BAB III

ANALISA JARINGAN BERJALAN

3.1. Tinjauan Perusahaan

PT. Metalogix Infolink Persada adalah perusahaan yang sedang berkembang yang bergerak di bidang jasa teknologi informasi khususnya penyediaan aplikasi perangkat lunak dan sistem untuk perbankan dengan jumlah karyawan sekitar 100 sampai 150 orang.Kebanyakan klien dari perusahaan ini adalah bank-bank swasta maupun daerah.

3.1.1. Sejarah Perusahaan

PT. Metalogix Infolink Persada pertama kali didirikan pada tahun 1997 dengan klien pertamanya adalah Bank Kharisma.Kantor pusat PT. Metalogix Infolink Persada berada di Multivision Tower lantai 7, jalan kuningan mulia kavling 9B, Jakarta Selatan.

Saat ini PT. Metalogix Infolink Persada merupakan salah satu penyedia aplikasi dan sistem *switching* untuk perbankan di indonesia. Kegiatan sehari-hari nya adalah memastikan sistem yang ada pada klien berjalan dengan baik dan juga melakukan *update* untuk aplikasi tersebut sesuai dengan permintaan dari klien.

3.2.2. Struktur Organisasi dan Fungsi

Struktur organisasi pada perusahaan ini seperti kebanyakan perusahaan-perusahaan teknologi informasi lainnya. Dipimpin oleh dewan direksi yang

merupakan posisi paling atas dari organisasi. Lalu dibawahnya ada direktur *solution* dan *operation* yang terbagi lagi menjadi beberapa divisi yang memiliki fungsi berbeda dan masing-masing divisi memiliki manajer dan staff dibawahnya.

Dalam struktur organisasi perusahaan ini memiliki beberapa divisi diantaranya adalah divisi infrastruktur yang bertanggung jawab akan infrastruktur kantor pusat mulai dari sistem teknologi informasi maupun non sistem teknologi informasi.

Divisi *Programmer*, merupakan divisi yang bertanggung-jawab atas segala sesuatu yang berhubungan dengan aplikasi yang ada pada klien.

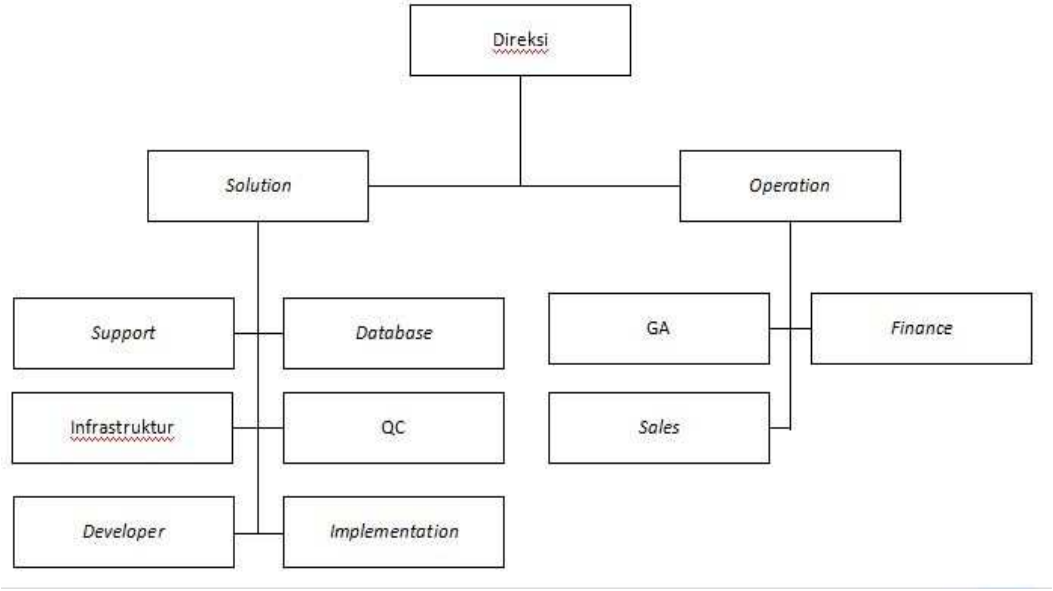
Divisi *Database*, merupakan divisi yang bertanggung-jawab akan*database* klien yang terhubung pada aplikasi ataupun sistem dari PT. Metalogix Infolink Persada.

