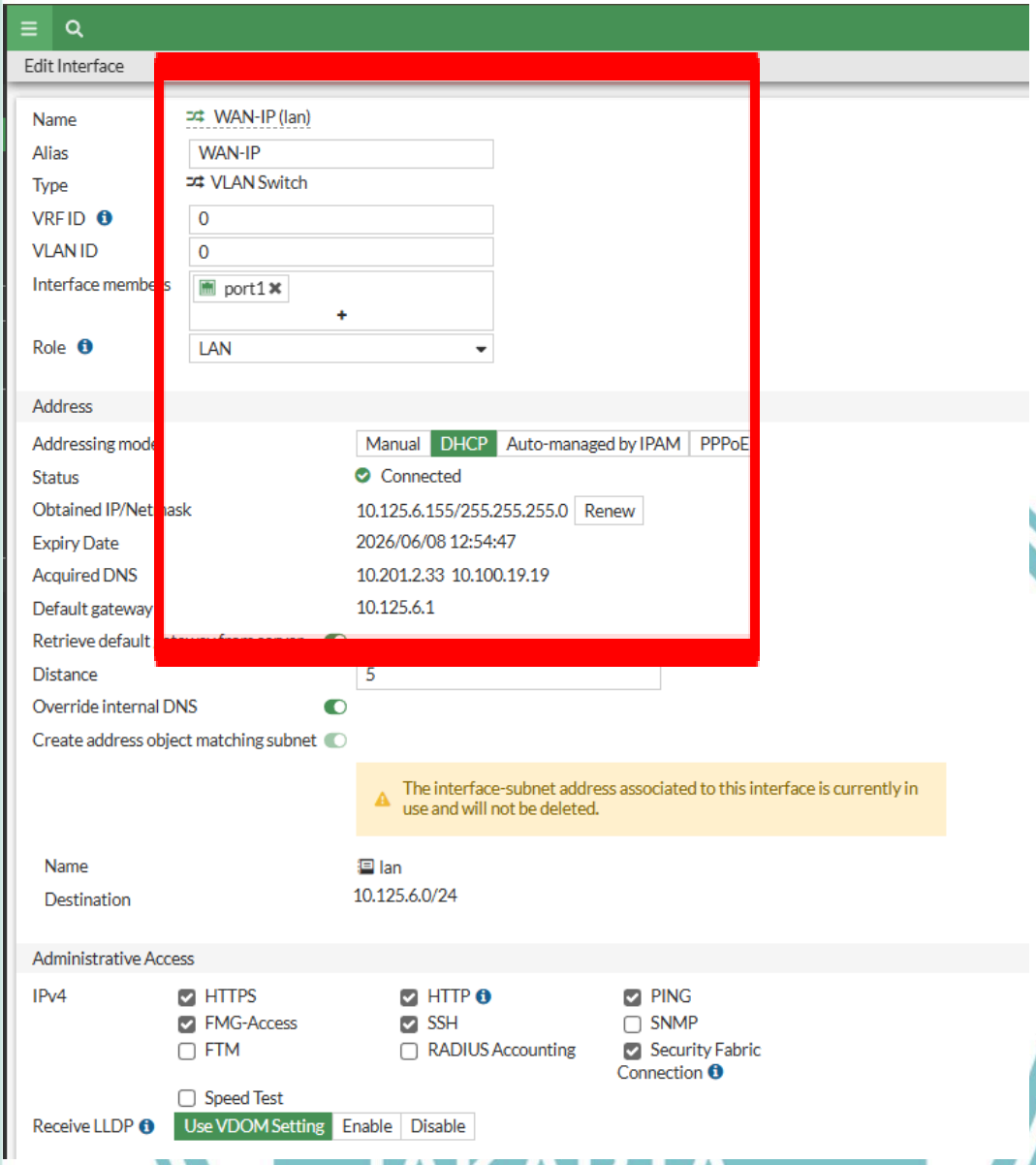
Gambar 4.8 Menu Interface

4.3.2 Konfigurasi Firewall

Setelah proses awal dan berhasil untuk login ke dalam *Interface* web FortiGate, tahap selanjutnya adalah konfigurasi firewall melalui menu *Network* pada *interface* web. Pada tahap ini konfigurasi difokuskan pada jaringan yang terhubung ke jaringan internal perusahaan. Konfigurasi pertama dilakukan dengan mengisi nama interface dan port apa saja yang tergabung didalamnya dan memilih *addressing mode* dhcp untuk bisa menerima alamat ip otomatis sehingga bisa memudahkan proses integrasi awal perangkat ke lingkungan jaringan yang sudah berjalan.

© 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



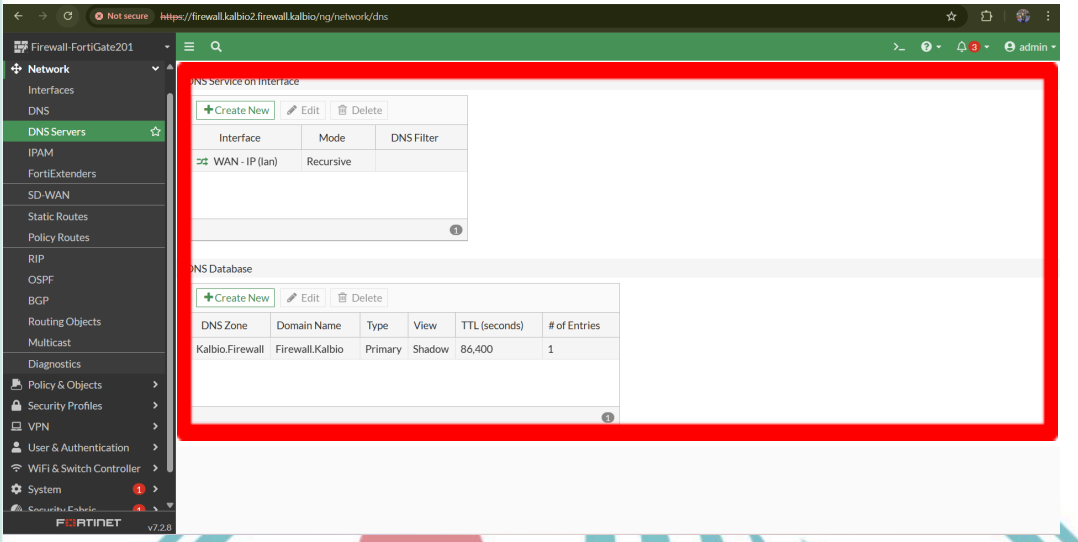
Gambar 4.9 Create Interface

Selanjutnya membuat DNS Database. Pada konfigurasi ini dibuat zona dengan nama Kalbio.Firewall dan Domain Name yaitu Firewall.Kalbio. Zona kemudian diatur sebagai *primary* dengan tampilan *shadow,* nilai TTL 86400 detik atau setara dengan 1 hari, serta status *Authoritative* kondisi aktif.

© Hak Cipta milik Politeknik Negeri Jakarta

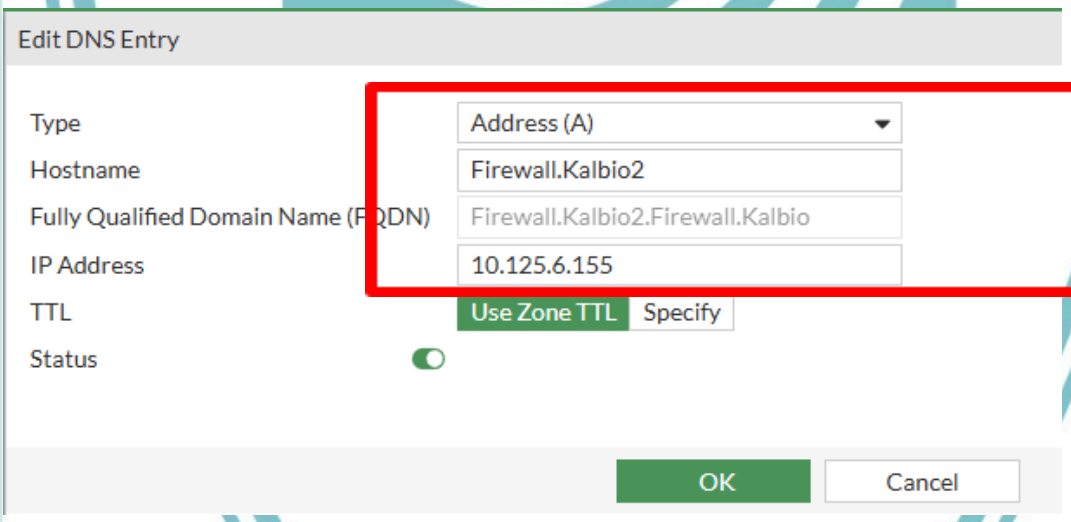
Hak Cipta :

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



Gambar 4.10 DNS Database

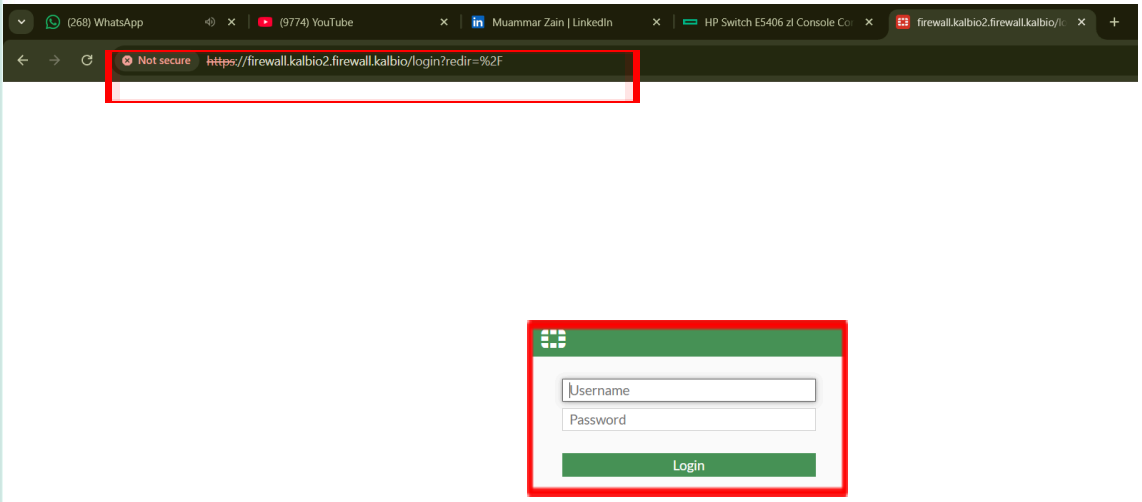
Setelah zona DNS berhasil dibuat, kemudian tambahkan juga dns entry berupa *Address* (A), *Hostname* yang digunakan adalah Firewall.Kalbio2 dan akan diarahkan ke IP 10.125.6.155.



Gambar 4.11 DNS Entries

Hasil dari konfigurasi tersebut dapat dilihat keberhasilan akses halaman login FortiGate melalui *browser* dengan menggunakan alamat firewall.kalbio2.firewall.kalbio. Hal ini menunjukkan konfigurasi yang dilakukan

telah berhasil dan berjalan sesuai dengan konfigurasi yang telah dilakukan.



Gambar 4.12 Login Page Sesudah DNS

Pada bagian ini firewall digunakan sebagai jalur menuju segmen *Operational Technology (OT)*. *interface* diatur sebagai physical interface dengan metode addressing dan alamat IP 10.10.200.1/24. Alamat ini berfungsi sebagai *gateway* untuk perangkat OT, termasuk juga Switch *Managable* dan perangkat mikrotik yang berada pada jalur distribusi menuju endpoint seperti Raspberrypi. Pada konfigurasi ini hanya layanan ping diaktifkan sebagai *administrative access* hal ini berguna untuk mengurangi resiko akses langsung ke jaringan OT.

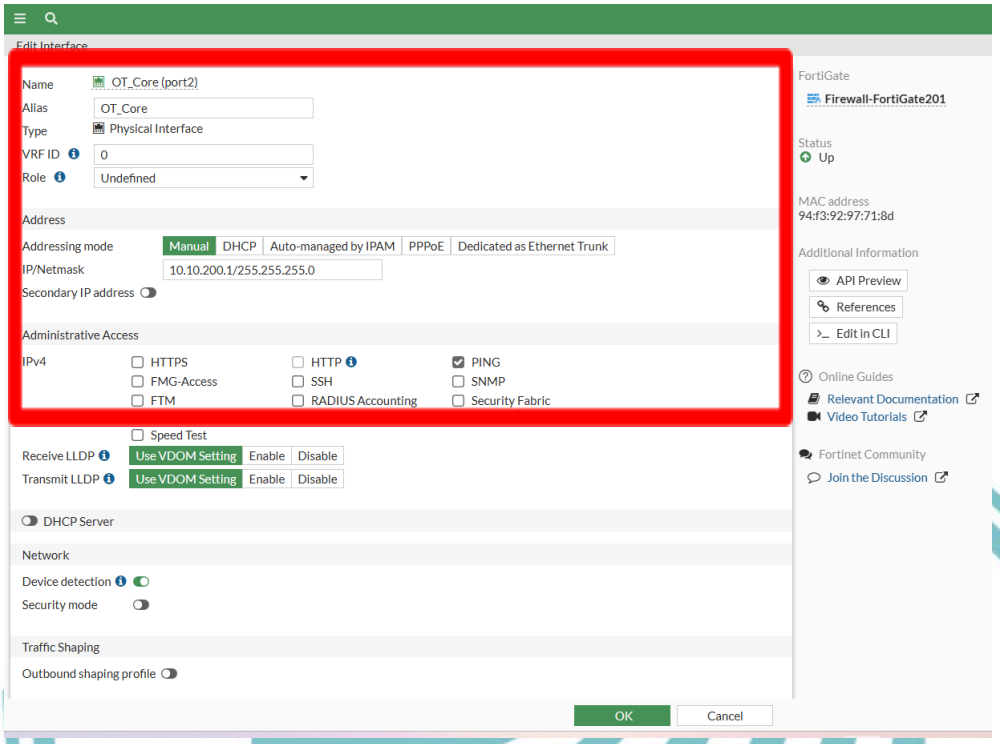
© Hak Cipta milik Politeknik Negeri Jakarta

