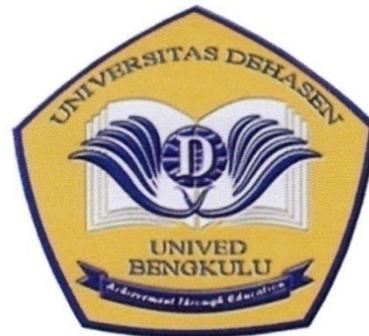


**IMPLEMENTASI SISTEM KEAMANAN DAN MONITORING
JARINGAN PADA SMA N 10 KOTA BENGKULU**

SKRIPSI



Disusun Oleh :

REFKI IQROMULLAH
NPM. 17010066

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS DEHASEN
BENGKULU
2023**

**IMPLEMENTASI SISTEM KEAMANAN DAN MONITORING
JARINGAN PADA SMA N 10 KOTA BENGKULU**

SKRIPSI

REFKI IQROMULLAH
NPM. 17010066

*Diajukan sebagai salah satu syarat untuk menyusun skripsi pada program studi
Informatika Universitas Dehasen Bengkulu*

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS DEHASEN
BENGKULU**

2023

**IMPLEMENTASI SISTEM KEAMANAN DAN MONITORING
JARINGAN PADA SMA N 10 KOTA BENGKULU**

SKRIPSI

Oleh :

REFKI IQROMULLAH
NPM. 17010066

Disetujui Oleh:

Pembimbing I,



Khairil, S.Kom, M.Kom
NIDN:02.130475.01

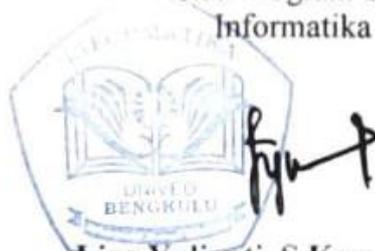
Pembimbing II,



Eko Suryana, S.Kom, M.Kom
NIDN: 02.151174.01

Mengetahui,

**Ketua Program Studi
Informatika**



Liza Yulianti, S.Kom, M. Kom
NIDN. 02.160772.01

**IMPLEMENTASI SISTEM KEAMANAN DAN MONITORING
JARINGAN PADA SMA N 10 KOTA BENGKULU**

SKRIPSI

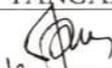
Disusun Oleh :

REFKI IQROMULLAH
NPM. 17010066

Telah dipertahankan di depan TIM penguji Fakultas Ilmu Komputer
Universitas Dehasen Bengkulu pada:

Hari : Sabtu
Tanggal : 17 Juni 2023

Skripsi ini telah diperiksa dan disetujui oleh Tim Penguji sbb :

PENGUJI	NAMA	NIDN	TANDA TANGAN
Ketua	Khairil, S.Kom., M.Kom	02.130475.01	
Sekretaris	Eko Suryana, S.Kom., M.Kom	02.151174.01	
Penguji I	Sapri, S.Kom, M.Kom	02.150171.02	
Penguji II	Eko Prasetyo Rohmawan, S.Kom., M. Kom	02.130488.01	

Mengetahui,

Dekan
Fakultas Ilmu Komputer


Siswanto, S.E., S.Kom., M.Kom
NIDN : 02.240363.01

DAFTAR RIWAYAT HIDUP



Penulis bernama Refki Iqromullah, di lahirkan di imigrasi permu, Kec. Kepahiang, Kab. Kepahiang, Prov. Bengkulu pada tanggal 18 April 1999, anak ketiga dari lima saudara, ayah saya bernama Ahmad Yaman dan ibu saya ber

nama Rohima. Menyelesaikan pendidikan di sekolah dasar negeri (SDN) 04 Kepahiang pada tahun 2011, kemudian penulis melanjutkan pendidikan pada sekolah menengah pertama (SMP) 03 kepahiang selesai pada tahun 2014 dan selanjutnya menyelesaikan pendidikan sekolah menengah kejuruan swasta 16 farmasi bhakti nusa bengkulu pada tahun 2017. Kemudian penulis melanjutkan pendidikan ke perguruan tinggi yaitu pada Universitas Dehasen (UNIVED) Bengkulu dengan mengambil Jurusan Informatika pada fakultas Ilmu Komputer, untuk jenjang strata satu (S-1) pada tahun 2017.

MOTTO DAN PERSEMBAHAN

MOTTO :

**Mereka menertawakan prosesku,
dan setelah itu mereka menanyakan gimana caranya.
Jadilah diri sendiri tanpa perlu mencerminkan diri pada orang lain,
banyak jalan dan cara untuk mencapai tujuan yang sama,
dengan versi yang berbeda.**

PERSEMBAHAN

Dengan mengucapkan Alhamdulillah atas semua limpahan rahmat dan Kasih sayangMu akhirnya tercapai juga suatu amanah, kewajiban, tujuan dan cita-cita. Kuyakin ini bukanlah akhir dari perjalanan dan perjuanganku, namun langkah awal untuk mewujudkan mimpi dan membahagiakan orang-orang yang ku kasih dan mengasihiku. Ku persembahkan karya kecil ini dengan sepenuh cinta untuk:

- ❖ Allah SWT yang telah memberikan Rahmat dan ridho yang luar biasa kepada saya.
- ❖ Kepada kedua orang tua (Ahmad Yaman dan Rohima) yang telah memberikan kasih sayang dan cintanya yang tulus, bekerja keras memeras keringat tanpa mengenal lelah dan tak henti berdoa demi tercapainya cita-cita saya.
- ❖ kakakku (Reefal Yara Ariwinanda dan Revianda Putra) dan adikku (Reski Wahyu Illahi dan Relianda Agung Wijaya) yang selalu memberikan dukungan materi dan motivasi.
- ❖ Untuk kekasihku Vira Octavia terimakasih sudah menjadi support system yang tak terlupakan selama beberapa tahun ini.
- ❖ Teman-teman seperjuangan angkatan 2016, 2017, 2018, 2019 yang selalu join dikantin terimakasih telah meluangkan waktu dalam tukar pikiran dan mencari ide-ide kreatif.
- ❖ Almamater kuning yang ku banggakan we love u.

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini :

Nama : REFKI IQROMULLAH

NPM : 17010066

Program Studi : Informatika

Menyatakan dengan sesungguhnya bahwa :

1. Selama melakukan penelitian dan pembuatan skripsi ini saya tidak melakukan pelanggaran etika akademik dalam bentuk apapun atau pelanggaran lain yang bertentangan dengan etika akademik.
2. Skripsi yang saya buat merupakan karya ilmiah saya sebagai penulis, bukan jiplakan atau karya orang lain.
3. Apabila dikemudian hari ditemukan bukti yang meyakinkan bahwa dalam proses pembuatan skripsi ini terdapat pelanggaran etika akademik atau skripsi ini hasil jiplakan atau skripsi ini hasil karya orang lain, maka saya bersedia menerima sanksi akademik yang ditetapkan oleh Universitas Dehasen Bengkulu.

Demikian Pernyataan ini Saya buat dengan sebenarnya untuk dipergunakan bilamana perlu.

Bengkulu, 10 Juni 2023

Yang Menyatakan,



REFKI IQROMULLAH

NPM.17010066

ABSTRAK

IMPLEMENTASI SISTEM KEAMANAN DAN MONITORING JARINGAN PADA SMA N 10 KOTA BENGKULU

Oleh:

Refki Iqromullah¹

Khairil, S.Kom., M.Kom²

Eko Suryana, S.Kom., M.Kom²

Salah satu sistem untuk dapat melakukan keamanan dan monitoring jaringan dapat menggunakan firewall dan grafana dengan sistem operasi linux ubuntu server. Dalam menjalankan sistem keamanan dan monitoring jaringan menggunakan firewall dan grafana di dukung oleh beberapa tool atau aplikasi lainnya seperti apache2, php dan MySQL. Jadi dengan menggunakan sistem keamanan dan monitoring jaringan dapat menggunakan firewall dan grafana dapat melakukan monitoring dan keamanan jaringan, dimana setiap aktifitas sesuai dengan pengaturan yang diberikan dilakukan oleh grafana, selanjutnya dari hasil monitoring tersebut akan dilakukan analisa yang mana aktifitas yang diperbolehkan dan tidak diperbolehkan. Selanjutnya dari hasil analisa tersebut akan di lakukan pembatasan menggunakan firewall. Linux ubuntu server 20.04 sistem operasi yang bersifat open source, sistem operasi Linux ubuntu server 20.04 ini sangat baik sebagai server untuk menjalankan sistem keamanan dan monitoring jaringan dapat menggunakan firewall dan grafana karena tidak membutuhkan spesifikasi hardware yang tinggi dan juga dapat diperoleh secara free karena bersifat open source.

