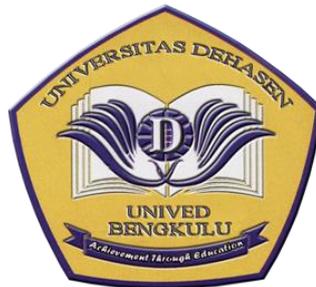


**PENERAPAN *FIREWALL* PADA SISTEM KEAMANAN JARINGAN
KOMPUTER DI SEKOLAH SMK NEGERI 5 SELUMA**

SKRIPSI



Oleh :

NOPRI DWIPOYONO
NPM. 16010104

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

**PENERAPAN *FIREWALL* PADA SISTEM KEAMANAN JARINGAN
KOMPUTER DI SEKOLAH SMK NEGERI 5 SELUMA**

SKRIPSI

**NOPRI DWIPOYONO
NPM. 16010104**

Diajukan Untuk Memperoleh Gelar Sarjana Komputer
Pada Program Studi Informatika

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

2023

**PENERAPAN *FIREWALL* PADA SISTEM KEAMANAN JARINGAN
KOMPUTER DI SEKOLAH SMK NEGERI 5 SELUMA**

SKRIPSI

Oleh :

NOPRI DWIPOYONO
NPM. 16010104

DISETUJUI OLEH :

PEMBIMBING I


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

PEMBIMBING II


Aji Sudarsono, S.Kom., M.Kom
NIDN. 02.270585.01

**MENGETAHUI,
KETUA PROGRAM STUDI
INFORMATIKA**

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

**PENERAPAN *FIREWALL* PADA SISTEM KEAMANAN JARINGAN
KOMPUTER DI SEKOLAH SMK NEGERI 5 SELUMA**

SKRIPSI

Disusun Oleh :

NOPRI DWIPOYONO
NPM. 16010104

Telah Dipertahankan di depan TIM Penguji
Universitas Dehasen Bengkulu

Hari : Sabtu
Tanggal : 17 Juni 2023

Skripsi ini telah diperiksa dan disetujui oleh TIM Penguji.

Penguji	Nama	NIDN	Tanda Tangan
Ketua	Khairil, S.Kom., M.Kom	02.130475.01	
Anggota	Aji Sudarsono, S.Kom., M.Kom	02.270585.01	
Anggota	Siswanto, SE, S.Kom, M.Kom	02.240363.01	
Anggota	Indra Kanedi, S.Kom., M.Kom	02.100581.01	

Mengetahui,
Dekan Fakultas Ilmu Komputer



Siswanto, SE, S.Kom, M.Kom
NIDN. 02.240363.01

RIWAYAT HIDUP



Nopri Dwipoyono adalah nama penulis ini. lahir pada 21 November 1998 di Lubuk Betung kabupaten Seluma provinsi Bengkulu, penulis merupakan anak ke dua dari dua bersaudara, dari pasangan Purwadi dan Kusumawati, penulis pertama kali masuk pendidikan di SD Negeri 8 Seluma pada tahun 2004 dan tamat 2010 pada tahun yang sama melanjutkan

pendidikan SMP Negeri 14 Seluma dan tamat pada tahun 2013, setelah tamat di SMP penulis melanjutkan ke SMA Negeri 4 Seluma dan tamat tahun 2016 dan pada tahun yang sama penulis terdaftar sebagai mahasiswa di Universitas Dehasen Fakultas Informatika Kota Bengkulu. Dengan ketekunan dan motivasi tinggi untuk terus belajar dan berusaha, penulis telah berhasil menyelesaikan pengerjaan tugas akhir skripsi ini, semoga dengan penulisan tugas akhir ini mampu memberikan kontribusi positif untuk dunia pendidikan Akhir kata penulis mengucapkan rasa syukur yang sebesar-besarnya atas terselesaikan skripsi yang berjudul " penerapan firewall pada keamanan jaringan komputer di sekolah SMK Negeri 5 Seluma "

MOTTO

“Hatiku tenang karena mengetahui bahwa apa yang melewatkanmu tidak akan pernah menjadi takdirku, dan apa yang ditakdirkan untukmu tidak akan pernah melewatkanmu”

(Umar bin Khattab)

“Nasib memang diserahkan kepada manusia untuk digarap, tetapi takdir harus ditandatangani di atas materai dan tidak boleh digugat kalau nanti terjadi apa-apa, baik atau buruk”

(Prof. Dr. Sapardi Djoko Damono)

Perbanyak bersyukur, kurangi mengeluh. Buka mata, jembarkan telinga, perluas hati. Sadari kamu ada pada sekarang, bukan kemarin atau besok, nikmati setiap momen dalam hidup, berpetuanglelah”

(Ayu Estiningtyas)

PERSEMBAHAN

Dengan Memanjatkan puji dan syukur kehadiran Allah SWT, dengan penuh kasih sayang dan kerendahan hati karya sederhana ini ku persembahkan kepada :

1. Kedua orang tua yang aku sayangi, bapakku Purwadi dan ibuku tercinta Kusumawati yang tiada henti memberikan motivasi serta merawatku, membesarkanku, mendidikku sejak kecil hingga dewasa serta mendukung dan mendoakan setiap langkah usaha dan perjuanganku hingga hari ini, esok dan seterusnya.
2. Kakakku Ike Purnamasari Amd.Keb yang selalu memberikan dorongan, nasehat, serta semangat kepadaku agar dapat menyelesaikan skripsi ini dengan baik
3. Buat keluarga besar di desa Lubuk Betung Kecamatan Sam, Kabupaten Seluma Terimakasih telah mendukung saya
4. Terimakasih untuk Bapak Khairil S.Kom., M.Kom pembimbing 1 dan Bapak Aji Sudarsono S.Kom., M.kom pembimbing 2 yang telah memberikan kontribusi berupa bimbingan, motivasi, saran atas terselesaikannya skripsi ini
5. Trimakasih untuk Bapak Siswanto SE., S.Kom., M.kom sebagai penguji 1 dan Bapak Indra Kanedi S.Kom., M.Kom sebagai penguji 2 yang telah banyak memberikan kritik dan saran yang sangat berharga demi terselesaikannya skripsi ini
6. Bapak Siswanto SE.,S.Kom., M.Kom selaku Dekan Fakultas Ilmu Komputer
7. Ibu liza Yulianti S.Kom, M.Kom ,selaku Ketua Program Studi Informatika
8. Teman-teman seperjuangan, (Raden dikky Zailani, Michel) yang selalu memberikan saran, semangat dan motivasi untuk menyelesaikan skripsi ini
9. Sahabat dan sepupuku (Adyaksah Lobi, Gendri, Guritno) yang selalu memberikan dorongan nasehat dan semangat untuk mencapai cita-citaku
10. Penyemangatku Firdaulan Suryono Putri
11. Almamater kuning yang aku bangga kan

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini :
Nama : Nopri Dwipoyono
NPM : 16010104
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 oranglain.
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 oranglain. Maka sya bersedia menerima sanksi akademik yang ditetapkan oleh Universitas Dehasen Bengkulu

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

Bengkulu, April 2023

Yang Menyatakan,



Nopri Dwipoyono
NPM.16010117

ABSTRAK

PENERAPAN *FIREWALL* PADA SISTEM KEAMANAN JARINGAN KOMPUTER DI SEKOLAH SMK NEGERI 5 SELUMA

Oleh :

Nopri Dwipoyono ¹⁾

Khairil, S.Kom., M.Kom²⁾

Aji Sudarsono, S.Kom., M.Kom²⁾

SMK Negeri 5 Seluma tersebut belum memiliki *firewall*, sehingga keamanan jaringan komputer di sekolah masih sangat minim baik dalam pembatasan akses dalam jaringan. Selain itu Akses internet di SMK Negeri 5 Seluma digunakan oleh guru dan staf untuk mengakses laman internet dengan browsing untuk mendapatkan informasi, namun terdapat beberapa guru dan staf yang mengakses laman sosial media dan laman lainnya yang membuat menurunnya efektifitas kinerja dari guru dan staf tersebut

Penerapan Firewall pada sistem keamanan jaringan komputer di Sekolah SMK Negeri 5 Seluma menggunakan Iptables untuk memonitoring proses lalu lintas paket data dalam jaringan. Dengan iptables, dapat mengatur lalu lintas jaringan dalam server seperti mengizinkan, memblokir atau melewati koneksi masuk dan keluar, mengelola port dan lain sebagainya di Jaringan Komputer Sekolah SMK Negeri 5 Seluma.

Berdasarkan pengujian yang telah dilakukan, maka dapat disimpulkan bahwa penerapan firewall pada sistem keamanan jaringan komputer di SMK Negeri 5 Seluma mampu memblokir serangan ping of death dan juga mampu membuka serta menutup akses beberapa port dalam jaringan dan memblokir situs web facebook.com, instragram.com, dan tokopedia.com

Kata Kunci : *Firewall, Sistem Keamanan, Jaringan Komputer, SMK Negeri 5 Seluma*

1) Calon Sarjana

2) Dosen Pembimbing

ABSTRACT

THE IMPLEMENTATION OF FIREWALL IN COMPUTER NETWORK SECURITY SYSTEM AT SMK NEGERI 5 SELUMA

By:

Nopri Dwipoyono¹⁾

Khairil²⁾

Aji Sudarsono²⁾

SMK Negeri 5 Seluma does not yet have a firewall, therefore computer network security at school is still very minimal, both in terms of limiting access to the network. In addition, internet access at SMK Negeri 5 Seluma is used by teachers and staff to access internet pages by browsing to get information, but there are several teachers and staff who access social media pages and other pages which reduce the effectiveness of the performance of these teachers and staff. Implementation of a Firewall on a computer network security system at SMK Negeri 5 Seluma uses Iptables to monitor packet data traffic processes in the network. With iptables, you can manage network traffic on servers such as allowing, blocking or skipping incoming and outgoing connections, managing ports and so on on the Computer Network at SMK Negeri 5 Seluma School. Based on the tests that have been carried out, it can be concluded that the implementation of a firewall on a computer network security system at SMK Negeri 5 Seluma is able to block ping of death attacks and is also able to open and close access to several ports in the network and block websites facebook.com, instgram.com , and tokopedia.com

Keywords: Firewall, Security System, Computer Network, SMK Negeri 5 Seluma

1) Student

2) Supervisors



KATA PENGANTAR

Puji syukur kepada Allah SWT berkat Rahmat, Hidayah, dan Karunia-Nya kepada kita semua sehingga penulis dapat menyelesaikan skripsi ini dengan judul **Penerapan *Firewall* Pada Sistem Keamanan Jaringan Komputer di Sekolah SMK Negeri 5 Seluma**. Skripsi ini disusun untuk memperoleh Gelar Sarjana Komputer pada Program Studi Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu.

