

ANALISIS SISTEM PENGELOLAAN, PEMELIHARAAN DAN KEAMANAN JARINGAN INTERNET PADA IT TELKOM PURWOKERTO

Afit Muhammad Lukman¹, Yusuf Bachtiar²

Teknik Informatika, AMIK BSI Purwokerto
¹afit.fml@bsi.ac.id, ²yusufbachtiar23@gmail.com

Abstract –In building a computer network it takes precision in choosing a network scheme so that it can be used effectively and efficiently. Such as the selection of network topology, the type of network and network devices to be used. The security system is also an important part of a computer network that has internet access to existing local networks to stay safe from outside threats. Here the authors do research in IT Telkom Purwokerto with the result that is, the topology used is the star and the type of client-server network. The server used is linux debian. The security system in IT Telkom purwokerto when analyzed is using authentication server system and using Virtual Private Network (VPN). Authentication server problems when there is no power, here the authors propose the procurement of Uninterruptible Power Supply (UPS) for more stable electricity. As for the security system itself is more effective if added a firewall that is demilitarized zone (DMZ) so that there is a wall separation between public network and local network so that the security system will be more effective.

Keywords: Network security system, Virtual Private Network (VPN), Authentication, Demilitarized Zone(DMZ)

Abstrak-Dalam membangun sebuah jaringan komputer dibutuhkan ketepatan dalam memilih skema jaringan sehingga dapat digunakan secara efektif dan efisien. Seperti pemilihan topologi jaringan, jenis jaringan dan perangkat jaringan yang akan dipakai. Sistem keamanan juga bagian penting dari sebuah jaringan komputer yang memiliki akses internet agar jaringan lokal yang ada tetap aman dari ancaman bahaya dari luar. Disini penulis melakukan riset di IT Telkom Purwokerto dengan hasil yaitu, topologi yang digunakan adalah star dan tipe jaringan *client-server*. Server yang digunakan adalah *linux debian*. Sistem keamanan yang ada di IT Telkom purwokerto saat dianalisis adalah menggunakan sistem server autentifikasi dan menggunakan *Virtual Private Network (VPN)*. Permasalahan server autentifikasi ketika tidak ada daya listrik, disini penulis mengusulkan pengadaan *Uninterruptible Power Supply (UPS)* agar listrik lebih stabil. Sedangkan untuk sistem keamanan sendiri lebih efektif jika ditambahkan suatu *firewall* yaitu *demilitarized zone (DMZ)* agar ada tembok pemisah antara jaringan publik dan jaringan lokal sehingga sistem keamanan akan lebih efektif.

Kata Kunci: Sistem keamanan Jaringan, *Virtual Privat Network (VPN)*, Autentifikasi, *Demiliterized Zone (DMZ)*

A. PENDAHULUAN

Internet merupakan kependekan dari *interconnected-networking* yang berarti sebuah sistem jaringan komputer yang beragam dan bersifat global yang terhubung diseluruh dunia. Dalam mengatur integrasi dan komunikasi jaringan komputer ini digunakan protokol yaitu TCP/IP. TCP (*Transmission Control Protocol*) bertugas memastikan bahwa semua hubungan bekerja dengan benar, sedangkan IP (*Internet Protocol*) yang mentransmisikan data dari satu komputer ke komputer lain. Pengguna diharuskan untuk berlangganan *Internet Service Provider* atau sering disebut dengan ISP untuk dapat menggunakan koneksi *internet*, yang berfungsi sebagai penghubung antara jaringan komputer yang kita gunakan dengan jaringan komputer global. Penggunaan jaringan *internet* sendiri dapat dilakukan dengan beberapa cara, yaitu akses *internet* dengan menggunakan jaringan kabel dan akses *internet* tanpa kabel atau jaringan *wireless*.

Dari kedua jenis jaringan tersebut memiliki keunggulan masing-masing. Jaringan kabel sendiri memiliki keunggulan dimana akses data sangat stabil. Hal ini sangat memudahkan pengguna jika melakukan transfer data yang sangat besar,

sehingga waktu yang diperlukan akan semakin singkat. Meskipun mempunyai keunggulan namun jaringan kabel juga memiliki kelemahan yang besar, yaitu tidak dapat melakukan mobilisasi atau berpindah tempat karena terhalang oleh kabel.

Sementara jaringan *wireless* memiliki keuntungan dimana pengguna dapat berpindah kemanapun yang dia inginkan, baik dimanapun kapanpun dapat dilakukan tanpa terhalang oleh kabel. Selain itu, biaya dari penggunaan jaringan *wireless* juga sangat murah. Jaringan komputer yang dikelola dengan baik akan memaksimalkan kinerja dari sistem jaringan tersebut. Jaringan komputer berfungsi sebagai penghubung antara satu komputer dengan komputer yang lainnya untuk dapat saling berbagi informasi ataupun komunikasi.

Ciri-ciri dari jaringan komputer yang dikelola dengan baik adalah dengan memiliki rancangan jaringan yang sesuai dengan kebutuhan dan mudah dalam implementasinya, serta memiliki keamanan jaringan yang tidak gampang ditembus dan performa jaringan yang baik. Hal ini akan membuat pengguna lebih nyaman ketika berinteraksi dalam jaringan.