Kata Kunci: **Grafana, Firewall, Linux Ubuntu Server**

Keterangan :

1: Peneliti

2: Pembimbing 1 dan Pembimbing 2

ABSTRACT

SECURITY SYSTEM IMPLEMENTATION AND MONITORING NETWORKS AT SMA N 10 CITY OF BENGKULU

By:

Refki Iqromullah¹
Khairil, S.Kom., M.Kom²
Eko Suryana, S.Kom., M.Kom²

One of the systems to be able to carry out network security and monitoring can use a firewall and Graphana with the Ubuntu Server Linux operating system. In running the security system and monitoring the network using a firewall and Graphana it is supported by several other tools or applications such as Apache2, PHP and MySQL. So by using a security system and network monitoring can use a firewall and grafana can monitor and network security, where every activity in accordance with the settings given is carried out by grafana, then from the monitoring results an analysis will be carried out which activities are allowed and which are not allowed. Furthermore, from the results of this analysis, restrictions will be made using a firewall. Linux ubuntu server 20.04 is an open source operating system, the Linux ubuntu server 20.04 operating system is very good as a server for running security systems and monitoring networks, you can use firewalls and graphana because it doesn't require high hardware specifications and can also be obtained free of charge because it is open. sources.

Keywords: Grafana, Firewall, Linux Ubuntu Server

Information:

1: Srudent

2: Supervisor

3: Co-Supervisor

KATA PENGANTAR

Puji Syukur penulis panjatkan kehadiran Allah SWT, karena berkat rahmat dan karunianya maka skripsi yang berjudul “**Implementasi Sistem Keamanan Dan Monitoring Pada Jaringan SMA N 10 Kota Bengkulu**”, dapat diselesaikan.

Pada kesempatan ini, penulis menyampaikan rasa penghargaan dan terima kasih kepada yang terhormat :

1. Bapak Prof. Kamaludin, S.E., M.M, selaku Rektor Universitas Dehasen Bengkulu.
2. Bapak Siswanto, S.E., S.Kom., M.Kom selaku Dekan Fakultas Ilmu Komputer.
3. Ibu Liza Yuliati, S.Kom., M.Kom selaku Ketua Program Studi Informatika..
4. Bapak Khairil, S.Kom., M.Kom selaku pembimbing I yang telah membimbing dengan penuh kesabaran dan rasa kekeluargaan bagi penulis sendiri.
5. Bapak Eko Suyana, S.Kom., M.Kom, selaku pembimbing II yang telah membimbing penulis dalam menyelesaikan laporan ini.
6. Bapak atau Ibu Dosen Fakultas Ilmu Komputer, Program Studi Informatika Universitas Dehasen Bengkulu
7. Seluruh Staf Karyawan/ti pada Fakultas Ilmu Komputer khususnya Program Studi Informatika Universitas Dehasen Bengkulu.
8. Rekan-rekan seperjuangan di Fakultas Ilmu Komputer khususnya Program Studi Informatika Universitas Dehasen Bengkulu.

Sehingga Tuhan Yang Maha Esa memberikan pahala yang setimpal kepada pihak yang telah memberikan bimbingan dan bantuan dalam menyelesaikan skripsi ini.

Penulis menyadari skripsi ini masih banyak terdapat kesalahan dan kekurangan. Untuk itu kritik dan saran yang bersifat membangun yang sangat diharapkan penulis, penulis berharap semoga skripsi ini dapat bermanfaat bagi semua pihak.

Bengkulu, Mei 2023

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
LEMBAR PENGESAHAN	iii
LEMBAR PERSETUJUAN	iv
RIWAYAT HIDUP	v
MOTTO	vi
PERSEMBAHAN.....	vii
SURAT PERNYATAAN	viii
ABSTRAK	ix
ABSTRACT	x
KATA PENGANTAR.....	xi
DAFTAR ISI.....	xiii
DAFTAR TABEL.....	xv
DAFTAR GAMBAR.....	xvi
DAFTAR LAMPIRAN	xviii
BAB I. PENDAHULUAN	
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	4
BAB II. LANDASAN TEORI	
2.1 Pengertian Implementasi	5
2.2 Pengertian Qos.....	7
2.3 Tinjauan Prometheus	9
2.4 Tinjauan Grafana	11
2.5 Tinjauan <i>Firewall</i>	12
2.5.1 Karakteristik <i>Firewall</i>	12
2.5.2 Teknik yang digunakan <i>Firewall</i>	13

2.5.3 Jenis-Jenis <i>Firewall</i>	14
2.6 Tinjauan Linux Ubuntu	17

BAB III. METODOLOGI PENELITIAN

3.1 Waktu dan Tempat Penelitian	22
3.2 Metode Penelitian	22
3.3 Perangkat Keras dan Perangkat Lunak.....	22
3.3.1 Perangkat Keras	22
3.3.2 Perangkat Lunak	23
3.4 Metode Pengumpulan Data	23
3.5 Analisa Sistem	24
3.5.1 Analisa Sistem Aktual	24
3.5.2 Analisa Sistem Yang Diusulkan	24
3.5.3 Prinsip Kerja Sistem	28
3.5.4 Rencana Kerja.....	29
3.6 Rencana Pengujian	30

BAB IV. HASIL DAN PEMBAHASAN

4.1 Hasil.....	37
4.2 Pembahasan	40
4.3 Hasil Pengujian.....	53

BAB V. KESIMPULAN DAN SARAN

5.1 Kesimpulan.....	59
5.2 Saran	59

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar	Halaman
3.1 Blok Diagram Global.....	25
3.4 Rencana Kerja.....	29
4.1 Tampilan Monitoring Grafana.....	38
4.2 Tampilan Alert Grafana.....	38
4.3 Tampilan Pengamanan di IPTable.....	39
4.4 Tampilan Spesifikasi Server Yang Digunakan.....	40
4.5 Tampilan Pilihan Bahasa Install Linux.....	41
4.6 Tampilan Pilihan Layout Keyboard.....	42
4.7 Tampilan Interface (Network Card)	42
4.8 Tampilan Input Proxy Linux	43
4.9 Tampilan Pilihan Respotary Linux.....	43
4.10 Tampilan Pilihan HDD Sistem Linux	44
4.11 Tampilan Komfirmasi Pilihan HDD Sistem Linux	44
4.12 Tampilan Pemberian User dan Password	45
4.13 Tampilan Konfirmasi Install OpenSSH Server	45
4.14 Tampilan Pilihan Paket Tambahan.....	46
4.15 Tampilan Proses Install Linux	46

DAFTAR TABEL

Tabel	Halaman
3.1 Rencana Pengujian	36

DAFTAR LAMPIRAN

Lampiran

1. Time Schedule
2. SK Pembimbing Akademik
3. Surat Izin Penelitian
4. Kartu Bimbingan Skripsi
5. Surat keterangan Selesai Penelitian
6. Surat Keterangan Demo Program
7. Struktur Organisasi
8. Dokumentasi

BAB I

PENDAHULUAN

1.1. Latar Belakang

Kebutuhan akan komunikasi data yang terintegrasi saat ini di Indonesia sudah menjadi kebutuhan utama bagi sebuah instansi pemerintah maupun swasta, apalagi ditambah banyak kantor instansi pemerintahan yang mulai membutuhkan data atau informasi yang saling terkait antara satu dengan lainnya. Terutama pada kantor-kantor untuk dapat melayani masyarakat dimana saja, yang dimana bisa diakses dimanapun berada (berpindah-pindah) tidak hanya di satu tempat saja. Kegiatan tersebut bisa menjadi sangat mahal dan memerlukan hardware dan dukungan teknis yang rumit.

Penggunaan infrastruktur yang handal dalam jaringan komputer sangat berpengaruh untuk mendukung kinerja atau performanya. *Server* adalah suatu perangkat jaringan yang digunakan untuk menjembatani antara dua atau lebih jaringan yang berbeda. Selain untuk menjembatani suatu jaringan, server juga dapat digunakan untuk mengelola lalu lintas jaringan. Server yang digunakan untuk implementasi ini adalah server dengan sistem operasi linux ubuntu server 20.04.

Salah satu faktor yang mendukung untuk kelancaran komunikasi data baik itu dalam jaringan LAN (*Local Area Network*) maupun jaringan global (*Internet*) adalah faktor keamanan. Untuk menjaga keamanan jaringan banyak cara yang dapat dilakukan seperti, memasang firewall yang mendukung jaringan, memasang server, memasang router, memasang firewall dan masih banyak cara lainnya untuk melakukan monitoring dan menjaga keamanan j

Dimana saat ini jaringan computer pada SMA 10 Kota Bengkulu khususnya jaringan LAN (*Local Area Network*) Lab, Tata Usaha dan bagian lainnya, serta jaringan tersebut tidak memiliki system monitoring dan sistem yang dapat mengatur dan manajemen jaringan, saat ini siswa masih dapat mengakses konten dengan bebas tanpa ada saringannya, sering terjadi download file dengan ukuran besar sehingga menyebabkan koneksi pada jaringan jadi lambat.

