

LAPORAN
PRAKTIK KERJA LAPANGAN



IMPLEMENTASI SISTEM SD-WAN DAN TUNNEL SITE-TO-SITE
IPSEC VPN PERANGKAT FORTIGATE

RANGGA AZIZZAN HUSSAEN

2207421017

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

DEPOK

2025

HALAMAN PENGESAHAN LAPORAN
PRAKTIK KERJA LAPANGAN

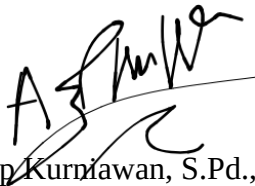
- a. Judul : Implementasi Sistem SD-WAN dan Tunnel site-to-site IPSec VPN Perangkat Fortigate
- b. Penyusun
- 1) Nama : Rangga Azizzan Hussaen
- 2) NIM : 2207421017
- c. Program Studi : Teknik Multimedia dan Jaringan
- d. Jurusan : Teknik Informatika dan Komputer
- e. Waktu Pelaksanaan : 21 Juli 2025 s.d. 30 Desember 2025
- f. Tempat Pelaksanaan : PT Tirta Nawasena Teknologi
- g. Alamat Pelaksanaan : Jl. Melati I Blok I9 No.6B, Pd. Jagung,
Kec.Serpong Utara, Kota Tangerang Selatan,
Banten 15323

Tangerang Selatan, 19 Desember 2025

Mengetahui,

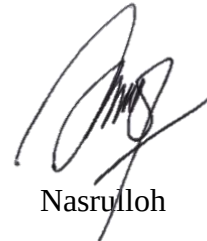
Pembimbing PNJ

Pembimbing Industri



Asep Kurniawan, S.Pd., M.Kom.

NIP. 199109262019031012

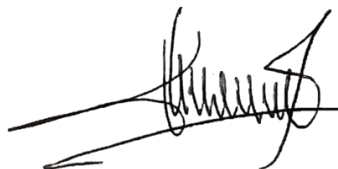


Nasrulloh

NRK. TNT002

Mengesahkan,

KPS Teknik Multimedia dan Jaringan



Dr. Indra Hermawan, S.Kom., M.Kom.

NIP. 198703132019031012

KATA PENGANTAR

Puji Syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmatNya, penulis dapat menyelesaikan laporan Praktik Kerja Lapangan ini. Penulisan laporan Praktik Kerja Lapangan ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Diploma Empat Politeknik. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan laporan Praktik Kerja Lapangan, sangatlah sulit bagi penulis untuk menyelesaikan Laporan Praktik Kerja Lapangan ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

- a. Asep Kurniawan, S.Pd., M.Kom, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan laporan Praktik Kerja Lapangan ini;
- b. Pihak PT Tirta Nawasena Teknologi yang telah banyak membantu dalam usaha memperoleh data yang penulis perlukan;
- c. Orang tua dan keluarga penulis yang telah memberikan bantuan dukungan moral dan material;
- d. Sahabat yang telah banyak membantu penulis dalam menyelesaikan laporan Praktik Kerja Lapangan ini.

Akhir kata, penulis berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga laporan Praktik Kerja Lapangan ini membawa manfaat bagi pengembangan ilmu.

Tangerang Selatan, 19 Desember 2025

Penulis

Rangga Azizzan Hussaen

DAFTAR ISI

HALAMAN PENGESAHAN LAPORAN PRAKTIK KERJA LAPANGAN	ii
KATA PENGANTAR	iii
DAFTAR ISI	iv
DAFTAR GAMBAR	vi
DAFTAR TABEL	vii
BAB I	1
PENDAHULUAN	1
1.1 Latar Belakang Kegiatan	1
1.2 Ruang Lingkup Kegiatan.....	2
1.3 Waktu dan Tempat Pelaksanaan.....	2
1.4 Tujuan dan Kegunaan.....	2
1.4.1 Tujuan	2
1.4.2 Kegunaan	3
BAB II.....	4
LANDASAN TEORI.....	4
2.1 Software-Defined WAN (SD-WAN)	4
2.2 Virtual Private Network (VPN).....	4
2.3 IP Security (IPSec)	5
2.4 FortiGate VM	5
2.5 Wireshark	5
2.6 Local Area Network (LAN)	6
2.7 Wide Area Network (WAN)	6
2.8 Internet Key Exchange (IKE).....	6
2.9 Network Performance.....	7
2.10 Network Address Translation (NAT).....	7
2.11 Internet Control Message Protokol (ICMP)	7
2.12 Domain Name System (DNS)	8
2.13 Firewall.....	8
2.14 Bandwidth	8
2.15 Topologi Jaringan.....	8

2.16 Standar TIPHON	9
BAB III	10
HASIL PELAKSANAAN MAGANG	10
3.1 Profil DUDI.....	10
3.2 Uraian Kegiatan Magang.....	11
3.3 Pembahasan Hasil Magang	13
3.4 Deskripsi Project	15
3.5 Implementasi	18
3.5.1 Konfigurasi Dasar	18
3.5.2 Implementasi SD-WAN dan Konektivitas Internet	20
3.5.3 Implementasi VPN Site-to-Site (Dial-up Mode)	23
3.6 Pengujian dan Pembahasan	27
BAB IV	32
PENUTUP.....	32
4.1 Kesimpulan.....	32
4.2 Saran.....	32
DAFTAR PUSTAKA	34

DAFTAR GAMBAR

Gambar 2.1 Konsep SD-WAN.....	4
Gambar 2.2 Tampilan Wireshark.....	5
Gambar 2.3 Topologi Jaringan.....	8
Gambar 3.1 Logo Perusahaan	10
Gambar 3.2 Struktur Organisasi Perusahaan	11
Gambar 3.3 Topologi Jaringan Proyek	14
Gambar 3.4 Diagram Alir Konfigurasi Implementasi SD-WAN dan Konektivitas Internet	15
Gambar 3.5 Diagram Alur Konfigurasi VPN Site-to-Site Metode Dial-up dengan Traversal.....	17
Gambar 3.6 Konfigurasi IP Address Interface Management	19
Gambar 3.7 Mengaktifkan Service DNS Server	19
Gambar 3.8 Konfigurasi Interface WAN1	20
Gambar 3.9 Konfigurasi Interface WAN2	20
Gambar 3.10 Konfigurasi Implementasi SD-WAN Zone.....	21
Gambar 3.11 Konfigurasi Performance SLA SD-WAN.....	22
Gambar 3.12 Konfigurasi Static Rules SD-WAN.....	22
Gambar 3.13 Konfigurasi Policy Interface Lokal ke SD-WAN	23
Gambar 3.14 Konfigurasi Fortigate Kantor Pusat Sebagai Responder.....	23
Gambar 3.15 Konfigurasi Autentikasi VPN IPSec Responder	24
Gambar 3.16 Konfigurasi Policy dan Routing VPN Responder.....	25
Gambar 3.17 Konfigurasi Fortigate Kantor Cabang Sebagai Initiator	25
Gambar 3.18 Konfigurasi Autentikasi VPN IPSec Initiator	26
Gambar 3.19 Konfigurasi Policy dan Routing VPN Initiator	26
Gambar 3.20 Mengaktifkan VPN Tunnel IPSec.....	27

DAFTAR TABEL

Tabel 3.1 Spesifikasi Firewall Fortigate	18
Tabel 3.2 Standar Parameter QoS (TIPHON).....	27
Tabel 3.3 Pengujian Parameter throughput, latency, dan jitter 2 ISP (SD-WAN)28	
Tabel 3.4 Pengujian Parameter throughput, latency, dan jitter 1 ISP (SD-WAN)28	
Tabel 3.5 Pengujian Parameter Packet Loss	29
Tabel 3.6 Pengujian Failover SD-WAN	30
Tabel 3.7 Pengujian Application Steering	30
Tabel 3.8 Pengujian Konektivitas VPN	31

BAB I

PENDAHULUAN

1.1 Latar Belakang Kegiatan

Teknologi yang berkembang menuntut tingginya *high availibilyt*, efisiensi biaya, performa optimal, dan fleksibilitas jaringan untuk memenuhi kebutuhan pengguna dengan bandwidth yang semakin tinggi. Untuk memenuhi kebutuhan bandwidth yang tinggi dan *high availability* tersebut, teknologi WAN berevolusi menjadi *Software Defined Wide Arena Network* atau SD-WAN.

Migrasi jaringan ke SD-WAN membantu mengelola infrastruktur IT menjadi lebih mudah. Teknologi ini menawarkan fleksibilitas, keamanan, serta kenyamanan bagi pengguna dalam melakukan skalabilitas infrastruktur IT. Dengan keunggulan dari tersebut, SD-WAN dapat diandalkan pada perusahaan-perusahaan yang memiliki banyak cabang.

Perangkat yang memiliki tekonologi tersebut salah satunya adalah Fortigate, yang merupakan perangkat firewall dari Fortinet.inc. Beberapa fitur yang ada pada perangkat ini adalah fitur website *filtering*, domain dan IP blocking, SD-WAN, Tunneling. Dengan memfilter paket jaringan yang keluar dan masuk dapat memberikan kemanan bagi perangkat yang ada pada infrastruktur yang ada di dalamnya.

PT Tirta Nawasena Teknologi merupakan perusahaan *Information and Communication Technology* (ICT) yang menyediakan berbagai kebutuhan IT bagi perusahaan. Kegiatan magang yang dilakukan merupakan permintaan implementasi perangkat firewall Fortigate dengan konfigurasi SD-WAN dan Tunneling Site-Site pada salah satu mitra.

Selama kegiatan peraktik kerja lapangan, penulis aktif dalam berbagai kegiatan operasional, salah satunya melakukan kegiatan konfigurasi perangkat firewall Fortigate.

Kegiatan konfigurasi yang dilakukan pada perangkat firewall Fortigate ini berupa penerapan fitur SD-WAN sebagai failover dan pengambil keputusan untuk jalur WAN berdasarkan kondisi link state, performa, serta kebijakan aplikasi, serta tunnel IPsec untuk menghubungkan jaringan local antara kantor pusat dengan kantor cabang dengan aman dengan metode dial-up.

1.2 Ruang Lingkup Kegiatan

Pelaksanaan magang dilakukan pada PT Tirta Nawasena Teknologi divisi *Network Operating Center* (NOC). Ruang lingkup kegiatan pada divisi ini berupa implementasi perangkat firewall Fortigate dengan rincian sebagai berikut:

- a. Mempelajari bagaimana melakukan konfigurasi dasar perangkat firewall Fortigate.
- b. Mempelajari bagaimana fungsi dan konfigurasi SD-WAN firewall Fortigate.
- c. Mempelajari bagaimana cara menghubungkan antar kantor cabang dengan menggunakan *Tunnel IPsec* dengan metode dial-up.

1.3 Waktu dan Tempat Pelaksanaan

Waktu Pelaksanaan : 21 Juli 2025 s.d. 30 Desember 2025

Tempat Pelaksanaan : PT Tirta Nawasena Teknologi

Divisi Pelaksanaan : Network Operating Center

Jam Pelaksanaan : Pukul 08.00 WIB hingga pukul 16.00 WIB

Alamat Perusahaan : Jl. Melati I Blok I9 No.6B, Pd. Jagung, Kec.Serpong
Utara, Kota Tangerang Selatan, Banten 15323

1.4 Tujuan dan Kegunaan

1.4.1 Tujuan

Adapun tujuan penulisan laporan magang dengan judul Implementasi Sistem SD-WAN dan Tunnel Site-to-Site IPsec VPN Perangkat Fortigate pada PT Tirta Nawasena Teknologi untuk mitra, sebagai berikut:

- a. Implementasi sistem SD-WAN dan Tunnel Site-to-Site IPsec VPN perangkat Fortigate
- b. Analisis kinerja SD-WAN dan Tunnel Site-to-Site IPsec VPN perangkat Fortigate

1.4.2 Kegunaan

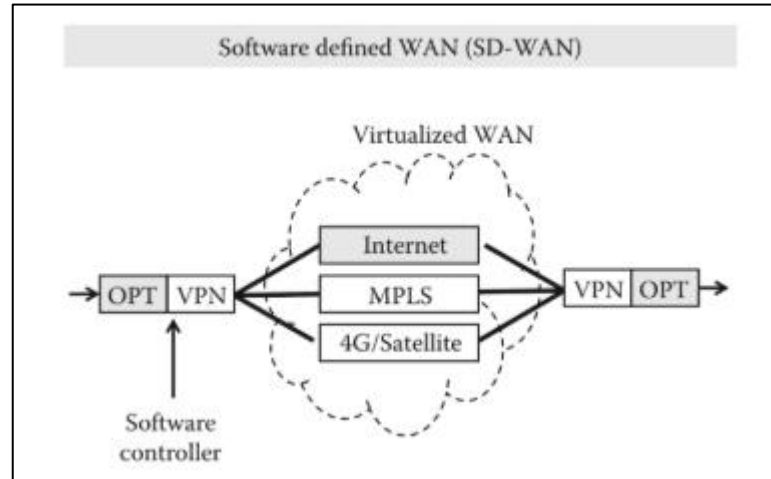
Kegunaan penulisan laporan magang dengan judul Implementasi Sistem SD-WAN dan Tunnel Site-to-Site IPSec VPN Perangkat Fortigate pada PT Tirta Nawasena Teknologi untuk mitra, sebagai berikut:

- a. Menentukan jalur WAN yang dilalui oleh *host* yang ada dengan kebijakan aplikasi yang telah ditentukan.
- b. Memperoleh informasi mengenai *destination* yang dituju *host* beserta jalur WAN yang dilalui.
- c. Menghubungkan jaringan lokal antara kantor pusat dengan kantor cabang agar dapat mengakses *resource* yang ada.

BAB II

LANDASAN TEORI

2.1 Software-Defined WAN (SD-WAN)



Gambar 2.1 Konsep SD-WAN
(Sumber: Terry Critchley, Making It in IT, 2017)

Software-Defined WAN (SD-WAN) merupakan sebuah pengembangan jaringan dari WAN, yang mengintegrasikan beberapa layanan konektivitas seperti internet *broadband*, *wireless* 4G/5G, VSAT serta lainnya.

Secara umum, *SD-WAN* didesain untuk mengontrol aliran data, fleksibilitas, kontrol terpusat, dan monitoring. Ini mempermudah dalam kustomisasi, pengoperasian, serta mengaplikasikan kebijakan dalam jaringan (Madhu, S., & Shankar, A, 2024).

2.2 Virtual Private Network (VPN)

Virtual Private Network (VPN) menjadi salah satu metode keamanan jaringan dalam pendistribusian layanan paket data di dalam jaringan internet. *VPN* menawarkan fungsional yang lebih fleksibel dan privasi. Pada jaringan komputer keamanan dalam pengiriman paket data sangat penting untuk menjamin bahwa paket data yang dikirimkan pada pihak yang dituju tidak dapat diakses pada pihak yang tidak berkepentingan (Firmansyah, F., Wahyudi, M., & Purnama, R. A., 2021).

Dengan mengimplementasikan *VPN*, akan memberikan perlindungan serta privasi dalam melindungi paket data dalam jaringan internet, serta menghubungkan akses *resource* jarak jauh pada jaringan lokal secara aman.

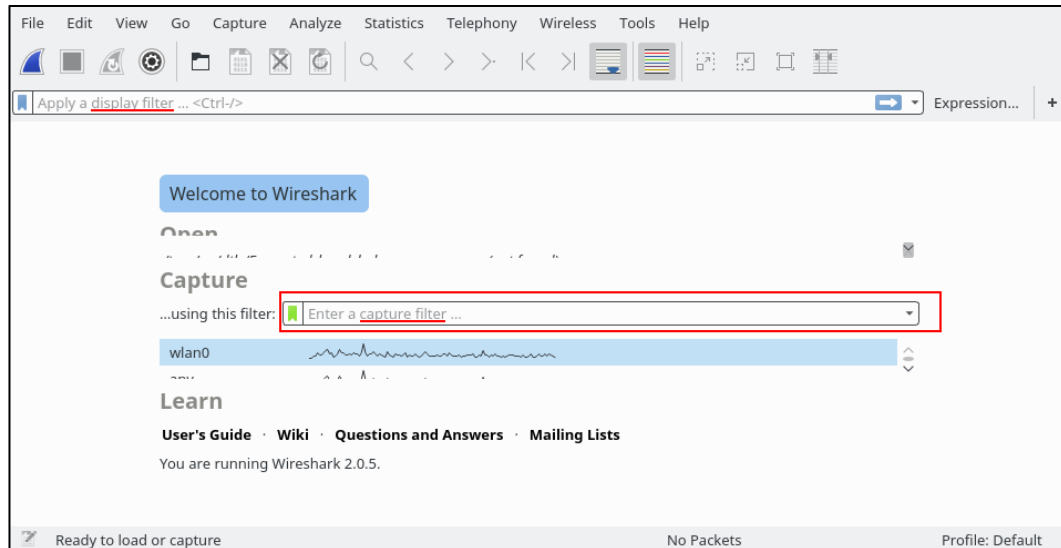
2.3 IP Security (IPSec)

Internet Protocol Security (IPSec) adalah protokol yang digunakan dalam membuat *VPN* untuk mengamankan paket data dalam jaringan internet. *IPSec* menawarkan 3 layanan utama, yaitu otentikasi dan integritas data, kerahasiaan, dan manajemen kunci (Wicaksana, P., Hadi, F., & Hadi, A. F., 2021)

2.4 FortiGate VM

FortiGate VM merupakan *cloud firewall* yang menyediakan keamanan Fortigate juga berfungsi sebagai *router gateway*. Perangkat ini menawarkan fitur unggulan seperti *Web Application Firewall (WAF)*, *Intrusion Prevention System (IPS)*, and *Antivirus* (Azami, M., Haryadi, I. P., & Husain., 2025).

2.5 Wireshark



Gambar 2.2 Tampilan Wireshark
(Sumber: wiki.wireshark.org, 2020)

Wireshark merupakan alat analisis protokol yang mengambil trafik dan mempresentasikan ke format yang dapat dipahami oleh manusia. Wireshark memberikan *framework* yang komprehensif untuk menganalisis lalu lintas jaringan, dan ini berjalan pada banyak sistem operasi.

Ini digunakan oleh *network administrator* dan *security analyst* pada skala yang luas, seperti industri, pemerintahan, dan organisasi non-profit. Dalam menganalisis, diperlukan untuk masuk ke *data stream* dan mengambil paket dari jaringan. Setelah paket didapatkan, dilakukan analisis paket untuk mengetahui bagaimana alur jaringan (Bock, L., 2022).

2.6 Local Area Network (LAN)

LAN merupakan jaringan komputer yang cakupannya relatif kecil, seperti kantor, sekolah, atau gedung. Jaringan ini menghubungkan berbagai perangkat dalam skala kecil agar setiap perangkat dapat saling berkomunikasi dan berbagi sumber daya (Alamin, Z., & Mu'min, M. A., 2024).

