

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
PALCOMTECH PALEMBANG

SKRIPSI

DESAIN DAN IMPLEMENTASI SITE TO SITE VPN MENGGUNAKAN
VYATTA DI PT. SARANA PEMBANGUNAN PALEMBANG JAYA



Oleh :

SYAFRUDIN
NPM. 011080010

Untuk Memenuhi Sebagian Dari Syarat-Syarat
Guna Mencapai Gelar Sarjana Komputer

PALEMBANG

2012

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
PALCOMTECH PALEMBANG

HALAMAN PENGESAHAN PEMBIMBING

Nama : SYAFRUDIN
Nomor Pokok : 011080010
Program Studi : Teknik Informatika
Jenjang Pendidikan : Strata Satu (S1)
Konsentrasi : Pengantar Jaringan Komputer
Judul : Desain dan Implementasi Site to Site VPN
menggunakan Vyatta di PT. Sarana
Pembangunan Palembang Jaya

Palembang, Agustus 2012

Mengetahui ,
Pembimbing

Menyetujui,
Ketua

Adelin, S.T.
NIDN : 0211127901

Rudi Sutomo, S.Kom., M.Si
NIP.028.PCT.08

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
PALCOMTECH PALEMBANG

HALAMAN PENGESAHAN PENGUJI

Nama : SYAFRUDIN
Nomor Pokok : 011080010
Program Studi : Teknik Informatika
Jenjang Pendidikan : Strata Satu (S1)
Konsentrasi : Pengantar Jaringan Komputer
Judul : Desain dan Implementasi Site to Site VPN
menggunakan Vyatta di PT. Sarana
Pembangunan Palembang Jaya

Penguji Skripsi

Tanggal : 18 September 2012 **Tanggal** : 18 September 2012
Penguji 1 : **Penguji 2** :

Febrianty, SE, M.Si
NIDN : 0013028001

Rudi Sutomo, S.Kom.,M.Si
NIDN : 0222057501

Disetujui Oleh,
Ketua

Rudi Sutomo, S.Kom.,M.Si
NIP. 028.PCT.08

Motto

- ✓ **“Jangan dipikirke be, tapi digaweke”. (Bila menghadapi suatu masalah jangan hanya dipikirkan saja, tetapi dikerjakan agar mendapatkan solusi untuk memecahkan masalah.**
- ✓ **Tiada doa yang lebih indah selain doa agar skripsi ini cepat selesai**
- ✓ **Pelajarilah ilmu yang kalian kehendaki, demi Allah kalian tidak akan mendapat pahala karena berhasil mengumpulkan ilmu sebelum kalian mengamalkannya . (Riwayat Abdul Hasan Ibnul Akhzam Melalui Anas, R.A)**
- ✓ **Jika engkau lunak terhadap dirimu maka hidup akan kejam terhadapmu, tetapi apa bila engkau kejam terhadap dirimu maka hidup akan lunak terhadapmu .**

Kupersembahkan Kepada :

- ✓ **Kedua Orang Tuaku tercinta atas doa dan dukungannya**
- ✓ **Sahabat seperjuangan skripsi Mudrika, Suherman, Nanda, Ibnu, Reska, Ari , Yoga dan lain-lain)**
- ✓ **Iwan Agusti, Awaludin dan Tri Handayani**
- ✓ **Sahabat-sahabat semuanya atas doa dan dukungannya.**
- ✓ **Keluargabesarku**
- ✓ **Almamaterku**

KATA PENGANTAR

Puji Syukur kepada Allah SWT, karena berkat karunia-Nya Penulis dapat menyelesaikan laporan Skripsi ini. Laporan Skripsi ini berjudul ” Desain dan Implementasi site to site Virtual Private Network (VPN) Menggunakan Vyatta pada PT. Sarana Pembangunan Palembang Jaya”. Adapun tujuan dari penulisan Skripsi untuk memenuhi syarat guna menyelesaikan Strata 1.

Ucapan terima kasih Penulis tujukan kepada Bapak Rudi Sutomo,S.Kom.,M.Si selaku Ketua STMIK Palcomtech, Bapak D. Tri Octavian selaku Ketua Program Studi Teknik Informatika, serta Bapak Yudi Wiharto, S.Kom selaku pembimbing Skripsi ini. Tidak lupa saya ucapan terima kasih penulis sampaikan juga Bapak Hendri selaku Ketua Yayasan Pendidikan PalComTech, selain itu juga penulis ucapkan terima kasih kepada Bapak Bahder Johan selaku direktur PT.SP2J dan Bapak Aries Rachmansyah selaku manager Unit Usaha BRT Trans Musi. Selaku Direktur PT Sarana Pembangunann Palembang Jaya yang telah memberikan izin kepada penulis untuk melakukan riset di kantor PT. Sarana Pembangunan Palembang Jaya dengan Unit Usaha BRT Trans Musi, serta kepada orang tuaku yang selalu mendoakan dan memberikan dukungan serta semua pihak yang telah membantu dan mendukung hingga terselesaikannya Laporan ini.Semoga Allah SWT memberikan berkah atas amal dan perbuatannya.

Kritik dan saran yang membantu dari semua pihak akan penulis terima dengan tangan terbuka demi kesempurnaan Skripsi ini. Penulis berharap mudah – mudahan Skripsi ini dapat berguna bagi kita semua.

Palembang, Agustus 2012

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN PEMBIMBING	ii
HALAMAN PENGUJI.....	iii
ABSTRAK	iv
HALAMAN MOTTO DAN PERSEMBAHAN.....	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	xii
DAFTAR TABEL	xvii
	B
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	4
1.6 Sistematika Penulisan.....	4
	B
BAB II GAMBARAN UMUM PERUSAHAAN	6
2.1 Profil Perusahaan.....	6
2.1.1. Sejarah Perusahaan.....	7
2.1.2. Visi dan Misi	8
2.2 Stuktur Organisasi	8
2.3 Tugas dan Wewenang.....	8
A. Manager	9
B. Assisten Manager Pool.....	9
C. Assisten Manager Administrasi dan Umum	10
D. Assisten Manager Operasional.....	11
E. Assisten Manager ASSIE dan IT.....	11

BAB III TINJAUAN PUSTAKA	12
3.1 Teori Pendukung	12
3.1.1 Jaringan Komputer	12
3.1.2 VPN (<i>Virtual Private Network</i>).....	16
3.1.2.1 Konsep KerjaVPN.....	17
3.1.2.2 Implementasi VPN.....	19
3.1.2.3 Protokol Tunneling utama VPN.....	21
3.1.3 Vyatta.....	24
3.1.4 LAN (<i>Local Area Network</i>).....	26
3.1.5 Model OSI.....	26
3.1.6 <i>Domain Name System</i> (DNS)	30
3.1.6.1 Sejarah Singkat DNS.....	30
3.1.6.2 Struktur DNS.....	31
3.1.6.2 Teori bekerja DNS.....	34
3.1.7 IP Addresss.....	34
3.1.7.1 Kelas-kelas IP Addresss.....	35
3.1.8 Komponen yang Dibutuhkan Jaringan Komputer LAN	37
3.2 Hasil Penelitian Terdahulu	38
BAB IV METODE PENELITIAN	44
4.1 Lokasi dan Waktu Penelitian.....	44
4.1.1 Lokasi.....	44
4.1.2 Waktu	44
4.2 Jenis Data	44
4.1.3 Data Primer	44
4.1.4 Data Sekunder	45
4.2 Teknik Pengumpulan Data	45
1. Metode pengematann (<i>Observation</i>).....	45
2. Metode Wawancara (<i>Interview</i>)	45
3. Metode Pustaka (<i>Study Literature</i>)	46
4.4 Jenis Penelitian	46
4.5 Teknik Pengembang Sistem	48
BAB V Hasil dan Pembahasan	53
5.1 Hasil.....	53
5.1.1 Topologi Jaringan	53

5.1.2	Spesifikasi Komputer.....	56
5.1.3	Desain Topologi.....	57
5.1.4	Spesifikasi Komputer Server	57
5.1.5	Konfigurasi Router 1.....	58
5.1.6	Setting Host Name dan IP Address.....	58
5.1.7	Cek Interface.....	60
5.1.8	Setting Interface IPSec.....	61
5.1.9	Setting IKE Group dan Proposal.....	61
5.1.10	Setting ESP Group dan Proposal	63
5.1.11	Setting IPSec Site to Site	64
5.1.12	Konfigurasi Router 2.....	69
5.1.13	Setting Host Name dan IP Address.....	69
5.1.14	Cek Interface.....	71
5.1.15	Setting Interface IPSec.....	71
5.1.16	Setting IKE Group dan Proposal.....	72
5.1.17	Setting ESP Group dan Proposal	74
5.1.18	Setting IPSec Site to Site	75
5.1.19	Hasil Koneksi Router 1	80
5.1.20	Hasil Koneksi Router 2.....	84
BAB VI	Simpulan dan Saran.....	88
6.1	Simpulan.....	88
6.2	Saran.....	88

DAFTAR PUSTAKA

DAFTAR GAMBAR

Gambar 2.1	Struktur Oganisasi Unit Usaha BRT Trans Musi.....	8
Gambar 3.1	Topologi <i>Bus</i>	10
Gambar 3.2	Topologi <i>Ring</i>	14
Gambar 3.3	Topologi <i>Bintang</i>	15
Gambar 3.4	Topologi <i>Tree</i>	16
Gambar 3.5	Konsep Kerja VPN.....	17
Gambar 3.6	Lapisan <i>Open Sistem Interconection (OSI)</i>	27
Gambar 3.7	Struktur DNS	32
Gambar 4.1	NDLC	48
Gambar 5.1	Topologi Jaringan PT. SP2J Sebelumnya	53
Gambar 5.2	Topologi Jaringan PT. SP2J Sesudahnya	54
Gambar 5.3	Topologi Jaringan Unit Usaha Trans Musi Sebelumnya.....	55
Gambar 5.4	Topologi Jaringan Unit Usaha Trans Musi Sesudahnya	56
Gambar 5.5	Desain Topologi Jaringan VPN Server	57
Gambar 5.6	Tampilan Perintah Masuk Ke konsol Vyatta Router 1	58
Gambar 5.7	Tampilan Perintah Configure	58
Gambar 5.8	Tampilan Perintah Setting Host-Name.....	59
Gambar 5.9	Tampilan Perintah Setting IP pada eth0	59
Gambar 5.10	Tampilan Perintah Setting IP pada eth1	59
Gambar 5.11	Tampilan Perintah commit	59
Gambar 5.12	Tampilan Perintah save	59
Gambar 5.13	Tampilan Perintah Untuk Melihat IP Address	60
Gambar 5.14	Tampilan Perintah Setting IPSec pada eth1	61
Gambar 5.15	Tampilan Perintah ipsec-interfaces	61
Gambar 5.16	Tampilan Perintah ike-group proposal router 1.....	61
Gambar 5.17	Tampilan Perintah encryption pada ike-group	62
Gambar 5.18	Tampilan Perintah Setting dh-group 2	62

Gambar 5.19	Tampilan Perintah Show ike-group router1	63
Gambar 5.20	Tampilan Perintah esp-group proposal router1	63
Gambar 5.21	Tampilan Perintah encryption pada esp-group.....	63
Gambar 5.22	Tampilan Perintah Show esp-group	64
Gambar 5.23	Tampilan perintah Site to Site	64
Gambar 5.24	Tampilan Setting authentication.....	65
Gambar 5.25	Tampilan Perintah vpn ipsec site to site	65
Gambar 5.26	Tampilan Perintah set authentication pre-shared-secret.....	65
Gambar 5.27	Tampilan perintah set ike-group router 1	66
Gambar 5.28	Tampilan perintah set local-ip	66
Gambar 5.29	Tampilan perintah set tunnel 1 local-subnet.....	66
Gambar 5.30	Tampilan perintah set tunnel 1 remote-subnet	66
Gambar 5.31	Tampilan perintah set tunnel 1 esp-group Router 1	67
Gambar 5.32	Tampilan perintah commit	67
Gambar 5.33	Tampilan Perintah save	67
Gambar 5.34	Tampilan perintah show vpn ipsec site-to-site peer	68
Gambar 5.35	Tampilan Perintah Masuk Ke konsol Vyatta Router 2.....	69
Gambar 5.36	Tampilan Perintah Configure	69
Gambar 5.37	Tampilan Perintah Setting Host-Name.....	69
Gambar 5.38	Tampilan Perintah Setting IP pada eth0	70
Gambar 5.39	Tampilan Perintah Setting IP pada eth1	70
Gambar 5.40	Tampilan Perintah commit	70
Gambar 5.41	Tampilan Perintah save	70
Gambar 5.42	Tampilan Perintah Untuk Melihat IP Address	71
Gambar 5.43	Tampilan Perintah Setting IPSec pada eth1	71
Gambar 5.44	Tampilan Perintah ipsec-interfaces	72
Gambar 5.45	Tampilan Perintah ike-group proposal router 2.....	72
Gambar 5.46	Tampilan Perintah encryption pada ike-group	73
Gambar 5.47	Tampilan Perintah Setting dh-group 2	73
Gambar 5.48	Tampilan Perintah Show ike-group router2	73
Gambar 5.49	Tampilan Perintah esp-group proposal router2	74

Gambar 5.50	Tampilan Perintah encryption pada esp-group.....	74
Gambar 5.51	Tampilan Perintah Show esp-group	75
Gambar 5.52	Tampilan perintah Site to Site	75
Gambar 5.53	Tampilan Setting authentication.....	76
Gambar 5.54	Tampilan Perintah vpn ipsec site to site	76
Gambar 5.55	Tampilan Perintah set authentication pre-shared-secret.....	76
Gambar 5.56	Tampilan perintah set ike-group router 2	77
Gambar 5.57	Tampilan perintah set local-ip	77
Gambar 5.58	Tampilan perintah set tunnel 1 local-subnet.....	77
Gambar 5.59	Tampilan perintah set tunnel 1 remote-subnet	77
Gambar 5.60	Tampilan perintah set tunnel 1 esp-group Router 2	78
Gambar 5.61	Tampilan perintah commit	78
Gambar 5.62	Tampilan Perintah save	78
Gambar 5.63	Tampilan perintah show vpn ipsec site-to-site peer	79
Gambar 5.64	Tampilan Ping client router 1 ke client router 2.....	80
Gambar 5.65	Tcpdump Proses ping client router 1 ke client router 2.....	80
Gambar 5.66	Tampilan Ping client router 1 ke server router 2.....	81
Gambar 5.67	Tcpdump Proses ping client router 1 ke server router 2.....	82
Gambar 5.68	Tampilan Mengambil data client router 2 ke client router 1 ..	82
Gambar 5.69	Tampilan Hasil Tcpdump client router 2 ke client router 1 ...	83
Gambar 5.70	Tampilan Ping client router 1 ke client router 2.....	84
Gambar 5.71	Tcpdump Proses ping client router 1 ke client router 2.....	84
Gambar 5.72	Tampilan Ping client router 1 ke server router 2.....	85
Gambar 5.73	Tcpdump Proses ping client router 1 ke server router 2.....	86
Gambar 5.74	Tampilan Mengambil data client router 1 ke client router 2..	86
Gambar 5.75	Tampilan Hasil Tcpdump client router 1 ke client router 2 ...	87

DAFTAR TABEL

Tabel 3.1	Contoh IP Address	35
Tabel 3.2	Pembagian kelas IP Address	36
Tabel 3.3	Berisikan hasil penelitian terdahulu.....	38

ABSTRACT

Syafrudin. *Design and Implementation Site to Site VPN Using Vyatta to PT. Development means Palembang Jaya.*

Increasingly rapid development of information technology, with the development of the company's PT. Sarana Jaya menggunakan Palembang Development of information technology as a means of auxiliary meningkatkan employee performance, but in practice there are many constraints in terms of both technical and non technical.

In this study builds a VPN technology on a WAN network (Wide Area Network) with a security protocol IPSec (Internet Protocol Security) based Vyatta operating system. Although the study only built facility site to site VPN on the LAN network, but is expected to be a network security solution at the moment.

Keywords: Site to site VPN, IPSec, Vyatta

ABSTRAK

Syafrudin. *Desain dan Implementasi Site to Site VPN Menggunakan Vyatta di PT. Sarana Pembangunan Palembang Jaya.*

Perkembangan teknologi informasi semakin cepat, dengan perkembangan itulah perusahaan PT. Sarana Pembangunan Palembang Jaya menggunakan teknologi informasi sebagai sarana pembantu meningkatkan kinerja karyawan namun dalam penerapannya banyak terjadi kendala baik dari segi teknis maupun non teknis.

Pada penelitian ini dibangun sebuah teknologi VPN pada jaringan WAN (Wide Area Network) dengan keamanan Protokol IPSec (Internet Protocol Security) berbasis sistem operasi Vyatta. Walaupun pada penelitian ini hanya dibangun fasilitas site to site VPN pada jaringan LAN saja, namun diharapkan dapat menjadi solusi keamanan jaringan pada saat ini.

Kata kunci : Site to site VPN, IPSec, Vyatta

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada saat ini teknologi berkembang sangat cepat tidak menutup kemungkinan setiap perusahaan dalam bidang apapun akan memanfaatkan seluruh teknologi yang terbaru, baik itu media cetak, media audio visual dan teknologi yang paling membantu dunia usaha ialah komputer. komputer saat ini telah menjadi kebutuhan dalam suatu perusahaan guna menunjang efektif dan efesiennya karyawan mengerjakan semua pekerjaan dalam kantor. dengan perkembangan komputer yang beragam terutama pada jaringan komputer permasalahan yang ada pada setiap perusahaan bisa diselesaikan. PT. SARANA PEMBANGUNAN PALEMBANG JAYA sebagai kantor pusat dan Unit Usaha Bus Rapid Transit BRT (TRANS MUSI) sebagai kantor cabang terdapat permasalahan pada jarak antar kantor, dimana pada saat karyawan dari kantor cabang ingin mengambil data-data penting perusahaan yang berada di kantor pusat maka yang dilakukan adalah dengan cara manual yaitu karyawan dari kantor cabang datang langsung ke kaantor pusat untuk mengambil data-data tersebut. Jelas cara ini sangat tidak efektif karena banyak waktu yang terbuang pada saat karyawan dalam perjalanan dan keamanan maupun kerahasiaan data perusahaan sangat tidak terjamin.