Saat ini banyak cara dan aplikasi yang dapat digunakan untuk melakukan *monitoring* jaringan, seperti *IPTable*, *Grafana*, *nagios*, *Zabbix* dan lainnya. *IPTable* dan *Grafana* dalam melakukan *monitoring* dan keamanan jaringan dapat berjalan diatas system operasi linux ubuntu *server*, sehingga tidak membutuhkan spesifikasi *server* yang tinggi dan disamping itu system operasi linux ubuntu *server* merupakan salah satu system operasi yang bersifat *open source*.

Dari uraian diatas maka penulis tertarik mengangkat judul “**Implementasi Sistem Keamanan Dan Monitoring Jaringan Pada SMA N 10 Kota Bengkulu**”.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas, maka rumusan masalah yaitu bagaimana merancang suatu Sistem Keamanan Dan Monitoring Jaringan Pada SMA N 10 Kota Bengkulu?.

1.3. Batasan Masalah

Mengingat begitu luasnya ruang lingkup pada penelitian ini, maka penulis membatasi permasalahan tersebut. Diantaranya adalah sebagai berikut:

1. Sistem operasi yang digunakan adalah linux ubuntu server 20.04

2. Aplikasi atau tool untuk melakukan monitoring dan keamanan menggunakan IPTable dan Grafana.
3. Monitoring jaringan di fokuskan pada trafik data
4. Monitoring dan keamanan jaringan dilakukan pada jaringan LAN Laboratorium computer, TU dan Perpustakaan SMA N 10 Kota Bengkulu.

1.4. Tujuan Penelitian

Adapun tujuan penelitian ini adalah:

1. Banyak hal yang dapat dipertimbangkan dalam penggunaan perangkat ini yakni, salah satunya adalah biaya. Dengan biaya yang cukup murah kita sudah membuat sistem jaringan yang handal dan efisien
2. Dengan pemanfaatan *IPTable* dan *Grafana* dapat membangun sebuah sistem keamanan pada jaringan computer dengan biaya rendah serta kemampuan yang mumpuni dalam melakukan monitoring dan pengamanan jaringan.
3. Sebagai salah satu syarat untuk penyusunan Skripsi Studi Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu.

1.5. Manfaat Penelitian

- 1) Bagi SMA N 10 Kota Bengkulu

Dapat dijadikan salah satu pedoman untuk dapat membangun jaringan komputer dengan menggunakan *server* dengan system operasi linux ubuntu server 20.04 dan *tool* atau aplikasi *IPTable* dan *Grafana*, kita sudah dapat mengelola suatu jaringan yang sangat kompleks. Banyak hal yang dapat dipertimbangkan dalam menggunakan perangkat ini, salah satunya adalah biaya. Dengan biaya yang cukup murah kita sudah membuat sistem jaringan yang handal dibantu dengan sistem

operasi yang bersifat *open source* dapat mengurangi pengeluaran biaya dan yang paling utama kinerja dalam melakukan monitoring dan keamanan pada jaringan.s

2) Bagi Penulis

- a. Dapat menambah Ilmu Pengetahuan dan Teknologi (IPTEK)
- b. Dapat menambah motivasi dan inspirasi untuk mengembangkan serta menerapkan perangkat lunak yang lebih baik, efektif, dan efisien.
- c. Dapat menentukan teknik membangun suatu jaringan komputer yang handal, efisien baik dari segi biaya dan lainnya.

BAB II

LANDASAN TEORI

2.1 Pengertian Implementasi

Menurut Irawan (2018:67), implementasi merupakan suatu proses mendapatkan suatu hasil yang sesuai dengan tujuan atau sasaran kebijakan itu sendiri. Dimana pelaksana kebijakan melakukan suatu aktivitas atau kegiatan..

Menurut Annur (2019:70) implementasi atau pelaksanaan adalah bermuara pada aktivitas, aksi, tindakan, atau adanya mekanisme suatu sistem. Implementasi bukan sekedar aktivitas, tetapi suatu kegiatan yang terencana dan untuk mencapai tujuan kegiatan.

Berdasarkan uraian mengenai kedua pendapat tentang pengertian implementasi, perlu kami memberikan batasan. Implementasi adalah pelaksanaan dari apa yang telah ditetapkan dan menerima segala akibat/dampak setelah dilaksanakan tersebut. Proses implementasi sekurang-kurangnya terdapat tiga unsur yang penting dan mutlak, yaitu:

1. Adanya program atau kebijakan yang dilaksanakan;
2. Target *groups*, yaitu kelompok masyarakat yang menjadi sasaran, dan diharapkan dapat menerima manfaat dari program tersebut, perubahan atau peningkatan;
3. Unsur pelaksana (*implementor*), baik organisasi atau perorangan, yang bertanggungjawab dalam pengelolaan, pelaksanaan, dan pengawasan dari proses implementasi tersebut.

2.2 Pengertian *Quality of Service* (QoS)

Menurut Romony (2020:19) QoS adalah suatu metode pengukuran yang digunakan untuk menghitung kualitas sebuah jaringan dan merupakan suatu usaha dalam mendefinisikan atau menggambarkan karakteristik dan model pada sebuah *service*. Beberapa parameter yang digunakan untuk mengukur QoS adalah sebagai berikut:

1. *Delay*

Delay adalah waktu yang diperlukan dalam proses pengiriman data dari asal ke tujuan. *Delay* dapat dipengaruhi oleh jarak, media fisik, *congestion* atau waktu proses yang lama.

2. *Data Loss*

Data loss adalah suatu parameter yang mengukur persentase data hilang yang dapat terjadi karena *collision* dan *congestion* pada jaringan.

3. *Throughput*

Throughput mengukur kecepatan pertukaran data yang diukur dalam bps (*bit per second*). *Throughput* adalah jumlah total dari paket yang berhasil dan sukses diterima dalam jangka waktu tertentu dibagi durasi jangka waktu tersebut.

4. *Jitter*

Jitter disebut juga variasi *delay*, dimana *jitter* berhubungan erat dengan *latency*, yang memperlihatkan banyaknya variasi *delay* pada transmisi data di jaringan. *Jitter* terjadi karena variasi-variasi dalam panjang antrian, dalam waktu pengolahan data, dan juga dalam waktu pembentukan ulang paket-paket di akhir perjalanan

Menurut Armanto (2020:9) *Quality of Service* (QoS) dapat dikatakan sebagai suatu terminology yang digunakan untuk mendefinisikan karakteristik suatu layanan (*Service*) jaringan untuk mengetahui seberapa baik kualitas yang ada pada layanan tersebut. QoS didesain untuk membantu *end server* menjadi lebih produktif dengan memastikan bahwa *user* mendapatkan kinerja yang handal dari aplikasi-aplikasi jaringan. Dengan adanya *Quality of Service* (QoS) maka *bandwidth* dapat digunakan secara optimal sehingga dapat meningkatkan kualitas layanan internet yang diterima oleh pengguna.

Sejarah jaringan komputer dimulai pada tahun 1940 di Amerika Serikat melalui proyek pengembangan komputer Model I di laboratorium Bell dan kelompok riset Harvard University yang dipimpin oleh Howard Aiken. Saat itu, proyek tersebut hanya bertujuan untuk memanfaatkan sebuah perangkat komputer sehingga dapat dipakai bersama. Pada tahun 1950, saat komputer mulai berkembang dan superkomputer lahir, muncullah

kebutuhan akan sebuah komputer yang mampu melayani banyak terminal. Kemudian ditemukanlah konsep TSS (*Time Sharing System*) atau sistem antrian. Pada tahun 1969, terbentuklah jaringan komputer pertama yang disebut ARPANET.

Manfaat atau keuntungan dibangunnya jaringan komputer adalah:

1. Komputer-komputer yang saling terhubung dapat melakukan *sharing file* maupun *sharing folder*, yaitu pemakaian *file* atau *direktori* secara bersama-sama.
2. Dengan adanya penyimpanan *file* terpusat (*file server*), file atau data yang ada di *server* dapat saling dibagi.
3. Memungkinkan pemakaian aplikasi secara bersama-sama oleh multiuser.
4. Memudahkan kita membackup data (membuat data cadangan).
5. Memungkinkan kita untuk mendapatkan data terbaru/terkini secara cepat.

Berdasarkan area atau luas wilayah, jaringan komputer dibedakan menjadi tiga, yaitu:

1. LAN (*Local Area Network*)

LAN atau Local Area Network adalah jaringan komputer untuk area yang tidak begitu luas. Batasan ukuran luas LAN adalah satu gedung. Contoh LAN adalah jaringan yang terdapat di sekolah-sekolah yang menghubungkan komputer milik siswa, komputer milik guru dan komputer milik bagian administrasi.