Penulis menyadari dalam penyusunan skripsi ini tidak akan selesai tanpa bantuan dari berbagai pihak. Karena itu pada kesempatan ini penulis ingin mengucapkan terima kasih kepada :

1. Bapak Siswanto, SE, S.Kom., M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas Dehasen Bengkulu.
2. Ibu Liza Yulianti, S.Kom., M.Kom selaku Ketua Program Studi Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu.
3. Bapak Khairil, S.Kom., M.Kom selaku Dosen Pembimbing I yang telah memberikan masukan serta arahan yang sifatnya membangun dalam penulisan skripsi ini
4. Bapak Aji Sudarsono, S.Kom., M.Kom selaku Dosen Pembimbing II yang telah memberikan masukan serta arahan yang sifatnya membangun dalam penulisan skripsi ini.
5. Bapak H. Khairul Mardani. S.Pd selaku Kepala Sekolah SMK Negeri 5 Seluma yang telah memberikan izin untuk melaksanakan penelitian di sekolah
6. Segenap Civitas Akademik Pada Program Studi Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu

Penulis juga menyadari sepenuhnya bahwa di dalam skripsi ini terdapat kekurangan dan jauh dari kata sempurna. Oleh sebab itu, kami berharap adanya kritik, saran dan usulan demi perbaikan skripsi yang telah kami buat di masa yang akan datang, mengingat tidak ada sesuatu yang sempurna tanpa saran yang membangun.

Bengkulu, Juni 2023

Penulis

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
LEMBAR PENGESAHAN	iii
LEMBAR PERSETUJUAN	iv
RIWAYAT HIDUP	v
MOTTO	vi
PERSEMBAHAN.....	vii
ABSTRAK	viii
KATA PENGANTAR.....	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR.....	xiv
DAFTAR LAMPIRAN.....	xvi
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	2
1.3. Batasan Masalah.....	3
1.4. Tujuan Penelitian	3
1.5. Manfaat Penelitian	3
BAB II LANDASAN TEORI	5
2.1. Jaringan Komputer	5
2.2. Topologi Jaringan.....	7
2.3. Wireless Local Area Network	10
2.4. Keamanan Jaringan Komputer	11
2.5. <i>Server</i>	12
2.6. <i>Ubuntu</i>	13
2.7. <i>TCP/IP</i>	16
2.8. <i>Firewall</i>	18
2.9. <i>Iptable</i>	21

2.10. <i>Flowchart</i>	24
BAB III METODOLOGI PENELITIAN	27
3.1. Tinjauan SMK Negeri 5 Seluma	27
3.1.1. Tempat dan Waktu Penelitian	28
3.1.2. Struktur Organisasi	28
3.2. Metode Penelitian	28
3.3. Perangkat Keras dan Perangkat Lunak	30
3.4. Metode Pengumpulan Data	31
3.5. Metode Perancangan Sistem	31
3.5.1. Analisa Sistem Aktual	32
3.5.2. Analisa Sistem Baru	33
3.6. Pengujian Sistem	40
BAB IV HASIL DAN PEMBAHASAN	Error! Bookmark
4.1. Hasil	Error! Bookmark
4.2. Pembahasan	Error! Bookmark
4.3. Pengujian Sistem	Error! Bookmark
BAB V PENUTUP	Error! Bookmark
5.1. Kesimpulan	Error! Bookmark
5.2. Saran	Error! Bookmark

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR TABEL

Tabel	Halaman
2.1. Simbol Flowchart	17
3.1. Pengujian Sistem	30

DAFTAR GAMBAR

Gambar	Halaman
2.1. Topologi Bus	7
2.2. Topologi Ring	9
2.3. Topologi Star	10
2.4. Topologi Star-Bus.....	10
2.5. Topologi Mesh.....	11
2.6. Iptables	13
3.1. Tahapan Metode NDLC	20
3.2. Skema Jaringan Saat Ini Di SMK Negeri 5 Seluma.....	24
3.3. Flowchart	25
3.4. Skema Jaringan Yang Akan Dibangun.....	26

DAFTAR LAMPIRAN

Lampiran

1. Time Schedule
2. Struktur Organisasi
3. Kartu Bimbingan Skripsi
4. Wawancara
5. Data Pendukung

BAB I

PENDAHULUAN

1.1. Latar Belakang

Banyaknya kemudahan yang didapat oleh pengguna internet menyebabkan teknologi tersebut tumbuh dengan sangat cepat. Hampir semua aspek informasi dapat diperoleh melalui internet mulai dari pendidikan, hiburan, olahraga, pemerintahan, sekolah, dan lain-lain. Internet bisa diakses hampir semua kalangan baik anak-anak maupun dewasa untuk mencari informasi.

SMK Negeri 5 Seluma merupakan salah satu Sekolah Menengah Kejuruan Negeri yang terdapat di Kabupaten Seluma. Akses internet di SMK Negeri 5 Seluma menggunakan indihome dengan bandwidth 40mbps dimana pengguna internet diperuntukkan untuk guru, staf dan praktek belajar yang berjumlah kurang lebih 30-40 orang. Indihome terkoneksi dengan komputer dan laptop di lingkungan kerja SMK Negeri 5 Seluma melalui akses LAN dan Wifi.

SMK Negeri 5 Seluma tersebut belum memiliki *firewall*, sehingga keamanan jaringan komputer di sekolah masih sangat minim baik dalam pembatasan akses dalam jaringan. Selain itu Akses internet di SMK Negeri 5 Seluma digunakan oleh guru dan staf untuk mengakses laman internet dengan browsing untuk mendapatkan informasi, namun terdapat beberapa guru dan staf yang mengakses laman sosial media dan laman lainnya yang membuat menurunnya efektifitas kinerja dari guru dan staf tersebut. Dalam proses

praktek belajar mengajar di Laboratorium, baik guru dan siswa dapat mengakses internet pada komputer masing-masing. Namun terkadang, diperlukan pembatasan akses internet pada komputer yang digunakan oleh siswa di Laboratorium untuk membantu siswa agar lebih fokus dalam praktek belajar di Laboratorium, karena terkadang terdapat beberapa siswa yang membuka laman web yang tidak berhubungan dengan pelajaran yang ada di Laboratorium.

Salah satu pelindung yang dibutuhkan untuk mendapatkan akses yang aman ketika berhubungan dengan jaringan komputer, baik dari luar (internet) maupun dari dalam (intranet) dengan cara membuat aturan tertentu pada *firewall*. Salah satu cara *firewall* mengamankan sistem jaringan komputer adalah dengan menerapkan penyaringan *port-port web*. Salah satu aplikasi *firewall* yang memiliki fitur untuk dapat melakukannya yaitu aplikasi *iptables* pada *linux*. Dengan adanya *iptables*, pihak sekolah dapat melakukan penyaringan trafik pada server, mengatur lalu lintas jaringan, termasuk mengizinkan atau memblokir koneksi yang masuk, keluar, atau sekedar melewati *server*.

Oleh karena itu dalam penelitian ini, penulis tertarik untuk mengangkat judul tentang **Penerapan Firewall Pada Sistem Keamanan Jaringan Komputer di Sekolah SMK Negeri 5 Seluma.**

1.2. Rumusan Masalah

Rumusan masalah dalam penelitian ini yaitu bagaimana penerapan *firewall* pada sistem keamanan jaringan komputer di Sekolah SMK Negeri 5 Seluma?

1.3. Batasan Masalah

Adapun batasan masalah pada penelitian ini, antara lain :

- a. *Firewall* yang digunakan yaitu *iptables* dengan sistem operasi *Linux Ubuntu 20.04.5*.
- b. Keamanan jaringan menggunakan *iptables* terkait terhadap 3 aspek yang diamankan yaitu *confidentiality, integrity, dan availability*..

1.4. Tujuan Penelitian

Adapun tujuan dari penelitian ini, antara lain :

- a. Untuk memperoleh Gelar Sarjana Komputer pada Program Studi Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu
- b. Untuk menerapkan *firewall* pada sistem keamanan jaringan komputer di Sekolah SMK Negeri 5 Seluma.

1.5. Manfaat Penelitian

Adapun manfaat dari penelitian yang diperoleh, antara lain :

- a. Bagi SMK Negeri 5 Seluma
 - 1) Dapat membantu mengamankan jaringan komputer yang terdapat di SMK Negeri 5 Seluma dengan membaca lalu lintas jaringan baik yang masuk dan keluar.
 - 2) Dapat membantu *filtering* pada jaringan di sekolah melalui *firewall* menggunakan *iptables*
- b. Bagi Pembaca

Dapat dijadikan bahan referensi dalam memanfaatkan *iptables* sebagai *firewall*.

BAB II

LANDASAN TEORI

2.1. Jaringan Komputer

Jaringan komputer secara istilah adalah kumpulan komputer yang saling berkaitan dan memiliki hubungan komunikasi antar mereka. Hubungan antara komputer memungkinkan terjadinya operasi yang tidak mungkin dilakukan dalam keadaan *stand alone*. Kata kunci dari jaringan komputer adalah komunikasi (Amien & Mukhtar, 2020).