Media yang digunakan pada jaringan LAN untuk komunikasi data antar perangkat umumnya menggunakan wired media kabel Untwisted Pair (UTP) dan wireless dengan media wireless Fidelity (WIFI). Perangkat yang ada dalam lingkup ini biasanya terdiri dari switch, hub, komputer, printer, access point.

2.7 Wide Area Network (WAN)

Jaringan yang cakupan wilayahnya meliputi antar negara bahkan antar benua. Media pengiriman data pada jaringan ini lebih bervariasi, seperti kabel optik, satelit, serta jaringan selular seperti 4G, 5G (Army, W. L., Barovih, G., Seta, H. B., Guntoro, Margiutomo, S. A. S., Arifianto, T., Pujiyanto, D., Mutasar, Nurhabibah, & Faj, T. I., 2022).

2.8 Internet Key Exchange (IKE)

Internet Key Exchange merupakan protokol *key management* yang digunakan untuk mengamankan komunikasi dan pertukaran kunci antara dua perangkat pada semua jaringan. Terdapat 2 phase dalam IKE Tunnel Negotiation, Phase 1 melakukan pertukaran proposal bagaimana untuk mengautentikasikan dan mengamankan channel, phase 2 mengasosiasikan cara mengamankan data yang ditransmisikan melalui IPSec tunnel setelah keamanan dan autentikasi terbentuk (Alapati, Y. K., Rao, K. S. & Sreeramamurthy, K., 2024).

2.9 Network Performance

Cara untuk memastikan kualitas layanan untuk memastikan performa dari sebuah jaringan. Melakukan pemeriksaan *network performance* ini penting dalam mengetahui seberapa efektif model jaringan yang digunakan. Performa jaringan dapat dimodelkan dan diukur dengan beberapa hal seperti *latency*, *jitter*, serta *packet loss*.

Latency merupakan waktu tempuh yang diperlukan dalam melakukan pengiriman data dari pengirim ke penerima hingga data kembali ke pengirim. *Jitter* merupakan variasi kedatangan paket yang terjadi dalam jaringan saat waktu tertentu. *Packet loss* merupakan istilah pada kondisi paket yang gagal untuk ditransmisikan pada alamat tujuan (Suprpto, A., 2020).

2.10 Network Address Translation (NAT)

Network Address Translation berfungsi untuk mengizinkan banyak perangkat dalam mengakses internet melalui satu IP Address. Terdapat 2 jenis NAT: 1 Static NAT (SNAT), 2 Dynamic NAT (DNAT).

Static NAT mengoneksikan IP private ke internet melalui 1 IP public tetap, hal ini dapat dijumpai dalam suatu perusahaan yang mana end device dapat terhubung ke internet walau berada dalam jaringan local. Dynamic NAT mengoneksikan IP private dengan IP Publik, ini memungkinkan jaringan Internet dapat mengakses layanan yang ada pada jaringan local (Suprpto, A., 2020).

2.11 Internet Control Message Protokol (ICMP)

ICMP merupakan suatu mekanisme yang digunakan oleh host dan gateway untuk mengirim notifikasi datagram yang mengalami masalah kepada host pengirim. ICMP digunakan untuk perangkat yang terhubung melalui Internet untuk analisis jaringan. Penggunaan ICMP yang terkenal adalah ping dan traceroute. ICMP juga digunakan untuk memberikan pesan kesalahan jika layanan yang diminta tidak ada, atau komputer atau router yang akan di akses tidak dapat dijangkau (Afif, N. & Ridwang., 2021).

2.12 Domain Name System (DNS)

Domain Name System (DNS) adalah sebuah sistem yang menyimpan informasi nama host ataupun nama domain dalam bentuk basis data yang tersebar didalam data jaringan komputer. Sebuah layanan jaringan yang menerjemahkan nama situs web menjadi alamat IP (Wibowo, A., 2023).

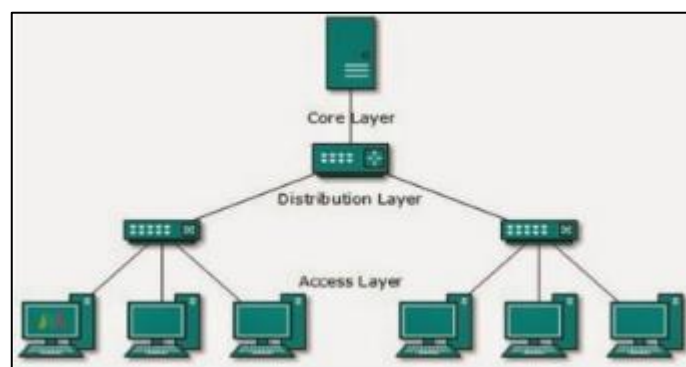
2.13 Firewall

Firewall berfungsi untuk mengamankan jaringan dengan mengevaluasi trafik-trafik yang keluar masuk pada jaringan internet atau jaringan lokal, mengizinkan trafik-trafik tertentu dan memblok yang lainnya. Firewall merupakan suatu mekanisme yang diterapkan terhadap *hardware*, *software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, menyaring, membatasi, bahkan menolak suatu kegiatan dalam jaringan (Irfana, Satraa, R. & Fattah, F., 2021).

2.14 Bandwidth

Bandwidth merupakan besaran yang menunjukkan seberapa banyak data yang dapat dilewatkan dalam koneksi melalui jaringan. *Bandwidth* sendiri menunjukkan volume data yang dapat ditransfer per unit waktu. Dengan *bandwidth* yang besar memungkinkan pengiriman informasi yang besar (Zackiansyah, A.A., 2022).

2.15 Topologi Jaringan



Gambar 2.3 Topologi Jaringan

(Sumber: Al-Khowarizmi, Pengantar Teknologi Informasi (Dalam Perkembangan Data Science), 2020)

Suatu cara atau konsep yang digunakan untuk menghubungkan dua komputer atau lebih, baik menggunakan kabel maupun nirkabel. Tujuan dari topologi jaringan adalah untuk kemudahan dalam pertukaran informasi. Topologi jaringan sangat penting pada perusahaan atau lembaga dengan ruang lingkup yang luas, karena akan mempengaruhi bagaimana aliran data berlangsung (Aldo, D., Ardi, Nengsih, Y.G., Syafrinal, I. & Putra, N. 2020).

2.16 Standar TIPHON

Quality of Service (QoS) dalam penelitian ini mengacu pada standar *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON)* yang diterbitkan oleh *European Telecommunications Standards Institute (ETSI)*. Sebagai badan standarisasi regional yang diakui di bidang telekomunikasi dan jaringan, ETSI menetapkan parameter spesifik untuk mengukur keandalan dan kinerja pengiriman data. Berdasarkan standar TIPHON tersebut, aspek-aspek krusial yang dianalisis meliputi *throughput*, *delay*, *jitter*, dan *packet loss*.

BAB III

HASIL PELAKSANAAN MAGANG

3.1 Profil DUDI



Gambar 3.1 Logo Perusahaan

PT Tirta Nawasena Teknologi merupakan penyedia layanan terpercaya dalam sektor *Facility Management* dan Solusi *TI End-to-End*. Fokus utama perusahaan meliputi pengelolaan sumber daya lintas industri, pengamanan aset, serta optimalisasi teknologi guna meningkatkan efisiensi operasional dan performa bisnis.

Kapabilitas teknis perusahaan terbukti melalui portofolio layanan yang komprehensif. Pada ranah infrastruktur dan basis data, layanan mencakup pengelolaan *DB Cluster SQL*, *End-to-End Network Management* (termasuk *Firewall*, *Switch*, & *Access Point*), serta pemeliharaan perangkat keras seperti penggantian komponen Dell EMC Unity 300. Ketahanan data diperkuat melalui *Deployment Backup System* menggunakan Dell EMC Data Domain.

Dalam aspek keamanan siber dan integritas data, solusi canggih diterapkan melalui implementasi Trend Micro (IPS, DDAN, & EDR) serta layanan Data *Privacy*, *Encryption* & *Integration*. Layanan ini mencakup proteksi data sensitif menggunakan *Advanced Encryption Standard* (AES), penerapan Format *Preserving Encryption* tanpa mengubah skema basis data, serta pemastian kepatuhan terhadap regulasi perlindungan data. Integrasi sistem didukung oleh pengembangan API, data staging dari sistem ERP, serta optimalisasi infrastruktur cloud dan *data warehouse* yang ada. Keseluruhan ekosistem teknologi ini dijaga kinerjanya melalui layanan *Support L1* untuk *troubleshooting* dan monitoring berkelanjutan.

Komitmen terhadap keunggulan dan profesionalisme telah membangun kepercayaan dari berbagai mitra strategis dan klien ternama, termasuk PNL, SBI, Epson, Waskita, SIG, Visindo Prima Nusantara, dan Universitas Negeri Jakarta.



Gambar 3.2 Struktur Organisasi Perusahaan

Dalam pelaksanaan magang, ditempatkan pada divisi NOC. Divisi tersebut bertanggung jawab untuk melakukan pengawasan, pengelolaan, dalam jaringan perusahaan. Terdapat layer 1 dan layer 2 pada divisi, layer 2 berperan sebagai leader yang bertanggung jawab kepada NOC head officer dan project manager.

3.2 Uraian Kegiatan Magang

Kegiatan pada minggu pertama membantu tim *system engineer* dalam melakukan penambahan *storage* pada *server* hypervisor *vmware vcenter*. Penambahan *storage* ini ditujukan untuk menambah kapasitas penyimpanan untuk operasional. Penambahan *storage* dilakukan dengan metode *hot plugging*, metode ini merupakan suatu metode yang dapat dilakukan pada sebuah server dalam menambahkan suatu komponen tanpa harus mematikan server, salah satunya menambahkan *storage*.

Selain penambahan *storage* dilakukan juga penambahan RAM pada *server*. Dalam penambahan RAM dilakukan dengan mematikan server secara bergantian agar server tetap berjalan. Dikarenakan server digunakan sebagai hypervisor vmware, selain penambahan dilakukan secara fisik, dilakukan juga penambahan dalam sisi hypervisor agar sistem dapat mengidentifikasi *resource* terbaru.

Di minggu kedua dan berikutnya penulis diposisikan ke dalam divisi *Network Operating Center* (NOC). Dalam divisi ini penulis ditugaskan untuk membantu tim NOC dalam memantau, mengelola, serta memelihara infrastruktur jaringan perusahaan.

Kegiatan yang dilakukan penulis dalam membantu tim NOC diuraikan sebagai berikut: 1. Pemantauan terhadap perangkat jaringan, 2. Mengerjakan permintaan sesuai dengan tiket yang diberikan, 3. Melakukan *backup* konfigurasi pada perangkat *firewall*, *core switch*, *distribution switch*, dan *policy management platform*, 4. Menyusun laporan mingguan untuk penggunaan *bandwidth* jaringan pada setiap wilayah, 5. Analisis user dengan *session* jaringan tertinggi, 6. Melakukan pemeriksaan terhadap utilitas penggunaan *resource* pada perangkat jaringan.

Dalam menjalani tugas sebagai NOC, terdapat beberapa aplikasi, *tools*, serta akun yang diberikan. Untuk melakukan pemantauan diperlukan aplikasi FortiClient VPN, ini diperlukan untuk dapat mengakses jaringan lokal serta *tools* yang diperlukan. *Tools* yang digunakan dalam pemantauan perangkat jaringan berupa PTRG. Perangkat yang ada dalam pemantauan berupa *firewall*, bila terdapat jaringan internet *down* maka akan dilakukan eskalasi kepada PIC terkait.

Penanganan tiket yang paling umum dilakukan adalah melakukan reset akun VPN. VPN yang digunakan merupakan salah satu fitur dari perangkat *firewall* Fortigate. Dalam menangani tiket yang ada, perusahaan menggunakan aplikasi ServiceDesk Plus digunakan dalam menerima tiket dan memproses tiket.

Selain Fortigate, perangkat *firewall* yang digunakan adalah Palo Alto. Palo Alto digunakan sebagai *layer* utama dalam keamanan jaringan. Terdapat beberapa fitur

yang digunakan seperti *blocking* IP dan URL, wifi captive portal, serta sebagai routing network.

Terdapat jadwal untuk melakukan backup konfigurasi perangkat jaringan. Perangkat yang dilakukan backup meliputi *firewall*, *core switch*, *distribution switch*, dan *policy management platform*. Untuk melakukan backup dilakukan dengan CyberArk.

CyberArk merupakan Privileged Access Management (PAM) yang berfungsi untuk mengamankan akun dengan akses tertinggi dalam sistem IT. Dengan CyberArk mengakses berbagai macam perangkat jaringan secara terpusat. Perangkat yang terdata dalam CyberArk terdiri dari *firewall*, *core switch*, dan *distribution switch*.

Terdapat *meeting* setiap minggu untuk memaparkan aktifitas NOC. Data yang dipaparkan berupa *consume bandwidth site*, *backup devices*, dan *Network Utilization By Session*. Data tersebut diperoleh dari fitur yang ada pada *firewall* Palo Alto. Data tersebut digunakan untuk menganalisis penggunaan jaringan untuk evaluasi pada bulan selanjutnya.

Perangkat *core switch*, *distribution switch*, dan *firewall* dilakukan *preventive maintenance* sebanyak satu kali seminggu. Ini ditujukan untuk mengaudit *resource* pada perangkat, seberapa mampu dalam menangani *traffic* saat kondisi padat.

Pengambilan data *Network Utilization By Session* dilakukan pada jam akhir kerja, pada seluruh wilayah cabang. Data yang diperoleh kemudian dilakukan analisis yang menghasilkan tiga wilayah dengan data *session* pada user yang paling tinggi.

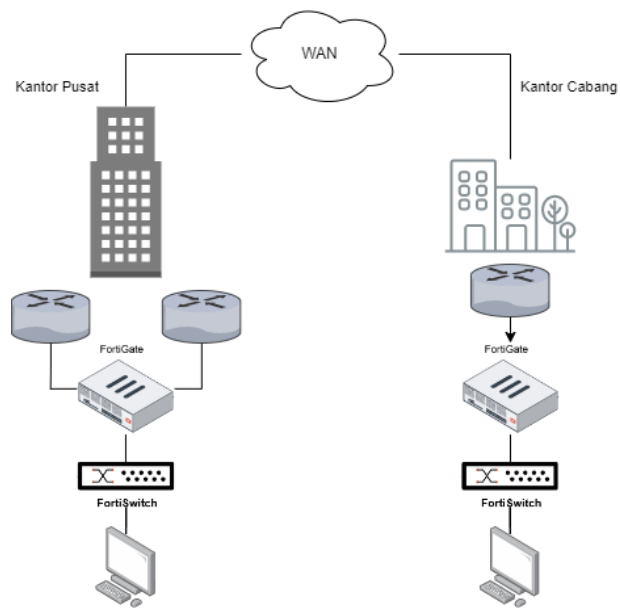
Uraian magang tersebut bersumber pada logbook harian yang dapat dilihat pada lampiran 1.

3.3 Pembahasan Hasil Magang

Project yang dilakukan selama magang di PT Tirta Nawasena Teknologi, yaitu melakukan konfigurasi pada perangkat *firewall* Fortigate VM untuk

menghubungkan jaringan lokal antara kantor pusat dengan kantor cabang. Protokol yang digunakan dalam project ini berupa VPN tunnel IPSec.

Pemilihan protokol IPSec untuk koneksi site-to-site didasarkan pada kemampuannya beroperasi dalam *network layer*. Hal ini memungkinkan interkoneksi antar-subnet tanpa perlu adanya konfigurasi tambahan pada sisi end-device.

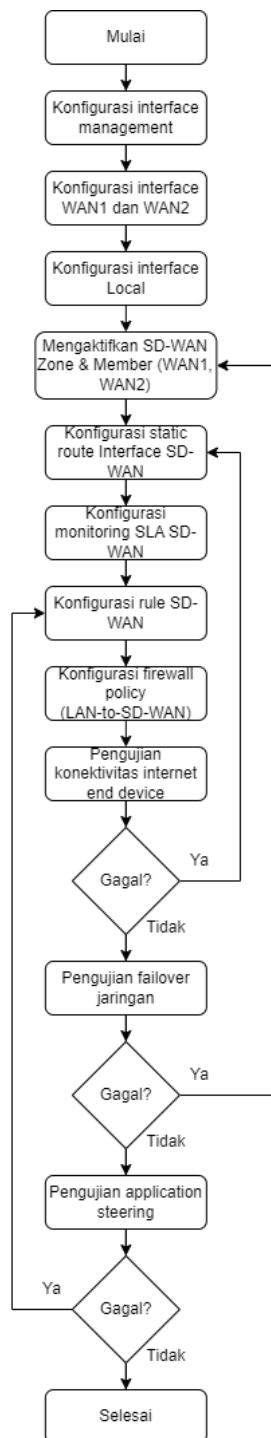


Gambar 3.3 Topologi Jaringan Proyek

Skenario yang ada pada project ini kantor pusat memiliki IP publik statis, sedangkan kantor cabang berada dalam NAT ISP. Dalam kondisi tersebut fortigate akan mendapatkan IP Private alih-alih IP Publik. Agar perangkat dapat saling berkomunikasi dan membuat tunnel, maka dilakukan implementasi dengan metode *dial-up*.

Kondisi tersebut mengharuskan perangkat Fortigate kantor pusat menjadi *responder*, sementara perangkat Fortigate kantor cabang berperan sebagai *initiator*. Sebagai responder diharuskan memiliki IP Publik statis agar layanan jaringan yang dibangun stabil. Untuk lebih detail dapat dilihat pada Gambar 3.2.

3.4 Deskripsi Project



Gambar 3.4 Diagram Alir Konfigurasi Implementasi SD-WAN dan Konektivitas Internet

Gambar 3.4 mengilustrasikan alur konfigurasi SD-WAN pada perangkat *firewall* Fortigate. Pada tahap awal dilakukan konfigurasi interface management untuk keperluan administratif. Dilanjutkan konfigurasi interface internet pada WAN1

dan WAN2. Setelah Fortigate dapat mengakses jaringan internet, kemudian konfigurasi interface lokal untuk jaringan perangkat end-device.

Untuk mengaktifkan fitur SD-WAN, buat zone dan member untuk SD-WAN dengan memasukkan interface WAN1 dan WAN2. Setelah terbentuk SD-WAN, dilakukan *default* route agar SD-WAN dapat menjangkau jaringan internet. Agar dapat berjalan optimal, diperlukan monitoring SLA SD-WAN agar sistem dapat menentukan jalur yang paling optimal.