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

© Hak Cipta milik Politeknik Negeri Jakarta

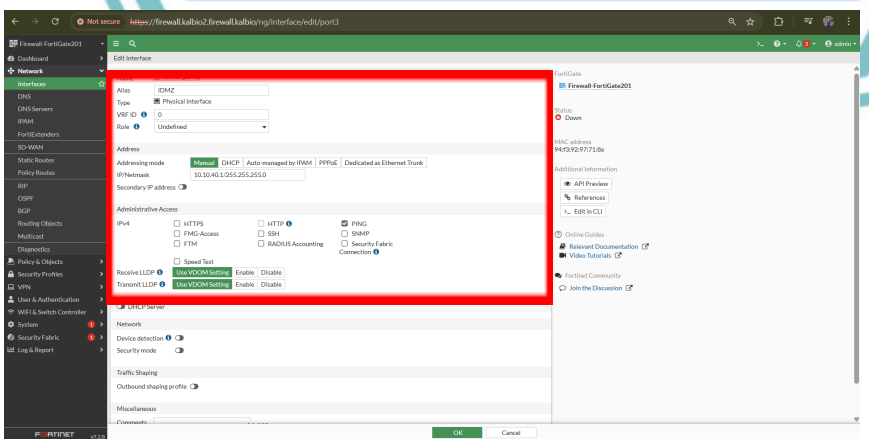
Hak Cipta :

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



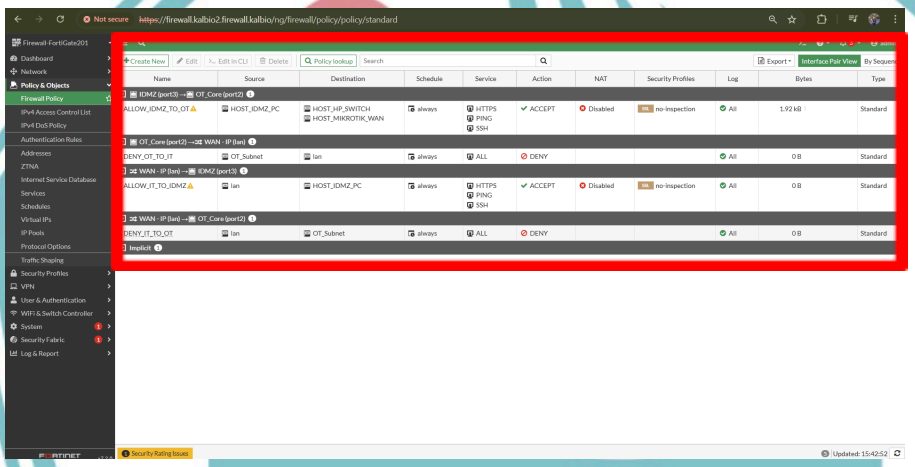
Gambar 4.13 Konfigurasi OT_Core

Konfigurasi *Interface* pada port ini yang akan digunakan sebagai zona perantara antara jaringan internal dan jaringan operasional. *Interface* ini akan dikonfigurasikan sebagai *physical interface* dengan metode *addressing* manual dengan alamat ip 10.10.40.1/24 dan digunakan sebagai gateway untuk host pada zona IDMZ. Pada port ini yang diaktifkan hanya layanan ping. Hal ini bertujuan agar zona IDMZ bisa terpisah dari jaringan internal dan subnet OT, sehingga akses hanya bisa dilakukan melalui jalur terpisah yang dilakukan oleh firewall policy.



Gambar 4.14 Konfigurasi IDMZ Port

Implementasi kebijakan keamanan pada firewall ini dibangun melalui empat *policy* utama. Yang pertama adalah ALLOW_IT_TO_IDMZ, yang fungsinya untuk memberikan akses dari jaringan internal menuju host IDMZ. policy kedua ALLOW_IDMZ_TO_OT, berfungsi untuk memberikan izin akses dari host IDMZ menuju perangkat yang berada pada subnet OT. Selanjutnya *policy* DENY_IT_TO_OT, yang digunakan untuk menolak *traffic* langsung dari jaringan internal menuju OT. Dan yang terakhir *policy* DENY_OT_TO_IT, sebagai penolak *traffic* dari OT menuju jaringan internal.



Gambar 4.15 Firewall Policy

4.3.3 Konfigurasi VPN

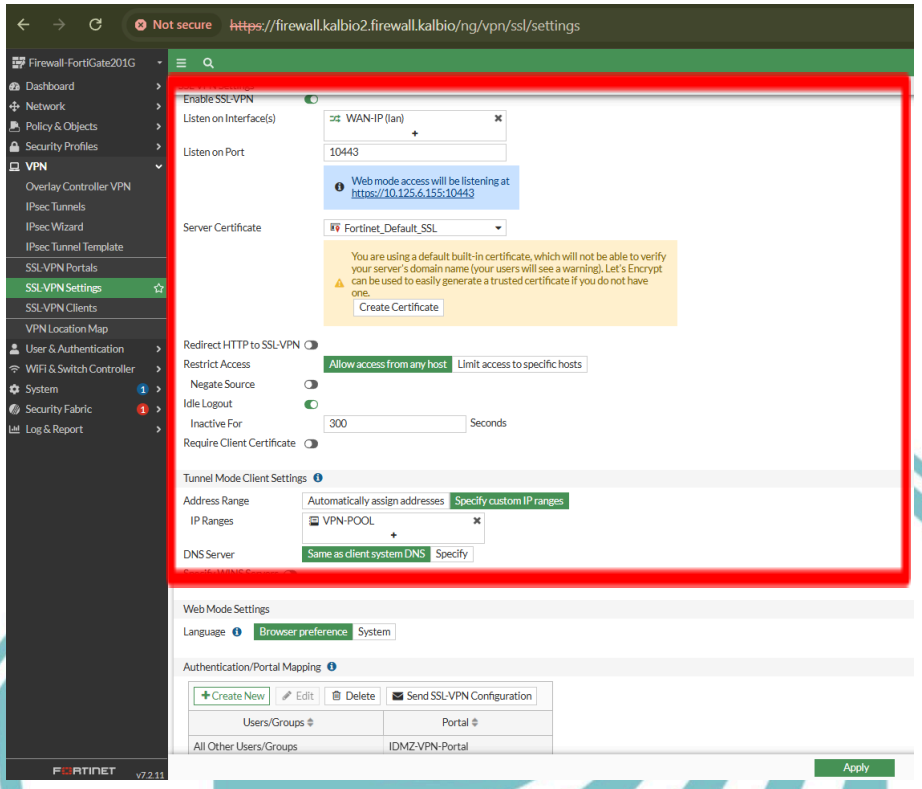
Pada tahap ini akan dilakukan konfigurasi SSL pada *FortiGate* agar para pengguna dari luar jaringan bisa mengakses zona produksi secara aman melalui zona IDMZ. Konfigurasi akan meliputi pembuatan portal, *user group*, dan *firewall policy* dan juga meliputi konfigurasi pada software *FortiClient.* Pada gambar 4.15 *Listen on Interface* diatur pada interface lan, selanjutnya port nya diatur menjadi 10443 dan ip pool yang akan digunakan adalah 10.10.50.0/24

© 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

© Hak Cipta milik Politeknik Negeri Jakarta

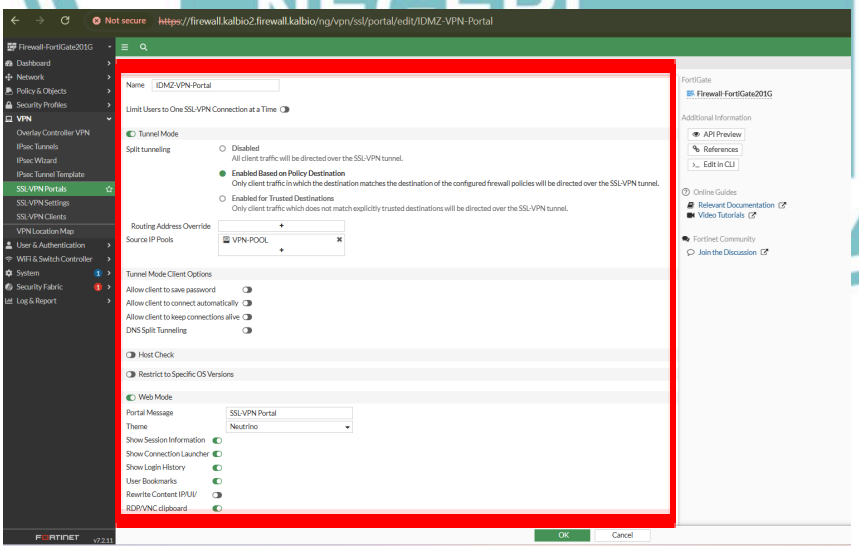
Hak Cipta :

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



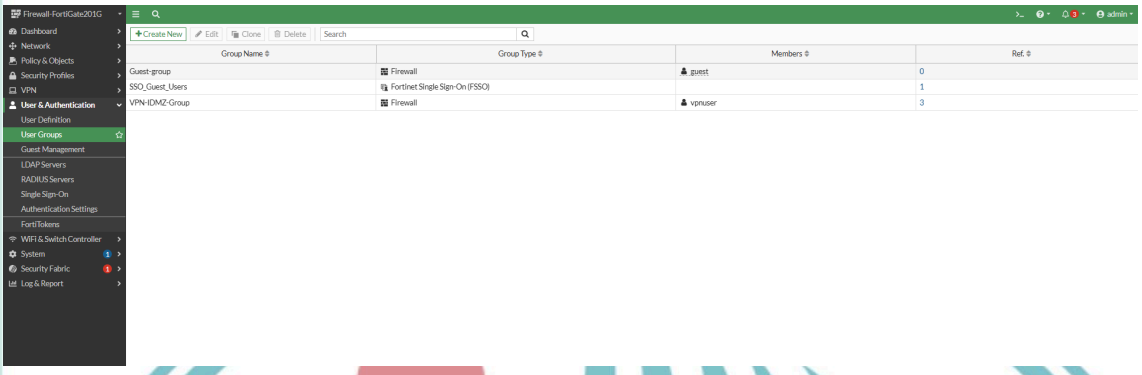
Gambar 4.16 Konfigurasi SSL VPN-Settings

Setelah mengkonfigurasi VPN-Settings selanjutnya melanjutkan ke tahap SSL-VPN Portal disini diisi dengan nama IDMZ-VPN-Portal. *Split tunneling* diaktifkan sesuai dengan *policy destination* yang akan dituju agar hanya trafik ke IDMZ dan OT yang akan melewati VPN.



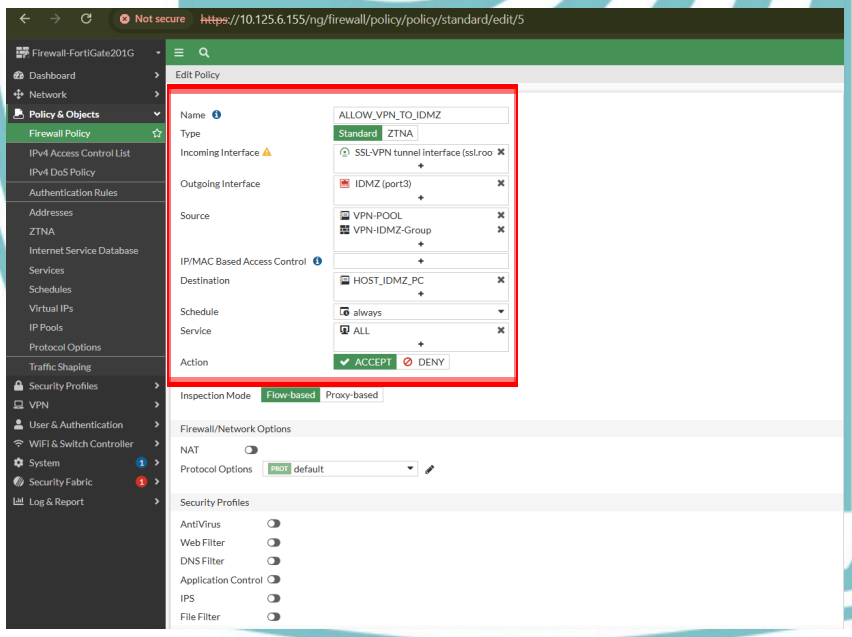
Gambar 4.17 Konfigurasi SSL VPN Portals

Konfigurasi selanjutnya adalah pembuatan *user* vpnuser dan menambahkan *user* tersebut dalam grup VPN-IDMZ-Group yang digunakan untuk autentikasi VPN.



Gambar 4.18 Konfigurasi User Groups

Tahap selanjutnya adalah membuat *firewall policy* ALLOW_VPN_TO_IDMZ yang akan mengizinkan trafik dari interface ssl.root menuju zona IDMZ.



Gambar 4.19 Firewall Policy VPN to IDMZ

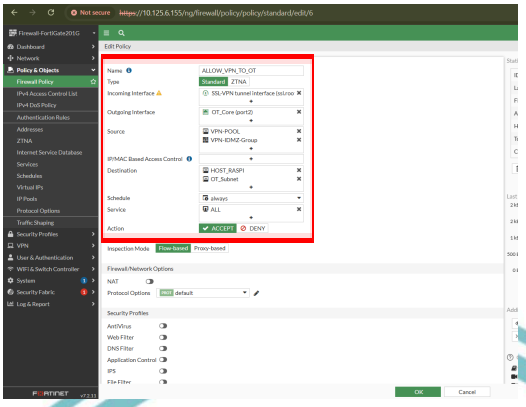
Setelah itu pembuatan *firewall policy* ALLOW_VPN_TO_OT yang akan mengizinkan trafik dari VPN menuju zona OT setelah melewati IDMZ.