Untuk mengatasi masalah keamanan dalam komunikasi data pada jaringan umum (*Public network/internet*) maka lahirlah *virtual private network* (VPN). Secara umum VPN merupakan suatu jaringan komunikasi lokal yang terhubung melalui media jaringan *Public*, infrastruktur *Public* yang paling banyak digunakan adalah jaringan *internet*. Didalam VPN terdapat perpaduan teknologi *tunneling* dan enkripsi yang membuat VPN menjadi teknologi yang handal untuk mengatasi permasalahan keamanan di alam jaringan.

Dalam implementasinya, VPN terbagi menjadi *remote acces* VPN dan *site-to-site* VPN. *site-to-site* VPN digunakan untuk menghubungkan antara 2 tempat yang letaknya berjauhan, seperti halnya kantor pusat dengan kantor cabang atau suatu perusahaan dengan perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, *supplier* atau pelanggan) disebut *ekstranet*. Sedangkan VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis *internetsite-to-site* VPN.

Sistem keamanan yang lain adalah menggunakan *firewall* DMZ. *Firewall* DMZ atau jaringan parameter adalah jaringan *security boundary* yang terletak diantara suatu jaringan privat LAN dan jaringan publik (*internet*). DMZ didefinisikan sebagai sebuah *host* atau jaringan kecil yang dimasukkan ke dalam sebuah zona netral diantara sebuah jaringan perusahaan privat dan jaringan publik. DMZ menghalangi *user* dari luar mengakses secara langsung sebuah *server* yang berisi data-data perusahaan.

Maka dari itu penulis ingin menganalisis bagaimana sistem pengelolaan jaringan pada Institut Teknologi Telkom Purwokerto apakah sudah baik atau belum. Seperti model jaringan yang dipakai saat ini yaitu *client-server* apakah sudah sesuai dengan kondisi kantor, serta topologi *star* yang diterapkan pada tempat tersebut apakah sudah efektif dan efisien.

Bagaimana dan memakai apa sistem keamanan yang dipakai di Institut Teknologi Telkom Purwokerto tersebut, apakah sudah cukup memadai atau diperlukan pembaharuan. Serta juga menganalisis apa saja masalah yang pernah atau sering dihadapi dalam masalah jaringan *internet* di tempat tersebut.

B. TINJAUAN PUSTAKA

1. Jaringan Komputer

Menurut Kristanto (dalam Tiranda, 2014) menyebutkan bahwa "Jaringan komputer merupakan sekelompok komputer otonom yang saling berhubungan satu sama lain, dengan

menggunakan satu *protocol* komunikasi sehingga seluruh komputer yang saling terhubung dapat berbagi informasi, program, sumber daya dan juga dapat saling menggunakan perangkat keras lainnya secara bersamaan, seperti *printer*, *hardisk* dan lain sebagainya."

Sedangkan menurut Zymon Machajewski mengatakan bahwa:Yang dimaksud dengan jaringan komputer adalah seperangkat komputer yang saling terkoneksi secara bersamaan satu sama lainnya dengan tujuan utama yaitu untuk saling membagikan atau *men-share resources* alias sumberdaya. Salah satu sumberdaya yang saat ini banyak digunakan di dalam sebuah jaringan komputer adalah sumber daya *internet*.

2. Model Jaringan

a. Peer to Peer

Jaringan komputer dimana setiap komputer yang terhubung dalam jaringan tersebut merupakan *client* sekaligus juga *server*. Jaringan ini dibentuk tanpa adanya kontrol terpusat dari sebuah *server* yang terdedikasi. Setiap komputer memiliki kedudukan yang sama. Pertukaran data antar komputer serta penggunaan fasilitas komputer yang terhubung pada jaringan *Peer To Peer* dapat dilakukan secara langsung tidak ada pengendali dan pembagian hak akses.

Jaringan *Peer To Peer* biasanya diterapkan pada jaringan dengan skala kecil 2 hingga 10 komputer dengan satu atau dua *peripheral*. Tujuan penggunaan jaringan *Peer To Peer* yang utama adalah penggunaan program, data atau *peripheral* secara bersama-sama. Untuk keamanan, setiap *user* komputer bertanggung jawab terhadap keamanan komputernya masing-masing.

b. Client- Server

Jaringan *client-server* didefinisikan sebagai suatu arsitektur jaringan komputer dimana perangkat *client* melakukan proses meminta data dan *server* yang memiliki tugas untuk memberikan respon berupa data terhadap *request* tersebut. Perangkat *client* biasanya berupa perangkat komputer dengan aplikasi *software* jaringan yang telah terinstal guna untuk meminta dan menerima data melalui jaringan. Salah satu contoh aplikasi *software* yang paling sering digunakan untuk meminta dan menerima data pada jaringan ialah *web browser*, dimana *user* dapat melakukan *request* untuk sebuah halaman web.

Server merupakan sebuah komputer yang dirancang khusus untuk melayani *client* dengan memproses *request* yang telah diterima dari *client* lalu kemudian mengirimkan kembali respon data kepada *client* melalui jaringan. *Server* menyimpan informasi dan data yang kompleks yang mungkin dibutuhkan *client*, oleh karena itu biasanya *server* terdiri dari komputer dengan performa yang tinggi baik dari segi pemrosesan maupun dari segi

memori, hal tersebut agar *server* mampu melayani *request* dari banyak *client* secara bersamaan.

