

Kajian Implementasi Jaringan Komputer *Wide Area Network* (WAN) pada PT. Adira Dinamika Multi *Finance*, Tbk di Jakarta

Mochamad Wahyudi, Ferry Lesmana
Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri
wahyudi@nusamandiri.ac.id
ferry@nusamandiri.ac.id

Abstract

PT. Adira Dinamika Multi Finance, Tbk which was established in 1990, is the biggest Automotive Finance Company in Indonesia. It has more than 214 branches across the country. To support the business operational needs, this company implements the following information systems : Ad1Sys (Core System), MS2 (a Surveyor Online system), Gapura (an online payment system), and custodian system. Whereas for its internal needs the company implements : Ad1Suites (an intranet system), Service Desk System (for handling information technology problems), Ad1Flow (a workflow system), and FAMS (an asset management system).

These information systems are connected through the company's computer Wide Area Network (WAN). This WAN is using Virtual Private Network (VPN) system, in which every branch office is connected to the head office through VPN technology.

This study is carried out through a direct observation at PT. Adira Dinamika Multi Finance for the purpose of getting more accurate data and identifying the core problem occurs in the implemented infrastructure of the company's information technology.

The type of VPN technology used in some branch offices of PT. Adira Dinamika Multi Finance is the VPN Dial. The core problems occur in the implemented infrastructure of the company's information technology are: the low speed rate in the online system of the branch office (pose) which disturbs costumer services, the frequent disconnected VPN Dial during PSTN's busy hours, the high cost VPN Dial connection, and the minimal need of mobile user due to Call Back/Remote Access Server (RAS) system.

Keywords: Wide Area Network (WAN), Virtual Private Network (VPN)

Pendahuluan

Wide Area Network (WAN) dipergunakan untuk menghubungkan jaringan-jaringan Local Area Network (LAN) satu dengan lainnya yang berdekatan maupun yang berjauhan dan menggunakan protokol yang sama atau berbeda-beda. Jika pada LAN hubungan jaringan komputer dapat dilakukan dengan perantara kabel-kabel milik internal perusahaan seperti : Kabel Koaksial, Kabel UTP / RJ-45, Serat Optik, dll, maka pada jaringan WAN pada umumnya jaringan komputer dihubungkan melalui jaringan milik perusahaan telekomunikasi sebagai media perantara. Perusahaan telekomunikasi di Indonesia yang menyediakan sambungan untuk WAN tersebut antara lain : PT.

Telekomunikasi Indonesia, PT. Indosat, PT. Lintas Arta, PT Excelcomindo Pratama (XL), dll. Menurut Wijaya (2004) ada beberapa teknologi yang dapat dipergunakan untuk dapat menghubungkan WAN, antara lain : Dial Up, Leased Line, VSAT, X.25, Frame Relay, Virtual Private Network (VPN), dll.

PT. Adira Dinamika Multi Finance, Tbk, berdiri sejak tahun 1990 dan merupakan perusahaan pembiayaan otomotif terbesar di Indonesia. PT. Adira Dinamika Multi Finance telah memiliki lebih dari 214 cabang yang tersebar diseluruh wilayah Indonesia. PT. Adira Dinamika Multi Finance adalah sebuah perusahaan pembiayaan konsumen yang pada saat ini

memfokuskan diri pada pembiayaan kendaraan (mobil dan sepeda motor), baik kendaraan baru maupun bekas. Dalam hal ini sepeda motor menyumbangkan pendapatan lebih besar pada PT. Adira Dinamika Multi *Finance* daripada mobil, yaitu dengan perbandingan 90:10.

Sistem Informasi pada PT. Adira Dinamika Multi *Finance* diklasifikasikan menjadi dua bagian, yaitu : sistem informasi yang digunakan untuk kebutuhan operasional bisnis PT. Adira Dinamika Multi *Finance* dan sistem informasi yang digunakan untuk kebutuhan internal perusahaan. Sistem informasi yang digunakan untuk kebutuhan bisnis antara lain sistem Ad1Sys (*Core System*), sistem MS2 (*Sistem Surveyor Online*), sistem Gapura (pembayaran *online*), sistem *custodian*, dll.

Sistem informasi yang digunakan untuk kebutuhan internal antara lain : sistem Ad1Suites (sistem *intranet*), sistem *Service Desk* (sistem penanganan masalah IT), sistem Ad1Flow (sistem *workflow*), sistem FAMS (sistem manajemen aset), dll.

Koneksi WAN pada PT. Adira Dinamika Multi *Finance* ini menggunakan sistem *Virtual Private Network* (VPN), dimana setiap kantor cabang terhubung ke kantor pusat menggunakan teknologi VPN, hanya saja sistem VPN yang digunakan pada beberapa kantor cabang menggunakan teknologi VPN *Dial*. Sistem komputerisasi yang ada mampu untuk melayani para nasabah atau pelanggan dalam bertransaksi. Untuk membuat sistem tersebut diperlukan sumber daya manusia dan infrastruktur teknologi informasi yang baik. Masalah kecepatan, keamanan data para pelanggan dan kemudahan dalam bertransaksi merupakan salah satu faktor yang sangat penting yang diinginkan oleh para pelanggan, sehingga kepuasan pelanggan atau konsumen terpenuhi. Sistem komputerisasi yang *online* tersebut membutuhkan koneksi realibel dan terus menerus antara kantor cabang dan kantor pusat PT. Adira Dinamika Multi *Finance* yang membutuhkan biaya koneksi yang cukup besar.