Agar SD-WAN dapat memisahkan traffic berdasarkan kebijakan, maka dilakukan konfigurasi rule SD-WAN berdasarkan interface yang telah ditentukan. Kebijakan yang ditentukan berupa *internet service* dan *application*. (tambahkan lagi)

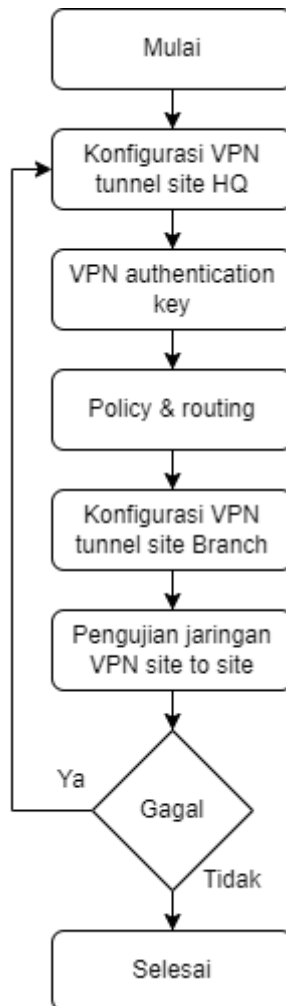
Agar jaringan lokal dapat mengakses internet melalui interface WAN maka dilakukan konfigurasi firewall policy. Policy dibuat untuk mengizinkan lalu lintas jaringan dari LAN menuju SD-WAN. Ini penting agar perangkat yang ada pada jaringan lokal dapat mengakses jaringan internet dengan kebijakan yang telah ditentukan.

Setelah konfigurasi SD-WAN dan konektivitas internet dilakukan, tahap selanjutnya melakukan pengujian. Perangkat end-device yang berada pada jaringan lokal firewall Fortigate harus bisa terhubung ke jaringan internet melalui member SD-WAN. Bila end-device tidak dapat konektivitas internet, maka dilakukan pengecekan pada konfigurasi static route interface SD-WAN, memastikan adanya default route 0.0.0.0/0 yang mengarah ke interface SD-WAN.

Pengujian dilanjutkan dengan failover konektivitas internet, karena salah satu fitur SD-WAN adalah melakukan failover bila salah satu jalur mengalami gangguan. Pengujian dilakukan dengan menonaktifkan salah satu interface WAN. Jika hasil pengujian menunjukkan end-device tidak dapat terkoneksi setelah beberapa saat salah satu interface WAN dimatikan, maka konfigurasi SD-WAN gagal, sehingga diperlukan pengecekan ulang pada SD-WAN zone dan member.

Pengujian terakhir dilakukan pada fitur *application steering*. Ini dilakukan agar kebijakan berdasarkan *internet service* dan *application* dapat berjalan sesuai

dengan apa yang ditetapkan. Indikator keberhasilan dilihat dari *forward traffic log*. Pada *destination port*, *SD-WAN quality*, dan *SD-WAN rule name* akan terdata jalur mana dipakai berdasarkan kebijakan yang ditetapkan. Jika indikator tidak terpenuhi, maka dilakukan konfigurasi ulang pada *rule* SD-WAN.



Gambar 3.5 Diagram Alur Konfigurasi VPN Site-to-Site Metode Dial-up dengan Traversal

Gambar 3.5 mengilustrasikan alur konfigurasi VPN Tunnel Site-to-Site antara perangkat Fortigate kantor utama dengan perangkat firewall Fortigate kantor cabang. Tahap pertama dilakukan konfigurasi perangkat firewall Fortigate sebagai responder dengan wizard VPN tunnel Site-to-Site dengan kunci otentikasi yang aman.

Konfigurasikan policy dan routing antara jaringan lokal kantor pusat dengan kantor cabang. Pada perangkat firewall Fortigate kantor cabang dilakukan

konfigurasi sebagai initiator dengan mengaktifkan opsi NAT Traversal pada wizard VPN karena perangkat berada di belakang NAT. Setelah tunnel terbentuk dilakukan konfigurasi routing dan firewall policy pada sisi kantor cabang.

Tahap akhir dilakukan pengujian jaringan VPN Site-to-Site antar perangkat end-device pada kantor pusat dengan kantor cabang. Bila dalam log VPN tidak terdapat data masuk dan keluar maka dilakukan pemeriksaan terhadap konfigurasi awal VPN. Indikator VPN berhasil dibuat dengan melihat paket data masuk dan keluar dan status active, serta perangkat end-device pada kedua kantor dapat saling berkomunikasi.

3.5 Implementasi

Tahap implementasi ini adalah realisasi dari topologi dan diagram alur yang telah dirancang sebelumnya. Pada *project* ini, konfigurasi dilakukan menggunakan lingkungan virtualisasi (Fortigate VM) dengan sistem operasi FortiOS versi 7. Implementasi dibagi menjadi 2, yaitu konfigurasi software-defined WAN (SD-WAN) untuk manajemen lalu lintas jaringan, dan membangun tunnel VPN IPSec Site-to-Site menggunakan metode dial-up untuk menghubungkan kantor cabang yang berada di balik NAT.

Pada konfigurasi yang akan dilakukan, rincian spesifikasi perangkat keras dan lunak yang digunakan dalam skenario implementasi dilampirkan pada Tabel 3.1.

Tabel 3.1 Spesifikasi Firewall Fortigate

<i>Processor</i>	1 core
RAM	2 GB
Port	3

3.5.1 Konfigurasi Dasar

Konfigurasi awal yang dilakukan berupa pemberian IP *address* pada *port management*. Selain untuk manajemen perangkat, ini digunakan juga sebagai *interface* jaringan lokal. Dalam melakukan konfigurasi ini menggunakan kabel *console* untuk masuk ke dalam sistem CLI dari perangkat firewall Fortigate.

```

FortiGate-UM64 (port3) # set ip
<class_ip&net_netmask>      IP address and subnet mask (syntax = 1.1.1.1/24).

FortiGate-UM64 (port3) # set ip 10.0.1.254/24
<Enter>

FortiGate-UM64 (port3) # set ip 10.0.1.254/24

FortiGate-UM64 (port3) # set allowaccess
ping          PING access.
https         HTTPS access.
ssh           SSH access.
snmp          SNMP access.
http          HTTP access.
telnet        TELNET access.
fgfm          FortiManager access.
radius-acct   RADIUS accounting access.
probe-response Probe access.
fabric        Security Fabric access.
ftm           FTM access.
speed-test    Speed test access.

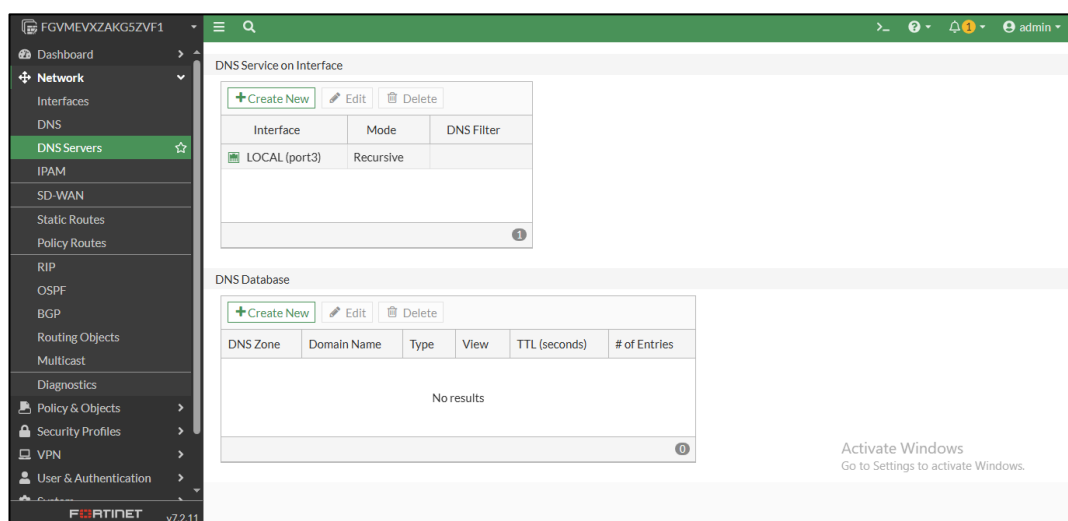
FortiGate-UM64 (port3) # set allowaccess ping https ssh
FortiGate-UM64 (port3) #

```

Gambar 3.6 Konfigurasi IP Address Interface Management

Berdasarkan Gambar 3.6 di atas, dilakukan konfigurasi IP *address* pada port 3. Pemberian IP dilakukan dengan format **[IP address]/[prefix]**. Setelah pemberian IP pada *interface*, selanjutnya memberikan akses *service*. Akses yang diberikan berupa *service* ping, https, dan juga ssh.

Tahap selanjutnya mengaktifkan *service* DNS Server pada perangkat firewall Fortigate. Ini dilakukan agar end-device dapat mengakses domain pada jaringan internet.

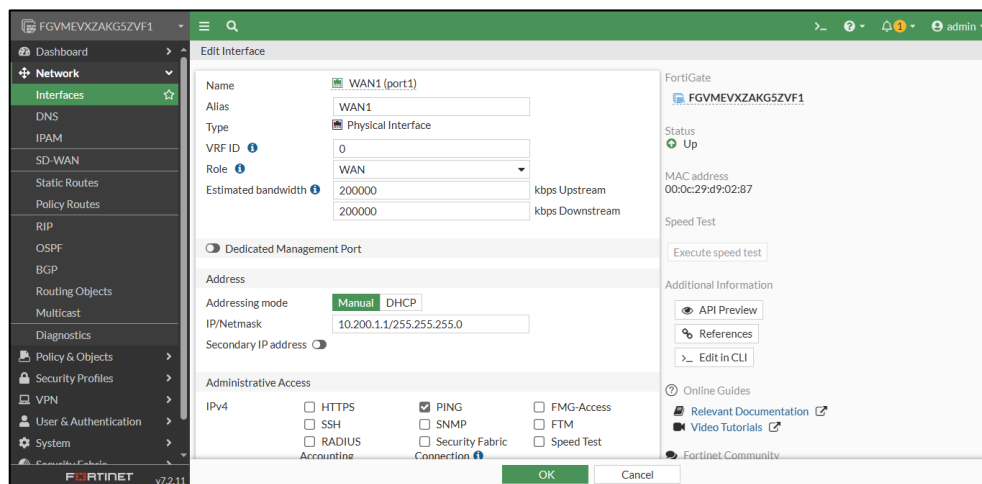


Gambar 3.7 Mengaktifkan Service DNS Server

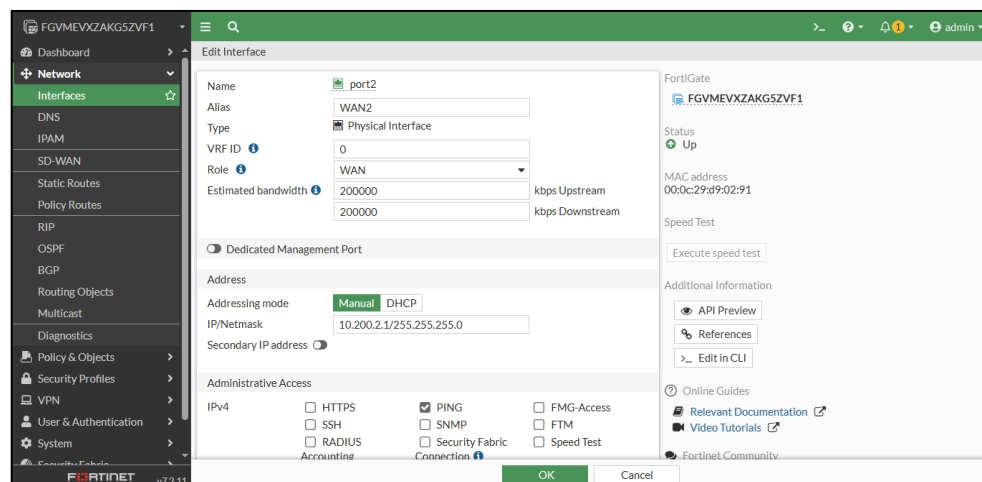
Dalam konfigurasi ini perangkat firewall Fortigate bertindak sebagai DNS Server. Mode yang digunakan adalah recursive, ini bertujuan agar Fortigate meneruskan permintaan domain dari end-device menuju DNS server publik yang telah dikonfigurasi pada menu System DNS. Dalam penerapannya dapat dilihat pada Gambar 3.7.

3.5.2 Implementasi SD-WAN dan Konektivitas Internet

Agar Fortigate mendapatkan akses internet, maka dilakukan konfigurasi pada interface WAN. Dalam skenario ini digunakan 2 interface WAN, ini bertujuan agar bila salah satu ISP mati, layanan internet masih dapat berjalan dengan ISP lainnya.



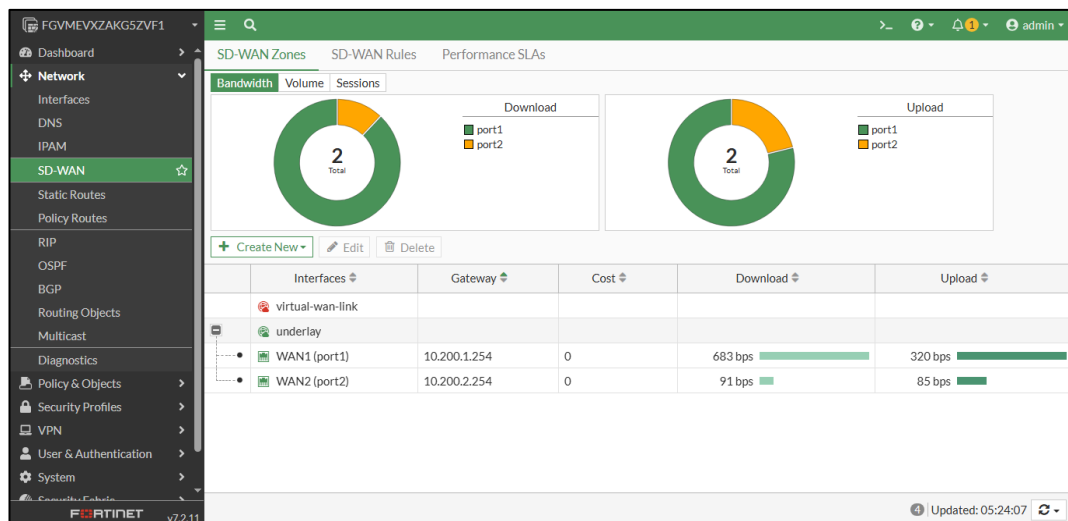
Gambar 3.8 Konfigurasi Interface WAN1



Gambar 3.9 Konfigurasi Interface WAN2

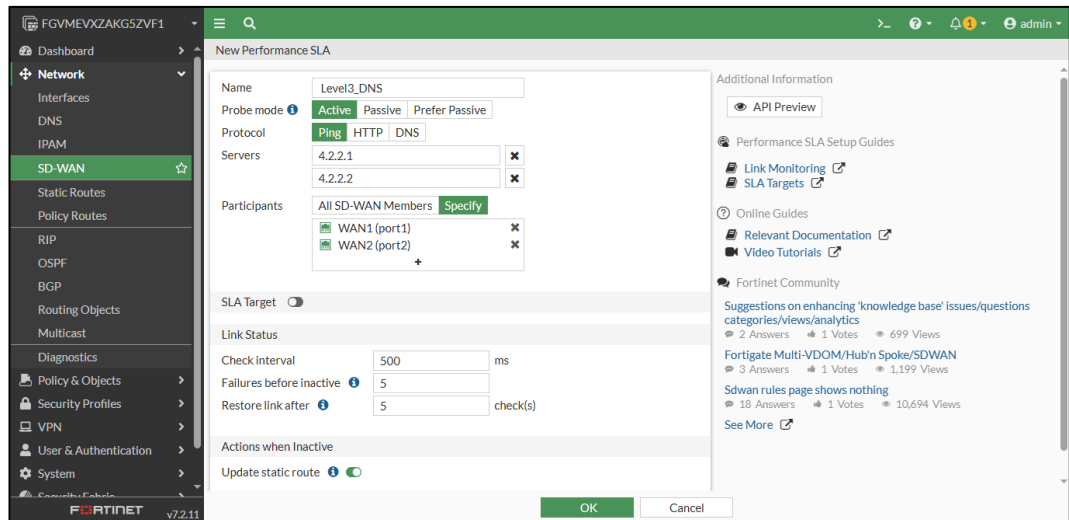
Konfigurasi *interface* WAN dilakukan dengan memilih role untuk interface, dalam hal ini menggunakan role WAN. Pemberian alias tidak wajib, namun disarankan agar mempermudah dalam identifikasi interface. Untuk nilai bandwidth diambil berdasarkan bandwidth yang diberikan oleh ISP. Detail konfigurasi WAN1 dapat dilihat pada Gambar 3.8 dan WAN2 pada Gambar 3.9.

Setelah interface WAN1 dan WAN2 terbentuk, tahap selanjutnya adalah membuat SD-WAN Zone. SD-WAN Zone berfungsi untuk menggabungkan menjadi objek tunggal sebagai jalur keluar internet.



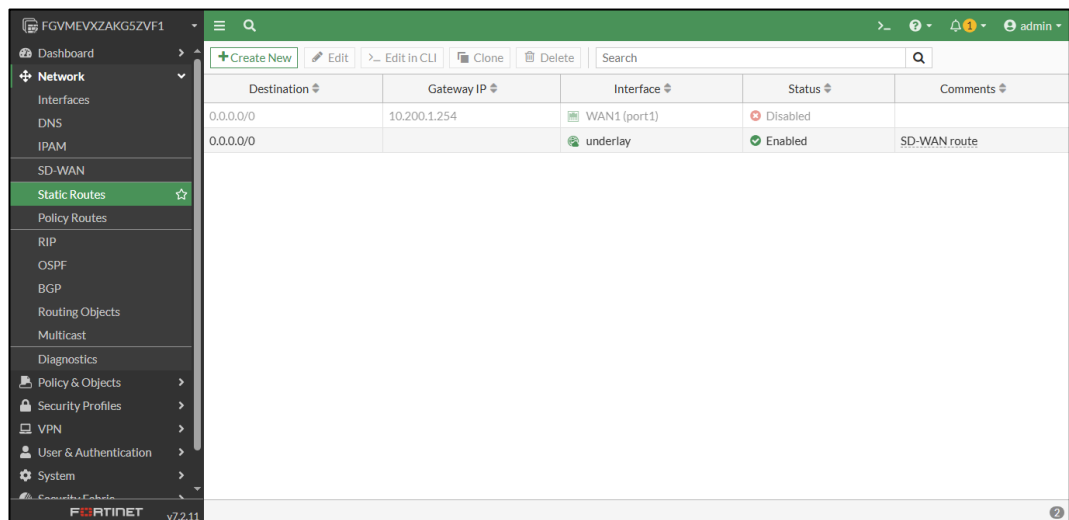
Gambar 3.10 Konfigurasi Implementasi SD-WAN Zone

Pada Gambar 3.10 dilakukan konfigurasi terhadap WAN1 dan WAN2 menjadi satu zone interface underlay. Ini dilakukan dengan menambahkan interface member kedalam zone yang dibuat. Nilai priority yang dikonfigurasi pada kedua interface tersebut adalah sama, ini dimaksudkan agar kondisi yang ditetapkan dalam mode *active-active*.