Dengan kemajuan teknologi ini maka banyak perusahaan mengandalkan teknologi informasi khususnya teknologi komputerisasi sebagai penunjang pekerjaan. Dari beragam jenis aplikasi-aplikasi keamanan jaringan yang sering kita dengar, nama *Virtual Private Network (VPN)* sangat banyak diterapkan kesemua keamanan jaringan. selain lebih mudah penerapannya dibandingkan dengan aplikasi-aplikasi lainnya *Virtual Private Network (VPN)* juga dapat digandengkan dengan aplikasi-aplikasi pendukung lainnya seperti *Domain Name System (DNS)* atau aplikasi lainnya. karena untuk penerapannya *Virtual Private Network (VPN)* menggunakan jaringan publik maka metode yang digunakan adalah *site to site* yaitu jaringan komputer dari masing-masing kantor dapat langsung berhubungan. Karena keamanan jaringan yang ditekankan maka perlu memberikan perhatian yang lebih untuk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, *hacking* dan tindakan *cyber crime* pada jaringan VPN

Berdasarkan uraian di atas, maka penulis berniat membantu persoalan perusahaan tentang keamanan jaringan global dengan aplikasi VPN (*Virtual Private Network*) menggunakan sistem operasi *Vyatta version 5* dengan metode *site to site* ini menjadi sebuah penelitian ilmiah yang berjudul “Implementasi *site to site Virtual Private Network (VPN)* Server menggunakan *Vyatta* di PT. SARANA PEMBANGUNAN PALEMBANG JAYA dengan Unit Usaha BRT Trans Musi.

1.2 Perumusan Masalah

Penulis merumuskan permasalahan ini dalam bentuk “Bagaimana Implementasi site to site Virtual Private Network (VPN) Server menggunakan Vyatta pada PT. SARANA PEMBANGUNAN PALEMBANG JAYA dengan Unit Usaha BRT Trans Musi?”.

1.3 Batasan Masalah

Penulis membatasi permasalahan agar penelitian ini tidak menyimpang serta tidak terlalu luas, yaitu Implementasi site to site Virtual Private Network (VPN) Server menggunakan Vyatta pada PT. SARANA PEMBANGUNAN PALEMBANG JAYA dengan Unit Usaha BRT Trans Musi.

1.4 Tujuan penelitian

Tujuan dari penelitian ini untuk mengimplementasikan pengamanan jaringan antara kantor pusat dan kantor cabang menggunakan sistem Virtual Private Network (VPN) Server dengan metode site to site yang berbasis IPSec pada PT. SARANA PEMBANGUNAN PALEMBANG JAYA dengan Unit Usaha BRT Trans Musi.

1.5 Manfaat penelitian

1. Bagi Penulis

Penulis dapat menerapkan mata kuliah Praktik Jaringan Komputer yang telah didapat selama mengikuti perkuliahan pada STMIK PalComTech.

2. Bagi Perusahaan PT. SARANA PEMBANGUNAN PALEMBANG JAYA dengan Unit Usaha BRT Trans Musi

Perusahaan dapat menggunakan jaringan untuk mengirim data-data penting perusahaan dan keamanan jaringan itu sendiri menggunakan Virtual Private Network (*VPN*) Server.

3. Bagi Akademik

Dapat menjadi referensi dalam penulisan karya ilmiah selanjutnya dan menjadi bahan bacaan pada perpustakaan dan ilmu pengetahuan.

1.6 Sistematika Penulisan

Skripsi ini ditulis dalam lima bab dan masing-masing bab terbagi dalam sub-sub bab. Sistematika penulisan skripsi ini disusun sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisikan tentang latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat, serta sistematika penulisan.

BAB II GAMBARAN UMUM PERUSAHAAN

Bab ini berisikan tentang profil PT. SARANA PEMBANGUNAN PALEMBANG JAYA dengan Unit Usaha BRT Trans Musi.

BAB III TINJAUAN PUSTAKA

Bab ini berisikan tentang referensi yang dipakai Penulis dalam melakukan penelitian ilmiahnya.

BAB IV METODE PENELITIAN

Bab ini akan menjelaskan lokasi dan waktu penelitian, jenis penelitian, jenis data, teknik pengumpulan data, populasi dan sampel, definisi operasional variabel penelitian.

BAB V HASIL DAN PEMBAHASAN

Bab ini berisikan tentang implementasi site to site VPN Server pada PT. SARANA PEMBANGUNAN PALEMBANG JAYA dengan Unit Usaha BRT Trans Musi.

BAB VI PENUTUP

Bab ini berisi kesimpulan dari semua uraian-uraian pada bab-bab sebelumnya dan juga berisi saran-saran yang diharapkan berguna dalam penelitian.

BAB II

GAMBARAN UMUM PERUSAHAAN

2.1 Profil Perusahaan

2.1.1 Sejarah Perusahaan

Unit Usaha Bus Rapid Transit (Trans Musi) adalah salah satu dari banyak Unit Usaha yang dimiliki oleh PT. SARANA PEMBANGUNAN PALEMBANG JAYA yang bergerak dibidang sosial yaitu alat transportasi massal dalam kota. Unit Usaha Bus Rapid Transit (Trans Musi) berada di Palembang didirikan pada tanggal 22 Februari 2010, BRT Trans Musi melakukan soft opening di terminal Alang-Alang Lebar. Soft opening ini dilakukan oleh Walikota Palembang, Ir. Eddy Santana Putra, MT dalam sebuah acara yang dihadiri jajaran Muspida, Kepala Dinas di lingkungan Pemerintah Kota, tokoh masyarakat, serta pimpinan PT. Sarana Pembangunan Palembang Jaya sebagai pengelola BRT Trans Musi.

Pimpinan PT. Sarana Pembangunan Palembang Jayadi pimpin oleh Bapak Ir. Bahder Johan dengan Unit Usaha Bus Rapid (Trans Musi) di pimpin oleh Manager Bapak Aries Rachmansyah.

2.1.2 Visi dan Misi

Visi Perusahaan Unit Usaha Bus Rapid Transit (Trans Musi):

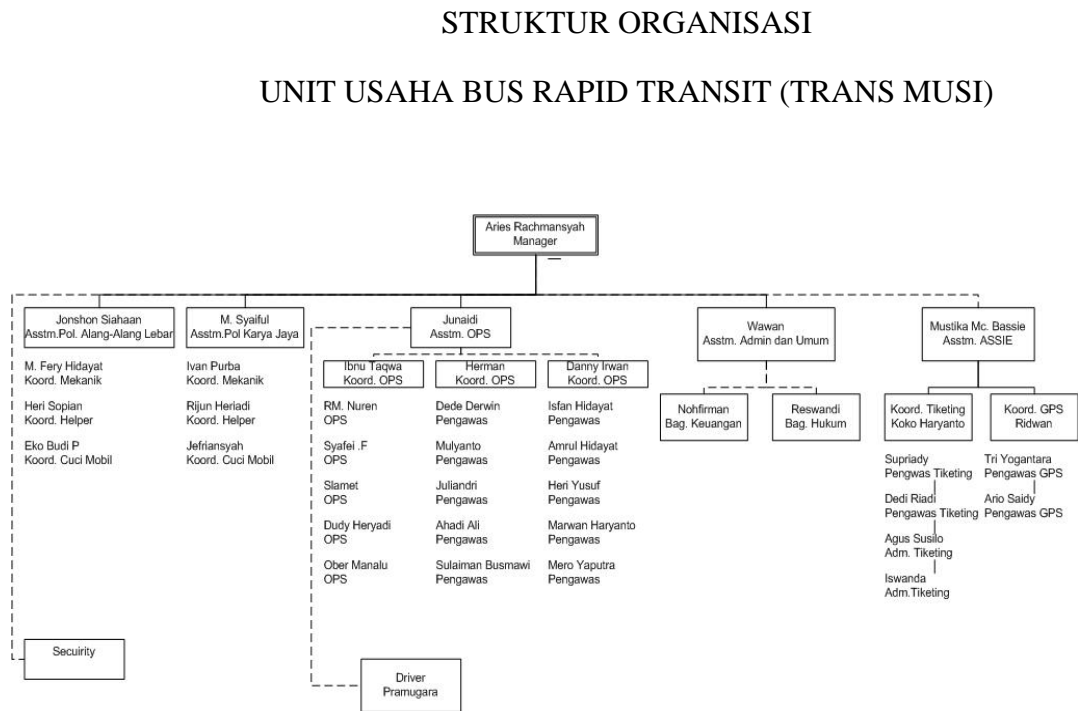
Saat ini Bus Rapid Transit (Trans Musi) terbaik ke-2 setelah Bus Trans Jakarta di Indonesia, dengan predikat tersebut Bus Rapid Transit (Trans Musi) sekarang menjadi alat transportasi yang ditunggu dan digemari oleh masyarakat kota Palembang, dengan ini Bus Rapid Transit (Trans Musi) menambah jumlah armada demi memenuhi seluruh koridor di dalam kota Palembang guna meningkatkan pelayanan masyarakat kota Palembang dan tidak menutup kemungkinan Bus Rapid Transit (Trans Musi) menjadi sarana transportasi terbaik di Indonesia.

Misi Perusahaan Unit Usaha Bus Rapid Transit (Trans Musi) :

BRT Trans Musi sendiri pada masa-masa mendatang diharapkan akan menjadi salah satu contoh pengelolaan transportasi kota yang baik, dan akan terus dikembangkan sehingga mampu menjangkau ke semua daerah di wilayah Palembang. Untuk mencapai hal tersebut, BRT Trans Musi akan mengembangkan armada yang dimiliki, baik melalui kerjasama dengan pemerintah kota Palembang maupun dengan pihak ketiga maupun swasta yang ingin berperan serta dalam memajukan pembangunan transportasi kota Palembang.

2.2 Struktur Organisasi

Secara sistematis struktur organisasi Unit Usaha Bus Rapid Transit (Trans Musi) sebagai berikut:



Sumber : Unit Usaha Bus Rapid Transit (Trans Musi) 2012

Gambar 2.1 Struktur Organisasi Unit Usaha Bus Rapid Transit (Trans Musi)

2.3 Tugas dan Wewenang

Didalam perusahaan, untuk melaksanakan kegiatan agar terkoordinir dengan baik dibutuhkan pembagian tugas dari masing-masing bagian atau unit kerja yang ada pada perusahaan. Dengan berpegangan kepada urutan

secara struktural organisasi pada Unit Usaha Bus Rapid Transit (Trans Musi).

A. Manager

Manager adalah pemimpin perusahaan tertinggi yang bertugas mengkoordinir semua kegiatan perusahaan dalam mencapai tujuan pokok perusahaan serta bertanggung jawab untuk membuat keputusan dalam setiap kegiatan perusahaan.

B. Assisten Manager Pool

Tugas dan tanggung jawab Asisten Manager Pool adalah sebagai berikut:

1. Menjaga kebersihan dan ketertiban di lingkungan Pool masing-Masing.
2. Menyiapkan dan menertipkan seluruh Bus sebelum dan sesudah Beroperasi.
3. Mengkoordinir setiap aspek demi menunjang maksimalnya bus Dalam beroperasi.
4. Memberikan Pengarahan atau Breifing setiap akan melakukan Operasional.

C. Asisten Manager Administrasi dan Umum

Tugas dan tanggung jawab Asisten Manager Administrasi dan Umum adalah sebagai berikut:

1. Menyusun dan menetapkan anggaran unit kerja dalam perusahaan.
2. Mencatat penerimaan kas dari laba pekerjaan
3. Menangani segala masalah pendapatan dan penggajian karyawan.
4. Membuat laporan keuangan perusahaan.
5. Menyelesaikan surat menyurat yang bersifat umum.
6. Bertanggung jawab atas proses legalnya operasi bus dijalan.
7. Bertanggung jawab atas pengadaan barang yang dibutuhkan bagian
Operasional.
8. Membuat daftar rincian biaya dari pekerjaan yang akan di kerjakan
Bagian Operasional
9. Menyelesaikan perkara hukum yang ada bila terjadi pada seluruh
Aspek Perusahaan.
10. Bertanggung jawab dan menyediakan kelengkapan atribut para
Awak Bus sebelum melaksanakan kegiatan operasional.

D. Asisten Manager Operasional

Tugas dan tanggung jawab Asisten Manager Operasional adalah sebagai berikut:

1. Bertanggung jawab dalam mengurus pekerjaan dilapangan dari *planning* operasional yang telah ditentukan..
2. Merencanakan penjadwalan kerja bagi seluruh unit bus maupun awak bus.
3. Bertanggung jawab atas pengawasan yang terjadi dilapangan.
4. Mengerjakan pekerjaan sesuai dengan apa yang telah direncanakan oleh bagian administrasi dan bertanggung jawab atas kualitas dari pekerjaan yang telah selesai dikerjakan.
5. Pada bagian ini juga Asisten Manager Operasional bertanggung Jawab atas kesiapan Driver dan Pramugara dalam melakukan Operasional.

E. Asisten Manager ASSIE dan IT

1. Bertanggung jawab atas bagian Teknologi Informasi dalam Berbagai aspek yang menunjang perusahaan.
2. Mengkoordinir tim pengawas GPS Bus demi memaksimalkan Operasional Bus.

3. Memberikan setiap laporan pekerjaan kepada manager dan
Memberikan masukan setiap kebijakan atau keputusan manager.
4. Melalui staffnya Asisten Manager ASSIE dan IT juga bertugas
Memperbaiki sistem informasi dalam kantor demi menunjang
Kegiatan Pekerjaan setiap karyawan perusahaan.

BAB III

TINJAUAN PUSTAKA

3.1 Teori Pendukung

3.1.1 Jaringan Komputer

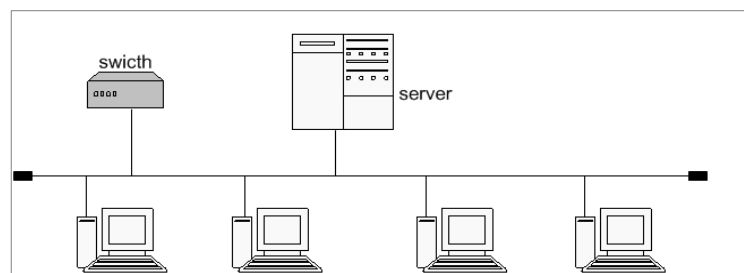
Menurut Taryana. S [3] :“Jaringan komputer adalah suatu gabungan berbagai perlengkapan komunikasi dan komputer yang dihubungkan satu sama lain lewat medium komunikasi secara elektronik”.

Menurut Nana (2007:9),jaringan adalah kumpulan dari beberapa komputer, baik jaringan komputer yang berskala kecil seperti dirumah atau kantor maupun yang berskala besar seperti antarkota dan provinsi.

Ada banyak topologi jaringan yang bisa diterapkan di jaringan *Local Area Network* (LAN) maupun *Wide Area Network* (WAN), contoh topologi jaringan :

a. *Topologi* ini adalah topologi yang awal digunakan untuk menghubungkan komputer. Dalam topologi ini masing masing komputer akan terhubung ke satu kabel panjang dengan beberapa terminal, dan pada akhir dari kable harus diakhiri dengan satu *terminator*.*Topologi* ini sudah sangat jarang digunakan didalam membangun jaringan komputer biasa karena memiliki beberapa

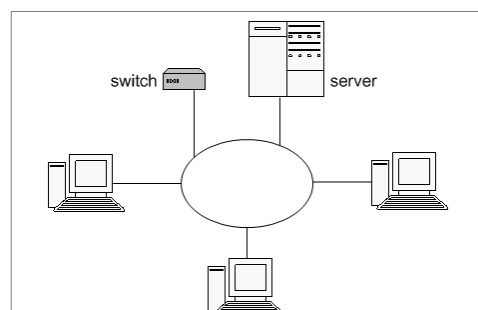
kekurangan diantaranya kemungkinan terjadinya tabrakan aliran data, jika salah satu perangkat putus atau terjadi kerusakan pada satu bagian komputer maka jaringan langsung tidak akan berfungsi sebelum kerusakan tersebut diatasi.



Sumber : diolah sendiri

Gambar 3.1 Topologi Bus

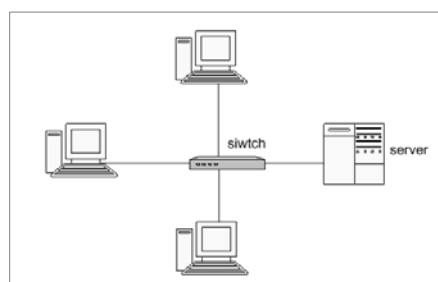
b. *Topologi* ini hampir sama dengan *topologi ring* akan tetapi pembuatannya lebih disempurnakan. Bisa di lihat dari perbedaan gambar. Didalam gambar jelas terlihat bagaimana pada token *ring* kabel penghubung di buat menjadi lingkaran terlebih dahulu dan nantinya akan di buat terminal-terminal untuk masing-masing komputer dan perangkat lain.



Sumber : diolah sendiri

Gambar 3.2 Topologi Ring

c. *Topologi* bintang atau yang lebih sering disebut dengan *topologistar*. Pada *topologi* ini sudah menggunakan bantuan alat lain untuk mengkoneksikan jaringan komputer. Contoh alat yang di pakai disini adalah *switch*. Pada gambar jelas terlihat satu *switch* berfungsi sebagai pusat penghubung komputer-komputer yang saling berhubungan. Keuntungan dari *topologi* ini sangat banyak sekali diantaranya memudahkan *admin* dalam mengelola jaringan, memudahkan dalam penambahan komputer atau terminal, kemudahan mendeteksi kerusakan dan kesalahan pada jaringan. Tetapi dengan banyaknya kelebihan bukan dengan artian *topologi* ini tanpa kekurangan. Kekurangannya diantaranya pemborosan terhadap kabel, kontrol yang terpusat pada *switch* terkadang jadi permasalahan kritis kalau seandainya terjadi kerusakan pada *switch* maka semua jaringan tidak akan bisa digunakan.