3. Topologi Jaringan

a. Topologi Star

Karakteristik dari topologi ini adalah *node* berkomunikasi langsung dengan *station* lain melalui *central node (Hub/Switch)*, *Traffic* data mengalir dari *node* ke *central node* dan diteruskan ke *node* tujuan. Jika salah satu segmen kabel terputus, jaringan lain tidak akan terputus.

b. Topologi Hierarchical/Tree

Tidak semua stasiun mempunyai kedudukan yang sama. Stasiun yang kedudukannya lebih tinggi menguasai stasiun di bawahnya, sehingga jaringan sangat tergantung ada stasiun yang kedudukannya lebih tinggi dan kedudukan stasiun yang sama, disebut *peer topology*.

c. Topologi Bus

Topologi ini merupakan bentangan satu kabel yang kedua ujungnya ditutup, dimana disepanjang kabel dipasang *node-node*. *Signal* dalam kabel dilewati satu arah sehingga memungkinkan sebuah *collision* terjadi.

d. Topologi Ring

Topologi jaringan yang berupa lingkaran tertutup yang berisi *node-node*. *Signal* mengalir dalam dua arah sehingga dapat menghindari terjadinya *collision* sehingga memungkinkan terjadinya pergerakan data sangat cepat. Semua komputer saling tersambung membentuk lingkaran. Data yang dikirim diberi *address* tujuan sehingga dapat menuju komputer yang dituju.

e. Topologi Daisy Chain (Linear)

Topologi ini merupakan peralihan dari topologi *Bus* dan topologi *ring*, di mana tiap simpul terhubung langsung ke dua simpul lain melalui segmen kabel, tetapi segmen membentuk saluran, bukan lingkaran utuh. Antar komputer seperti terhubung seri.

Keuntungannya dari topologi ini adalah instalasi dan pemeliharaannya murah, sedangkan kerugiannya adalah kurang handal dan tidak sesuai dengan kemajuan jaman.

4. Perangkat Keras Jaringan

Dalam sebuah sistem komputer, perangkat keras didefinisikan sebagai komponen-komponen komputer yang dapat ditangkap dengan indera peraba kita. Sejumlah perangkat keras merupakan komponen pokok yang harus ada di sebuah komputer, sedangkan komponen-komponen lainnya adalah komponen pendukung untuk menambah fungsi komputer.

Komponen perangkat keras komputer terbagi menjadi:

a. Input Devices (Bagian Input)

Bagian *Input* merupakan alat-alat yang dapat digunakan untuk memasukan data ke dalam komputer. Alat *Input* data diantaranya *keyboard* (digunakan dalam *Input* data berbentuk teks ke dalam komputer), *mouse* (alat yang digunakan sebagai *pointer*), *scanner* (alat yang digunakan untuk memasukan data yang berbentuk *image*), kamera digital (alat yang digunakan untuk menyimpan gambar), dan *digitizer* (alat yang digunakan untuk menggambar langsung ke dalam komputer).

b. Bagian Pengolah Utama Dan Memori

- 1) *Processor (CPU)* merupakan jantungnya sistem komputer, tapi walaupun demikian *processor* ini tidak akan memberikan manfaat tanpa komponen pendukung lainnya.
- 2) *Memory*, sebagai penyimpan pada dasarnya dapat dibagi menjadi memori utama dan kedua tau tambahan. Fungsi memori utama adalah untuk menyimpan program, data, sistem operasi, sebagai penyangga dan penyimpanan gambar
- 3) *Bus* merupakan kabel-kabel yang tersusun dengan rapi dan digunakan untuk menghubungkan antara CPU dengan *primary storage*. Bus digunakan untuk mentransfer data atau informasi dari *memory* ke berbagai macam peralat *Input, output*, atau dengan kata lain bus merupakan suatu sirkuit yang digunakan sebagai jalur transformasi antara dua atau lebih alat-alat dalam sistem komputer.
- 4) *Cache Memory, cache* berfungsi sebagai *buffer* (media penyesuai) antara CPU yang berkecepatan yang lebih rendah. Tanpa *cache* memori CPU harus menunggu data dan instruksi diterima dan *main memory* atau menunggu hasil pengolahan selesai dikirim ke *main memory* baru proses selanjutnya bisa dilakukan. *Cache memory* diletakkan di antara CPU dengan *main memory*.
- 5) *Mother Boar/Main Board* merupakan papan rangkaian tercetak yang berfungsi sebagai tempat penampungan komponen-komponen pendukung suatu sistem komputer.
- 6) *Driver Card* merupakan papan rangkaian tercetak yang berfungsi memperluas kemampuan suatu sistem komputer.

c. Bagian Output (Output Device)

Peralatan *output* merupakan peralatan-peralatan yang digunakan untuk mengeluarkan informasi hasil pengolahan data. Ada beberapa macam peralatan *output* yang biasa digunakan yaitu:

- 1) *Printer*, yaitu peralatan yang digunakan untuk mengeluarkan informasi hasil pengolahan data ke kertas atau transparansi.
- 2) *Monitor*, merupakan alat yang digunakan untuk menayangkan hasil pengolahan data atau informasi dalam bentuk visual pada *Monitor* yang ditempatkan di depan mata.
- 3) Liquid Display Projector (LCD), merupakan alat yang digunakan untuk menayangkan

hasil pengolahan data atau informasi dengan cara memancarkannya atau memproyeksikannya ke dinding atau bidang lainnya yang vertikal.