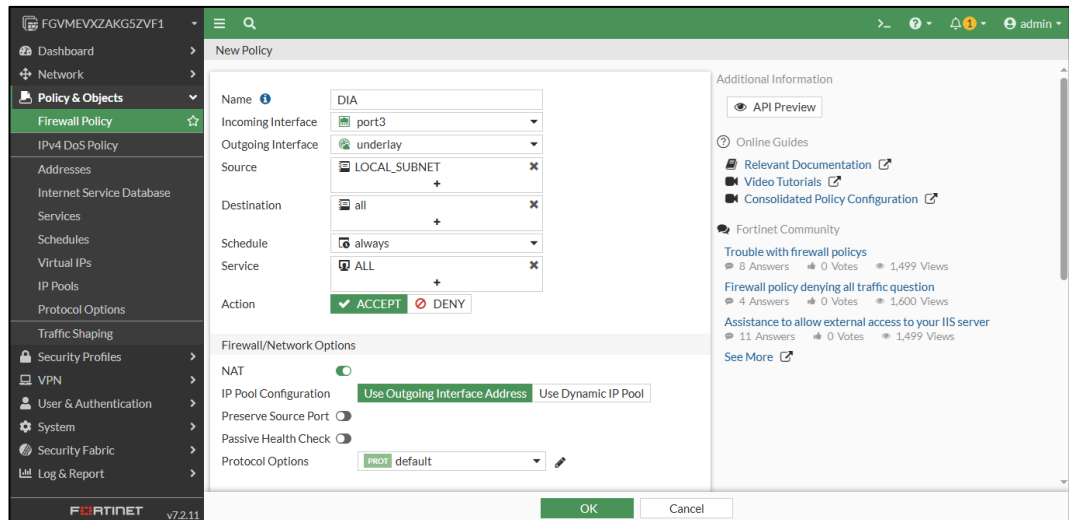
Gambar 3.11 Konfigurasi Performance SLA SD-WAN

Performance SLA digunakan untuk mengontrol kualitas terhadap SD-WAN yang telah dibuat. Sebagai alat ukur kualitas jalur yang digunakan, maka akan dilakukan protokol *ping* terhadap server 4.2.2.1 dan 4.2.2.2 sebagai acuan. Dengan interval pengiriman paket *ping* setiap 500ms. Untuk detailnya dapat dilihat pada Gambar 3.11.



Gambar 3.12 Konfigurasi Static Rules SD-WAN

Membuat default route **0.0.0.0/0** untuk interface SD-WAN agar dapat mengarahkan seluruh trafik yang menuju internet agar melalui interface SD-WAN. Ini menyederhanakan tabel routing agar tidak perlu membuat static route untuk setiap interface WAN.

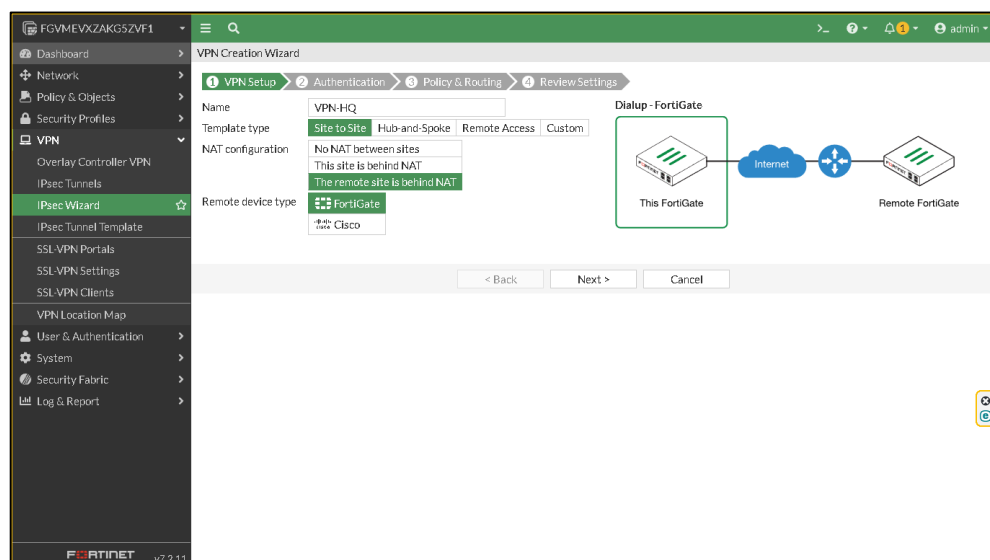


Gambar 3.13 Konfigurasi Policy Interface Lokal ke SD-WAN

Agar jaringan lokal dapat mengakses internet, maka dilakukan *allow* trafik dari interface port lokal ke interface SD-WAN. Berikan akses *all* pada *destination* dan *service* agar end-device mendapatkan akses penuh. Centang opsi NAT agar jaringan lokal dapat mengakses internet.

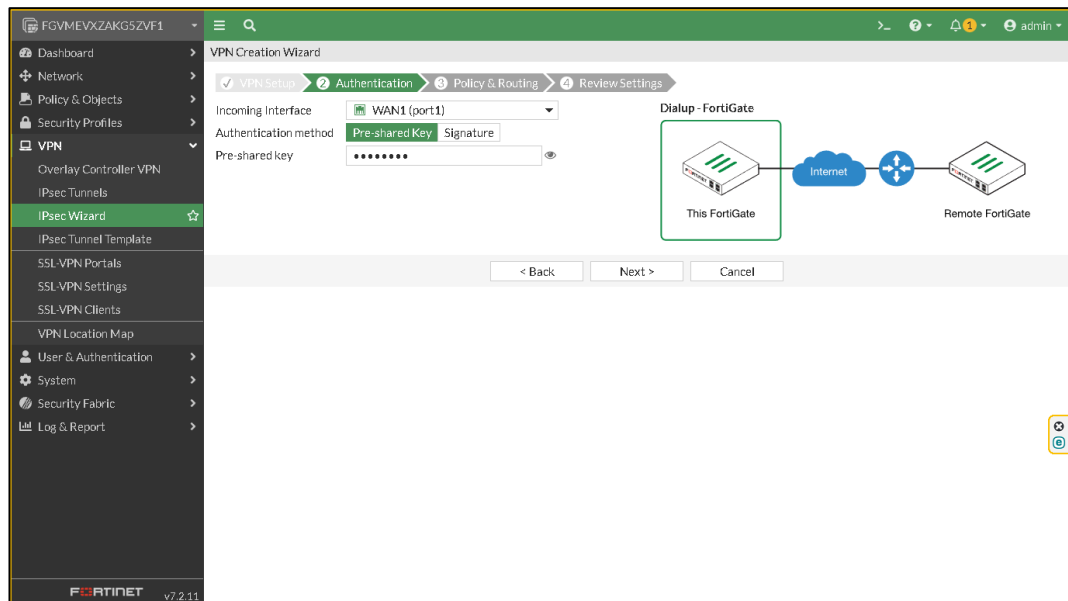
3.5.3 Implementasi VPN Site-to-Site (Dial-up Mode)

Untuk membuat VPN Site-to-Site, dibutuhkan konfigurasi pada dua sisi, pada kantor cabang dan kantor utama. Perangkat Fortigate kantor pusat berperan sebagai *responder* dan perangkat Fortigate kantor cabang sebagai *initiator*.



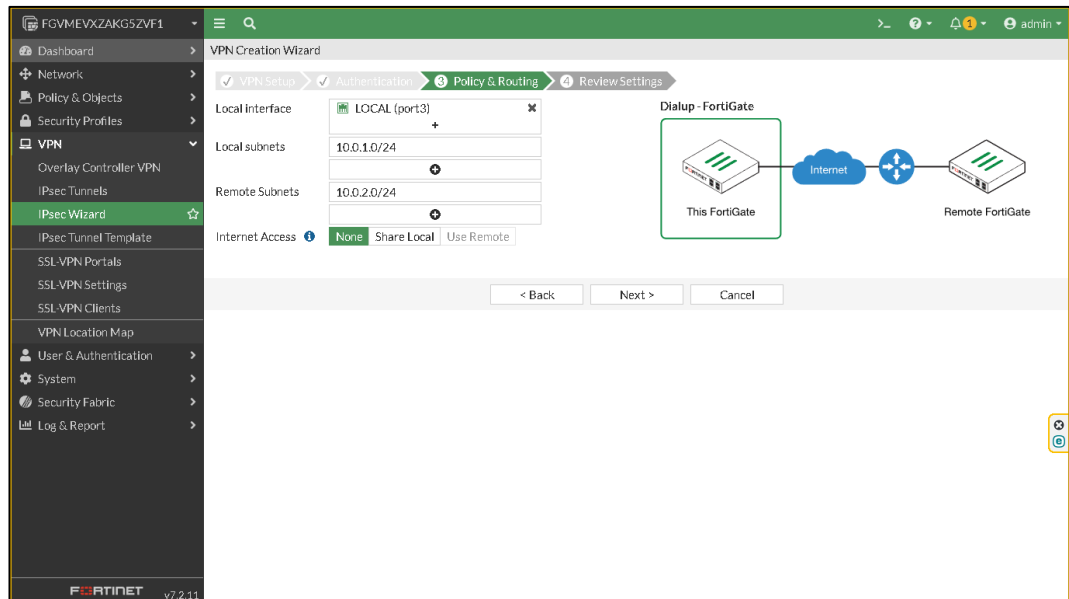
Gambar 3.14 Konfigurasi Fortigate Kantor Pusat Sebagai Responder

Pada Gambar 3.14 dilakukan konfigurasi VPN dengan menu VPN Wizard untuk mempermudah dalam pembuatan tunnel. Agar tunnel dibuat antar perangkat Fortigate, maka dipilih tipe Site-to-Site dengan *device* Fortigate. Dikarenakan perangkat Fortigate kantor pusat memiliki IP Publik statis dan kantor cabang berada dalam kondisi NAT ISP, maka dipilih konfigurasi **the remote site is behind NAT**.



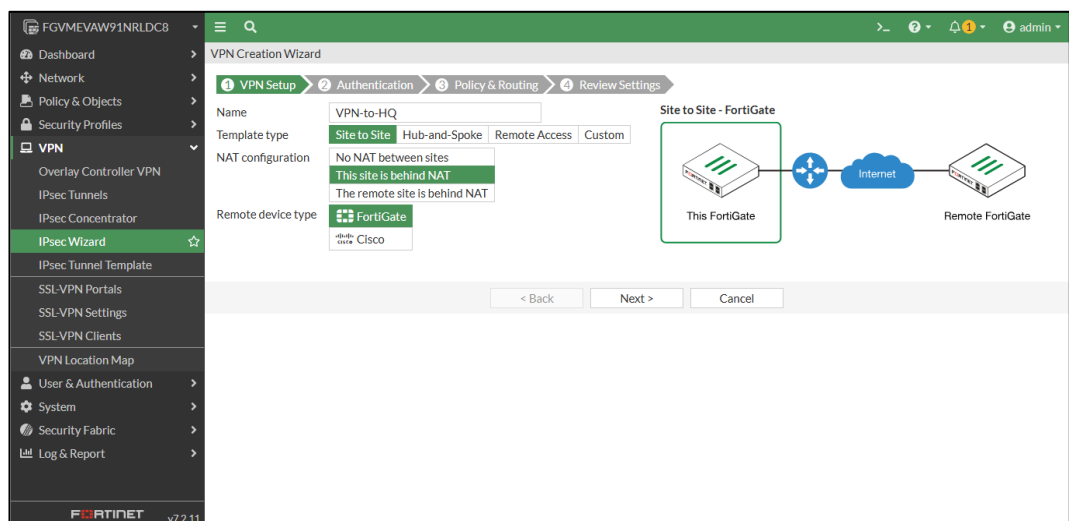
Gambar 3.15 Konfigurasi Autentikasi VPN IPsec Responder

Langkah selanjutnya membuat autentikasi pada tunnel yang akan dibuat. Pada Gambar 3.15 dilakukan pemilihan interface yang akan digunakan sebagai jalur tunnel. Agar tunnel dapat dibangun, diperlukan metode autentikasi yang sama. Pre sharedkey berfungsi untuk memverifikasi identitas peer sebelum sesi IKE dibangun.



Gambar 3.16 Konfigurasi Policy dan Routing VPN Responder

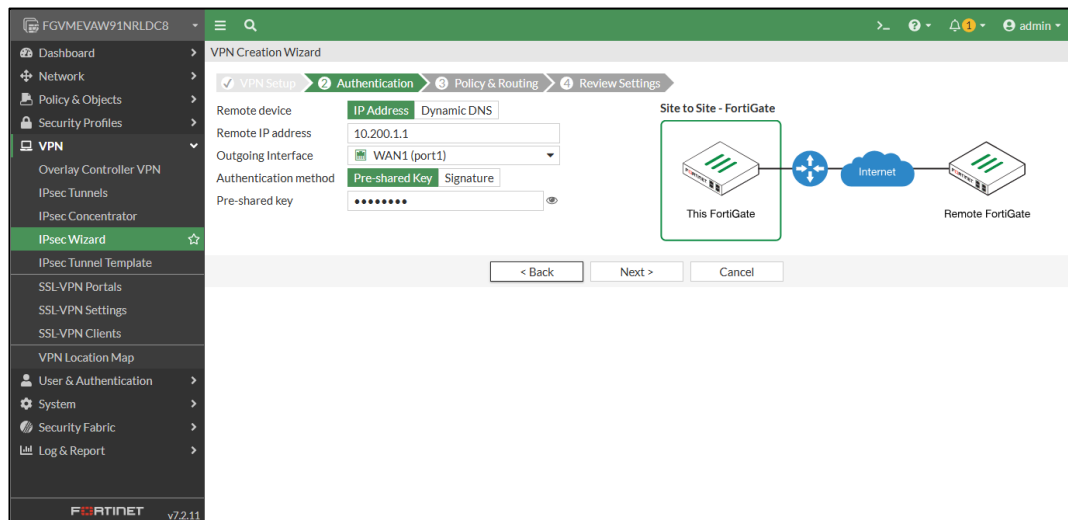
Dilakukan konfigurasi policy dan routing untuk jaringan lokal pada antar perangkat Fortigate. Ini dilakukan agar jaringan lokal pada kantor pusat dan kantor cabang. Dalam skenario yang ditetapkan, perangkat end-device mendapat akses internet dari masing-masing Fortigate, ini dilakukan agar tidak membebani jalur VPN Tunnel yang dibuat, sehingga hanya ditujukan untuk mengakses resource pada kantor pusat saja.



Gambar 3.17 Konfigurasi Fortigate Kantor Cabang Sebagai Initiator

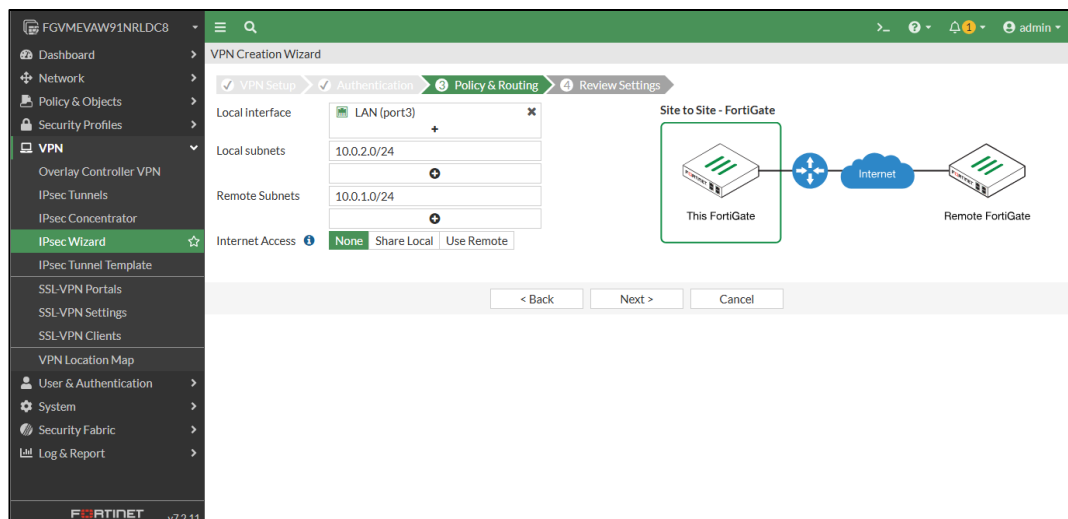
Pada perangkat Fortigate kantor cabang dilakukan konfigurasi VPN IPsec Wizard seperti kantor pusat, namun dengan kondisi yang disesuaikan sebagai

initiator. Pada Gambar 3.17 Dikarenakan perangkat Fortigate Cabang berada pada kondisi dibelakang NAT ISP, maka dipilih konfigurasi **this site is behind NAT**.



Gambar 3.18 Konfigurasi Autentikasi VPN IPsec Initiator

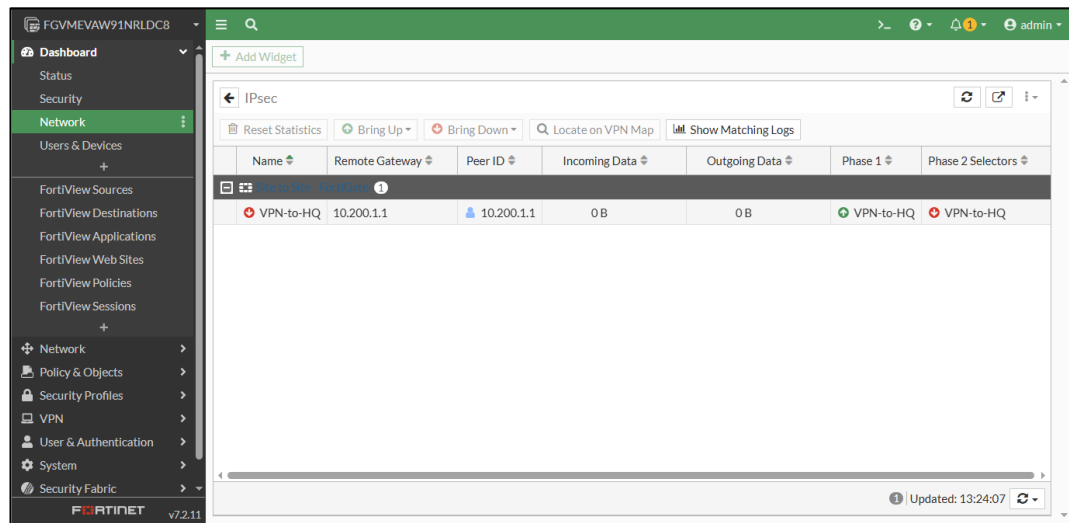
Langkah selanjutnya membuat autentikasi pada tunnel yang akan dibuat. Pada Gambar 3.18 dilakukan pemilihan interface yang akan digunakan sebagai jalur tunnel. Agar tunnel dapat dibangun, diperlukan metode autentikasi yang sama dengan *Responder*.