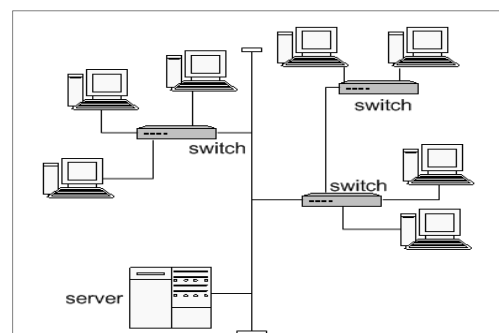


Sumber : diolah sendiri

Gambar 3.3 Topologi Bintang

d. *Topologi* Pohon, *Topologi* pohon atau di sebut juga *topologi hirarki* dan bisa juga disebut *topologi* bertingkat merupakan *topologi*

yang bisa digunakan pada jaringan di dalam ruangan kantor yang bertingkat. Pada gambar bisa kita lihat hubungan antar satu komputer dengan komputer lain merupakan percabangan dengan hirarki yang jelas sentral pusat atau yang berada pada bagian paling atas merupakan sentral yang aktif.



Sumber : diolah sendiri

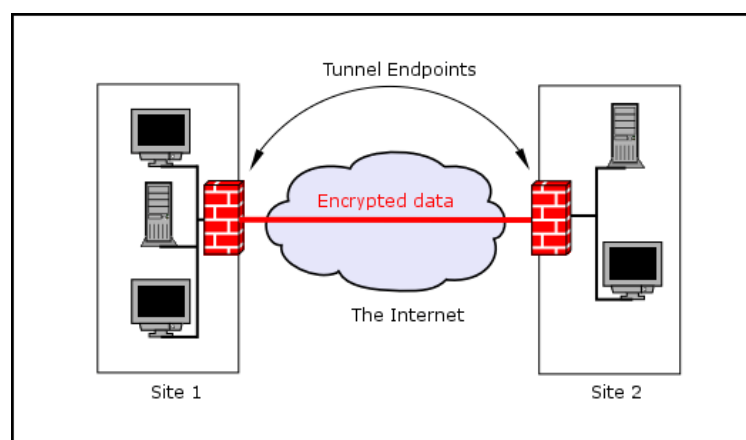
Gambar 3.4 Topologi Tree

3.1.2 VPN (*Virtual Private Network*)

VPN (*Virtual Private Network*) adalah suatu jaringan pribadi yang dibuat dengan menggunakan jaringan publik, atau dengan kata lain menciptakan suatu WAN yang sebenarnya terpisah baik secara fisik maupun geografis sehingga secara logikal membentuk satu network tunggal, paket data yang mengalir antar site maupun dari user yang melakukan remote akses akan mengalami enkripsi dan autentikasi sehingga menjamin keamanan, integritas dan validitas data. Perlu

penerapan teknologi tertentu agar walaupun menggunakan medium yang umum, tetapi *traffic* (lalu lintas) antar *remote-site* tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan *traffic* yang tidak semestinya ke dalam *remote-site*.

3.1.2.1 Konsep kerja VPN



Sumber : diolah sendiri

Gambar 3.5 Konsep kerja VPN

Dari gambar diatas secara sederhana cara kerja VPN adalah sebagai berikut:

- VPN membutuhkan sebuah server yang berfungsi sebagai penghubung antar PC, **Server VPN** ini bisa berupa komputer dengan aplikasi VPN Server atau sebuah Router, misalnya MikroTik RB 750.
- Untuk memulai sebuah koneksi, komputer dengan aplikasi VPN Client mengontak Server VPN, VPN Server kemudian

memverifikasi *username* dan *password* dan apabila berhasil maka VPN Server memberikan IP Address baru pada komputer client dan selanjutnya sebuah koneksi / tunnel akan terbentuk.

- Untuk selanjutnya komputer client bisa digunakan untuk mengakses berbagai resource (komputer atau LAN) yang berada dibelakang VPN Server misalnya melakukan transfer data, ngeprint dokument, browsing dengan gateway yang diberikan dari VPN Server, melakukan remote desktop dan lain sebagainya.

Keuntungan atau Manfaat VPN

Beberapa keuntungan dari teknologi VPN diantaranya adalah:

- *Remote Access*, dengan VPN kita dapat mengakses komputer atau jaringan kantor, dari mana saja selama terhubung ke internet
- Keamanan, dengan koneksi VPN kita bisa berselancar dengan aman ketika menggunakan akses internet publik seperti *hotspot* atau *internet cafe*.
- Menghemat biaya setup jaringan, VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan public yang sudah

ada tanpa perlu membangun jaringan pribadi.

Kekurangan atau Kelemahan VPN

Setiap ada kelebihan pasti ada kekurangannya, beberapa kekurangan dari VPN diantaranya adalah:

- Koneksi internet (jaringan publik) yang tidak bisa kita prediksi. Hal ini dapat kita maklumi karena pada dasarnya kita hanya "*nebeng*" koneksi pada jaringan pihak lain sehingga otomatis kita tidak mempunyai kontrol terhadap jaringan tersebut.
- Perhatian lebih terhadap keamanan. Lagi-lagi karena faktor penggunaan jaringan publik, maka kita perlu memberikan perhatian yang lebih untuk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, hacking dan tindakan cyber crime pada jaringan VPN

3.1.2.2 Implementasi VPN

1. Remote Access VPN

Remote access yang biasa juga disebut *virtual private dial-up network* (VPDN), menghubungkan antara pengguna yang *mobile* dengan *local area network* (LAN). Jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan khusus

perusahaannya dari berbagai lokasi yang jauh (*remote*) dari perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerjasama dengan *enterprise service provider* (ESP). ESP akan memberikan suatu *network access server* (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan *software* klien untuk komputer-komputer yang digunakan pegawai perusahaan tersebut.

Untuk mengakses jaringan lokal perusahaan, pegawai tersebut harus terhubung ke NAS dengan men-*dial* nomor telepon yang sudah ditentukan. Kemudian dengan menggunakan *software* klien, pegawai tersebut dapat terhubung ke jaringan lokal perusahaan.

Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan *remote access* VPN untuk membangun WAN. VPN tipe ini akan memberikan keamanan, dengan mengenkripsi koneksi antara jaringan lokal perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi ini adalah ISP.

2. Site-to-site VPN

Jenis implementasi VPN yang kedua adalah *site-to-site* VPN. Implementasi jenis ini menghubungkan antara 2 kantor atau lebih yang letaknya berjauhan, baik kantor yang dimiliki perusahaan itu

sendiri maupun kantor perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, *supplier* atau pelanggan) disebut **ekstranet**. Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis **intranet** *site-to-site* VPN.

3.1.2.3 Protokol *Tunneling* Utama VPN

1. Point-to-Point Tunneling Protocol (PPTP)

PPTP dikembangkan oleh Microsoft dan Cisco merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP (Snader, 2005). Teknologi jaringan PPTP merupakan pengembangan dari remote access Point-to-Point protocol yang dikeluarkan oleh Internet Engineering Task Force (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagrams agar dapat ditransmisikan melalui internet. PPTP juga dapat digunakan pada jaringan private LAN-to-LAN.

PPTP terdapat sejak dalam sistem operasi Windows NT server dan Windows NT Workstation versi 4.0. Komputer yang berjalan

dengan sistem operasi tersebut dapat menggunakan protokol PPTP dengan aman untuk terhubung dengan private network sebagai klien dengan remote access melalui internet. PPTP juga dapat digunakan oleh komputer yang terhubung dengan LAN untuk membuat VPN melalui LAN.

Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya public-switched telephone network (PSTNs) untuk membangun VPN. Pembangunan PPTP yang mudah dan berbiaya murah untuk digunakan secara luas, menjadi solusi untuk remote users dan mobile users karena PPTP memberikan keamanan dan enkripsi komunikasi melalui PSTN ataupun internet.

2. Layer 2 Tunneling Protocol (L2TP)

L2TP adalah tunneling protocol yang memadukan dua buah tunneling protokol yaitu L2F (Layer 2 Forwarding) milik cisco dan PPTP milik Microsoft (Gupta, 2003). L2TP biasa digunakan dalam membuat Virtual Private Dial Network (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi didalamnya. Umumnya L2TP menggunakan port 1702 dengan protocol UDP untuk mengirimkan L2TP *encapsulated* PPP frames sebagai data yang di tunnel. Terdapat dua model tunnel yang dikenal (Lewis, 2006), yaitu *compulsory* dan *voluntary*. Perbedaan utama keduanya

terletak pada *endpoint tunnel*-nya. Pada *compulsory tunnel*, ujung tunnel berada pada ISP, sedangkan pada *voluntary* ujung tunnel berada pada client remote.

3. IPsec

IPSec merupakan suatu pengembangan dari protokol IP yang bertujuan untuk menyediakan keamanan pada suatu IP dan *layer* yang berada di atasnya (Carmouche, 2006). IPSec (*Internet Protocol Security*) merupakan salah satu mekanisme yang diimplementasikan pada *Virtual Private Network*. Paket IP tidak memiliki aspek *security*, maka hal ini akan memudahkan untuk mengetahui isi dari paket dan alamat IP itu sendiri. Sehingga tidak ada garansi bahwa menerima paket IP merupakan dari pengirim yang benar, kebenaran data ketika ditransmisikan. IPSec merupakan metode yang memproteksi IP datagram ketika paket ditransmisikan pada *traffic*. IPSec berkerja pada *layer* tiga OSI yaitu *network layer* sehingga dapat mengamankan data dari *layer* yang berada atasnya.

IPSec terdiri dari dua buah *security* protokol (Carmouche, 2006) :

- a. AH (*Authentication Header*) melakukan autentikasi datagram untuk mengidentifikasi pengirim data tersebut
- b. ESP (*Encapsulating Security Header*) melakukan enkripsi dan layanan autentikasi.

IPSec menggunakan dua buah protokol berbeda untuk menyediakan pengamanan data yaitu AH dan ESP keduanya dapat dikombinasikan ataupun berdiri sendiri. IPSec memberikan layanan *security* pada *level* IP dengan memungkinkan suatu *system* memilih protokol *security* yang dibutuhkan, algoritma yang digunakan untuk layanan, dan menempatkan kunci kriptografi yang dibutuhkan untuk menyediakan layanan. Dua buah protokol yang digunakan untuk memberikan layanan keamanan yaitu autentikasi protokol yang ditunjuk pada *header* protokol yaitu AH (*Authentication Header*) dan sebuah protokol yang mengkombinasikan enkripsi dan autentikasi yang ditunjuk oleh *header* paket untuk format tersebut yaitu ESP (*Encapsulating Security Payload*).

3.1.3 Vyatta

Vyatta adalah sistem operasi yang berfungsi sebagai router untuk mengatur jaringan di dalam sebuah gedung atau fasilitas yang berhubungan dengan jaringan, yaitu adanya aktivitas Server dan Client dalam melakukan transaksi data secara digital. Vyatta telah mengubah dunia networking dengan mendistribusikan router, firewall dan VPN sebagai komoditi dengan cara yang sama seperti Komoditi Linux memasarkan Sistem Operasinya.

Setiap bulannya lebih dari 10.000 user di seluruh dunia telah beralih ke Vyatta open-source, sebagai alternatif untuk menekan harga yang tidak fleksibel dari vendor. Vyatta ini bisa di download secara gratis di Vyatta.com.

Vyatta bisa membantu anda agar:

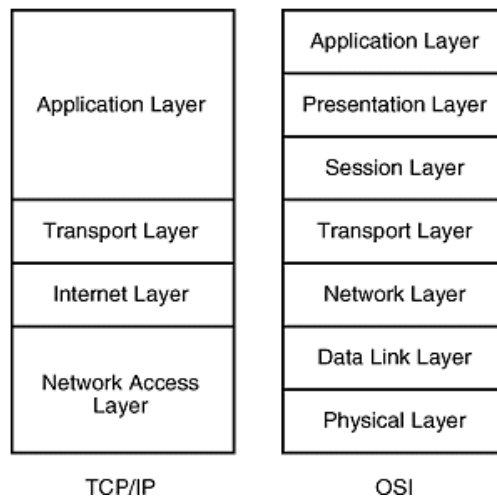
- * Mampu mengimplementasikan BGP dalam skala besar
- * Membagikan internet di kantor anda
- * Menjaga Jaringan anda tetap aman dengan stateful-inspection firewall
- * Koneksi ke remote office dengan aman melalui VPN
- * Menghindari biaya dalam upgrade jaringan
- * Bisa menjalankan lingkungan jaringan secara virtual di Xen dan Vmware
- * Menambah jaringan dan keamanan ke dalam Server-Blade pada data center anda
- * Menawarkan dan mengelola jasa jaringan dan keamanan

3.1.4 LAN (*Local Area Network*)

jaringan pribadi dalam sebuah gedung atau kampus yg ukurannya sampai \pm 1 km. Digunakan untuk pemakaian resource bersama (misalnya printer) dan saling bertukar informasi. Kecepatan transmisi mulai dari 10 sampai 100 Mbps.

3.1.5 Model OSI

Menurut Andi (1995:293), *Open sistem interconetion* (OSI) adalah suatu dekripsi abstrak mengenai desain lapisan-lapisan komunikasi dan protokol jaringan komputer yang dikembangkan sebagai bagian dari inisiatif *Open Systems Interconnection* (OSI). Model ini disebut juga dengan model Tujuh lapisan *Open sistem interconetion* (OSI). Setiap lapisan berfungsi untuk melakukan fungsi-fungsi spesifik untuk mendukung lapisan di atasnya dan sekaligus juga menawarkan layanan untuk lapisan yang ada di bawahnya. Tiga lapisan terbawah akan fokus pada melewatkan trafik melalui jaringan kepada suatu sistem yang terakhir. Empat lapisan teratas akan bermain pada sistem terakhir untuk menyelesaikan proses komunikasinya



Sumber : diolah sendiri

Gambar 3.6 Lapisan *Open sistem interconetion* (OSI)

Open sistem interconetion (OSI) mempunyai 7 lapisan khusus pelayanan jaringan.

1. Lapisan *Physical*, lapisan ini berkomunikasi secara langsung dengan media komunikasi, dan mempunyai dua tanggung jawab mengirim dan menerima bit-bit. Bit adalah satuan terkecil dari informasi dalam komunikasi data. Sebuah bit hanya mempunyai dua nilai 1 dan 0. lapisan komunikasi yang lain bertanggung jawab terhadap pengumpulan bit-bit ini menjadi kelompok yang mewakili pesan data. Lapisan *physical* menggambarkan pola bit yang akan digunakan, tetapi tidak mendefinisikan medianya. Lapisan ini hanya menggambarkan bagaimana data dikodekan menjadi sinyal-sinyal dan karakteristik antar muka tambahan media.
2. Lapisan *Data Link*, lapisan ini bertanggung jawab untuk menyediakan komunikasi dari *node* ke *node* pada satu jaringan local.

Node adalah yang diterapkan untuk *router* dan *host*. Agar menyediakan pelayanan ini, lapisan data link melakukan dua fungsi. Lapisan tersebut harus menyediakan mekanisme alamat yang memungkinkan pesan-pesan untuk dikirim ke *node* yang benar. Lapisan ini juga harus menterjemahkan pesan-pesan dari lapisan yang lebih tinggi menjadi bit-bit yang dapat ditransmisikan oleh lapisan *physical*.

3. Lapisan *Network*, lapisan ini berfungsi untuk menambahkan *header* pada pesan yang termasuk alamat asal dan tujuan jaringan. Kombinasi dari data dan lapisan *network* disebut paket. Informasi alamat jaringan digunakan untuk mengirimkan pesan ke jaringan benar. Setelah pesan tersebut sampai pada jaringan yang benar, lapisan data *link* dapat menggunakan alamat *node* untuk mengirimkan pesan ke *node* tertentu

4. Lapisan *Transport*, lapisan ini bertanggung jawab membagi pesan-pesan menjadi *fragmen-fragmen* yang cocok dengan pembatasan ukuran yang dibentuk oleh jaringan. Pada sisi penerimaan, lapisan *transport* menggabungkan kembali fragmen untuk mengembalikan pesan aslinya. Lapisan *transport* memberikan *service acces point* (SAP) ID kepada setiap paket, SAP ID adalah suatu alamat yang mengidentifikasi proses yang mengawali pesan. SAP ID memungkinkan lapisan *transport* dari *node* penerimaan melewatkan pesan ke proses yang sesuai.

5. Lapisan *Session*, lapisan ini bertanggung jawab untuk mengendalikan *dialog* antar *node*. Suatu dialog adalah percakapan formal dimana dua *node* sepakat untuk bertukar data. Komunikasi data berlangsung dalam tiga mode dialog, seperti :

a *Simplex*. Suatu node mengirimkan secara sendirian, ketika yang lain menerima secara sendirian.

b *Half-duplex*. Hanya satu *node* yang boleh mengirimkan pada suatu saat, dan *node-node* secara bergiliran mengirim.

c *Full-duplex*. *Node-node* dapat mengirim dan menerima secara bersamaan. Komunikasi *full-duplex* biasanya membutuhkan beberapa bentuk pengendalian aliran untuk memastikan bahwa peralatan pengiriman tidak lebih cepat dari pada peralatan lain yang menerima.

6. Lapisan *Presentation*, lapisan ini bertanggung jawab untuk menyajikan data kepada lapisan aplikasi. Lapisan presentation secara langsung menterjemahkan data dari satu format ke format yang lain. Lapisan Presentation merupakan lapisan *Open sistem interconetion* (OSI) yang paling jarang diterapkan.

7. Lapisan *Application*, lapisan ini menyediakan pelayanan aplikasi yang digunakan untuk berkomunikasi melalui jaringan. Beberapa contoh pelayanan lapisan application.

1. Pengiriman *elektronicemail*. Suatu protokol untuk menangani *electronic mail* dapat digunakan oleh berbagai aplikasi.

2. *Remote file acces.* Aplikasi-aplikasi lokal dapat diberi kemampuan untuk memulai dan mengendalikan proses pada *node-node* yang lain.
3. Manajemen jaringan. Protokol manajemen jaringan dapat memungkinkan berbagai aplikasi mengakses informasi manajemen jaringan.