Dalam LAN kita dapat workgroup atau kumpulan dari beberapa komputer atau user yang melakukan sharing resources atau berbagi sumber daya. Sebagai contoh, workgroup guru terdiri dari user guru1, guru2, guru3 dan seterusnya, sedangkan workgroup siswa terdiri dari user siswa1, siswa2 dan seterusnya. Penggunaan workgroup seperti ini akan memudahkan penanganan atau manajemen jaringan.

2. MAN (*Metropolitan Area Network*)

MAN atau *Metropolitan Area Network* adalah jaringan komputer yang menghubungkan komputer-komputer dalam suatu kota. Contoh jaringan ini adalah jaringan antar beberapa sekolah dalam satu kota. Konsep MAN sama seperti LAN, yakni melakukan sharing *resources* atau berbagi pakai sumber daya, hanya saja lingkungannya lebih luas.

3. WAN (*Wide Area Network*)

WAN atau *Wide Area Network* adalah jaringan komputer dengan cakupan geografis paling luas hingga menjangkau pulau lain, negara lain, benua lain, bahkan luar angkasa. WAN biasanya merupakan kumpulan dari sejumlah LAN dan MAN.

2.2 **Tijauan Grafana**

Menurut Abdullah (2018:18) Grafana adalah perangkat analisis dan visualisasi metrik berbasis open source. Grafana paling sering digunakan untuk memvisualisasikan data deret waktu untuk infrastruktur dan analisis aplikasi. Namun Grafana tidak hanya sebatas hal itu saja, kerap kali servis digunakan untuk visualisasi sensor industri, pengimplementasian *internet of thing* (IoT), pengamatan cuaca dan pengontrolan proses yang sedang berjalan. Ada berbagai macam opsi penataan dan pemformatan yang diekspos setiap panel untuk memungkinkan pembuatan desain yang sempurna. Terdapat lima jenis panel dalam Grafana, yaitu grafik, singlestat, dashlist, tabel dan teks. Panel grafik memungkinkan untuk membuat grafik metric dan seri sebanyak yang diinginkan. Panel singlestat membutuhkan pereduksian sebuah query ke sebuah nomor. Dashlist dan teks adalah panel khusus yang tidak terhubung ke sumber data apapun.



Gambar 2.1 Logo Grafana

Grafana adalah analitik sumber terbuka multi-platform dan aplikasi web visualisasi interaktif. Ini memberikan bagan, grafik, dan peringatan untuk web saat terhubung ke sumber data yang didukung. Ada juga versi Grafana *Enterprise* berlisensi dengan kemampuan tambahan yang tersedia sebagai instalasi yang dihosting sendiri atau akun di layanan *cloud Grafana Labs*. Ini dapat diperluas melalui sistem *plug-in*. Pengguna akhir dapat membuat *dashboard* pemantauan yang kompleks menggunakan pembuat *kueri* interaktif. Grafana dibagi menjadi *front end* dan *back end*, masing-masing ditulis dalam *TypeScript* dan *Go*.

Sebagai alat visualisasi, Grafana adalah komponen yang populer dalam monitoring stack, sering digunakan dalam kombinasi dengan database deret waktu seperti InfluxDB, Prometheus dan Graphite, platform pemantauan seperti Sensu, Icinga, Checkmk, Zabbix, Netdata, dan PRTG, SIEM seperti Elasticsearch dan Splunk, dan sumber data lainnya. Antarmuka pengguna Grafana awalnya didasarkan pada Kibana versi 3. Grafana adalah software visualisasi dan analisis open source. Grafana memungkinkan pengguna memvisualisasikan data dari database deret waktu menjadi grafik yang mudah dibaca, Seperti dapat dilihat pada tampilan gambar dibawah ini:

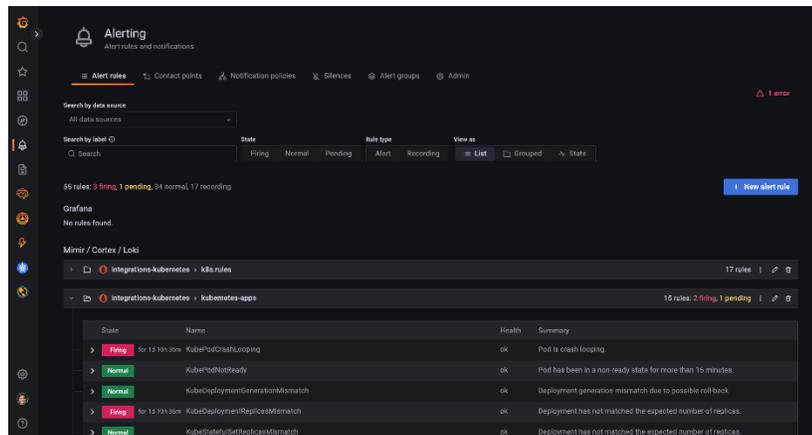


Gambar 2.2 Tampilan Visualisasi Monitoring Grafana

Dari tampilan gambar diatas dapat dilihat Grafana dapat menampilkan hasil monitoring dalam bentuk grafik sehingga mempermudah dalam pembacaan data. Grafana sendiri pertama kali diterbitkan pada tahun 2014 oleh Torkel Ödegaard. Pada saat itu, antarmuka yang digunakan oleh Grafana didasarkan pada Kibana 3 dan basis data deret waktu yang ditargetkan seperti InfluxDB dan Prometheus. Namun seiring berjalannya waktu, Grafana juga akan mendukung database relasional seperti MySQL, PostgreSQL, dan lain-lain. Grafana sangat cocok untuk membuat Dashboard yang dinamis dengan berbagai menu bawaan. Grafana juga memiliki dashboard template yang bisa digunakan untuk mengumpulkan variabel data yang digunakan, Grafana sangat support dalam visualisasi data dalam bentuk time series.

Grafana digunakan untuk menampilkan status service yang berjalan pada aplikasi maupun server yang digunakan. Namun Grafana bukan hanya digunakan untuk itu saja tetapi juga dapat digunakan dalam visualisasi sensor industri, pengimplementasian *Internet of thing* (IoT), pengamatan cuaca dan pengontrolan proses yang sedang berjalan. Terdapat berbagai macam pilihan untuk membuat *dashboard* yang bagus . Grafana memiliki

beberapa panel yang dapat digunakan seperti grafik, *single stat*, *dashlist*, *tabel* dan *teks*. Panel grafik digunakan dalam pembuatan grafik metric dan seri sebanyak yang diinginkan.



Gambar 2.3 Alert Yang Ditampilkan Grafana

Beberapa data *source* yang didukung dari Grafana, antara lain : *Graphite*, *InfluxDB*, *OpenTSDB*, *IPTable*, *Elasticsearch*, dan *CloudWatch*. Grafana hadir dengan *plugin* data *source* yang sangat lengkap untuk *InfluxDb*. Grafana mendukung berbagai macam *editor query* dengan fitur yang kaya, *anotasi* dan *templating queries*

2.5 Tinjauan Firewall

Menurut Kusuma (2022:699) *Firewall* atau dinding api adalah sistem perangkat lunak yang mengizinkan lalu lintas jaringan yang dianggap aman untuk dapat melaluinya dan mencegah lalu lintas jaringan yang dianggap tidak aman. Pada dasarnya sebuah *firewall* dipasang pada sebuah *router* yang berjalan pada *gateway* antara jaringan lokal dengan jaringan Internet. *Firewall* juga dapat dikatakan sebuah sistem pengaman, jadi *firewall* bisa berupa apapun baik *hardware* maupun *software*. *Firewall* dapat digunakan untuk memfilter paket-paket dari luar dan dalam jaringan di mana ia berada. Jika pada kondisi normal semua orang dari luar jaringan anda dapat bermain-main ke computer anda, dengan *firewall* semua itu dapat diatasi dengan mudah.

Firewall merupakan gabungan antara perangkat keras komputer (*Hardware*) dan perangkat lunak Komputer (*Software*), yang ditujukan untuk mengatur dan mengawasi lalu lintas paket data didalam jaringan komputer. Segmen tersebut dapat merupakan sebuah *workstation, server, router*, atau *local area network (LAN)*. *Firewall* secara umum di peruntukkan untuk melayani:

1. Mesin / komputer Setiap individu yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi.
2. Jaringan Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang dimiliki oleh perusahaan, organisasi dsb.