Divisi QC, merupakan *quality control* untuk aplikasi yang dibangun ataupun *update* yang di *develop* oleh *developer* yang akan dirilis ke klien.

Divisi Implementasi, divisi dimana perubahan ataupun aplikasi baru yang sudah selesai dirilis oleh QC dikirim ke client untuk pengetesan dan juga implementasi disisi klien.

Divisi *Support*, bertanggung-jawab akan sistem yang sudah berjalan pada operasional klien. Mengatasi *problem* yang ditemukan dikemudian hari pada aplikasi pada klien.

Divisi *Sales*, merupakan penghubung dan koneksi pertama perusahaan ke klien dalam memulai dan menjaga hubungan bisnis perusahaan.



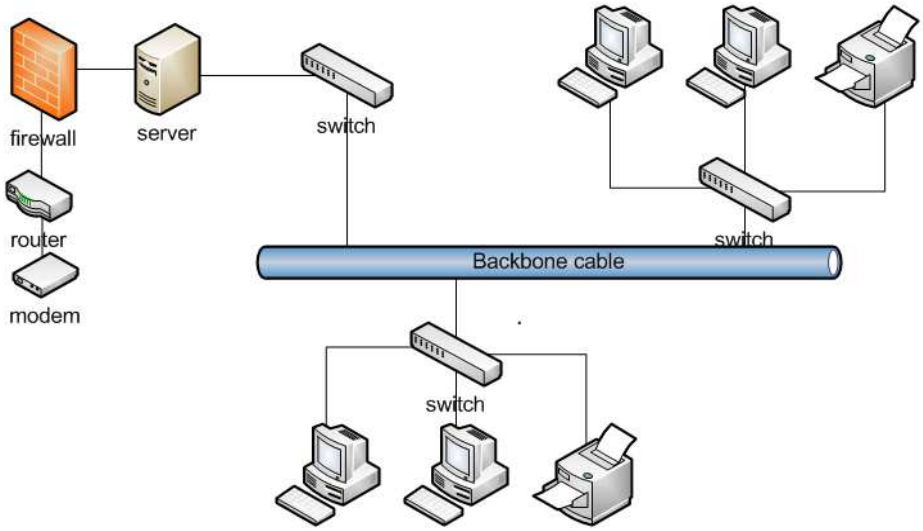
Gambar 3.1. Bagan Organisasi

3.2. Skema Jaringan Berjalan

Selama melakukan riset dan melakukan pengamatan di PT. Metalogix Infolink Persada.Penulis berhasil mendapatkan beberapa data dari jaringan berjalan di perusahaan ini. Namun tidak semua data yang penulis bisa dapatkan karena ada beberapa data yang bersifat *confidential* perusahaan.

3.2.1. Topologi Jaringan

Setelah melakukan riset di PT. Metalogix Infolink Persada, penulis dapat menyimpulkan bahwa topologi yang dipakai adalah topologi *tree*. Karena adanya penggunaan beberapa *switch* yang terhubung ke sebuah kabel *backbone* ke *server* utama.



Gambar 3.2. Topologi kantor XLink

3.2.2. Arsitektur Jaringan

Kantor pusat PT. Metalogix Infolink Persada menggunakan protokol TCP/IP. Protokol ini mencakup protokol DHCP, DNS, SMTP dan masih banyak lainnya.

Dalam pengalamatan IP nya di kantor ini menggunakan IPv4 dengan menggunakan DHCP server sebagai pusat layanan yang otomatis memberikan IP address ke perangkat pengguna dengan penggunaan kelas C dikarenakan jumlah komputer ataupun alat *network* lainnya masih dalam skala kecil saja.

Untuk keperluan *email* di PT. Metalogix Infolink Persada menggunakan Zimbra sebagai *web server* nya dengan penggunaan *port* SSL 443 dengan otentikasi *username* dan *password*. Penggunaan SSL dikarenakan lebih aman dibanding *port* standar *mail server* yaitu port 80.