Jaringan komputer merupakan suatu sistem yang terdiri dari komputer-komputer dan perangkat-perangkat jaringan lainnya yang terhubung satu sama lain, bekerja sama untuk mencapai suatu tujuan. Perangkat jaringan sangat penting untuk berlangsungnya hubungan atau komunikasi antar komputer. Informasi berpindah dari komputer ke komputer lainnya dengan menggunakan jaringan daripada melalui perantara manusia, sehingga membuat pertukaran informasi menjadi lebih cepat dan mudah (Simargolang, et al., 2021).

Jaringan komputer adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (service). Pihak yang meminta/menerima layanan disebut klien (client) dan yang memberikan/mengirim layanan disebut peladen (server) (Husen & Surbakti, 2020).

Sebuah jaringan komputer terdiri dari dua atau lebih perangkat komputasi yang terhubung untuk berbagi komponen dari jaringan berupa sumber daya dan informasi yang disimpan jaringan tersebut. Komputer lokal adalah komputer *desktop* yang biasa digunakan, perlu terhubung ke jaringan *workstation* dan server sebagai tempat penyimpanan dan pengendali komputer *client* sehingga setiap *client* dapat berbagi sumber daya, informasi, komunikasi satu sama lainnya. Jika satu jaringan *workstation* terhubung dengan jaringan *workstation* jaringan lainnya akan menjadi jaringan yang lebih besar dan membutuhkan dukungan *hardware* yang baik untuk *firewall* yang lebih kuat (Hendry, 2018).

Adapun potensi jaringan komputer antara lain :

- a. Mengintegrasikan dan berbagai pakai peralatan
- b. Komunikasi, jaringan komputer memungkinkan terjadinya komunikasi antar pemakai komputer.
- c. Perlindungan Data dan Informasi, jaringan komputer dimanfaatkan pula untuk mendistribusikan proses dan aplikasi sehingga dapat mengurangi terjadinya *bottleneck* atau tumpukan pekerjaan pada satu bagian.
- d. Keteraturan Aliran Informasi, jaringan komputer mampu mengalirkan data-data komputer *client* dengan cepat untuk mengintegrasikan dalam komputer server.

Suatu jaringan sering diklasifikasikan berdasarkan wilayah geografis yang dicakup. Adapun klasifikasinya sebagai berikut (Hendry, 2018):

- 1) *Local Area Network* (LAN), merupakan jaringan yang terhubung dalam area yang kecil seperti sebuah ruang kelas. Dari segi biaya LAN hanya

membutuhkan biaya yang murah dikarenakan cakupannya yang kecil, akan tetapi LAN juga sangat cepat untuk diimplementasikan sehingga LAN umumnya dianggap sebagai blok bangunan jaringan untuk menciptakan jaringan yang lebih besar.

- 2) *Metropolitan Area Network* (MAN), merupakan jaringan yang terhubung secara lokal tapi cakupannya lebih luas dibandingkan dengan LAN. MAN sendiri membutuhkan koneksi transfer data yang lebih cepat dibandingkan LAN. Sehingga dibutuhkan harga yang relatif mahal untuk menerapkan jaringan MAN ini dikarenakan dibutuhkan serat optik (FO) untuk mengimplementasikannya.
- 3) *Wide Area Network* (WAN), WAN perkembangan dari jaringan MAN, sehingga cakupan yang luas membutuhkan koneksi jarak jauh dan adanya perluasan jaringan terjadi peningkatan biaya jaringan. Sehingga WAN dibutuhkan untuk jaringan yang sangat luas untuk berkomunikasi satu sama lain.

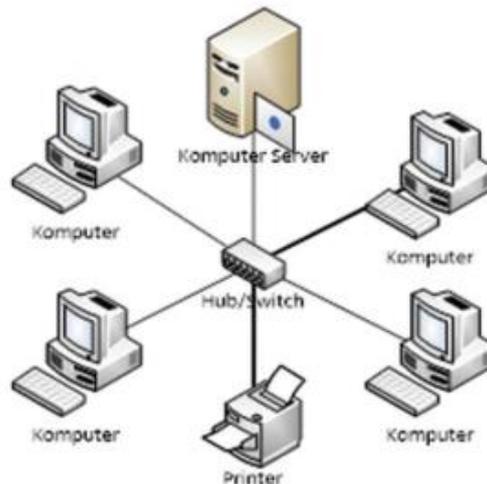
Adapun klasifikasi jaringan berdasarkan tipe jaringannya, antara lain :

- 1) Jaringan *peer to peer*, merupakan jaringan yang dianggap sama kedudukannya rekan satu sama lain.
- 2) Jaringan berbasis *server*, tidak seperti *peer to peer* yang beroperasi tanpa kontrol pusat dan sulit mengamankan jaringannya

2.2. Topologi Jaringan

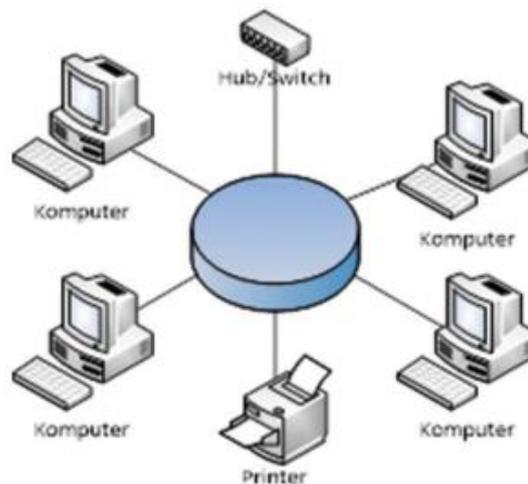
Topologi jaringan adalah hubungan geometris antara unsur-unsur dasar penyusun jaringan, yaitu *node*, *link*, dan *station*. Topologi jaringan dapat dibagi menjadi 5 kategori utama yaitu (Husen & Surbakti, 2020) :

1. Topologi *star* (bintang) merupakan bentuk topologi yang berupa konvergensi dari *node* tengah ke setiap *node* atau pengguna. Topologi jaringan bintang termasuk topologi jaringan dengan biaya menengah.



Gambar 2.1. Topologi Star

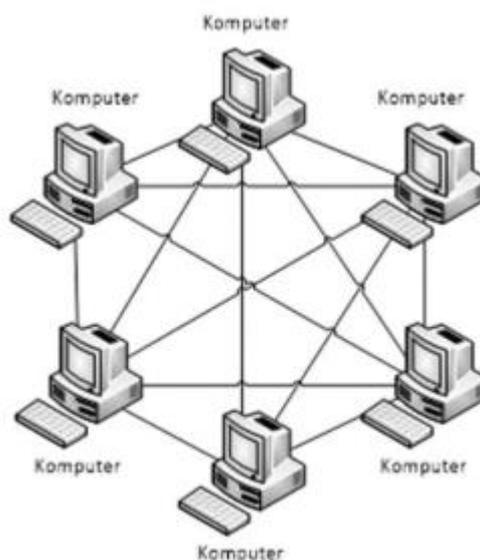
2. Topologi *ring* (cincin) adalah topologi jaringan berbentuk rangkaian titik yang masing-masing terhubung ke dua titik lainnya, sedemikian sehingga membentuk jalur melingkar seperti cincin.



Gambar 2.2. Topologi Ring

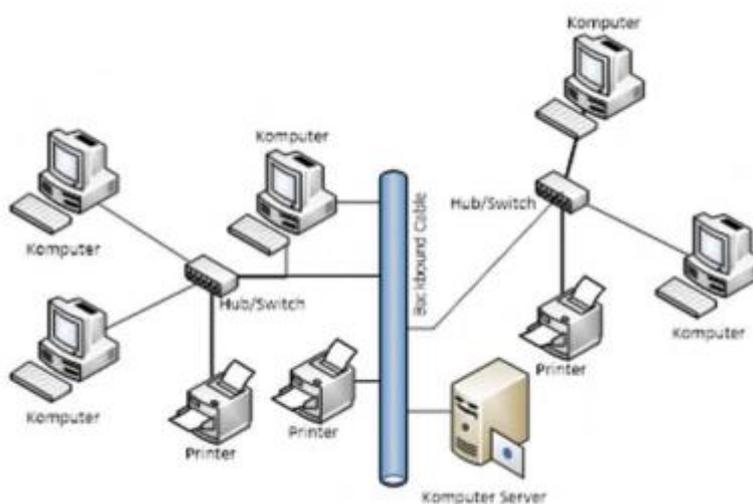
3. Topologi *mesh* (jala) adalah suatu bentuk hubungan antar perangkat dimana setiap perangkat terhubung secara langsung ke perangkat lainnya yang ada

di dalam jaringan. Akibatnya, dalam topologi *mesh* setiap perangkat dapat berkomunikasi langsung dengan perangkat yang dituju (*dedicated links*)



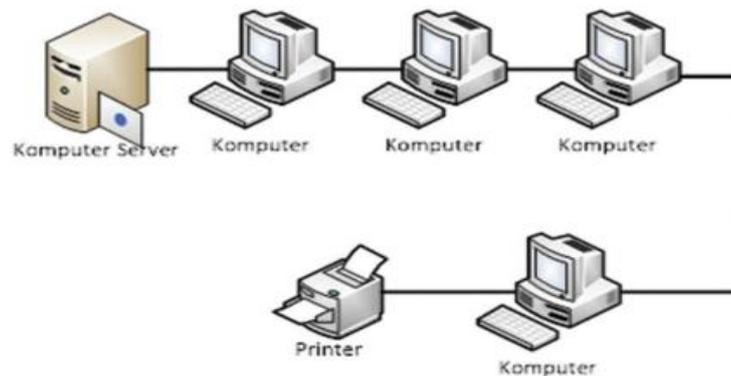
Gambar 2.3. Topologi Mesh

4. Topologi *tree* (pohon) adalah kombinasi karakteristik antara topologi bintang dan topologi bus. Topologi ini terdiri atas kumpulan topologi bintang yang dihubungkan dalam satu topologi bus sebagai jalur tulang punggung atau *backbone*. Komputer-komputer dihubungkan ke *hub*, sedangkan *hub* lain dihubungkan sebagai jalur tulang punggung.