Tujuan penelitian ini adalah penulis ingin melakukan kajian yang mendalam tentang imlementasi jaringan komputer WAN pada PT. Adira Dinamika Multi *Finance*, agar penulis mendapatkan gambaran tentang penggunaan teknologi jaringan WAN yang diimplementasikan pada perusahaan pembiayaan otomotif terbesar di Indonesia. Dimana jaringan komputer yang terhubung pada PT. Adira Dinamika Multi *Finance*, yaitu menghubungkan lebih dari 214 kantor cabang yang tersebar diseluruh wilayah Indonesia (jaringan *enterprise*).

Metode Penelitian

Penulis melakukan pengamatan secara langsung (observasi) pada PT. Adira Dinamika Multi *Finance*. Hal ini penulis maksudkan untuk mendapatkan data-data yang akurat dan pokok permasalahan yang terjadi yang berkaitan dengan infrastruktur teknologi informasi yang digunakan. Penulis melakukan analisis terhadap masalah yang ada, kemudian penulis mencoba untuk mencari solusi pemecahan permasalahannya. Usulan dari penulis tentang perubahan terhadap infrastruktur yang ada, penulis lakukan analisa dan pengujian dengan menggunakan perangkat lunak (*software*) simulator yang dapat menggambarkan situasi yang sebenarnya terjadi pada PT. Adira Dinamika Multi *Finance*.

Tinjauan Pustaka

Dalam terminologi yang lebih sederhana, suatu VPN adalah perluasan dari sebuah *private internet* melalui *public network* (*internet*) untuk memastikan keamanan dan konektifitas yang hemat biaya antara koneksi. Perluasan *private internet* ini dibantu dengan *private logical "tunnel"*. *Tunnel* ini memungkinkan koneksi kedua pihak untuk menukar data melalui suatu cara yang menyerupai komunikasi *point-to-point*. Tujuan utama VPN adalah untuk memberikan kemampuan yang sama seperti *private leased line* dengan biaya yang lebih terjangkau menggunakan *infrastruktur public* (*internet*). Perusahaan telepon telah lama menyediakan suatu *resource khusus* untuk *private shares*. VPN membuat suatu *protected sharing* pada *resource pulic*.

1. **Authentication User dan Kendali Akses**

Authentication user dan kendali akses adalah dua langkah paling dasar yang dapat diambil untuk mencegah ancaman keamanan dan mengamankan data sensitif yang tersimpan dalam jaringan. Proses membuktikan identifikasi pemakai dikenal sebagai *authentication user*. Mengizinkan akses ke sumber daya jaringan tertentu selagi menolak akses ke yang lain dikenal sebagai kendali akses.

2. **Enkripsi Data**

Data encryption (cryptography) adalah satu komponen terpenting dalam keamanan VPN dan memegang peran utama dalam pengamanan data selama pemindahan. *Cryptography* adalah mekanisme pengubahan data ke dalam suatu format tak terbaca, yang dikenal sebagai *ciphertext*, sedemikian sehingga akses tidak sah kepada data dapat dicegah ketika data dipindahkan melalui suatu media transmisi yang tak aman.

Pengirim dan penerima bersama dengan proses enkripsi, membentuk suatu *cryptosystem*. Suatu *cryptosystem* digolongkan berdasarkan banyaknya kunci yang digunakannya. Suatu kunci dapat berupa suatu angka, kata, atau bahkan suatu ungkapan yang digunakan untuk kepentingan enkripsi dan dekripsi.

3. **Tunneling**

Tunneling merupakan suatu teknik pengenkapsulasian seluruh paket data. Aspek terpenting dari *tunneling* adalah paket data asli, atau disebut dengan *payload*, bisa merupakan protokol yang berbeda. Daripada mentransfer paket asli, yang bisa saja tidak dapat berjalan pada infrastruktur yang ada, pada *header* paket ditambahkan protokol yang kompatibel. *Header* ini berfungsi supaya paket bisa dikirimkan dengan baik melalui infrastruktur yang ada.

Ketika paket berjalan melalui *tunneling* menuju *node* tujuan, paket ini melalui suatu jalur, yang disebut *tunnel*. Setelah sampai, penerima mengembalikan paket ini ke *format* asal.

4. **Point-to-point Protocol (PPP)**

PPP adalah suatu protokol enkapsulasi yang memudahkan transportasi lalu lintas jaringan melalui penghubung *point-to-point serial*. Keuntungan PPP yang paling utama adalah bahwa PPP dapat beroperasi pada peralatan terminal data (DTE) yang manapun atau peralatan koneksi data (DCE) mencakup EIA/TIA-232-C dan ITU-T V.35. Point lain bahwa PPP membatasi transmisi *rate*. Selama transmisi, satu-satunya pembatasan *transmission-based* dikenakan oleh DCE/DTE yang merupakan penghubung digunakan (*interface*). Akhirnya, satu-satunya kebutuhan PPP adalah ketersediaan dari koneksi *duplex* (dua jalur), dimana baik sinkronisasi maupun tak sinkronisasi dan dapat beroperasi dalam suatu *switch* atau *dedicated mode*.