3.1.6 Domain Name System (DNS)

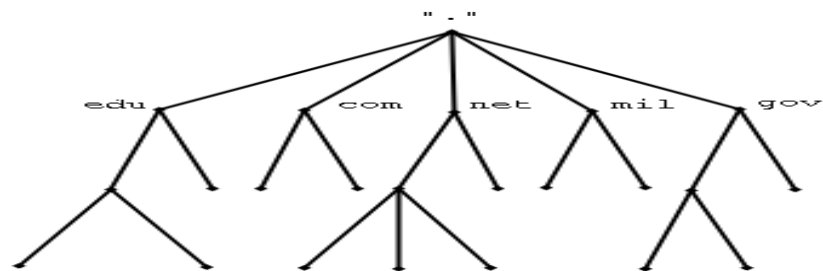
3.1.6.1 Sejarah singkat DNS

Penggunaan nama sebagai pengabstraksi alamat mesin di sebuah jaringan komputer yang lebih dikenal oleh manusia mengalahkan TCP/IP, dan kembali ke zaman ARPAnet. Dahulu, setiap komputer di jaringan komputer menggunakan file HOSTS.TXT dari SRI (sekarang SIR International), yang memetakan sebuah alamat ke sebuah nama (secara teknis, file ini masih ada - sebagian besar system operasi modern menggunakannya baik secara baku maupun melalui konfigurasi, dapat melihat Hosts file untuk menyamakan sebuah nama host menjadi sebuah alamat IP sebelum melakukan pencarian via DNS). Namun, sistem tersebut diatas mewarisi beberapa keterbatasan yang mencolok dari sisi prasyarat, setiap saat sebuah alamat komputer berubah, setiap sistem yang hendak berhubungan dengan komputer tersebut harus melakukan update terhadap file Hosts.

Dengan berkembangnya jaringan komputer, membutuhkan sistem yang bisa dikembangkan: sebuah sistem yang bisa mengganti alamat host hanya di satu tempat, host lain akan mempelajari perubahan tersebut secara dinamis. Inilah DNS.

Paul Mockapetris menemukan DNS di tahun 1983; spesifikasi asli muncul di RFC 882 dan 883. Tahun 1987, penerbitan RFC 1034 dan RFC 1035 membuat update terhadap spesifikasi DNS. Hal ini membuat RFC 882 dan RFC 883 tidak berlaku lagi. Beberapa RFC terkini telah memproposikan beberapa tambahan dari protokol inti DNS.

3.1.6.2 Struktur DNS



Sumber : diolah sendiri

Gambar 3.7 Struktur DNS

A. Top Level Internet Domain, TLD

Merupakan rujukan kepada huruf-huruf terakhir setelah tanda titik dalam sebuah nama domain. TLD dibagi menjadi 2, yaitu:

1. generic Top Level Domain (gTLD)

Dipergunakan oleh macam-macam organisasi, sebagai contoh, .com untuk organisasi komersial, .org untuk organisasi nonkomersial, edu untuk lembaga pendidikan Amerika, dll. Domain ini terdiri dari 3 huruf atau lebih. Sebagian besar gTLD tersedia untuk dapat digunakan secara luas, tetapi untuk alasan historis, .mil (militer Amerika Serikat) dan .gov (Pemerintahan Federal Amerika Serikat) dibatasi dan hanya dapat digunakan oleh kedua otoritas tersebut. Domain-domain dalam gTLD disubklasifikasikan ke dalam ranah yang disponsori (sponsored top-level domains (sTLD)), misalnya .aero, .coop dan .museum, dan ranah yang tidak disponsori (unsponsored top-level domains (uTLD)), misalnya .biz, .info, .name and .pro.

2. country code Top Level Domain (ccTLD)

Dipergunakan untuk kode negara atau wilayah dependensi. Terdiri dari 2 huruf, misalnya .jp untuk Jepang, .id untuk Indonesia, uk untuk Inggris, sg untuk Singapura.

B. Second-Level Domains

Dapat berisi host dan domain lain, yang disebut dengan subdomain. Second level di Indonesia antara lain go.id untuk lembaga pemerintahan Indonesia ; mil.id untuk lembaga militer Indonesia ; sch.id untuk lembaga pendidikan tingkat sekolah.

C. Third Level Domain

merupakan nama sebelum Second Level Domain dan Top Level Domain. Misalnya nama domain yang anda miliki adalah domainku.com, maka anda dapat menambahkan nama lain sebelum domainku, yaitu mail.domainku.com atau search.domainku.com. Third level domain biasanya dikenal dengan sebutan “Subdomain”.

Dengan adanya sistem berbentuk hierarki/pohon ini maka tidak ada nama host yang sama pada domain/subdomain yang sama, karena masing-masing dari node/titik-cabang mempunyai nama unik dan tidak boleh ada yang menyamainya kecuali berbeda sub-tree/sub pohon. Tidak akan ada konflik antar organisasi karena masing-masing organisasi mempunyai domain yang berbeda-beda dan ini diatur oleh InterNIC untuk TLD. Kedalaman pohon dibatasi sampai level 127.

3.1.6.3 Teori bekerja DNS

Pengelola dari sistem DNS terdiri dari tiga komponen:

- 1.DNS resolver, sebuah program klien yang berjalan di komputer pengguna, yang membuat permintaan DNS dari program aplikasi.
- 2.recursive DNS server, yang melakukan pencarian melalui DNS sebagai tanggapan permintaan dari resolver, dan mengembalikan jawaban kepada para resolver tersebut;
- 3.authoritative DNS server yang memberikan jawaban terhadap permintaan dari recursor, baik dalam bentuk sebuah jawaban, maupun dalam bentuk delegasi (misalkan: mereferensikan ke authoritative DNS server lainnya).

3.1.7 IP Address

IP address adalah alamat yang diberikan pada jaringan komputer dan peralatan jaringan yang menggunakan protokol TCP/IP. IP address terdiri atas 32 bit angka biner yang dapat dituliskan sebagai empat kelompok angka desimal yang dipisahkan oleh tanda titik seperti 192.168.1.1.

Network ID			Host ID
192	168	1	1

Tabel 3.1 Contoh IP Address

IP address terdiri atas dua bagian yaitu network ID dan host ID, dimana network ID menentukan alamat jaringan komputer, sedangkan host ID menentukan alamat host (komputer, router, switch). Oleh sebab itu IP address memberikan alamat lengkap suatu host beserta alamat jaringan di mana host itu berada.

3.1.7.1 Kelas-kelas IP Address

Untuk mempermudah pemakaian, bergantung pada kebutuhan pemakai, IP address dibagi dalam tiga kelas seperti diperlihatkan pada tabel dibawah

Kelas	Network ID	Host ID	Default Sub net Mask
A	xxx.0.0.1	xxx.255.255.254	255.0.0.0
B	xxx.xxx.0.1	xxx.xxx.255.254	255.255.0.0
C	xxx.xxx.xxx.1	xxx.xxx.xxx.254	255.255.255.0

Tabel 3.2 Pembagian kelas IP Address

IP address kelas A diberikan untuk jaringan dengan jumlah host yang sangat besar. Range IP 1.xxx.xxx.xxx. – 126.xxx.xxx.xxx, terdapat 16.777.214 (16 juta) IP address pada tiap kelas A. Pada IP address kelas A, network ID ialah 8 bit pertama, sedangkan host ID ialah 24 bit berikutnya. Dengan demikian, cara membaca IP address kelas A, misalnya 113.46.5.6 ialah:

Network ID = 113

Host ID = 46.5.6

IP address di atas berarti host nomor 46.5.6 pada network nomor 113.

IP address kelas B biasanya dialokasikan untuk jaringan berukuran sedang dan besar. Pada IP address kelas B, network ID ialah 16 bit pertama, sedangkan host ID ialah 16 bit berikutnya. Dengan demikian, cara membaca IP address kelas B, misalnya 132.92.121.1 :

Network ID = 132.92

Host ID = 121.1

IP address di atas berarti host nomor 121.1 pada network nomor 132.92. Dengan panjang host ID 16 bit, network dengan IP

address kelas B dapat menampung sekitar 65000 host. Range IP 128.0.xxx.xxx – 191.155.xxx.xxx.

IP address kelas C awalnya digunakan untuk jaringan berukuran kecil (LAN). Host ID ialah 8 bit terakhir. Dengan konfigurasi ini, bisa dibentuk sekitar 2 juta network dengan masing-masing network memiliki 256 IP address. Range IP 192.0.0.xxx – 223.255.255.x. Pengalokasian IP address pada dasarnya ialah proses memilih network ID dan host ID yang tepat untuk suatu jaringan. Tepat atau tidaknya konfigurasi ini tergantung dari tujuan yang hendak dicapai, yaitu mengalokasikan IP address seefisien mungkin.

3.1.8 Komponen Yang Dibutuhkan Jaringan Komputer LAN

Hardware Yang Dibutuhkan Dalam Jaringan adalah :

- a. Network Interface Card (NIC) berfungsi sebagai Interface Fisik atau penghubung antar komputer menggunakan kabel jaringan ke peralatan penghubung. Card dipasang pada slot tambahan yang terdapat di masing-masing komputer. Setelah card terpasang, pasang kabel jaringan ke port yang terdapat pada NIC agar komputer yang satu dengan yang lain dapat terhubung secara fisik

b. Switch berfungsi menggabungkan beberapa segmen atau kelompok LAN. Switch bekerja di layer 2 pada model referensi OSI. Device ini memiliki kemampuan lebih dibanding dengan repeater atau hub.

3.2 Hasil Penelitian Terdahulu

Tabel 3.3 Berisikan hasil penelitian terdahulu

No	Judul	Nama Pembuat	Metodologi	Keterangan
1.	Optimalisasi Interkoneksi <i>Virtual Private Network</i> (Vpn) Dengan Menggunakan <i>Hardware Based</i> dan Lix (<i>Indonesia Internet Exchange</i>) Sebagai Alternatif Jaringan Skala Luas (Wan)	Deris Stiawan dan Dian Palupi Rini	Analisis kebutuhan jaringan WAN pada sebuah perusahaan melalui studi pustaka dan literatur, Perancangan dan alternatif solusi, Evaluasi hasil	Tulisan ini diharapkan dapat memberikan gambaran tentang alternatif interkoneksi jaringan skala luas (WAN) yaitu teknologi VPN dengan memanfaatkan interkoneksi IIX.
2.	Penggunaan Teknologi Komunikasi Data Berbasis VPN-IP Untuk Pemilihan Umum	Rijal Faadilah dan Djumhadi	Studi literatur, Studi lapangan, Wawancara	Penggunaan teknologi komunikasi data berbasis VPN IP MPLS untuk Pemilu 2009, untuk proses awal seperti scanning Formulir C1-IT, pengiriman data dari KUPD ke KPU Pusat sangat tepat dan sangat aman karena jalur yang digunakan merupakan jalur VPN. Sehingga

				gangguan spam dan hacker pada tahap ini tidak akan terjadi. Namun perlu diantisipasi ketika data tersebut diproses dan diupload ke Web Sever KPU bisa saja pembobolan dari hacker terjadi.
--	--	--	--	--

1. Optimalisasi Interkoneksi *Virtual Private Network* (Vpn) Dengan Menggunakan *Hardware Based* dan *Lix* (*Indonesia Internet Exchange*) Sebagai Alternatif Jaringan Skala Luas (Wan).

Kegiatan untuk komunikasi data langsung ke server suatu kantor, memerlukan suatu teknologi hardware dan dukungan teknis yang rumit sehingga hal ini akan menyebabkan pembiayaan menjadi mahal. Padahal kebutuhan koneksi data berupa sistem informasi yang terintegrasi saat ini sangat tinggi, dari sistem teknologi client server biasa sampai dengan implementasi sistem seperti *ERP*, *Supply Chain*, *CRM*, *E-business* dan sebagainya. Namun tidak semua perusahaan mempunyai anggaran yang banyak terutama untuk membiayai komunikasi data sirkuit, bandwidth dan biaya lainnya dari sebuah provider.

Selama ini pengguna teknologi wide area network (WAN) menjadi salah satu solusi banyak perusahaan untuk komunikasi data. WAN adalah jaringan komunikasi yang meliputi area geografis yang luas dan biasanya

menggunakan fasilitas dari transmisi provider, seperti perusahaan telepon atau lainnya. Infrastruktur inilah yang nantinya menjadi penghubung antara kantor pusat ke kantor cabang-cabang dan *telecomutters*. Namun ada beberapa hal yang harus diperhatikan dalam memilih solusi infrastruktur jaringan komunikasi ini, diantaranya : Bandwidth, Teknologi Skability, Support IP Based, Easy Configuration & maintenance, Low Cost dan security.

Tulisan ini diharapkan dapat memberikan gambaran tentang alternatif interkoneksi jaringan skala luas (WAN) yaitu teknologi VPN dengan memanfaatkan interkoneksi IIX

2. Penggunaan Teknologi Komunikasi Data Berbasis VPN-IP Untuk Pemilihan Umum.

Berbagai kalangan menilai bahwa sistem informasi dan teknologi yang diterapkan oleh Komisi Pemilihan Umum (KPU) untuk Pemilihan Umum (PEMILU) 2009 memang termasuk cukup canggih, namun cukup disesalkan pula karena jumlah server yang disediakan tidak sebanding dengan data yang diupload. Sistem yang diterapkan saat ini berbeda dibandingkan PEMILU 2004 lalu, dimana pada proses tabulasi langsung dilakukan secara online dari berbagai wilayah dan bisa segera terlihat hasilnya. Sedangkan dalam PEMILU 2009 Komisi Pemilihan Umum (KPU) menggunakan teknologi ICR (Intelligent Character Recognition). ICR pada dasarnya merupakan suatu sistem yang mampu mengenali

tulisan tangan dan menterjemahkannya ke dalam kode atau simbol digital sehingga data dapat dimengerti oleh komputer. Terdapat beberapa bagian penting yang terkandung dalam ICR ini, antara lain preprocessing, character segmentation, character recognition.

Preprocessing merupakan teknik dalam pengolahan citra guna meningkatkan kualitas gambar sehingga memudahkan untuk melakukan proses selanjutnya. Lalu character segmentation bertugas menganalisa sebuah citra teks hasil scanning, lalu menemukan lokasi teks dan mengekstrak huruf per huruf untuk diolah pada tahap character recognition. Character recognition sendiri terdiri dari feature extraction dan classification yang bertugas menemukan informasi yang signifikan dari citra sebuah huruf dan merepresentasikannya dalam vector fitur. Kemudian vektor tersebut diolah oleh classifier guna menentukan berbagai jenis huruf yang ada. Seperti diketahui proses perhitungan suara pada PEMILU 2009 ini, KPU telah membuat kesepakatan dengan berbagai pihak bahwa teknologi yang digunakan adalah ICR.

VPN-IP mengkombinasikan berbagai unsur dalam teknologi IP untuk memberi layanan yang memenuhi berbagai komponen layanan komunikasi baku yang ditawarkan oleh teknologi sebelumnya. Semisal yang ditawarkan oleh saluran sewa (leased line), frame relay dan ATM (Asynchronous Transport Mode). Komponen-komponen layanan komunikasi itu, menurut Achmad Sugiarto, GM Datakom Divisi Multi Media PT Telkom (2005), antara lain keandalan, jangkauan, dan

keamanan penggunaan. Teknologi VPN-IP memiliki tingkat fleksibilitas yang lebih baik dibandingkan dengan leased line, frame relay, maupun ATM, dan juga menawarkan solusi yang lebih murah.

Hasil penelitian InternetWeek Research memperlihatkan bahwa alasan utama para manajer teknologi informasi (TI) memilih teknologi VPN-IP dibandingkan dengan teknologi lainnya adalah untuk mengurangi biaya komunikasi yang cukup tinggi. Alasan ini merupakan dasar yang kuat bagi manajer TI untuk menggunakan layanan VPN-IP karena tidak perlu waktu berlama-lama untuk mendapat persetujuan dari manajemen. Lebih dari separuh manajer TI yang diteliti mengatakan bahwa mereka telah dan akan menggunakan layanan VPN-IP dalam waktu enam bulan ke depan dan merencanakan semua layanan komunikasi seperti Intranet, extranet, Internet voice, e-commerce, dan aplikasi multimedia lainnya yang akan diintegrasikan dengan layanan VPN-IP.

- 1) Penggunaan teknologi komunikasi data berbasis VPN IP MPLS untuk Pemilu 2009, untuk proses awal seperti scanning Formulir C1-IT, pengiriman data dari KUPD ke KPU Pusat sangat tepat dan sangat aman karena jalur yang digunakan merupakan jalur VPN. Sehingga gangguan spam dan hacker pada tahap ini tidak akan terjadi. Namun perlu diantisipasi ketika data tersebut diproses dan diupload ke Web Sever KPU bisa saja pembobolan dari hacker terjadi.

- 2) Pemanfaatan fitur layanan pada VPN IP MPLS khususnya layanan data untuk Pemilu 2009 telah dipergunakan secara optimal dari yang disediakan. Perlu dikembangkan fitur-fitur yang lain seperti video conference, VoIP dan aplikasi lain untuk lebih memaksimalkan fitur-fitur yang bisa dilayani oleh jaringan VPN IP MPLS.

BAB IV

METODE PENELITIAN

4.1 Lokasi dan Waktu Penelitian

4.1.1 Lokasi

Penelitian ini dilakukan di kantor Unit Usaha BRT Trans Musi Jl. Demang Lebar Daun No. 507 A.

Penelitian yang saya lakukan pada PT. SARANA PEMBANGUNAN PALEMBANG JAYA dengan Unit Usaha BRT Trans Musi melanjutkan dari Praktek kerja lapangan yang sudah selesai.

4.1.2 Waktu

Adapun penelitian ini dilakukan selama 1 bulan yang dimulai tanggal 01 Februari 2012 sampai dengan 02 Maret 2012.

4.2 Jenis Data

4.2.1 Data Primer

Data Primer menurut pendapat Hasan (2001:33) adalah "data yang diperoleh atau dikumpulkan oleh orang yang melakukan penelitian atau yang bersangkutan memerlukannya. Data Primer disebut juga data asli atau data baru". Data primer didapat langsung

oleh penulis dari para staff karyawan Unit Usaha Bus Rapid Transit (Trans Musi).

4.2.2 Data Sekunder

Data Sekunder menurut pendapat Hasan (2001:33) adalah “data yang diperoleh atau dikumpulkan dari sumber-sumber yang telah ada. Data sekunder disebut juga data tersedia”. Data sekunder disini adalah data yang diperoleh dari para staff karyawan Unit Usaha Bus Rapid Transit (Trans Musi) data tersebut yaitu Sejarah Singkat, Struktur Organisasi, Pembagian Tugas, Data Pekerjaan yang telah atau sedang dikerjakan.

4.3 Teknik Pengumpulan Data

Dalam penulisan skripsi ini teknik pengumpulan data yang dilakukan adalah :

1. Metode Pengamatan (*Observation*)

Yaitu pengumpulan data yang dilakukan dengan mengamati langsung objek yang akan diteliti dan kemudian mencatatnya secara sistematis, contohnya Penulis melihat langsung cara kerja perusahaan dalam jaringan komputer antar kantor.