Gambar 2.4. Topologi Tree

5. Topologi linear (beruntut) biasa disebut dengan topologi bus beruntut, tata letak ini termasuk tata letak umum. Satu kabel utama menghubungkan tiap titik sambungan (komputer) yang dihubungkan dengan penyambung yang disebut dengan penyambung -T dan pada ujungnya harus diakhiri dengan sebuah penamat (*terminator*). Penyambung yang digunakan berjenis BNC (*British Naval Connector*), sedangkan kabel yang digunakan adalah RG58. Pemasangan dari topologi bus beruntut ini sangat sederhana dan murah tetapi hanya dapat terdiri dari 5-17 komputer.



Gambar 2.5. Topologi Linear

2.3. Wireless Local Area Network

Wireless LAN (WLAN) merupakan teknologi LAN yang menggunakan frekuensi dan transmisi radio sebagai media penghantarnya, pada area tertentu menggantikan fungsi kabel. Konfigurasi jaringan WLAN adalah terdiri dari akses point yang dihubungkan ke pengguna melalui media udara (frekuensi dan transmisi radio) (Harun, 2019).

WLAN atau Wireless Local Area Network merupakan salah satu jaringan komputer bersifat lokal yang memanfaatkan gelombang radio sebagai media transmisi data. Informasi data elektronik ditransfer dari satu komputer ke komputer lain melalui gelombang radio

Setiap Network WLAN memerlukan wireless access point (AP) untuk mentransmisikan dan menerima data dari pengguna. Tidak seperti netowrk wired yang beroperasi pada full duplex (pengiriman dan penerimaan pada waktu yang bersamaan), wireless network beroperasi pada full duplex, jadi terkadang AP juga bisa diartikan sebagai wireless hub. Perbedaan terbesar antara wired Lan dan WLAN adalah WLAN mentransmisikan data dengan radiasi gelombang energi, dinamakan gelombang radio, sedangkan wired LAN mentransmisikan sinyal elektrik melalui kabel (Adhiatma, 2020).

Berdasarkan IEEE Standard, jarak jangkauan wifi yang menggunakan standard 802.11, seperti Tabel 2.1..

Tabel 2.1. 802.11 Wireless Standards

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 Ghz	2,4 Ghz	2,4 Ghz	2,4/5 Ghz	5 Ghz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors	100 ft (30,48 meter)	100 ft (30,48 meter)	125 ft (38,1 meter)	225 ft (68,58 meter)	90 ft (27,432 meter)
Typical Range Outdoors	400 ft (121,92 meter)	450 ft (137,16 meter)	450 ft (137,16 meter)	825 ft (251,46 meter)	1000 ft (304,8 meter)

Sumber : <https://wirelessdmx.com/wp-content/uploads/2016/07/802.11-Wireless-Standards.png>

2.4. Keamanan Jaringan Komputer

Keamanan Jaringan dapat diartikan sebagai keadaan aman pada suatu susunan yang menjalankan sistem komputer. Keamanan jaringan juga dapat diartikan sebagai proses untuk mengidentifikasi dan mencegah adanya *user* yang tidak mempunyai izin (penyusup) dari sistem jaringan komputer. Tujuan

dibangunnya suatu sistem keamanan jaringan adalah untuk menanggulangi dan mencegah ancaman dari jaringan luar yang dapat berupa ancaman logik atau fisik. Ancaman logik adalah sebuah ancaman yang berupa pengambilan data secara tidak sah atau pencurian data oleh penyusup dengan cara mencari celah yang terbuka pada sistem keamanan jaringan, sedangkan ancaman fisik yaitu sebuah ancaman yang bertujuan untuk merusak sistem jaringan dari sisi *hardware* sebuah komputer (Anggraini, 2018).

Keamanan jaringan dalam aspek keamanan mempunyai 5 aspek yang dijelaskan sebagai berikut :

- 1) *Confidentiality* yaitu mengharuskan suatu data hanya bisa diakses oleh pengguna yang sah atau memiliki izin akses.
- 2) *Integrity* yaitu mengharuskan suatu data hanya bisa diubah oleh pengguna yang sah atau memiliki izin wewenang.
- 3) *Availability* yaitu mengharuskan informasi hanya tersedia bagi pengguna yang sah atau memiliki izin akses untuk kebutuhan tersebut.
- 4) *Authentication* yaitu mengharuskan penerima atau pengirim suatu data dapat dibuktikan dengan identitas yang asli dan tidak palsu yang dapat diidentifikasi.
- 5) *Nonrepudiation* yaitu mengharuskan penerima atau pengirim suatu data tidak dapat menolak adanya pengiriman dan penerimaan pesan.

2.5. *Server*

Server adalah sebuah sistem komputer yang menyediakan jenis layanan (*service*) tertentu dalam sebuah jaringan komputer. *Server* juga menjalankan perangkat lunak administratif yang mengontrol akses terhadap

jaringan dan sumber daya yang terdapat di dalamnya, seperti halnya berkas atau alat pencetak (printer) dan memberikan akses kepada *client* anggota jaringan (Husen & Surbakti, 2020).

Sebuah *server* memiliki beberapa fungsi penting, diantaranya sebagai berikut :

- 1) Melayani dan bertanggungjawab penuh terhadap permintaan data dari komputer klien
- 2) Menyediakan berbagai macam *resource* untuk dapat digunakan semua komputer klien yang masuk dalam jaringan, baik itu berupa perangkat keras maupun perangkat lunak/aplikasi
- 3) Bertanggungjawab dalam mengatur lalu lintas data
- 4) Menyimpan berbagai *file* dan data untuk dapat diakses bersama-sama menggunakan protokol FTP
- 5) Mengatur hak akses (*permissions*) ke dalam sebuah jaringan, sehingga tidak semua klien mampu mengakses data yang terdapat dalam komputer *server*
- 6) Menyediakan aplikasi dan *database* yang mampu dijalankan di semua *komptuer* klien
- 7) Memberikan perlindungan untuk komputer klien dengan pemasangan *firewall* atau anti *malware* di komputer klien.

2.6. *Ubuntu*

Ubuntu adalah salah satu distribusi *linux* yang berbasiskan *debian* dan didistribusikan menjadi perangkat lunak sistem operasi yang bebas. *Ubuntu* adalah proyek yang disponsori perusahaan Canonical LTD yang berasal dari

Afrika Selatan. *ubuntu* adalah sejenis sistem operasi yang berbasis *linux* *debian* (Husen & Surbakti, 2020).

Ubuntu adalah bagian daripada distribusi *linux* yang berbasis *Debian GNU/Linux* dan memiliki *interface desktop*. *Ubuntu* adalah sepenuhnya sistem operasi *opensource* 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. *Ubuntu* adalah sistem operasi lengkap berbasis *linux*, tersedia secara bebas dan mempunyai dukungan baik yang berasal dari komunitas maupun ahli tenaga profesional. sistem operasi tersebut memiliki berbagai kelebihan distribusi *debian* diantaranya adalah pemaketan (*packaging*), pemilihan aplikasi yang luas (*application choice*), siklus pembaharuan dilakukan secara rutin (*updates*), dikenal stabilitas dan kualitasnya terutama di sisi server (*stability and quality*) (Hanafi & Habibi, 2020).

Adapun tampilan sistem operasi *linux ubuntu* seperti Gambar 2.6.



Gambar 2.6. Tampilan Sistem Operasi *Linux Ubuntu*

Arsitektur keamanan pada *Linux* memiliki 6 komponen, diantaranya sebagai berikut (Hanafi & Habibi, 2020) :

1) Akun Pemakai (*User Account*)

Root memiliki wewenang dalam mengadministrasi sistem secara keseluruhan. *Root* dapat mengontrol sistem *file*, pengguna, sumber daya, bahkan akses jaringan. Jika ada satu pengguna yang melanggar aturan, *root* bisa membuat akunnya beku, tanpa mengganggu yang lain. *Root* juga dapat mengatur siapa saja yang dapat mengakses suatu *file*, memberikan hak khusus pada pengguna tertentu.

2) Kontrol akses secara diskresi (*Discretionary Access Control*)

Setiap pemakai *linux* memiliki akun tersendiri yang dimana masing-masing akun tersebut dibedakan dengan *username* dan *password*. Setiap *file* memiliki atribut kepemilikan, grup, dan pengguna umum. Satu *file*, bisa diberikan atribut tertentu, sehingga hanya dapat dibaca atau dieksekusi oleh pemiliknya saja. Pembatasan ketat ini dinamakan *Discretionary Access Control* yang menyebabkan virus jarang ditemui atau jarang tersebar di *linux*.

3) Kontrol Akses Jaringan (*Network Access Control*)

Network Access Control merupakan pembatasan antar jaringan yang akan dimasuki ke dalam *linux*. *Linux* dapat memilih *host* yang berhak/tidak berhak mengaksesnya dengan menggunakan alat pengontrolan akses antar jaringan. Alat pengontrolan akses ini dinamakan *firewall*

4) Enkripsi (*Encryption*)

Enkripsi merupakan suatu metode yang digunakan untuk melakukan pengkodean pada suatu data sehingga data tersebut tidak bisa dibaca sembarangan dan bila data tersebut ingin dibaca harus didekripsi.