5. **Point-to-Point Tunneling Protocol (PPTP)**

PPTP adalah suatu solusi kepemilikan yang memungkinkan transfer data yang aman antar suatu *client* dan *server* perusahaan dengan cara menciptakan suatu VPN melalui suatu *internetwork* yang berbasis IP yang dikembangkan oleh konsorium PPTP, yaitu : Microsoft Corporation, Ascend Communications COM, US Robotics dan ECI Telematics. PPTP memfasilitasi permintaan transmisi VPNs melalui jaringan *internetwork* yang tidak aman. PPTP tidak hanya memfasilitasi transmisi yang aman melalui *internetwork public* yang berbasis TCP/IP, tetapi juga melalui *internet private*.

6. **Layer 2 Tunneling Protocol (L2TP)**

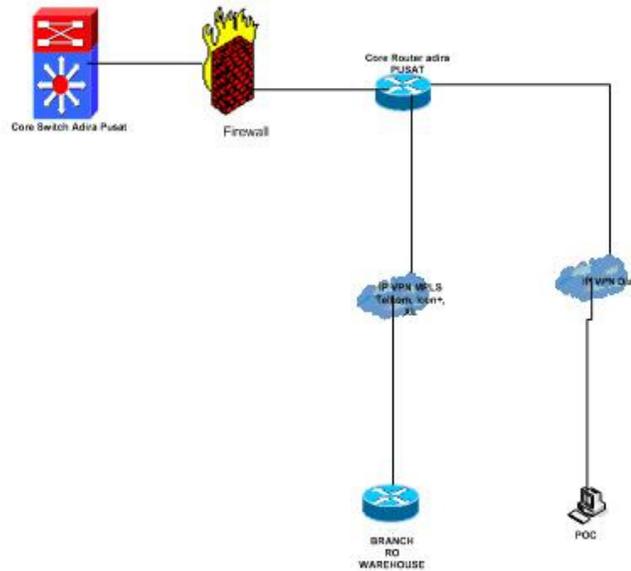
Dikembangkan oleh Cisco System, L2TP juga untuk menggantikan IPSec sebagai *tunneling*. Bagaimanapun, IPSec masih menjadi protokol yang dominan untuk menjamin komunikasi dalam internet. L2TP adalah suatu kombinasi layer 2 Forwarding (L2F) dan PPTP dan digunakan untuk encapsulated point-to-point (PPP) frame untuk dikirimkan melalui X.25, FR dan ATM network.

Hasil dan Pembahasan

Topologi jaringan yang digunakan pada PT. Adira Dinamika Multi Finance agar dapat berkomunikasi dengan kantor

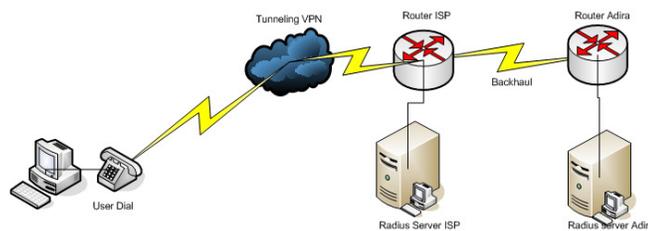
cabang, *Regional Office* (RO) ataupun dengan *Pose* (turunan dari RO), dimana setiap cabang atau RO telah menggunakan layanan VPN MPLS dari beberapa *Internet Service Provider* (ISP), seperti : Telkom, Icon+ (anak perusahaan PLN), XL dan ada juga yang menggunakan teknologi VSAT dari Sanatel, dengan *bandwith* yang beragam (tergantung dari kebutuhan dilokasi). Misalnya untuk cabang biasanya menggunakan 256 Kbps sampai dengan

512 Kbps, dan untuk *Regional Office* (RO) biasanya menggunakan *bandwith* 64 Kbps sampai dengan 128 Kbps, dan untuk Poc atau Pose sendiri hanya menggunakan layanan VPN *Dial* dengan otentikasi yang ada di *Server Radius* dengan mendaftarkan *user* yang akan menggunakan layanan VPN *Dial* ini, dengan kecepatan 56 Kbps (walaupun rata-ratanya adalah hanya 30 - 45 Kbps).