© 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

© Hak Cipta milik Politeknik Negeri Jakarta

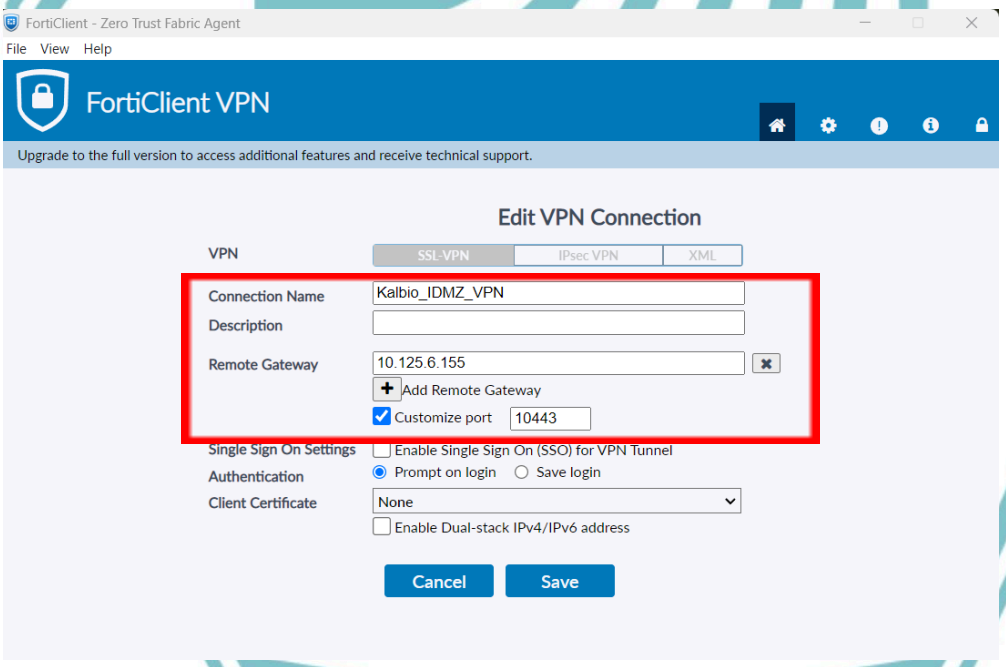
Hak Cipta :

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



Gambar 4.20 Firewall Policy VPN to OT

Dengan demikian konfigurasi VPN dari sisi web interface sudah selesai namun, perlu dilakukan konfigurasi dari sisi *FortiClient* VPN dengan remote gateway 10.125.6.155 dan port 10443.



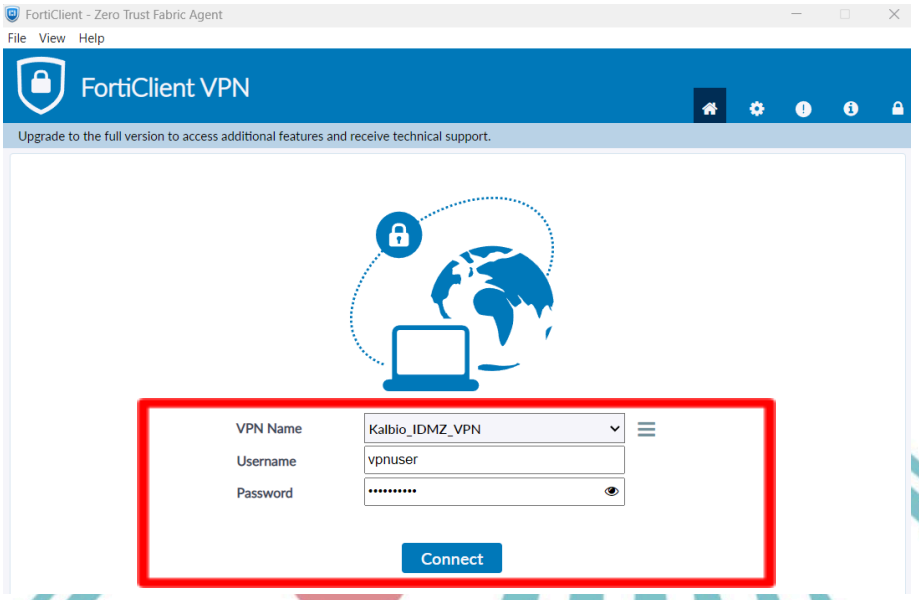
Gambar 4.21 FortiClient VPN

Tahap terakhir adalah melakukan login dengan *username* dan *password* untuk bisa mengakses ke dalam jaringan VPN.

© Hak Cipta milik Politeknik Negeri Jakarta

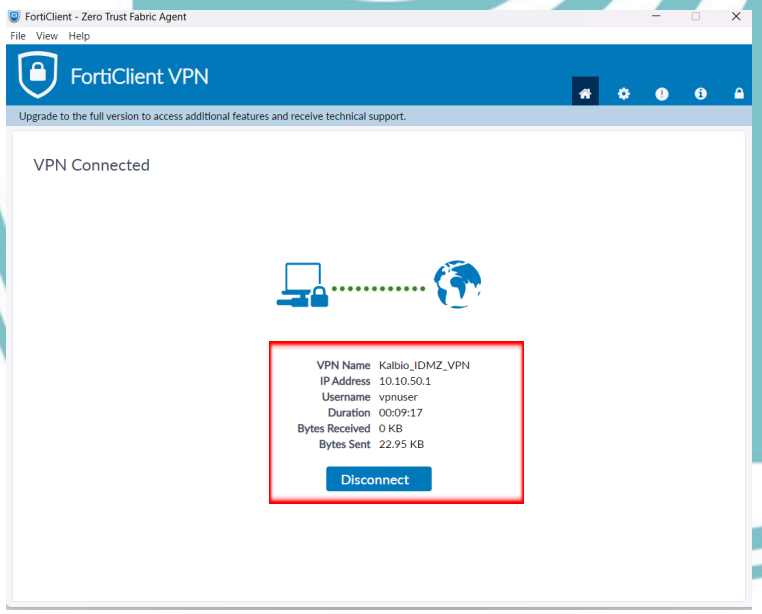
Hak Cipta :

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



Gambar 4.22 Login VPN

Konfigurasi berhasil dilakukan jika VPN bisa terhubung seperti gambar dibawah ini.



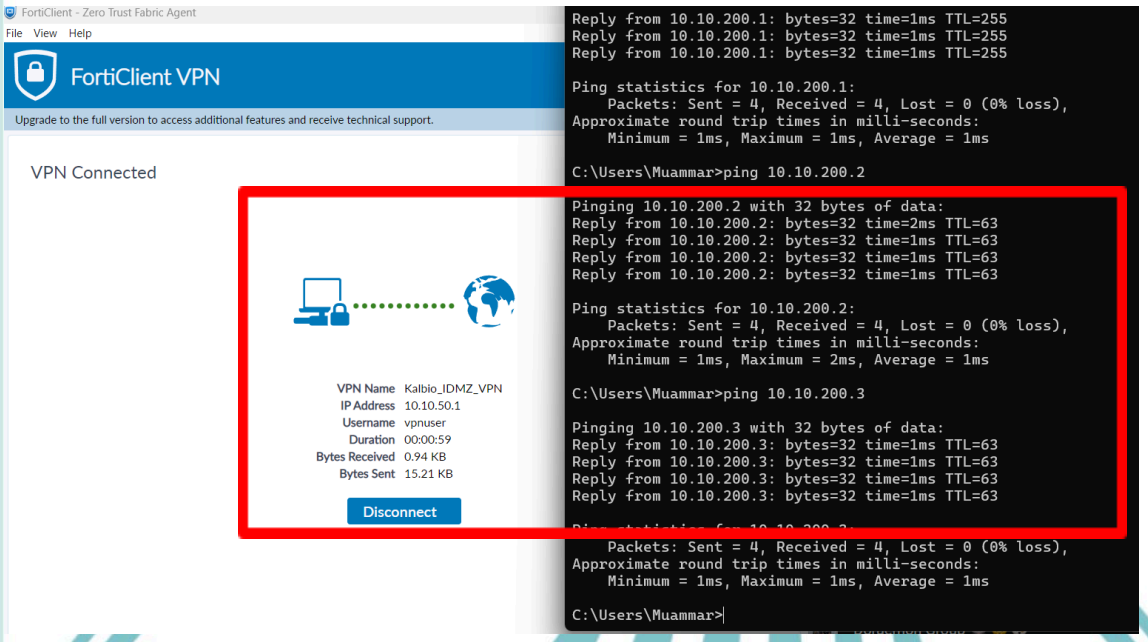
Gambar 4.23 Login Berhasil

Ketika login sudah berhasil maka selanjutnya melakukan testing dengan melakukan ping ke gateway IDMZ, Zona OT dan Raspberry PI.

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

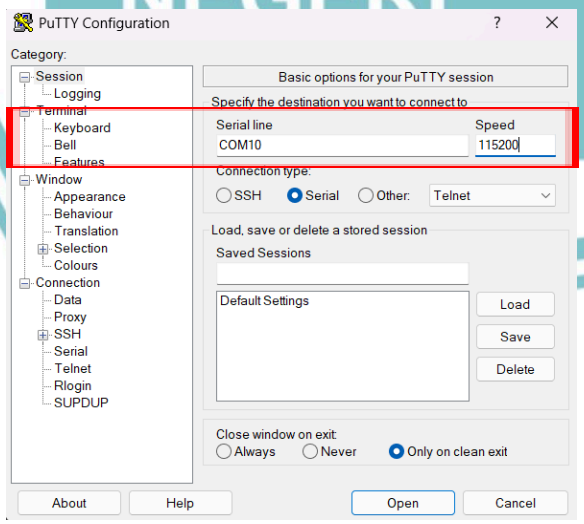
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
   a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
   b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.24 Ping Berhasil

4.3.4 Konfigurasi Switch Managable

Selanjutnya adalah tahap konfigurasi pada *Switch Managable* yang digunakan sebagai perangkat distribusi jaringan yang fungsinya untuk menghubungkan segmen jaringan dengan perangkat lain. Konfigurasi pada switch dilakukan melalui aplikasi PuTTY dengan menggunakan koneksi serial dari laptop administrator ke port console switch.



Gambar 4.25 Interface PuTTY

Pada tahap awal konfigurasi switch *managable,* hal yang dilakukan pertama kali adalah reset perangkat untuk mengembalikan kondisi switch pada pengaturan awal. Hal ini bertujuan untuk memastikan perangkat tidak memiliki perangkat tidak memiliki konfigurasi yang sebelumnya yang dapat mempengaruhi proses implementasi sistem yang akan dibuat. Hal lain yang dilakukan selain reset juga meliputi pengaturan hostname serta username dan password untuk meningkatkan keamanan akses menuju perangkat switch.

```
OT-SWITCH# conf t
OT-SWITCH(config)# password manager user-name admin
New password for Manager: **********
Please retype new password for Manager: **********
```

Gambar 4.26 Pengaturan Password

Selanjutnya dilakukan pembuatan VLAN, hal ini digunakan sebagai segmentasi jaringan yang merepresentasikan zona *Operational Technology* (OT) dalam arsitektur IDMZ.

```
ProCurve Switch 4208vl# conf t
ProCurve Switch 4208vl(config)# hostname OT-SWITCH
OT-SWITCH(config)# vlan 1
OT-SWITCH(vlan-1)# name "OT"
OT-SWITCH(vlan-1)# ip address 10.10.200.2 255.255.255.0
OT-SWITCH(vlan-1)# unttaged 1-2
Invalid input: unttaged
OT-SWITCH(vlan-1)# untaged 1-2
Invalid input: untaged
OT-SWITCH(vlan-1)# untagged 1-2
Invalid input: 1
OT-SWITCH(vlan-1)# exit
OT-SWITCH(config)# ip default-gateway 10.10.200.1
OT-SWITCH(config)# write memory
```

Gambar 4.27 Konfigurasi VLAN

Setelah konfigurasi VLAN selesai, dilakukan pengecekan dengan memasukkan perintah show vlan 1

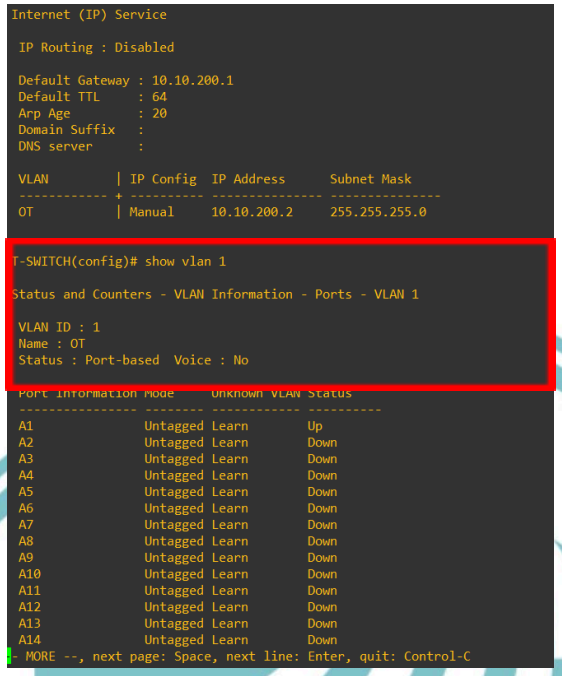
© Hak Cipta milik Politeknik Negeri Jakarta

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

© Hak Cipta milik Politeknik Negeri Jakarta

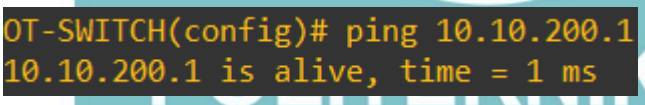
Hak Cipta :

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



Gambar 4.28 Hasil VLAN

Pada tahap terakhir, dilakukan pengujian konektifitas untuk memastikan VLAN yang sudah dibuat telah terhubung dengan akses FortiGate. Pengujian ini dilakukan dengan melakukan ping ke alamat IP FortiGate.



Gambar 4.29 Hasil Ping

4.3.5 Konfigurasi Mikrotik RB750G R3

Selanjutnya pada tahap ini, proses selanjutnya adalah konfigurasi mikrotik sebagai perangkat NATR, hal yang harus dilakukan adalah login dengan memilih alamat MAC perangkat dan memasukkan username dan password setelah itu *connect* untuk masuk ke halaman *interface* konfigurasi mikrotik.