5) *Logging*

Logging merupakan prosedur dari sistem operasi atau aplikasi dimana prosedur tersebut merekam setiap kejadian dan menyimpan rekaman tersebut untuk dapat dianalisa. Rekaman tersebut berupa kapan pengguna *login* dari sistem, rekaman pesan *error*, rekaman informasi *login*, dan rekaman kejadian pada *kernel*

6) Deteksi Penyusupan (*Intrusion Detection*)

Sistem keamanan *linux* dapat mendeteksi penyusupan data. Aktivitas mendeteksi penyusupan secara cepat dengan menggunakan program khusus secara otomatis yang disebut *Intrusion Detection System*

2.7. *TCP/IP*

TCP/IP (singkatan dari *Transmission Control Protocol/Internet Protocol*) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (*protocol suite*). Protokol ini juga merupakan protokol yang paling banyak digunakan saat ini. Data tersebut diimplementasikan dalam bentuk perangkat lunak (*software*) di sistem operasi. Protokol ini juga bersifat *routable* yang berarti protokol ini cocok untuk menghubungkan sistem-sistem berbeda (seperti Microsoft Windows dan keluarga *UNIX*) untuk membentuk jaringan yang heterogen. Dalam *TCP/IP* terdapat 5 layer yang akan dijelaskan berikut. *Physical Layer* (lapisan fisik) merupakan lapisan terbawah yang mendefinisikan besaran fisik seperti media komunikasi, tegangan, arus, dan sebagainya. Lapisan ini dapat bervariasi

bergantung pada media komunikasi pada jaringan yang bersangkutan. Network Access Layer mempunyai fungsi yang mirip dengan Data Link layer pada OSI. Lapisan ini mengatur penyaluran data *frame-frame* data pada media fisik yang digunakan. Lapisan ini biasanya memberikan servis untuk deteksi dan koreksi kesalahan dari data yang ditransmisikan (Sondakh, et al., 2014).

Beberapa contoh protokol yang digunakan pada lapisan ini adalah X.25 jaringan publik, *Ethernet* untuk jaringan *Ethernet*, AX.25 untuk jaringan Paket Radio. Internet Layer mendefinisikan bagaimana hubungan dapat terjadi antara dua pihak yang berada pada jaringan yang berbeda seperti *Network Layer* pada OSI. Pada jaringan Internet yang terdiri atas puluhan juta *host* dan ratusan ribu jaringan lokal, lapisan ini bertugas untuk menjamin agar suatu paket yang dikirimkan dapat menemukan tujuannya di mana pun berada. *Transport Layer* mendefinisikan cara-cara untuk melakukan pengiriman data antara *end to end host*. Lapisan ini menjamin bahwa informasi yang diterima pada sisi penerima adalah sama dengan informasi yang dikirimkan pada pengirim. *Application Layer* merupakan lapisan terakhir dalam arsitektur *TCP/IP* yang berfungsi mendefinisikan aplikasi-aplikasi yang dijalankan pada jaringan. Karena itu, terdapat banyak protokol pada lapisan ini, sesuai dengan banyaknya aplikasi *TCP/IP* yang dapat dijalankan. Contohnya adalah *SMTP* (*Simple Mail Transfer Protocol*) untuk pengiriman *e-mail*, *FTP* (*File Transfer Protocol*) untuk transfer *file*, *HTTP* (*Hyper Text Transfer Protocol*) untuk aplikasi web, *NNTP* (*Network News Transfer Protocol*) untuk distribusi *news group* dan lain-lain. Setiap aplikasi pada umumnya menggunakan *protocol*

TCP dan *IP*, sehingga keseluruhan keluarga protokol ini dinamai dengan *TCP/IP*.

2.8. *Firewall*

Firewall adalah perangkat keamanan jaringan berbasis perangkat keras atau perangkat lunak yang memantau lalu lintas jaringan masuk dan keluar dan mengizinkan atau memblokir paket data berdasarkan seperangkat aturan keamanan. Tujuannya adalah untuk membuat penghalang antara jaringan internal dan lalu lintas masuk dari sumber eksternal (seperti internet). *Firewall* memonitor setiap paket yang lewat, mempertimbangkan sumbernya, tujuan, dan jenis data yang dikandungnya, dan membandingkan informasi tersebut dengan seperangkat aturan internal (Sastradipraja & Segar, 2022).

Secara umum terdapat 2 jenis *firewall* berdasarkan lokasi dimana *firewall* tersebut bekerja yaitu (Sahal, 2018) :

1. *Personal Firewall*

Firewall yang didesain untuk melindungi komputer saat komputer terhubung ke internet. Ada beberapa fitur pada *personal firewall* ini seperti proteksi terhadap virus, *anti-spam*, *anti-malware* dan *anti-spyware*. Contoh dari *firewall* jenis ini adalah *iptables* sistem berbasis *Linux* dan *Windows Firewall with Advanced Security (WFAS)* pada sistem berbasis *Windows*.

2. *Network Firewall*

Firewall yang didesain untuk melindungi secara keseluruhan jaringan komputer dari berbagai serangan, biasanya jenis *firewall* ini digunakan oleh perusahaan-perusahaan. Terdapat 2 bentuk pada *firewall* ini, yaitu perangkat yang terdedikasi dan perangkat yang di-*install* pada sebuah

server. Network *firewall* ini juga memiliki fitur yang dimiliki oleh personal *firewall* ditambah dengan beberapa fitur lainnya yaitu *circuit level gateway*, *application level gateway* dan juga *NAT gateway*. Network *firewall* umumnya menggunakan teknologi *routing* untuk menentukan paket yang akan diizinkan atau ditolak. Contoh dari Network *Firewall* ini adalah *Cisco ASA*, *Checkpoint Firewall*, *Palo Alto Firewall*, dan lain-lain.

Sedangkan tipe-tipe *firewall* berdasarkan apa yang akan dilakukan terhadap paket data yang melewati jaringan adalah (Sahal, 2018) :

1. *Packet Filtering Firewall*

Tipe *firewall* yang memeriksa dan membandingkan alamat sumber dari paket lewat dengan aturan atau kebijakan yang telah terdaftar pada *filtering firewall*. Pada *firewall* tipe ini akan diatur apakah paket data tersebut akan diperbolehkan lewat atau menolaknya.

2. *Application Level Gateway (Proxy)*

Firewall ini tidak memperbolehkan paket data yang datang untuk melewati *firewall* secara langsung. *Application level gateway* menyediakan kontrol tingkat tinggi pada *traffic* antara dua jaringan yang isi layanan tertentu didalamnya dapat dimonitor dan di filter sesuai dengan kebijakan keamanan jaringan.

3. *Circuit Level Gateway*

Circuit level gateway mengatasi koneksi *TCP* dan tidak menyediakan paket tambahan seperti *processing* atau *filtering*. *Firewall* jenis ini akan menyembunyikan jaringan dari pengguna ketika koneksi akan terjadi dari pengguna. Pengguna akan berhadapan langsung dengan *firewall* pada saat

di jaringan yang hendak di akses oleh pengguna setelah mengubah alamat *IP* dari paket yang ditransmisikan oleh dua belah pihak.

4. *NAT Gateway*

Fitur ini secara otomatis menyediakan proteksi terhadap sistem yang berada di balik *firewall* karena *NAT firewall* hanya mengizinkan koneksi yang datang dari komputer-komputer yang berada di balik *firewall*.

Terdapat 4 jenis arsitektur *firewall* yang sering digunakan untuk membangun jaringan, yaitu (Sahal, 2018) :

1. Arsitektur *firewall* dengan *dial-up*,

Merupakan model *firewall* yang sering digunakan jaringan lokal yang terhubung dengan internet dengan menggunakan piranti modem sebagai *dial-up*.

2. Arsitektur *firewall single router*.

Pada arsitektur ini, koneksi internet terhubung langsung ke sebuah *router* melalui *interface* dan diteruskan ke jaringan lokal pada *interface* lainnya. Sistem *firewall* langsung ditempatkan di bawah *router* ini. Arsitektur dengan *proxy server*.

Pada model arsitektur ini, selain menjadi *gateway*, *router* juga di *install* dan diset menjadi *proxy server* yang memfilter setiap paket data yang keluar masuk, serta *firewall* yang terintegrasi dengan proses *routing* ini juga melakukan filterasi setiap *request* data menuju layanan protokol *http* atau *https* pada *port* tertentu

3. Arsitektur *firewall* kompleks

Pada model arsitektur ini, jenis *firewall* yang dipasang tidak hanya berfungsi sebagai *hardware*, tetapi juga berfungsi sebagai pintu masuk dan penyaring data menuju mesin lainnya.

2.9. *Iptable*

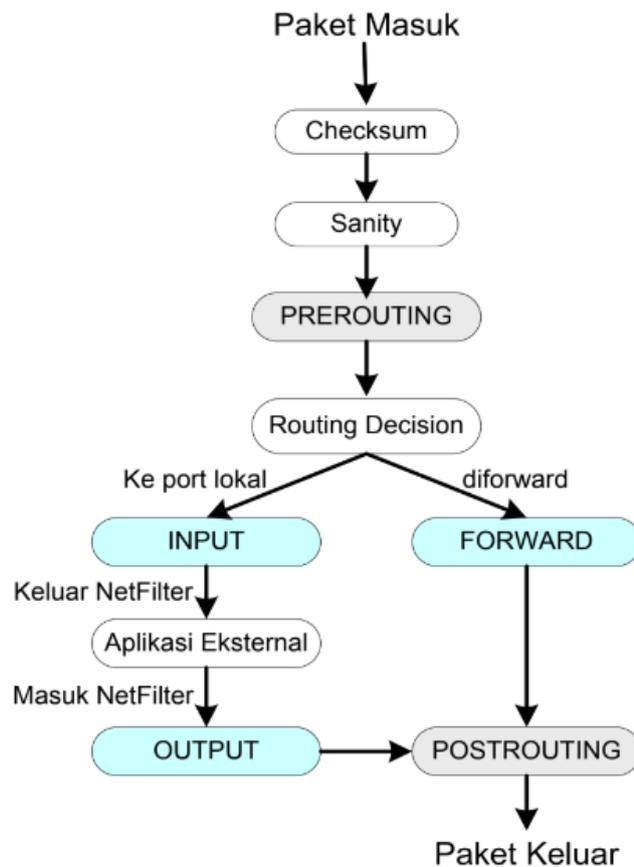
Iptables adalah *firewall* yang secara *default* di *install* pada semua distribusi *linux*, seperti *Ubuntu*, *Fedora* dan lainnya. Pada saat melakukan instalasi pada *linux*, *iptables* sudah langsung ter-*install*, tetapi pada umumnya *iptables* mengizinkan semua *traffic* untuk lewat. *Iptables* adalah suatu *tools* dalam sistem operasi *linux* yang berfungsi sebagai alat untuk melakukan filter (penyaringan) terhadap lalu lintas data. Secara sederhana digambarkan sebagai pengatur lalu lintas data. Dengan *iptables* inilah kita akan mengatur semua lalu lintas dalam komputer, baik yang masuk ke komputer, keluar dari komputer, ataupun *traffic* yang sekedar melewati komputer (Santoso, 2017).