- 4) Speaker, merupakan alat yang digunakan untuk mengeluarkan hasil pengolahan data atau informasi dalam bentuk suara.

d. Bagian Komunikasi

Peralatan komunikasi adalah peralatan-peralatan yang digunakan agar komunikasi data bisa berjalan dengan baik. Ada banyak jenis peralatan komunikasi, beberapa diantaranya adalah *Network Card* untuk LAN dan *wireless LAN*, *HUB/Switching* dan *access point wireless LAN*, *fiber optic* dan *reouter* dan *range extender*, berbagai macam Modem (*internal*, *eksternal*, *PCMA*) dan *wirelesscardbusadapter*, pemancar dan penerima, *very small aperture satellite* (VSAT) dan satelit.

5. Perangkat Lunak (Software)

Software adalah kumpulan dari program-program yang digunakan untuk menjalankan aplikasi tertentu pada komputer, sedangkan program merupakan kumpulan dari perintah-perintah komputer yang tersusun secara sistematis.

Software dapat dikelompokkan menjadi dua yaitu:

a. Perangkat Lunak Sistem (System Software)

Perangkat lunak sistem merupakan kumpulan dari perangkat lunak yang digunakan untuk mengendalikan sistem komputer yang meliputi sistem operasi (*Operating System*), *Interpreter* dan *Compiler*.

- 1) *Operating system* berfungsi untuk mengendalikan hubungan antara komponen-komponen yang terpasang dalam suatu sistem komputer misalnya *keyword* dengan CPU, dengan layar *Monitor* dan lain-lain.
- 2) *Interpreter* merupakan *software* yang berfungsi sebagai penerjemah bahasa yang dimengerti oleh manusia ke dalam bahasa yang dimengerti oleh manusia ke dalam bahasa yang dimengerti oleh komputer (bahasa mesin) per perintah.
- 3) *Compiler* berfungsi untuk menerjemah bahasa yang dipahami oleh manusia ke dalam bahasa yang dipahami oleh komputer secara langsung atau *file*.

b. Perangkat Lunak Aplikasi (Application Software)

Perangkat lunak aplikasi atau sering disebut "paket aplikasi" merupakan *software* jadi yang siap digunakan. *Software* ini dibuat perusahaan perangkat lunak tertentu (*Software House*) baik dari dalam maupun dari luar negeri yang umumnya berada di Amerika.

Macam-macam *application software* :

- 1) Aplikasi pengolah angka (*ms.excel*, *lotus 123*)
- 2) Aplikasi pengolah kata (*ms.word*, *notepad*)

- 3) Aplikasi pengolah grafis (*adobe photoshop*, *paint*)
- 4) Aplikasi pengolah presentasi (*ms.power point*)
- 5) Aplikasi pengolah data (*visual foxpro*, *ms.access*)
- 6) Aplikasi internet (*google*, *safari*)
- 7) Aplikasi video editing (*ulead*, *pinneacle studio*)
- 8) Program pengembangan komputer (*visual basic*, *java*)
- 9) Pengembang web (*blogger*, *wordpress*)

6. TCP/IP dan Subnetting

IP address adalah sebuah sistem pengalamatan unik setiap *host* yang terkoneksi ke jaringan berbasis *TCP/IP*. *IP address* bisa dianalogikan seperti sebuah alamat rumah. Ketika sebuah datagram dikirim, informasi alamat inilah yang menjadi acuan datagram agar bisa sampai ke *device* yang dituju. *IP address* terbagi dalam 2 versi, *IPv4* dan *IPv6*. Sebuah *IP address* versi 4 atau *IPv4* terbentuk dari 32 *binarybits*. Dari 32 *binarybits* tersebut terbagi lagi menjadi 4 *octet* (1 *octet* = 8 *bits*). Nilai tiap *octet* di antara 0 sampai 255 dalam format desimal, atau 00000000 - 11111111 dalam format *binary*. Setiap *octet* dikonversi menjadi desimal dan dipisahkan oleh tanda titik (*dot*).

a. Sistem komunikasi

Berdasarkan bagaimana perangkat saling berkomunikasi, terbagi menjadi beberapa jenis, yakni sebagai berikut:

- 1) *Unicast*, merupakan komunikasi antar sebuah *host* atau *point-to-point*. Contoh : *HTTP*
- 2) *Broadcast*, merupakan metode komunikasi dari sebuah *host* ke semua *host* yang masih dalam satu jaringan. Alamat *broadcast* digunakan dalam komunikasi *one-to-everyone*. Contoh : *ARP Ethernet*.
- 3) *Multicast*, merupakan metode komunikasi dari sebuah *host* ke banyak *host* yang bergabung dalam group *multicast* yang sama. Alamat *multicast* digunakan dalam komunikasi *one-to-many*. Contoh : *Video Streaming*.
- 4) *Anycast*, merupakan metode komunikasi dari sebuah *host* ke *host* atau kelompok *host* lain yang diset memiliki IP sama. Contoh : *6to4 relay*.