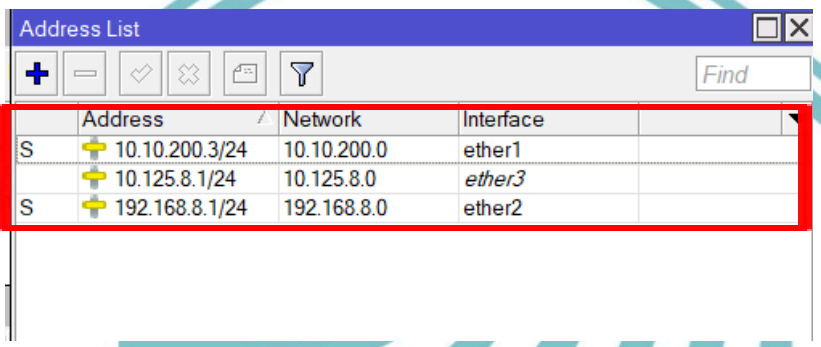


© Hak Cipta milik Politeknik Negeri Jakarta

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

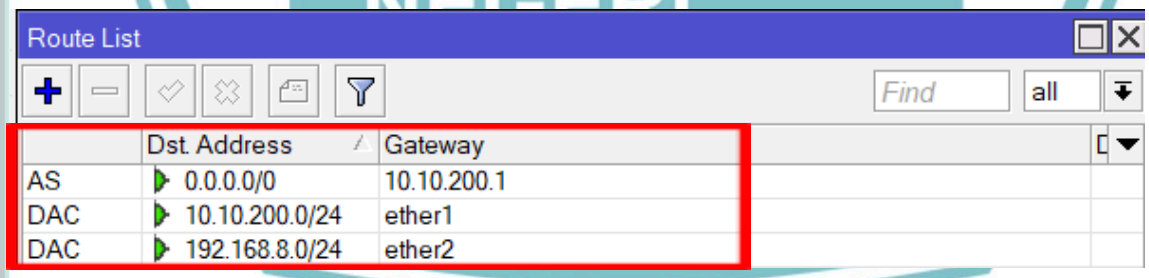
Gambar 4.30 Login Winbox

Langkah selanjutnya adalah mengkonfigurasikan alamat IP pada perangkat MikroTik. *Interface* pada ether1 di konfigurasikan dengan alamat 10.10.200.3/24 yang terhubung dengan segmen OT, sedangkan *interface e*ther2 di konfigurasikan 192.168.8.1/24 sebagai gateway ke jaringan lokal Raspberry Pi. Hal ini menunjukan mikrotik digunakan sebagai perangkat penghubung antara subnet OT dan subnet endpoint produksi atau Raspberry Pi.



Gambar 4.31 Konfigurasi Address List

Setelah melakukan setting untuk *address list* konfigurasi selanjutnya adalah melakukan routing pada perangkat MikroTik. Pada penelitian ini terdapat default route dengan *destination* 0.0.0.0/0 mengarah ke *gateway* 10.10.200.1, yaitu *interface* OT pada firewall FortiGate. Selain itu juga route terhubung langsung ke subnet 10.10.200.0/24 di ether1 dan 192.168.8.0/24.

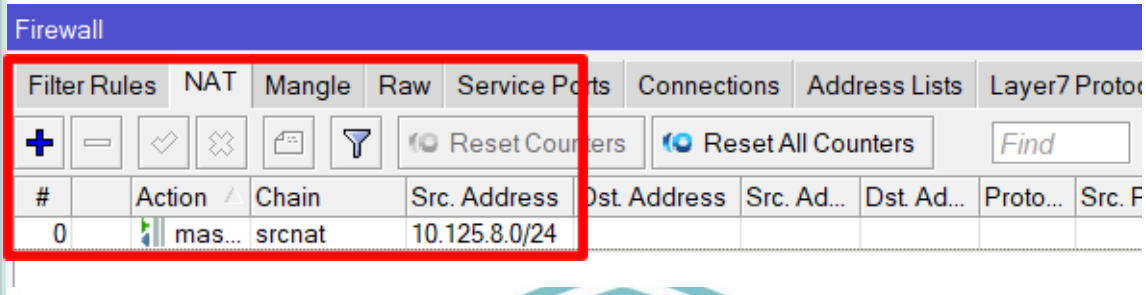


Gambar 4.32 Route List

Konfigurasi selanjutnya adalah *Network Address Translation* (NAT) pada perangkat MikroTik. Pada konfigurasi ini ditetapkan rule srcnat dengan *action masquarade* untuk subnet 192.168.8.0/24. *Rule* ini berfungsi agar trafik dari jaringan lokal yang digunakan Raspberry Pi, berhasil diteruskan melalui *interface* yang terhubung ke subnet OT.

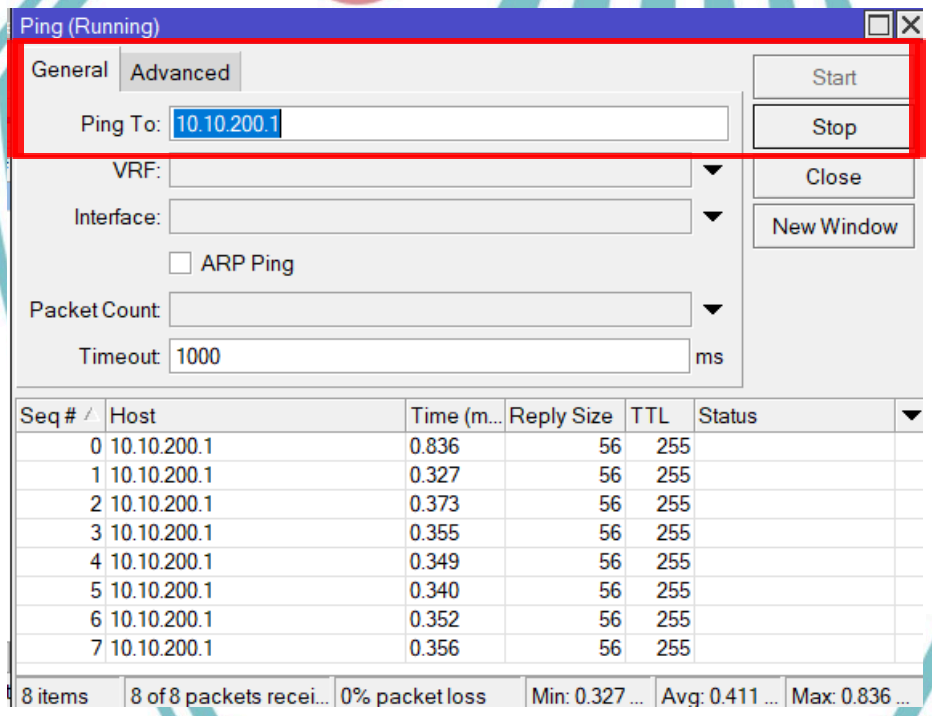
© Hak Cipta milik Politeknik Negeri Jakarta

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



Gambar 4.33 Firewall NAT

Tahap terakhir adalah dilakukan pengujian konektivitas dari perangkat MikroTik menuju alamat 10.10.200.1 yang merupakan *gateway* OT pada firewall FortiGate. Hasilnya menunjukkan jalur komunikasi dari MikroTik menuju firewall melalui switch OT telah terhubung dengan baik.

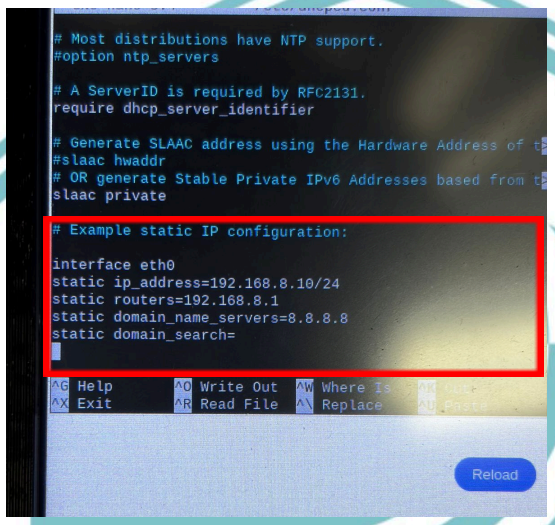


Gambar 4.34 Ping Test

4.3.6 Konfigurasi Raspberry PI

Pada tahap ini Raspberry PI dikonfigurasikan sebagai endpoint di level jaringan 0-2 yang terhubung ke perangkat mikrotik. Konfigurasi pada jaringan mikrotik dilakukan pada interface eth0 dengan IP 192.168.8.10/24 dan gateway 192.168.8.1. Hal ini bertujuan agar Raspberry PI bisa berkomunikasi dengan jaringan lokal pada endpoint serta akan meneruskan akses ke subnet OT melalui

perangkat mikrotik yang bertugas sebagai penghubung. Setelah dilakukan konfigurasi maka harus dilakukan verifikasi konektivitas menggunakan ping menuju ke alamat ip 192.168.8.1 , 10.10.200.2 dan 10.10.200.3. Sehingga bisa disimpulkan bahwa Raspberry PI sudah bisa terhubung dan berkomunikasi dengan baik sebagai *endpoint* pada tahap pengujian sistem.



© Hak Cipta milik Politeknik Negeri Jakarta

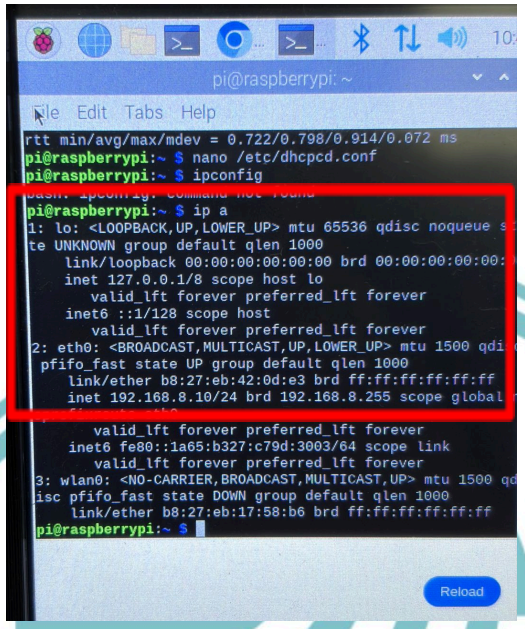
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© Hak Cipta milik Politeknik Negeri Jakarta

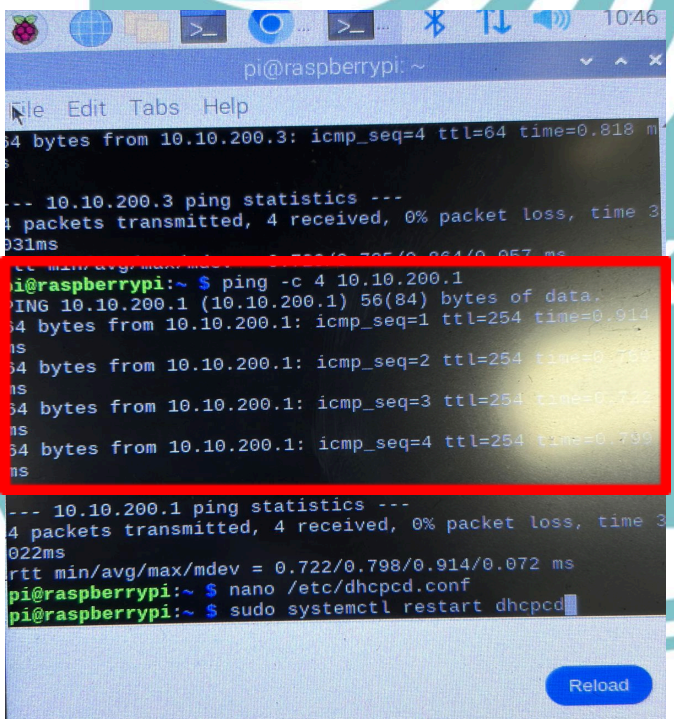
Hak Cipta :

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

Gambar 4.35 Konfigurasi IP Raspberry Pi



Gambar 4.36 Cek IP Raspberry PI



Gambar 4.37 Ping Menuju Zona IDMZ

4.4 Pengujian Sistem

Pengujian ini bertujuan untuk melakukan evaluasi terhadap hasil implementasi pada penelitian *Industrial Demilitarized Zone* (IDMZ) pada infrastruktur jaringan

© 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

PT Kalbio Global Medika, dengan harapan mengetahui rancangan yang sudah dibangun dapat berjalan sesuai dengan tujuan penelitian. Pada pengujian ini, dapat diketahui sejauh mana penerapan IDMZ mampu meningkatkan kontrol akses terhadap zona produksi, membatasi segala macam akses yang tidak sah, serta tetap menjaga kualitas jaringan pada lingkungan yang digunakan. Beberapa aspek yang diukur yaitu, kualitas jaringan (*QoS)* , efektivitas *firewall* dalam pemblokiran akses yang tidak sah , dan pencatatan log pada setiap trafik yang melewati sistem. Hasil dari pengujian ini akan memberikan banyak pemahaman yang lebih mendalam tentang sistem dan mampu memberikan koreksi maupun penyesuaian agar implementasi sistem yang sudah dibuat dapat lebih maksimal.

4.4.1 Prosedur Pengujian

Prosedur pengujian adalah langkah untuk menguji sistem yang sudah dibuat. Prosedur pengujian harus dilakukan dengan baik dan benar agar bisa mendapatkan hasil yang maksimal. Berikut adalah pengujian yang dilakukan:

1. Pengujian *QoS* sebelum implementasi
2. Pengujian *QoS* setelah implementasi
3. Pengujian Firewall
4. Pengujian Pencatatan Log

Dengan dilakukannya beberapa skema pengujian diatas, diharapkan bahwa sistem akan bekerja optimal sesuai dengan kebutuhan dan rancangan yang telah dibuat

4.4.1.1 Pengujian QoS Sebelum Implementasi

Pengujian *Quality of Service* (QoS) sebelum implementasi dilakukan untuk mengetahui kondisi awal dari segi performa jaringan pada topologi *existig* sebelum diterapkannya *Industrial Demilitarized Zone* (IDMZ). Parameter yang diuji meliputi *throughput*, *delay*, *jitter*, dan *packet loss* , skema pengujian dilakukan dengan melakukan uji konektivitas dari laptop *client* yang menggunakan WSL2 dengan sistem operasi ubuntu menuju Raspberry Pi yang terhubung langsung dengan instrumen produksi dan Lab yang akan berperan sebagai *endpoint*. Pada sisi endpoint, iperf3 server dijalankan terlebih dahulu agar Raspberry Pi tersebut dapat menerima koneksi dari client yang bertindak sebagai penguji. Pengujian ini dilakukan selama 4 hari dengan 2 sesi pengujian yaitu di

© 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

sesi pagi dan siang, sehingga total ada 8 sesi pengujian. Berikut ini adalah contoh perhitungan dengan menggunakan rumus:

Data yang diambil adalah data pada hari ke 1 sesi ke 1 dari sisi receiver

Transfer = 138 MBytes

Time = 32.79 s

Karena pada output dengan menggunakan tools iperf3 satuan "MBytes" yang umunya berbasis MiB maka harus dikonversikan terlebih dahulu:

Konversi data ke Mbit 138 MiB = $\frac{138\ MiB}{8}$ = 1104 Mibit

1104 Mibit = 1104 × 1,048576 Mbit = 1157,6Mbit

Hitung *Throughput*

Throughput = $\frac{1157{,}6\ Mbit}{32{,}79}$ = 35,3 Mbit/s

Hasil tersebut sama dengan nilai throughput nilai *receiver* yang dicatat pada tabel pengujian yang ada pada tabel berikut ini.