Gambar 3.19 Konfigurasi Policy dan Routing VPN Initiator

Seperti pada responder, initiator dilakukan juga konfigurasi policy dan routing. Pada remote dan local subnet disesuaikan dengan network yang digunakan.

Untuk akses internet end-device menggunakan jalur Fortigate lokal, tidak menggunakan jalur Fortigate kantor pusat.



Gambar 3.20 Mengaktifkan VPN Tunnel IPsec

Setelah semua konfigurasi pembuatan tunnel selesai, langkah selanjutnya adalah mengaktifkan VPN dari perangkat Fortigate kantor cabang (initiator). Ini dilakukan karena tunnel tidak aktif otomatis setelah konfigurasi dilakukan, sehingga diperlukan bring up VPN secara manual.

3.6 Pengujian dan Pembahasan

Untuk memverifikasi hasil konfigurasi, dilakukan serangkaian pengujian konektivitas guna memastikan jaringan yang digunakan sesuai dengan standar operasional. Pengujian dilakukan dengan kombinasi utilitas, meliputi Command Prompt (Ping) untuk uji konektivitas dasar, Speedtest CLI untuk pengukuran bandwidth, dan Wireshark untuk analisis protokol lalu lintas data.

Evaluasi jaringan dilakukan dengan pengukuran parameter QoS. Dalam pengujian ini akan divalidasi berdasarkan kategori kualitas layanan standar TIPHON (ETSI TS 101 329-1). Parameter kelayakan yang ditetapkan adalah sebagai berikut:

Tabel 3.2 Standar Parameter QoS (TIPHON)

Kategori Kualitas	Indeks	Throughput	Latency	Jitter	Packet Loss
Sangat Bagus	4	> 2.1 Mbps	< 150 ms	0 ms	0%
Bagus	3	1.2 – 2.1	150 – 300 ms	0 – 75 ms	3%

		Mbps			
Sedang	2	700 – 1200 Kbps	300 – 450 ms	75 – 125 ms	15%
Buruk	1	< 700 Kbps	> 450 ms	125 – 225 ms	25%

Berikut data pengujian parameter *throughput*, *latency*, dan *jitter* yang didapatkan pada *host* dengan utilitas *ookla speedtest cli* terhadap server PT Mora Telematika Indonesia (Moratel) dengan skenario 2 ISP (SD-WAN):

Tabel 3.3 Pengujian Parameter *throughput*, *latency*, dan *jitter* 2 ISP (SD-WAN)

Nomor Pengujian	Throughput Download (Mbps)	Throughput Upload (Mbps)	Latency / Idle (ms)	Jitter (ms)
1	94.10	93.64	8.95	2.76
2	78.50	93.90	13.13	2.91
3	91.44	93.56	10.09	0.25
4	93.79	94.02	9.64	1.23
5	87.35	94.15	17.06	20.30
Rata-rata	89.04	93.85	11.77	5.49
Index	4	4	4	3

Dalam hasil pengujian pada Tabel 3.3 didapatkan data *throughput* download sebesar 89.04 Mbps dan *upload* 93.85 Mbps dengan *latency* 11.77ms dan *jitter* 5.49 ms. Ini menunjukkan fitur SD-WAN dapat berjalan tanpa mempengaruhi kualitas jaringan.

Dilakukan pengujian parameter *throughput*, *latency*, dan *jitter* pada *host* dengan utilitas *ookla speedtest cli* terhadap server PT Mora Telematika Indonesia (Moratel) dengan skenario 1 ISP (SD-WAN):

Tabel 3.4 Pengujian Parameter *throughput*, *latency*, dan *jitter* 1 ISP (SD-WAN)

Pengujian Ke-	Throughput Download (Mbps)	Throughput Upload (Mbps)	Latency / Idle (ms)	Jitter (ms)
1	67.78	51.07	8.78	0.36
2	70.63	49.74	9.95	0.32
3	70.11	51.10	15.25	2.68
4	69.08	51.20	10.33	11.34
5	66.73	48.83	8.99	1.10
Rata-rata	68.87	50.39	10.66	3.16
Index	4	4	4	3

Dalam hasil pengujian tersebut didapatkan data *throughput* download sebesar 68.87 Mbps dan *upload* 50.39 Mbps dengan *latency* 10.66 ms dan *jitter* 3.16 ms. Pada data tersebut dapat diketahui bahwa dengan 1 ISP akan mendapatkan *latency*

dan *jitter* yang lebih rendah, ini karena sistem tidak perlu melakukan pemilihan jalur mana WAN.

Untuk pengujian *packet loss* dilakukan secara terpisah dengan mengirimkan paket data dengan utilitas ping pada server Google DNS (8.8.8.8). Pengujian dilakukan dengan skenario 1 ISP (SD-WAN) dan 2 ISP (SD-WAN). Hasil pengujian dapat disajikan pada tabel berikut:

Tabel 3.5 Pengujian Parameter Packet Loss

Pengujian Ke-	Skenario	Paket Dikirim	Paket Diterima	Packet Loss
1	1 ISP	100	100	0%
2		100	100	0%
3		100	100	0%
4		100	100	0%
5		100	99	1%
Rata-rata		100	99.8	0.2%
Index		-	-	4
1	2 ISP	100	100	0%
2		100	100	0%
3		100	100	0%
4		100	100	0%
5		100	100	0%
Rata-rata		100	100	0%
Index		-	-	4

Pada skenario pengujian dengan 2 ISP (SD-WAN), stabilitas jaringan menunjukkan performa yang sangat memuaskan. Dari total 500 paket yang dikirimkan dalam 5 kali percobaan, tidak ditemukan adanya paket yang hilang *packe loss* 0% dibandingkan skenario dengan 1 ISP yang terdapat *packet loss* 0.2%.

Hal ini menunjukkan bahwa mekanisme SD-WAN berhasil memilih jalur terbaik menuju internet. Dengan keseluruhan pengujian mendapat index 4 (sangat bagus). Untuk data lengkapnya dapat dilihat pada Tabel 3.5.

SD-WAN sendiri berfungsi juga sebagai *failover* jaringan. SD-WAN memeriksa setiap WAN untuk memastikan layanan aktif. Bila SD-WAN mendeteksi salah satu interface WAN mati atau tidak dapat mengirimkan data, maka secara otomatis akan menggunakan jalur WAN lain.

Tabel 3.6 Pengujian Failover SD-WAN

Pengujian Ke-	Skenario Gangguan	Status Interface	Respon Sistem	Durasi Downtime	Status failover
1	Disable WAN1	WAN1 Down WAN2 UP	1x Request Timed Out	4.85 detik	Berhasil
2	Enable WAN1	WAN1 UP WAN2 UP	Tidak ada gangguan	Tidak ada gangguan	Tanpa failover
3	Disable WAN2	WAN1 UP WAN2 Down	1x Request Timed Out	4.56 detik	Berhasil
4	Enable WAN2	WAN1 UP WAN2 UP	Tidak ada gangguan	Tidak ada gangguan	Tanpa failover
5	Disable WAN1	WAN1 Down WAN2 UP	1x Request Timed Out	4.82 detik	Berhasil
6	Enable WAN1	WAN1 UP WAN2 UP	Tidak ada gangguan	Tidak ada gangguan	Tanpa failover
7	Disable WAN2	WAN1 UP WAN2 Down	1x Request Timed Out	4.64 detik	Berhasil
8	Enable WAN2	WAN1 UP WAN2 UP	Tidak ada gangguan	Tidak ada gangguan	Tanpa failover
Rata-rata			1 Paket data	4.72 detik	100%

Pada Tabel 3.6 didapatkan data untuk hasil pengujian *failover* dengan rata-rata RTO sebanyak 1 kali, dengan waktu *downtime* pada 4.72 detik dengan 100% sistem *failover* bekerja. Sistem *failover* bekerja dengan mengganti jalur yang mengalami kendala, jika jalur tersebut aktif kembali akan tetap menggunakan jalur pengganti.

Pengujian *application steering* dilakukan dengan cara *host* mengakses aplikasi atau layanan internet yang terdapat pada *rules* SD-WAN. SD-WAN mengarahkan lalu lintas jaringan ke tujuan sesuai dengan *rules*. Critical-DIA akan diarahkan pada *interface* WAN1 dan non Non-Critical-DIA akan melalui *interface* WAN2.

Tabel 3.7 Pengujian Application Steering

Pengujian ke-	Aplikasi Terdeteksi	Kategori Rule	Interface Terpilih	Interface Yang Diharapkan	Status Pengujian
1	Microsoft Portal (Office 365)	Critical-DIA	WAN1 (port1)	WAN1	Sesuai
2	YouTube	Critical-DIA	WAN1 (port1)	WAN1	Sesuai
3	Facebook	Non-Critical-DIA	WAN2 (port2)	WAN2	Sesuai
4	HTTP Browser	Critical-DIA	WAN1 (port1)	WAN1	Sesuai

Berdasarkan hasil pengujian pada Tabel 3.7 Didapatkan data bahwa rules yang ditetapkan dalam SD-WAN *application steering* sesuai dengan hasil log pada Fortigate.

Setelah dilakukan konfigurasi VPN Tunneling Site-to-Site pada kedua perangkat Fortigate, dilakukan serangkaian pengujian dengan skenario komunikasi antara *host* kantor cabang dengan *host* kantor pusat, pengujian dilakukan dengan utilitas ping.

Tabel 3.8 Pengujian Konektivitas VPN

Pengujian Ke-	Paket Dikirim	Paket Diterima	Packet Loss (%)	Latency Avg (ms)	Status Koneksi
1	100	100	0%	4	Terhubung
2	100	100	0%	4	Terhubung
3	100	100	0%	3	Terhubung
4	100	100	0%	2	Terhubung
5	100	100	0%	4	Terhubung
Rata-rata	100	100	0%	3.4	Terhubung
Index			4	4	

Berdasarkan hasil pengujian yang terdapat pada Tabel 3.8 didapatkan data packet loss rata-rata sebesar 0% dengan latency 3.4 ms. Data tersebut masuk kedalam index 4, yang artinya kualitas jaringan sangat bagus.

BAB IV

PENUTUP

4.1 Kesimpulan

Implementasi infrastruktur jaringan berbasis Fortigate berhasil dilakukan, di mana fitur SD-WAN mampu mengelola jalur internet secara dinamis dan Tunnel Site-to-Site VPN terbukti efektif dalam memfasilitasi pertukaran data yang handal antara kantor pusat dan cabang. Implementasi sistem SD-WAN dan Tunnel Site-to-Site IPsec VPN perangkat Fortigate.

Hasil analisis kinerja SD-WAN dan Tunnel Site-to-Site IPsec VPN perangkat Fortigate berdasarkan data pada tabel diatas, menunjukkan indikator jaringan dalam kondisi baik dengan nilai throughput pada index 4 (Sangat bagus), latency dengan index 4 (Sangat bagus), jitter pada nilai index 3 (Bagus), dan packet loss pada nilai index 4 (Sangat bagus).

Serta fitur failover SD-WAN mencapai 100% dengan waktu downtime pada 4.72 detik. Koneksi jaringan tunnel VPN yang dibangun masuk kedalam kategori stabil dengan 0% packet loss dan latency 3.4 ms.

Penerapan aturan *application steering* berbasis kategori aplikasi memungkinkan distribusi beban trafik sesuai dengan kebutuhan bisnis. Berdasarkan hasil pengujian, semua aplikasi dan *service* internet yang diakses oleh *host* menggunakan jalur WAN yang telah ditetapkan berdasarkan rules yang telah dibuat.

4.2 Saran

Berdasarkan pengalaman praktik kerja yang telah dilaksanakan selama kurang lebih 5 bulan di divisi Network Operating Center (NOC), penulis memiliki beberapa saran yang diharapkan dapat menjadi masukan bagi perusahaan untuk pengembangan program magang selanjutnya:

- a. Disarankan agar peserta magang dapat dilibatkan lebih dalam pada kegiatan yang bersifat project-based, tidak hanya terbatas pada fungsi

monitoring dan eskalasi tiket gangguan. Keterlibatan dalam tahap konfigurasi awal atau simulasi topologi akan sangat membantu mahasiswa dalam memahami siklus implementasi jaringan secara menyeluruh, serta menyelaraskan pemahaman teori dengan praktik industri.

- b. Penulis menyarankan agar perusahaan dapat melibatkan peserta magang dalam kegiatan troubleshooting secara on-site ke tempat klien, setidaknya ikut mengamati. Hal ini diperlukan agar mahasiswa dapat memahami korelasi antara alarm yang muncul pada dashboard monitoring dengan kondisi fisik perangkat di lapangan, serta mempelajari standar prosedur operasional saat berhadapan langsung dengan user.

DAFTAR PUSTAKA

- Afif, N. & Ridwang. (2021) *Teknologi dan Manajemen Jaringan Komputer*. Makassar: Alauddin University Press. Diakses pada 11 Desember 2025, pada <https://repositori.uin-alauddin.ac.id/24245/1/Teknologi%20dan%20Manajemen%20Jaringan%20Komputer.pdf>
- Alamin, Z., & Mu'min, M. A. (2024). Memahami dan menguasai jaringan komputer. PT Mafy Media Literasi Indonesia. Diakses pada 27 November 2025, pada https://www.researchgate.net/publication/386057151_Memahami_dan_Menguasai_Jaringan_Komputer/link/675daef0da24c8537c70c83d/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
- Alapati, Y. K., Rao, K. S. & Sreeramamurthy, K. (2024) *Network security fundamentals*. Tamil Nadu, India: Leilani Katie Publication. Diakses pada 30 November 2025, pada https://www.google.co.id/books/edition/Network_Security_Fundamentals/iKkVEQAAQBAJ?hl=en&gbpv=1
- Aldo, D., Ardi, Nengsih, Y.G., Syafrinal, I. & Putra, N. (2020) Pengantar Teknologi Informasi. Solok: Insan Cendekia Mandiri. Diakses pada 12 Desember 2025, pada https://www.google.co.id/books/edition/PENGANTAR_TEKNOLOGI_INFORMASI/nzMXEAAAQBAJ?hl=en&gbpv=0
- Ardiansyah, A., & Pamuji, F. Y. (2025). Penerapan standar TIPHON untuk kinerja quality of service jaringan internet: Studi kasus di jaringan Alfanet. JATI (Jurnal Mahasiswa Teknik Informatika), 9(5). Diakses pada 18 Desember 2025, pada <https://ejournal.itn.ac.id/jati/article/view/15112/8202>
- Army, W. L., Barovih, G., Seta, H. B., Guntoro, Margiutomo, S. A. S., Arifianto, T., Pujiyanto, D., Mutasar, Nurhabibah, & Faj, T. I. (2022). *Teknologi Jaringan Komputer*. Kabupaten Bandung: Widina Bhakti Persada. Diakses pada 27 November 2025, pada https://www.researchgate.net/profile/Mutasar-Mutasar/publication/382564359_TEKNOLOGI_JARINGAN_KOMPUTE

[R/links/66a397aa75fcd863e5df33fd/TEKNOLOGI-JARINGAN-KOMPUTER.pdf?origin=publication_detail&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uRG93bmxxvYWQlLCJwcmV2aW91c1BhZ2UiOiJwdWJsZWdGlvbiJ9fQ](https://www.researchgate.net/publication/360789107_Role_of_Information_Technology_in_Educational_Management?origin=publication_detail)

Azami, M., Haryadi, I. P., & Husain. (2025). Design and Implementation of Network Security Using Fortinet Firewall at the Communication and Information Service of Central Lombok Regency. *Journal of Applied Informatics and Engineering Applications*, 5(1). Diakses pada 21 November 2025, pada <https://www.ioinformatic.org/index.php/JAIEA/article/view/1356/985>

Bock, L. (2022). Learn Wireshark: A definitive guide to expertly analyzing protocols and troubleshooting networks using Wireshark (2nd ed.). Packt Publishing. ISBN 978-1803231679. Diakses pada 23 November 2025, pada https://books.google.co.id/books?hl=en&lr=&id=4HF5EAAAQBAJ&oi=fnd&pg=PP1&dq=wireshark&ots=Clo51ZNCp0&sig=JobaOk1myFWFcZnKf4enOZCFxvw&redir_esc=y#v=onepage&q=wireshark&f=false

Firmansyah, F., Wahyudi, M., & Purnama, R. A. (2021). Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP. *JUITA: Jurnal Informatika*, 7(2). Diakses pada 20 November 2025, pada <https://jurnalnasional.ump.ac.id/index.php/JUITA/article/view/4491/2826>

Irfana, Satraa, R. & Fattah, F. (2021) 'Keamanan Jaringan VLAN dan VoIP Menggunakan Firewall', Buletin Sistem Informasi dan Teknologi Islam, 2(1), pp. 27-35. Diakses pada 11 Desember 2025, pada https://www.researchgate.net/publication/367618655_Keamanan_Jaringan_VLAN_dan_VoIP_Menggunakan_Firewall/link/63d94c21c97bd76a824e89b8/download?tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

Madhu, S., & Shankar, A. (2024). An Analysis of Software-Defined Wide Area Networks: Foundation, Advantages and Difficulties. *International Journal*

of Engineering Research & Technology (IJERT), Vol. 13, Issue 03. Diakses pada 20 November 2025, pada <https://www.ijert.org/research/analysis-of-software-defined-wide-area-networks-foundation-advantages-and-difficulties-IJERTV13IS030013.pdf>

Suprpto, A. (2020) *Pengantar jaringan komputer: Pendekatan praktis untuk pemula*. Yogyakarta: Deepublish. Diakses pada 30 November 2025, pada https://www.researchgate.net/publication/366635551_PENGANTAR_JARINGAN_KOMPUTER?utm_source=chatgpt.com

Wicaksana, P., Hadi, F., & Hadi, A. F. (2021). *Perancangan implementasi VPN server menggunakan protokol L2TP dan IPSec sebagai keamanan jaringan*. Jurnal KomtekInfo, 8(3), 169–175. Diakses pada 21 November 2025, pada <https://jkomtekinfo.org/ojs/index.php/komtekinfo/article/view/128/124>

Wibowo, A. (2023) *Infrastruktur Internet: Jilid 1*. Semarang: Yayasan Prima Agus Teknik. Diakses pada 11 Desember 2025, pada https://digilib.stekom.ac.id/assets/dokumen/ebook/feb_A8yKPd_pXAEumI-dwUjJ-KqX7d8-e7JdgDCm9DqHkA_do9gH-XjcTw_1692675444.pdf

Zackiansyah, A.A. (2022) *Easy and Practice PPPoE Server, VPN PPTP, Bandwidth Management, Mikrotik Hotspot with Mikrotik RouterBoard*. Surabaya: XP Solution Surabaya. Diakses pada 12 Desember 2025, pada https://www.google.co.id/books/edition/Easy_and_Practice_PPPoE_Server_VPN_PPTP/XP18EAAAQBAJ?hl=en&gbpv=0

LAMPIRAN

1. Surat Keterangan Magang

 PT. Tirta Nawasena Teknologi Jl. Villa Melati Mas Raya No. 6 Blok I9 Tangerang Selatan 15323, Banten Ph. (+62) 888 1772 211 Email: info@tirtanawasena.com	PT. Tirta Nawasena Teknologi Jl. Villa Melati Mas Raya No. 6 Blok I9 Tangerang Selatan 15323, Banten Ph. (+62) 888 1772 211 Email: info@tirtanawasena.com
---	--

SURAT KETERANGAN
No. 01/SK/HRD/TNT/X11/2025

Yang betanda tangan dibawah ini, Human Resource Departemen dari PT. Tirta Nawasena Teknologi, dengan ini menerangkan bahwa :

Nama : Rangga Azizhan Hussaen
NIM / ID : 2207421017
Instisusi Pendidikan : Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan

Telah melakukan program Magang pada divisi Network Operation Center (NOC) pada PT. Tirta Nawasena Teknologi, terhitung sejak :

Periode Magang : 21 Juli – 30 Desember 2025

Selama masa magang, yang bersangkutan telah menjalankan tugas dan tanggung jawab dengan baik sesuai dengan standar dan ketentuan perusahaan, dengan rincian tugas sebagai berikut :

1. Melaksanakan operasional dan monitoring jaringan menggunakan PRTG serta penanganan tiket gangguan melalui ServiceDesk Plus, termasuk eskalasi insiden jaringan dan firewall.
2. Melakukan implementasi dan konfigurasi perangkat jaringan, meliputi Access Point Ruijie, firewall Fortigate (SD-WAN, VPN IPSec, DNAT, IP Pool, routing failover), serta mendukung upgrade server VMware vCenter.
3. Melaksanakan pemeliharaan dan administrasi sistem berupa backup konfigurasi perangkat jaringan, manajemen akun VPN, serta preventive maintenance perangkat jaringan secara berkala.
4. Menyusun laporan dan dokumentasi NOC, termasuk laporan bandwidth, aktivitas backup, analisis utilisasi jaringan, dan dokumentasi preventive maintenance.