b. Publik IP Address

Public IP address merupakan *IP address* yang dapat diakses di jaringan *internet*. *IP Public* juga dikenal sebagai *globally routable unicast IP address*. Ketika sebuah perangkat memiliki *IP Public* dan terkoneksi ke jaringan *internet*, maka perangkat tadi bisa diakses darimanapun melalui jaringan *internet* juga. Akan tetapi kita tidak bisa memasang sembarang *IP Public* di sebuah *device*. Ada aturan mengenai alokasi *IP Public*. Kita bisa mendapatkan *Public IP address* dari pinjaman ISP atau alokasi dari APNIC/IDNIC (www.idnic.net).

c. IP Private

Pada arsitektur IP address, *Private IP Address* adalah IP address yang diperuntukkan untuk jaringan lokal. IP *private* tidak boleh ada di jaringan *internet* dan tidak dapat diakses di jaringan *internet*. Pada implementasi di jaringan real, biasanya jaringan lokal menggunakan IP *Private*, kemudian ditambahkan sebuah *router* yang menjembatani jaringan lokal yang menggunakan IP *private* dengan jaringan publik yang menggunakan IP *Public*. Untuk cakupan IP *Private*, Anda bisa lihat tabel IP *Private* di pembahasan mengenai CIDR.

d. IP Khusus

Selain IP *Private* dan IP *Public*, ada beberapa IP khusus lain. IP ini sudah memiliki tujuan penggunaan khusus yang sudah disepakati secara internasional, sehingga tidak dapat digunakan untuk pengalamatan sebuah *host*.

e. Kelas IP

Pada awal mula design IP address, IP address dibagi dalam beberapa kelas. Kelas IP dibedakan berdasarkan jumlah *bitsnetwork* ID. Masing masing kelas memiliki jumlah *network* yang berbeda, dan jumlah *host* di tiap *network* yang berbeda pula. Pembagian IP address berdasarkan kelas ini sudah mulai ditinggalkan digantikan dengan sistem CIDR. Akan tetapi, ada baiknya kita coba lihat sejarah kelas IP address ini.

f. Subnet Mask

Subnet Mask merupakan nilai yang dibentuk dari angka *biner 32 bits*. sama seperti IP address. Dari angka *biner 32 bits* ini, juga dipisahkan dengan tanda *dot* pada setiap *octet*. Fungsi dari *subnet mask* ini adalah membedakan *network* id dan *host* id. pada gambar kelas IP, kita bisa melihat alokasi nilai *bits* pada masing - masing *identifier*. Didalam *subnet mask* semua *bit* yang dialokasikan untuk *network* id diwakili oleh angka *biner 1* sedangkan semua *bit* alokasi *host* id akan diwakili oleh angka *biner 0*.

Selain membedakan *identifier*, *subnet mask* juga digunakan untuk menentukan letak suatu *host*, apakah di jaringan yang masih dalam satu segmen, atau sudah berbeda segmen.

g. Subnetting

Subnetting adalah sebuah mekanisme perhitungan pembagian *network* menjadi *network* dengan skala yang lebih kecil, biasa disebut *subnet*. *Subnetting* dilakukan dengan meminjam nilai *bits* yang dialokasikan pada *host* id, sehingga memungkinkan penggunaan IP address yang lebih efisien. *Subnetting* biasa disebut juga Variable Length *subnet mask* (VLSM). *Subnet* ting biasa diterapkan dengan mengubah nilai *subnet mask*. Contoh kasus misalnya sebuah perusahaan hanya memiliki 60 komputer yang akan terhubung dalam satu jaringan menggunakan IP kelas C dengan *subnet maskdefault 255.255.255.0*. Untuk alasan keamanan dan efisiensi jaringan, maka hanya perlu alokasi IP kurang lebih sejumlah 60 IP address. Disinilah fungsi *subnetting* dibutuhkan.

7. Sistem Keamanan Jaringan

a. Autentikasi

Autentikasi adalah proses pengenalan peralatan, sistem operasi, kegiatan, aplikasi dan identitas *user* yang terhubung dengan jaringan

komputer. Autentikasi dimulai pada saat *userlogin* ke jaringan dengan cara memasukkan *password*.

Tahapan autentikasi adalah:

- 1) Autentikasi untuk mengetahui lokasi dari peralatan pada suatu simpul jaringan (*data link layer* dan *network layer*)
- 2) Autentikasi untuk mengenal sistem operasi yang terhubung ke jaringan (*transport layer*)
- 3) Autentikasi untuk mengetahui fungsi/proses yang sedang terjadi di suatu simpul jaringan (*session* dan *presentation layer*)
- 4) Autentikasi untuk mengenali *user* dan aplikasi yang digunakan (*application layer*).

b. Enkripsi

Enkripsi adalah teknik pengkodean data yang berguna untuk menjaga data/file baik di dalam komputer maupun pada jalur komunikais dari pemakai yang tidak dikehendaki. Enkripsi diperlukan untuk menjaga kerahasiaan data.