Program *iptables* adalah modul di *linux* yang memberikan dukungan langsung terhadap *kernel linux* mulai versi 2.4 untuk keamanan sistem serta beberapa keperluan jaringan lainnya. Paket *iptables* dapat digunakan untuk melakukan seleksi terhadap paket-paket yang datang baik *input*, *output* maupun *forward* berdasarkan *IP address*, identitas jaringan, nomor *port*, *source* (asal), *destination* (tujuan), protokol yang digunakan bahkan berdasarkan tipe koneksi terhadap setiap paket (data) yang diinginkan. *Software iptabel* dapat melakukan kalkulasi terhadap paket dan menerapkan prioritas *traffic* berdasar jenis layanan (*service*). *Tool iptables* dapat digunakan untuk mendefinisikan sekumpulan aturan keamanan berbasis *port* untuk mengamankan *host-host* tertentu. *Tool* ini

juga dapat dimanfaatkan untuk membangun *router* atau *gateway*, tentunya hanya dengan menggunakan sistem operasi *linux* (Husni, 2020).

Paket yang masuk diperiksa apakah rusak, *mal-information* atau tidak, kemudian diberikan ke *chain input*. Tergantung pada informasi yang terdapat di dalam *header* paket dan kebijakan dalam *ruleset*, keputusan yang diambil untuk suatu paket dapat berupa :

- 1) *Accept*, artinya menerima paket dan diproses lebih lanjut oleh *kernel*
- 2) *Drop*, artinya menolak paket tanpa pemberitahuan sama sekali
- 3) *Reject*, artinya mengembalikan paket ke asalnya dengan pesan kesalahan *ICMP*
- 4) *Log*, artinya melakukan log (pencatatan) terhadap paket yang bersesuaian
- 5) *Return*, artinya jika paket berasal dari *chain user-defined* akan dikembalikan ke *chain* yang memanggil sedangkan untuk *chain input*, *output* dan *forward* akan dijalankan kebijakan *default*.
- 6) Mengirimnya ke *chain user-defined*



Gambar 2.6. Perjalanan Paket Di Dalam *Firewall IPtables*

Keterangan Gambar 2.6. antara lain :

- 1) *Checksum* yaitu pemeriksaan untuk memastikan paket yang diterima tidak rusak (*corrupt*). Jika paket *corrupt* maka langsung ditolak (drop)
- 2) *Sanity* yaitu paket-paket yang *malformed* akan di drop
- 3) *Chain input*, yaitu *chain firewall* pertama yang menguji paket-paket yang masuk. Jika paket tidak di drop atau di *reject* oleh *rule* pada *chain input* maka paket diteruskan
- 4) *Deamsquerade*, yaitu proses yang dilakukan sebelum paket melompat ke *chain output*. Saat suatu paket datang dari jaringan eksternal (merupakan jawaban dari paket yang menuju jaringan eksternal yang di *masquerade*)

maka paket tersebut harus di *demasquerade* dan melompat ke *chain output*.

- 5) *Routing decision*, yaitu bagian tujuan suatu paket diuji untuk menentukan apakah paket akan menuju *local process* atau ke *chain forward*
- 6) *Local process*, yaitu suatu proses yang berjalan pada mesin *firewall*. Proses tersebut dapat menerima dan mengirim suatu paket ke *chain output*.
- 7) *Lo interface*, yaitu suatu proses dimana paket dikirim dari suatu proses lokal ke proses lokal lain melalui sistem *interface loopback (lo)*
- 8) *Chain forward*, yaitu *chain* yang berisi rule-rule untuk mengarahkan paket-paket yang tidak di *masquerade* yang dialamatkan ke mesin lain
- 9) *Chain output* yaitu *chain* yang berisi rule-rule untuk mengarahkan paket-paket ke jaringan eksternal.

2.10. Flowchart

Flowchart adalah representasi secara simbolik dari suatu algoritma atau prosedur untuk menyelesaikan suatu masalah, dengan menggunakan *flowchart* akan memudahkan pengguna melakukan pengecekan bagian-bagian yang terlupakan dalam analisis masalah, di samping itu *flowchart* juga berguna sebagai fasilitas untuk berkomunikasi antara pemrogram yang bekerja dalam tim suatu proyek. *Flowchart* membantu memahami urutan-urutan logika yang rumit dan panjang. *Flowchart* membantu mengkomunikasikan jalannya program ke orang lain (bukan pemrogram) akan lebih mudah (Santoso & Nurmalina, 2017).

Flowchart adalah dalam bahasa Indonesia diagram alir, merupakan diagram yang memuat simbol-simbol grafis yang menyatakan aliran algoritma

atau proses dari langkah-langkah instruksi dalam bentuk-bentuk kotak persegi dan bulat dan pernyataan instruksi, dimana hubungan dan urutan proses tiap instruksi ditunjukkan dengan simbol tanda panah (Anggrawan, 2018)

Flowchart adalah bagan-bagan yang mempunyai arus menggambarkan langkah-langkah penyelesaian suatu masalah merupakan cara penyajian dari suatu algoritma. Ada 2 (dua) macam *flowchart* :

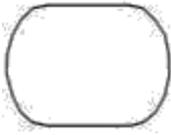
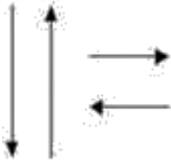
a. *System Flowchart*

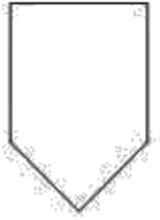
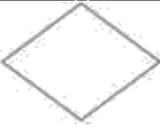
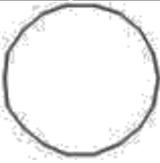
Urutan proses dalam sistem dengan menunjukkan alat media *input*, *output* serta jenis penyimpanan dalam proses pengolahan data.

b. *Program Flowchart*

Urutan instruksi yang digambarkan dengan simbol tertentu untuk memecahkan masalah dalam suatu program.

Tabel 2.1. Simbol *Flowchart*

Simbol	Keterangan	Penjelasan
	Simbol <i>Terminator</i> (simbol <i>start</i> dan <i>end</i>)	Simbol untuk tanda mulai (<i>start</i>) dan tanda selesai (<i>stop/end</i>) dari kegiatan proses
	Simbol Arah Aliran	Simbol yang menghubungkan antara simbol yang satu dengan simbol lainnya (atau antara kegiatan proses) dan sekaligus menyatakan arah proses
	Simbol keluaran/masukan (<i>Input/output</i>)	Simbol yang menyatakan proses <i>input</i> dan <i>output</i> (berlaku untuk semua media <i>input</i> dan <i>output</i>)
	Simbol Proses	Simbol yang melambangkan kegiatan pemrosesan/pengolahan

		<i>input</i>
	Simbol Konektor	Simbol untuk tanda penyambungan proses pada lembar atau halaman yang berbeda.
	Simbol Percabangan atau Pilihan Keputusan	Simbol proses pemilihan keputusan tergantung kondisi, jika pemeriksaan kondisi terpenuhi benar maka jalur pilihan yang diproses adalah jalur ya atau <i>yes</i> , dan sebaliknya jika pemeriksaan tidak terpenuhi tidak benar, maka jalur tidak atau <i>No</i> .
	Simbol Konektor	simbol untuk tanda penyambungan proses pada lembar atau halaman yang sama

BAB III

METODOLOGI PENELITIAN

3.1. Tinjauan SMK Negeri 5 Seluma

SMK Negeri 5 Seluma beralamat di jalan Desa Telaten Semidang Alas Kabupaten Seluma yang berdiri pada Tanggal 13 Juli 2014 Sesuai dengan Keputusan Bupati Seluma No.527 Tahun 2014 dengan luas tanah 6965M2 berakreditasi B tentang Pendirian Sekolah Menengah Kejuruan (SMK) Jumlah Siswa Pertama 45 siswa Jurusan TKJ (Teknik Komputer Jaringan). Pada Tahun 2016 menambah jurusan akuntansi. Pada Tahun 2019 menambah lagi jurusan TBSM (Teknik dan Bisnis Sepeda Motor). Pada saat ini jumlah siswa sebanyak 313 siswa dengan 3 jurusan TKJ, Akuntansi dan TBSM.

Visi Sekolah yaitu menciptakan sumber daya manusia unggul dalam prestasi, mandiri, cerdas, kreatif, terampil dan berkeahlian dalam bidangnya, beriman dan bertaqwa kepada Tuhan Yang Maha Esa.

Misi Sekolah, antara lain :

- a. Melaksanakan bimbingan dan pembelajaran secara efektif menumbuhkembangkan kepribadian mandiri, kreatif, inovatif secara optimal sesuai dengan bakat dan minat yang dimiliki siswa
- b. Menumbuhkan semangat belajar yang kuat, disiplin dalam upaya mencapai sumber daya unggul dalam prestasi
- c. Menumbuhkembangkan semangat kewirausahaan yang berkemampuan menghadapi dan melihat peluang usaha dimasa depan

- d. Melakukan pelatihan dan keterampilan yang berkeahlian dalam bidangnya dalam upaya mencapai sumber daya yang mandiri dan siap memasuki lapangan pekerjaan.
- e. Menerapkan manajemen partisipatif dengan melibatkan seluruh warga sekolah, lingkungan sekolah dan kelompok yang terkait dengan sekolah.

3.1.1. Tempat dan Waktu Penelitian

Tempat penelitian ini akan dilaksanakan di SMK Negeri 5 Seluma yang beralamat di Jalan Telatan Kecamatan Semidang Alas Kabupaten Seluma Provinsi Bengkulu. Dan waktu penelitian dimulai pada Bulan Oktober 2022 sampai dengan Maret 2023.