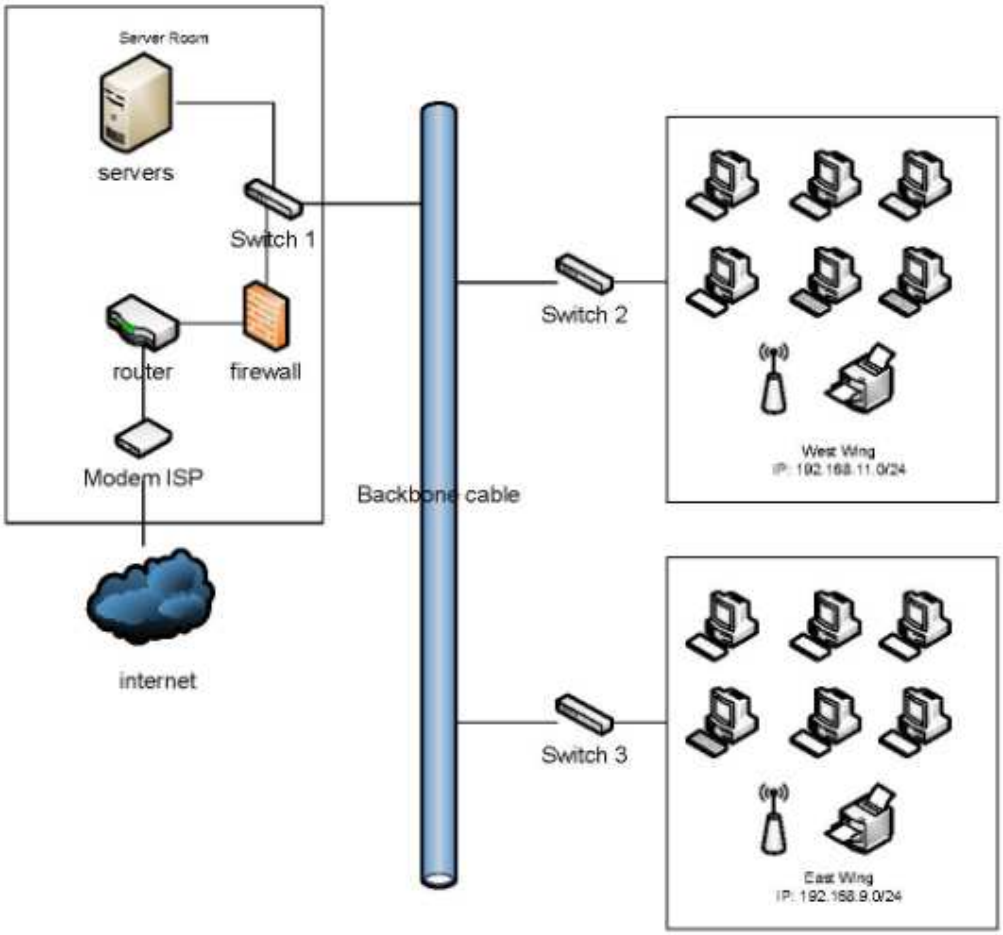
Model sistem yang digunakan adalah sistem *Client-Server*, sebuah aplikasi dibagi menjadi dua bagian yang terpisah, tetapi masih merupakan sebuah kesatuan yakni komponen klien dan komponen *server*.

Komponen klien juga sering disebut sebagai *front-end*, sementara komponen server disebut sebagai *back-end*. Komponen klien dari aplikasi tersebut dijalankan dalam sebuah *workstation* dan menerima masukan data dari pengguna.

Komponen klien tersebut akan menyiapkan data yang dimasukkan oleh pengguna dengan menggunakan teknologi pemrosesan tertentu dan mengirimkannya kepada komponen *server* yang dijalankan di atas mesin *server*, umumnya dalam bentuk *request* terhadap beberapa layanan yang dimiliki oleh *server*.

Komponen *server* akan menerima request dari klien, dan langsung memprosesnya dan mengembalikan hasil pemrosesan tersebut kepada klien. Klien pun menerima informasi hasil pemrosesan data yang dilakukan *server* dan menampilkannya kepada pengguna, dengan menggunakan aplikasi yang berinteraksi dengan pengguna.