Tabel 4.5 Hasil Pengujian QoS Sebelum Implementasi

Hari	Sesi	Throughput Sender (Mbps)	Throughput Receiver (Mbps)	Throughput Rata - Rata (Mbps)	Delay (ms)	Jitter (ms)	Packet Loss(%)
Hari 1	Sesi 1	38.7	35.3	37.00	4.960	0.175	0
Hari 1	Sesi 2	43.2	38.7	40.95	7.752	0.192	0
Hari 2	Sesi 1	29.3	29.1	29.20	7.917	0.487	0
Hari 2	Sesi 2	32.4	29.4	30.90	6.854	0.216	0
Hari 3	Sesi 1	36.3	36.0	36.15	8.371	0.539	0
Hari 3	Sesi 2	38.5	34.9	36.70	4.948	0.190	0
Hari 4	Sesi 1	35.2	34.5	34.85	7.649	0.254	0
Hari 4	Sesi 2	38.5	35.0	36.75	10.320	0.456	0
Rata-rata		35.313 Mbps			7.346 ms	0.314 ms	0

© 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

Berdasarkan hasil pengujian yang telah dilakukan sebelum implementasi IDMZ, nilai *throughput* rata rata 35.313 Mbps hal ini menunjukkan jalur komunikasi dari laptop menuju endpoint produksi pada kondisi *existing* masih mampu untuk membawa beban transfer data dengan cukup baik. Artinya, jaringan masih sanggup untuk melakukan pertukaran data tanpa adanya *bottleneck* yang berat pada saat proses pengujian. Tetapi, dengan adanya variasi *throughput* pada hari ke 1 dimana kondisi paling tinggi dan hari ke 2 yang paling rendah mengindikasikan bahwa performa jaringan dipengaruhi oleh beban jaringan yang berubah-ubah. Pada intinya jaringan cukup baik dari segi performanya namun kestabilannya belum konsisten dari waktu ke waktu. Untuk parameter *Delay* dengan rata-rata 7.346 ms, nilai ini menggambarkan waktu tempuh paket dari client ke endpoint relatif lebih kecil sehingga komunikasi masih cukup responsif untuk akses layanan, Pada hari ke 4 memiliki delay lebih tinggi dibandingkan dengan hari lain. Maknanya pada kondisi tertentu seperti jam sibuk atau sedang adanya proses di instrumen tersebut respon jaringan bisa lebih lambat dibandingkan biasanya. Nilai *jitter* rata-rata adalah 0.314 ms menunjukkan bahwa variasi *delay* rendah, sehingga aliran data cenderung stabil. Untuk *packet loss* 0% pada semua sesi hal ini menunjukkan kualitas dan keberhasilan dalam pengiriman paket tergolong baik. Secara keseluruhan hasil *QoS* sebelum implementasi IDMZ ini menunjukkan jaringan *existing* memiliki performa yang baik dan stabil namun masih menunjukkan adanya fluktuasi dari sisi *throughput* dan *delay.* Data ini digunakan untuk menjadi *baseline* untuk menilai performa dari penerapan IDMZ kedepannya.

4.4.1.2 Pengujian QoS Sesudah Implementasi

Pengujian *Quality of Service* setelah penerapan *Industrial Demilitarized Zone* (IDMZ) dilakukan dengan metode yang sama dengan pengujian sebelumnya, yaitu dengan tools iperf3 dari laptop client yang terhubung ke VPN menuju endpoint produksi yang berupa device Raspberry PI. Pengujian dilakukan selama 4 hari dengan 2 sesi per hari pagi dan siang hari. Pada pengujian hari ke 2 sesi ke 2, nilai *throughput* yang tercatat sebesar 1.75 Mbps nilai ini adalah nilai yang jauh dibawah rata-rata pengujian lainnya. Setelah dilakukan pengecekan, kondisi ini terjadi dikarenakan adanya aktivitas jaringan yang padat selama periode

© 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

pengujian berlangsung. Kondisi ini menunjukan adanya kerentanan terhadap fluktuasi beban, sehingga mekanisme pengujian berbasis prioritas trafik / *Quality of Service* dapat menjadi rekomendasi untuk penelitian selanjutnya.

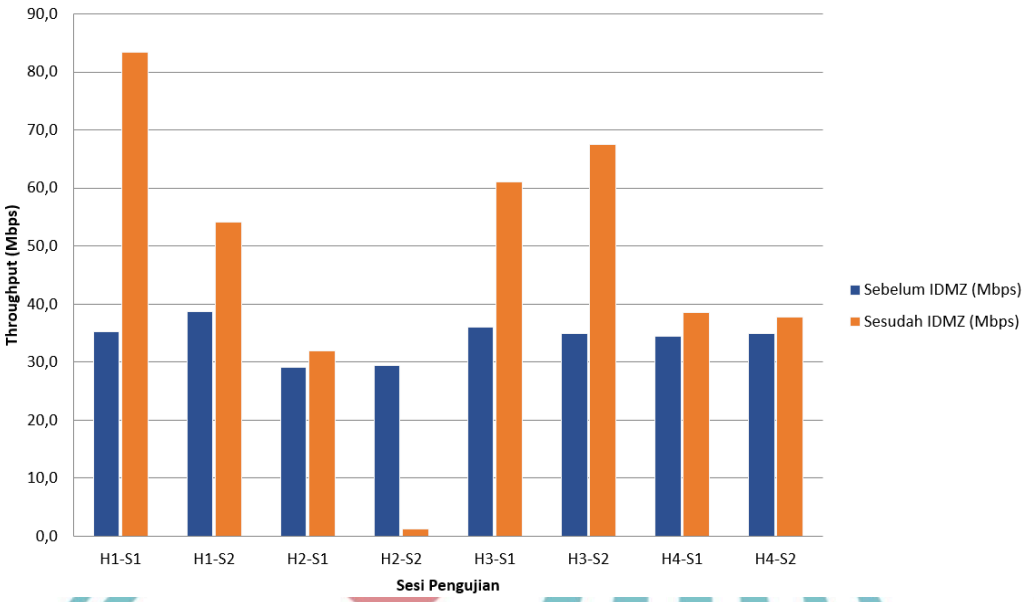
Tabel 4.6 Hasil Pengujian Sesudah Implementasi

Hari	Sesi	Throughput Sender (Mbps)	Throughput Receiver (Mbps)	Throughput Rata - Rata (Mbps)	Delay (ms)	Jitter	Packet Loss(%)
Hari 1	Sesi 1	92.1	83.4	87.75	8.565	0.966	0
Hari 1	Sesi 2	59.6	54.2	56.90	7.596	0.627	0
Hari 2	Sesi 1	43.1	32.0	37.55	19.993	0.872	0
Hari 2	Sesi 2	2.20	1.30	1.75	39.502	1.293	0
Hari 3	Sesi 1	65.9	61.0	63.45	9.279	1.364	0
Hari 3	Sesi 2	72.1	67.5	69.8	6.148	0.825	0
Hari 4	Sesi 1	53.6	38.6	46.1	9.931	0.000	0
Hari 4	Sesi 2	41.7	37.8	39.75	5.799	0.633	0
Rata-rata			50.381 Mbps		13.351 ms	0.823 ms	0

Hasil perbandingan QoS juga divisualisasikan dalam bentuk grafik untuk mempermudah proses analisis terhadap perubahan nilai setiap parameter sebelum dan sesudah implementasi IDMZ. Berikut ini adalah parameter rata-rata throughput ditunjukkan pada gambar 4.35

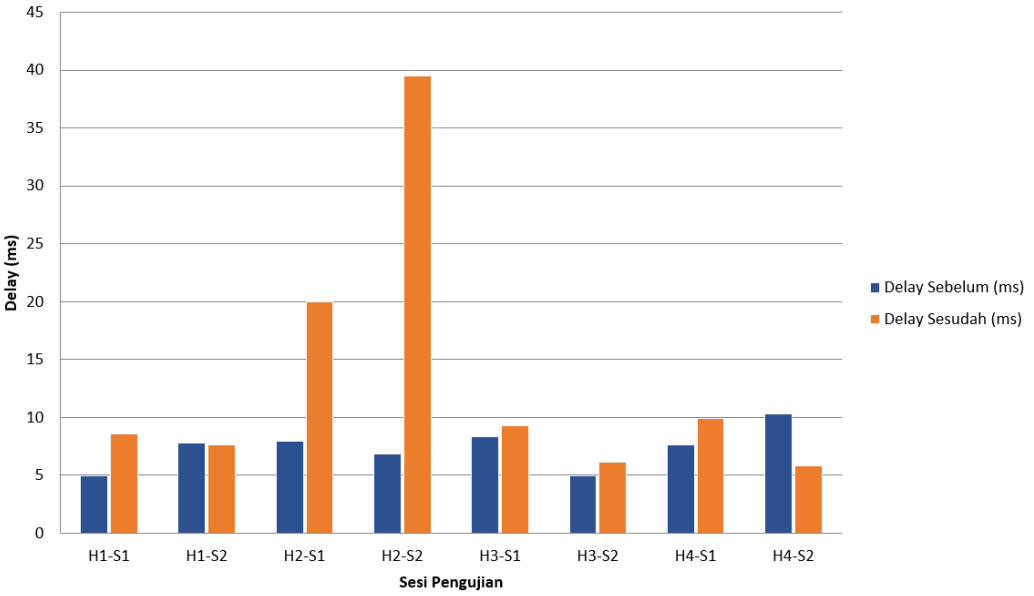
© Hak Cipta milik Politeknik Negeri Jakarta

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



Gambar 4.38 Grafik Perbandingan Throughput

Berdasarkan gambar 4.38, Nilai *Throughput* sebelum dan sesudah implementasi IDMZ mengalami perubahan. Pada kondisi sebelum implementasi parameter *throughput* cenderung lebih stabil dibandingkan pasca implementasi IDMZ. Tetapi adanya peningkatan *Throughput* setelah implementasi menunjukkan bahwa segmentasi jaringan dan pengaturan akses melalui *firewall* tidak menghambat proses pengiriman data. Berikut ini adalah parameter rata-rata *delay* ditunjukkan pada gambar 4.39

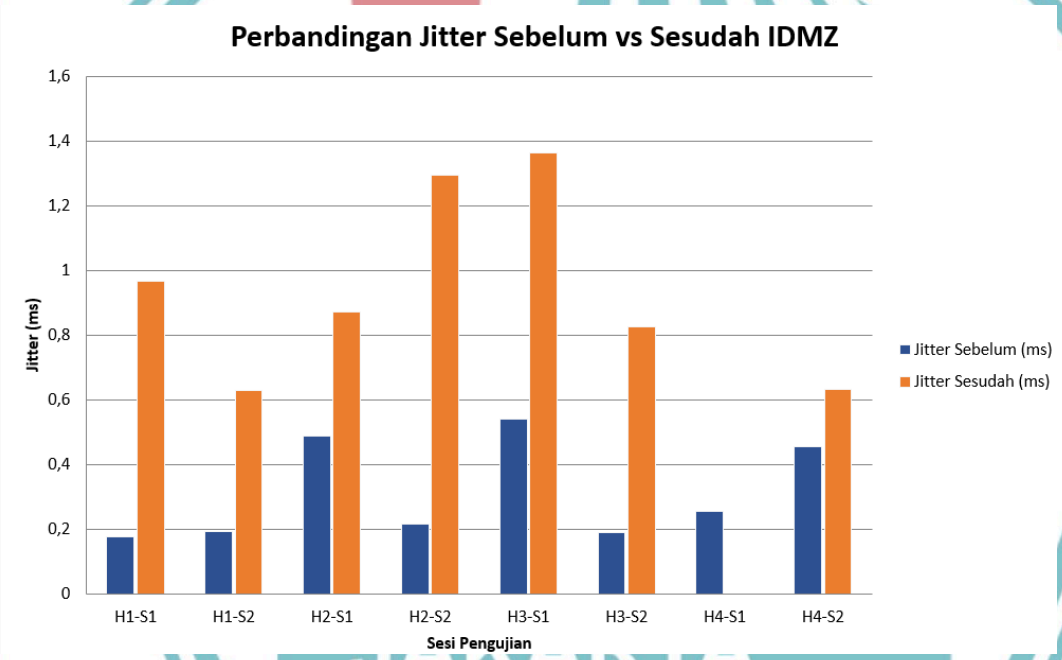


© Hak Cipta milik Politeknik Negeri Jakarta

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

Gambar 4.39 Grafik Perbandingan Delay

Berdasarkan gambar 4.39, nilai rata-rata *delay* sebelum implementasi relatif lebih stabil, namun pasca implementasi nilai *delay* mengalami peningkatan terutama pada hari ke 2 yang menunjukkan adanya lonjakan yang cukup tinggi dibandingkan hari lainnya. Kesimpulannya parameter *delay* mengalami penurunan performa secara angka karena nilai rata-ratanya meningkat dari 7,346 ms ke 13,351 ms pasca implementasi. Meskipun nilai *delay* pasca implementasi mengalami kenaikan, nilai tersebut masih berada jauh dibawah batas kategori sangat baik menurut TIPHON yaitu kurang dari 150 ms.Berikut ini adalah parameter rata-rata *jitter* ditunjukkan pada gambar 4.40