Demikian Surat Keterangan Magang dibuat dengan sebenar-benarnya untuk digunakan sebagaimana mestinya.

Tangerang Selatan, 22 Desember 2025


(**Camelia Fatimah**)
Human Resource

2. Tabel Rincian Tugas Harian

F3



**KEMENTERIAN PENDIDIKAN TINGGI, RISET,
DAN TEKNOLOGI**

**POLITEKNIK NEGERI JAKARTA
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**

Jl. Prof. DR. G.A. Siwabessy, Kampus UI, Depok 16425
Telp: (021)91274097, Hunting Fax : (021) 7863531, (021)7270036
Laman :<http://www.pnj.ac.id>, e-mail : tik.pnj@gmail.com

BUKU PENGHUBUNG PEMBIMBING MAGANG INDUSTRI

1. Nama Mahasiswa : Rangga Azizzan Hussaen
2. NIM : 2207421017
3. Program Studi : Teknik Multimedia dan Jaringan
4. Nama Perusahaan/Industri : PT Tirta Nawasena Teknologi
5. Nama Pembimbing Industri : Nasrulloh

No	Hari/Tgl	Aktivitas yang Dilakukan	Tanda Tangan
1	Senin, 21/07/2025	- Membantu tim system engineer dalam melakukan penambahan storage vmware vcenter - Memasang SAS storage pada server	
2	Selasa, 22/07/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
3	Rabu, 23/07/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
4	Kamis, 24/07/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
5	Jumat, 25/07/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
6	Senin, 28/07/2025	Melakukan monitoring perangkat jaringan internet firewall melalui PRTG	

		- Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
7	Selasa, 29/07/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait - Melakukan reset account VPN Fortigate user	
8	Rabu, 30/07/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait - Melakukan konfigurasi DNAT (Dynamic Network Address Translation) pada firewall Fortigate - Melakukan konfigurasi DNAT (Dynamic Network Address Translation) pada firewall Fortigate dengan IP Pools	
9	Kamis, 31/07/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait - Melakukan konfigurasi routing failover - Melakukan cek data user account VPN Fortigate	
10	Jumat, 01/08/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait - Melakukan konfigurasi routing failover	
11	Senin, 04/08/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait - Melakukan reset account VPN Fortigate user	
12	Selasa, 05/08/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait - Melakukan cek data user account VPN Fortigate	

13	Rabu, 06/08/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
14	Kamis, 07/08/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
15	Jumat, 08/08/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait - Backup konfigurasi perangkat firewall palo alto, fortigate, <i>distribution switch</i>, dan clearpass policy aruba	
16	Senin, 11/08/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait - Backup konfigurasi perangkat firewall palo alto, fortigate, <i>distribution switch</i>, dan clearpass policy aruba	
17	Selasa, 12/08/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait - Melakukan penambahan akses pada account VPN	
18	Rabu, 13/08/2025	- Melakukan konfigurasi Dial-Up IPsec VPN antara 2 perangkat FortiGate - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
19	Kamis, 14/08/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati	

		ke PIC terkait	
20	Jumat, 15/08/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait - Backup konfigurasi perangkat firewall palo alto, fortigate, <i>distribution switch</i>, dan clearpass policy aruba	
21	Senin, 18/08/2025	- Libur nasional hari kemerdekaan Indonesia	
22	Selasa, 19/08/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
23	Rabu, 20/08/2025	- Konfigurasi SD-WAN firewall Fortigate - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
24	Kamis, 21/08/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
25	Jumat, 22/08/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, <i>distribution switch</i>, dan clearpass policy aruba - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
26	Senin, 25/08/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, <i>distribution switch</i>, dan clearpass policy aruba - Melakukan monitoring perangkat jaringan internet firewall melalui	

		PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
27	Selasa, 26/08/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
28	Rabu, 27/08/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
29	Kamis, 28/08/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
30	Jumat, 29/08/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, <i>distribution switch</i> , dan clearpass policy aruba - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
31	Senin, 01/09/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, <i>distribution switch</i> , dan clearpass policy aruba - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
32	Selasa, 02/09/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	

33	Rabu, 03/09/2025	- Membuat dokumentasi prevented maintenance distribution switch dan firewall palo alto - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
34	Kamis, 04/09/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
35	Jumat, 05/09/2025	- Libur nasional maulid nabi	
36	Senin, 08/09/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, <i>distribution switch</i>, dan clearpass policy aruba - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
37	Selasa, 09/09/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
38	Rabu, 10/09/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
39	Kamis, 11/09/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	

40	Jumat, 12/09/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, <i>distribution switch</i>, dan clearpass policy aruba - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
41	Senin, 15/09/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, <i>distribution switch</i>, dan clearpass policy aruba - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
42	Selasa, 16/09/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
43	Rabu, 17/09/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
44	Kamis, 18/09/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
45	Jumat, 19/09/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, <i>distribution switch</i>, dan clearpass policy aruba - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
46	Senin, 22/09/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, <i>distribution switch</i>, dan clearpass policy aruba - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG	

		- Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
47	Selasa, 23/09/2025	- Konfigurasi access point ruijie - Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
48	Rabu, 24/09/2025	- Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
49	Kamis, 25/09/2025	- Membuat dokumentasi prevented maintenance distribution switch dan firewall palo alto - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
50	Jumat, 26/09/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, <i>distribution switch</i>, dan clearpass policy aruba - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
51	Senin, 29/09/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, <i>distribution switch</i>, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
52	Selasa, 30/09/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG	

		- Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
53	Rabu, 01/10/2025	- Membuat dokumentasi prevented maintenance distribution switch dan firewall palo alto - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
54	Kamis, 02/10/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
55	Jumat, 03/10/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
56	Senin, 06/10/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
57	Selasa, 07/10/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	

58	Rabu, 08/10/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
59	Kamis, 09/10/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
60	Jumat, 10/10/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
61	Senin, 13/10/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
62	Selasa, 14/10/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	

63	Rabu, 15/10/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
64	Kamis, 16/10/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
65	Jumat, 17/10/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
66	Senin, 20/10/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
67	Selasa, 21/10/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
68	Rabu, 22/10/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	

		ke PIC terkait	
69	Kamis, 23/10/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
70	Jumat, 24/10/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
71	Senin, 27/10/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
72	Selasa, 28/10/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
73	Rabu, 29/10/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	

74	Kamis, 30/10/2025	- Membuat dokumentasi prevented maintenance distribution switch dan firewall palo alto - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
75	Jumat, 31/10/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
76	Senin, 03/11/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
77	Selasa, 04/11/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
78	Rabu, 05/11/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	

79	Kamis, 06/11/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
80	Jumat, 07/11/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
81	Senin, 10/11/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
82	Selasa, 11/11/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
83	Rabu, 12/11/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
84	Kamis, 13/11/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	

		ke PIC terkait	
85	Jumat, 14/11/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
86	Senin, 17/11/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
87	Selasa, 18/11/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
88	Rabu, 19/11/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
89	Kamis, 20/11/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	

90	Jumat, 21/11/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
91	Senin, 24/11/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
92	Selasa, 25/11/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
93	Rabu, 26/11/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
94	Kamis, 27/11/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
95	Jumat, 28/11/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat	

		jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
96	Senin, 01/12/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
97	Selasa, 02/12/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
98	Rabu, 03/12/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
99	Kamis, 04/12/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
100	Jumat, 05/12/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	

101	Senin, 08/12/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
102	Selasa, 09/12/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
103	Rabu, 10/12/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
104	Kamis, 11/12/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
105	Jumat, 12/12/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
106	Senin, 15/12/2025	- Backup konfigurasi perangkat firewall palo alto, fortigate, distribution switch, dan clearpass policy aruba - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui	

		PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
107	Selasa, 16/12/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
108	Rabu, 17/12/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
107	Kamis, 18/12/2025	- Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	
108	Jumat, 19/12/2025	- Membuat laporan mingguan NOC (Penggunaan bandwidth, backup perangkat, SLA, VPN dan lainnya) - Analisis session end device tertinggi pada setiap site - Melakukan monitoring perangkat jaringan internet firewall melalui PRTG - Melakukan follow up insiden jalur internet jaringan firewall yang mati ke PIC terkait	

Tangerang Selatan, 19 Desember 2025

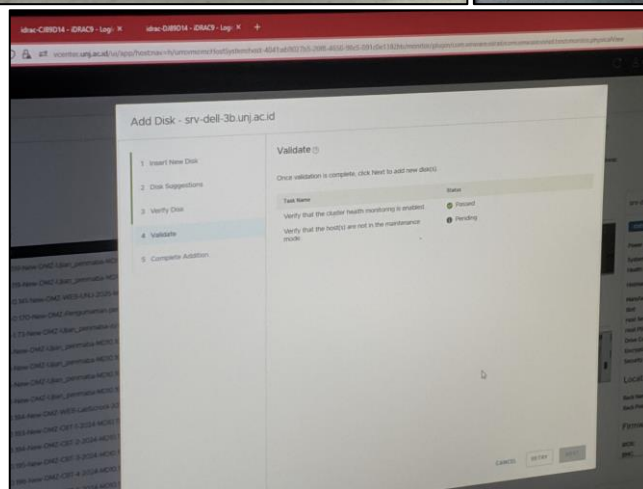
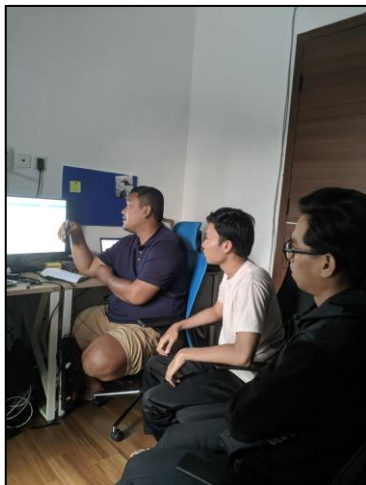
Supervisor Perusahaan,

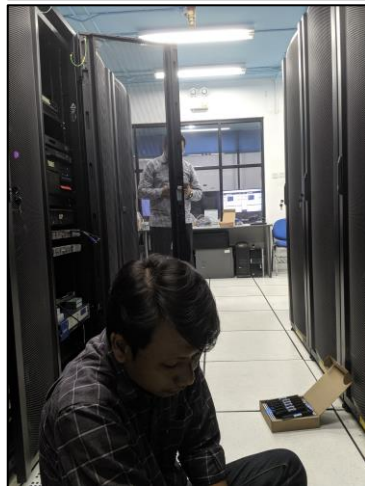
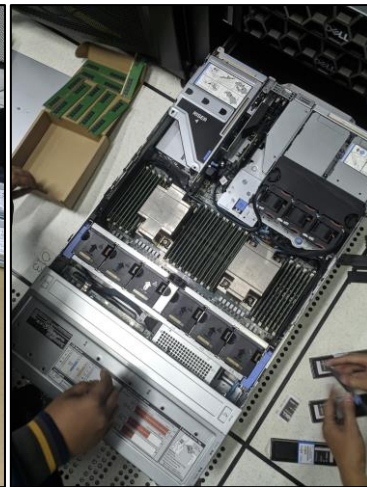
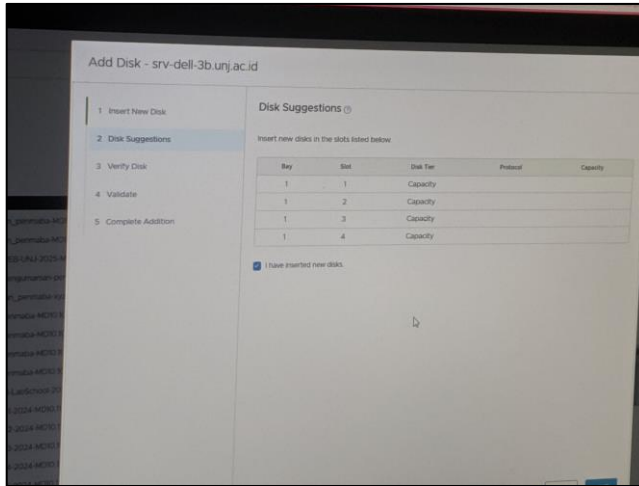


(Nasrulloh)
NRK. TNT002

3. Lampiran Kegiatan Magang







4. Lampiran Pengujian Proyek

```
C:\Users\DV1-rangga\Downloads\ookla-speedtest-1.2.0-win64>speedtest -s 30400

Speedtest by Ookla

      Server: PT. Mora Telematika Indonesia - Jakarta (id: 30400)
      ISP: PT Indonesia Comnets Plus
Idle Latency: 17.06 ms (jitter: 20.30ms, low: 9.64ms, high: 50.05ms)
  Download: 87.35 Mbps (data used: 151.0 MB)
           112.65 ms (jitter: 23.59ms, low: 10.96ms, high: 170.86ms)
    Upload: 94.15 Mbps (data used: 75.1 MB)
           141.96 ms (jitter: 43.55ms, low: 14.81ms, high: 210.53ms)
Packet Loss: 0.0%
Result URL: https://www.speedtest.net/result/c/50dab78a-e1cb-44cb-ae71-7f39f134aa0b
```

```
C:\Users\DV1-User\Downloads\ookla-speedtest-1.2.0-win64>speedtest -s 30400

Speedtest by Ookla

      Server: PT. Mora Telematika Indonesia - Jakarta (id: 30400)
      ISP: PT Indonesia Comnets Plus
Idle Latency: 8.99 ms (jitter: 1.10ms, low: 8.69ms, high: 10.96ms)
  Download: 66.73 Mbps (data used: 78.1 MB)
           44.63 ms (jitter: 12.82ms, low: 18.55ms, high: 96.52ms)
    Upload: 48.83 Mbps (data used: 43.7 MB)
           50.57 ms (jitter: 14.15ms, low: 17.95ms, high: 97.22ms)
Packet Loss: 0.0%
Result URL: https://www.speedtest.net/result/c/43b98163-07d5-4331-8f2e-c5ca809d17bc
```

```
C:\Users\DV1-rangga\Downloads\ookla-speedtest-1.2.0-win64>speedtest -s 30400

Speedtest by Ookla

      Server: PT. Mora Telematika Indonesia - Jakarta (id: 30400)
      ISP: PT Indonesia Comnets Plus
Idle Latency: 9.64 ms (jitter: 1.23ms, low: 8.85ms, high: 11.06ms)
  Download: 93.79 Mbps (data used: 105.0 MB)
           102.91 ms (jitter: 20.13ms, low: 14.16ms, high: 170.83ms)
    Upload: 94.02 Mbps (data used: 48.7 MB)
           139.98 ms (jitter: 42.74ms, low: 17.88ms, high: 238.85ms)
Packet Loss: 0.0%
Result URL: https://www.speedtest.net/result/c/c2bd20fd-b303-477e-93bb-f9895b58d234
```

```
C:\Users\DV1-rangga\Downloads\ookla-speedtest-1.2.0-win64>speedtest -s 30400

Speedtest by Ookla

      Server: PT. Mora Telematika Indonesia - Jakarta (id: 30400)
      ISP: PT Indonesia Comnets Plus
Idle Latency: 10.33 ms (jitter: 11.34ms, low: 8.68ms, high: 30.99ms)
  Download: 69.08 Mbps (data used: 60.2 MB)
           55.66 ms (jitter: 17.57ms, low: 22.44ms, high: 178.57ms)
    Upload: 51.20 Mbps (data used: 53.3 MB)
           51.03 ms (jitter: 13.27ms, low: 27.85ms, high: 110.36ms)
Packet Loss: 0.0%
Result URL: https://www.speedtest.net/result/c/1ffb608-6d9a-472e-9c03-11ce67ce2312
```

```
C:\Users\DV1-rangga\Downloads\ookla-speedtest-1.2.0-win64>speedtest -s 30400

Speedtest by Ookla

Server: PT. Mora Telematika Indonesia - Jakarta (id: 30400)
ISP: PT Indonesia Comnets Plus
Idle Latency: 10.09 ms (jitter: 0.25ms, low: 9.77ms, high: 10.34ms)
Download: 91.44 Mbps (data used: 88.9 MB)
45.10 ms (jitter: 6.09ms, low: 13.43ms, high: 76.57ms)
Upload: 93.56 Mbps (data used: 95.1 MB)
40.22 ms (jitter: 6.38ms, low: 23.28ms, high: 90.49ms)
Packet Loss: 0.7%
Result URL: https://www.speedtest.net/result/c/471af6bf-ed15-4f9a-a0d4-7ebe6ba1b8fd
```

```
C:\Users\DV1-rangga\Downloads\ookla-speedtest-1.2.0-win64>speedtest -s 30400

Speedtest by Ookla

Server: PT. Mora Telematika Indonesia - Jakarta (id: 30400)
ISP: PT Indonesia Comnets Plus
Idle Latency: 15.25 ms (jitter: 2.68ms, low: 10.30ms, high: 18.64ms)
Download: 70.11 Mbps (data used: 84.8 MB)
62.29 ms (jitter: 19.41ms, low: 12.44ms, high: 236.60ms)
Upload: 51.10 Mbps (data used: 53.4 MB)
48.97 ms (jitter: 13.76ms, low: 18.90ms, high: 98.22ms)
Packet Loss: 0.0%
Result URL: https://www.speedtest.net/result/c/f66908ee-ab15-41a9-8221-4413e3de91c2
```

```
C:\Users\DV1-rangga\Downloads\ookla-speedtest-1.2.0-win64>speedtest -s 30400

Speedtest by Ookla

Server: PT. Mora Telematika Indonesia - Jakarta (id: 30400)
ISP: PT Indonesia Comnets Plus
Idle Latency: 13.13 ms (jitter: 2.91ms, low: 9.40ms, high: 20.08ms)
Download: 78.50 Mbps (data used: 81.5 MB)
115.35 ms (jitter: 27.49ms, low: 18.20ms, high: 230.66ms)
Upload: 93.90 Mbps (data used: 79.6 MB)
29.57 ms (jitter: 4.80ms, low: 9.97ms, high: 49.98ms)
Packet Loss: 0.0%
Result URL: https://www.speedtest.net/result/c/63e08666-acac-4729-a389-45cf5fbfafa1
```

```
C:\Users\DV1-rangga\Downloads\ookla-speedtest-1.2.0-win64>speedtest -s 30400

Speedtest by Ookla

Server: PT. Mora Telematika Indonesia - Jakarta (id: 30400)
ISP: PT Indonesia Comnets Plus
Idle Latency: 9.95 ms (jitter: 0.32ms, low: 9.45ms, high: 10.27ms)
Download: 70.63 Mbps (data used: 75.1 MB)
46.93 ms (jitter: 15.42ms, low: 18.05ms, high: 111.59ms)
Upload: 49.74 Mbps (data used: 32.0 MB)
49.30 ms (jitter: 13.36ms, low: 26.95ms, high: 105.75ms)
Packet Loss: 0.0%
Result URL: https://www.speedtest.net/result/c/98823d83-8395-44cb-bcf7-a21874301df0
```

```
C:\Users\DV1-rangga\Downloads\ookla-speedtest-1.2.0-win64>speedtest -s 30400

Speedtest by Ookla

Server: PT. Mora Telematika Indonesia - Jakarta (id: 30400)
ISP: PT Indonesia Comnets Plus
Idle Latency: 8.95 ms (jitter: 2.76ms, low: 8.56ms, high: 18.87ms)
Download: 94.10 Mbps (data used: 70.7 MB)
46.94 ms (jitter: 8.06ms, low: 11.11ms, high: 92.34ms)
Upload: 93.64 Mbps (data used: 110.5 MB)
98.78 ms (jitter: 24.02ms, low: 32.56ms, high: 495.58ms)
Packet Loss: 0.0%
Result URL: https://www.speedtest.net/result/c/d8f1b0db-8018-423c-9fe4-a2c12325c196
```

```
C:\Users\DV1-rangga\Downloads\ookla-speedtest-1.2.0-win64>speedtest -s 30400
```