2.4.1 Karakteristik *Firewall*

Karakteristik *firewall* dibagi menjadi 3, yaitu:

1. Seluruh hubungan atau kegiatan dari dalam ke luar, harus melewati *firewall*. Hal ini dapat dilakukan dengan cara memblok atau membatasi baik secara fisik semua akses terhadap jaringan lokal, kecuali melewati *firewall*. Banyak sekali bentuk jaringan yang memungkinkan.
2. Hanya kegiatan yang terdaftar atau dikenal yang dapat melewati atau melakukan hubungan, hal ini dapat dilakukan dengan mengatur *policy* pada konfigurasi keamanan lokal. Banyak sekali jenis *firewall* yang dapat dipilih sekaligus berbagai jenis *policy* yang ditawarkan.
3. Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan atau kelemahan. hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan *operating system* yang relatif aman

2.4.2 Teknik Yang Digunakan Firewall

Teknik-teknik yang digunakan *firewall* ada 4, yaitu:

5. *Service control* (kendali terhadap layanan) Berdasarkan jenis-jenis layanan yang digunakan di internet dan boleh diakses baik untuk kedalam ataupun keluar *firewall*. Biasanya *firewall* akan memeriksa nomor *IP Address* dan juga nomor *port* yang digunakan baik pada protokol TCP dan UDP, bahkan bisa dilengkapi *software* untuk *proxy* yang akan menerima dan menterjemahkan setiap permintaan akan suatu layanan sebelum mengijinkannya. Bahkan bisa jadi *software* pada *server* itu sendiri, seperti layanan untuk *web* ataupun untuk *mail*.
6. *Direction Control* (kendali terhadap arah) Berdasarkan arah dari berbagai permintaan (*request*) terhadap layanan yang akan dikenali dan diijinkan melewati *firewall*.
7. *User control* (kendali terhadap pengguna) Berdasarkan pengguna atau *user* untuk dapat menjalankan suatu layanan, artinya ada *user* yang dapat dan ada yang tidak dapat menjalankan suatu servis, hal ini di karenakan *user* tersebut tidak diijinkan untuk melewati *firewall*. Biasanya digunakan untuk membatasi *user* dari jaringan lokal untuk mengakses keluar, tetapi bisa juga diterapkan untuk membatasi terhadap pengguna dari luar.
8. *Behavior Control* (kendali terhadap perlakuan) Berdasarkan seberapa banyak layanan itu telah digunakan. Misal *firewall* dapat memfilter email untuk menanggulangi atau mencegah *spam*

2.4.3 Jenis-Jenis Firewall

Jenis-jenis *firewall* ada 3, yaitu:

1. *Packet Filtering Router*

Packet Filtering diaplikasikan dengan cara mengatur semua *packet* IP baik yang menuju, melewati atau akan dituju oleh packet tersebut. Pada jenis ini packet tersebut akan diatur apakah akan diterima dan diteruskan, atau di tolak. Penyaringan *packet* ini di konfigurasi untuk menyaring *packet* yang akan di transfer secara dua arah (baik dari atau ke jaringan lokal). Aturan penyaringan didasarkan pada *header* IP dan *transport header*, termasuk juga alamat awal (IP) dan alamat tujuan (IP), protokol transport yang digunakan (UDP,TCP), serta nomor *port* yang digunakan. Kelebihan dari jenis ini adalah mudah untuk diimplementasikan, transparan untuk pemakai, lebih cepat. Adapun kelemahannya adalah cukup rumitnya untuk menyetting paket yang akan difilter secara tepat, serta lemah dalam hal autentikasi. Adapun serangan yang dapat terjadi pada firewall dengan jenis ini adalah:

a. *IP address spoofing*

intruder (penyusup) dari luar dapat melakukan ini dengan cara menyertakan atau menggunakan *ip address* jaringan lokal yang telah diijinkan untuk melalui *firewall*.

b. *Source routing attacks*

jenis ini tidak menganalisa informasi *routing* sumber IP, sehingga memungkinkan untuk mem-*bypass firewall*.

c. *Tiny Fragment attacks*

intruder (penyusup) membagi IP kedalam bagian-bagian (*fragment*) yang lebih kecil dan memaksa terbaginya informasi mengenai *TCP header*. Serangan jenis ini di *design* untuk menipu aturan penyaringan yang bergantung kepada informasi dari *TCP header*. Penyerang berharap hanya bagian (*fragment*) pertama saja yang akan di periksa dan sisanya akan bisa lewat dengan bebas. Hal ini dapat di tanggulangi dengan cara menolak semua packet dengan protokol TCP dan memiliki *offset* sama dengan 1 pada *IP fragment* (bagian IP)

2. *Application-Level Gateway*

Application-level Gateway yang biasa juga di kenal sebagai *proxy server* yang berfungsi untuk memperkuat atau menyalurkan arus aplikasi. Jenis ini akan mengatur semua hubungan yang menggunakan layer aplikasi, baik itu ftp, http, gopher dll. Cara kerjanya adalah apabila ada pengguna yang menggunakan salah satu aplikasi semisal ftp untuk mengakses secara *remote*, maka *gateway* akan meminta user memasukkan alamat *remote host* yang akan di akses.

Saat pengguna mengirimkan *user ID* serta informasi lainnya yang sesuai maka *gateway* akan melakukan hubungan terhadap aplikasi tersebut yang terdapat pada *remote host*, dan menyalurkan data diantara kedua titik. Apabila data tersebut tidak sesuai maka firewall tidak akan meneruskan data tersebut atau menolaknya. Lebih jauh lagi, pada jenis ini *firewall* dapat di konfigurasi untuk hanya mendukung beberapa aplikasi saja dan menolak aplikasi lainnya untuk melewati *firewall*.

Kelebihannya adalah relatif lebih aman daripada jenis *packet filtering router* lebih mudah untuk memeriksa (audit) dan mendata (log) semua aliran data yang masuk pada level aplikasi. Kekurangannya adalah pemrosesan tambahan yang berlebih pada setiap hubungan yang akan mengakibatkan terdapat dua buah sambungan koneksi antara pemakai dan *gateway*, dimana *gateway* akan memeriksa dan meneruskan semua arus dari dua arah.

3. *Circuit-level Gateway*

Jenis ketiga ini dapat merupakan sistem yang berdiri sendiri, atau juga dapat merupakan fungsi khusus yang terbentuk dari jenis *application-level gateway*. Jenis ini tidak mengizinkan koneksi TCP *end to end* (langsung).

Cara kerjanya yaitu: *gateway* akan mengatur kedua hubungan TCP tersebut, 1 antara dirinya dengan TCP pada pengguna lokal (*inner host*), serta 1 lagi antara dirinya dengan TCP pengguna luar (*outside host*). Saat dua buah hubungan terlaksana, *gateway* akan menyalurkan TCP segment dari satu hubungan ke lainnya tanpa memeriksa isinya.

Fungsi pengamanannya terletak pada penentuan hubungan mana yang diijinkan. Penggunaan jenis ini biasanya dikarenakan administrator percaya dengan pengguna internal (*internal users*).

2.5 Tinjauan IPTable

Menurut Mardiansyah (2021:191) Iptables adalah suatu *tools* dalam sistem operasi linux yang berfungsi sebagai alat untuk melakukan *filtering* (penyaringan) terhadap (*traffic*) lalu lintas data. Secara sederhana digambarkan sebagai pengatur lalu lintas data. Dengan iptables inilah akan bisa mengatur semua lalu lintas dalam komputer, baik yang

masuk ke komputer, keluar dari komputer, ataupun *traffic* yang sekedar melewati komputer. Iptables merupakan sistem *firewall* di sistem *open source* yang mendukung layer 3 (*Network layer*), layer 4 (*Transport layer*) dan layer 7 OSI layer.

Dengan kemampuan tools iptables ini, dapat dilakukan banyak hal. Salah satunya yaitu dapat membuat aturan (*rule*) untuk arus lalu lintas data. Aturan-aturan itu dapat mencakup banyak hal, seperti besar data yang boleh lewat, jenis paket/datagram yang dapat diterima, mengatur *traffic* berdasarkan asal dan tujuan data, *forwarding*, *NAT*, *redirecting*, pengelolaan *port* dan firewall.

2.5.1 Cara Kerja IPTable

Iptables bekerja dengan cara membaca lalu lintas jaringan dan membandingkannya dengan serangkaian aturan yang sudah dibuat. Aturan dalam iptables berbentuk *table* yang terdiri dari serangkaian *rules* atau aturan yang disebut *chain*. Ada tiga *table* utama dalam Iptables, yaitu *Filter*, *NAT* dan *Mangle*.

2.5.1 Tabel *Filter* Pada IPTables

Tabel *Filter* adalah tabel yang paling sering digunakan untuk mengatur lalulintas jaringan dalam server. Tabel *filter* memungkinkan Anda bisa mengizinkan, memblokir atau memutus koneksi dari IP address atau *port* tertentu. Tabel *filter* terdiri dari beberapa *rule*, yaitu:

1. *Accept*: menerima paket masuk.
2. *Reject*: menolak paket masuk.
3. *Drop*: memutuskan koneksi paket.
4. *Log*: mencatat paket.