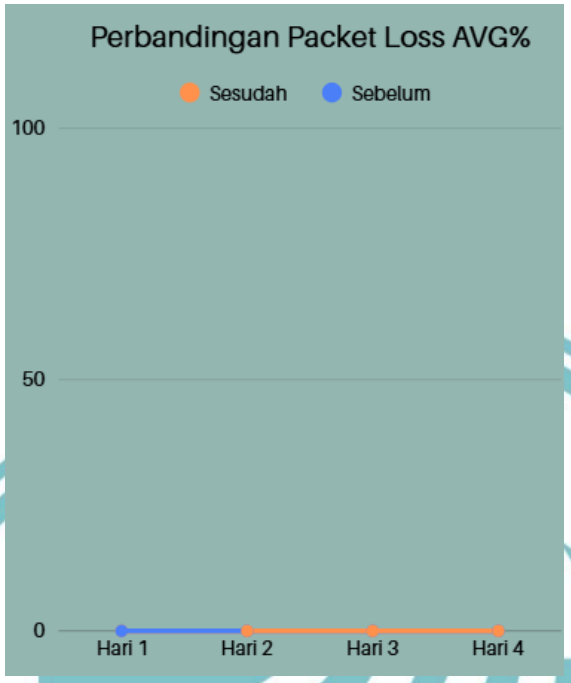


Gambar 4.40 Grafik Perbandingan Jitter

Berdasarkan gambar 4.40, nilai rata-rata *jitter* sebelum implementasi lebih stabil dan berada pada nilai yang rendah di setiap hari pengujian. Kenaikan parameter *jitter* pasca implementasi IDMZ dapat dipengaruhi oleh adanya tambahan proses pada jalur komunikasi jaringan, seperti pemeriksaan trafik dan proses routing antar segmentasi jaringan. Walaupun demikian nilai *jitter* masih berada dalam kategori baik berdasarkan standar TIPHON. Berikut ini adalah parameter rata-rata *packet loss* ditunjukkan pada gambar 4.41

© 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



Gambar 4.41 Grafik Perbandingan Packet Loss

Berdasarkan gambar 4.41, nilai *packet loss* sebelum dan sesudah implementasi tetap berada pada angka 0%. Kondisi ini menunjukan bahwa tidak ada kejadian kehilangan paket pada setiap proses komunikasi jaringan. Dengan demikian, parameter *packet loss* tidak memberikan dampak negatif terhadap implementasi IDMZ dan kualitas pengiriman paket tetap berada dalam kategori sangat baik.

4.4.1.3 Analisis Perbandingan QoS Sebelum & Sesudah

Untuk mengetahui dampak penerapan *Industrial Demilitarized Zone* (IDMZ) terhadap performa sebuah jaringan, maka harus dilakukan perbandingan nilai rata-rata *Quality of Service* (QoS) sebelum dan sesudah implementasi. Parameter yang akan dibandingkan meliputi *throughput, delay, jitter* dan *packet loss*. Hasil perbandingan keseluruhan pengujian ditunjukan pada tabel 4.10

Tabel 4.7 Analisis Perbandingan QoS

Parameter	Sebelum	Sesudah	Arah	Kategori Sebelum	Kategori Sesudah	Keterangan
Throughout	35.313	50.381	Lebih besar lebih	Sangat Baik	Sangat Baik	Throughput rata rata meningkat

© 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

			baik			pasca implementasi IDMZ (Lebih Baik)
Delay	7.346	13.351	Lebih kecil lebih baik	Sangat Baik	Sangat Baik	Delay rata-rata naik pasca implementasi IDMZ (Lebih Buruk)
Jitter	0.314	0.823	Lebih kecil lebih baik	Baik	Baik	Jitter rata rata naik pasca implementasi IDMZ (Lebih Buruk)
Packet Loss	0.000	0.000	Lebih kecil lebih baik	Sangat Baik	Sangat Baik	Packet Loss tetap 0% selama pengujian (Tetap Baik)

Berdasarkan Tabel 4.10, Implementasi IDMZ memberikan pengaruh terhadap beberapa parameter Qos. Nilai *Throughput* mengalami peningkatan dari 35.313 Mbps menjadi 50.381, hal ini menunjukan adanya peningkatan kemampuan jaringan dalam mengirimkan data. Selain itu juga nilai *Packet Loss* juga berada pada 0% yang menandakan bahwa tidak ada paket data yang hilang selama proses pengujian. Namun, nilai *delay* dan *jitter* mengalami peningkatan setelah implementasi IDMZ. Kenaikan tersebut terjadi karena adanya penambahan proses pada jalur komunikasi seperti segmentasi jaringan , pemeriksaan *firewall* dan *routing*. Meskipun demikian nilai tersebut masih berada kategori baik berdasarkan standar TIPHON. Dengan demikian implementasi IDMZ tetap layak digunakan karena mampu meningkatkan aspek keamanan jaringan tanpa menurunkan kualitas jaringan secara signifikan.

4.4.1.4 Pengujian Firewall

Pengujian *Firewall* dilakukan dengan tujuan untuk mengetahui hasil dari konfigurasi *firewall* yang telah dilakukan dan apakah segmentasi jaringan yang sudah dirancang dapat membatasi akses antar zona sesuai dengan kebijakan yang

© 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

ditetapkan. Pengujian di tahap ini dilakukan dengan cara menguji konektivitas dari host menuju interface IDMZ dan subnet OT untuk melihat apakah akses yang diizinkan dapat berjalan dan bisa membatasi akses langung menuju subnet OT. Hasil pengujian dari host uji menuju perangkat pada subnet OT dengan alamat IP 10.10.200.2 dan10.10.200.3, berdasarkan hasil ping menunjukan bahwa seluruh paket mengalami *Request Timed Out*. Hasil ini menunjukan bahwa akses pada skenario pengujian ini tidak berhasil menuju perangkat OT.

```
C:\Users\Muammar>ping -n 4 10.10.200.2

Pinging 10.10.200.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.200.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Gambar 4.42 Hasil Pengujian 1

```
C:\Users\Muammar>ping -n 4 10.10.200.3

Pinging 10.10.200.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.200.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Muammar>
```

Gambar 4.43 Hasil Pengujian 2

Selanjutnya melakukan uji konektivitas dari host menuju *interface* IDMZ pada *firewall* FortiGate dengan IP 10.10.40.1. Berdasarkan hasil yang didapatkan dari uji ping seluruh paket berhasil diterima kembali dengan nilai 0% *Packet Loss* sehingga bisa disimpulkan bahwa hasil ini menunjukan *interface* IDMZ pada *firewall* telah aktif dan bisa digunakan sebagai jalur perantara.

© 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