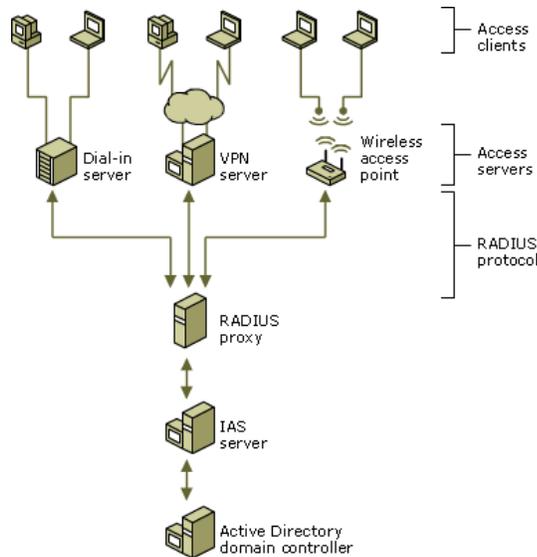
Sumber : PT. Adira Dinamika Multi *Finance*

Gambar 1. Topologi jaringan komputer pada PT. Adira Dinamika Multi *Finance*



Sumber : PT. Adira Dinamika Multi *Finance*

Gambar 2 . Topologi Jaringan VPN *Dial* pada PT. Adira Dinamika Multi *Finance*

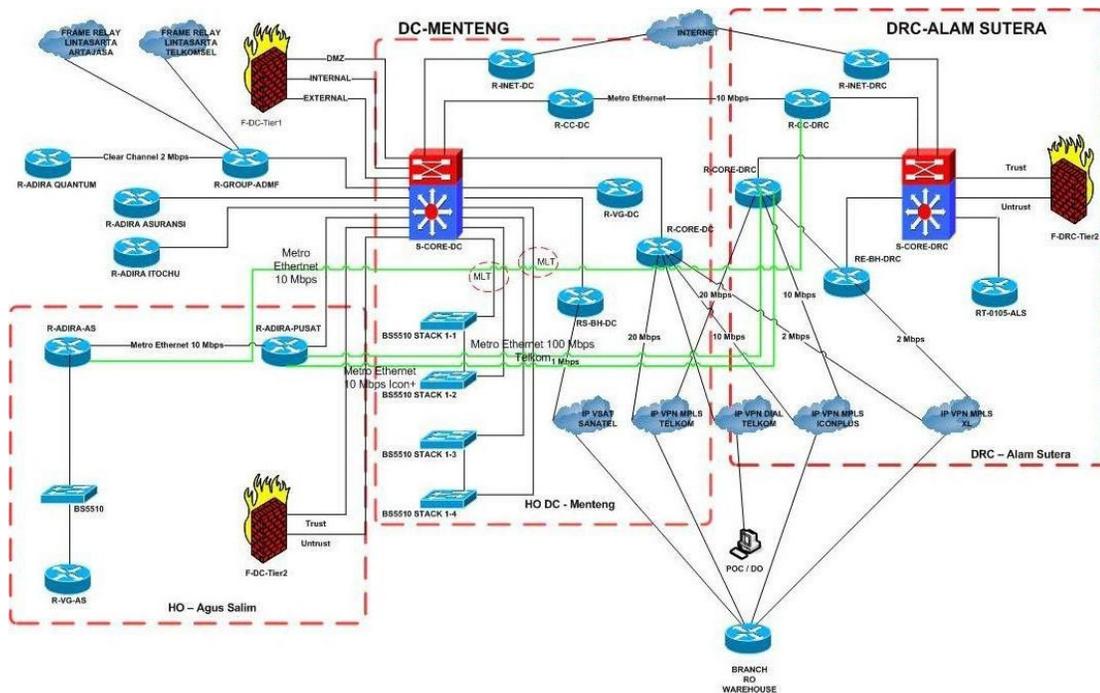


Sumber : PT. Adira Dinamika Multi Finance

Gambar 3. Akses VPN Dial pada PT. Adira Dinamika Multi Finance

Arsitektur jaringan yang digunakan pada PT. Adira Dinamika Multi Finance adalah sistem operasi jaringan model *Virtual Private Network* (VPN). Sistem operasi jaringan VPN memungkinkan *user/cabang* dapat mengakses tanpa batasan jarak dan

bisa mengakses sumber daya informasi yang terpusat, PT. Adira Dinamika Multi Finance juga menggunakan beberapa *Internet Service Provider* (ISP) yang digunakan untuk keperluan layanan VPN ini.



Sumber : PT. Adira Dinamika Multi Finance

Gambar 4. Skema Jaringan Komputer pada PT. Adira Dinamika Multi Finance

Sistem keamanan jaringan komputer yang diterapkan pada PT. Adira Dinamika Multi Finance saat ini sudah sangat bagus, karena kompleksitas sistem jaringan *enterprise*, membuat keamanan yang diterapkan benar-benar harus diperhitungkan dengan sangat detail. Pada kantor pusat atau *Data Centre* terdapat dua buah *firewall* yang mengatur akses ke dalam dan keluar sistem *intranet*, dimana untuk mengatur akses dari luar *segment server* tapi masih dalam lingkup *intranet*, PT. Adira Dinamika Multi Finance menggunakan firewall tipe Juniper ISG 2000 yang difungsikan untuk firewall Internal F-Tier2. Akses (*policy*) siapa saja yang berhak mengakses ke dalam ruang *Farm Server* atau ruang *Data Centre* dan juga terdapat di *Disaster Recovery Center* (DRC) yang terdapat di daerah Perumahan Alam Sutera Tangerang. Karena sifatnya modular, solusi ini memungkinkan untuk menambah keamanan *Gateway* dengan kemampuan *Intrusion Detection and Prevention* (IDP). Sedangkan untuk F-Tier1 atau *firewall* keseluruhan dimana akses yang diproses adalah untuk dari dalam dan luar jaringan menggunakan perangkat lunak (*software*) McAfee *Firewall Enterprise* (*Sidewinder*) 1100 dimana *level* aplikasi

yang banyak dan protokol paling umum digunakan.