2.5.3 Perintah Iptables

Beberapa contoh perintah dasar dari *rule* dalam tabel *filter* yang paling sering digunakan:

1. Whitelist IP Address

Mengizinkan koneksi masuk:

```
iptables -A INPUT -s IP_Address -j ACCEPT
```

Mengizinkan koneksi keluar:

```
iptables -A OUTPUT -d IP_Address -j ACCEPT
```

2. Memblokir IP Address

Memblokir koneksi masuk:

```
iptables -A INPUT -s IP_Address -j DROP
```

Memblokir koneksi keluar:

```
iptables -A OUTPUT -d IP_Address -j DROP
```

3. Membuka Port

Membuka port masuk:

```
iptables -A INPUT -p tcp -dport nomor_port -j ACCEPT
```

Membuka port keluar:

```
iptables -A OUTPUT -p tcp -d -dport nomor_port -j ACCEPT
```

4. Memblokir Port

Memblokir port masuk:

```
iptables -A INPUT -p tcp -dport nomor-port -j DROP
```

Memblokir port keluar:

iptables -A OUTPUT -p tcp -dport nomor_port -j DROP

2.6 Tjauan Linux Ubuntu

Menurut Mardiansyah (2021:192) Ubuntu adalah salah satu distribusi linux yang berbasis Debian dan didistribusikan menjadi perangkat lunak sistem operasi yang bebas. Secara singkat dan jelasnya yaitu ubuntu adalah sejenis sistem operasi berbasis linux Debian.

Berdasarkan basisnya, distro Linux dibagi antara :

1. Debian seperti Knoppix, Ubuntu, KuliAx, BlankON, dan lain-lain.
2. RPM (*RedHat Package Manager*) seperti PC Linux OS, Fedora Core, IGOS, CentOS, EduLinux, dan lain-lain.
3. Slackware seperti Slackware, Kate OS, Truva Linux, ZenCafe Linux, Wolfix dan lain-lain.

Distribusi-distribusi menggunakan kernel Linux yang disetujui Linus Torvalds sehingga menjamin kompatibilitas. Perbedaan antara lain pada :

1. Paket-paket perangkat lunak yang disetakan di distribusi.
2. Struktur direktori.
3. Metode pemaketan perangkat lunak.
4. Inisialisasi sistem.

Ubuntu adalah salah satu distribusi Linux yang berbasis Debian GNU/Linux dan memiliki interface desktop (Wikipedia, 2008). Ubuntu adalah sepenuhnya sistem operasi open source yang dibangun berdasarkan kernel Linux. Nama Ubuntu sendiri diambil dari bahasa kuno Afrika Zulu dan Xhosa (oo-boon-too) yang artinya “rasa

perikemanusiaan terhadap orang lain”.

Berdasarkan Ubuntu *Documentation Project* dijelaskan bahwa lingkungan desktop bawaan Ubuntu adalah GNOME, platform pengembangan dan keluarga desktop UNIX dan Linux terdepan. Skema penomoran versi Ubuntu didasarkan pada tanggal rilis sebuah versi dari distribusi. Nomor versi berasal dari tahun dan bulan rilis, bukan mencerminkan versi sebenarnya dari perangkat lunak.

Ubuntu mempunyai filosofi sebagai berikut:

9. Bahwa perangkat lunak harus tersedia dengan bebas biaya
10. Bahwa aplikasi perangkat lunak tersebut harus dapat digunakan dalam bahasa lokal masing-masing dan untuk orang-orang yang mempunyai keterbatasan fisik
11. Bahwa pengguna harus mempunyai kebebasan untuk mendapatkan, mengubah, dan mendistribusikan perangkat lunak sesuai dengan apa yang mereka butuhkan tanpa halangan apapun

Ubuntu terdiri dari banyak paket, kebanyakan berasal dari distribusi di bawah lisensi lisensi software bebas. Namun, beberapa *software* khususnya driver menggunakan *Proprietary software*. Lisensi yang pada umumnya adalah GNU *General Public License* (GNU GPL) dan GNU *Lesser General Public License* (GNU LGPL), dengan tegas menyatakan bahwa pengguna dengan bebas dapat menjalankan, menggandakan, mempelajari, memodifikasi, dan mendistribusikan tanpa pembatasan apapun. Namun tetap ada *software proprietary* yang dapat berjalan di Ubuntu. Ubuntu berfokus pada ketersediaan kegunaan pada orang dengan disabilitas. Ubuntu juga berfokus pada internasionalisasi dan aksesibilitas untuk dapat menjangkau banyak orang. Dalam hal

keamanan, perangkat sudo dapat meningkatkan privilege secara sementara untuk melakukan tugas administratif, sehingga akun root dapat terus terkunci, dan mencegah orang tidak terauthorisasi melakukan perubahan sistem atau membuka kelemahan keamanan.

Desktop Ubuntu memakai desktop *environment* grafis. Sebelum Ubuntu 11.04 interaksi grafis pengguna adalah GNOME versi 2, tetapi setelah versi 11.04, berubah menjadi Unity. Unity adalah lingkungan desktop yang dikembangkan oleh Canonical yang awalnya dirancang untuk edisi Netbook. Tetapi GNOME dipakai kembali mulai versi 17.10.

Pemasangan Ubuntu biasa (bukan minimal) termasuk perangkat lunak berikut ini:

1. Perangkat dokumen
2. LibreOffice
3. OpenOffice (sebelum 11.04)
4. Peramban
5. Mozilla Firefox
6. E-Mail browser
7. Mozilla Thunderbird
8. Evolution (sebelum Ubuntu 11.10)
9. Game-game ringan
10. Sudoku
11. Chess
12. mines

Dan beberapa software juga termasuk ke dalam CD instalasi sebelum Ubuntu 11.04 seperti Transmission, GIMP. Namun *software* tersebut dihilangkan dari CD instalasi karena ukurannya yang besar. Ubuntu juga dapat menjalankan program Windows lewat *Wine* atau *Virtual Machine* (seperti *VMware workstation* atau *Virtual Box*).

Ubuntu, tidak seperti Debian, mengompile paket mereka menggunakan fitur gcc seperti PIE dan proteksi *Buffer Overflow* untuk memproteksi *software* mereka. Fitur Ekstra tersebut menambah keamanan secara signifikan dengan pemakaian performance hanya 1% pada 32 bit dan 0,01% pada 64 bit.

Pemasangan perangkat lunak tambahan di Ubuntu dapat dilakukan melalui Ubuntu *Software*, antarmuka perintah (melalui perintah `apt` atau `apt-get`). Dukungan untuk sistem paket lintas-sistem seperti *Snap* dan *Flatpak* telah tersedia sebagai alternatif.

BAB III

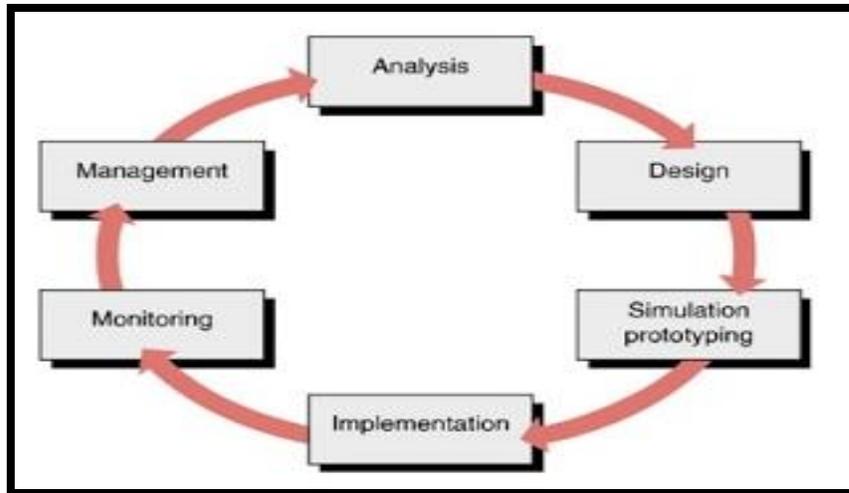
METODOLOGI PENELITIAN

3.1 Tempat dan Waktu Penelitian

Penelitian dilakukan pada SMA N 10 Kota Bengkulu, mulai dari Maret 2022 sampai dengan selesai. Struktur Organisasi terlampir

3.2 Metodologi Penelitian

Dalam Penelitian skripsi ini penulis menggunakan metode penelitian *Network Development Life Cycle* (NDLC) merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi, daur hidup pengembangan aplikasi, dan analisis pendistribusian data. Jika pengimplementasian teknologi jaringan dilaksanakan dengan efektif, maka akan memberikan sistem informasi yang akan memenuhi tujuan strategis, kemudian pendekatan top-down dapat diambil. Berikut ini adalah tahapan dari NDLC



Gambar 3.1 Tampilan Sirkulasi (Tahapan) Metode NDLC

Keterangan:

1. *Analysis*

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa topologi jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya:

- a. Wawancara, dilakukan dengan pihak terkait yaitu guru dan tenaga pendidik pada laboratorium computer SMA N 10 Kota Bengkulu.
- b. Survey langsung kelapangan, pada tahap analisis juga biasanya dilakukan survey langsung kelapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya sebelum masuk ke tahap desain.
- c. Membaca manual atau *blueprint* dokumentasi, pada analisis awal ini juga dilakukan dengan mencari informasi dari manual-manual atau blueprint dokumentasi yang mungkin pernah dibuat sebelumnya.

d. Menelaah setiap data yang didapat dari data-data sebelumnya, maka perlu dilakukan analisa data tersebut untuk masuk ke tahap berikutnya.