2. Metode Wawancara (*Interview*)

Yaitu pengumpulan data yang dilakukan dengan cara wawancara atau tanya jawab secara langsung Kepada *Manager* Unit Usaha

Bus Rapid Transit (Trans Musi). tentang Sejarah perusahaan dan Sistem Jaringan Komputer dalam perusahaan tersebut.

3. Metode Pustaka (*Study Literature*)

Yaitu pengumpulan data yang dilakukan dengan cara dibantu buku-buku (dari perpustakaan) yang berhubungan dengan penulisan skripsi ini.

4.4 Jenis Penelitian

Secara umum penelitian dapat diartikan sebagai suatu proses pengumpulan dan analisis data yang dilakukan secara sistematis dan logis untuk mencapai tujuan- tujuan tertentu.

1. Penelitian Ilmiah

Menggunakan kaidah-kaidah ilmiah (Mengemukakan pokok-pokok pikiran, menyimpulkan dengan melalui prosedur yang sistematis dengan menggunakan pembuktian ilmiah/meyakinkan. Ada dua kriteria dalam menentukan kadar/tinggi-rendahnya mutu ilmiah suatu penelitian yaitu:

1. Kemampuan memberikan pengertian yang jelas tentang masalah yang diteliti;
2. Kemampuan untuk meramalkan: sampai dimana kesimpulan yang sama dapat dicapai apabila data yang sama ditemukan di tempat/waktu lain;

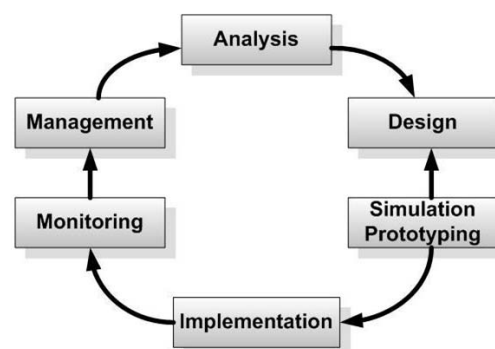
Ciri-ciri penelitian ilmiah adalah:

1. *Purposiveness*, fokus tujuan yang jelas;
 2. *Rigor*, teliti, memiliki dasar teori dan disain metodologi yang baik;
 3. *Testibility*, prosedur pengujian hipotesis jelas
 4. *Replicability*, Pengujian dapat diulang untuk kasus yang sama atau yang sejenis;
 5. *Objectivity*, Berdasarkan fakta dari data aktual : tidak subjektif dan emosional;
 6. *Generalizability*, Semakin luas ruang lingkup penggunaan hasilnya semakin berguna;
 7. *Precision*, Mendekati realitas dan *confidence* peluang kejadian dari estimasi dapat dilihat;
 8. *Parsimony*, Kesederhanaan dalam pemaparan masalah dan metode penelitiannya
2. Penelitian non ilmiah (Tidak menggunakan metode atau kaidah-kaidah ilmiah
- Berdasarkan Spesialisasi Bidang (ilmu) garapannya : Bisnis (Akunting, Keuangan, Manajemen, Pemasaran), Komunikasi (Massa, Bisnis, Kehumasan/PR, Periklanan), Hukum (Perdata, Pidana, Tatanegara, Internasional), Pertanian (agribisnis,

- Berdasarkan dari hadirnya variabel (ubahan) : variabel adalah hal yang menjadi objek penelitian, yang ditatap, yang menunjukkan variasi baik kuantitatif maupun kualitatif. Variabel : masa lalu, sekarang, akan datang. Penelitian yang dilakukan dengan menjelaskan / menggambarkan variabel masa lalu dan sekarang (sedang terjadi) adalah penelitian deskriptif (*to describe* = membeberkan/menggambarkan). Penelitian dilakukan terhadap variabel masa yang akan datang adalah penelitian eksperimen.

4.5 Teknik Pengembangan Sistem

Dalam penelitian ini hanya menggunakan beberapa teknik pengembangan sistem yang di ambil dari tahapan dalam NDLC yang sesuai dengan penelitian ini.



Gambar 1. NDLC

Sumber : diolah sendiri

Gambar 4.1 NDLC

Pada gambar di atas dapat dilihat terdapat enam tahapan dalam NDLC dan pada penelitian ini saya hanya menggunakan empat tahapan yaitu Analysis, Design, Simulation Prototyping dan Implementasi yang penjelasannya sebagai berikut:

1. **Analysis** : Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan user, dan analisa topologi / jaringan yang sudah ada saat ini. Metode yang biasa digunakan pada tahap ini diantaranya ;
 - a. Wawancara, dilakukan dengan pihak terkait melibatkan dari struktur manajemen atas sampai ke level bawah / operator agar mendapatkan data yang konkrit dan lengkap. pada kasus di Computer Engineering biasanya juga melakukan brainstorming juga dari pihak vendor untuk solusi yang ditawarkan dari vendor tersebut karena setiap mempunyai karakteristik yang berbeda
 - b. survey langsung lapangan, pada tahap analisis juga biasanya dilakukan survey langsung lapangan untuk mendapatkan hasil sesungguhnya dan gambaran seutuhnya sebelum masuk ke tahap design, survey biasa dilengkapi dengan alat ukur seperti GPS dan alat lain sesuai kebutuhan untuk mengetahui detail yang dilakukan.
 - c. membaca manual atau blueprint dokumentasi, pada analysis awal ini juga dilakukan dengan mencari informasi dari manual-manual atau blueprint dokumentasi yang mungkin pernah dibuat sebelumnya. Sudah menjadi keharusan dalam setiap pengembangan

suatu sistem dokumentasi menjadi pendukung akhir dari pengembangan tersebut, begitu juga pada project network, dokumentasi menjadi syarat mutlak setelah sistem selesai dibangun.

d. menelaah setiap data yang didapat dari data-data sebelumnya, maka perlun dilakukan analisa data tersebut untuk masuk ke tahap berikutnya. Adapun yang bias menjadi pedoman dalam mencari data pada tahap analysis ini adalah ;

- User / people : jumlah user, kegiatan yang sering dilakukan, peta politik yang ada, level teknis user
- Media H/W & S/W : peralatan yang ada, status jaringan, ketersediaan data yang dapat diakses dari peralatan, aplikasi s/w yang digunakan
- Data : jumlah pelanggan, jumlah inventaris sistem, sistem keamanan yang sudah ada dalam mengamankan data.
- Network : konfigurasi jaringan, volume trafik jaringan, protocol, monitoring network yang ada saat ini, harapan dan rencana pengembangan kedepan
- Perencanaan fisik : masalah listrik, tata letak, ruang khusus, system keamanan yang ada, dan kemungkinan akan pengembangan kedepan.

2. **Design** : Dari data-data yang didapatkan sebelumnya, tahap Design ini akan membuat gambar design topology jaringan interkoneksi yang

akan dibangun, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada. Design bias berupa *design struktur topology, design akses data, design tata layout perkabelan, dan sebagainya* yang akan memberikan gambaran jelas tentang project yang akan dibangun.

Biasanya hasil dari design berupa ;

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

3. **Simulation Prototype** : beberapa networker's akan membuat dalam bentuk simulasi dengan bantuan Tools khusus di bidang network seperti BOSON, PACKET TRACERT, NETSIM, dan sebagainya, hal ini dimaksudkan untuk melihat kinerja awal dari network yang akan dibangun dan sebagai bahan presentasi dan sharing dengan team work lainnya. Namun karena keterbatasan perangkat lunak simulasi ini, banyak para networker's yang hanya menggunakan alat Bantu tools VISIO untuk membangun topology yang akan didesign.
4. **Implementation** : di tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam implementasi networker's akan menerapkan semua yang telah direncanakan dan di design sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil / gagalnya project yang akan dibangun dan ditahap inilah

Team Work akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis.

Ada beberapa Masalah-masalah yang sering muncul pada tahapan ini, diantaranya ;

- a. jadwal yang tidak tepat karena faktor-faktor penghambat,
- b. masalah dana / anggaran dan perubahan kebijakan
- c. team work yang tidak solid
- d. peralatan pendukung dari vendor

makanya dibutuhkan manajemen project dan manajemen resiko untuk meminimalkan sekecil mungkin hambatan-hambatan yang ada.

BAB V

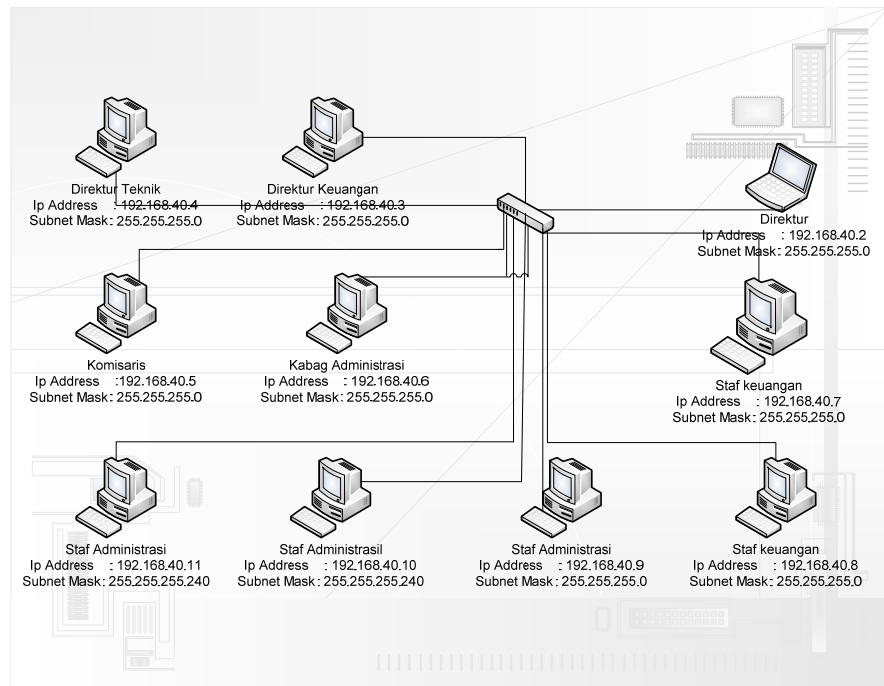
HASIL DAN PEMBAHASAN

5.1 Hasil

5.1.1 Topologi Jaringan

a. PT. Sarana Pembangunan Palembang Jaya

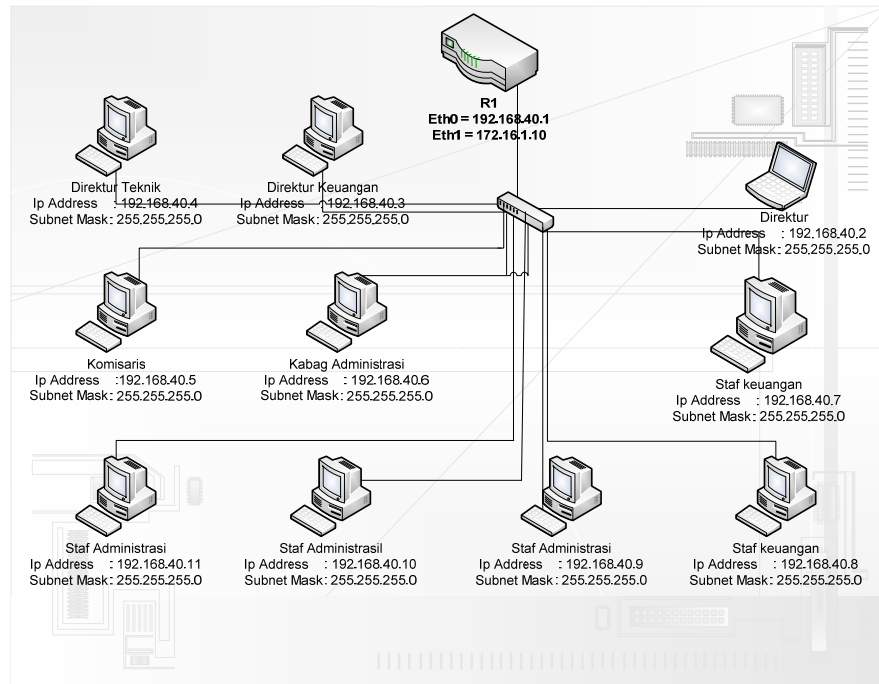
Topologi yang digunakan PT. Sarana Pembangunan Palembang Jaya menggunakan topologi star yang terdiri dari 10 (sepuluh) PC terhubung dengan switch dan sebuah DNS Server.



Sumber : diolah sendiri

Gambar 5.1 Topologi Jaringan PT. Sarana Pembangunan Palembang Jaya sebelum penambahan Router1

Topologi ini adalah kelanjutan dari topologi PT. Sarana Pembangunan Palembang Jaya sebelumnya hanya saja terjadi penambahan sebuah Router1.

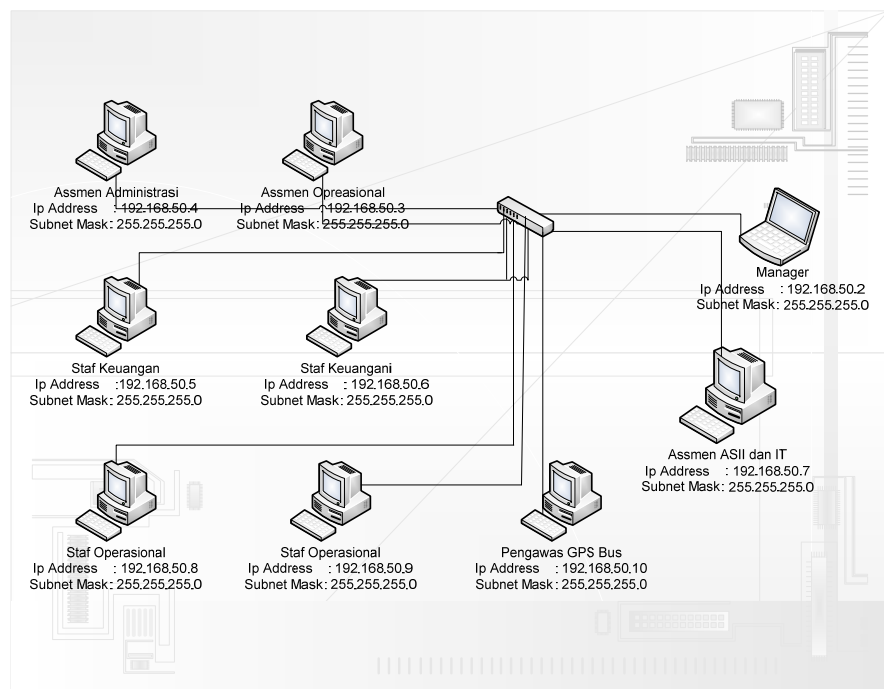


Sumber : diolah sendiri

Gambar 5.2 Topologi Jaringan PT. Sarana Pembangunan Palembang Jaya sesudah penambahan Router 1.

b. Unit Usaha Bus Rapid Transit BRT Trans Musi

Topologi yang digunakan Unit Usaha Bus Rapid Transit BRT Trans Musi menggunakan topologi star yang terdiri dari 9 (sembilan) PC terhubung dengan switch dan sebuah DNS Server.

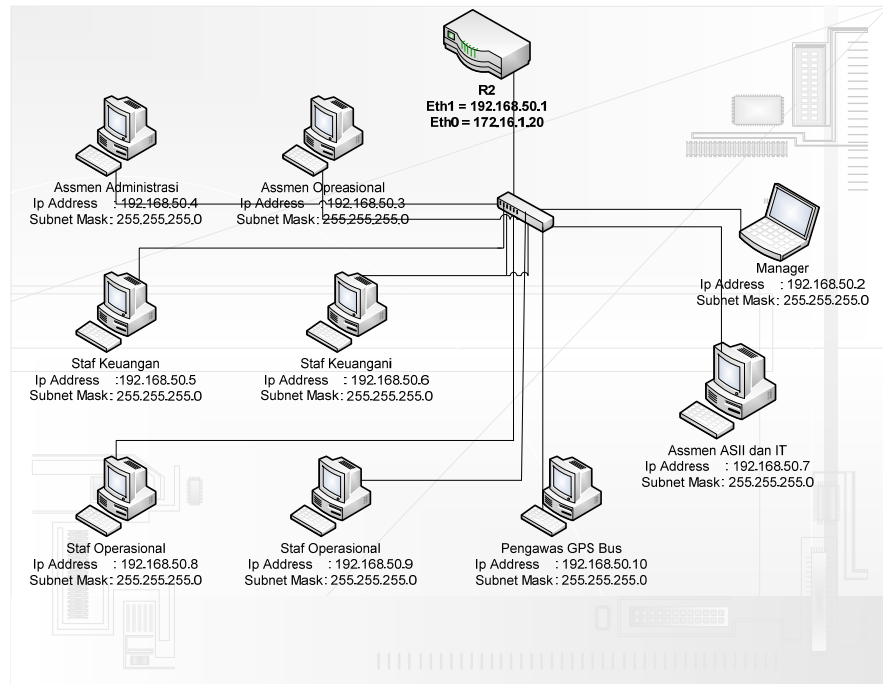


Sumber : diolah sendiri

Gambar 5.3 Topologi Jaringan Unit Usaha Bus Rapid Transit BRT

Trans Musi.

Topologi ini adalah kelanjutan dari topologi Unit Usaha Bus Rapid Transit BRT Trans Musi Jaya sebelumnya hanya saja terjadi penambahan sebuah Router 2.



Sumber : diolah sendiri

Gambar 5.4 Topologi Jaringan Unit Usaha Bus Rapid Transit Trans Musi sesudah penambahan Router 2.