Core Router yang digunakan juga menggunakan produk dari Juniper series M-10i yang telah diakui kehandalannya dimana *router* ini menangani semua *link* dari setiap *provider* dan melakukan *routing* dengan sempurna. Pada sisi *Core Switch*-pun PT. Adira Dinamika Multi Finance mempercayakan kepada merk Nortel Series 8306, karena menawarkan keamanan yang ramah dan memastikan bahwa *future* ini juga akan dimaksimalkan untuk *wiring*, dengan kinerja yang terdapat pada Layer-2 dan Layer-3 serta standarisasi berbasis *Power-of-Ethernet*. Dengan jumlah 68 *port per chassis* dan kecepatan 10 GB, standar berbasis otomatis media QoS pengaturan *Virtual Local Area Network* (VLAN) dapat mengurangi *Total Cost of Ownership* (TCO).

Perangkat keras (*hardware*) utama yang berhubungan langsung antara kantor pusat dengan koneksi setiap kantor pada PT. Adira Dinamika Multi Finance, seperti : *Router, Firewall, Core Switch* dan *Switch* dapat dilihat pada tabel berikut :

Tabel 1. Perangkat Keras (*hardware*) Utama

Nama Perangkat	Spesifikasi Perangkat	Keterangan
<i>Firewall F-Tier1</i>	<i>Dual Power Supply, RAID 1, Fiber Interface 4, Copper Interface (base/max) 8/14 - GB</i>	McAfee <i>Firewall Enterprise</i> (<i>sidewinder</i> 1100)
<i>Core Router</i>	<i>FPC Slots and Full Duplex Throughput per slot 2 built-in 4 Gbps, Redundancy, PICs per chassis 8</i>	Merk Juniper M10i
<i>Firewall F-Tier2</i>	<i>Number of Interface Up to 16 mini GBIC up to 10/100/1000, or up to 4 10GE, maximum VPN Tunnels 10.000</i>	Merk Juniper ISG 2000
<i>Core Switch</i>	<i>Class-leading 10 G Ethernet Port Density - up to 68 Ports per Chassis, High performance - up to 464Gbps switching capacity & 928Gbps per Switch Cluster</i>	Merk Nortel P 8306
<i>Router</i>	<i>2 fastethernet, 1 ethernet, 1 V35 dan 1 voip card</i>	Merk Maipu 2600 dan 1700E

Sumber : PT. Adira Dinamika Multi Finance

Perangkat lunak (*software*) yang akan digunakan dalam mengkonfigurasi dan monitoring koneksi jaringan yang digunakan, dimana untuk *operating system*

pada setiap komputer menggunakan Microsoft Windows XP Service Pack 2, Windows Server 2003, JunOS yang digunakan pada *router* yang berbasiskan

Juniper, dan untuk perangkat *monitoring* menggunakan *tools* dari CA *Transforming IT Management Spectrum One Click*, *Symantec Endpoint*, *Secure CRT* untuk akses Telnet dan SSH, *Paessler Router Traffic Grapher (PRTG)*, *IP Scanner* dan *Calc IP Subnetting*, *Network Vantage* dan *Steel Belted Radius (SBR) Enterprise Edition*.

Permasalahan yang terjadi dan berkaitan dengan infrastruktur teknologi Informasi pada PT. Adira Dinamika Multi *Finance* berdasarkan hasil pengamatan penulis antara lain :

1. Lambatnya sistem *online* pada kantor anak cabang (*pose*) yang menggunakan koneksi VPN *Dial*, sehingga mengganggu kenyamanan dalam pelayanan nasabah.
2. Sering terputusnya koneksi VPN *Dial* apabila koneksi layanan PSTN sedang sibuk atau penuh.
3. Mahalnya biaya koneksi VPN *Dial* yang dipergunakan pada setiap jam kerja (*office hour*) dan ditambah lagi dengan pemakaiannya yang lebih dari delapan jam dalam satu hari.
4. Kebutuhan *user mobile* yang tidak maksimal karena menggunakan sistem *Call Back/Remote Access Server (RAS)*.

VPN *Instant* adalah salah satu solusi bagi pelanggan korporasi yang memerlukan solusi akses ke dalam *resource* jaringan *private* milik perusahaan melalui media *internet* secara aman dan mudah. Akses ke *resource* jaringan *private*, akses ke *e-mail*, *web portal* internal suatu korporasi. Akses ke *data/database* yang tersimpan di dalam *server* internal suatu

perusahaan, baik dalam bentuk *FTP Server*, *File Sharing*, dll. Akses ke fasilitas komunikasi suatu korporasi, misalnya : IP PABX/VoIP, *Web Meeting*, dll. Akses kontrol ke suatu perangkat di internal suatu perusahaan.