- 1) Teknik enkripsi
 - a) DES (*Data Encryption Standard*)
 - b) RSA (*Rivest Shamir Adelman*)

c. VPN

VPN merupakan suatu koneksi antar dua jaringan yang dibuat untuk mengkoneksikan kantor pusat, kantor cabang, *telecommuters*, *suppliers*, dan rekan bisnis lainnya, ke dalam suatu jaringan dengan menggunakan infrastruktur telekomunikasi umum dan menggunakan metode enkripsi tertentu sebagai media pengamanannya. VPN merupakan sebuah jaringan *private* yang menghubungkan satu node jaringan ke node jaringan lainnya dengan menggunakan jaringan public seperti *internet*. Data yang dilewatkan akan diencapsulation (dibungkus) dan dienkripsi, supaya data tersebut terjamin kerahasiaannya.

A. Solusi VPN

Penggunaan sistem VPN bisa menggunakan suatu perangkat khusus produksi vendor tertentu yang dibuat untuk melakukan proses komunikasi lewat jaringan *internet*. Seperti produk dari vendor *cisconetwork*, *2Com*, *NortelNetwork*, *linksys* dan sebagainya. Sistem tersebut sering disebut sebagai solusi *HardwareBased*, sedangkan sistem yang menggunakan perangkat lunak sebagai sistem utamanya sering disebut sebagai solusi *Software Based*.

Ada tiga macam tipe interkoneksi VPN, yaitu:

- 1) Access VPN

Access VPN membuat koneksi jarak jauh untuk mengakses ke jaringan *intranet* atau *ekstranet* pelanggan dan penggunaan bergerak dengan menggunakan infrastruktur PSTN *dial-up*, ISDN, DSL, atau *Mobile IP* untuk membuat koneksi yang aman bagi *mobileuser*, *telecommuters* dan kantor cabang
- 2) Intranet VPN

Intranet VPN menghubungkan kantor pusat, kantor cabang dan *remoteuser* ke dalam jaringan *internal* dengan menggunakan infrastruktur koneksi *dedicated*.
- 3) Extranet VPN

Extranet VPN menghubungkan dengan pihak luar seperti pelanggan, *supplier*, rekan bisnis, atau suatu komunitas ke dalam jaringan

Internal dengan menggunakan koneksi *dedicated*.

d. Demilitarized Zone(DMZ)

Firewall DMZ atau jaringan perimeter adalah jaringan *security boundary* yang terletak diantara suatu jaringan privat LAN dan jaringan publik (*internet*). DMZ didefinisikan sebagai sebuah *host* komputer atau jaringan kecil yang dimasukkan kedalam sebuah zona netral diantara sebuah jaringan perusahaan *private* dan jaringan publik. DMZ menghalangi *user* dari luar mengakses secara langsung sebuah *server* yang berisi data-data perusahaan.

Konsep DMZ pada dasarnya mengaplikasikan konsep NAT (*NetworkAddressTranslation*) dan PAT (*Port Address Translation*). NAT berfungsi mengarahkan alamat riil menjadi alamat *Internal* sedangkan PAT berfungsi untuk mengarahkan data yang masuk melalui *port* atau sekumpulan *port* dan protokol. Umumnya, setiap layanan yang diberikan kepada pengguna di jaringan *eksternal* dapat ditempatkan dalam DMZ. Yang paling umum dari layanan ini adalah *web server*, *mailserver*, *ftp server*, *VoIP server* dan *DNS server*.

C. METODE PENELITIAN

Metode penelitian yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut:

1. Studi Literatur

Mengumpulkan data melalui buku, jurnal, dan *internet* yang berhubungan dengan analisis dan perancangan yang dilakukan.

2. Observasi

Mengumpulkan data analisis melalui pihak Institut Teknologi Telkom Purwokerto untuk mengetahui sistem jaringan yang sedang berjalan di tempat tersebut

3. Analisis

Menganalisis sistem yang ada dari data-data yang telah dikumpulkan dan mencari solusi dari permasalahan yang ada.

4. Perancangan

Mengusulkan rancangan tata kelola sistem jaringan dengan mempertimbangkan kesesuaian antara kebutuhan, efisiensi dan dampak yang ada terhadap sistem jaringan yang sedang berjalan.

D. HASIL DAN PEMBAHASAN

1. Tinjauan Perusahaan

Institut Teknologi Telkom Purwokerto (IT Telkom) adalah perguruan tinggi yang dikelola oleh Telkom Foundation dan merupakan perguruan tinggi yang fokus di bidang Telematika (Telekomunikasi dan Informatika). Institut Teknologi Telkom Purwokertomemiliki dua fakultas yaitu Fakultas Teknik Telekomunikasi dan Elektro, dengan program studi D3 Teknik Telekomunikasi,

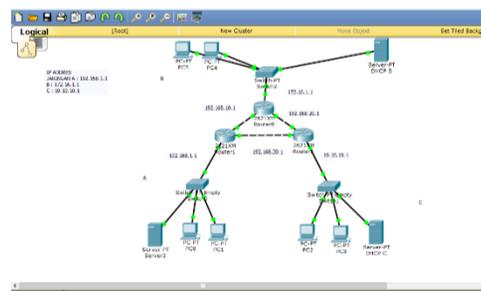
S1 Teknik Telekomunikasi, dan S1 Teknik Elektro. Fakultas Teknologi Industri dan Informatika dengan Program studi, S1 Teknik Informatika, S1 Rekayasa Perangkat Lunak, S1 Sistem Informasi, S1 Teknik Industri dan S1 Desain Komunikasi Visual..IT Telkom Purwokerto merupakan perguruan tinggi yang menerapkan konsep *Information and Communication Technology (ICT)* atau Teknologi Informasi dan Komunikasi (TIK).