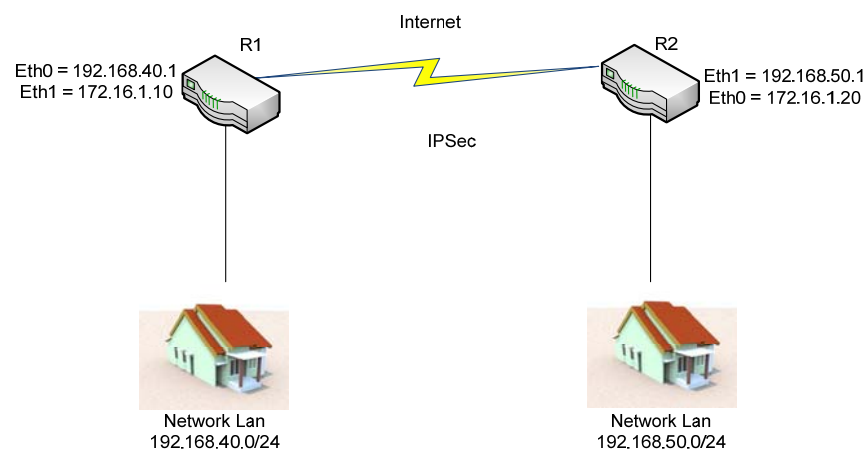
5.1.2 Spesifikasi Komputer

Spesifikasi komputer yang terdapat pada PT. Sarana Pembangunan Palembang Jaya dan Unit Usaha Bus Rapid Transit BRT Trans Musi yaitu :

1. Motherboard
2. Prosesor

3. Memory 2 Gb DDR3
4. Harddisk 320 Gb
5. Monitor LCD 14.0"
6. Keyboard + Mouse

5.1.3 Desain Topologi



Sumber : diolah sendiri

Gambar 5.5 Desain topologi jaringan VPN server

5.1.4 Spesifikasi Komputer Server

Untuk menunjang pembangunan project VPN Server maka penulis mengusulkan pengadaan sebuah server, dimana server itu nanti akan mengatur data sehingga lebih teratur. Adapun kriteria komputer bisa dijadikan sebagai computer VPN Server yaitu :

1. Motherboard
2. Prosesor

3. Memory 2 Gb DDR3
4. Harddisk 320 Gb
5. Monitor LCD 14.0"
6. Keyboard + Mouse
7. DVD-super multi DL Drive
8. LAN Card TP-Link 10/100 Mbps

5.1.5 Konfigurasi Router 1

Pertama masuk ke konsole vyatta dan masukkan password

```
Login as:vyatta
Welcome to vyatta
vyatta@192.168.40.1's password
```

Gambar 5.6 Tampilan Perintah masuk ke konsole vyatta pada router 1

Setelah melakukan penginstallan vyatta pada computer server dan masuk ke konsole vyatta dengan cara login dengan nama vyatta dan masukkan password 12345.

5.1.6 Setting Host Name dan IP Address

Ketikan configure untuk masuk dan setting Host Name dan IP Address.

```
vyatta@~$ configure
```

Gambar 5.7 Tampilan Perintah configure

Pada perintah ini fungsi *configure* menghilangkan tanda ~\$ dan masuk ketahap settingan.


```
vyatta@~t# set system host-name sp2j-r1
```

Gambar 5.8 Tampilan Perintah setting host-name

Setelah berubah tanda ~\$ menjadi # maka langsung bisa setting host-name untuk router 1 yang diberi nama sp2j-r1.

```
vyatta@sp2j-r1# set interfaces ethernet eth0 address 192.168.40.1/24
```

Gambar 5.9 Tampilan Perintah setting ip pada eth0 untuk local

Tahap selanjutnya setting ip pada eth0 untuk local pada router 1 yaitu 192.168.40.1/24.

```
vyatta@sp2j-r1# set interfaces ethernet eth1 address 172.16.1.10/16
```

Gambar 5.10 Tampilan Perintah setting ip di eth1 untuk router 1

Sama seperti tahapan sebelumnya setting ip eth1 ini berfungsi sebagai ip yang akan digunakan pada router 1.

```
vyatta@sp2j-r1# commit
```

Gambar 5.11 Tampilan Perintah commit

Perintah *commit* berguna melakukan apply pada setiap settingan atau edit yang telah kita lakukan.

```
vyatta@sp2j-r1# save
```

Gambar 5.12 Tampilan Perintah save

Setiap selesai melakukan settingan dan editan sebaiknya ketikkan perintah *save* agar tersimpan.

5.1.7 Cek Interface

Pada langkah ini untuk melihat IP Address sudah terpasang dengan benar.

```
vyatta@sp2j-r1# show interfaces
ethernet eth0 {
    address 192.168.40.1/24
    hw-id 00:e0:4c:13:76:db
}
ethernet eth1 {
    address 172.16.1.10/16
    hw-id 90:f6:52:04:b9:14
}
loopback lo {
}
```

Gambar 5.13 Tampilan Perintah untuk melihat IP Address

Perintah *show interfaces* untuk melihat settingan atau editan yang telah kita lakukan sudah benar atau belum.

5.1.8 Setting Interface IPsec

Perintah ini untuk setting interface IPsec pada Router 1

```
vyatta@sp2j-r1# set vpn ipsec ipsec-interfaces interface eth1
```

Gambar 5.14 Tampilan Perintah untuk setting IPsec di eth1 pada Router 1

Langkah ini dimana melakukan settingan IPsec di eth1 pada router1 disinilah kita membuat suatu terowongan jaringan yang rahasia.

```
vyatta@sp2j-r1# show vpn ipsec ipsec-interfaces  
+interface eth1
```

Gambar 5.15 Tampilan Perintah ipsec-interfaces

Perintah selanjutnya melihat apakah ipsec yang telah kita pasang pada eth1 sudah benar atau belum maka ketikkan *show von ipsec ipsec-interfaces*.

5.1.9 Setting Ike Group dan Proposal

Perintah selanjutnya setting Ike Group dan Proposal

```
vyatta@sp2j-r1# set vpn ipsec ike-group router1 proposal 1
```

Gambar 5.16 Tampilan Perintah settingan ike-group router 1 proposal 1

Pada perintah ini melakukan *ike-group router1 proposal 1* adalah *Internet Key Exchange (IKE)* yaitu melakukan pengajuan group protocol pada router 1.

```
vyatta@sp2j-r1# set vpn ipsec ike-group router1 proposal 1
encrvption aes256
```

Gambar 5.17 Tampilan Perintah settingan encryption

Setelah melukan pengajuan group protocol selanjutnya menambahkan perintah sebelumnya dengan perintah *encryption aes256* yaitu memasang enkripsi 256 bit sehingga data akan melewati router 1 akan di enkripsikan terlebih dahulu sebelum sampai ke client.

```
vyatta@sp2j-r1# set vpn ipsec ike-group router1 proposal 1 dh-group 2
```

Gambar 5.18 Tampilan Perintah setting dh-group 2

Setelah setting enkripsi selanjutnya setting *dh-group 2* yaitu untuk mengatur pertukaran kunci atau password, makin lama no dh nya makin aman tapi membutuhkan waktu agak lama dalam proses tersebut.

```
vyatta@sp2j-r1# show vpn ipsec ike-group router1
+proposal 1 {
+  dh-group 2
+  encryption aes256
+}
```

Gambar 5.19 Tampilan Perintah show ike-group router1

Selanjutnya melihat hasil dari setting yang sudah dilakukan benar atau belum dengan ketikkan *show vpn ipsec ike-group router1*.

5.1.10 Setting ESP group dan proposal

Perintah selanjutnya setting ESP dan proposal pada router 1

```
vyatta@sp2j-r1# set vpn ipsec esp-group router1 proposal 1
```

Gambar 5.20 Tampilan Perintah esp-group router1 proposal 1

Setelah setting ike group maka selanjutnya melakukan setting *esp-group router1 proposal1* sama seperti settingan ike-group hanya *esp-group* bertujuan melakukan pengamana pada public.

```
vyatta@sp2j-r1# set vpn ipsec esp-group router1 proposal 1
encrvption aes256
```

Gambar 5.21 Tampilan Perintah esp-group router1 proposal 1 encryption

Setelah melukan pengajuan *asp-group* selanjutnya menambahkan perintah sebelumnya dengan perintah *encryption aes256* yaitu

memasangkan enkripsi 256 bit sehingga data akan melewati router 1 akan di enkripsikan terlebih dahulu sebelum sampai ke client.

```
vyatta@sp2j-r1# show vpn ipsec esp-group router1
+proposal 1 {
+  encryption aes256
+}
```

Gambar 5.22 Tampilan perintah show esp-group

Lain dengan settingan ike-group di esp-group tidak lagi melakukan perintah dh-group dan langsung melihat hasil dari settingan esp-group dengan ketikan *show vpn ipsec esp-group router1*.

5.1.11 Setting IPSec Site to site

Perintah selanjutnya setting IPSec site to site

```
vyatta@sp2j-r1# set vpn ipsec site-to-site peer 172.16.1.20
```

Gambar 5.23 Tampilan perintah setting site-to-site

Perintah selajutnya adalah membuat sistem *site-to-site* yaitu situs ke situs yang ditujukan pada ip router 2 guna menghubungkan antara Router 1 dan Router 2 dan memasukkan ip Router 2 dengan cara mengetikkan *set vpn ipsec site-to-site peer 172.16.1.20*.

```
vyatta@sp2j-r1# set vpn ipsec site-to-site peer 172.16.1.20
authentication mode pre-shared-secret
```

Gambar 5.24 Tampilan perintah setting authentication mode pre-shared-secret

Setelah melakukan settingan site-to-site maka perintah selanjutnya menambahkan *authentication mode pre-shared-secret* yaitu memasangkan autentikasi rahasia pada jaringan tersebut.

```
vyatta@sp2j-r1# edit vpn ipsec site-to-site peer 172.16.1.20
[edit vpn ipsec site-to-site peer 172.16.1.20]
```

Gambar 5.25 Tampilan perintah edit vpn ipsec site-to-site peer 172.16.1.20

Setelah memasukkan perintah autentikasi pada antar jaringan router 1 dan router 2 tahap selanjutnya adalah mengaktifkan sistem yang telah kita buat tadi dan menambahkan [*edit vpn ipsec site-to-site peer 172.16.1.20*].

```
vyatta@sp2j-r1# set authentication pre-shared-secret udinpalcom
```

Gambar 5.26 Tampilan perintah set authentication pre-shared-secret

Pada tahap ini dibutuhkan sebuah password rahasia untuk menghubungkan antara router 1 dan router 2 dan pada setiap router password yang digunakan harus sama, dapat dilihat *udinpalcom* yang menjadi password rahasia tersebut.

```
vyatta@sp2j-r1# set ike-group router1
```

Gambar 5.27 Tampilan perintah set ike-group router 1

Sebelumnya settingan ike-group sudah dilakukan dan pada tahap ini hanya mengaktifkan ike-group di dalam settingan site-to-site ini dengan perintah *set ike-group router1*.

```
vyatta@sp2j-r1# set local-ip 172.16.1.10
```

Gambar 5.28 Tampilan perintah set local-ip

Selanjutnya masukkan juga ip dari router 1 dengan perintah *set local-ip 172.16.1.10* ini bertujuan mengaktifkan ip router 1.

```
vyatta@sp2j-r1# set tunnel 1 local-subnet 192.168.40.0/24
```

Gambar 5.29 Tampilan perintah set tunnel 1 local-subnet

Setelah mengaktifkan ip router 1 selanjutnya setting ip local pada router 1 ataupun perusahaan utama dengan perintah *set tunnel 1 local-subnet 192.168.40.0/24*.

```
vyatta@sp2j-r1# set tunnel 1 remote-subnet 192.168.50.0/24
```

Gambar 5.30 Tampilan perintah set tunnel 1 remote-subnet

Setelah setting ip local pada router 1 selanjutnya *remote* ip local dari router 2 atau perusahaan cabang dengan perintah *set tunnel 1*

remote-subnet 192.168.50.0/24 agar client dari router 1 dan client dari router 2 dapat saling berhubungan dengan melewati antar router.

```
vyatta@sp2j-r1# set tunnel 1 esp-group router1
```

Gambar 5.31 Tampilan perintah set tunnel 1 esp-group Router 1

Sama seperti ike-group, esp-group juga harus diaktifkan pada settingan site-to-site ini dengan cara *set tunnel 1 esp-group router1* ini bertujuan jika antar client dari masing-masing router berinteraksi maka akan dibaca oleh router 1.

```
vyatta@sp2j-r1# commit
```

Gambar 5.32 Tampilan perintah commit

Sama seperti settinga yang lain, pada akhir settinga jangan lupa melakukan *apply* atau mengaktifkan setiap settingan yang telah dilakukan dengan perintah *commit*.

```
vyatta@sp2j-r1# save
```

Gambar 5.33 Tampilan perintah save

Pada setiap akhir dari semua settingan ada baiknya melakukan penyimpanan dengan perintah *save*.

```
vyatta@sp2j-r1# show vpn ipsec site-to-site peer 172.16.1.20

authentication {
    pre-shared-secret udinpalcom
}

ike-group router1

local-ip 172.16.1.10

tunnel 1 {
    esp-group router1

    local-subnet 192.168.40.0/24

    remote-subnet 192.168.50.0/24
}
```

Gambar 5.34 Tampilan perintah show vpn ipsec site-to-site peer

Untuk melihat seluruh settingan yang telah dilakukan pada konfigurasi site-to-site apakah sudah benar atau belum maka ketikkan perintah *show vpn ipsec site-to-site peer 172.16.1.20*.

5.1.12 Konfigurasi Router 2

Sama seperti router 1 pertama masuk ke konsol vyatta dan masukkan password.

```
Login as:vyatta
Welcome to vyatta
vyatta@192.168.50.1's password
```

Gambar 5.35 Tampilan Perintah masuk ke konsol vyatta pada router 2

Setelah melakukan penginstallan vyatta pada computer server dan masuk ke konsol vyatta dengan cara login dengan nama vyatta dan masukkan password 12345.

5.1.13 Setting Nama Host Name dan IP Address

Ketikan configure untuk masuk dan setting Host Name dan IP Address.

```
vyatta@~$ configure
```

Gambar 5.36 Tampilan Perintah configure

Pada perintah ini fungsi *configure* menghilangkan tanda ~\$ dan masuk ketahap settingan.

```
vyatta@~t# set system host-name sp2j-r2
```

Gambar 5.37 Tampilan Perintah setting host-name

Setelah berubah tanda ~\$ menjadi # maka langsung bisa setting host-name untuk router 2 yang diberi nama sp2j-r2.

```
vyatta@sp2j-r2# set interfaces ethernet eth0 address 172.16.1.20/16
```

Gambar 5.38 Tampilan Perintah configure set eth0 untuk ip router 2

Sama seperti tahapan konfigurasi pada router 1 sebelumnya setting ip eth1 ini berfungsi sebagai ip yang akan digunakan pada router 2.

```
vyatta@sp2j-r2# set interfaces ethernet eth1 address 192.168.50.1/24
```

Gambar 5.39 Tampilan Perintah configure set eth1 untuk ip local

Tahap selanjutnya setting ip pada eth0 untuk local pada router 2 yaitu 192.168.50.1/24.

```
vyatta@sp2j-r2# commit
```

Gambar 5.40 Tampilan Perintah commit

Perintah *commit* berguna melakukan apply pada setiap settingan atau edit yang telah kita lakukan.

```
vyatta@sp2j-r2# save
```

Gambar 5.41 Tampilan Perintah save

Setiap selesai melakukan settingan dan editan sebaiknya ketikkan perintah *save* agar tersimpan.

5.1.14 Cek Interface

Pada langkah ini untuk melihat IP Address sudah terpasang dengan benar.

```
vyatta@sp2j-r2# show interfaces
ethernet eth0 {
    address 172.16.1.20/16
    hw-id b8:a3:86:98:0a:0b
}
ethernet eth1 {
    address 192.168.50.1/24
    hw-id 74:ea:3a:85:be:d9
}
loopback lo {
}
```

Gambar 5.42 Tampilan Perintah untuk melihat IP Address

Perintah *show interfaces* untuk melihat settingan atau editan yang telah kita lakukan sudah benar atau belum.

5.1.15 Setting Interface IPSec

Perintah ini untuk setting interface IPSec pada Router 2

```
vyatta@sp2j-r2# set vpn ipsec ipsec-interfaces interface eth0
```

Gambar 5.43 Tampilan Perintah untuk setting IPSec di eth0 pada router 2

kebalikan dari router 1 dimana melakukan settingan IPsec di eth0 pada router 2 disinilah kita membuat suatu terowongan jaringan yang rahasia.

```
vyatta@sp2j-r2# show vpn ipsec ipsec-interfaces
+interface eth0
```

Gambar 5.44 Tampilan Perintah ipsec-interfaces

Perintah selanjutnya melihat apakah ipsec yang telah kita pasang pada eth0 sudah benar atau belum maka ketikkan *show von ipsec ipsec-interfaces*.

5.1.16 Setting Ike Group dan Proposal

Perintah selanjutnya setting Ike Group dan Proposal

```
vyatta@sp2j-r2# set vpn ipsec ike-group router2 proposal 1
```

Gambar 5.45 Tampilan Perintah settingan ike-group router2 proposal 1

Pada perintah ini melakukan *ike-group route2 proposal 1* adalah *Internet Key Exchange (IKE)* yaitu melakukan pengajuan group protocol pada router 2.

```
vyatta@sp2j-r2# set vpn ipsec ike-group router2 proposal 1
  encryption aes256
```

Gambar 5.46 Tampilan Perintah settingan encryption

Sama seperti router 1 pengajuan group protocol selanjutnya menambahkan perintah sebelumnya dengan perintah *encryption aes256* yaitu memasang enkripsi 256 bit sehingga data akan melewati router 2 akan di enkripsikan terlebih dahulu sebelum sampai ke client.

```
vyatta@sp2j-r2# set vpn ipsec ike-group router2 proposal 1 dh-group 2
```

Gambar 5.47 Tampilan Perintah setting dh-group 2

Setelah setting enkripsi selanjutnya setting *dh-group 2* yaitu untuk mengatur pertukaran kunci atau password, makin lama no dh nya makin aman tapi membutuhkan waktu agak lama dalam proses tersebut.

```
vyatta@sp2j-r2# show vpn ipsec ike-group router2
+proposal 2 {
+  dh-group 2
+  encryption aes256
+}
```

Gambar 5.48 Tampilan Perintah show ike-group router2

Selanjutnya melihat hasil dari setting yang sudah dilakukan benar atau belum dengan ketikkan *show vpn ipsec ike-group router2*.