```
C:\Users\Muammar>ping -n 4 10.10.40.1

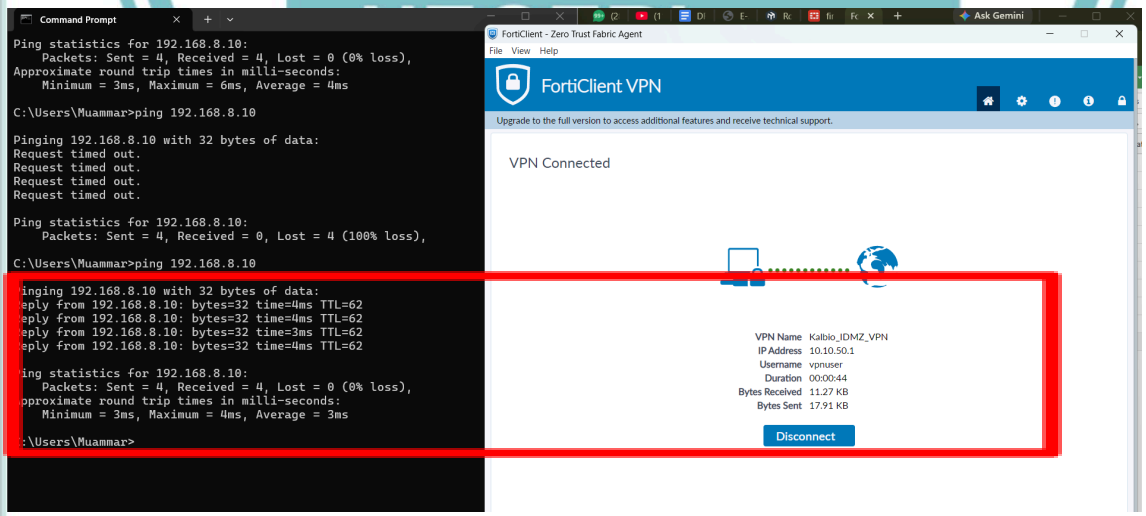
Pinging 10.10.40.1 with 32 bytes of data:
Reply from 10.10.40.1: bytes=32 time<1ms TTL=255
Reply from 10.10.40.1: bytes=32 time<1ms TTL=255
Reply from 10.10.40.1: bytes=32 time<1ms TTL=255
Reply from 10.10.40.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.40.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Muammar>
```

Gambar 4.44 Pengujian 3

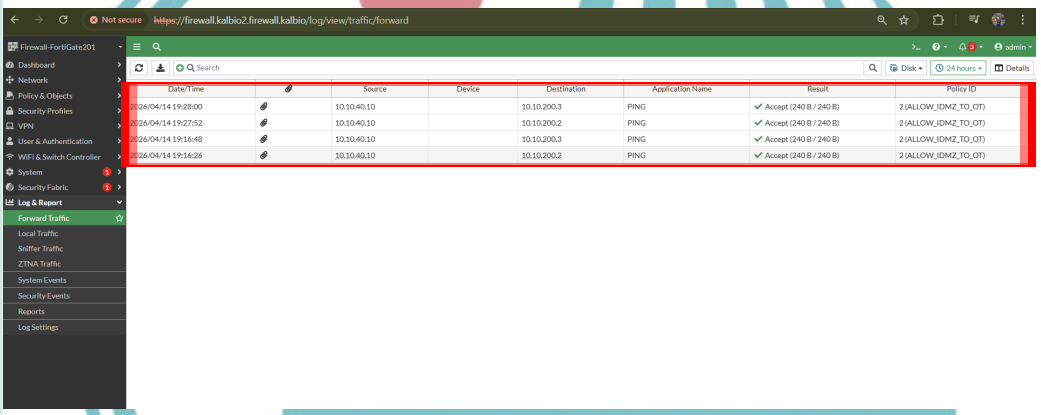
Pengujian selanjutnya adalah akses VPN menuju *endpoint* Raspberry Pi dilakukan setelah user berhasil terhubung ke SSL-VPN menggunakan *FortiClient*. Berdasarkan hasil pengujian, client memiliki IP VPN 10.10.50.1 dan berhasil melakukan ping menuju Raspberry Pi dengan alamat IP 192.168.8.10. Keberhasilan ini membuktikan bahwa akses remote menuju *endpoint* Raspberry Pi tidak dilakukan secara langsung dari jaringan luar dan jaringan IT, melainkan harus melewati mekanisme VPN dan *policy firewall*.



Gambar 4.45 Pengujian 4

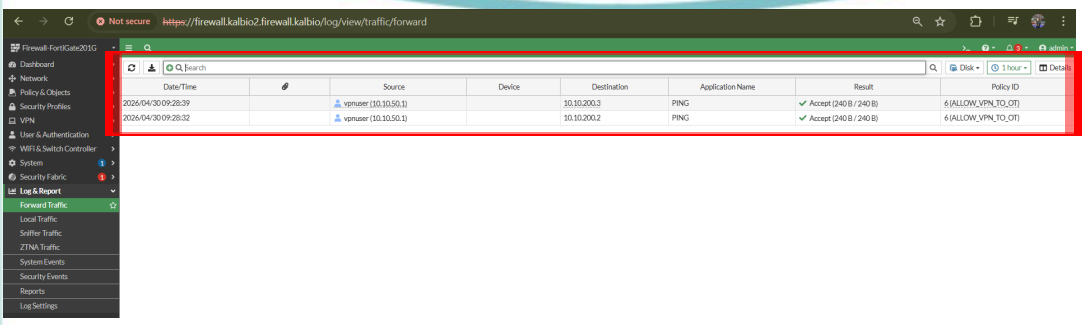
4.4.1.5 Pengujian Pencatatan Log

Hasil pengujian pencatatan log pada *firewall* fortigate melalui menu *Forward Traffic* adalah trafik dari host pada zona IDMZ dengan alamat IP 10.10.40.10 menuju perangkat subnet OT 10.10.200.2 , 10.10.200.3 dan endpoint raspberry pi berhasil tercatat oleh sistem hasil ini mencatat informasi penting terkait akses antar zona yang meliputi alamat IP , sumber , tujuan, jenis akses dan waktu akses serta tindakan dari *firewall* serta *policy* yang digunakan. Dengan begitu akses dari zona IDMZ menuju zona OT tidak hanya dapat dikendalikan melalui *firewall policy* tetapi juga bisa tercatat melalui log sebagai bukti keamanan jaringan.



Gambar 4.46 Log Tersimpan

Pengujian pencatatan log juga dilakukan untuk memverifikasi seluruh aktivitas yang berasal dari VPN agar tercatat dengan baik pada FortiGate. Pengujian ini dilaksanakan setelah client berhasil terhubung melalui SSL-VPN dengan alamat IP dari subnet VPN-POOL yang sudah dibuat. Hasil menunjukan bahwa seluruh pengujian trafik dari *interface* ssl.root berhasil tercatat pada menu *Forward Traffic*.



© Hak Cipta milik Politeknik Negeri Jakarta

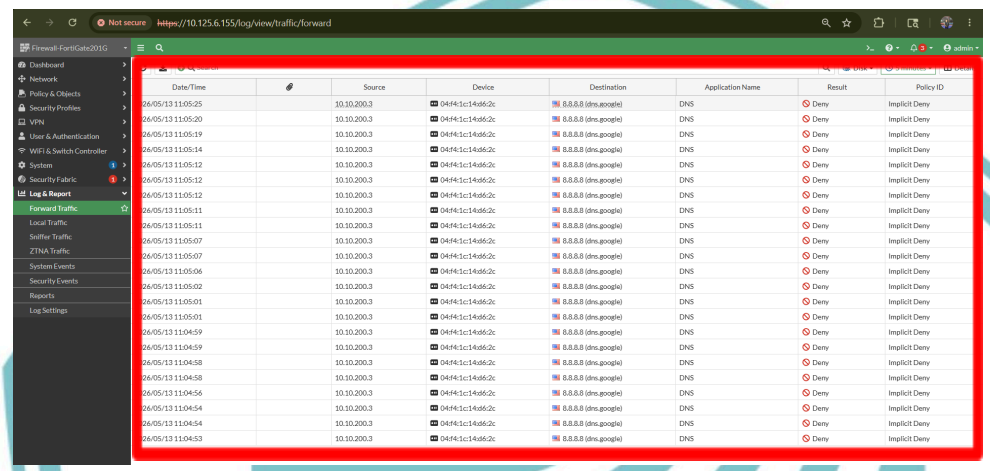
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

© 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

Gambar 4.47 Log VPN Tersimpan

Pengujian pencatatan log juga dilakukan dengan cara akses langsung dari *client* Internal/IT langsung menuju zona OT ataupun *endpoint* Raspberry PI. Hasil pengujian tersebut menunjukkan bahwa trafik tersebut mencatat menu *Forward Traffic* dengan status *Deny*. Hal ini menunjukan bahwa *FortiGate* berhasil memblokir trafik yang tidak sesuai dengan *policy* yang telah ditentukan.



Gambar 4.48 Log Deny

4.4.1.6 Pengujian *Firewall* dan Konektivitas

Pengujian *firewall* dan konektivitas dibuat agar bisa menentukan keberhasilan implementasi segmentasi jaringan berbasis IDMZ. Pengujian dilakukan dengan menguji konektivitas yang berasal dari beberapa sumber mulai dari client VPN, Host zona IDMZ, client internal (IT) menuju perangkat tujuan pada zona OT maupun endpoint Raspberry Pi. Hasil pengujian akan dinilai berdasarkan keberhasilan koneksi untuk akses yang diizinkan dan kegagalan koneksi untuk akses yang tidak diizinkan.

Tabel 4.8 Skenario Pengujian

NO	Skenario	Sumber	Tujuan	Hasil yang diharapkan	Hasil
1	VPN menuju Raspberry Pi	Client VPN	Raspberry Pi 192.168.8.10	Berhasil Ping	Berhasil

© 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

		10.10.50.1			
2	IDMZ menuju Raspberry Pi	PC IDMZ 10.10.40.10	Raspberry Pi 192.168.8.10	Berhasil Ping	Berhasil
3	VPN menuju OT	Client VPN 10.10.50.1	Perangkat OT 10.10.200.1	Berhasil Ping	Berhasil
4	IDMZ menuju OT	PC IDMZ 10.10.40.10	Perangkat OT 10.10.200.1	Berhasil Ping	Berhasil
5	Internal menuju OT	Client internal (IT)	Perangkat OT 10.10.200.1	Gagal	Gagal
6	Internal menuju Raspberry Pi	Client Internal (IT)	Raspberry Pi 192.168.8.10	Gagal	Gagal

4.4.1.7 Analisis Efektivitas Firewall

Efektivitas firewall pada penelitian ini dianalisis berdasarkan kemampuan firewall dalam memblokir akses tidak sah dari jaringan IT menuju OT. Pengujian dilakukan dengan skenario client dari jaringan IT mencoba mengakses *endpoint* Raspberry Pi yang berada pada zona OT tanpa koneksi VPN. Hasil pengujian efektivitas *firewall* ditunjukkan pada tabel dibawah

Tabel 4.9 Analisis Efektivitas Firewall

NO	Percobaan	Sumber	Tujuan	Kondisi	Hasil Aktual	Status
1	Percobaan 1	Internal/IT	Switch OT	Tanpa VPN	Destination Unreachable	Berhasil Diblokir
2	Percobaan 2	Internal/IT	Raspberry PI	Tanpa VPN	Request Time Out	Berhasil Diblokir
3	Percobaan 3	Internal/IT	Switch	Tanpa	Destinati	Berhasil

© 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

			OT	VPN	on Unreach able	Diblokir
4	Percobaan 4	Internal/IT	Raspbe rry PI	Tanpa VPN	Request Time Out	Berhasil Diblokir
5	Percobaan 5	Internal/IT	Switch OT	Tanpa VPN	Destinati on Unreach able	Berhasil Diblokir
6	Percobaan 6	Internal/IT	Raspbe rry PI	Tanpa VPN	Request Time Out	Berhasil Diblokir
7	Percobaan 7	Internal/IT	Switch OT	Tanpa VPN	Destinati on Unreach able	Berhasil Diblokir
8	Percobaan 8	Internal/IT	Raspbe rry PI	Tanpa VPN	Request Time Out	Berhasil Diblokir
9	Percobaan 9	Internal/IT	Switch OT	Tanpa VPN	Destinati on Unreach able	Berhasil Diblokir
10	Percobaan 10	Internal/IT	Raspbe rry PI	Tanpa VPN	Request Time Out	Berhasil Diblokir

Hasil efektivitas pemblokiran sebesar 100% pada 10 percobaan hal ini menunjukkan bahwa konfigurasi *firewall policy* pada FortiGate telah berfungsi sesuai fungsi *deny*. Prinsip ini menyatakan seluruh trafik yang tidak secara eksplisit diizinkan dalam kebijakan firewall akan diblokir secara otomatis.

Efektivitas *firewall* dihitung berdasarkan jumlah percobaan akses yang tidak sah berhasil di blokir dibandingkan dengan total percobaan pengujian. Rumus yang digunakan adalah sebagai berikut:

$$Persentase\ Pemblokiran = \frac{Jumlah\ Percobaan\ Berhasil\ Diblokir}{Jumlah\ Total\ Percobaan} \text{ x } 100\%$$

$$Persentase\ Pemblokiran = \frac{10}{10} \text{ x } 100\% = 100\%$$

Berdasarkan hasil perhitungan tersebut firewalll memperoleh nilai 100% dalam memblokir akses langsung dari jaringan IT menuju OT dan Raspberry PI, Hal ini juga menunjukkan bahwa kebijakan firewall yang ditetapkan telah berjalan sesuai pada rancangan awal yaitu mencegah *client* yang tidak terhubung VPN untuk mengakses zona OT dan Raspberry PI secara langsung.

© 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

© 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

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian mengenai implementasi dan analisis *Industrial Demilitarized Zone* (IDMZ) pada infrastruktur jaringan PT Kalbio Global Medika dapat disimpulkan sebagai berikut:

1. Implementasi arsitektur keamanan jaringan berbasis Industrial Demilitarized Zone (IDMZ) pada infrastruktur jaringan PT Kalbio Global Medika berhasil membentuk zona pemisah yang jelas antara jaringan IT, IDMZ, OT, dan endpoint Raspberry Pi, sehingga akses langsung dari jaringan internal menuju zona produksi tidak dapat dilakukan tanpa melalui mekanisme verifikasi yang telah ditetapkan .
2. Implementasi segmentasi jaringan dan kontrol akses berbasis kebijakan firewall FortiGate dan SSL-VPN berhasil diterapkan dengan efektivitas pemblokiran sebesar 100% — seluruh 10 percobaan akses langsung dari jaringan IT menuju zona OT tanpa VPN berhasil diblokir sesuai policy yang dikonfigurasi .
3. Berdasarkan hasil pengujian Quality of Service (QoS), penerapan IDMZ tidak menurunkan performa jaringan secara signifikan. Nilai throughput meningkat dari 35,313 Mbps menjadi 50,381 Mbps. Nilai delay meningkat dari 7,346 ms menjadi 13,351 ms dan jitter dari 0,314 ms menjadi 0,823 ms, namun keduanya masih berada dalam kategori baik berdasarkan standar TIPHON. Packet loss tetap 0% pada seluruh sesi pengujian
4. Mekanisme pencatatan log pada firewall FortiGate melalui menu Forward Traffic berhasil merekam seluruh aktivitas trafik antar zona, mencakup alamat IP sumber, tujuan, jenis layanan, waktu akses, serta tindakan firewall yang diambil, sehingga dapat digunakan sebagai bukti audit akses menuju zona produksi.

© 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

5.2 Saran

Berdasarkan analisis dan pengujian terhadap keseluruhan sistem yang sudah dirancang, masih memiliki beberapa kekurangan untuk dilakukan perbaikan dan improvisasi pada penelitian berikutnya. Berikut ini adalah saran-saran dari penulis:

1. Pada penelitian selanjutnya penulis menyarankan agar sistem sebaiknya dilengkapi mekanisme redudansi pada perangkat yang dipakai, hal ini bertujuan agar salah satu koneksi terkendala gangguan atau down, sistem masih akan beroperasi dengan menggunakan perangkat backup.
2. Melakukan pengujian lebih lanjut terhadap aspek *load testing* dan *stress testing* yang mencakup serangan dengan volume trafik tinggi dan durasi yang lebih lama.

© 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

DAFTAR PUSTAKA

Arbie, F.R. dan Raharjo, M. 2024. "Implementasi Keamanan Jaringan dengan Metode Security Profiles menggunakan Fortigate pada Komisi Aparatur Sipil Negara." Jurnal Informatika Terpadu, Vol. 10, No. 1, hlm. 27–34.

Arslan, M.Z. dan Firdaus, A.R. 2026. "Analisis Implementasi Firewall Hardware Fortinet pada Infrastruktur Jaringan di RSKIA Sadewa Yogyakarta." JATI (Jurnal Mahasiswa Teknik Informatika), Institut Teknologi Nasional Malang.

Aryandi, H.A., Tatuhey, E.L. dan Lahallo, J. 2023. "Analisis Quality of Service Pada Jaringan Internet Dinas Lingkungan Hidup dan Kebersihan." Jurnal Ilmiah JATISI, Vol. 10, No. 4, hlm. 291–300.

Anggraeni, N.K.A.S. dan Jasa, L. 2022. "Literatur Review Analisis Metode De-Militarized Zone (DMZ) dan Switch Port Security Sebagai Metode Keamanan Jaringan". *Majalah Ilmiah Teknologi Elektro*, 21(2), hlm. 195. https://doi.org/10.24843/MITE.2022.v21i02.P06

Apilioguliarı, L. 2022. "Digital Transformation in Project-Based Manufacturing: Developing the ISA-95 Model for Vertical Integration". *International Journal of Production Economics*, 245, 108413. https://doi.org/10.1016/j.ijpe.2022.108413

Fernando, M., Jasa, L. dan Hartati, R.S. 2022. "Monitoring System Kecepatan dan Arah Angin Berbasis Internet of Things (IoT) Menggunakan Raspberry Pi 3". *Majalah Ilmiah Teknologi Elektro*, 21(1), hlm. 135–142. https://doi.org/10.24843/MITE.2022.v21i01.P18