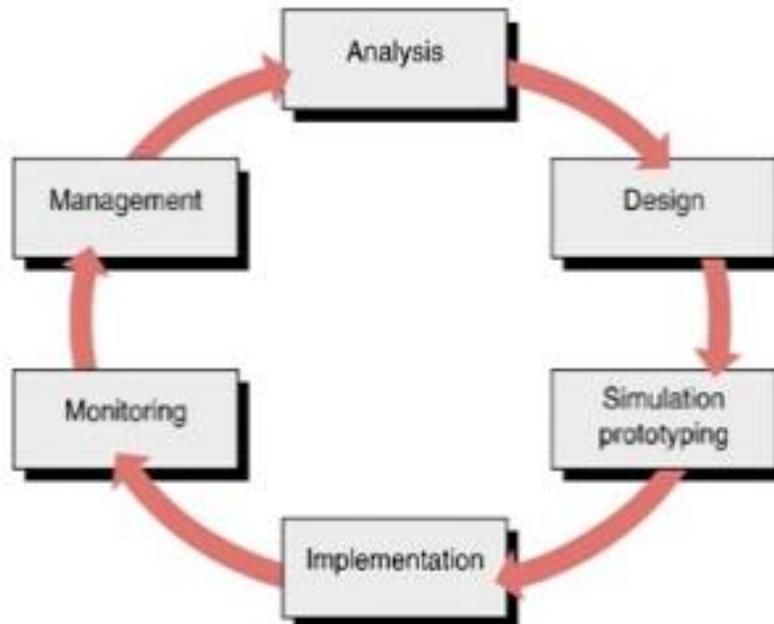
3.1.2. Struktur Organisasi

Adapun struktur organisasi SMK Negeri 5 Seluma dapat dilihat di lampiran.

3.2. Metode Penelitian

Dalam melaksanakan penelitian ini, penulis menggunakan metode *Network Development Life Cycle* (NDLC) yang merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, daur hidup pengembangan aplikasi, dan analisis pendistribusian data.

Adapun tahapan yang dilakukan dalam NDLC terdiri dari *Analysis, Design, Simulation Prototyping, Implementation, Monitoring, dan Management*, seperti terlihat pada Gambar 3.1.



Gambar 3.1. 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.

2. *Design*

Membuat gambaran desain topologi jaringan yang akan dibangun sesuai dengan analisa kebutuhan yang telah dilakukan.

3. *Simulation Prototype*

Tahap dimana dilakukan simulasi dengan bantuan *tools* khusus di bidang jaringan yang digunakan untuk melihat kinerja awal jaringan yang akan dibangun.

4. *Implementation*

Tahap dimana akan dilakukan penerapan rancangan yang telah dibuat agar dapat diuji di lapangan agar dapat menyelesaikan masalah teknik dan non teknis.

5. *Monitoring*

Tahap dimana dilakukan pengamatan terhadap infrastruktur perangkat keras, dan memperhatikan jalannya iptable pada sistem operasi linux ubuntu di dalam jaringan yang telah dibangun

6. *Management*

Tahap dimana menentukan kebijakan untuk membuat/mengatur agar sistem yang telah dibangun dapat berjalan dengan baik dan berlangsung lama.

3.3. Perangkat Keras dan Perangkat Lunak

1. Perangkat Keras (*Hardware*)

Adapun spesifikasi perangkat keras (*Hardware*), antara lain :

a. Laptop 1

- 1) Processor Intel(R) Core(TM) i3 CPU M330 @2.13Ghz
- 2) Ram 8GB
- 3) Hdd 500GB

b. Laptop 2

- 1) Processor Intel(R) atom(TM) CPU N2600 @1.60GHz
- 2) Ram 2GB
- 3) Hdd 320GB

c. Laptop Server

- 1) Processor Amd A8-6410 APU With AMD Radeon R5 Graphics
- 2) Ram 4GB

- 3) Hdd 500GB
2. Perangkat Lunak (*Software*)
 - a. Sistem Operasi Linux Debian dan Windows
 - b. Microsoft Visio

3.4. Metode Pengumpulan Data

Metode pengumpulan data digunakan untuk memperoleh data yang dapat mendukung permasalahan yang akan dibahas. Metode pengumpulan data yang digunakan dalam penelitian ini, antara lain :

- a. Observasi

Tahap ini, penulis melakukan observasi dengan cara mengamati sistem jaringan yang sudah ada di SMK Negeri 5 Seluma.

- b. Wawancara

Tahap ini, penulis melakukan wawancara dengan memberikan pertanyaan-pertanyaan yang terkait dengan masalah penelitian kepada Ibu Wiwi Novitasari, S.Kom selaku Kepala Lab Komputer di SMK Negeri 5 Seluma (data terlampir).

- c. Studi Pustaka

Tahap ini, penulis mengumpulkan beberapa literatur yang berkaitan dengan penelitian yang didapatkan berupa artikel, jurnal (dari internet) dan buku (dari perpustakaan).

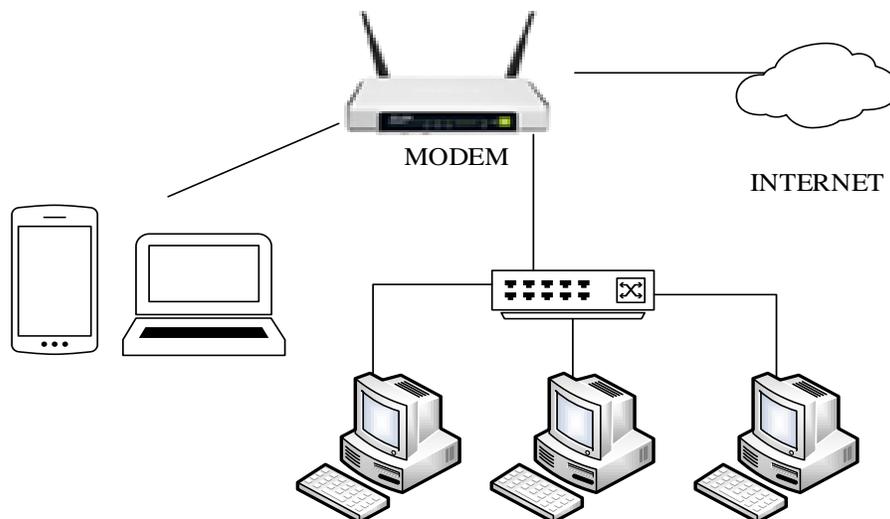
3.5. Metode Perancangan Sistem

3.5.1. Analisa Sistem Aktual

Akses internet di SMK Negeri 5 Seluma menggunakan indihome dengan bandwidth 40mbps dimana pengguna internet diperuntukkan untuk guru, staf dan praktek belajar yang berjumlah kurang lebih 30-40 orang. Indihome terkoneksi dengan komputer dan laptop di lingkungan kerja SMK Negeri 5 Seluma melalui akses LAN dan Wifi. Namun pada SMK Negeri 5 Seluma tersebut belum memiliki *firewall*, sehingga keamanan jaringan komputer di sekolah masih sangat minim.

Selain itu akses internet di SMK Negeri 5 Seluma digunakan oleh guru dan staf untuk mengakses laman internet dengan browsing untuk mendapatkan informasi, namun terdapat beberapa guru dan staf yang mengakses laman sosial media dan laman lainnya yang membuat menurunnya efektifitas kinerja dari guru dan staf tersebut. Dalam proses praktek belajar mengajar di Laboratorium, baik guru dan siswa dapat mengakses internet pada komputer masing-masing. Namun terkadang, diperlukan pembatasan akses internet pada komputer yang digunakan oleh siswa di Laboratorium untuk membantu siswa agar lebih fokus dalam praktek belajar di Laboratorium, karena terkadang terdapat beberapa siswa yang membuka laman web yang tidak berhubungan dengan pelajaran yang ada di Laboratorium.

Adapun skema jaringan komputer saat ini di SMK Negeri 5 Seluma, seperti pada Gambar 3.2.



Gambar 3.2. Skema Jaringan Saat ini Di SMK Negeri 5 Seluma

3.5.2. Analisa Sistem Baru

Sistem baru merupakan pengembangan dari sistem lama yang selama ini sudah ada di SMK Negeri 5 Seluma, yaitu dengan membangun firewall menggunakan iptables pada sistem operasi linux ubuntu. Dengan adanya iptables, pihak sekolah dapat mengatur lalu lintas jaringan dalam server seperti mengizinkan, memblokir atau melewatkan koneksi masuk dan keluar, mengelola port dan lain sebagainya. Iptables bekerja dengan cara membaca lalu lintas jaringan dan membandingkannya dengan serangkaian aturan/rule yang sudah dibuat. Dalam *iptables* terdapat 3 buah *table*, dimana masing-masing *table* memiliki beberapa *chain*, seperti Tabel 3.1.

Tabel 3.1. Tiga Table pada Iptables

Table	Fitur	Keterangan
Mangle	Prerouting, input,	Digunakan untuk melakukan manipulasi packet misalnya, melakukan perubahan

	forward, output, postrouting	pada TTL, pada table ini juga dapat dilakukan proses menandai packet untuk mempermudah identifikasi pada chain selanjutnya
Nat	Prerouting, forward, postrouting,	digunakan untuk melakukan proses NAT (Network Address Translation), misalnya melakukan perubahan source atau destination address, table ini akan berkaitan dengan proses routing. Redirect adalah salah satu contoh penggunaan pada table ini.
Filter	Input, forward, output,	digunakan untuk menolak atau mengizinkan paket yang masuk, keluar, maupun yang hanya lewat

Adapun *flowchart* dalam tahapan dari implementasi *firewall iptables* seperti Gambar 3.3.