2. *Design.*

Dari data-data yang didapatkan sebelumnya, tahap design ini akan membuat gambar desain topologi jaringan computer yang akan dibangun. Diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Desain bisa berupa desain struktur topologi, desain akses data, desain *layout* perkabelan, dan sebagainya yang akan memberikan gambaran jelas tentang proyek yang akan dibangun. Biasanya hasil dari design berupa:

- a. Gambar-gambar topologi (*server farm, firewall, datacenter, storages, lastmiles*, perkabelan, titik akses dan sebagainya);
- b. Gambar-gambar detail estimasi kebutuhan yang ada.

3. *Simulation Prototype.*

Simulasi dilakukan untuk topologi jaringan, disini penulis menggunakan topologi star, Untuk melakukan simulasi penulis menggunakan paket *tracert*.

4. *Implementation.*

Pada tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi pekerja jaringan akan menerapkan semua yang telah direncanakan dan didesain sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil/gagalnya proyek yang akan dibangun dan ditahap inilah *team work* akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis. Ada beberapa Masalah-masalah yang sering muncul pada tahapan ini, diantaranya:

- a. Jadwal yang tidak tepat karena faktor-faktor penghambat

- b. Masalah dana/anggaran dan perubahan kebijakan
- c. Team work yang tidak solid

peralatan pendukung dari vendor makanya dibutuhkan manajemen proyek dan manajemen resiko untuk meminimalkan sekecil mungkin hambatan-hambatan yang ada.

5. *Monitoring.*

Setelah implementasi tahapan *monitoring* merupakan tahapan yang penting, agar jaringan komputer dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan awal dari user pada tahap awal analisis, maka perlu dilakukan kegiatan *monitoring*. Monitoring menggunakan Grafana, diantaranya melakukan monitoring trafik data seperti lalu lintas data dan bandwidth yang digunakan.

6. *Management.*

Pada level manajemen atau pengaturan, salah satu yang menjadi perhatian khusus adalah masalah kebijakan (*policy*). Kebijakan perlu dibuat untuk membuat/mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur *reliability* terjaga. *Policy* akan sangat tergantung dengan kebijakan level management dan strategi bisnis perusahaan tersebut. IT sebisa mungkin harus dapat mendukung atau alignment dengan strategi bisnis perusahaan. Manajemen jaringan yang digunakan yaitu IPTable.

3.3 Perangkat Keras dan Perangkat Lunak

3.3.1 Perangkat Keras

Adapun instrumen perangkat keras yang digunakan dalam penelitian ini adalah Personal Komputer dengan spesifikasi sebagai berikut :

1. PC Server dengan Spesifikasi Core i3
2. Laptop Core i3 untuk melakukan konfigurasi
3. Switch HUB
4. Lan Card
5. Kabel LAN (UTP), RJ 45 dan peralatan jaringan lainnya

3.3.2 Perangkat Lunak

Perangkat lunak yang penulis gunakan dalam penelitian ini adalah :

1. Sistem Operasi Windows 10 pada clien
2. Sistem Operasi Linux Ubuntu Server 20.04 pada server
3. IPTable dan Grafana untuk melakukan monitoring
4. Browser chrome

3.4 Metode Pengumpulan Data

Adapun metode penelitian yang digunakan penulis adalah :

a. Observasi

Yaitu melakukan observasi atau pengamatan langsung di Laboratorium Komputer SMA N 10 Kota Bengkulu pada *server* terhadap IPTable dan Grafana untuk melakukan monitoring Keamanan Jaringan.

b. wawancara

Yaitu melakukan proses tanya jawab yang dilakukan secara langsung pada guru TKJ dan staff laboratorium computer SMA N 10 Kota Bengkulu Bapak Saiful.

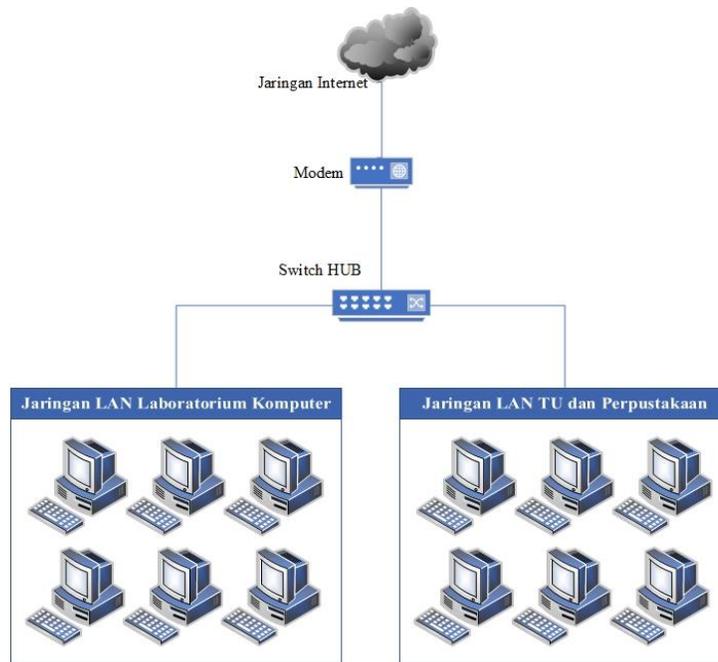
c. Pustaka

Yaitu suatu metode pengumpulan data yang diambil dari perpustakaan atau instansi yang berupa karya ilmiah, jurnal, buku-buku serta dari *internet* yang berhubungan dengan penulisan ini. Tujuan dari studi pustaka ini adalah untuk mendalami dan memperoleh keterangan yang lengkap terhadap obyek yang diteliti.

3.5 Analisa Sistem

3.5.1 Analisa Sistem Aktual

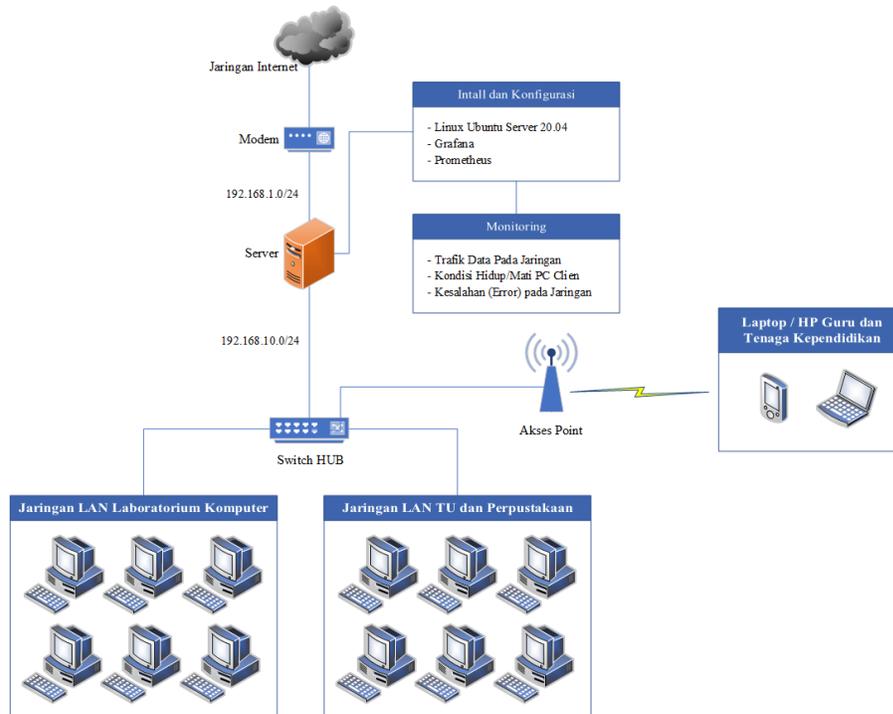
Sebagaimana telah diuraikan dalam latar belakang masalah, koneksi jaringan komputer pada SMA N 10 Kota Bengkulu masih berdiri sendiri-sendiri yaitu jaringan LAN pada Labor, TU dan ruangan guru. Disamping jaringan LAN masih berdiri sendiri-sendiri, jaringan komputer pada SMA N 10 Kota Bengkulu belum memiliki system monitoring dan keamanan sehingga sangat rentan disalah gunakan oleh pihak-pihak yang tidak bertanggung jawab. Adapun skema jaringan yang berjalan saat ini dapat dilihat pada tampilan gambar dibawah ini:



Gambar 3.2 Blok Diagram Global Aktual

3.5.2 Analisa Sistem Yang Diusulkan

Blok diagram global dari jaringan komputer pada SMA N 10 Kota Bengkulu yang terdiri dari jaringan komputer labor dan jaringan komputer Tata Usaha yang diusulkan. Jaringan computer yang diusulkan menggunakan satu IP Address untuk jaringan lokal yaitu IP Address class C dengan network 192.168.10.0/24, seperti dapat dilihat pada gambar 3.1 berikut.