Untuk meningkatkan kualitas pengelolaan dan mutu lulusan, IT Telkom Purwokerto dikelola bersama dengan Telkom University Bandung sehingga kualitas lulusan dapat disetarakan dengan lulusan dari Telkom University Bandung.IT Telkom Purwokerto dalam meningkatkan kualitas pengelolaan memiliki visi menjadi perguruan tinggi yang unggul dalam pengembangan sains, teknologi dan teknik berbasis teknologi telematika dan membentuk insan yang berkarakter. IT Telkom Purwokerto miliki misi menyelenggarakan dan mengembangkan pendidikan berbasis teknologi telematika yang berkualitas dan pembentukan karakter yang unggul, mengembangkan riset dan menyebarluaskan sains, teknologi dan teknik yang terkini, menerapkan dan memanfaatkan sains, teknologi dan teknik bagi kemaslahatan masyarakat, mengembangkan tatakelola berbasis *best practices* dan menjalin kerjasama yang berkualitas dengan institusi pendidikan, pemerintah dan dunia industri di dalam dan luar negeri.

2. Skema Jaringan Berjalan

Topologi jaringan yang digunakan di Institut Teknologi Telkom Purwokerto adalah topologi *star*. Topologi *star* dipilih dikarenakan sesuai dengan situasi di lingkungan Institut Teknologi Telkom yang sering terjadi penambahan jumlah *client*. Selain itu, dengan menggunakan topologi *star* akses ke *station* lain dirasa lebih cepat dan lebih penting lagi jika salah satu segmen kabel putus tidak akan berpengaruh terhadap kinerja jaringan yang lainnya.

Gambar2. Skema Jaringan



3. Keamanan Jaringan

Sistem keamanan dan perawatan secara fisik pada Institut Teknologi Telkom Purwokerto adalah dengan cara seperti *aces point* ditaruh diatas agar tidak rawan dicuri atau rusak. Ruangan selalu dikunci bila pada malam hari. Sedangkan

untuk sistem keamanan secara non fisik yang sudah dipakai di Institut teknologi Telkom Purwokerto adalah menggunakan *server* autentifikasi yang berfungsi untuk mengenali *user* yang berinteraksi ke jaringan dan memuat semua informasi dari *user* tersebut.

Metode autentifikasi yang dipakai menggunakan metode *something you know* yang cara ini mengandalkan kerahasiaan informasi, contohnya adalah *password* dan *PIN*. Cara ini berasumsi bahwa tidak ada seorangpun yang mengetahui rahasia itu kecuali anda seorang. Cara kerja *server* autentifikasi yaitu *server* akan mengecek setiap *client* yang mencoba untuk mengakses ke jaringan dengan daftar *client* yang sudah terdaftar pada jaringan. Jika *client* tersebut tidak terdaftar maka akses akan ditolak, jika sudah terdaftar maka *client* diizinkan untuk mengakses ke dalam jaringan.

Sistem keamanan yang dipakai juga menggunakan *Virtual Private Network (VPN)*. Untuk jenis *VPN* yang dipakai adalah *Point to Point Protocol (PPTP)*. Secara sederhana, sistem kerja *VPN* di Institut Teknologi Telkom Purwokerto adalah sebagai berikut:

- a) *VPN* membutuhkan sebuah *server* yang berfungsi sebagai penghubung antar PC. Institut Teknologi Telkom Purwokerto menggunakan *router* mikrotik sebagai *serverVPN*.
- b) Untuk memulai sebuah koneksi, komputer dengan aplikasi *VPNclient* mengontak *serverVPN*, *VPNserver* kemudian memverifikasi *username* dan *password* dan apabila berhasil maka *VPNserver* memberikan *IP address* baru pada komputer *client* dan selanjutnya sebuah koneksi akan terbentuk.
- c) Untuk selanjutnya komputer *client* bisa digunakan untuk mengakses *resource* yang berada dibelakang *VPNserver* misalnya melakukan transfer data, print dokumen, *browsing* dengan *gateway* yang diberikan dari *VPNserver*, melakukan *remote dekstop* dan lain sebagainya.
- d) Dengan menggunakan *VPN* kita juga banyak mendapat keuntungan seperti, adanya fitur *remote acces* yang memungkinkan kita mengakses jaringan dari mana saja selama terhubung ke internet. Keamanan saat kita berselancar menggunakan akses internet publik.

5. Permasalahan

Permasalahan yang terjadi pada jaringan internet di Institut Teknologi Telkom Purwokerto adalah sebagai berikut :

- a) Permasalahan *server* autentifikasi ketika terjadi pemadaman listrik dari PLN.
- b) Kecepatan *bandwith* yang kurang maksimal dikarenakan banyaknya pengguna atau *client* yang mencapai 500 *client*.
- c) Kurangnya sistem *firewall* saat terkoneksi ke internet saat dipakai untuk *browsing* dapat menimbulkan pemakaian yang disalahgunakan oleh *client*.