5.1.17 Setting ESP group dan proposal

Perintah selanjutnya setting ESP dan proposal pada router 2

```
vyatta@sp2j-r2# set vpn ipsec esp-group router2 proposal 1
```

Gambar 5.49 Tampilan Perintah esp-group router2 proposal 1

Setelah setting ike group maka selanjutnya melakukan setting *esp-group router2 proposal1* sama seperti settingan ike-group hanya esp-group bertujuan melakukan pengamana pada public.

```
vyatta@sp2j-r2# set vpn ipsec esp-group router2 proposal 1
encryption aes256
```

Gambar 5.50 Tampilan Perintah esp-group router2 proposal 1 encryption

Sama seperti pada router 1 setelah melukan pengajuan *esp-group* selanjutnya menambahkan perintah sebelumnya dengan perintah *encryption aes256* yaitu memasang enkripsi 256 bit sehingga data akan melewati router 2 akan di enkripsikan terlebih dahulu sebelum sampai ke client.


```
vyatta@sp2j-r2# show vpn ipsec esp-group router2
+proposal 1 {
+  encryption aes256
+}
```

Gambar 5.51 Tampilan perintah show esp-group

Lain dengan settingan ike-group di esp-group tidak lagi melakukan perintah dh-group dan langsung melihat hasil dari settingan esp-group dengan ketikan *show vpn ipsec esp-group router2*.

5.1.18 Setting IPSec Site to site

Perintah selanjutnya setting IPSec site to site

```
vyatta@sp2j-r2# set vpn ipsec site-to-site peer 172.16.1.10
```

Gambar 5.52 Tampilan perintah setting site-to-site

Perintah selajutnya adalah membuat system *site-to-site* yaitu situs ke situs yang mana menghubungkan antara Router 1 dan Router 2 dan memasukkan ip Router 1 dengan cara mengetikkan *set vpn ipsec site-to-site peer 172.16.1.10*.

```
vyatta@sp2j-r2# set vpn ipsec site-to-site peer 172.16.1.10
authentication mode pre-shared-secret
```

Gambar 5.53 Tampilan perintah setting authentication mode pre-shared-secret

Setelah melakukan settingan site-to-site maka perintah selanjutnya menambahkan *authentication mode pre-shared-secret* yaitu memasang autentikasi rahasia pada jaringan tersebut.

```
vyatta@sp2j-r2# edit vpn ipsec site-to-site peer 172.16.1.10  
[edit vpn ipsec site-to-site peer 172.16.1.10]
```

Gambar 5.54 Tampilan perintah edit vpn ipsec site-to-site peer 172.16.1.10

Sama seperti pada router 1 setelah memasukkan perintah autentikasi pada antar jaringan router 2 dan router 1 tahap selanjutnya adalah mengaktifkan sistem yang telah kita buat tadi dan menambahkan *[edit vpn ipsec site-to-site peer 172.16.1.10]*.

```
vyatta@sp2j-r2# set authentication pre-shared-secret udinpalcom
```

Gambar 5.55 Tampilan perintah set authentication pre-shared-secret

Pada tahap ini dibutuhkan sebuah password rahasia untuk menghubungkan antara router 2 dan router 1 dan pada setiap router password yang digunakan harus sama, dapat dilihat *udinpalcom* yang menjadi password rahasia tersebut.

```
vyatta@sp2j-r2# set ike-group router2
```

Gambar 5.56 Tampilan perintah set ike-group Router 2

Sebelumnya settingan ike-group sudah dilakukan dan pada tahap ini hanya mengaktifkan ike-group di dalam settingan site-to-site ini dengan perintah *set ike-group router2*.

```
vyatta@sp2j-r2# set local-ip 172.16.1.20
```

Gambar 5.57 Tampilan perintah set local-ip

Selanjutnya masukkan juga ip dari router 2 dengan perintah *set local-ip 172.16.1.20* ini bertujuan mengaktifkan ip router 2.

```
vyatta@sp2j-r2# set tunnel 1 local-subnet 192.168.50.0/24
```

Gambar 5.58 Tampilan perintah set tunnel 1 local-subnet

Setelah mengaktifkan ip router 2 selanjutnya setting ip local pada router 1 ataupun perusahaan utama dengan perintah *set tunnel 1 local-subnet 192.168.50.0/24*.

```
vyatta@sp2j-r2# set tunnel 1 remote-subnet 192.168.40.0/24
```

Gambar 5.59 Tampilan perintah set tunnel 1 remote-subnet

Setelah setting ip local pada router 2 selanjutnya *remote* ip local dari router 1 atau perusahaan cabang dengan perintah *set tunnel 1 remote-subnet 192.168.40.0/24* agar client dari router 2 dan client dari router 1 dapat saling berhubungan dengan melewati antar router.

```
vyatta@sp2j-r2# set tunnel 1 esp-group router2
```

Gambar 5.60 Tampilan perintah set tunnel 1 esp-group Router 1

Sama seperti ike-group, esp-group juga harus diaktifkan pada settingan site-to-site ini dengan cara *set tunnel 1 esp-group router2* ini bertujuan jika antar client dari masing-masing router berinteraksi maka akan dibaca oleh router 2.

```
vyatta@sp2j-r2# commit
```

Gambar 5.61 Tampilan perintah commit

Sama seperti settinga yang lain, pada akhir settinga jangan lupa melakukan *apply* atau mengaktifkan setiap settingan yang telah dilakukan dengan perintah *commit*.

```
vyatta@sp2j-2# save
```

Gambar 5.62 Tampilan perintah save

Pada setiap akhir dari semua settingan ada baiknya melakukan penyimpanan dengan perintah *save*.

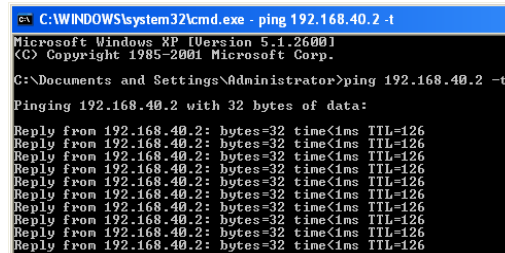
```
vyatta@sp2j-r2# show vpn ipsec site-to-site peer 172.16.1.10
authentication {
  pre-shared-secret udinpalcom
}
ike-group router2
local-ip 172.16.1.20
tunnel 1 {
  esp-group router2
  local-subnet 192.168.50.0/24
  remote-subnet 192.168.40.0/24
}
```

Gambar 5.63 Tampilan perintah show vpn ipsec site-to-site peer

Untuk melihat seluruh settingan yang telah dilakukan pada konfigurasi site-to-site apakah sudah benar atau belum maka ketikkan perintah *show vpn ipsec site-to-site peer 172.16.1.20*.

5.1.19 Hasil Koneksi Router 1

1. Ping dari client router 2 ke client router 1



```

C:\WINDOWS\system32\cmd.exe - ping 192.168.40.2 -t
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.40.2 -t
Pinging 192.168.40.2 with 32 bytes of data:

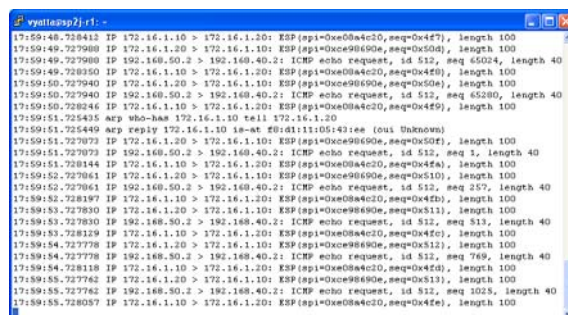
Reply from 192.168.40.2: bytes=32 time<1ms TTL=126
Reply from 192.168.40.2: bytes=32 time<1ms TTL=126
Reply from 192.168.40.2: bytes=32 time<1ms TTL=126
Reply from 192.168.40.2: bytes=32 time<1ms TTL=126
Reply from 192.168.40.2: bytes=32 time<1ms TTL=126
Reply from 192.168.40.2: bytes=32 time<1ms TTL=126
Reply from 192.168.40.2: bytes=32 time<1ms TTL=126
Reply from 192.168.40.2: bytes=32 time<1ms TTL=126
Reply from 192.168.40.2: bytes=32 time<1ms TTL=126
Reply from 192.168.40.2: bytes=32 time<1ms TTL=126

```

Gambar 5.64 Tampilan Ping dari client router 2 ke client router 1

Setelah semua router berjalan dengan baik, maka tahap selanjutnya membuktikan hasil koneksi antar client dari masing-masing router dan yang pertama ialah bagaimana client dari router 2 ping lewat Run Cmd ke client pada router 1 dan hasilnya Reply from yang berarti antara client dari router 2 dan client router 1 sudah terkoneksi dengan baik.

Hasil Tcpdump dari ping client router 2 ke client router 1



```

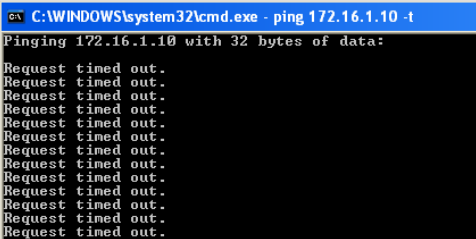
vyn1esppzj,1: -
17:59:46.728413 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xe084c20,seq=0x447), length 100
17:59:49.727980 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xc98690e,seq=0x50d), length 100
17:59:49.727980 IP 192.168.50.2 > 192.168.40.2: ICMP echo request, id 512, seq 45024, length 40
17:59:49.728350 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xe084c20,seq=0x448), length 100
17:59:50.727940 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xc98690e,seq=0x50e), length 100
17:59:50.727940 IP 192.168.50.2 > 192.168.40.2: ICMP echo request, id 512, seq 45030, length 40
17:59:50.728246 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xe084c20,seq=0x449), length 100
17:59:51.725435 arp who-has 172.16.1.10 tell 172.16.1.20
17:59:51.725449 arp reply 172.16.1.10 is-at 80:81:11:05:43:ea (oui Unknown)
17:59:51.727073 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xc98690e,seq=0x50f), length 100
17:59:51.727073 IP 192.168.50.2 > 192.168.40.2: ICMP echo request, id 512, seq 1, length 40
17:59:51.728144 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xe084c20,seq=0x44a), length 100
17:59:52.727061 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xc98690e,seq=0x510), length 100
17:59:52.727061 IP 192.168.50.2 > 192.168.40.2: ICMP echo request, id 512, seq 257, length 40
17:59:52.728197 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xe084c20,seq=0x44b), length 100
17:59:53.727830 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xc98690e,seq=0x511), length 100
17:59:53.728129 IP 192.168.50.2 > 192.168.40.2: ICMP echo request, id 512, seq 513, length 40
17:59:53.728129 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xe084c20,seq=0x44c), length 100
17:59:54.727778 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xc98690e,seq=0x512), length 100
17:59:54.727778 IP 192.168.50.2 > 192.168.40.2: ICMP echo request, id 512, seq 746, length 40
17:59:54.728118 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xe084c20,seq=0x44d), length 100
17:59:55.727762 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xc98690e,seq=0x513), length 100
17:59:55.727762 IP 192.168.50.2 > 192.168.40.2: ICMP echo request, id 512, seq 1023, length 40
17:59:55.728057 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xe084c20,seq=0x44e), length 100

```

Gambar 5.65 Tampilan Hasil Tcpdump dari ping client router 2 ke client router 1

Setelah melihat dari hasil ping antara client dari router 2 ke client router 1 maka hasil selanjutnya dapat dilihat dari router 1 dengan cara ketikkan `Tcpdump -I eth1` pada server VPN router 1 dan hasilnya ialah pada tampilan router 1 terdapat banyak kata ESP pada proses tunneling yang berarti koneksi antara client dari router 2 dan client router 1 terdapat sistem enkripsi pengiriman data melewati router 1 maka sistem VPN site-to-site telah berhasil pada router 1.

2. Ping dari client router 2 ke server router 1

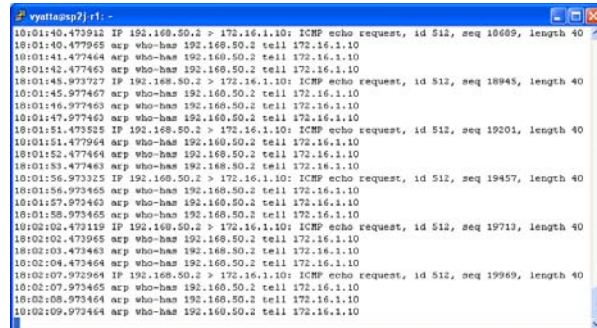
A screenshot of a Windows command prompt window. The title bar reads "C:\WINDOWS\system32\cmd.exe - ping 172.16.1.10 -t". The command prompt shows the command "ping 172.16.1.10 -t" and the output "Pinging 172.16.1.10 with 32 bytes of data:" followed by 12 lines of "Request timed out.".

```
ca C:\WINDOWS\system32\cmd.exe - ping 172.16.1.10 -t
Pinging 172.16.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Gambar 5.66 Tampilan Ping dari client router 2 ke server router 1

Untuk melihat hasil selanjutnya dari router 1 adalah bagaimana jika ping melalui Run Cmd antara client dari router 2 ke server router 1 maka hasilnya Request timed out yang berarti tidak bisa terkoneksi dengan baik karena sistem yang telah dibuat pada router 1 ialah tidak dapat mengakses router 1 karena VPN site-to-site yang berarti network to network antar client dari masing-masing router saja.

Hasil Tcpcdump ping dari client router 2 ke server router 1



```

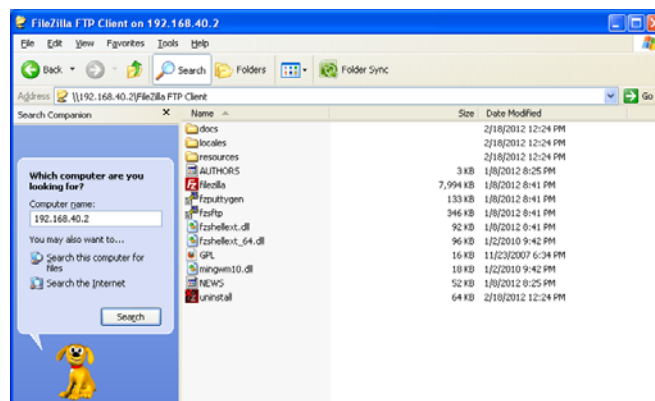
vysitaosp2] r1: -
10:01:40.473512 IP 192.168.50.2 > 172.16.1.10: ICMP echo request, id 512, seq 10689, length 40
10:01:40.477955 arp who-has 192.168.50.2 tell 172.16.1.10
10:01:41.477464 arp who-has 192.168.50.2 tell 172.16.1.10
10:01:42.477463 arp who-has 192.168.50.2 tell 172.16.1.10
10:01:45.973277 IP 192.168.50.2 > 172.16.1.10: ICMP echo request, id 512, seq 10945, length 40
10:01:45.977467 arp who-has 192.168.50.2 tell 172.16.1.10
10:01:46.977463 arp who-has 192.168.50.2 tell 172.16.1.10
10:01:47.977463 arp who-has 192.168.50.2 tell 172.16.1.10
10:01:51.473225 IP 192.168.50.2 > 172.16.1.10: ICMP echo request, id 512, seq 10201, length 40
10:01:51.477964 arp who-has 192.168.50.2 tell 172.16.1.10
10:01:52.477464 arp who-has 192.168.50.2 tell 172.16.1.10
10:01:53.477463 arp who-has 192.168.50.2 tell 172.16.1.10
10:01:56.973225 IP 192.168.50.2 > 172.16.1.10: ICMP echo request, id 512, seq 19457, length 40
10:01:56.973465 arp who-has 192.168.50.2 tell 172.16.1.10
10:01:57.973463 arp who-has 192.168.50.2 tell 172.16.1.10
10:01:58.973465 arp who-has 192.168.50.2 tell 172.16.1.10
10:02:00.472119 IP 192.168.50.2 > 172.16.1.10: ICMP echo request, id 512, seq 19713, length 40
10:02:02.473965 arp who-has 192.168.50.2 tell 172.16.1.10
10:02:03.473463 arp who-has 192.168.50.2 tell 172.16.1.10
10:02:04.473464 arp who-has 192.168.50.2 tell 172.16.1.10
10:02:07.972594 IP 192.168.50.2 > 172.16.1.10: ICMP echo request, id 512, seq 19969, length 40
10:02:08.973464 arp who-has 192.168.50.2 tell 172.16.1.10
10:02:09.973464 arp who-has 192.168.50.2 tell 172.16.1.10

```

Gambar 5.67 Tampilan Hasil Tcpcdump proses ping dari client router 2 ke server router 1

Dan dapat dilihat dari tampilan router 1 tidak terdapat kata-kata ESP yang berarti antara client dari router 2 koneksi atau ping ke router 1 tidak terdapat enkripsi data dan enkripsi data hanya terjadi jika client dari masing-masing router melakukan aktivitas koneksi yang melalui router 1.

3. Mengambil data dari client router 2 ke client router 1



Gambar 5.68 Tampilan Mengambil data dari client router 2 ke client router 1

Dan yang terakhir adalah bagaimana client dari router 2 ingin mengambil sebuah data dari client router 1 melalui search atau bisa langsung ketikkan alamat dari komputer client router 2 yaitu \\192.168.40.2 dan contoh tampilannya seperti di atas.

Hasil Tcpcdump dari proses pengambilan data dari client router 2 ke client router 1

```

vyattaesp2j.r1: -
18:04:48.152142 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xce98690e,seq=0x68f), length 196
18:04:48.152142 IP 192.168.50.2.1105 > 192.168.40.2.microsoft-ds: P 23801:23913(112) ack 215316
win 64390
18:04:48.152953 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xe08a4c20,seq=0x6a9), length 196
18:04:48.153279 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xce98690e,seq=0x690), length 196
18:04:48.153279 IP 192.168.50.2.1105 > 192.168.40.2.microsoft-ds: P 23913:24025(112) ack 215420
win 64286
18:04:48.154210 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xe08a4c20,seq=0x6aa), length 196
18:04:48.326451 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xce98690e,seq=0x691), length 84
18:04:48.326451 IP 192.168.50.2.1105 > 192.168.40.2.microsoft-ds: . ack 215524 win 64182
18:04:51.755060 arp who-has 172.16.1.10 tell 172.16.1.20
18:04:51.755071 arp reply 172.16.1.10 is-at f8:d1:11:05:43:ee (oui Unknown)
18:04:58.107448 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xce98690e,seq=0x692), length 132
18:04:58.107448 IP 192.168.50.2.1105 > 192.168.40.2.microsoft-ds: P 24025:24068(43) ack 215524
win 64182
18:04:58.108211 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xe08a4c20,seq=0x6ab), length 132
18:04:58.108526 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xce98690e,seq=0x693), length 132
18:04:58.108526 IP 192.168.50.2.1105 > 192.168.40.2.microsoft-ds: P 24068:24107(39) ack 215567
win 64139
18:04:58.109585 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xe08a4c20,seq=0x6ac), length 132
18:04:58.169859 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xce98690e,seq=0x694), length 84
18:04:58.169859 IP 192.168.50.2.1105 > 192.168.40.2.microsoft-ds: . ack 215606 win 64100
18:05:03.105464 arp who-has 172.16.1.20 tell 172.16.1.10
18:05:03.105534 arp reply 172.16.1.20 is-at b8:a3:86:98:0a:0b (oui Unknown)