VPN *Instant* memungkinkan pelanggan korporasi untuk dapat melakukan akses ke sumber daya sistem informasinya yang bersifat *private network/intranet* dan menggunakan VPN IP, melalui media *internet* secara aman dan mudah. Sistem koneksi dan keamanan yang digunakan adalah protokol keamanan *internet Secure Socket Layer (SSL)*. Kemudahan akses ke jaringan *private* melalui *internet* secara aman, melalui *interface* berbasis web (*secure*), yang telah umum dikenal oleh pelanggan. Memiliki fleksibilitas jarak (*coverage*) akses layanan secara nasional, bahkan global melalui media *internet*. Koneksi *internet* yang dipergunakan juga bisa bermacam-macam, seperti layanan *internet* dari PT. Telekomunikasi Indonesia (Telkom) dengan produk-produknya seperti : Telkom *Speedy*, Telkomnet *Instant*, Telkom *Hotspot*, dll maupun melalui layanan *internet* dari *provider* lain.

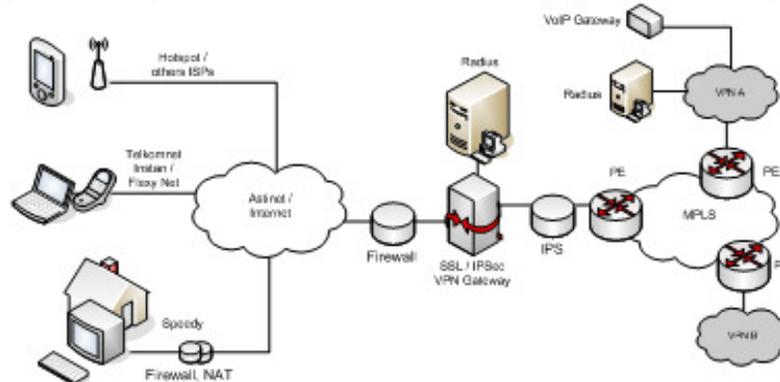
Perusahaan tidak perlu membangun sendiri kebutuhan akan *portal* ke *internet*, sehingga dapat meringankan biaya investasi perangkat dan biaya untuk perawatan perangkat. Investasi yang minimal pada sisi *remote site/telecommuter*, yaitu memanfaatkan perangkat komputer yang sudah ada pada sisi pelanggan. Baik menggunakan sistem operasi berbasis Microsoft Windows, Linux maupun Apple Macintosh.

Tabel 2. Komparasi produk yang digunakan oleh PT. Adira Dinamika Multi *Finance* saat ini sekarang dari Telkom

No	Item	Produk		
		VPN IP	VPN Dial	VPN Instant
1	Tarif	Fixed Abodemen/Site	Fixed Abodement Backhoul + Port + Domain + Usage Access	Fixed Abodement Port + Usage Access
2	Kecepatan	Fixed	Tergantung kecepatan akses Dial Up dan Bandwidth Backhoul	Tergantung kecepatan akses ke Internet dan Bandwidth Backhoul
3	CPE	Router	Komputer atau Router	Komputer atau Mobile Device
4	Media Akses	Leased Line atau SDLAM	PSTN/CDMA (Telkom Flexi)	Semua media akses ke Internet
5	Kebutuhan Akses	Dedicated	On Demand	On Demand
6	Topologi Jaringan	Antar Cabang	Antar Cabang atau Single Client ke Kantor Cabang	Single Client ke Kantor Cabang

Berikut ini adalah topologi jaringan yang penulis usulkan untuk dapat dipergunakan pada PT. Adira Dinamika Multi *Finance* untuk menggantikan layanan VPN *Dial*

yang saat di gunakan. Hal ini dimaksudkan agar permasalahan dengan infrastruktur teknologi Informasi pada PT. Adira Dinamika Multi *Finance* dapat diatasi.



Gambar 5. Topologi Jaringan Usulan

Usulan topologi jaringan ini tidak akan melakukan perubahan pada inti dari infrastruktur teknologi informasi yang ada pada PT. Adira Dinamika Multi *Finance*. Penulis mengusulkan untuk tetap memanfaatkan semua infrastruktur yang ada pada PT. Adira Dinamika Multi *Finance* dan penulis hanya menggantikan jenis koneksi yang digunakan saat ini dari VPN *Dial* menjadi VPN *Instant*.

Instant untuk menggantikan VPN *Dial* tidak membutuhkan penambahan penggantian *hardware* yang ada. Infrastruktur yang ada hanya tinggal dikonfigurasi sedikit untuk melakukan penyesuaian dengan perubahan yang ada. *User* dapat menggunakan dari media koneksi *internet* apa saja untuk dapat terkoneksi ke kantor pusat. Misalnya : 3G Broadband, ADSL, GPRS, dll. Hal ini disebabkan karena PT. Adira Dinamika Multi *Finance* telah mempunyai *backhaul* dari PT. Telekomunikasi Indonesia, Tbk yang dapat dipergunakan untuk akses VPN *Dial* sebesar 256 Kbps, jadi hanya dikenakan untuk biaya sewa *port* dimana kelipatan dari 10 port untuk penggunaan 10 user.