Speedtest by Ookla

```
Server: PT. Mora Telematika Indonesia - Jakarta (id: 30400)
ISP: PT Indonesia Comnets Plus
Idle Latency: 8.78 ms (jitter: 0.36ms, low: 8.29ms, high: 9.19ms)
Download: 67.78 Mbps (data used: 48.1 MB)
44.68 ms (jitter: 12.06ms, low: 15.92ms, high: 118.24ms)
Upload: 51.07 Mbps (data used: 58.3 MB)
53.74 ms (jitter: 16.60ms, low: 25.45ms, high: 306.29ms)
Packet Loss: 0.0%
Result URL: https://www.speedtest.net/result/c/6d716e1b-234e-48e8-9451-7025864a0c6c
```

```
Command Prompt
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=43ms TTL=126
Reply from 8.8.8.8: bytes=32 time=39ms TTL=126
Reply from 8.8.8.8: bytes=32 time=30ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
Reply from 8.8.8.8: bytes=32 time=52ms TTL=126
Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
Reply from 8.8.8.8: bytes=32 time=28ms TTL=126
Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=31ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=30ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 66ms, Average = 26ms

C:\Users\Dell Optiplex 360>
```

```
Command Prompt
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=24ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=57ms TTL=126
Reply from 8.8.8.8: bytes=32 time=62ms TTL=126
Reply from 8.8.8.8: bytes=32 time=36ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
Reply from 8.8.8.8: bytes=32 time=41ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=32ms TTL=126
Reply from 8.8.8.8: bytes=32 time=21ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 73ms, Average = 27ms

C:\Users\Dell Optiplex 360>
```

```
Command Prompt

Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=21ms TTL=126
Reply from 8.8.8.8: bytes=32 time=39ms TTL=126
Reply from 8.8.8.8: bytes=32 time=21ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=24ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 66ms, Average = 25ms

C:\Users\Dell Optiplex 360>
```

```
Command Prompt

Reply from 8.8.8.8: bytes=32 time=53ms TTL=126
Reply from 8.8.8.8: bytes=32 time=43ms TTL=126
Reply from 8.8.8.8: bytes=32 time=34ms TTL=126
Reply from 8.8.8.8: bytes=32 time=35ms TTL=126
Reply from 8.8.8.8: bytes=32 time=54ms TTL=126
Reply from 8.8.8.8: bytes=32 time=54ms TTL=126
Reply from 8.8.8.8: bytes=32 time=28ms TTL=126
Reply from 8.8.8.8: bytes=32 time=48ms TTL=126
Reply from 8.8.8.8: bytes=32 time=39ms TTL=126
Reply from 8.8.8.8: bytes=32 time=30ms TTL=126
Reply from 8.8.8.8: bytes=32 time=32ms TTL=126
Reply from 8.8.8.8: bytes=32 time=55ms TTL=126
Reply from 8.8.8.8: bytes=32 time=37ms TTL=126
Reply from 8.8.8.8: bytes=32 time=49ms TTL=126
Reply from 8.8.8.8: bytes=32 time=32ms TTL=126
Reply from 8.8.8.8: bytes=32 time=31ms TTL=126
Reply from 8.8.8.8: bytes=32 time=24ms TTL=126
Reply from 8.8.8.8: bytes=32 time=31ms TTL=126
Reply from 8.8.8.8: bytes=32 time=31ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 153ms, Average = 33ms

C:\Users\Dell Optiplex 360>
```

```
Select Command Prompt

Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
Reply from 8.8.8.8: bytes=32 time=32ms TTL=126
Reply from 8.8.8.8: bytes=32 time=51ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
Reply from 8.8.8.8: bytes=32 time=31ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=32ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 187ms, Average = 29ms

C:\Users\Dell Optiplex 360>
```

```
Command Prompt

Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=32ms TTL=126
Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
Reply from 8.8.8.8: bytes=32 time=21ms TTL=126
Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=48ms TTL=126
Reply from 8.8.8.8: bytes=32 time=28ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
Reply from 8.8.8.8: bytes=32 time=30ms TTL=126
Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=30ms TTL=126
Reply from 8.8.8.8: bytes=32 time=34ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 100, Received = 99, Lost = 1 (1% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 279ms, Average = 34ms

C:\Users\DV1-rangga>
```

```
Command Prompt

Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=21ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=31ms TTL=126
Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
Reply from 8.8.8.8: bytes=32 time=24ms TTL=126
Reply from 8.8.8.8: bytes=32 time=36ms TTL=126
Reply from 8.8.8.8: bytes=32 time=30ms TTL=126
Reply from 8.8.8.8: bytes=32 time=28ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=36ms TTL=126
Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
Reply from 8.8.8.8: bytes=32 time=30ms TTL=126
Reply from 8.8.8.8: bytes=32 time=28ms TTL=126
Reply from 8.8.8.8: bytes=32 time=32ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=32ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 132ms, Average = 32ms

C:\Users\DV1-rangga>
```

```
Command Prompt

Reply from 8.8.8.8: bytes=32 time=21ms TTL=126
Reply from 8.8.8.8: bytes=32 time=24ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=85ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=21ms TTL=126
Reply from 8.8.8.8: bytes=32 time=21ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=40ms TTL=126
Reply from 8.8.8.8: bytes=32 time=58ms TTL=126
Reply from 8.8.8.8: bytes=32 time=35ms TTL=126
Reply from 8.8.8.8: bytes=32 time=36ms TTL=126
Reply from 8.8.8.8: bytes=32 time=37ms TTL=126
Reply from 8.8.8.8: bytes=32 time=31ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=69ms TTL=126
Reply from 8.8.8.8: bytes=32 time=47ms TTL=126
Reply from 8.8.8.8: bytes=32 time=57ms TTL=126
Reply from 8.8.8.8: bytes=32 time=50ms TTL=126
Reply from 8.8.8.8: bytes=32 time=35ms TTL=126
Reply from 8.8.8.8: bytes=32 time=37ms TTL=126
Reply from 8.8.8.8: bytes=32 time=28ms TTL=126
Reply from 8.8.8.8: bytes=32 time=24ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 85ms, Average = 33ms

C:\Users\DV1-rangga>
```

```

C:\Users\DV1-rangga> Select Command Prompt

Reply from 8.8.8.8: bytes=32 time=34ms TTL=126
Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
Reply from 8.8.8.8: bytes=32 time=32ms TTL=126
Reply from 8.8.8.8: bytes=32 time=51ms TTL=126
Reply from 8.8.8.8: bytes=32 time=45ms TTL=126
Reply from 8.8.8.8: bytes=32 time=41ms TTL=126
Reply from 8.8.8.8: bytes=32 time=57ms TTL=126
Reply from 8.8.8.8: bytes=32 time=82ms TTL=126
Reply from 8.8.8.8: bytes=32 time=49ms TTL=126
Reply from 8.8.8.8: bytes=32 time=38ms TTL=126
Reply from 8.8.8.8: bytes=32 time=50ms TTL=126
Reply from 8.8.8.8: bytes=32 time=28ms TTL=126
Reply from 8.8.8.8: bytes=32 time=37ms TTL=126
Reply from 8.8.8.8: bytes=32 time=40ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
Reply from 8.8.8.8: bytes=32 time=31ms TTL=126
Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
Reply from 8.8.8.8: bytes=32 time=32ms TTL=126
Reply from 8.8.8.8: bytes=32 time=32ms TTL=126
Reply from 8.8.8.8: bytes=32 time=28ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 167ms, Average = 38ms

C:\Users\DV1-rangga>

```

```

C:\Users\DV1-rangga> Select Command Prompt

Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=21ms TTL=126
Reply from 8.8.8.8: bytes=32 time=24ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=20ms TTL=126
Reply from 8.8.8.8: bytes=32 time=24ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=21ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=22ms TTL=126
Reply from 8.8.8.8: bytes=32 time=48ms TTL=126
Reply from 8.8.8.8: bytes=32 time=51ms TTL=126
Reply from 8.8.8.8: bytes=32 time=38ms TTL=126
Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
Reply from 8.8.8.8: bytes=32 time=56ms TTL=126
Reply from 8.8.8.8: bytes=32 time=53ms TTL=126
Reply from 8.8.8.8: bytes=32 time=53ms TTL=126

Ping statistics for 8.8.8.8:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 105ms, Average = 30ms

C:\Users\DV1-rangga>

```

The screenshot displays the Wireshark network protocol analyzer interface. The main window shows a packet capture of ICMP Echo (ping) requests and replies between the source IP 10.0.1.11 and the destination IP 8.8.8.8. The packet list on the left shows 22 packets, with the first packet being an ICMP Echo request (type 8) and the subsequent packets being replies (type 0). The packet details pane on the right shows the structure of the selected packet (packet 1), which is an ICMP Echo request. The packet bytes pane at the bottom shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and ICMP Echo request data.

No.	Time	Source	Destination	Protocol	Length	Info
143	18.3602838	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=57ms TTL=126
144	19.277286	10.0.1.11	8.8.8.8	ICMP	74	Request to 8.8.8.8: bytes=32 time=41ms TTL=126
145	19.280282	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
146	20.287183	10.0.1.11	8.8.8.8	ICMP	74	Request to 8.8.8.8: bytes=32 time=31ms TTL=126
165	20.312625	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=26ms TTL=126
167	21.301137	10.0.1.11	8.8.8.8	ICMP	74	Request to 8.8.8.8: bytes=32 time=29ms TTL=126
168	21.332745	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
169	22.314826	10.0.1.11	8.8.8.8	ICMP	74	Request to 8.8.8.8: bytes=32 time=31ms TTL=126
170	22.340607	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
200	23.322731	10.0.1.11	8.8.8.8	ICMP	74	Request to 8.8.8.8: bytes=32 time=33ms TTL=126
209	23.352661	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
210	24.337235	10.0.1.11	8.8.8.8	ICMP	74	Request to 8.8.8.8: bytes=32 time=25ms TTL=126
211	24.363107	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=31ms TTL=126
213	25.344193	10.0.1.11	8.8.8.8	ICMP	74	Request to 8.8.8.8: bytes=32 time=27ms TTL=126
214	25.372784	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=30ms TTL=126
215	26.365793	10.0.1.11	8.8.8.8	ICMP	74	Request to 8.8.8.8: bytes=32 time=26ms TTL=126
216	26.393028	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=28ms TTL=126
217	27.373250	10.0.1.11	8.8.8.8	ICMP	74	Request to 8.8.8.8: bytes=32 time=27ms TTL=126
218	27.402891	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126

Summary statistics for 8.8.8.8:
 Packets: Sent = 33, Received = 33, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 24ms, Maximum = 57ms, Average = 30ms

Frame 1: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on 0
 Ethernet II, Src: VMware_Sc01e2 (08:0c:29:5c:9f:e2), Dst: VMware_d9:02:9b (08:00:07:09:02:9b)
 Internet Protocol Version 4, Src: 10.0.1.11, Dst: 8.8.8.8
 Internet Control Message Protocol

Command Prompt
 C:\Users\ DELL Optiplex 360>
 C:\Users\ DELL Optiplex 360>

Activate Windows
 Go to Settings to activate Windows.

wireshark Ethernet\NFTS3CS.pcap

Packets: 224 - Displayed: 56 (25.0%) - Drooped: 0 (0.0%)

Profile: Default

Wireshark interface showing a packet capture of ICMP Echo (ping) requests and replies. The packet list on the left shows a single packet (No. 259) from 10.0.1.11 to 8.8.8.8. The packet details pane shows the Internet Control Message Protocol (ICMP) Echo (ping) request. The packet bytes pane shows the raw data of the packet, including the IP header and ICMP payload. A Command Prompt window is overlaid on the right, showing the output of the ping command: "Packets: Sent = 47, Received = 47, Lost = 0 (0% loss), Minimum = 20ms, Maximum = 67ms, Average = 28ms".

Wireshark interface showing a packet capture of ICMP Echo (ping) requests and replies. The packet list on the left shows multiple packets (No. 86 to 180) from 10.0.1.11 to 8.8.8.8. The packet details pane shows the Internet Control Message Protocol (ICMP) Echo (ping) request. The packet bytes pane shows the raw data of the packet, including the IP header and ICMP payload. A Command Prompt window is overlaid on the right, showing the output of the ping command: "Packets: Sent = 47, Received = 47, Lost = 0 (0% loss), Minimum = 20ms, Maximum = 67ms, Average = 28ms".

Wireshark interface showing a packet capture of ICMP Echo (ping) requests and replies. The packet list on the left shows multiple packets (No. 39 to 134) from 10.0.1.11 to 8.8.8.8. The packet details pane shows the Internet Control Message Protocol (ICMP) Echo (ping) request. The packet bytes pane shows the raw data of the packet, including the IP header and ICMP payload. A Command Prompt window is overlaid on the right, showing the output of the ping command: "Packets: Sent = 47, Received = 47, Lost = 0 (0% loss), Minimum = 20ms, Maximum = 67ms, Average = 28ms".