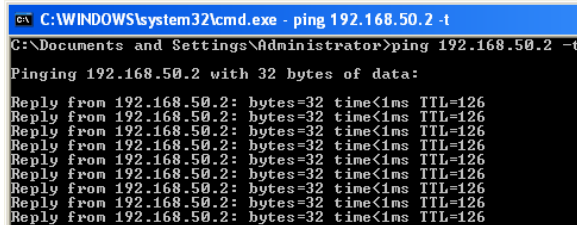
```

Gambar 5.69 Tampilan Hasil Tcpcdump dari proses pengambilan data dari client router 2 ke client router 1

Dan pada tampilan router 1 melalui Tcpcdump adalah terdapat kata ESP dan Microsof yang berarti data yang diambil oleh client router 2 dari client router 1 telah melalui tahap enkripsi data yang dilakukan router 1.

5.1.20 Hasil Koneksi Router 2

1. Ping dari client router 1 ke client router 2



```

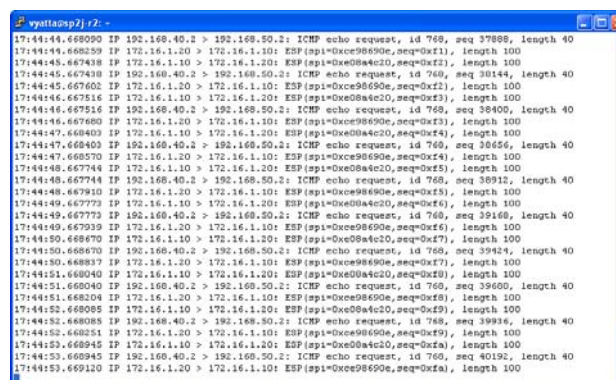
C:\WINDOWS\system32\cmd.exe - ping 192.168.50.2 -t
C:\Documents and Settings\Administrator>ping 192.168.50.2 -t
Pinging 192.168.50.2 with 32 bytes of data:
Reply from 192.168.50.2: bytes=32 time<1ms TTL=126
Reply from 192.168.50.2: bytes=32 time<1ms TTL=126
Reply from 192.168.50.2: bytes=32 time<1ms TTL=126
Reply from 192.168.50.2: bytes=32 time<1ms TTL=126
Reply from 192.168.50.2: bytes=32 time<1ms TTL=126
Reply from 192.168.50.2: bytes=32 time<1ms TTL=126
Reply from 192.168.50.2: bytes=32 time<1ms TTL=126
Reply from 192.168.50.2: bytes=32 time<1ms TTL=126

```

Gambar 5.70 Tampilan Ping dari client router 1 ke client router 2

Sama halnya dengan hasil dari router 1 Setelah semua router berjalan dengan baik, maka tahap selanjutnya membuktikan hasil koneksi antar client dari masing-masing router dan yang pertama ialah bagaimana client dari router 1 ping lewat Run Cmd ke client pada router 2 dan hasilnya Reply from yang berarti antara client dari router 1 dan client router 2 sudah terkoneksi dengan baik.

Hasil Tcpcdump proses ping dari client router 1 ke client router



```

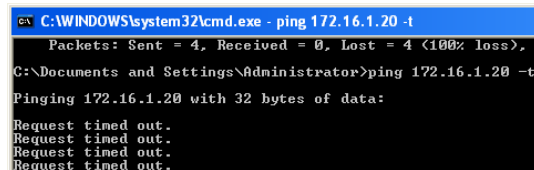
17:44:44.668090 IP 192.168.40.2 > 192.168.50.2: ICMP echo request, id 768, seq 37888, length 40
17:44:44.668239 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf1), length 100
17:44:44.667438 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf2), length 100
17:44:45.667438 IP 192.168.40.2 > 192.168.50.2: ICMP echo request, id 768, seq 38144, length 40
17:44:45.667602 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf2), length 100
17:44:46.667516 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf3), length 100
17:44:46.667516 IP 192.168.40.2 > 192.168.50.2: ICMP echo request, id 768, seq 38400, length 40
17:44:46.667680 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf3), length 100
17:44:47.668403 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf4), length 100
17:44:47.668403 IP 192.168.40.2 > 192.168.50.2: ICMP echo request, id 768, seq 38656, length 40
17:44:47.668570 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf4), length 100
17:44:48.667744 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf5), length 100
17:44:48.667744 IP 192.168.40.2 > 192.168.50.2: ICMP echo request, id 768, seq 38912, length 40
17:44:48.667910 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf5), length 100
17:44:49.667773 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf6), length 100
17:44:49.667773 IP 192.168.40.2 > 192.168.50.2: ICMP echo request, id 768, seq 39168, length 40
17:44:49.667939 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf6), length 100
17:44:50.668670 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf7), length 100
17:44:50.668670 IP 192.168.40.2 > 192.168.50.2: ICMP echo request, id 768, seq 39424, length 40
17:44:50.668837 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf7), length 100
17:44:51.668040 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf8), length 100
17:44:51.668040 IP 192.168.40.2 > 192.168.50.2: ICMP echo request, id 768, seq 39680, length 40
17:44:51.668204 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf8), length 100
17:44:52.668085 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf9), length 100
17:44:52.668085 IP 192.168.40.2 > 192.168.50.2: ICMP echo request, id 768, seq 39936, length 40
17:44:52.668251 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xf9), length 100
17:44:53.668945 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xfa), length 100
17:44:53.668945 IP 192.168.40.2 > 192.168.50.2: ICMP echo request, id 768, seq 40192, length 40
17:44:53.669110 IP 192.16.1.10 > 172.16.1.10: ESP (spi=0xcce98690e,seq=0xfa), length 100

```

Gambar 5.71 Tampilan Hasil Tcpcdump dari ping client router 1 ke client router 2

Setelah melihat dari hasil ping antara client dari router 1 ke client router 2 maka hasil selanjutnya dapat dilihat dari router 1 dengan jika pada server VPN router 1 memakai eth1 maka pada server router 2 memakai eth0 cara ketikan `Tcpdump -I eth0` dan hasilnya ialah pada tampilan router 2 terdapat banyak kata ESP pada proses tunneling yang berarti koneksi antara client dari router 1 dan client router 2 terdapat sistem enkripsi pengiriman data melewati router 2 maka sistem VPN site-to-site telah berhasil pada router 2.

2. Ping dari client router 1 ke server router 2

A screenshot of a Windows command prompt window. The title bar reads "C:\WINDOWS\system32\cmd.exe - ping 172.16.1.20 -t". The command prompt shows the following text:

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
C:\Documents and Settings\Administrator>ping 172.16.1.20 -t  
Pinging 172.16.1.20 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.
```

Gambar 5.72 Tampilan Ping dari client router 1 ke server router 2

Untuk melihat hasil selanjutnya dari router 2 adalah bagaimana jika ping melalui Run Cmd antara client dari router 1 ke server router 2 maka hasilnya Request timed out yang berarti tidak bisa terkoneksi dengan baik karena sistem yang telah dibuat pada router 2 ialah tidak dapat mengakses router 1 karena VPN site-to-site yang berarti network to network antar client dari masing-masing router saja.

Hasil Tcpcdump proses ping dari client router 1 ke server router 2

```

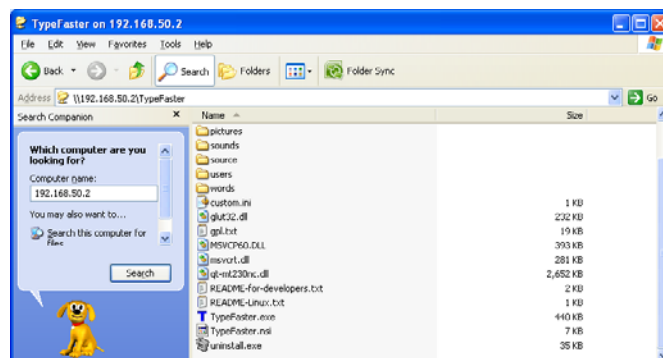
vyatta@sp2j:r2: -
17:46:22.793755 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:23.789759 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:24.789758 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:28.206655 IP 192.168.40.2 > 172.16.1.20: ICMP echo request, id 768, seq 52224, length 40
17:46:28.290250 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:29.289759 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:30.289760 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:33.787201 IP 192.168.40.2 > 172.16.1.20: ICMP echo request, id 768, seq 52400, length 40
17:46:33.790261 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:34.789759 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:35.789759 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:39.287717 IP 192.168.40.2 > 172.16.1.20: ICMP echo request, id 768, seq 52736, length 40
17:46:39.290255 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:40.289759 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:41.289759 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:44.788540 IP 192.168.40.2 > 172.16.1.20: ICMP echo request, id 768, seq 52992, length 40
17:46:44.789761 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:45.789759 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:46.789758 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:50.288556 IP 192.168.40.2 > 172.16.1.20: ICMP echo request, id 768, seq 53248, length 40
17:46:50.290256 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:51.289759 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:52.289759 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:55.789302 IP 192.168.40.2 > 172.16.1.20: ICMP echo request, id 768, seq 53504, length 40
17:46:55.789760 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:56.789759 arp who-has 192.168.40.2 tell 172.16.1.20
17:46:57.789759 arp who-has 192.168.40.2 tell 172.16.1.20
17:47:01.289842 IP 192.168.40.2 > 172.16.1.20: ICMP echo request, id 768, seq 53760, length 40
17:47:01.294258 arp who-has 192.168.40.2 tell 172.16.1.20

```

Gambar 5.73 Tampilan Hasil Tcpcdump proses ping dari client router 1 ke server router 2

Dan dapat dilihat dari tampilan router 2 tidak terdapat kata-kata ESP yang berarti antara client dari router 1 koneksi atau ping ke router 2 tidak terdapat enkripsi data dan enkripsi data hanya terjadi jika client dari masing-masing router melakukan aktivitas koneksi yang melalui router 2.

3. Mengambil data dari client router 1 ke client router 2



Gambar 5.74 Tampilan Mengambil data dari client router 1 ke client router 2

Dan yang terakhir adalah bagaimana client dari router 1 ingin mengambil sebuah data dari client router 2 melalui search atau bisa langsung ketikkan alamat dari komputer client router 1 yaitu \\192.168.50.2 dan contoh tampilannya seperti di atas.

Hasil Tcpcdump dari proses pengambilan data dari client router 1 ke client router 2

```

vyatta@sp2j:~$ -
17:53:11.538864 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xae98690e,seq=0x489), length 132
17:53:11.575565 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xae084c20,seq=0x46e), length 196
17:53:11.575565 IP 192.168.40.2.1045 > 192.168.50.2.microsoft-ds: P 5526:5630(104) ack 19122 win 65279
17:53:11.576023 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xae98690e,seq=0x48a), length 220
17:53:11.576642 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xae084c20,seq=0x470), length 220
17:53:11.576642 IP 192.168.40.2.1045 > 192.168.50.2.microsoft-ds: P 5630:5770(140) ack 19261 win 65140
17:53:11.576824 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xae98690e,seq=0x48b), length 132
17:53:11.577276 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xae084c20,seq=0x471), length 148
17:53:11.577276 IP 192.168.40.2.1045 > 192.168.50.2.microsoft-ds: F 5770:5833(83) ack 19312 win 65089
17:53:11.577452 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xae98690e,seq=0x48c), length 212
17:53:11.578122 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xae084c20,seq=0x472), length 292
17:53:11.578122 IP 192.168.40.2.1045 > 192.168.50.2.microsoft-ds: P 5033:6033(200) ack 19444 win 64957
17:53:11.578722 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xae98690e,seq=0x48d), length 244
17:53:11.579270 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xae084c20,seq=0x473), length 132
17:53:11.579270 IP 192.168.40.2.1045 > 192.168.50.2.microsoft-ds: F 6033:6070(45) ack 19604 win 64797
17:53:11.579460 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xae98690e,seq=0x48e), length 132
17:53:11.765934 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xae98690e,seq=0x48f), length 132
17:53:11.766238 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xae084c20,seq=0x474), length 84
17:53:11.766238 IP 192.168.40.2.1045 > 192.168.50.2.microsoft-ds: . ack 19643 win 64758
17:53:15.053758 arp who-has 172.16.1.10 tell 172.16.1.20
17:53:15.053832 arp reply 172.16.1.10 is-at f8:d1:11:05:43:ee (oui Unknown)
17:53:15.967095 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xae084c20,seq=0x475), length 132
17:53:15.967095 IP 192.168.40.2.1045 > 192.168.50.2.microsoft-ds: P 6070:6121(43) ack 19643 win 64758
17:53:15.967366 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xae98690e,seq=0x490), length 132
17:53:15.967701 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xae084c20,seq=0x476), length 132
17:53:15.967701 IP 192.168.40.2.1045 > 192.168.50.2.microsoft-ds: F 6121:6160(39) ack 19686 win 64715
17:53:15.967858 IP 172.16.1.20 > 172.16.1.10: ESP (spi=0xae98690e,seq=0x491), length 132
17:53:16.154232 IP 172.16.1.10 > 172.16.1.20: ESP (spi=0xae084c20,seq=0x477), length 84
17:53:16.154232 IP 192.168.40.2.1045 > 192.168.50.2.microsoft-ds: . ack 19725 win 64676

```

Gambar 5.75 Tampilan Hasil Tcpcdump dari proses pengambilan data dari client router 1 ke client router 2

Dan pada tampilan router 2 melalui Tcpcdump adalah terdapat kata ESP dan Microsoft yang berarti data yang diambil oleh client router 1 dari client router 2 telah melalui tahap enkripsi data yang dilakukan router 2

BAB VI

SIMPULAN DAN SARAN

6.1 Simpulan

Berdasarkan hasil analisis dan pembahasan yang dilakukan peneliti, dapat diambil kesimpulan bahwa telah dibangun *site to site VPN Server* dengan pengamanan protokol *IPSec* yang menggunakan sistem operasi *vyatta* yang berguna sebagai jalur network global antara PT. Sarana Pembangunan Palembang Jaya (SP2J) sebagai perusahaan induk dan Unit Usaha BRT Trans Musi sebagai anak perusahaan.

Konfigurasi pengamanan protokol *IPsec* ini bertujuan membangun sebuah terowongan jaringan rahasia antar perusahaan sebagai guna pengamana paket pengiriman dari masing-masing perusahaan.

6.2 Saran

Dari penelitian ini penulis memberikan saran untuk perkembangan *VPN Server* antara kantor PT. Sarana Pembangunan Palembang Jaya dan kantor Unit Usaha BRT Trans Musi yaitu :

1. Diharapkan pengembangan *site to site VPN server* ini berkelanjutan agar dapat melakukan pertukaran data antara kantor pusat dan kantor cabang dapat bekerja lebih

maksimal tanpa ada kendala yang dapat menghambat pekerjaan.

2. Untuk keamanan yang lebih maksimal sebaiknya pada komputer VPN server pada masing-masing kantor ini ditambahkan sebuah password yang rahasia karena pada pembuatan VPN server masih menggunakan password *default*.
3. Demi memudahkan pertukaran data maka sistem DNS yang telah ada pada masing-masing kantor dapat digandengkan atau disatukan dengan VPN server karena dengan dibantunya dengan sistem DNS menghindari kesalahan atau kelupaan *ip* pada komputer yang akan melakukan pengiriman dan pengambilan data.
4. Karena sistem VPN server ini adalah sistem yang dilakukan melalui *ip public* maka masing-masing kantor harus menambahkan *resource bandwidth* yang lebih besar dari sebelumnya untuk memaksimalkan kerja dari VPN server ini.

DAFTAR PUSTAKA

- Administrator, 2006. *Pengantar Cisco Router*, ilmukomputer.org (Online), (<http://ilmukomputer.org/2006/08/25/pengantar-cisco-router/>), diakses 27 juli 2012
- Administrator, 2008. *IPSec Vpn Pada Cisco Router*, ilmukomputer.org (Online), (<http://ilmukomputer.org/2008/05/28/ipsec-vpn-pada-cisco-router/>), diakses 27 juli 2012
- Departemen Pendidikan Nasional, 2008. *Kamus Besar Bahasa Indonesia Pusat Bahasa*, PT. Gramedia Pustaka Utama, : Jakarta
- Deris Stiawan, Dian Palupi Dini, 2009. *Optimalisasi Interkoneksi Virtual Private Network (Vpn) Dengan Menggunakan Hardware Based dan Lix (Indonesia Internet Exchange) Sebagai Alternatif Jaringan Skala Luas (Wan)*, (<http://eprints.unsri.ac.id/89/1/7.pdf>), diakses 29 juli 2012
- Rachman, Oscar, 2011. *Teknologi, Konsep, Konfigurasi dan Troubleshooting Router*, Informatika, : Bandung
- Rijal Fadilah, Djumhadi, 2009. *Penggunaan Teknologi Komunikasi Data Berbasis VPN-IP MPLS Untuk Pemilihan Umum*, (http://repository.upnyk.ac.id/251/1/C-9_VPNIP_RIJAL.pdf), diakses 29 juli 2012
- Setiawan, Agung. 2007. *Pengantar Sistem Komputer*, Informatika, : Bandung
- Stiawan, Deris, 2005. *Sistem Keamanan Komputer*, Elex Media Komputindo, : Jakarta
- Sofana, Iwan, 2008. *Membangun Jaringan Komputer Membuat Jaringan Komputer (Wire & Wireless) untuk Pengguna Windows dan Linux*, Informatika, : Bandung

Sopandi, Dede, 2008. *Instalasi dan Konfigurasi Jaringan Komputer*,
Informatika, : Bandung

Suarna, Nana, 2007, *Pengantar Jaringan*, Yrama Widya, : Bandung

Suarna, Nana, 2007, *Pengantar LAN (Local Area Network)*, Yrama Widya, :
Bandung

http://www.vyatta.com/download/trial_software/VyattaCore
diakses 15 juni 2012