Pada sisi keamanan jaringan yang ada pada PT. Adira Dinamika Multi *Finance*, penulis juga tidak melakukan perubahan terhadap sistem yang telah dimiliki. Mengingat sistem keamanan jaringan yang telah ada sudah sangat baik, yaitu dengan menggunakan dua buah firewall yang diintegrasikan untuk akses internal dan eksternal dengan pembatasan pada Layer-1 (Tier1) McAfee *Firewall Enterprise* (sidewinder 1100) dan Layer-2 (Tier 2) merk Juniper ISG 2000 serta manajemen jaringan menggunakan Core Switch terdistribusi dengan *Multi Layer* merk Nortel P 8306, sehingga membuat stabilitas dan keamanan jaringan yang cukup handal dengan pemberian VLAN ID setiap *port*-nya dan beberapa fungsi *Network Address Translation* (NAT).

Untuk melakukan pemantauan terhadap jaringan komputer yang dimiliki oleh PT. Adira Dinamika Multi *Finance*, *network administrator* dan *network operator* menggunakan *software Paessler Router Traffic Grapher* (PRTG), dimana sistem operasinya menggunakan Microsoft Windows XP Service Pack 2, Microsoft Office 2007, dan beberapa software tambahan yang digunakan, seperti : *Secure CRT*, *Network Vantage* dan *Steel Belted Radius* (SBR) *Enterprise Edition*.

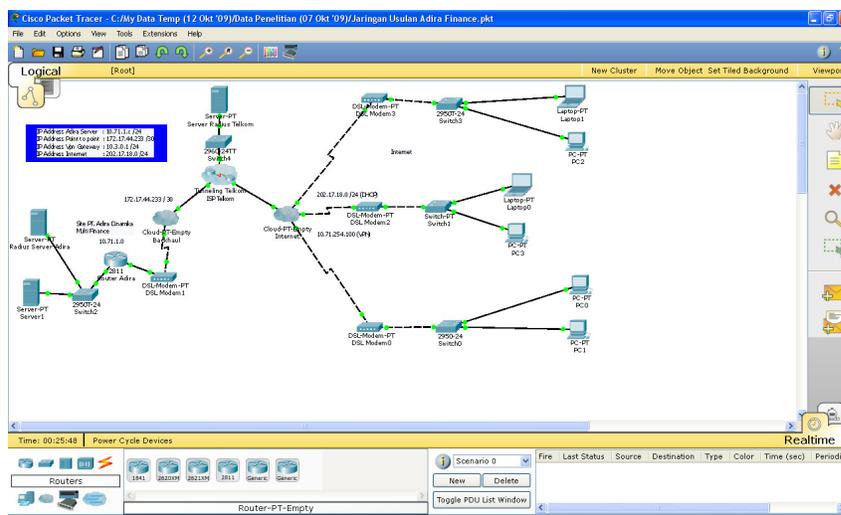
Pada sisi perangkat keras (*hardware*), yang ada pada PT. Adira Dinamika Multi *Finance*, penulis juga tidak melakukan perubahan pada sisi *hardware* yang ada. Implementasi menggunakan layanan VPN

Sehubungan dengan adanya kendala dalam implementasi usulan dari penulis apabila langsung diterapkan pada sistem jaringan yang ada, pada penelitian ini penulis mencoba untuk menggambarkan

usulan penulis dalam bentuk simulasi implementasi jaringan usulan tersebut menggunakan *software* simulator untuk menimplementasikan jaringan komputer. *Software* yang penulis gunakan adalah *Cisco Packet Tracer versi 5.2.0.0068* keluaran dari Cisco, Inc.

Penulis memberikan gambaran koneksi yang digunakan untuk mengimplementasikan jaringan usulan tersebut menggunakan *software Cisco Packet Tracer*. Penulis menggunakan *software* simulator ini dikarenakan adanya keterbatasan *software* diluar produk Cisco,

dimana pada PT. Adira Dinamika Multi *Finance Core Router* yang digunakan adalah merk Juniper M10i yang memiliki sistem operasi JunOS. Meskipun demikian konsep yang ada tidak mengalami perubahan, hanya *router* saja yang berbeda. *Router* yang seharusnya dipergunakan yang seharusnya produk Juniper, sedangkan untuk keperluan simulasi usulan penulis untuk implementasi jaringan usulan pada PT. Adira Dinamika Multi *Finance* penulis menggunakan *router* produk Cisco. Adapun konfigurasi jaringan usulan menggunakan *software* simulator dapat dilihat pada gambar berikut :



Gambar 6. Usulan Topologi VPN Instant PT. Adira Dinamika Multi *Finance*

Konfigurasi pada *Core Router* sesungguhnya tidak ada perubahan yang terlalu banyak hanya perlu mengganti dengan *IP Address point-to-point* yang diberikan pengganti *IP Address point-to-point VPN Dial*. Pada sisi *Radius Server*, *user* yang akan mengakses VPN harus didaftarkan terlebih dahulu.

Apabila *user* yang terdaftar atau *user* yang berhak telah terkoneksi ke *internet*, maka *user* tersebut dapat mengakses alamat <http://www.telkomvpn.com> untuk masuk ke jaringan milik PT. Adira Dinamika Multi *Finance* (VPN) dengan memasukan *user name* dan *password* dimana *user name* dan *password* tersebut akan diperiksa oleh *Radius Server*.