Wireshark capture of ICMP Echo (ping) requests and replies between 10.0.1.11 and 8.8.8.8. The packet list shows 23 requests and 23 replies. The packet details pane shows the structure of an ICMP Echo (ping) request, including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
199	9.377854	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
279	10.337079	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=33ms TTL=126
280	10.378945	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=28ms TTL=126
291	11.343002	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=32ms TTL=126
292	11.378668	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
298	12.362183	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=37ms TTL=126
299	12.387742	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=59ms TTL=126
300	13.372870	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=49ms TTL=126
301	13.398201	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=70ms TTL=126
302	14.394612	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=62ms TTL=126
303	14.417708	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=35ms TTL=126
304	15.408833	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=45ms TTL=126
305	15.437716	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
371	16.449624	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
372	16.478880	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=23ms TTL=126
379	17.469971	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
380	17.497527	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
382	18.485444	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
383	18.507457	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=22ms TTL=126

Frame 66: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on Ethernet II, Src: VMware_Sc:9f:e2 (00:0c:29:5c:9f:e2), Dst: VMware_d9:02:9b (08:00:27:00:02:9b), Internet Protocol Version 4, Src: 10.0.1.11, Dst: 8.8.8.8, Internet Control Message Protocol, Type: Echo (ping) request (8), Code: 0

Ping statistics for 8.8.8.8:
Packets: Sent = 23, Received = 23, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 22ms, Maximum = 70ms, Average = 35ms

Wireshark capture of ICMP Echo (ping) requests and replies between 10.0.1.11 and 8.8.8.8. The packet list shows 48 requests and 48 replies. The packet details pane shows the structure of an ICMP Echo (ping) request, including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
238	21.732803	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
239	21.755073	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=30ms TTL=126
240	22.740686	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=32ms TTL=126
241	22.763302	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
242	23.758165	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
243	23.787883	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
244	24.770486	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=25ms TTL=126
245	24.797681	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=27ms TTL=126
281	25.786749	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=57ms TTL=126
282	25.817546	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=68ms TTL=126
283	26.795406	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
284	26.827940	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
285	27.802108	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
286	27.827687	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
287	28.826337	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
288	28.848279	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
289	29.829688	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
290	29.857445	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
297	30.850663	10.0.1.11	8.8.8.8	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126
298	30.877948	8.8.8.8	10.0.1.11	ICMP	74	Reply from 8.8.8.8: bytes=32 time=29ms TTL=126

Frame 7: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on Ethernet II, Src: VMware_Sc:9f:e2 (00:0c:29:5c:9f:e2), Dst: VMware_d9:02:9b (08:00:27:00:02:9b), Internet Protocol Version 4, Src: 10.0.1.11, Dst: 8.8.8.8, Internet Control Message Protocol, Type: Echo (ping) request (8), Code: 0

Ping statistics for 8.8.8.8:
Packets: Sent = 48, Received = 48, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 22ms, Maximum = 71ms, Average = 29ms

Wireshark capture of ICMP Echo (ping) requests and replies between 10.0.1.11 and 8.8.8.8. The packet list shows 212 requests and 212 replies. The packet details pane shows the structure of an ICMP Echo (ping) request, including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
61	9.170296	8.8.8.8	10.0.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=2724/41994, ttl=126 (request in 60)
62	10.146766	10.0.1.11	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2725/42250, ttl=128 (reply in 63)
63	10.178266	8.8.8.8	10.0.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=2725/42250, ttl=126 (request in 62)
94	11.154982	10.0.1.11	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2726/42506, ttl=128 (reply in 95)
95	11.188166	8.8.8.8	10.0.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=2726/42506, ttl=126 (request in 94)
96	12.175193	10.0.1.11	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2727/42762, ttl=128 (reply in 97)
97	12.207030	8.8.8.8	10.0.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=2727/42762, ttl=126 (request in 96)
98	13.195710	10.0.1.11	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2728/43018, ttl=128 (reply in 99)
99	13.228059	8.8.8.8	10.0.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=2728/43018, ttl=126 (request in 98)
114	14.212471	10.0.1.11	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2729/43274, ttl=128 (no response found!)
152	19.038020	10.0.1.11	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2730/43530, ttl=128 (reply in 153)
153	19.102348	8.8.8.8	10.0.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=2730/43530, ttl=126 (request in 152)
154	20.040264	10.0.1.11	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2731/43786, ttl=128 (reply in 155)
155	20.091073	8.8.8.8	10.0.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=2731/43786, ttl=126 (request in 154)
187	21.056953	10.0.1.11	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2732/44042, ttl=128 (reply in 188)
188	21.093229	8.8.8.8	10.0.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=2732/44042, ttl=126 (request in 187)
189	22.064948	10.0.1.11	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2733/44298, ttl=128 (reply in 190)
190	22.118365	8.8.8.8	10.0.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=2733/44298, ttl=126 (request in 189)
191	23.086346	10.0.1.11	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2734/44554, ttl=128 (reply in 192)
192	23.125650	8.8.8.8	10.0.1.11	ICMP	74	Echo (ping) reply id=0x0001, seq=2734/44554, ttl=126 (request in 191)

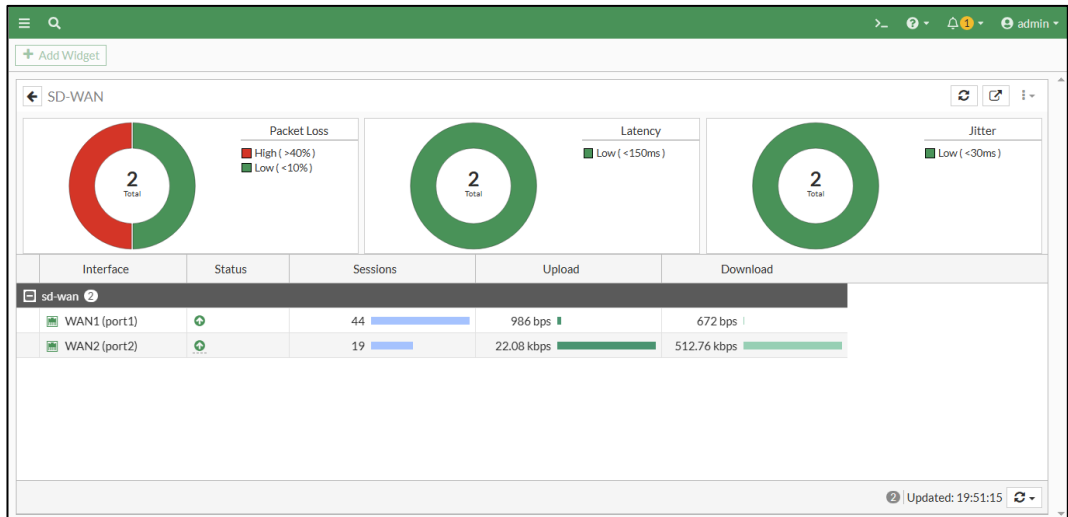
Frame 114: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF{...} Ethernet II, Src: VMware_Sc:9f:e2 (00:0c:29:5c:9f:e2), Dst: VMware_d9:02:9b (08:00:27:00:02:9b), Internet Protocol Version 4, Src: 10.0.1.11, Dst: 8.8.8.8, Internet Control Message Protocol, Type: Echo (ping) request (8), Code: 0

0000 00 0c 29 d9 02 9b 00 0c 29 5c 9f e2 00 00 45 00)\....E
0010 00 3c d9 c0 00 00 01 45 d0 0a 00 01 00 00 00 <.....E.....
0020 00 08 08 00 42 b2 00 01 0a a9 61 62 63 64 65 66 8....abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstu
0040 77 61 62 63 64 65 66 67 68 69 wabcedfg hi

Wireshark packet capture window showing ICMP Echo (ping) requests and replies. The packet list shows a sequence of pings from 10.0.1.11 to 8.8.8.8. The packet details pane shows the selected packet (No. 109) with fields: Identifier (BE): 1 (0x0001), Identifier (LE): 256 (0x0100), Sequence Number (BE): 2371 (0x9943), Sequence Number (LE): 17161 (0x4309). The packet bytes pane shows the raw data of the ICMP Echo request.

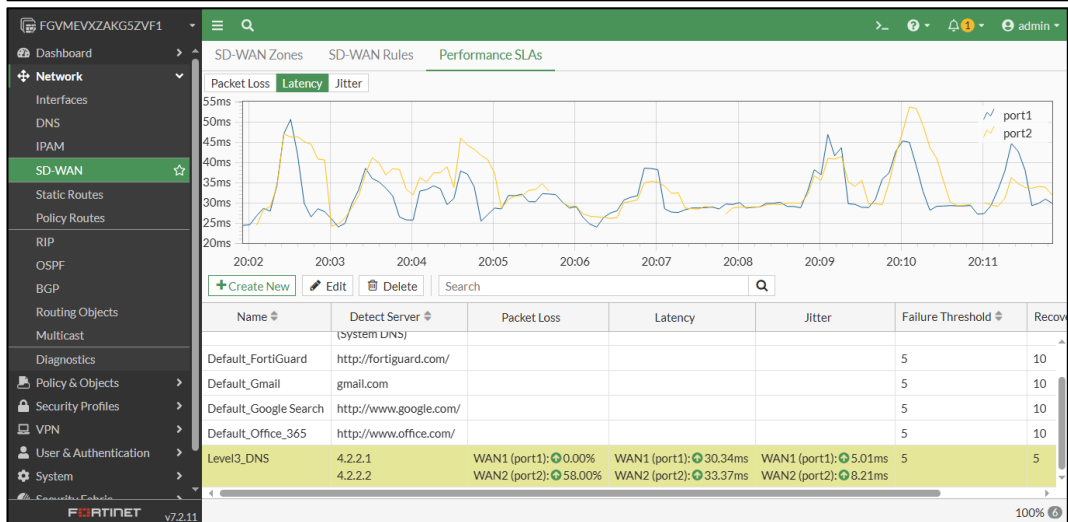
Wireshark packet capture window showing ICMP Echo (ping) requests and replies. The packet list shows a sequence of pings from 10.0.1.11 to 8.8.8.8. The packet details pane shows the selected packet (No. 109) with fields: Identifier (BE): 1 (0x0001), Identifier (LE): 256 (0x0100), Sequence Number (BE): 2371 (0x9943), Sequence Number (LE): 17161 (0x4309). The packet bytes pane shows the raw data of the ICMP Echo request.

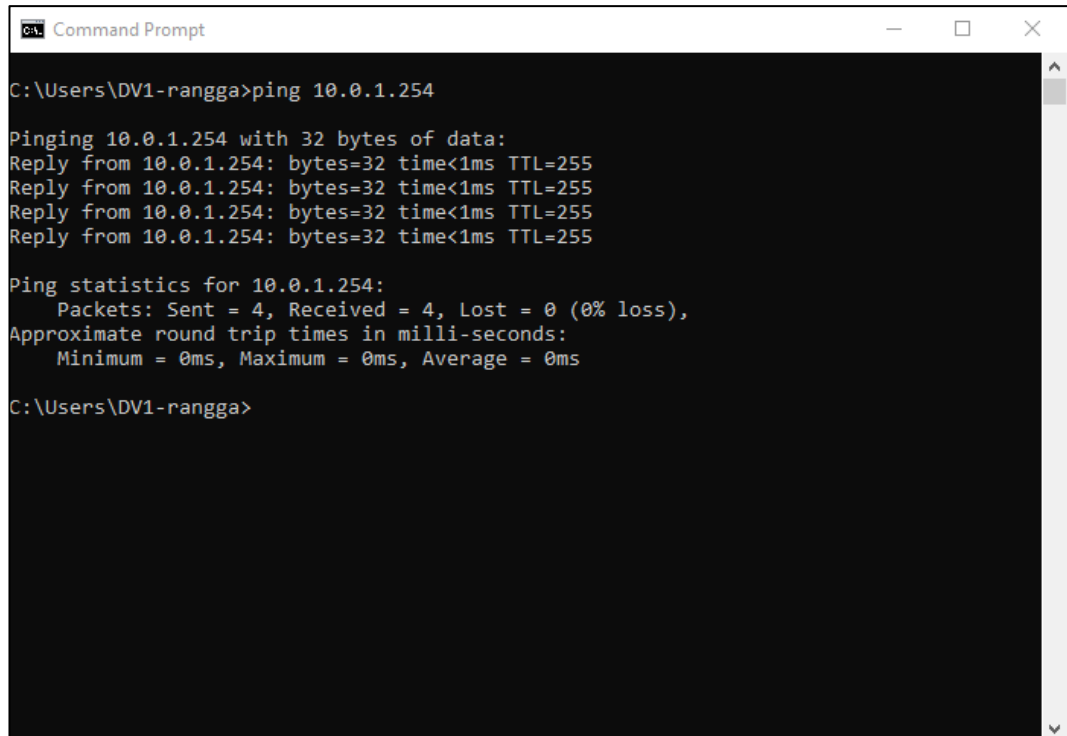
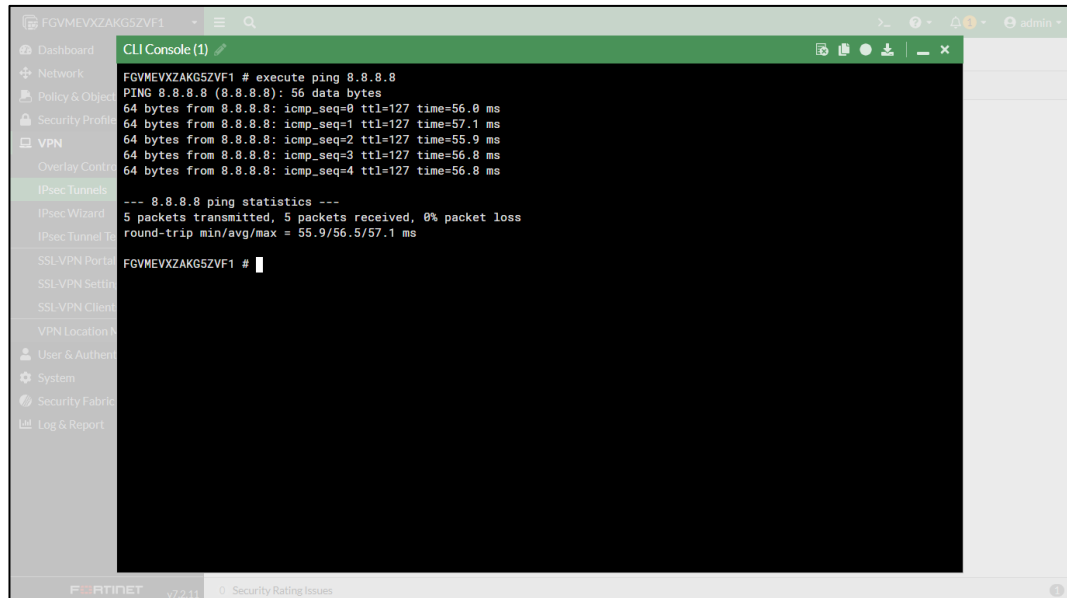
SD-WAN Events log window showing a summary of events. The log table includes columns for Date/Time, Level, Message, Log Description, and Log Details. The log shows a series of SD-WAN health-check member change events, including warnings and notices. The log details pane shows the selected event (Warning) with fields: Absolute Date/Time, Last Access Time, VDOM, Log Description, Source, Data, Message, Security, and Other.



SD-WAN Quality = "seq_num(1 port1), alive, selected", "seq_n..."

Destination	Application Name	Result	Policy ID	Destination Interface	SD-WAN Quality	SD-WAN Rule Name
8.45 (cp601.prod.do.dsp.mp.microsoft.com)	Microsoft.Porta	✓ Accept (UTM Allowed)	1 (DIA)	WAN1 (port1)	Seq_num(1 port1), alive, selected	Critical-DIA
8.45 (cp601.prod.do.dsp.mp.microsoft.com)	Microsoft.Porta	✓ Accept (UTM Allowed)	1 (DIA)	WAN1 (port1)	Seq_num(1 port1), alive, selected	Critical-DIA
0.208.14 (scontent.xx.fbcdn.net)	Facebook	✓ Accept (UTM Allowed)	1 (DIA)	WAN2 (port2)	Seq_num(2 port2), alive, selected	Non-Critical-DIA
0.208.35 (fbsbx.com)	Facebook	✓ Accept (UTM Allowed)	1 (DIA)	WAN2 (port2)	Seq_num(2 port2), alive, selected	Non-Critical-DIA
0.208.35 (fbsbx.com)	Facebook	✓ Accept (UTM Allowed)	1 (DIA)	WAN2 (port2)	Seq_num(2 port2), alive, selected	Non-Critical-DIA
0.208.14 (scontent.xx.fbcdn.net)	Facebook	✓ Accept (UTM Allowed)	1 (DIA)	WAN2 (port2)	Seq_num(2 port2), alive, selected	Non-Critical-DIA
0.208.14 (scontent.xx.fbcdn.net)	Facebook	✓ Accept (UTM Allowed)	1 (DIA)	WAN1 (port1)	Seq_num(1 port1), alive, selected	Critical-DIA
60.82 (rr7---sn-pjvo2aopq-jb3s.googlevideo.com)	YouTube	✓ Accept (UTM Allowed)	1 (DIA)	WAN1 (port1)	Seq_num(1 port1), alive, selected	Critical-DIA
60.82 (rr7---sn-pjvo2aopq-jb3s.googlevideo.com)	YouTube	✓ Accept (UTM Allowed)	1 (DIA)	WAN1 (port1)	Seq_num(1 port1), alive, selected	Critical-DIA
127.11 (edge.microsoft.com)	Microsoft.Porta	✓ Accept (UTM Allowed)	1 (DIA)	WAN1 (port1)	Seq_num(1 port1), alive, selected	Critical-DIA
246.59 (edge-cloud-resource-static.azureedge...	HTTPS.BROWSER	✓ Accept (UTM Allowed)	1 (DIA)	WAN1 (port1)	Seq_num(1 port1), alive, selected	Critical-DIA
9.8 (thaka.bing.com)	HTTPS.BROWSER	✓ Accept (UTM Allowed)	1 (DIA)	WAN1 (port1)	Seq_num(1 port1), alive, selected	Critical-DIA
9.9 (r.bing.com)	Microsoft.Porta	✓ Accept (UTM Allowed)	1 (DIA)	WAN1 (port1)	Seq_num(1 port1), alive, selected	Critical-DIA
71.136 (assets.msn.com)	Microsoft.Porta	✓ Accept (UTM Allowed)	1 (DIA)	WAN1 (port1)	Seq_num(1 port1), alive, selected	Critical-DIA
18.91 (img-s-msn-com.akamaized.net)	HTTPS.BROWSER	✓ Accept (UTM Allowed)	1 (DIA)	WAN1 (port1)	Seq_num(1 port1), alive, selected	Critical-DIA





DigiSigner Document ID: 02f93d10-fbbe-4274-be5d-402d5f2054f0

Signer

Email: asepkurniawan@tik.pnj.ac.id
IP Address: 2001:448a:2098:1fec:f9d4:55cf:aaf1:a5d3

Signature



Email: indrahermawan@tik.pnj.ac.id
IP Address: 103.36.14.70



Event	User	Time	IP Address
Upload document	starking.sk83@gmail.com	12/20/2025 3:01:43AM EST	158.140.191.64
Open document	starking.sk83@gmail.com	12/20/2025 3:01:46AM EST	158.140.191.64
Close document	starking.sk83@gmail.com	12/20/2025 3:02:06AM EST	158.140.191.64
Send for signing	starking.sk83@gmail.com	12/20/2025 3:02:20AM EST	158.140.191.64
Open document	asepkurniawan@tik.pnj.ac.id	12/20/2025 3:19:37AM EST	2001:448a:2098:1fec:f9d4:55cf:aaf1:a5d3
Sign document	asepkurniawan@tik.pnj.ac.id	12/20/2025 3:20:20AM EST	2001:448a:2098:1fec:f9d4:55cf:aaf1:a5d3
Close document	asepkurniawan@tik.pnj.ac.id	12/20/2025 3:20:20AM EST	2001:448a:2098:1fec:f9d4:55cf:aaf1:a5d3
Download document	starking.sk83@gmail.com	12/20/2025 3:20:46AM EST	158.140.191.64
Open document	starking.sk83@gmail.com	12/21/2025 10:06:05PM EST	103.18.34.162
Close document	starking.sk83@gmail.com	12/21/2025 10:07:07PM EST	103.18.34.162
Send for signing	starking.sk83@gmail.com	12/21/2025 10:07:18PM EST	103.18.34.162
Open document	indrahermawan@tik.pnj.ac.id	12/21/2025 10:09:11PM EST	103.36.14.70
Sign document	indrahermawan@tik.pnj.ac.id	12/21/2025 10:09:27PM EST	103.36.14.70
Close document	indrahermawan@tik.pnj.ac.id	12/21/2025 10:09:27PM EST	103.36.14.70
Open document	starking.sk83@gmail.com	12/21/2025 10:12:25PM EST	103.18.34.162
Close document	starking.sk83@gmail.com	12/21/2025 10:26:06PM EST	103.18.34.162