Gambar 3.2 Blok Diagram Global Yang Di Usulkan

Keterangan Gambar

1. Internet Global merupakan jaringan internet yang umumnya.
2. Modem berfungsi untuk menghubungkan ke jaringan internet global. Dalam hal ini pada SMA N 10 Kota Bengkulu menggunakan Telkom Spedy Indihome dengan kecepatan 20 Mbps
3. Akses point digunakan untuk memancarkan sinyal wifi. Dan akses jaringan dengan menggunakan wifi hanya dapat diakses oleh guru dan tenaga kependidikan
4. Server berfungsi untuk melakukan monitoring dan pengamanan jaringan. Adapun pada server penulis melakukan installasi dan konfigurasi:

- a. Linux ubuntu server 20.04

Linux ubuntu server 20.04 merupakan sistem operasi yang digunakan pada PC server

- b. Grafana dan IPTable

Grafana dan IPTable merupakan tool yang digunakan untuk melakukan monitoring dan pengamanan jaringan. adapun monitoring dilakukan meliputi trafik data, UP/Down Client dan kesalahan (Error) yang terjadi pada jaringan. Berdasarkan data yang di dapat dari proses monitoring tersebut dilakukan pengamanan meliputi alamat web yang di blokir seperti (www.aladel.com dan www.sbobet.com), IP Address yang dapat mengakses jaringan dan lainnya yang dianggap perlu.

5. Swirch Hub berfungsi untuk membagi koneksi jaringan

3.5.3 Prinsip Kerja Sistem

Prinsip kerja sistem disini bertujuan untuk memfokuskan kerja sistem yang akan di gunakan dari rancangan blok diagram. Sistem pengujian yang akan di lakukan melalui proses persiapan alat alat yang di butuhkan, koneksi terhadap jaringan lan, koneksi terhadap jaringan internet global, menginstall software yang diperlukan. Sampai pada akhir mendapat kesimpulan berupa kemampuan dari pada Grafana dalam melakukan monitoring jaringan, seperti:

- a. Monitoring lalu lintas data
- b. Monitoring website yang dibuka
- c. Monitoring Trafik Jaringan

Dari hasil monitor tersebut akan dilakukan pembatasan pada *IPTable* dengan menggunakan server linux ubuntu server 20.04 untuk melakukan monitoring dan pengamanan jaringan. Sebagian rules yang diterapkan pada *IPTable*, dapat dilihat pada table dibawah ini:

Table 3.1 Rencana rules yang akan di terapkan

No	Source	Destination	Service	Action
1	192.168.10.0/24	192.168.1.1	any	Postrouting (NAT)
2	192.168.10.0/24	0.0.0.0	tcp/udp	limit --limit \$lim
3	192.168.10.0/24	www.aladel.com	HTTP/HTTPS	DROP
4	192.168.1.1	192.168.10.1	SSH	DROP
5	0.0.0.0	0.0.0.0	ICMP	DROP
6	... dst			

Keterangan:

1. Melakukan Network Address Translation (NAT), berfungsi untuk menjembatani IP Lokal ke Modem supaya jaringan lokal dapat melakukan akses internet
2. Untuk membatasi limit pemakaian dari jaringan lokal dan juga digunakan untuk membatasi kecepatan akses. Dimana pembagian bandwidth per IP Address Client Maksimal sebesar 2 MB dengan Maksimal Download sebesar 200 MB
3. Memblokir akses ke www.aladel.com dari jaringan lokal (192.168.10.0/24)
4. Untuk melakukan blokir akses ke SSH server (IP Server = 192.168.10.1 dan IP Modem = 192.168.1.1) dari jaringan internet
5. Untuk menghindari ping flood dari semua IP
6. Dan seterusnya

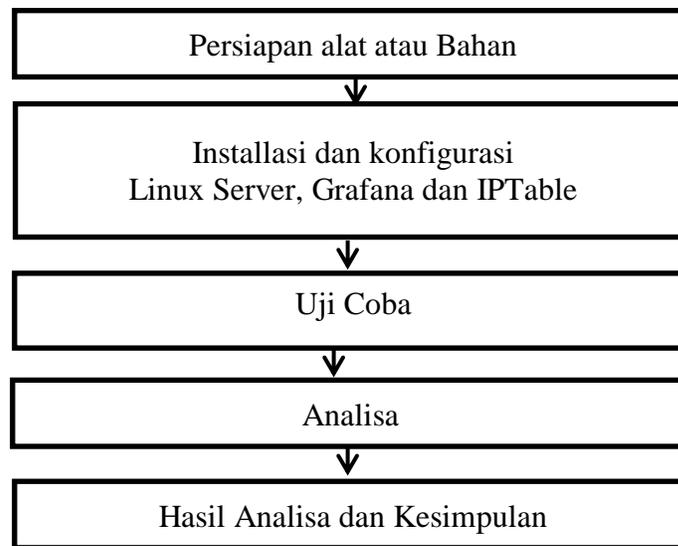
Nomor 1 pada rules diatas berfungsi untuk memperbolehkan IP Address dengan alamat network 192.168.10.0/24 untuk melakukan akses, nomor 2 dan 3 untuk melakukan blokir port 21 dan 22 (nomor 2 untuk blokir port 21 dari semua alamat IP Address dan nomor 3 blokir port berdasarkan request yang melalui eth1)

dan nomor 4 dan 5 untuk melakukan blokir alamat www.facebook.com atau facebook.com.

Berdasarkan rule tersebut maka ketika adanya request dari jaringan LAN yang menggunakan salah satu rule (khusus DROP) maka akan muncul indicator di halaman Grafana berupa icon lampu merah berkedip-kedip.

3.5.3 Rencana Kerja

Adapun rencana kerja dalam ini tidak terlepas dari blok diagram yang merupakan suatu pernyataan gambar yang ringkas, dari gabungan sebab dan akibat antara masukkan dan keluaran dari suatu sistem.



Gambar 3.3 Rencana Kerja

Keterangan :

1. Persiapan alat atau bahan.

Pada tahap ini penulis melakukan persiapan alat berupa mempersiapkan PC dan server linux yang akan penulis pakai. Diantara alat dan bahan yang digunakan adalah kabel UTP, RJ 45, Switch Hub dan lainnya

2. Installasi dan Konfigurasi

Pada tahap ini dilakukan installasi dan konfigurasi linux ubuntu server 20.04, Grafana dan IPTable. Pada tahap ini dilakukan konfigurasi-konfigurasi pada Grafana dan IPTable, diantaranya pengaturan IP Address dan pengaturan lainnya semua dengan fungsi dan kegunaan IPTable di terapkan

3. Uji Coba

Pada tahap ini penulis melakukan uji coba terhadap jaringan, IPTable dan Grafana dalam melakukan monitoring dan pengamanan jaringan. Yaitu melakukan ujicoba mulai dari konfigurasi, IP Address, koneksi dan ujicoba dalam monitoring dan pengamanan jaringan sesuai dengan penelitian.

4. Analisa

Maka setelah melakukan ujicoba penulis melakukan analisa data-data yang penulis dapati. Yaitu melakukan Analisa terhadap hasil ujicoba yang dilakukan seperti kemampuan Grafana dan IPTable dalam melakukan monitoring dan keamanan jaringan sampai Analisa terhadap pengembangan jaringan berdasarkan hasil monitoring

3.5.4 Rencana Pengujian

Pengujian sistem dilakukan menggunakan metode *black box*, yaitu dengan menguji kemampuan sistem berdasarkan spesifikasi yang telah ditentukan.

Tabel 3.2 Rencana Pengujian

No	Instrumen Pengujian	Analisa	Hasil	Ket
1	Kemampuan Grafana dalam melakukan monitoring jaringan a. Monitoring lalu lintas data b. Monitoring website yang dibuka c. Monitoring Trafik Jaringan			
2	Kemampuan IPTable dalam melakukan pengamanan jaringan seperti, Pemblokiran alamat-alamat situs/web yang tidak boleh diakses atau hal yang bisa membuat jaringan tidak stabil			
3	Kemampuan sistem operasi linux ubuntu server dalam mejalankan Grafana dan IPTable untuk melakukan monitoring dan keamanan jaringan			