3.2.3. Skema Jaringan



Gambar 3.3. Skema Jaringan Xlink

Dari skema diatas diketahui bahwa koneksi antar komputer terpusat pada *switch* yang terhubung ke *switch* lainnya melalui kabel *backbone*. *Switch* utama yaitu *switch* 1 pada gambar adalah *switch* yang berada pada ruangan *data center*. Pada *switch* tersebut terhubung *server-server* dan juga perangkat *firewall* dan *modem* juga *router*.

Server-server yang ada terdiri dari DHCP *server*, yaitu *server* yang tugasnya mendistribusikan *IP address* secara otomatis pada *host client* saat

menerima *request* untuk *IP* dari *host client* tersebut. Dan juga ada *FTP server* dimana *server* tersebut menyimpan file-file kantor.

Server-server tersebut terhubung ke *internet* melalui *router* yang menggunakan koneksi dari ISP dan juga perangkat *firewall* untuk menyaring data yang keluar masuk ke dalam dan keluar jaringan kantor.

3.2.4. Keamanan Jaringan

Untuk keamanan jaringan PT. Metalogix Infolink Persada menggunakan satu buah mesin *firewall* sebagi pintu pertama untuk mengontrol keluar-masuknya data dari luar jaringan kantor maupun internet.

Untuk keamanan di sisi perangkat seperti *personal computer*, s*erver* dan *notebook* menggunakan anti*virus Kaspersky Antivirus* untuk menangkal *virus*, *trojan* maupun *malware* yang dapat merusak sistem operasi maupun data-data penting yang ada.

3.2.5. Spesifikasi Hardware dan Software Jaringan

Tabel 3.1. Spesifikasi Perangkat Jaringan

Spesifikasi Hardware dan Software			
No	Perangkat	Hardware	Software
1	Server	HP Proliant DL180 - Processor: Intel Xeon (6 cores, 1.70 GHz, 15MB cache) - RAM: 3 x 8 GB DDR3 PC-12800	OS Windows 2008 Server R2 Antivirus Kaspersky 6.0 VMWare VSphere

		- HDD: 3 TB	Linux SUSE Enterprise
2	Switch	Cisco Catalyst 2900 series (24 port)	
3	Firewall	Cisco ASA 5500 series	
4	Router	Cisco router 1900 series	
5	Modem	Linksys AG-241	
6	Wireless Access Point	Cisco Aironet 3600 series	

3.3. Permasalahan Sistem Jaringan

Selama penulis melakukan riset di PT. Metalogix Infolink Persada ini hampir tidak pernah penulis menemukan masalah dalam sistem jaringannya. Hanya saja ada beberapa kendala yang sering ditemui oleh para *engineer* di lapangan saat ingin mendapatkan *update file* aplikasi klien dari kantor pusat. Saat ini yang sedang berjalan adalah penggunaan *email*, FTP dan aplikasi *chat* seperti *telegram* dan *whatsapp* sebagai sarana pengiriman data dari dalam ke luar kantor ataupun sebaliknya. Dengan metode ini penulis merasa kurangnya keamanan data yang dikirim karena melalui jaringan internet bebas yang dimana banyak celah keamanan yang bisa dimanfaatkan oleh pihak lain untuk mengambil data tersebut secara ilegal.

3.4. Alternatif Pemecahan Masalah

Untuk masalah yang sudah diuraikan pada sub-bab diatas, maka penulis mempunyai alternatif solusi yaitu penggunaan jalur VPN berbasis L2TP/IPsec yang penulis rasa dapat membantu menyelesaikan masalah diatas.

Keamanan penggunaan VPN adalah dengan membuat satu jalur *private* antara kantor pusat dengan komputer para e*ngineer* yang berada diluar kantor pusat yang melalui jaringan global (internet). VPN mengganti IP kantor yang dipakai menjadi IP *anonymous* saat melewati jaringan global dengan proses *encrypt* dan *decrypt* data dengan *IPSec* ataupun *key* dan dan juga autentikasi dengan *login*. Dengan demikian maka akan sulit bagi pihak yang tidak bertanggung-jawab di jaringan global yang bisa melacak ataupun mengambil data yang dikirim.