6. Alternatif Pemecahan Masalah

a. Spesifikasi Hardware Usulan

Untuk mengatasi masalah autentifikasi yang diakibatkan karena permasalahan arus listrik, disini penulis ingin mengusulkan adanya penambahan *Uninterruptible Power Supply (UPS)* agar listrik tetap aman dan stabil walaupun mengalami pemadam listrik oleh PLN.

b. Mengatasi Kecepatan Transfer Data

Penggunaan koneksi internet yang maksimal tentunya akan membuat nyaman saat digunakan, untuk itu diperlukan pengaturan penggunaan *bandwidth* internet secara benar. Ada beberapa cara yang bisa diterapkan untuk memaksimalkan koneksi internet, diantaranya:

- 1) Membatasi Kecepatan Transfer Data
Membatasi kecepatan transfer data adalah tugas dari *administrator, administrator* disini harus mengelola jaringan yaitu dengan membagi *bandwidth* dengan adil bagi para pengakses internet, misalnya dengan membagi rata besar *bandwidth* ke setiap *client* sehingga tiap *client* mempunyai jatah *bandwidth* yang sama dan tidak akan mengambil *bandwidth* dari *client* yang lain.
- 2) Membatasi Jumlah Data Yang Dapat di Transfer
Dengan membatasi jumlah data juga dapat menjadi solusi agar kecepatan koneksi internet dapat maksimal.
- 3) Pemilihan Hardware Jaringan
Media transmisi yang digunakan juga berpengaruh terhadap kecepatan *bandwidth*, misalnya dengan menggunakan kabel fiber optik akan memiliki *bandwidth* lebih besar dibandingkan dengan kita menggunakan kabel telepon biasa.
- 4) Merawat Perangkat Internet Secara Berkala
Perangkat yang terawat dengan baik dan teratur pastinya memiliki kondisi yang lebih baik dan hal ini berdampak terhadap koneksi internet. Pengecekan perangkat secara berkala juga dapat mencegah dan mengontrol kerusakan yang mungkin akan terjadi.

c. Keamanan Jaringan Usulan

Sistem keamanan yang ada di Institut Teknologi Telkom Purwokerto sebenarnya sudah cukup baik dan memadai, namun disini penulis ingin memberi saran untuk penambahan sistem *DMZ* sebagai sistem proteksi keamanan jaringan internet di Institut Teknologi Telkom Purwokerto tersebut agar keamanan jaringan internet lebih maksimal. Konfigurasi *DMZ* bisa diimplementasikan menggunakan *linux debian*.

E. KESIMPULAN

Berdasarkan hasil analisa yang dilakukan di Institut Teknologi Telkom Purwokerto, maka dapat ditarik kesimpulan secara umum:

1. Perlunya menyediakan alat back up listrik yang memadai disaat terjadi pemadaman listrik seperti menggunakan *Uninterruptible Power Supply* (UPS).
2. Kecepatan *bandwith* yang kurang maksimal diakibatkan banyaknya pengguna yang memakai secara bersamaan.
3. Perlunya sistem proteksi dalam penggunaan internet dengan menambahkan *demilitarized zone* (DMZ).

DAFTAR PUSTAKA

- [1] Oktivasari, Prihatin. Utomo Andri Budhi. (2016). Analisa *Virtual Private Network* Menggunakan *Open VPNDan Point To point Tunneling Protocol*. Jurnal Penelitian Komunikasi dan Opini Publik, 2 (20): 187-189. <https://jurnal.kominfo.go.id/index.php/jpkop/article/download/658/489>(diakses 25 mei 2018)
- [2] Fajar Irianto, Jelang,2014. Pengertian dan Jenis-jenis Topologi Jaringan. STMIK RAHARJA: Jurnal Teknik Informatika.
- [3] Purbo, Onno W. 2018. INTERNET-TCP/IP: KONSEP&IMPLEMENTASI. Yogyakarta: Andi
- [4] Purwanto Deny, Dana Raditya Damar. (2015). Sistem Keamanan Jaringan Model *Client Server* Menggunakan Enkripsi Data (MD5) Pada Dinas Kesehatan Kota Cirebon. Jurnal Online ICT STMIK IKMI, 1 (13): 4 <http://stmik-ikmi-cirebon.net/ejournal/index.php/JICT/article/view/103/98> (diakses 20 mei 2018)
- [5] Afrianto, Irawan.2014 *Virtual Private Network* Sebagai Sistem Pengamanan Data Pada Jaringan Komputer. Studi Kasus Jaringan Komputer Unikom
- [6] Sugeng, Winarno dkk. 2015. Jaringan Komputer dengan *TCP/IP*. Bandung. Modula.
- [7] Kuncoro, Satriyo. 2018. Implementasi Autentikasi pada *Virtual Privat Network* (VPN) Menggunakan *Kerberos*. Jakarta: Program Studi Informatika FTI-UKSW.
- Saefudin, Arif. 2018. Perancangan dan Implementasi *Virtual Privat Network* (VPN) pada CV. Yudhistira Amarta Ceta. Jakarta: Program Studi Teknik Informatika FTI-UKSW.