Gambar 3.3. Flowchart

Adapun rule/aturan kebijakan yang akan digunakan pada firewall antara lain :

1. Whitelist IP Address

a) Mengizinkan koneksi masuk: `iptables -A INPUT -s IP_Address -j ACCEPT`

b) Mengizinkan koneksi keluar: `iptables -A OUTPUT -d IP_Address -j ACCEPT`

2. Memblokir IP Address

- a) Memblokir koneksi masuk: `iptables -A INPUT -s IP_Address -j DROP`
- b) Memblokir koneksi keluar: `iptables -A OUTPUT -d IP_Address -j DROP`

3. Membuka Port

- a) Membuka port masuk: `iptables -A INPUT -p tcp -dport nomor_port -j ACCEPT`
- b) Membuka port keluar: `iptables -A OUTPUT -p tcp -dport nomor_port -j ACCEPT`

4. Memblokir Port

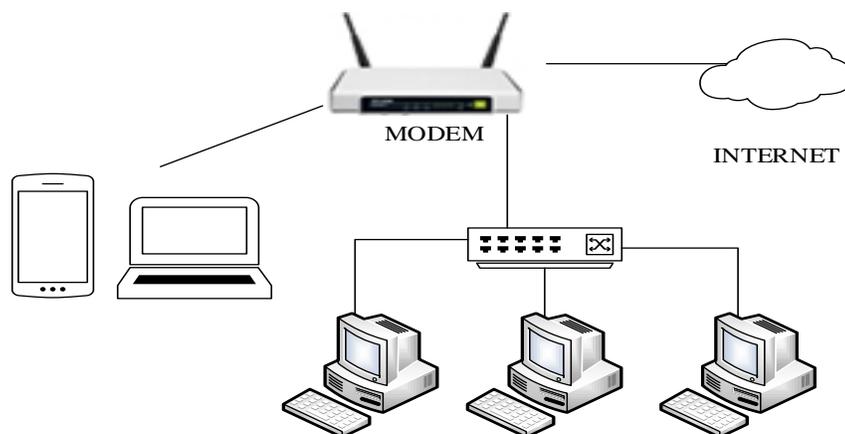
- a) Memblokir port masuk: `iptables -A INPUT -p tcp -dport nomor_port -j DROP`
- b) Memblokir port keluar: `iptables -A OUTPUT -p tcp -dport nomor_port -j DROP`

Metode penelitian yang digunakan mengacu pada metode NDLC dimana terdapat 6 tahapan antara lain :

1. *Analysis*

Akses internet di SMK Negeri 5 Seluma menggunakan indihome dengan bandwidth 40mbps dimana pengguna internet diperuntukkan untuk guru, staf dan praktek belajar yang berjumlah kurang lebih 30-40 orang. Indihome terkoneksi dengan komputer dan laptop di lingkungan kerja SMK Negeri 5 Seluma melalui akses LAN dan Wifi. Namun pada SMK Negeri 5 Seluma tersebut belum memiliki *firewall*, sehingga keamanan jaringan komputer di sekolah masih sangat minim.

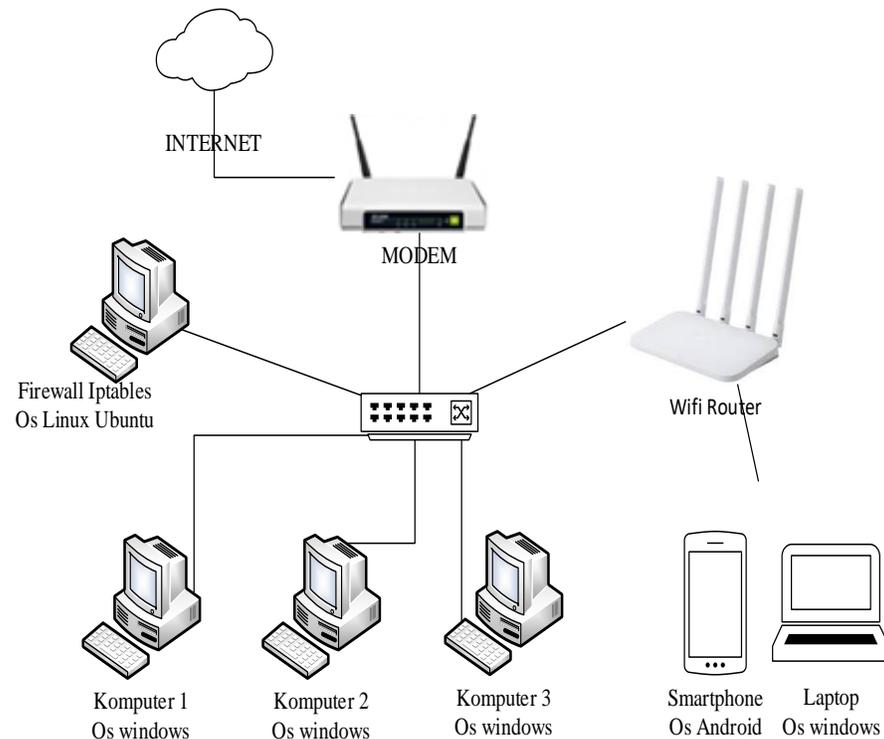
Selain itu akses internet di SMK Negeri 5 Seluma digunakan oleh guru dan staf untuk mengakses laman internet dengan browsing untuk mendapatkan informasi, namun terdapat beberapa guru dan staf yang mengakses laman sosial media dan laman lainnya yang membuat menurunnya efektifitas kinerja dari guru dan staf tersebut. Dalam proses praktek belajar mengajar di Laboratorium, baik guru dan siswa dapat mengakses internet pada komputer masing-masing. Namun terkadang, diperlukan pembatasan akses internet pada komputer yang digunakan oleh siswa di Laboratorium untuk membantu siswa agar lebih fokus dalam praktek belajar di Laboratorium, karena terkadang terdapat beberapa siswa yang membuka laman web yang tidak berhubungan dengan pelajaran yang ada di Laboratorium..



Gambar 3.2. Skema Jaringan Saat ini Di SMK Negeri 5 Seluma

2. Design

Berdasarkan analisa sistem yang telah dilakukan, maka dilakukan pengembangan terhadap jaringan komputer yang ada saat ini dengan menambahkan *firewall iptables*. Tipe jaringan yang digunakan menggunakan topologi star. Adapun skema jaringan yang akan dibangun seperti Gambar 3.4.



Gambar 3.4. Skema Jaringan Yang Akan Dibangun

Pada Gambar 3.4. tersebut ditambahkan 1 perangkat yang bertugas sebagai firewall dengan menggunakan sistem operasi linux ubuntu. Firewall yang digunakan yaitu iptables untuk memonitoring proses lalu lintas paket data dalam jaringan. Penerapan firewall Iptables pada sistem keamanan jaringan di SMK Negeri 5 Seluma antara lain :

- a. *Iptables* sebagai *firewall* sehingga proses lalu-lintas data dari internet ke LAN atau sebaliknya menjadi lebih aman dan cepat.
- b. Dengan *Iptables* pengaturan *firewall* menjadi lebih berlapis baik di-*filter* dari segi *port*, *url* ataupun *ip address*.
- c. Dapat memblok/mem-filter situs-situs yang dapat menurunkan kinerja guru/staf.

Adapun aturan-aturan yang digunakan pada firewall iptables tersebut,

antara lain :

No	Aturan	Keterangan
1	<code>iptables -A INPUT -p icmp --icmp-type 8 -m conntrack --ctstate NEW -j DROP</code>	Memblokir jika terdapat permintaan ping dalam jaringan (serangan <i>ping of death</i>)
2	<code>iptables -A INPUT -s 192.168.1.2/32 -p tcp --dport 22 -j ACCEPT</code>	Memperbolehkan akses untuk ip address 192.168.1.2 untuk akses ke port 22 pada server
3	<code>iptables -t filter -A INPUT -s 0/0 -p tcp --dport 80 -j ACCEPT</code>	Memperbolehkan seluruh network bisa mengakses port 80 pada server
4	<code>iptables -A INPUT -p tcp -m string --string 'facebook.com' --algo bm -j DROP</code> <code>iptables -A FORWARD -p tcp -m string --string 'facebook.com' --algo bm -j DROP</code> <code>iptables -A OUTPUT -p tcp -m string --string 'facebook.com' --algo bm -j DROP</code>	Menutup semua akses jaringan sehingga tidak dapat mengakses situs facebook.com
5	<code>iptables -A INPUT -p tcp -m string --string 'instagram.com' --algo bm -j DROP</code> <code>iptables -A FORWARD -p tcp -m string --string 'instagram.com' --algo bm -j DROP</code> <code>iptables -A OUTPUT -p tcp -m string --string 'instagram.com' --algo bm -j DROP</code>	Menutup semua akses jaringan sehingga tidak dapat mengakses situs instagram.com
6	<code>iptables -A INPUT -p tcp -m string --string 'tokopedia.com' --algo bm -j DROP</code> <code>iptables -A FORWARD -p tcp -m string --string 'tokopedia.com' --algo bm -j DROP</code> <code>iptables -A OUTPUT -p tcp -m string --string 'tokopedia.com' --algo bm -j DROP</code>	Menutup semua akses jaringan sehingga tidak dapat mengakses situs tokopedia.com

3. *Simulation Prototype*

Pada tahap ini, tidak dilakukan simulasi dengan bantuan tools, karena langsung melakukan penerapan terhadap jaringan komputer yang ada.

4. *Implementation*

Tahap dimana jaringan yang akan dibangun akan diterapkan ke sistem jaringan yang ada di SMK Negeri 5 Seluma dengan menambahkan *Iptables* sebagai sistem keamanan jaringan komputer.

5. *Management*

Tahap dimana menentukan kebijakan untuk membuat/ mengatur agar sistem yang telah dibangun dapat berjalan dengan baik dan berlangsung lama.

3.6. Pengujian Sistem

Pengujian sistem yang dilakukan seperti Tabel 3.1.

Tabel 3.1. Pengujian Sistem

Pengujian	Hasil Pengujian	Keterangan
Melakukan serangan ping of deatch dalam jaringan		
Mengakses port 22 SSH pada jaringan		
Mengakses port 80 HTTP pada jaringan		
Mengakses situs web facebook.com		

Mengakses situs web instagram.com		
Mengakses situs web tokopedia.com		