Ganesan, E., Andreasen, F.S., Freed, M. dan Escolero, R.E. 2024. "Industrial Network Segmentation Model with Sub-Zone and Sub-Conduit Support". *Technical Disclosure Commons, Defensive Publications Series*, 11 Maret. Art. 6775.

Hussain, M.I., He, J., Zhu, N., Zardari, Z.A., Razque, F., Hussaina, S. dan Pathan, M.S. 2021. "An Archetype for Mitigating the Security Threats in Multi-Cloud Environment by Implementing Tree-Based Next-Generation Firewalls". *Journal of Intelligent & Fuzzy Systems*, 41, hlm. 125–136. https://doi.org/10.3233/JIFS-200835

© 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

Mardianto dan Sutoyo, M.N. 2022. "Implementasi Jaringan Point to Multi Point Menggunakan Metode NDLC". *Jurnal MULTINETICS*, 8(2), hlm. 151–159.

Murad, F.A., Kurniawan, A. and Rasyiidin, M.Y.B., 2025. *Port Knocking pada Mikrotik untuk meningkatkan keamanan WiFi di era industri 4.0*. Jurnal Review Pendidikan dan Pengajaran (JRPP), 8(1), pp.2115–2122. Available at: http://journal.universitaspahlawan.ac.id/index.php/jrpp

Nuñez Alvarez, J.R., Pérez Zamora, Y., Benítez Pina, I. dan Noriega Angarita, E. 2021. "Demilitarized Network to Secure the Data Stored in Industrial Networks". *International Journal of Electrical and Computer Engineering (IJECE)*, 11(1), hlm. 611–619. https://doi.org/10.11591/ijece.v11i1.pp611-619

Ocaka, A., O'Briain, D., Davy, S. dan Barrett, K. 2021. Cybersecurity Threats, Vulnerabilities, Mitigation Measures in Industrial *Control and Automation Systems: A Technical Review*. Ireland: Institute of Technology Carlow dan Waterford Institute of Technology.

Perducat, C., Mazur, D.C., Mukai, W., Sandler, S.N., Anthony, M.J. dan Mills, J.A. 2023. "Evolution and Trends of Cloud on Industrial OT Networks". *IEEE Open Journal of Industry Applications*, 4, hlm. 291. https://doi.org/10.1109/OJIA.2023.3309669

Putra, I.B.A.E.M., Adnyana, M.S.I.D. dan Jasa, L. 2021. "Analisis Quality of Service pada Jaringan Komputer". *Majalah Ilmiah Teknologi Elektro*, 20(1), hlm. 95. https://doi.org/10.24843/MITE.2021.v20i01.P11

Saputro, A., Saputro, N. dan Wijayanto, H. 2020. "Metode Demilitarized Zone dan Port Knocking untuk Keamanan Jaringan Komputer". *CyberSecurity dan Forensik Digital*, 3(2), hlm. 22–27.

Tuasamu, Z., Lewaru, N.A.I.M., Idris, M.R., Syafaat, A.B.N., Faradilla, F., Fadlan, M., Nadiva, P. dan Efendi, R. 2023. "Analisis Sistem Informasi Akuntansi Siklus Pendapatan Menggunakan DFD dan Flowchart pada Bisnis Porobico". *Jurnal Bisnis dan Manajemen (JURBISMAN)*, 1(2), hlm. 495–510. https://ejournal.lapad.id/index.php/jurbisman/article/view/181

© 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

DAFTAR RIWAYAT HIDUP



MUAMMAR ZAIN

Lahir di depok, 1 Oktober 2004. Penulis merupakan anak tunggal, dari pasangan Abidin dan Wahyuni. Penulis memasuki pendidikan formal di SD Negeri Depok 2 pada tahun 2010. Kemudian melanjutkan pendidikan menengah pertama di SMP Negeri 1 Depok pada tahun 2016. Selanjutnya melanjutkan pendidikan atas di SMK Negeri 1 Cibinong pada tahun 2019. Setelah itu pada tahun 2022, Penulis berkesempatan untuk melanjutkan pendidikan tinggi di Politeknik Negeri Jakarta Jurusan Teknik Informatika dan Komputer, Program Studi D4 Teknik Multimedia dan Jaringan.

© 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

LAMPIRAN

Lampiran 1 - Surat Pengantar Pengambilan Data

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
POLITEKNIK NEGERI JAKARTA
Jalan Prof. Dr. G. A.Siwabessy, Kampus UI, Depok 16425
Telepon (021) 7270036, Hunting, Fax (021) 7270034
Laman: http://www.pnj.ac.id Posel: humas@pnj.ac.id

Nomor : 18024/PL3/PK.01.09/2025 — 23 Desember 2025
Perihal : Permohonan Izin Observasi

Kepada Yth.
PT Kalbio Global Medika
Kawasan Industri Delta Silicon 3, Jl. Soka No.2 Blok F19, Cicau, Kec. Cikarang Pusat, Kabupaten Bekasi, Jawa Barat 17530

Dengan hormat,
Sehubungan dengan mata kuliah Skripsi yang dilaksanakan pada semester 8 (delapan) Program Studi Teknik Multimedia dan Jaringan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta. Dengan ini kami mohon kesediaan Bapak/Ibu agar dapat mengizinkan mahasiswa kami untuk melakukan observasi di PT Kalbio Global Medika dengan judul penelitian "Implementasi dan Analisis Demilitarized Zone (DMZ) pada Infrastruktur Jaringan PT Kalbio Global Medika".

Tugas mata kuliah ini bertujuan untuk menambah wawasan terkait dengan aplikasi teori yang sudah dipelajari di Kampus dengan kondisi lapangan sebagai wadah pembelajaran dan penambah informasi mengenai mata kuliah tersebut. Adapun berikut adalah nama mahasiswa kami:

No.	Nama dan Nim	Semester/ Program Studi	Nomor Telepon dan Email	Tujuan Observasi
1	Muammar Zain 2207421010	8 / Teknik Multimedia dan Jaringan	081290414235 muammar.zain.tik22@mhsw.pnj.ac.id	Ingin mengetahui data-data penunjang dan wawancara untuk Skripsi

Demikian surat ini kami buat, atas perhatian dan kerjasama Bapak/Ibu kami ucapkan terima kasih.

a.n Direktur,
Wakil Direktur Bidang Kemahasiswaan
a.b.
Ketua Jurusan,

Dr. Anita Hidayati, S.Kom., M.Kom.
NIP. 197908032003122003

Tembusan :
1. Direktur;
2. Wakil Direktur Bidang Akademik;
3. Kepala Bagian Keuangan dan Umum
4. Kasubbag. Umum Politeknik Negeri Jakarta.

© 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

Lampiran 2 - Surat Balasan dari Perusahaan

KALBE
Kalbio Global Medika

PT KALBIO GLOBAL MEDIKA
Head Office & Manufacturing Site :
Kawasan Industri Delta Silicon 3, Jl. Soka Blok F-19 No. 002
Lippo Cikarang, Kel. Cicau, Kec. Cikarang Pusat, Bekasi 17530
Phone : (021) 5094 3200, Web : www.kalbio.co.id

SURAT KETERANGAN
018/KGM-HR/I/2026

Dengan Hormat,

Menindaklanjuti surat Nomor: 18024/PL3/PK.01.09/2025 perihal Permohonan Izin Observasi, dengan ini kami sampaikan bahwa PT Kalbio Global Medika mengizinkan observasi untuk mengetahui data penunjang dan wawancara untuk Skripsi mahasiswa berikut:

Nama	: Muammar Zain
NIM	: 2207421010
Semester	: 8
Program Studi	: Teknik Multimedia dan Jaringan
Topik	: "Analisis Demilitarized Zone (DMZ) pada Infrastruktur Jaringan PT Kalbio Global Medika"

Observasi akan dilakukan pada Selasa, 20 Jan 2026 didampingi oleh sdr. Ade Kurnia Rahman selaku IT Operation Supervisor dan sdr. Vincent Cunardy selaku IT Application Supervisor untuk melengkapi hasil wawancara yang telah dilakukan tanggal Jumat, 09 Jan 2026. Hasil observasi dan wawancara wajib dijaga kerahasiaan informasi, termasuk dan tidak terbatas pada data teknikal, informasi produk dan proses, dan hasil pengujian. Informasi tersebut tidak boleh digunakan untuk keperluan selain skripsi dan publikasi jurnal internal, dan tidak boleh disebarluaskan ke pihak lain tanpa ijin tertulis dari PT Kalbio Global Medika. Jika terbukti ada penyebaran informasi rahasia ke pihak lain tanpa ijin tertulis dari PT Kalbio Global Medika, maka pihak yang menyebarkan bersedia menanggung tuntutan hukum.

Atas perhatian dan kerjasamanya, kami ucapkan terimakasih.

Senin, 19 Jan 2026
Hormat Kami,

KALBE
Kalbio Global Medika

Steven Amadeus
IT Manager

Lampiran 3 - Dokumentasi Wawancara



© 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

© 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

Lampiran 4 - Lembar Wawancara

Lembar Wawancara

Narasumber : Vincent Cunardy & Ade Kurnia Rahman

Tanggal Wawancara : 09 Januari 2026

No	Pertanyaan	Jawaban
1	Boleh dijelaskan gambaran pembagian jaringan antara jaringan IT dan OT itu apa aja?	Jaringan IT adalah jaringan berbasis bisnis yang mempunyai kebutuhan untuk terhubung dengan internet karena secara kebutuhan masih harus terhubung dengan akses jaringan luar. Sedangkan untuk jaringan OT adalah jaringan operasional yang tujuannya hanya untuk menghubungkan mesin mesin produksi / peralatan manufaktur ke server dan keperluannya hanya untuk mengakses ke jaringan intranet / jaringan lokal
2	Untuk ssid di jaringan PT Kalbio itu ada apa aja dan siapa aja yang bisa mengaksesnya ?	Untuk ssid di kalbio ada beberapa jenis yaitu Onekalbe.net yang digunakan untuk menunjang operasional bisnis adalagi Kalbe_guest untuk tamu dan vendor . Lalu untuk jaringan OT akan menggunakan jaringan kabel agar tidak mengakses dengan menggunakan kabel lan
3	Apakah benar jika sudah terhubung ke jaringan internal itu	Untuk proses sekarang iya masih bisa diakses dari jaringan office namun diharapkan nantinya jaringan OT dapat

	bisa langsung mengakses ke jaringan OT hanya dengan mengetahui alamat IP nya?	bisa terpisah dari jaringan *office* sehingga untuk mengakses dari jaringan *office* ke OT akan melewati *firewall* security
4	Apa saja aset yang dianggap sangat rahasia dan kritikal yang ada di jaringan OT/Server Produksi?	Data proses seperti recept yang ada pada machine yang merupakan data data kritikal dalam proses produksi dan memiliki nilai intrinsik yang harus dipertahankan dan tidak boleh disebarluaskan tanpa izin
5	Siapa saja yang memiliki hak akses untuk bisa tergabung pada jaringan OT?	IT sebagai system administrator serta user yang berada di lapangan manufaktur dan mengakses menggunakan device yang ditetapkan dan dapat mengakses jaringan OT
6	Apa yang menjadi tolak ukur keberhasilan implementasi IDMZ sendiri?	Dengan penerapan IDMZ bisa meningkatkan security level pada perusahaan terutama pada area produksi yang dimana dengan penerapan IDMZ ini bisa mencegah dan mengurangi kebocoran data pada sisi level OT dan tidak menimbulkan downtime pada area OT ketika sisi IT mengalami kendala downtime
7	Langkah pengujian atau testing apa saja yang dilakukan?	Scope pengujian yang dilakukan meliputi pengujian akses ke jaringan OT dari area Office pengujian dari sisi OT ke sisi Office , Pengaksesan menggunakan jaringan luar kalbe via VPN ke jaringan OT

© 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

Cikarang 09 Januari 2026



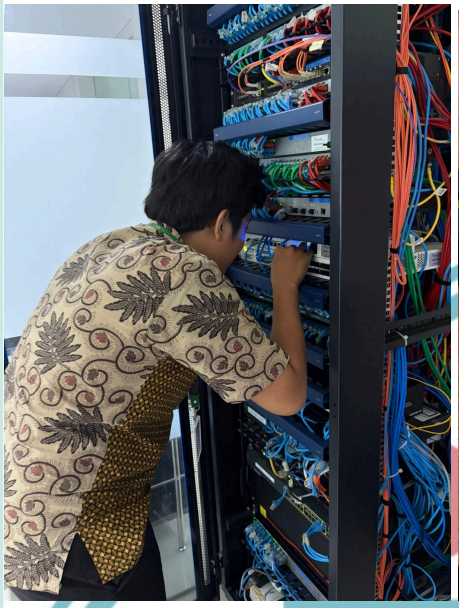
Vincent Cunardy

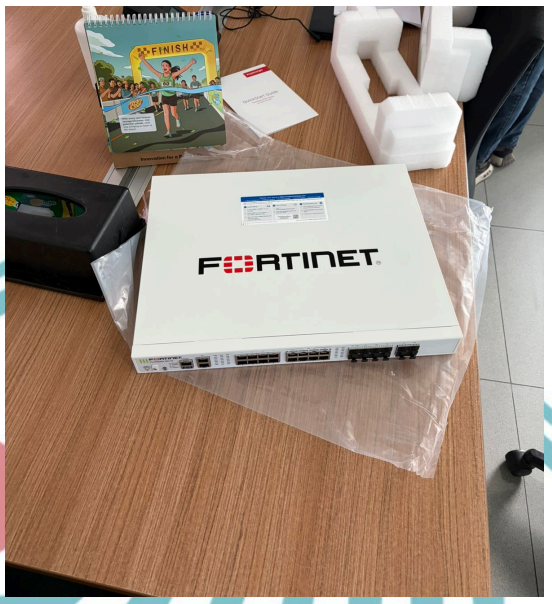
© Hak Cipta milik Politeknik Negeri Jakarta

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

Lampiran 5 - Dokumentasi Kegiatan









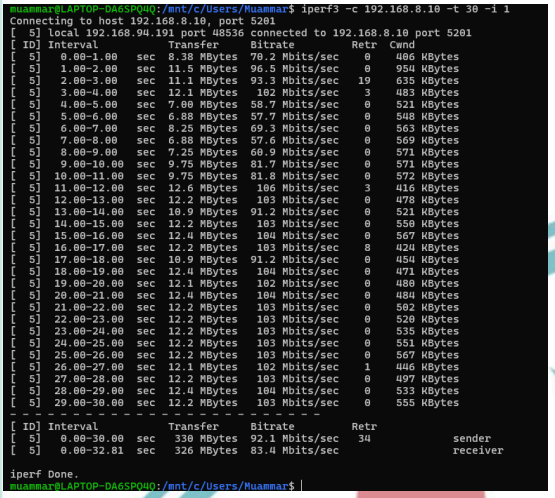
© Hak Cipta milik Politeknik Negeri Jakarta

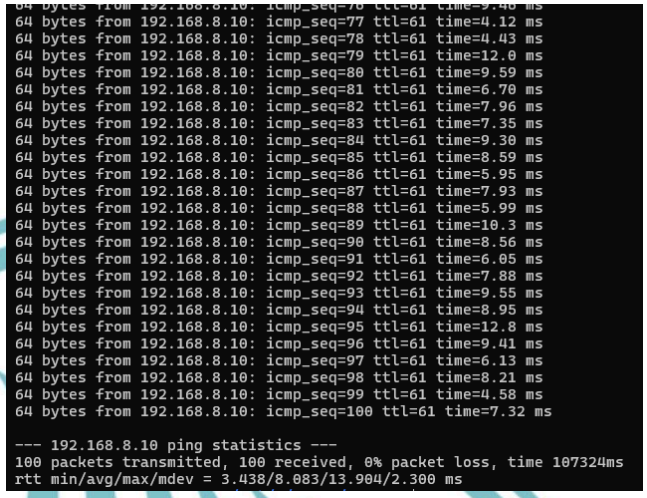
Hak Cipta :
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

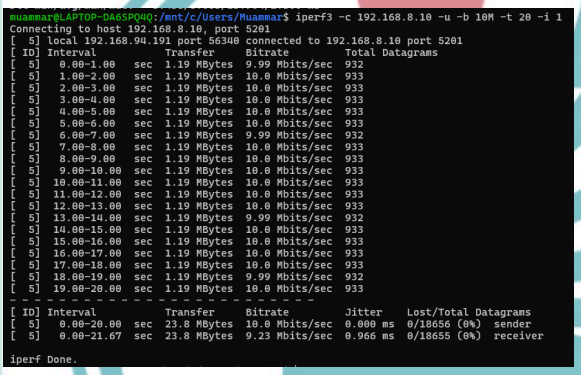
© Hak Cipta milik Politeknik Negeri Jakarta

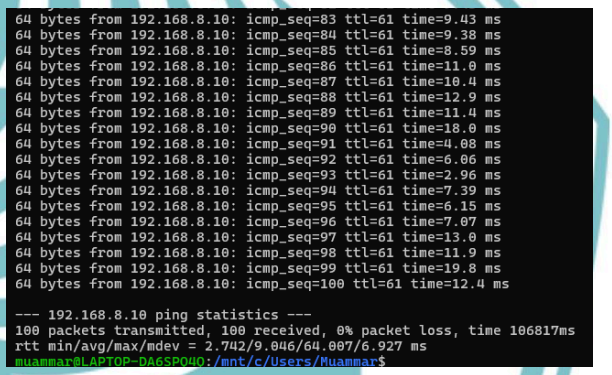
Hak Cipta :

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









Link Lampiran Lengkap:
https://drive.google.com/drive/folders/1Yr8_toHpbU0EHIwQ2vCJtbCi7VWLaAKR?usp=sharing