Kesimpulan

PT. Adira Dinamika Multi *Finance* memiliki sistem informasi yang dibagi menjadi dua bagian, yaitu : digunakan untuk kebutuhan operasional bisnis dan untuk kebutuhan internal perusahaan. Sistem informasi yang digunakan untuk kebutuhan bisnis antara lain : sistem Ad1Sys (*Core System*), sistem MS2 (*Sistem Surveyor Online*), sistem Gapura (pembayaran *online*), sistem *custodian*, dll. Sedangkan yang digunakan untuk kebutuhan internal antara lain : sistem Ad1Suites (sistem *intranet*), sistem *Service Desk* (sistem penanganan masalah IT), sistem Ad1Flow (sistem *workflow*), sistem FAMS (sistem manajemen aset), dll. Sistem informasi tersebut terkoneksi dengan jaringan komputer WAN milik PT. Adira Dinamika Multi *Finance* menggunakan sistem VPN, dimana setiap

kantor cabang terhubung ke kantor pusat menggunakan teknologi VPN.

Tujuan penelitian ini adalah penulis ingin melakukan kajian yang mendalam tentang implementasi jaringan komputer WAN pada PT. Adira Dinamika Multi Finance, agar penulis mendapatkan gambaran tentang penggunaan teknologi jaringan WAN menghubungkan lebih dari 214 kantor cabang yang tersebar diseluruh wilayah Indonesia (jaringan *enterprise*).

Penulis melakukan pengamatan secara langsung (observasi) pada PT. Adira Dinamika Multi Finance untuk mendapatkan data-data yang akurat dan pokok permasalahan yang terjadi yang berkaitan dengan infrastruktur teknologi informasi yang digunakan.

Teknologi VPN yang digunakan pada beberapa kantor cabang PT. Adira Dinamika Multi Finance menggunakan teknologi VPN *Dial*. Permasalahan yang terjadi dan berkaitan dengan infrastruktur teknologi Informasi pada PT. Adira Dinamika Multi Finance berdasarkan hasil pengamatan penulis antara lain : lambatnya sistem *online* pada kantor anak cabang (*pose*) yang menggunakan koneksi VPN *Dial*, sering terputusnya koneksi VPN *Dial* apabila koneksi layanan PSTN sedang sibuk atau penuh, mahalnya biaya koneksi VPN *Dial* adanya kebutuhan *user mobile* yang tidak maksimal karena menggunakan sistem *Call Back/Remote Access Server* (RAS).

Berdasarkan hasil pengamatan yang penulis lakukan pada PT. Adira Dinamika Multi Finance, mengusulkan untuk melakukan perubahan terhadap infrastruktur teknologi informasi yang saat ini digunakan yang pada awalnya untuk menghubungkan kantor pusat dengan beberapa kantor cabang menggunakan teknologi VPN *Dial*, penulis usulkan untuk menggunakan teknologi VPN *Instant*. Usulan ini tidak akan melakukan perubahan pada inti dari infrastruktur teknologi informasi yang ada pada PT. Adira Dinamika Multi Finance, baik dari sisi keamanan data maupun *software* yang digunakan. Penulis mengusulkan untuk

tetap memanfaatkan semua infrastruktur yang ada pada PT. Adira Dinamika Multi Finance dan penulis hanya menggantikan jenis koneksi yang digunakan saat ini dari VPN *Dial* menjadi VPN *Instant* saja.

Daftar Pustaka

- Brenton, Chris. 2005. Network Security. Jakarta : PT. Elek Media Komputindo.
- Cisco. Configuring IPSec Between Hub and Remote PIXes with VPN Client and Extended Authentication. Diambil dari : http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_exam ple09186a0080094cea.shtml. (12 Oktober 2009)
- Lammle, Todd. 2005. Cisco Certified Network Associate. Jakarta : PT. Elek Media Komputindo.
- Rafiudin, Rahmat. 2006. Membangun Firewall dan Traffic Filtering Berbasis Cisco. Yogyakarta : Penerbit Andi.
- Telkom. 2007. Solusi Enterprise - IP Virtual Network. Diambil dari : <http://www.telkom.co.id/produk-layanan/korporat/data-internet/solusi-enterprise-ip-virtual-network.html>. (30 Januari 2007)
- VPN Consortium. 2009. VPN Technologies: Definitions and Requirements. Diambil dari : <http://www.vpnc.org/vpn-technologies.html>. (12 Oktober 2009)
- W. Purbo, Onno. 2001. TCP/IP Standar Desain dan Implementasinya. Jakarta : PT. Elek Media Komputindo.
- Wijaya, Hendra. Ir. 2004. Belajar Sendiri Cisco Router. Edisi Baru untuk mengambil Sertifikat CCNA (640-801). Jakarta : PT. Elek Media Komputindo.
- _____. Ir. 2006. Belajar Sendiri Cisco ADSL Router, PIX Firewall dan VPN. Jakarta : PT. Elek Media Komputindo.